MODUL
GURU PEMBELAJAR

Paket Keahlian

TEKNIK KOMPUTER DAN JARINGAN

(SMK)

"Sistem Keamanan Jaringan Komputer"

dan

PEDAGOGIK

"Penilaian dan Evaluasi Pembelajaran"

Kelompok Kompetensi H

Direktorat Jenderal Guru dan Tenaga Kependidikan
Kementerian Pendidikan dan Kebudayaan
Tahun 2016

MODUL
GURU PEMBELAJAR

PAKET KEAHLIAN
PEDAGOGIK

Kelompok Kompetensi H

Penulis : Nasrah Natsir, S.Pd., M.Pd

Direktorat Jenderal Guru dan Tenaga Kependidikan
Kementrian Pendidikan dan Kebudayaan
Tahun 2016

HALAMAN PERANCIS

Penulis :

Nasrah Natsir, M.Pd, 085242642377, nasrah.natsir@gmail.com

Layouter:

1. Abd. Hakim, S.Kom.,M.T
(Email: abdhakimx@gmail.com ; Telp: 085256372755)

Ilustrator :

1. Faizal Reza Nurzeha, Amd
(Email : faizalrezanurzeha@gmail.com ; Telp: 085242177945)

KATA SAMBUTAN

Peran guru profesional dalam proses pembelajaran sangat penting sebagai kunci keberhasilan belajar siswa. Guru profesional adalah guru yang kopeten membangun proses pembelajaran yang baik sehingga dapat menghasilkan pendidikan yang berkualitas. Hal ini tersebut menjadikan guru sebagai komponen yang menjadi fokus perhatian pemerintah pusat maupun pemerintah daerah dalam peningkatan mutu pendidikan terutama menyangkut kopetensi guru.

Pengembangan profesionalitas guru melalui program Guru Pembelajar (GP) merupakan upaya peningkatan kompetensi untuk semua guru. Sejalan dengan hal tersebut, pemetaan kopetensi guru telah dilakukan melalui uji kompetensi guru (UKG) untuk kompetensi pedagogik dan profesional pada akhir tahun 2015. Hasil UKG menunjukanpeta kekuatan dan kelemahan kompetensi guru dalam penguasaan pengetahuan. Peta kompetensi guru tersebut dikelompokan menjadi 10 (sepuluh) kelopok kompetensi. Tindak lanjut pelaksanaan UKG diwujudkan dalam bentuk pelatihan guru paska UKG melalui program Guru Pembelajar.Tujuannya untuk meningkatkan kompetensi guru sebagai agen perubahaan dan sumber belajar utama bagi peserta didik. Program Guru Pembelajar dilaksanakan melalui pola tatap muka, daring (*online*) dan campuran (*blended*) tatap muka dengan *online*.

Pusat Pengembangan dan Pemberdayaan Pendidik dan Tenag Kependidikan (PPPPTK), Lembaga Pengembangan dan Pemberdayaan Pendidik dan Tenaga Kependidikan Kelautan Perikanan Teknologi Informasi dan Komunikasi (LP3TK KPTK) dan Lembaga Pengembangan dan Pemberayaan Kepala Sekolah (LP2KS) merupakan Unit Pelaksana Teknis di lingkungan Direktorat Jendral Guru dan Tenaga Kependidikan yang bertanggung jawab dalam mengembangkan perangkat dan melaksanakan peningkaan kompetensi guru sesuai dengan bidangnya. Adapun peragkat pembelajaran yang dikembangkan tersebut adalah modul untuk program Guru Pembelajar (GP) tatap muka dan GP *online* untuk semua mata pelajaran dan kelompok kompetensi. Dengan modul ini diharapkan program GP memberikan sumbangan yang sangat besar dalam peningkatan kualitas kompetensi guru.Mari kita sukseskan program GP ini untuk mewujudkan Guru Mulia Karena Karya.

Jakarta, Februari 2016
Direktur Jendral
Guru dan Tenaga Kependidikan

Sumarna Surapranata, Ph.D
NIP. 195908011985031002

KATA PENGANTAR

Profesi guru dan tenaga kependidikan harus dihargai dan dikembangkan sebagai profesi yang bermartabat sebagaimana diamanatkan Undang-Undang Nomor 14 Tahun 2005 tentang Guru dan Dosen. Hal ini dikarenakan guru dan tenaga kependidikan merupakan tenaga profesional yang mempunyai fungsi, peran, dan kedudukan yang sangat penting dalam mencapai visi pendidikan 2025 yaitu “Menciptakan Insan Indonesia Cerdas dan Kompetitif”. Untuk itu guru dan tenaga kependidikan yang profesional wajib melakukan pengembangan keprofesian berkelanjutan.

Buku pedoman Pedoman Penyusunan Modul Diklat Pengembangan Keprofesian Berkelanjutan Bagi Guru dan Tenaga Kependidikan untuk institusi penyelenggara program pengembangan keprofesian berkelanjutan merupakan petunjuk bagi penyelenggara pelatihan di dalam melaksakan pengembangan modul yang merupakan salah satu sumber belajar bagi guru dan tenaga kependidikan. Buku ini disajikan untuk memberikan informasi tentang penyusunan modul sebagai salah satu bentuk bahan dalam kegiatan pengembangan keprofesian berkelanjutan bagi guru dan tenaga kependidikan.

Pada kesempatan ini disampaikan ucapan terima kasih dan penghargaan kepada berbagai pihak yang telah memberikan kontribusi secara maksimal dalam mewujudkan buku ini, mudah-mudahan buku ini dapat menjadi acuan dan sumber inspirasi bagi guru dan semua pihak yang terlibat dalam pelaksanaan penyusunan modul untuk pengembangan keprofesian berkelanjutan. Kritik dan saran yang membangun sangat diharapkan untuk menyempurnakan buku ini di masa mendatang.

Makassar,Februari 2016
Kepala LPPPTK KPTK Gowa
Sulawesi Selatan,

Dr. H. Rusdi, M.Pd,
NIP 19650430 1991 93 1004

DAFTAR ISI

BAB IPENDAHULUAN

A. Latar Belakang

Remedial dan pengayaanmerupakan komponen penting dalam penyelenggaraan pendidikan.Upaya meningkatkan kualitas pendidikan dapat ditempuh melalui peningkatan kualitas pembelajaran dan kualitas sistem penilaiannya.Keduanya saling terkait, sistem pembelajaran yang baik akan menghasilkan kualitas belajar yang baik. Kualitas pembelajaran ini dapat dilihat dari hasil penentuanmetode pembelajaran dan penilaiannya. Selanjutnya sistem metode pembelajaran yang tepat akan berimplikasi pada penentuan penilaian yang tepat pula untuk mememperoleh hasil belajar yang baik pula. Oleh karena itu, dalam upaya peningkatan kualitas pendidikan diperlukan perbaikan sistem pembelajaran dan penilaian yang diterapkan. Diharapkan dengan perbaikan sistempembelajaran dan penilaian maka amanat Undang-Undang Sistem Pendidikan Nasional Tahun 2003 pasal 58 ayat (1) bahwa ”evaluasi hasil belajar peserta didik dilakukan oleh pendidik untuk memantau proses, kemajuan, dan perbaikan hasil belajar peserta didik secara berkesinambungan” dapat diwujudkan.

Peranan remedial dan pengayaan dalam pendidikan yang diawali dengan pemaparan tentang teoriremedial dan pengayaan dalam pembelajaran termasuk di dalamnya standar pembelajaran.Dalam konteks perbaikan dan peningkatan kualitas pendidikan melalui peningkatan kualitas sistem penilaian, maka peranan guru, siswa, dan sekolah menjadi sesuatu yang sangat diharapkan. Bagaimana kedudukan ketiga komponen tersebut dibahas secara tuntas dan gamblang sehingga siswa sebagai subjek dan sekaligus sebagai objek dalam proses pendidikan menjadi pebelajar yang yang lebih baik dan termotivasi untuk terus belajar. Karakteristik dan jenis-jenis penilaian kelas yang memungkinkan untuk diterapkan dalam konteks nyata di dalam kelas disajikan dalam bahasa yang mudah, komunikatif, dan sederhana.

Modul ini merupakan salah satu media yang berusaha untuk menjelaskan secara tuntas dan aplikatif tentang pengayaan dan remedial.Selaian itu, modul ini juga merupakan perpaduan antara contoh praktik dalam kelas yang dilakukan

oleh guru dengan hasil penelitian oleh para dosen yang konsen terhadap pengayaan dan remedial, sehingga menarik dan mudah untuk diterapkan dalam situasi nyata dalam kelas.

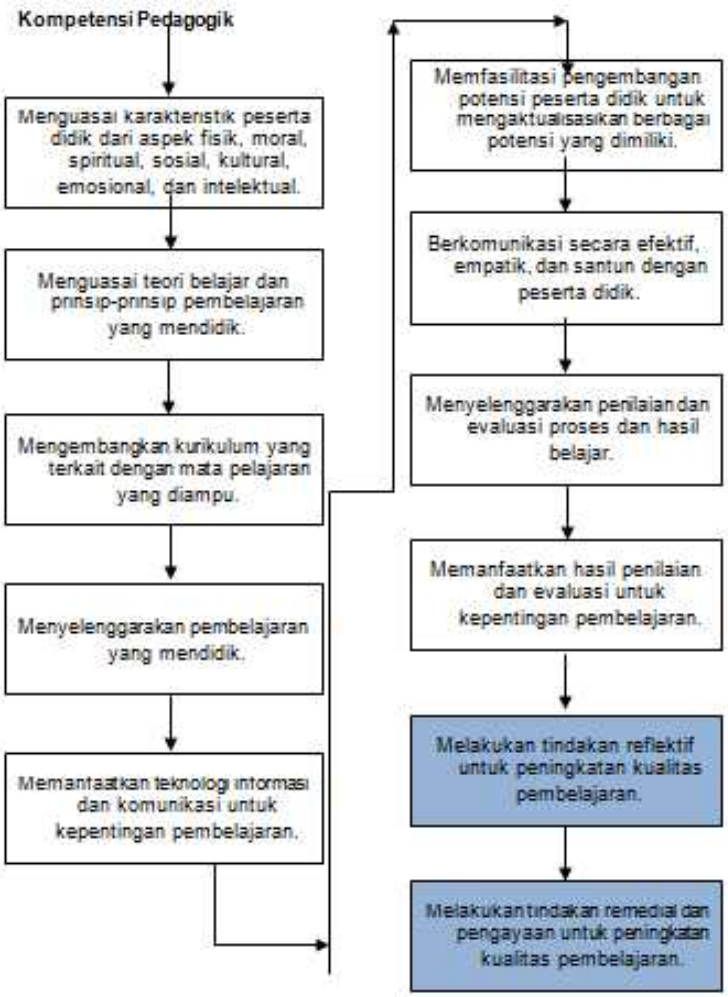
B. Tujuan

Setelah Anda mengikuti pelatihan ini, Anda diharapkan dapat memenuhi kebutuhan berikut:

1. Mampu menyelenggarakan remedial dan pengayaanproses dan hasil belajar siswa.
2. Mampu memanfaatkanremedial dan pengayaanuntuk kepentingan pembelajaran.

C. Peta Kompetensi

Standar Kompetensi Guru Mata Pelajaran di SD/MI, SMP/MTs, SMA/MA, dan SMK/MAK*


Kompetensi Pedagogik
Menguasai karakterstik peserta didik dari aspek fisik, moral, spiritual, sosial, kultural, emosional, dan intelektual.
Menguasai teori belajar dan prinsip-prinsip pembelajaran yang mendidik.
Mengembangkan kurikulum yang terkait dengan mata pelajaran yang diampu.
Menyelenggarakan pembelajaran yang mendidik.
Memanfaatkan teknologi informasi dan komunikasi untuk kepentingan pembelajaran.
Memfasilitasi pengembangan potensi peserta didik untuk mengaktualisasikan berbagai potensi yang dimiliki.
Berkomunikasi secara efektif, empatik, dan santun dengan peserta didik.
Menyelenggarakan penilaian dan evaluasi proses dan hasil belajar.
Memanfaatkan hasil penilaian dan evaluasi untuk kepentingan pembelajaran.
Melakukan tindakan reflektif untuk peningkatan kualitas pembelajaran.
Melakukan tindakan remedial dan pengayaan untuk peningkatan kualitas pembelajaran.

D. Saran Cara Penggunaan Modul

Modul ini diarahkan untuk memahami secara sistematis remedial dan pegayaan pembelajaran. Modul ini terdiri dari 4 (enam) pembelajaran yang memuat materi remedial dan pengayaan. Untuk memudahkan Anda mempelajari modul ini berikut gambaran singkat pembelajaran yang disajikan dalam modul ini:

1. Kegiatan Pembelajaran I

   Kegiatan Pembelajaran I memuat konsep dasar kegiatan remedial danpengayaan pada kegiatan pembelajaran ini disajikan secara runtut (1) Menjelaskan pengertian kegiatan remedial, (2) Menganalisis jenis-jenis kegiatan remedial, (3) Menjelaskan pengertian kegiatan pengayaan, (4) Menjelaskan hakikat kegiatan pengayaan, (5) Menjelaskan bentuk-bentuk kegiatan pengayaan, dan (6) Menjelaskan faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan pengayaan.

2. Kegiatan Pembelajaran II

   Kegiatan Pembelajaran II memuat prosedur remedial dan pengayaan**.** Pada kegiatan pembelajaran ini disajikan secara runtut prosedur (1) Menjelaskan prosedur pengajaran remedial, dan (2) Menjelaskan langkah-langkah pelaksanaan pengajaran pengayaan.

3. Kegiatan Pembelajaran III

   Kegiatan Pembelajaran III memuat strategi remedial dan pengayaan. Pada kegiatan pembelajaran ini disajikan secara runtut (1) Menjelaskan strategi yang dipergunakan dalam pelaksanaan pengajaran remedial, (2) Membedakan strategi pengajaran remedial dari strategi pembelajaran biasa, (3) Menganalisis strategipengajaran remedial,

Anda dapat mempelajari keseluruhan modul ini secara berurutan untuk memberi kemudahan. Anda tidak dituntut untuk memahami dan menguasai bagian demi bagian dalam modul ini untuk memberi kemudahan yang lain karena masing-masing aktivitas pembelajaran disajikan secara runtut dan saling berkaitan. Setiap bagian aktivitas pembelajaran dilengkapi dengan contoh soal sebagai bahan latihan. Jika menemukan masalah atau sedikit kesulitan dalam menggunakan modul ini, maka Anda dapat mendiskusikan dengan rekan atau peserta yang lain

1

KEGIATAN PEMBELAJARAN

Kegiatan Pembelajaran I

Konsep Dasar Kegiatan Remedial dan Pengayaan

A. Tujuan

1. Peserta diklat diharapkan mampu menjelaskan pengertian kegiatan remedial
2. Perserta diklat diharapkan mampu menganalisis jenis-jenis kegiatan remedial
3. Peserta diklat diharapkan mampu menjelaskan pengertian kegiatan pengayaan
4. Peserta diklat diharapkan mampu menjelaskan hakikat kegiatan pengayaan
5. Peserta diklat diharapkan mampu menjelaskan bentuk-bentuk kegiatan pengayaan
6. Peserta didik diharapkan mampu menjelaskan faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan pengayaan

B. Indikator Pencapaian Kompetensi

1. Menjelaskan pengertian kegiatan remedial
2. Menganalisis jenis-jenis kegiatan remedial
3. Menjelaskan pengertian kegiatan pengayaan
4. Menjelaskan hakikat kegiatan pengayaan
5. Menjelaskan bentuk-bentuk kegiatan pengayaan
6. Menjelaskan faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan pengayaan

C. Uraian Materi

1. Kegiatan Remedial

a. Hakikat Kegiatan Remedial (perbaikan)

Remedial merupakan suatu treatmen atau bantuan untuk mengatasi kesulitan belajar.Ditinjau dari arti kata, “remedial” berarti “sesuatu yang berhubungan dengan perbaikan”.Dengan demikian pengajaran remedial, adalah suatu bentuk pengajaran yang bersifat penyembuhan atau bersifat perbaikan. Menurut Priyatno remedial

merupakan suatu bentuk bantuan yang diberikan kepada seseorang atau sekelompok siswa yang menghadapi masalah belajar dengan maksud memperbaiki kesalahan-kesalahan dalam proses dan hasil belajar mereka.

Remedial diartikan sebagai kegiatan yang dilaksanakan untuk membetulkan kekeliruan yang dilakukan siswa.Kalau dikaitkan dengan kegiatan pembelajaran, kegiatan remediasi dapat diartikan sebagai suatu kegiatan yang dilaksanakan untuk memperbaiki kegiatan pembelajaran yang kurang berhasil.Kekurangberhasilan pembelajaran ini biasanya ditunjukkan oleh ketidakberhasilan siswa dalam menguasai kompetensi yang diharapkan dalam pembelajaran.Remedial atau perbaikan diberikan kepada peserta didik yang belum tuntas belajar atau belum mencapai SKBM (Standar Ketuntasan Belajar Minimal) setelah mengikuti tes kompetensi dasar tertentu, ujian blok, atau ujian semester. Program remedial ini dilakukan dua kali, sehingga bila peserta didik sudah melaksanakan remedial atau perbaikan sebanyak dua kali namun nilainya belum mencapai SKBM maka penanganannya harus melibatkan orang tua peserta didik dengan melibatkan pihak Bimbingan dan Konseling untuk mengetahui kemungkinan sebab lain dari kelambanan peserta didik tersebut. Sifat pokok kegiatan pembelajaran remedial ada tiga yaitu: (1) menyederhanakan konsep yang komplek (2) menjelaskan konsep yang kabur (3) memperbaiki konsep yang salah tafsir. Beberapa perlakuan yang dapat diberikan terhadap sifat pokok remedial tersebut antara lain berupa: penjelasan oleh guru, pemberian rangkuman, dan *advance organizer*, pemberian tugas dan lain-lain.

Proses pengajaran remedial ini sifatnya lebih khusus karena disesuaikan dengan karakteristik kesulitan belajar yang dihadapi murid. Proses bantuan lebih ditekankan pada usaha perbaikan cara mengajar, menyesuaikan materi pelajaran, arah belajar dan menyembuhkan hambatan-hambatan yang dihadapi. Jadi dalam pengajaran remedial yang diperbaiki atau yang disembuhkan adalah keseluruhan proses belajar mengajar yang meliputi metode mengajar,

penguasaan materi pelajaran, cara belajar, alat belajar dan lingkunagn turut mempengaruhi proses belajar mengajar. Tidak sedikit dalam proses pembelajaran remedial guru dituntut lebih bersabar, jangan bosan untuk mengulang-ulang, serta lebih runut pembelajaran itu disampaikan dengan suara dan intonasi yang jelas dan lugas. Melalui pengajaran remedial, murid yang mengalami kesulitan belajar dapat diperbaiki atau disembuhkan sehingga dapat mencapai hasil yang diharapkan sesuai dengan kemampuan.Kesulitan belajar yang dihadapi murid mungkin beberapa mata pelajaran atau satu mata pelajaran atau satu kemampuan khusus dari mata pelajaran tertentu.Penyembuhan ini mungkin mencakup sebagian aspek kepribadian atau sebagian kecil saja. Demikian pula proses penyembuhan, ada yang dalam jangka waktu lama atau dalam waktu singkat. Hal ini tergantung pada sifat, jenis dan latarbelakang kesulitan belajar yang dihadapi murid.

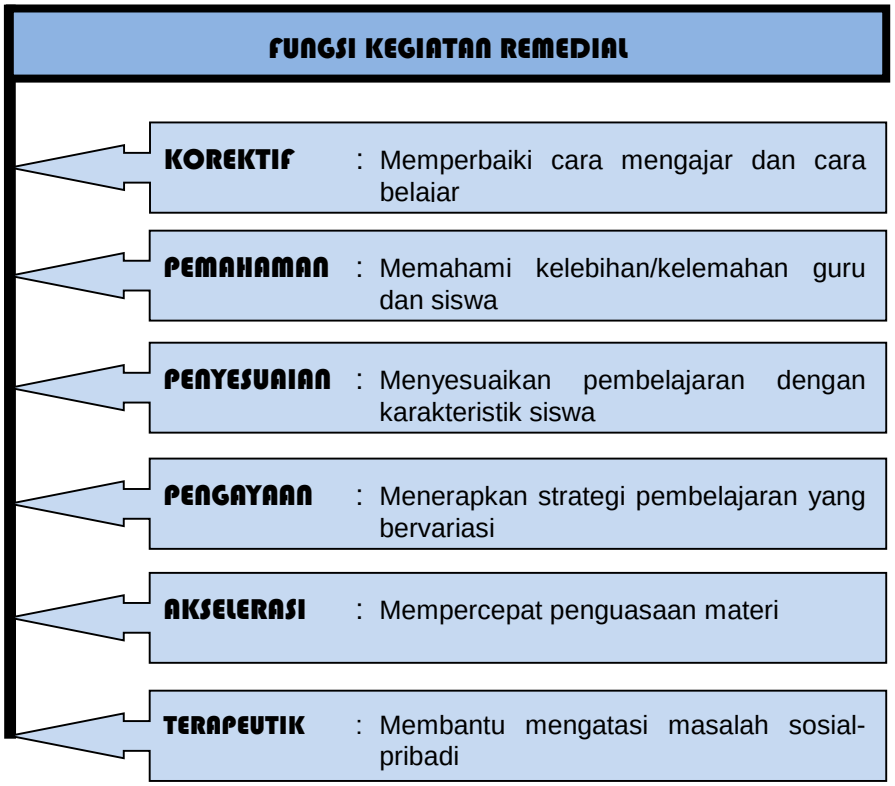
Dari pengertian di atas diketahui bahwa suatu kegiatan pembelajaran dianggap sebagai kegiatan remediasi apabila kegiatan pembelajaran tersebut ditujukan untuk membantu siswa yang mengalami kesulitan dalam memahami materi pelajaran.

b. Tujuan dan fungsi kegiatan remedial

Secara umum, kegiatanremedial adalah yang aktivitas membantu siswa untuk mencapai standar kompetensi yang telah ditetapkan berdasarkan kurikulum. Sedangkan tujuan khusus dari remedial adalahmembantu peserta didik yang kesulitan dalam menguasai materi pembelajaran melalui kegiatan pembelajaran tambahan dan diusahakan agar proses pembelajaran tersebutberlangsung secara interaktif, inspiratif, menyenangkan, menantang, dan memotivasi peserta didik untuk berpartisipasi aktif, serta memberikan kesempatan yang cukup bagi prakarsa, kreativitas, dan kemandirian sesuai dengan bakat, minat, dan perkembangan fisik serta psikologis peserta didik.

Sebagai salah satu cara dalam membantu siswa yang gagal menguasai kompetensi yang telah ditargetkan, kegiatan remedial memiliki beberapa fungsi yang penting bagi keseluruhan proses

pembelajaran. Warkitri, dkk (1991) menyebutkan enam fungsi kegiatan remedial dalam proses pembelajaran. Keenam fungsi kegiatan remedial tersebut adalah fungsi korektif, pemahaman, penyesuaian, pengayaan, akselerasi, dan terapeutik.



Gambar 1.1 Fungsi Kegiatan remedial
Sumber : Warkitri, dkk (1991)

Untuk lebih jelasnya marilah kita bahas satu per satu dari keenam fungsi kegiatan remedial tersebut.

a) *Fungsi Korektif*

Fungsi korektif ini adalah usaha untuk memperbaiki atau meninjau kembali sesuatu yang dianggap kurang maupun keliru dalam proses pembelajaran. Pembelajaran remedial mempunyai fungsi korektif karena pembelajaran ini dilakukan dalam rangka perbaikan dalam proses pembelajaran.

b) *Fungsi pemahaman*

Kegiatan remedial mempunyai fungsi pemahaman karena dalam kegiatan pemahaman ini akan terjadi proses pemahaman baik pada diri guru maupun pada diri siswa.

Fungsi pemahaman dalam kegiatan remedial dimaksudkan agar guru berusaha untuk membantu peserta didik untuk memahami dirinya dalam hal jenis dan sifat kesulitan yang dialami, serta kelebihan dan kelemahan yang dimiliki.

c) *Fungsi penyesuaian*

Kegiatan remedial juga memiliki fungsi penyesuain karena pelaksanaan remedial disesuaikan dengan kesulitan dan karakteristik individu siswa yang mengalami kesulitan belajar.Artinya bahwa kegiatan ini membantu siswa untuk belajar sesuai dengan keadaan dan kemampuan yang dimilikinya sehingga siswa tidak menjadikannya sebagai beban.

Tuntutan belajar yang diberikankepada murid telah disesuaikan dengan sifat jenis dan latar belakang kesulitannya sehingga murid diharapkan lebih terdorong untuk belajar.Karena semua aspek kegiatan remedial disesuaikan dengan kekuatan dan karakteristik individu siswa, maka siswa menjadi lebih semangat dan termotivasi untuk belajar lebih giat lagi sehingga memberikan peluang bagi siswa untuk memperoleh prestasi yang lebih baik.

d) *Fungsi pengayaan (enrichment)*

Kegiatan remedial juga memiliki fungsi pengayaan dalam prosesnya karena melalui kegiatan remedial guru memanfaatkan sumber belajar, metode atau alat bantu pembelajaran yang lebih variatif dari proses pembelajaran biasa pada umumnyauntuk meningkatkan hasil belajar yang lebih optimal.Kalau layanan pengulangan dan perbaikan ditujukan kepada siswa yang mempunyai kelemahan yang sangat mendasar, maka layanan pengayaan ini ditujukan pada siswa yang mempunyai kelemahan yang ringan, yang hakikatnya masih dapat meningkatkan diri hasil-hasil belajarnya lebih optimal.

e) *Fungsi akselerasi*

Fungsi akselerasi yang ada pada kegiatan remedial merupakan usaha guru untuk mempercepat pelaksanaan proses dan hasil pembelajaran, dalam arti meningkatkan efisiensi dan

efektivitas pembelajaran. Dengan memeberikan kesempatan belajar yang lebih efektif dan efisien tersebut, guru dalam semester yang sama mapu memberikan layanan pembelajaran baik regular maupun tambahan, tanpa menambah waktu ke semester berikutnya.

f) Kegiatan terapeutik

Kegiatan remedial juga mempunyai fungsi terapeutik karena artinya dalam proses pengajaran remedial secara langsung atau tidak langsung juga menyembuhkan beberapa gangguan atau hambatan kepribadian yang berkaitan dengan kesulitan belajar. Dalamkegiatan remedial, guru dapat membantu mengatasi kesulitan siwa dalam aspek sosial-pribadi. Biasanya siswa yang kesulitan atau kurang berhasil dalam proses belajar sering merasa rendah diri atau terisolasi dalam pergaulan sosial disekolahnya.

2. Jenis-Jenis Kegiatan Remedial

Sukiman (2012) menjelaskan bahwa pemberian remedial didasarkan atas latar belakang bahwa pendidik perlu memperhatikan perbedaan individual peserta didik.Dengan diberikannya pembelajaran remedial bagi peserta didik yang belum mencapai tingkat ketuntasan belajar, maka peserta didik ini memerlukan waktu lebih lama dari pada mereka yang telah mencapai tingkat penguasaan.Setelah diketahui kesulitan yang dihadapi siswa, langkah berikutnya adalah memberikan perlakuan berupa pembelajaran remedial.

Menurut buku Panduan Penyelenggaraan Pembelajaran Remedial, bentuk-bentuk pelaksanaan pembelajaran remedial diantaranya:

1) Pemberian pembelajan ulang dengan metode dan media yang berbeda. Melalui kegiatan ini guru akanmenjelaskan kembali materi yang belum dipahami atau dikuasai oleh siswa. Pembelajaran ulang bisa dilakukan dengan cara penyederhanaan materi, variasi cara penyajian, penyederhanaan tes/pertanyaan, guru harus berorientasi pada kesulitan yang dihadapi oleh siswa.

2) Pemberian bimbingan secara khusus, misalnya bimbingan perorangan. Dalam hal pembelajaran klasikal peserta didik mengalami kesulitan, perlu alternative tindak lanjut berupa pemberian bimbingan secara individual. Pemberian bimbingan ini merupakan implikasi peran pendidik sebagai tutor. Untuk lebih memudahkan dalam proses bimbingan ini, guru sebaiknya menggunakan berbagai alat peraga dan memberi kesempatan pada siswa untuk menggunakan alat peraga tersebut. Konsep yang sukar dipahami pada proses bimbingan akan lebih mudah dipelajari dan menjadi menarik jika disajikan dengan menggunakan media.
3) Pemberian tugas-tugas, latihan secara khusus. Dalam rangka menerapkan prinsip pengulangan, tugas-tugas latihan perlu diperbanyak agar peserta didik tidak mengalami kesulitan belajar dalam mengerjakan tes akhir. Peserta didik perlu diberi latihan intensif (*drill)* untuk membantu menguasai kompetensi yang ditetapkan.
4) Pemanfaatan tutor sebaya. Sumber belajar tidak hanya dari guru melainkan dari teman sekelas yang nilai kompetensinya lebih tinggi dari teman yang lainnya, mereka biasa disebut sebagai tutor sebaya, mereka adalah teman sekelas yang mempunyai kecepatan belajar lebih. Mereka perlu dimanfaatkan untuk memberikan tutorial kepada rekannya yang mengalami keterlambatan belajar. Pembelajaran tutor sebaya dapat meningkatkan hasil belajar siswa, Bantuan belajar oleh teman sebaya dianggap dapat menghilangkan kecanggungan antara sumber belajar dan peserta didik, bahasa teman sebaya lebih mudah dipahami, selain itu dengan teman sebaya tidak ada rasa malu untuk mengungkapkan kesulitan-kesulitan yang dihadapinya. Diharapkan dengan teman sebaya peserta didik lebih terbuka dan akrab.

Dari uraian tersebut diatas anda dapat mengetahui bahwa ada beberapa bentuk atau metode remedial yang dapat diaplikasikan guru dalam kegiatan remedial.Hal yang perlu diperhatikan bahwa dalam membantu siswa memahami materi pelajaran melalui kegiatan remedial guru harus menerapkan metode yang berbeda dengan metode pembelajaran yang telah dipakai pada pembelajaran reguler.Di samping itu, metode yang dipilih turut menentukan keberhasilan kegiatan remedial,

berhasil tidaknya kegiatan remedial sangat tergantung pada kemampuan guru dalam menerapkan metode yang dipilih.

3. Hakiat Kegiatan Pengayaan

Secara umum pengayaan (*enrichment*)…*is usually the addition of disciplines or areas of learning not normally found in the regular curriculum and the used at both the elementary and the secondary level. One may also find more difficult or in-depth material available on the typical curricular subjects* (Clark, 1988: 202). Sedangkan menurut mantan Rektor Universitas Muhammadyah Jakarta Mochtar Buchori; *program pengayaan* atau *enrichment program* adalah suatu program belajar yang disusun dengan materi di atas program standar untuk para siswa yang dinilai memiliki kemampuan belajar yang lebih tinggi daripada yang dituntut oleh program standar (Buhori, 1995: 189).Dengan demikian dalam pengayaan merupakan pengalaman atau kegiatan peserta didik yang melampaui persyaratan minimal yang ditentukan oleh kurikulum dan tidak semua peserta didik dapat melakukannya. Dengan kata lain kegiatan ini diperuntukkan bagi siswa yang tergolong cepat dan mampu (di atas rata-rata) dalam menyelesaikan tugas belajarnya. Siswa yang telah tergolong cepat dan mampu dalam menyelesaikan tugas belajarnya sebelum waktu yang ditentukan memiliki kelebihan waktu yang perlu dimanfaatkan.Kelebihan waktu yang tidak dikelola atau dimanfaatkan secara baik dapat menimbulkan hal-hal negatif yang dapat mengganggu jalannya pembelajaran.Jika ada peserta didik yang lebih mudah dan cepat mencapai penguasaan kompetensi minimal yang ditetapkan, maka sekolah perlu memberikan perlakuan khusus berupa program pembelajaran pengayaan.Pembelajaran pengayaan berupaya mengembangkan keterampilan berpikir, kreativitas, keterampilan memecahkan masalah, eksperimentasi, inovasi, penemuan, keterampilan seni, keterampilan gerak, dan sebagainya.Pembelajaran pengayaan memberikan pelayanan kepada peserta didik yang memiliki kecerdasan lebih dengan tantangan belajar yang lebih tinggi untuk membantu mereka mencapai kapasitas optimal dalam belajarnya.

Pembelajaran pengayaan merupakan pembelajaran tambahan dengan tujuan untuk memberikan kesempatan pembelajaran baru bagi

peserta didik yang memiliki kelebihan sedemikain rupa sehingga mereka dapat mengoptimalkan perkembangan minat, bakat, dan kecakapannya.Oleh karena itu, guru perlu merancang kegaiatan bagi siswa yang tergolong cepat agar perkembangan mereka tidak terganggu dan tidak mengganggu siswa lain yang membutuhkan tambahan bimbingan. Selain itu menurut Sukiman (2012)pembelajaran pengayaan merupakan pembelajaran tambahan dengan tujuan untuk memberikan kesempatan pembelajaran baru bagi peserta didik yang memiliki kelebihan sedemikian sehingga mereka dapat mengoptimalisasikan perkembangan minat, bakat dan kecakapan.Dengan demikian, yang dimaksud dengan kegiatan pengayaan adalah kegiatan yang diberikan kepada kepada siswa kelompok cepat dalam memanfaatkan kelebihan waktu yang dimilikinya sehingga mereka memiliki pengetahuan yang lebih kaya dan keterampilan yang lebih baik.

Tugas yang dapat diberikan guru pada siswa yang mengikuti kegiatan pengayaan di antaranya adalah memberikan kesempatan menjadi tutor sebaya, mengembangkan latihan praktis dari materi yang sedang dibahas, membuat hasil karya, melakukan suatu proyek, membahas masalah, atau mengerjakan permainan yang harus diselesaikan siswa. Apapun kegiatan yang dipilih guru, hendaknya kegiatan pengayaan tersebut menyenangkan dan mengembangkan kemampuan kognitif tinggi sehingga mendorong siswa untuk mengerjakan tugas yang diberikan

4. Bentuk-Bentuk Pelaksanaan Pengayaan

Kegiatan pengayaan dilaksanakan dengan tujuan memberikan kesempatan kepada siswa untuk memperdalam penguasaan materi pelajaran yang berkaitan dengan tugas belajar yang sedang dilaksanakan sehingga tercapai tingkat perkembangan yang optimal.Dalam membantu siswa memanfaatkan sisa waktu yang dimilikinya, guru dapat merancang berbagai kegiatan yang menyenangkan dan mendorong siswa untuk belajar.Banyak jenis kegiatan yang dapat dirancang dan dilaksanakan oleh guru dalam mengembangkan potensi siswa dan memanfaatkan sisa waktu yang dimiliki siswa kelompok cepat. Beberapa diantaranya akan kita bahas berikut ini:

a. Guru Profesional

Dorothy Sisk dalam*Creative Teaching of The Gifted,*(1987). Mengemukakan bahwa elemen utama dalam proses pembelajaran pengayaan adanya layanan guru professional; adalah guru yang "dipercaya" sebagai orang yang mampu memberikan layanan pembelajaran karena kompetensinya (akademik, pedagogik, sosial, dan personalnya) memberikan rasa percaya serta keberbakatannya sebagai guru yang penuh kehangatan, menantang dan menyenangkan (Sisk, 1987: 235)

Ia hadir bukan sekedar memenuhi kewajiban kehadirannya, melainkan ia hadir penuh makna dan semangat serta memberi inspirasi bagi para siswanya karena kemampuannya pembelajarannyayang penuh kehangatan mengingat baik *kompetensi akademik* yang memiliki pengetahuan luas; *kompetensi pedagogik* dengan cara mengajar yang piawai dengan kedekatan, keterbukaan, metodenya yang variatif dan tidak membosankan; *kompetensi sosial* sebagai guru yang mementingkan interaksi dan kerjasama yang kohesif; serta *kompetensi personalnya*, di mana ia sebagai pribadi yang rajin, ulet bekerja, matang secara emosional, serta penuh gairah serta memiliki vitalitas dan gaya hidup yang kreatif-inovatif (Sisk, 1987: 239-241).

Kompetensi-kompetensi guru profesional seperti di atas, adalah penting, bahkan menjadi faktor utamakalau bukan faktor pertama dalam memberikan rasa "percaya" bagi anak unggulan maupun yang memiliki kemampuan di atas rata-rata, untuk terus berprestasi lebih jauh lagi. Tidak sedikit hati para siswa yang memiliki potensi unggul itu merasa terpukul setelah melihat gurunya yang secara akademik dan pedagogik guru tersebut menempatkan dirinya sebagai "guru domestik" dan"tradisional", di mana ia kurang memiliki kemampuan dan pengetahuan yang luas, serta gaya mengajarnya yang kelihatan mengulang-ulang menampakkan "mandeknya" keterampilan pembelajaran (Supardan, 2015: 47-51) .

b. Tutor Sebaya

Kegiatan tutor sebaya tidak hanya kita jumpai pada kegiatan remedial saja, kegiatan ini ternyata juga sangat efektif diterapkan pada

kegiatan pengayaan. Para siswa akan saling membantu untuk memahami materi pembelajaran yang diberikan oleh guru. Bagi siswa yang memiliki jiwa sosial yang tinggi, ia akan memberikan penjelasan konsep-konsep atau ide kepada teman sekelasnya, mereka akan berusaha sebaik mungkin mencari cara yang tepat untuk memaparkan materi pembelajaran agar temannya dapat memahami penjelasannya. Tetapi guru juga harus menyadari, bahwa tumbuhnya jiwa sosial seperti ini tidaklah bersifat *"a given"* melainkan sebgaia buah hasil latihan sebelumnya, di mana guru harus memberi contoh dan keteladanan yang berarti dari guru itu sendiri kepada para siswanya.

Melalui kegiatan tutor sebaya ini, pemahaman siswa akan semakin matang terhadap materi tersebut, selain konsep materi itu akan dijelaskan didepan teman-temannya, mereka juga harus menemukan dan menguasai teknik, strategi, dan metode yang tepat untuk menjelaskan konsep tersebut.

Disamping itu, tutor sebaya dapat mengembangkan kemampuan kognitif tingkat tinggi. Untuk dapat berperan sebagai tutor yang baik, siswa harus memberikan penjelasan yang dapat dimengerti oleh temannya, siswa juga diharapkan lebih mampu memandang suatu konsep atau ide dari berbagai sudut pandang, mampu memikirkan contoh-contoh yang dapat digunakan untuk menjelaskan konsep yang sedang dibahas, serta harus menganalisis berbagai komponen lainnya yang mendukung proses belajar mengajar. Dengan demikian, melalui tutor sebaya, siswa kelompok cepat dapat meningkatkan pemahamannya terhadap materi pelajaran di samping mengembangkan kemampuan kognitifnya.

Pertanyaannya, mengapa dengan tutor sebaya anak bisa belajar bersama dalam meningkatkan prestasi belajarnya.Jawabannya tiada lain karena melalui teman sebaya (*peer group*), biasanya ada keterbukaan, kesetaraan, dan kebersamaan.Dalam *peer group*, dengan sebayanya remaja akan berusaha untuk diterima dan berusaha untuk tidak ditolak. Inilah yang dalam Teori Kebutuhan Maslowdikenal sebagai*KebutuhanPemilikan dan Cinta* serta *Kebutuhan Dihargail*, yaitu kebutuhan untuk pertemanan /persahabatan, dan kebutuhan hubungan

intim. Sedangkan yang termasuk dalam Kebutuhan akan Dihargai, adalah kebutuhan untuk prestise, penerimaan dan status, maupun penghargaan diri yang menghasilkan perasaan edekuat, kompeten dan kepercayaan diri (Maslow, 1987/1954: 17).

c. Mengembangkan Latihan

Disamping memberikan tutorial kepada teman-temannya yang termasuk kelompok lambat, kelompok siswa yang unggul dan cepat mampu juga dapat diminta untuk memberikan atau mengembangangkan latihan praktis yang dapat dilaksanakan oleh teman-temannya yang lambat sehingga mereka akan lebih mudah memahami materi pelajaran. Misalnya saja siswa dalam kelompok unggul dan cepat mampu diminta untuk membuat soal-soal latihan untuk dikerjakan secara bersama-sama atau secara individu oleh teman-temannya dalam kelompok lambat guna pendalaman materi yang menuntut banyak latihan.Merekan juga diminta untuk memberikan komentar terhadap jawaban yang diberikan oleh siswa lain. Selain itu, guru juga dapat meminta siswa kelompok unggul dan cepat mampu untuk membuat soal-soal latihan yang cocok digunakan oleh guru dalam kegiatan remedial atau sebagai bahan bagi mereka dalam kegiatan tutor sebaya.

d. Mengembangkan Media dan Sumber Pembelajaran

Memberikan kesempatan bagi kelompok cepat dan unggul untuk mengembangkan kemampuannya membuat media atau karya yang berkaitan dengan materi yang akan dipelajari. Hasil karya tersebut bisa berupa model, permainan atau modul yang bisa dimanfaatkan sebagai sumber belajar bagi siswa yang mengalami kesulitan dalam memahami materi tersebut.

e. Melakukan proyek

Melakukan suatu proyek atau ikut serta dalam mempersiapkan suatu laporan khusus yang sesuai dengan materi yang sedang dipelajari merupakan suatu kegiatan pengayaan yang sangat menarik dan paling menyenangkan bagi siswa kelompok unggul atau cepat ini.Melalui kegiatan ini motivasi belajar siswa akan meningkat, mereka akan berusaha sebaik dan semaksimal mungkin melaksanakan kegiatan ini dengan harapan dikemudian hari mereka akan mendapat kesempatan

lagi untuk melakukan proyek berikutnya. Disamping itu kegiatan ini juga memberikan kesempatan yang besar bagi mereka dalam mengembangkan bakat dan minat yang mereka miliki atau untuk menambah dan meningkatkan wawasan mereka.

f. Memberikan permainan, masalah atau kompetisi antar siswa

Siswa kelompok cepat biasanya sangat suka dengan kegiatan menantang, khususnya memecahkan masalah yang sulit. Oleh karena itu, dalam kegiatan pengayaan guru dapat memberikan tugas kepada siswa kelompok cepat untuk memecahkan suatu masalah atau games yang berkaitan dengan materi pelajaran. Kegiatan tersebut bukan hanya bertujuan untuk mengasah kemampuan mereka dalam memecahkan masalah atau permainan yang diberikan, melainkan juga mereka bisa saling bekerja samadengan bertukar pikiran satu sama lain atau bahkan saling membandingkan strategi dan teknik yang mereka pergunakan dalam memecahkan permasalahan tersebut.

g. Pengayaan dalam Ekstrakurikuler

Akhir-akhir ini banyak sekolah di kota-kota besar yang menyelenggarakan program pengayaan secara ekstrakurikuler, yaitu program pengayaan *bidang drumband*. Jika kita mau jujur, kebanyakan kegiatan dari kegiata-kegiatan ini diselenggarakan bukan semata-mata untuk kepentingan siswa, tetapi terutama dalam beberapa kasus banyak terjadi untuk mengharumkan nama daerah, nama sekolah, dan sebagainya. Maka peralatan yang serba mahal diperoleh baik dari sumbangan Bupati ,Walikotamaupun Gubernur juga terjadi.

Timbul pertanyaan, salahkah kegiatan pengayaan seperti ini? Tentu saja belum, bahkan mungkin tidak, sejauh para siswa yang berkepentingan masih merasakan manfaat pribadi dari pembelajaran model ini.Akan tetapi praktek pengayaan ini jika mengarah kepada upaya sekolah yang menekan dan mengeksploitasi para siswa hanya untuk mengharumkan instritusi (sekolahan) semata-mata.Kegiatan pengayaan seperti ini bersifat eksploittif tidak lagi edukatif (Buhori, 1995: 192).

5. Faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan pengayaan.

Dari uraian yang telah dipaparkan sebelumnya, dapat kita ketahui bahwa ada beberapa kegiatan pengayaan yang dapat dilakukan guru dalam membantu siswa mengembangkan potensinya. Agar kegiatan tersebut mencapai tujuan secara optimal, mari kita perhatikan beberapa faktor yang harus dipertimbangkan guru dalam dalam menentukan kegiatan pengayaan. Sugihartono, dkk (2012)mengemukakan tiga faktor yang harus dipertimbangkan dalam memilih dan melaksanakan kegiatan pengayaan.Ketiga faktor tersebut adalah faktor peserta didik, kegiatan pengayaan, dan waktu.

Gambar 1.2 Faktor Penentu PelaksanaanPengayaan
Adaptasi dari Feldhusen & Kolloff (1979) serta Sugihartono, dkk (2012)

1. *Faktor Peserta Didik*, dalam melakukan kegiatan pengayaan guru harus menyadari dan memahami bahwa peserta didik mempunyai beberapa kesamaan dan perbedaan yang sifatnya individual. Baik yang berkenaan dengan faktor minat maupun faktor psikologis lainnya. Kesesuaian kegiatan pengayaan dengan minat siswa akanmendorong siswa berhasil dalam belajarnya. Sebaliknya proses kegiatan pengayaan yang berlangsung tidak sesuai dengan minat siswa akan berakibat pada menurunnya semangat atau motivasi siswa dalam mengikuti pelajaran. Karena itu dalam memberikan kegiatan pengayaan harus memperhatikan sifat individual peserta didik seperti bakat, minat, hobbi dan keterampilan lain yang dimiliki dan disukai atau dikuasai oleh siswa.
2. *Faktor kegiatan pengayaan*, kegiatan pengayaan yang diberikan oleh guru harus menunjang pengembangan potensi peserta didik secara optimal. Dalam hal ini kegiatan pengayaan jangan sampai

memberatkan, merugikan, menyusahkan dan menimbulkan kesulitan bagi peserta didik sehingga menyebabkan proses perkembangannya terganggu bahkan mandek. Sehubungan dengan hal itu Feldhusen dan Kollof (1986) mengemukakan betapa pentingnya strategi dan metode pembelajaran pengayaan itu sifatnya harus *powerful;*yang mampu mengaktifkan (*activating)*, menantang (*challenging*), bermakna (*meaningful*) dan menyenangkan (*delightful*). Dalam pembelajaran pengayaan biasanya menghindari hal-hal yang bersifat pengulangan, karena pada diri anak yang memiliki kemampuan di atas rata-rata (apalagi anak berbakat) sering merasa cepat jenuh jika pembelajaran kurang *powerful*(Supardan, 2015:*47).*Diharapkan setelah mengikuti kegiatan pengayaan ini makan pengetahuan atau keterampilan, bahkan nilai atau sikap yang dimiliki oleh siswa akan meningkat secara optimal.

3. Faktor waktu, salah satu tujuan dari kegiatan pengayaan adalah kegiatan pembelajaran yang dilakukan untuk memanfaatkan kelebihan waktu yang dimiliki oleh kelempok belajar cepat, sambil menunggu siswa lambat juga menguasai kompetensi yang telah ditetapkan. Setelah siswa lambat menguasai kompetensi tersebut maka kegiatan pengayaan dihentikan dan semua siswa akan kembali megikuti kegiatan pembelajaran secara bersama-sama.Guru harus memilih kegaiatan pengayaan yang tepat sesuai dengan waktu yang telah tersedia bagi setiap siswa sesuai denga perbedaan individu yang dimiliki masing-masing siswa, kelebihan waktu yang dimiliki oleh siswa tentunya akan berbeda satu sama lain. Kenyataan ini menuntut kemampuan dan kreativitas guru dalam mempersiapkan dan melaksanakan kegiatan pengayaan. Guru harus mampu menyesuaikan jenis kegiatan pengayaan dengan kebutuhan dan waktu yang dimiliki oleh masing-masing siswa. Diharapkan setelah kegiatan pengayaan ini berlangsung siswa tersebut sudah menguasai materi pengayaan secara utuh dan menyeluruh (siswa sudah dapat melihat hasil dari kegiatan tersebut).

Itulah tiga faktor yang harus diperhatikan oleh guru dalam memilih dan melaksanakan kegiatan pengayaan.Dengan memperhatikan faktor-

faktor tersebut diharapkan kegiatan pengayaan yang dilaksanakan dapat benar-benar bermanfaat bagi siswa kelompok cepat sehingga kemampuannya berkembang secara optimal, dan waktu yang tersisa bisa dimanfaatkan sebaik mungki.

D. Aktivitas Pembelajaran

Adapun inti dari aktivitas pembelajaran modul ini bagi peserta diklat adalah sebagai berikut: Alokasi waktu yang disediakan untuk pembelajaran satu ini adalah 100 menit atau 2 x 50 menit, dengan rincian sebagai berikut:

Tabel 1. Aktivitas Kegiatan Pembelajaran I

No.	Waktu	Kegiatan
1.	20 menit	Apersepsi yang berkaitan dengan kegiatan mengidentifikasi dan memehami teori konsep dasar kegiatan remedial dan pengayaan
2.	50 menit	• Membagi kelompok diskusi. • Mendiskusikan (1) Pengertian kegiatan remedial, (2) Jenis-jenis kegiatan remedial, (3) Pengertian kegiatan pengayaan, (4) Hakikat kegiatan pengayaan, (5) Bentuk-bentuk kegiatan pengayaan, dan (6) Faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan remedial dan pengayaan
3.	30 menit	Menyajikan/mensimulasikan teori remedial dan pengayaan yang terdapat pada pembelajaran I terhadap peserta diklat

E. Latihan/ Kasus/ Tugas

Cocokkan jawaban Anda dengan Kunci jawaban yang terdapat dibagian akhir modul ini.Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan anda terhadap materi Kegiatan Pembelajaran 1

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100\%$$

Arti tingkat penguasaan: 90 – 100% = baik sekali

80 - 89% = baik

70 – 79% = cukup

< 70% = kurang

Apabila mencapai tingkat 80% **Bagus!** atau lebih, Anda dapat meneruskan dengan modul selanjutnya. Jika masih dibawah 80%, Anda harus mengulangi materi Kegiatan pembelajaran 1, terutama bagian yang belum dikuasai.

SoalEssay

1. Sifat pokok kegiatan pembelajaran remedial ada tiga yaitu…

   ……..

   ……..

2. Gambar fungsi kegiatan remedial menurut Warkiti adalah…

3. Yang diharapkan dari pemberian kegiatan remedial kepada murid adalah…

   ……..

   ……..

F. Rangkuman

Kegiatan remedial adalah kegiatan yang ditujukan untuk membantu siswa yang mengalami kesulitan dalam menguasai materi pelajaran.Sesuai dengan pengertiannya, tujuan kegiatan remedial ialah membantu siswa mencapai tujuan pembelajaran yang telah ditetapkan dalam kurikulum yang berlaku.

Dalam kaitannya dengan proses pembelajaran, fungsi kegiatan remedial adalah:

1. Memperbaiki cara belajar siswa dan cara mengajar guru (fungsi korektif);
2. Meningkatkan pemahaman guru dan siswa terhadap kelebihan dan kekurangan dirinya (fungsi pemahaman);

3. Menyesuaikan pembelajaran dengan karakteristik siswa (fungsi penyesuaian);
4. Mempercepat penguasaan siswa terhadap materi pelajaran (fungsi akselerasi);
5. Membantu megatasi kesulitan siswa dalam aspek sosial-pribadi (fungsi terapeutik)

Perbedaan kegiatan remedial dari pembelajaran biasa terletak pada pendekatan yang digunakan dalam perencanaan dan pelaksanaan pembelajaran.Kegiatan remedial direncanakan dan dilaksanakan berdasarkan kebutuhan individu atau kelompok siswa.Sementara itu, pembelajaran biasa menerapkan pendekatan klasikal, baik dalam perencanaan maupun dalam pelaksanaan.

Dalam melakasanakan kegiatan remedial guru dapat menerapkan berbagai jenis kegiatan remedial termasuk metode dan media, sesuai dengan kesulitan yang dihadapi dan tingkat kemampuan siswa serta menekankan pada segi kekuatan yang dimiliki siswa.

Kegiatan pengayaan adalah kegiatan yang diberikan kepada siswa kelompok cepat agar mereka dapat mengembangkan potensinya secara optimal dengan memanfaatkan sisa waktu yang dimilikinya.

Kegiatan pengayaan dilaksakan dengan tujuan memberikan kesempatan kepada siswa untuk memperdalam penguasaan materi pelajaran yang berkaitan dengan tugas belajar yang sedang dilaksanakan sehingga tercapai tingkat perkembangan yang optimal.

Tugas yang dapat diberikan guru pada siswa yang mengikuti kegiatan pengayaan diantaranya adalah memberikan kesempatan menjadi tutor sebaya, mengembangkan latihan praktis dari materi yang sedang dibahas, membuat hasil karya, melakukan suatu proyek, membahas masalah atau mengerjakan permainan yang harus diselesikan siswa. Apa pun kegiatan yang dipilih guru, hendaknya kegiatan pengayaan tersebut menyenangkan dan mengembangkan kemampuan kognitif tinggi sehingga mendorong siswa untuk mengerjakan tugas yang diberikan.

Dalam memilih dan melaksanakan kegiatan pengayaan, guru harus memperhatikan:

1. Faktor siswa, baik faktor minat maupun faktor psikologis lainnya;

2. Faktor manfaat edukatif;
3. Faktor waktu.

G. Umpan Balik dan Tindak Lanjut

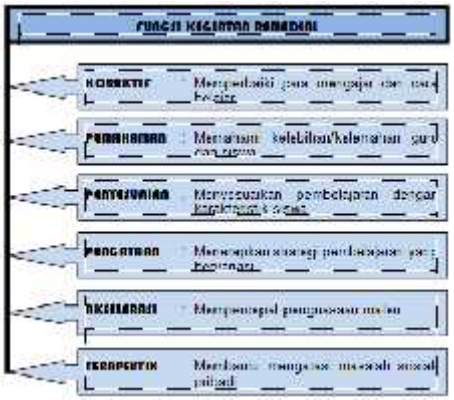
Adapun umpan balik dalam kegiatan Pembelajaran I ini adalah: jawablah semua latihan pada Kegiatan Pembelajaran ini. Kemudian cocokkan jawaban Anda dengan kunci jawaban dan nilai hasilnya.Apabila benar semua, maka pemahaman Anda 100 %.Apabila salah satu, maka pemahaman Anda 80 %.Apabila yang salah ada dua, maka pemahaman Anda 60 %.Apabila yang salah salah ada tiga, maka pemahaman 40 %. Apabila yang salah ada empat atau lima, maka pemahaman 20 %, dan apabila semua, maka pemahaman 0 %.

Selanjutnya apabila Anda mendapatkan hasil 80 % ke atas, maka Anda dinyatakan lulus dan silahkan melanjutkan ke Kegiatan Pembelajaran II, akan tetapi apabila mendapatkan 0 %, 25 %, 40 % atau 60 %, maka Anda diminta membaca dan memahami isi modul kembali dan menjawab latihan-latihan yang telah disiapkan.

H. Kunci Jawaban

Kunci jawaban essay

1. Sifat pokok kegiatan pembelajaran remedial adalah
   (1) menyederhanakan konsep yang komplek
   (2) menjelaskan konsep yang kabur
   (3) memperbaiki konsep yang salah tafsir.
2. Gambar fungsi kegiatan remedial menurut Warkiti



3. Murid yang mengalami kesulitan belajar dapat diperbaiki atau disembuhkan sehingga dapat mencapai hasil yang diharapkan sesuai dengan kemampuan

2

KEGIATAN PEMBELAJARAN

Kegiatan Pembelajaran II

Prosedur Remedial dan Pengayaan

A. Tujuan

1. Peserta diklat diharapkan mampu menjelaskan prosedur pengajaran remedial.
2. Perserta diklat diharapkan mampu menjelaskan langkah-langkah pelaksanaan pengajaran pengayaan.

B. Indikator Pencapaian Kompetensi

1. Menjelaskan prosedur pengajaran remedial.
2. Menjelaskan langkah-langkah pelaksanaan pengajaran pengayaan.

C. Uraian Materi

1. Prosedur Pengajaran Remedial

Pengajaran remedial merupakan salah satu tahapan kegiatan utama dalam keseluruhan kerangka pola layanan bimbingan belajar.Dalam topik ini kita akan membahas tentang langkah-langkah yang sebaiknya ditempuh oleh guru dalam melaksanakan kegiatan remedial.

Dalam melaksanakan kegiatan remedial sebaiknya mengikuti langkah sebagai berikut:

a. Analisis Hasil Diagnosis

Melalui kegiatan diagnosis guru akan mengetahui para siswa yang perlu mendapatkan bantuan. Untuk keperluan kegiatan remedial, tentu yang menjadi fokus perhatian adalah siswa-siswa yang mengalami kesulitan dalam belajar yang ditunjukkan tidak tercapainya kriteria keberhasilan belajar. Apabila kriteria keberhasilan 80 %, maka siswa yang dianggap berhasil jika mencapai tingkat penguasaan 80 % ke atas, sedangkan siswa yang mencapai tingkat penguasaannya di bawah 80 % dikategorikan belum berhasil.

Mereka inilah yang perlu mendapatkan remedial. Setelah guru mengetahui siswa-siswa mana yang harus mendapatkan remedial, informasi selanjutnya yang harus diketahui guru adalah topik atau

materi apa yang belum dikuasai oleh siswa tersebut. Dalam hal ini guru harus melihat kesulitan belajar siswa secara individual. Hal ini dikarenakan ada kemungkinan masalah yang dihadapi siswa satu dengan siswa yang lainnnya tidak sama. Padahal setiap siswa harus mendapat perhatian dari guru.

b. Menemukan Penyebab Kesulitan

Sebelum Anda merancang kegiatan remedial, terlebih dahulu harus mengetahui mengapa siswa mengalami kesulitan dalam menguasai materi pelajaran. Faktor penyebab kesuliatan ini harus diidentifikasi terlebih dahulu, karena gejala yang sama yang ditunjukkan oleh siswa dapat ditimbulkan sebab yang berbeda dan faktor penyebab ini akan berpengaruh terhadap pemilihan jenis kegiatan remedial.

c. Menyusun Rencana Kegiatan Remedial

Setelah diketahui siswa-siswa yang perlu mendapatkan remedial, topik yang belum dikuasai setiap siswa, serta faktor penyebab kesulitan, langkah selanjutnya adalah menyusun rencana pembelajaran. Sama halnya pada pembelajaran pada umumnya, komponen-komponen yang harus direncanakan dalam melaksanakan kegiatan remedial adalah sebagai berikut;

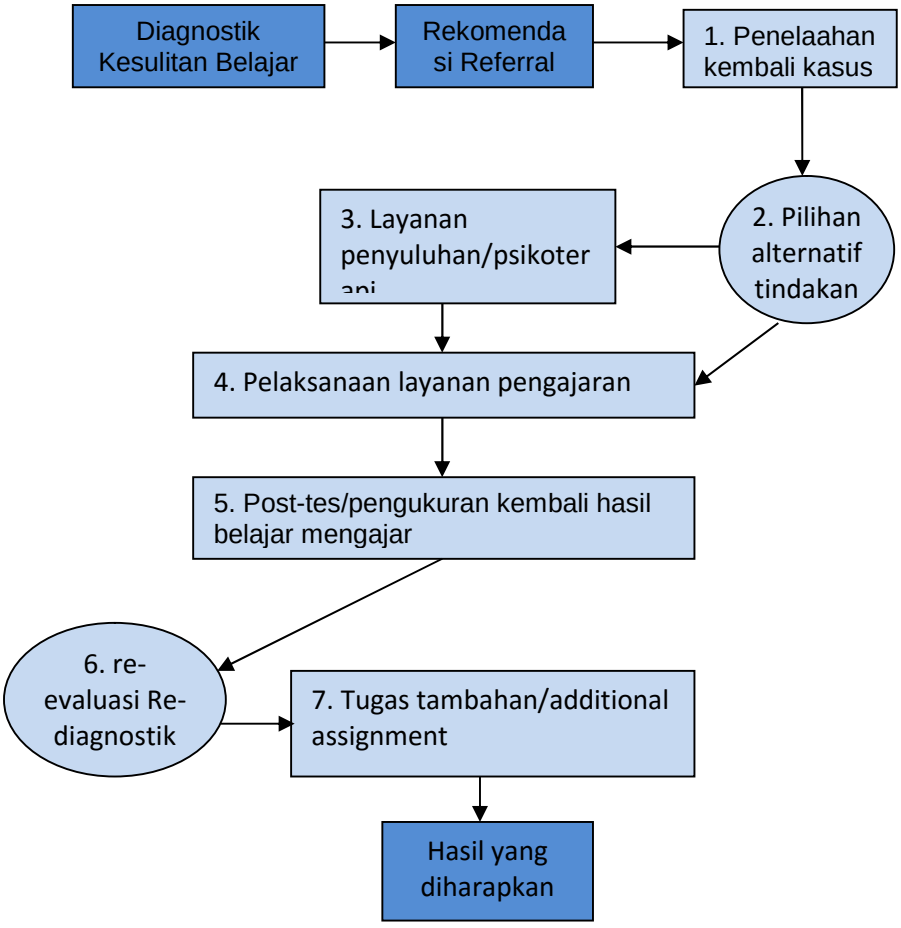
1. Merumuskan indikator hasil belajar
2. Menentukan materi yang sesuai engan indikator hasil belajar
3. Memilih strategi dan metode yang sesuai dengan karakteristik siswa
4. Merencanakan waktu yang diperlukan
5. Menentukan jenis, prosedur dan alat penilaian.
6. Melaksanakan Kegiatan Remedial

Setelah kegiatan perencanaan remedial disusun,langkah berikutnya adalah melaksanakan kegiatan remedial. Sebaiknya pelaksanaan kegiatan remedial dilakukan sesegera mungkin, karena semakin cepat siswa dibantu mengatasi kesulitan yang dihadapinya, semakin besar kemungkinan siswa tersebut berhasil dalam belajarnya.

d. Menilai Kegiatan Remedial

Untuk mengetahui berhasil tidaknya kegiatan remedial yang telah dilaksanakan, harus dilakukan penilaian. Penilaian ini dapat dilakukan dengan cara mengkaji kemajuan belajar siswa.Apabila siswa mengalami kemauan belajar sesuai yang diharapkan, berarti kegiatan remedial yang direncanakan dan dilaksanakan cukup efektif membantu siswa yang mengalami kesulitan belajar. Tetapi, apabila siswa tidak mengalami kemajuan dalam belajarnya berarti kegiatan remedial yang direncanakan dan dilaksanakan kurang efektif. Untuk itu guru harus menganalisis setiap komponen pembelajaran.

Adapaun prosedur pelaksanaan remedial menurut Abin Syamsuddin (2012) Secara skematik, prosedur pelaksanaan kegiatan remedial dapat digambarkan sebagai berikut:



Gambar 2.1 Prosedur pengajaran Remedial
Abin Syamsuddin (2012)

Dari gambar skematik tersebut dapat dikembangkan sekurang-kurangnya empat alternatif prosedur sesuai dengan keperluannya, keempat alternative itu adalah:

a. Prosedur I, mencakup langkah 1-2-3-4-5-6;
b. Prosedur II, mencakup langkah 1-2-(3)-4-5-6;
c. Proedur III, mencakup langkah 1-2-3-4-5-6-(7); dan
d. Prosedur IV, mencakup langkah 1-2-(3)-4-5-6-(7).

Untuk lebih jelasnya, kita akan mendeskripsikan fungsi, tujuan/sasaran, dan kegiatannya sebagai berikut:

1) *Penelaahan kembali kasus dengan permasalahaannya*

Langkah ini merupakan tahapan paling fundamental dalam pengajaran remedial karena merupakan landasan pangkal dari langkah-langkah kegiatan berikutnya. Sasaran pokok langkah ini adalah: (a) diperolehnya gambaran yang lebih defenitif mengenai karakteristik kasus beserta permasalahannya; (b) diperolehnya gambaran yang lebih defenitif mengenai fasibilitas alternatif tindakan remedial yang direkomendasikan.

Sesuai dengan sasaran tersebut maka kegiatan dalam langkah ini difokuskan kepada suatu analisis rasional atas hasil investigasi yang telah dilakukan atau hasil rekomendasi dari guru bidang studi, wali kelas, petugas BK atau ahli lainnya. Secara lebih jelasnya, analisis ini nantinya akan digunakan sebagai kegiatan pengecekan atau penelitian kembali terhadap:

a) Kebenaran (validitas) dan kelengkapan data informasi yang mendukung pernyataan atau deskripsi tentang karakteristik kasus beserta permasalahannya;
b) Bahanrelevansi antara tafsiran/perkiraan/dugaan dan kesimpulan yang dibuat dengan data informasi pendukungnya serta konsistensi antara berbagai data/informasi dengan tafsiran dan kesimpulannya satu sama lain secara integral;
c) Ketepatan estimasi kemungkinan penanganannya berdasarkan hasil diagnosis yang didukung oleh data/informasi yang tersedia dan yang relevan;

d) Fisibilitas dari setiap alternatif tindakan remedial yang direkomendasikan.

Berdasarkan hasil telaan diatas diharapkan terjawab pertanyaan-pertanyaan berikut:

a) Kasus siapa yang perlu mendapat penanganan?
   (1) Hanya satu atau dua dari keseluruhan anggota kelompok/kelas.
   (2) Sebagian besar anggota kelompok tertentu (kelompok lambat) dari keseluruhan siswa kelas.
   (3) Sebagian terbesar atau bahkan keseluruhan siswa dikelas.
b) Seberapa jauh tingkat kelemahannya secara umum dilihat dari segi kriteria atau indicator keberhasilan yang diharapkan?
   (1) Sekitar 60%; atau
   (2) Sekitar 50%; atau
   (3) Sekitar 40%; atau
   (4) Sekitar 30%; atau kurang dari itu.
c) Di manakah letak kelemannya dipandang dari ruang lingkup dan urutan bidang/program studi yang bersangkutan?
   (1) Pada sebagian besar atau bahkan mungkin keseluruhan bidang studi;
   (2) Pada bidang studi tertentu saja; atau
   (3) Pada unit tertentu dari suatu bidang studi saja; dan sebagainya
d) Pada tingkat dan kawasan hasil belajar manakah kasus itu mengalami kelemahan dipandang dari taksonomi tujuan-tujuan pendidikan?
   (1) *Kognitif: ra*nah ini mencakup kegiatan mental (otak). Segala upaya yang menyangkut aktivitas otak adalah termasuk dalam ranah kognitif. Ranah kognitif memiliki enam jenjang atau aspek, yaitu:Pengetahuan/hafalan/ingatan *(knowledge)*, pemahaman *(comprehension),* Penerapan *(application)* Analisis *(analysis)* Sintesis *(syntesis)* dan penilaian/penghargaan/evaluasi *(evaluation)*; dan atau
   (2) *Afektif:* ranah ini berkaitan dengan sikap dan nilai. Ranah afektif mencakup watak perilaku seperti perasaan, minat, sikap, emosi, dan nilai. Beberapa pakar mengatakan bahwa sikap seseorang dapat diramalkan perubahannya bila seseorang telah memiliki

kekuasaan kognitif tingkat tinggi. ranah afektif menjadi lebih rinci lagi ke dalam lima jenjang, yaitu: *Receiving* atau *attending*(menerima atua memperhatikan), *Responding* (menanggapi) mengandung arti "adanya partisipasi aktif", *Valuing* (menilai atau menghargai), *Organization* (mengatur atau mengorganisasikan) *Characterization by evalue or calue complex* (karakterisasi dengan suatu nilai ataukomplek nilai).

(3) *Psikomotor: r*anah ini merupakan ranah yang berkaitan dengan pola gerak-gerik, keterampilan perilaku umum, perilaku khusus, eksresif, komunikatif atau kemampuan bertindak setelah seseorang menerima pengalaman belajar tertentu. Hasil belajar psikomotor ini sebenarnya merupakan kelanjutan dari hasil belajar kognitif (memahami sesuatu) dan dan hasil belajar afektif (yang baru tampak dalam bentuk kecenderungan-kecenderungan berperilaku).

e) Faktor manakah yang merupakan penyebab utama keterlambatan dalam proses belajar mengajar dipandang dari segi *raw inputs* (siswa sendiri) yang bersangkutan?

a. Terbatasnya kemampuan dasar intelektual, baik itu kemampuan umum atau bakat khusus.
b. Kurangnya minat dan motivasi: *n-Ach* rendah, malas, kurang berminat.
c. Sikap yang kurang positif terhadap: guru dan bahan pelajaran
d. Kebiasaan belajar yang salah atau kurang memadai dalam: mengorganisasikan waktu/fasilitas belajar; sumber atau bahan pelajaran; dan melalaikan tugas/memandang enteng terhadap pekerjaan sekolah yang diberikan oleh guru.
e. Kurangnya mengetahui pengatahuan dan keterampilan dasar yang diperlukan, misalnya dalam: mencari/menghimpun, mengamati/mengobservasi, mencatat dan mengorganisasikan informasi, fakta, konsep prinsip/kaidah/dalil, prosedur yang dipelajari dikelas; mengoperasikan atau mengaplikasikan prinsip, metode, teknik yang telah dipelajari ke dalam pemecahan masalah; dan atau mengoperasikan kaidah-kaidah logika (sebab-

akibat, asosiasi, diferensi, komparasi, dan sebagainya) formula dalam melakukan analisis sintesis dan evaluasi.

f. Belum cukup matang *(immaturation)* dan siap *(readiness)* untuk mengikuti program belajar mengajar utama yang bersangkutan.

f) Faktor manakah yang mungkin menjadi penyebab utama dari komponen instrumental input (sarana penunjang) dari proses belajar mengajar yang bersangkutan?

(1) Program kurang serasi (satu program buat semua, program tidak efekif) dengan keragaman siswa;

(2) Kurang serasinya bahan atau sumber belajar yang tersedia dengan yang diperlukan, baik itu dari jumlah yang terbatas atau langka, tak terbaca, sulit untuk dipahami;

(3) Strategi, metode, dan teknik belajar-mengajar kurang serasi dengan keragaman siswa (terlalu bersifat klasikal/uniform, tiada layanan individual); dan atau

(4) Fasilitas teknis yang ada tidak relevan dengan apa yang diperlukan (jumlah, tempat dan kesempatan waktunya terbatas, sukar di-manageatau dioperasikan atau bahannya langka/mahal).

(5) Kurang serasinya hubungan/kondisi objektif guru dengan siswa dan bidang studi yang bersangkutan, dilihat dari guru kurang menguasai bahan, metode, teknik dan sumber yang diperlukan dalam proses pembelajaran, guru kurang tanggap/responsive terhadap situasi kelas atau dinamika kelompok, penampilan guru kurang menarik atau meyakinkan, adanya beberapa sifat pribadi yang kurang menunjang terhadap tugas dan perannya sebagai guru, keadaan kelas yang terlalu besar jumlahnya atau terlalu heterogen sifat atau latarbelakangnya dan guru terlalu banyak/berat beban mengajarnya.

(6) Kurangnya daya dukung fasilitas fisik yang diperlukan dalam proses pembelajaran seperti: kurangnya ruang belajar, ruang kerja, laboratorium, perpustakaan dan lain sebagainya

g) Faktor manakah yang terdapat dalam lingkungan yang diduga merupakan sumber penyebab utama kesulitan yang dialami oleh siswa?

a. *Di sekolah:* apakah iklim sosial cukup sehat dan merangsang untuk belajar (interaksi siswa dengan guru, siswa dengan siswa, siswa dengan personel sekolah lainnya),
b. *Di rumah:* apakah iklim iklim rumah sudah kondusif, nyaman, dan tersedianya daya dukung fasilitas belajar yang cukup tersedia,
c. *Di masyarakat:* apakah cukup tersedia ruang/tempat *(space)* memperkaya pengalaman belajar (perpustakaan umum, fasilitas rekreasi, pusat kegiatan belajar, dan sebagainya).

h) Apakah komponen output turut menjadi salah satu sebab kesulitan belajar-mengajar?
   a. Terlalu tingginya tuntutan standar (kriteria atau indikator keberhasilan) hasil belajar *(level of mastery* 90% atau lebih)
   b. Terlalu menekankan pada satu aspek saja (kognitif saja, keterampilan atau psikomotor saja, sedangkan yang lainnya diabaikan
   c. Tidak adanya patokan sebagai ukuran baku yang dapat dijadikan pedoman baku/umum bagi setiap guru dan siswa.

Melalui kegiatan diagnosis, guru akan mengetahui para siswa yang perlu mendapat bantuan, faktor-faktor penyebab atau alasan mereka bisa ikut kegiatan remedial. Untuk keperluan kegiatan remedial, tentu yang menjadi sorotan adalah siswa-siswa yang mengalami kesulitan dalam belajar yang ditunjukkan dengan tidak tercapainya kriteria keberhasilan belajar.Sebagai contoh perhatikan tabel hasil tes formatif berikut ini.

Tabel 2. Hasil Tes Formatif

Nama Siswa	Kompetensi Dasar I						Kompetensi dasar II				Total skor	%
	Hasil Belajar 1.1			Hasil Belajar 1.2			Hasil belajar 2.1		Hasil belajar 2.2			
	Ind 1	Ind 2	Ind 3	Ind 1	Ind 2	Ind 3	Ind 1	Ind 2	Ind 1	Ind 2		
Anang	1	1	1	1	1	1	1	1	1	0	9	90
Basir	1	1	1	1	1	1	0	0	0	0	6	60
Candra	1	1	0	1	0	1	0	0	0	0	4	40
Desy	1	1	1	1	1	1	1	1	1	1	10	100
Ema	0	0	0	1	1	1	0	0	1	1	5	50

Firman	1	1	1	0	0	0	1	1	0	0	5	50
Gani	1	1	1	1	1	1	0	0	1	1	8	80
Herman	1	1	1	1	1	1	0	0	1	1	8	80
Ika	1	1	1	1	1	1	0	0	0	0	6	60
Yudi	1	1	1	1	1	1	1	0	0	0	7	70

Catatan:
Ind = Indikator
1 = Jawaban benar
0 = Jawaban salah

Apabila kita menggunakan kriteria keberhasilan 80% maka siswa dianggap berhasil jika mencapai tingkat penguasaan 80%.Dapatkah anda menentukan siapa saja dari 10 siswa tersebut di atas yang perlu mendapatkan kegiatan remedial?

Siswa yang perlu mengikuti kegiatan remedial adalah…

Tepat sekali, yang perlu mendapat kegiatan remedial adalah mereka yang total skornya kurang dari 80%. Ada enam siswa yang harus mendapatkan kegiatan remedial.Keenam siswa tersebut adalah Basir, Candra, Erna, Firman, Ika, dan Yudi.

Setelah kita mengetahui siswa-siswa yang perlu mendapatkan kegitan remedial, informasi selanjutnya yang harus diketahui oleh guru adalah kompetensi apa yang belum dikuasai oleh siswa-siwa tersebut. Dalam hal ini, guru harus melihat kesulitan belajar yang dihadapi oleh siswa secara individual, Mengapa? Sebab ada kemungkinan, siswa yang satu menghadapi masalah dalam kompetensi dasar I. sementara siswa yang lain menghadapi masalah dalam menguasai kompetensi dasar II. Padahal setiap siswa yang mengalami kesulitan harus mendapat perhatian dari guru.

Kita kembali pada Tabel hasil tes formatif.Dari tabel tersebut diketahui bahwa Erna mengalami kesulitan mengusai hasil belajar 1.1 pada kompetensi dasar I dan hasil belajar 2.1 pada kompetensi 2.Sementara itu, Firman menghadapi masalah dalam menguasai hasil belajar 1.2 pada kompetensi dasar I dan hasil belajar 2.2 pada kompetensi 2.Begitu pula dengan Basir, Candra, Ika, dan Yudi menghadapi masalah yang berbeda.

2) *Menentukan alternatif pilihan tindakan*

Langkah ini merupakan lanjutan logis dari langkah pertama. Dari hasil penelaahan yang kita lakukan pada langkah pertama itu akan diperoleh kesimpulan mengenai dua hal pokok, yaitu:

a) Karakteristik khusus yang akan ditangani secara umum, dapat dikategorikan pada salah satu dari tiga kemungkinan dibawah ini:
   (1) Kasus yang bersangkutan dapat disimpulkan hanya memiliki kesulitan dalam menemukan dan mengembangkan pola strategi/metode/teknik belajar yang lebih sesuai, efektif dan efisien;
   (2) Kasus yang bersangkutan dapat disimpulkan disamping memiliki kesulitan dalam menemukan dan mengembangkan pola strategi/metode/teknik belajar yang lebih sesuai, efektif dan efisien itu, juga dihadapkan kepada hambatan-hambatan ego-emosional, potensial-fungsional, soaial-psikologis dalam penyesuaian dengan dirinya dan lingkungannya;
   (3) Kasus yang bersangkutan disimpulkan telah memiliki kecenderungan ke arah kemampuannya menemukan dan mengembangkan pola-pola strategi/metode/teknik belajar yang sesuai, efektif dan efisien namun terhambat oleh kondisi *ego*-emosional, sosial-psikologis dan faktor *instrumental-environmental* lainnya.
b) Alternatif pemecahan dianggap lebih strategis apabila:
   (1) Misalnya apabila kasusnya termasuk kategori yang pertama maka alternatif pemecahan masalahnyalangsung kepada langkah keempat yaitu pelaksanaan pengajaran remedial,
   (2) Misalnya kasusnya termasuk kategori kedua atau ketiga maka alternatif pemecahannya harus menempuh langkah ketiga (Layanan BK/Psikoterapi) dahulu sebelum lanjut ke langkah ke-4 yaitu pelaksanaan pengajaran remedial.

Dengan demikian, sasaran pokok kegiatan yang dilakukan dalam tahapan ini ialah membuat keputusan pilihan alternatif mana yang ditempuh berdasarkan pertimbangan rasional yang seksama. Berikut akan dipaparkan beberapa prinsip yang dijadikan dasar pertimbangan yang paling fundamental dalam proses pengambilan keputusan, yaitu:

a) *Efektivitas,* dalam arti lebih ampuh untuk menjamin tercapainya tujuan pengajaran remedial yang diharapkan,
b) *Efisiensi,* dalam arti lebih memerlukan usaha dan pengorbanan serta fasilitas seminimal mungkin dengan hasil yang diharapkan seoptimal mungkin.
c) *Keserasian,*dalam arti seseuaian dengan: (1) jenis karakteristik, intensitas, dan latar belakang permasalahannya; (2) jumlah, jenis, dan sifat kepribadian kasus; (3) tingkat penguasaan teori, kemahiran praktik, dan sifat kepribadian guru yang akan menanganinya; (4) kesediaan dan kecukupan daya dukung fasilitas teknis (instrument/bahan/sumber, dan sebagainya) yang diperlukan; (5) kesediaan dan kecukupan daya dukung/sarana penunjang/lingkungan (ruang/waktu dengan kelengkapannya, sikap/bantuan pihak lain) yang diperlukan; (6) waktu dan kesempatan yang tersedia pada pihak guru, pihak lain, dan yang bersangkutan.

Sudah barang tentu di atas semua pertimbangan itu, guru akhirnya harus mengambil keputusan atau tindakan alternatif bukan hanya atas dasar alasan-alasan teknis operasional belaka, melainkan juga pertimbangan etika dan tanggung jawab moral kemanusiaan bahwa kasus siswa itu amanat allah, Tuhan Yang Maha Esa, yang dititipkan kepadanya sehingga perlu dibantu demi kelangsungan dan kebahagiaan hidupnya. Seyogianya pertimbangan-pertimbangan lain pun seperti tanggung jawab administratif, tanggung jawab professional turut mewarnai keputusan yang akan diambil.

3) *Layanan bimbingan dan konseling/psikoterapi*

Langkah ini pada dasarnya bersifat pilihan bersyarat *(opimal dan conditional)* ditinjau dari kerangka keseluruhan prosedur pengajaran remedial.Dalam menghadapi kasus tipe kedua dan ketiga (baca paragraf pertama) kecil kemungkinannya langsung kepada langkah ke-4 (pelaksanaan pengajaran remedial), tanpa terlebih dahulu menempuh langkah ketiga yang merupakan *pra kondisinya.*

Oleh karena itu, sasaran pokok yang hendak dituju oleh layanan ini ialah terciptanya kesehatan mental (*kasus mental health),* dalam arti ia terbebas dari hambatan dan ketegangan batinnya untuk kemudian siap

sedia kembali melakukan kegiatan belajar secara wajar dan realistis. Di dalam praktiknya, langkah ini kemungkinan pada bagian-bagian tertentu masih dapat ditangani oleh guru yang bersangkutan yang sudah cukup berpengalaman dan dianugerahi sifat-sifat kepribadian yang cocok untuk tugas tersebut, dan lebih maksimal hasilnya apabila dalam kegiatan tersebut sang guru dibantu oleh petugas BK, wali kelas, psikolog, dokter, dan sebagainya).

Di antara sekian banyak masalah kesulitan penyesuaian, yang masih dapat ditangani oleh para guru pada umumnya, diantaranya:

a) *Kasus kesulitan belajar dengan latar belakang kurangnya motivasi dan minat belajar*

Meningkatkan motivasi belajar siswa adalah salah satu kegiatan integral yang wajib ada dalam kegiatan pembelajaran.Selain memberikan dan mentransfer ilmu pengetahuan, guru juga bertugas untuk meningkatkan motivasi dan minat siwa untuk belajar.Tak bisa dipungkiri bahwa motivasi belajar siswa satu dengan yang lainnya sangat berbeda, untuk itu penting bagi guru untuk selalu senantiasa memberikan motivasi kepada siswa supaya siswa senantiasa memiliki semangat belajar dan mampu menjadi siswa yang berprestasi serta dapat mengembangkan diri secara optimal.

Proses pembelajaran akan berhasil manakala siswa mempunyai motivasi dalam belajar. Tetapi bagaiman dengan siswa yang mengalami kesulitan belajar disebabkan oleh kurangnya motivasi dan minat dalam belajar? Berikut ini akan kita bahas mengenai beberapa cara atau teknik yang disarankan oleh kaum psikolog dan pendidik untuk membantu kasus tipe ini menurut (Wina Senjaya 2008) adalah:

(1)Memperjelas tujuan yang ingin dicapai.

Tujuan yang jelas dapat membuat siswa paham kearah mana ia ingin dibawa. Pemahaman siswa terhadap tujuan pembelajaran dapat menumbuhkan minat siswa untuk belajar yang pada gilirannya dapat meningkatkan motivasi belajar mereka. Semakin jelas tujuan yang ingin dicapai, maka akan semakin kuat motivasi belajar siswa. Oleh sebab itu, sebelum

proses pembelajaran dimulai hendaknya guru menjelaskan terlebih dahulu tujuan yang ingin dicapai.

(2) Membangkitkan minat siswa.

Siswa akan terdorong untuk belajar manakala mereka memiliki minat untuk belajar. Oleh karena itu, mengembangkan minat belajar siswa merupakan salah satu teknik dalam mengembangkan motivasi belajar. Salah satu cara yang logis untuk momotivasi siswa dalam pembelajaran adalah mengaitkan pengalaman belajar dengan minat siswa. Pengaitan pembelajaran dengan minat siswa adalah sangat penting, dan karena itu tunjukkanlah bahwa pengetahuan yang dipelajari itu sangat bermanfaat bagi mereka. Demikian pula tujuan pembelajaran yang penting adalah membangkitkan hasrat ingin tahu siswa mengenai pelajaran yang akan datang, dan karena itu pembelajaran akan mampu meningkatkan motivasi instrinsik siswa untuk mempelajari materi pembelajaran yang disajikan oleh guru.

(3) Ciptakan suasana yang menyenangkan dalam belajar.

Siswa hanya mungkin dapat belajar baik manakala ada dalam *suasana* yang menyenangkan, merasa aman, bebas dari takut. Usahakan agar kelas selamanya dalam suasana hidup dan segar, terbebas dari rasa tegang. Untuk itu guru sekali-kali dapat melakukan hal-hal yang lucu.

(4) Menggunakan variasi metode penyajian yang menarik.

Guru harus mampu menyajikan informasi dengan menarik, dan asing bagi siswa-siswa. Sesuatu informasi yang disampaikan dengan teknik yang baru, dengan kemasan yang bagus didukung oleh alat-alat berupa sarana atau media yang belum pernah dikenal oleh siswa sebelumnya sehingga menarik perhatian bagi mereka untuk belajar.Dengan pembelajaran yang menarik, maka akan membangitkan rasa ingin tahu siswa di dalam kegiatan pembelajaran yang selanjutnya siswa akan termotivasi dalam pembelajaran

(5) Berilah komentar terhadap hasil pekerjaan siswa.

Siswa butuh penghargaan.Penghargaan bisa dilakukan dengan mmemberikan komentar yang positif. Setelah siswa selesai mengerjakan suatu tugas, sebaiknya berikan komentar secepatnya, misalnya dengan memberikan tulisan " bagus" atau "teruskan pekerjaanmu" dan lain sebagainya. Komentar yang positif dapat meningkatkan motivasi belajar siswa, Sebaliknya pemberian celaan kurang menumbuhkan motivasi dalam belajar.Bahkan menimbulkan efek psikologis yang lebih jelek.

(6) Ciptakan persaingan dan kerjasama

Persaingan yang sehat dapat menumbuhkan pengaruh yang baik untuk keberhasilan proses pemebelajaran siswa. Melalui persaingan siswa dimungkinkan berusaha dengan sungguh-sungguh untuk memperoleh hasil yang terbaik).Oleh sebab itu, guru harus mendesain pembelajaran yang memungkinkan siswa untuk bersaing baik antar kelompok maupun antar individu.

(7) Berikan penilaian

Banyak siswa yang belajar karena ingin memperoleh nilai bagus.Untuk itu mereka belajar dengan giat.Bagi sebagian siswa nilai dapat menjadi motivasi yang kuat untuk belajar.Oleh karena itu, penilaian harus dilakukan dengan segera agar siswa secepat mungkin mengetahui hasil kerjanya.Penilaian harus dilakukan secara objektif sesuai dengan kemampuan siswa masing-masing.

Penilaian secara terus menerus akan mendorong siswa belajar, oleh karena setiap anak memilki kecenderungan untuk memperoleh hasil yang baik. Disamping itu, para siswa selalu mendapat tantangan dan masalah yang harus dihadapi dan dipecahkan, sehingga mendorongnya belajar lebih teliti dan seksama.

b) Kasus kesulitan belajar yang berlatar belakang sikap negatif terhadap guru, pelajaran dan situasi belajar.

Pengelolaan kelas merupakan usaha dalam mengatur segala hal dalam proses pembelajaran, seperti lingkungan fisik dan sistem pembelajaran di kelas.Strategi belajar apapun yang ditempuh guru

akan menjadi tidak efektif jika tidak didukung dengan iklim dan kondisi kelas yang kondusif. Oleh karena itu guru perlu menata dan mengelola lingkungan belajar di kelas sedemikian rupa sehingga menyenangkan, aman, dan menstimulasi setiap anak agar terlibat secara maksimal dalam proses pembelajaran. Ada beberapa alternatif teknik yang disarankan untuk membina sikap positif terhadap belajar dan mengembangkan situasi belajar dengan pengaturan lingkungan belajar, antara lain:

(1) Ciptakan iklim sosial yang sehat didalam kelas atau kelompok studi baik antara siswa dan siswa maupun antara siwa dan guru.

(2) Berikan kesempatan memperoleh pengalaman yang menyenangkan dan memuaskan atau memperoleh kesempatan untuk sukses dalam belajar meskipun prestasi yang dimiliki sangat rendah sekalipun.

(3) Maksimalkan teknologi, Salah satu alat yang membantu guru untuk menciptakan suasana aktif dan segar adalah teknologi. Manfaatkan teknologi yang ada, seperti laptop, internet dan projektor untuk mengubah materi pelajaran text book ke audio visual. Dengan penyajian yang baik dan menarik, fokus anak akan lebih terarah pada materi yang disampaikan. Jangan ragu untuk mengotak-atik atau membuat sesuatu yang berbeda dengan teknologi.

c) *Kasus kesulitan belajar dengan latar belakang kebiasaan belajar yang salah.*

Ada banyak faktor mengapa anak memiliki kebiasaan salah dalam belajar. Faktor-faktor tersebut adalah:

(1) Faktor lingkungan

Faktor lingkungan yang turut mendorong terjadinya kebiasaan buruk anak dalam belajar antara lain adalah : lingkungan fisik rumah yang tidak mendukung, fasilitas belajar yang terbatas, lingkungan keluarga yang tidak berpendidikan, Kontrol yang lemah dari orangtua, lingkungan sekolah yang kurang mendorong tumbuhnya semangat untuk belajar di rumah, lingkungan masyarakat yang kurang mendukung terhadap iklim

belajar yang baik, anak banyak berteman dengan kelompok yang malas belajar.

(2) Faktor pribadi anak

Faktor pribadi anak mengapa memiliki kebiasaan buruk dalam belajar, dapat disebabkan hal-hal sebagai berikut : motivasi yang rendah, *need for achievement* anak rendah, kesehatan anak yang terganggu, tidak tahu bagaimana belajar yang baik, tidak ada kedisplinan dalam belajar, tidak bisa mengatur waktu, anak salah memilih teman bergaul.

Berikut kami paparkan beberapa cara yang disarankan bisa membantu menyelesaikan kasus kebiasaan salah dalam belajar antara lain:

(1) Tunjukkan akibat atau pengaruh kebiasaan yang salah terhadap prestasi belajar dan kehidupan seseorang;

(2) Berikan kesempatan masa transisi untuk berlatih dengan pola-pola kebiasaan baru dan meninggalkan kebiasaan lama yang salah. .

4) *Melaksanakan pengajaran remedial*

Setelah kita mengatahui siswa-siswa yang perlu mendapatkan kegiatan remedial, faktor-faktor penghambat siswa dalam menguasai kompetensi pembelajaran yang telah ditentukan atau menguasai materi pelajaran, dan kompetensi-kompetensi apa saja yang belum dikuasai oleh oleh setiap siswa, langkah selanjutnya adalah melaksanakan kegiatan/pengajaean remedial. Tetapi sebelumnya pelaksanaan dimulai ada baiknya kita menyusun perencanaan kegiatan remedial sebelumnya. Sama halnya dengan pembelajaran biasa, komponen-komponen yang harus diperhatikan dalam perencanaan kegiatan remedial adalah:

a) Merumuskan kompetensi atau tujuan pembelajaran.

b) Menemukan materi pelajaran sesuai dengan kompetensi atau tujuan yang telah dirumuskan.

c) Memilih dan merancang kegiatan remedial sesuai dengan masalah dan faktor penyebab kesulitan serta karakteristik siswa.

d) Merencanakan waktu yang diperlukan untuk melaksanakan kegiatan remedial.

e) Menentukan jenis, prosedur dan alat penilaian untuk mengetahui tingkat keberhasilan siswa.

Setelah rencana pembelajaran/kegiatan remedial selesai disusun langkah selanjutnya adalah melaksanakan kegiatan remedial.Mungkin anda bertanya kapan waktu yang tepat kegiatan remedial ini diadakan.Jawabannya adalah segera setelah rencana tersebut disusun.Semakin cepat siswa dibantu mengatasi kesulitan yang dihadapinya, maka semakin besar pula kemungkinan siswa tersebut berhasil dalam belajarnya. Biasanya kegiatan remedial diadakan diluar jam belajar biasa. Oleh karena itu, dituntut kerelaan dan keikhlasan dari guru untuk menyediakan atau menyisihkan waktu tambahan diluar jam belajar untuk membantu siswa yang memerlukan bantuan.

5) *Mengadakan pengukuran prestasi belajar kembali*

Dengan selesainya dilakukan pengajaran remedial, langkah selanjutnya adalah mendeteksi ada tidaknya perubahan pada diri individu yang memiliki kasus.Oleh karena itu, perlu diadakan pengukuran kembali.Hasil dari pengukuran ini akan memberikan informasi seberapa jauh atau seberapa besar perubahan telah terjadi, baik dalam arti kuantitatif maupun kualitatif. Cara dan instrument yang digunakan dalam pengukuran pada langkah ini sebaiknya sama dengan apa yang digunakan pada waktu post-test atau tes sumatif dari proses belajar mengajar utama atau reguler.

Apabila siswa telah mencapai kemajuan seperti yang kita harapkan, berarti kegitan remedial yang kita rencanakan dan laksanakan cukup efektif untuk membantu siswa yang mengalami kesulitan belajar.Tetapi apabila siswa tidak mengalami kemajuan dalam belajarnya atau belum mencapai kemajuan belajar yang diharapkan berarti rencana dan pelaksanaan kegiatan remedial kurang efektif. Untuk itu, guru harus menganalisis setiap komponen pembelajaran, dengan mengajukan pertanyaan sebagai berikut:

Kompetensi atau tujuan: Apakah kompetensi atau tujuan yang dirumuskan terlalu tinggi atau terlalu rendah bagi siswa?

Materi	:	Apakah materi prasyarat yang belum dikuasai oleh siswa?
Kegiatan	:	Apakah kegiatan remedial yang diterapkan sesuai dengan kebutuhan dan kemampuan siswa?
Waktu	:	Apakah waktu yang disediakan cukup atau kurang?
Penilaian	:	Apakah alat penilaian yang digunakan sesuai dengan kompetensi atau tujuan yang telah ditetapkan? .

2. Pelaksanaan Pengajaran Pengayaan

Pemberian pembelajaran pengayaan pada hakikatnya adalah pemberian bantuan bagi peserta didik yang memiliki kemampuan lebih(di atas rata-rata), baik dalam kecepatan maupun kualitas belajarnya.Agar pemberian pengayaan tepat sasaran maka perlu ditempuh langkah-langkah sistematis, yaitu (1) mengidentifikasi kelebihan kemampuan peserta didik, dan (2) memberikan perlakuan (treatment) pembelajaran pengayaan.

a. Identifikasi Kelebihan Kemampuan Belajar

1) Tujuan

Identifikasi kemampuan berlebih peserta didik dimaksudkan untuk mengetahui jenis serta tingkat kelebihan belajar peserta didik. Kelebihan kemampuan belajar itu antara lain meliputi:

a) Belajar lebih cepat.

Peserta didik yang memiliki kecepatan belajar tinggi ditandai dengan cepatnya penguasaan kompetensi (SK/KD) mata pelajaran tertentu.

b) Menyimpan informasi lebih mudah

Peserta didik yang memiliki kemampuan menyimpan informasi lebih mudah, akan memiliki banyak informasi yang tersimpan dalam memori/ingatannya dan mudah diakses untuk digunakan.

c) Keingintahuan yang tinggi.

Banyak bertanya dan menyelidiki merupakan tanda bahwa seorang peserta didik memiliki hasrat ingin tahu yang tinggi.

d) Berpikir mandiri.

Peserta didik dengan kemampuan berpikir mandiri umumnya lebih menyukai tugas mandiri serta mempunyai kapasitas sebagai pemimpin.

e) Superior dalam berpikir abstrak.

Peserta didik yang superior dalam berpikir abstrak umumnya menyukai kegiatan pemecahan masalah.

f) Memiliki banyak minat.

Mudah termotivasi untuk meminati masalah baru dan berpartisipasi dalam banyak kegiatan.

2) Teknik

Teknik yang dapat digunakan untuk mengidentifikasi kemampuan berlebih peserta didik dapat dilakukan antara lain melalui: tes IQ, tes inventori, wawancara, pengamatan, dsb.

a) Tes IQ (Intelligence Quotient) adalah tes yang digunakan untuk mengetahui tingkat kecerdasan peserta didik. Dari tes ini dapat diketahui tingkat kemampuan spasial, interpersonal, musikal, intrapersonal, verbal, logik/matematik, kinestetik, naturalistik, dsb.

b) Tes inventori. Tes inventori digunakan untuk menemukan dan mengumpulkan data mengenai bakat, minat, hobi, kebiasaan belajar, dsb.

c) Wawancara. Wanwancara dilakukan dengan mengadakan interaksi lisan dengan peserta didik untuk menggali lebih dalam mengenai program pengayaan yang diminati peserta didik.

d) Pengamatan (observasi). Pengamatan dilakukan dengan jalan melihat secara cermat perilaku belajar peserta didik. Dari pengamatan tersebut diharapkan dapat diketahui jenis maupun tingkat pengayaan yang perlu diprogramkan untuk peserta didik.

b. Bentuk Pelaksanaan Pembelajaran Pengayaan

Bentuk-bentuk pelaksanaan pembelajaran pengayaan dapat dilakukan antara lain melalui:

1) Belajar Kelompok. Sekelompok peserta didik yang memiliki minat tertentu diberikan pembelajaran bersama pada jam-jam pelajaran sekolah biasa, sambil menunggu teman-temannya yang mengikuti pembelajaran remedial karena belum mencapai ketuntasan.
2) Belajar mandiri. Secara mandiri peserta didik belajar mengenai sesuatu yang diminati.
3) Pembelajaran berbasis tema. Memadukan kurikulum di bawah tema besar sehingga peserta didik dapat mempelajari hubungan antara berbagai disiplin ilmu.
4) Pemadatan kurikulum. Pemberian pembelajaran hanya untuk kompetensi/materi yang belum diketahui peserta didik. Dengan demikian tersedia waktu bagi peserta didik untuk memperoleh kompetensi/materi baru, atau bekerja dalam proyek secara mandiri sesuai dengan kapasitas maupun kapabilitas masing-masing.

Perlu diperhatikan bahwa penyelenggaraan pembelajaran pengayaan ini terutama terkait dengan kegiatan tatap muka untuk jam-jam pelajaran sekolah biasa.Namun demikian kegiatan pembelajaran pengayaan dapat pula dikaitkan dengan kegiatan tugas terstruktur dan kegiatan mandiri tidak terstruktur.Sekolah dapat juga memfasilitasi speserta didik dengan kelebihan kecerdasan dalam bentuk kegiatan pengembangan diri dengan spesifikasi pengayaan kompetensi tertentu, misalnya untuk bidang sains.Pembelajaran seperti ini diselenggarakan untuk membantu peserta didik mempersiapkan diri mengikuti kompetisi tingkat nasional maupun internasional seperti olimpiade internasional fisika, kimia dan biologi.

Sebagai bagian integral dari kegiatan pembelajaran, kegiatan pengayaan tidak lepas kaitannya dengan penilaian. Penilaian hasil belajar kegiatan pengayaan, tentu tidak sama dengan kegiatan pembelajaran biasa, tetapi cukup dalam bentuk portofolio, dan harus dihargai sebagai nilai tambah (lebih) dari peserta didik yang normal.

D. Aktivitas Pembelajaran

Adapun inti dari aktivitas pembelajaran modul ini bagi peserta diklat adalah sebagai berikut: Alokasi waktu yang disediakan untuk pembelajaran II ini adalah 100 menit atau 2 x 50 menit, dengan rincian sebagai berikut:

Tabel 3.Aktivitas Kegiatan pembelajaran II

No.	Waktu	Kegiatan
1.	20 menit	Apersepsi yang berkaitan dengan kegiatan mengidentifikasi dan memehami prosedur remedial dan pengayaan**.**
2.	50 menit	• Membagi kelompok diskusi. • Mendiskusikan (1) Menjelaskan prosedur pengajaran remedial, dan (2) Menjelaskan langkah-langkah pelaksanaan pengajaran pengayaan
3.	30 menit	Menyajikan/mensimulasikan prosedur remedial dan pengayaan yang terdapat pada pembelajaran II terhadap peserta diklat

E. Latihan/ Kasus/ Tugas

1. Faktor manakah yang terdapat dalam lingkungan yang diduga merupakan sumber penyebab utama kesulitan yang dialami oleh siswa?

   ……

   ……

2. Komponen output turut menjadi salah satu sebab kesulitan belajar-mengajar, adalah…

   ……

   ……

3. Bentuk pelaksanaan pembelajaran pengayaan adalah…

   ……

   ……

F. Rangkuman

Prosedur pengajaran remedial merupakan salah satu tahapan kegiatan utama dalam keseluruhan kerangka pola layanan bimbingan belajar. Langkah-langkah yang harus ditempuh dalam kegiatan remedial adalah:

1. Diagnostik kesulitan belajar mengajar

2. Penelaan kembali kasus
3. Pilihan alternatif tindakan
4. Layanan penyuluhan/psikoterapi
5. Pelaksanaan layanan pengajaran remedial
6. Post-tes/ pengukuran kembali hasil belajar mengajar
7. Re-evaluasi Re-diagnostik
8. Tugas tambahan

Prosedur pengajaran pengayaan adalah langkah-langkah sistematis, yaitu (1) mengidentifikasi kelebihan kemampuan peserta didik, dan (2) memberikan perlakuan (treatment) pembelajaran pengayaan. Dan hal ini terbagi menjadi beberapa bagian antara lain:

1. Identifikasi Kelebihan Kemampuan Belajar

   Identifikasi kemampuan berlebih peserta didik dimaksudkan untuk mengetahui jenis serta tingkat kelebihan belajar peserta didik
2. Bentuk Pelaksanaan Pembelajaran Pengayaan

   Bentuk-bentuk pelaksanaan pembelajaran pengayaan dapat dilakukan antara lain melalui: a) Belajar Kelompok, b) Belajar mandiri, c) Pembelajaran berbasis tema, d) Pemadatan kurikulum.

G. Umpan Balik dan Tindak Lanjut

Adapun umpan balik dalam kegiatan Pembelajaran II ini adalah: jawablah semua latihan pada Kegiatan Pembelajaran ini. Kemudian cocokkan jawaban Anda dengan kunci jawaban dan nilai hasilnya.Apabila benar semua, maka pemahaman Anda 100 %.Apabila salah satu, maka pemahaman Anda 80 %.Apabila yang salah ada dua, maka pemahaman Anda 60 %.Apabila yang salah salah ada tiga, maka pemahaman 40 %. Apabila yang salah ada empat atau lima, maka pemahaman 20 %, dan apabila semua, maka pemahaman 0%.

Selanjutnya apabila Anda mendapatkan hasil 80 % ke atas, maka Anda dinyatakan lulus dan silahkan melanjutkan ke Kegiatan Pembelajaran III, akan tetapi apabila mendapatkan 0 %, 25 %, 40 % atau 60 %, maka Anda diminta membaca dan memahami isi modul kembali dan menjawab latihan-latihan yang telah disiapkan

H. Kunci Jawaban

Kunci jawaban essay

1. Faktor manakah yang terdapat dalam lingkungan yang diduga merupakan sumber penyebab utama kesulitan yang dialami oleh siswa?
   a. *Di sekolah:* apakah iklim sosial cukup sehat dan merangsang untuk belajar (interaksi siswa dengan guru, siswa dengan siswa, siswa dengan personel sekolah lainnya),
   b. *Di rumah:* apakah iklim iklim rumah sudah kondusif, nyaman, dan tersedianya daya dukung fasilitas belajar yang cukup tersedia,
   c. *Di masyarakat:* apakah cukup tersedia ruang/tempat *(space)* memperkaya pengalaman belajar (perpustakaan umum, fasilitas rekreasi, pusat kegiatan belajar, dan sebagainya).
2. Apakah komponen output turut menjadi salah satu sebab kesulitan belajar-mengajar?
   a. Terlalu tingginya tuntutan standar (kriteria atau indikator keberhasilan) hasil belajar *(level of mastery* 90% atau lebih)
   b. Terlalu menekankan pada satu aspek saja (kognitif saja, keterampilan atau psikomotor saja, sedangkan yang lainnya diabaikan
   c. Tidak adanya patokan sebagai ukuran baku yang dapat dijadikan pedoman baku/umum bagi setiap guru dan siswa.
3. Bentuk Pelaksanaan Pembelajaran Pengayaan yaitu

   Bentuk-bentuk pelaksanaan pembelajaran pengayaan dapat dilakukan antara lain melalui:

   5) Belajar Kelompok. Sekelompok peserta didik yang memiliki minat tertentu diberikan pembelajaran bersama pada jam-jam pelajaran sekolah biasa, sambil menunggu teman-temannya yang mengikuti pembelajaran remedial karena belum mencapai ketuntasan.
   6) Belajar mandiri. Secara mandiri peserta didik belajar mengenai sesuatu yang diminati.
   7) Pembelajaran berbasis tema. Memadukan kurikulum di bawah tema besar sehingga peserta didik dapat mempelajari hubungan antara berbagai disiplin ilmu.
   8) Pemadatan kurikulum. Pemberian pembelajaran hanya untuk kompetensi/materi yang belum diketahui peserta didik. Dengan

demikian tersedia waktu bagi peserta didik untuk memperoleh kompetensi/materi baru, atau bekerja dalam proyek secara mandiri sesuai dengan kapasitas maupun kapabilitas masing-masing.

3

KEGIATAN PEMBELAJARAN

Kegiatan Pembelajaran III

Strategi Remedial dan Pengayaan

A. Tujuan

1. Peserta diklat diharapkan mampu menjelaskan strategi yang dipergunakan dalam pelaksanaan pengajaran remedial
2. Peserta diklat diharapkan mampu membedakan strategi pengajaran remedial dari strategi pembelajaran biasa
3. Perserta diklat diharapkan mampu menganalisis strategi pengajaran remedial

B. Indikator Pencapaian Kompetensi

1. Menjelaskan strategi yang dipergunakan dalam pelaksanaan pengajaran remedial
2. Membedakan strategi pengajaran remedial dari strategi pembelajaran biasa
3. Menganalisis strategipengajaran remedial

C. Uraian Materi

1. Pengertian strategi pengajaran

Strategi pengajaran merupakan suatu serangkaian rencana kegiatan yang termasuk didalamnya penggunaan metode dan pemanfaatan berbagai sumber daya atau kekuatan dalam suatu pembelajaran.Strategi pengajaran disusun untuk mencapai suatu tujuan tertentu.Strategi pengajaran mencakup pendekatan, model, metode, dan teknik pembelajaran yang spesifik.

Menurut Newman dan Logan (Abin Syamsuddin Makmun, 2003), ada empat unsur strategi dari setiap usaha, yaitu:

a. Mengidentifikasi dan menetapkan spesifikasi dan kualifikasi hasil (*out put*) dan sasaran (*target*) yang harus dicapai, dengan mempertimbangkan aspirasi dan selera masyarakat yang memerlukan.
b. Mempertimbangkan dan memilih jalan pendekatan utama (basic way) yang paling efektif untuk mencapai sasaran
c. Mempertimbangkan dan menetapkan langkah-langkah (steps) yang akan ditempuh sejak titik awal sampai dengan sasaran

d. Mempertimbangkan dan menetapkan tolok ukur (kriteria) dan patokan ukuran untuk mengukur dan menilai taraf keberhasilan

Keempat unsur tersebut, jika diimplementasikan dalam konteks pembelajaran adalah sebagai berikut:

a. Menetapkan spesifikasi dan kualifikasi tujuan pembelajaran yakni perubahan perilaku peserta didik
b. Mempertimbangkan dan memilih system pendekatan pembelajaran yang dianggap paling efektif
c. Mempertimbangkan dan menetapkan langkah-langkah atau prosedur, metode dan teknik pembelajaran
d. Menetapkan norma-norma dan batas minimal ukuran keberhasilan pembelajaran

Secara umum strategi adalah suatu garis-garis besar haluan yang untuk bertindak dalam usaha mencapai sasaran yang telah ditentukan /ingin dicapai.Dalam kegiatan belajar mengajar, strategi dapat diartikan sebagai pola-pola umum kegiatan belajar mengajar yang melibatkan antara kegiatan guru dan anak didik untuk mencapai tujuan yang telah digariskan dari pembelajaran itu sendiri.

2. Strategi dan pendekatan remedial

Strategi belajar mengajar pada pengajaran biasa yaitu kelas klasikal, dimana siswa berkumpul dalam satu kelas untuk mendapat pengajaran dengan metode yang sama untuk semua siswa, pendekatan dan teknik yang sama serta pemberian evaluasi (ulangan) menggunakan alat yang sama (seragam) untuk semua siswa. Sedang pada pengajaran remedial strategi yang diberikan bersifat individual sesuai TIK yang mana yang sulit dan belum dituntaskan oleh siswa, metode penyampaian tidak sama antar satu siswa dengan siswa lainnya hal ini tergantung sejauh mana kesulitan siswa belajar, biasanya melibatkan berbagai pihak seperti guru bidang studi dan BP, alat evaluasi yang digunakan disesuaikan dengan kesulitan belajar yang dihadapi oleh siswa. Selanjutnya mengenai bahan pengajaran, untuk bahan pengajaran biasa lebih banyak dan luas, sedang bahan pengajaran untuk remedial hanya tertentu saja, yakni pada bahan yang belum dikuasai oleh siswa saja (Edwan, 2015)

a. Menelaah kembali siswa yang akan diberikan bantuan. Kegiatan ini dimaksudkan agar kita memperoleh gambaran berapa lama bantuan harus diberikan, kapan oleh siapa dan sebagainya.
b. Alternatif tindakan. Jika sudah mendapat gambaran lengkap. Lalu tentukan alternatif tindakan dapat berupa :
    1) Disuruh mengulangi bahan yang telah diberikan dengan memberikan arahan terlebih dulu
    2) Disuruh mencoba alternatif kegiatan lain yang setara dengan kegiatan belajar mengajar yang sudah ditempuhnya dan mempunyai tujuan yang sama
    3) Bila kesulitan belajar bukan karena kesulitan belajar, tapi karena faktor lain seperti sikap negatif terhadap guru, situasi belajar dan sebagainya maka siswa perlu dibimbing oleh konselor. Jika sudah mampu mengatasi masalah maka dapat diberi pengajaran remedial.

Banyak siswa yang mengalami kesulitan dalam belajar misalnya tidak mampu menyerap bahan pembelajaran dengan baik, tidak dapat konsentrasi dalam belajar, tidak mampu mengerjakan tes dan sebagainya.siswa yang mengalami kesulitan belajar yang mengakibatkan prestasi belajarnya rendah, maka guru atau konselor harus memberikan layanan bimbingan dengan baik. Layanan tersebut lebih dikenal dengan pengajaran remedial.Bagi peserta didik yang tidak mengalami kesulitan belajar tidak berarti harus didiamkan saja, mereka juga perlu mendapatkan penanganan tersendiri, kalau tidak mereka akan mengalami penyimpangan karena kepuasan intelektual mereka tidak terpenuhi. Layanan bimbingan belajar bagi peserta didik yang tidak mengalami kesulitan belajar lebih dikenal dengan pengayaan atau *enrichement*.

Sasaran akhir pengajaran remedial identik dengan pengajaran biasa (pada umumnya), yaitu membantu setiap siswa dalam batas-batas normalitas tertentu agar dapat mengembangkan diri seoptimal mungkin sehingga dapat mencapai tingkat penguasaan atau ketuntasan (*level of mastery*) tertentu, sekurang-kurangnya sesuai dengan batas-batas criteria keberhasilan yang dapat diterima (*minimum acceptable performance*) (Makmun, 357:2012)

Mengingat secara empirik sasaran tingkat strategis itu tidak selamanya dapat dicapai dengan pendekatan sistem pengajaran konvensional, maka

perlu dicari upaya pendekatan strategis lainnya. Strategi dan pendekatan remedial diklasifikasikan menjadi tiga yaitu:

a. Strategi dan pendekatan pengajaran remedial yang bersifat kuratif

Tindakan pengajaran remedial dikatakan bersifat kuratif kalau dilakukan setelah program PBM utama selesai diselenggarakan. Tindakan ini didasarkan atas kenyataan empirik bahwa ada seseorang atau sejumlah orang atau bahkan mungkin sebagian besar atau seluruh anggota kelas/kelompok belajar dapat dipandang tidak mampu menyelesaikan proses PBM secara sempurna, sesuai dengan criteria keberhasilan yang ditetapkan. Program PBM dapat diartikan sebagai program untuk tiap pertemuan, untuk satuan (unit) bahan pelajaran atau satuan waktu (mingguan, bulanan, triwulan, semesteran, tahunan dan sebagainya) tertentu (Makmun, 2012:357).

Pengajaran remedial dapat dikatakan bersifat kuratif apabila dilakukan setelah berlangsungnya program belajar mengajar sesuai dengan kriteria keberhasilan yang ditetapkan. Pendekatan kuratif tindakan remedial berpangkap dari hasil *post test diagnostic* berdasarkan data-data hasil tes sumatif.Adapun yang menjadi sasaran pokok pengajaran remedial yang bersifat kuratif adalah:

1) Murid yang prestasinya jauh dibawah kriteria keberhasilan, diusahakan pada suatu saat tertentu dapat mencapai kriteria keberhasilan minimal tersebut.
2) Murid yang masih kurang sedikit dari keberhasilan minimal diupayakan suatu saat dapat disempurnakan

Gambar 3.1 Diagram langkah pengajaran remedial
Sumber: Makmun, (2012)

Untuk mencapai sasaran-sasaran pokok tersebut para ahli psikologi pendidikan telah mengembangkan beberapa teknik pendekatan yaitu pendekatan pengulangan *(repeatition),* pengayaan *(enrichment)* serta kecepatan *(accelleration)* yang secara visual dalam bagan berikut:

1) Pendekatan Pengulangan *(repeatition)*

   Sejalan dengan diagnosisnya, pengulangan terdiri dari beberapa tingkatan :

   a) Pada setiap akhir jam pertemuan tertentu
   b) Pada setiap akhir unit (satuan bahan) pelajaran tertentu
   c) Pada akhir setiap satuan program studi (triwulan/semester)

   Pelaksanaan layanan pengajaran remedial mungkin diberikan dan diorganisasikan:

   a) Secara perseorangan (Individual), kalau ternyata siswa yang memerlukan bantuan itu jumlahnya terbatas atau.
   b) Secara kelompok (peers gorup), kalau ternyata terdapat sejumlah siswa yang mempunyai jenis/lokasi/sifat kesalahan atau kesulitan bersama, bukan mustahil terjadi juga dalam bidang studi tertentu dialami oleh kelas secara keseluruhan (Makmun, 2012:359)

   Pengajaran remedial dapat diberikan dan diorganisasi secara individual maupun secara kelompok.Secara individual apabila ternyata murid mempunyai jenis/lokasi/sifat kesulitan belajar yang sama. Ada beberapa kemungkinan waktu dan cara pelaksanaan pengajaran remedial yaitu:

   a) Dilaksanakan pada pertemuankelas biasa, jika memang sebagian besar anggota kelas mengalami kesulitan yang serupa, di mana:
      1) Bahan pelajaran dipresentasikan kembali
      2) Diadakan latihan/penugasan soal kembali yang bentuknya sejenis dengan soal terdahulu;
      3) Diadakan pengukuran dan penilaian kembali untuk mendeteksi hasil peningkatannya ke arah keberhasilan yang diharapkan.
   b) Dilakukan diluar jam pertemuan biasa, jika yang mengalami kesulitan belajar itu hanya seorang murid atau sejumlah murid tertentu. Misalnya:

1) Diadakan jam pelajaran tambahan pada hari/jam tempat tertentu, kalau yang mengalami kesulitan itu hanya seseorang/sejumlah orang tertentu, kalau yang mengalami kesulitan itu hanya seorang/sejumlah orang tertentu (umpamanya, pada sore hari, sehabis jam pelajaran biasa, waktu istirahat untuk siswa dan lain sebagainya)
2) Diberikan dalam bentuk pekerjaan rumah (home work) dengan diperiksa kembali hasil pekerjaannya oleh guru (Mkmun, 2012:360)

c) Dilaksanakan pada kelas remedial (khusus bagi murid), yang mengalami kesulitan belajar tertentu, dimana :
1) Murid lain belajar dalam kelas biasa, sednagkan murid tertentu belajar dengan mendapatkan bimbingan khusus dari guru yang sama atau guru mata pelajaran sampai yang bersangkutan mencapai tingkat penguasaan tertentu untuk kemudian bersama-sama lagi dengan teman-temannya dikelas biasa
2) Dilakukan pengulangan secara total, jika ternyata murid yang bersangkutan prestasinya sangat jauh dari batas kriteria keberhasilan minimal yang kita kenal sebagai tinggal kelas

d) Diadakan pengulangan secara total, kalau ternyata siswa yang bersangkutan prestasinya sangat jauh dari batas kriteria keberhasilan minimal dalam hampir keseluruhan program (komponen bidang studinya); secara konvensional kita kenal sebagai tinggal kelas.

2) Pengayaan dan Penguatan(*enrichment and reinforcement*)

Pengayaan adalah kegiatan tambahan yang di berikan kepada siswa yang telah mencapai ketentuan dalam belajar yang dimaksudkan untuk menambah wawasan atau memperluas pengetahuannya dalam materi pelajaran yang telah dipelajarinya.Di samping itu pembelajaran pengayaan bisa juga diartikan memberikan pemahaman yang lebih mendalam dari pada sekedar standar kompotensi dalam kurikulum.

Kalau layanan pengulangan ditujukan kepada siswa yang mempunyai kelemahan sangat mendasar, layanan pengayaan ditujukan kepada siswa yang mempunyai kelemahan yang ringan bahkan secara akademik mungkin sangat kuatdan berbakat(*the gifted, the accelerated students*)

Layanan pengayaan diberikan kepada murid yang mempunyai kelemahan ringan, dengan materi program pengayaan bersifat :

a) Ekuivalen (horizontal) dengan program proses belajar mengajar utamanya sehingga nilai bobot kredit dapat perhitungkan bagi murid yang bersangkutan.
b) Sekedar suplementer terhadap program proses belajar utama tanpa menambah bobot kredit tertentu yang penting dapat meningkatkan penguasaan pengetahuan, keterampilanbagi murid yang relatif lemahdan memberikan kesibukan kepada murid yang cepat belajar untuk mengisi kelebihan waktunya dibandingkan teman-teman sekelasnya.

Sasarannya ditujukan kepada siswa yang mempunyai kelemahan ringan atau bahkan siswa yang mempunyai kemampuan tingi atau unggul, materi yang diberikan yaitu yang masih ada kaitannya (ekuivalen). Dengan materi pokok atau dapat juga merupakan tambahan (suplementer) sehingga akan memperoleh cakrawala yang lebih luas dari materi tersebut. Dengan demikian bagi siwa yang berkemampuan lebih mempunyai kesibukan yang bersifat positif.Baik bagi dirinya maupun bagi lingkungannya, sedang kemampuannya dapat ditingkatkan secara optimal. Pelaksanaannya dapat dengan memberikan tugas-tugas (take home) bakat siswa yang lemah dengan dikerjakan di rumah atau tambahan pada saat temannya yang lain sedang mengikuti pelajaran utama, mereka yang berkemampuan lebih mendapat tugas tambahan. Setelah selesai tugas tersebut sebaiknya diperiksa oleh guru.

Adapun teknik pelaksanaannya adalah: guru memberikan tugas/soal pekerjaan rumah kepada murid-murid yang relatif lemah, sedangkan kepada murid-murid yang cepat belajarnya tugas yang diberikan guru harus dikerjakan di kelas itu juga, sementara murid-

murid lain mengerjakan proses belajar mengajar utamanya. Sebaliknya guru memeriksa dan memperhitungkan dengan pemahaman bobot kredit apabila memberikan pekerjaan rumah atau tugas tambahan.

Baik dalam rangka pekerjaan rumah maupun tugas tambahan yang seyogyanya diperiksa oleh guru, apalagi kalau ada perhitungannya dengan penambahan bobot kredit bagi siswa yang akan merupakan intensif baginya.

3) Percepatan(acceleration)

Alternatiflain yang dapat kita berikan layanan kepada kasus berbakat atau unggulan, tetapi menunjukkan kesulitan psikososial atau egoemosional ialah dengan jalan mengadakan akselerasi atau promosi yang lebih tinggi kepada program PBM berikutnya. Pelaksanaan layanan pengajaran secara akseleratif ini tentu perlu adanya kerjasama diantara para guru yang bersangkutan disekolah tertentu, bahkan akan sangat membantu kalau sudah dikembangkan secara modular sehingga para guru akan mudah mengadministrasikannya meskipun banyak siswa dalam hal tertentu mempunyai program studi yang beragam.

Pelayanan akselerasi diberikan kepada murid berbakat yang menunjukkan kesulitan psikososial yaitu dengan jalan mengadakan akselarasi atau promosi kepada program utama berikutnya yang lebih tinggi dengan dua kemungkinancara pelaksanaannya:

a) Promosi penuh status akademisnya ke tingkat yang lebih tinggi sebatas kemungkinannya menunjukkan keunggulan yang menyeluruh dari program studi yang ditempuhnya dengan luar biasa. Dalam hal ini dapat dilakukan dengan cara*"placement test"* dari tingkat yang akan dimasuki.
b) Maju berkelanjutan *(continous progress)* pada beberapa bidang studi tertentu dimana kasus sangat menonjol dapat diberikan layanan dengan program pelajaran yang lebih tinggi sebatas kemampuannya dan status akademisnya tetap bersama-sama teman seagkatannya.

Ketiga teknik pendekatan yang bersifat kuratif tersebut diadministrasikan secara efektif guna keperluan peningkatan prestasi

akademis maupun kemampuan penyesuaiannya mungkin berangsur-angsur dapat dikurangi dalam lingkungan dan sistem persekolahan.

b. Strategi dan pendekatan pengajaran remedial yang bersifat preventif

Kalau staretgi dan teknik kuratif ditunjukkan kepada siswa yang secara empiric sudah nyata-nyata menunjukkan kesulitan tertentu (prestasi lemah, kurang mampu melakukan penyesuaian), pendekatan preventif ditunjukkan kepada siswa tertentu yang berdasarkan data/informasi yang dapat diantisipasikan atau diprediksi atau setidak-tidaknya patut diduga akan mengalami kesulitan dalam menyelesaikan suatu program studi tertentu yang akan ditempuhnya.

Oleh karena itu, sasaran pokok dari pendekatan proventif itu berusaha sedapat mungkin agar hambatan-hambatan yang diantisipasikan itu dapat direduksi seminimal mungkin sehingga siswa yang bersangkutan diharapkan dapat mencapai prestasi dan kemampuan penyesuaian sesuai dengan criteria keberhasilan yang ditetapkan (Makmun, 2012:362)

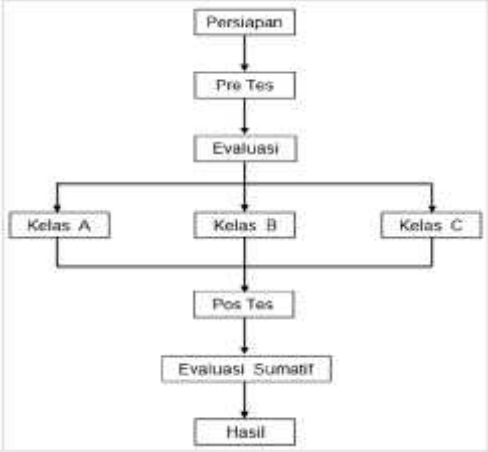
Sasaran pokok dari pendekatan preventif adalah berupaya sedapat mungkin agar hambatan-hambatan dapat mencapai prestasi dapat diatasi dan mengembangkan kemampuan sesuai dengan kriteria keberhasilan yang diterapkan, pendekatan revensit bertolak dari hasil pretest atau *test of entering behaviors*.Pendekatan preventif merupakan tindak lanjut dari *pre teaching diagnostic.* Berdasarkan hasil *pre test teaching diagnostic* ini maka secara garis besar murid dapat diidentifikasikan kedalam tiga kategori, yaitu:

1) Mereka yang diperkirakan akan mampu menyelesaikan program proses belajar mengajar utama sesuai dengan waktu yang telah disediakan kategori normal rata-rata)
2) Mereka yang diperkirakan akan sanggup menyelesaikan program lebih cepat dari waktu yang telah ditetapkan (murid yang cepat)
3) Mereka yang diperkirakan akan terlambat atau tidak akan menyelesaikan program sesuai dengan batas waktu yang telah ditetapkan

Atas dasar perkiraan di atas, maka ada tiga alternatif kemungkinan teknik layanan pengajaran yang bersifat remedial:

1) Layanan kepada kelompok belajar homogeny.

Langkah pelayanan kelompok kepada kelompok belajar homogen dapat dijelaskan dalam bagan sebagai berikut :

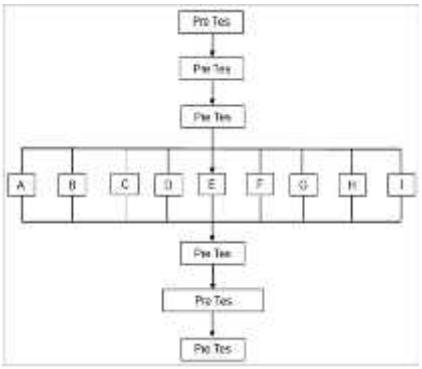


Gambar 3.2 Kelompok belajar homogeny
Sumber: Makmun, (2012)

Dari bagan di atas nampak bahwa setelah diadakan penilaian terhadap murid dikelompokkan ke dalam kelompok A (murid yang cepat), kelompok B (kemampuan murid rata-rata) dan kelompok C (kemampuan murid lambat) program kepada ketiga kelompok dengan ruang lingkup ekuivalen, tetapi diorganisasikan secara relatif berbeda. Perbedaan tersebut terletak dalam cara menerangkan, taraf kesukaran dalam memberikan tugas/soal, dan sebagainya. Misal murid yang termasuk kelompok A sudah tentu diberikan tugas/soal dengan taraf kesukaran dan jumlah relatif lebih banyak dari kelompok lainnya.

2) Layanan pengajaran individual

Konsep dasar teknik layanan pengajaran individual sama dengan teknik layanan kepada kelompok belajar homogen yaitu peyesuaian layanan pengajaran yang disesusaikan dengan kondisi obyektif murid. Namun pada teknik layanan pengajaran individual secara fundamental diberikan kepada murid secara individual.Langkah-langkah pengajaran individual secara visual digambarkan sebagai berikut:



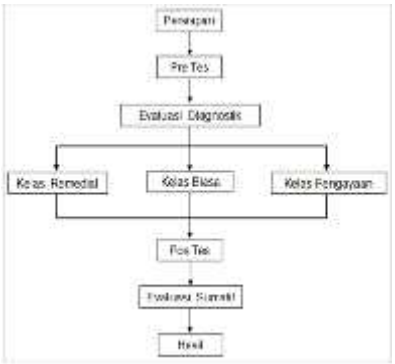
Gambar 3.3 Diagram kelompok belajar individu
Sumber: Makmun, (2012)

Pada teknik pengajaran individual ini, setiap murid mempunyai waktu tersendiri.Ia mempunyai kebebasan melakukan konsultasi dengan guru atau pihak lain yang diperlukan degan tidak terikat keharusan mengikuti pelajaran seperti biasa di kelas. Namun ia terikat oleh batas waktu akhir periode belajara yang telah ditetapkan.

Walaupun kegiatan belajar murid secara individual, tetapi masing-masing dari murid dituntut menempuh *post test* atau tes sumatif tertentu diorganisasikan secara baku. Keperluan, program pengajaran individual, biasanya telah diorganisasikan dalam bentuk modul diman pada prinsipnya setiap murid mendapat layanan secara individual.

3) Layanan pengajaran secara kelompok dilengkapi kelas khusus remedial dan pengayaan

Teknik layanan ini dapat digambarkan dalam bagan sebagai berikut :



Gambar 3.4 Diagram remedial dilengkapi dengan kelas khusus
Sumber: Makmun, (2012)

Pada teknik pertama (layanan kelompok belajar homogen) sejak awal sampai *post test* ataumasing-maisng murid mengikuti porgram A, B,atau C dan tidak terjadi perpindahan selama program berlangsung, tetapi pada teknik kegiatan ini pada prinsipnya murid berada dalam satu kelas yang samadengan mengikuti proses belajar mengajar utama yang sama pula. namun di samping itu kepada murid yang cepat belajarnya telah disediakan paket program pengayaan khusus, begitu pula kepada murid yang ternyata mempunyai kesulitan-kesulitan tertentu telahdisediakan tepat/waktu dan program layanan remedial.

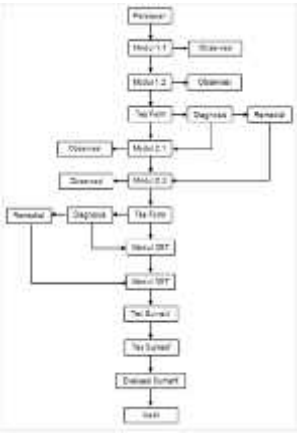
Setelah murid-murid selesai dengan program pengayaan atau program remedial, mereka kembali lagi ke dalam kelompok dan program belajar utama bersama-sama dengan teman sekelasnya. Pada akhirnya mereka juga harus menempuh *post test* secara bersama-sama pula. teknik pelayanannya dapat sama dengan teknik pertama yaitu dilakukan oleh beberapa guru dalam satu waktu yang bersamaan tau berada dan dapat pula dilakukan oleh guru yang sama pada saat yang berbeda asal program dan fasilitas teknisnya sudah dipersiapkan

4) Strategi dan pendekatan pengajaran remedial yang bersifat pengembangan (Development)

Kalau pendekatan kuratif merupakan tindak lanjut dari *post diagnostik teaching* dan pendekatan preventif merupakan tindak lanjut dari *pre-teaching* diagnostik, pendekatan pengembangan merupakan tindak lanjut dari *during teaching diagnostic* atau berupaya diagnosis yang dilakukan guru selama berlangsung program proses belajar mengajar.

Sasaran pokok dari strategi pendekatan pengembangan ini adalah agar murid mampu mengatasi kesulitan atau hambatan-hambatan yang mungkin dialami selama melaksanakan kegiatan proses belajar mengajar. Bantuan segera *(intermediate treatment)* dari saat ke saat selama berlangsungnya proses belajar mengajar. Pada akhirnya murid diharapkan akan dapat menyelesaiakan program secara tuntas sesuai dengan kriteria keberhasilan yang ditetapkan.

Pelaksanaan strategi pendektan pengembangan ini diperlukan adanya pengorganisasian program proses belajar mengajar yang sistematis seperti dalam bentuk sistem pengajaran berprogram, sistem pengajaran modul, *self instrctional audiotutorial system* dan sebagainya. Dengan demikian proses layanan diagnosis dan remedial itu dapat secara sekuensial dari unit ke unit secara teratur. Secara visual pendekatan pengembangan ini dapat digambarkan sebagai berikut :



Gambar 3.5 Strategi remedial dengan teknik pengembangan
Sumber: Makmun, (2012)

Dari bagan tersebut di atas menunjukkan bahwa ada rangkaian perkembangan diagnosis dan remedial yang berlangsung selama proses belajar mengajar, dari modul ke modul atau unit ke unit. Dalam hal ini guru harus mengadakan observasi atau memonitor selama proses belajar berlangsung kemudian tiap selesai tes formatif hendaknya diadministrasikan.

Informasi dari kedua aktivitas itu merupakan *feed back* (umpan balik) dari guru untuk segera mengadakan evaluasi diagnosis. Tindakan selanjutnya adalah guru segera melakukan bantuan remedial baik kepada murid secara kelompok maupun secara individual, tergantung pada pola proses belajar mengajar mana yang digunakan. Kegiatan proses belajar mengajar baru dilanjutkan kepada tingkat berikutnya (modul/ unit tertentu) apabila murid betul-betul telah menyelesaikan program terdahulu secara tuntas (sesuai kriteria keberhasilan yang ditetapkan).

Sudah barang tentu kalau program ini disajikan dalam bentuk modul, murid yang sudah dipandang memenuhi tidak perlu saling menunggu temannya. Dengan perkataan lain bahwamurid yang bersangkutan sebaiknya diperkenankan maju ke tingkat program yang lebih tinggi. Kegiatan seperti dilakukan sepanjang satuan program yang lebih besar diselesaikan (tahunan, semester). Pada akhirnya selayaknya diadakan suatu tes yang menyeluruh (sumatif test)

Sasaran utama pendekatan ini adalah agar siswa bisa menghadapi hambatan/kesulitan yang mungkin dialaminya selama melaksanakan kegiatan proses belajar mengajar. Mereka diberi bantuan segera(immediate treatment) dari waktu ke waktu selama berlangsung pembelajaran. Harapan dari teknik ini adalah siswa diharapkan akan menyelesaikan program secara tuntas sesuai dengan kriteria keberhasilan yang telah ditentukan. Agar strategi dan teknik pendekatan ini dapat diopersionalkan secara teknis dan sistematis, diperlukan adanya pengorganisasian program pembelajaran/PBM yang sistematis, seperti sistem pembelajaran berprogram, system modul, self instructional audio tutorial system. Dengan demikian, proses layanan diagnostic dan remedial dapat dilakukan dari unit ke unit secara teratur.

3. Strategi dan prosedur pengajaran remedial

Secara metodologis dapat juga dikatakan bahwa penanganan kasus kesulitan belajar-mengajar itu mungkin dapat dilakukan melalui pendekatan pengajaran remedial, bimbingan dan konseling psikoterapi dan/atau pendekatan lainnya. Pendekatan yang seyoginya dikuasai atau setidak-tidaknya dikenal oleh para guru pada umumnya dan guru bidang studi pada khususnya ialah apa yang disebut pengajar remedial. Sedangkan kalau guru tersebut bertugas sebagai wali kelas atau petugas bimbingan, seyoginya minimal menguasai atau setidak-tidaknya mengenal prinsip-prinsip dasar bimbingan dan konseling (Makmun, 2007:342).

Menurut Goldschmind (Wijaya, 2011:116) “modul adalah sejenis kegiatan belajar mengajar yang berencana, didesain untuk membantu siswa menyelesaikan tujuan-tujuan tertentu”

Menurut Wijaya (2010:11) strategi dalam pengajaran remedial mencakup:

a) Pengelolaan penyelenggaraan pengajaran oleh orangtua, masyarakat dan guru di sekolah dalam sistem pengajaran modul. Modul adalah unit program belajar mengajar terkecil secara terinci digariskan sebagai berikut:
   1) Tujuan instruksional umum
   2) Tujuan instruksional khusus
   3) Pokok-pokok materi yang akan dipelajari dan diajarkan
   4) Kedudukan fungsi satuan dalam kesatuan program yang lebih luas
   5) Peranan guru dalam proses belajar mengajar
   6) Alat dan sumber yang akan dipakai
   7) Kegiatan belajar mengajar yang akan/harus dilakukan dan dihayati siswa secara berurutan
   8) Lembaran kerja yang akan dikerjakan selama berlangsung proses belajar mengajar itu.

Berdasarkan pendapat tersebut maka dapat disimpulkan bahwa pengajaran modul adalah pengajaran yang sebagian atau seluruhnya didasarkan atas modul.Pengajar yang mengutamakan metode konvensional, kemungkinan memanfaatkan juga modul dalam pengajarannya. Jadi, modul merupakan salah satu alternatif jawaban yang dianggap tepat oleh para ahli dalam menanggapi dan memecahkan masalah pendidikan dan pengajaran yang sangat kompleks dewasa ini.modul dapat dirumuskan sebagai suatu unit yang lengkap yang berdiri sendiri dan terdiri atas sesuatu rangkaian kegiatan belajar yang disusun untuk membantu siswa mencapai sejumlah tujuan yang dirumuskan secara khusus dan jelas atau satu paket/program pengajaran yang terdiri dari satu unit konsep bahan pelajaran atau program belajar mengajar terkecil.

Modul adalah semacam paket program untuk keperluan belajar.Dari satu paket program belajar, modul terdiri atas komponen-komponen yang berisi tujuan belajar, materi pelajaran, metode belajar, alat, sumber dan sistem evaluasi. Melalui sistem pengajaran modul sangat dimungkinkan:

a. Adanya peningkatan motivasi belajar secara maksimal

b. Adanya peningkatan kreativitas guru dalam menyiapkan alat dan bahan yang diperlukan serta pelayanan individual yang lebih mantap
c. Mewujudkan prinsip maju berkelanjutan secara tidak terbatas
d. Mewujudkan belajar yang lebih berkonsentrasi

Dalam menyiapkan, melaksanakan dan mengevaluasi system pengajaran modul dan terprogram dengan langkahh-langkah dalam dua tahapan:

a) Tahapan penulisan dan pencetakan modul, mencakup kegiatan-kegiatan sebagai berikut:
   1) Survey dan promosi, dengan maksud agar penelitian itu dapat diselenggarakan dengan baik, penuh rasa tanggung jawab dan mendapatan dukungan dari berbagai pihak. Survey dan promosi diarahkan ke lapangan, perseorangan, lembaga pendidikan, para pakar dalam berbagai ilmu pengetahuan dan para pejabat pemerintahan
   2) Tim melakukan orientasi pembinaan dan mengembangkan latihan penulisan modul
   3) Menulis dan mencetak modul, menggandakannya sesuai dengan kebutuhan
   4) Selanjutnya dilakukan orientasi penentuan guru-guru yang akan diangkat menjadi supervisor atau guru modul
b) Tahapan uji-coba komponen-komponen modul sebagai suatu system penyampaian baru untuk kelasIV, antara lain:
   1) Mengangkat dan melatih guru-guru modul dan para pengawas pengajaran. Mereka berperan sebagai pengelola pengajaran
   2) Pelibatan sumber-sumber masyarakat, seperti:
      (a) Siswa SLTA yang disiapkan untuk menjadi seorang tutor
      (b) Keterlibatan orangtua dalam memantau keggiatan belajar
      (c) Anggota masyarakat yang terampil, disiapkan sebagai manusia sumber. Mereka ditempatkan di pusat-pusat belajar
      (d) Media, alat-alat peraga dan sumber-sumber masyarakat lainnya yang berfungsi memperkaya pengalaman belajar
   3) Mempersiapkan guru bantu (non-teaching personal) yang bertugas membantu guru modul

4) Melaksanakan system pengajaran terprogram yang disusun dalam bentuk modul
5) Mendirikan pusat-pusat belajar masyarakat yang bertujuan untuk memaksimalkan penggunaan gedung-gedung yang telah ada dan sumber-sumber masyarakat lainnya yang mudah dijangkau

Dalam pelaksanaannya, guru modul yang menuntut lazimnya disebut supervisor pengajaran, dibantu oleh beberapa tenaga lainnya.

1) *Guru keliling*, ialah guru bidang studi yang tidak dimodulkan. Ia adalah guru kelas yang sangat terlatih dan professional
2) *Guru bantu,* ialah guru yang bertugas membantu guru modul
3) *Tutor,* yaitu seorang sukarelawan, yang bertugas membantu siswa

b) Pendekatan sumber

Pendekatan sumber yaitu pendekatan yang menekankan pada kebutuhan individu yang sedang mengalami kesulitan belajar, terutama siswa yang lamban belajar dan prestasi rendah. System pengajaran yang digunakan adalah system pengajaran yang adaptif, yaitu system pengajaran yang responsive dan relevan dengan kebutuhan semua siswa dalam konteks fisik, mental dan social

Program sumber dikembangkan sebagai bagian yang tak terpisahkan dari kurikulum sekolah.Pendidikan khusus yang telah ada dijadikan instrument guru dalam menemukan kebutuhan belajar siswa.Sebagai suatu model, pendekatan sumber itu masih tetap menuntut adanya pendidikan khusus di sekolah yang fungsinya diubah menjadi suatu system adaptif, yaitu system yang responsive dan relevan dengan kebutuhan siswa.

Dalam praktiknya, pendekatan sumber tidak menuntut adanya sarana yang harus disiapkan oleh sekolah, terutama yang menyangkut ruangan, alat dan fasilitas lainnya. Tugas pokok pendekatan sumber adalah untuk menemukan cara-cara yang baik dalam membantu siswa yang sedang menghadapi kesulitan belajar

c) Proyek khusus dibidang sistem pengajaran tepat.

Proyek khusus dibidang sistem pengajaran tepat melibatkan tujuh langkah kegiatan yaitu:

1) Identifikaasi pengkajian target yang berguna
2) Pengembangan dan pengkajian materi pelajaran yang akan diberikan

3) Pengkajian lebih lanjut dari hasil pengkajian terdahulu tentang bentuk-bentuk tingkah lakupada setiap target
4) Identifikasi keadaan siswa sendiri, terutama dalam segala hal kelemahan tingkah laku yang dirasakannya
5) Pelaksanaan program pengajaran remedial pada kelompok kecil, kelompok yang terdiri atas siswa yang sedang menderita kelemahan-kelemahan itu
6) Identifikasi siswa yang tidak berhasil atau gagal meraih sukses belajar dalam kelompok kecil di atas
7) Pengembangan dan penerapan program pengajaran individual untuk siswa yang mendapat kegagalan dalam kelompok kecil itu

Pada dasarnya, tahapan-tahapan dalam proses mengajar memiliki hubungan erat dengan penggunaan strategi mengajar. Maksudnya ialah bahwa setiap penggunaan strategi mengajar harus selalu merupakan rangkaian yang utuh dalam tahapan-tahapan mengajar. Setiap proses mengajar harus melalui tiga tahapan, yakni:

a) Tahap prainstruksional, yaitu persiapan sebelum mengajar dimulai
b) Tahap instruksional, yakni saat-saat mengajar (penyajian materi)
c) tahap evaluasi dan tindak lanjut, yakni penilaian atas hasil belajar siswa setelah mengikuti pengajaran dan penindak lanjutannya(Syah, 2010:213)

Inti dari pengajaran harus teratur dan sistematis. Perbanyak menggunakan contoh kehidupan sehari-hari atau dari apa yang pernah dialami.

D. Aktivitas Pembelajaran

Adapun inti dari aktivitas pembelajaran modul ini bagi peserta diklat adalah sebagai berikut: Alokasi waktu yang disediakan untuk pembelajaran III ini adalah 100 menit atau 2 x 50 menit, dengan rincian sebagai berikut:

Tabel 4. Kegiatan pembelajaran III

No.	Waktu	Kegiatan
1.	20 menit	Apersepsi yang berkaitan dengan kegiatan mengidentifikasi dan memehami strategi remedial dan pengayaan**.**
2.	50 menit	• Membagi kelompok diskusi.

		• Mendiskusikan (1) strategi yang dipergunakan dalam pelaksanaan pengajaran remedial, (2) strategi pengajaran remedial dari strategi pembelajaran biasa, (3) strategi pengajaran remedial, (4) pengertian teknik pengajaran remedial, dan (5) teknik yang dipergunakan dalam pengajaran remedial.
3.	30 menit	Menyajikan/mensimulasikan strategi remedial dan pengayaan yang terdapat pada pembelajaran III terhadap peserta diklat

E. Latihan/ Kasus/ Tugas

Soal *Multiple choice*

1. Salah satu layanan yang bukan merupakan alternative kemungkinan teknik layanan pengajaran bersifat remedial, adalah
   a. Layanan kepada kelompok belajar homogeny
   b. Layanan pengajaran individual
   c. Layanan pengajaran secara kelompok dilengkapi kelas khusu remedial dan pengayaan
   d. Layan pengajaran kelompok berlangsung secara intensif
2. System pengajaran sangat dimungkinkan untuk:
   a. Mengevaluasi system pengajaran modul
   b. Adanya peningkatan motivasi belajar secara maksimal-
   c. Menjelaskan kedudukan fungsi satuan dalam kesatuan program yang lebih luas
   d. Membantu siswa menyelesaikan tujuan-tujuan belajar
3. Cara pelaksanaan pelayanan akselerasi diberikan kepada murid berbakat yang menunjukkan kesulitan psikososial yaitu:
   a. Maju berkelanjutan pada beberapa bidang studi tertentu-
   b. Peningkatan prestasi akademis
   c. Penyesuaian proses belajar antara lingkungan dan system persekolahan
   d. Melaksanakan proses administrasi secara efektif dan efisien

4. Layanan pengayaan diberikan kepada murid yang mempunyai kelemahan ringan, dengan materi program pengayaan yang bersifat:
   a. Ekuivalen (horizontal) dengan proses belajar mengajar-
   b. Efiesiensi pelaksanaan proses belajar mengajar
   c. Peningkatan efektivitas pemanfaatan sumber belajar
   d. Pemberian tugas secara maksimal kepada siswa agar dapat belajar lebih giat
5. Beberapa kemungkinan waktu dan cara pelaksanaan pengajaran remedial, kecuali:
   a. Dilaksanakan pada pertemuan kelas biasa
   b. Dilaksanakan diluar jam pertemuan biasa
   c. Dilaksanakan pada kelas remedial
   d. Dilaksanakan setiap saat bagi siswa yang mengalami kesulitan belajar

F. Rangkuman

Strategi pengajaran remedial adalah:

1. Strategi dan pendekatan pengajaran remedial yang bersifat kuratif yaitu tindakan pengajaran remedial yang dilakukan setelah program PBM utama selesai diselenggarakan.
2. Strategi dan pendekatan pengajaran remedial yang bersifat preventif adalah suatu tindakan yang berupaya sedapat mungkin agar hambatan-hambatan dapat mencapai prestasi dapat diatasi dan mengembangkan kemampuan sesuai dengan kriteria keberhasilan yang diterapkan.
3. Strategi dan pendekatan pengajaran remedial yang bersifat pengembangan (*Development*) Sasaran pokok dari strategi pendekatan pengembangan ini adalah agar murid mampu mengatasi kesulitan atau hambatan-hambatan yang mungkin dialami selama melaksanakan kegiatan proses belajar mengajar.

Teknik yang dapat digunakan untuk mendiagnosis kesulitan belajar antara lain: tes prasyarat (prasyarat pengetahuan, prasyarat keterampilan), tes diagnostik, wawancara, pengamatan dan sebagainya.

Beberapa teknik dan strategi yang dipergunakan dalam pelaksanaan pembelajaran remedial antara lain: (1) Pemberian Tugas, (2) Kegiatan Kelompok. (3) Tutorial Sebaya dan (4) Menggunakan Sumber Lain

G. Umpan Balik dan Tindak Lanjut

Apabila Anda mendapatkan hasil 80 % ke atas, maka Anda dinyatakan lulus pada Kegiatan Pembelajaran III ini, akan tetapi apabila mendapatkan 0 %, 25 %, 40 % atau 60 %, maka Anda diminta membaca dan memahami isi modul kembali dan menjawab latihan-latihan yang telah disiapkan.

H. Kunci Jawaban

Kunci jawaban pilihan ganda

1. **D**. Layanan pengajaran kelompok berlangsung secara intensif
2. **B**. Adanya peningkatan motivasi belajar secara maksima
3. **A**. Maju berkelanjutan pada beberapa bidang studi tertentu.
4. **A**. Ekuivalen (horizontal) dengan proses belajar mengajar
5. **A**. Dilaksanakan pada pertemuan kelas biasa

EVALUASI

Kegiatan Pembelajaran I

Untuk mengetahui kompetensi akhir yang anda miliki, maka isilah cek lis (√) seperti pada tabel pernyataan di bawah ini sesuai kemampuan yang anda miliki.

Tabel 5 Evaluasi akhir kegiatan pembelajaran I

Sub Kompetensi	Pernyataan (indikator)	Saya dapat melakukan pekerjaan ini dengan Komputen		Bila jawaban "Ya" kerjakan
		Ya	Tidak	
Konsep Dasar Kegiatan Remedial dan Pengayaan	1. Menjelaskan pengertian kegiatan remedial 2. Menganalisis jenis-jenis kegiatan remedial 3. Menjelaskan pengertian kegiatan pengayaan 4. Menjelaskan hakikat kegiatan pengayaan 5. Menjelaskan bentuk-bentuk kegiatan pengayaan 6. Menjelaskan faktor-faktor yang harus diperhatikan dalam melaksanakan kegiatan pengayaan			

Apabila anda menjawab TIDAK pada salah satu pernyataan di atas, maka pelajarilah modul Kegiatan Pembelajaran I

Kegiatan Pembelajaran II

Untuk mengetahui kompetensi akhir yang anda miliki, maka isilah cek lis (√) seperti pada tabel pernyataan di bawah ini sesuai kemampuan yang anda miliki.

Tabel 6. Evaluasi akhir kegiatan pembelajaran II

Sub Kompetensi	Pernyataan (indikator)	Saya dapat melakukan pekerjaan ini dengan Komputen		Bila jawaban "Ya" kerjakan
		Ya	Tidak	
Prosedur Remedial dan Pengayaan	1. Menjelaskan prosedur pengajaran remedial. 2. Menjelaskan langkah-langkah pelaksanaan			

	pengajaran pengayaan.			

Apabila anda menjawab TIDAK pada salah satu pernyataan di atas, maka pelajarilah modul Kegiatan Pembelajaran II

Kegiatan Pembelajaran III

Untuk mengetahui kompetensi akhir yang anda miliki, maka isilah cek lis (√) seperti pada tabel pernyataan di bawah ini sesuai kemampuan yang anda miliki.

Tabel 7. Evaluasi akhir kegiatan pembelajaran III

Sub Kompetensi	Pernyataan (indikator)	Saya dapat melakukan pekerjaan ini dengan Komputen		Bila jawaban "Ya" kerjakan
		Ya	Tidak	
Strategi Remedial dan Pengayaan	1. Menjelaskan strategi yang dipergunakan dalam pelaksanaan pengajaran remedial 2. Membedakan strategi pengajaran remedial dari strategi pembelajaran biasa 3. Menganalisis strategipengajaran remedial 4. Menjelaskan pengertian teknik pengajaran remedial 5. Menjelaskan teknik yang dipergunakan dalam pengajaran remedial			

Apabila anda menjawab TIDAK pada salah satu pernyataan di atas, maka pelajarilah modul Kegiatan Pembelajaran III kembali, akan tetapi jika saudara menjawab semua dengan YA berarti saudara telah memahami dengan baik modul pembelajaran pengayaan dan remedial ini.

PENUTUP

Dalam pembelajaran remedial diperlukan upaya untuk menyebuhkan atau perbaikan layanan pembelajaran baik strategi, metode, dan materi dari pelajaran yang sebelumnya dianggap sulit untuk dipahami sehingga memperoleh daya serap yang rendah.Tujuan guru melaksanakan kegiatan remedial adalah membantu siswa dalam mencapai tujuan kompetensi yang telah ditentukan agar mencapai hasil belajar yang lebih baik.Terdapat 6 fungsi dalam pembelajaran remedial yaitu (1) fungsi korektif, (2) fungsi pemahaman, (3) fungsi penyesuaian, (4) fungsi pengayaan, (5) fungsi akselerasi, (6) fungsi terapeutik.

Hal ini berbeda dengan pembelajaran pengayaan (*enrichment*); yakni suatu kegiatan yang diberikan kepada siswa kelompok cepat mampu menguasai pelajaran (kemampuan di atas rata-rata), agar mereka lebih mampu lagi mengembangkan potensinya secara optimal dengan memanfaatkan sisa waktu yang dimilikinya.Kegiatan pengayaan dilaksanakan dengan tujuan memberikan kesempatan kepada siswa untuk memperdalam penguasaan materi pelajaran yang berkaitan dengan tugas belajar yang sedang dilaksanakan sehingga tercapai tingkat perkembangan yang optimal. Terdapat 3 faktor dalam pembelajaran pengayaan yaitu (1) faktor siswa, (2) faktor kegiatan edukatif, (3) faktor waktu.

Langkah-langkah yang harus ditempuh dalam kegiatan remedial yaitu Analisis hasil diagnosis, Identifikasi penyebab kesulitan, Penyusunan rencana dan Pelaksanaan kegiatan.Sedangkan langkah-langkah untuk pelaksanaan pembelajaran pengayaan yaitu Identifikasi Kelebihan Kemampuan Belajar dan Bentuk Pelaksanaan Pembelajaran Pengayaan.

DAFTAR PUSTAKA

Arikunto.(2013). *Dasar-Dasar Evaluasi Pendidikan*. Jakarta: Bumi Aksara.

Clark, B. (1988) *Growing Up Gifted, Third Edition*, California State University, Los Angeles:Merril Publishing Company.

Edwan.(2015).Prosedur Pelaksanaan Pengajaran Remedial.

Feldhusen, J. and Kollof, P. (1986) The Purdue three-stage enrichment model for gifted education at the elementary level. Dalam J.Renzulli (Ed) *Systems and Models for Developing Programs for the Gifted and Talented*. Mansfield Center, CT: Creative Learning Press.

Khaerunnisa.(2013). Http:///www.makalah konsep dasar metode dan teknik pembelajaran.com, diunduh 20 Oktober 2015

Makmun.(2012). Psikologi Kependidikan. Bandung: Remaja Rosdakarya.

Maslow, A.H. (1987/1954) *Motivation and personality* (Edisi Ketiga), Revised by R Frager, J. Fadiman, C) New York: Harper & Row.

Prasetyo.(2013). Evaluasi dan Remediasi Belajar. Jakarta: Trans Info Media.

Sudijono.(2013).. Pengantar Evaluasi Pendidikan. Jakarta: Rajagrafindo Persada.

Sugihartono. (2012). PsikologiPendidikan. Yogyakarta: UNY Press.

Sukiman. (2012). PengembanganSistemEvaluasi. Yogyakarta: InsanMadani.

Sukardi.(2011). Evaluasi Pendidikan Prinsip & Operasionalnya. Jakarta: Bumi Aksara.

Sumiah, N, Aminuyati, dan Khosmas, F.Y (2015) *Analisis Keterampilan Mengajar Guru dalam Meningkatkan Hasil Belajar pada Mata Pelajaran Ekonomi*, Laporan Penelitian, Program Studi Pendidikan Ekonomi FKIP Untan, Pontianak Kalimantan Selatan.

Supardan, D (2015) *Pembelajaran IPS: Perspektif Filosofi dan Penilaian*, Jakarta: Bumi Aksara.

Undang-Undang Nomor 20 Tahun 2003 Tentang Sistem Pendidikan Nasional

Utami Budi. 2014. Http:///pengajaran rimidal.com, diunduh 25 September 2015

Wijaya.(2010). Pendidikan Remedial. Bandung: Remaja Rosda Karya.

Wina Senjaya. 2008. Strategi Pembelajaran; Berorientasi Standar Proses Pendidikan. Jakarta: Kencana Prenada Media Group. diunduh 25 September 2015

http://little-chiyoo.blogspot.com/2012/12/kegiatan-remidial-kegiatan-pengayaan_14.html, diunduh pada tanggal 30 Oktober 2015.

http://yuriena.wordpress.com/2010/08/29/tujuan-dan-fungsi-pengajaran-remedial/, diunduh pada 30 Oktober 2015.

http://conditionaloflife.blogspot.com/2013/05/konsep-dasar-pengajaran-remedial-dan.html, diunduh pada 5 November 2015.

http://little-chiyoo.blogspot.com/2012/12/kegiatan-remidial-kegiatan-pengayaan_14.html, diunduh pada tanggal 5 November 2015.

http://conditionaloflife.blogspot.com/2013/05/konsep-dasar-pengajaran-remedial-dan.html, diunduh pada tanggal 5 November 2015.

GLOSARIUM

Interaktif	:	Bersifat saling melakukan aksi; antar-hubungan; salingaktif
Kompetensi	:	Merupakan seperangkat pengetahuan, keterampilan, dan perilaku yang harus dimiliki, dihayati, dikuasai, dan diaktualisasikan oleh guru dalam melaksan akan tugas keprofesionalan.
Eksperimentasi	:	Hal yang mendasari penemuan atas alat-alat dan teknik bagi awal sinema, sebuah dunia baru penglihatan yang mulai memandang dan mencoba meniru alam dengan merekam berbagai gejala (alamiah maupun disengaja) yang tampak di depan lensa.
Inovasi	:	Suatu penemuan baru yang berbeda dari yang sudah ada atau yang sudah dikenal sebelumnya
Kognitif	:	Berhubungan dengan atau melibatkan kognisi; Berdasar kepada pengetahuan faktual yg empiris
Fundamental	:	Bersifat dasar (pokok); mendasar
Defenitif	:	sudah pasti (bukan untuk sementara)
Relevansi	:	hubungan; kaitan:
Integral	:	mengenai keseluruhannya; meliputi seluruh bagian yang perlu untuk menjadikan lengkap; utuh; bulat; sempurna:
Estimasi	:	1 perkiraan: 2 penilaian; pendapat:
Fisibilitas	:	sesuatu yang dapat dilaksanakan; keterlaksanaan; kelaikan; kelayakan
Taksonomi	:	1 klasifikasi bidang ilmu; kaidah dan prinsip yang meliputi pengklasifikasian objek; 2 cabang biologi yang menelaah penamaan, perincian, dan pengelompokan makhluk hidup berdasarkan persamaan dan pembedaan sifatnya; 3 *Ling* klasifikasi unsur bahasa menurut hubungan hierarkis; urutan satuan fonologis atau gramatikal yang dimungkinkan dalam satuan bahasa
Asosiasi	:	1 persatuan antara rekan usaha; persekutuan dagang; 2 perkumpulan orang yang mempunyai kepentingan

bersama; 3 tautan dalam ingatan pada orang atau barang lain; pembentukan hubungan atau pertalian antara gagasan, ingatan, atau kegiatan pancaindra;

Komparasi : perbandingan

Relevan : kait-mengait; bersangkut-paut; berguna secara langsung:

Heterogen : terdiri atas berbagai unsur yang berbeda sifat atau berlainan jenis; beraneka ragam;

Tutor : intruktur yang membantu peserta didik memahami dan menjelaskan materi pembelajaran.

Terapeutik : membantu mengatasi masalah sosial-pribadi

MODUL
GURU PEMBELAJAR

Paket Keahlian

Teknik Komputer dan Jaringan

Kelompok Kompetensi H

Penulis: Antonius Duty Susilo, M.T.

Direktorat Jenderal Guru dan Tenaga Kependidikan Kementrian Pendidikan dan Kebudayaan
Tahun 2016

HALAMAN PERANCIS

Penulis:

Antonius Duty Susilo, M.T., 0816559940., dutymlg@gmail.com

Penelaah:

Bagus Budi Setiawan., S.ST., 081523401., bagus.setiawan@gmail.com

Ilustrator :

1. Siera Maulida Asrin, S.T., 089653910250., siera.asrin@gmail.com
2. Faizal Reza Nurzeha, A.Md., 085242177945., faizalrezanurzeha@gmail.com

Layouter :

Liyani, M.T., 081241091006., liyanialia@gmail.com

KATA SAMBUTAN

Peran guru profesional dalam proses pembelajaran sangat penting sebagai kunci keberhasilan belajar siswa. Guru profesional adalah guru yang kopeten membangun proses pembelajaran yang baik sehingga dapat menghasilkan pendidikan yang berkualitas. Hal ini tersebut menjadikan guru sebagai komponen yang menjadi fokus perhatian pemerintah pusat maupun pemerintah daerah dalam peningkatan mutu pendidikan terutama menyangkut kopetensi guru.

Pengembangan profesionalitas guru melalui program Guru Pembelajar (GP) merupakan upaya peningkatan kompetensi untuk semua guru. Sejalan dengan hal tersebut, pemetaan kopetensi guru telah dilakukan melalui uji kompetensi guru (UKG) untuk kompetensi pedagogik dan profesional pada akhir tahun 2015. Hasil UKG menunjukan peta kekuatan dan kelemahan kompetensi guru dalam penguasaan pengetahuan.

Peta kompetensi guru tersebut dikelompokan menjadi 10 (sepuluh) kelopok kompetensi. Tindak lanjut pelaksanaan UKG diwujudkan dalam bentuk pelatihan guru paska UKG melalui program Guru Pembelajar. Tujuannya untuk meningkatkan kompetensi guru sebagai agen perubahaan dan sumber belajar utama bagi peserta didik. Program Guru Pembelajar dilaksanakan melalui pola tatap muka, daring (*online*) dan campuran (*blended*) tatap muka dengan *online*.

Pusat Pengembangan dan Pemberdayaan Pendidik dan Tenag Kependidikan (PPPPTK), Lembaga Pengembangan dan Pemberdayaan Pendidik dan Tenaga Kependidikan Kelautan Perikanan Teknologi Informasi dan Komunikasi (LP3TK KPTK) dan Lembaga Pengembangan dan Pemberayaan Kepala Sekolah (LP2KS) merupakan Unit Pelaksana Teknis di lingkungan Direktorat Jendral Guru dan Tenaga Kependidikan yang bertanggung jawab dalam mengembangkan perangkat dan melaksanakan peningkaan kompetensi guru sesuai dengan bidangnya.

Adapun peragkat pembelajaran yang dikembangkan tersebut adalah modul untuk program Guru Pembelajar (GP) tatap muka dan GP *online* untuk semua mata pelajaran dan kelompok kompetensi. Dengan modul ini diharapkan program GP memberikan sumbangan yang sangat besar dalam peningkatan kualitas kompetensi guru. Mari kita sukseskan program GP ini untuk mewujudkan Guru Mulia Karena Karya.

Jakarta, Februari 2016
Direktur Jendral
Guru dan Tenaga Kependidikan

Sumarna Surapranata, Ph.D
NIP. 195908011985031002

KATA PENGANTAR

Profesi guru dan tenaga kependidikan harus dihargai dan dikembangkan sebagai profesi yang bermartabat sebagaimana diamanatkan Undang-Undang Nomor 14 Tahun 2005 tentang Guru dan Dosen. Hal ini dikarenakan guru dan tenaga kependidikan merupakan tenaga profesional yang mempunyai fungsi, peran, dan kedudukan yang sangat penting dalam mencapai visi pendidikan 2025 yaitu "Menciptakan Insan Indonesia Cerdas dan Kompetitif". Untuk itu guru dan tenaga kependidikan yang profesional wajib melakukan pengembangan keprofesian berkelanjutan.

Buku pedoman Pedoman Penyusunan Modul Diklat Pengembangan Keprofesian Berkelanjutan Bagi Guru dan Tenaga Kependidikan untuk institusi penyelenggara program pengembangan keprofesian berkelanjutan merupakan petunjuk bagi penyelenggara pelatihan di dalam melaksakan pengembangan modul yang merupakan salah satu sumber belajar bagi guru dan tenaga kependidikan. Buku ini disajikan untuk memberikan informasi tentang penyusunan modul sebagai salah satu bentuk bahan dalam kegiatan pengembangan keprofesian berkelanjutan bagi guru dan tenaga kependidikan.

Pada kesempatan ini disampaikan ucapan terima kasih dan penghargaan kepada berbagai pihak yang telah memberikan kontribusi secara maksimal dalam mewujudkan buku ini, mudah-mudahan buku ini dapat menjadi acuan dan sumber inspirasi bagi guru dan semua pihak yang terlibat dalam pelaksanaan penyusunan modul untuk pengembangan keprofesian berkelanjutan. Kritik dan saran yang membangun sangat diharapkan untuk menyempurnakan buku ini di masa mendatang.

Makassar, Februari 2016
Kepala LPPPTK KPTK Gowa
Sulawesi Selatan,

Dr. H. Rusdi, M.Pd,
NIP 19650430 1991 03 1 004

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

PENDAHULUAN

A. Latar Belakang

Guru dan tenaga kependidikan wajib melaksanakan kegiatan pengembangan keprofesian secara berkelanjutan agar dapat melaksanakan tugas profesionalnya. Program Pengembangan Keprofesian Berkelanjutan (PKB) adalah pengembangan kompetensi Guru dan Tenaga Kependidikan yang dilaksanakan sesuai kebutuhan, bertahap, dan berkelanjutan untuk meningkatkan profesionalitasnya.

PKB sebagai salah satu strategi pembinaan guru dan tenaga kependidikan diharapkan dapat menjamin guru dan tenaga kependidikan mampu secara terus menerus memelihara, meningkatkan, dan mengembangkan kompetensi sesuai dengan standar yang telah ditetapkan. Pelaksanaan kegiatan PKB akan mengurangi kesenjangan antara kompetensi yang dimiliki guru dan tenaga kependidikan dengan tuntutan profesional yang dipersyaratkan.

Di dalam pelaksanaan diklat yang dilaksanakan oleh PPPPTK diperlukan modul sebagai salah satu sumber belajar guru. Modul Diklat PKG Teknik Komputer dan Jaringan Grade 8 ini disusun sebagai acuan bagi penyelenggaraan PKB Diklat dan pelatihan dalam upaya pengembangan keprofesian secara berkelanjutan agar dapat melaksanakan tugas secara professional, meningkat, dan mengembangkan kompetensi sesuai dengan standar yang telah ditetapkan.

Modul Diklat PKG Guru TKJ Grade 8 ini mempelajari tentang Menganalisis kemungkinan potensi ancaman dan serangan terhadap keamanan jaringan, menganalisis sistem keamanan jaringan yang diperlukan menerapkan langkah-langkah penguatan *host (host hardening), m*embangun *server* DMZ, menguji keamanan jaringan, *host* dan *server, m*enganalisis fungsi dan cara kerja *server autentikasi, m*enganalisis sistem pendeteksi dan penahan ancaman/serangan yang masuk ke jaringan *(snort, tripwire, portsentry), m*enerapkan tata cara pengamanan komunikasi data menggunakan teknik *kriptografi*

Tujuan disusunnya modul diklat PKB Guru TKJ Grade 8 ini adalah memberikan pengetahuan, ketrampilan dan sikap kepada guru atau peserta diklat tentang Membangun sistem keamanan jaringan komputer berdasarkan Topologi Jaringan yang digunakan.

.Sedangkan indikator pencapaian kompetensinya adalah :

1. Menganalisis kemungkinan potensi ancaman dan serangan terhadap keamanan jaringan
2. Menganalisis sistem keamanan jaringan yang diperlukan
3. Menerapkan langkah-langkah penguatan *host (host hardening)*
4. Membangun *server* DMZ
5. Menguji keamanan jaringan, *host* dan *server*
6. Menganalisis fungsi dan cara kerja *server autentikasi*
7. Menganalisis sistem pendeteksi dan penahan ancaman/serangan yang masuk ke jaringan *(snort, tripwire, portsentry)*
8. Menerapkan tata cara pengamanan komunikasi data menggunakan teknik *kriptografi*

B. Peta Kompetensi

Modul ini merupakan modul ke-8 dari 10 modul yang dikembangkan. Berdasarkan struktur jenjang diklat PKB Modul mengadministrasi sistem operasi jaringan ini termasuk jenjang Dasar. Modul ini akan digunakan untuk Program Pengembangan Keprofesian Berkelanjutan (PKB) bagi guru-guru produktif Sekolah menengah Kejuruan pada paket keahlian Teknik Komputer dan Jaringan.

Modul Paket keahlian TKJ adalah

Tabel 1.1. Nomor dan Nama Modul Paket Keahlian TKJ

No	Nama Modul
1	Merencanakan sistem komunikasi data
2	Merencanakan Sistem Komunikasi data menggunakan VoIP
3	Mengadministrasi Sistem Operasi Jaringan
4	Mengadministrasi layanan jaringan pada server tingkat dasar

5	Mengadministrasi layanan jaringan pada server tingkat lanjut
6	Membangun Jaringan Nirkabel berdasarkan Topologi Jaringan yang digunakan
7	Membangun Sistem Keamanan Jaringan Nirkabel berdasarkan Topologi Jaringan yang digunakan
8	Membangun sistem keamanan jaringan komputer
9	Menerapkan sistem monitoring jaringan komputer
10	Membuat *project* sistem jaringan *small office home office (SOHO)*

Keterkaitan antara Kompetensi Inti Guru (KIG), Kompetensi Guru paket Keahlian (KGPK) dan Indikator Pencapaian Kompetensi (IPK) ditunjukkan seperti tabel berikut ini.

Tabel 1.2. Keterkaitan antara KIG, KGPK dan IPK

Kompetensi Inti Guru (KIG) Menguasai materi, struktur, konsep dan pola pikir keilmuan yang mendukung mata pelajaran yang diampu		
No	**Kompetensi Guru Paket Keahlian (KGPK)**	**Indikator Pencapaian Kompetensi (IPK)**
8	Membangun sistem keamanan jaringan komputer berdasarkan Topologi Jaringan yang digunakan	8.1 Menganalisis kemungkinan potensi ancaman dan serangan terhadap keamanan jaringan 8.2 Menganalisis sistem keamanan jaringan yang diperlukan *8.3* Menerapkan langkah-langkah penguatan *host (host hardening)* 8.4 Membangun *server* DMZ 8.5 Menguji keamanan jaringan, *host* dan *server* 8.6 Menganalisis fungsi dan cara kerja *server autentikasi* *8.7* Menganalisis sistem pendeteksi dan penahan ancaman/serangan yang masuk ke jaringan *(snort, tripwire, portsentry)* 8.8 Menerapkan tata cara pengamanan komunikasi data menggunakan teknik *kriptografi*

C. Ruang Lingkup Penggunaan Modul

Modul ini terdiri dari 8 kegiatan pembelajaran. Setiap kegiatan pembelajaran terdiri dari tujuan pembelajaran, indikator essential, uraian materi, aktifitas pembelajaran, latihan/tugas/kasus, rangkuman dan umpan balik.

D. Cara Penggunaan Modul

Modul mengadministrasi sistem operasi jaringan ini terdiri dari 8 kegiatan belajar. Peserta diklat dapat mempelajari sesui dengan urutan kegiatan belajar. 8 kegiatan belajar tersebut tidak memiliki ketergantungan secara penuh, sehingga peserta diklat dapat mempelajari tidak secara berurutan. Akan tetapi untuk masing-masing kegiatan belajar mempunyai keterkaitan secara penuh. Ini berarti untuk setiap kegiatan belajar yang dipelajarai harus secara berurutan sesuai dengan urutan kegiatan pembelajaran.

Untuk setiap kegiatan pembelajaran, uruatan yang harus dilakukan oleh peserta diklat dalam mempelajari modul ini adalah :

1. Membaca tujuan pembelajaran sehingga memahami target atau goal dari kegiatan belajar tersebut.
2. Membaca indikator pencapaian kompetensi sehingga memahami obyek yang akan dijadikan kriteria pengukuran untuk mencapai tujuan pembelajaran.
3. Membaca uraian materi pembelajaran sehingga memiliki pengetahuan, ketrampilan dan sikap terhadap kompetensi yang akan dicapai
4. Melakukan aktifitas pembelajaran dengan urutan atau kasus permasalahan sesuai dengan contoh.
5. Mengerjakan latihan/soal atau tugas dengan mengisi lembar kerja yang telah disediakan.

6. Menjawab pertanyaan dalam umpan balik yang akan mengukur tingkat pencapaian kompetensi melalui penilaian diri.

1

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 1: Menganalisis Kemungkinan Potensi Ancaman Dan Serangan Terhadap Keamanan Jaringan

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa:

- Melalui praktikum peserta diklat dapat menganalisis kemungkinan potensi ancaman dan serangan terhadap keamanan jaringan.

B. Indikator Pencapaian Kompetensi

- Memahami konsep analisis potensi ancaman dan serangan terhadap keamanan jaringan.
- Menggunakan tool Nmap pada sistem operasi Kali Linux.
- Mampu menganalisa kemungkinan terhadap potensi ancaman dan serangan terhadap keamanan jaringan.

C. Uraian Materi

Jaringan komputer sebagai tulang punggung dari teknologi informasi diharapkan dapat menyediakan layanan yang aman bagi penggunanya. Layanan yang aman tersebut termasuk hak akses pengguna lain terhadap data. Oleh karena itu dalam suatu jaringan komputer perlu dilakukan analisis aspek confidentiality yang merupakan salah satu aspek dari keamanan informasi. Analisis ini bertujuan untuk mengukur tingkat kerahasian informasi setiap pengguna pada suatu jaringan komputer. Analisis ini dilakukan dengan cara melakukan ekspoitasi terhadap celah keamanan pada salah satu port yang terbuka di setiap client/hosts melalui internal jaringan komputer untuk mencuri informasi dari pengguna yang berada pada client/host yang dieksploit.

Analisa keamanan jaringan perlu dilakukan untuk mengetahui bagaimana status keamanan jaringan. Analisa awal terhadap status keamanan jaringan adalah sebagai berikut :

1. Vulnerability

Vulnerability adalah aktivitas menganalisis suatu jaringan untuk mengetahui bagian dari sistem yang cenderung/sering untuk diserang (kelemahan pada sistem jaringan). Aktivitas ini sangat membantu untuk meningkatkan keamanan jaringan dengan mengetahui dan mencatat sistem yang cenderung di serang.

2. Threat

Threat adalah aktivitas menganalisa jaringan dengan tujuan untuk mengetahui dan mempelajari kemungkinan acaman atau serangan yang datang dari luar maupun dari dalam yang dapat merusak pertahanan keamanan jaringan, seperti:

- Destruction yaitu usaha untuk merusak sistem pada jaringan, seperti virus, torojan dan lain-lain.
- Denial yaitu usaha untuk melumpuhkan kerja suatu layanan dalam jaringan
- Theft yaitu usaha mencuri informasi-informasi penting dalam jaringan
- Modification yaitu usaha untuk merubah data penting dalam jaringan
- Fraud yaitu usaha penipuan terhadap suatu sistem informasi seperti carding, pemalsuan data dan lain-lain.

3. Impact

Impact adalah tindakan menganalisis pengaruh-pengaruh apa saja yang diakibatkan oleh serangan yang terjadi dalam jaringan, seperti destruction, denial, dll.

4. Frequency

Frequency adalah kegiatan menganalisis dan mencatat tingkat keseringan suatu serangan dalam jaringan dalam kurun waktu tertentu. Contohnya mencatat frekuensi host dalam jaringan terkena virus/serangan lain.

5. Recommended Countermeasures

Setelah menganalisa dan mencatat beberapa obyek pada tahap analisa diatas, masalah-masalah yang terjadi dalam jaringan dapat dengan mudah

diselesaikan dan langkah-langkah pencegahannya. Kemudian hasilnya akan menjadi suatu pedoman yang berguna untuk peningkatan keamanan jaringan selanjutnya.

1. Mengenali Ancaman Terhadap Network Security

Langkah awal dalam mengembangkan rencana network security yang efektif adalah dengan mengenali ancaman yang mungkin datang. Dalam RFC 1244, Site security Handbook, dibedakan tiga tipe ancaman :

1. Akses tidak sah, oleh orang yang tidak mempunyai wewenang.
2. Kesalahan informasi, segala masalah yang dapat menyebabkan diberikannya informasi yang penting atau sensitif kepada orang yang salah, yang seharusnya tidak boleh mendapatkan informasi tersebut.
3. Penolakan terhadap service, segala masalah mengenai security yang menyebabkan sistem mengganggu pekerjaan-pekerjaan yang produktif.

2. Port Scanner

Server adalah host yang menyediakan sebuah layanan supaya client dapat mengakses layanan tersebut. Server sendiri, dalam pemrograman berbasis socket, terdiri dari IP dan nomor port. Contohnya socket 192.168.0.101:22, alamat IP tersebut berarti memiliki nomor port 22 (layanan berbasis protokol SSH) atau dengan kata lain host dengan nomor IP 192.168.0.101 membuka port 22 untuk layanan SSH. Dari segi keamanan, layanan tersebut memiliki beberapa kelemahan seperti kesalahan pemrograman, penggunaan password yang kurang aman atau sensitive data tidak terenkripsi. Kelemahan seperti itu dapat menjadikan host menjadi rentan akan serangan. Maka, host sebaiknya meminimalkan port yang terbuka.

Port Scanner adalah program khusus yang dirancang untuk menemukan layanan apa saja yang dijalankan pada host jaringan. Penyerang harus mengetahui kelemahan target sebelum dia melakukan serangan. Penyerang akan mencari tahu kelemahan yang ada pada layanan tersebut jika port terbuka. Terdapat beberapa tool yang dapat digunakan untuk menganalisa celah dalam keamanan jaringan, yaitu nessus, nmap, wireshark, dan lain-lain. Kegiatan praktik ini akan

menggunakan nmap sebagai tool dalam melihat atau menganalisa celah dalam jaringan komputer.

3. NMAP

Nmap (Network Mapper) adalah sebuah tool open source untuk mengeksplorasi dan audit keamanan jaringan. Nmap menggunakan IP raw untuk menentukan host mana saja yang tersedia pada jaringan, layanan, sistem operasi, jenis firewall dan sejumlah karakteristik lainnya. Dalam port scanner, nmap dapat membuat tabel yang berisi angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered).

Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup berarti port tidak memiliki aplikasi yang sedang listening, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi penyelidikan Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup.

Keunggulan yang dimiliki Nmap adalah:

- Nmap dapat digunakan dalam jaringan berskala besar.
- Nmap dapat berjalan diberbagai macam sistem operasi.
- Mudah digunakan
- Free
- Dokumentasi program Nmap lengkap dan baik.

Penggunaan Nmap

 # nmap {target} [scan tipe] [opsi]

Scan Tipe

Ada 2 macam scan tipe, yaitu TCP scan dan NON-TCP Scan.

TCP SCAN :

-sA (ACK scan).

Gunakan ACK scan untuk memetakan aturan firewall. Dapat membantu menentukan apakah firewall itu merupakan simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu firewall yang menjalankan advance packet filtering.

-sF (FIN scan)

Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX. Teknik ini mengirim suatu paket FIN ke port sasaran. FIN scan dapat membedakan port "tertutup" dan port "terbuka | filtered" pada beberapa sistem.

-sM (Maimon scan)

Teknik ini akan mengirimkan FIN dan ACK. Terhadap beberapa sistem BSD beserta turunannya dapat membedakan antara port "tertutup" dan port "terbuka | filtered".

-sN (Null scan)

Teknik ini membuat off semua flag. Null scan dapat membedakan port "tertutup" dan port "terbuka| filtered" pada beberapa sistem.

-sS (TCP SYN scan)

SYN Scan adalah teknik yang paling popular dan merupkan scan default dari nmap. Teknik ini tidak menggunakan 3 way hanshae secara lengkap, maka dari itu sering diset half open scanning. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING. Teknik ini tidak membuat koneksi penuh, maka tidak akan terdeteksi dan tidak tercatat pada log jaringan.

-sT (TCP connect scan)

Jenis scan ini konek ke port sasaran dan menyelesaikan three-way handshake (SYN, SYN/ACK, dan ACK). Scan jenis ini mudah terdeteksi oleh sistem sasaran.

-sW (Window scan)

Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem sistem tertentu (sebagai contoh, AIX dan FreeBSD) sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan.

-sX (Xmas Tree scan)

Teknik ini mengirimkan suatu paket FIN, URG, dan PUSH ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.

NON-TCP

-sU (UDP scan)

UDP port scan. UDP pada umumnya lebih lambat dan lebih sulit untuk memindai dari TCP, dan sering diabaikan oleh auditor keamanan.

-sO (IP scan protokol)

Scan IP protokol (TCP, ICMP, IGMP, dll) untuk menemukan layanan yang didukung oleh mesin target.

-sL (Scan List)

Hanya daftar mana yang akan dipindai (dengan nama reverse DNS jika tersedia).

-sP (Ping pemindaian)

Hanya melakukan ping scan (host discovery), maka mencetak host yang menanggapi.

SCAN OPTION

-A (Enable all advanced/aggressive options)

Merupakan TCP scan dengan mengakrifkan semua opsi yang ada, deteksi OS (-O), deteksi versi (-sV), script scanning (-sC), dan traceroute (- traceroute).

-O (Operating system detection)

Mendeteksi hanya sistem operasi.

-sV (Version detection)

Untuk menemukan versi dari layanan tertentu dari suatu host.

-sI (Idle Scan (Zombie))

Paket spoofing yang dikirimkan sehingga target tidak mengetahui. Inputan ini harus diiringi dengan –sl.

-b (FTP bounce attack)

Menggunakan layanan server FTP untuk scan port host lain dengan mengirimkan file ke setiap port yang menarik dari sebuah host target.

Ping Options

-PN (Don't ping before scanning)

Jangan memeriksa target sebelum scanning. Scan setiap target yang terdaftar.

-PB (Default ping type)

Kirim probe ICMP ping dan probe ACK untuk melihat apakah target yang up (seperti-PE-PA).

-PA (ACK ping)

Kirim satu ACK atau lebih untuk memeriksa target. Berikan daftar port atau memakai port default. Contoh masukan:

22,53,80

-PS (SYN ping)

Mengirim satu atau lebih probe SYN untuk memeriksa target. Berikan daftar port atau memakai port default.

Contoh masukan: 22,53,80

-PU (UDP probe)

Mengirim satu atau lebih probe UDP untuk memeriksa target. Berikan daftar port atau memakai port default.

-PO (IPProto probe)

Mengirim satu atau lebih probe protokol IP raw untuk memeriksa target. Berikan daftar port atau memakai port default.

4. Aktor Penyerang

Terdapat 2 jenis aktor dari serangan yang diluncurkan pada jaringan, yaitu:

- ***Hacker*: para ahli komputer yang memiliki kekhususan dalammenjebol keamanan sistem komputer dengan tujuan publisitas.**
- ***Cracker*:**penjebol sistem komputer yang bertujuan untuk melakukan pencurian atau merusak sistem.

5. Mengenal Jenis-jenis Serangan Umum

Terkadang para administrator keliru dalam menangkap apa yang sedang berlangsung. Sebuah aktifitas kecil, disangkanya normal-normal saja. Padahal bisa jadi itu adalah aksi penyerangan yang hebat. Serangan tersebut dapat berupa pasif, artinya hanya memantau dan mencuri informasi sedangkan ada aksi yang aktif yaitu dengan tujuan untuk mengubah atau merusak data dan jaringan.

Berikut ini adalah jenis-jenis serangan umum:

1. Trojan Horse

   Trojan adalah bentuk program (malware) yang kelihatan seperti berjalan normal membentuk fungsi-fungsi yang kita inginkan., padahal faktanya membahayakan. Trojan biasanya datang menyelinap dengan software lain yang kita install.

   Berikut contoh kerusakan yang ditimbulkan Trojan horse:

   - Mengintal virus-virus.
   - Secara random mematikan komputer.
   - Mematikan dan menggangu fungsi-fungsi antivirus dan program firewall.
   - Menginstall program backdoor pada sebuah komputer.
   - Membuat korup file-file.
   - Terhapus dan tertimpanya data-data dalam komputer.

- Memata-matai user-user komputer, mengoleksi informasi-informasi seperti kebiasaan browsing atau komunikasi.
- Mencatat log untuk menyimpan password.

2. Virus

   Virus merupakan salah satu bentuk Trojan, yaitu program yang dapat meng-copy dan menempelkan dirinya sendiri ke program lain, untuk menginfeksi data dalam komputer. Virus ini datang dalam berbagai bentuk dan telah merugikan banyak orang.

3. Worm

   Worm adalah program yang dapat menduplikasi dirinya sendiri. Biasanya menggunakan koneksi jaringan untuk mengirim Salinan dirinya ke node-node lain. Semua aktifitas ini dilakukan tanpa keterlibatan manusia. Berbeda dengan virus, worm tidak menempelkan dirinya ke aplikasi lain. Worm biasanya tersebar dari address book dari alamat email.

4. Logic Bomb

   Logic bomb biasanya adalah potongan kode yang disisipkan secara sengaja ke sebuah software sistem sehingga dapat membentuk fungsi-fungsi yang keliru atau merugikan. Bom logika atau bom waktu adalah suatu program yang beraksi karena dipicu oleh sesuatu kejadian atau setelah selang waktu berlalu.Program ini biasanya ditulis oleh orang dalam yang akan mengancam perusahaan atau membalas dendam kepada perusahaan karena sakit hati.

5. Eavesdropping

   Eavesdropping memungkinkan pelaku penipuan untuk mengamati komunikasi atau transmisi data pribadi. Salah satu cara untuk menangkap sinyal adalah dengan menyusun penyadap suara (wiretap). Secara umum, komunikasi-komunikasi jaringan berada dalam posisi dan format yang tidak aman. Banyak sekali peluang dimana seseorang dapat secara diam-diam mendengar pembicaraan paket yang dikirim.

6. Spoofing

   Spoofing adalah tekhnik yang digunakan untuk mengakses yang tidak sah ke suatu komputer dimana si penyerang masuk dengan cara berpura-pura memalsukan bahwa mereka host yang dapat dipercaya. Serangan ini seringkali dibentuk dengan bantuan URL Spoofing, yang mengeksploitasi bug-bug browser web daam rangka menampilkan URL palsu atau dengan menyalahgunaka DNS Cache untuk mengarahkan user masuk ke dalam situs yang palsu.

7. Denial-of-service

   Serangan yang paling sering dilakukan oleh *hacker* untuk melumpuhkan suatu sistem aplikasi komputer atau server dengan cara menghabiskan sumber daya *resource* server, diharapkan dari lumpuhnya sistem server akan turut melumpuhkan sistem pengamanan server sehingga penyerang dapat melakukan aktivitas pembobolan atau perusakan. Sistem kerja serangan ini sebenarnya amat sederhana yaitu membanjiri server dengan jumlah lalu lintas data yang tinggi, atau melakukan *request data* ke sebuah server sehingga server tidak lagi dapat melakukan penerimaan dan menjadi lumpuh. Serangan DDos ini juga yang paling banyak menghabiskan *bandwidth* sebuah *website*, untuk itu Anda harus melengkapi *website* dengan Firewall untuk melindungi dari serangan ini.

   Dalam sebuah serangan *Denial of Service*, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

   - Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai *traffic flooding*.
   - Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga

request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*.

- Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

8. Man-in-the-middle Attack

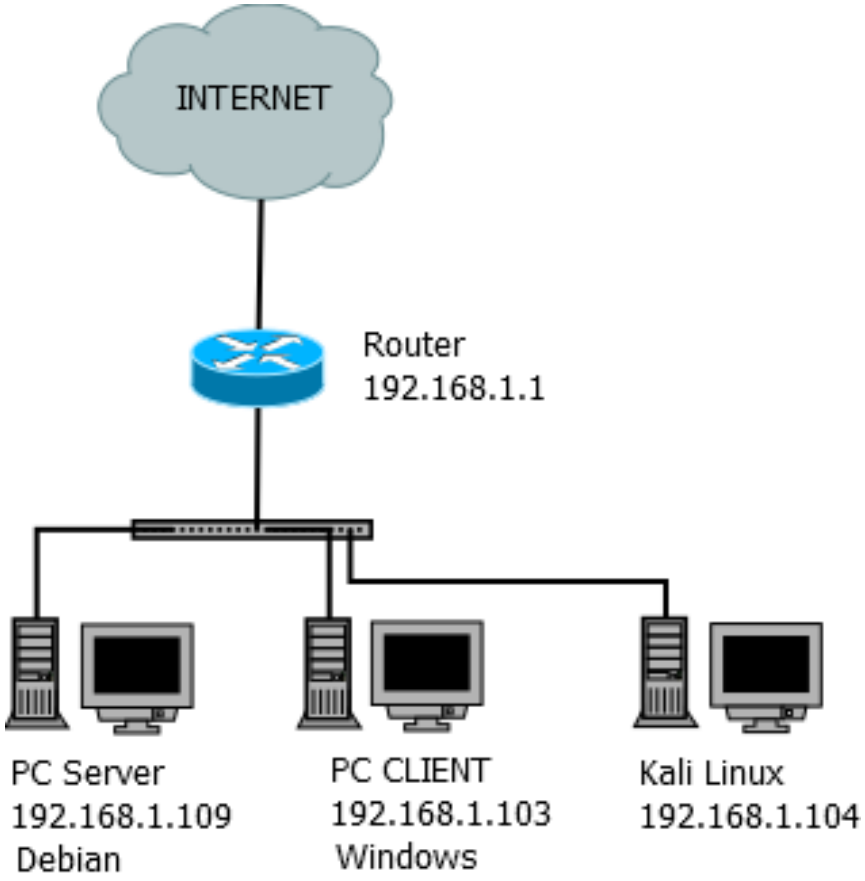
   Dalam serangan mitm, seorang attacker akan berada di tengah-tengah komunikasi antara dua pihak. Seluruh pembicaraan yang terjadi di antara mereka harus melalui attacker dulu di tengah. Attacker dengan leluasa melakukan penyadapan, pencegatan, pengubahan bahkan memalsukan komunikasi

9. Serangan Layer Aplikasi

   Serangan layer aplikasi biasanya tertuju pada server-server aplikasi. Penyerangan dengan sengaja menimbulkan kesalahan pada sistem operasi atau server aplikasi. Ini menyebabkan penyerang memperoleh kemampuan untuk melakukan bypass control akses normal. Dari situasi ini, penyerang mengambil banyak keuntungan: memperoleh control atas aplikasi-aplikasi, sistem atau jaringan.

D. Aktivitas Pembelajaran

Praktikum ini akan Nmap akan berada pada sistem operasi Kali Linux. Kali linux yang digunakan adalah Kali Linux 2.0. Berikut adalah topologi jaringannya:



Gambar 1.1 Topologi Jaringan Praktikum Nmap Linux

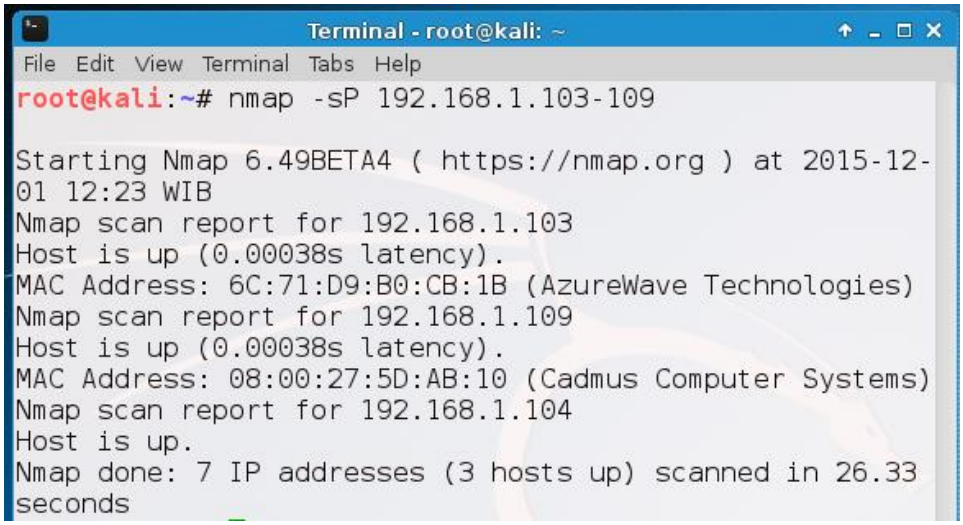
1. Mencari IP Address Target

Seumpama kita tidak mengetahui IP PC dan sistem operasinya, maka dapat menggunakan perintah

#nmap –sP [iprange]

Contoh :

#nmap –sP 192.168.1.103-109



Gambar 1.2 Nmap Mencari IP Address Target

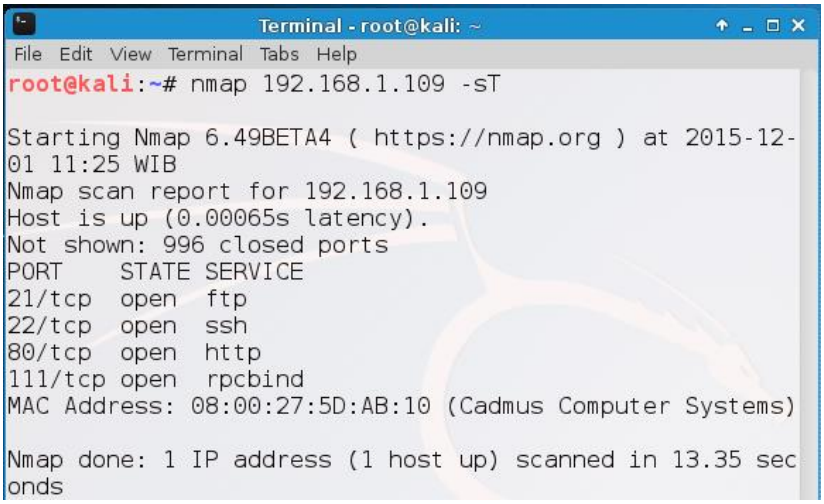
Perintah ini berarti pengguna nmap ingin mengetahui semua IP Address yang aktif dalam suatu jaringan dengan IP area 192.168.1.103-192.168.1.109.
Gambar dibawah ini menunjukkan 3 host yang sedang aktif, yaitu 192.168.1.103, 192.168.1.109 dan 192.168.1.104.

2. Port Scanning

Setelah IP Address target telah diketahui, atau ketika seorang Administrator server ingin mengetahui celah port atau port yang terbuka pada servernya, gunakan perintah

-sT

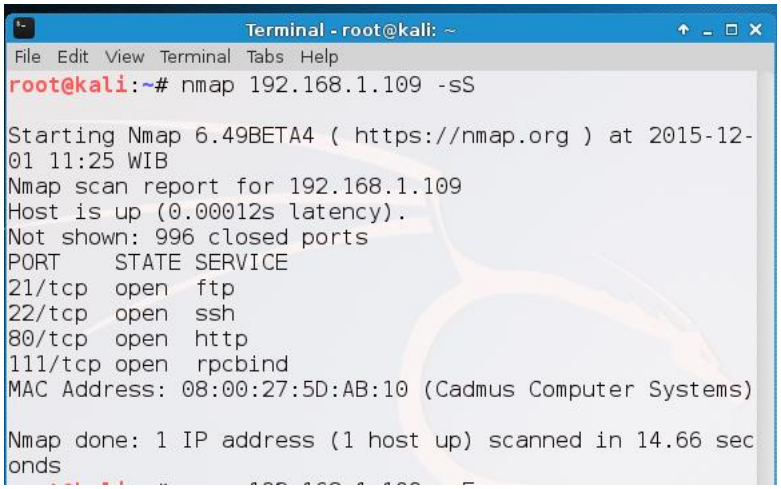
#nmap 192.168.1.109 –sT



Gambar 1.3 Nmap Port Scanning sT

#nmap 192.168.1.109 –sS

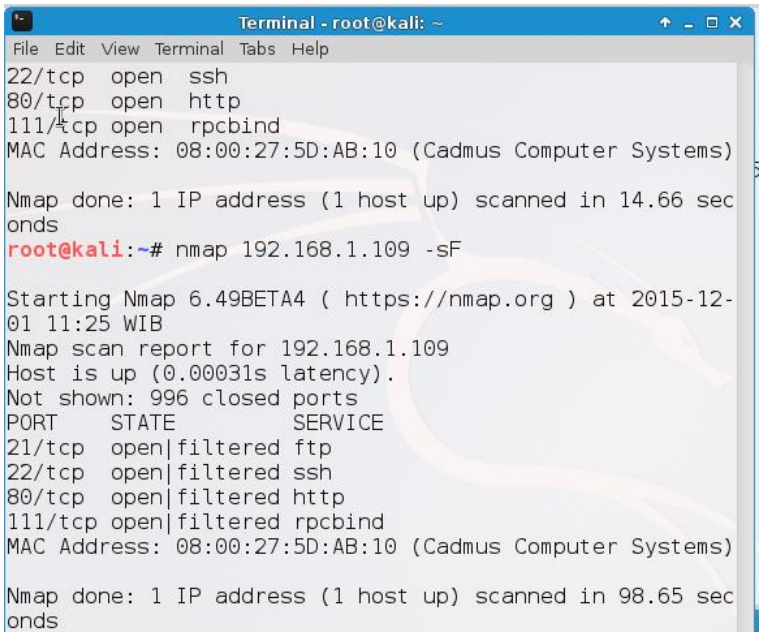
-sS ini membuka tidak koneksi TCP secara utuh, dan tersembunyi. Sedangkan –sT membuka TCP secara utuh dan memiliki kelebihan yaitu tercepat.



Gambar 1.4 Nmap Port Scanning sS

#nmap 192.168.1.109 –sF

Teknik ini dapat menampilkan informasi state dari layanan.



Gambar 1.5 Nmap Port Scanning sF

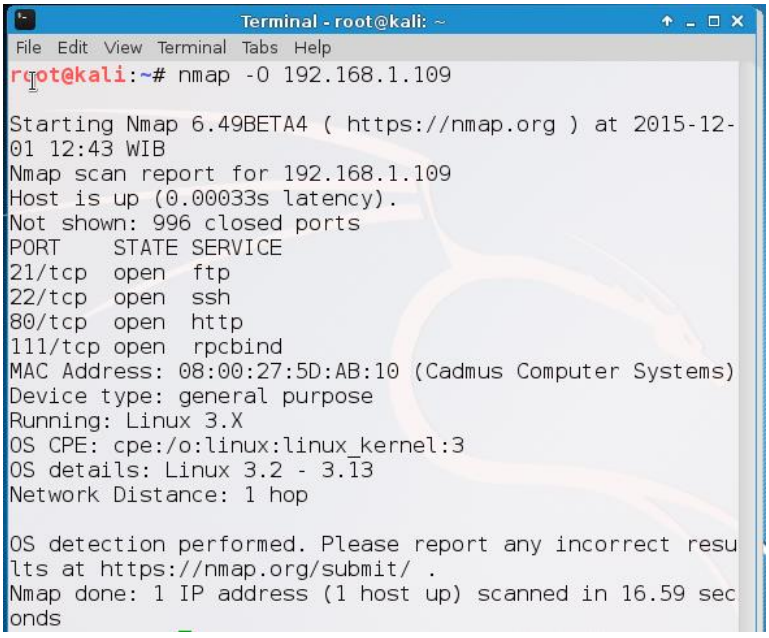
3. Mendeteksi Sistem Operasi Target

Untuk mendeteksi sistem operasi dari suatu host, digunakan perintah

 # nmap –O [iptarget]

Contoh :

 # nmap –O 192.168.1.109



Gambar 1.6 Nmap Deteksi Sistem Operasi

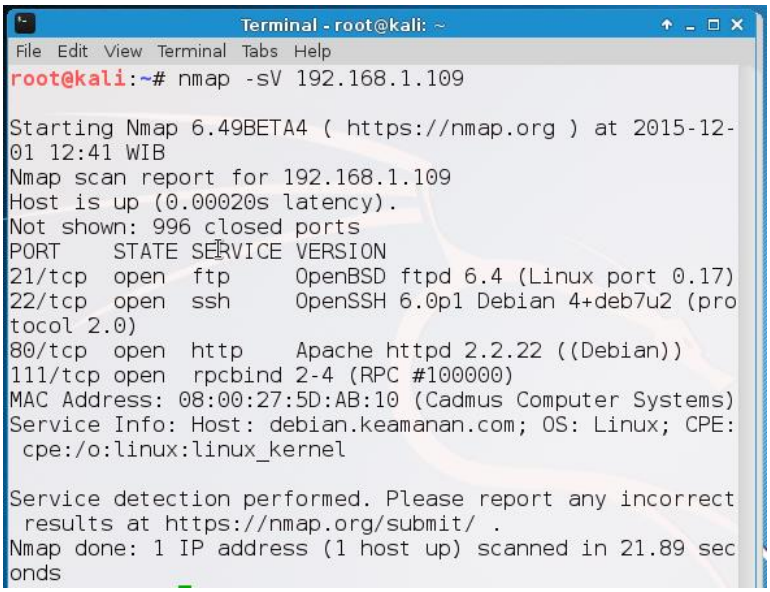
4. Memindai Nomor Port dan Versi Layanan

Untuk mendeteksi sistem operasi dari suatu host, digunakan perintah

 # nmap –sV [iptarget]

Contoh :

 # nmap –sV 192.168.1.109



Gambar 1.7 Nmap Memindai Port dan Versi Layanan

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiatan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.

6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Untuk mengetahui sistem operasi dari suatu host digunakan perintah apa? beri contohnya!

……
……
……
……
……

2. Untuk memindai port dari suatu host dengan 3-way handshake digunakan perintah apa? berikan contohnya!

……
……
……
……
……

3. Apa perbedaan –sT dan –sS pada perintah scan options nmap?

……
……
……
……
……

F. Rangkuman

Analisa awal terhadap status keamanan jaringan adalah sebagai vulnerability, threat, impact, frequency dan recommended countermeasures. Port Scanner adalah program khusus yang dirancang untuk menemukan layanan apa saja yang dijalankan pada host jaringan. Penyerang harus mengetahui kelemahan target sebelum dia melakukan serangan. Penyerang akan mencari tahu kelemahan yang ada pada layanan tersebut jika port terbuka. Nmap (Network Mapper) adalah sebuah tool open source untuk mengeksplorasi dan audit

keamanan jaringan. Nmap menggunakan IP raw untuk menentukan host mana saja yang tersedia pada jaringan, layanan, sistem operasi, jenis firewall dan sejumlah karakteristik lainnya. Dalam port scanner, nmap dapat membuat tabel yang berisi angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered).

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang analisa kemungkinan potensi serangan keamanan jaringan dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami perintah Nmap untuk mengetahui sistem operasi dari suatu host serta berapa prosen pencapaian kompetensinya?
3. Apakah saudara sudah memahami perintah untuk melihat port yang terbuka dari suatu host berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. #nmap –O [iptarget]
   Contoh : #nmap –O 192.168.0.103
2. #nmap –sT [iptarget]
   Contoh : #nmap –sT 192.168.0.109
3. -sS ini membuka tidak koneksi TCP secara utuh, dan tersembunyi. Sedangkan –sT membuka TCP secara utuh dan memiliki kelebihan yaitu tercepat.

2

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 2: Menganalisis Sistem Keamanan Jaringan Yang Diperlukan

A. Tujuan Pembelajaran

Setelah mengikuti kegiatanbelajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menganalisis sistem keamanan jaringan yang diperlukan

B. Indikator Pencapaian Kompetensi

- Memahami konsep analisis sistem keamanan jaringan yang diperlukan

C. Uraian Materi

Kemajuan teknologi di bidang teknologi informasi saat ini sudah berkembang pesar khususnya di bidang jaringan. Kemajuan teknologi tersebut mendorong perusahaan meningkatkan akses kontrol setiap bagian perusahaan yang ada. Salah satu contohnya adalah ketika IT Manager membuat user account untuk setiap user agar dapat mengolah akses yang dimiliki. Dari hal tersebut dapat mengancam keamanan sistem maupun data dari perusahaan yang terdapat pada sistem. Salah satu contohnya adalah ketika user pada jaringan LAN (Local Area Network) mengakses website/server yang mengandung konten tidak baik pada Internet kemudian men-download-nya yang ternyata file tersebut berisi virus, worm, trojan dan sebagainya.

Dengan demikian, penyerang dapat memasuki bahkan merusak sistem yang dapat berdampak buruk bagi perusahaan. Oleh karena itu, dibutuhkannya suatu software atau hardware yang dapat digunakan sebagai penghalang bagi penyerang tersebut untuk masuk ke dalam sistem. Berikut ini adalah software atau hardware yang dapat digunakan seorang administrator jaringan untuk mengamankan jaringan dari serangan pihak luar:

1. **Firewall**

Firewall merupakan suatu sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan luar. Firewall dapat diimplementasikan dalam perangkat keras maupun perangkat lunak atau bahkan keduanya. Secara umum, firewall memisahkan antara public network dengan private network. Firewall bekerja dengan menyaring lalu lintas jaringan yang menggunakan alamat IP, port number, dan protokol. Untuk linux, IP Tables digunakan untuk firewall. Iptables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalu lintas data.

Secara konseptual, Firewall terbagi menjadi dua yaitu:

a. Network Level

   Firewall Network Level ini bekerja berdasarkan keputusan terhadap alamat sumber, alamat tujuan, dan port yang terdapat dalam setiap paket. Firewall Network Level ini bekerja dengan sangat cepat dan transparan bagi penggunanya.

b. Application Level

   Firewall Application Level ini adalah host yang berjalan sebagai proxy server yang di mana tidak mengijinkan lalu lintas antar jaringan serta dapat melakukan loggin dan auditing setiap lalu lintas yang melaluinya. Firewall Application Level ini menyediakan laporan audit yang lebih terperinci.

Berikut adalah beberapa contoh dari Firewall yang bersifat free:

a. Ipchains

   Ipchains adalah user-space portion dari kode terbaru paket filter Linux yang diperkenalkan dalam kernel versi 2.1.102.

b. Falcon Project

   Falcon terdiri dari tiga modul utama yaitu proxy Falcon (ditulis dalam Perl), 3rd-party proxy (squid/qmail/BIND8) yang dimodifikasi untuk lingkungan chroot dan konsep umum untuk OS hardening.

c. Juniper

   Juniper didesain agar bekerja pada dual homed bastion host yang tidak mem-forwarrd paket-paket antara interface. Juniper mengimplementasikan fasilitas proxy transparan hingga memungkinkan mesin-mesin internal untuk

mengakses Internet secara transparan seolah-olah terhubung secara langsung ke Internet.

d. Floppyfw

   Floppyfw menggunakan kemampuan firewall dasar Linux yang memiliki sistem packaging yang sederhana. Sangat sesuai untuk mengamankan jaringan pada ADSL dan kabel menggunakan IP statik dan DHCP.

e. T.Rex Open Source Firewall

   T.Rex Open Source Firewall berjalan pada Linux, Solaris, dan AIX. Fitur yang ditawarkan oleh T.Rex ini mencakup dukungan untuk VPN (Virtual Private Network), NAT (Network Address Translation), dan aplikasi proxy tinggi seperti web caching, workload balancing, content filtering, high availability, dukungan SOCKS, dan sebagainya.

Sedangkan di bawah ini adalah contoh Firewall dengan versi commercial:

a. Checkpoint Firewall-1

   Checkpoint Firewall-1 adalah suite produk keamanan yang telah mendukung enterprise security, access control, autentikasi, content security, NAT, Reporting Module, VPN, Intrusion Detection, High Availability, LDAP User Account Management, dan Third Party Security Device Management.

b. Raptor

   Raptor didasarkan pada arsitektur proxy based yang memonitor seluruh lalu lintas pada level aplikasi serta men-scan seluruh aplikasi dan protokol yang keluar dan masuk jaringan.

c. Xsentry

   XSentry 1.1 Firewall terdiri dari XSentry Administration Client dan XSentry Firewall Server.

Berikut adalah beberapa kriteria yang menjadi perhitungan bagi firewall untuk mengijinkan suatu paket data dapat lewat atau tidak:

a. Alamat IP dari sumber
b. Port TCP/UDP sumber
c. Alamat IP dari komputer tujuan
d. Port TCP/UDP tujuan data pada komputer tujuan
e. Informasi dari header yang disimpan dalam paket data.

Fungsi umum firewall adalah :

- Mengatur dan mengontrol lalu lintas jaringan
- Melakukan autentikasi terhadap akses
- Melindungi sumber daya dalam jaringan privat
- Mencatat semua kejadian, dan melaporkan kepada administrator

Paket filtering firewall adalah salah satu jenis teknologi keamanan yang digunakan untuk mengatur paket-paket apa saja yang diizinkan masuk ke dalam sistem atau jaringan dan paket-paket apa saja yang diblokir. *Packet filtering* umumnya digunakan untuk memblokir lalu lintas yang mencurigakan yang datang dari alamat IP yang mencurigakan, nomor port TCP/UDP yang mencurigakan, jenis protokol aplikasi yang mencurigakan, dan kriteria lainnya.

Bagian yang diperiksa dari paket data tersebut adalah bagian header yang berisi informasi penting, yaitu:

- IP address sumber
- IP address tujuan
- Protokol (TCP/UDP/ICMP)
- Port sumber dari TCP atau UDP
- Port tujuan dari TCP atau UDP
- Tipe pesan dari ICMP
- Ukuran dari paket

Internet adalah gabungan PC yang dihubungkan melalui router-router yang saling terkoneksi dimana setiap PC memiliki alamat yang berbeda-beda (unik). Firewall jenis ini bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam Access Control List firewall, router tersebut akan mencoba memutuskan apakah hendak meneruskan paket yang masuk tersebut ke tujuannya atau menghentikannya.

Cara Kerja Firewall

Firewall mengawasi paket data yang lewat melalui router. Router ini dapat berfungsi sebagai sebuah server karena itu router ini dituntut untuk dapat memberikan route pada paket yang datang kepadanya. Router juga memikirkan bagaimana suatu paket data dapat sampai pada tujuan yang sebenarmya. Dalam hal ini, router tersebut saling berkomunikasi melalui protokol untuk memberikan route terhadap paket data yang datang. Protokol ini disebut Routing Information Protocol (RIP) yang menghasilkan sebuah tabel routing. Tabel routing inilah yang menunjukkan kemana paket data akan dikirim.

Pada beberapa sistem, teknik pengamanan jaringan dapat hanya dilakukan dengan memasang router filtering dan hanya pada lokasi tertentu saja pada jaringan kita. Oleh karena itu, router yang berfungsi sebagai filter harus dapat mengambil keputusan apakah paket berasal dari jaringan lokal atau berasal dari luar (internet), kegiatan ini disebut *source address forgery*.

Yang diperiksa dari sebuah paket data adalah bagian header nya yang mengandung informasi penting tentang paket tersebut.

- **Protokol,** informasi yang terdapat pada header ini tersusun atas byte-byte. Byte ke 9 merupakan informasi tentang protokol yang digunakan.
- **Alamat IP Sumber,** adalah IP address sumber yang mengirimkan paket data tersebut (berukuran 32 byte).
- **Alamat IP Tujuan,** adalah IP address tujuan paket tersebut dikirimkan (berukuran 32 byte).
- **Port Sumber (TCP/UDP),** adalah port yang menjadi tempat keluarnya paket data pengirim. Pada setiap akhir dari koneksi TCP atau UDP tersambung dengan sebuah port, Walaupun port-port TCP terpisah dan cukup jauh dari port-port UDP. Port-port yang mempunyai nomor dibawah 1024 diterbalikan karena nomor-nomor ini telah didefinisikan secar khusus, sedangkan untuk port-port yang bernomor diatas 1024 (inklusif) lebih dikenal dengan port ephermal. Konfigurasi dari nomor pengalamatan ini diberikan sesuai dengan pilihan dari vendor.
- **Port Tujuan,** adalah port yang menjadi saluran masuk paket data pada komputer penerima paket data.
- **Status Koneksi,** status koneksi memberitahkan apakah paket data yang dikirimkan adalah paket pertama dari sesi di jaringan. Jika paket merupakan

paket pertama maka pada TCP header diberlakukan ‘false’ atau 0 dan untuk mencegah sebuah host untuk mengadakan koneksi dengan menolak atau membuang paket yang mempunyai bit set ‘false’ atau 0.

Header pada paket data tersebut kemudian diperiksa , dengan cara membandingkannya dengan policy atau kebijakan yang telah dibuat oleh administrator jaringan. Apabila ada salah satu kebijakan tadi dilanggar, maka paket data yang datang akan di drop.

Metode paket filtering firewall ini memiliki beberapa keunggulan, yaitu :

- Performa yang tinggi, karena melakukan pengecekan terhadap banyak faktor (port, ip address, dll).
- Dapat diterapkan pada perangkat jaringan biasa router atau switch tanpa memerlukan perangkat tambahan.
- Efektif

Disamping itu paket filtering firewall ini juga memiliki kelemahan yang berkaitan dengan konfigurasi, yaitu :

- Konfigurasi kompleks, agak sulit dalam mengkonfigurasi karena penguasaan terhadap port, ip address, dll.
- Mudah terjadi kesalahan dalam konfigurasi.
- Susah untuk mengkonfig pada protokol yang dinamis (misalnya FTP)
- Tidak dapat meng-filter berdasarkan content (misalnya lampiran pada email, javascript, ActiveX)

2. **Honeypot**

Honeypot adalah suatu server virtual yang terlihat seperti server asli sehingga dapat menjadi umpan yang berfungsi untuk mengalihkan perhatian. Honeypot tidak menjalankan layanan yang sebagaimana umumnya server lakukan. Honeypot berpura-pura menjalankan layanan yang umumnya server lakukan sehingga akan membuat para penyusup berpikir bahwa dia adalah server sesungguhnya. Selain penjelasan di atas, honeypot juga berfungsi untuk melihat tehnik yang digunakan oleh para penyusup untuk masuk ke dalam server sehingga dapat mengumpulkan bukti sehingga para pelaku dapat diproses secara hukum.

Terdapat beberapa unsur yang terdapat dalam honeypot, yaitu:

a. Monitoring / Logging Tools
b. Alerting Mechanism
c. Keystroke Logger
d. Packet Analyzer
e. Forensic Tools

Honeypot dapat diklasifikasikan berdasarkan tingkat interaksi yang dimilikinya. Semakin tinggi tingkat aktivitas penyerang di dalam sistem, maka semakin tinggi pula tingkat interaksi yang dimiliki honeypot. Honeypot memiliki dua tingkat interaksi, yaitu:

a. Low Interaction Honeypot

   Tipe honeypot yang hanya mensimulasikan sebagian service saja seperti hanya service FTP saja. Contoh dari jenis honeypot ini adalah Honeyd, Mantrap, Specter.

b. High Interaction Honeypot

   Tipe honeypot ini menggunakan keseluruhan resource sistem yang di mana honeypot ini dapat dikatakan sangat mirip dengan sistem (server) aslinya. Contoh honeypot ini adalah Honeynet.

3. **Antivirus**

Antivirus merupakan suatu software yang dibuat yang bertujuan untuk mengantisipasi dan menghapus virus yang menyerang sistem jaringan komputer. Antivirus dalam keamanan jaringan komputer memiliki fitur security network yang bertugas untuk melindungi dan menjaga keamanan komputer ketika terhubung dengan jaringan lokal (LAN) maupun jaringan Internet. Antivirus ini bekerja dengan mengidentifikasi IP address dan domain yang mencoba terhubung dengan komputer. Kemudian antivirus akan memverifikasi IP address dan domain tersebut apakah aman atau tidak. Jika aman, maka akan terhubung namun jika tidak maka fitur security network akan menyala dan akan langsung memutuskan koneksi.

Berikut adalah kelebihan dari antivirus:

a. Merupakan software keamanan yang memberikan service real time bagi sebuah system,
b. Berguna untuk detection, repair, block akses yang tidak disetujui oleh sistem,
c. Berguna untuk menangkal serangan dari program yang bersifat jahat yang berasal dari luar sistem.

4. IDS (Intrusion Detection System)

IDS (Intrusion Detection System) merupakan suatu aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi adanya aktivitas yang mencurigakan dalam suatu sistem atau jaringan. Ada dua jenis dari IDS sendiri, yaitu:

a. Network IDS (NIDS)
b. Host IDS (HIDS)

Pada IDS yang berbasikan network atau jaringan, IDS akan meneripa copy paket yang ditujukan pada suatu host untuk kemudian memeriksa paket-paket tersebut. IDS akan memberikan suatu tanda peringatan kepada admin jika ditemukan adanya paket yang berbahaya. IDS hanya akan memeriksa salinan dari paket asli sehingga walaupun ditemukan sebuah paket yang berbahaya, paket tersebut akan tetap mencapai host yang ditujunya. Berikut adalah beberapa hal yang harus dilakukan admin jika IDS mendeteksi suatu serangan:

a. Memberikan peringat berupa SMS, e-mail atau yang lainnya,
b. Mengkonfigurasi ulang firewall,
c. Menjalankan program respon terhadap serangan,
d. Logging serangan dan event.

Berikut adalah kelebihan yang dimiliki oleh IDS:

a. Dapat mendeteksi serangan baik dari luar maupun dari dalam
b. Dapat disesuaikan dengan mudah dan memberikan perlindungan untuk keseluruhan jaringan
c. Dapat dikelola secara terpusat
d. Menyediakan pertahanan dari dalam
e. Menyediakan layer tambahan untuk perlindungan
f. IDS memonitoring Internet untuk perlindungan
g. IDS melacak aktivitas pengguna dari saat masuk hingga keluar

Dalam menerapkan IDS, dibutuhkan suatu program yang dapat menjalankan IDS. Berikut adalah contoh program IDS:

a. Chkwtmp

   Program yang melakukan pengecekan terhadap entry kosong.

b. Tcplogd

   Program yang mendeteksi stealth scan yang merupakan scanning yang dilakukan tanpa harus membuat sebuah sesi TCP.

c. Hostsentry

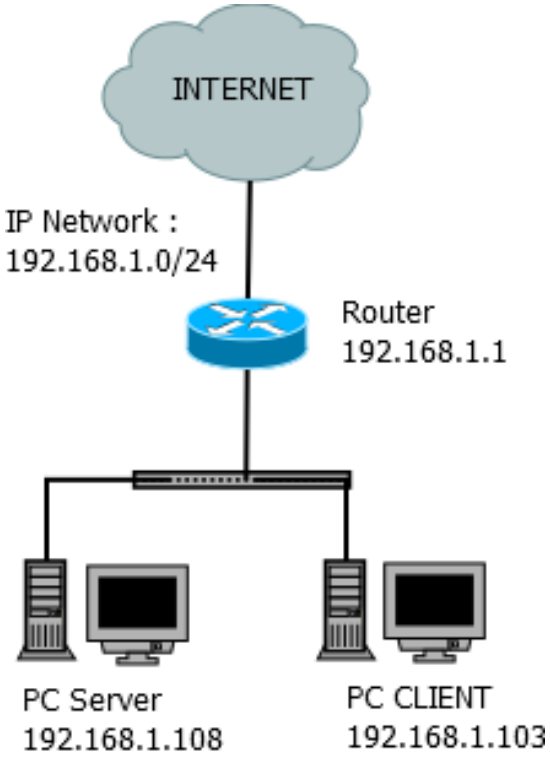
   Program yang mendeteksi login anomali.

d. Snort

   Snort pada umumnya merujuk kepada IDS yang sifatnya ringan karena diperuntukkan bagi jaringan kecil. Snort sangat fleksibel karena arsitekturnya yang berbasis rule.

D. Aktivitas Pembelajaran

Pada praktikum ini, firewall akan dipasang pada router debian untuk pengamanan dan antisipasi serangan dari luar. Selain firewall, akan diinstal antivirus Norton Security pada PC Client. Berikut ini adalah topologinya.



Gambar 2.1 Topologi Sistem Keamanan Jaringan

Untuk konfigurasi firewall Linux, biasanya memakai implementasi firewall

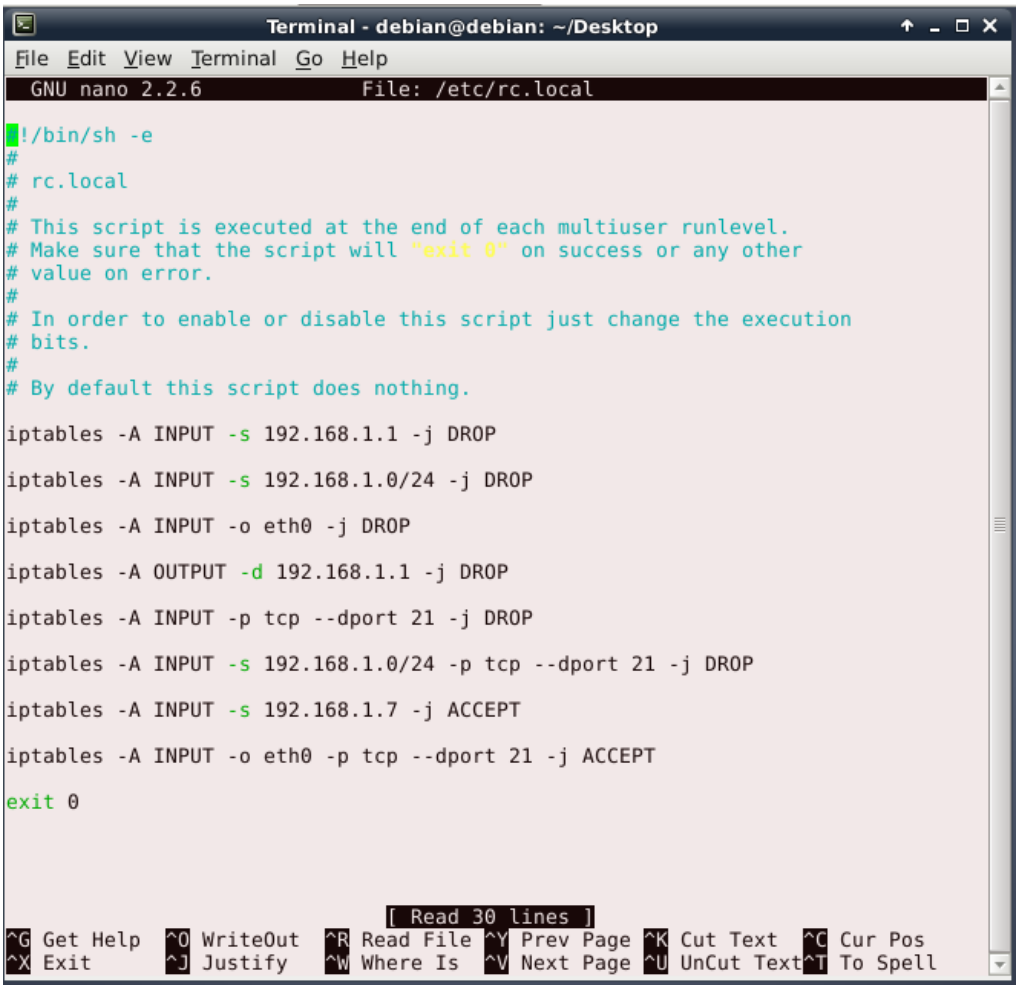
IP Tables yang merupakan packet filter. IP Tables adalah peningkatan dari IP Chains dan menyediakan fitur lanjutan semacam stateful packet filtering, NAT, MAC Address filtering dan sebagainya. Di dalam IP Tables ada tiga kelompok aturan yang disebut chain, masing-masing berisi aturan tentang apa yang harus dilakukan oleh komputer, kemudian keluar dari komputer dan melewati komputer.

1. **Pemasangan Firewall Pada Router**

1. Buka pengaturan default firewall pada direktori /etc/rc.local menggunakan nano

Gambar 2.2 Buka Pengaturan Default Firewall

2. Ketik baris perintah yang ingin diaplikasikan untuk firewall pada file tersebut kemudian simpan file tersebut kembali.



Gambar 2.3 Pengaplikasian Firewall

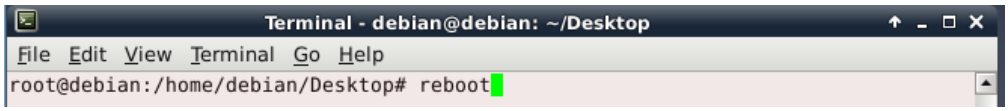
Penjabaran perintah di atas:

- Perintah ‘iptables –A INPUT –s 192.168.1.1 –j DROP’ digunakan untuk memblokir paket yang ingin masuk ke dalam jaringan melalui alamat ip 192.168.1.1.
- Perintah ‘iptables –A INPUT –s 192.168.1.0/24 –j DROP’ digunakan untuk memblokir paket data yang ingin masuk ke dalam jaringan melalui semua alamat ip dari network id 192.168.1.0 dengan subnet /24.
- Perintah ‘iptables –A INPUT –o eth0 –j DROP’ digunakan untuk memblokir semua paket data yang ingin memasuki jaringan melalui interface Ethernet0.
- Perintah ‘iptables –A OUTPUT –d 192.168.1.1 –j DROP’ digunakan untuk memblokir semua paket data yang akan keluar dari jaringan dengan alamat ip tujuan 192.168.1.1.

- Perintah ‘iptables –A INPUT –p tcp --dport 21 –j DROP’ digunakan untuk memblokir paket data tcp yang akan memasuki jaringan melalui port 21 (FTP).
- Perintah ‘iptables –A INPUT –s 192.168.1.0/24 –p tcp --dport 21 –j DROP’ digunakan untuk memblokir paket data tcp yang akan memasuki jaringan dari semua alamat ip dengan network id 192.168.1.0 subnet /24 melalui port 21 (FTP).
- Perintah ‘iptables –A INPUT –s 192.168.1.7 –j ACCEPT’ digunakan untuk mengizinkan paket data dari alamat 192.168.1.7 memasuki jaringan.
- Perintah ‘iptables –A INPUT –o eth0 –p tcp --dport 21 -j ACCEPT ’ digunakan untuk mengizinkan paket data tcp dari interface Ethernet 0 melalui port 21.

Bentuk perintah secara umum seperti di bawah ini:
iptables –A [INPUT | OUTPUT] –s [alamat_ip | newtwork_id/subnet_mask] –o [interface] –p [tcp|udp] --dport [nomor_port] –j[ACCEPT | DROP]

3. Setelah menyimpan file rc.local, reboot perangkat dengan perintah di bawah ini:

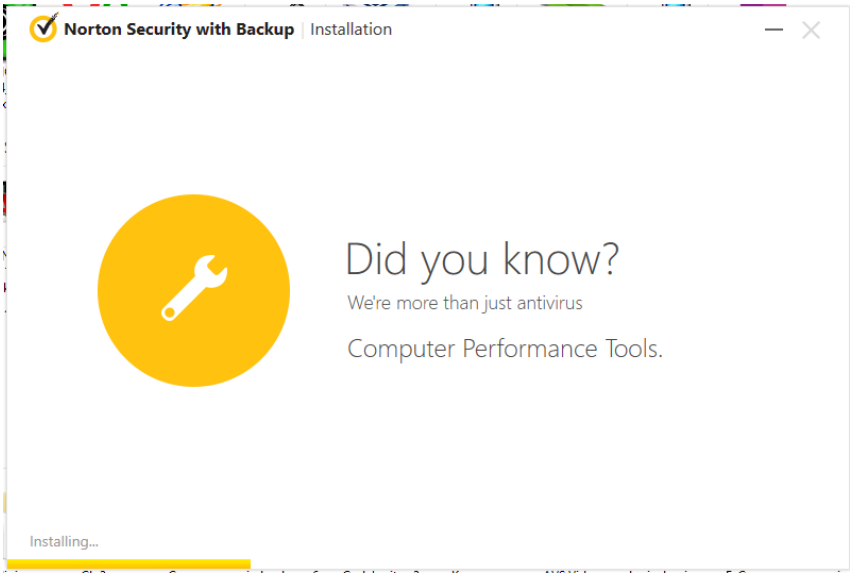


Gambar 2.4 Reboot File

2. **Pemasangan Antivirus Pada Client**

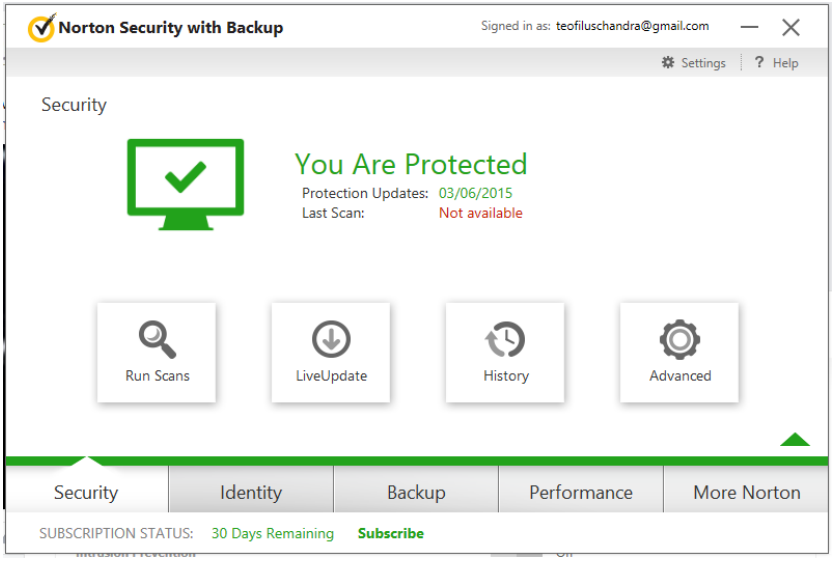
Antivirus yang dipasang pada Client adalah Norton Internet Security yang sekarang bernama Norton Security. Aplikasi ini dapat diunduh pada website resminya yaitu us.norton.com. Antivirus Keunggulan pertama Norton Security yaitu mengidentifikasi, menjaga informasi pribadi dan menghentikan ancaman-ancaman online dengan cepat. Fitur-fitur dari Norton antara lain Norton Identity Safe in the Cloud untuk melindungi informasi pribadi dan finansial dari penjahat cyber dan menjaga keamanan pengguna dari situs-situs laman palsu. Norton juga memiliki firewall untuk mencegah serangan dari jaringan internet.

1. Install Norton Security pada PC Client.



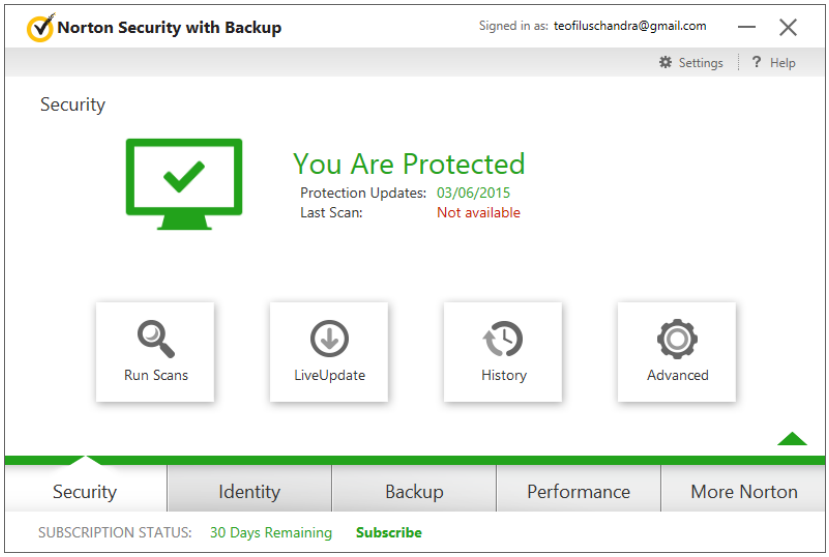
Gambar 2.5 Install Norton Security

2. Masuk dalam menu security



Gambar 2.6 Menu Norton Security

3. Aktifkan pengamanan yang dibutuhkan dalam jaringan, seperti Intrusion Prevention atau Smart Firewall. Fitur ini dapat diaktifkan untuk mode install yang berbayar.



Gambar 2.7 Aktifkan Pengamanan Norton Security

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiaan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Untuk memblokir paket data tcp yang akan memasuki jaringan melalui SSH digunakan perintah apa?

   ……

   ……

.....

.....

.....

2. Untuk memblokir semua paket yang akan masuk melalui eth0 digunakan perintah apa?

.....

.....

.....

.....

.....

3. Apakah perintah untuk mengizinkan paket data dari alamat 192.168.1.3 memasuki jaringan?

.....

.....

.....

.....

.....

F. Rangkuman

Software atau hardware yang dapat digunakan seorang administrator jaringan untuk mengamankan jaringan dari serangan pihak luar. Seorang administrator juga harus bisa menganalisis jaringan untuk mengamankan jaringan dari serangan. Ada beberapa mekanisme dari software atau hardware yang dapat digunakan untuk menjaga jaringan, yaitu firewall, honeypot, anti virus dan honeypot.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang perintah yang ada pada IP Tables dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami konsep untuk menganalisis sistem keamanan jaringan yang diperlukan serta berapa prosen pencapaian kompetensinya?

3. Apakah saudara sudah memahami perintah untuk memblokir paket tcp yang masuk melalui port SMTP dan berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. iptables –A INPUT –p tcp --dport 22 –j DROP adalah perintah untuk blok paket tcp dengan port layanan SSH.
2. iptables –A INPUT –o eth0 –j DROP untuk memblokir paket data yang masuk melalui Ethernet 0.
3. iptables –A INPUT –s 192.168.1.3 –j ACCEPT adalah perintah yang digunakan untuk mengijinkan paket data dari alamat 192.168.1.3 memasuki jaringan.

3

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 3: Menerapkan Langkah-Langkah Penguatan Host (Host Hardening)

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menerapkan langkah-langkah penguatan host (host hardening).

B. Indikator Pencapaian Kompetensi

- Memahami konsep menerapkan langkah-langkah penguatan host (host hardening).
- Mampu menerapkan langkah-langkah penguatan host.

C. Uraian Materi

Host Hardening adalah prosedur yang meminimalkan ancaman yang datang dengan mengatur konfigurasi dan menonaktifkan aplikasi dan layanan yang tidak diperlukan. Instalasi firewall, instalasi antivirus, menghapus cookie, membuat password , menghapus program yang tidak diperlukan itu semua termasuk dalam Host Hardening. Host Hardening menyediakan berbagai perlindungan dalam sistem komputer. Perlindungan tersebut diberikan dalam bentuk berbagai lapisan yang biasa disebut dengan istilah pertahanan berlapis. Lapisan tersebut meliputi lapisan OSI seperti aplikasi, transport, fisik, dll.

Terdapat beberapa macam dari host hardening yang biasa disebut dengan elemen. Berikut adalah elemen dari host hardening:

a) Hardening System: Security Policy

Keberadaan dokumen “Kebijakaan Keamanan” atau “Security Policies” merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran

kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis.

Tujuan dasar dari suatu kebijakan (Policy);

- Melindungi pengguna (*user)* dan informasi
- Membuat aturan sebagai arahan untuk pengguna *(user*), sistem administrator, manajemen dan petugas keamanan sistem informasi (**IT security**)
- Menetapkan petugas keamanan untuk pengawasan, penyelidikan atau pemeriksaan
- Membantu mengurangi resiko yang mungkin akan muncul
- Membantu arahan kepatuhan pada peraturan dan undang-undang
- Menetapkan peraturan resmi perusahaan mengenai keamanan

Pihak-pihak yang wajib menggunakan **IT Security Policy**:

- Manajemen – pada semua tingkatan
- Technical staff – sistem administrator dan lainny
- Pengguna (*user*)

b) Hardening System: Kriptografi

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan. Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya *eavesdropping* dan *cheating*.

c) Hardening System: Firewall

Firewall adalah sebuah sistem yang didesain untuk mencegah akses yang tidak sah tidak sah ke atau dari jaringan pribadi. Firewall dapat diimplementasikan dalam perangkat keras dan perangkat lunak,

atau kombinasi keduanya. Firewall sering digunakan untuk mencegah pengguna internet yang terhubung ke jaringan internet. Semua pesan yang masuk dan keluar dari internet harus melewati firewall. Firewall ini bertindak sebagai pengawas setiap pesan dan memblok jika tidak memenuhi kriteria keamanan tertentu.

Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi firewall mengatur, memfilter dan mengontrol lalu lintas data yang diijinkan untuk mengakses jaringan privat yang dilindungi. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain:

- Alamat IP dari komputer sumber.
- Port TCP/UDP sumber dari sumber.
- Alamat IP dari komputer tujuan.
- Port TCP/UDP tujuan data pada komputer tujuan.
- Informasi dari header yang disimpan dalam paket data.

d) Hardening System: IDS (Intrusion Detection System)

Intrusion Detection System (IDS) adalah suatu tindakan untuk mendeteksiadanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau device. Sebuah IDS dapat diimplementasikan melalui software atau aplikasi yangterinstall dalam sebuah device, dan aplikasi tersebut dapat memantau paketjaringan untuk mendeteksi adanya paket-paket ilegal seperti paket yang merusakkebijakan rules keamanan, dan paket yang ditujukan untuk mengambil hak aksessuatu pengguna.

e) Hardening System: Backup

Backup yaitu membuat salinan data atau file-file komputer ke media penyimpanan lain untuk menjamin keamanan atau keselamatan data jika terjadi kerusakan data utama. Backup data dianjurkan secara berkala setiap periode tertentu. Dari beberapa kondisi digunakan sebuah backup yang beriringan dengan master datanya. Sebagai contoh pada sebuah jaringan komputer dibuat server backup yang berjalan beriringan dengan server utamanya. Jika server utama dan server backup diupdate

secara bersamaan, maka jika server utama mati akan digantikan oleh server backup.

Kegiatan backup dalam *hardening system* memiliki beberapa tujuan, yaitu:

- Untuk menjaga keamanan data, terutama data yang memiliki kepenetingan khusus.
- Untuk pengarsipan data.

f) Hardening System: Auditing System

Audit adalah suatu proses yang sistematik untuk mendapatkan dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan mengenai kegiatan dan kejadian dengan tujuan untuk menentukan tingkat kesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan serta menyampaikan hasil-hasilnya kepada pihak yang berkepentingan.

Ada beberapa manfaat untuk melakukan audit sistem jaringan, yaitu:

- Dapat mengidentifikasi kelebihan dan kekurangan suatu jaringan komputer.
- Dapat mengevaluasi sistem keamanan pada jaringan komputer.
- Memahami konsep dasar audit jaringan komputer.
- Memahami dasar-dasar teknik audit jaringan komputer.
- Mengetahui dan memahami fasilitas yang sudah ada, dan untuk lebih di tingkatkan

Prosedur melakukan audit sistem:

1. Memeriksa apakah ada fungsi manajemen Jaringan yang kuat dengan otoritas untuk membuat standar dan prosedur
2. Memeriksa apakah tersedia dokumen mengenai inventarisasi peralatan Jaringan, termasuk dokumen penggantian peralatan
3. Memeriksa apakah tersedia prosedur untuk memantau *network usage* untuk keperluan peningkatan kinerja dan penyelesaian masalah yang timbul

4. Memeriksa apakah ada *control* secara aktif mengenai pelaksanaan standar untuk aplikasi-aplikasi *on-line* yang baru diimplementasikan

g) Hardening System: Digital Forensik dan Penanganan Pasca Insiden.

Digital forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital merupakan hasil ekstrak dari barang bukti elektronik seperti Personal Komputer, mobilephone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Secara umum ada 4 (empat) tahapan yang harus dilakukan dalam implementasi Digital Forensik, yaitu:

1. **Pengumpulan *(Acquisition)***

Mengumpulkan dan mendapatkan bukti-bukti yang mendukung penyelidikan. Tahapan ini merupakan tahapan yang sangat menentukan karena bukti-bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan dan diproses sesuai hukum hingga akhirnya dijebloskan ke tahanan. Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, pen drive, hard disk, atau CD-ROM), PDA, handphone, smart card, sms, e-mail, cookies, log file, dokumen atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Penelusuran bisa dilakukan untuk sekedar mencari *"ada informasi apa disini?"* sampai serinci pada *"apa urutan peristiwa yang menyebabkan terjadinya situasi terkini?"*.

2. **Pemeliharaan *(Preservation)***

Memelihara dan menyiapkan bukti-bukti yang ada. Termasuk pada tahapan ini melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan.

Bahkan menghidupkan komputer dengan tidak hati-hati bisa saja merusak/merubah barang bukti tersebut.

3. **Analisa *(Analysis)***

Melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-*explore* kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan, antara lain: siapa yang telah melakukan, apa yang telah dilakukan

4. **Presentasi *(Presentation)***

Menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara ilmiah di pengadilan. Laporan yang disajikan harus di cross check langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung.

Cara kerja hardening yaitu dengan menggunakan suatu metode untuk mengevaluasi keamanan sistem jaringan dan komputer dengan mensimulasikan kemungkinan serangan yang terjadi dari pihak yang tidak bertanggung jawab atau disebut juga dengan System Penetration. Selain menggunakan System Penetration, hardening juga menggunakan Pacthing dengan melakukan perbaikan terhadap suatu celah keamanan yang telah dideteksi mengalami kerusakan.

1. Enkripsi / Dekripsi

Salah satu metode yang digunakan untuk meningkatkan keamanan adalah dengan menggunakan teknik enkripsi dan dekripsi atau lebih dikenal dengan istilah Kriptografi. Dengan menggunakan teknik ini, data-data yang dikirim (disebut juga plaintext) akan diubah dengan teknik tertentu sehingga akan menghasilkan suatu data yang terlindungi (chippertext) sehingga tidak dapat disadap.

Namun saat ini masih banyak service yang ada di Internet yang belum menggunakan teknik ini atau masih menggunakan plaintext sebagai autentifikasinya. Dengan teknik seperti tersebut, akan sangat mudah untuk melakukan penyadapan (sniffer). Berikut adalah beberapa contoh service yang masih menggunakan plaintext untuk authentication:

a. Akses jarak jauh dengan menggunakan telnet atau rlogin
b. Transfer file dengan menggunakan FTP
c. Akses e-mail dengan menggunakan POP3 dan IMAP4
d. Proses pengiriman e-mail dengan menggunakan SMTP
e. Akses web dengan menggunakan HTTP

2. Firewall

Firewall merupakan suatu sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan luar. Firewall dapat diimplementasikan dalam perangkat keras maupun perangkat lunak atau bahkan keduanya. Secara umum, firewall memisahkan antara public network dengan private network. Firewall bekerja dengan menyaring lalu lintas jaringan yang menggunakan alamat IP, port number, dan protokol.

Berikut adalah beberapa kriteria yang menjadi perhitungan bagi firewall untuk mengijinkan suatu paket data dapat lewat atau tidak:

a. Alamat IP dari sumber
b. Port TCP/UDP sumber
c. Alamat IP dari komputer tujuan
d. Port TCP/UDP tujuan data pada komputer tujuan
e. Informasi dari header yang disimpan dalam paket data.

3. Logs

Logs dapat dikatakan sebagai suatu catatan lengkap yang berisi arus lalu lintas dalam suatu jaringan. Oleh karena itu, diwajibkan bagi seorang system administrator untuk melihat log dari system dari waktu ke waktu. Dengan melihat log, system administrator dapat melihat seluruh aktifitas yang sedang terjadi dan dapat melakukan antisipasi jika terlihat ada beberapa aktifitas mecurigakan yang sedang terjadi.

4. IDS (Instrusion Detection System)

IDS (Intrusion Detection System) merupakan suatu aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi adanya aktivitas yang mencurigakan dalam suatu sistem atau jaringan. Ada dua jenis dari IDS sendiri, yaitu:

a. Network IDS (NIDS)
b. Host IDS (HIDS)

Pada IDS yang berbasikan network atau jaringan, IDS akan meneripa copy paket yang ditujukan pada suatu host untuk kemudian memeriksa paket-paket tersebut. IDS akan memberikan suatu tanda peringatan kepada admin jika ditemukan adanya paket yang berbahaya. IDS hanya akan memeriksa salinan dari paket asli sehingga walaupun ditemukan sebuah paket yang berbahaya, paket tersebut akan tetap mencapai host yang ditujunya.

Berikut adalah beberapa hal yang harus dilakukan admin jika IDS mendeteksi suatu serangan:

a. Memberikan peringat berupa SMS, e-mail atau yang lainnya,
b. Mengkonfigurasi ulang firewall,
c. Menjalankan program respon terhadap serangan,
d. Logging serangan dan event.

5. IPS (Intrusion Prevention System)

IPS (Intrusion Prevention System) ada suatu sistem yang digunakan untuk mendeteksi dan melindungi suatu sistem keamanan dari serangan oleh pihak luar maupun pihak dalam. IPS membuat suatu akses kontrol dengan melihat konten aplikasi daripada IP address. Terdapat dua jenis dari IPS yaitu Network IPS dan Host IPS.

Sebuah IPS bersifat lebih aktif dari IDS dikarenakan IPS bekerja sama dengan firewall sehingga dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem. Sistematika dari IPS sendiri adalah IPS = IDS + Firewall. Jadi, apabila IPS menemukan suatu paket yang berbahaya, maka IPS akan memberitahukan kepada firewall untuk segera menolak paket data tersebut.

6. Honeypot

Honeypot adalah suatu server virtual yang terlihat seperti server asli sehingga dapat menjadi umpan yang berfungsi untuk mengalihkan perhatian. Honeypot tidak menjalankan layanan yang sebagaimana umumnya server lakukan. Honeypot berpura-pura menjalankan layanan yang umumnya server lakukan sehingga akan membuat para penyusup berpikir bahwa dia adalah server sesungguhnya.

Selain penjelasan di atas, honeypot juga berfungsi untuk melihat tehnik yang digunakan oleh para penyusup untuk masuk ke dalam server sehingga dapat mengumpulkan bukti sehingga para pelaku dapat diproses secara hukum.

Honeypot dapat diklasifikasikan berdasarkan tingkat interaksi yang dimilikinya. Semakin tinggi tingkat aktivitas penyerang di dalam sistem, maka semakin tinggi pula tingkat interaksi yang dimiliki honeypot. Honeypot memiliki dua tingkat interaksi, yaitu Low Interaction Honeypot dan High Interaction Honeypot.

7. Configuration

Salah satu peranan yang mengatur keamanan komputer adalah configuration. Configuration akan sangat membantu mengamankan komputer atau jaringan yang ada. Dengan melakukan configuration yang baik dan hati-hati akan membantu dan memberikan sistem keamanan dari serangan yang terjadi. Kebanyakan kasus penyerangan yang terjadi akibat kesalahan konfigurasi adalah kasus penggantian Home Page dari website dari pihak tertentu.

8. Antivirus

Anti virus merupakan suatu software yang dibuat yang bertujuan untuk mengantisipasi dan menghapus virus yang menyerang sistem jaringan komputer. Anti virus dalam keamanan jaringan komputer memiliki fitur security network yang bertugas untuk melindungi dan menjaga keamanan komputer ketika terhubung dengan jaringan lokal (LAN) maupun jaringan Internet.

Anti virus ini bekerja dengan mengidentifikasi IP address dan domain yang mencoba terhubung dengan komputer. Kemudian anti virus akan memverifikasi IP address dan domain tersebut apakah aman atau tidak. Jika aman, maka akan terhubung namun jika tidak maka fitur security network akan menyala dan akan langsung memutuskan koneksi.

D. Aktivitas Pembelajaran

1. SSH

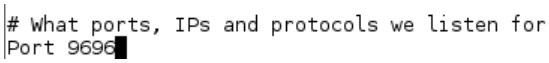
   Jika diperlukan akses ke komputer lain dalam jaringan, jangan gunakan telnet karena telnet mengirimkan semua informasi semua informasi termasuk data penting seperti password dalam bentuk teks biasa. Untuk itu SSH dapat digunakan karena ia memiliki fungsi yang sama dengan telnet. Bedanya,

pada ssh setiap data yang akan dikirim diacak terlebih dahulu sehingga lebih aman.

Mengatur koneksi ssh(secure shell) melalui file sshd_config pada direktori /etc/ssh

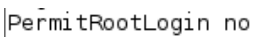
Gambar 3.1 Mengatur Koneksi SSH

- Mengubah port default ssh dari port 22 ke port lain



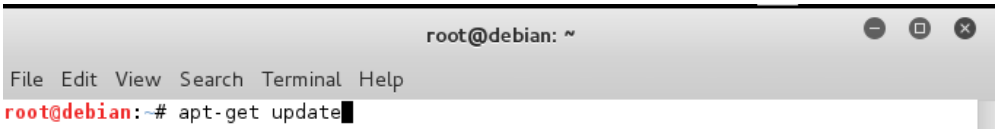
Gambar 3.2 Mengubah Port Default SSH

- Menolak login root pada ssh



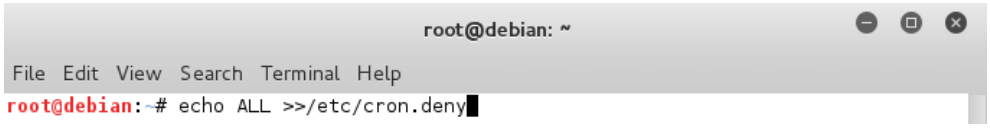
Gambar 3.3 Menolah Login Root Pada SSH

2. Selalu menjaga sistem selalu update



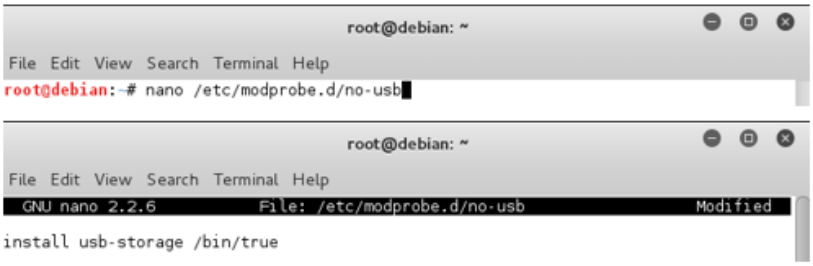
Gambar 3.4 Sistem Update

3. Memblokir semua user yang tidak berkepentingan untuk mengakses server tersebut



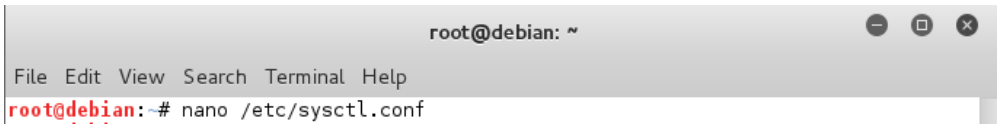
Gambar 3.5 Memblokir User

4. Mencegah agar USB drive terbaca



Gambar 3.6 Mencegah USB Drive Terbaca

5. Mengabaikan ping dari luar dengan cara edit file sysctl.conf pada direktori /etc



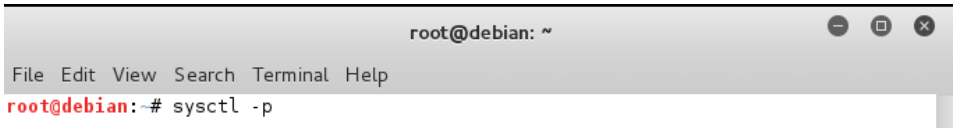
Gambar 3.7 Mengabaikan Ping

- Tambah baris perintah di bawah ini

```
net.ipv4.icmp_echo_ignore_all = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

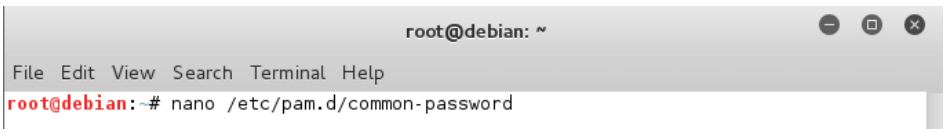
Gambar 3.8 Perintah Mengabaikan Ping

- Load pengaturan baru yang telah disimpan



Gambar 3.9 Load Pengaturan Baru Disimpan

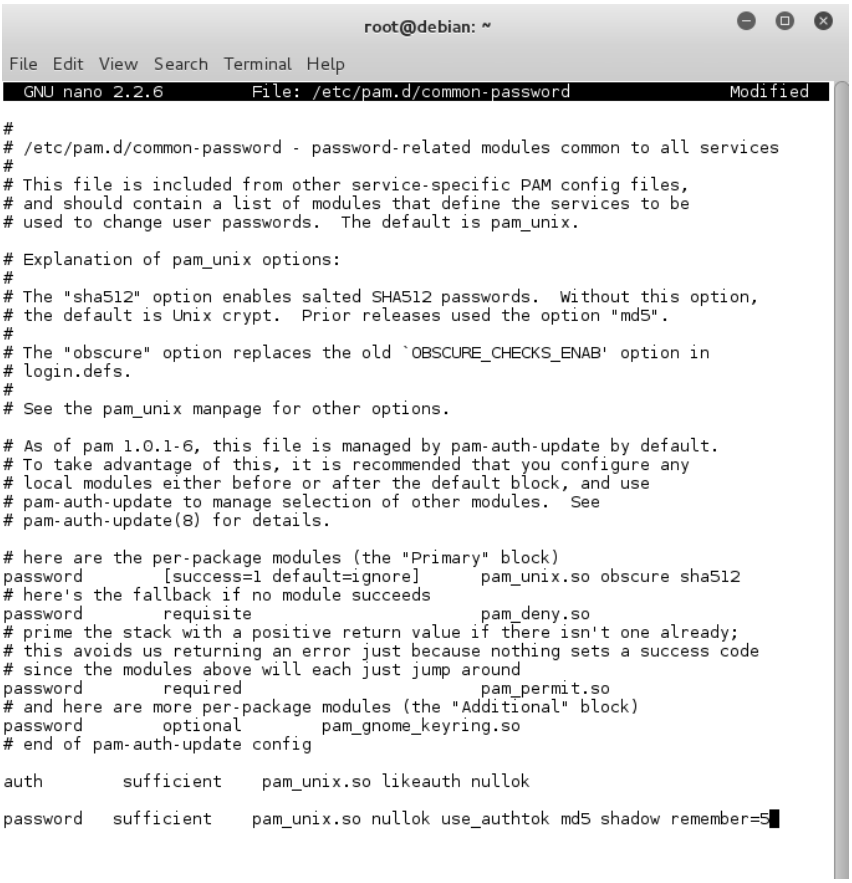
6. Mencegah user untuk menggunakan password lama
   - Buka file common-password pada direktori /etc/pam.d



Gambar 3.10 Membuka File Common-password

   - Tambahkan perintah

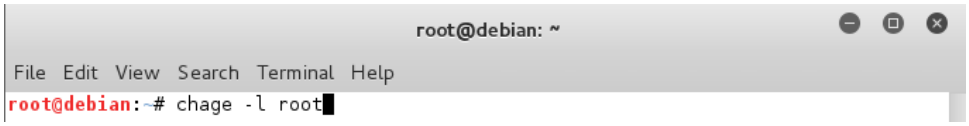
auth sufficient pam_unix.so likeauth nullok
password sufficient pam_unix.so nullok use_authtok md5 shadow remember=5



Gambar 3.11 Mencegah Menggunakan Password Lama

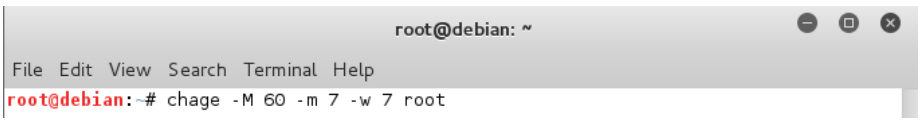
7. Meminta user untuk mengubah password secara berkala

- Perintah untuk mengetahui infornasi tanggal kadaluarsa suatu kata sandi



Gambar 3.12 Mengetahui Informasi Tanggal Kadaluarsa

- Perintah untuk mengatur waktu validasi suatu kata sandi



Gambar 3.13 Mengatur Waktu Validasi

penjelasan parameter:

-M mengatur batas maksimal masa berlaku kata sandi

-m mengatur batas minimal masa berlaku kata sandi

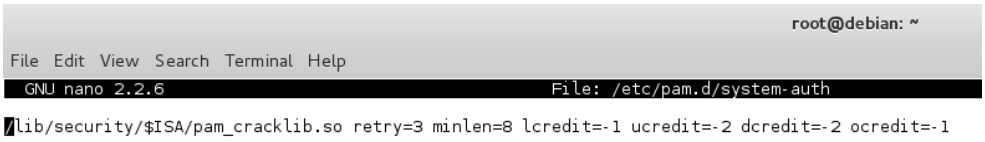
-w mengatur batas toleransi untuk mengubah kata sandi lama dengan yang baru

8. Meminta user untuk menggunakan kata sandi yang cukup aman dengan kombinasi yang rumit
   - Buat file system-auth pada direktori /etc/pam.d

Gambar 3.14 Membuat File System-auth

   - Tambahkan perintah

/lib/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=-1 ucredit=-2 dcredit=-2 ocredit=-1



Gambar 3.15 Perintah User Menggunakan Kata Sandi Yang Aman

Penjelasan parameter:

Retry: maksimal percobaan

Minlen: minimal panjang karakter

Lcredit: jumlah minimal huruf kecil

Ucredit: jumlah minimal huruf kapital

Dcredit: jumlah minimal angka

Ocredit: jumlah minimal karakter lain

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiatan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah di bawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.

2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Untuk melihat tanggal kadaluarsa password digunakan perintah apa?

……
……
……
……
……

2. Bagaimana langkah untuk menguatkan keamanan SSH?

……
……
……
……
……

F. Rangkuman

Host Hardening adalah prosedur yang meminimalkan ancaman yang datang dengan mengatur konfigurasi dan menonaktifkan aplikasi dan layanan yang tidak diperlukan. Instalasi firewall, instalasi antivirus, menghapus cookie, membuat password , menghapus program yang tidak diperlukan itu semua termasuk dalam Host Hardening. Host Hardening menyediakan berbagai perlindungan dalam sistem komputer. Perlindungan tersebut diberikan dalam bentuk berbagai lapisan

yang biasa disebut dengan istilah pertahanan berlapis. Lapisan tersebut meliputi lapisan OSI seperti aplikasi, transport, fisik, dll.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang konsep hardening host dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami perintah untuk mengamankan akses pada layanan SSH serta berapa prosen pencapaian kompetensinya?
3. Apakah saudara sudah memahami perintah untuk meminta user memakai password yang aman dan berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. Chage –l root adlah perintah untuk melihat kadaluarsa dari password.
2. Mengatur koneksi ssh(secure shell) melalui file sshd_config pada direktori /etc/ssh

   #nano /etc/ssh/sshd_config

   kemudian mengubah port default ssh dari port 22 ke port lain dan menolak login root pada ssh

4

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 4: Membangun Server DMZ

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat membangun server DMZ.

B. Indikator Pencapaian Kompetensi

- Memahami konsep DMZ pada jaringan komputer.
- Mampu membangun server DMZ menggunakan Linux.

C. Uraian Materi

DMZ adalah singkatan untuk Demilitarized Zone istilah ini berasal dari bahasa militer, yang berarti daerah penyangga antara dua musuh. DMZ pada jaringan komputer dipakai ketika suatu sub network yang terpisah dari sub network internall untuk keperluan keamanan. DMZ berisi server yang dapat diakses oleh internet, seperti Web (HTTP) server, server FTP, SMTP (e-mail) server dan DNS server.

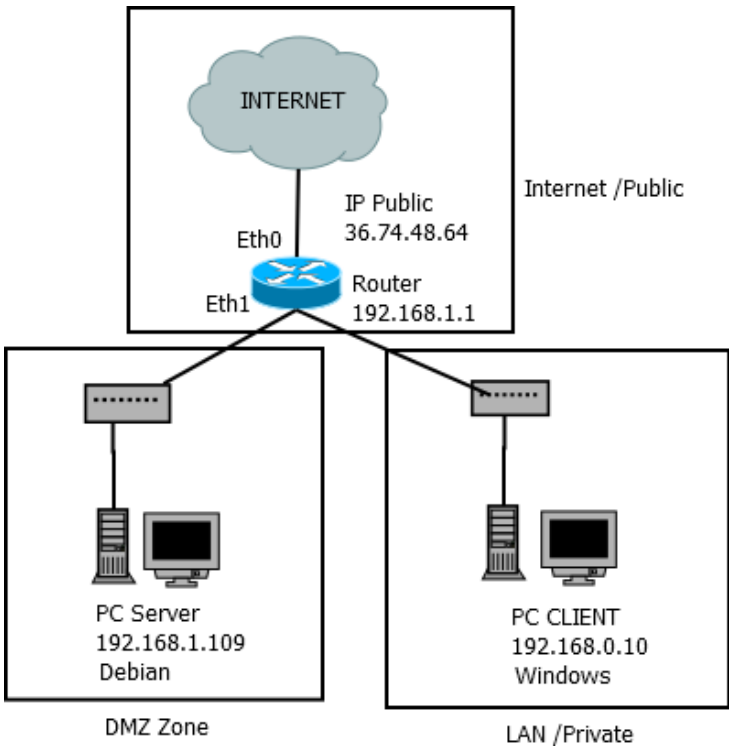
Tujuan dari DMZ adalah untuk menjaga server publik terpisah dari LAN supaya aman jika pada suatu saat server public diserang dari luar. Hal ini dikarenakan tidak ada firewall yang menjamin keamanan jaringan 100 %aman. Dalam menjaga LAN, firewall menolak traffic dari DMZ untuk ditujukan ke LAN, sama halnya dari WAN ke LAN. Pada saat Web Server diserang, LAN masih diproteksi dan penyusup harus menembus firewall untuk bisa masuk ke LAN.

Konsep dari DMZ adalah misalnya jika seorang pengguna server FTP pada jaringan publik, maka cracker dapat melakukan cracking pada server FTP dengan memanfaatkan layanan Network Interconnection System (NIS), dan Network File System (NFS). Sehingga cracker tersebut dapat mengakses seluruh sumber daya jaringan, atau jika tidak, akses jaringan dapat dilakukan dengan sedikit upaya, yaitu dengan menangkap paket yang beredar di jaringan, atau dengan metoda yang lain. Namun dengan menggunakan lokasi server FTP yang berbeda, maka cracker hanya dapat mengakses DMZ tanpa mempengaruhi

sumber daya jaringan yang lain. Selain itu dengan melakukan pemotongan jalur komunikasi pada jaringan internal, trojan dan sejenisnya tidak dapat lagi memasuki jaringan.

Secara umum DMZ dibangun berdasarkan tiga buah konsep, yaitu: NAT (Network Address Translation), PAT (Port Addressable Translation), dan Access List. NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari “real address” ke alamat internal. Misal : jika kita memiliki IP publik 202.9.12.2, kita dapat membentuk suatu NAT langsung secara otomatis pada data-data yang datang ke jaringan privat yaitu 192.168.1.4. Kemudian PAT akan mengarahkan data yang masuk melalui port, sekumpulan port dan protokol, serta alamat IP pada port atau sekumpulan port. Sehingga dapat dilakukan kendali ketat pada setiap data yang mengalir dari dan ke jaringan. Sedangkan access list berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan. Misalnya, Administrator dapat menolak atau memperbolehkan semua paket ICMP yang datang ke seluruh alamat IP kecuali untuk sebuah paket ICMP yang tidak diinginkan.

D. Aktivitas Pembelajaran



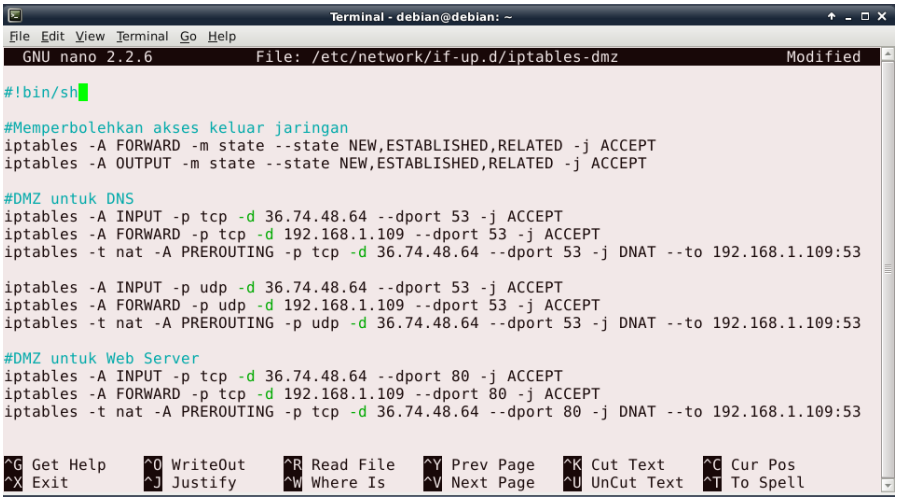
Gambar 4.1 Topologi Jaringan DMZ

Gambar diatas adalah topologi jaringan yang akan dibuat untuk praktikum ini. Router Debian akan dikonfigurasi supaya beberapa layanan dari server Debian dapat diakses menggunakan IP Publik.

1. Buat file iptables-dmz pada direktori /etc/network/if-up.d/iptables-dmz

Gambar 4.2 Membuat File Iptables-dmz

2. Ketikkan perintah berikut ini pada file iptables-dmz. Untuk menambah layanan cukup tambahkan perintah iptables yang sama dengan port layanan tersebut.

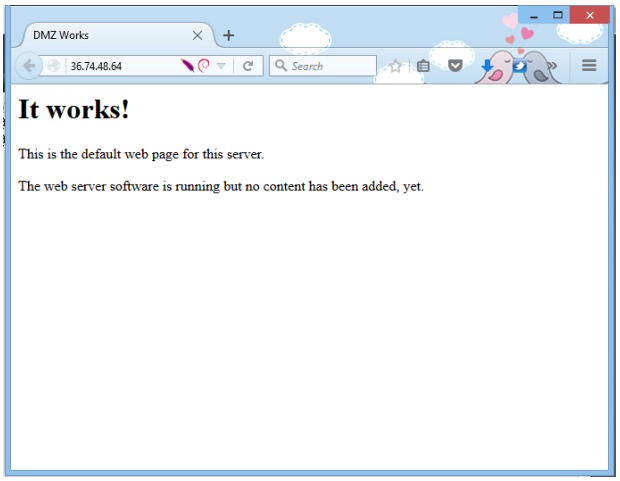


Gambar 4.3 Menambah Layanan Iptables

3. Buat file yang telah dibuat menjadi executable.

Gambar 4.4 Membuat File Menjadi Executable

4. Restart komputer.
5. Cek DMZ pada komputer client dengan menggunakan IP Publik.



Gambar 4.5 Mengecek DMZ Pada Komputer Client

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiaan yang dilakukan adalah membentuk kelompok diskusi. Setiap

kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengaumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Apakah kegunaan NAT pada DMZ?

……
……
……
……
……

2. Berikan contoh perintah untuk IP Tables jika layanannya adalah FTP!

……
……
……
……
……

3. Digunakan untuk apakah DMZ pada keamanan jaringan?

……
……
……
……
……

F. Rangkuman

DMZ adalah singkatan untuk Demilitarized Zone istilah ini berasal dari bahasa militer, yang berarti daerah penyangga antara dua musuh. DMZ pada jaringan komputer dipakai ketika suatu sub network yang terpisah dari sub network internall untuk keperluan keamanan. Tujuan dari DMZ adalah untuk menjaga server publik terpisah dari LAN supaya aman jika pada suatu saat server public diserang dari luar. Hal ini dikarenakan tidak ada firewall yang menjamin keamanan jaringan 100 % aman.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang konsep DMZ dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami perintah untuk membangun DMZ serta berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari “real address” ke alamat internal. Misal : jika kita memiliki IP publik 202.9.12.2, kita dapat membentuk suatu NAT langsung secara otomatis pada data-data yang datang ke jaringan privat yaitu 192.168.1.4.
2. iptables -A INPUT -p tcp -d 36.74.48.64 --dport 21 -j ACCEPT
   iptables -A FORWARD -p tcp -d 192.168.1.109 --dport 21 -j ACCEPT
   iptables -t nat -A PREROUTING -p tcp -d 36.74.48.64 --dport 21 -j DNAT --to 192.168.1.109:21
3. DMZ adalah mekanisme dalam jaringan komputer untuk memisahkan server dari LAN supaya jika ada cracker masuk dalam server, cracker tersebut tidak akan dapat masuk ke dalam jaringan lokal.

5

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 5: Menguji Keamanan Jaringan, Host Dan Server

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menguji keamanan jaringan pada server yang telah dibangun.

B. Indikator Pencapaian Kompetensi

- Memahami konsep pengujian keamanan jaringan, host dan server.
- Mampu melakukan pengujian atau penetration testing pada server.
- Mampu menggunakan tool DOS untuk penetration testing.

C. Uraian Materi

Sistem keamanan jaringan yang dibangun oleh seseorang yang bekerja pada IT Security tidak dapat menemukan kelemahan dalam sistemnya jika ia tidak menguji sistem tersebut. Pengujian ini digunakan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem dan mengetahui dampak yang terjadi dari hasil eksploitasi yang dilakukan oleh penyerang.

Pengujian tersebut lebih dikenal dengan istilah penetration testing. Penetration Testing adalah metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Aktifitas ini adalah salah satu komponen penting dari Security Audit. Konsep untuk melakukan kegiatan penetration testing dapat dilakukan dengan beberapa langkah-langkah berikut :

1. Reconnaissance (Pengumpulan Informasi)

Reconnaissance adalah langkah pertama dari Penetration Testing yang dimulai dengan menentukan target pengujian berdasarkan scope pengerjaan. Setelah target ditentukan, research dilakukan untuk mengumpulkan informasi pada target

seperti: ports apa yang digunakan untuk komunikasi,dimana lokasinya, tipe services yang diberikan kepada clientnnya (web,database, dll). Data-data ini dibutuhkan untuk langkah selanjutnya yang akan dilakukan untuk penetration testing. Deliverable dari langkah reconnaissance harus mencakup list dari semua asset yang dimiliki target,aplikasi yang terkait dengan asset, services yang digunakan, dan pemilik aset.

Information Gathering difokuskan untuk dapat mengumpulkan informasi secukupnya mengenai sistem target. proses pengumpulan informasisendiri berbagi menjadi dua, yaitu passive information gathering dan active information gathering. Pengumpulan informasi menggunakan teknik passive information gathering dapat menggunakan service WHOIS, DNS, Search Engine (Google), Website Analisis Security(netcraft) dan tools seperti Maltego, metagofil dan tracerout. Sedangkan untuk prosedur active information gathering biasanya hacker menggunakan teknik Port Scanning, Banner Grab, Fingerprinting, Network Mapping dan ARP Poisoning

2. Target Evaluasi

Tujuan dari langkah Target Evaluation adalah melakukan evaluasi data yang telah didapatkan dan mengklasifikasikannya menjadi beberapa bagian, yaitu:

- Kemungkinan-kemungkinan kelemahan target
- Identifikasi dan penentuan prioritas kerentanan pada sistem target
- Pemetaan kelemahan sistem terhadap pemilik asset
- Menemukan dokumen-dokumen

3. Exploitation

Pada langkah ini eksploitasi mulai dilakukan pada target dengan cara mencoba berbagai serangan yang sudah disesuaikan dengan data-data yang sebelumnya diperoleh. Tujuan dari kegiatan eksploitasi adalah sebagai berikut :

- Melakukan eksploitasi terhadap vulnerabilities (kerentanan)
- Memperoleh foothold (pijakan) pada sistem target
- Pengambilan data (service atau user) pada system
- Social engineering

- Serangan pada sistem atau aplikasi lain yang ada pada target menemukan dokumen-dokumen

4. Privilage Excalation (Pengambilan Akses)

Privilege Escalation mencakup kegiatan identifikasi dan password cracking terhadap akun user, dan ruang pada sistem yang lainnya. Sebuah contoh adalah mendapatkan akses user, identifikasi shadow file yang berisi user login administrator, memperoleh password administrator melalui password cracking, dan memasuki sistem aplikasi internal dengan hak akses administrator.

Tujuan dari kegiatan privelege escalation adalah sebagai berikut :

- Memperoleh level akses yang tinggi ke sistem dan network target
- Memperoleh informasi akun user lain pada system
- Memperoleh akses sistem lain dengan hak yang tinggi

5. Maintaining a Foothold (Pengamanan Akses)

Pada langkah ini hal penting yang dilakukan adalah menghapus semua jejak kegiatan penetration test yang telah dilakukan. Penghapusan bukti mencakup beberapa hal seperti menghapus user logs, menggunakan saluran yang telah dimasking, dan menghapus pesan error yang mungkin di sebabkan oleh kegiatan penetration testing.

Tujuan dari kegiatan maintaining foothold adalah sebagai berikut:

- Menetapkan beberapa metode akses terhadap target
- Menghilangkan bukti adanya akses yang tidak diizinkan
- Memperbaiki sistem dari dampak eksploitasi
- Mengamankan akses pada target

Beberapa teknik yang dapat digunakan untuk pentest adalah

1. DOS

   Jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah

pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

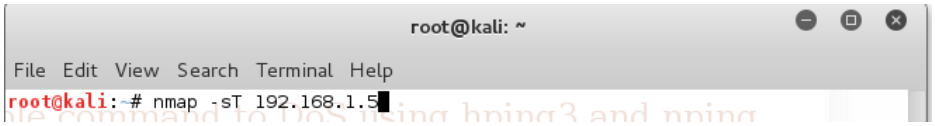
Ciri-ciri Serangan DOS awalnya terjadi pada jaringan dimana hacker atau cracker mencoba mengeksploitasi kelemahan protocol TCP (Transmision Control Protocol) inilah yang disebut dengan SYN Flooding Attack, kemudian seiring perjalanan diciptakan juga serangan-serangan untuk eksploitas kelemahan Sistem Operasi, layanan jaringan atau Aplikasi sistem bahkan tools yang digunakan pun semakin banyak bahkan bisa didapatkan secara gratis. Contohnya adalah Hping. Hping adalah aplikasi yang hampir sama kegunaanya dengan command ping, tetapi hping3 dapat juga mengirimkan paket TCP, UDP, ICMP dan RAW IP protocols

2. Sql Injection

SQL injection adalah kegiatan menyisipkan perintah SQL kepada suatu statement SQL yang ada pada aplikasi yang sedang berjalan. SQL injection tersebut dapat terjadi dikarenakan keamanan pada level aplikasi (dalam hal ini aplikasi web) masih kurang sempurna. Kurang sempurnanya adalah pada cara aplikasi meng-handle inputan yang boleh di proses ke dalam database. Misalnya pada suatu web yang terdapat fasilitas login, terdapat dua buah inputan pada umumnya, yaitu username dan password. Jika karakter yang masuk melalui dua buah inputan tersebut tidak difilter (disaring) dengan baik maka bisa menimbulkan efek SQL injection, ini dikarenakan biasanya inputan tersebut secara sistem akan menjadi bagian dari kriteria dari suatu perintah SQL di dalam aplikasi web-nya.

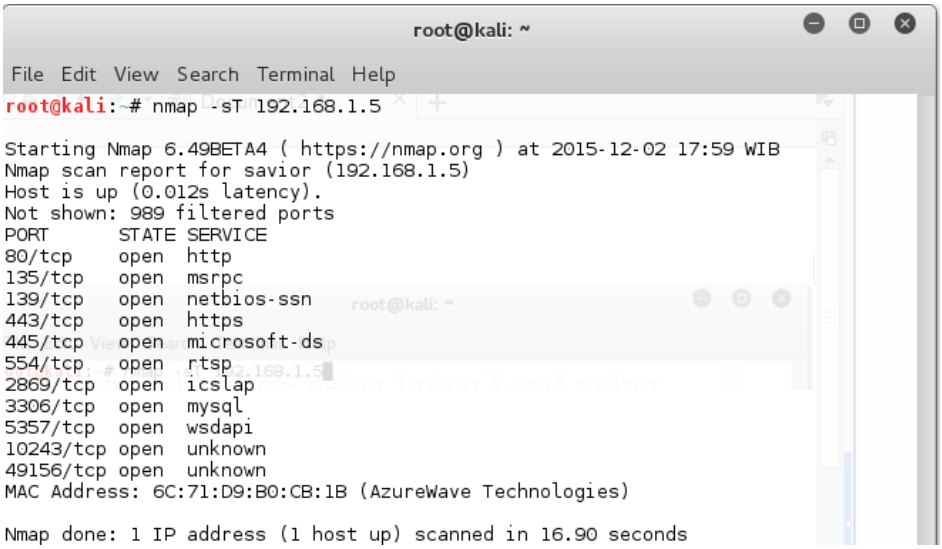
D. Aktivitas Pembelajaran

1. Gunakan perintah nmap -sT [alamat_ip] untuk scanning port yang terbuka dari target yg akan diserang



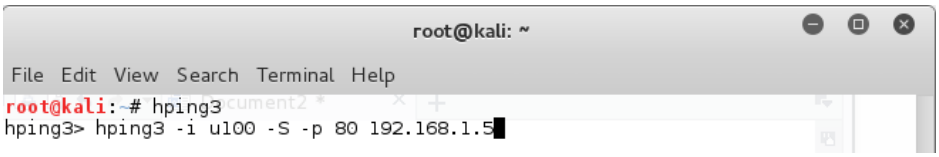
Gambar 5.1 Perintah Nmap sT

2. Setelah menunggu proses selesai, maka akan tampil port target yang sedang terbuka



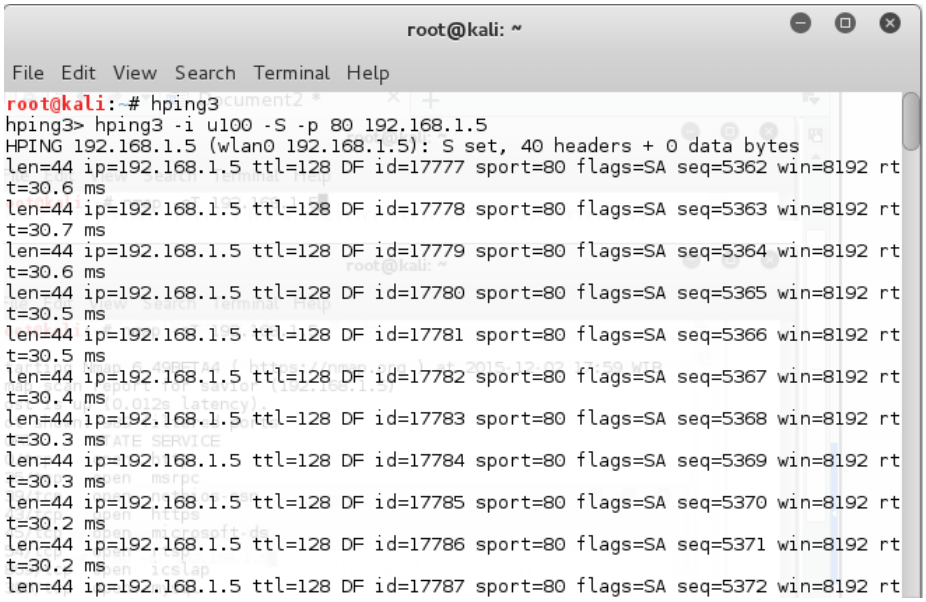
Gambar 5.2 Tampilan Port Target

3. Berdasarkan informasi yang didapat dari nmap, gunakan perintah hping3 -i u100 -S -p [nomor_port] [alamat_ip]



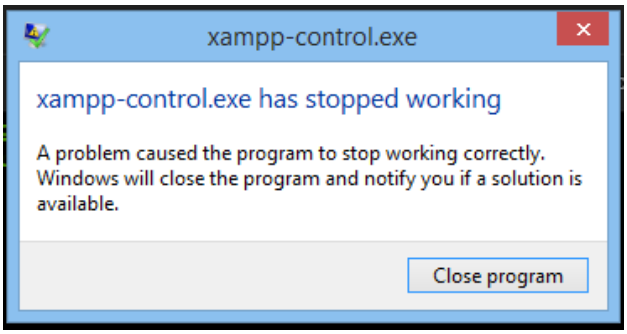
Gambar 5.3 Perintah Hping

4. Jika tampilan terminal menampilkan seperti gambar di bawah ini, maka proses ddos telah berjalan dan menyerang target



Gambar 5.4 Tampilan Terminal Setelah Proses Ddos Berjalan

5. Jika server tidak memiliki pengamanan, maka akan terserang seperti pada gambar berikut.



Gambar 5.5 Hasil Serangan

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiaan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.

3. Mengaumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Untuk scanning port yang terbuka pada target digunakan perintah apa?

……
……
……
……
……

2. Bagaimana cara menggunakan perintah hping untuk menyerang target dengan IP 192.168.1.2 dengan port SSH?

……
……
……
……
……

F. Rangkuman

Sistem keamanan jaringan yang dibangun oleh seseorang yang bekerja pada IT Security tidak dapat menemukan kelemahan dalam sistemnya jika ia tidak menguji sistem tersebut. Pengujian ini digunakan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem dan mengetahui dampak yang terjadi dari hasil eksploitasi yang dilakukan oleh penyerang.

Pengujian tersebut lebih dikenal dengan istilah penetration testing. Penetration Testing adalah metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Aktifitas ini adalah salah satu komponen penting dari Security Audit.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang perintah dasar hping dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami konsep dasar untuk penetration testing serta berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. Nmap –sT [IP-Target].
2. hping3 -i u100 -S -p 23 192.168.1.2

6

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 6: Menganalisis Fungsi Dan Cara Kerja Server Autentikasi

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menganalisis fungsi dan cara kerja server autentikasi.

B. Indikator Pencapaian Kompetensi

- Memahami konsep menganalisis fungsi dan cara kerja server autentikasi.

C. Uraian Materi

1. Authentication

Authentication merupakan suatu proses yang bertujuan untuk proses validasi user yang akan masuk ke dalam sistem. Authentication melakukan pengenalan terhadap peralatan, sistem operasi, aplikasi dan identifikasi user saat ingin memasuki jaringan suatu sistem. Proses authentication dimulai dari user harus memasuki username dan password untuk proses identifikasi. Melakukan Authentication berarti mengecek suatu objek atau user terhadap konfirmasi kebenarannya dengan mengecek ke daftar user apakah user tersebut berhak untuk memasuki suatu sistem atau tidak.

Dengan kata lain, Autentikasi adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

Berikut adalah tahapan authentication:

a) Mengetahui lokasi dari Data Link Layer dan Network Layer,

b) Mengenal Transport Layer yang merupakan pengenalan sistem operasi yang terhubung dengan jaringan,
c) Mengetahui proses yang sedang terjadi di dalam suatu jaringan (Session Layer dan Presentation Layer),
d) Mengenali user dan application yang digunakan (Application Layer).

Selain itu authentification juga merupakan salah satu dari banyak metode yang digunakan untuk menyediakan bukti bahwa dokumen tertentu yang diterima secara elektronik benar-benar datang dari orang yang bersangkutan dan tak berubah caranya adalah dengan mengirimkan suatu kode tertentu melaui e-mail dan kemudian pemilik e-mail mereplay email tersebut atau mengetikan kode yang telah dikirimkan.

Dalam server, authentication server berfungsi untuk mengenali user yang berintegrasi ke jaringan dan memuat semua informasi dari user tersebut, dalam praktek biasanya authentification server mempunyai backupp yang berfungsi untuk menjaga jika server itu ada masalah sehingga jaringan dan pelayanan tidak terganggu. Dalam aplikasi Web, dibutuhkan mekanisme yang dapat melindungi data dari pengguna yang tidak berhak mengaksesnya, misalnya sebuah situs Web yang berisikan foto-foto keluarga dan hanya dapat diakses sesama anggota keluarga. Mekanisme ini dapat diimplementasikan dalam bentuk sebuah proses login yang biasanya terdiri dari tiga buah tahapan yaitu : identifikasi, otentikasi dan otorisasi.

Metode-Metode Autentikasi

Autentikasi bertujuan untuk membuktika siapa administrator sebenarnya, apakah administrator benar-benar orang yang administrator klaim sebagai dia (who you claim to be). Ada banyak cara untuk membuktikan siapa administrator.
Metode autentikasi bisa dilihat dalam 4 kategori metode:
Metode autentikasi bisa dilihat dalam 4 kategori metode:

a. *Something you know*

Ini adalah metode autentikasi yang paling umum. Cara ini mengadministratorlkan kerahasiaan informasi, contohnya adalah password

dan PIN. Cara ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali administrator seorang.

b. *Something you have*

Cara ini biasanya merupakan faktor tambahan untuk membuat autentikasi menjadi lebih aman. Cara ini mengadministratorlkan barang yang sifatnya unik, contohnya adalah kartu magnetic/smartcard, hardware token, USB token dan sebagainya. Cara ini berasumsi bahwa tidak ada seorangpun yang memiliki barang tersebut kecuali administrator seorang.

c. *Something you are*

Ini adalah metode yang paling jarang dipakai karena faktor teknologi dan manusia juga. Cara ini menghadministratorlkan keunikan bagian-bagian tubuh administrator yang tidak mungkin ada pada orang lain seperti sidik jari, suara atau sidik retina. Cara ini berasumsi bahwa bagian tubuh administrator seperti sidik jari dan sidik retina, tidak mungkin sama dengan orang lain.

d. *Something you do*

Melibatkan bahwa setiap user dalam melakukan sesuatu dengan cara yang berbeda. Contoh: Penggunaan analisis suara (voice recognation), dan analisis tulisan tangan.

Ada beberapa metode untuk melakukan autentikasi, salah satunya dan yang paling umum adalah menggunakan password. Tetapi jika user menggunakan password yang sama (password statis) beberapa kali untuk masuk ke dalam suatu sistem, password tersebut akan menjadi rentan terhadap sniffer jaringan. Salah satu bentuk serangan ke sistem komputer jaringan adalah seseorang mencoba masuk ke dalam suatu koneksi jaringan untuk mendapatkan informasi autentikasi, seperti ID login dan password yang berbeda setiap kali user akan masuk ke sistem. Sistem autentikasi One Time Password (OTP) dibuat untuk mengatasi serangan seperti diatas.

Authentication Pada Cisco

Cisco merupakan suatu lembaga network yang terbesar dan tersebar di seluruh dunia. Untuk melakukan authentication pada cisco, cisco telah menyediakan beberapa cara yaitu:

1. PPP (Point-to-Point Protocol)

PPP (Point-to-Point Protocol) merupakan sebuah protokol dari Cisco yang berjalan pada data link layer pada koneksi jaringan point-to-point. PPP mendukung dua jenis authentication, yaitu jenis clear text PAP (Password Authentication Protocol) dan jenis enkripsi CHAP (Chalange Handshake Authentication Protocol). PPP dapat digunakan untuk komunikasi synchronous dan asynchronous dan dapat menerapkan authentication dengan cara melalui PAP dan CHAP. PPP bekerje sama halnya dengan login secara umum, yaitu user memasukkan username dan password yang kemudian akan dibandingkan dengan data yang ada pada database rahasia. Sedangkan pada CHAP, password akan dienkripsi menggunakan metode hash dan MD5.

2. RADIUS

RADIUS (Remote Authentication Dial-In User Service) merupakan suatu metode atau network protocol yang berfungsi untuk keamanan komputer yang digunakan untuk mengatur akses seperti authentication, otorisasi dan pendaftaran akun user secara terpusat untuk mengakses jaringan sehingga lebih terkontrol. RADIUS juga merupakan protocol yang membawa paket data yang terdapat encapsulation di dalamnya. RADIUS ini diterapkan pada sebuah jaringan yang menggunakan konsep client-server. RADIUS server menyediakan keamanan dengan melakukan authentication dan otorisasi terhadap koneksi yang dilakukan oleh user.

Berikut adalah proses dari RADIUS:

a. RADIUS akan mengidentifikasi user ketika ingin terhubung denganjaringan
b. RADIUS mengecek username dan password user di dalam database RADIUS server
c. Setelah itu, RADIUS akan mengecek hak dari user untuk mengakses layanan dalam jaringan komputer
d. Setelah user layak untuk masuk ke dalam jaringan, maka RADIUS akan mengecek segala aktifitas dari user mulai dari durasi waktu dan kegiatan transfer data yang dilakukan oleh user
e. RADIUS melakukan pelaporan bisa dalam satuan waktu (jam, menit, detik, dll) atau dapat mengirim laporan dalam bentuk transfer data (Byte, Mbyte atau Kbyte).

Berikut adalah beberapa contoh RADIUS server yang tersedia secara gratis (free), yaitu Citron RADIUS server, ICRADIUS, XtRADIUS, OpenRADIUS, YARDRRADIUS dan JRadius.

3. TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) merupakan suatu program yang paling sering menggunakan Cisco yang berfungsi untuk meng-authentication multiuser (radius server) dalam mengakses suatu sistem. TACACS+ merupakan suatu protocol buatan Cisco yang berguna untuk memberikan akses kontrol yang lebih terpusat. TACACS+ ini bekerja pada jaringan yang mendukung AAA server.

Kelebihan dari TACACS sendiri adalah:

a. Menyediaan layanan authentication, authorization, dan accounting
b. Menyediakan fitur logging untuk setiap user setiap saat ketika user tersebut terhubung ke jaringan.

Authentication Pada Linux

Sistem Autentikasi di Squid

Squid mendukung 4 skema autentikasi, yaitu:

1. Basic
2. Digest
3. NTLM
4. Negotiate

2. Basic Authentication

Ini adalah skema autentikasi yang didukung oleh semua peramban (browser) utama. Dan lebih dari itu, bisa berfungsi dengan baik di semua platform OS. Jadi kalau ingin menggunakan skema autentikasi yang yakin berfungsi dengan baik di semua browser, pakailah skema autentikasi basic. Skema autentikasi basic ini memiliki satu kelemahan utama, yaitu proses pengiriman data user dan password dikirim dalam format plain text. Jadi sangat rentan terhadap proses snip atau penyadapan saat proses autentikasi berlangsung.

Skema ini tidak disarankan ketika layanan yang diberikan akan diakses melalui jaringan internet. Tapi masih bisa ditolerir jika layanan itu dibuat untuk kalangan terbatas, misalnya LAN kantor. Dan karena squid pada umumnya digunakan di jaringan terbatas, skema autentikasi ini masih bisa digunakan.

Helper atau program bantu untuk autentikasi ke backend

Squid menyediakan beberapa program bantu untuk skema autentikasi basic, antara lain:

1. LDAP: Autentikasi ke LDAP.
2. NCSA: Menggunakan format penulisan username dan password format NCSA.
3. MSNT: Autentikasi ke domain Windows NT.
4. PAM: Menggunakan skema autentikasi PAM yang umum digunakan di sistem operasi Unix/Linux.
5. SMB: Menggunakan server SMB seperti Windows NT atau Samba.
6. getpwam: Menggunakan cara kuno, berkas password di Unix/Linux.
7. SASL: Mengggunakan pustaka SASL.
8. mswin_sspi: Windows native authenticator.
9. YP: Menggunakan database NIS.

3. Negotiate Authentication

Protokol negotiate diperkenalkan oleh Microsoft, sering dikenal juga sebagai SPNEGO. Skema autentikasi ini memperbarui skema Single Sign On yang sebelumnya menggunakan autentikasi NTLM. Skema ini bisa dianggap sebagai wrapper (atau alat bantu) untuk menggunakan salah satu dari autentikasi ke Kerberos atau NTLM. Kelebihan skema ini, jauh lebih aman bila dibandingkan dengan skema autentikasi NTLM.

4. Digest Authentication

Skema autentikasi digest diperkenalkan untuk mengatasi kelemahan yang ada di skema autentikasi basic. Skema ini lebih aman, karena pada saat autentikasi, data username dan password tidak dikirim dalam format plain text. Secara umum, kelebihan skema autentikasi digest dibandingkan skema autentikasi

basic, yaitu lebih aman. Namun, Internet Explorer 5 & 6 adalah salah satu browser yang tidak mendukung skema autentikasi digest.

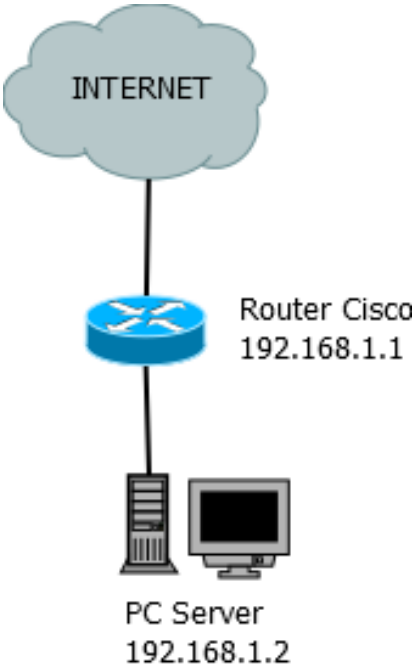
5. NLTM Authentication

Ini adalah skema autentikasi yang diperkenalkan oleh Microsoft. Dengan menggunakan skema autentikasi NTLM, semua user yang sudah login ke domain, ketika mengakses squid tidak akan diminta lagi username dan password. Ini yang kita kenal sebagai proses Single Sign On. Jika sudah sukses autentikasi di satu layanan, ketika ingin menggunakan layanan lain tidak perlu memasukkan login dan password lagi, proses autentikasi berlangsung secara transparan.

Sayangnya, seperti yang mungkin Administrator sudah bisa tebak, ini hanya berfungsi dengan baik di sistem operasi Windows. Dan tidak semua browser mendukung skema autentikasi NTLM. Internet Explorer dan Firefox adalah salah satu browser yang mendukung skema autentikasi NTLM. Chrome, Safari dan Opera adalah contoh browser yang belum mendukung skema autentikasi NTLM.

D. Aktivitas Pembelajaran

Pada praktikum ini, akan digunakan server Debian yang akan diinstall dan dikonfigurasi TACACS, kemudian Router Cisco untuk uji coba. Topologinya seperti pada berikut: Topologinya seperti pada gambar berikut:



Gambar 6.1 Topologi Jaringan

1. Install software dependensi dari Tac-plus. Paket yang harus diintall terlebih dahulu adalah gcc bison, flex, dan libwrap0-dev

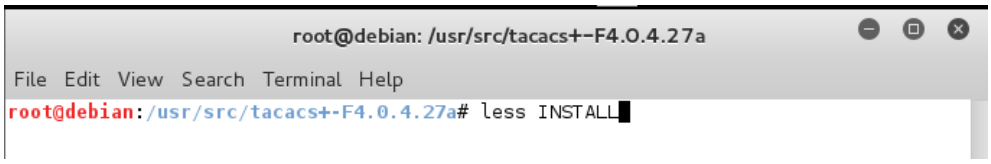
Gambar 6.2 Install Software Dependensi

2. Install Tac-plus

   Download Tac-plus dengan perintah

   #wget ftp://ftp.shrubbery.net/pub/tac_plus/tacacs+-F4.0.4.26.tar.gz

3. Masuk ke dalam file tacacs kemudian install tacacs.

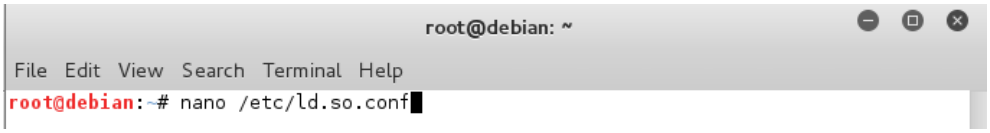


Gambar 6.3 Install Tacacs

4. Masukkan perintah berikut ini untuk instalasi tacacs

Gambar 6.4 Perintah Instalasi Tacacs

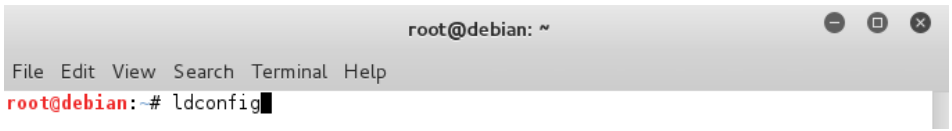
5. Perbaiki library link ke dalam library untuk memastikan TACACS+ daemon start dengan baik.



Gambar 6.4 Perbaiki Library Link

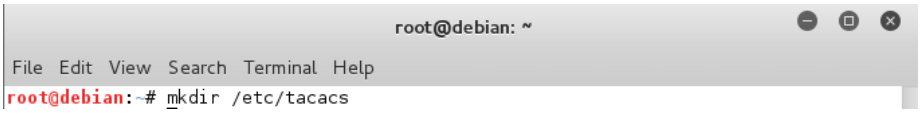
Gambar 6.5 Memastikan TACACS+ Daemon Start Dengan Baik

6. Reload library



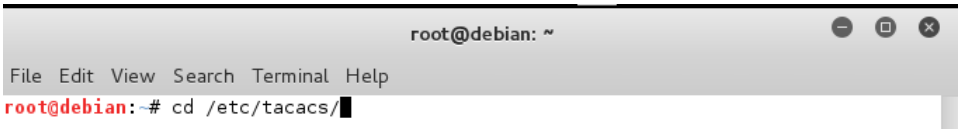
Gambar 6.6 Reload Library

7. Buat direktory tacacs



Gambar 6.7 Membuat Directory Tacacs

8. Masuk ke dalam direktori yang sudah dibuat



Gambar 6.8 Masuk Direktori

9. Buat file kosong didalamnya dengan nama tac_plus.conf

Gambar 6.9 Membuat File Kosong

10. Ubah permission menjadi 755

Gambar 6.10 Mengubah Permission Menjadi 755

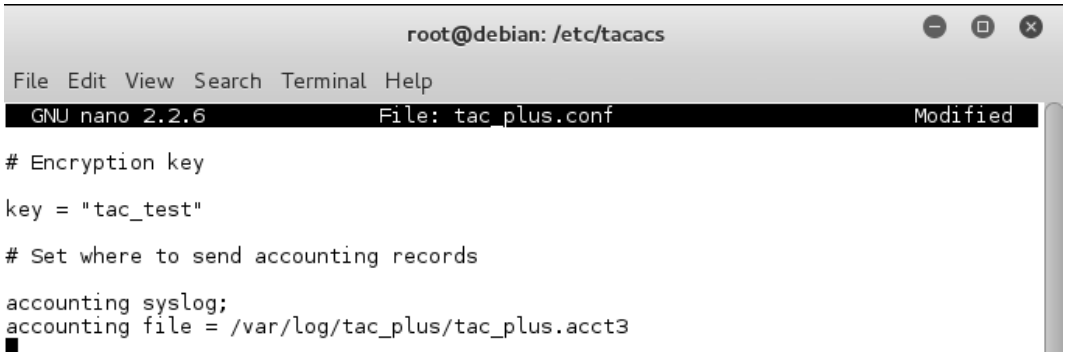
11. Buat direktori /var/log/tac_plus

Gambar 6.11 Membuat Direktori

12. Buat file kosong didalam direktory yang sudah dibuat dengan nama tac_plus.acct

Gambar 6.12 Membuat File Kosong Dalam Direktori

13. Edit file pada /var/log/tac_plus , key untuk TACACS server ini adalah "tac_test"



Gambar 6.13 Mengedit File

14. Masih tetap didalam tac_plus.conf, tambahkan user yang ada, misal:

default authentication = file /etc/passwd
user = admin {
login = cleartext "123456"
enable = cleartext "enableadmin"
}
user = joko {
login = file /etc/passwd
enable = cleartext "enablejoko"
}

Maksud dari perintah tersebut adalah jika tidak ada user di dalam list user, maka akan dilihat pada user linux. Kemudian, membuat username dengan nama admin untuk login dan 123456 untuk passwordnya dan enableadmin adalah password untuk masuk ke privileged mode.

User kedua adalah username joko dengan password untuk login diambil dari database linux dan password privileged mode enablejoko, jika mau mengambil password privileged mode lewat database linux juga bisa.

15. jalankan tacacs+nya dengan mengetikkan

#tac_plus -C /etc/tac_plus.conf -d 16 -l /var/log/tac_plus.login

Konfigurasi pada Cisco

Untuk test TACACS+ Server, digunakan Router Cisco dengan perintah:

```
Router(config)#aaa new-model
Router(config)#aaa authentication login default group tacacs+ local
Router(config)#aaa authentication enable default group tacacs+ enable
Router(config)#tacacs-server host 192.168.1.2
Router(config)#tacacs-server key tac_test
```

Gambar 6.14 Test TACACS+ Server Router Cisco

Penjelasan perintah :

1. AAA new-model adalah perintah untuk mengaktifkan AAA security services.
2. AAA authentication login default group tacacs+ local: semua password pada semua interface akan menggunakan TACACS+ untuk authentication. Jika tidak ada TACACS+ server yang merespon, maka network access server akan menggunakan lokal username yang ada.
3. AAA authentication enable default group tacacs+ enable: mengaktifkan authentikasi untuk grup tacacs.
4. TACACS-server host, perintah ini untuk mengaktifkan tacacs server pada alamat ip tacacs server yang inputkan.
5. TACACS-server key, perintah ini untuk mengaktifkan key atau kunci dari tacacs server.

Jangan lupa untuk mengaktifkan port 49 pada firewall.

Konfigurasi tersebut akan berjalan jika server dan router aktif dan dapat saling bertukar informasi. Setelah semua berjalan, logout dari router, masuk kedalam router lagi dan masukkan username dan password sesuai dengan konfigurasi anda pada tacacs+ server

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiaan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.

3. Mengaumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Apa saja paket yang harus diinstal sebelum mengintstal TACACS pada linux?

……
……
……
……
……

2. Perintah apa yang harus ditambahkan dalam tac_plus.conf untuk membuat user “eko” dengan password “1234” dan password enable “enableeko” ?

……
……
……
……
……

3. Perintah apa untuk menjalankan tacacs ?

……
……
……
……
……

F. Rangkuman

Authentication merupakan suatu proses yang bertujuan untuk proses validasi user yang akan masuk ke dalam sistem. Authentication melakukan pengenalan

terhadap peralatan, sistem operasi, aplikasi dan identifikasi user saat ingin memasuki jaringan suatu sistem. Proses authentication dimulai dari user harus memasuki username dan password untuk proses identifikasi

Dengan kata lain, Autentikasi adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Authentication terdiri dari *Basic Authentication,Negotiate Authentication, Digest Authentication,* dan NLTM *Authentication*.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang konsep dasar tacacs dan berapa proses pencapaian kompetensinya?
2. Apakah saudara sudah memahami konsep menganalisis fungsi dan cara kerja server autentikasi serta berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. gcc bison, flex, dan libwrap0-dev
2. user = eko {
   login = cleartext “1234”
   enable = cleartext “enableeko”
   }
3. #tac_plus -C /etc/tac_plus.conf -d 16 -l /var/log/tac_plus.login

7

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 7: Menganalisis Sistem Pendeteksi Dan Penahan Ancaman/Serangan Yang Masuk Ke Jaringan (Snort)

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menganalisis sistem pendeteksian dan penahan ancaman/serangan yang masuk ke jaringan.

B. Indikator Pencapaian Kompetensi

- Memahami konsep analisa sistem pendeteksi dan penahan ancaman/serangan yang masuk ke jaringan.
- Menggunakan tool snort sebagai pendeteksi serangan yang masuk ke jaringan.

C. Uraian Materi

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Serangan tersebut dilancarkan oleh Cracker yang bermaksud untuk merusak jaringan komputer yang terkoneksi pada internet ataupun mencuri informasi penting yang ada pada jaringan tersebut. Adanya firewall telah banyak membantu administrator jaringan untuk mengamankan jaringannya, akan tetapi seiring dengan berkembangnya teknologi sekarang, firewall tidak dapat mengatasi serangan-serangan yang terjadi. Karena itu telah berkembang teknologi IDS dan IPS sebagai pembantu pengaman data pada suatu jarigan komputer. Dengan adanya IDS (Intrusion Detection System) dan IPS (Instrusion Prevention System), maka serangan – serangan tersebut lebih dapat dicegah ataupun dihilangkan. IDS (Intrusion Detection System) berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam) sedangkan IPS (Intrusion Prevention System) berguna untuk mendeteksi serangan dan menindaklanjutinya dengan pemblokan serangan.

1. **IDS (Instrusion Detection System)**

IDS adalah tool, metode, sumber daya yang memberikan laporan terhadap aktivitas jaringan komputer. IDS bekerja pada layer network dari OSI model maka dari itu IDS dapat menganalisis paket untuk menemukan pola dan pola tersebut akan disimpan ke dalam data log. Tujuan dari IDS adalah mengkarakteristikkan gejala atau kejadian yang menunjukkan adanya instrusi atau gangguan. Pendeteksian instrusi merupakan proses pemantauan dan analisis kejadian yang terjadi pada sebuah komputer atau pada jaringan. Umumnya IDS memberi notifikasi kepada sistem administrator ketika terdapat kemungkinan terjadinya intrusi.

Tujuan dari IDS adalah meminimalkan perkiraan kerugian dari intrusion. Jadi pastikan bahwa IDS yang digunakan itu memiliki teknologi sbb :

1. Akurasi yang tinggi.

   Akurasi merupakan ketelitian, jadi IDS yang baik itu harus memiliki ketelitian yang baik untuk mengenal tindakan-tindakan penyerangan. Pada saat ini sudah banyak IDS yang memiliki level ketelitian yang sangat tinggi, mampu secara realtime mendeteksi dan melakukan 'blocking' terhadap tindakan-tindakan yang mencurigakan. Tidak hanya itu, IDS juga harus mampu memeriksa dan menganalisa secara menyeluruh paket-paket data yang dipergunakan. Membedakan paket data yang keluar masuk dalam lalu lintas jaringan pun harus dapat dihandalkan sehingga dapat mengenal benar karakteristik traffic penyerang.

   Untuk dapat melakukan hal tersebut, maka diperlukan IDS dengan karakterisitik :

   - Mampu menganalisa protokol dari semua sumber lalu lintas data (trafic)
   - Mampu menganalisa protokol secara stateful untuk Layer 3 sampai Layer 7
   - Mampu melakukan perbandingan secara Context-base, multiple-trigger, multiple-pattern
   - Signature dengan tujuan bisa mengenal dan mengetahui jenis exploit yang dipergunakan.
   - Mampu melakukan 'Forward' dan 'Backward' apabila terjadi proses overlap (penumpukan data) pada IP Fragmen (Layer 3)

- Mampu melakukan 'Forward' dan 'Backward' apabila terjadi proses overlap (penumpukan data) pada TCP Segment
- Mampu melakukan 'Forward' dan 'Backward' apabila terjadi kerancuan dan ketidakberesan didalam implementasi protokol (layer 4)
- Mampu melakukan kontrol pada tingkat aplikasi protokol seperti : HTTP, FTP, Telnet, RPC Fragmentasi, SNMP (Layers 6 and 7)

2. Mampu mencegah serangan dan tidak hanya mendeteksi.

   Jangan gunakan IDS yang hanya dapat mendeteksi serangan saja, tapi gunakan IDS yang sudah mampu melakukan pencegahan terhadap serangan. IDS yang baik tidak memiliki batasan metoda pendeteksian dan dapat dipercaya dalam mencegah suatu serangan.

   Pencegahan serangan dapat dipenuhi oleh IDS jika IDS memiliki karakteristik:

   - Dapat beroperasi secara in-line
   - Memiliki kehandalan dan ketersediaan
   - Deliver high performance
   - Kebijakan policy pada IDS bisa diatur

3. Memiliki cakupan yang luas dalam mengenal proses attacking

   IDS harus memiliki pengetahuan yang luas, bisa mengenal apa yang tidak dikenalnya, mampu melakukan deteksi DoS mempergunalan analisis 'signature' dan mampu menditeksi segala sesuatu yang mencurigakan.

   Untuk memenuhi kriteria ini IDS harus :

   - Mampu melakukan proses deteksi trafic dan pembersihan terhadap host (Layer 3 - 7)
   - Mampu malakukan 'scanning' TCP dan UDP
   - Mampu memeriksa keberadaan 'Backdoor'

4. Hasil analisis terhadak trafik bisa diterima

   Karena banyak paket data yang keluar masuk maka IDS harus mampu menangani area data yang sangat luas, bisa ditempatkan didalam topologi yang berbeda, dapat dihadapkan dengan switch dan data yang terenkripsi.

5. Dapat memberikan informasi tentang ancaman2 yang terjadi
6. Memiliki tingkat Forensik yang canggih dan mampu menghasilkan reporing yang baik

7. Memiliki sensor yang dapat dipercaya untuk memastikan pendeteksian dan pencegahan.

Arsitektur

Arsitektur IDS terdapat tiga komponen utama, yaitu:

1. Sensor

   Sensor ini akan mengumpulkan data dan meneruskannya kepada analyzer. Contoh data yang dikumpulkan adalah paket data pada jaringan dan log file.

2. Analyzer

   Analyzer ini akan menerima masukan dari sensor dan menentukan apakah masukan tersebut termasuk intrusi.

3. User Interface

   User Interface ini memungkinkan pengguna untuk meluhat keluaran dari sistem.

Tipe IDS

IDS akan dipasang di berbagai tempat pada jaringan untuk meningkatkan keamanan dan proteksi sebuah perusahaan. Pada umumnya, terdapat dua jenis IDS yang digunakan saat ini, yaitu IDS berbasis jaringan dan IDS berbasis host.

a. Host-Based Intrusion Detection System (HIDS)

   Merupakan aplikasi perangkat lunak khusus yang diinstal pada komputer (biasanya server) untuk mendeteksi serangan pada host tersebut. HIDS sangat efektif untuk server aplikasi Internet-accessible, seperti web atau e-mail server karena mereka dapat melihat aplikasi pada source-nya untuk melindungi mereka. Sebagai contoh, ada tidaknya file yang diubah atau ada usaha untuk mendapatkan akses ke file yang sensitif.

b. Network-Based Intrusion Detection System (NIDS)

   NIDS memeriksadata yang ditransmisikan melalui jaringan sehingga dapat memonitor beberapa host secara bersamaan. NIDS biasanya dikembangkan di depan dan di belakang firewall dan VPN gateway untuk mengukur keefektifan peranti-peranti keamanan tersebut dan berinteraksi dengan mereka untuk mernperkuat keamanan jaringan.

4. Snort

Snort merupakan suatu software untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real time traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort dapat diunduh secara gratis di situs resminya yaitu www.snort.org dan perangkat lunak ini dapat berjalan pada sistem operasi Linux, BSD, Solaris dan Windows. Snort adalah bagian dari IDS dan juga memiliki kemampuan realtime alert yang mekanisme pemasukan alert tersebut dapat berupa user, syslog, file, uni socket ataupun melalui database.

Snort merupakan bagian dari IDS yang terdiri dari beberapa komponen, yaitu :

1. Packet Decoder

   Packet Decoder mengambil paket dari berbagai jenis perangkat jaringan dan mempersiapkan paket data untuk dapat masuk ke *preprocessed* atau untuk dikirim ke mesin deteksi (*Detection Engine*).

2. Preprocessors

   Preprocessors adalah komponen atau plug-ins yang dapat digunakan dengan Snort untuk mengatur atau memodifikasi paket data sebelum Detection Engine melakukan beberapa operasi untuk mengetahui apakah paket sedang digunakan oleh penyusup.

3. The Detection Engine

   Detection Engine adalah jantung dari snort. Tanggung jawabnya adalah untuk mendeteksi jika ada aktivitas intrusi dalam sebuah paket. Paket yang datang akan di test dan dibandingkan dengan rule yang telah ditetapkan. Jika sebuah paket cocok dengan rule apa pun, maka tindakan yang tepat diambil tetapi jika tidak paket dibuang. Tindakan yang tepat mungkin akan mendata paket (Logging packet) atau menghasilkan alert. Detection Engine adalah timecritical penting dari Snort.

4. Logging and Alerting System

   Tergantung pada apa yang Detection Engine temukan dalam sebuah paket, paket digunakan untuk mencatat aktivitas atau menghasilkan peringatan (alert).

5. Output Modules

Output modul atau plug-in dapat melakukan operasi yang berbeda-bedatergantung pada bagaimana ingin menyimpan output yang dihasilkan olehlogging dan system alert dari snort. Dapat berupa XML, Database, syslog, binary format dan teks.

Alasan memilih snort :

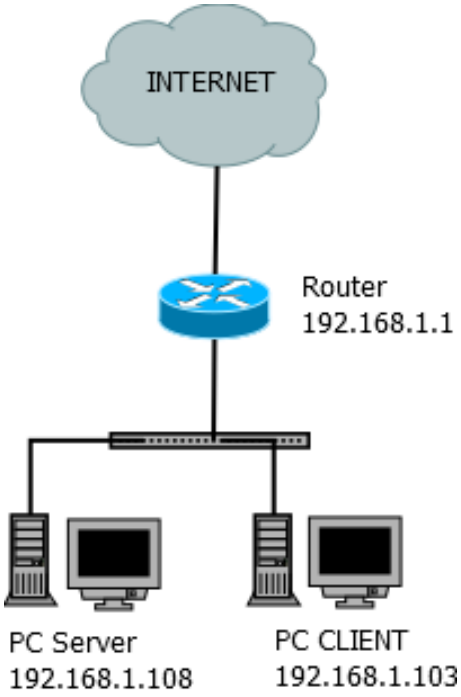
- Snort adalah program yang free dan open source
- Snort dapat berjalan secara kontinu pada sistem dengan sesedikit mungkin campur tangan dari manusia
- Snort tidak mengakibatkan overhead terhadap sistem IDS yang mengakibatkan komputer menjadi lambat dan mengakibatkan terjadinya drop paket yang seharusnya diterima oleh sistem.
- Logging Snort bisa dikirim ke data base (mysql).

Snort.conf

File ini merupakan suatu otak dari snort itu sendiri. Pada file ini user dapat melakukan setting meliputi Network and configuration variables, snort decoderdan detection engine configuration.

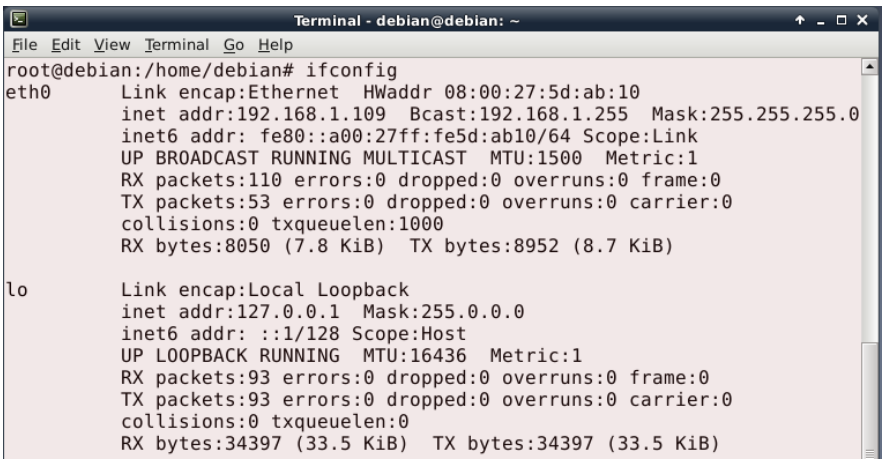
D. Aktivitas Pembelajaran

Dalam praktek kali ini, akan dijelaskan mengenai konfigurasi SNORT yang akan dipasang pada PC server dengan sistem operasi Linux, sedangkan PC Client menggunakan Windows. SNORT ini akan bertindak sebagai keamanan server. Berikut ini adalah topologi jaringan yang dibuat.

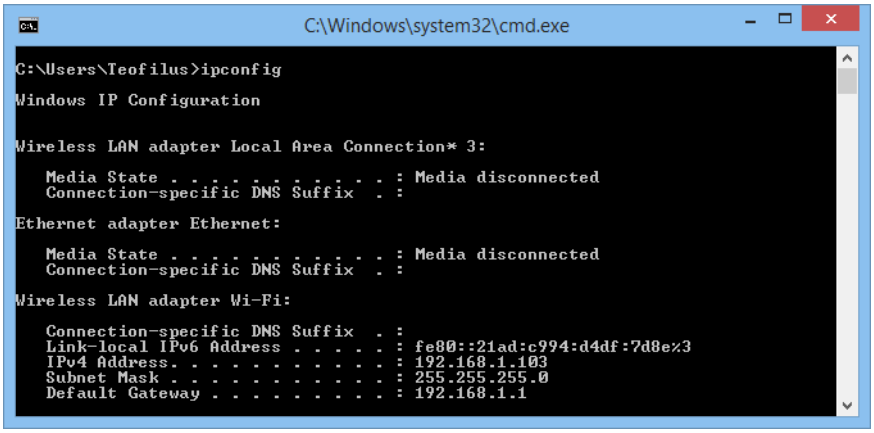


Gambar 7.1 Topologi Jaringan Snort

1. Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router, lalu cek ip address dengan perintah #ifconfig. Untuk windows, gunakan perintah #ipconfig pada Command Prompt. Untuk membangun topologi seperti pada topologi dibawah ini, maka pada praktikum ini, router harus diatur sebagai DHCP Server. Snort akan dipasang pada PC server yang memiliki IP Address 192.168.1.109.

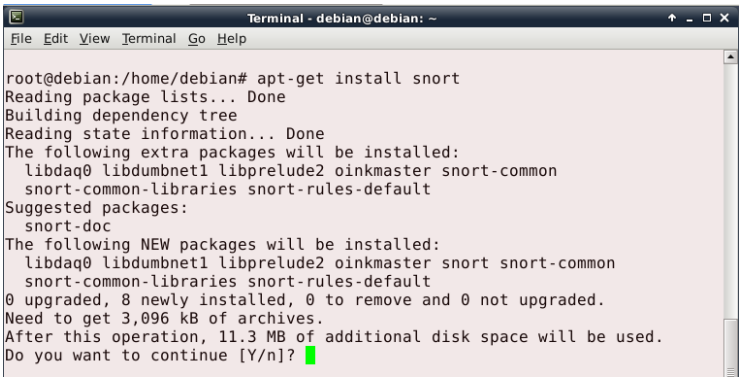


Gambar 7.2 IP Address Pada Debian



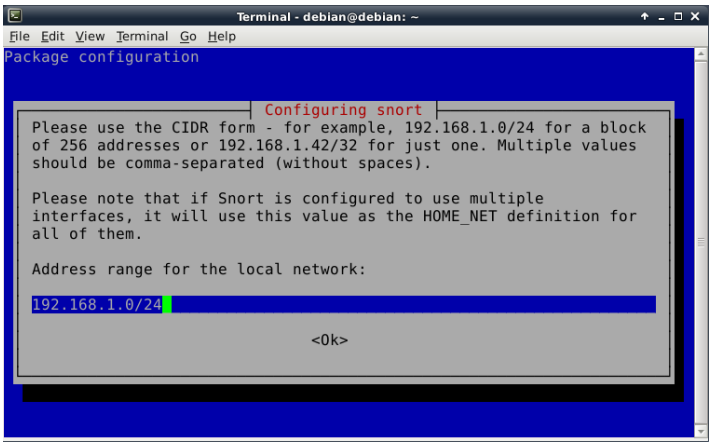
Gambar 7.3 IP Address Pada Windows

2. Lakukan instalasi snort pada PC Server dengan perintah #apt-get install snort



Gambar 7.4 Instalasi Snort Pada PC Server

3. Masukkan range network yang akan dianalisa. IP Network pada topologi diatas adalah 192.168.1.0/24



Gambar 7.5 Masukkan Range Network

4. Menjalankan snort

Terdapat tiga mode untuk menjalankan snort, yaitu:

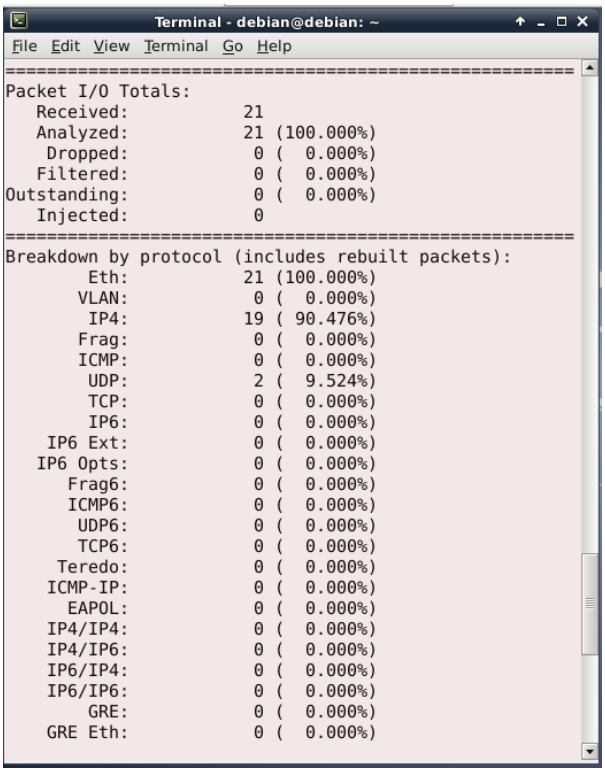
a. Sniffer mode

Mode ini digunakan untuk melihat paket yang lewat pada lalu lintas jaringan tersebut.

a) #snort –v

snort –v digunakan untuk melihat header TCP/IP paket yang lewat.

Gambar 7.6 Perintah Snort -v

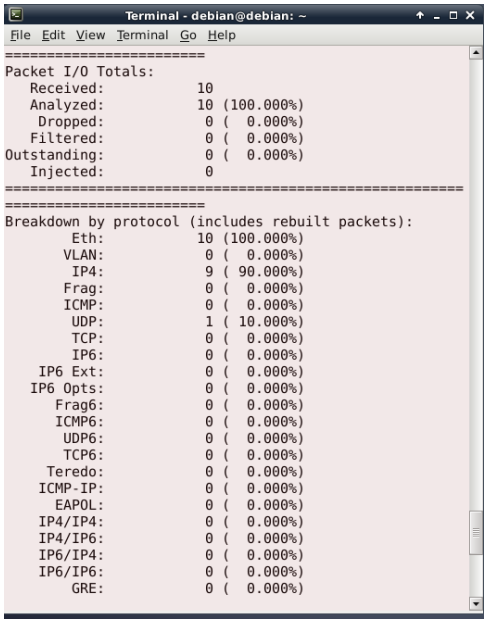


Gambar 7.7 Tampilan Header TCP/IP

b) #snort –vd

Snort –vd digunakan untuk melihat isi paket.

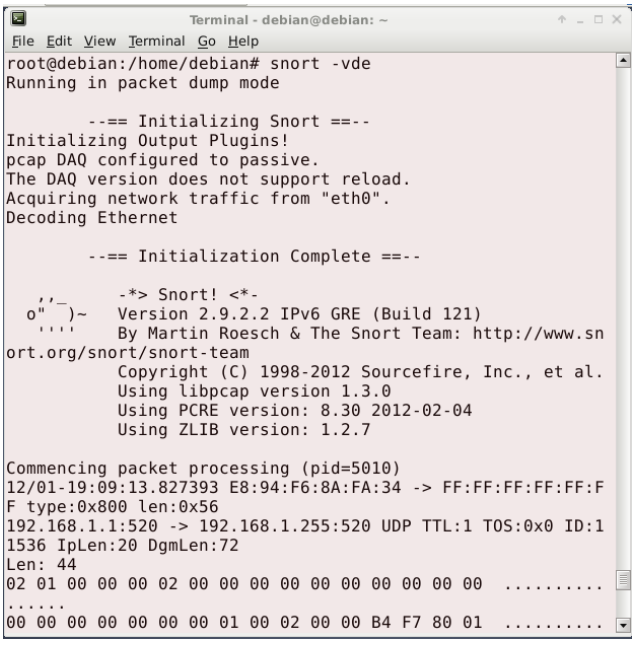
Gambar 7.8 Perintah Snort –vd



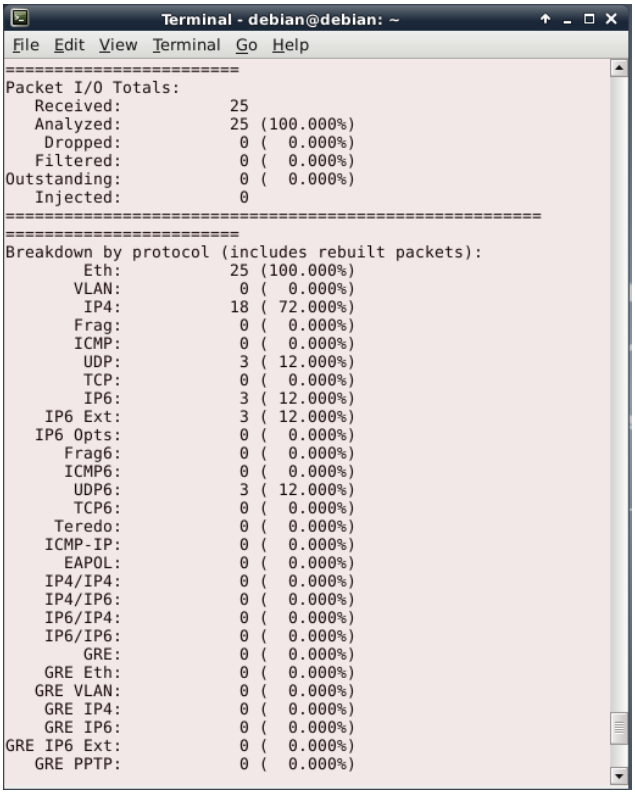
Gambar 7.9 Tampilan Isi Paket

c) #snort –vde

Tambahan –e atau snort –vde digunakan untuk melihat header link layer paket seperti ethernet header.



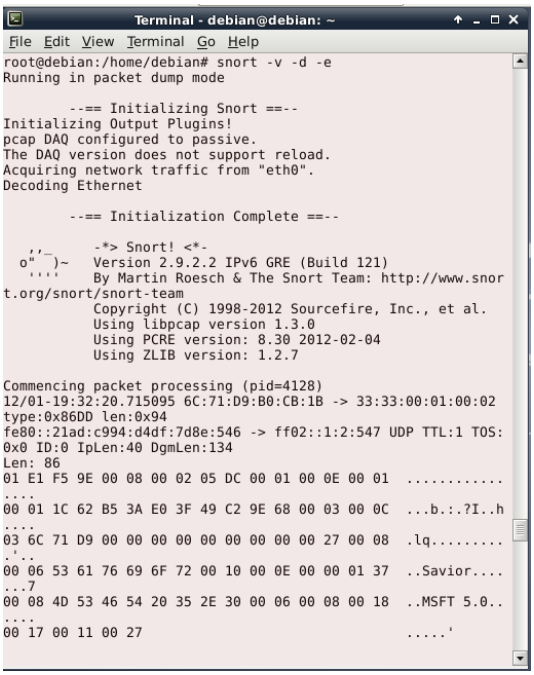
Gambar 7.10 Perintah Snort –vde



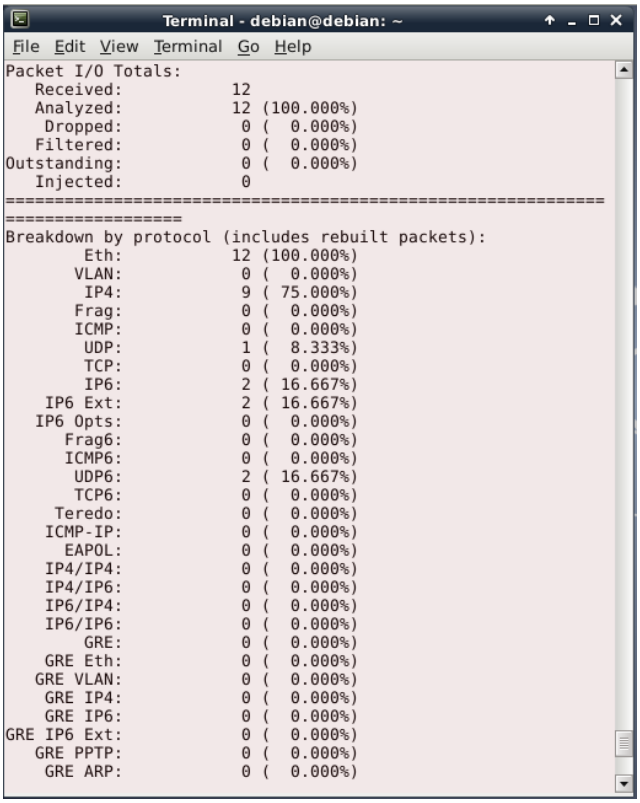
Gambar 7.11 Tampilan Header Link Layer

d) #snort –v –d –e

Untuk melihat paket yang lewat, untuk melihat isi paket dan untuk melihat header link layer paket seperti ethernet header dalam satu perintah.



Gambar 7.12 Perintah Snort –v –d –e



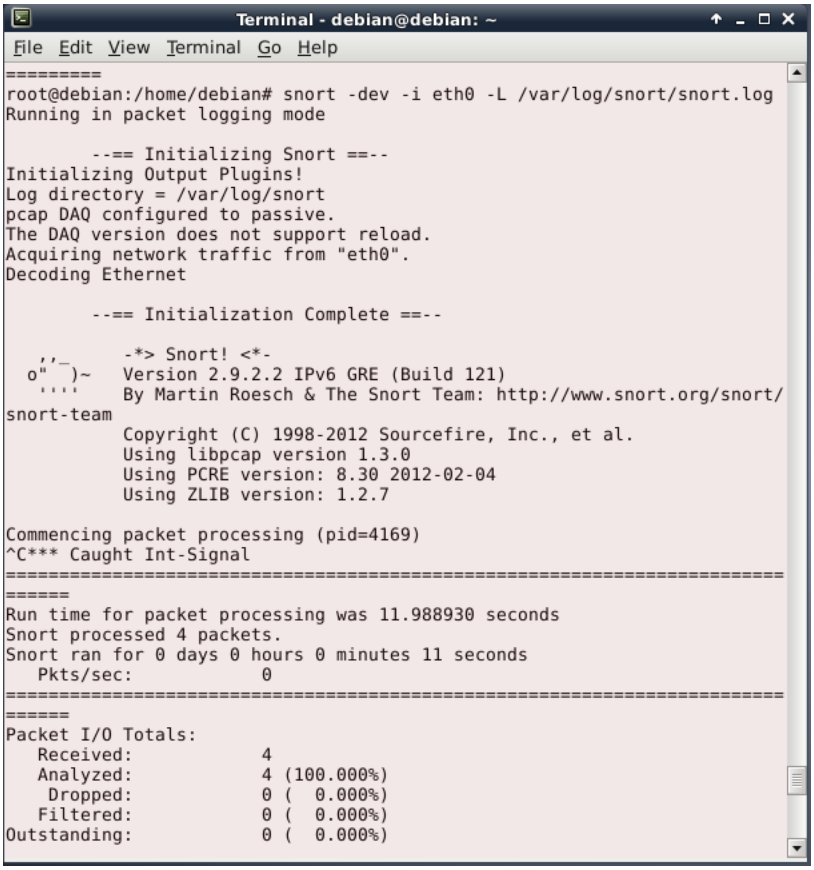
Gambar 7.13 Tampilan Hasil Snort –v –d –e

b. Packet Logger Mode

Mode ini digunakan untuk mencatat semua paket yang lewat pada lalu lintas jaringan tersebut untuk dianalisa. Jalankan snort pada PC Server, kemudian jalankan Nmap untuk port scanning. Untuk mempermudah pembacaan masukkan hasil snort ke dalam file, jalankan perintah berikut :

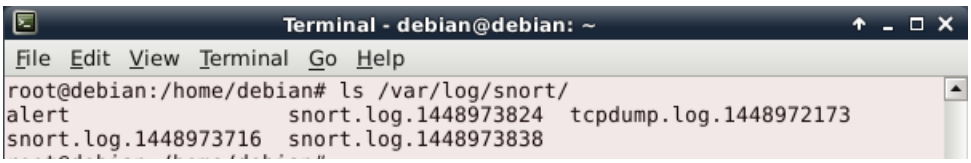
a) #snort –dev –i eth0 –L /var/log/snort/snort.log

Akan menghasilkan sebuah file di folder /var/log/snort, lihat dengan perintah :



Gambar 7.14 Tampilan Snort –dev – i

b) # ls /var/log/snort

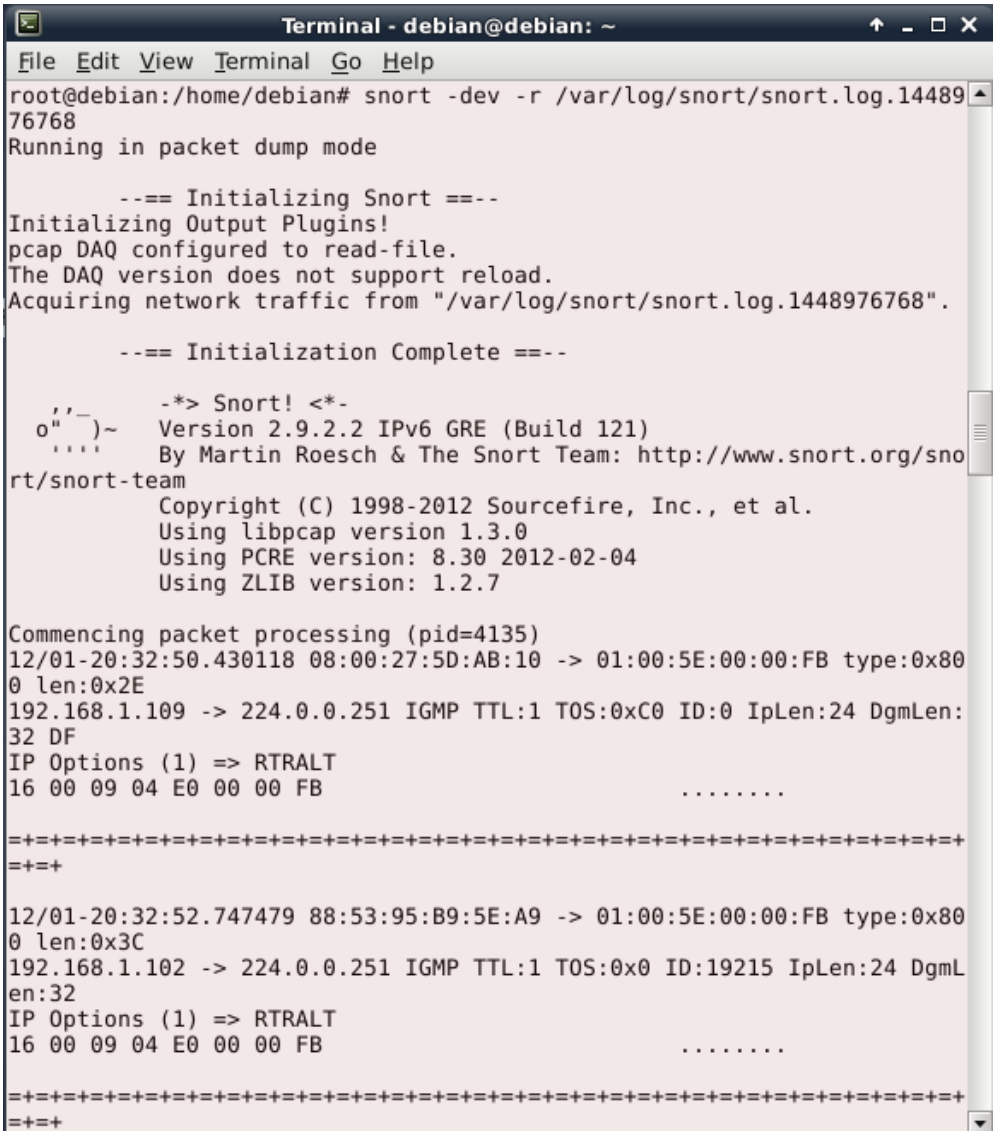


Gambar 7.15 File Snort

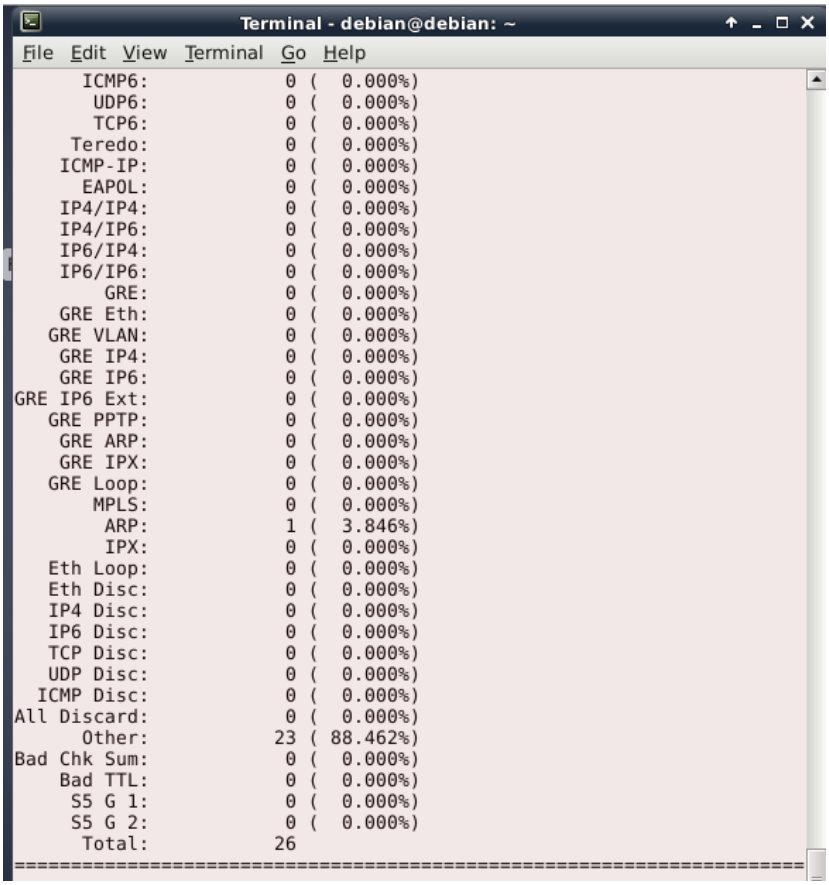
Pada gambar diatas terlihat sudah ada 3 file snort dan 1 file tcpdump pada direktori /var/log/snort/.

c) Untuk membaca file snort (misal : snort.log.1234) berikan option –r pada snort# **snort -dev -r /var/log/snort/snort.log.1234**

Pada gambar dibawah ini, sistem membaca file snort yang ada di /var/log/snort ,dan ada 14 packet yang diproses oleh snort.



Gambar 7.16 Proses Pembacaan File Snort



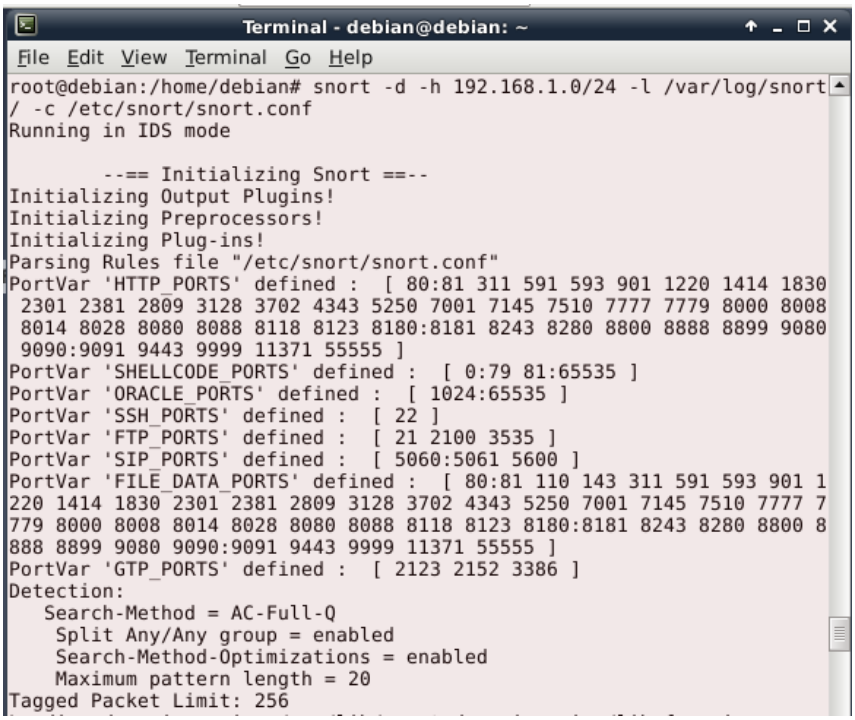
Gambar 7.17 Proses Pembacaan File Snort (Lanjutan)

c. Intrusion Detection System

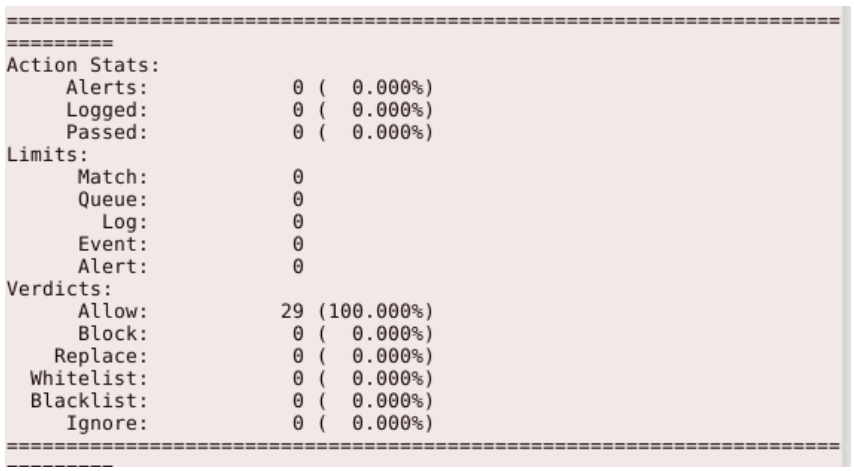
Mode ini akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer dengan aturan / rules yang akan membedakan paket normal atau paket yang bertujuan untuk menyerang.

a) #snort -d -h 192.168.1.0/24 -l /var/log/snort -c /etc/snort/snort.conf

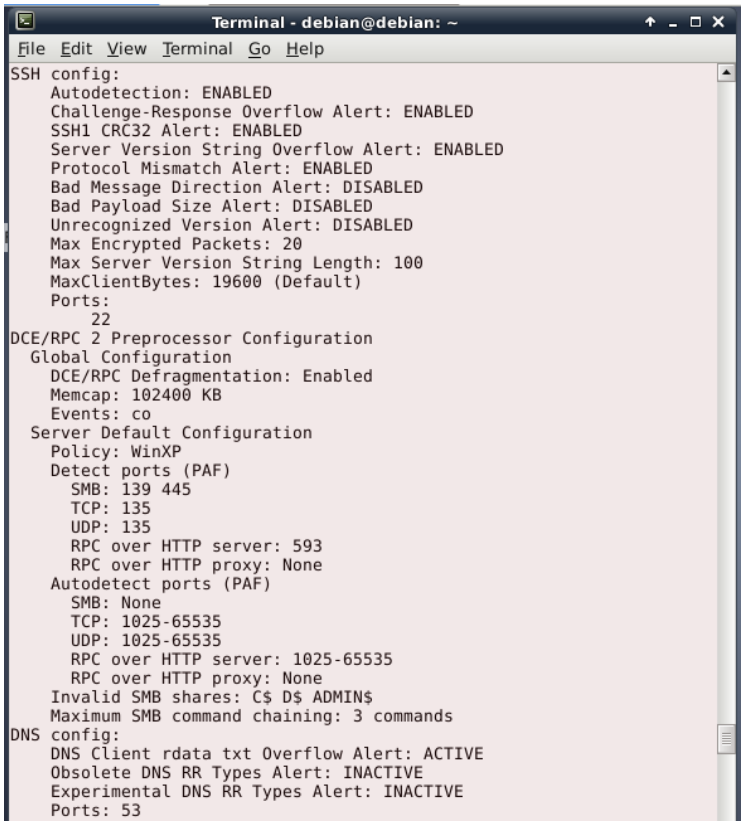
Pada percobaan dibawah, snort dijalankan dengan mode NIDS(Network Intrusion Detection System), terlihat pada gambar Server Default Configuration adalah WinXP dengan port yang terdeteksi SHB: 139,445 , TCP:135, UDP:135,dan tidak ada alerts



Gambar 7.18 Snort Mode NIDS



Gambar 7.19 Snort Mode NIDS (lanjutan 1)

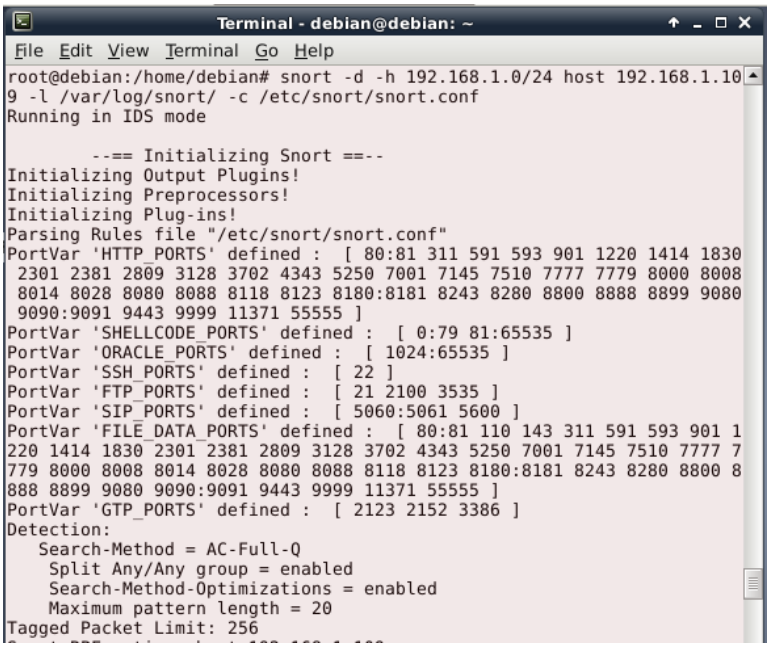


Gambar 7.20 Snort Mode NIDS (lanjutan 2)

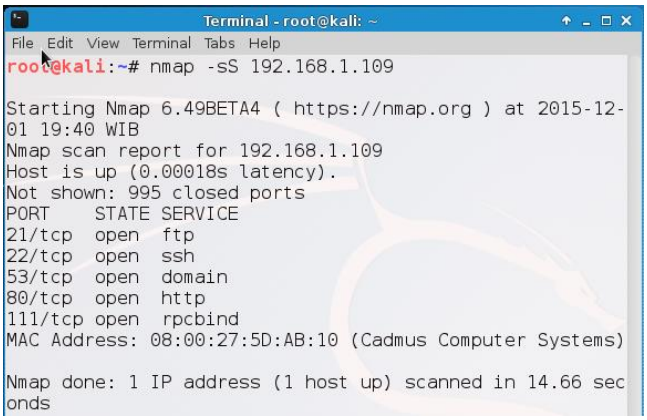
b) Kemudian jalankan scanning dari komputer lain dengan nmap menuju computer yang anda pasangi snort (PC Server). Terlebih dulu jalankan snort dengan mode NIDS, kemudian lakukan scanning dengan perintah :

#snort -d -h 192.168.1.0/24 host <no_ip_snort> -l /var/log/snort –c /etc/snort/snort.conf

#nmap -sS -v <no_ip_snort>

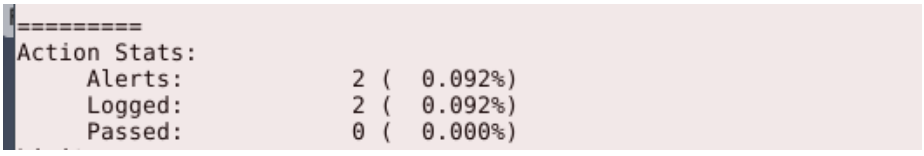


Gambar 7.21 Snort Scanning



Gambar 7.22 Snort Scanning (lanjutan)

Pada proses aktivitas snort, terlihat kegiatan nmap diketahui snort sebagai alerts.



Gambar 7.23 Proses Aktivasi Snort

d. Membuat Rule Dalam Snort

a) Buat rule baru yaitu alltcp.rules dan simpan di /etc/snort/rules

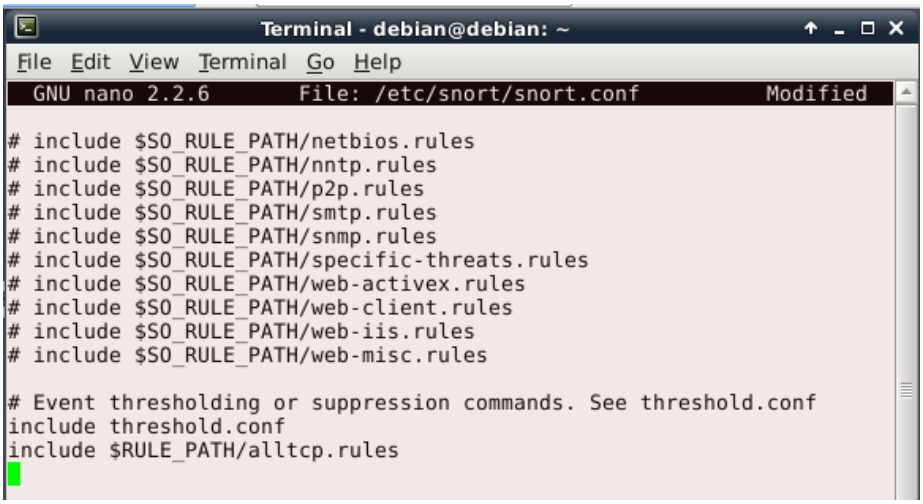
#vim /etc/snort/rules/alltcp.rules

Gambar 7.24 Membuat Rule Baru

b) Masuk ke dalam snort.conf. Beri tanda # pada semua rule lain dan tambahkan rule yang sudah dibuat yaitu : alltcp.rules.

#vim /etc/snort/snort.conf

include $RULE_PATH/alltcp.rules



Gambar 7.25 Menandai Rule

c) Lakukan restart aplikasi snort anda :

 # /etc/init.d/snort restart

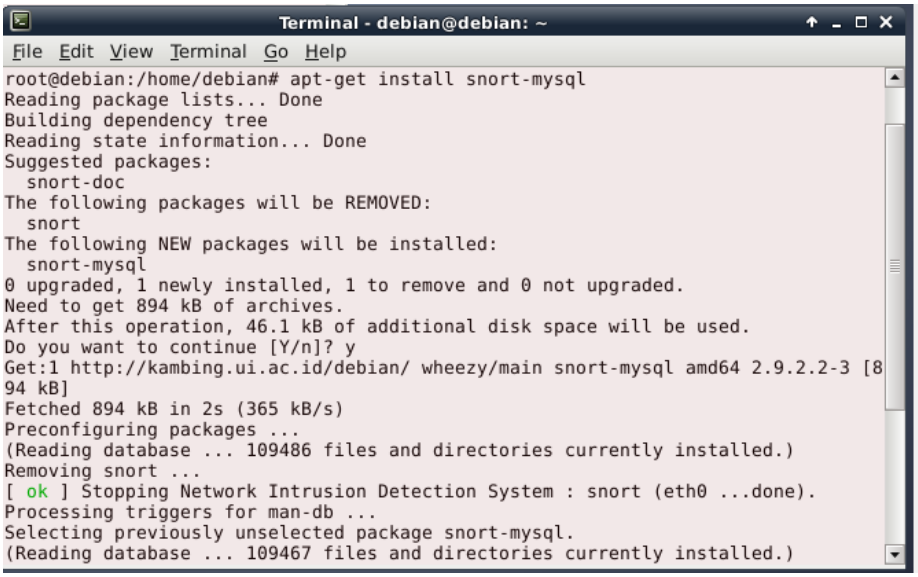
d) Bukalah halaman web untuk mengakses “www.twitter.com”, ketika membuka www.twitter.com ,pada snort terlihat informasi baru yang muncul

Gambar 7.26 Mencoba Snort Pada Halaman Website

e. Snort dan Database MySQL

Snort dapat juga diintegrasikan pada mysql yang nantinya log file akan tersimpan dalam database.

a) Install snort-mysql



Gambar 7.27 Instal Snort-MySQL

b) Buat dan konfigurasi database snort

```
mysql> create database snort;
Query OK, 1 row affected (0.00 sec)

mysql> grant all on snort.*to snort@localhost identified by 'admin';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges
    -> ;
Query OK, 0 rows affected (0.06 sec)

mysql> exit
Bye
```

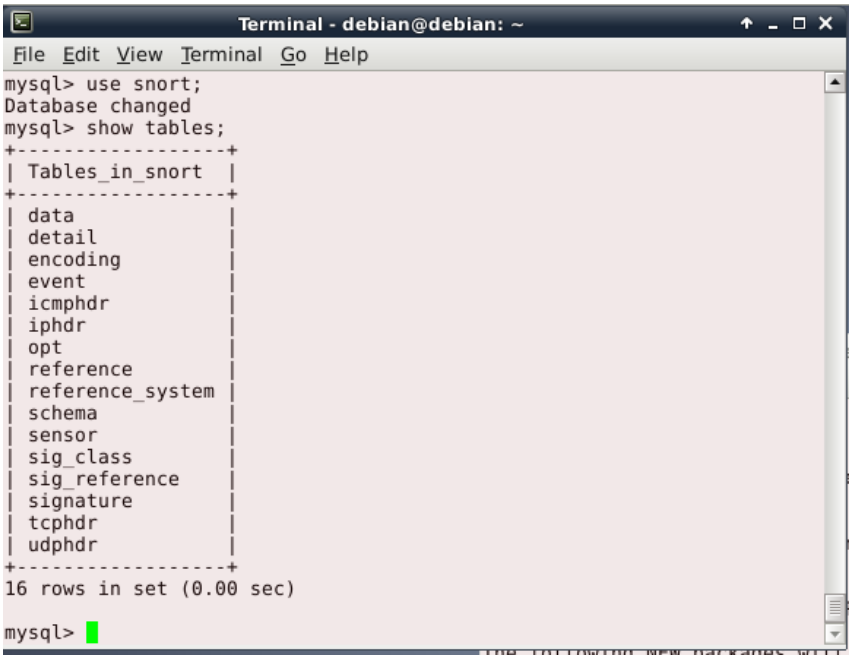
Gambar 7.28 Konfigurasi Database Snort

c) Masukkan tabel pada snort dengan tabel yang sudah disediakan

```
root@debian:/home/debian# gzip -d /usr/share/doc/snort-mysql/create_my
sql.gz
root@debian:/home/debian# mysql -u root -p snort < /usr/share/doc/snor
t-mysql/create_mysql
Enter password:
```

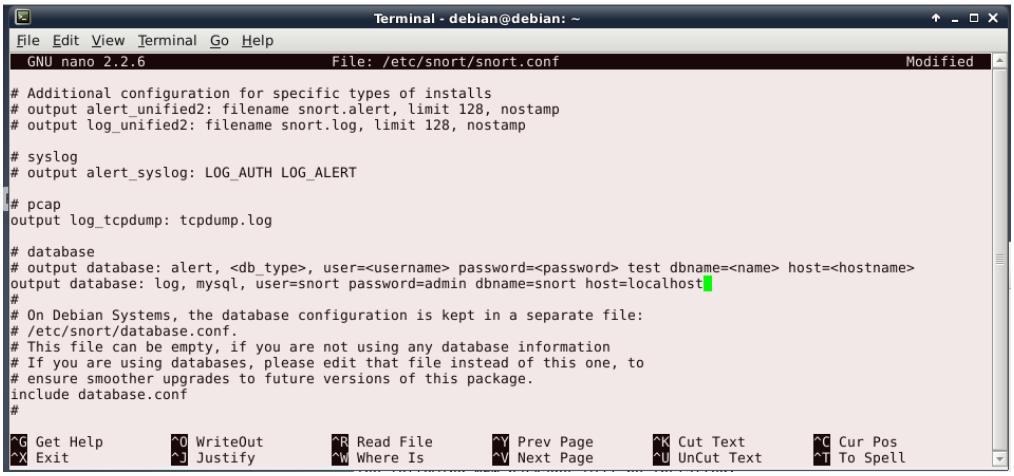
Gambar 7.29 Memasukkan Tabel pada Snort

d) Cek tabel dalam database snort.



Gambar 7.30 Mengecek Tabel Dalam Database Snort

e) Konfigurasi snort.conf untuk mengkonfigurasi database. Cari kata kunci database dan hilangkan tanda #, kemudian isi user, password, nama database dan letak host.



Gambar 7.31 Konfigurasi Snort.conf Untuk Database

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiaan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah dibawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengaumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Untuk menjalankan snort hanya untuk melihat isi dari paket digunakan perintah apa?

……

……
……
……
……

2. Untuk menjalankan snort pada mode IDS pada suatu host digunakan perintah apa?

……
……
……
……
……

3. Bagaimana cara menjalankan snort untuk NIDS?

……
……
……
……
……

F. Rangkuman

IDS (Intrusion Detection System) berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam) sedangkan IPS (Intrusion Prevention System) berguna untuk mendeteksi serangan dan menindaklanjutinya dengan pemblokan serangan. Tujuan dari IDS adalah mengkarakteristikkan gejala atau kejadian yang menunjukkan adanya instrusi atau gangguan. Pendeteksian instrusi merupakan proses pemantauan dan analisis kejadian yang terjadi pada sebuah komputer atau pada jaringan. Umumnya IDS memberi notifikasi kepada sistem administrator ketika terdapat kemungkinan terjadinya intrusi.

G.Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang perintah dasar snort dan berapa prosen pencapaian kompetensinya?

2. Apakah saudara sudah memahami perintah untuk melihat paket dalam suatu jaringan menggunakan snort serta berapa prosen pencapaian kompetensinya?
3. Apakah saudara sudah memahami perintah mengintegrasikan snort dan mysql dan berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. Untuk melihat isi paket dalam jaringan, maka digunakan perintah snort -vd.
2. Untuk menjalankan snort sebagai IDS pada suatu host, maka digunakan perintah #snort -d -h 192.168.1.0/24 host <no_ip_snort> -l /var/log/snort –c /etc/snort/snort.conf
3. #snort -d -h 192.168.1.0/24 -l /var/log/snort -c /etc/snort/snort.conf

8

KEGIATAN PEMBELAJARAN

Kegiatan Belajar 8: Menerapkan Tata Cara Pengamanan Komunikasi Data Menggunakan Teknik Kriptografi

A. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar ini diharapkan bahwa :

- Melalui praktikum peserta diklat dapat menerapkan tata cara pengamanan komunikasi data menggunakan teknik kriptografi.

B. Indikator Pencapaian Kompetensi

- Memahami konsep menerapkan tata cara pengamanan komunikasi data menggunakan teknik kriptografi.
- Mampu menerapkan one-time-password pada SSH.

C. Uraian Materi

Pada awal perkembangannya, jaringan komputer digunakan hanya untuk pengiriman e-mail antar perguruan tinggi untuk keperluan riset dan untuk berbagi penggunaan printer dalam suatu perusahaan. Untuk memenuhi tujuan tersebut, aspek keamanan jaringan pada saat itu tidak mendapat perhatian penting. Namun kini, saat jaringan komputer juga telah digunakan untuk berbagai aktivitas perbankan dan perdagangan, terutama melalui Internet, aspek keamanan menjadi masalah yang harus mendapat perhatian besar.

Kriptografi merupakan ilmu untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Kriptografi berasal dari Bahasa Yunani yaitu Crypto dan Grafia yang berati penulisan bahasa. Kriptografi bertujuan untuk menjaga kerahasiaan informasi sehingga informasi tersebut tidak dapat diketahui oleh pihak tertentu. Dalam metode Kriptografi, suatu pesan (plain text) harus melalui proses enkripsi terlebih dulu menjadi bentuk yang tidak berarti (cipher text) sebelum dikirimkan ke penerima.

1. *Algoritma Kriptografi*

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (secure).

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

- *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetaprahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatualgoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
- *Data integrity*(keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan)data yang tidak sah (oleh pihak lain).
- *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- **Plaintext** (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.

- **Enkripsi** (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti.

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.
Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext),* notasinya :

$$\mathbf{E_e(M) - C}$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext),* notasinya :

$$\mathbf{D_d(C) = M}$$

Sehingga dari dua hubungan diatas berlaku :

$$\mathbf{D_d(E_e(M)) = M}$$

Terdapat dua jenis algoritma dalam kriptografi yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.* Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci

ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia *(secret-key algorithm).*

Kelebihan :

- Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
- Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem*real-time*

Kelemahan :

- Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkankunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemenkunci tersebut.
- Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"keydistribution problem"*

Contoh dari algoritma simetris adalah DES (Data Encryption Standart).

Sedangkan untuk algoritma asimetris sendiri adalah Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key).* Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

. Pada umumnya kunci publik *(public key)* digunakan sebagai kunci enkripsi sementara kunci privat *(private key)* digunakan sebagai kunci dekripsi.

Kelebihan :

- Masalah keamanan pada distribusi kunci dapat lebih baik
- Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebihsedikit

Kelemahan :

- Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
- Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang

dibandingkan dengan algoritma simetris.

Contoh algoritma : RSA, DSA, ElGamal

2. *Teknik Dasar Kriptografi (Enkripsi)*

Dalam Kriptografi, terdapat 5 teknik dasar dalam melakukan Kriptografi yaitu:

a. Substitusi

Substitusi adalah metode enkripsi yang merubah karakter pada informasi (Plaintext) menjadi karakter yang tersandi (Chipertext). Langkah dalam melakukan substitusi adalah dengan membuat tabel substitusi (dibuat terserah) dan mengganti setiap karakter Plaintext dengan karakter subtitusi yang tersedia. Untuk melakukan teknik ini, tabel substitusi juga haris dimiliki oleh penerima pesan. Berikut adalah contoh penggunaan substitusi:

Caesar Chiper

Tabel Substitusi	: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Deret Inversi	: TEDABCZYXWVUFSRQPONMLKJIHG
Kunci	: A=T
Plaintext	: KRIPTOGRAFI
Enkripsi	: WPXRNSZPTCX
Dekripsi	: KRIPTOGRAFI

b. Blocking

Sistem enkripsi blocking ini membagi plaintext menjadi beberapa block yang terdiri dari beberapa karakter yang kemudian akan dienkripsikan secara independen. Untuk melakukan teknik blocking ini, plaintext harus dituliskan secara vertikal ke bawah berurutan pada lajur dan dilanjutkan pada kolom berikutnya sampai karakter seluruhnya tertulis. Sedangkan untuk mengubahnya ke bentuk chipertext, plaintext yang dituliskan dalam bentuk vertikal tersebut dibaca secara horizontal.

c. Permutasi

Teknik enkripsi permutasi juga sering disebut dengan istilah transposisi yang di mana pada teknik ini memindahkan atau merotasi karakter dengan aturan tertentu. Pada teknik permutasi, identitas dari karakter tetap, hanya saja

posisinya yang diacak. Untuk melakukan permutasi, umumnya plaintext dibagi menjadi blok-blok yang memiliki panjang yang sama.

d. Ekspansi

Teknik enkripsi ekspansi merupakan suatu metode sederhana yang mengacak pesan dengan mengekspansi suatu pesan dengan aturan tertentu. Teknik ini meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata dengan menambahkan akhiran “an”. Jika kata diawali dengan huruf vokal atau bilangan genap, ditambahi akhiran “i”. Contoh : BELAJAR setelah diekspansi menjadi ELAJARBAN.

e. Pemampatan

Teknik enkripsi pemampatan merupakan teknik enkripsi dengan mengurangi panjang pesan dengan suatu cara sehingga menyembunyikan isi dari pesan. Contoh: menggunakan cara dengan menghilangkan setiap karakter ketiga secara berurutan. Karakter yang dihilangkan disatukan kembali dan disusulkan sebagai lampiran dari pesan utama dengan diawali oleh suatu karakter khusus (“*” atau yang lainnya).

3. *Solusi Enkripsi Modern*

Berikut adalah beberapa contoh solusi enkripsi modern yang ada saat ini:

a. Data Encryption Standard (DES)
   - Standart bagi USA Government
   - Didukung ANSI dan IETF
   - Popular untuk metode secret key
   - Terdiri dari 40-bit, 56-bit, dan 3x56-bit (Triple DES)

b. Advanced Encryption Standart (AES)
   - Untuk menggantikan DES (diterbitkan pada akhir tahun 2001)
   - Menggunakan variabel length block chipper
   - Panjang kunci (key length) 128-bit, 192-bit, dan 256-bit
   - Dapat diterapkan untuk smart card

c. Digital Certificated Server (DCS)
   - Verifikasi untuk digital signature
   - Autentikasi user

- Menggunakan public dan private key
- Contoh : Netscape Certificate Server

d. IP Security (IPSec)

IPSec (singkatan dari ***IP Security***) adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP. IPSec mendefiniskan beberapa standar untuk melakukan enkripsidata dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (*internetwork layer*). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman. IPSec didefinisikan oleh badan Internet Engineering Task Force (IETF) dan diimplementasikan di dalam banyak sistem operasi. Windows 2000 adalah sistem operasi pertama dari Microsoft yang mendukung IPSec.

IPSec diimplementasikan pada lapisan transport dalam OSI Reference Model untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. IPSec umumnya diletakkan sebagai sebuah lapsian tambahan di dalam stack protokol TCP/IP dan diatur oleh setiap kebijakan keamanan yang diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan filter yang diasosiasikan dengan kelakuan tertentu. Ketika sebuah alamat IP, nomor port TCP dan UDP atau protokol dari sebuah paket datagram IP cocok dengan filter tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut.

Dalam sistem operasi Windows 2000, Windows XP, dan Windows Server 2003, kebijakan keamanan tersebut dibuat dan ditetapkan pada level domainActive Directory atau pada *host* individual dengan menggunakan *snap-in* IPSec Management dalam Microsoft Management Console (MMC).

Kebijakan IPSec tersebut, berisi beberapa peraturan yang menentukan kebutuhan keamanan untuk beberapa bentuk komunikasi. Peraturan-peraturan tersebut digunakan ntuk memulai dan mengontrol komunikasi yang aman berdasarkan sifat lalu lintas IP, sumber lalu lintas tersebut dan tujuannya. Peraturan-peraturan tersebut dapat menentukan metode-metode autentikasi dan negosiasi, atribut proses *tunneling*, dan jenis koneksi.

Kelebihan:

- Enkripsi public/private key
- Dirancang oleh CISCO System
- Menggunakan DES 40-bit dan authentication
- Built-in pada produk CISCO
- Solusi tepat untuk Virtual Private Network (VPN) dan Remote Network Access

e. Kerberos

Kerberos pertama kali dikembangkan pada dekade 1980-an sebagai sebuah metode untuk melakukan autentikasi terhadap pengguna dalam sebuah jaringan yang besar dan terdistribusi. Kerberos menggunakan enkripsi kunci rahasia/kunci simetris dengan algoritma kunci yang kuat sehingga klien dapat membuktikan identitas mereka kepada server dan juga menjamin privasi dan integritas komunikasi mereka dengan server. Protokol ini dinamai Kerberos, karena memang Kerberos (atau Cerberus) merupakan seekor anjing berkepala tiga (protokol Kerberos memiliki tiga subprotokol) dalam mitologi Yunani yang menjadi penjaga Tartarus, gerbang menuju Hades (atau Pluto dalam mitologi Romawi).

Protokol Kerberos memiliki tiga subprotokol agar dapat melakukan aksinya:

- ***Authentication Service (AS) Exchange***: yang digunakan oleh *Key Distribution Center* (KDC) untuk menyediakan *Ticket-Granting Ticket* (TGT) kepada klien dan membuat kunci sesi logon.

- ***Ticket-Granting Service (TGS) Exchange***: yang digunakan oleh KDC untuk mendistribusikan kunci sesi layanan dan tiket yang diasosiasikan dengannya.
- ***Client/Server (CS) Exchange***: yang digunakan oleh klien untuk mengirimkan sebuah tiket sebagai pendaftaran kepada sebuah layanan.

Kelebihan:

- Solusi untuk user authentication
- Dapat menangani multiple platform/system
- Free charge (open source)
- IBM menyediakan versi komersial : Global Sign On (GSO)

f. Point to Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP)
   - Dirancang oleh Microsoft
   - Autentication berdasarkan PPP(Point to point protocol)
   - Enkripsi berdasarkan algorithm Microsoft (tidak terbuka)
   - Terintegrasi dengan NOS Microsoft (NT, 2000, XP)

g. Remote Access Dial-in User Service (RADIUS)
   - Multiple remote access device menggunakan 1 database untuk authentication
   - Didukung oleh 3com, CISCO, Ascend
   - Tidak menggunakan encryption

h. RSA Encryption
   - Dirancang oleh Rivest, Shamir, Adleman tahun 1977
   - Standar de facto dalam enkripsi public/private key
   - Didukung oleh Microsoft, apple, novell, sun, lotus
   - Mendukung proses authentication
   - Multiplatform

i. Secure Hash Algorithm (SHA)
   - Dirancang oleh National Institute of Standard and Technology (NIST) USA.
   - Bagian dari standar DSS (Decision Support System) USA dan bekerja sama dengan DES untuk digital signature.
   - SHA-1 menyediakan 160-bit message digest

- Versi : SHA-256, SHA-384, SHA-512 (terintegrasi dengan AES)

j. MD5
   - Dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
   - Menghasilkan 128-bit digest.
   - Cepat tapi kurang aman

k. Secure Shell (SSH)
   - Digunakan untuk client side authentication antara 2 sistem
   - Mendukung UNIX, windows, OS/2
   - Melindungi telnet dan FTP (File Transfer Protocol)

l. Secure Socket Layer (SSL)
   - Dirancang oleh Netscape
   - Menyediakan enkripsi RSA pada layes session dari model OSI.
   - Independen terhadap servise yang digunakan.
   - Melindungi system secure web e-commerce
   - Metode public/private key dan dapat melakukan authentication
   - Terintegrasi dalam produk browser dan web server Netscape.

m. Security Token
   - Merupakan suatu aplikasi untuk penyimpanan password dan data dari user pada smart card.

n. Simple Key Management for Internet Protocol
   - Seperti SSL bekerja pada level session model OSI.
   - Menghasilkan key yang statik, mudah bobol.

4. *PKI (Public Key Infrastructure)*

Dalam ilmu kriptografi, PKI (Public Key Infrastructure) adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data serta untuk memastikan keaslian baik dari data maupun pengirim dan mencegah adanya penyangkalan data. PKI menggunakan teknik-teknik kriptografi antara lain fungsi Hash, algoritma simetrik dan algoritma asimetrik. Fungsi Hash digunakan bersamaan dengan algoritma asimetrik dalam bentuk tanda tangan digital yang bertujuan untuk memastikan keaslian dan integritas dari data yang ada beserta dengan pengirimnya. Sedangkan algoritma simetrik digunakan untuk mengamankan data dengan cara enkripsi.

Komponen-komponen PKI antara lain: - Subscriber, - Certification Authority (CA), - Registration Authority (RA), - Sertifikat Digital. Secara praktis wujud PKI adalah penggunaan sertifikat digital. Sertifikat digital adalah sebuah file komputer yang berisi data-data tentang sebuah public key, pemiliknya (subscriber atau CA), CA yang menerbitkannya dan masa berlakunya.

PKI telah diimplementasikan dengan berbagai aplikasi seperti S/MIME, HTTPS, VPN, dll. Anda dapat melihat fitur S/MIME pada software email yang terkenal seperti Outlook Express, Mozilla Mail/Thunderbird, dan Evolution.

5. *PGP (Pretty Good Privacy)*

PGP (Pretty Good Privacy) merupakan suatu program yang digunakan untuk mengenkripsi suatu dokumen tertentu. PGP menggunakan Private-Public Key sebagai dasar dari autentifikasinya. PGP dibuat berdasarkan konsep dari Private Key Cyptography yang digunakan untuk mengenkripsi dalam hubungan komunikasi antara dua mesin. Informasi yang biasanya menggunakan konsep PGP adalah seperti e-mail, credit card, atau informasi rahasia yang menggunakan Internet sebagai media pengiriman.

PGP (Pretty Good Privacy) bekerja dengan menggabungkan beberapa bagian dari key konvensional dan public key cryptography sehingga PGP dapat dikatakan sebagai Hybrid Cryptosystem. Berikut adalah prinsip kerja dari PGP:

a. PGP menggunakan teknik yang disebut public key encryption dengan menggunakan dua buah kode yang saling berhubungan yang sangat tidak mungkin untuk memecahkan satu dengan yang lainnya,
b. Jika membuat suatu kunci, maka secara otomatis akan dihasilkan sepasang kunci yaitu public key dan secret key. Public key dapat diberikan ke manapun tujuan yang inginkan, baik melalui telephone, internet, keyserver, dsb. Secret key disimpan pada mesin dan menggunakan messager decipher akan dikirimkan kembali. Jadi, dengan menggunakan public key, hanya dapat didekripsi oleh secret key yang dimiliki oleh pemilik,
c. PGP menggunakan dua buah kunci, yaitu untuk enkripsi (public key) dan dekripsi (private key).

Keuntungan dari menggunakan PGP (Pretty Good Privacy) sendiri adalah Aman, Fleksibel, dan Gratis.

6. *Kriptografi Pada Password Linux*

Linux telah menyediakan mekanisme password sendiri untuk sistemnya. Password tersebut disimpan dalam suatu file teks yang terletak di /etc/passwd. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Berikut ini adalah contoh isi file /etc/passwd :

```
root:..CETo68esYsA:0:0:root:/root:/bin/bash
bin:jvXHHBGCK7nkg:1:1:bin:/bin:
daemon:i1YD6CckS:2:2:daemon:/sbin:
adm:bj2NcvrnubUqU:3:4:adm:/var/adm:
rms:x9kxv932ckadsf:100:100:Richard M Stallman:/home/rms:/bin/bash
dmr:ZeoW7CaIcQmjhl:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:IK40Bb5NnkAHk:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Keterangan :

Field Pertama	: Nama login
Field Kedua	: Password yang terenkripsi
Field Ketiga	: User ID
Field Keempat	: Group ID
Field Kelima	: Nama sebenarnya
Field Keenam	: Home directory user
Field Ketujuh	: User Shell

Password login yang terdapat pada file /etc/passwd dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut tidak mengurangi kemungkinan password tersebut dibongkar (crack). Karena penyerang (attacker) dapat melakukan dictionary-based attack dengan cara:

- Menyalin file /etc/passwd tersebut

- Menjalankan program-program yang berguna untuk membongkar password, contohnya adalah Crack (www.users.dircon.co.uk/~crypto) dan John the Ripper (www.openwall.com/john/).

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program utility shadow password yang menjadikan file /etc/passwd tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file /etc/shadow yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file /etc/passwd yang telah di-shadow:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
js:x:100:100:Joko Susilo:/home/rms:/bin/bash
```

Dengan demikian, penggunaan shadow password akan mempersulit attacker untuk melakukan dictionary-based attack terhadap file password. Selain menggunakan shadow password beberapa distribusi Linux juga menyertakan program hashing MD5 yang menjadikan password yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu passphrase.

Fitur yang telah disediakan oleh linux tersebut akan tidak aman jika pemakai tidak menggunakan password yang baik. Ada beberapa kriteria yang dapat digunakan untuk membuat password yang baik:

- Gunakan password kombinasi antara huruf kapital dan huruf kecil dan angka / karakter.
- Gunakan password dengan karakter-karakter non-alfabet.
- Jangan menggunakan nama login.
- Jangan menggunakan nama pertama atau akhir.
- Jangan menggunakan nama pasangan atau anak.
- Jangan menggunakan informasi lain seperti nomor telpon, tanggal lahir.

- Jangan menggunakan password yang terdiri dari seluruhnya angka ataupun huruf yang sama.
- Jangan menggunakan kata-kata yang ada di dalam kamus, atau daftar kata lainnya.
- Jangan menggunakan password yang berukuran kurang dari enam karakter.

Contoh distribusi Linux yang telah menyertakan utility shadow password dan MD5 hash adalah : RedHat 6.2, Trustix Secure Linux 1.1.

7. *One Time Password*

One Time Password atau sering disebut OTP dapat digunakan sabagai static password maupun hased password. Apabila user menggunakan password static, maka akan rentan kena serangan. Salah satu bentuk serangan dari jaringan yaitu seseorang yang tidak berkepentingan masuk kedalam jaringan untuk mendapatkan informasi autentikasi,yaitu ID Login dan password pada saat user akan masuk kedalam sistem. Maka sistem OTP dibuat untuk mengatasi serangan semacam itu.

Sistem OTP ini hanya melindungi terhadap serang pasif (Passive attack), bukan melindungi terhadap serangan aktif(active attack). Sistem OTP terdiri dari 2 entitas yaitu generator dan server. Secara umum generator akan menerima masukan berupa passphrase rahasia user dan challenge dari server,yang nantinya akan menghasilkan OTP. Server bertugas mengirimkan challenge yang sesuai dengan user, memverivikasi OTP yang diterima., dan menyimpan OTP yang terbaru. Proses yang dilakukan pada generator OTP dapat dibagi menajdi 3 yaitu proses awal dimana semua input dikombinasikan, proses perhitungan dimana fungsi hash diterapkan beberapa kali, dan proses output dimana OTP 64 bit dikonversi ke bentuk yang mudah dibca manusia.

D. Aktivitas Pembelajaran

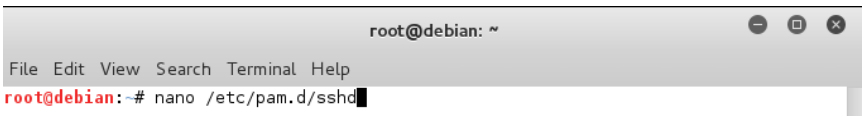
Praktikum ini akan dijelaskan mengenai penggunaan One-time password pada layanan SSH di Server Debian dan contoh kriptografi untuk mengecek file

(biasanya unduhan dari internet) supaya user dapat memastikan bahwa file yang telah diunduh sama dengan yang diterima.

1. Install library one time password dan file binary one time password.

Gambar 8.1 Install Library One Time Password

2. Setting pada file sshd yang terletak pada direktori etc/pam.d

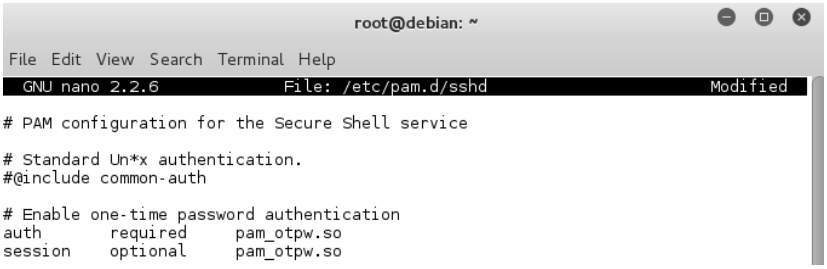


Gambar 8.2 Gambar Setting File sshd

3. Tambahkan # pada baris @include common-auth
4. Tambahkan perintah

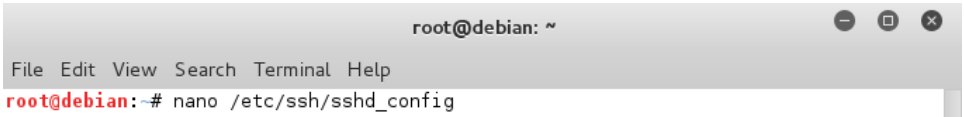
   auth required pam_otpw.so

   session optional pam_otpw.so



Gambar 8.3 Perintah Session Optional

5. Buka file sshd_config pada direktori /etc/ssh



Gambar 8.4 Membuka File sshd_config

6. Jangan ubah parameter dibawah ini

```
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
```

Gambar 8.5 Parameter

7. Ubah parameter PasswordAuthentication menjadi no dan PubkeyAuthentication menjadi yes

```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no

PubkeyAuthentication yes
```

Gambar 8.6 Mengubah Parameter Password Authentication

8. Restart service ssh dengan perintah dibawah

```
root@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# service ssh restart
```

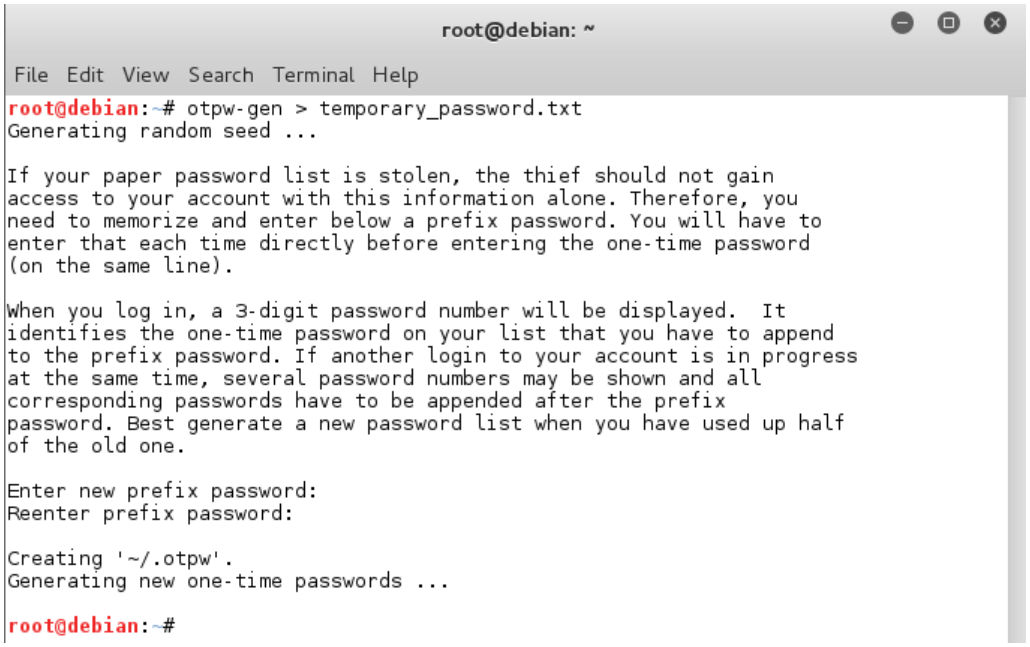
Gambar 8.7 Restart Services

9. Bangkitkan dan simpan one time password ke dalam file temporary_password.txt dengan perintah di bawah ini

```
root@debian: ~
File  Edit  View  Search  Terminal  Help
root@debian:~# otpw-gen > temporary_password.txt
```

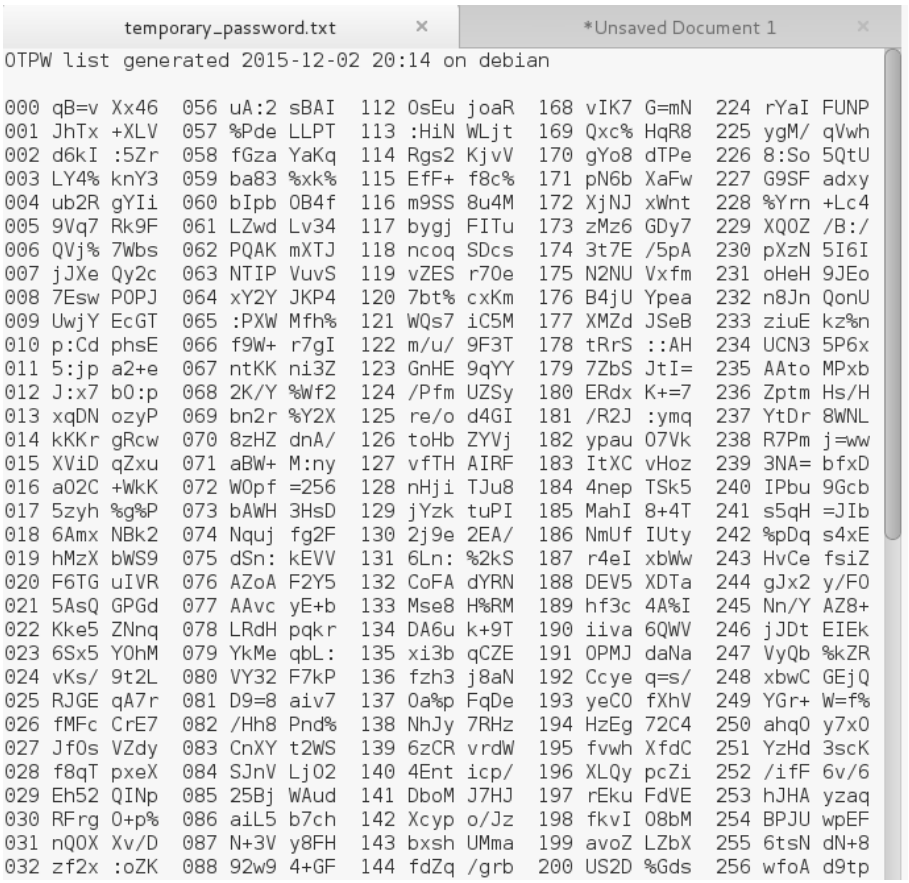
Gambar 8.8 Membangkitkan dan Menyimpan One Time Password

10. Anda akan diminta memasukkan prefix password



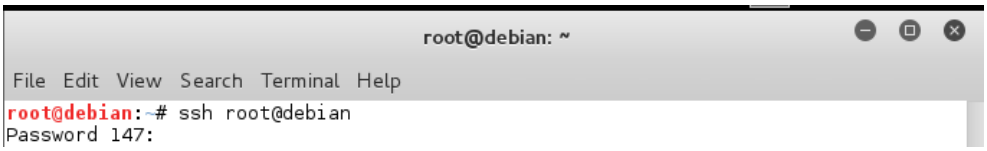
Gambar 8.9 Memasukkan Prefix Password

11. Contoh tampilan otp yg telah dibangkitkan



Gambar 8.10 Tampilan OTP

12. Jika berhasil, maka tampilan awal ssh anda akan berubah menjadi

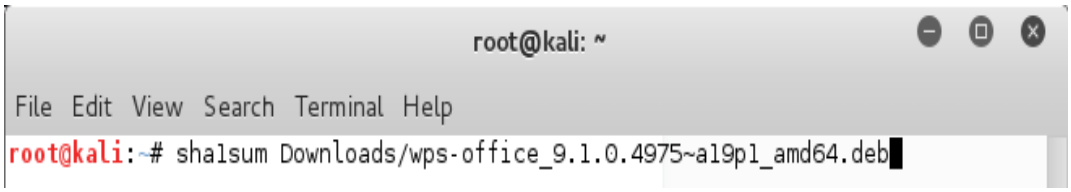


Gambar 8.11 Tampilan SSH

13. Untuk memasukkan otp, anda harus menanmbahkan 3 digit prefix password yang telah dimasukkan pada awal pembangkitan list otp kemudian diikuti oleh password otp yg nomornya diminta pada saat itu (pada contoh password ke 147) tanpa dipisah dengan spasi.
    Misal 032, maka password adalah 111 zf2x:oZK.
14. Keamanan Valid File
    Setiap orang pernah melakukan download file dari internet. Dunia teknologi mendorong kita memberi celah pada penyerang. Salah satunya menggunakan sha1sum, teknik ini merupakan penerapan kriptografi dalam transfer file. Jadi, file asli akan dikenakan proses SHA1 sehingga menghasilkan sebuah chipper text dimana chipper text tersebut digunakan untuk mengecek apakah file yang telah di download mengalamai perubahan atau tidak. Jika hasil sha1sum dari file yang telah didownload pengguna berbeda dari sha1sum yang dicantumkan pada laman web pengembang, maka file tersebut telah tersisipi file lain. Berikut cara mengeceknya menggunakan terminal.
15. Pastikan tempat anda mengunduh file menyediakan chipper text hasil sha1sum dari file tersebut. Berikut contoh dari chipper text suatu file

Gambar 8.12 Memastikan Chipper Text

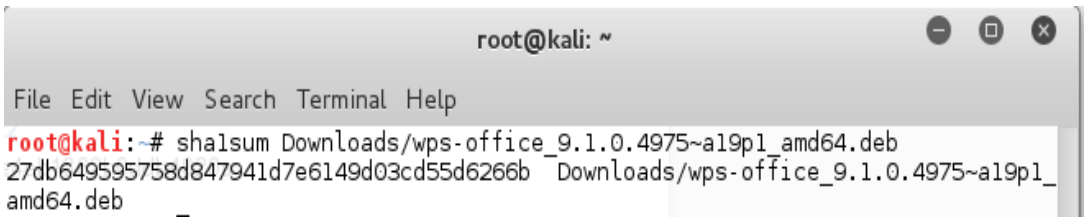
16. Setelah melakukan download file, maka lakukan perintah dibawah ini



Gambar 8.13 Perintah Setelah Download File

17. Berikut hasil dari menjalankan perintah diatas

Dari website, file wps-office_9.1.0.4975~a19p1_amd64.deb memiliki chipper text27db649595758d847941d7e6149d03cd55d6266b Dan hasil dari sha1sum file yang telah didownload adalah 27db649595758d847941d7e6149d03cd55d6266b



Gambar 8.14 Hasil Perintah

Dalam kegiatan ini peserta diklat akan melakukan analisis terhadap sistem keamanan. Kegiatan yang dilakukan adalah membentuk kelompok diskusi. Setiap kelompok terdiri dari 3-4 orang, kemudian membaca seluruh langkah di bawah ini kemudian lakukan dengan cermat dan teliti.

1. Membaca dan mengamati uraian materi pada kegiatan belajar di atas.
2. Menanyakan serta mendiskusikan kepada kelompok kecil tersebut berkaitan dengan materi pembelajaran.
3. Mengumpulkan informasi dan mencoba mencari informasi berkaitan dengan materi yang relevan melalui sumber belajar (buku, teman sebaya, internet).
4. Mengasosiasi atau menalar berkaitan dengan materi yang dipelajari.
5. Mengkomunikasikan serta mendiskusikan hasilnya dalam kelompok dan membuat kesimpulan.
6. Membuat laporan aktifitas pembelajaran dan mengkomunikasikan hasil laporan dan pembahasan tersebut dengan tutor.

E. Latihan

1. Paket apa yang harus diinstall untuk mengaktifkan OTP?

……
……
……
……
……

2. Bagaimana cara membangkitkan OTP dan menyimpannya dalam txt?

……
……
……
……
……

3. Bagaimanakah cara membaca OTP?

……
……
……
……

……

F. Rangkuman

Kriptografi bertujuan untuk menjaga kerahasiaan informasi sehingga informasi tersebut tidak dapat diketahui oleh pihak tertentu. Dalam metode Kriptografi, suatu pesan (plain text) harus melalui proses enkripsi terlebih dulu menjadi bentuk yang tidak berarti (cipher text) sebelum dikirimkan ke penerima. Algoritma simetris adalah algoritma yang konvensional yang di mana kunci enkripsi dan dekripsi menggunakan algoritma yang sama. Contoh dari algoritma simetris adalah DES (Data Encryption Standart). Sedangkan untuk algoritma asimetris sendiri adalah algoritma dalam kriptografi yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Kunci yang digunakan untuk enkripsi disebut private key dan kunci untuk melakukan dekripsi disebut dengan public key. Contoh dari alogritma asimetris adalah RSA.

G. Umpan Balik

Beberapa umpan balik yang harus peserta diklat jawab adalah sebagai berikut :

1. Apakah saudara sudah memahami tentang konsep tata cara penerapan pengamanan komunikasi data menggunakan teknik kriptografi dan berapa prosen pencapaian kompetensinya?
2. Apakah saudara sudah memahami perintah untuk menerapkan one time password pada layanan SSH yang berhubungan dengan proses serta berapa prosen pencapaian kompetensinya?
3. Apakah saudara sudah memahami cara input otp dengan kombinasi passwordnya dan berapa prosen pencapaian kompetensinya?

H. Kunci Jawaban

1. Libpam-otpw otpw-bin adalah paket yang harus diinstall untuk mengaktifkan OTP.
2. Bangkitkan dan simpan one time password ke dalam file temporary_password.txt
3. Cara membaca OTP adalah dengan cara input kombinasi [Prefix][Kode dari Temporary_Password.txt].