

Case study tugas keamanan jaringan:

1. PT. Cyber script ingin membengun server web dengan centos diperusahaanya.
2. PT. Cyber script ingin server aman dari serangan cracker
3. Aplikasi dalam server yang akan dibuka adalah: Web Server, FTP Server, Open SSH Server
4. Pada aplikasi Open SSH, portnya dicustom menjadi 1995
5. Server beralamat pada IP 10.10.10.1/29
6. Yang dapat mengakses SSH hanya IP 10.10.10.3
7. PT. Cyber menyewa jasa konsulting untuk menyelesaikan project ini

IPTABLES

#BASIC RULES

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A INPUT -m state --state INVALID -j DROP
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -p icmp -m limit --limit 10/sec -j ACCEPT
```

##FTP

```
iptables -A INPUT -m state --state NEW -p tcp --dport 21 -j ACCEPT
```

##SSH

```
iptables -A INPUT -s 192.168.56.1 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

##WEB

```
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
```

##LOOPBACK

```
iptables -A INPUT -s 127.0.0.1 -m state --state NEW -p tcp --dport 3306 -j ACCEPT
```

##DROP ALL

```
iptables -A INPUT -j DROP
```

```
iptables -A FORWARD -m state --state INVALID -j DROP
```

```
iptables -A OUTPUT -m state --state INVALID -j DROP
```

```
---- note kill firewall bawaan centos file: /etc/sysconfig/iptables
```

```
$ systemctl stop firewalld
```

```
$ systemctl mask firewalld
```

```
$ yum install iptables-services
```

```
$ systemctl enable iptables
```

```
$ systemctl enable ip6tables
```

NMAP MOST COMMAND

```
nmap -p 1-65535 localhost
```

```
nmap -p 80,443 8.8.8.8
```

```
nmap 1.1.1.1 8.8.8.8
```

```
nmap -p 8.8.8.0/28
```

```
nmap --top-ports 20 192.168.1.106
```

```
nmap -iL list.txt === list.txt as host list ip or domain
```

```
nmap -oN output.txt securitytrails.com == output file
```

```
nmap -p 80 -n 8.8.8.8 (disable dns res)
```

```
nmap -A -T4 cloudflare.com ( os dll)
```

```
nmap -sV localhost (service daemon)
```

```
nmap -sT 192.168.1.1 (tcp/udp)
```

```
nmap -Pn --script vuln 192.168.1.105
```

Selamat mengerjakan, All is Well--