

Nama : Ferza Reyaldi
NIM : 09021281924060
Mata Kuliah : Keamanan Jaringan Komputer

Tugas Pertemuan 5 (Pertemuan 15)

Carilah arti dari berbagai jenis attack yang dicantumkan dalam slide ini

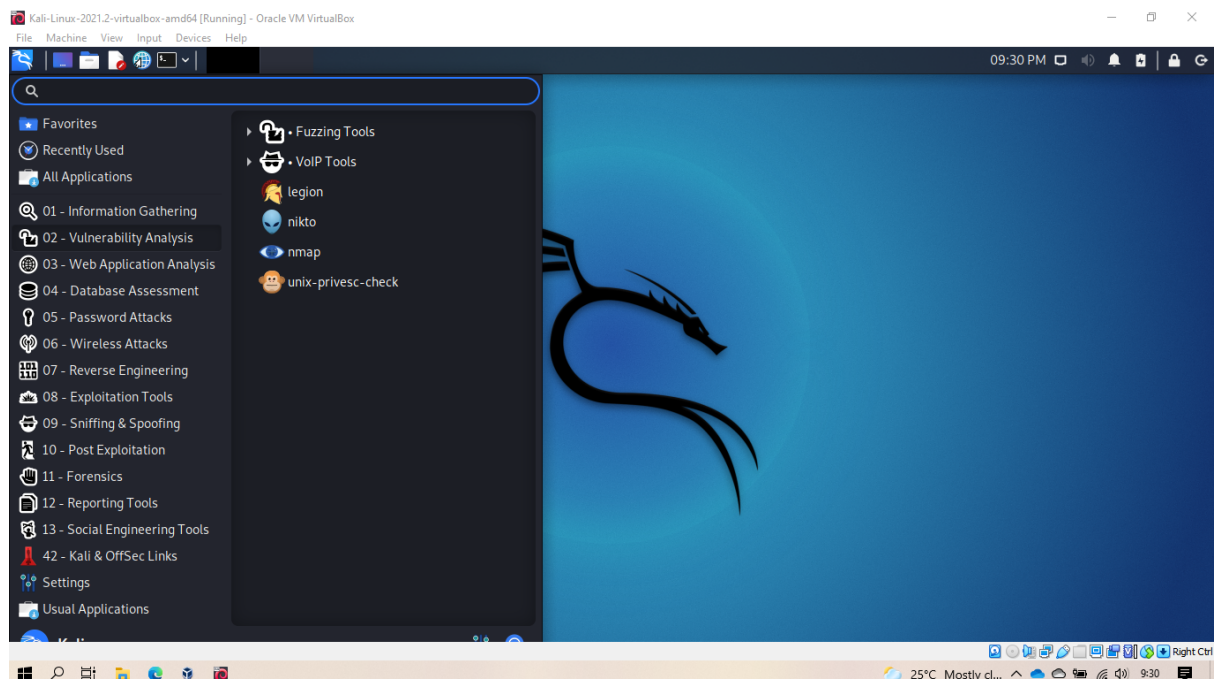
Jawab:

- **Passive attack** Merupakan threat terhadap aspek Confidentiality, passive attack tidak menyebabkan kerusakan pada sistem namun attacker hanya membaca dan menganalisa informasi. Contohnya: Traffic analysis, Eavesdropping, dan Monitoring.
- **Active attack** merupakan threat terhadap aspek Integrity, Authentication, dan Availability. Attacker berusaha mengambil alih sistem sehingga Active attack cenderung menyebabkan kerusakan pada sistem. Contohnya: Spoofing, Modification, Fabrication, Denial of services, Sinkhole, dan Sybil.
- **Advanced attack** adalah pengembangan dari active attack. Advanced attack banyak diimplementasikan pada routing, seperti memanipulasi tabel routing, memunculkan routing loop, mendupikasi packet data, dan sebagainya. Contohnya: Black hole attack, Rushing attack, Replay attack, Byzantine attack, dan Location disclosure attack.

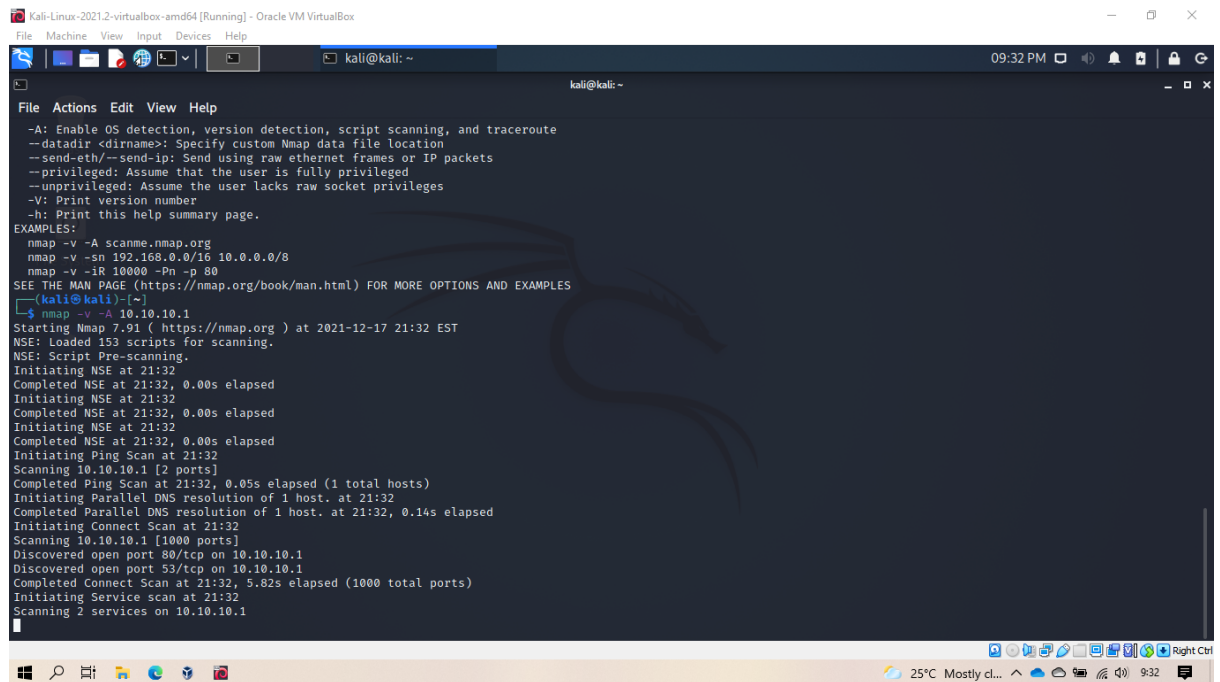
Lakukan passive attack menggunakan port scanner yaitu nmap ke komputer target. IP Address komputer target: 10.10.10.1

Jawab:

- 1) Klik menu start kali linux > 02 - Vulnerability Analysis > nmap



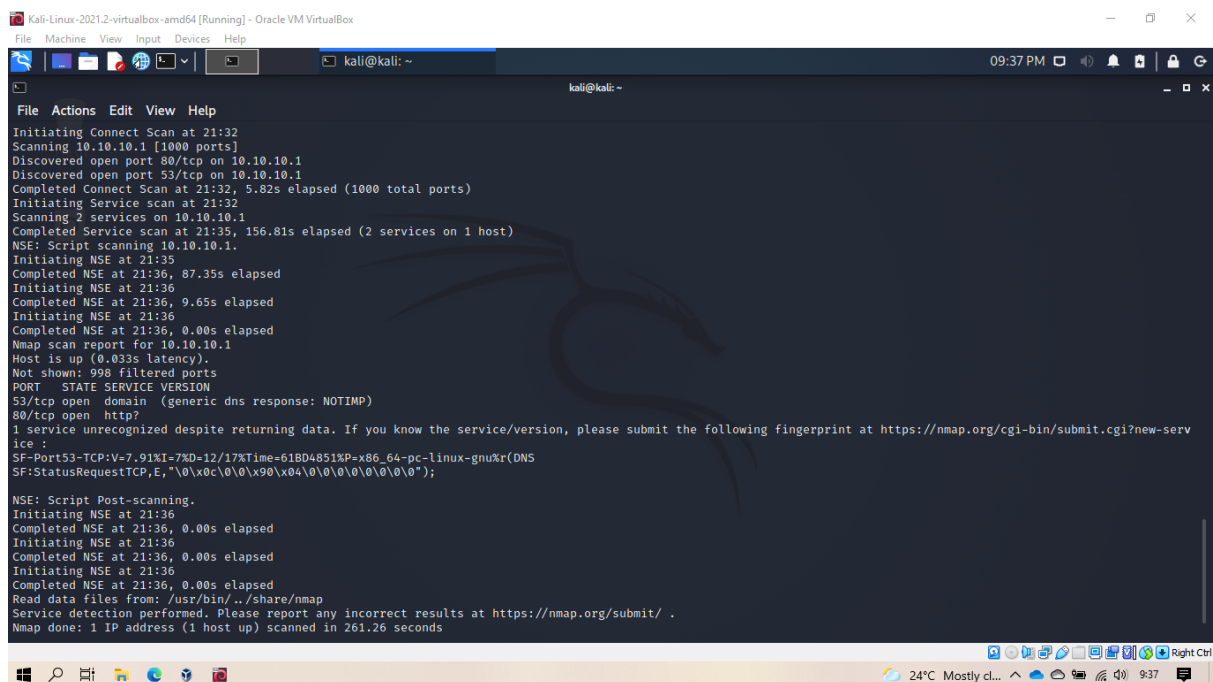
2) Jalankan perintah nmap -v -A 10.10.10.1



```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
09:32 PM
File Actions Edit View Help
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 100000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali:~$ nmap -v -A 10.10.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-17 21:32 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating Ping Scan at 21:32
Scanning 10.10.10.1 [2 ports]
Completed Ping Scan at 21:32, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:32
Completed Parallel DNS resolution of 1 host. at 21:32, 0.14s elapsed
Initiating Connect Scan at 21:32
Scanning 10.10.10.1 [1000 ports]
Discovered open port 80/tcp on 10.10.10.1
Discovered open port 53/tcp on 10.10.10.1
Completed Connect Scan at 21:32, 5.82s elapsed (1000 total ports)
Initiating Service scan at 21:32
Scanning 2 services on 10.10.10.1
```

Hasil dan Analisis Singkat

Jawab:



```
Initiating Connect Scan at 21:32
Scanning 10.10.10.1 [1000 ports]
Discovered open port 80/tcp on 10.10.10.1
Discovered open port 53/tcp on 10.10.10.1
Completed Connect Scan at 21:32, 5.82s elapsed (1000 total ports)
Initiating Service scan at 21:32
Scanning 2 services on 10.10.10.1
Completed Service scan at 21:35, 156.81s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.1.
Initiating NSE at 21:35
Completed NSE at 21:36, 87.35s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 9.65s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Nmap scan report for 10.10.10.1
Host is up (0.033s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain (generic dns response: NOTIMP)
80/tcp    open  http
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.91I=7&O=12/17&T=61BD4851P=x86_64-pc-linux-gnu&R(DNS
SF-StatusRequestTCP,E,"0x0c000x90x040000000000");
NSE: Script Post-scanning.
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Initiating NSE at 21:36
Completed NSE at 21:36, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 261.26 seconds
```

Berdasarkan hasil yang didapatkan dari port scanner nmap, beberapa poin yang dapat disimpulkan:

- Scan dilakukan pada 2 server dan 1 host.
- Nmap melakukan scanning pada 1 IP address (10.10.10.1) selama 261.26 detik.
- Terdapat 1 layanan tidak dikenali meskipun mengembalikan data.
- 53/tcp merupakan open domain dengan generic dns response: NOTIMP
- 80/tcp merupakan open http.

Kemudian dilakukan submit fingerprint pada <https://nmap.org/cgi-bin/submit.cgi> dengan memilih:

Submit a Fingerprint/Correction! _____

Submit a to the database.

Keluaran yang dihasilkan sebagai berikut.

Fingerprint _____

Paste the fingerprint output from Nmap here:

```
SF--Port53--TCP:V=7.91%I=7%O=12/17%Time=61804851%P=x86_64-pc-linux-gnu%r(DNS
SF:StatusRequestTCP,E,"\\0\\x0c\\0\\0\\x90\\x04\\0\\0\\0\\0\\0\\0");
```

Fingerprint looks good!