LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Footprinting & Scanning

DI SUSUN OLEH

Nama	: M Abdul Aziz
NIM	: 21/474516/SV/18951
Hari, Tanggal	: Selasa, 28 Maret 2023
Kelas	: RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

Praktikum Keamanan Informasi 1
Footprinting & Scanning

I. Tujuan

- Mengidentifikasi kerentanan dan pengungkapan informasi menggunakan Metasploit *Framework.*
- Ekstrak informasi akurat tentang jaringan menggunakan Metasploit Framework.
- Melakukan teknik pemindaian jaringan menggunakan Nmap.

II. Latar Belakang

Footprinting adalah langkah awal sebelum penyerang (*attacker*) melakukan penyerangan, yakni mengumpulkan informasi mengenai target, yang tujuannya adalah untuk merangkai apa yang ditemukan (*blueprint* dari suatu jaringan), sehingga ia mendapatkan gambaran yang jelas tentang sistem keamanan yang dimiliki target. Informasi yang ditampilkan dalam kegiatan ini, dapat berupa sejarah perusahaan, nama domain, VPN (*Virtual Private Network*) point, nomor telepon, nama orang-orang yang terkait di dalamnya, alamat email perusahaan, hubungan dengan perusahaan lain, lokasi perusahaan, topologi peta dan informasi penting lainnya.

Tahapan pertama pada fase peretasan adalah melakukan footprinting atau pengintaian. Footprinting mengumpulkan seluruh informasi yang berguna mengenai target penyerangan. Pada fase ini dilakukan beberapa hal yaitu:

1. Mengumpulkan informasi dasar tentang target dan jaringan ini
2. Menentukan system operasi yang digunakan, platfroms yang dijalankan,versi web server dan lainnya.
3. Dilakukan dengan teknik seperti WHOIS,DNS,jaringan dan organisasi query.
4. Cari kerentanan dan exploitasi untuk meluncurkan serangan.

Tujuan dari footprinting yaitu untuk mengumpulkan informasi dari target bisa melalui jaringan internet.

Scanning adalah tahap untuk mengetahui IP dari komputer target, Sistem Operasi komputer target, layanan apa saja yang tersedia dan celah keamanan apa saja yang ada pada komputer target.

Sebuah port dapat dianalogikan seperti sebuah pintu yang kita gunakan untuk keluar masuk rumah. Pada komputer, port juga digunakan untuk keluar masuk data. Hanya saja di komputer setiap jenis komunikasi data diberi port yang berbeda. Misalnya untuk komunikasi web melalui port 80, untuk SSH lewat port 22, ftp lewat port 21 dll. Setiap port yang terbuka (open) dapat menjadi jalan masuk ke komputer target. Hanya saja anda harus mencari cara/tools yang tepat untuk bisa masuk ke port tersebut.

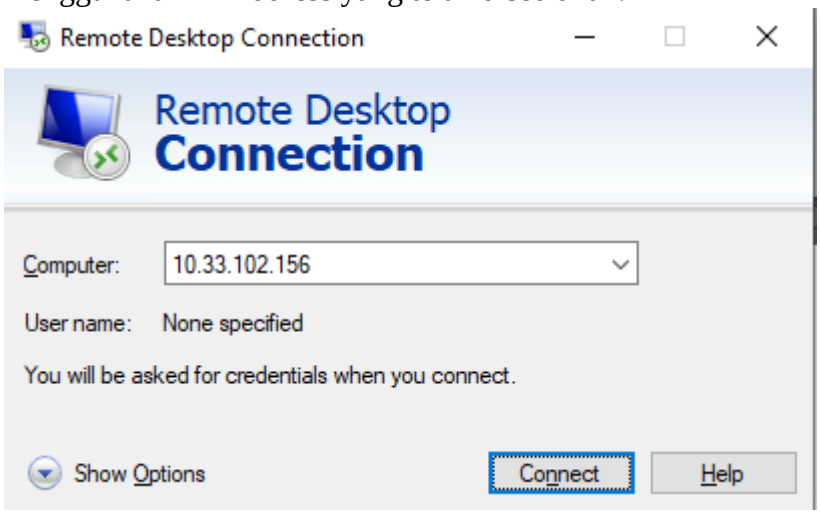
III. Alat & Bahan

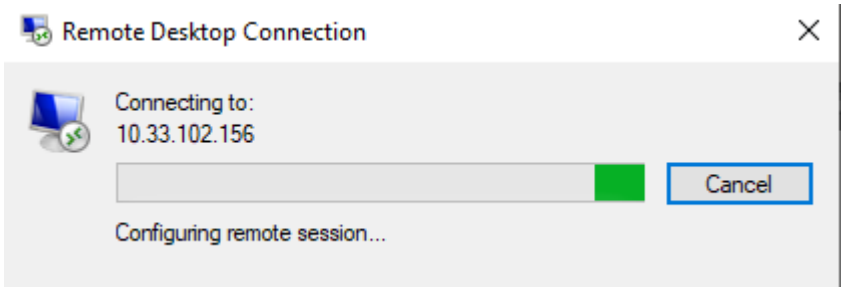
- Software Remote Desktop Connection
- Kali Linux
- Laptop/PC
- Koneksi Internet

IV. Instruksi Kerja

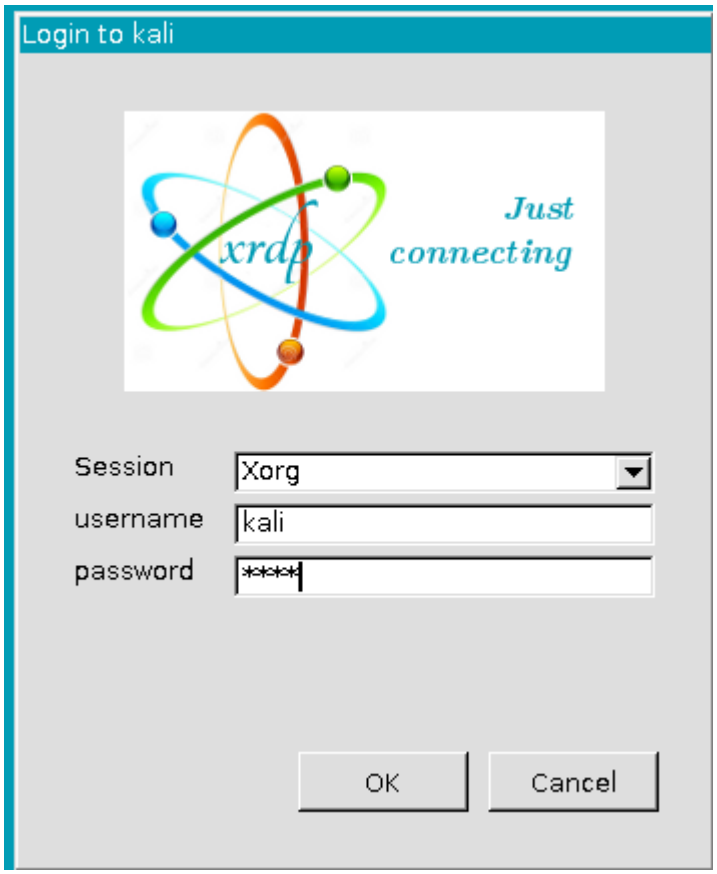
A. Footprinting & Reconnaissance

1. Jalankan Kali Linux dengan *Remote Dekstop Connection* di Windows menggunakan IP Address yang telah disediakan.

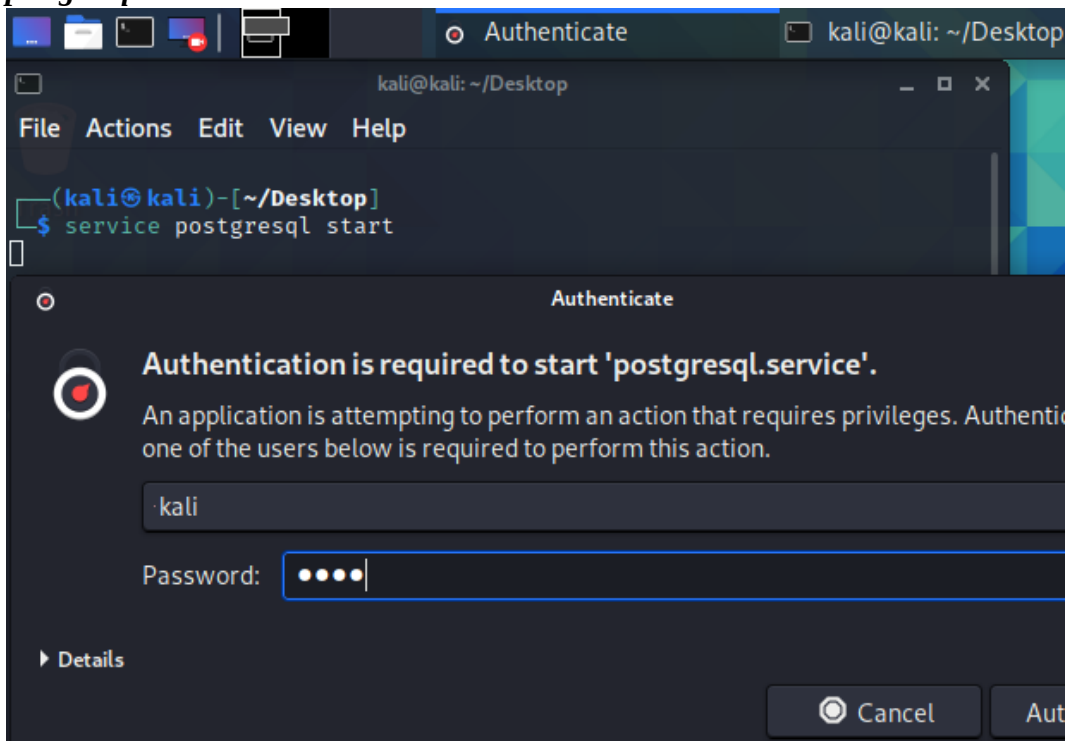




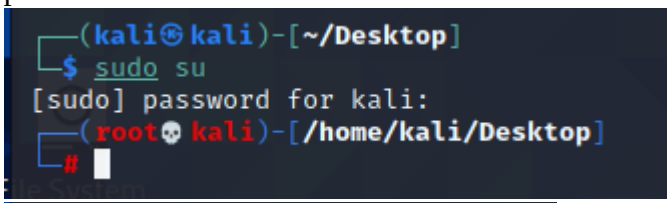
2. Masuk dengan user: kali & password: kali

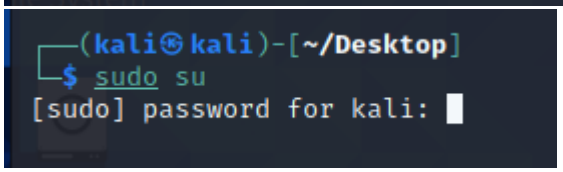


3. Setelah masuk ke Dekstop Kali Linux, jalankan terminal dan ketik ***service postgresql start*** lalu tekan enter



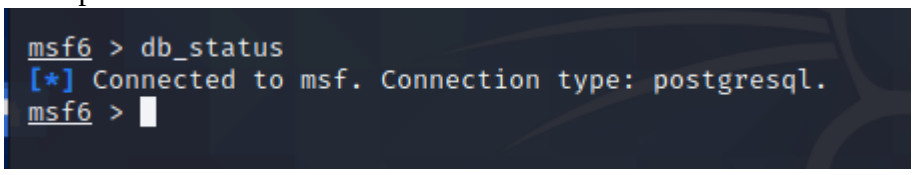
4. Masuk sebagai *root* dengan mengetikkan ***sudo su*** kemudian masukan password: kali.





5. Jalankan Metasploit Framework dengan mengetikkan ***msfconsole*.**

6. Ketikkan ***db_status*** untuk memastikan database sudah terhubung dengan metasploit



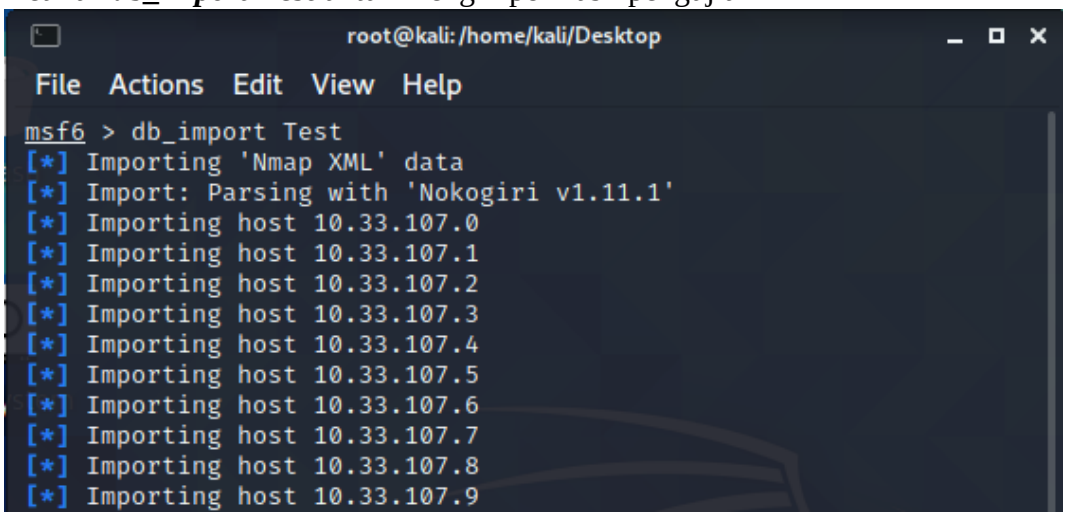
7. Ketik ***nmap -Pn -sS -A -oX Test 10.33.107.0/24*** dan tekan Enter. Dibutuhkan sekitar 10 menit bagi namp untuk menyelesaikan pemindaian subnet.

```
msf6 > nmap -Pn -sS -A -oX Test 10.33.107.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.33.107.0/24

Host discovery disabled (-Pn). All addresses will be marked '
up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-28 14:15 C
DT
```

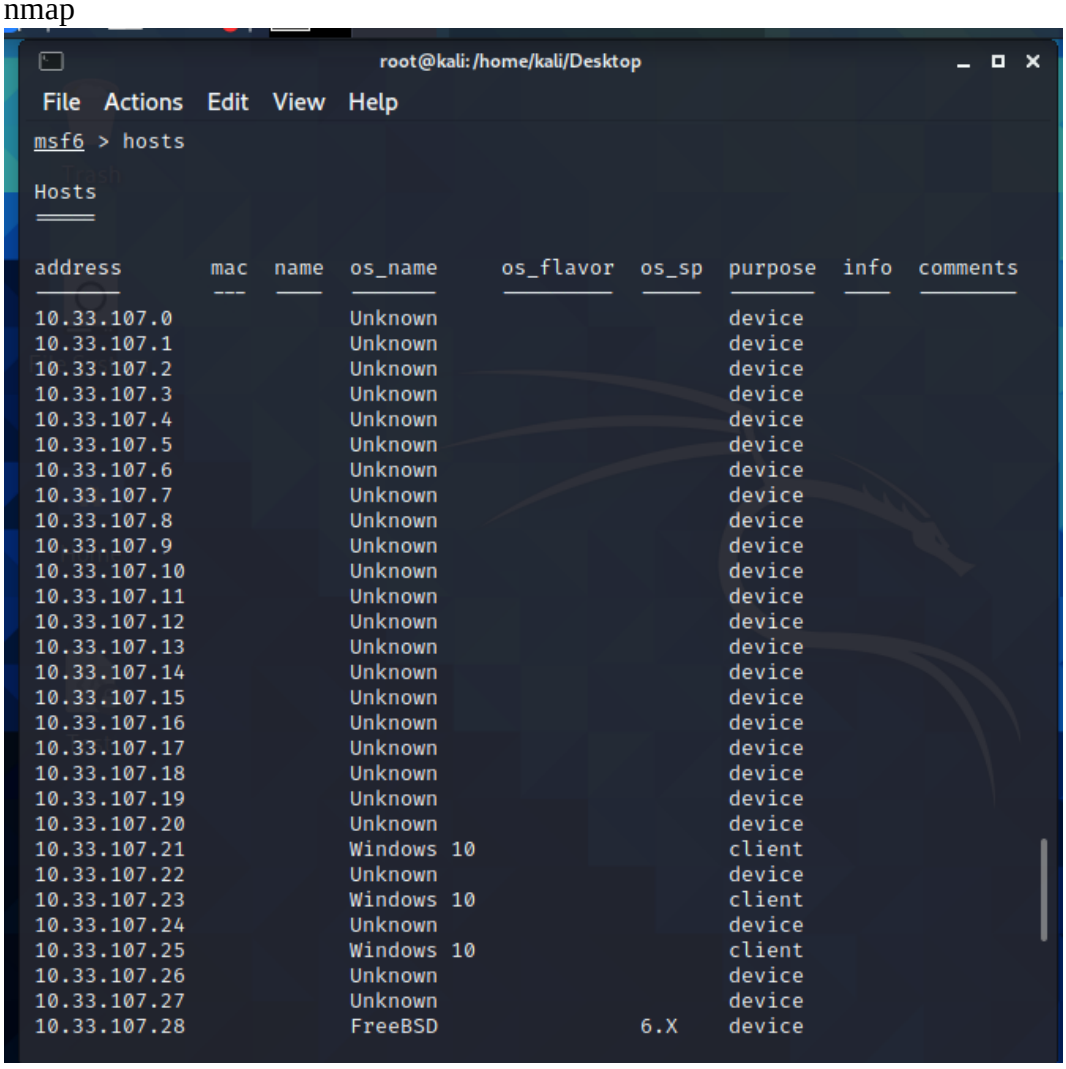
8. Setelah selesai, maka akan muncul pesan **Nmap done** dengan menampilkan jumlah total host yang aktif di subnet yang telah di scan

```
Nmap scan report for 10.33.107.40
Host is up (0.0010s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
Warning: OSScan results may be unreliable because we could not fin
d at least 1 open and 1 closed port
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (95%), Microsoft Windows 10|2
008 (93%), Juniper JUNOS 12.X|10.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe
:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_
server_2008 cpe:/o:freebsd:freebsd:6.3 cpe:/o:juniper:junos:12.1 c
pe:/o:juniper:junos:10
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Window
s 10 (93%), Microsoft Windows Server 2008 or 2008 Beta 3 (91%), Mi
crosoft Windows Server 2008 SP1 (87%), m0n0wall 1.3b11 - 1.3b15 (F
reeBSD 6.3) (86%), Juniper SRX-series firewall (JUNOS 12.1) (86%),
 Microsoft Windows 10 1511 - 1607 (86%), Juniper SRX100-series or
SRX200-series firewall (JUNOS 10.4 - 12.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 3306/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.33.107.21
2   1.15 ms 10.33.107.40

Nmap scan report for 10.33.107.41
Host is up (0.0023s latency).
```

9. Ketikan ***db_import*** **Test** untuk mengimpor hasil pengujian



10. Ketik ***hosts*** untuk menampilkan detail host yang telah dikumpulkan oleh nmap



11. Ketik ***db_nmap -sS -A 10.33.107.84***

```
msf6 > db_nmap -sS -A 10.33.107.84
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-30 01:46 CDT
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 11.80 seconds
msf6 >
```

12. Nmap memindai mesin dan memberi Anda detail layanan yang berjalan di mesin. Ini adalah bagaimana Anda dapat menemukan layanan pada masing-masing mesin.
13. Untuk mendapatkan informasi layanan dari semua komputer aktif di jenis subnet ketik ***services*** dan tekan Enter.

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help
msf6 > services
Services
========

host           port  proto  name            state  info
----           ----  -----  ----            -----  ----
10.33.107.21   135   tcp    msrpc           open   Microsoft Windows RPC
10.33.107.21   139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
10.33.107.21   445   tcp    microsoft-ds    open   Windows 10 Pro 15063 microsoft-ds workgro
up: WORKGROUP
10.33.107.21   1521  tcp    oracle-tns      open   Oracle TNS listener 1.5.0.0.0 unauthorize
d
10.33.107.21   2030  tcp    device2         open
10.33.107.21   3306  tcp    mysql           open   MySQL unauthorized
10.33.107.21   5357  tcp    http            open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.33.107.23   135   tcp    msrpc           open   Microsoft Windows RPC
10.33.107.23   139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
```

14. Ketik ***use scanner/smb/smb_version*** dan tekan Enter untuk memuat modul pemindai SMB.

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) >
```

15. Kemudian ketik ***show options*** dan tekan Enter untuk menampilkan opsi konfigurasi yang terkait dengan modul.

```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) >
```

16. Ketik ***set RHOSTS 10.33.107.8-16*** and press Enter. Kemudian ketik set ***THREADS 100*** dan tekan Enter. Untuk menampilkan opsi konfigurasi yang terkait dengan modul ketik run dan tekan Enter.

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 10.33.107.27-37
RHOST ⇒ 10.33.107.27-37
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS ⇒ 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.33.107.35:445      - SMB Detected (versions:1, 2, 3) (preferr
ed dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption c
apabilities:AES-128-CCM) (signatures:optional) (uptime:3d 6h 19m 55s
) (guid:{1b739ba4-340e-4722-a6cb-6df3cb894295}) (authentication doma
in:DESKTOP-AIVUJRL)
[+] 10.33.107.35:445      -   Host is running Windows 10 Pro (build:
15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGROUP)
[*] 10.33.107.27-37:      - Scanned  3 of 11 hosts (27% complete)
[*] 10.33.107.27-37:      - Scanned  3 of 11 hosts (27% complete)
[*] 10.33.107.27-37:      - Scanned  6 of 11 hosts (54% complete)
[*] 10.33.107.27-37:      - Scanned  6 of 11 hosts (54% complete)
[*] 10.33.107.27-37:      - Scanned  6 of 11 hosts (54% complete)
[*] 10.33.107.27-37:      - Scanned  9 of 11 hosts (81% complete)
[*] 10.33.107.27-37:      - Scanned 10 of 11 hosts (90% complete)
[*] 10.33.107.27-37:      - Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

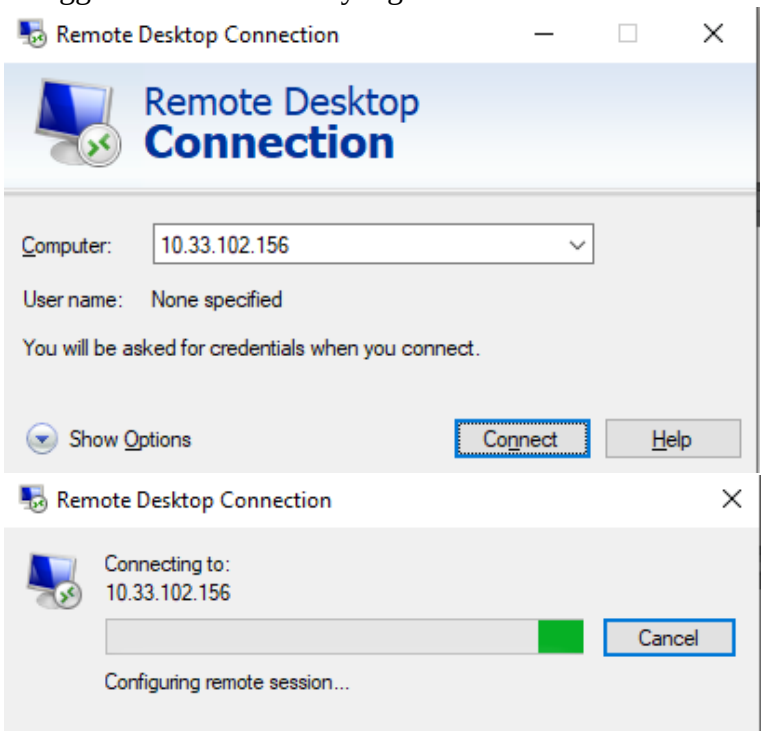
17. Ketikkan kembali ***hosts*** untuk menampilkan ***os_flavor***

```
msf6 > hosts

Hosts
=====

address       mac  name  os_name     os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------     ---------  -----  -------  ----  --------
10.33.107.0                Unknown                       device
10.33.107.1                Unknown                       device
10.33.107.2                Unknown                       device
10.33.107.3                Unknown                       device
10.33.107.4                Unknown                       device
10.33.107.5                Unknown                       device
10.33.107.6                Unknown                       device
10.33.107.7                Unknown                       device
10.33.107.8                Unknown                       device
```

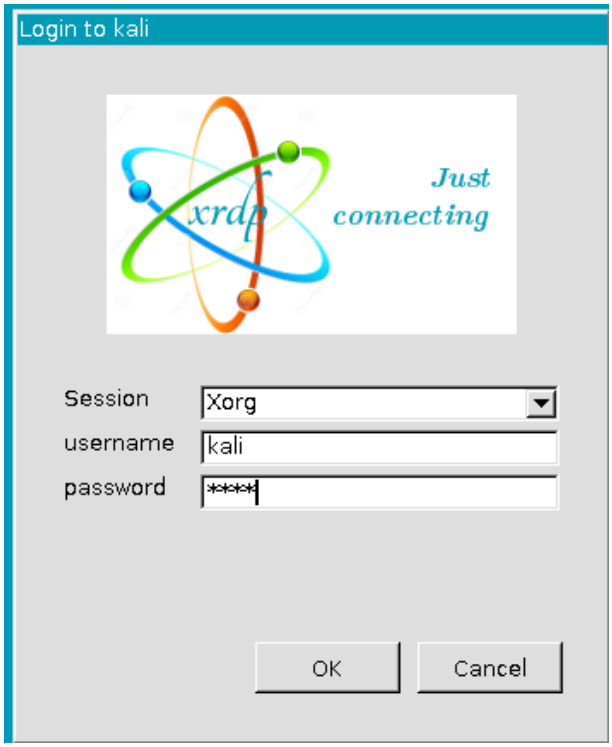
- Di lab ini Anda telah mempelajari cara mengekstrak informasi yang akurat tentang jaringan menggunakan Metasploit Framework.
- Apa sistem operasi yang diinstal di domain 10.33.107.9-15?
  Sistem operasi yang diinstall di domain 10.33.107.9-15 dari hasil pengujian pada praktikum ini tidak diketahui. Hal ini dapat terjadi karena adanya kemungkinan *host* mati ataupun tidak adanya host yang terhubung menggunakan alamat IP tersebut.
- Versi Paket Layanan mana yang diinstal di mesin 10.33.107.44?
  Versi paket layanan yang diinstall di mesin 10.33.107.44 tidak ditemukan.

B. Teknik Scanning

1. Jalankan Kali Linux dengan *Remote Dekstop Connection* di Windows menggunakan IP Address yang telah disediakan.



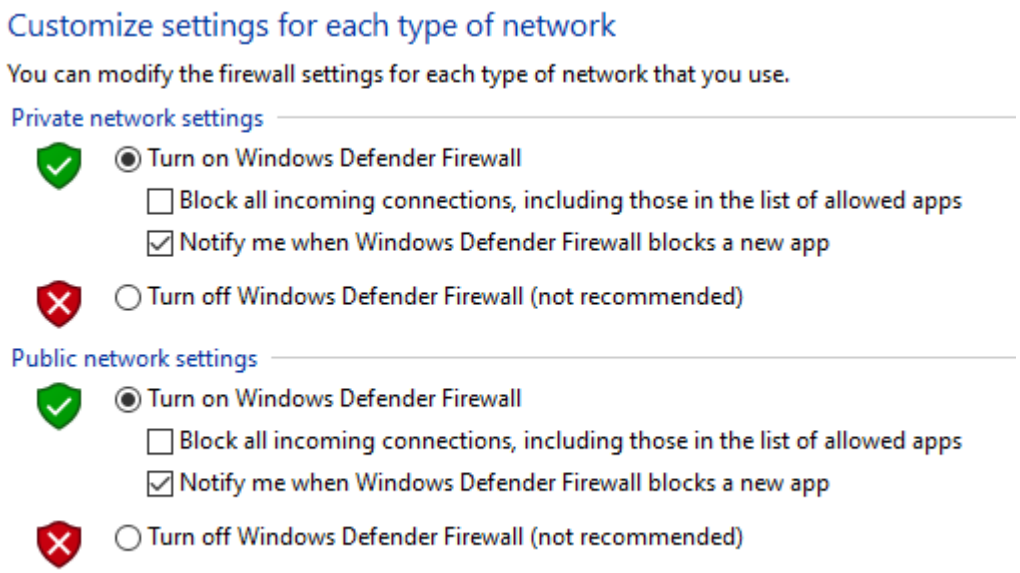
2. Masuk dengan user: kali & password: kali



3. Setelah masuk ke Dekstop Kali Linux, buka terminal dan jalankan nmap dengan mengetikkan perintah ***nmap -sT -T3 -A 10.33.194.185*** (IP PC windows) dan tekan Enter untuk melakukan TCP Connect Scan pada Windows machine.

```
└─# nmap -sT -T3 -A 10.33.194.185
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-30 02:29 CDT
Nmap scan report for 10.33.194.185
Host is up (0.0034s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
808/tcp  open  mc-nmf          .NET Message Framing
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

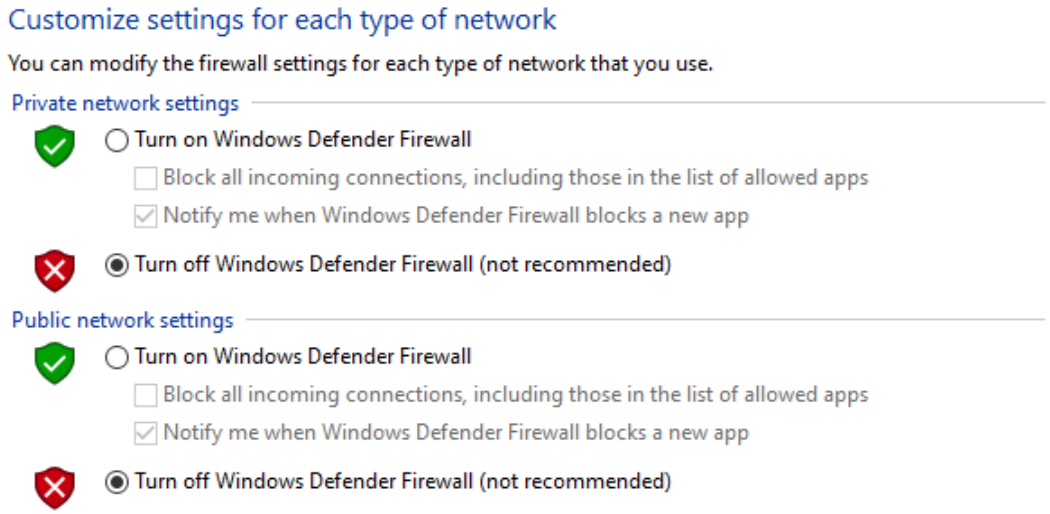
4. Beralih ke mesin Windows, masuk ke mesin, dan aktifkan Windows Firewall.



5. Beralih kembali ke mesin Kali Linux. Ketik ***nmap -sX -T4 10.33.194.185*** di command prompt dan tekan Enter untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Ini menampilkan hasilnya seperti yang ditunjukkan pada tangkapan layar. Hasil Nmap menunjukkan bahwa semua port dibuka/difilter yang berarti firewall dikonfigurasi pada komputer target.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap -sX -T4 10.33.194.185
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-30 02:38 CDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.13 seconds
```

6. Beralih ke mesin Windows dan matikan Windows Firewall.



7. Beralih kembali ke mesin Kali Linux. Ketik ***nmap -sA -v -T4 10.33.194.185*** di terminal baris perintah. Ini memulai ACK Scan dan menampilkan disposisi port, seperti yang ditunjukkan pada tangkapan layar.

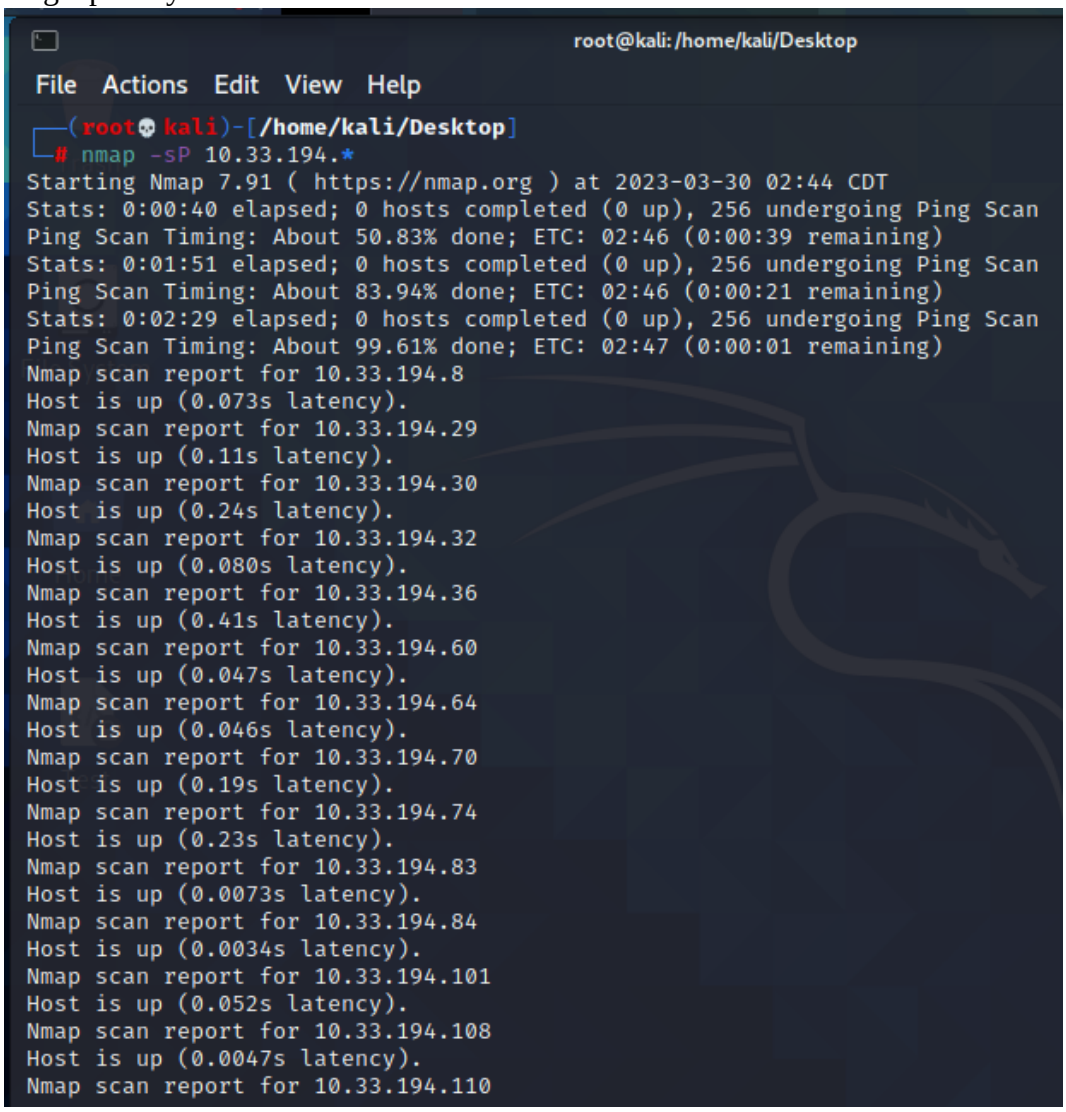
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nmap -sA -v -T4 10.33.194.185
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-30 02:36 CDT
Initiating Ping Scan at 02:36
Scanning 10.33.194.185 [4 ports]
Completed Ping Scan at 02:36, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:36
Completed Parallel DNS resolution of 1 host. at 02:36, 0.00s elapsed
Initiating ACK Scan at 02:36
Scanning 10.33.194.185 [1000 ports]
Completed ACK Scan at 02:36, 0.19s elapsed (1000 total ports)
Nmap scan report for 10.33.194.185
Host is up (0.010s latency).
All 1000 scanned ports on 10.33.194.185 are unfiltered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
           Raw packets sent: 1004 (40.152KB) | Rcvd: 1068 (42.708KB)
```

8. Ketik perintah ***nmap -Pn -p 80 -sI 10.33.194.185 10.33.194.147***, dan tekan Enter.

```
msf6 > nmap -Pn -p 80 -sI 10.33.194.185 10.33.194.147
[*] exec: nmap -Pn -p 80 -sI 10.33.194.185 10.33.194.147

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times w
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-29 12:33 CDT
Idle scan zombie 10.33.194.185 (10.33.194.185) port 80 cannot be used because it
QUITTING!
msf6 >
```

9. Sekarang alih-alih memeriksa sistem individual, kita akan memeriksa semua sistem yang hidup di jaringan dengan melakukan sapuan ping. Di jendela terminal, ketik ***nmap -sP 10.33.194.**** dan tekan Enter untuk memindai seluruh subnet untuk sistem yang hidup. Nmap memindai subnet

dan menampilkan daftar sistem yang hidup seperti yang ditunjukkan pada tangkapan layar.



V. Pembahasan

Pada praktikum ini, mahasiswa akan melakukan identifikasi terhadap kerentanan dan pengungkapan informasi menggunakan Metasploit Framework. Metasploit Framework sendiri merupakan sebuah penetration tool yang cukup powerfull untuk melakukan penestrasi kedalam sebuah system. Metasploit termasuk sebuah framework penetrasi jaringan komputer yang free dan open source, yang diciptakan oleh H.D. Moore pada tahun 2003 dan kini diakuisisi oleh Rapid7. Selain itu, mahasiswa juga akan melakukan *scanning* menggunakan Nmap.

Dalam praktikum ini menggunakan VM dengan OS Kali Linux yang merupakan sistem operasi yang mendukung Metasploit Framework. Untuk menjalankan Metasploit Framework pada Kali Linux bisa dilakukan dengan mengetikkan perintah *msfconsole*. Setelah itu perlu juga memastikan bahwa database telah terhubung ke Metasploit, sehingga *scanning* dapat dijalankan. Pada praktikum ini, *scanning* dilakukan terhadap subnet untuk mengetahui jumlah total *host* yang aktif di subnet. Saat *scanning* selesai, maka perlu melakukan impor hasil pengujian dan melakukan pengecekan terhadap host dan detail informasi yang telah dikumpulkan oleh Nmap. Pada praktikum ini berfokus pada informasi *os_flavor* dimana setelah ditampilkan, Nmap belum mengumpulkan informasi tersebut.

Selanjutnya adalah *scanning* SYN serta menyimpan hasilnya ke dalam *database* agar. Nmap memindai mesin dan memberikan informasi detail layanan yang berjalan di mesin, sehingga pengguna dapat menemukan layanan yang berjalan pada setiap mesin yang berhasil dipindai. Untuk mendapatkan informasi layanan dari semua komputer aktif di jenis subnet, kita dapat menggunakan perintah *services*.

Selanjutnya adalah pemindaian SMB. SMB (*Server Message Block*) sendiri merupakan protokol jaringan lapisan aplikasi yang memfasilitasi komunikasi jaringan sambil memberikan akses bersama ke file klien, printer dan port serial. Setelah termuat, cek opsi konfigurasi yang terkait dengan modul dengan perintah show options. Untuk mengeksploitasi sebuah modul, pada kasus ini adalah modul pemindai SMB kita perlu menggunakan set RHOSTS dan diatur ke target IP Address tertentu, pada praktikum ini yaitu 10.33.107.8-16. Dalam hal ini, fitur RHOSTS dilengkapi dengan THREADS dimana THREADS yang digunakan adalah 100. Untuk menampilkan opsi konfigurasi yang terkait dengan modul dapat menggunakan perintah *run*. Lalu coba kembali perintah *hosts* dan dapat dilihat pada Instruksi Kerja bagian Footprinting & Reconnaissance langkah 18 bahwa informasi terkait *os_flavor* telah dikumpulkan.

Pengujian berikutnya adalah TCP Connect Scan pada Windows machine. Hal ini dapat dilakukan dengan mengetikkan perintah nmap -sT -T3 -A 10.33.107.41 (IP PC windows). Dalam hal ini, -T digunakan untuk mengatur template waktu dan

-A digunakan untuk mengaktifkan deteksi OS, deteksi versi, pemindaian skrip, dan rute pelacak. Pada kasus ini, pemindaian TCP dalam mode agresif dengan waktu normal (-T3). Sebelum melakukan pemindaian Xmas dengan waktu agresif (-T4), pastikan terlebih dahulu bahwa Windows Firewall masih dalam kondisi aktif. Dari hasil pemindaian dapat dilihat bahwa semua port dibuka atau difilter yang berarti firewall dikonfigurasi pada komputer target. Lalu matikan kembali Windows Firewall. Selanjutnya pemindaian ACK terhadap IP PC Windows dan melihat disposisi port. Pada hasil capture, dapat dilihat bahwa penyerang mengirim paket probe ACK dengan nomor urut acak dan tidak ada response yang berarti port difilter dimana response tanpa filter berarti port ditutup.

Selanjutnya adalah melakukan pemindaian IDLE terhadap PC lain (tetangga), dimana jika port tidak terbuka pada mesin target, maka terus lakukan pemindaian dengan menyelidiki port lain. Pada hasil pemindaian dapat dilihat bahwa port 80 pada Windows Server closed|filtered. Selanjutnya melakukan pemindaian terhadap semua sistem yang hidup di jaringan dengan melakukan sapuan PING menggunakan perintah nmap -sP 10.33.107.* untuk memindai seluruh subnet untuk sistem yang hidup.

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1. Dalam praktikum ini, mahasiswa belajar menggunakan Metasploit Framework dan Nmap untuk melakukan identifikasi kerentanan dan pengungkapan informasi. OS yang digunakan adalah Kali Linux untuk melakukan scanning subnet, mengkaji informasi OS, melakukan pemindaian SMB, TCP Connect Scan, dan pemindaian port dengan berbagai teknik.
2. Pada saat melakukan *scanning OS* pada suatu host dan hasil yang didapatkan adalah *unknown*, maka terdapat kemungkinan bahwa host mati ataupun tidak adanya host yang menggunakan IP yang digunakan untuk *scanning*.
3. Metasplit Framework dapat digunakan untuk melakukan identifikasi terhadap kerentanan serta dapat mengungkapkan informasi dari suatu target.
4. Kita dapat mengungkapkan suatu informasi dari target menggunakan tools pendukung seperti NMAP.
5. Scanning pada subnet dilakukan untuk mengetahui jumlah total host yang aktif di subnet.

VII. Daftar Pustaka

Supardianto. (March 14, 2021). Apa itu Footprinting?. Retrieved April 02, 2023, from https://if.polibatam.ac.id/rekayasa-keamanan-siber/blog/?p=57#:~:text=Footprinting%20adalah%20langkah%20awal%20sebelu

Ismail, J. (2019). Kajian 3: Scanning Network. Retrieved April 02, 2023, from https://julismail.staff.telkomuniversity.ac.id/scanning-network/

Ahmad, A. (2021). Apa kegunaan & keunggulan Metasploit?. Retrieved April 02, 2023, from https://id.quora.com/Apa-kegunaan-dan-keunggulan-Metasploit/answer/Abista-Ahmad-2

Mulyawan, R. (October 02, 2019). Mengenal Pengertian SMB (Server Message Block) Protocol: Tujuan, Fungsi dan Cara Kerjanya!. Retrieved April 02, 2023, from https://rifqimulyawan.com/blog/pengertian-smb/