LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Pertemuan 7 – *Footprinting & Scanning*

DISUSUN OLEH

Nama	: Sofiyanatul Munawaroh
NIM	: 21/474781/SV/19035
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

Pertemuan 7 – *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

Aspek penting dari *footprinting* adalah mengidentifikasi tingkat risiko dari informasi organisasi yang dipublikasikan.

Footprinting adalah langkah pertama dalam *ethical hacking*, yang bertujuan mengumpulkan informasi dari *target network* dan *environment*. Dengan *footprinting*, kita dapat mencari celah untuk menembus dan mengevaluasi *target network.*

Setelah selesai melakukan proses *footprinting* secara metodologikal, kita akan mendapatkan *blueprint* dari *security profile* dari *target organization*. Istilah *blueprint* disini adalah *system profile* yang unik dari *target organization* yang diperoleh melalui *footprinting.*

Footprinting dapat dikategorikan menjadi *passive* dan *active footprinting*. *Objective* dari *footprinting* adalah mengumpulkan informasi *network*, sistem informasi dan informasi organisasi dari target.

Dalam hal mengumpulkan informasi, selain *footprinting* terdapat juga *reconnaissance*. *Reconnaissance* adalah tahap kegiatan dimana penyerang mengumpulkan informasi sebanyak mungkin mengenai target. Informasi yang diperoleh dari hasil kegiatan ini berupa informasi dasar yang berguna, seperti: IP *Address, topology network, network resources* dan informasi personal tentang *user* yang diperlukan untuk tahap selanjutnya. Pada tahapnya, *search engine* umumnya digunakan untuk memperoleh informasi dari sumber online, saat *offline* pengumpulan informasi dicapai dengan membawa bagian dari informasi yang tersebar ditambah dengan rekayasa sosial (*social engineering*) sebagai data digunakan untuk melakukan pengintaian terhadap lingkungan target.

Pengimplementasiannya sendiri dapat menggunakan *scanning*. *Scanning* adalah proses mengumpulkan informasi *detail* mengenai target dengan menggunakan teknik *reconnaissance* yang kompleks dan agresif.

Network scanning berupa kumpulan prosedur untuk mengidentifikasi *hosts, ports*, dan *service* dalam sebuah *network. Network scanning* juga digunakan untuk mencari *active machine* dalam sebuah *network* dan mengidentifikasi OS yang digunakan.

Tujuan dari *scanning* adalah mencari celah yang dapat dieksploitasi, lakukan *probing* sebanyak mungkin, kemudian *track* yang *responsive* atau berguna bagi keperluan *attack.*

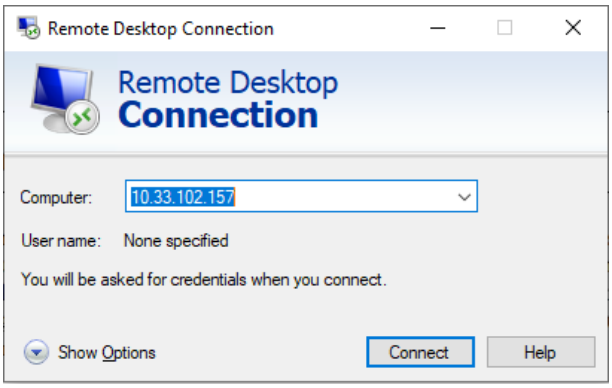
III. Alat dan Bahan

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

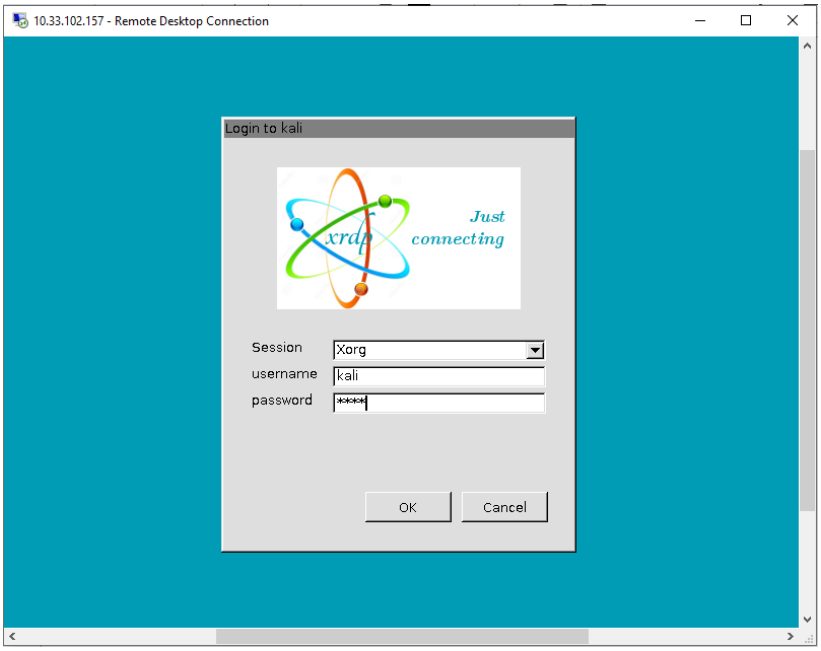
IV. Instruksi Kerja

A. *Footprinting & Reconnaissance*

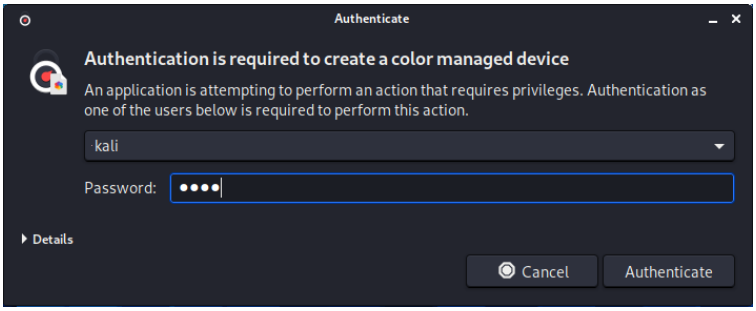
1. Jalankan Kali Linux dengan *Remote Desktop Connection* di Windows menggunakan IP *Address* yang telah disediakan.



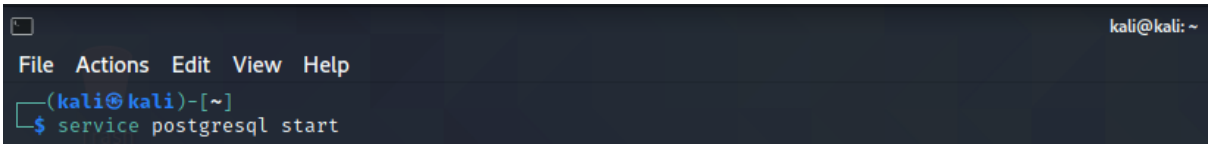
2. Masuk dengan *user*: kali & *password*: kali.



3. Saat pertama kali masuk ke *Desktop* Kali Linux, akan diminta untuk memasukkan *password.*



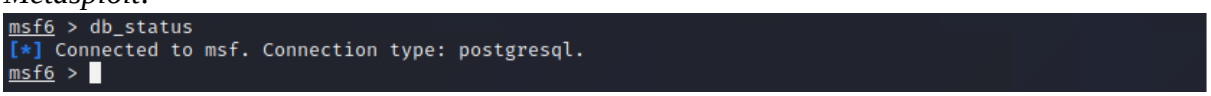
4. Setelah masuk ke *Desktop* Kali Linux, jalankan *terminal* dan ketik *service* ***postgresql start*** lalu tekan *enter*.



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

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

7. Ketikkan **db_status** untuk memastikan *database* sudah terhubung dengan *Metasploit*.



8. Ketik **nmap -Pn -sS -A -oX Test 10.33.107.0/24** dan tekan *Enter*. Dibutuhkan sekitar 10 menit bagi nmap 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 2023-03-27 20:32 CDT
```

9. 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 (0.0016s latency).
Not shown: 993 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 Windows 10 Pro 15063 microsoft-ds (workgroup: WORKGROUP)
1521/tcp open  oracle-tns   Oracle TNS listener 1.5.0.0.0 (unauthorized)
2030/tcp open  device2?
3306/tcp open  mysql        MySQL (unauthorized)
|_sslv2: ERROR: Script execution failed (use -d to debug)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 2 hops
Service Info: Host: DESKTOP-AIVUJRL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h59m38s, deviation: 4h02m14s, median: 20m12s
|_nbstat: NetBIOS name: DESKTOP-AIVUJRL, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:37:13:6a (Quanta Computer)
| smb-os-discovery:
|   OS: Windows 10 Pro 15063 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-AIVUJRL
|   NetBIOS computer name: DESKTOP-AIVUJRL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-28T09:07:56+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-03-28T02:07:53
|_  start_date: 2023-03-06T05:15:56

TRACEROUTE (using port 110/tcp)
```

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

```
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.11.1'
[*] Importing host 10.33.107.191
[*] Successfully imported /home/kali/Test
msf6 >
```

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

```
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
```

```
10.33.107.9              Unknown                     device
10.33.107.10             Unknown                     device
10.33.107.11             Unknown                     device
10.33.107.12             Unknown                     device
10.33.107.13             Unknown                     device
10.33.107.14             Unknown                     device
10.33.107.15             Unknown                     device
10.33.107.16             Unknown                     device
10.33.107.17             Unknown                     device
10.33.107.18             Unknown                     device
10.33.107.19             Unknown                     device
10.33.107.20             Unknown                     device
10.33.107.21             Windows 10                  client
10.33.107.22             Windows 10                  client
10.33.107.23             FreeBSD              6.X    device
10.33.107.24             Unknown                     device
10.33.107.25             Windows 10                  client
10.33.107.26             Windows 10                  client
10.33.107.27             FreeBSD              6.X    device
10.33.107.28             FreeBSD              6.X    device
10.33.107.29             FreeBSD              6.X    device
10.33.107.30             Unknown                     device
10.33.107.31             FreeBSD              6.X    device
10.33.107.32             Windows 10                  client
10.33.107.33             FreeBSD              6.X    device
10.33.107.34             Windows 10                  client
10.33.107.35             Windows 10                  client
10.33.107.36             Windows 10                  client
10.33.107.37             FreeBSD              6.X    device
```

12. Ketik **db_nmap -sS -A 10.33.107.84** dan *Enter*.

```
msf6 > db_nmap -sS -A 10.33.107.84
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:25 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 11.83 seconds
msf6 >
```

13. Nmap memindai mesin dan memberi Anda *detail* layanan yang berjalan di mesin. Ini adalah bagaimana Anda dapat menemukan layanan pada masing-masing mesin.

14. Untuk mendapatkan informasi layanan dari semua komputer aktif di jenis *subnet* ketik **services** dan tekan *Enter*.

```
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 workgroup: WORKGROUP
10.33.107.21  1521  tcp    oracle-tns     open   Oracle TNS listener 1.5.0.0.0 unauthorized
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
10.33.107.22  135   tcp    msrpc          open   Microsoft Windows RPC
10.33.107.22  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
10.33.107.22  445   tcp    microsoft-ds   open   Windows 10 Pro 15063 microsoft-ds workgroup: WORKGROUP
10.33.107.22  1521  tcp    oracle-tns     open   Oracle TNS listener 1.5.0.0.0 unauthorized
10.33.107.22  3306  tcp    mysql          open   MySQL unauthorized
10.33.107.22  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.33.107.23  3306  tcp    mysql          open   MySQL unauthorized
10.33.107.25  135   tcp    msrpc          open   Microsoft Windows RPC
10.33.107.25  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
10.33.107.25  445   tcp    microsoft-ds   open   Windows 10 Pro 15063 microsoft-ds workgroup: WORKGROUP
10.33.107.25  1521  tcp    oracle-tns     open   Oracle TNS listener 1.5.0.0.0 unauthorized
10.33.107.25  2030  tcp    device2        open
10.33.107.25  3306  tcp    mysql          open   MySQL unauthorized
10.33.107.25  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.33.107.26  135   tcp    msrpc          open   Microsoft Windows RPC
10.33.107.26  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
10.33.107.26  445   tcp    microsoft-ds   open   Windows 10 Pro 15063 microsoft-ds workgroup: WORKGROUP
10.33.107.26  1521  tcp    oracle-tns     open   Oracle TNS listener 1.5.0.0.0 unauthorized
10.33.107.26  3306  tcp    mysql          open   MySQL unauthorized
10.33.107.26  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
```

```
10.33.107.27   3306  tcp    mysql           open   MySQL unauthorized
10.33.107.28   3306  tcp    mysql           open   MySQL unauthorized
10.33.107.29   3306  tcp    mysql           open   MySQL unauthorized
10.33.107.31   3306  tcp    mysql           open   MySQL unauthorized
10.33.107.32   135   tcp    msrpc           open   Microsoft Windows RPC
10.33.107.32   139   tcp    netbios-ssn     open   Microsoft Windows netbios-ssn
10.33.107.32   445   tcp    microsoft-ds    open   Windows 10 Pro 15063 microsoft-ds workgroup: WORKGROUP
10.33.107.32   1521  tcp    oracle-tns      open   Oracle TNS listener 1.5.0.0.0 unauthorized
10.33.107.32   2030  tcp    device2         open
10.33.107.32   3306  tcp    mysql           open   MySQL unauthorized
```

15. 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) >
```

16. 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) >
```

17. 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 RHOSTS 10.33.107.27-37
RHOSTS => 10.33.107.27-37
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.33.107.30:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities
 23s) (guid:{0bb18c4f-6535-47e8-baf2-3c5c58c1c2a8}) (authentication domain:DESKTOP-AIVUJRL)
[+] 10.33.107.30:445      -   Host is running Windows 10 Pro (build:15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGR
[*] 10.33.107.28:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities
 41s) (guid:{7dee740f-4374-45e4-bfb3-9b4e6e539f18}) (authentication domain:DESKTOP-AIVUJRL)
[+] 10.33.107.28:445      -   Host is running Windows 10 Pro (build:15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGR
[*] 10.33.107.35:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities
55m 31s) (guid:{1b739ba4-340e-4722-a6cb-6df3cb894295}) (authentication domain:DESKTOP-AIVUJRL)
[+] 10.33.107.35:445      -   Host is running Windows 10 Pro (build:15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGR
[*] 10.33.107.34:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities
1h 30m 50s) (guid:{72bb8913-dab4-4bbd-b6d3-f633670108c1}) (authentication domain:DESKTOP-AIVUJRL)
[+] 10.33.107.34:445      -   Host is running Windows 10 Pro (build:15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGR
[*] 10.33.107.37:445      - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities
0h 10m 41s) (guid:{82b2c672-a1ba-4042-9f17-57b4cb6e707d}) (authentication domain:DESKTOP-AIVUJRL)
[+] 10.33.107.37:445      -   Host is running Windows 10 Pro (build:15063) (name:DESKTOP-AIVUJRL) (workgroup:WORKGR
[*] 10.33.107.27-37:      - Scanned  5 of 11 hosts (45% complete)
[*] 10.33.107.27-37:      - Scanned  5 of 11 hosts (45% complete)
[*] 10.33.107.27-37:      - Scanned  5 of 11 hosts (45% complete)
[*] 10.33.107.27-37:      - Scanned  5 of 11 hosts (45% complete)
[*] 10.33.107.27-37:      - Scanned  7 of 11 hosts (63% 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) >
```

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

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

Hosts
=====

address         mac  name            os_name     os_flavor  os_sp  purpose  info  comments
-------         ---  ----            -------     ---------  -----  -------  ----  --------
10.33.107.0                          Unknown                       device
```

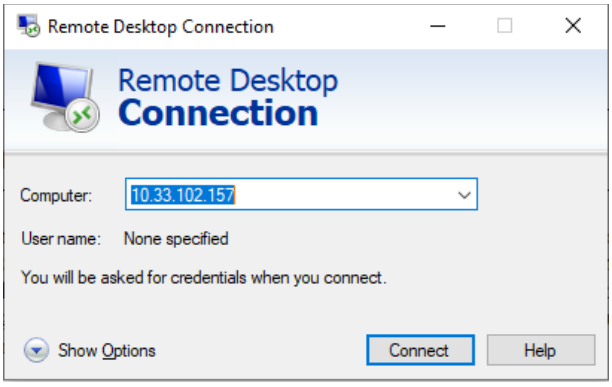
```
10.33.107.1                     Unknown                 device
10.33.107.2                     Unknown                 device
10.33.107.3                     Unknown                 device
10.33.107.4                     Unknown                 device
10.33.107.5                     Unknown                 device
10.33.107.6                     Unknown                 device
10.33.107.7                     Unknown                 device
10.33.107.8                     Unknown                 device
10.33.107.9                     Unknown                 device
10.33.107.10                    Unknown                 device
10.33.107.11                    Unknown                 device
10.33.107.12                    Unknown                 device
10.33.107.13                    Unknown                 device
10.33.107.14                    Unknown                 device
10.33.107.15                    Unknown                 device
10.33.107.16                    Unknown                 device
10.33.107.17                    Unknown                 device
10.33.107.18                    Unknown                 device
10.33.107.19                    Unknown                 device
10.33.107.20                    Unknown                 device
10.33.107.21                    Windows 10              client
10.33.107.22                    Windows 10              client
10.33.107.23                    FreeBSD         6.X     device
10.33.107.24                    Unknown                 device
10.33.107.25                    Windows 10              client
10.33.107.26                    Windows 10              client
10.33.107.27                    FreeBSD         6.X     device
10.33.107.28        DESKTOP-AIVUJRL Windows 10 Pro      6.X     client
10.33.107.29                    FreeBSD         6.X     device
10.33.107.30        DESKTOP-AIVUJRL Windows 10 Pro              client
10.33.107.31                    FreeBSD         6.X     device
10.33.107.32                    Windows 10              client
10.33.107.33                    FreeBSD         6.X     device
10.33.107.34        DESKTOP-AIVUJRL Windows 10 Pro              client
10.33.107.35        DESKTOP-AIVUJRL Windows 10 Pro              client
10.33.107.36                    Windows 10              client
10.33.107.37        DESKTOP-AIVUJRL Windows 10 Pro      6.X     client
10.33.107.38                    Windows 10              client
10.33.107.39                    Windows 10              client
10.33.107.40                    Windows 10              client
```

Sistem operasi yang diinstal di *domain* 10.33.107.9-15 tidak diketahui (*unknown*).

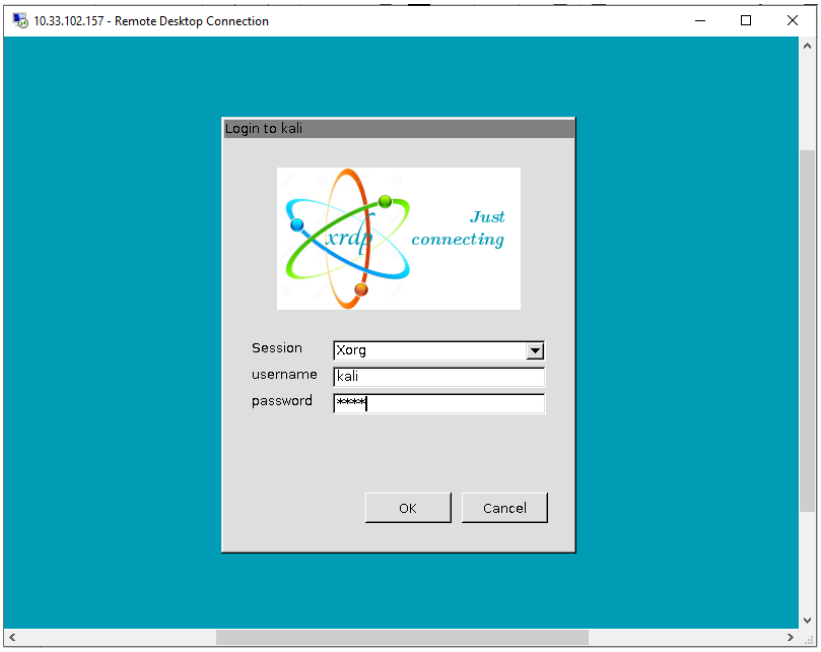
Versi paket layanan yang diinstal di mesin 10.33.107.44 tidak ter-*captured.*

B. *Scanning*

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



2. Masuk dengan *user*: kali & *password*: kali.



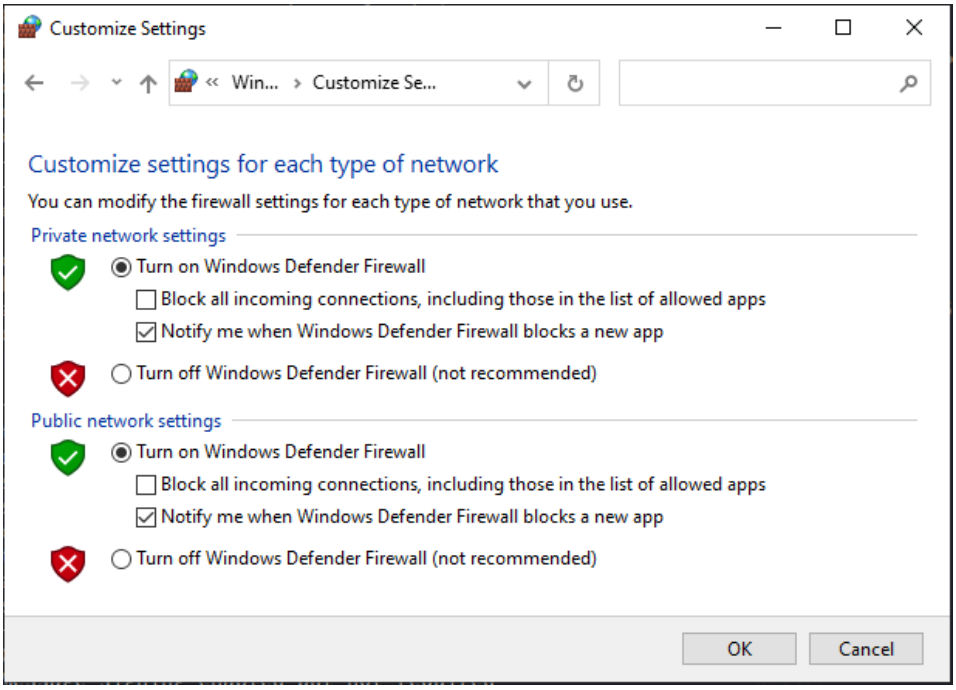
3. Ketik perintah **nmap -sT -T3 -A 10.33.107.41 (IP PC windows)** dan tekan *Enter* untuk melakukan TCP *Connect Scan* pada Windows *machine*.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -T3 -A 10.33.107.41
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:49 CDT
Nmap scan report for 10.33.107.41
Host is up (0.00053s latency).
Not shown: 994 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 Windows 10 Pro 19045 microsoft-ds (workgroup: WORKGROUP)
1521/tcp open  oracle-tns   Oracle TNS listener 1.5.0.0.0 (unauthorized)
2030/tcp open  device2?
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: Host: DESKTOP-N6K23J9; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h59m47s, deviation: 4h02m28s, median: 20m11s
|_nbstat: NetBIOS name: DESKTOP-N6K23J9, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:37:14:58 (Quanta Computer)
| smb-os-discovery:
|   OS: Windows 10 Pro 19045 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-N6K23J9
|   NetBIOS computer name: DESKTOP-N6K23J9\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-28T10:10:57+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-03-28T03:10:57
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.28 seconds
```

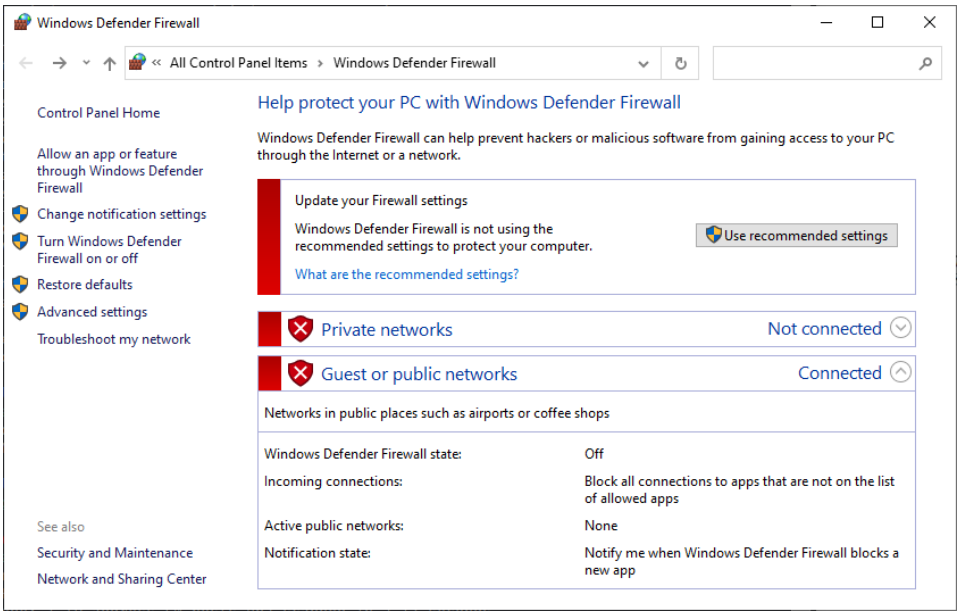
4. Beralih ke mesin Windows, masuk ke mesin, dan aktifkan Windows *Firewall*.



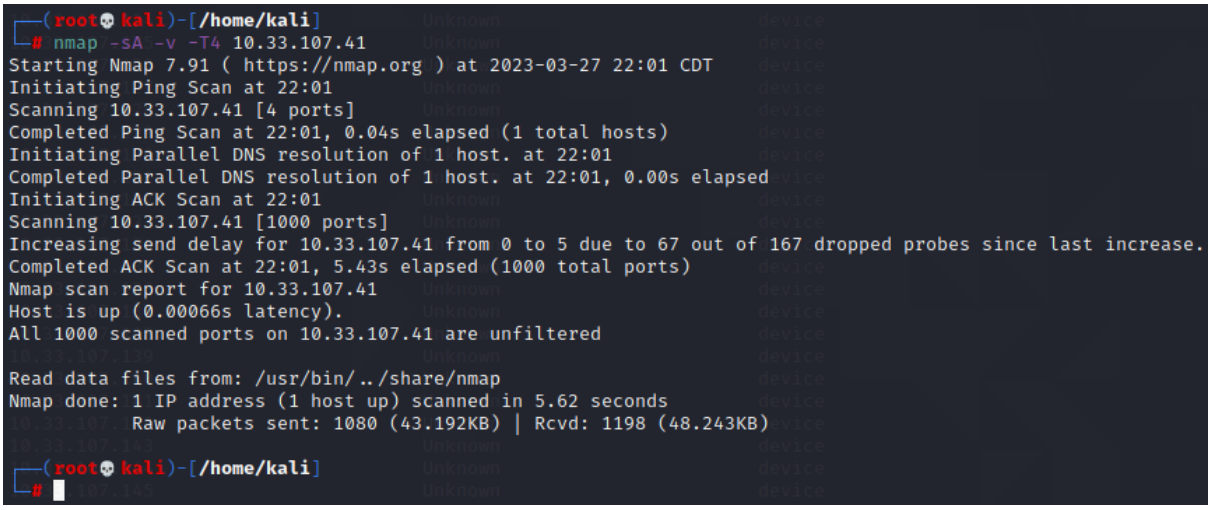
5. Beralih kembali ke mesin Kali Linux. Ketik **nmap -sX -T4 10.33.107.41 (IP PC windows)** di *command prompt* dan tekan *Enter* untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Ini menampilkan hasilnya seperti yang ditunjukkan pada tangkapan layar. Hasil Nmap menunjukkan bahwa semua *port* dibuka/difilter yang berarti *firewall* dikonfigurasi pada komputer target.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sX -T4 10.33.107.41
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:59 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
┌──(root💀kali)-[/home/kali]
└─#
```

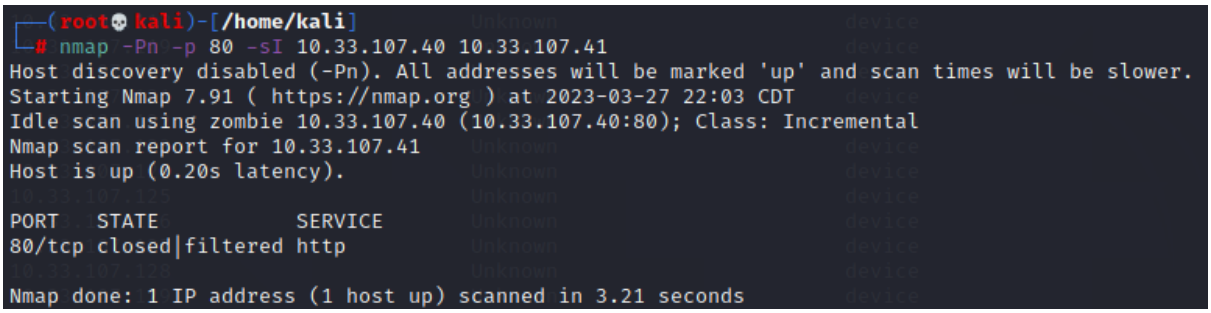
6. Beralih ke mesin Windows dan matikan Windows *Firewall*.



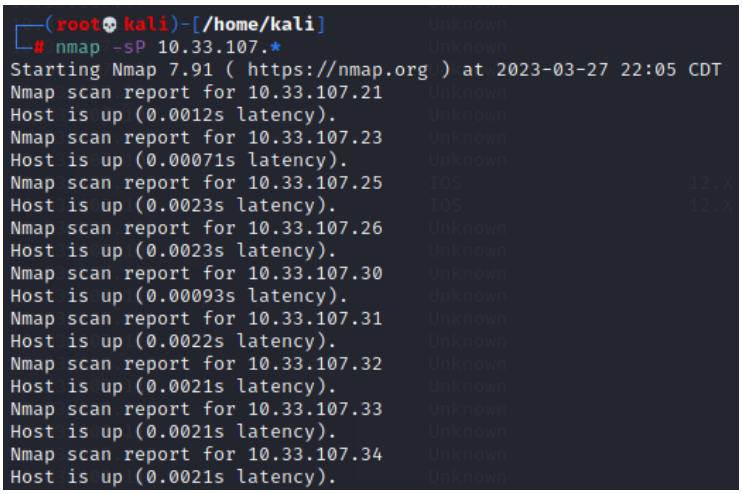
7. Beralih kembali ke mesin Kali Linux. Ketik **nmap -sA -v -T4 10.33.107.41** di *terminal* baris perintah. Ini memulai ACK *Scan* dan menampilkan disposisi *port*, seperti yang ditunjukkan pada tangkapan layar.

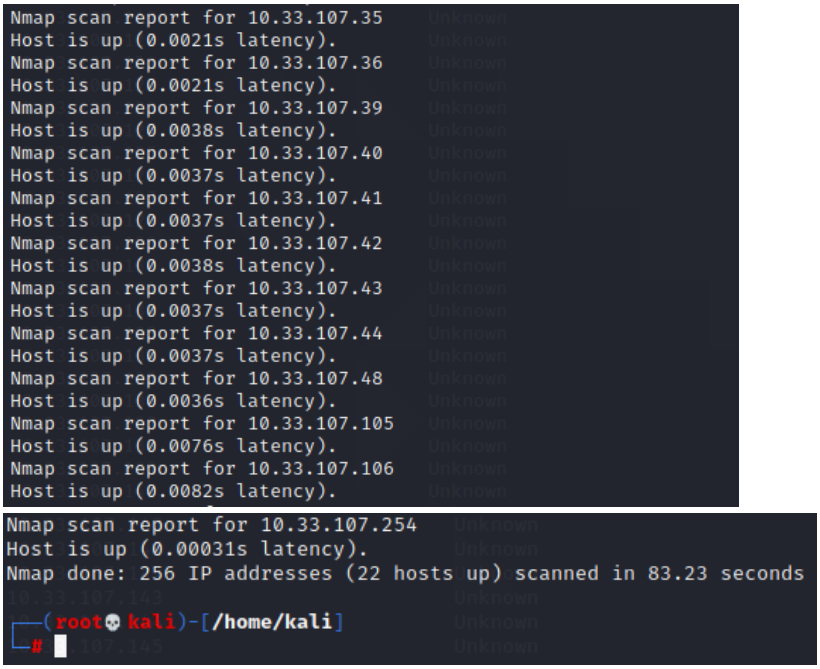


8. Ketik perintah nmap -Pn -p 80 -sI 10.33.107.40 (**IP PC tetangga**) 10.33.107.41, dan tekan *Enter*.



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 10.33.107.*** 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. Hasil dan Pembahasan

Pada praktikum ini, mahasiswa diminta untuk melakukan identifikasi terhadap kerentanan dan pengungkapan informasi menggunakan *Metasploit Framework. Metasploit* sendiri adalah sebuah proyek keamanan komputer yang dapat menyediakan informasi tentang kerentanan keamanan dan membantu dalam pengujian penetrasi dan pengembangan *signature* IDS. Selain itu, mahasiswa juga akan menggunakan beberapa jenis teknik pemindaian jaringan menggunakan *Nmap.*

Dalam praktiknya menggunakan Kali Linux yang merupakan *platform* yang mendukung *Metasploit Framework.* Untuk meluncurkan *Metasploit Framework* pada Kali Linux bisa dengan mengetikkan perintah **msfconsole** dan tunggu hingga diluncurkan. Setelah itu pastikan bahwa *database* telah terhubung ke *Metasploit*, lalu baru bisa melakukan *scanning.* Pada praktikum ini, dilakukan *scanning* terhadap *subnet* untuk mengetahui jumlah total *host* yang aktif di *subnet*. Saat *scanning* selesai, lakukan impor hasil pengujian dan lakukan pengecekan terhadap *host* dan *detail* yang telah dikumpulkan oleh *Nmap.* Pada kasus ini, kita berfokus pada informasi **os_flavor** dimana setelah dicek *Nmap* belum mengumpulkan informasi tersebut.

Kemudian melakukan *scanning* SYN dan menyimpan hasilnya ke dalam *database. Nmap* memindai mesin dan memberikan informasi *detail* layanan yang berjalan di mesin, sehingga pengguna dapat menemukan layanan pada masing-masing mesin. Seperti halnya untuk mendapatkan informasi layanan dari semua komputer aktif di jenis *subnet* dapat menggunakan perintah **services.**

Selanjutnya memuat modul pemindai SMB. SMB (*Server Message Block*) adalah protokol *client/server* yang ditujukan sebagai layanan untuk berbagi berkas (*file sharing*) di dalam sebuah jaringan. 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 **set THREADS 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.

Pada praktikum di modul berikutnya, dilakukan TCP *Connect Scan* pada Windows *machine* dengan 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), aktifkan terlebih dahulu Windows *Firewall.* 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.

Berikutnya 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

1. Untuk melakukan identifikasi terhadap kerentanan dan pengungkapan informasi menggunakan *Metasploit Framework.*
2. Kali Linux merupakan salah satu *platform* yang mendukung *Metasploit.*
3. Terdapat berbagai jenis dari *Nmap Scanning* yang dapat digunakan berdasarkan fungsi dan target yang ingin dipindai.

VII. Daftar Pustaka

SkillPlus. (2022). *Konsep Footprinting.* Diakses pada 1 April 2023 dari https://skillplus.web.id/konsep-footprinting/

Wahyu, Dimas. (Tanpa Tahun). *Reconnaissance.* Diakses pada 1 April dari http://edocs.ilkom.unsri.ac.id/831/1/Dimas%20Wahyudi_09011281320004_KJK_Tugas_1.pdf#:~:text=Reconnaissance%20adalah%20tahap%20kegiatan%20dimana%20penyerang%20mengumpulkan%20informasi,%28attack%29%20sebuah%20sistem%2C%20seperti%20terlihat%20pada%20gambar%201.

SkillPlus. (2022). *Konsep Network Scanning – Pengenalan.* Diakses pada 1 April dari https://skillplus.web.id/konsep-network-scanning-pengenalan/#:~:text=Network%20scanning%20berupa%20kumpulan%20prosedur%20untuk%20mengidentifikasi%20hosts%2C,dalam%20sebuah%20network%20dan%20mengidentifikasi%20OS%20yang%20digunakan.

Alfian, F. (2019). *Mengenal Tentang SMB (Server Message Block)*. Diakses pada 1 April dari http://nguprek.com/mengenal-tentang-smb-server-message-block/