

**LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 7**



DI SUSUN OLEH:

Nama : Bintang Nur K
NIM : 21/481453/SV/19790
Kelas : RI4AA
Hari, tanggal : Selasa, 28 Maret 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng
Asisten Praktikum : Gabriella Alvera Chaterine

**PROGRAM SARJANA TERAPAN (DIV)
TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

PERTEMUAN 7

FOOTPRINTING DAN RECONNAISSANCE

I. TUJUAN

- Menunjukkan bagaimana mengidentifikasi kerentanan dan pengungkapan informasi menggunakan Metasploit Framework.
- Mahasiswa belajar ekstrak informasi akurat tentang jaringan menggunakan Metasploit Framework.
- Menjelaskan kepada mahasiswa bagaimana cara menggunakan jenis berikut 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

Reconnaissance adalah teknik paling awal sekali yang dilakukan oleh seorang hacker sebelum serangan dilakukan. Dengan cara ini seorang penyerang akan memperoleh informasi awal seperti, IP, DNS Server, Domain, Tabel Routing, reconnaissance dibagi menjadi 2 jenis, yaitu passive reconnaissance dan active reconnaissance.

- Passive reconnaissance adalah melakukan kegiatan reconnaissance tanpa berhubungan secara langsung dengan target, contoh: mendapatkan informasi melalui situs atau surat kabar.

- Active reconnaissance adalah melakukan kegiatan reconnaissance dengan cara berhubungan langsung dengan target, contoh: mendapatkan informasi melalui telepon atau email dengan target.

III. ALAT DAN BAHAN

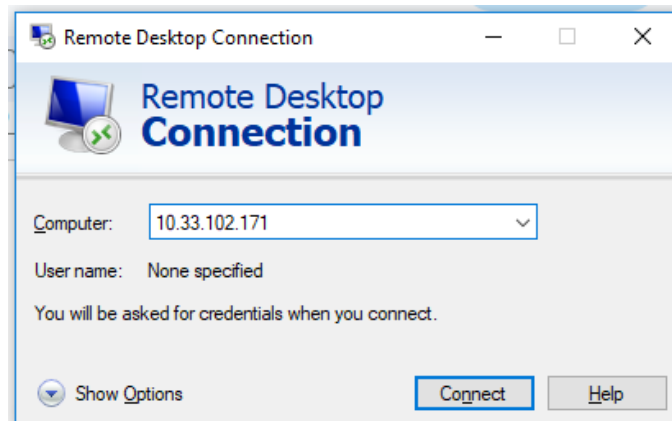
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

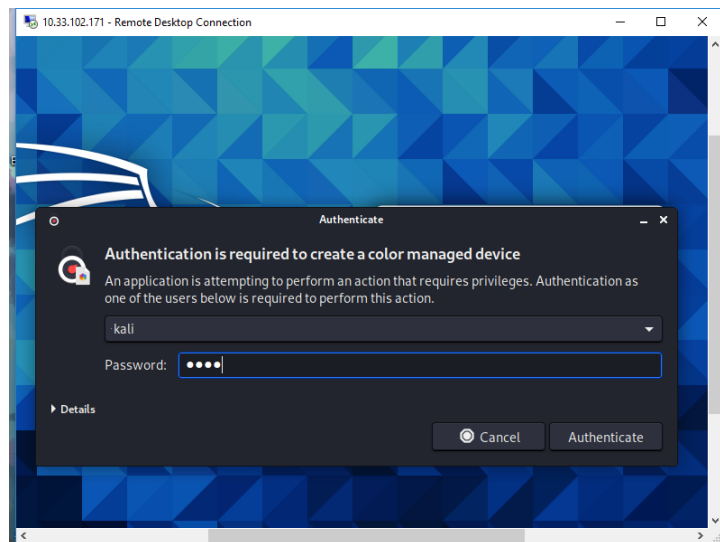
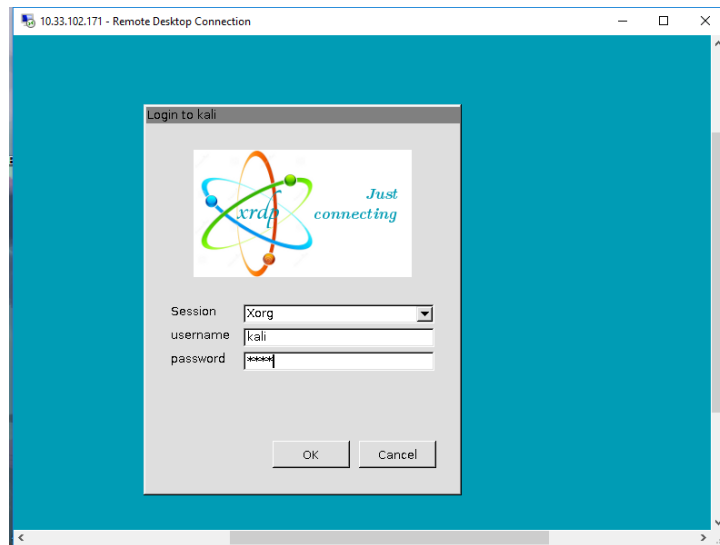
- Koneksi Internet
- Remote Desktop Connection
- Komputer / PC

IV. LANGKAH KERJA DAN HASIL

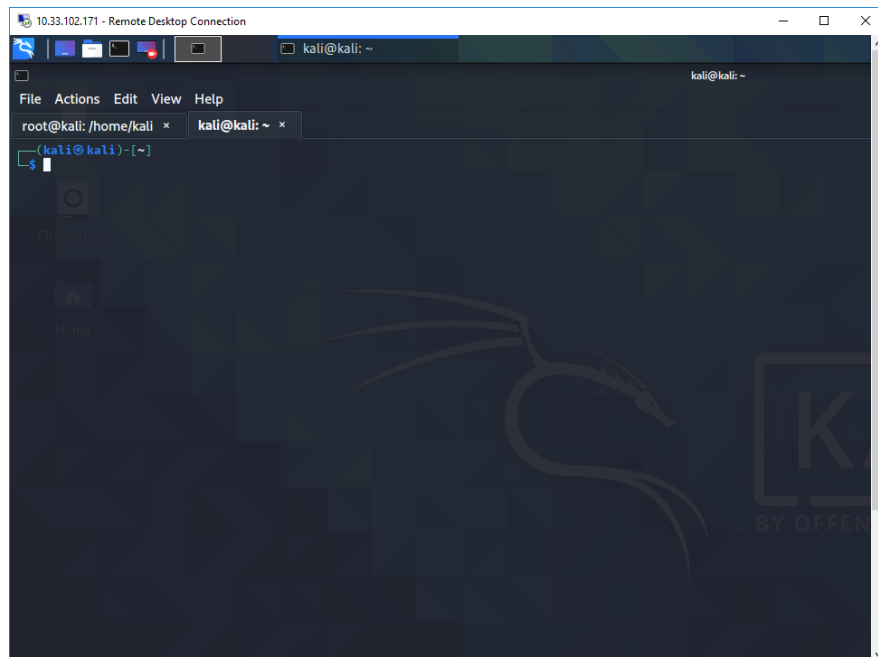
Pengumpulan Informasi Menggunakan Metasploit

1. Jalankan mesin Kali Linux dengan Remote Desktop Connection di PC windows. Masukkan masing-masing IP yang sudah di sediakan

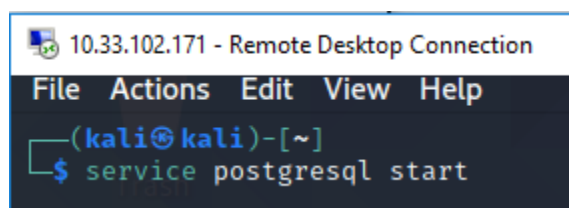
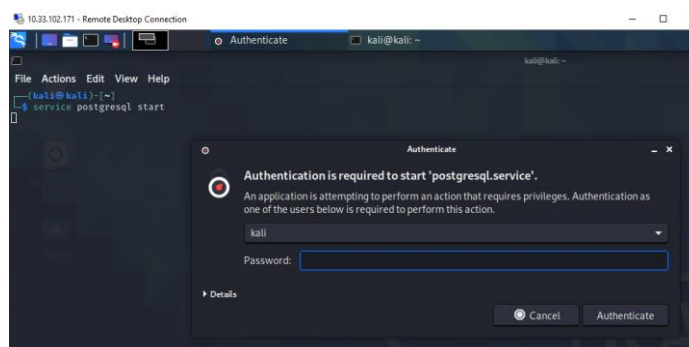




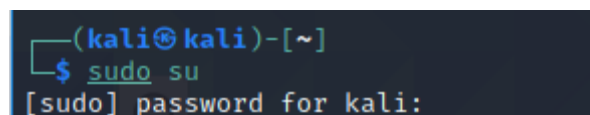
2. Masukkan password mhs_123 pilih username mahasiswa
3. Desktop Kali Linux muncul, klik ikon Terminal



4. Di jendela terminal, ketik `service postgresql start` dan tekan Enter.



5. Masuk akun sebagai root, ketik `sudo su` masukkan password : `mhs_123`



6. Ketik `msfconsole` dan tekan Enter. Tunggu hingga Metasploit Framework diluncurkan

```

root@kali)~[/home/kali]
# msfconsole
File System

+-----+
| METASPLOIT by Rapid7 |
+-----+
|
| ==c(-----)(o(-----)(_)
| Home
|
| \ \
|  \  RECON
|   \
|
+-----+
|
| *****[***
| EXPLOIT
|
| [msf >]
|
| \ \
| (a)(a)(a)(a)(a)(a)(a)/
| *****
|
+-----+
|
| o o o
|
| o o
|
| o
|
| ^^^^^^^^^^^^^^^^^^
| PAYLOAD
|
| (a)(a)""""**|(a)(a)**|(a)
|
| = = = = =
|
+-----+
|
| \ \ \ \ \ / \ / \ /
| )===== (
| LOOT
|
| C ||
|
| '-----'
|
+-----+

= [ metasploit v6.0.30-dev ]
+ -- ==[ 2099 exploits - 1129 auxiliary - 357 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: View all productivity tips with the
tips command

msf6 >

```

- Di baris perintah msf, ketik `db_status` dan tekan Enter. Jika Anda mendapatkan postgresql yang dipilih, no connection, maka database tidak dimulai.

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

8. Jika Anda mendapatkan postgresql terhubung ke pesan msf, lewat ke Langkah 13
9. Keluar dari metasploit dengan mengetik exit dan tekan Enter.
10. Untuk menginisialisasi database ketik msfdb init dan tekan Enter.
11. Sekarang restart layanan postgresql dengan mengetik service postgresql restart
12. Luncurkan kembali kerangka kerja metasploit dengan mengetik msfconsole dan tekan Enter. Tunggu hingga kerangka metasploit dimulai dan memberi Anda baris perintah msf
13. Periksa kembali apakah databse terhubung ke metasploit dengan mengetik db_status dan tekan Enter.

14. 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 > db_status
[*] Connected to msf. Connection type: postgresql.
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 20:23 CDT
```

15. Setelah selesai, Anda akan mendapatkan pesan Nmap done dengan nmap yang menunjukkan jumlah total host yang aktif di subnet.

```
Nmap scan report for 10.33.107.47
Host is up (0.16s latency).
All 1000 scanned ports on 10.33.107.47 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
- Hops 1-27 are the same as for 10.33.107.51
28 ...
29 113.97 ms 10.33.102.254
30 ...

Nmap scan report for 10.33.107.48
Host is up (0.0011s latency).
Not shown: 996 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)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
rdp-ntlm-info:
  Target_Name: DESKTOP-PD7QHPL
  NetBIOS_Domain_Name: DESKTOP-PD7QHPL
  NetBIOS_Computer_Name: DESKTOP-PD7QHPL
  DNS_Domain_Name: DESKTOP-PD7QHPL
  DNS_Computer_Name: DESKTOP-PD7QHPL
  Product_Version: 10.0.15063
_ System_Time: 2023-03-28T02:08:09+00:00
ssl-cert: Subject: commonName=DESKTOP-PD7QHPL
Not valid before: 2023-01-24T08:45:25
Not valid after: 2023-07-26T08:45:25
ssl-date: 2023-03-28T02:08:56+00:00; +20m21s from scanner time.
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-PD7QHPL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h03m31s, deviation: 3h07m32s, median: 20m19s
|_smb-os-discovery:
```

```
Host script results:
_clock-skew: mean: -1h03m31s, deviation: 3h07m32s, median: 20m19s
smb-os-discovery:
  OS: Windows 10 Pro 15063 (Windows 10 Pro 6.3)
  OS CPE: cpe:/o:microsoft:windows_10::-
  Computer name: DESKTOP-PD7QHPL
  NetBIOS computer name: DESKTOP-PD7QHPL\x00
  Workgroup: WORKGROUP\x00
  System time: 2023-03-28T09:08:47+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: 2023-03-28T02:08:44
  start_date: 2023-03-02T03:57:56
```

```
TRACEROUTE (using port 199/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 10.33.107.51
2 0.82 ms 10.33.107.48
```

```
Nmap scan report for 10.33.107.49
Host is up (0.079s latency).
All 1000 scanned ports on 10.33.107.49 are filtered
Too many fingerprints match this host to give specific OS details
```

```
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
- Hops 1-28 are the same as for 10.33.107.51
29 ...
30 752.40 ms 10.33.102.254
```

```
Nmap scan report for 10.33.107.50
Host is up (0.0019s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
3306/tcp open mysql MySQL (unauthorized)
```

```
Not shown: 997 filtered ports
PORT STATE SERVICE
3306/tcp open mysql MySQL (unauthorized)
sql-test: ERROR: Script execution failed (use -d to debug)
ssl-date: ERROR: Script execution failed (use -d to debug)
sslls: ERROR: Script execution failed (use -d to debug)
tls-alpn: ERROR: Script execution failed (use -d to debug)
tls-heartbeats: ERROR: Script execution failed (use -d to debug)
SMB/tcp open http-proxy sqlmap
http-title: TightVNC desktop (desktop-fc3j0u4)
SMB/tcp open vnc VNC (protocol 3.8)
vnc-info:
  Protocol version: 3.8
  Security types:
    VNC Authentication (2)
    Tight (16)
  Tight auth subtypes:
    STW-WaDmP (2)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 9.2-RELEASE (910), Microsoft Windows 10 (920), Microsoft Windows Server 2008 or 2008 R2 x64 (990), m0n0wall 1.1011 - 1.1015 (FreeBSD 6.3) (800), Juniper SRX210 Fi
11 (JUNOS 12.1) (800), Juniper Networks JUNOS 12 (800), Juniper Networks JUNOS 9.0R2.10 (800), Juniper SRX100-series or SRX200-series firewall (JUNOS 10.4 - 12.1) (800), Microsoft Windows Serv
on SPI (800), Netasq 0.9 Firewall (800)
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 10.33.107.51
2 3.78 ms 10.33.107.50

Nmap scan report for 10.33.107.51
Host is up (0.071s latency).
All 1000 scanned ports on 10.33.107.51 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
2 0.43 ms 10.33.102.254
3 241.25 ms 10.33.102.254
4 103.53 ms 10.33.102.254
5 107.44 ms 10.33.102.254
6 200.38 ms 10.33.102.254
```

16. Ketik db_import Test dan tekan Enter untuk mengimpor hasil pengujian.

10.33.102.171 - Remote Desktop Connection

```
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.11.1'
[*] Importing host 10.33.107.0
[*] Importing host 10.33.107.1
[*] Importing host 10.33.107.2
[*] Importing host 10.33.107.3
[*] Importing host 10.33.107.4
[*] Importing host 10.33.107.5
[*] Importing host 10.33.107.6
[*] Importing host 10.33.107.7
[*] Importing host 10.33.107.8
[*] Importing host 10.33.107.9
[*] Importing host 10.33.107.10
[*] Importing host 10.33.107.11
[*] Importing host 10.33.107.12
[*] Importing host 10.33.107.13
[*] Importing host 10.33.107.14
[*] Importing host 10.33.107.15
[*] Importing host 10.33.107.16
[*] Importing host 10.33.107.17
[*] Importing host 10.33.107.18
[*] Importing host 10.33.107.19
[*] Importing host 10.33.107.20
[*] Importing host 10.33.107.21
[*] Importing host 10.33.107.22
[*] Importing host 10.33.107.23
[*] Importing host 10.33.107.24
[*] Importing host 10.33.107.25
[*] Importing host 10.33.107.26
[*] Importing host 10.33.107.27
[*] Importing host 10.33.107.28
[*] Importing host 10.33.107.29
[*] Importing host 10.33.107.30
[*] Importing host 10.33.107.31
[*] Importing host 10.33.107.32
[*] Importing host 10.33.107.33
[*] Importing host 10.33.107.34
[*] Importing host 10.33.107.35
[*] Importing host 10.33.107.36
[*] Importing host 10.33.107.37
[*] Importing host 10.33.107.38
[*] Importing host 10.33.107.39
[*] Importing host 10.33.107.40
[*] Importing host 10.33.107.41
[*] Importing host 10.33.107.42
[*] Importing host 10.33.107.43
[*] Importing host 10.33.107.44
```

```

[*] Importing host 10.33.107.42
[*] Importing host 10.33.107.43
[*] Importing host 10.33.107.44
[*] Importing host 10.33.107.45
[*] Importing host 10.33.107.46
[*] Importing host 10.33.107.47
[*] Importing host 10.33.107.48
[*] Importing host 10.33.107.49
[*] Importing host 10.33.107.50
[*] Importing host 10.33.107.51
[*] Importing host 10.33.107.52
[*] Importing host 10.33.107.53
[*] Importing host 10.33.107.54
[*] Importing host 10.33.107.55
[*] Importing host 10.33.107.56
[*] Importing host 10.33.107.57
[*] Importing host 10.33.107.58
[*] Importing host 10.33.107.59
[*] Importing host 10.33.107.60
[*] Importing host 10.33.107.61
[*] Importing host 10.33.107.62
[*] Importing host 10.33.107.63
[*] Successfully imported /home/kali/Test
msf6 >

```

17. Ketik host dan tekan Enter untuk menampilkan host dan detailnya seperti yang dikumpulkan oleh nmap.

```

msf6 > 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			Windows 10			client		
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		
10.33.107.38			Windows 10			client		
10.33.107.39			Windows 10			client		

```
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      Windows 10   client
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
10.33.107.38      Windows 10   client
10.33.107.39      Windows 10   client
10.33.107.40      Windows 10   client
10.33.107.41      Windows 10   client
10.33.107.42      Windows 10   client
10.33.107.43      Windows 10   client
10.33.107.44      Windows 10   client
10.33.107.45      Unknown      device
10.33.107.46      FreeBSD     6.X device
10.33.107.47      Unknown      device
10.33.107.48      Windows 10   client
10.33.107.49      Unknown      device
10.33.107.50      FreeBSD     6.X device
10.33.107.51      Unknown      device
10.33.107.52      Unknown      device
10.33.107.53      Unknown      device
10.33.107.54      Unknown      device
10.33.107.55      Unknown      device
10.33.107.56      Unknown      device
10.33.107.57      Unknown      device
10.33.107.58      Unknown      device
10.33.107.59      Unknown      device
10.33.107.60      Unknown      device
10.33.107.61      Unknown      device
10.33.107.62      Unknown      device
10.33.107.63      Unknown      device
10.33.107.84      Unknown      device

msf6 > 
```

Apakah Nmap sudah mengumpulkan informasi os_flavor?

Jawab: Belum

18. KETIK db_nmap -sS -A 10.33.107.84 dan Enter.

```
msf6 > db_nmap -sS -A -Pn 10.33.107.84
[*] Nmap: Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:20 CDT
[*] Nmap: Nmap scan report for 10.33.107.84
[*] Nmap: Host is up (0.23s latency).
[*] Nmap: All 1000 scanned ports on 10.33.107.84 are filtered
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: TRACEROUTE (using proto 1/icmp)
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1  1.30 ms  10.33.102.254
[*] Nmap: 2  ... 5
[*] Nmap: 6  953.99 ms 10.33.102.254
[*] Nmap: 7  954.00 ms 10.33.102.254
[*] Nmap: 8  954.01 ms 10.33.102.254
[*] Nmap: 9  954.02 ms 10.33.102.254
[*] Nmap: 10 954.09 ms 10.33.102.254
[*] Nmap: 11 ...
[*] Nmap: 12 986.80 ms 10.33.102.254
[*] Nmap: 13 986.76 ms 10.33.102.254
[*] Nmap: 14 986.74 ms 10.33.102.254
[*] Nmap: 15 986.75 ms 10.33.102.254
[*] Nmap: 16 986.74 ms 10.33.102.254
[*] Nmap: 17 935.96 ms 10.33.102.254
[*] Nmap: 18 ... 21
[*] Nmap: 22 977.98 ms 10.33.102.254
[*] Nmap: 23 977.95 ms 10.33.102.254
[*] Nmap: 24 977.94 ms 10.33.102.254
[*] Nmap: 25 977.93 ms 10.33.102.254
[*] Nmap: 26 977.92 ms 10.33.102.254
[*] Nmap: 27 977.92 ms 10.33.102.254
[*] Nmap: 28 ... 30
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 65.58 seconds

msf6 > 
```

19. Nmap memindai mesin dan memberi Anda detail layanan yang berjalan di mesin. Ini adalah bagaimana Anda dapat menemukan layanan pada masing-masing mesin.
20. 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    mssqlrpc             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    mssqlrpc             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    mssqlrpc             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    mssqlrpc             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    mssqlrpc             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
10.33.107.32 5357  tcp    http                  open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.33.107.33 3306  tcp    mysql                 open   MySQL unauthorized
10.33.107.34 135   tcp    mssqlrpc             open   Microsoft Windows RPC
10.33.107.34 139   tcp    netbios-ssn          open   Microsoft Windows netbios-ssn

```

21. 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) >

```

22. 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    10.33.107.0/24  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) >

```

23. 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 10.33.107.8-16
RHOSTS => 10.33.107.8-16
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.33.107.8-16:      - Scanned 2 of 9 hosts (22% complete)
[*] 10.33.107.8-16:      - Scanned 4 of 9 hosts (44% complete)
[*] 10.33.107.8-16:      - Scanned 6 of 9 hosts (66% complete)
[*] 10.33.107.8-16:      - Scanned 7 of 9 hosts (77% complete)
[*] 10.33.107.8-16:      - Scanned 7 of 9 hosts (77% complete)
[*] 10.33.107.8-16:      - Scanned 7 of 9 hosts (77% complete)
[*] 10.33.107.8-16:      - Scanned 7 of 9 hosts (77% complete)
[*] 10.33.107.8-16:      - Scanned 8 of 9 hosts (88% complete)
[*] 10.33.107.8-16:      - Scanned 9 of 9 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > |
```

24. Ketik host dan tekan Enter. Sekarang Anda dapat melihat bahwa informasi os_flavor telah dikumpulkan dan ditampilkan seperti yang ditunjukkan pada tangkapan layar.

```
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  FreeBSD  6.X  device
10.33.107.29  FreeBSD  6.X  device
10.33.107.30  Unknown  device
10.33.107.31  Windows 10  client
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
10.33.107.38  Windows 10  client
10.33.107.39  Windows 10  client
```

```
10.33.102.171 - Remote Desktop Connection
msf6 auxiliary(scanner/smb/smb_version) >
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      Windows 10   client
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
10.33.107.38      Windows 10   client
10.33.107.39      Windows 10   client
10.33.107.40      Windows 10   client
10.33.107.41      Windows 10   client
10.33.107.42      Windows 10   client
10.33.107.43      Windows 10   client
10.33.107.44      Windows 10   client
10.33.107.45      Unknown      device
10.33.107.46      FreeBSD     6.X device
10.33.107.47      Unknown      device
10.33.107.48      Windows 10   client
10.33.107.49      Unknown      device
10.33.107.50      FreeBSD     6.X device
10.33.107.51      Unknown      device
10.33.107.52      Unknown      device
10.33.107.53      Unknown      device
10.33.107.54      Unknown      device
10.33.107.55      Unknown      device
10.33.107.56      Unknown      device
10.33.107.57      Unknown      device
10.33.107.58      Unknown      device
10.33.107.59      Unknown      device
10.33.107.60      Unknown      device
10.33.107.61      Unknown      device
10.33.107.62      Unknown      device
10.33.107.63      Unknown      device
10.33.107.84      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?

Jawab: Linux

Versi Paket Layanan mana yang diinstal di mesin 10.33.107.44?

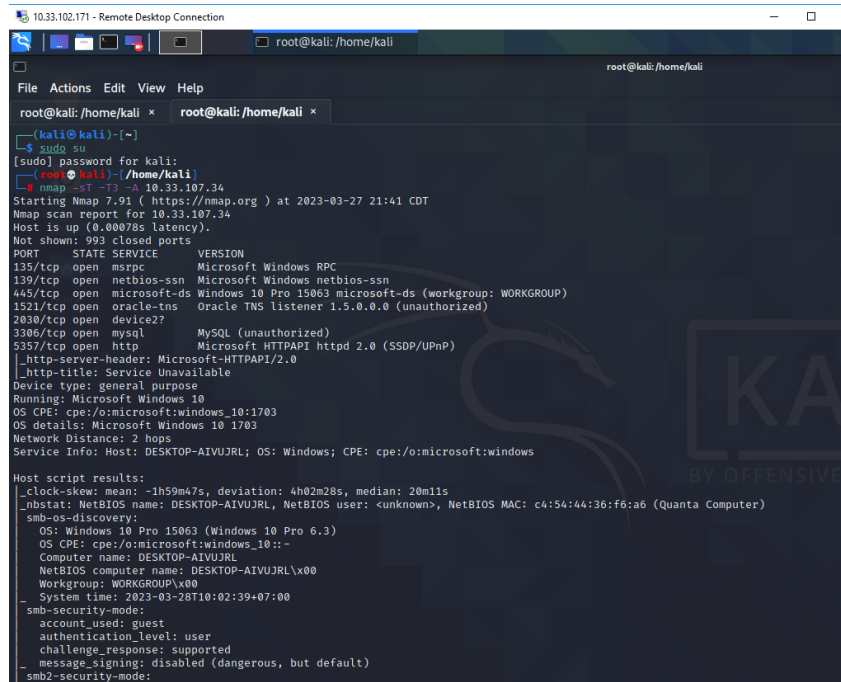
Jawab: tidak diketahui

Menjelajahi Berbagai Teknik Pemindaian Jaringan

Langkah Praktikum

1. Jalankan mesin Kali Linux dengan Remote Dekstop Connection di PC windows. Masukkan masing-masing IP yang sudah di sediakan

2. Masukkan password mhs_123 pilih username mahasiswa
3. Desktop Kali Linux muncul, klik ikon Terminal
4. Ketik perintah nmap -sT -T3 -A 10.10.10.10 (IP PC windows) dan tekan Enter untuk melakukan TCP Connect Scan pada Windows machine.



```
10.33.102.171 - Remote Desktop Connection
root@kali: /home/kali
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
(kali@kali) [~]
$ sudo su
[sudo] password for kali:
(root@kali) (/home/kali)
# nmap -sT -T3 -A 10.33.107.34
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:41 CDT
Nmap scan report for 10.33.107.34
Host is up (0.00078s 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)
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: -1h59m47s, deviation: 4h02m28s, median: 20m11s
_nbstat: NetBIOS name: DESKTOP-AIVUJRL, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:36:f6:a6 (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: 2023-03-28T10:02:39+07:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  smb2-security-mode:
```



```
10.33.102.171 - Remote Desktop Connection
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)
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

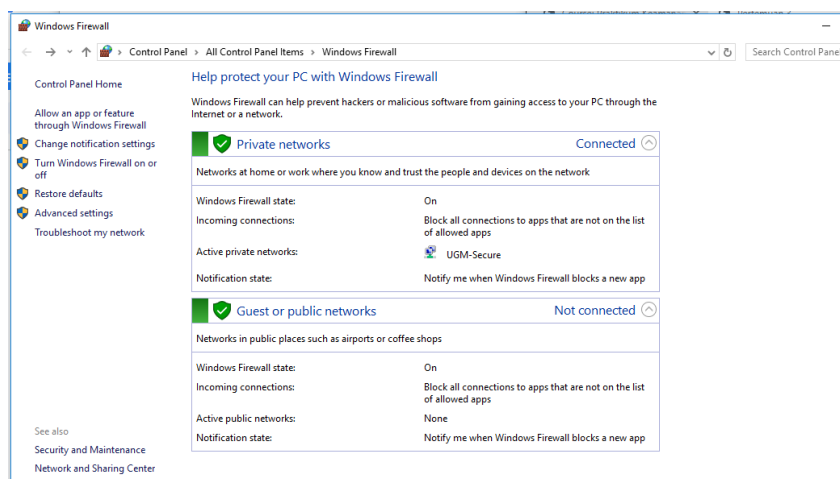
Host script results:
|_clock-skew: mean: -1h59m47s, deviation: 4h02m28s, median: 20m11s
|_nbstat: NetBIOS name: DESKTOP-AIVUJRL, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:36:f6:a6 (Quanta Computer)
|_smb-os-discovery:
|_  OS: Windows 10 Pro 15063 (Windows 10 Pro 6.3)
|_  OS CPE: cpe:/o:microsoft:windows_10::-
|_  Computer name: DESKTOP-AIVUJRL
|_  NetBIOS computer name: DESKTOP-AIVUJRLx00
|_  Workgroup: WORKGROUP\x00
|_  System time: 2023-03-28T10:02:39+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: 2023-03-28T03:02:39
|_  start_date: 2023-03-09T01:29:03

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.65 ms 10.33.102.254
2 1.46 ms 10.33.107.34

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.41 seconds

root@kali:~/home/kali
```

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



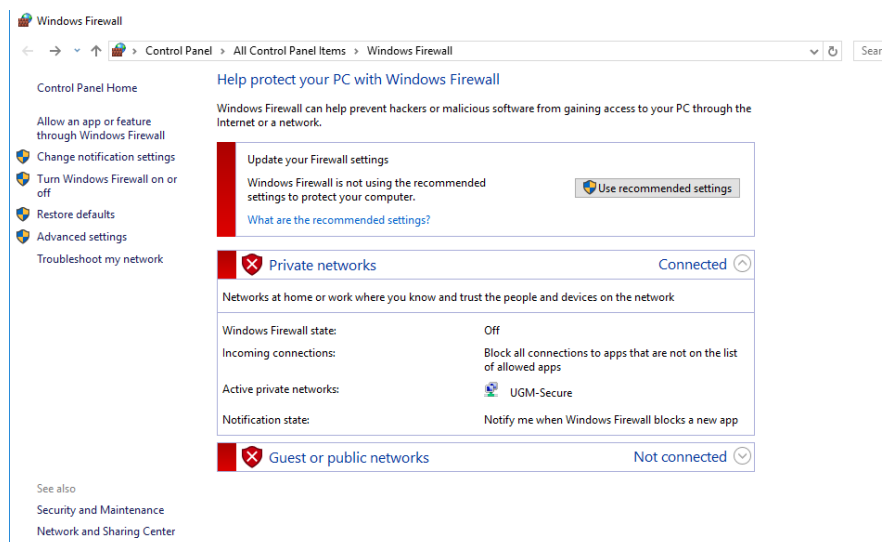
6. Beralih kembali ke mesin Kali Linux. Ketik nmap -sX -T4 10.10.10.12 di command prompt dan tekan Enter untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Ini menampilkan hasilnya seperti yang ditunjukkan pada tangkapan layar.

Hasil Nmap menunjukkan bahwa semua port dibuka/difilter yang berarti firewall dikonfigurasi pada komputer target

```
(root@kali)-[/home/kali]
# nmap -sX -T4 10.33.102.254
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:55 CDT
Nmap scan report for 10.33.102.254
Host is up (0.00030s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  filtered ftp
22/tcp    open  filtered ssh
23/tcp    open  filtered telnet
80/tcp    open  filtered http
2000/tcp  open  filtered cisco-sccp
8291/tcp  open  filtered unknown
MAC Address: 48:A9:8A:66:83:38 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

7. Beralih ke mesin Windows dan matikan Windows Firewall.



8. Beralih kembali ke mesin Kali Linux. Ketik `nmap -sA -v -T4 10.10.10.12` di terminal baris perintah. Ini memulai ACK Scan dan menampilkan disposisi port, seperti yang ditunjukkan pada tangkapan layar.

```
(root@kali)-[/home/kali]
# nmap -sA -v -T4 10.33.102.254
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 22:00 CDT
Initiating ARP Ping Scan at 22:00
Scanning 10.33.102.254 [1 port]
Completed ARP Ping Scan at 22:00, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:00
Completed Parallel DNS resolution of 1 host. at 22:00, 0.01s elapsed
Initiating ACK Scan at 22:00
Scanning 10.33.102.254 [1000 ports]
Completed ACK Scan at 22:00, 0.06s elapsed (1000 total ports)
Nmap scan report for 10.33.102.254
Host is up (0.00038s latency).
All 1000 scanned ports on 10.33.102.254 are unfiltered
MAC Address: 48:A9:8A:66:83:38 (Unknown)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)

(root@kali)-[/home/kali]
#
```

9. Ketik perintah `nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12`, dan tekan Enter

```
(root@kali)-[/home/kali]
# nmap -Pn -p 80 -sI 10.33.107.35 10.33.107.34
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 22:13 CDT
Idle scan using zombie 10.33.107.35 (10.33.107.35:80); Class: Incremental
Nmap scan report for 10.33.107.34
Host is up (0.20s latency).

PORT      STATE      SERVICE
80/tcp    closed|filtered http

Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds

(root@kali)-[/home/kali]
#
```

10. 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.

```
(root@kali)-[/home/kali]
# nmap -sP 10.33.107.35
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 22:14 CDT
Nmap scan report for 10.33.107.35
Host is up (0.0022s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

(root@kali)-[/home/kali]
#
```

V. ANALISIS

Pada praktikum keamanan informasi ini melakukan Pengumpulan Informasi Menggunakan Metasploit dan Menjelajahi Berbagai Teknik Pemindaian Jaringan, dimana tujuannya untuk menunjukkan bagaimana mengidentifikasi kerentanan dan pengungkapan informasi menggunakan Metasploit Framework serta cara menggunakan jenis teknik pemindaian jaringan menggunakan Nmap.

Langkah pertama yang dilakukan adalah dengan membuka “remote desktop connection” yang ada di PC windows, kemudian masukkan IP yang sudah ditentukan. Untuk IP yang saya gunakan adalah “10.33.102.171” setelah memasukkan IP maka kita akan diarahkan untuk memasukkan username serta password yang digunakan yaitu “username= kali” dan “password= kali”, Ketika masuk ke Remote Desktop Connectionnya pada bagian Authentication masukkan password yang sama, selanjutnya akan muncul desktop kali Linux lalu kita pilih ikon terminal dan masukkan perintah seperti yang ada pada modul.

Ketik `db_import Test` berguna untuk mengimpor hasil pengujian

Ketik `host` untuk menampilkan host dan detailnya seperti yang dikumpulkan oleh nmap.

Pada praktikum cara menggunakan Teknik pemindaian jaringan, Langkah pertama sama seperti sebelumnya yakni buka *remote desktop connection* dan masukkan username serta password kita, lalu masuk pada bagian terminal. Masukkan perintah `nmap -sT -T3 -A 10.33.107.34` (IP PC windows). Hal ini bertujuan untuk melakukan TCP Connect Scan pada Windows machine. Di sini `-T` digunakan untuk mengatur templat waktu dan `-A` digunakan untuk mengaktifkan deteksi OS, deteksi versi, pemindaian skrip, dan rute pelacak. TCP Connect Scan adalah bentuk paling dasar dari tcp scanning. Panggilan sistem `connect()` yang disediakan oleh sistem operasi Anda digunakan untuk membuka koneksi ke setiap port yang menarik pada mesin. Jika port

mendengarkan, connect() akan berhasil, jika tidak, port tidak dapat dijangkau. Salah satu keuntungan kuat dari teknik ini adalah Anda tidak memerlukan hak istimewa khusus. Ini melakukan pemindaian TCP dalam mode agresif dengan waktu normal (-T3). Setelah menyelesaikan pemindaian, hasilnya ditampilkan seperti yang ditunjukkan pada tangkapan layar. Gulir untuk membaca hasil pemindaian lengkap. Dibutuhkan, kira-kira, 5 menit untuk menyelesaikan pemindaian. Hasil pemindaian mencakup semua port terbuka, Hasil Sidik Jari Sistem Operasi, hasil nbstat, hasil penemuan smb-os, versi smb, dan sebagainya.

Beralih ke windows, masuk ke pengaturan dan aktifkan “windows firewall” dan balik lagi ke terminal untuk memasukkan perintah “nmap -sX -T4 10.33.102.254” untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Lalu balik lagi ke windows firewall untuk dimatikan dan Kembali ke terminal untuk perintah selanjutnya yakni masukkan perintah “nmap -sA -v -T4 10.33.102.254” berguna untuk memulai ACK Scan dan menampilkan disposisi port, pada hal ini penyerang mengirim paket probe ACK dengan nomor urut acak.

Tidak ada respons yang berarti port difilter dan respons tanpa filter berarti port ditutup. Selanjutnya ketik perintah nmap -Pn -p 80 -sI 10.33.107.35 (IP PC/IP zombie) 10.33.107.34 (IP server/lawan).

Dengan cara ini, kita dapat menggunakan berbagai teknik pemindaian lainnya, seperti Inverse TCP Flag Scan dan Stealth Scan, untuk menemukan port terbuka, layanan yang berjalan di port, dan sebagainya.

Ada beberapa istilah pada footprinting yaitu:

- *Open source atau passive information gathering*

Mengumpulkan informasi tentang sebuah target yang diperoleh dari sumber yang bersifat umum.

- *Active information gathering (mengumpulkan informasi aktif)*

Mengumpulkan informasi baik dari ilmu keahlian teknik di website-website, wawancara ataupun dengan tanya jawab.

- *Anonymous footprinting (Foot printing tidak diketahui (misteri)*

Mengumpulkan informasi dari sumber yang dimana penulis dari informasi tersebut tidak bisa diidentifikasi atau tidak diketahui siapa penulisnya.

- *Pseudonymous footprinting(footprinting dengan nama samaran)*

Mengumpulkan informasi yang dipublikasikan dengan nama yang berbeda disebuah percobaan untuk menjaga rahasia pribadi atau kebebasan pribadi.

- *Organizational or private footprinting (organisasi atau footprinting pribadi*

Mengumpulkan informasi dari sebuah web organisasi berdasarkan penanggalan atau jasa email (email-service)

- *Internet footprinting : Mengumpulkan informasi target dari internet*
.

VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Tahapan pertama pada fase peretasan adalah melakukan footprinting atau pengintaian.
- Tujuan dari footprinting yaitu untuk mengumpulkan informasi dari target bisa melalui jaringan internet.
- Scanning adalah kegiatan yang bertujuan mencari celah jalur penyusupan yang lebih spesifik
- 3 macam tipe scanning: port scanning, network scanning dan vulnerability scanning.
- Network Enumeration, dilakukan untuk melihat domain yang digunakan oleh sebuah organisasi. Dengan menggunakan tools “whois” kita dapat melakukan kegiatan ini.

VII. DAFTAR PUSTAKA

Prak KI 1. (2023). Materi Pertemuan 7. Retrieved April 3, 2023, from Elok UGM

Supardianto. (2021, June 15). *Apa ITU footprinting?* Blog Rekayasa Keamanan Siber. Retrieved April 3, 2023, from <https://if.polibatam.ac.id/rekayasa-keamanan-siber/blog/?p=57>

Vilela, A. B. (2015, October 20). *Definisi footprinting Dan Cara jerja serta contohnya.* Academia.edu. Retrieved April 3, 2023, from https://www.academia.edu/17049934/Definisi_Footprinting_dan_cara_jerja_serta_contohnya

Jenis - Jenis Serangan Cyber crime. Codepolitan. (n.d.). Retrieved April 3, 2023, from <https://www.codepolitan.com/jenis-jenis-serangan-cyber-crime/>