LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 7 BAGIAN I
FOOTPRINTING DAN RECONNAISSANCE

DISUSUN OLEH:

Nama	: Yana Dayinta Nesthi
Kelas	: RI4AA
NIM	: 21/478358/SV/19272
Dosen	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

FOOTPRINTING DAN RECONNAISSANCE

A. TUJUAN

Tujuan dari lab ini adalah untuk menunjukkan bagaimana mengidentifikasi kerentanan dan pengungkapan informasi menggunakan Metasploit Framework. Siswa akan belajar bagaimana: Ekstrak informasi akurat tentang jaringan menggunakan Metasploit Framework.

B. DASAR TEORI

Footprinting merupakan metode dalam keamanan komputer yang digunakan untuk mengumpulkan informasi tentang sistem komputer dan entitas yang terkait. Footprinting menjadi salah satu tahap pra-serangan sebelum melakukan serangan secara langsung. Baik itu hacker etis atau hacker jahat menggunakan teknik ini untuk menemukan kelemahan dan kerentanan keamanan dalam jaringan. Proses keamanan siber dari teknik footprinting melibatkan profil organisasi dan pengumpulan data sebanyak mungkin tentang sistem komputer, infrastruktur, dan jaringan tertentu untuk mengidentifikasi celah yang bisa dimanfaatkan.

Terdapat dua jenis teknik footprinting, yaitu aktif dan pasif. Footprinting aktif dilakukan dengan menggunakan alat dan teknik seperti ping sweep atau perintah traceroute untuk mengumpulkan data tentang target tertentu. Hal ini sering memicu sistem deteksi intrusi (IDS) target. Footprinting pasif merupakan pendekatan yang lebih diam-diam karena tidak memicu IDS target. Teknik ini melibatkan pengumpulan informasi tentang target dengan mencari sumber publik seperti media sosial, posting pekerjaan, dan situs web perusahaan.

Footprinting menjadi bagian penting dalam latihan peretasan awal. Ini merupakan teknik pengintaian pasif di mana seseorang mengumpulkan semua informasi yang tersedia tentang sistem komputer atau jaringan untuk mendapatkan akses ke dalamnya. Profesional keamanan menggunakan teknik ini untuk mengevaluasi postur keamanan organisasi dan memberikan informasi penting mengenai kerentanan keamanan siber. Bagi para hacker, teknik ini digunakan untuk mengumpulkan informasi tentang target yang kemudian dapat digunakan dalam merencanakan serangan.

Footprinting dan reconnaissance terkait tetapi konsep yang berbeda dalam bidang keamanan siber. Footprinting adalah proses pengumpulan informasi tentang jaringan target dan lingkungannya, yang dapat membantu para hacker menemukan peluang untuk menembus dan menilai jaringan target. Footprinting adalah langkah pertama dalam setiap serangan, di mana penyerang mengumpulkan informasi tentang target dengan menggunakan berbagai cara. Footprinting dapat bersifat pasif atau aktif, tergantung pada apakah penyerang berinteraksi langsung dengan target. reconnaissance pasif melibatkan pengumpulan informasi yang tersedia secara publik, seperti nama domain tingkat atas dan sub-domain target melalui layanan web. reconnaissance aktif melibatkan penggunaan alat

dan teknik, seperti melakukan ping sweep atau menggunakan perintah traceroute, untuk mengumpulkan informasi tentang target.

Reconnaissance adalah tahap pengumpulan informasi dalam hacking etis, di mana data tentang sistem target dikumpulkan. Reconnaissance adalah istilah yang lebih luas yang mencakup reconnaissance sebagai salah satu komponennya. reconnaissance dapat bersifat aktif atau pasif, tergantung pada apakah penyerang berinteraksi langsung dengan target. reconnaissance aktif melibatkan penggunaan alat seperti pemindai untuk mengumpulkan informasi tentang sistem yang ditargetkan. Reconnaissance pasif melibatkan pengumpulan informasi tentang target tanpa berinteraksi langsung dengannya.

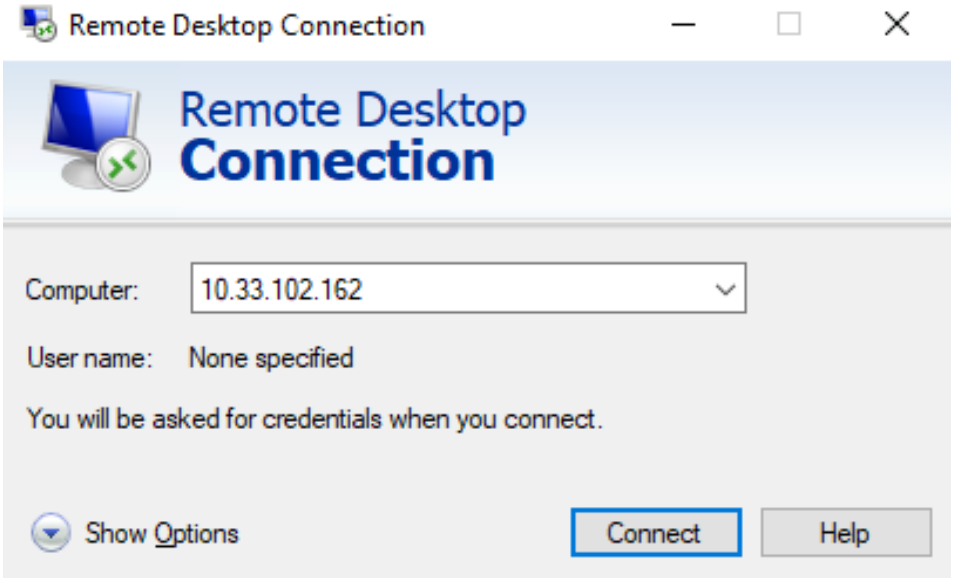
Secara ringkas, footprinting adalah bagian dari proses reconnaissance yang lebih besar, yang melibatkan pengumpulan informasi tentang sistem target. Footprinting adalah langkah pertama dalam setiap serangan, di mana penyerang mengumpulkan informasi tentang target dengan menggunakan berbagai cara. Footprinting dapat bersifat pasif atau aktif, tergantung pada apakah penyerang berinteraksi langsung dengan target. reconnaissance adalah tahap pengumpulan informasi dalam hacking etis, di mana data tentang sistem target dikumpulkan. reconnaissance dapat bersifat aktif atau pasif, tergantung pada apakah penyerang berinteraksi langsung dengan target.

C. ALAT DAN BAHAN

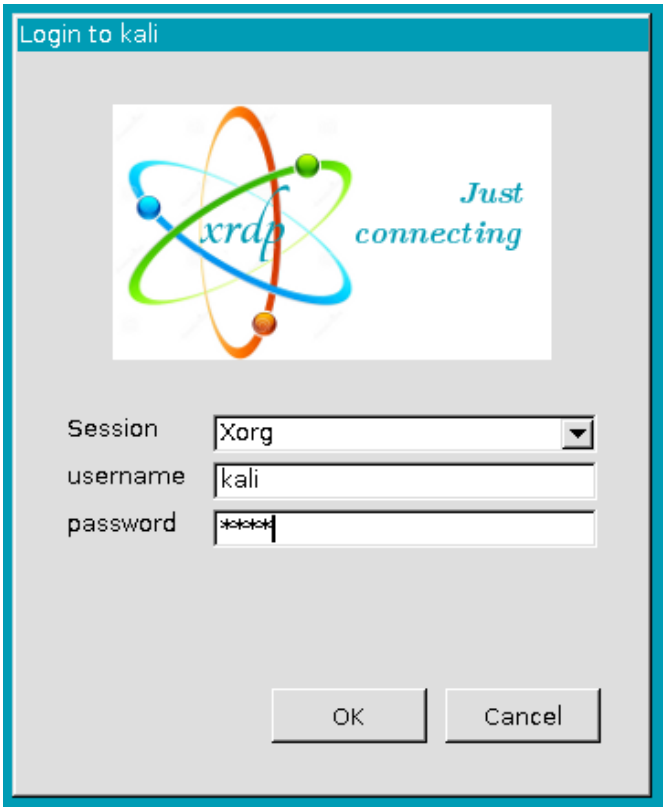
a. PC
b. Koneksi internet
c. OS Windows

D. HASIL DAN ANALISIS

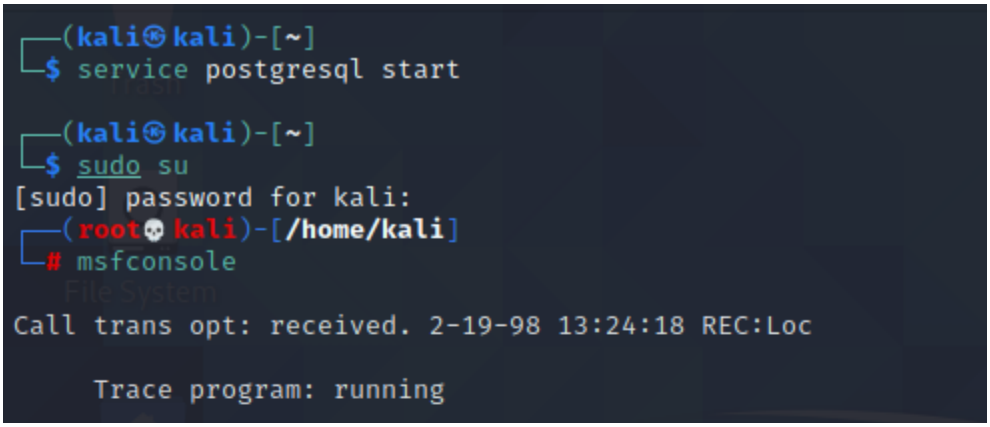
1. Jalankan mesin Kali Linux dengan Remote Desktop Connection di PC windows. Masukkan masing-masing IP yang sudah disediakan



2. Masukkan password kali pilih username kali



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



7. Di baris perintah msf, ketik db_status dan tekan Enter. Jika Anda mendapatkan postgresql yang dipilih, no connection , maka database tidak dimulai.
8. Jika Anda mendapatkan postgresql terhubung ke pesan msf, lewati ke Langkah 13.

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

9. 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 2023-03-27 20:22 CDT
```

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

```
Nmap scan report for 10.33.107.100
Host is up (0.43s latency).
All 1000 scanned ports on 10.33.107.100 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
-   Hops 1-30 are the same as for 10.33.107.49
```

```
TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
-   Hop 1 is the same as for 10.33.107.49
2   10.33 ms 10.33.107.105

Nmap scan report for 10.33.107.106
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
|   1024 2e:d8:af:eb:89:dd:91:0c:6b:20:40:77:65:9b:48:69 (RSA1)
|_  1024 57:99:15:56:bf:03:9d:20:45:30:e9:86:f5:2c:c9:c8 (RSA)
|_sshv1: Server supports SSHv1
23/tcp  open  telnet     Cisco router telnetd
80/tcp  open  http       Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_access
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=IOS-Self-Signed-Certificate-1865015680
| Not valid before: 1993-03-01T00:01:04
|_Not valid after:  2020-01-01T00:00:00
|_ssl-date: 1993-04-19T20:11:50+00:00; -29y342d05h54m16s from scanner time.
Device type: switch
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:catalyst_1900 cpe:/h:cisco:catalyst_2820 cpe:/h:cisco:catalyst_2960 cpe:/
h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_4500 cpe:/h:cisco:catalyst_6513 cpe:/o:cisco:ios:1
2.2
OS details: Cisco Catalyst 1900, 2820, 2960, 3560, 3750, 4500, or 6513 switch (IOS 12.2)
Network Distance: 2 hops
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
```

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

```
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 10.33.107.123
[*] Importing host 10.33.107.124
[*] Importing host 10.33.107.125
[*] Importing host 10.33.107.126
[*] Importing host 10.33.107.127
[*] Successfully imported /home/kali/Test
```

12. Ketik hosts dan tekan Enter untuk menampilkan host dan detailnya seperti yang 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
```

```
10.33.107.21               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
10.33.107.38               Windows 10                    client
10.33.107.39               Windows 10                    client
```

Apakah Nmap sudah mengumpulkan informasi os_flavor?

13. KETIK db_nmap -sS -A -Pn 10.33.107.84 dan Enter. Ditambah -Pn karena mengikuti saran pada hasil console (baris kedua)

```
msf6 > db_nmap -sS -A 10.33.107.84
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 20:37 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 3.59 seconds
```

Setelah ditambahkan -Pn:

```
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 20:50 CDT
[*] Nmap: Nmap scan report for 10.33.107.84
[*] Nmap: Host is up (0.16s 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   0.23 ms   10.33.102.254
[*] Nmap: 2   ... 5
[*] Nmap: 6   987.91 ms 10.33.102.254
[*] Nmap: 7   987.92 ms 10.33.102.254
[*] Nmap: 8   987.93 ms 10.33.102.254
[*] Nmap: 9   987.94 ms 10.33.102.254
[*] Nmap: 10  988.02 ms 10.33.102.254
[*] Nmap: 11  977.56 ms 10.33.102.254
[*] Nmap: 12  981.31 ms 10.33.102.254
[*] Nmap: 13  981.24 ms 10.33.102.254
[*] Nmap: 14  981.22 ms 10.33.102.254
[*] Nmap: 15  981.21 ms 10.33.102.254
[*] Nmap: 16  981.19 ms 10.33.102.254
[*] Nmap: 17  ...
[*] Nmap: 18  970.96 ms 10.33.102.254
[*] Nmap: 19  ... 21
[*] Nmap: 22  982.19 ms 10.33.102.254
[*] Nmap: 23  982.13 ms 10.33.102.254
[*] Nmap: 24  982.13 ms 10.33.102.254
[*] Nmap: 25  ... 27
```

```
[*] Nmap: 28  961.74 ms 10.33.102.254
[*] Nmap: 29  951.54 ms 10.33.102.254
[*] Nmap: 30  951.49 ms 10.33.102.254
[*] 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 65.50 seconds
```

14. Nmap memindai mesin dan memberi Anda detail layanan yang berjalan di mesin. Ini adalah bagaimana Anda dapat menemukan layanan pada masing-masing mesin.
15. 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:
ORKGROUP
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:
ORKGROUP
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:
ORKGROUP
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:
ORKGROUP
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:
ORKGROUP
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
```

16. Ketik use scanner/smb/smb_version dan tekan Enter untuk memuat modul pemindai SMB.
17. Kemudian ketik show options dan tekan Enter untuk menampilkan opsi konfigurasi yang terkait dengan modul.

```
msf6 > use scanner/smb/smb_version
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 wi
th syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

18. 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 THREADS 100
THREADS ⇒ 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.33.107.8-16:       - Scanned 1 of 9 hosts (11% complete)
[*] 10.33.107.8-16:       - Scanned 4 of 9 hosts (44% 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 8 of 9 hosts (88% complete)
[*] 10.33.107.8-16:       - Scanned 9 of 9 hosts (100% complete)
[*] Auxiliary module execution completed
```

19. Ketik hosts dan tekan Enter. Sekarang dapat terlihat jika informasi os_flavor sudah terkumpul.

```
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
```

```
10.33.107.21               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
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
```

PEMBAHASAN:

Cara menjalankan Kali Linux dengan Remote Desktop Connection di PC windows, mulai dari memasukkan IP dan password Kali, membuka terminal, memulai PostgreSQL, masuk sebagai root, menjalankan Metasploit Framework, melakukan pemindaian subnet menggunakan Nmap, mengimpor hasil pengujian, menampilkan host dan detailnya, mendapatkan informasi layanan dari semua komputer aktif di subnet, memuat modul pemindai SMB, dan menampilkan opsi konfigurasi yang terkait dengan modul tersebut. Terakhir, mengecek apakah informasi os_flavor sudah terkumpul. Namun sayangnya, pada praktikum kali ini meskipun sudah dicoba beberapa kali, pada bagian os_flavor tetap kosong dan tidak menampilkan informasi apapun.

E. KESIMPULAN

Footprinting adalah metode dalam keamanan komputer untuk mengumpulkan informasi tentang sistem komputer dan entitas yang terkait. Ada dua jenis footprinting: pasif dan aktif, di mana yang pasif lebih diam-diam dan tidak memicu IDS target. Cara menjalankan Kali Linux dengan Remote Desktop Connection di PC Windows melibatkan beberapa langkah, termasuk memulai PostgreSQL, menjalankan Metasploit Framework, melakukan pemindaian subnet menggunakan Nmap, mengimpor hasil pengujian, menampilkan host dan detailnya, dan mengecek informasi os_flavor.

LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
PERTEMUAN 7 BAGIAN 2
MENJELAJAHI BERBAGAI TEKNIK PEMINDAIAN JARINGAN

DISUSUN OLEH:

Nama	: Yana Dayinta Nesthi
Kelas	: RI4AA
NIM	: 21/478358/SV/19272
Dosen	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

Menjelajahi Berbagai Teknik Pemindaian Jaringan

A. TUJUAN

Praktikum ini akan menunjukkan berbagai opsi pemindaian menggunakan Nmap

B. DASAR TEORI

Pemindaian jaringan merujuk pada proses mengenali host aktif pada suatu jaringan dan memetakan alamat IP mereka. Proses ini dikenal juga sebagai penemuan host dan sering merupakan langkah awal yang diambil oleh peretas saat menyiapkan serangan. Ada dua jenis pemindaian jaringan utama, yaitu pemindaian port dan pemindaian kerentanan. Pemindaian port mengidentifikasi port terbuka di jaringan yang dapat menerima atau mengirim data. Pemindaian kerentanan mengidentifikasi kerentanan potensial dalam jaringan .

Pemindaian jaringan sangat penting dalam keamanan jaringan karena membantu mengenali kerentanan potensial dan area jaringan yang lebih rentan terhadap serangan. Dengan melakukan pemindaian jaringan secara teratur, organisasi dapat mendeteksi dan memperbaiki masalah keamanan secara proaktif sebelum aktor jahat mengeksploitasi kerentanan tersebut. Selain itu, pemindaian jaringan membantu organisasi mematuhi standar dan regulasi industri dengan mengenali kerentanan jaringan yang harus ditangani.

Terdapat berbagai alat dan layanan open-source dan berbayar yang tersedia untuk pemindaian jaringan, seperti Nmap untuk pemindaian port, Nessus untuk pemindaian kerentanan, dan Fping untuk ping sweeping. Alat-alat ini dapat memberikan informasi berharga tentang jaringan dan membantu mengenali kerentanan potensial. Pemindaian jaringan juga dapat merujuk pada packet sniffing, atau pemindaian pasif, yang menangkap dan melacak lalu lintas yang bergerak di atas jaringan dalam bentuk paket.

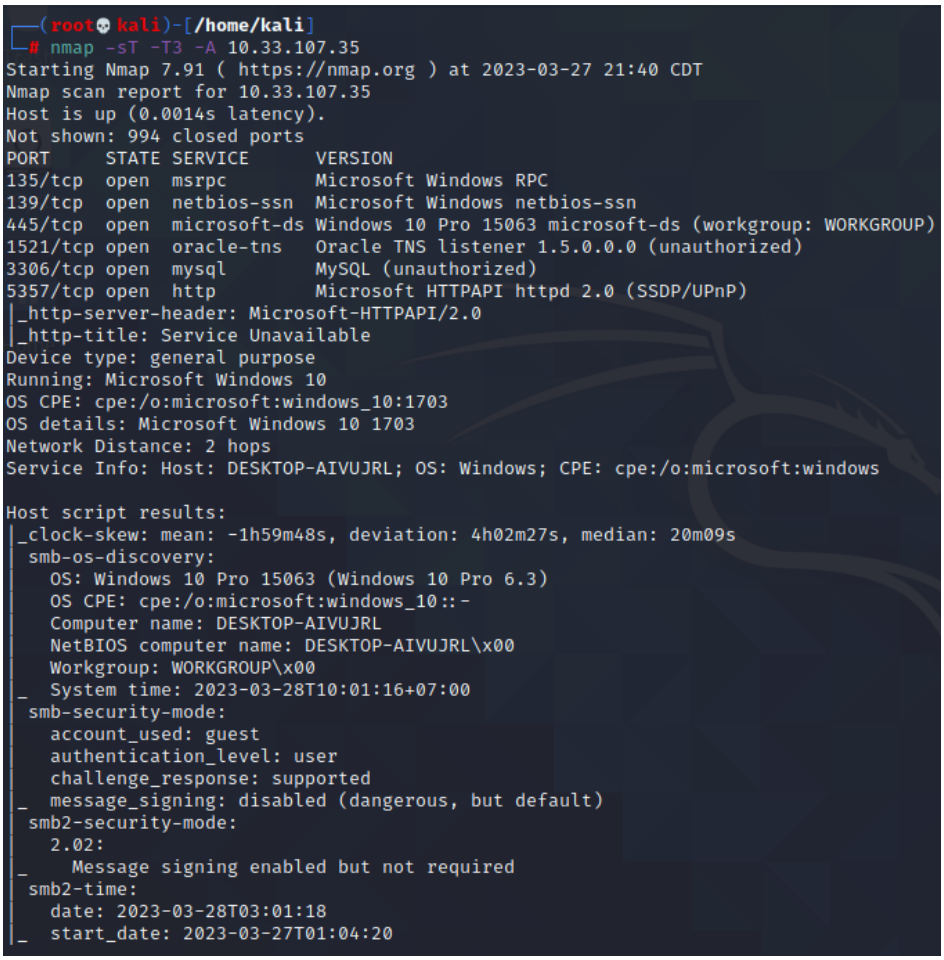
Secara singkat, pemindaian jaringan adalah proses mengenali host aktif pada suatu jaringan dan memetakan alamat IP mereka. Ini sangat penting dalam keamanan jaringan karena membantu mengenali kerentanan potensial dan area jaringan yang lebih rentan terhadap serangan. Terdapat berbagai alat dan layanan yang dapat digunakan untuk pemindaian jaringan, seperti Nmap untuk pemindaian port dan Nessus untuk pemindaian kerentanan. Pemindaian jaringan yang teratur dapat membantu organisasi menjaga infrastruktur jaringan yang aman dan mematuhi standar dan regulasi industri.

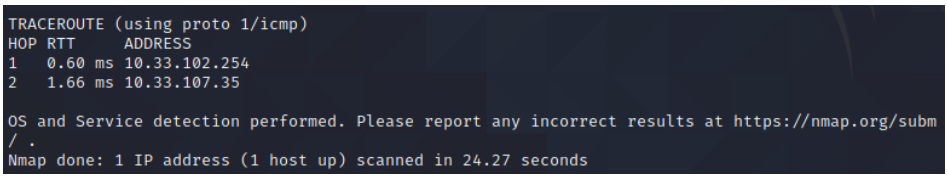
C. ALAT DAN BAHAN

a. PC
b. OS Windows

D. HASIL DAN ANALISIS

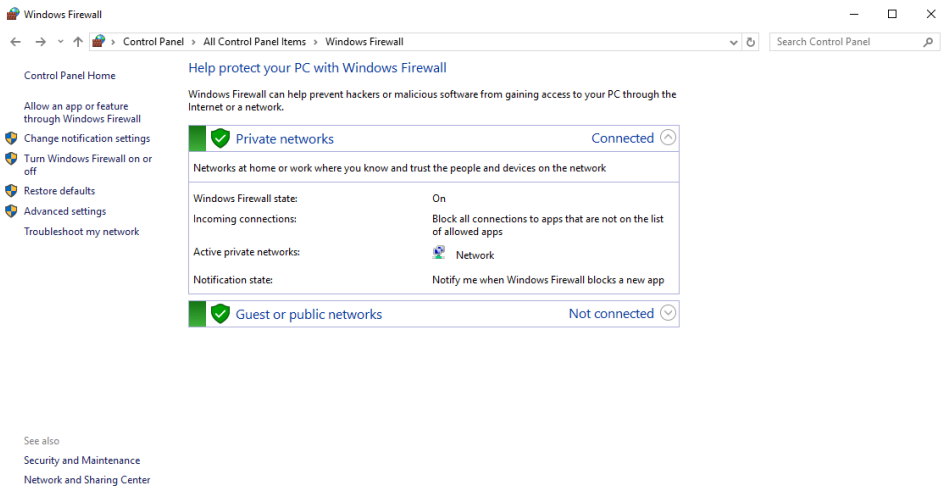
1. Jalankan mesin Kali Linux dengan Remote Desktop Connection di PC windows. Masukkan masing-masing IP yang sudah disediakan
2. Masukkan password kali pilih username kali
3. Desktop Kali Linux muncul, klik ikon Terminal
4. Ketik perintah nmap -sT -T3 -A 10.10.10.10 (IP PC windows) dan tekan Enter untuk melakukan TCP Connect Scan pada Windows machine





\

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

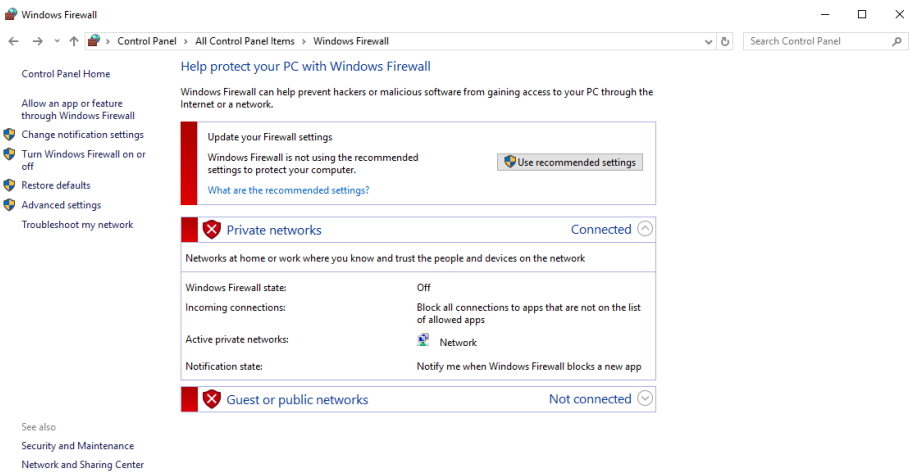


6. Beralih kembali ke mesin Kali Linux. Ketik nmap -sX -T4 10.10.10.12 di command prompt dan tekan Enter untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Ini menampilkan hasilnya seperti yang ditunjukkan pada tangkapan layar. Hasil Nmap menunjukkan bahwa semua port dibuka/di filter yang berarti 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 21:49 CDT
Nmap scan report for 10.33.102.254
Host is up (0.00042s 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 1.41 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 21:55 CDT
Initiating ARP Ping Scan at 21:55
Scanning 10.33.102.254 [1 port]
Completed ARP Ping Scan at 21:55, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:55
Completed Parallel DNS resolution of 1 host. at 21:55, 0.00s elapsed
Initiating ACK Scan at 21:55
Scanning 10.33.102.254 [1000 ports]
Completed ACK Scan at 21:55, 0.06s elapsed (1000 total ports)
Nmap scan report for 10.33.102.254
Host is up (0.00036s 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 0.23 seconds
           Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
```

9. Ketik perintah nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12, dan tekan Enter. Jika port tidak terbuka pada mesin target, terus pemberlakukan pemindaian IDLE dengan menyelidiki port lain. Hasil pemindaian menyatakan bahwa port 80 pada Windows Server 2012 closed|filtered.

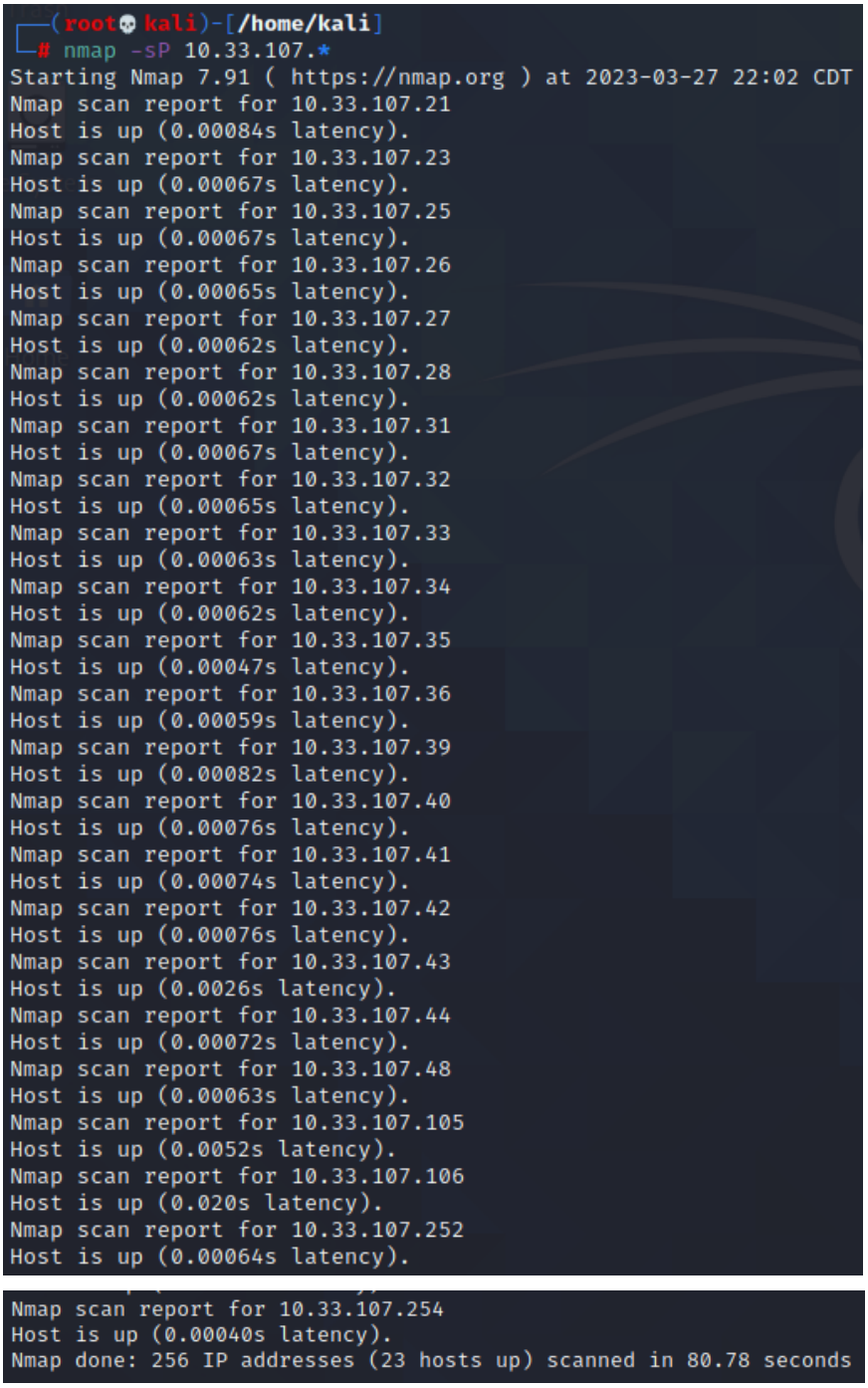
```
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn -p 80 -sI 10.33.107.31 10.33.102.254
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 22:06 CDT
Idle scan using zombie 10.33.107.31 (10.33.107.31:80); Class: Incremental
Nmap scan report for 10.33.102.254
Host is up (0.0017s latency).

PORT   STATE           SERVICE
80/tcp closed|filtered http
MAC Address: 48:A9:8A:66:83:38 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

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.



Dengan cara ini, Anda 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.

Setelah lab selesai, tutup jendela terminal dan jendela firewall windows yang terbuka. Di lab ini,

Anda telah belajar cara menggunakan jenis berikut teknik pemindaian jaringan menggunakan Nmap.

- TCP Connect Scan
- Xmas Scan
- ACK Flag Scan
- UDP Scan
- IDLE Scan

PEMBAHASAN:

Ini adalah ringkasan dari penggunaan teknik pemindaian jaringan TCP Connect Scan dengan opsi -T dan -A pada Nmap. Teknik ini menggunakan panggilan sistem connect() untuk membuka koneksi ke setiap port pada mesin dan mendeteksi apakah port tersebut terbuka atau tidak. Tidak memerlukan hak istimewa khusus dan memakan waktu sekitar 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. Selain itu, pada praktikum ini juga memberikan informasi tentang teknik pemindaian jaringan lainnya seperti Xmas Scan, ACK Flag Scan, UDP Scan, IDLE Scan.

E. KESIMPULAN

Teknik pemindaian jaringan TCP Connect Scan memanfaatkan panggilan sistem connect() untuk membuka koneksi ke setiap port pada mesin dan mengidentifikasi apakah port tersebut terbuka atau tidak. Hasil dari pemindaian ini mencakup informasi mengenai semua port yang terbuka, sistem operasi, hasil nbstat, hasil penemuan smb-os, versi smb, dan lain sebagainya.

F. DAFTAR PUSTAKA

Cisco. (2020, February 16). *Reconnaissance vs Footprinting*. Cisco Learning Network. Diakses pada April 1, 2023, dari https://learningnetwork.cisco.com/s/question/0D53i00000Ksr7uCAB/reconnaissance-vs-footprinting

EC-Council. (n.d.). *What Are Footprinting and Reconnaissance?* EC-Council. Diakses pada April 1, 2023, dari https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/basics-footprinting-reconnaissance/

Sekyour. (2022). *Network Scanning*. Identifying Active Hosts, Open Ports, and Vulnerabilities. Diakses pada April 1, 2023, dari https://sekyour.com/post/network-scanning/

Zola, A. (n.d.). *What is footprinting in ethical hacking?* TechTarget. Diakses pada April 1, 2023, dari https://www.techtarget.com/searchsecurity/definition/footprinting