LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 7

Footprinting & Scanning

DISUSUN OLEH

Nama	: Muhamad Alan Dharma Saputro S
NIM	: 21/481348/SV/19761
Hari, Tanggal	: Selasa, 28 Maret 2023
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Kelas	: RI4AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. Tujuan

1. Memahami bagaimana ekstrak informasi akurat tentang jaringan menggunakan Metasploit Framework.
2. Memahami berbagai teknik pemindaian jaringan.

B. Latar Belakang.

Metasploit framework adalah sebuah penetration tool yang cukup kuat untuk menyusup ke sistem. Metasploit termasuk sebuah framework penetrasi jaringan komputer yang free dan open source, metasploit dikembangkan oleh H.D. Moore pada tahun 2003 dan sekarang Rapid7 membelinya. Metasploit Framework juga bisa disebut sebagai platform pengembangan untuk membuat alat dan aset keamanan. Fungsi dasar dari metasploit framework adalah membuat modul, memungkinkan pengguna untuk mengkonfigurasikan modul exploit dan mengujinya pada target yang dimaksud. Metasploit Framework memfasilitasi tugas penyerang, mengeksploitasi penulis, dan penulis muatan. Keuntungan utama dari kerangka kerja ini adalah pendekatan modular yaitu memungkinkan kombinasi eksploitasi apa pun dengan muatan apa pun.

Software pemindaian port dalam mode dasar mengirimkan permintaan koneksi ke komputer target pada setiap port secara bergantian dan mencatat port mana yang merespons atau tampak terbuka untuk penyelidikan lebih lanjut. Dengan menyetel flag TCP yang berbeda atau mengirimkan jenis paket TCP yang berbeda, pemindaian port dapat mengembalikan hasil yang berbeda atau mencari port yang terbuka dengan cara yang berbeda. Pemindaian SYN memberi tahu pemindai port port mana yang mendengarkan dan mana yang tidak, tergantung pada respons yang dihasilkannya. Pemindaian FIN menghasilkan respons dari port tertutup - tetapi port terbuka dan mendengarkan tidak mengirimkan respons, memungkinkan pemindai port untuk menentukan port mana yang terbuka dan mana yang tidak.

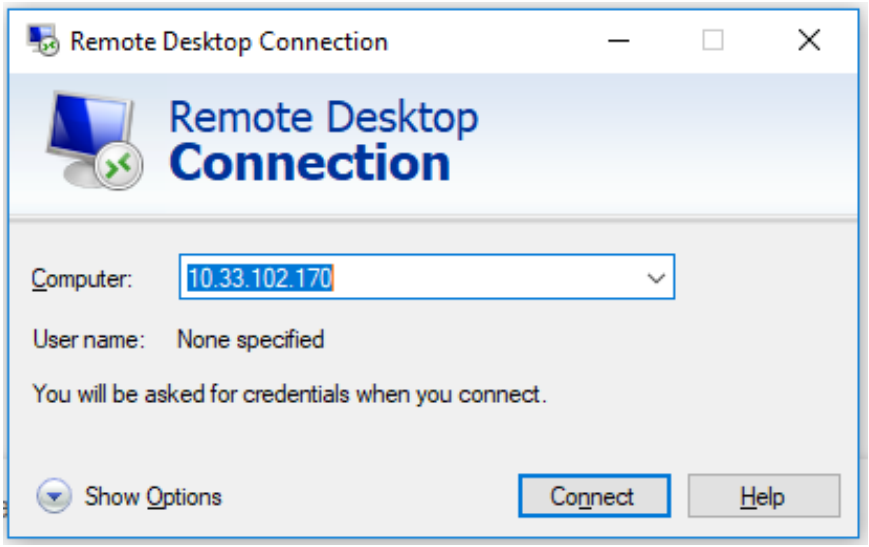
C. Alat dan Bahan

- Mesin Kali Linux

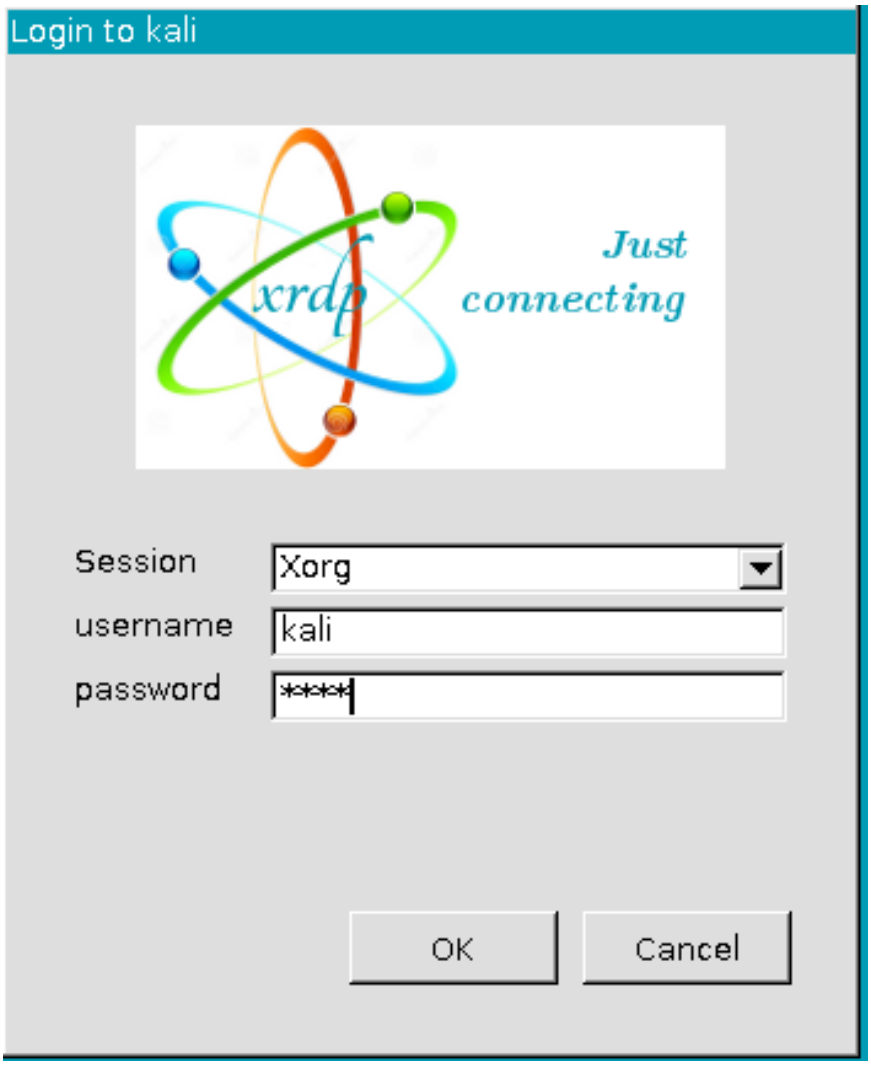
D. Intruksi Kerja

Footprinting dan Reconnaissance

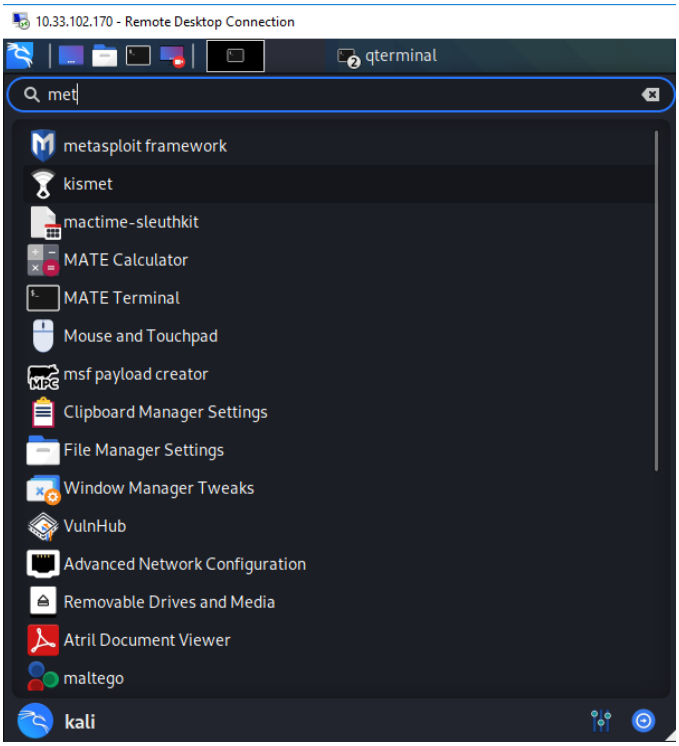
1. Jalankan mesin Kali Linux dengan Remote Dekstop Connection di PC windows. Masukkan masing-masing IP yang sudah di sediakan.



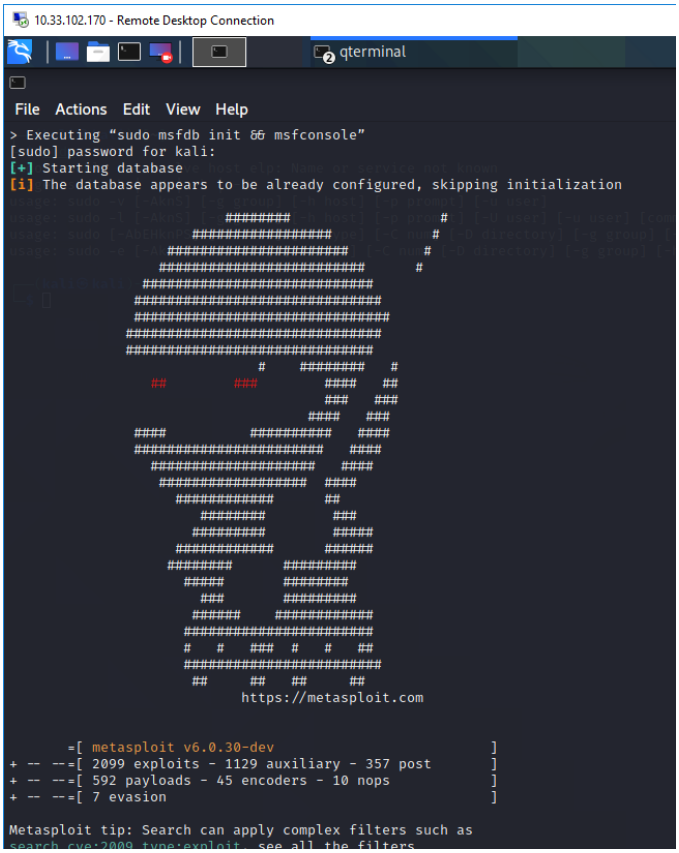
2. Login ke Kali Linux dengan memasukkan username dan password yaitu kali.



3. Desktop Kali Linux muncul, tuliskan dipencarian MATE Terminal lalu klik.

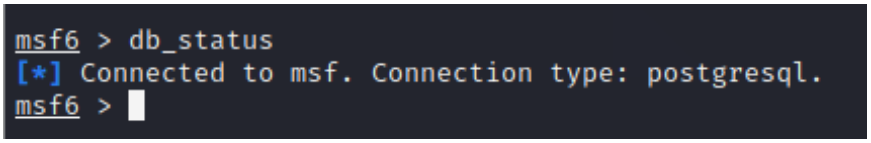


4. Di jendela terminal, ketik sudo msfdb init && msfconsole, untuk masuk ke database. Masukkan password yaitu kali.

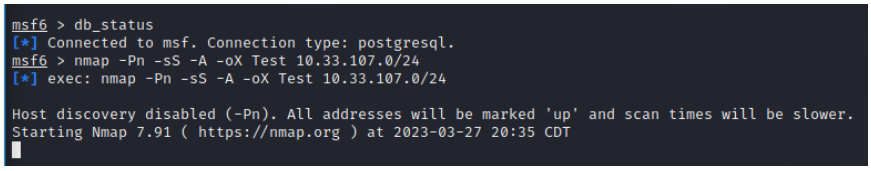


5. Tunggu hingga Metasploit Framework diluncurkan.

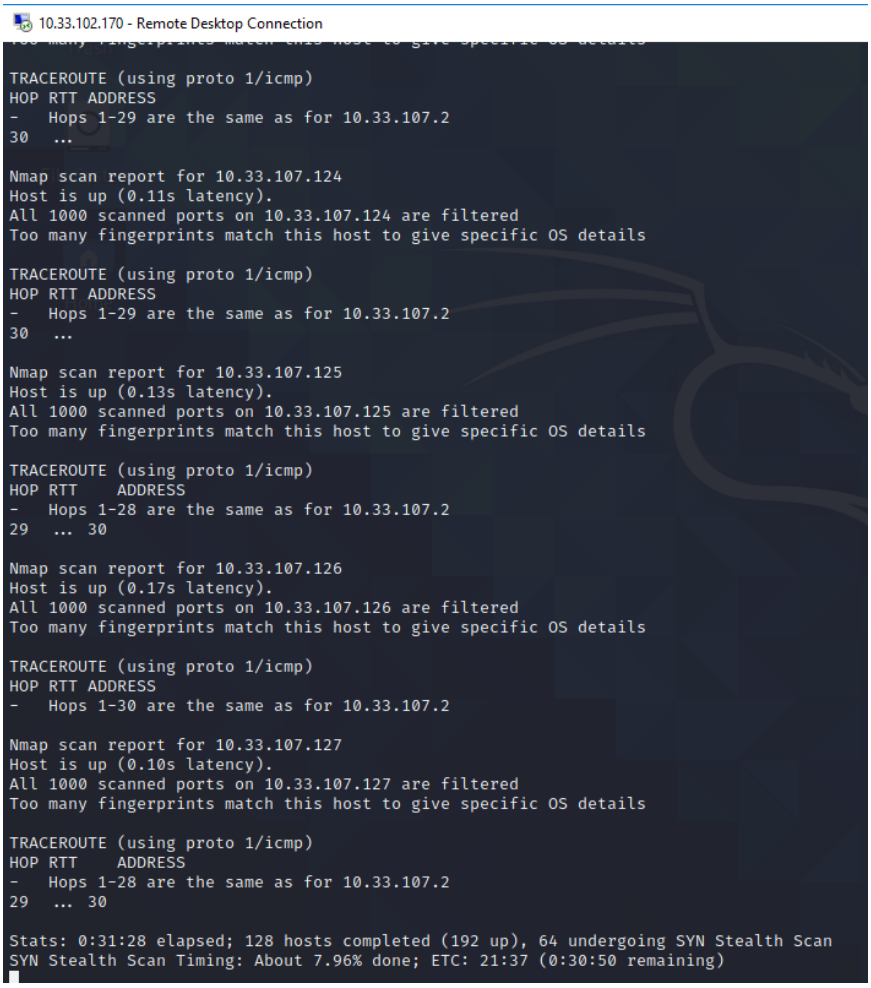
6. Di baris perintah msf, ketik db_status dan tekan Enter. Jika Anda mendapatkan postgresql yang dipilih, no conecction , maka database tidak dimulai.



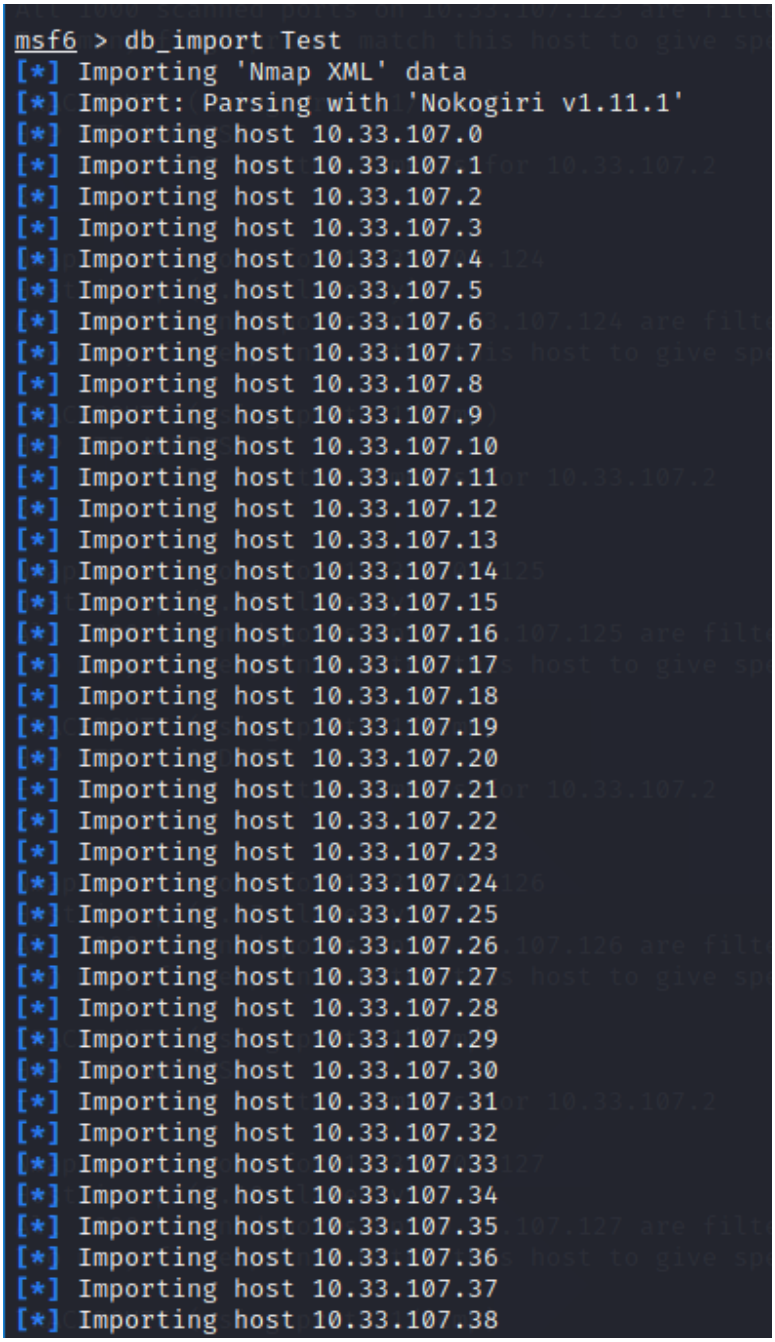
7. Ketik nmap -Pn -sS -A -oX Test 10.33.107.0/24 dan tekan Enter. Dibutuhkan sekitar 10 menit bagi namp untuk menyelesaikan pemindaian subnet.



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



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



10. 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
10.33.107.4                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               Unknown                        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
```

11. 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 21:11 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 3.51 seconds
msf6 >
```

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

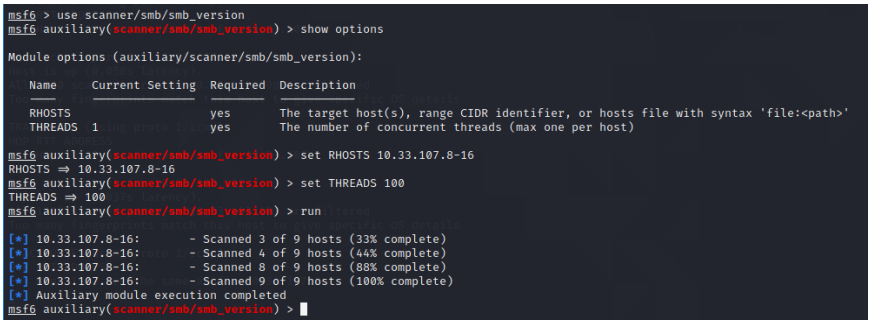
```
msf6 > services
Services
========

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    tcpwrapped      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
10.33.107.31  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
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    msrpc           open   Microsoft Windows RPC
```

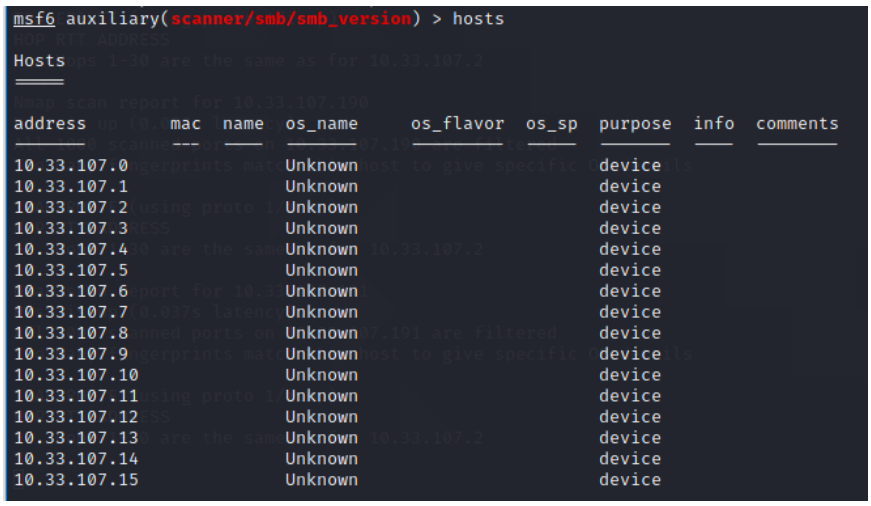
13. Ketik use scanner/smb/smb_version dan tekan Enter untuk memuat modul pemindai SMB.

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

15. 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.



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



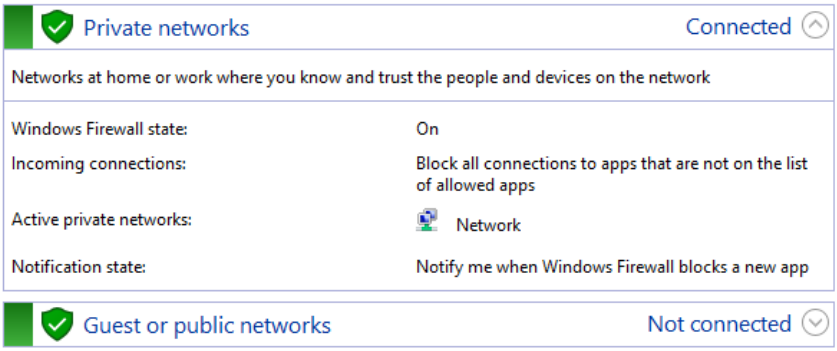
Menjelajahi Berbagai Teknik Pemindaian Jaringan

1. Desktop Kali Linux muncul, klik ikon Terminal
2. Ketik perintah nmap -sT -T3 -A 10.33.107.32 (IP PC windows) dan tekan Enter untuk melakukan TCP Connect Scan pada Windows machine.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sT -T3 -A 10.33.107.32
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-27 21:55 CDT
Nmap scan report for 10.33.107.32
Host is up (0.00080s 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: -1h59m48s, deviation: 4h02m28s, median: 20m10s
|_nbstat: NetBIOS name: DESKTOP-AIVUJRL, NetBIOS user: <unknown>, NetBIOS MAC: c4:54:44:37:0d:be (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: 2023-03-28T10:16:43+07:00
| smb-security-mode:
|   account_used: <blank>
|   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: 2023-03-28T03:16:43
|_  start_date: 2023-03-14T03:33:04
```

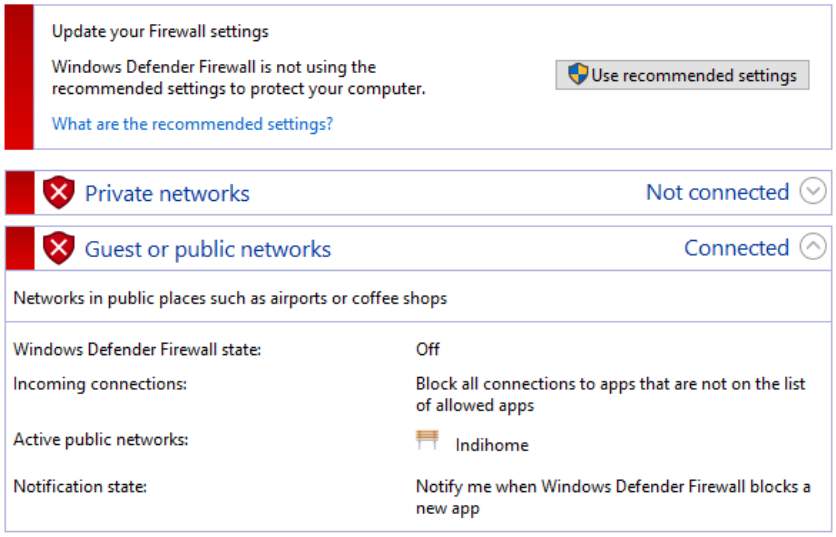
3. Beralih ke mesin Windows , masuk ke mesin, dan aktifkan Windows Firewall.



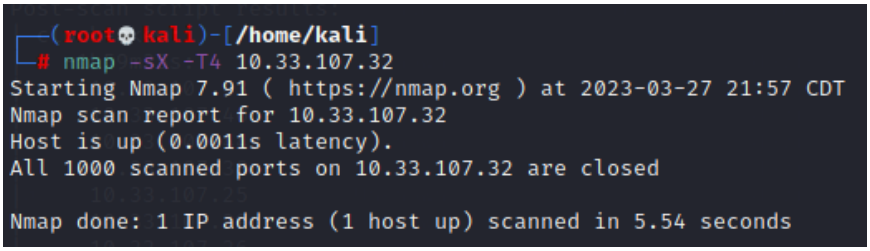
4. Beralih kembali ke mesin Kali Linux. Ketik nmap -sX -T4 10.33.107.32 (IP Windows Server) di command prompt dan tekan Enter untuk melakukan pemindaian Xmas dengan waktu agresif (-T4). Ini menampilkan hasilnya seperti yang ditunjukkan pada tangkapan layar. Hasil Nmap menunjukkan bahwa semua port dibuka/difilter yang berarti firewall dikonfigurasi pada komputer target.

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sX -T4 10.33.107.32
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 2.12 seconds
```

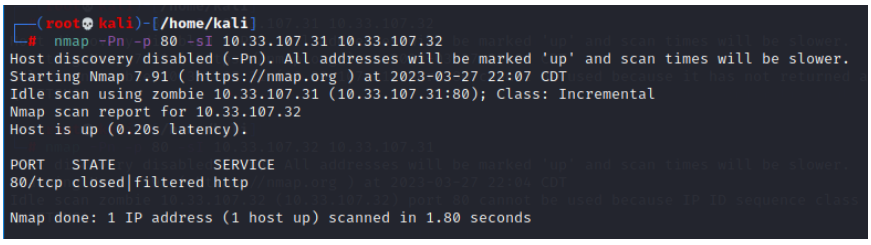
5. Beralih ke mesin Windows dan matikan Windows Firewall.



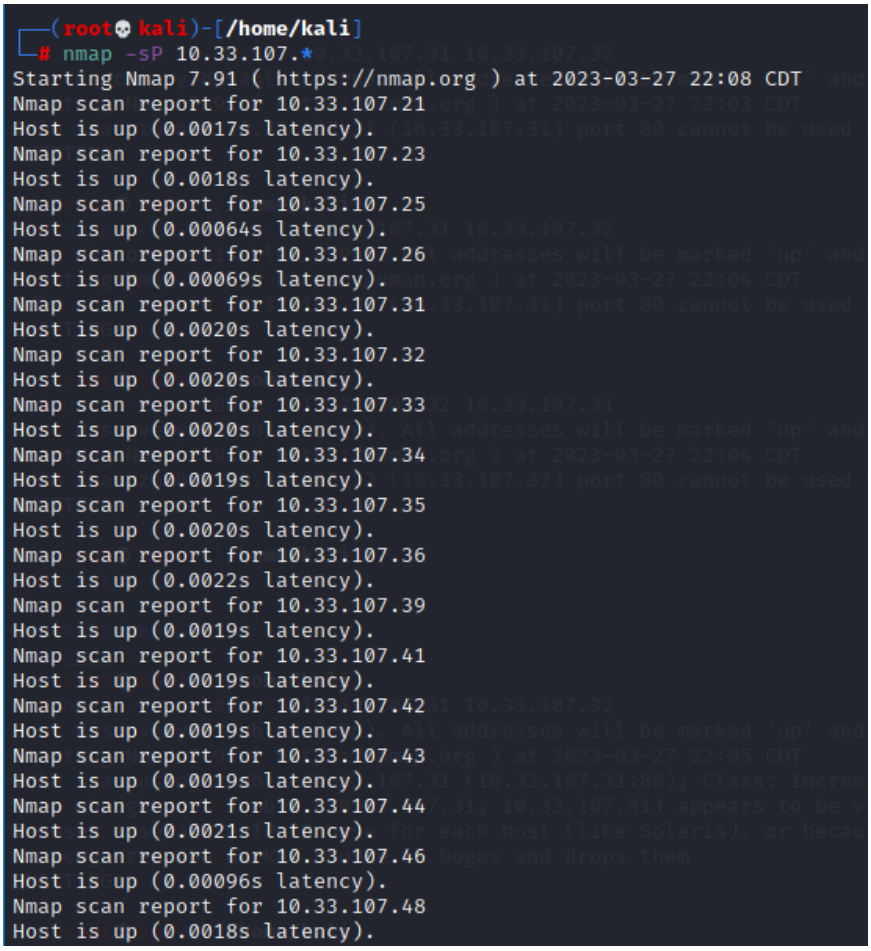
6. Beralih kembali ke mesin Kali Linux. Ketik nmap -sA -v -T4 10. di terminal baris perintah. Ini memulai ACK Scan dan menampilkan disposisi port, seperti yang ditunjukkan pada tangkapan layar.



7. Ketik perintah nmap -Pn -p 80 -sI 10.33.107.31 (IP target) 10.33.107.32, dan tekan Enter.



8. 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.



E. Pembahasan

Pada praktikum kali ini melakukan ekstrak jaringan serta melakukan scanning pada Linux. Dengan footprinting kita dapat mengumpulkan informasi sebanyak mungkin tentang target. Mesin Linux yang digunakan dilakukan dengan remote desktop connection, dengan measukkan IP address sesuai ketentuan sehingga dapat masuk pada sistem Linux. Setelah masuk kedalam sistem Linux, buka terminal yang ada pada Linux lalu keik “sudo msfdb init && msfconsole” agar dapat menggunakan Metasploit Framework. Metasploit Framework merupakan tool yang digunakan untuk menyerang jaringan.

Setelah memberikan perintah tersebut, terminal akan menampilkan banner. Selanjutnya perintah db_status berfungsi untuk mengecek koneksi database postgresql. Perintah -Pn digunakan untuk perlakukan semua host sebagai online. Perintah -sS digunakan untuk memindai TCP SYN. Perintah -A digunakan untuk mengaktifkan deteksi OS. Untuk mengaktifkan seluruh host membutuhkan waktu yang lama, jika sudah terminal akan menampilkan seluruh traceroute jaringan yang terhubung. Dilanjutkan dengan perintah db_import akam mengimport hasil file pemindaian yang

sudah terdeteksi tadi. Perintah host digunakan untuk menampilakn semua daftar host dalam database tersebut. Perintah db_nmap diguakan untuk mejalankan nmap dari Metasploit Framework dan mencatat output secara otomatis. Perintah service digunakan untuk menampilkan semua layanan pada database tadi. Untuk mengetahui opsi konfigurasi yang terkait dengan modul, masukkan perintah set RHOSTS 10.33.107.8-16 and press Enter. Kemudian ketik set THREADS 100.

Dari beberapa perintah tadi, kita sudah mendapatkan begitu banyak informasi dalam jaringan tersebut, contohnya seperti port yang digunakan, daftar host dan layanan serta OS yang digunakan. Selanjutnya memahami berbagai teknik scanning jaringan. Perintah -sT memiliki fungsi yang sama seperti -sS namun berbeda protocol yang digunakan, protocol yang digunakan yaitu pemindaian TCP Connect(). Perintah -T3 (-T<0-5>) berfungsi untuk mensetel templat pengaturan waktu (lebih tinggi lebih cepat). Perintah -sX berfungsi untuk pemindaian TCP Xmas. Perintah -Pn berfungsi utuk memperlakukan semua host sebagai online. Perintah -p untuk memindai port tertentu, pada kasus ini yang digunakan yaitu port 80. Terakhir perintah -sP berfungsi untuk melakukan pemindaian pada jaringan.

F. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. Perintah “sudo msfdb init && msfconsole” digunakan untuk meluncurkan Metasploit Framework.
2. Setiap perintah diatas digunakan untuk melihat informasi penting yang terdapat pada jaringan.
3. Software pemindaian port dalam mode dasar mengirimkan permintaan koneksi ke komputer target pada setiap port secara bergantian dan mencatat port mana yang merespons atau tampak terbuka untuk penyelidikan lebih lanjut.

G. Daftar Pustaka

Bradley, T. (no date) Pengantar pemindaian port, Pengantar Port Scanning di Keamanan Jaringan. Available at: https://id.eyewated.com/pengantar-pemindaian-port/ (Accessed: April 2, 2023).

Mr.boga (2018) Mengenal Basic Command Metasploit framework, Mengenal Basic Command Metasploit Framework. Blogger. Available at: http://droidboga.blogspot.com/2018/04/mengenal-basic-command-metasploit.html (Accessed: April 3, 2023).

Options summary: Nmap network scanning (no date) Options Summary | Nmap Network Scanning. Available at: https://nmap.org/book/man-briefoptions.html (Accessed: April 3, 2023).

Siregar, H. (2020) Apa Saja fungsi metasploit?, Dictio Community. Available at: https://www.dictio.id/t/apa-saja-fungsi-metasploit/125145 (Accessed: April 2, 2023).