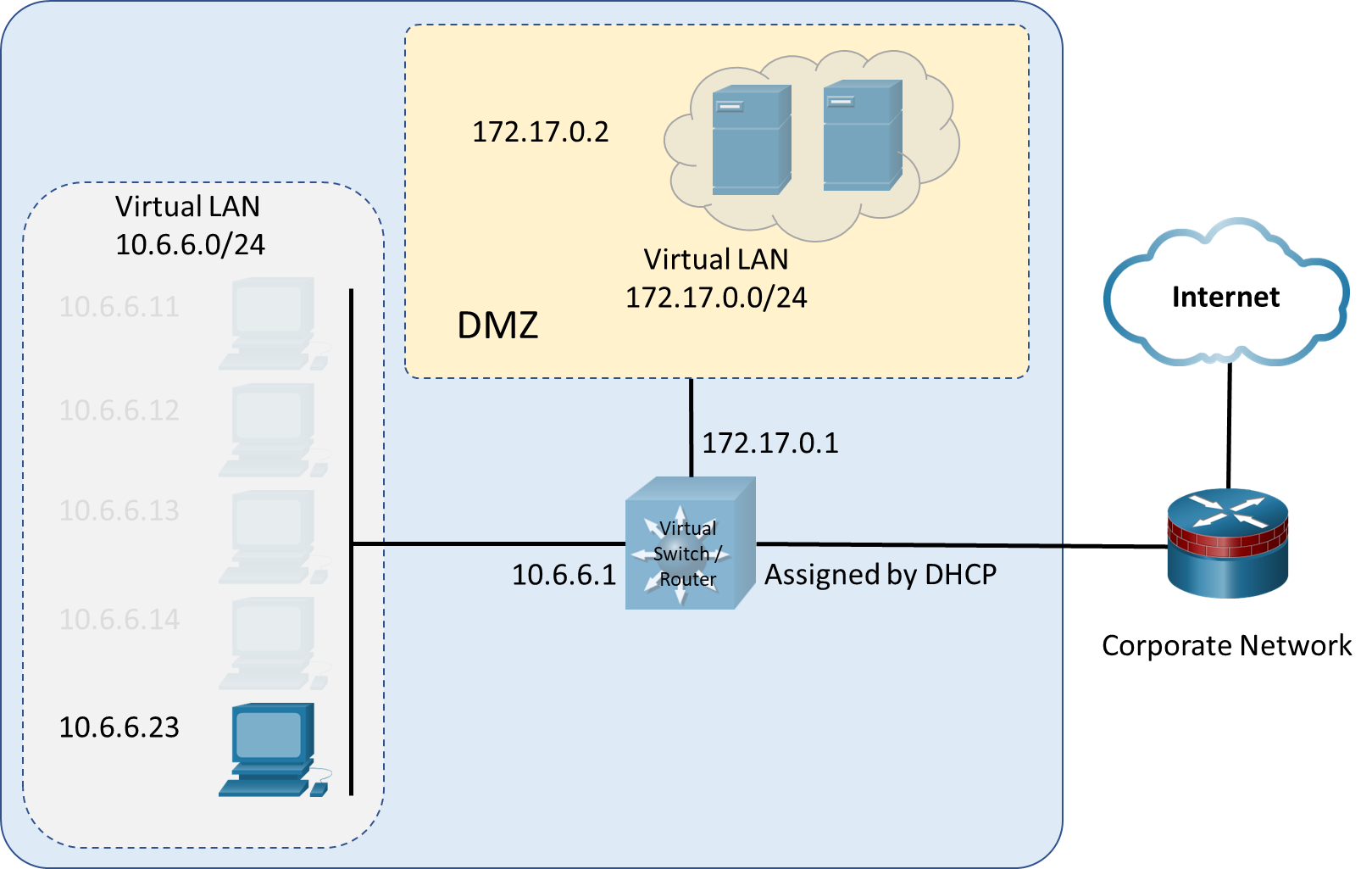
Lab - Enumeration with Nmap

# Topology



# Objectives

Nmap is a powerful open-source tool for network mapping and discovery. In this lab, you will use Nmap as part of your active reconnaissance strategy.

* Investigate Nmap
* Perform Basic Nmap Scans

# Background / Scenario

A Wireshark capture shows unusual activity on a machine on the 10.6.6.0 DMZ network. You’ve been asked to do some active recon on the machine to determine what services it may be offering and if there are vulnerable applications that could present security issues. The IP address of the suspicious computer is 10.6.6.23. You have access to a Kali Linux system on the 10.6.6.0 network.

# Required Resources

* Kali VM customized for Ethical Hacker course

# Instructions

## Investigate Nmap

### Log into Kali Linux and verify the environment.

* + - 1. Log into the Kali system with the username **kali** and the password **kali***.* You are presented with the Kali desktop.
      2. Open a terminal window.
      3. Verify that Kali has an interface in the 10.6.6.0/24 network using the **ifconfig** command.
      4. Use the **nmap -V** command to verify that Nmap is installed and to display the Nmap version. The output will be similar to what is shown below.

┌──(kali㉿Kali)-[~]

└─$ **nmap -V**

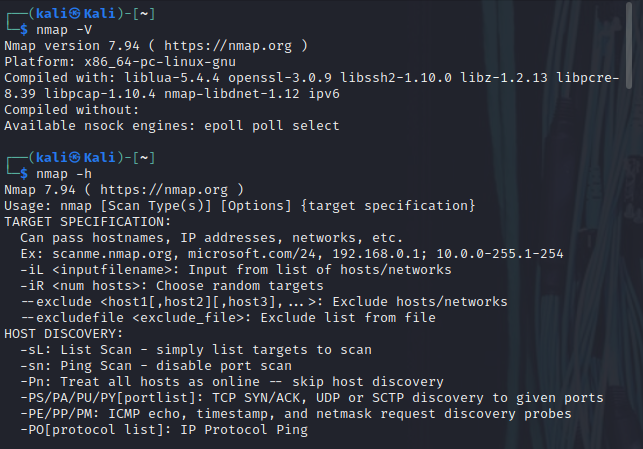
Nmap version 7.93 ( https://nmap.org )

Platform: x86\_64-pc-linux-gnu

Compiled with: liblua-5.3.6 openssl-3.0.7 libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6

Compiled without:

Available nsock engines: epoll poll select



### Investigate Nmap Options and Features

1. Using the command **nmap** without specifying any options or targets returns a list of commonly used Nmap options. To access the Nmap help system use the command **nmap -h**.The help output is divided into sections based on the type of detection that the option supports.
2. The man page for Nmap provides additional information. To access the man page, enter the command **man nmap**. To exit the man pages, press **q** to quit and return to the terminal prompt.

Use the man page for Nmap to complete the table.

Common NMAP Options

| **Option** | **Description** |
| --- | --- |
| **-A** | Aggressive scan that enables OS detection, version detection, script scanning and traceroute |
| **-O** | Enables OS detection |
| **-p <port ranges>** | Allows for specific ports or port ranges to be scanned |
| **-sF** | Performs TCP FIN scan |
| **-sn** | Performs host discovery scan |
| **-sS** | Performs TCP SYN scan |
| **-sT** | Performs TCP Connect scan |
| **-sV** | Probes open ports to determine service/version info |
| **-T<0-5>** | Sets the timing of the scan. Higher numbers produce results faster. Slower scans elude detection better. |
| **-v** | Increases the verbosity of the output |
| **--open** | Only reports open (or possibly open) ports |

Blank Line, No additional information

## Perform Basic Nmap Scans

### Initiate a basic Nmap scan of the target computer.

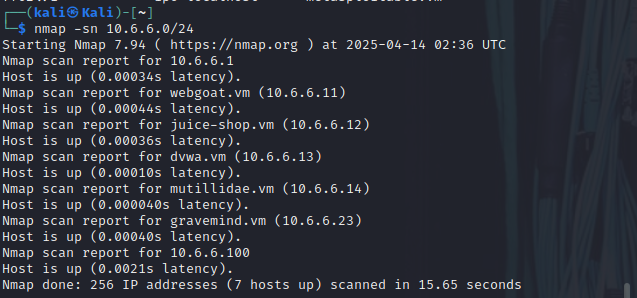
* + - 1. To quickly scan the DMZ for active hosts, you can perform a discovery scan. In a discovery scan, the scanning host sends an ICMP echo request (ping), a TCP SYN to port 443, a TCP ACK to port 80, and an ICMP timestamp request. A response to any of the requests indicates that the host is up and the IP protocol stack on the host is functioning. Enter the following command to scan the DMZ network:

┌──(kali㉿Kali)-[~]

└─$ **nmap -sn 10.6.6.0/24**

#### question:

How many active hosts are located in DMZ network?



Type your answers here.

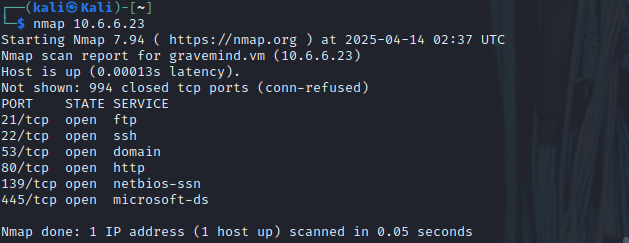
* + - 1. The host 10.6.6.23 was identified as suspicious in a Wireshark capture, and it is necessary to perform additional reconnaissance to discover more about the computer and its services. Use the **nmap** command to execute a default scan on the target host.

┌──(kali㉿Kali)-[~]

└─$ **nmap 10.6.6.23**

#### Question:

What ports are listed as open on the target host (10.6.6.23)?



Type your answers here.

By default, Nmap performs a connect scan of 1000 most common TCP ports. This makes use of the operating system’s networking software to establish a full TCP connection. This type of scan creates a lot of networking traffic and increases the probability of detection by intrusion detection services. You can also specify a TCP connect scan using the command option **nmap -sT**.

The output of the connect scan includes the status codes shown in the table:

| **Status** | **Response Received** | **Interpretation** |
| --- | --- | --- |
| Open | TCP SYN-ACK | There is a service listening on the identified port. |
| Closed | TCP RST | There is no service listening on the identified port. |
| Filtered | No response, or an ICMP destination unreachable message received. | The port is being filtered by a firewall. |

Blank Line, No additional information

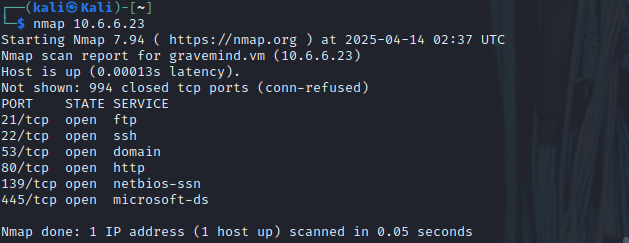
* + - 1. The **-O** option can be used to further determine information about the operating system running on the target host. Some Nmap options require additional permissions and must be run as **root** or using the **sudo** command. To find operating system information on the target host, use the **nmap -O** command. Enter the password of **kali** when prompted.

┌──(kali㉿Kali)-[~]

└─$ **sudo nmap -O 10.6.6.23**

#### Question:

What operating system is the target host running?



Type your answers here.

### Obtain additional information about the host and services.

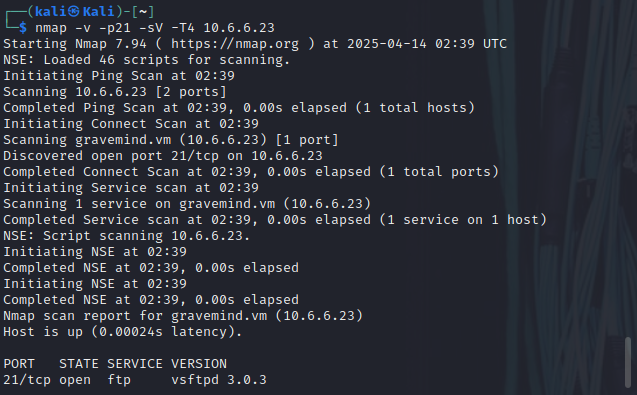
* + - 1. To provide additional information about the target computer, it is possible to combine different options into a single command line. The previous command identified several potentially open ports on the 10.6.6.23 host. You can use **-v**, **-p**, and **-sV** to find additional information about the services running on the open ports. This command provides information about the FTP service running on port 21 on the target in verbose mode, with the timing set to fast (**-T4**):

┌──(kali㉿Kali)-[~]

└─$ **nmap -v -p21 -sV -T4 10.6.6.23**

#### question:

What did you discover about the type and version of FTP server that is running on the host?



Type your answers here.

* + - 1. The **-A** option executes OS detection, version detection, script scanning, and traceroute. The **-A** scan can be very intrusive and therefore will be detected by many IDS systems, so ensure that you have permission before attempting this scan outside of the lab environment. To gather more information regarding the FTP service, enter the command **nmap -A -p21 10.6.6.23**.

The sample detailed output of this command is shown below:

┌──(kali㉿Kali)-[~]

└─$ **nmap -p21 -sV -A 10.6.6.23**

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-16 22:36 UTC

Nmap scan report for 10.6.6.23

Host is up (0.00044s latency).

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.6.6.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 3

| vsFTPd 3.0.3 - secure, fast, stable

|\_End of status

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| -rw-r--r-- 1 0 0 16 Aug 13 2021 file1.txt

| -rw-r--r-- 1 0 0 16 Aug 13 2021 file2.txt

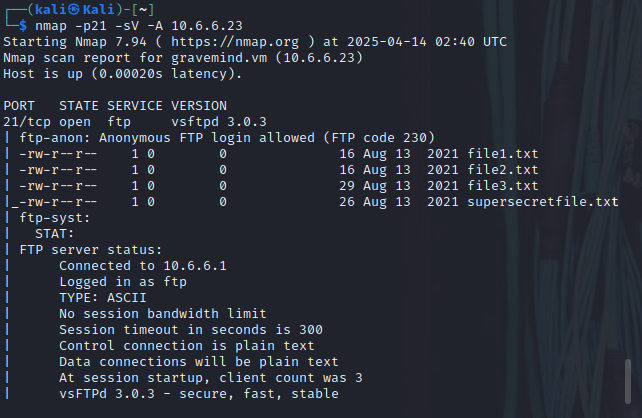
| -rw-r--r-- 1 0 0 29 Aug 13 2021 file3.txt

|\_-rw-r--r-- 1 0 0 26 Aug 13 2021 supersecretfile.txt

Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds

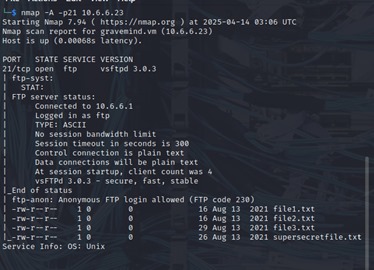


* + - 1. Examine the output of the **nmap -A** command. Notice that the output indicates that a connection was made between the Kali Linux system and the target FTP service.

#### Questions:

How many files on the FTP server are accessible through this connection?

Type your ans

wers here.

What weakness in the FTP server configuration enabled the Kali Linux system to log into the FTP server?

Kelemahan dalam konfigurasi server FTP yang memungkinkan sistem Kali Linux untuk masuk adalah karena server FTP mengizinkan login sebagai "anonymous" (pengguna anonim) tanpa memerlukan username dan password yang valid.

Type your answers here.

### Investigate SMB Services with Scripts

The Server Message Block (SMB) protocol is a network file sharing protocol supported on Windows computers and by SAMBA on Linux. SMB enables applications to read and write files or request services over a network. Open public shares or shared devices such as print servers on a network, can be accessed through SMB.

* + - 1. The earlier scan of open ports on the target computer indicates that the SMB ports 139 and 445 are open. Find more information on these ports using the **-A** and **-p** command options. The **-A** option executes several functions including running the default scripts. Specify more than one port to scan by listing them separately with a comma between them.

┌──(kali㉿Kali)-[~]

└─$ **nmap -A -p139,445 10.6.6.23**

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-01 22:47 UTC

Nmap scan report for 10.6.6.23

Host is up (0.00014s latency).

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)

Service Info: Host: 868CF29B394C

Host script results:

| smb2-time:

| date: 2023-03-01T22:47:38

|\_ start\_date: N/A

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.9.5-Debian)

| Computer name: 868cf29b394c

| NetBIOS computer name: 868CF29B394C\x00

| Domain name: \x00

| FQDN: 868cf29b394c

|\_ System time: 2023-03-01T22:47:35+00:00

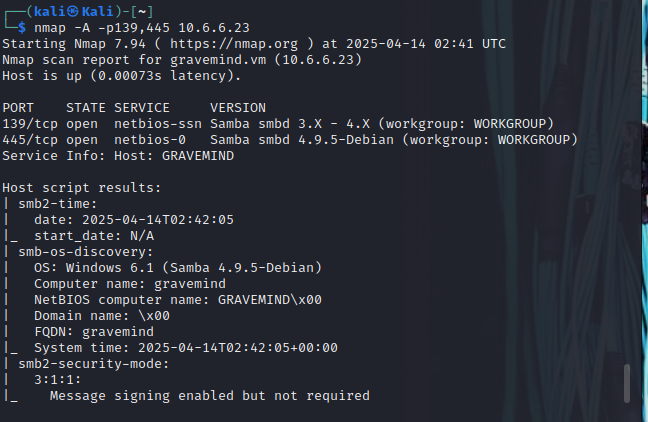
| smb2-security-mode:

| 311:

|\_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 22.05 seconds



* + - 1. Examine the information returned by the Nmap scan. From this information, it can be determined that the target computer is a member of the default workgroup, named WORKGROUP, and that SMB supported on this host through SAMBA on Linux.

#### Question:

What is the NetBIOS computer name assigned to the target host?



Type your answers here.

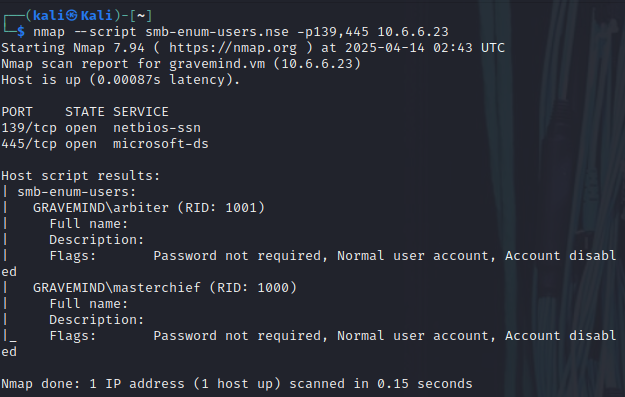
* + - 1. Nmap contains the powerful Nmap Scripting Engine (NSE), which enables the programming of various Nmap options and conditional actions to be taken as a result of the responses. NSE has built-in scripts that enumerate users, groups, and network shares. One of the more commonly used scripts for SMB discovery is the **smb-enum-users.nse** script. Use the Nmap NSE script with the command:

┌──(kali㉿Kali)-[~]

└─$ **nmap --script smb-enum-users.nse -p139,445 10.6.6.23**

#### question:

Did the script uncover any SMB usernames on the target host? If so, how many?



Type your answers here.

* + - 1. A serious security concern is the existence of publicly shared directories (folders). You can enumerate the network shares using another NSE script, **smb-enum-shares.nse.** To discover shared directories on the target computer. Use the Nmap share enumeration script with the command:

┌──(kali㉿Kali)-[~]

└─$ **nmap --script smb-enum-shares.nse -p445 10.6.6.23**

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-01 22:52 UTC

Nmap scan report for 10.6.6.23

Host is up (0.00016s latency).

PORT STATE SERVICE

445/tcp open microsoft-ds

Host script results:

| smb-enum-shares:

| account\_used: <blank>

| \\10.6.6.23\IPC$:

| Type: STYPE\_IPC\_HIDDEN

| Comment: IPC Service (Samba 4.9.5-Debian)

| Users: 1

| Max Users: <unlimited>

| Path: C:\tmp

| Anonymous access: READ/WRITE

| \\10.6.6.23\print$:

| Type: STYPE\_DISKTREE

| Comment: Printer Drivers

| Users: 0

| Max Users: <unlimited>

| Path: C:\var\lib\samba\printers

| Anonymous access: READ/WRITE

| \\10.6.6.23\workfiles:

| Type: STYPE\_DISKTREE

| Comment: Confidential Workfiles

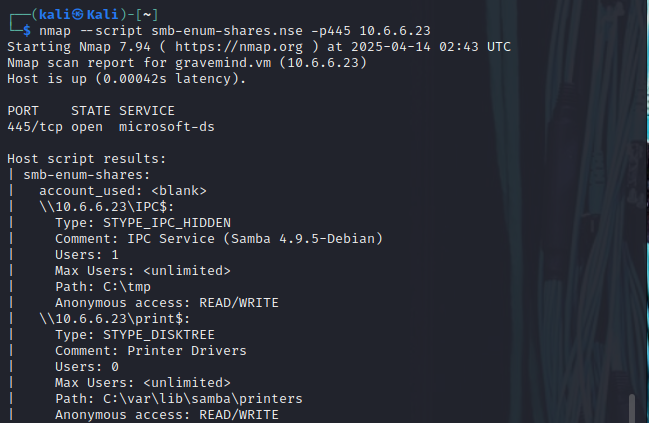
| Users: 0

| Max Users: <unlimited>

| Path: C:\var\spool\samba

|\_ Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 12.92 seconds



* + - 1. Examine the output created by the **smb-enum-shares** script. In the output, share names that end with a “$” character represent hidden shares that include system and administrative shares.

#### Questions:

How many hidden shares were discovered on the target host?

1. IPC$

Type your answers here.

What serious security risk is uncovered in this script output?

1. Hasil menunjukkan bahwa akses anonim diizinkan dengan hak baca dan tulis (READ/WRITE) pada dua share berikut:

[\\10.6.6.23\IPC$](\\\\10.6.6.23\\IPC$)

[\\10.6.6.23\print$](\\\\10.6.6.23\\print$)

ur answers here.

There are preprogrammed scripts that can provide additional SMB discovery capabilities if an authorized user account is available. Take time and investigate some of the NSE scripts that enumerate Windows and SAMBA systems.

# Reflection Questions

* 1. Nmap is a powerful tool for network discovery. Think about the ways that Nmap can discover and enumerate computers that you used in this lab. How can Nmap be used by internal network technicians to inventory and secure local computers? How can these same tools be used by malicious actors to perform reconnaissance before an attack?

Type your answers here.

* 1. If you were tasked with creating a report on the status of the target host (10.6.6.23), what serious security risks would you include in your report?

**Jawaban**

1. Nmap adalah alat yang sangat kuat untuk melakukan network discovery (penemuan jaringan) dan enumeration (pengumpulan informasi detail tentang perangkat di jaringan). Dalam lab ini, Nmap digunakan untuk memindai jaringan dan menemukan perangkat yang terhubung, termasuk alamat IP, port yang terbuka, serta layanan yang berjalan di atas port tersebut.

Penggunaan Nmap oleh Teknisi Jaringan Internal:

Teknisi jaringan internal dapat menggunakan Nmap untuk:

Inventarisasi Perangkat Lokal

Dengan melakukan pemindaian pada subnet jaringan lokal, teknisi dapat mengetahui perangkat apa saja yang aktif di jaringan, lengkap dengan alamat IP dan MAC-nya.

Identifikasi Port dan Layanan

Nmap dapat mengidentifikasi port yang terbuka dan layanan yang berjalan (seperti HTTP, SSH, FTP), sehingga teknisi bisa memastikan hanya layanan yang diperlukan saja yang berjalan.

Pemeriksaan Keamanan dan Kerentanan

Dengan script scanning atau integrasi dengan tool seperti NSE (Nmap Scripting Engine), teknisi dapat mengidentifikasi konfigurasi yang tidak aman atau layanan yang rentan.

Audit dan Pemeliharaan Rutin

Digunakan sebagai bagian dari audit keamanan secara berkala untuk memastikan bahwa tidak ada perangkat atau layanan baru yang muncul tanpa sepengetahuan tim IT.

Penggunaan Nmap oleh Aktor Jahat:

Sayangnya, alat yang sama juga bisa digunakan oleh penyerang untuk melakukan reconnaissance pengintaian awal sebelum serangan), seperti:

Menemukan Target

Penyerang dapat memindai jaringan untuk mengetahui perangkat mana yang aktif dan mungkin menjadi target potensial.

Menganalisis Layanan Rentan

Dengan melihat port dan layanan yang terbuka, penyerang bisa mencari celah keamanan atau kerentanan spesifik yang dapat dieksploitasi.

Fingerprinting Sistem Operasi dan Aplikasi

Nmap bisa digunakan untuk mengidentifikasi jenis sistem operasi dan versi aplikasi yang berjalan, yang sangat berguna bagi penyerang untuk menyesuaikan metode serangan.

Merencanakan Serangan yang Lebih Lanjut

Informasi hasil pemindaian bisa digunakan sebagai dasar untuk melakukan eksploitasi atau serangan lanjutan seperti brute force, exploit, atau DoS.

1. Jika saya ditugaskan untuk membuat laporan mengenai status host target dengan alamat IP 10.6.6.23, maka saya akan mencantumkan beberapa risiko keamanan serius yang mungkin ditemukan selama proses pemindaian, misalnya dengan menggunakan Nmap. Berikut ini adalah risiko-risiko yang perlu dimasukkan dalam laporan:

1. Port Terbuka yang Tidak Diperlukan

Jika ditemukan banyak port terbuka, terutama port yang tidak digunakan atau tidak penting, maka ini menjadi celah potensial bagi penyerang. Setiap port terbuka adalah titik masuk yang bisa dieksploitasi.

2. Layanan Rentan yang Teridentifikasi

Misalnya, jika host menjalankan layanan lama seperti FTP tanpa enkripsi, Telnet, atau versi lama dari Apache atau SMB, maka ini merupakan risiko besar karena layanan tersebut dikenal memiliki celah keamanan.

3. Sistem Operasi dan Aplikasi Tidak Terbarukan

Jika fingerprinting menunjukkan bahwa sistem operasi atau perangkat lunak yang berjalan belum diperbarui, maka sangat besar kemungkinan terdapat vulnerability yang belum ditambal (unpatched).

4. Tidak Ada Firewall atau IDS/IPS

Jika host terlihat tidak terlindungi oleh firewall, atau tidak menunjukkan tanda-tanda adanya sistem deteksi intrusi, maka ini memperbesar kemungkinan host akan menjadi target serangan langsung.

5. Penggunaan Protokol Tidak Aman

Penggunaan protokol seperti HTTP (tanpa HTTPS), Telnet, atau FTP menunjukkan bahwa data bisa ditangkap dengan mudah melalui sniffing oleh pihak tidak berwenang.

6. Informasi Sistem yang Terbuka

Jika selama pemindaian Nmap ditemukan banner atau detail versi sistem secara terbuka, maka ini memberikan penyerang informasi berharga untuk melakukan targeted attack.

s here.

end of docujjjmentj