

Lab Journal for VM Configuration and Vulnerability Scanning for Network Security

Khoi Nguyen Pham
Swinburne University of Technology
School of Science, Computing and Engineering Technologies
Hawthorn, Victoria 3122, Australia
Email: nguyenpham1441887@gmail.com

I. OBJECTIVE

Perform various scanning, testing, and enumeration tasks from a Kali Linux VM to a Window 11 VM.

II. PRECONFIGURATIONS

- Download Virtual Box as well as Kali Linux and Window ISOs.
- Set them in an internal network and manually configure their IPs as 192.168.20.10 and 192.168.20.11.
- Turn off Window Firewall.
- Test connectivity using the ping command.

Open ports are caused by the services running on your system, not by the firewall itself. The firewall simply controls who can access those open ports. It may block incoming traffic from external networks or restrict the ability of tools like Nmap to connect to the open ports. Disabling the firewall temporarily or allowing specific ports through the firewall can help with Nmap scans, but it does not change the fact that those services are listening on those ports.

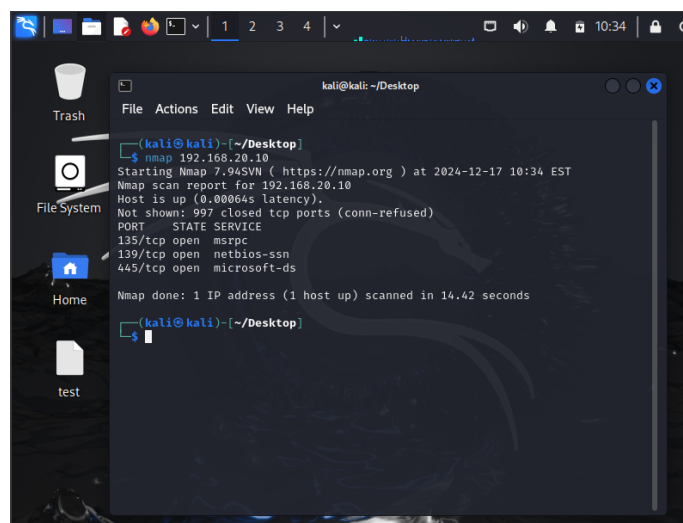
III. NMAP SCANS

Nmap (Network Mapper) is a free tool used to explore and secure networks. It helps:

- Find devices on a network.
- Scan ports to see which are open or closed.
- Identify services (like web servers) and their versions.
- Detect operating systems on devices.
- Check for security vulnerabilities using special scripts.

A. *nmap*

This scan identifies open ports and services on the target machine. A typical output might look like this:

A screenshot of a Kali Linux desktop environment. A terminal window is open, displaying the output of an Nmap scan. The terminal title is 'kali@kali: ~/Desktop'. The command entered is 'nmap 192.168.20.10'. The output shows the Nmap version (7.94SVN), the scan time (2024-12-17 10:34 EST), and the target host (192.168.20.10). It reports that the host is up with a latency of 0.00064s. A table of open ports is shown: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The scan took 14.42 seconds to complete. The desktop background is dark, and there are icons for Trash, File System, Home, and test on the left sidebar.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)~[~/Desktop]
$ nmap 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 10:34 EST
Nmap scan report for 192.168.20.10
Host is up (0.00064s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds

(kali@kali)~[~/Desktop]
$
```

Fig. 1. Output of nmap

Explanation of the Results: When running an Nmap scan on your target system, the scan will reveal open ports and the services running on those ports. These open ports don't directly indicate vulnerabilities, but they are potential attack surfaces.

Key Ports and Their Potential Implications:

a. Port 135: Microsoft Remote Procedure Call (RPC)

- **What It Is:** This port is used for remote communication between computers on a network. It allows different software processes on a computer to communicate with each other. It's mostly used by Microsoft Windows to enable services like file and printer sharing and remote management.
- **Vulnerabilities:** If this port is open and the system isn't properly secured or updated, it can be targeted by attacks that exploit weaknesses in the RPC service.
 - For example, **MS03-026** is a vulnerability in older versions of Windows, which allowed the **Blaster worm** to spread. An attacker could send a specially crafted message to this port and potentially take control of the system.
 - **Remote Code Execution:** If vulnerabilities exist in RPC, attackers can send malicious commands to execute code on the target system remotely.

b. Port 139: NetBIOS Session Service

- **What It Is:** This port is used for older network protocols, primarily for file and printer sharing between Windows computers. It's part of a legacy system used before modern file sharing methods were introduced.
- **Vulnerabilities:**
 - **SMB Relay Attacks:** This type of attack takes advantage of communication between the computers over NetBIOS, where an attacker can intercept and alter messages to gain unauthorized access.
 - **Information Disclosure:** NetBIOS can sometimes reveal sensitive information, such as a list of available computers, usernames, and network shares, which can be used for further attacks.

c. Port 445: Server Message Block (SMB)

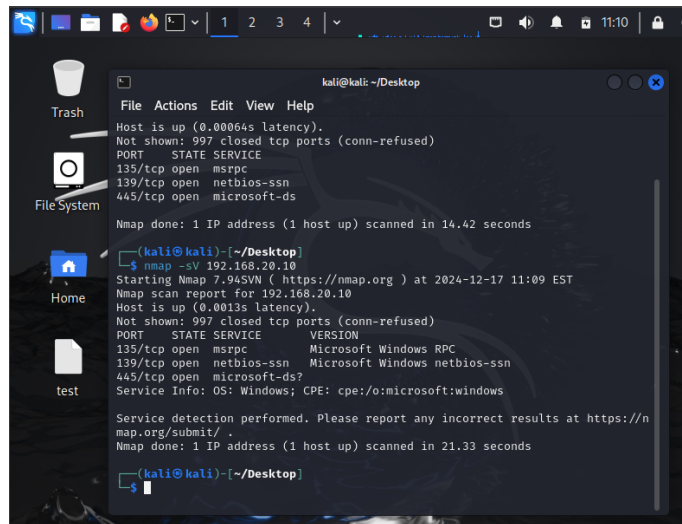
- **What It Is:** This port is used for file sharing, printer sharing, and other network services between Windows computers. It's part of the **Server Message Block (SMB)** protocol, which is used by modern Windows systems for network communication.
- **Vulnerabilities:**
 - **EternalBlue:** This is one of the most famous exploits, which targets a flaw in the SMB protocol (especially in older versions of SMB). The **WannaCry** ransomware, for example, used this vulnerability to spread across networks, allowing attackers to execute code remotely on vulnerable systems.
 - **Man-in-the-Middle Attacks:** Open port 445 can be exploited in **SMB relay attacks**, where attackers intercept SMB traffic between systems to gain unauthorized access.

d. Port 3389: Remote Desktop Protocol (RDP)

- **What It Is:** This port is used for **Remote Desktop Protocol**, which allows users to remotely control another computer's desktop, usually for administrative purposes. It's commonly used to access Windows machines from a remote location.
- **Vulnerabilities:**
 - **Brute Force Attacks:** RDP is often targeted by attackers who try to guess the username and password through brute force. If weak credentials are used, an attacker can gain unauthorized access to the system.
 - **BlueKeep Vulnerability:** This vulnerability (CVE-2019-0708) in RDP allowed attackers to execute remote code on unpatched systems, giving them complete control of the machine. This exploit was particularly concerning because it didn't require authentication, meaning an attacker could exploit it even without valid login credentials.
 - **Ransomware Attacks:** Because RDP is commonly used to manage systems, attackers often target RDP to gain access and deploy ransomware, locking files or demanding payment for access restoration.

B. `nmap -sV`

This command will give details about the version of each service running on the open ports:



```
kali@kali: ~/Desktop
File Actions Edit View Help
Host is up (0.00064s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds

(kali@kali)~[~/Desktop]
$ nmap -sV 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 11:09 EST
Nmap scan report for 192.168.20.10
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (conn-refused)
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?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 21.33 seconds

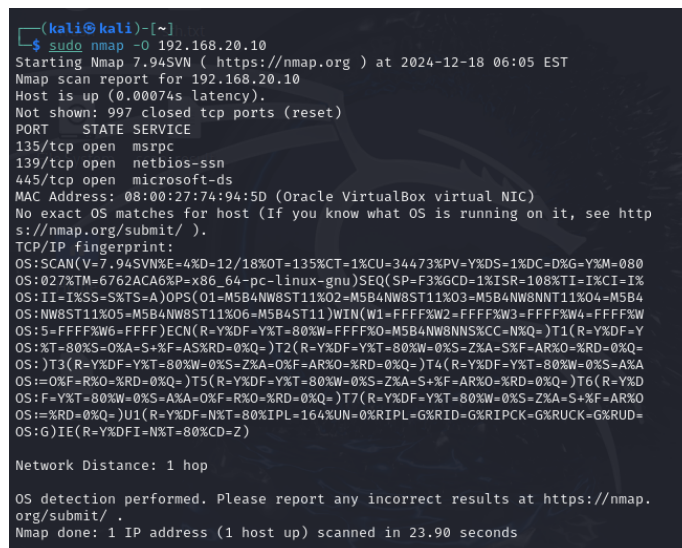
(kali@kali)~[~/Desktop]
$
```

Fig. 2. Output of nmap -sV

You now know which versions of the services are running on each open port, which is important because vulnerabilities are often version-specific.

C. nmap -O

Gives information about the operating system running on the target machine:



```
(kali@kali)~[~]
$ sudo nmap -O 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 06:05 EST
Nmap scan report for 192.168.20.10
Host is up (0.00074s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:74:94:5D (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/18%OT=135%CT=1%CU=34473%PV=Y%DS=1%DC=D%G=Y%M=080
OS:027%TM=6762ACA6%P=x86_64-pc-linux-gnu)SEQ(SP=F3%GCD=1%ISR=108%TI=I%CI=I%
OS:II-I%SS=S%TS=A)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4
OS:NW8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W
OS:5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y
OS:%T=80%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=
OS:)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A
OS:=0%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%D
OS:F=Y%T=80%W=0%S=A%A=0%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O
OS:=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=80%CD=Z)

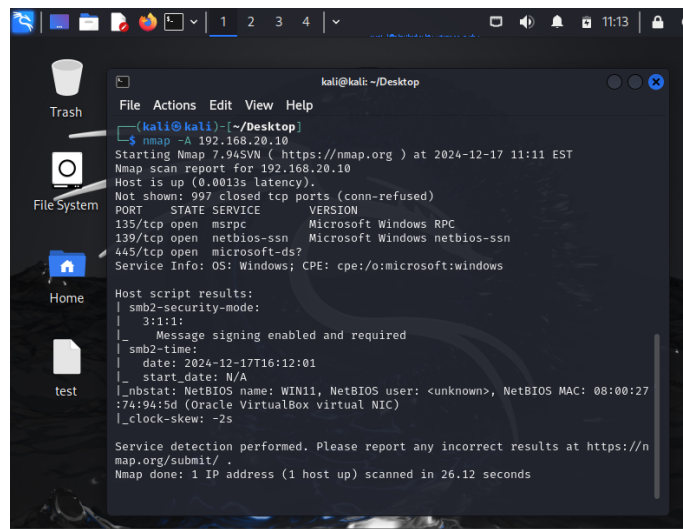
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 23.90 seconds
```

Fig. 3. Output of nmap -O

D. nmap -A

The -A option combines several advanced scanning techniques, including OS detection, version detection, script scanning, and traceroute. This will give more detailed information about the target, which is especially useful for vulnerability assessment.

A terminal window titled 'kali@kali: ~/Desktop' showing the output of the command 'nmap -A 192.168.20.10'. The output includes the Nmap version (7.94SVN), the target IP (192.168.20.10), and the scan results. The host is up with a latency of 0.0013s. The scan shows 997 closed TCP ports (conn-refused). The open ports are 135/tcp (msrpc, Microsoft Windows RPC), 139/tcp (netbios-ssn, Microsoft Windows netbios-ssn), and 445/tcp (microsoft-ds). The service info for 445/tcp is OS: Windows; CPE: cpe:/o:microsoft:windows. The host script results show smb2-security-mode: 3.1.1 (Message signing enabled and required) and smb2-time: date: 2024-12-17T16:12:01, start_date: N/A. The netbios name is WIN11, NetBIOS user is <unknown>, and NetBIOS MAC is 08:00:27:74:94:5d (Oracle VirtualBox virtual NIC). The clock skew is -2s. The service detection was performed, and the results are reported at https://nmap.org/submit/. The scan was done in 26.12 seconds.

```
kali@kali:~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nmap -A 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 11:11 EST
Nmap scan report for 192.168.20.10
Host is up (0.0013s latency).
Not shown: 997 closed tcp ports (conn-refused)
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?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

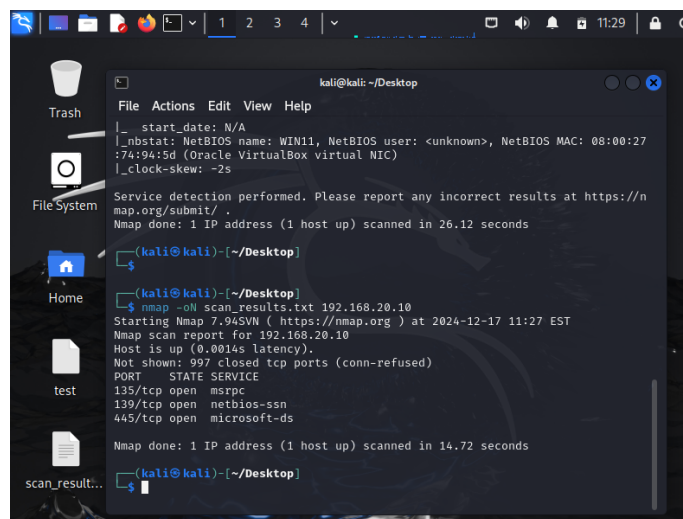
Host script results:
|_ smb2-security-mode:
|   3.1.1:
|     - Message signing enabled and required
|_ smb2-time:
|   date: 2024-12-17T16:12:01
|   start_date: N/A
|_ nbstat: NetBIOS name: WIN11, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:74:94:5d (Oracle VirtualBox virtual NIC)
|_ clock-skew: -2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 26.12 seconds
```

Fig. 4. Output of nmap -A

E. nmap -oN

Saving scan results to a file:

A terminal window titled 'kali@kali: ~/Desktop' showing the output of the command 'nmap -oN scan_results.txt 192.168.20.10'. The output is identical to the previous figure, but the scan was done in 14.72 seconds. The terminal window also shows the command 'nmap -oN scan_results.txt 192.168.20.10' being entered and the resulting output.

```
kali@kali:~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nmap -oN scan_results.txt 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 11:27 EST
Nmap scan report for 192.168.20.10
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds
```

Fig. 5. Output of nmap -oN

F. nmap --script vuln

The `--script vuln` flag runs Nmap's built-in vulnerability scripts, which are designed to test for known vulnerabilities in common services.

```

(kali@kali)-[~/Desktop]
$ nmap --script vuln 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 11:31 EST
Nmap scan report for 192.168.20.10
Host is up (0.0022s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 30.04 seconds

```

Fig. 6. Output of `nmap --script vuln`

G. Scan for SMB Vulnerabilities - `nmap --script smb-vuln-ms17-010 -p 445`

Given that SMB is running, check whether it's vulnerable to known exploits like EternalBlue (MS17-010):

```

(kali@kali)-[~/Desktop]
$ nmap --script smb-vuln-ms17-010 -p 445 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 04:53 EST
Nmap scan report for 192.168.20.10
Host is up (0.0010s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds

```

Fig. 7. Output of `nmap --script smb-vuln-ms17-010 -p 445`

H. `nmap --script msrpc-enum -p 135`

Port 135 could potentially be used for Remote Code Execution (RCE) or exploited if not secured. Use Nmap to enumerate RPC services:

```

(kali@kali)-[~]
$ nmap --script msrpc-enum -p 135 192.168.20.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 05:27 EST
Nmap scan report for 192.168.20.10
Host is up (0.0017s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

```

Fig. 8. Output of `nmap --script msrpc-enum -p 135`

IV. ENUMERATIONS

A. Enumerate SMB Services (Port 445) - `smbclient -L //IP -N`

Use `smbclient` to try and list SMB shares. No shares should be accessible anonymously. If you find shares, document them and investigate their permissions.

```

(kali@kali)-[~]
$ smbclient -L //192.168.20.10 -N
session setup failed: NT_STATUS_ACCESS_DENIED

```

Fig. 9. Output of `smbclient`

B. Enumerate NetBIOS (Port 139) - `nbtsan`

Port 139 (NetBIOS-ssn) is typically unnecessary for modern Windows systems. We can use tools to enumerate it.

```
(kali@kali)-[~]
$ nbtscan 192.168.20.10
Doing NBT name scan for addresses from 192.168.20.10
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.20.10	WIN11	<server>	<unknown>	08:00:27:74:94:5d

Fig. 10. Output of nbtscan

Minimal output if NetBIOS is not actively in use. If we see NetBIOS information, it indicates legacy settings.

C. Enumerate RPC Services (Port 135) - rpcclient

Port 135 is tied to Microsoft RPC (Remote Procedure Call). Enumerating this port can reveal services running over RPC. Use rpcclient to Enumerate Users and check for any accessible user accounts or domain info:

```
(kali@kali)-[~]
$ rpcclient -U "" 192.168.20.10
Password for [WORKGROUP\]:
Cannot connect to server. Error was NT_STATUS_LOGON_FAILURE
```

Fig. 11. Output of rpcclient -U