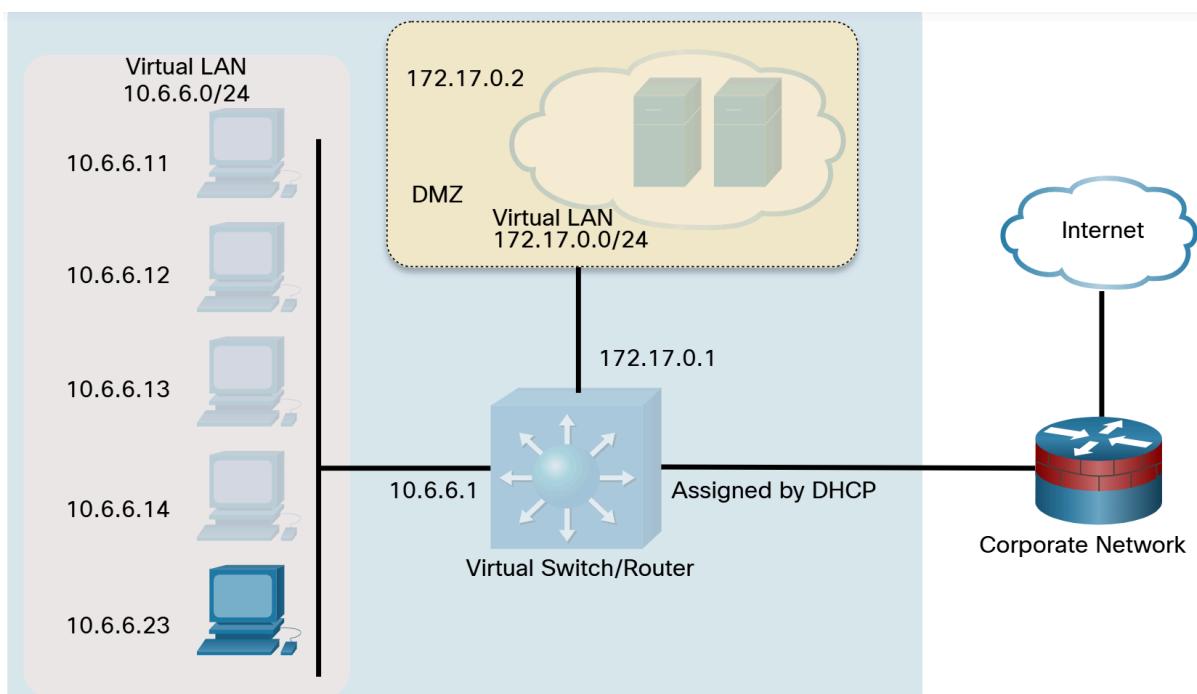


Enumeration with Nmap

Topology



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.

Part 1: Investigate Nmap

Log into Kali Linux and verify the environment.

Verify that Kali has an interface in the 10.6.6.0/24 network using the **ifconfig** command.

```
(kali㉿Kali)-[~]
$ ifconfig
br-339414195aeb: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.5.5.1 netmask 255.255.255.0 broadcast 10.5.5.255
        inet6 fe80::42:9cff:feb2:7bd5 prefixlen 64 scopeid 0x20<link>
            ether 02:42:9c:b2:7b:d5 txqueuelen 0 (Ethernet)
            RX packets 128 bytes 7368 (7.1 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 24 bytes 4040 (3.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-355ee7945a88: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::42:99ff:fe59:49bf prefixlen 64 scopeid 0x20<link>
            ether 02:42:99:59:49:bf txqueuelen 0 (Ethernet)
            RX packets 100 bytes 16263 (15.8 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 17 bytes 3678 (3.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-internal: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    [inet 10.6.6.1 netmask 255.255.255.0 broadcast 10.6.6.255]
        inet6 fe80::42:48ff:fe18:46fa prefixlen 64 scopeid 0x20<link>
            ether 02:42:48:18:46:fa txqueuelen 0 (Ethernet)
            RX packets 127 bytes 7340 (7.1 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 25 bytes 4801 (4.6 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Part 2: Perform Basic Nmap Scans

To quickly scan the DMZ for active hosts, you can perform a discovery scan.

```
(kali㉿Kali)-[~]
$ nmap -sn 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-15 00:32 UTC
Nmap scan report for 10.6.6.1 (10.6.6.1)
Host is up (0.019s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0019s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0029s latency).
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.0042s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0017s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0031s latency).
Nmap scan report for 10.6.6.100
Host is up (0.0053s latency)
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.45 seconds
```

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.

```
(kali㉿Kali)-[~]
$ nmap 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-15 00:40 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00025s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

The **-O** option can be used to further determine information about the operating system running on the target host.

```
(kali㉿Kali)-[~]
$ sudo nmap -O 10.6.6.23
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 18:01 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
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 1.96 seconds
```

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
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 18:18 UTC
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 18:18
Scanning 10.6.6.23 [2 ports]
Completed Ping Scan at 18:18, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 18:18
Scanning gravemind.vm (10.6.6.23) [1 port]
Discovered open port 21/tcp on 10.6.6.23
Completed Connect Scan at 18:18, 0.00s elapsed (1 total ports)
Initiating Service scan at 18:18
Scanning 1 service on gravemind.vm (10.6.6.23)
Completed Service scan at 18:18, 0.02s elapsed (1 service on 1 host)
NSE: Script scanning 10.6.6.23.
Initiating NSE at 18:18
Completed NSE at 18:18, 0.00s elapsed
Initiating NSE at 18:18
Completed NSE at 18:18, 0.00s elapsed
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00039s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix
```

The **-A** option executes OS detection, version detection, script scanning, and traceroute.

```
(kali㉿Kali)-[~]
$ nmap -p21 -sV -A 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 18:32 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| 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
|_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 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

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. 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.

```
(kali㉿Kali)-[~]
$ nmap -A -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 18:47 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.012s 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: GRAVEMIND

Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|_  smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
smb2-time:
|   date: 2025-12-19T18:47:44
|   start date: N/A
smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: gravemind
|   NetBIOS computer name: GRAVEMIND\x00
|   Domain name: \x00
|   FQDN: gravemind
|_  System time: 2025-12-19T18:47:45+00:00
```

Nmap contains the powerful **Nmap Scripting Engine (NSE)** which 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.

```
(kali㉿Kali)-[~]
$ nmap --script smb-enum-users.nse -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 19:11 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.012s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| smb-enum-users:
|_ GRAVEMIND\arbiter (RID: 1001)
|   Full name:
|   Description:
|   Flags:      Normal user account, Account disabled, Password not required
|_ GRAVEMIND\masterchief (RID: 1000)
|   Full name:
|   Description:
|   Flags:      Normal user account, Account disabled, Password not required
Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
```

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**.

```
└─(kali㉿Kali)-[~]
$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 19:45 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0032s 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 7.68 seconds
```

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**.