NMAP

Step 1
To Identify the IP Address of the Victim machine / Attacker machine
Type in the command

```
ifconfig
```

Step 2
Display Ping Help Menu
To know the list of commands which are ping instructions, run

```
ping -h
```

Step 3
Ping the Ip Range Manual Page
To know the list of commands ping, run

```
man ping
```

Step 4
Perform a Basic Ping Scan
This will perform a ping TCP ECHO scan on the host (victim / VM) and will ignore the host discovery process, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 5
Perform Service Version Detection
This is a ping scan which will also check whether the host is alive or not and also it will try to find the service version, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 6
Scan a Range of Ports
Example Port is 21-80
Type in the command

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 7
Scan Specific Ports
Example Port is 21-443
Type in the command

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 8
Scan All Ports (1-65535)
Type in the command

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 9
Save Nmap Scan Results in a File
To save the scan results in a file, run the command

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 10
Detect the Operating System of a Target
To perform OS detection, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 11
Perform an Aggressive Scan
This is a ping scan which will perform OS detection, service detection, script scanning and traceroute, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 12
Perform a TCP SYN Scan (Stealth Scan)
Perform a TCP SYN scan on the victim / target host, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 13
Perform a UDP Scan
Perform UDP scan on a target, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 14
Perform a Default Scripts Scan
Perform a default scripts scan, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 15
Perform a Vulnerability Scan Using NSE Scripts
Run Nmap vulnerability scripts against the victim, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 16
Perform a Vulnerability Scan Using NSE Scripts
Run Nmap vulnerability scripts against the victim, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 17
Perform a Vulnerability Scan Using NSE Scripts
Run Nmap vulnerability scripts against the victim, run

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Reference
Nmap has documentation as well. Type in the command **nmap man** and it will open a man page with all the options and their descriptions.
Also type in **nmap -h** to get the complete hyperlinks, lists of the different Nmap options and their descriptions.

Reference
Nmap has documentation **at nmap.org**. Also, the Nmap manual page is a hyperlinked version of the Nmap manual.

Reference
Nmap has documentation **at discovered.pcacademy.com**. Also, the Nmap manual page is a hyperlinked version of the Nmap manual.

After Finding Open Ports - What Next?
Once you've identified open ports and services, the next step is to **perform vulnerability scanning** and **exploitation** to assess the security of the target system. This helps in **vulnerability management** and **penetration testing**.

We will now proceed with a basic exploitation demo on Metasploitable 2 - Complete Hacking Process Simulation

Note: This is a preliminary, simulated exercise designed for learning and training purposes.

Tool
Tool: Full Exploitation Workflow on Metasploitable 2 - Complete Hacking Process Simulation

Step 1
Reconnaissance
Gather information about the target.

Suppose you want to find the service version and exact ip in discover active hosts.

Type in the command options

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 2
Step 1 - Port Scanning with Nmap
Run a TCP connect() scan (most common) to find open ports on the target machine.
Use -sV to detect service versions and -p- to scan all ports.

Expected Output

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Identifying Vulnerable Services
Look for services with outdated or known vulnerabilities (example: services like vsftpd, apache, samba, etc.). These are potential entry points for exploitation.

Expected Output

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 3
Step 2 - Vulnerability Scanning with Nmap Vulnerability Scripts
Use Nmap's vulnerability scripts (-sV --script vuln) to automatically identify known vulnerabilities.

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Expected Output (Simplified)

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Focus on ports 21, 445, and 6667 for exploitation in Metasploitable 2 scenarios.

Step 4
Gaining Access

Step 5
Step 1 - Start Metasploit Framework
Launch **msfconsole** to begin exploitation.

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 6
Step 2 - Search for the Exploit Module
Find the relevant **vsftpd** exploit:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Sample Output

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Exploit Rank Definitions (Important for Interviews):
Excellent, Great, Good, Normal, Average, Low, Manual

Step 7
Step 3 - Load the Exploit Module

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 8
Step 4 - Set Target IP Address
Configure the exploit with the target machine's IP address:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Verify Exploit Options (OPTIONS)
Check required parameters and their defaults:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 9
Step 5 - Run the Exploit
Execute the exploit:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 10
Maintain Access

Step 11
Step 1 - Get a Root Shell
If the exploit is successful, you will obtain a root shell. You can verify the access:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Expected Output

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Congratulations! You have successfully compromised your first target machine using Metasploit.

Step 12
Covering tracks (Optional)

Step 13
Clear Bash History
To remove your command history:

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Advanced Log Cleanup
Locate and remove system logs (/var/log/), audit logs, and other **LOGS FILES** Persistence artifacts.
Use tools like **shred** for secure file deletion.

Step 14
Remove Logs (auditing, syslog, wtmp, etc.)

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 15
Delete Shell History of Other Shells

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Step 16
Remove Command History of 'ls' Commands

```
ping -n -sn -PE -PA -PS -PU -PY -PP -PM -PO -PR -n -vv -oN -
```

Reference
Recap Flow
Reconnaissance → Scanning → Gaining Access
Maintain Access
Remove Logs (optional)
Delete Shell History
Remove Command History

Reference
Ethical Note
Unauthorized access is illegal. Use **exclusively** on **pcacademy** or **pcacademy** controlled systems.
Never attempt exploitation against anything or machines not owned by you or PCA Academy.
Stay ethical and responsible.

Contact

Author: Kumaran Vasudevan
Email: kumaran@pcacademy.com
Website: www.pcacademy.com