Nmap (network mapper)

Official website links - https://nmap.org/
https://nmap.org/docs.html
https://nmap.org/book/intro.html

IBM links- https://www.ibm.com/docs/en/dsm?topic=guide-nmap-scanner-overview
https://www.ibm.com/docs/en/dsm?topic=overview-adding-nmap-remote-result-import

```
┌──(kali㉿kali)-[~]
└─$ man nmap
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -help
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Introduction

Nmap is a tool used for network mapping and it is one of the most popular ethical hacking tools in the market. Nmap is used to discover free networks around you. Network administrators find Nmap very useful as they always need to map their networks.

Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing. Gordon Lyon (pseudonym Fyodor Vaskovich) created it to help map an entire network easily and find its open ports and services.

Hackers also started using Nmap for auditing networks and other purposes.

In this guide, we are going to look at What Nmap is, Nmap commands, and some more useful information about Nmap.

What is Nmap?

Nmap is a short form of Network Mapper and it's an open-source tool that is used for mapping networks, auditing and security scanning of the networks. The reason behind its development is to quickly find large networks at a specific location. For the discovery of networks, the raw IP packets are used by Nmap. The most common use of Nmap is for security audits of networks.

As we see the rise in IoT devices and therefore, the networks are getting more complex for the companies using IoT devices. In this situation, Nmap comes into view where it can be used for auditing the network traffic between web servers of the organisation and the IoT devices.

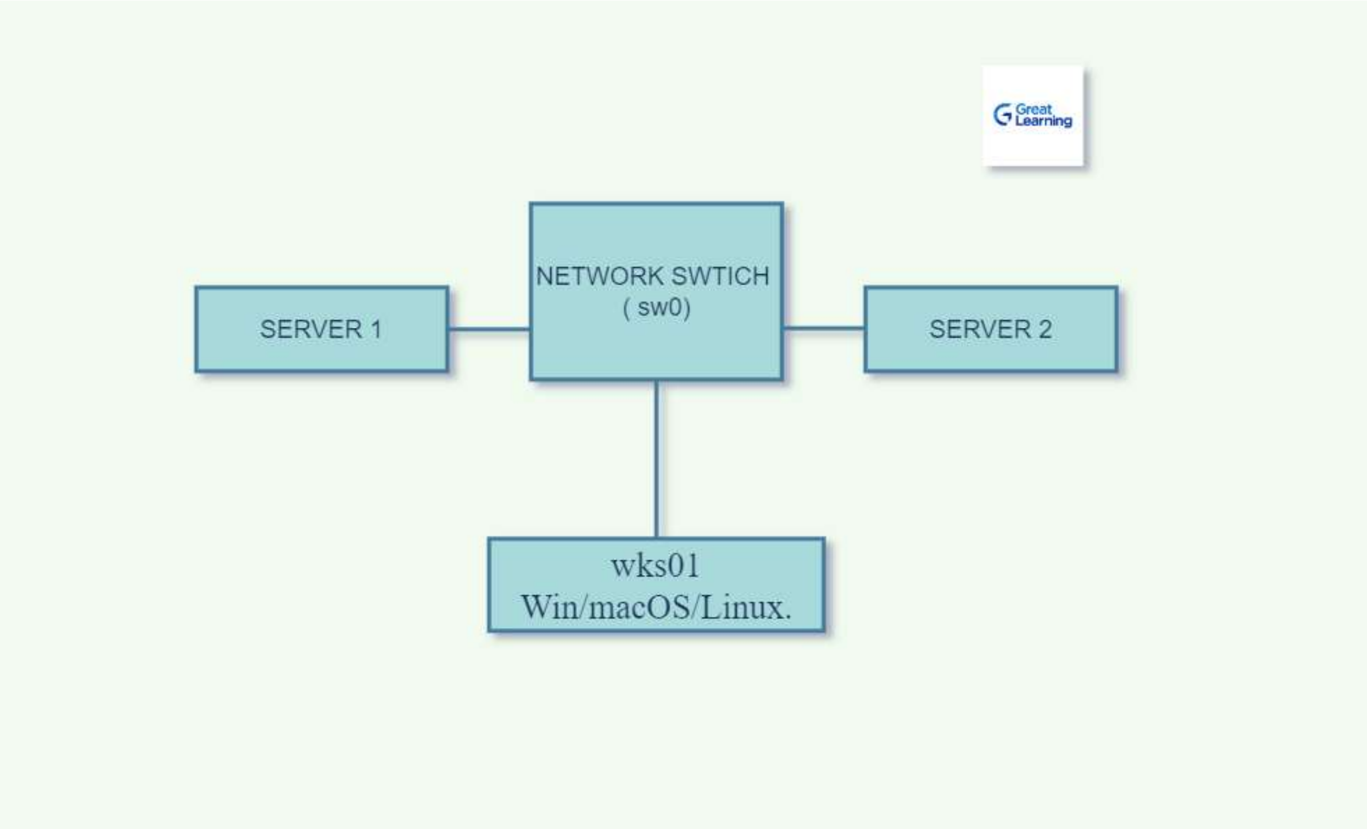
Why learn about Nmap?

There can be various reasons to learn about Nmap. However, some of them include the following:

- It allows you to quickly find the networks and the devices on a specific network.
- Nmap is useful to find out which services are running on a system that includes all the web services and DNS servers.
- You can also find information about the operating system running on devices on a network.
- The GUI of Nmap is Zenmap which you can use to see the mappings of a network to use it for reporting and to enhance its usage.
- You can easily find out unauthorized services on your network.
- Nmap helps you to find the devices with open ports and you can look at them to enhance their security.

Nmap Command Examples in Linux and Unix

The port scanning is restricted and may result in an unethical practice from some jurisdictions' point of view. Therefore, the Unix Lab setup can be done as follows:



In the above diagram, the Lab is set up in this way where,

- Server (1) is powered by an Operating system such as Win/macOS or Linux that will work as an unpatched server.
- Wks01 shows your operating system used for scanning the local networks using Nmap.
- Server (2) works the same as the server(1) where it is also powered by the operating system but the difference is that it is a fully patched server integrated with a firewall.
- All three systems such as Server(1), wks01 or the operating system, and server(2) are connected via a network switch.

Check out this Linux Tutorial

Features of Nmap

There are several features of Nmap that include the following:

- **OS Detection:** OS scanning can be done in Nmap that detects the OS, version of the OS, and other details about it.
- **Service Detection:** The several service probs found in the Nmap-services-probe-file are used to get the responses from network services and their applications.
- **Host discovery:** This method is used by network hosts to gather data about other hosts in the network by the use of TCP and UDP protocols.
- **Target Specification:** The target specification feature can be used to specify a Target IP address that you want to scan in Nmap.

- **IPv6 Support:** IPv6 means Internet Protocol version 6 and it can be used in Nmap for scanning the network. As IPv6 is capable of scanning larger addresses than IPv4, it makes scanning through CIDR-style scanning ranges that make it idle for scanning larger addresses.
- **NSE Functionality:** NSE stands for Nmap Scripting Engine and it comes in Nmap functionality that you can use for host discovery, network scanning, and target specification.
- **TLS/SSL scanning:** The TLS deployment problems can be analyzed fastly with the help of Nmap.

Nmap Commands

Here is the list of Nmap Commands

1. Scan a Range of IP Address
2. Port Scanning
3. Ping Scan Using Nmap
4. Saving the Nmap Scan Output to a File
5. Most Popular Ports Scanning
6. Display Open Ports:
7. Exclude Host/ IP Addresses for the Scan
8. Service Version Detection

1. **Scan a Range of IP Address:** To scan a range of IP addresses, the Nmap command is as follows:

```
nmap 192.168.1.1-24
```

```
ifconfig, copy echo0 ip, cd Desktop, nmap –oG -192.168.1.0-255 –vv > /home/Desktop/Result
```

- 2. **Port Scanning**: There are multiple commands in Nmap for scanning ports such as:

To scan TCP port 80, the following Nmap command can be used:

```
nmap -p T:80 192.168.1.1
```

To scan UDP port 53:

```
nmap -p U:53 192.168.1.1
```

To scan the range of ports:

```
nmap -p 80-160 192.168.1.1
```

We can also combine all these commands to scan multiple ports:

```
nmap -p U:53, 112, 135, T:80, 8080 192.168.1.1
```

- 3. **Ping Scan Using Nmap**: It can be used for host discovery and the following command can be used:

```
nmap -sP 192.168.1.1/20
```

- 4. **Saving the Nmap Scan Output to a File**: The syntax for the command to save the Nmap output to a text file is as follows:

```
nmap 192.168.1.1 > op.txt
```

```
nmap -oN /temp/files/output/ 192.168.1.1
```

```
nmap -oN op.txt 192.168.1.1
```

- 5. **Most Popular Ports Scanning**: The most popular TCP ports can be scanned using TCP SYN scan and the following command exists for this purpose:

```
nmap -sS 192.168.1.1
```

- the above command is used for stealthy scan

For OS fingerprinting, the following command can be used:

```
nmap -sT 192.168.1.1
```

- 6. **Display Open Ports**: The command for displaying open ports on the network is as follows:

```
nmap –open 192.168.1.1
```

```
nmap –open server2.gl.biz
```

```
nmap –open 192.168.0.1
```

- 7. **Exclude Host/ IP Addresses for the Scan**: In order to exclude the hosts from the Nmap scan, you can use the following Nmap commands:

If you are scanning a number of hosts/networks, then you can exclude hosts/IPs from a scan by using:

```
nmap 192.168.1.1-24 –exclude 192.168.1.4
```

or

```
nmap 192. 168.1.1-24 –exclude 192.168.1.3, 192.168.1.7
```

for excluding more than one host.

- 8. **Service Version Detection:** The service version can be detected for IPv4 script with the help of Nmap by using any of the following commands:

```
nmap -A 192.168.1.254



or



nmap -v -A 192.168.1.1



or



nmap -A -iL /user/temp/list.txt
```

NMAP Commands Cheat Sheet

The following is a Nmap Command CheatSheet that contains some useful Nmap Commands:

Nmap commands for Port Selection:

Description	Commands
To scan a single port using Nmap:	nmap -p 8 192.168.1.1

To scan a range of ports using Nmap:	nmap -p 1-20 192.168.1.1
For scanning common ports of the network:	nmap -F 192.168.1.1
If you want to scan all the 65532 ports of the network, then use the corresponding command:	nmap -p- 192.168.1.1

Nmap Commands for Target Selection:

Description	**Commands**
To scan a single IP host:	nmap 192.168.1.1
For scanning the range of IPs:	nmap 192.168.1.1-15
If you want to scan a single host:	nmap www.<hostname>.com
For scanning targets from text file, you should use the corresponding Nmap command:	nmap -iL target-ip-lists.txt

These commands are used to perform default scans using Nmap and it scans 1000 TCP ports where host discovery will also take place.

Nmap commands for OS and Version Detection:

Description	**Commands**
For detection of OS and the services:	nmap -A 192.168.1.1
To detect aggressive services:	nmap -sV –version-intensity 4 192.168.1.1

For standard version detection: nmap -sV 192.168.1.1

The above commands are used to determine the operating system running on a particular port of the network. The command that we discussed for aggressive services detection can be used for the services running on unusual ports of the network.

Nmap commands for different Output Formats:

Description	Commands
If you want to save default output to a file:	nmap -oN op.txt 192.168.1.1
To save the output in all formats:	nmap -oA op 192.168.1.1
To save results in XML format:	nmap -oX op.xml 192.168.1.1
To save the Nmap results in format for grep:	nmap -oG op.txt 192.168.1.1

The default output can also be saved by simple redirecting the file with the command: command>file. In the above command, oN is used to save the results and also monitors the terminal for scanning.

Nmap command for IP address info:

To get the information of IP Address:	nmap- –script=asn-query, whois, ip-geolocation-stateloc 192.168.0.1/22

The command above can be used to get the details related to the IP address and owner of that IP address. This command uses WhoIS, GeoIP location lookups and ASN query.

Nmap commands to gather HTTP service information:

Description	Commands
To get the HTTP headers of web services:	nmap –script=http-title 192.168.1.0/24

Command to find web apps from specific paths:	nmap –script=http-enum 192.168.1.0/24
To gather the data about page titles from HTTP services:	nmap –script=http-title 192.168.10/24

These commands used to get the details about HTTP service are very useful for larger networks as it identifies the HTTP services on the network and reports immediately results.

To get more information about NSE scripts:

Description	**Commands**
To scan some default scripts:	nmap -sV -sC 192.168.1.1
Nmap command for scanning a set of scripts:	nmap -sV –script=aqb* 192.168.1.1
To scan a specific NSE script:	nmap -sV -p 443 –script=ssl-gl.nse 192.168.1.1
To get help for a script:	nmap –script-help=ssl-gl

There are several NSE scripts in nmap that can be used for a wide range of security testing in the network. These scripts are also helpful in the discovery of new networks. The -sV parameter used in the commands above is used as a service detection parameter.

Nmap commands for port scan types:

Description	**Commands**
To scan selected ports	nmap -Pn -F 192.168.1.1
Nmap command to scan UDP ports:	nmap -sU -p 123, 161, 162, 192.168.1.1
To scan using TCP SYN scan :	nmap -sS 192.168.1.1

To scan using TCP connect to port:	nmap -sT 192.168.1.1

These commands are very useful to scan port types. The SYN scan requires some privileged access and it uses TCP connect scan for insufficient privileges. The -Pn in the above commands is used for the PING parameter.

Conclusion

Nmap is a powerful tool used for networking and security auditing of networks. Nmap is helpful for quickly finding useful information about the networks, ports, hosts, and operating systems. There are other settings of Nmap too that enhance its productivity. In this article, we discussed the features of Nmap and why it should be learned. Also, we saw its cheatsheet where we included some commonly used commands of Nmap. Here comes the end of this article.

Frequently Asked Questions

Why is the Nmap command used?

The Nmap commands are used for a number of reasons that include security configurations and network auditing. The major reason for using Nmap is that it helps to find out networks very quickly and no complex configurations are needed to do this. Nmap also supports commands and scripting which makes it very useful for network administrators.

How many commands are there in Nmap?

There is a number of commands in Nmap and the number differs from version to version. Also, commands can be joined to make another command which means the total number of commands can also be increased. However, there are 50+ commands available in Nmap.

Do hackers use Nmap?

The answer is Yes because Nmap can be used to gain access to uncontrolled ports on the network that may lead to providing access to the system. The hackers run the commands to get into the targeted system and can exploit the vulnerabilities of that system.

How do I scan an IP with Nmap?

To scan an IP, you must know the subnet you are connected to. The following command can be used to scan an IP with Nmap:

```
nmap 192.168.1.1
```

What is the Nmap tool?

Nmap is a very useful network scanning tool. Nmap is used to identify the devices connected to a network with the help of IP packets. It can also be used to get information about the services running on the network and the OS.

How to install Nmap Linux?

The following steps can be followed to install Nmap Linux:

1. First update the list of Ubuntu packages and you also need to make sure before you install the Nmap, that all the packages are up-to-date. The command can be used to update packages on Ubuntu:

```
sudo apt-get update
```

2. Now after updating all the packages, you can install Nmap by using the following command:

```
sudo apt-get install nmap
```

3. Finally, in order to check if it is successfully installed on your system or not, you may use the following command and it will give you the version details of Nmap if installed successfully.
nmap –version

What does Nmap do for Linux?

Nmap uses IP packets to find the devices connected to a network and it also provides information about the OS and the services running on it.

How do you run Nmap?

To run Nmap, you need to check if it is installed on your system or not by using the following command:
nmap –version
If nmap is not installed, then you need to install it first and then you can run it by using the command below:
nmap [hostname] or nmap [ip-address]
You need to use the hostname or ip-address that you want to run Network Mapping.

Important blogs Links –

https://www.javatpoint.com/what-is-nmap#

https://u-next.com/blogs/cyber-security/nmap-commands/

https://www.tutorialspoint.com/nmap-cheat-sheet

https://www.interviewbit.com/blog/nmap-commands/

https://www.stationx.net/nmap-cheat-sheet/

https://www.upguard.com/blog/how-to-use-nmap#:~:text=network%2C%20read%20on.-,What%20is%20Nmap%3F,its%20open%20ports%20and%20services. \

https://www.geeksforgeeks.org/nmap-cheat-sheet/

https://www.upguard.com/blog/how-to-use-nmap#:~:text=network%2C%20read%20on.-,What%20is%20Nmap%3F,its%20open%20ports%20and%20services.