1. Syntax for scanning a single IP.

Syntax:

```
nmap <ip address>
```

Here <ip address> needs to be replaced by the actual IP address for which one would need to perform the snif!

2. Syntax for scanning a host.

Syntax:

```
nmap <host name>
```

Here <host name> needs to be replaced by actual host address for which one would need to perform the snif.

3. Scanning a range of IPs.

Syntax:

```
nmap <ip address range>
```

Here <ip address range> needs to be replaced by a range of IP addresses for which one would need to perform the snif.

4. Scanning a single port.

Syntax:

```
nmap -p <port number> <IP address>
```

5. Scanning range of ports.

Syntax:

```
nmap -p <range of port number> <IP address>
```

6. Scanning 100 most common ports.

Syntax:

```
nmap -f <IP address>
```

7. Scan using TCP SYN scan.

Syntax:

```
nmap -sS <IP address>
```

How to Use Nmap in Kali Linux?

- Nmap can be used for specific utilities as mentioned in the list above, and specific tasks can be accomplished by utilizing various options available with Nmap. Nmap mainly aims at protecting the network by performing a sniffing which leads to detailed network analysis. The detailed network analysis enables the admin who built the system to protect on a network to have complete detail about the packet traffic. Being vigilant and prepared allows the admin to quickly respond to attacks.

- The first way to use Nmap is to use the command to scan single IP. Using this, the “threat sniffer” who is noticing some unfamiliar activities from a single IP can scan so that the false positives and false negatives can be distinguished and hit the target if the IP is a notorious one. False positives trigger alert unnecessarily, which might hide any attack. Using the utility to distinguish false positives and false negatives will allow false positives to come out in the open and keep the network analyst on toes to respond to any true positive attack without worrying about the false positives.
- The next way to use Nmap is by scanning a host for information that might make it a high-value target on a network that the hacker is on the lookout for. For example, attackers prey on the specific host containing financial information.
- In an extended scenario of scanning an IP address, a user also has the flexibility to use Nmap to scan a range of IP addresses to look for instances or loopholes through which an attack might be possible. In an advanced situation of port selection, Nmap might be used extensively as well. Nmap allows user to also scan ports along with the utility we mentioned above about scanning IP address and range of IP address. Using a scan of the port, one can quickly determine if malware is attacking as malware generally hits a

specific port in the host. Now, if we are not aware of the ports that are malfunctioning, we can scan a range of ports, similar to one we had for scanning the range of IP addresses. Nmap also provides the functionality to scan the 100 most common ports and even scan all the available 65535 ports (this scan will take a lot of time).

Examples of Kali Linux Nmap

Given below are the examples of Kali Linux Nmap:

Example #1

The syntax for scanning a single IP.

Syntax:

```
nmap 192.27.9.91
```

Output

Example #2

The syntax for scanning a host.

Syntax:

```
nmap www.yahoo.com
```

Example #3

Scanning a range of IPs.

Syntax:

```
nmap 192.27.9.89-91
```

Example #4

Scanning a single port.

Syntax:

```
nmap -p 80 192.27.9.91
```

Example #5

The scanning range of ports.

Syntax:

```
nmap -p 81-90 127.27.9.91
```

Example #6

Scanning 100 most common ports.

Syntax:

```
nmap -f 192.27.9.91
```

Example #7

Scan using TCP SYN scan.

Syntax:

```
nmap -sS 192.27.9.91
```

Conclusion

This article has a flavor of how Nmap comes in handy for a penetration tester or a network analyst. Using the details printed on the console, one can take a copy of the same into a text editor perform required analytics. Along with this, Kali Linux provides utility to get the entire result of the Nmap on a file and utilize it later for its numerous other uses. With just its one base command with multiple other options, Nmap helps users with loads of information to protect machines from unwanted attacks.

https://www.educba.com/kali-linux-nmap/