Practical No. 6

Aim: List and Use of NMAP Command in Kali Linux.

1. Introduction to Kali NMap

Kali Linux Nmap is defined as a utility which is extensively used by penetration testers for network discovery and auditing the security of a system. In addition to the tasks mentioned earlier, users find the use of Nmap in various other tasks like network inventory, managing schedules for any service upgrades, host monitoring, service uptime tracking etc. Nmap stands for “Network Mapper”. Nmap utilizes novel ways of using IP packets for determining the hosts available on the network, services offered by the hosts, operating systems they are running on, types of packets or firewalls being used and many such characteristics. Also important to note that Nmap was adjudged as a security product of the year by Linux Journal, Info World and many such associations.

2. What Does Nmap Do?

Nmap is used to offer detailed, real-time information on our networks and the devices connected to them. Nmap's primary uses can be divided into three categories. First, the program provides detailed information about each **IP** active on our networks, after which each IP can be scanned. This helps administrators determine whether an IP address is being used by a legitimate service or by a malicious outsider.

Second, Nmap gives us information about the entire network. It can be used to display a list of **active hosts** and **open ports**, as well as **identify the operating system** of all connected devices. This makes it an important aspect of penetration as well as a handy tool for ongoing system monitoring. Nmap can be used with the **Metasploit** framework to probe and then patch network vulnerabilities.

Third, Nmap is also a useful tool for users who want to secure their personal and corporate websites. Scanning our **web server** with **Nmap**, especially if we are hosting our website from home, is effectively replicating how a hacker would attack our site. This method of **"attacking"** our own site is a very effective means of finding security vulnerabilities.

Nmap is easy to use, and majority of its tools are familiar to system admins from other programs. Nmap has the advantages of combining a variety of these capabilities into a single package, rather than forcing us to switch between other network monitoring tools. You must be familiar with the **command-line** interface in order to use Nmap.

Although most sophisticated users can write scripts to automate common operations, but basic network monitoring does not require this.

3. 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).

4. Syntax of Kali Linux Nmap

In Kali Linux, analyzing network or in hacking terms, we call it as “sniffing network” is an important skill and tools for the same is without a doubt the absolute necessity so that we can uncover the potential attacks possible in the weak points in the network and fix them to safeguard our system. Below are some syn-taxes which pose great help in “network sniffing”.

i. **Syntax for scanning a single IP.**

```
nmap <ip address>
```

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

ii. **Syntax for scanning a host.**

```
nmap <host name>
```

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

iii. Scanning a range of IPs.

```
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.

iv. **Scanning a single port.**

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

v. **Scanning range of ports.**

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

vi. **Scanning 100 most common ports.**

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

vii. **Scan using TCP SYN scan.**

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

4. Examples of Kali Linux Nmap

Given below are the examples of Kali Linux Nmap:

Example #1

The syntax for scanning a single IP.

```
nmap 192.27.9.91
```

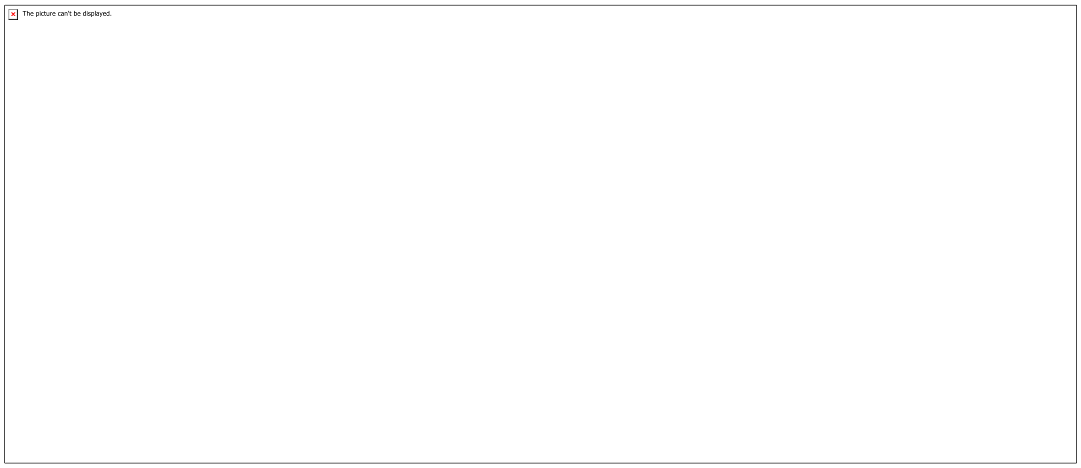
Output:

Example #2

The syntax for scanning a host.

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

Output:



Example #3

Scanning a range of IPs.

```
nmap 192.27.9.89-91
```

Output:

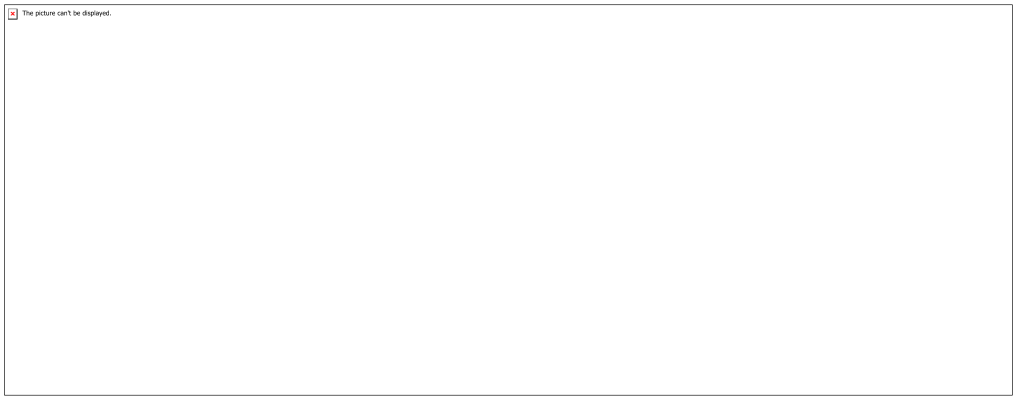
All the IP address in the range of 89 to 91 (namely 192.27.9.89, 192.27.9.90, 192.27.9.91) are scanned.

Example #4

Scanning a single port.

```
nmap -p 80 192.27.9.91
```

Output:



Only port 8o is scanned, and the result is printed on the console.

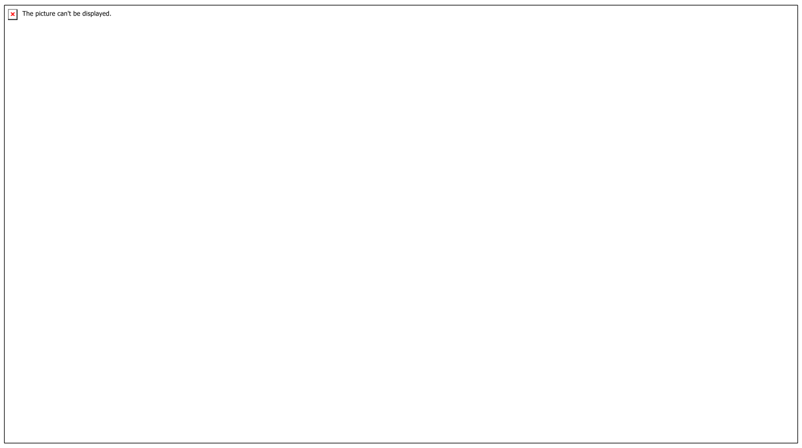
Example #5

The scanning range of ports.

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

All the ports in the range 81-90 are tested, and the result is printed on the console.

Output:

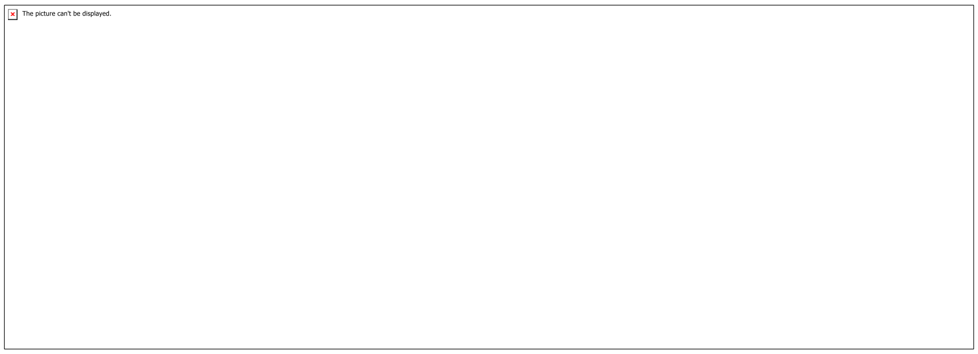


Example #6

Scanning 100 most common ports.

```
nmap -f 192.27.9.91
```

Output:



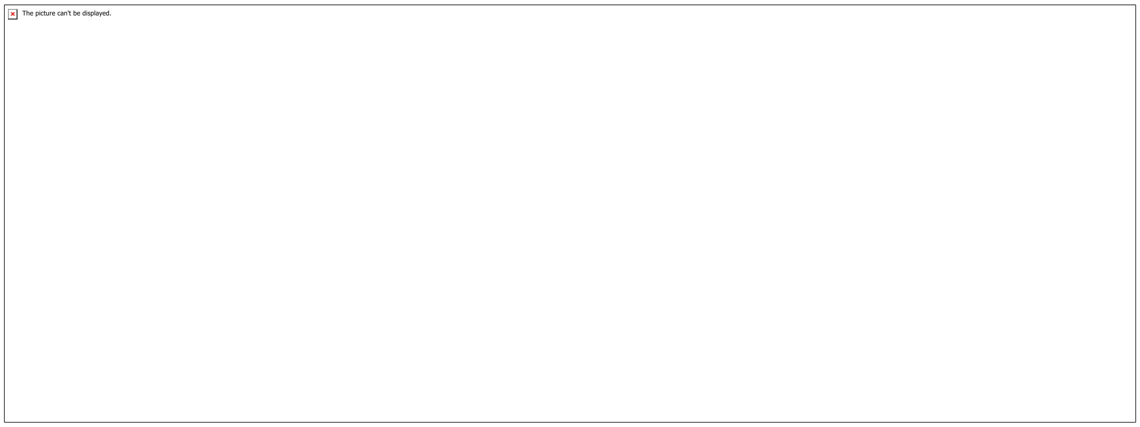
Since this IP address runs on only one port, not all 100 ports have been tested.

Example #7

Scan using TCP SYN scan.

```
nmap -sS 192.27.9.91
```

Output:



We see that both the repository, the one for experimental is also in place in the source.list.

5. 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.