Hello Everyone! In this video, you will learn about Nmap, the network mapper and its usage for a security professional as well as an attacker. This utility is used by both attackers or security professionals with different intentions.

Nmap (*Network Mapper*) is a free and open-source network scanner.
It is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
It provides a number of features for probing computer networks, including host discovery and service and operating system detection. Its features are extensible using scripts that provide more advanced service detection.
Before proceeding to learn nmap, it can be noted, that using nmap to scan any machine without proper authority or permission is unauthorized. Therefore, a virtual environment has been provided to you for experimenting with this command. Please note that, you have to scan the given target(windows) machine only. Scanning any other machine may block your candidature and you may face legal action.

Let's understand some important nmap command syntaxes. Nmap command can be used with the ipaddress of the host machine, to be scanned by default. If you want to scan with hostname, simply replace the IP address with the host name in the command syntax.
For example, nmap cdac.in command will scan the machine with hostname cdac.in.

You can use nmap to scan specific ports or scan entire port ranges on a local or remote server. In this example, all 65535 ports have been scanned on a machine.
Nmap is able to scan all possible ports, a range of ports or a specific single port by using the command line option p, as shown.

This screenshot shows the usage of nmap command to scan specific ports 80 and 443 on a machine. This command shows, the status of the ports (open/closed or filtered) on the target machine.

You can also scan multiple consecutive IP addresses using nmap for open ports and running services. The screen shot shows you, using nmap for scanning 9 iP addresses starting from 192.168.45.130 to 192.168.45.138.

Rather than providing comma separated ip addresses to nmap command, you can use CIDR notation of ip addresses to specify a range of addresses also. CIDR range specifies classless address. Here in the screen shot, you can see a CIDR range 192.168.45.0/24 to be scanned, which represents 256 addresses starting from 192.168.45.0 to 192.18.45.2255.

Nmap allows you to use wildcards also to scan an IP range. In the given screenshot, you can see, that wild card character star has been used to represent the complete class c address range starting from 192.168.45.0 to 192. 168.45.255.

If you ever need to exclude certain IPs from the IP range scan, you can use the "–exclude" option with Nmap command. This option is used, when you want to scan a range of ip addresses excluding few of them. E.G. you want to scan all the public ip addresses of an organization, but the one running firewall or honeypot is required to be excluded.

Nmap maintains a database of the ports which are *usually* open on Internet machines, known as top ports. You can scan for these ports using –top-ports command option with number of top ports to be scanned. Here top 20 ports are being scanned on the machine with ip address 192.168.1.130.

This is sometimes possible for a network administrator, to scan same set of machines again and again using Nmap. In such situations, nmap allows you to record the ip addresses or host names in a text file and use this text file every time you scan rather than typing all the ip addresses again and again.

The “-iL” parameter lets you read from that file, and scan all those hosts for you. Here, the screenshot shows that the site.txt file contains all the ip addresses and host names to be scaned and the command line option –iL allows reading from this file to scan these hosts using nmap.

As nmap allows to read the ip address list from a text file, it also allows to write the scanning results in a text file for later analysis using –oN option. It can clearly be seen in the screenshot that scanning output has been recorded in a file output.txt, which can be read later on.

Nmap not only scans for open ports on one or many machines, it also allows to detect the Operating system and various services running on the remote hosts using –A parameter.
In the given screenshot, the operating system of the remote host is identified. Another parameter –T4 has been used to make the scanning process faster. Nmap allows controlling the speed of scan using the options starting from T0(very Low) to T5(extremely aggressive).

As option A allows you to see the services running on remote host, the V option allows you to see the version of these running services also. This can be done by using -sV

parameter. The service version detection has been depicted here for the localhost that is the same computer.

Nmap also allows you to scan using specially crafted packets, with TCP or UDP protocols. To Use TCP, T parameter is used and for UDP scan U parameter is used. Most of the applications, except few use TCP protocol. Therefore, it is good to do TCP scan for them. Similarly, few applications such as DHCP, DNS, SNMP etc. use the services of UDP protocol. Therefore, performing UDP scan for these applications or ports associated with them is the preferred choice.

Nmap can be used to list out the live hosts in a network. This may help the administrator/attacker to focus on the running machines only to save the unnecessary efforts.
-sP command line option is used with the range of ip addresses for this.

Thank You!