*NMAP*

* What is Nmap?
  + Nmap is an open source utility that is used for finding vulnerable services on a network by scanning through different ports.
* Installation:
  + Windows OS: Nmap can be installed on the Windows workstation by visiting the official website (<https://nmap.org/download.html>) and downloading self-installer.
  + Linux OS: Nmap can be installed on Linux OS using following commands as per the appropriate Linux Distro:
    - “yum install nmap” / “sudo apt-get install nmap”
  + Mac OS: Nmap can be installed on Mac OS by following installation instructions mentioned on the official Nmap website: <https://nmap.org/download.html#macosx>
* Throughout this guide, all the commands are run on Ubuntu 20.04 OS and the outputs are taken on the same OS.
* After installing Nmap, the various options/switches can be found by running “man nmap” command on Linux which provide manual of Nmap. Below screenshot shows the output of same command:

Text

Description automatically generated

* Nmap contains different types of switches to run a variety of scans against the target system and the usage of each switch are provided in detail in next section of this guide.
* For testing the switches, a vulnerable virtual machine setup is created in same network range as the Attacker machine (Ubuntu 20.04) and various switches are used against this target system to analyse their outputs which are as follows:
  + -sn: This option is used for scanning hosts on the network and once the available hosts are discovered nmap stops the port scan.
    - Nmap -sn 192.168.133.0/24

Text

Description automatically generated

* + -PO [protocol list]: This option is used for performing host discovery with the specified port number set in the IP header.
    - Nmap -PO 192.168.133.0/24

Text

Description automatically generated

* Similar to -PO, the -PS and -PU options can also be used for performing various port scans as shown below:
  + -PS [portlist]: This option sends TCP request whereas an empty packet will be sent with SYN flag set.
  + -PU [portlist]: This option is used to send UDP packet for discovery to the given ports.
    - Nmap -PS 192.168.133.0/24
    - Nmap -PU 192.168.133.0/24

Text

Description automatically generated

Text

Description automatically generated

* + -sO: This option is used for determining supported IP protocols by target machine
    - Namp -sO 192.168.133.128

Text

Description automatically generated

* + -O: This option is used for determining OS version
    - Nmap -O 192.168.133.128

Text

Description automatically generated

* + -sV: This option probes open ports and determines service/version information
    - Nmap -sV -p 22 192.168.133.128

Text

Description automatically generated

* + -sT: This option is used for performing TCP connect scan on the target systems
    - Nmap -sT -sV 192.168.133.128

A screenshot of a computer

Description automatically generated with medium confidence

* + -sS: This option is usef for performing stealth scan on target system to identify vulnerable services
    - Nmap -sS -sV 192.168.133.128

A close-up of a document

Description automatically generated with medium confidence

* + sF: This option performs TCP FIN scan on target system to identify vulnerable services
    - Nmap -sF -sV 192.168.133.128

Text

Description automatically generated

* As observed, each scan performed results different output as per the appropriate circumstances on the target system/network and provides results in depth if used in correct way for identifying vulnerable servieces on the target network