**Module 3: Scanning Classroom Notes**

* Network Scanning Tool:

Nmap:(port scanning,Vulnerability Scanning, Security Auditing)

* Network Mapper tool and Security Port Scanner

( Usage command: nmap [Scan Type(s)] [options] Target Network/ IP

* Scan Techniques:
* -sS (Semi Scan- For Bypassing logs from firewall/Syslog server)
* -sT (TCP Syncronization)
* -sA (syn with Acknowledge)
* -T4 (Scan Speed)
* -sn ( host discovery in network)
* -sU (Scanning udp port)
* Specific Port Scan: Nmap -p(port number) Target host ip
* Port Range Scan: Nmap -p(Port range) Target host ip
* Operating System Detection: Nmap -O Target host ip
* Running Service and Version Detection: Nmap -sV Target host ip

Nmap Commands Cheat Sheets:

<https://cdn.comparitech.com/wp-content/uploads/2019/06/Nmap-Cheat-Sheet.pdf>

* Firewall/IDS Evasion and Spoofing:
* -f : Packet Fragmenting ( command: nmap -f [Target Ip]
* -g / -source-port( Defining specific port for connection by Setting port Number: Command: nmap -g[port number][Target Ip]
* -D (sending random dummy ip in network from single host)

(Command: nmap -D RND:[no.of Ip] [Target Ip]

RND- for Random Ip Generator

D- for decoy source ip

* Mac Spoofing: Sending traffic using fake mac-address

(Command: nmap -spoof-mac [Mac-address][Target Ip]

* Packet Crafting tool:
* Colasoft Packet Builder in windows 11(for Custom Packet Building)
* Ping Sweep Tools:
* Angry IP Scanner & Advance IP Scanner tools

( For Host Discovery, For Alive host Discovery)

To find out which IP addresses are in use, identify active devices, and retrieve information such as hostname and MAC address.

* Mega Ping,Netscan , Hping3 & SX tools
* Used for Network Scanning and Enumeration.