**NETWORK MAPPING AND ENUMERATION TOOLS**

NMAP COMMANDS  
  
nmap -sS <target IP> (simple scan)

Nmap –sT <target IP> ( sT to scan TCP)

Nmap –sU <target IP> (sU to scan UDP)

Nmap –sT cerifiedhacker.com

Nmap –sT scanme.org

Nmap –sT testphp.vulnweb.com

Nmap –sT ipaddress –O

-O scans operating system

-A aggressively scans & detects services + detects hardwares types.

-sV scans & detects services & versions

\*\*\*\*\* multiple scans at once

Nmap –sT 192.167.1.7 –sV –A –O

Entire network with all scans at once

Nmap –sT ipaddress/24 –sV –A –O

Nmap –sS ipaddress –p (-P scans ports)

Nmap –sS ipaddress –p- (scans entire range of ports)

Nmap –sS ipaddress –p-100 (range of ports)

Nmap –sS ipddress –F (Fsast scan top 100 (popular) port)

-oN filename.txt (save the scans into a textpath)

\*\*\*\*\* How to scan ports

Popular ports:

20,21 – FTP

22 – SSH

23 – Telnet

25 – SMTP

\*\*\*\*\*\*\* how to scan a list of networks?

Nmap –iL ipaddress –sV –A –O

ENUMERATION

Enum4linux –a <target ip>

NETBIOS ENUMERATION: mapping the network.

SNMP ENUMERATION: find info about routers, networks,switches, servers.

Snmp-check <target ip> –public

NFS ENUMERATION 🡪 works on servers.

Showmount -a <target ip>

Showmount –e <target ip>

Showmount –d <target ip>

SMTP ENUMERATION ->port 25

Nmap –p 25 –script=smtp-enum-users <target ip or domain name>

Nmap –script=ftp-anon –p 20,21,22 <target ip or domain name>

<https://highon.coffee/blog/nmap-cheat-sheet/#scan-techniques>