NMAP COMMANDS

1) **nmap -sV <TARGET> -p 1-65535** (Scan for running services on all 65535 ports)

2) **nmap -sS <TARGET> -p 80** (Its not always required to scan all TCP connections. This is known as "Half Open" You can issue a sync packet (SYN) and wait for a response)

3) **nmap -O <TARGET>** (This command lets you search for the operating system and version on a host)

4) **nmap -A <TARGET>** (Use this type of scan to identify what payloads would be most effective on a targets system. It uses TCP/IP fingerprinting method)

5) **nmap -sP <TARGET>** (Search for which hosts are running on a network, by sending ICMP echo request packets to each IP address on the network you're scanning – NOTE some sites will BLOCK this request)

6) **nmap -F <TARGET>** (Fast scan, which ignores lots of the ports but gives results very quick)

7) **nmap –top-ports 20 <TARGET>** (Using the "–top-ports" parameter along with a specified number lets you scan the "X" most common ports for that host)

8) **nmap -sT <TARGET>** (scan for UDP-based services)

9) **nmap -A -T4 <TARGET>** (using the "-A" enables OS and service detection, at the same time using "-T4" gives you a faster execution)

10) **nmap -sU <TARGET>** (UDP scan, by sending packets to the targeted port. If no response is received, the port will be considered as OPEN | FILTERED)