Nmap scan types Reference
TCP connect() Scan [-st] – full three-way handshake
- very effective, provides a clear picture of the ports you can and cannot access
- may trigger warning on FW, IPS or IDS
- uses a system call (connect()) to begin a TCP connection to target.
  a. Success – connection made
  b. Fail – connection could not be made (system is offline, port closed, or error occurred)

-[ss] SYN Stealth Scan – sends SYN, waiting for SYN/ACK, sends RST sent to tear down before full connection establishment
Response:
- SYN/ACK – port OPEN
- RST – port CLOSED
- No response – FILTERED (requires further probing – subject to FW rules)
Note: SYN scan can be detected – use “timing options” to hide your activity

-[sf,sn,sx] FIN, Null and Xmas Tree Scan –TCP header flags set, useful for IDS and FW detection evasion – never makes even part of a connection. Can be used to detect OS running.
Response:
- CLOSED port – responds with an RST upon receiving packets
- OPEN port – drop incoming packets (it’s listening for packets with SYN set)
- SF - FIN send a packet with only the FIN flag set,
- SX - Xmas Tree Scan sets the FIN, URG and PUSH flags,
- SN - Null scan sends a packet with no flags switched on.
Note: TCP/IP implementation following RFC 793 required.
Microsoft Windows does not follow the RFC, and will ignore these packets even on closed ports.
OS Detection – with running along an OS scan
- MS Windows system - SYN scan shows open ports, and the FIN/NUL/XMAS does not, chances are you’re looking at a Windows box

-[sp] Ping Scan - lists the hosts within the specified range that responded to a ping - detect computers online, rather than ports open.
Methods:
1. ICMP ECHO REQUEST (ping request) packet sent to the destination system.
2. ICMP ECHO REPLY received - system is up, ICMP packets are NOT blocked
   a. no response - Nmap will try a "TCP Ping", to determine whether ICMP is blocked, or host is really not online
   b. TCP Ping - sends either a SYN or an ACK packet to any port (80 is the default) on the remote system.
      a. RST or SYN/ACK received - system is online
      b. No response – system is offline, or the chosen port is filtered (not responding to anything)
3. Ping scan as root - the default is to use the ICMP and ACK methods.
4. Ping scan as non-root users will use the connect() method, which attempts to connect to a machine, waiting for a response, and tearing down the connection as soon as it has been established (similar to the SYN/ACK method for root users, but establishes a full TCP connection!)

[-po] – disable ICMP scan type
[-su] UDP Scan - sends 0-byte UDP packets to each target port on the victim.
  a. ICMP Port Unreachable message received - port is closed,
  b. Otherwise – port is assumed open.
[-si] Idle Scanning - advanced, highly stealthed technique.
No packets sent to the target which can be identified to originate from the scanning machine. A zombie host (and optionally port) must be specified for this scan type.
Read more http://www.insecure.org/nmap/idlescan.html

[-aA] ACK Scan - used to map firewall rule sets, distinguish stateful/stateless firewalls,
Response:
  a. RST - "unfiltered" (that is, it was allowed to send its RST through whatever firewall was in place).
  b. No response – “filtered” (firewall prevented the RST coming back from the port).
- stateless firewall – blocked incoming SYN packets
- stateful firewall - tracks connections and blocks unsolicited ACK packets
Note: ACK scan will NEVER show ports in the "open" state – always use in conjunction with another scan type

[-sw] TCP Window scan - similar to the ACK scan, can sometimes detect open ports as well as filtered/unfiltered ports due to anomalies in TCP Window size reporting by some operating.

[-sr] RFC Scan - used in conjunction with other scan types to try to determine if an open TCP or UDP port is an RFC service, and if so, which program, and version numbers are running on it. Decoys are not supported with RFC scans.

[-sl] List scan - prints a list of IPs and names WITHOUT actually pinging or scanning the hosts. DNS resolution will be used, disable it using the -n option.

[-sv] enables version detection – determine service/version info - critical in determining an entry point for an attack

[-oO] enables OS fingerprinting


Nmap output Reference
-numeric <filename>] standard Nmap format
-xml <filename> XML format
-gf <filename> Greppable format
-o [basename] all outputs using basename

Nmap Timing options
[-TO] Paranoid: Very slow, used for IDS evasion
[-T1] Sneaky: Quite slow, used for IDS evasion

[-T2] Polite: Slowly down to consume less bandwidth, runs ~10 times slower than default
[-T3] Normal: Default, a dynamic timing model based on target responsiveness
[-T4] Aggressive: Assumes a fast and reliable network and may overwhelm targets
[-T5] Insane: Very aggressive; will likely overwhelm targets or miss open ports

Nmap Scripting Engine
Default location of scripts available:
[-sc] Run default scripts
--script-updatedb Update script database

-sx -script <filename> | <category> | <directory> | <expression>[,...] Run individual or groups of scripts

Scripting Engine
Read more http://www.insecure.org/nmap/vscan/

Nmap Commands Cheat Sheet
# nmap [Scan Type(s)] [Options] [target specification]

Ping scan
# nmap -sP <target-range>
SYN scan discovered alive host
# nmap -sS -A <target host>
SYN scan of another host, with more information on output
# nmap -sS -0 -P -A <target host>
Scan 100 most common ports of <target> “Fast”
# nmap -sS <target host>
Scan specific ports on target
# nmap -p <target port>
Using scripting engine
Scan using default safe scripts
nmap -sV -sc <target host>
Get help for a script
# nmap --script-help=ssl-heartbleed
Scan using a specific NSE script
# nmap -sV -p 443 -script=ssl-heartbleed.nse <target host>
Scan with a set of scripts
# nmap -sV --script=smb* <target host>
Scan for “Heartbleed” vulnerability
# nmap -sV -p 443 --script=ssl-heartbleed <target range>

WARNING: Only scan hosts and networks that you own or have permission to scan! Don’t be evil. LIFARS LLC is not responsible for misuse of information provided in this document.
TIP: You can use scanme.nmap.org to test and learn nmap!