Professor Messer's Quick Reference Guide to NMAP

Professor Messer

Contributed By:
shravansofts2011@gmail.com

SCAN OPTION SUMMARY

Scan Name	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Stealth Scan	-sF	YES	YES	NO
Xmas Tree Stealth Scan	-sX	YES	YES	NO
Null Stealth Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

HOST AND PORT OPTIONS

Exclude Targets	--exclude <host1 [,host2],...>
Exclude Targets in File	--excludefile <exclude_file>
Read Targets from File	-iL <inputfilename>
Pick Random Numbers for Targets	-iR <num_hosts>
Randomize Hosts	--randomize_hosts, -rH
No Random Ports	-r
Source Port	--source-port <portnumber>
Specify Protocol or Port Numbers	-p <port_range>
Fast Scan Mode	-F
Create Decoys	-D <decoy1 [,decoy2][,ME],...>
Source Address	-S <IP_address>
Interface	-e <interface>
List Interfaces	--iflist

TUNING AND TIMING OPTIONS

Time to Live	--ttl
Use Fragmented IP Packets	-f, -ff
Maximum Transmission Unit	--mtu <databytes>
Data Length	--data-length <databytes>
Host Timeout	--host-timeout <milliseconds>
Initial Round Trip Timeout	--initial-rtt-timeout <milliseconds>
Minimum Round Trip Timeout	--min-rtt-timeout <milliseconds>
Maximum Round Trip Timeout	--max-rtt-timeout <milliseconds>
Maximum Parallel Hosts per Scan	--max-hostgroup <number>
Minimum Parallel Hosts per Scan	--min-hostgroup <number>
Maximum Parallel Port Scans	--max-parallelism <number>
Minimum Parallel Port Scans	--min-parallelism <number>
Minimum Delay Between Probes	--scan-delay <milliseconds>
Maximum Delay Between Probes	--max-scan-delay
Timing Policies	--timing, -T<0|1|2|3|4|5>

PING OPTIONS

ICMP Echo Request Ping	-PE, -PI
TCP ACK Ping	-PA[portlist], -PT[portlist]
TCP SYN Ping	-PS[portlist]
UDP Ping	-PU[portlist]
ICMP Timestamp Ping	-PP
ICMP Address Mask Ping	-PM
Don't Ping	-P0, -PN, -PD
Require Reverse	-R
Disable Reverse DNS	-n
Specify DNS Servers	--dns-servers

REAL-TIME INFORMATION OPTIONS

Verbose Mode	--verbose, -v
Version Trace	--version-trace
Packet Trace	--packet-trace
Debug Mode	--debug, -d
Interactive Mode	--interactive
Noninteractive Mode	--noninteractive

OPERATING SYSTEM FINGERPRINTING

OS Fingerprinting	-O
Limit System Scanning	--osscan-limit
More Guessing Flexibility	--osscan-guess, --fuzzy
Additional, Advanced, and Aggressive	-A

VERSION DETECTION

Version Scan	-sV
Don't Exclude Any Ports	--allports
Set Version Intensity	--version-intensity
Enable Version Scanning Light	--version-light
Enable Version Scan All	--version-all

RUN-TIME INTERACTIONS

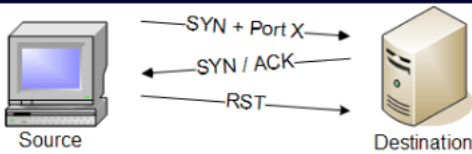|	
Display Run-Time Help	?
Increase / Decrease Verbosity	v / V
Increase / Decrease Debugging	d / D
Increase / Decrease Packet Tracing	p / P
Any Other Key	Print Status

LOGGING OPTIONS

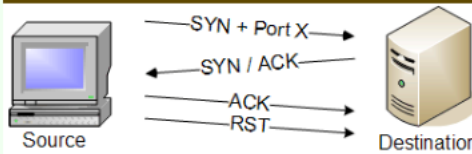|	
Normal Format	-oN <logfilename>
XML Format	-oX <logfilename>
Grepable Format	-oG <logfilename>
All Formats	-oA <basefilename>
Script Kiddie Format	-oS <logfilename>
Resume Scan	--resume <logfilename>
Append Output	--append-output

MISCELLANEOUS OPTIONS

Quick Reference Screen	--help, -h
Nmap Version	--version, -V
Data Directory	--datadir <directory_name>
Quash Argument Vector	-q
Define Custom Scan Flags	--scanflags <flagval>
(Uriel) Maimon Scan	-sM
IPv6 Support	-6
Send Bad TCP or UDP Checksum	--badsum

Professor Messer's Quick Reference Guide to
NMAP
Contributed By:
shravansofts2011@gmail.com

Identifying Open Ports with Nmap

TCP SYN SCAN (-sS)

SYN + Port X →
← SYN / ACK
RST →

Source — Destination

TCP connect() SCAN (-sT)

SYN + Port X →
← SYN / ACK
ACK →
RST →

Source — Destination

TCP FIN SCAN (-sF)

FIN + Port X →

Source — Destination

TCP XMAS TREE SCAN (-sX)

FIN, URG, PuSH + Port X →

Source — Destination

TCP NULL SCAN (-sN)

00000000 + Port X →

Source — Destination

TCP PING SCAN (-sP)

ICMP Echo Request →
← ICMP Echo Reply

Source — Destination
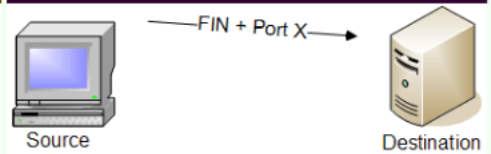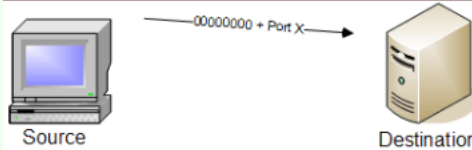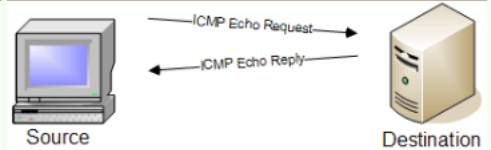
VERSION DETECTION SCAN (-sV)

Version scan identifies open ports with a TCP SYN scan...

SYN + Port X →
← SYN / ACK
RST →

Source — Destination
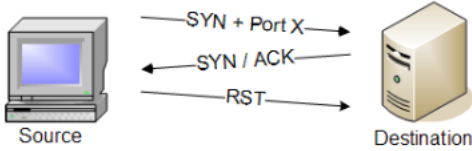
...and then queries the port with a customized signature.

HTTP GET →
← HTTP Data
ACK →
← HTTP Data
ACK / FIN →
← ACK

Source — Destination

UDP SCAN (-sU)

UDP + Port X →
← UDP + Port X Data

Source — Destination

IP PROTOCOL SCAN (-sO)

IP Protocol 0xXX →
← RST

Source — Destination

TCP ACK SCAN (-sA)

TCP ACK + Port X →
← RST

Source — Destination

TCP WINDOW SCAN (-sW)

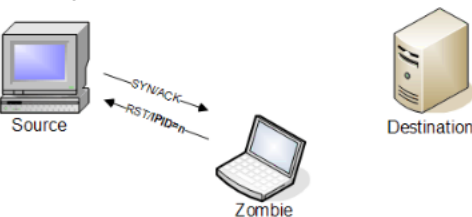TCP ACK + Port X →
← RST + WIN=NON-ZERO
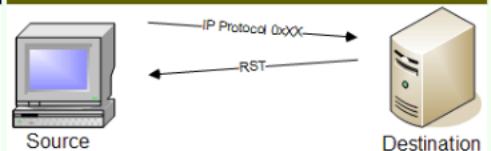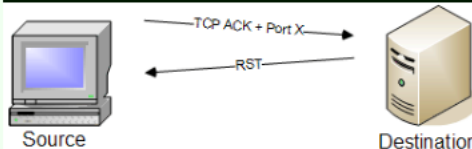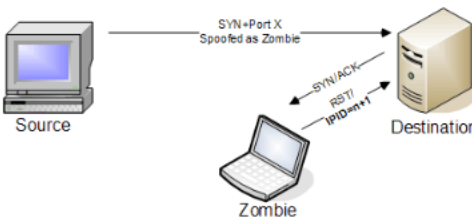
Source — Destination
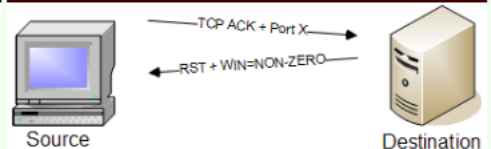
### IDLESCAN (-sI <zombie host:[probeport]>)

Step 1: Nmap sends a SYN/ACK to the zombie workstation to induce a RST in return. This RST frame contains the initial IPID that nmap will remember for later.

SYN/ACK →
← RST/IPID=n

Source — Zombie

Step 2: Nmap sends a SYN frame to the destination address, but nmap spoofs the IP address to make it seem as if the SYN frame was sent from the zombie workstation.

SYN+Port X
Spoofed as Zombie →

SYN/ACK
RST/
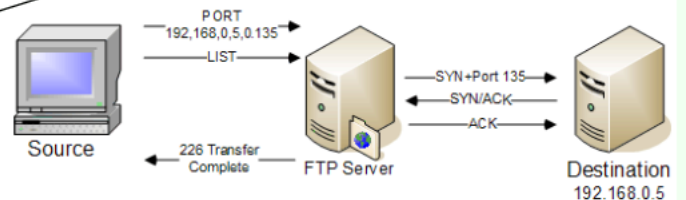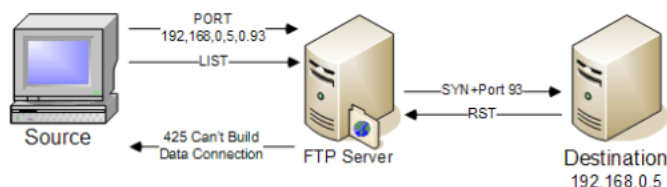IPID=n+1

Source — Destination — Zombie

Step 3: Nmap repeats the original SYN/ACK probe of the zombie station. If the IPID has incremented, then the port that was spoofed in the original SYN frame is open on the destination device.

SYN/ACK →
← RST/IPID=n+2

Source — Zombie — Destination
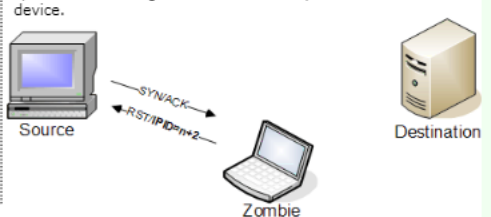
FTP BOUNCE ATTACK (-b <ftp_relay_host>)

A closed port will result with the FTP server informing the source station that the FTP server can't build the connection.

PORT
192,168,0,5,0,93 →
LIST →
← 425 Can't Build Data Connection

Source — FTP Server

SYN+Port 93 →
← RST

FTP Server — Destination 192.168.0.5

PORT
192,168,0,5,0,135 →
LIST →
← 226 Transfer Complete

Source — FTP Server

SYN+Port 135 →
← SYN/ACK
ACK →

FTP Server — Destination 192.168.0.5

An open port completes the transfer over the specified connection.

FATMA GÖKSU
ÇALIKOGLU