Nmap

Task 1: Used Orcale Virtual Box to run Kali Linux OS

Task 2: Learned every computer has a max of 65,535 ports. Ports are networking constructs used to direct traffic to the right application on a server.

Task 3: Nmap is a pentesting tool ran from the terminal. Switches, or command arguments tell a program to do different things. For example,

-sS is the first switch listed in the help menu for a Syn Scan

-sU for a UDP scan

-O to detect which Operating System the target it running on

-sV detects the version of the services running on the target

-v to increase the verbrosity when you need more information that the default output provided

-vv verbrosity level two

-oA Allows toe save nmap results in three major formats

(To reduce network traffic/ detection, should only be ran once)

-oN save nmap results in “normal” format

-oG results saved in a “grepable” format

-A enables “aggressive” mode:

Activates service detection,

operating system detection,

a traceroute and common script scanning

-T5 sets the timing template to Level 5.

There are five levels of timing template offered by Nmap.

Used to increase scan speeds. (Higher speeds are noisier, and can have errors)

-p 80 Tells Nmap to only scan port 80

(Can choose which port to scan –p)

-p 1000-1500 tells namp to scan ports 1000-1500

-p- tells Nmap to scan ***All*** ports

--script to activate a script from the Nmap scripting library

--script=vuln activates all scripts in the “vuln” category

Task 4

Task 5

Task 6

Task 7

Task 8

Task 9

Task 10

Nmap Scripting Engine (NSE):

NSE Scripts are written in the Lua programming language.

Can be used to scan for vulnerabilities, to automating exploits for them.

NSE is particularly useful for reconnaissance w/ an extensive script library.

Task 11

--script=<script-name> to run a specific script.

Multiple scripts can be run simultaneously by separating them by comma.

--script-args scripts that require arguments

Nmap –script-help <script-name> Nmap scrips built-in help menus.

Task 12

By Default, Nmap stores its scripts on Linux at: **/usr/share/nmap/scripts**

Can use **grep** command, or **ls** command

( **grep “ftp” /usr/share/nmap/scripts/script.db** )

( **ls -l /usr/share/nmap/scripts/\*ftp\*** )

\* asterisks on either side of search term is used for categories of scripts.

Task 13

Bypassing Firewalls w/ -Pn

-Pn

tells Nmap to not bother pinging the host before scanning it, treats the target host as being alive, effectively bypassing the ICMP block.

Nmap switches considered useful for Firewall evasion:

-f fragments packets, makes it less likely the packets will be detected by a firewall or IDS.

--mtu <number> Accepts a maximum transmission unit size, multiples of 8, to use for the packets sent

--scan-delay <time>ms

adds delay between packets sent,

Useful in evading any time-based firewall/IDS triggers.

--badsum generates invalid checksum for packets.

can be used to determine the presence of a firewall/IDS

ICMP a frequently relied upon protocol that is often blocked.

Requires the use of the –Pn switch.

--data-length appends an arbitrary length of random data to end of packets.

Task 14

Scanned Target Machine: Does not respond to ICMP (ping) requests.

Scanned w/ Xmas scan on first 999 ports of target IP – 999 ports open or filtered

Task 15

Conclusion: Learned using nmap docs is best at a point reference.