CS437 LAB 1
Report

Uğur Öztunç
28176

Nmap queries used on target hosts:

1. *nmap -p0- -v -sV -sC -traceroute -T4 [TARGET]:* In this scanning query, I used '-p0-' flag to scan all possible ports, to identify all open ports and services running on target hosts, including their versions and potential vulnerabilities. The '-v' flag is for verbose output for more detailed understanding. '-sV' enables service and version detection and '-sC' allows script scanning to provide additional insights into the services. I also used '-traceroute' flag to see the network path from my remote server to target hosts. Lastly, I added '-T4' flag to specify the timing template for scans. Since that I am scanning safe hosts for testing purposes, there is no need to be stealthy so I performed slightly aggressive scans to reduce time.

2. *nmap -O -v [TARGET]:* This additional query is for detecting the target OS type. Simply, I used '-O' flag, which enables OS detection, for making guesses about targets' OS types. And again '-v' flag is used for more detailed scanning results.

Online sources used to make query decisions:

1. *https://linux.die.net/man/1/nmap*
2. *https://nmap.org/*
3. *https://www.digitalocean.com/community/tutorials/nmap-switches-scan-types*

Results for *64.176.188.181*:

nmap -p0- -v -sV -sC -traceroute -T4 64.176.188.181

By looking results, I see 65,536 total ports have been scanned and 65,524 ports of them is filtered, which means we cannot have a clear information about those ports. About the remaining 12 ports, I see following:

- Port 22 (tcp) is open and listening for ssh with the version "OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)". I conclude that the host is running Ubuntu-based system and might imply that system is needed to remotely controlled.
- Port 66 (tcp) is open with service 'sqlnet?'. As I searched on internet, the question marks indicates that the when Nmap is not be able to identify the service clearly by host responses, it identifies the service by checking a list of known port-service pairs (https://svn.nmap.org/nmap/nmap-services). When I take a glance at the fingerprint-strings part, as far as I can interpret, I see that the service is related with a webserver activity. There are HTTP responses, server references as "Werkzeug and Python", content types (text/html), and HTTP request methods allowed (GET, HEAD, OPTIONS).
- Port 67 (tcp) is closed, which indicates that DHCPS service is not active for incoming connections.
- Port 89 (tcp) is opened with an HTTP service. I see that the service accepts GET and HEAD methods, and has a header of 'nginx/1.25.2'. This indicates target host is running a nginx web server with version 1.25.2.
- Port 112, 245, 555, 898, 1002, and 1111 are closed but I can see the service names.
- Port 9200 (tcp) is open and running an HTTP-related service but it is unclear. I see that there are HTTP responses with a name 'Green goblin' but I cannot find out what actually it is.

- Port 9300 (tcp) is open and running Apache HTTP server. From the results of this port, I can only say that the server is accepting GET, HEAD, and POST methods.

After the port results, nmap shows the fingerprints of 2 unrecognized services for user to submit details to nmap.org if known. Finally, I see the traceroute result which shows that my remote server reached target host after 14 hops.

nmap -O -v 64.176.188.181

Based on aggressive OS guesses, host is very likely running a Linux-based OS, though the exact match of OS and its version is not certain. Also there is uptime guess in output, which suggests that host has been online since 13 Sep 2023.

Results for *45.63.99.102*:

nmap -p0- -v -sV -sC -traceroute -T4 45.63.99.102

All 65,536 possible ports have been scanned. I see that 65,530 ports are closed and not shown in output, 2 is filtered and remaning 4 port is open. Here are the information about open and filtered ports:

- Port 22 (tcp) is open and is running SSH service with the version "OpenSSH 8.2p1 Ubuntu 4ubuntu0.2." This indicates that the host is running an Ubuntu-based system and it is likely that the host is needed to be controlled remotely just like previous target host.
- Port 25 (tcp) is running SMTP service but it is filtered, which blocks my remote server to gain further information about SMTP service running on target host.
- Port 80 (tcp) is open and running an HTTP service, specifically, the Nginx web server version 1.18.0 on Ubuntu. The HTTP response for this port contains a reference to a page named “remediation.sabanciuniv.edu.”, and adittionaly it accepts GET, HEAD, POST, and OPTIONS methods.
- Port 443 (tcp) is open and is serving an SSL/HTTP service, and also running Nginx 1.18.0. As I searched on internet (https://nmap.org/nsedoc/scripts/ssl-cert.html) to further investigate the information from this port, I found out that the SSL certificate information is provided, and it is issued by Let's Encrypt. This service also supports same methods as port 80 does.
- Port 5001 (tcp) is open and running another SSL/HTTP service with Nginx 1.18.0. It seems that this service is for returning a "404 Not Found" page.
- Port 11211 (tcp) is filtered, indicating that the “memcache” service is not accessible from my remote server.

By looking the results I concluded that the host seems to host a website. To be sure, I entered the Ip address to my browser and it redirected me to “https://remediation.sabanciuniv.edu/”. In addition, without even performing OS detection scanning, I found out that host is likely running a Linux-based operating system. Lastly, traceroute result shows that with 11 hops, my remote server reachs the host.

nmap -O -v 45.63.99.102

Unlike the OS detection operations on previous host, this time I obtained more clear and detailed results. Device type is stated as “general purpose”, which means device is not specialized for a specific purpose, such as router or game console, and be able to perform variety of functions (https://nmap.org/book/osdetect-device-types.html). The host is running a Linux-based operating system with a kernel version between 4.15 to 5.6. Also, I see that the host is running since 19 Oct 2023.