CS473 - Homework # 1 Spring 2019
Instructors: Mobin Javed and Fareed Zaffar

Muhammad Haseeb 20100192

Question 1: Nmap and Wireshark

(1) Port Scanning using Nmap

1. What is the full command you used to run the port scan (including arguments)?
sudo nmap -vv -A -p- -sS -T4 scanme.nmap.org

2. What is the IP address of scanme.nmap.org?

45.33.32.156

3. What operating system is the target server running?

OS: Linux; Device: security-misc; CPE: cpe:/o:linux:linux_kernel

4. What ports are open on the target server? What applications are running on those ports? (For this part, you only need to report the service name printed by Nmap.)

22/tcp ssh
80/tcp http
2000/tcp tcpwrapped (not actually a service)
5060/tcp tcpwrapped (not actually a service)
8008/tcp http
9929/tcp nping-echo
31337/tcp tcpwrapped (not actually a service)

5. The target machine is running an SSH server. What SSH software and version is being used?

OpenSSH 6.6.1p1 Ubuntu

6. The target machine is also running a web server. What web server software and version are being used? What ports does it run on?

Port 80: Apache httpd 2.4.7 (Ubuntu)
Port 8008: Fortinet FortiGuard block page

(2) Wireshark Packet Sniffing

1. What does it mean for a port on scanme.nmap.org to be “closed”? More specifically, what is the TCP packet type, if any, the server gives in response to a SYN packet sent to port that is “closed”?

A closed port means there is no service listening on that specific port. TCP [RST, ACK] packet is given by a closed port in response to a SYN packet.

2. What does it mean for a port on scanme.nmap.org to be “filtered”? More specifically, what is the TCP packet type, if any, the server gives in response to a SYN packet sent to port that is “filtered”?

A filtered port means that any type of packet filterer/firewall is in use on that specific port. Typically, an ICMP type 3 (Unreachable error) packet or nothing is given by a filtered port in response to a SYN packet.

3. In addition to performing an HTTP GET request to the web server, what other HTTP request types does Nmap send?

POST, PROPFIND and OPTIONS (help taken from a friend as I could not initially find these).

Question 2: Port Scanner

File attached. {optimized for linux with *semaphores*, running it on Windows won’t make it run faster.}
In global variables, you can tweek total_ports variable. (Set it to 10000 and it will take minute and give you just one less than all open ports)

Question 3: Reconnaissance

1. Run Nmap on the VM image and list all the open ports and services. Explain any three services from the list. Do you see any "unknown" services in the scan result? Why is Nmap unable to determine which service this is (in the case of unknown)?

Port, Service

21, FTP
22, SSH
23, telnet
25, SMTP
53, DNS
80, HTTP
111, rpcbind
139, netbios-ssn
445, netbios-ssn
512, exec
513, login
514, tcpwrapped
1099, java-rmi
1524, bindshell
2049, nfs
2121, FTP
3306, mySQL
5432, postgresql
5900, vnc
6000, x11
6667, irc
8009, ajp13
8180, HTTP

Service FTP on port 21: FTP is an acronym for File Transfer Protocol. As the name suggests, FTP is used to transfer files between computers on a network. You can use FTP to exchange files between computer accounts, transfer files between an account and a desktop computer, or access online software archives. Many FTP sites are heavily used and require several attempts before connecting.

Service SSH on port 22: SSH service has a client/server architecture. An SSH *server* program, typically installed and run by a system administrator, accepts or rejects incoming connections to its host computer. Users then run SSH *client* programs, typically on other computers, to make requests of the SSH server, such as "Please log me in," "Please send me a file," or "Please execute this command." All communications between clients and servers are securely encrypted and protected from modification.

Service telnet on port 23: Telnet is a protocol that enables you to attach to remote computers (called hosts) over a TCP/IP network, more like SSH but far less secure. It is installed as a service on servers for encrypting communication just like SSH. Once a telnet consumer establishes a connection to the remote host, your client becomes a virtual terminal, permitting you to speak with the remote host from your laptop. In most cases, you'll need to log into the remote host, which requires that you have an account on that system. Often, you'll be able to log in as guest or public while not having an account.

Yes, there are a bunch of unknown services reported by nmap. Most of the times NMAP reports a service as unknown if the port is closed or not responding. Also, Nmap port scan usually refer the known ports listed in /usr/share/nmap/nmap-services and /etc/services file. When it finds a port, which is not listed in these files, the service is labeled as unknown in port scan output.

2. Run Nikto on the aforementioned server and list all the vulnerabilities that the tool outputs (just the name or the code).

- **Anit-clickjacking header not present**
- **X-XSS-Protection header not defined**
- **X-content-Type-Options header not set**
- **Apache outdated**
- **Uncommon header found**
- **Apache mod_negotiation enabled with MultiViews**
- **OSVDB-877**
- **OSVDB-3268**
- **OSVDB-48**
- **OSVDB-12184**
- **OSVDB-3092**
- **OSVDB-3233**
- **OSVDB-3268**

3. As mentioned above, not all reported items will be vulnerabilities. Some will be warnings, and some might be just pieces of information that are harmless. Hence, create categories and try to organize the information into these categories. You need to have a very good understanding of what is a problem and what is not. Find at least one vulnerability that is a false positive (not really a vulnerability) and three actual vulnerabilities.

Vulnerabilities:

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php

+ OSVDB-3268: /doc/: Directory indexing found.

+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.

+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

Warnings:

+ Uncommon header 'tcn' found, with contents: list

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

Information:

+ Server: Apache/2.2.8 (Ubuntu) DAV/2

+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10

False Positive (not actually a vulnerability):

+ Web Server returns a valid response with junk HTTP methods.

+ Uncommon header 'tcn' found, with contents: list

That's nothing, the header is just rarely used but it is of no issue.

Actual Vulnerabilities:

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

4. Distinguish a web-specific vulnerability from a host or OS-based vulnerability. Give one example of each from your scan and then explain both.

Host-based vulnerability:

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

It is a host-based vulnerability. It shows that the host has not updated the said software and it can potentially help attackers to exploit this outdated software (of course, there must be a reason that the new version of the software is released).

Web-based vulnerability:

+ The anti-clickjacking X-Frame-Options header is not present.

It is a web-based vulnerability. It shows that the content of this site can be placed in a x-frame which in turn has many vulnerabilities as it opens a lot of doors for attackers to attack through. One can do phishing attacks easily by this. As the name implies, clickjacking is a main threat if this header is not used by the site.

5. Lastly, give an explanation on how we can solve at least three of the identified vulnerabilities. The goal is to determine how well you understand the output of a security tool and how you would approach the problems reported, to solve them.

First 3 vulnerabilities (in red color above) can be simply eliminated by the host by including the said headers in packets. And the fourth vulnerability (also in red color) can be solved by updating the software (Apache). This suffice the requirements of answer, but let me solve one more interesting vulnerability, **+ OSVDB-3268: /doc/: Directory indexing found.**

The best way for doing this is to disable it with webserver apache2. For example, in Ubuntu 14.X - open /etc/apache2/apache2.conf change from

```
<Directory /var/www/>
Options Indexes FollowSymLinks
    AllowOverride None
Require all granted
</Directory>
```

to

```
<Directory /var/www/>
    Options FollowSymLinks
     AllowOverride None
   Require all granted
</Directory>
```

This will disable directory listing from all folder that apache2 serves.