**Lab 05A­­**

Description: This lab will demonstrate the installation and use of nmap to improve security in Linux.

Perform the following activities on the specified virtual machines.  Record your commands and answer any questions in the lab activities.

Part 1) Ubuntu 18.04.1 Server  
Part 2) Fedora 28-1.1 Server

PROCEDURE: Use the book and the appropriate man pages to form commands to complete the following tasks.  (Tip: You will need to work with root privileges to perform these commands.)

RESOURCES: [Installation Security Resources](https://canvas.highline.edu/courses/1862999/pages/installation-security-resources)

Part 1)

**On Ubuntu Server 18.04.1:**

Install nmap  
Run nmap using the command **nmap -vv -A 127.0.0.1**

Running the command with the -A option will perform the following scans:

* OS Detection
* Version Detection
* Default Scripts
* Traceroute

The -vv option will increase the verbosity level.

Explain the meaning of the output you receive, and   
describe how you could correct any vulnerabilities found:

Services running: FTP

Port: 21

Version: vsftpd 3.0.3

A screenshot of a cell phone

Description automatically generated

Figure 1 FTP - Port 21

Vulnerabilities:

* No vulnerabilities or public exploits were discovered for vsftpd 3.0.3
* Disable anonymous user login to prevent file transfers.
* If directory traversal exists, it is possible to perform remote code execution to get a shell on the remote system.

Services running: SSH

Port: 22

Version: OpenSSH 7.6p1

A screenshot of a cell phone

Description automatically generated

Figure 2 SSH - Port 22

Vulnerabilities:

* Use complex passwords to prevent brute-force attacks
* Disable passwords (as an authentication method) and use SSL/TLS certificates instead or PKI.
* Change default usernames (admin, root) and passwords
* Disable root login

A screenshot of a cell phone

Description automatically generated

Figure 3 Results of nmap (ssh\*) script scan

Services running: HTTP/HTTPS

Ports: 80/443

Version: Apache httpd 2.4.29

A screenshot of a cell phone

Description automatically generated

Figure 4 HTTP/HTTPS - Ports 80/443

Vulnerabilities:

* Check supported HTTP Methods:
  + The PUT method allows you to write files to the server.
* Check for information leakage:
  + Exposed IP’s

A screenshot of a cell phone

Description automatically generated

Service running: MySQL

Port: 3306

Version: MySQL 5.7.29

A screenshot of a cell phone

Description automatically generated

Figure 5 MySQL - Port 3306

Vulnerabilities:

* The version of MySQL running on the remote host with MySQL 5.7.x < 5.7.29 has multiple vulnerabilities.

<https://www.tenable.com/plugins/nessus/132957>

Part 2)

**On Fedora Server 28.1-1:**

Install nmap  
Run nmap using the command **nmap -vv -A 127.0.0.1**

Running the command with the -A option will perform the following scans:

* OS Detection
* Version Detection
* Default Scripts
* Traceroute

The -vv option will increase the verbosity level.

**Explain the meaning of the output you receive, and   
describe how you could correct any vulnerabilities found:**

Services running: FTP

Port: 21

Version: vsftpd 3.0.3

A close up of a piece of paper

Description automatically generated

Figure 1 FTP - Port 21

Vulnerabilities:

* No vulnerabilities or public exploits were discovered for vsftpd 3.0.3
* Disable anonymous user login to prevent file transfers.
* If directory traversal exists, it is possible to perform remote code execution to get a shell on the remote system.

Services running: SSH

Port: 22

Version: OpenSSH 7.6p1

A screenshot of a cell phone

Description automatically generated

Figure 6 SSH - Port 22

Vulnerabilities:

* Use complex passwords to prevent brute-force attacks
* Disable passwords (as an authentication method) and use SSL/TLS certificates instead or PKI.
* Change default usernames (admin, root) and passwords
* Disable root login

A screenshot of a cell phone

Description automatically generated

Figure 7 Results of nmap (ssh\*) script scan

Services running: HTTP/HTTPS

Ports: 80/443

Version: Apache httpd 2.4.29

A screenshot of a cell phone

Description automatically generated

Figure 8 HTTP/HTTPS - Ports 80/443

A screenshot of a cell phone

Description automatically generated

Vulnerabilities:

* Check supported HTTP Methods:
  + The PUT method allows you to write files to the server.

Service running: HTTPS

Port: 9090

Location: <https://192.168.166.164:9090/system>

A screenshot of a cell phone

Description automatically generated

Figure Admin Login Page - Port 9090

A screenshot of a computer screen

Description automatically generated

Figure Admin Login Page – Port 9090

Vulnerabilities:

Admin pages:

* Exposed Admin pages will add an additional attack vector.
* This application was found on port 9090
* It is possible to brute force the admin page using a fuzzer such as burpsuite or wfuzz.

Service running: MySQL

Port: 3306

Version: MySQL 5.7.29



Figure 11 MySQL - Port 3306

Vulnerabilities:

I wasn’t able to find the version no. so no vulnerabilities were found.