TASK-1:

1. Showing systems that are alive

A screenshot of a computer

Description automatically generated

1. Using the **nbtscan** tool on each of the alive IP Address, confirm the correct IP Address of your Metasploitable2 VM.

Correct IP Address for Metasploitable is **192.168.56.102**

A screenshot of a computer

Description automatically generated

1. Create fpingOutput.txt file to save data.

A screenshot of a computer program

Description automatically generated

1. Text file of Alive Address call as fpingOutput.txt

A screenshot of a computer

Description automatically generated

Data of fpingOutput.txt

1)192.168.56.1

2) 192.168.56.100

3) 192.168.56.102

TASK-2:

1. use NMAP (again from within your Kali Linux VM) and perform a single NMAP scan with the following options: TCP SYN, OS detection, version detection, and verbose output.

A screen shot of a computer screen

Description automatically generated

A computer screen shot of text

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of white text

Description automatically generated

A computer screen shot of a computer error

Description automatically generated

1. highlighting the section that you have selected to investigate for vulnerabilities. Research this version of the service.

A screen shot of a computer

Description automatically generated

* I selected proFTPD 1.3.1 for explaining.

1. When proFTPD 1.3.1 was it released?

Ans. ProFTPD version 1.3.1 was released on April 6, 2012.

1. Is it the newest version? If not, when was it updated?

Ans. No, that is not the most recent version. The latest version of proFTPD 1.3.1 was released on September 26, 2019.

1. Is there a known vulnerability for this service?

Ans. Yes, proFTPD 1.3.1 has a known vulnerability. The bug is a mod\_copy command execution weakness that allows remote attackers to execute arbitrary commands with the rights of the proFTPD daemon's user. This vulnerability was discovered in November 2010 and has subsequently been fixed in subsequent versions of proFTPD. To circumvent this issue, users should upgrade to a newer version of proFTPD. Long commands from an FTP client are interpreted as multiple commands by ProFTPD 1.3. 1, allowing remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.

An attacker can exploit a buffer overflow vulnerability in the ProFTPD 1.3.1 version to execute arbitrary code on the victim machine. This may be accomplished by sending a specially designed request to the FTP server, which can cause the server to crash or allow the attacker to obtain system access.

An attacker can exploit this vulnerability and obtain system access by sending a malicious request to the FTP server, leading it to execute arbitrary code. This code can then be used to acquire system access, elevate privileges, and carry out more attacks. It is crucial to note that this vulnerability has been addressed in newer versions of ProFTPD, thus upgrading is advised.

References:

[1] *ProFTPD*. The ProFTPD Project: Home. (n.d.). http://www.proftpd.org/

[2] *Proftpd Proftpd version 1.3.1 : Security vulnerabilities, CVES*. Proftpd Proftpd version 1.3.1 : Security vulnerabilities, CVEs. (n.d.). https://www.cvedetails.com/vulnerability-list/vendor\_id-9520/product\_id-16873/version\_id-435968/Proftpd-Proftpd-1.3.1.html

[3] *Release versioning*. ProFTPD. (n.d.). http://www.proftpd.org/docs/howto/Versioning.html

[4] *Search results*. CVE. (n.d.). https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=proftpd#:~:text=ProFTPD%20Server%201.3.,mod\_sql\_mysql%20and%20(2)%20mod\_sql\_postgres.&text=SQL%20injection%20vulnerability%20in%20ProFTPD,1%20through%201.3.

[5] *Proftpd+proftpd+1.3.1 vulnerabilities and exploits*. Vulmon. (n.d.). https://vulmon.com/searchpage?q=proftpd%2Bproftpd%2B1.3.1