TASK – 1

1. Provide a screenshot(s) of your fping sweep that would show: all alive systems, generate a target list from a provided IP network and showing the final stats upon exit. Only provide the screenshots showing the command used and the final stats. No need to provide screenshots of all of the IP Addresses. Confirm the IP Address of your Metasploitable 2 VM using nbtscan for each of the alive systems. Be sure to include the actual commands and options that were used.

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Provide screenshots of your NMAP scan discovering a remote service using the options for TCP SYN, OS detection, version detection and verbose output . Be sure to include the actual command that was used.

A screen shot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer program

Description automatically generated



A screenshot of a computer screen

Description automatically generated

A screen shot of a computer program

Description automatically generated

1. From the output of the NMAP, select an open port / service running on that port. Provide a brief description in your own words of what that remote service is and what it does

A screen shot of a computer

Description automatically generated



1. I selected proFTPD 1.3.1 for explaining.
2. ProFTPD version 1.3.1 was released on April 6, 2012.
3. No, that is not the most recent version. The latest version of proFTPD 1.3.1 was released on September 26, 2019.
4. 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.

TASK – 2

1. Provide a screenshot of the Target IP address and type of cracking / tool you are attempting to crack

A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

1. Run your choice of password cracker from either Medusa, John or Hydra. Use the provided text files to check against a list of users and passwords. If you test one service and find no results, try testing another – continue to try until you find a success. Provide the output of all successes and/or failures in your report.

A screen shot of a computer code

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screen shot of a computer code

Description automatically generated

1. After you find a success, use the information you found (i.e. username and password) to access the system through the service you exploited. Include a description of what you did and a screenshot showing the success in your report including the username and password used.

A screen shot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

Here, I used Ncrack module to crack password. I used “ ncrack -U users.txt -P passwords.txt ftp:// 192.168.56.102 “ to find username and password of the system. After completing the method it found username and password and shows message **1 service scanned in 72.88 seconds**.

After that I used ftp 192.168.56.102 to connect with Metasploitable 2, where I insert name and password to check successful login and it worked and it shows me message **230 Login successful**.

A screenshot of a computer screen

Description automatically generated

Q.1. how i could improve your password cracking results in about one or two paragraphs. Be sure to think about the previous steps and how they are used in the exploitation phase.

Ans-1. Consider the following ways to increase password cracking results:

1. Build extensive and diverse wordlists: It is critical to build comprehensive and diverse wordlists. Include typical passwords, permutations, data breach passwords, and industry-specific keywords. Consider developing bespoke wordlists depending on the target's profile, such as personal information or established trends. Update and expand your wordlists on a regular basis to accommodate new passwords and trends.
2. Investigate advanced password cracking techniques: To improve your chances of success, investigate advanced password cracking techniques. Passwords that follow specified patterns can be cracked using rule-based attacks such as permutations, capitalization rules, or appending/prepending letters. Furthermore, combining several cracking strategies, such as hybrid assaults that mix wordlists and brute-force approaches, may produce superior results.
3. Utilize password complexity requirements: Examine any accessible data about the target system's password complexity requirements. You can alter your cracking strategy if you know the minimum length, character kinds, or pattern constraints. Concentrate your efforts on cracking passwords that meet those criteria to increase your chances of success.
4. Optimize hardware resources: Cracking passwords may be a resource-intensive procedure. Increase the speed and efficiency of your cracking attempts by using high-performance technology such as GPUs or dedicated password cracking devices. If feasible, parallelize the cracking operation to take use of several CPU cores or distributed systems.Optimize hardware resources: Cracking passwords may be a resource-intensive procedure. Increase the speed and efficiency of your cracking attempts by using high-performance technology such as GPUs or dedicated password cracking devices. If feasible, parallelize the cracking operation to take use of several CPU cores or distributed systems.

Ans-2. Prior steps, such as network scanning, service discovery, and password cracking, are critical in the exploitation phase. Here's how these steps can help with the extraction process:

1. Network scanning: Network scanning aids in the identification of possible targets as well as the discovery of active systems and services inside a network. You can learn a lot about the network architecture, open ports, and operating services by executing a thorough network scan. This information is critical for detecting possible vulnerabilities and exploitation targets.
2. Service discovery: Once the active services on the target systems have been discovered, you may use service discovery techniques such as Nmap scans to acquire more information. This includes identifying the service's version and operating system, which can aid in determining specific vulnerabilities or weaknesses associated with those versions. During the exploitation phase, this information informs the selection of relevant exploits or attack paths.
3. Password cracking is the process of gaining unauthorized access to systems by exploiting weak or readily guessable passwords. You attempt to break passwords using programs such as John the Ripper or Hydra in order to obtain acceptable credentials for authentication. Successful password cracking gives you the credentials you need to exploit services that need authentication.
4. Exploitation: After gathering information via network scanning, service discovery, and password cracking, you may go on to the exploitation step. This entails gaining unauthorized access or control over the target systems by exploiting known vulnerabilities, poor settings, or gained credentials. Depending on the individual vulnerabilities and access permissions gained, exploiting might include a variety of tactics such as exploit execution, privilege escalation, lateral movement, or data exfiltration.

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>

[6] drd\_, & Linda, M. (2020b, October 8). *How to Brute-Force FTP Credentials & Get Server Access*. WonderHowTo. <https://null-byte.wonderhowto.com/how-to/brute-force-ftp-credentials-get-server-access-0208763/>

[7] *John the ripper password cracker*. Openwall. (n.d.). <https://www.openwall.com/john/>