Contents

Purpose 3

Scope 3

Summary of findings 3

Information Gathering

1. Passive Information Gathering 4
2. Active Information Gathering
3. Other Tools and Software

Attack Plan 9

Execution Report and Results

Appendix A 13

Appendix B 14

Purpose

The CEO of a small business has asked that system pen testing be done. Even though intranet systems have been set up by network administrators, servers may still contain sensitive data. On the other hand, this report provides thorough FTP server pen testing.

Scope

The disk which runs as FTP server requires few tools and software's to perform penetration testing. The IP address is additionally specified on the disk. The fact that the server uses FTP nonetheless limits this disk. Pen testing is done based on active and passive information gathering.

Summary of Findings

All the risks connected to the disk's possibilities are discussed in this report. There are vulnerabilities on the server, according to the metrics listed below. Metrics that include the high and low severity features indicate that the server has a 10% high severity.

Figure 3.1 - Severity of vulnerabilities using green bone

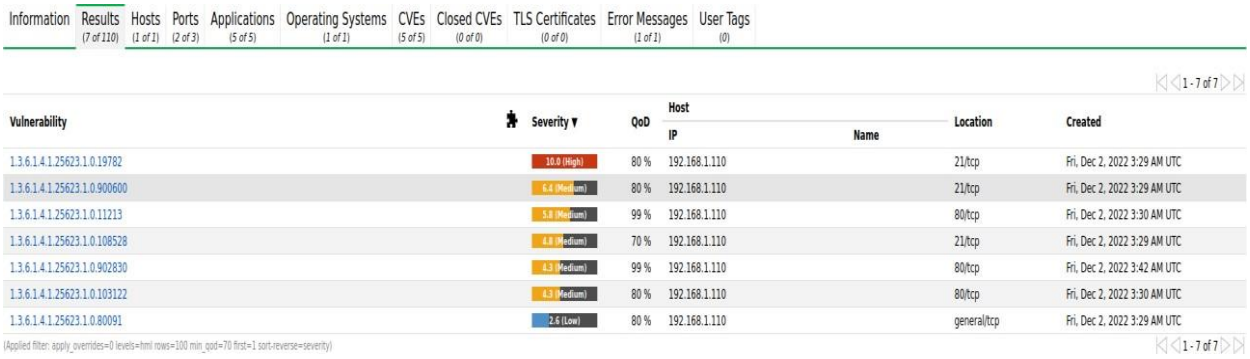
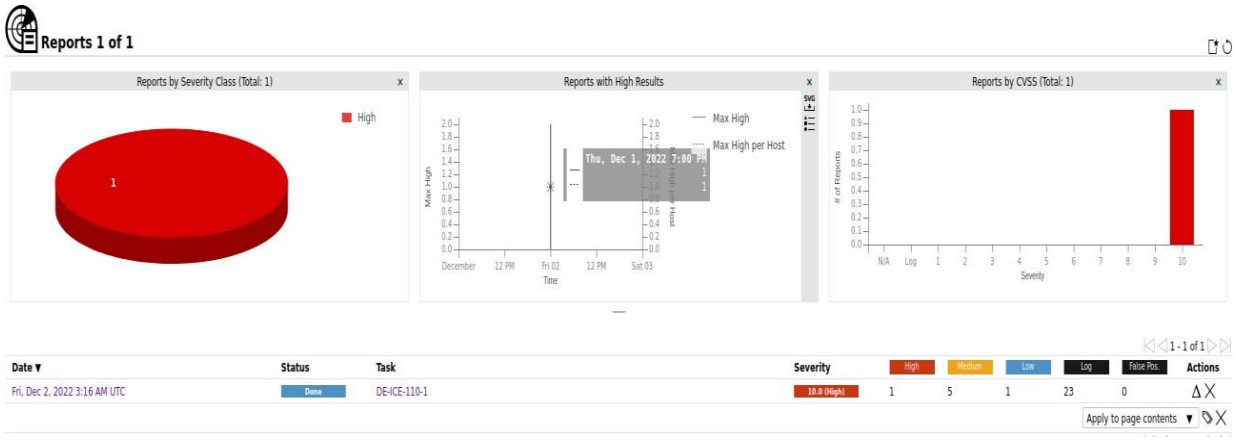


Figure 3.2 - Viewing the high severity vulnerability



The measurements also reveal that there are 5 moderately serious vulnerabilities, 1 low severity vulnerability, and 1 high severity vulnerability. Active recon actions like scanning, user enumeration, and server vulnerability analysis are carried out. are carried out depending on the severity to identify the systems and locate the sensitive data. Passive recon activities are carried out throughout the report, including the identification of IP addresses, external websites, technologies, content of interest, and vulnerabilities. Active recon Additionally, an attack plan is carried out to examine the sensitive data based on the information gathered.

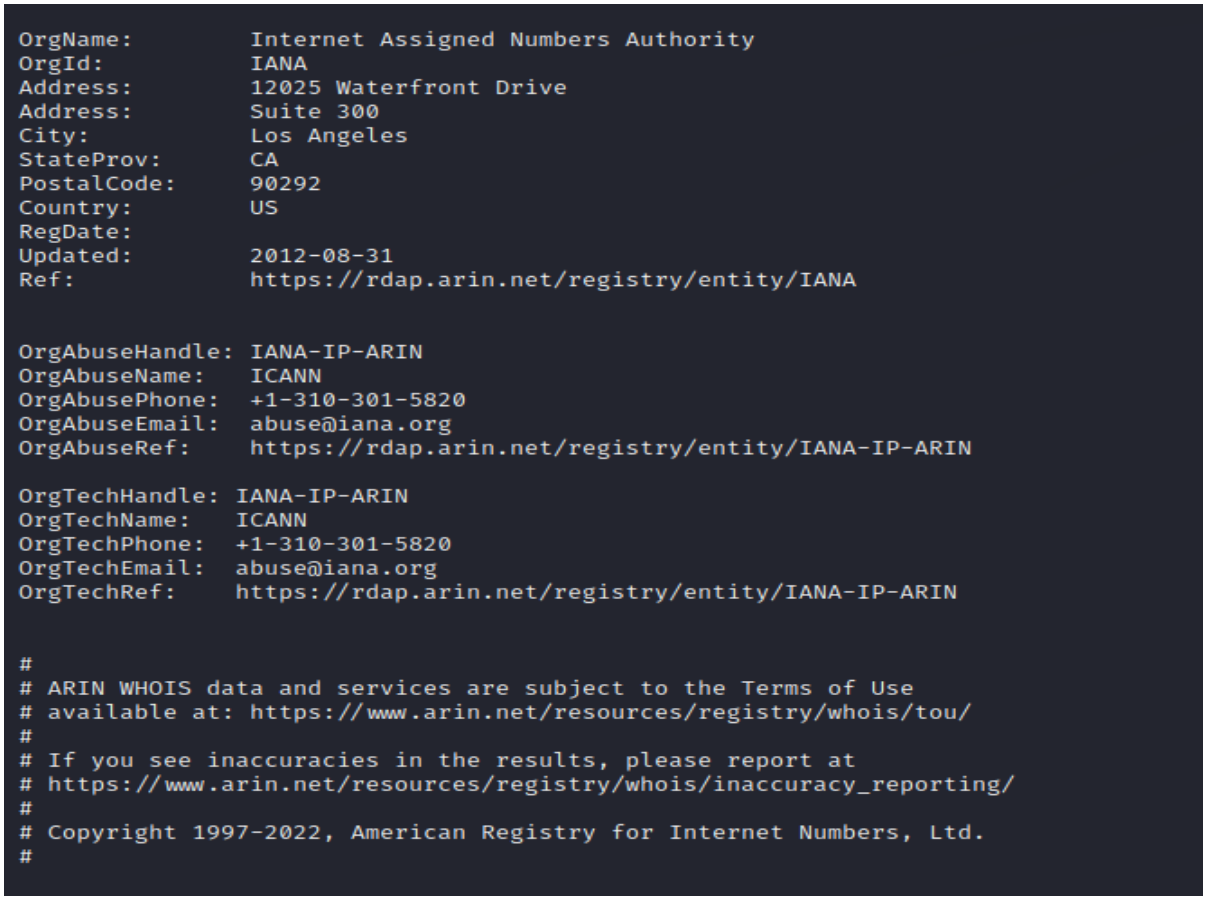
Information Gathering

- Passive Information Gathering
    1. Identifying IP address and sub-domains
    2. Identifying External and People
    3. Identifying Technologies

Identifying IP address and sub-domains

Even the disk is configured with the IP address, using “whois” gives all details of the as shown. We can see that server is available at Waterfront Drive in Los Angeles, URL link and with email as abuse@iana.org

Figure 4.1 - Server information using “whois”



```
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#
```

Identifying External and People

As the server has already been identified as an FTP server, some of its data may pose a risk of sensitive information being accessed. There are admin email addresses on the screen below that can access the file system with full privileges.

Figure 5.1 - Identifying the people through the FTP server

Identifying Technologies

Penetration testing can be applied using the OSINT framework in accordance with the necessary standards. When the IP address is provided below, the results from Shodan and Reverse DNS lookup are found. All ports and organizations that used can be seen using the Shodan report. There aren't any weaknesses under it, though. Likewise, the reverse DNS lookup, no entries are discovered.

Figure 5.2 - OSINT framework

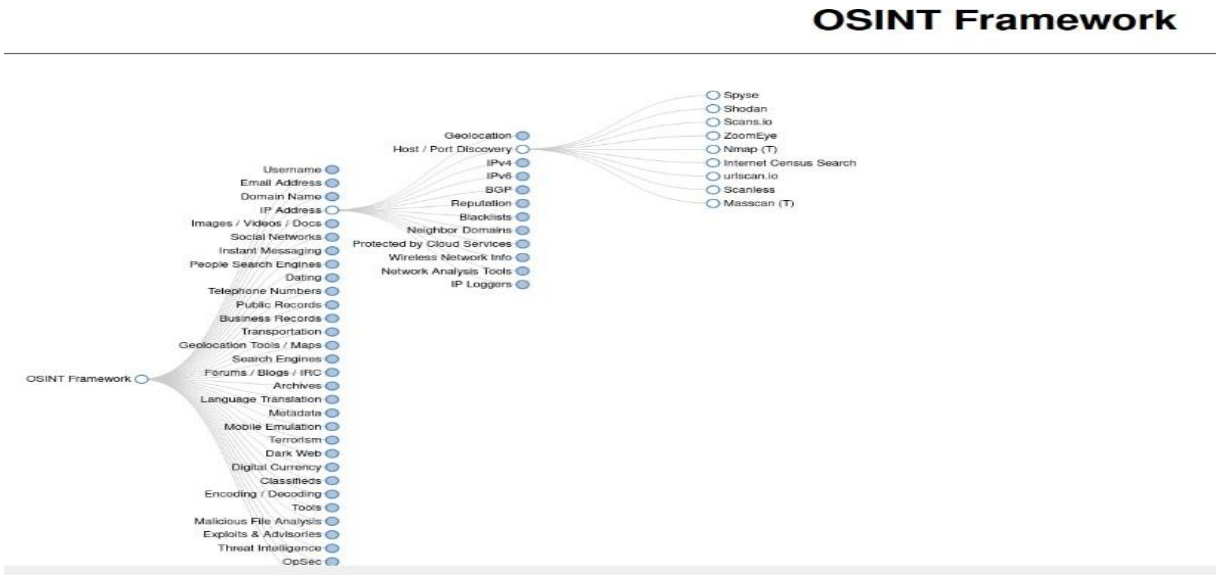


Figure 6.1 - Shodan Report

Figure 6.2 - Reverse DNS report

Conclusion:

After gathering the data through passive recon efforts, admin names are discovered to be risky and no vulnerabilities.

Active Information Gathering

Nmap is used to exploit the disk for active recon activities through ping scanning, TCP port scanning, version scanning, and OS identification. The MAC address identifies open ports as well as services and versions that are known using scanning techniques. Hackers can gather this data using enumeration techniques to exploit the disk. However, a firewall can identify and track down hackers.

Figure 7.1 - Ping scanning

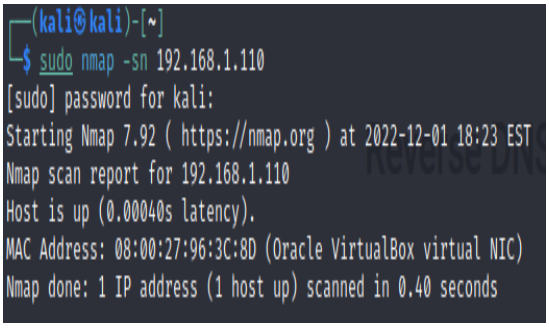


Figure 7.2 - Port Scanning

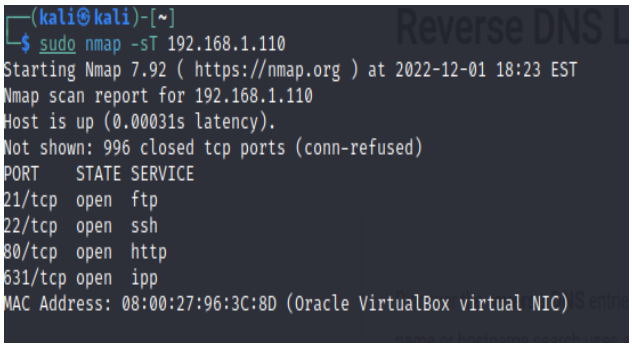


Figure 7.3 - OS Detection

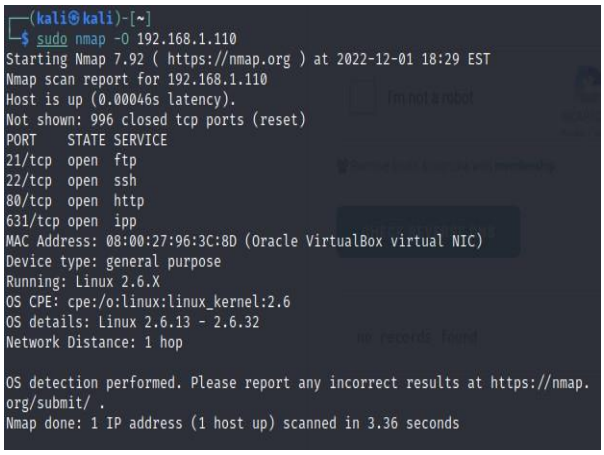
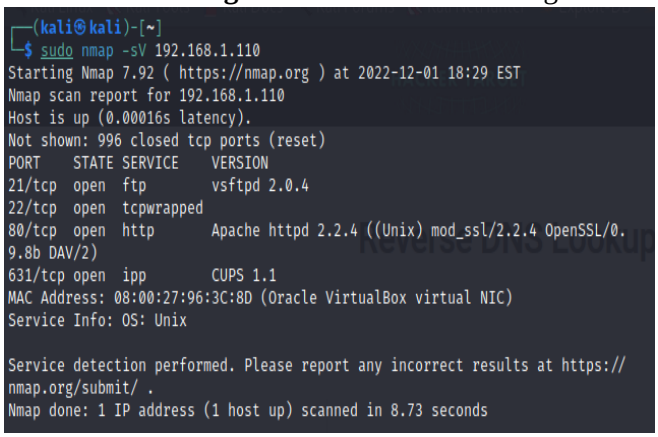


Figure 7.4 - Version Scanning



Conclusion:

Nmap is used to access the disk for active recon purposes using ping scanning, TCP port scanning, UDP port scanning, and OS identification. With this MAC address, services, open ports, and version information about the device are known. To take advantage of the disk, hackers can obtain this information by employing enumeration methods. A firewall, on the other hand, can recognize and locate hackers.

Other Tools and Software

To identify any vulnerabilities on the disk, Greenbone, one of the open-source vulnerability management tools, is installed. This software has produced a report that allows one to see the severity levels. According to reports, a high severity has been discovered that can affect the systems and aid in the identification of any vulnerabilities. As indicated in the report below, common vulnerabilities and exposures have a specific number and status that might indicate how much of an impact they may have on the systems. According to the vulnerability assessment, port 21 on the FTP server is where most vulnerabilities are found.

Figure 8.1 - Common and Vulnerability Exposures

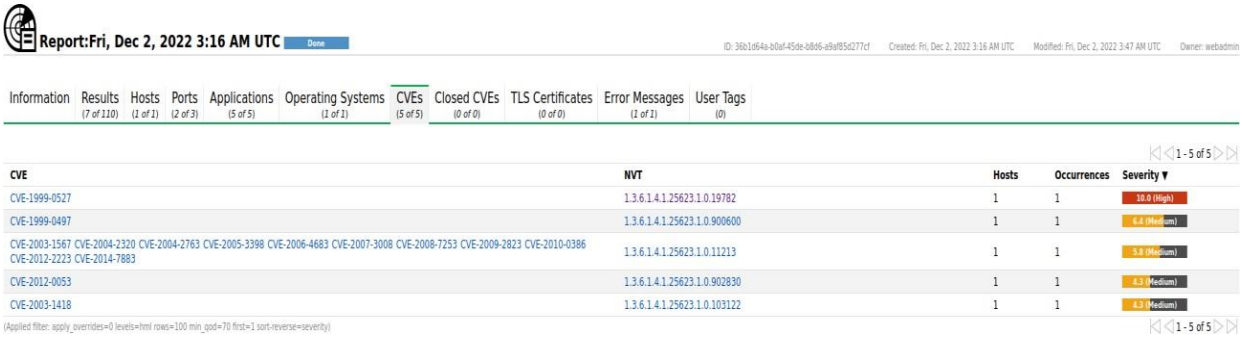
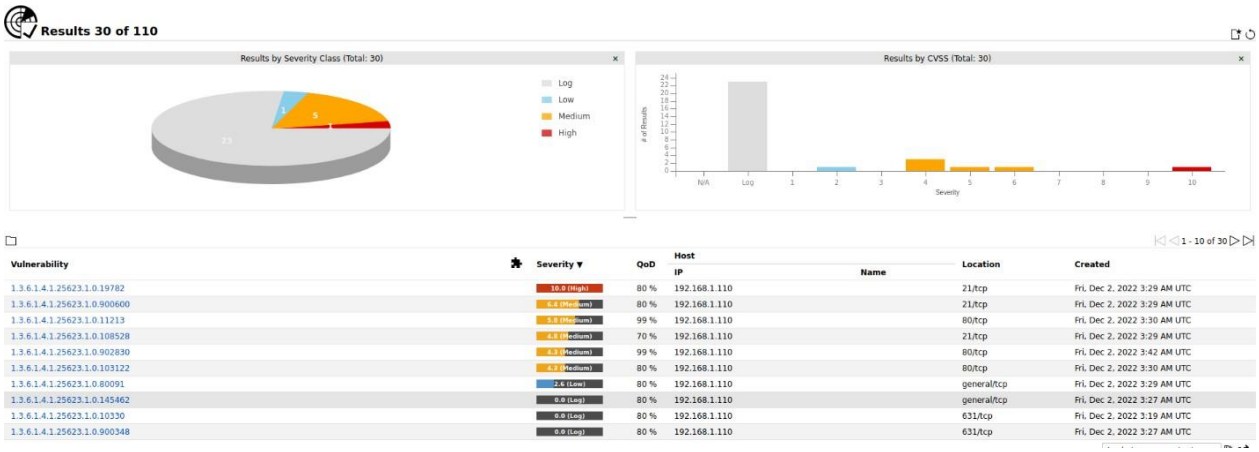


Figure 8.2 - Vulnerability report of disk



Conclusion:

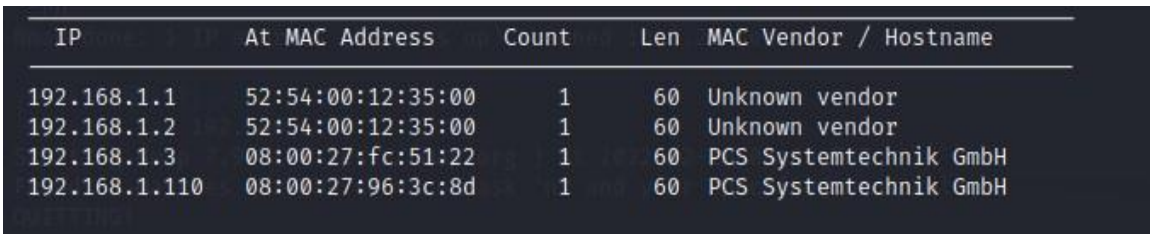
The severity of vulnerability information has been discovered using the Greenbone software.

Attack Plan

Environment:

For collecting the information or attacking on Live CD, a kali Linux machine and Live disk are required on Oracle Virtual Box. To operate the Live CD, it must bridge the network with kali which has IP address.

Figure 9.1 - Target's IP address



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	52:54:00:12:35:00	1	60	Unknown vendor
192.168.1.2	52:54:00:12:35:00	1	60	Unknown vendor
192.168.1.3	08:00:27:fc:51:22	1	60	PCS Systemtechnik GmbH
192.168.1.110	08:00:27:96:3c:8d	1	60	PCS Systemtechnik GmbH

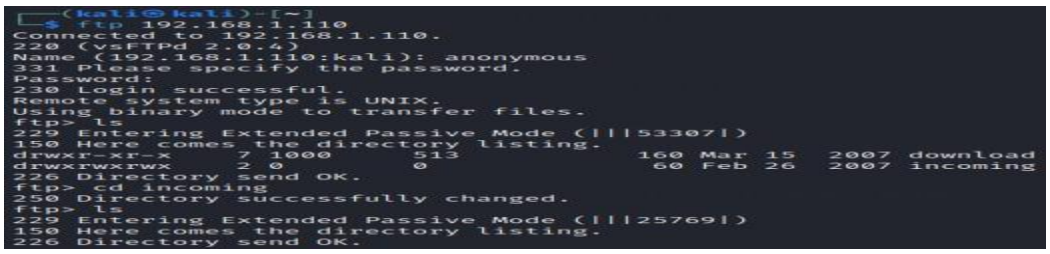
1. Some admin names and email addresses can be used as advantages in account brute forcing from the passive recon activities. The potential usernames include adamsa, aadams, adams, banterb, bbanter, banter, coffee, ccoffee, and coffee.
2. On the other hand, the username and password can be found using hydra or john ripper.
3. From the active recon activities, it is observed that are few services like http, ftp, ssh and ipp are running on the different ports. Considering each service as an advantage in finding the vulnerabilities.
4. In this report, giving the priority in connecting to the FTP server as the purpose is to do penetration testing on FTP server.
5. Later, trying to connect the other services to exploit using enumeration techniques.
6. By connecting the services, we may get privileges of users and ultimately finding any information on the systems, yet this can easily be found on the firewall of the systems which can give the data who is trying to connect. Additionally, the network administrators can easily find out and disconnect the connections.

Note: Considering the target IP address as 192.168.1.110 by the process of elimination.

Execution Report and Results:

1. As the report's focus is on FTP servers, using anonymous authentication to connect to the FTP servers on Kali was successful.

Figure 9.2 - Connected FTP Server through kali



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.0.4)
Name (192.168.1.110:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53307|)
150 Here comes the directory listing.
drwxr-xr-x    7 1000     513           160 Mar 15  2007 download
drwxrwxrwx    2 0        0              60 Feb 26  2007 incoming
226 Directory send OK.
ftp> cd incoming
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||25769|)
150 Here comes the directory listing.
226 Directory send OK.
```

2. Two folders on the system, incoming and download, can be utilized for brute force attacks. However, there are no files listed under incoming.
3. There is a shadow file under the download folder and trying to view the passwords in the shadow file.
4. Attempting to save the file on the system later, then using John Ripper to try and crack the password using darkcode.txt, which revealed "Complexity" as one of the root passwords.
5. When attempting to connect via SSH using the credentials root and Complexity, the connection was unsuccessful.

Figure 10.1 - Viewing the download folder

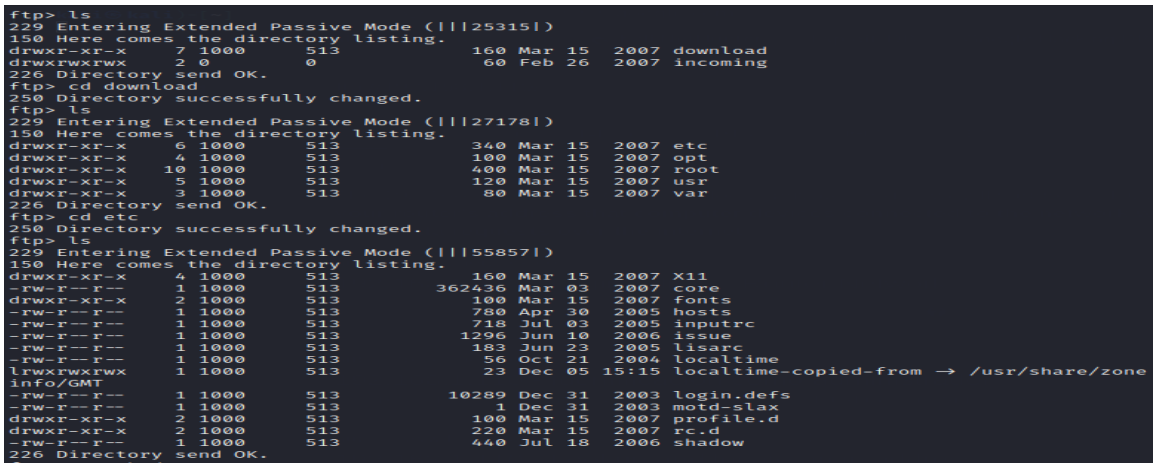


Figure 10.2 - Viewing the Shadow file

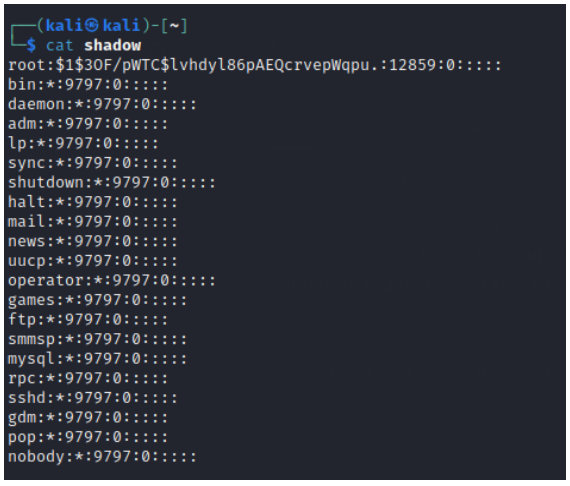
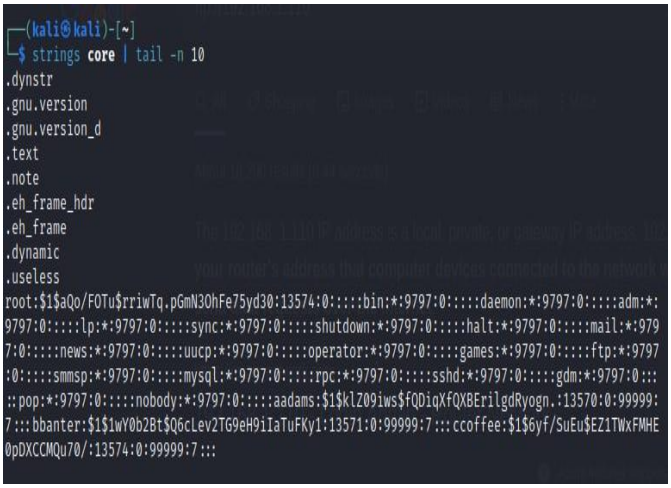


Figure 10.3 - Viewing the Core file



6. According on the data gathered from passive recon efforts, the folder displays various passwords that matched. Consequently, keep all the passwords in one file.
7. John Ripper was used to attempt to crack the password once more, and it produced the passwords "toor" and "Zymurgy" for the admin and bbanter, respectively.

Figure 11.1 - Cracking the root password

Figure 11.2 - Cracking the user and admin password

Figure 11.3 - Viewing the sensitive information

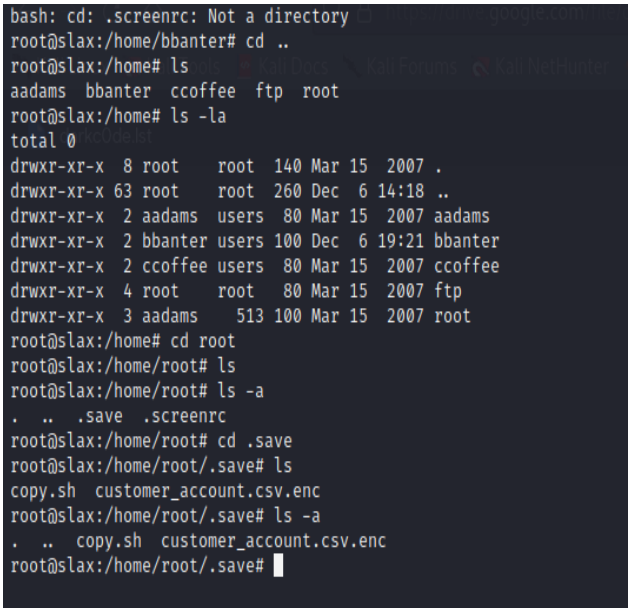
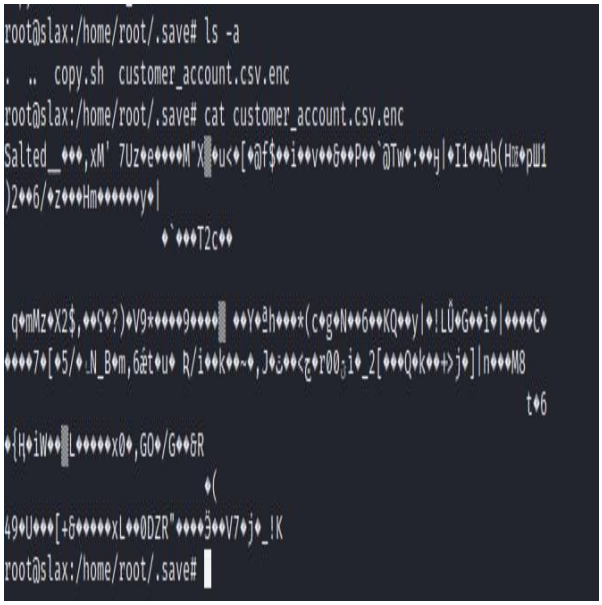
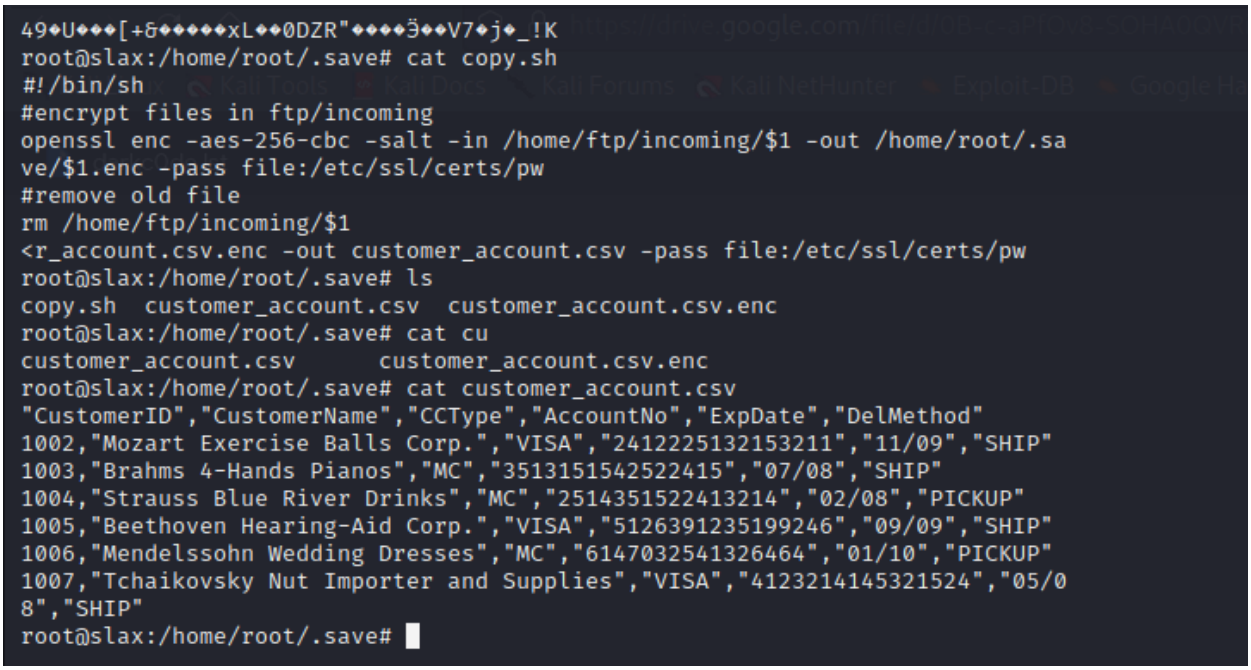


Figure 11.4 - Viewing the encrypted file



8. When attempting to connect the SSH with bbanter credentials to see to get the privileges on the file system.
9. There by trying with the root user who can have the complete privileges on the file system which worked with the password as “Complexity”
10. On the system there are folders as .save and .screenc in which .save has some sensitive data file named as customer_account.csv.enc which is an encrypted file.
11. Using decryption tools like openssl , decrypting the file which gave the credit card account details.

Figure 12 - Cracked the sensitive data on the FTP Server



Conclusion:

Through this execution report, there is a sensitive data of customer’s credit card details which proved to network administrator that the severs are not secured.

References:

Treizesec. (2016, December 3). *De-ice S1.110*. Pentest Writeups. Retrieved December 11, 2022, from https://pentestwriteups.wordpress.com/2016/07/21/de-ice-s1-110/

De-ICE: S1.110. Vulnerable By Design ~ VulnHub. (n.d.). Retrieved December 11, 2022, from https://www.vulnhub.com/entry/de-ice-s1110,9/

Appendix A:

Information Gathering: The process of gathering information before attacking the target Actively communicating with the target directly or passively interacting with the target indirectly are both viable options for accomplishing it.

Source : Ethical hacking: Passive information gathering with Maltego | Infosec Resources (infosecinstitute.com)

OSINT Framework: Open-Source Intelligence Tools, or OSINT, are used in the web application's querying of many data sources.

Source : *OSINT framework*. OSINT Framework. (n.d.). Retrieved December 12, 2022, from https://osintframework.com/

Shodan: An internet-linked device search engine called Shodan compiles data on all devices that are directly connected to the internet.

Source: *What is shodan? - shodan help center*. Shodan. (n.d.). Retrieved December 12, 2022, from https://help.shodan.io/the-basics/what-is-shodan

Exploit: A piece of code called a "exploit" is used to identify security flaws and manipulate them.

Source: Cisco. (2021, April 5). *What is an exploit?* Cisco. Retrieved December 12, 2022, from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

Port: A port is a physical docking location on a computer where an external device can be plugged in.

Source: *What is network port?* Tutorials Point. (n.d.). Retrieved December 12, 2022, from https://www.tutorialspoint.com/what-is-network-port

Firewall: A firewall is a piece of network security equipment that keeps track of all network traffic, both coming inside and going out.

Source: *What is a Firewall?* Forcepoint. (2022, October 24). Retrieved December 12, 2022, from https://www.forcepoint.com/cyber-edu/firewall

Nmap: Nmap, or Network Mapper, is a Linux command-line utility that is free and open-source and used to scan networks for IP addresses and ports.

Source: *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time (freecodecamp.org)*

Common Vulnerability Enumeration(CVE): It is a list which evaluates the comprehensiveness of the information sources.

Source: *Towards a common enumeration of vulnerabilities*. CVE. (n.d.). Retrieved December 12, 2022, from https://cve.mitre.org/docs/docs-2000/cerias.html

FTP : FTP stands for the file transfer protocol, a common protocol that TCP/IP supports that is used to move data from one site to another.

Source: *What is FTP?* Tutorials Point. (n.d.). Retrieved December 12, 2022, from https://www.tutorialspoint.com/what-is-ftp

HTTP: It is http server stands for Hyper Text Transfer Protocol which is a application protocol used in request-response protocol.

Source: *What is HTTP?* Tutorials Point. (n.d.). Retrieved December 12, 2022, from https://www.tutorialspoint.com/what-is-http

SSH: SSH stands for Secure shell which is a secure network communication protocol used to connect to remote devices securely.

Source: *What is SSH and what does it stand for?* MUO. (2021, January 8). Retrieved December 12, 2022, from https://www.makeuseof.com/what-is-ssh/

IPP: IPP stands for Internet Printing Protocol is a secure application-level protocol used for network printing.

Source: *How to use the internet printing protocol*. How to Use the Internet Printing Protocol - Printer Working Group. (n.d.). Retrieved December 12, 2022, from https://www.pwg.org/ipp/ippguide.html

Brute force Attack: Brute force assault is a hacking technique that employs trial and error to break encryption, login credentials, and passwords.

Source: *What is a brute force attack? Definition, Types & How It Works*. Fortinet. (n.d.). Retrieved December 12, 2022, from https://www.fortinet.com/resources/cyberglossary/brute-force-attack

Enumeration: It refers to the method of removing usernames, machine names, network resources, shares, and services from a system.

Source: *Enumeration and its types*. Ethical Hacking. (n.d.). Retrieved December 12, 2022, from https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types

John Ripper: A well-known password cracking tool called John Ripper is open-source and incorporates several cracking programs.

Source: *What is John the Ripper? | Definition from TechTarget*

Hydra: A brute-forcing program called Hydra uses quick dictionary assaults to help break network service passwords.

Source: Shivanandhan, M. (2022, November 18). *How to use Hydra to hack passwords – penetration testing tutorial*. freeCodeCamp.org. Retrieved December 12, 2022, from https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/

Encrypted files: An encrypted file is one that has had an encoding algorithm applied to it to scramble the data.

Source: Communications, B. (2021, October 28). *What is file encryption?* Box Blog. Retrieved December 12, 2022, from https://blog.box.com/what-is-file-encryption

Decryption: Decryption is the process of restoring encrypted data to its original state.

Source: *What is decryption? definition of decryption, decryption meaning*. The Economic Times. (n.d.). Retrieved December 12, 2022, from https://economictimes.indiatimes.com/definition/decryption

Sensitive data: Information that is confidential and is stored, processed, or managed by a person or organization is referred to as sensitive data.

Source: Brown, S. (2022, October 27). *What is sensitive data? definition, examples, and more*. StrongDM. Retrieved December 12, 2022, from https://www.strongdm.com/blog/sensitive-data

Vulnerability: A vulnerability is a flaw in an organization's internal controls, system processes, or both.

Source: *What is vulnerability in cyber security? types and meaning*. Intellipaat Blog. (2022, November 18). Retrieved December 12, 2022, from https://intellipaat.com/blog/vulnerability-in-cyber-security/

Shadow: In the Linux file system, a shadow file is used to store passwords in an encrypted format.

Source: *All-pairs testing*. Wikipedia. (2021, November 10). Retrieved December 12, 2022, from https://en.wikipedia.org/wiki/All-pairs_testing

Core file: This file, known as a core dump, provides all the data needed to debug the application after it crashes.

Source: *How to read a core dump file in linux – systran box*. (n.d.). Retrieved December 12, 2022, from https://www.systranbox.com/how-to-read-core-dump-file-in-linux/

OpenSSL: An open-source command-line utility called OpenSSL is frequently used to create private keys and identify certificate data

Source: SVadmin. (2021, April 5). *What is openssl in linux?* OS Today. Retrieved December 12, 2022, from https://frameboxxindore.com/linux/what-is-openssl-in-linux.html

Appendix B:

Subject	Section(s)	Page(s)
Figure 3.1 to 3.2	Summary of findings	3
Figure 4.1	Information Gathering	4
Figure 5.1 to 5.2	Information Gathering	5
Figure 6.1 to 6.2	Information Gathering	6
Figure 7.1 to 7.4	Information Gathering	7
Figure 8.1 to 8.2	Other Tools and Software	8
Figure 9.1	Attack Plan	9
Figure 9.2	Execution Report and Results	9
Figure 10.1 to 10.3	Execution Report and Results	10
Figure 11.1 to 11.4	Execution Report and Results	11
Figure 12	Execution Report and Results	12