Post-Exploitation, Privilege Escalation, and Evidence Collection Assessment

Objective

The objective of this task was to simulate post-exploitation activities after gaining initial access to a vulnerable system. The focus was on privilege escalation, traffic capture, and proper evidence handling while maintaining chain-of-custody practices.

Environment and Tools

- **Target System:** Linux-based vulnerable service (DistCC)
- **Attacker System:** Kali Linux
- **Tools Used:**
    a. Metasploit Framework
    b. Wireshark
    c. Hashing utilities (SHA256)

Post-Exploitation and Privilege Escalation

Initial access was gained using the **DistCC Remote Command Execution vulnerability**. The Metasploit module was configured with a reverse shell payload, resulting in a command shell session running under the **daemon** user context.

Exploit Used
exploit/unix/misc/distcc_exec

Payload
payload/cmd/unix/reverse

After gaining the low-privileged shell, privilege escalation was simulated using Nmap interactive mode, a known misconfiguration technique on older Linux systems. This allowed escalation from the daemon user to root, demonstrating a complete system compromise.

Evidence Collection

All exploitation and escalation traffic was captured in real time using Wireshark. The captured traffic was saved as a **traffic_log.pcap** file to preserve evidence of attacker actions.

Evidence Details

Item	Description	Collected By	Date	Hash Value
Traffic_log.pcap	Exploitation & Reverse Shell Traffic	VAPT Intern	13-01-2026	ee88132aa30edce46cf268c5d7b34f4a05f9cb16d47067159d6a2808a9eb4955

The file traffic_log.pcap was hashed using SHA256 to ensure integrity and support chain-of-custody requirements.

Evidence Collection Summary

During post-exploitation, all attacker activity was captured using Wireshark and securely stored as a packet capture file. The evidence was hashed to preserve integrity and support forensic validation. This process ensures that collected data can be reliably referenced during reporting or incident response activities.

Conclusion

This task successfully demonstrated how attackers can escalate privileges after initial access and how defenders can capture and preserve forensic evidence. Proper evidence handling is critical for incident response, investigations, and legal defensibility.