Post-Exploitation Assessment: Privilege Escalation and Persistence

Intern name: Cinchana S
Date: 23-01-2026

Executive Summary

A privilege escalation assessment was conducted on a vulnerable Linux system following initial access. System enumeration identified misconfigured privilege handling, allowing escalation from a daemon-level shell to full root privileges. Persistence was successfully established using scheduled task execution.

Scope

- Target System: Vulnerable Linux VM (Metasploitable2)
- Attacker System: Kali Linux
- Tools Used:
    - Netcat
    - LinPEAS
    - Local Linux utilities

Methodology (Execution)

Initial Access

- Obtained a reverse shell as a low-privileged user (daemon) using exploit/unix/misc/distcc_exec.

Enumeration

- Enumerated privilege context and system configuration.
- Identified effective root privileges.

Privilege Escalation

- Converted effective root privileges into a full root UID shell.

- Verified unrestricted root access.

Persistence

- Created a scheduled task (cron job) to maintain persistent access.

Privilege Escalation Log

Test ID	Technique	Target IP	Status	Outcome
001	Privilege Context Abuse	192.168.0.9	Success	Root shell

Attack Execution Log

Step	Action	Result
1	Reverse shell obtained	Daemon shell
2	Shell upgraded to full TTY	Interactive access
3	Privilege escalation executed	Root privileges obtained
4	Root access verified	Full UID 0 confirmed

Persistence Log

Method	Location	Result
Cron Job	/etc/crontab	Persistent root-level access

Impact

An attacker gaining low-level access can escalate to full root privileges and maintain persistent access, resulting in complete system compromise.

Remediation

- Enforce least-privilege principles
- Monitor scheduled tasks and cron jobs
- Restrict privilege escalation vectors
- Regularly audit system configurations

Conclusion

The system was fully compromised through privilege escalation and persistence techniques. Successful escalation to root and persistent access demonstrate critical security misconfigurations.

Summary

After gaining an initial shell, system enumeration revealed elevated privileges. The shell was upgraded to a full interactive session and escalated to complete root access. Persistence was established using a cron job, demonstrating full system compromise and long-term attacker access.