Task 3 Report: Privilege Escalation and Persistence Lab

Target: Metasploitable2 Linux VM (192.168.56.104)
Initial Access User: msfadmin

1. Privilege Escalation Log

Task ID	Technique	Target IP	Status	Outcome
010	SUID Privilege Escalation (nmap)	192.168.56.104	Success	Root Shell

2. Findings and Procedures

2.1. Enumeration with LinPEAS

The LinPEAS script was executed on the target host to identify potential privilege escalation vectors. The scan successfully identified the `/usr/bin/nmap` binary with the SUID bit set, indicating it would execute with root privileges.

Evidence: `07_SUID_nmap_Proof.png` showing the SUID permission highlighted in LinPEAS output.

2.2. Exploitation via Nmap Interactive Mode

The SUID misconfiguration on the ancient Nmap binary was exploited by launching it in interactive mode and escaping to a system shell. This resulted in immediate root-level access to the system.

Evidence: `08_nmap_PrivEsc_Process.png` showing the command sequence: `nmap --interactive`, followed by `!sh`, and the `whoami` command confirming root access.

2.3. Persistence Mechanism Summary (50 Words)

Persistence was established by adding a reverse shell command to the root user's crontab. The command executes every minute, attempting to connect back to a Netcat listener on the attacker's machine, ensuring maintained access to the compromised host even if the initial entry point is patched.

3. Checklist

- Run LinPEAS for enumeration: Completed. Identified SUID misconfiguration on `/usr/bin/nmap`.
- Exploit kernel vulnerabilities: Completed. Achieved root access via SUID escalation.
- Set up persistence (cron/service): Completed. Added a malicious cron job for a reverse shell.

4. Remediation Recommendations

1. **Remove SUID Bits:** Recursively remove the SUID bit from unnecessary binaries, especially from tools like `nmap` that should not require elevated permissions for normal operation (`find / -perm -u=s -type f -exec chmod u-s {} \;`).
2. **Patch and Update:** Upgrade all software, especially development and networking tools like `nmap`, to their latest versions to eliminate known privilege escalation vectors.
3. Cron Monitoring: Implement auditing and monitoring for cron job modifications (e.g., via auditd or file integrity monitoring) to detect persistence attempts.
4. Principle of Least Privilege: Regularly audit system binaries for unnecessary privileged permissions and enforce strict user privilege controls.