Target: Windows PrivEsc Arena

Executive Summary

This phase of the assessment focused on activities after initial compromise. The primary objectives were to escalate privileges on a Windows system and collect forensic evidence. The "AlwaysInstallElevated" system misconfiguration was successfully exploited to gain NT `AUTHORITY\SYSTEM` privileges, and critical evidence including password hashes was collected from the compromised host.

1. Privilege Escalation Analysis

The assessment identified that the Windows target was vulnerable to privilege escalation through the "AlwaysInstallElevated" policy vulnerability. This misconfiguration allows any user to install Microsoft Installer (MSI) packages with elevated SYSTEM privileges, effectively bypassing normal user access controls.

Evidence of Vulnerability: The output of the `reg query` command confirms that both registry values required for this exploit are set to 1, making the system vulnerable.
Reference: *Screenshot `15_Always_Install_Elevated_Possible.png`*

https://Screenshots/15_Always_Install_Elevated_Possible.png

2. Privilege Escalation Execution

Reverse shell payload was created using msfvenom and uploaded to Windows machine as a .msi file. The execution of this malicious MSI package granted a new Meterpreter session with `NT AUTHORITY\SYSTEM` privileges, the highest level of access on a Windows system.

Evidence of Success: The Metasploit output shows the successful creation of the payload and the establishment of a new SYSTEM-level session.
Reference: *Screenshot `16_Always_Install_Elevated_Success.png`*

https://Screenshots/16_Always_Install_Elevated_Success.png

3. Evidence Collection

With SYSTEM-level access, the Meterpreter `hashdump` command was executed to extract password hashes from the Security Account Manager (SAM) database. These hashes can be used for offline password cracking or lateral movement within the network.

Evidence Collected: The output shows the extracted LM and NTLM hashes for all local user accounts on the system.
Reference: *Screenshot 17_Windows_Hashdump.png*

https://Screenshots/17_Windows_Hashdump.png

4. Findings Log

Finding ID	Vulnerability	CVSS Score	Remediation
F004	Windows AlwaysInstallElevated Privilege Escalation	7.8 (High)	**1.** Set `AlwaysInstallElevated` registry values to `0` **2.** Apply Microsoft security patches **3.** Implement least privilege policies

5. Remediation Recommendations

1. **Registry Modification:** Set both `HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated` and `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated` registry values to `0` to disable this feature.
2. **Group Policy:** Implement Group Policy settings to restrict installer privileges across the domain.
3. **Patch Management:** Ensure all Windows systems are updated with the latest security patches from Microsoft.
4. **User Training:** Educate system administrators about the risks of enabling elevated installation privileges.

Appendix: Screenshot Evidence

- `15_Always_Install_Elevated_Possible.png`: Registry confirmation of vulnerability

- `16_Always_Install_Elevated_Success.png`: Successful privilege escalation execution
- `17_Windows_Hashdump.png`: Extracted password hashes from SAM database

Distribution: Security Team, System Administrators, IT Management