CTF/Box Writeup Template

Introduction

- **Box/Challenge Name:** [Name of the Box or Challenge]
- **Platform:** [TryHackMe, HacktheBox, VulnHub, etc.]
- **Difficulty Level:** [Beginner/Intermediate/Advanced]
- **Objectives:** Briefly outline what you aim to achieve with this box/challenge.
- **Tools Used:** List the tools you used during the engagement.

Pre-Engagement

Scope Definition

- Define the boundaries of the test, including which systems, networks, and applications will be tested.

Rules of Engagement

- Detail any rules or guidelines given before starting the challenge. This might include limitations on brute-forcing, denial-of-service attacks, etc.

Reconnaissance

Passive Recon

- Discuss any information gathered without directly interacting with the target. This can include information from forums, previous writeups, and other open-source intelligence (OSINT).

Active Recon

- **Host Discovery:** Document how you identified active machines or services in the target network.
- **Port Scanning:** List the ports you discovered open and the services running on them.
- **Service Enumeration:** Detail the specific versions and configurations of the services identified during port scanning. Mention any initial vulnerabilities or misconfigurations you may have noticed.

Vulnerability Analysis

- **Vulnerability Scanning:** Discuss any automated scanning tools or techniques used to identify vulnerabilities.
- **Manual Testing and Research:** Explain any manual testing techniques employed to verify or discover vulnerabilities. Include any specific vulnerabilities found, with references to CVEs or other advisories if applicable.

Exploitation

- **Exploit Details:** Describe the vulnerability exploited, including any relevant CVE numbers or exploit database references.

- **Exploit Execution:** Step-by-step guide on how the exploit was carried out, including any custom scripts or commands used.
- **Initial Access:** Detail how initial access was gained and what level of access you obtained (e.g., user shell, admin shell).

Post-Exploitation

- **Privilege Escalation:** Explain the methods used to escalate privileges, including any specific tools or exploits.
- **Persistence:** Discuss any techniques employed to maintain access to the system.
- **Lateral Movement:** If applicable, detail how you moved within the network to target additional systems.
- **Data Exfiltration:** Describe how any sensitive data was identified and securely exfiltrated from the target environment.

Analysis and Reporting

- **Findings Summary:** Provide a summary of the vulnerabilities discovered, exploited, and any data exfiltrated.
- **Impact Analysis:** Discuss the potential impact of the vulnerabilities if they were exploited by a malicious actor.
- **Remediation Recommendations:** Offer detailed recommendations for mitigating the identified risks.
- **Lessons Learned:** Reflect on the engagement, including what went well, what could be improved, and any new techniques learned.

Conclusion

Wrap up your writeup with any final thoughts, the overall experience of the challenge, and acknowledgments if you were working with or inspired by others.