**Executive Summary**

*Provide a description of the business importance of your findings. I.e., summarize the most critical vulnerability/ies discovered; explain why they’re critical, and how they can harm the business; and how quickly the business should act to fix the issues you discovered.*

**Attack Narrative**

This assessment involved the attempted compromise of multiple machines on the target subnet. Each phase of the test is documented below.

**Reconnaissance**

**General Reconnaissance**

*Summarize your Nmap scan results/findings*.

**Enumeration and Vulnerability Analysis**

This section summarizes the most critical vulnerabilities affecting the target network.

*FIll out the table below for your target. Under* ***Vulnerabilities****, include things like: “Exposed Login Server”, “Exposed Web Server”, etc.*

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **Operating System** | **Vulnerabilities** | **Risk (Low/Med/High)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Web Server Analysis**

*Summarize the steps you took to analyze the web server, and document your findings. This should include a summary of the steps you took to investigate it; vulnerabilities you discovered; and any steps you took to exploit it.*

**Network Analysis**

*Summarize the steps you took to break into the SSH server. This should include a summary of the steps you took to investigate it; vulnerabilities you discovered; and any steps you took to exploit it.*

**Post-Exploitation Exploration and Privilege Escalation**

*Summarize the steps you took to escalate from a user shell to a root shell. This should include a summary of how you identified the correct privilege escalation method; the command you ran to execute it; and a screenshot proving that it succeeded.*

*In addition, include paths to each of the flags you find on the target.*

**Conclusion and Recommendations**

Based on the results documented above, we recommend the client take the following steps to remediate the vulnerabilities identified on the target machine.

**Web Server**

*Suggest a patch for each vulnerability you identified and exploited in the web server.*

**Network Services**

*Suggest a patch for each vulnerability you identified and exploited in the SSH server.*

**Hardening the Server**

*Suggest a patch for each vulnerability you identified and exploited to achieve privilege escalation.*