**ITSC 304 – Operating System Exploitation**

**Final Project Report**

Coleton Sanheim

Submitted: 2022-04-22

Introduction:

This is the report for the final project. As per the project specifications Me and D’Artagnan worked together for this project, however we each used our own machines and tools to complete this. I used VirtualBox to host three Virtual machines, a Kali Linux machine that will be that attacker, and a Windows 7 and ubuntu 14 machine to act as the victims. The goal here was to perform an exploit on both of the machines. The threat grading structure we referenced was the standard CVSS v3.0 structure.

Information Gathering:

We used the tool Nessus to gather information about the vulnerable machines. The first step we did was to scan for open ports on the machines, and we found that for the Linux machine the only port that was open was 22 while with the Windows machine the open ports included 135,137,139,445,3389,5357,49152,49153, 49154, 49155, 49156, 49157. The next step was to perform an advanced scan on the vulnerable machines to determine what vulnerabilities were present. Most of the vulnerabilities found for the Ubuntu machine was simply warnings that the OS was outdated and likely insecure, the only serious vulnerability found was a privilege escalation vulnerability through SSH. For the windows machine there was many more vulnerabilities found that could be exploited. (a total of 8 in the High-Critical range)

Vulnerability Assessment:

The vulnerabilities that were selected was <https://attack.mitre.org/techniques/T1021/001/> for the windows machine and <https://attack.mitre.org/techniques/T1548/003/> for the ubuntu.

The windows exploit was a remote code execution exploit that took advantage of remote desktop protocol to run arbitrary code, more specifically using the bluekeep attack. This allows a shell to be opened and more exploitation to be performed. The Ubuntu exploit was a post-exploitation vulnerability that allows an attacker to escalate privilege using a vulnerability in sudo and sudo caching.

Exploitation/Vulnerability Confirmation:

For the Windows machine it was a targeted attack that would only take a matter of minutes to perform. Using Metasploit console we were able to use the exploit to spawn a meterpreter shell on the victim machine. For the Ubuntu machine we used a hydra bruteforce attack to crack the SSH password. This can take a long time depending on how complex the password is. Once access was gained, we were able to install a backdoor into the machine to be able to access it remotely and establish persistence.

Post Exploitation:

For the windows machine we were able to use Meterpreter and Metasploit scripts to enumerate the directory and steal information from the victim. It would also theoretically be possible to do any kind of attack here, as the functionality of these tools is quite high. For the Ubuntu machine once we gained access through SSH into the machine, we were able to create a backdoor and establish persistence using a Metasploit generated backdoor executable. Further, we were able to perform the privilege escalation attack described before to escalate our privileges to that of the root user.

Conclusion:

These exploits were possible as the machines we were testing on were wildly out of date. The main suggestion I would give to mitigate the potential vulnerabilities would be to make sure that all systems and applications are updated to their latest builds so as these specific vulnerabilities are patched. Another issue that I noticed and would also recommend fixing would to be to ensure that all unused ports are closed on the machines as open ports only introduce new vectors of attack into these machines.