Project: Threat and Vulnerability Analysis Project

By: Alexander Ho

Professor Chen

ITN 261

Date: 12/1/2021

Within this project, I learned how to do a threat and vulnerability analysis using two virtual machines. When doing a threat and vulnerability analysis for this project, I needed to install an attacker system and a target system. The two virtual machines I used were Microsoft Edge Windows 10 and Metasploitable 2. In this project, the OS virtualization software I will be using as the attacker system is Microsoft Edge Windows 10. For the target system, the virtual machine I will be using is Metasploitable 2.  When doing this threat, the vulnerability analysis I needed is to set up a virtualization software tool that is reliable and efficient. For this project, I installed VMWare Workstation Pro, which provides a controlled environment when navigating between the two virtual machines. Also, I learned VMware Workstation Pro uses a tabs feature when navigating between virtual machines that are open, which makes it great for threat and vulnerability analysis testing.

The first testing tool I used was a discovery and mapping tool called Nmap. I learned that Nmap is a discovery and mapping tool that identifies ports, services, and versions of software when scanning a target system environment. The installation of Nmap was simple and easy to install. After installing Nmap I scanned the target system of Metasploitable 2. The profile scan used within Nmap was the intense scan with the command being “nmap -T4 -A -v 92.168.126.128”. The second testing tool I used was the vulnerability scanning software that can scan a target host machine and identify the vulnerabilities called Nessus. I learned that this tool raises alerts when vulnerabilities are discovered when vulnerabilities are in either low, medium, high, or critical status. I completed a vulnerability scan against the Metasploitable 2 target host and identified seventy-three vulnerabilities. Within the scan, there were eleven critical vulnerabilities, ten high vulnerabilities, twenty-seven medium vulnerabilities and five low vulnerabilities. After scanning, the target system is completed, and the vulnerability results are completed. The last part of this project is to demonstrate a penetration test. Within the Nessus scanner, there is an option to export vulnerability scans of the targeted systems.

The third testing tool I used to successfully run and demonstrate penetration testing is the software called Metasploit Pro. I learned that the Metasploit Pro is designed for enterprise security programs, and it is an advanced penetration testing tool. When getting started to do penetration testing within this software, I imported the Nessus scan file of the Metasploit target system. After importing the Nessus file within the penetration option, I started to configure the exploit settings. I learned that there are different payload types and other advanced settings that configure the exploits. After the testing was finished, I was able to view three active sessions. Within session two, I was able to access the file system, command shell, collect system data, create a proxy pivot, and terminate the session.

A challenge that I encountered within this project was the storage space on my hard drive. The solution I used to increase more space for this project was to use a portable hard drive when installing VMWare and saving the virtual machines. Another challenge was the attacker system MS Edge Windows 10 would randomly freeze and not respond. The solution to this was to increase the virtual machine amount of CPU cores for each processor, memory, and storage space.

Within the last part of this project, learning and demonstrating about penetration testing into the target system was very helpful against an attacker who can maintain system access. There are four phases a hacker has maintained a way to get into the victim’s computer system. The first phase is when a hacker maintains persistence and must not be detected. It is critical for attackers to be stealthy and not be detected by any users or IT staff. Next, the second phase is to infiltrate the system and get high-level permissions to the machine which is called privilege escalation. This allows the attacker to establish a new user as the administrator and install other malicious software. The third phase is using a backdoor software which allows the attacker to login to the server without any detection. When using a backdoor software, they are usually difficult to survive within the system because of the security patches. Overall, there weren’t a lot of things I would have done differently throughout the project. I installed the three testing tools successfully and completed a penetration test using an attacker and target system.