|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 1 Report |

Table of Contents

[1.0 Introduction – PenTest+ Vulnerability Scans 3](#_Toc145366763)

[2.0 Lab Results – Vulnerability Scans 4](#_Toc145366764)

[3.0 Technical Review – PenTest+ Vulnerability Scans 11](#_Toc145366765)

[4.0 Introduction – PenTest+ Metasploit Framework 12](#_Toc145366766)

[5.0 Lab Results – Metasploit Framework 13](#_Toc145366767)

[6.0 Technical Review – PenTest+ Metasploit Framework 21](#_Toc145366768)

[7.0 References: 22](#_Toc145366769)

[8.0 Activity Log 23](#_Toc145366770)

# Introduction – PenTest+ Vulnerability Scans

During the execution of this lab, an evaluation was done to test the basics of vulnerability against a theoretically vulnerable host. In doing so, the tool Openvas was used to execute a generalization of common vulnerabilities related both back to CVEs as well as common attack vectors. To accomplish testing on a more expansive level and to eliminate the possibility of false positives, a username, and SSH credentials were provided to execute such attacks as brute force. This also for a clearer vision into how attackers would emulate their own reconnaissance against our internal host and systems. Through these executions, I was able to create multiple reports that can be directly fed to our internal team to handle any possible security flaws as well as identification of steps for remediation and overall severity.

# 2.0 Lab Results – Vulnerability Scans

A screenshot of a computer

Description automatically generated

Figure 1.0 – Initial login using openvas in the kali os and browser.

A screenshot of a computer

Description automatically generated

Figure 1.1 – Setting up the SSH credentials to use against the vulnerable host

A screenshot of a computer

Description automatically generated

Figure 1.2 – Creating the target based on vulnerable hosts IP found in Nmap scan.

A screenshot of a computer

Description automatically generated

Figure 1.3 – Target was successfully created and ready to be scanned.

A screenshot of a computer

Description automatically generated

Figure 1.4 – Task is created and ready to have a scan executed

A screenshot of a computer

Description automatically generated

Figure 1.5 – Scan is being executed against the vulnerable instance based on our target list created.

A screenshot of a computer

Description automatically generated

Figure 1.6 – A report is generated to display the results of our vulnerability scan on the host.

A screenshot of a computer

Description automatically generated

Figure 1.7 – Findings related to SSH Brute Force. As noted, the vulnerability was successful, and mitigation plans as well as detection methods are listed.

A screenshot of a computer

Description automatically generated

Figure 1.8 – After successfully using the provided ssh credentials on the vulnerable host, a script was executed linspeas.sh for a privilege escalation meta information. This includes such things as passwords in configuration files, cron jobs, services and processes on the target host.

A screenshot of a computer

Description automatically generated

Figure 1.9 – Critical information such as possible SSH files are found in the scan as well as other important security findings to attempt further escalation of said attack.

# 3.0 Technical Review – PenTest+ Vulnerability Scans

In this security assessment, a vulnerable host was scanned using the OpenVAS as well as Nmap tool suites on the Kali OS. The execution of the scan used the identification of the vulnerable hosts' IP identification through the usage of Nmap. Furthermore, a robust scan including top attack vectors was executed against the ‘common’ port list. The common port list includes but is not limited to these scans of TCP/UDP ports in usage with SSH, FTP, web server, etc. Upon the scan, the report generation showed several highly critical vulnerabilities that needed further review. Upon review, the findings showed were indeed proven security v vulnerabilities and not false readings, which were verified by using other tooling suites for validation such as Nmap scan and linespea script. The remediation of said vulnerabilities should be limited to the most critical findings to avoid any potential threats or exposure.

# Introduction – PenTest+ Metasploit Framework

During the execution of this lab, an evaluation was done to expand on the skillset of using Metasploit framework. Key security vulnerabilities, scans, hosts, exploits, and payloads were executed to identify potential openings. These attacks included a focus on creating shells through brute force, as well as privilege escalation. In these attack vectors, key attack points were exploited and the ability to capture a super user login on the host was completed.

# 5.0 Lab Results – Metasploit Framework

A computer screen shot of a computer

Description automatically generated

Figure 2.0 – Start the Metasploit framework while watching ports 1-65535.

A computer screen shot of a computer

Description automatically generated

Figure 2.1 – Start the interactive msfconsole, allowing for easy search of potential attacks. In this case, we are focusing on the FTP attack, vsftpd\_234\_backdoor.

A screenshot of a computer

Description automatically generated

Figure 2.2- Set using Nmap Ip for the exploitable host, then execute attack payload. Which in this case was successful and a shell was created.

A screenshot of a computer

Description automatically generated

Figure 2.3 – Execute new attack using ftp login scanner.

A screenshot of a computer

Description automatically generated

Figure 2.4 – Create user and passwords through nano editor.

A screenshot of a computer

Description automatically generated

Figure 2.5 – The username and list created is executed against the host to attempt login through brute force attempts on FTP.

A screenshot of a computer

Description automatically generated

Figure 2.6 – A reverse shell payload is sent against the vulnerable host.

A screenshot of a computer

Description automatically generated

Figure 2.7 – The exploit is executed using our local kali session as the lhost. Once executed, we can see that we are on user distccd.

A screenshot of a computer

Description automatically generated

Figure 2.8 – Changing into a multiple session so as not to close our connected session with the vulnerable host.

A screenshot of a computer

Description automatically generated

Figure 2.9 – A reverse TCP is created on the vulnerable host, our last step is to test if our msfadmin has access, which it should now.

# 6.0 Technical Review – PenTest+ Metasploit Framework

In this security assessment, a vulnerable host was scanned using the Metasploit framework. Once the initial scan was executed for ports 1-66535, our session was created. In this security evaluation, the usage of multiple payloads to attempt reverse shells and brute force was executed. While brute force attacks on SSH initially failed, the usage of other critical payload vulnerabilities identified a gap in the system, allowing open sessions to be completed. The open ports and vulnerability to reverse shells allow security professionals to inject their own code as well as users. In future attempts to avoid these types of attacks, ports should be monitored and restricted, as well as SU permissions should be limited to avoid the creation of escalated users.

# 7.0 References:

[1] Niazi, R. (2022) A beginner’s guide to metasploit in Kali Linux (with practical examples), MUO. Available at: https://www.makeuseof.com/beginners-guide-metasploit-kali-linux

[2] Home (no date) CVE. Available at: https://cve.mitre.org/cve/

# 8.0 Activity Log

| **Member Name** | **Task Date** | **Task Details** |
| --- | --- | --- |
| Carl Laneave | 9/09/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |