Introduction:

This final report is based on the metasploitable 3 machine, which is intentionally vulnerable and is mainly used for learning purposes. The primary purpose of this project is to identify the vulnerabilities, mitigate them, and fix them so that the virtual machine is made as secure as possible.

Methodology:

The assessment began with initial scans using Nessus Advanced and Nmap.

1. **Nmap:** This program was used to find open ports on the network and the operating services. I found active devices, services, and configurations on the network by performing a thorough network scan.

2. **Nessus Advanced:** A thorough vulnerability scan of the network was carried out using Nessus. This utility detected vulnerabilities such as outdated software, inadequate setups, and missing updates. In network services and system applications, it also identified possible security vulnerabilities.

Findings:

1. ProFTPD mod_copy Information Disclosure – CRITICAL
2. SSH Weak Algorithms supported- MEDIUM
3. PhpMyAdmin prior to 4.8.6 SQLi VULNERABILITY- CRITICAL
4. Drupal Coder Module Deserialization RCE – CRITICAL
5. SMB Signing Not Required-MEDIUM
6. IP Forwarding -MEDIUM
7. PHP Unsupported Version Detection- CRITICAL
8. Drupal Database Abstraction API SQLi -HIGH
9. Web Application Potentially Vulnerable to Clickjacking -MEDIUM
10. Browsable Web Directories-MEDIUM
11. Web Servers Allows Password Auto Completion-LOW
12. SSH Server CBC Mode Ciphers Enabled-LOW (**See more in Appendix A)**

Fixes Implemented: (Appendix B)

I implemented the following fixes to address the vulnerabilities found:

- FTP: To resolve the mod_copy information leak issue, ProFTPD was upgraded to version 1.3.5a/1.3.6 or later.
- SSH: The SSH server was configured to use powerful ciphers and MACs (message authentication codes) to improve security.
- PhpMyAdmin: The SQL injection vulnerability has been fixed by updating PhpMyAdmin to the most recent version.
- Drupal Coder Module: To fix the deserialization vulnerability, disabled the current coder module, downloaded the latest version, and relocated the files to the modules directory of the Drupal installation.
- SMB: Restarted the service to take effect after configuring samba. conf to require server and client signatures.
- IP Forwarding: Updated the sysctl.conf file and set the net.ipv4.ip_forward value to 0 to deactivate IP forwarding.
- PHP: Upgraded PHP to the required version to eliminate vulnerabilities caused by the previous version.
- Browsable Web Directories: To stop directory listings, I used root access to disable the autoindex module and restarted the web server.
- Clickjacking: To fix the web application clickjacking vulnerability, I changed the.htaccess file with security headers.
- Password Auto Completion: I used root access to edit the config module and added header rule lines to stop password auto completions.

Post Fix Analysis: (Appendix C)

After successfully fixing the vulnerabilities other than the ones that are caused by compatibility concerns with the virtual machine os, like SSL /TLS versions and Certificate issues, the virtual machine is now more secure than earlier, and the Nessus scan provides more proof that the machine now has more security posture.

Conclusion:

The project gave me significant hands-on experience in identifying and addressing various vulnerabilities within a purposely vulnerable virtual machine of Metasploitable 3. I obtained real experience in cybersecurity methods and procedures by safeguarding network services, web applications, system services, and outdated software. Updating and continuously monitoring Metasploitable 3 will be necessary to keep it secure in the future to avoid security issues related SSL/TLS which still exist as vulnerabilities.However, this project emphasized the need to harden our network systems occasionally.

Appendix

- Appendix A: Metasploitable3_PreFix_Scan.pdf
- Appendix B: Metasploitable3_Fix_Implementation.pdf
- Appendix C: Metasploitable3_PostFix_Report.pdf