



Virtual Lab Report

Career Simulation 4

Created By:

- ✓ Ozzy Pratt
- ✓ Jordan Burge
- ✓ Ivan Arias
- ✓ Largo Cimballi
- ✓ Alpha Theoro

Executive Summary

The "Virtual Lab" project is a collaborative effort in which each team member focuses on different exploitation scenarios to understand various network attacks and their implications comprehensively. This project involves setting up individual virtual machines (VMs) or Vocareum machines, installing the necessary software, and configuring initial settings to conduct specific network attacks.

Team Responsibilities

Ivan - Web Penetration Testing

Ivan will perform a comprehensive web penetration test using Mr. Robot VM. He will document each step meticulously, detailing the findings and overall results. This documentation will include an overview and a detailed report of his penetration testing journey.

Ozzy - Man-In-The-Middle (MITM)

Ozzy will focus on Man-In-The-Middle attacks, including techniques such as ARP Spoofing, DNS Spoofing, and SSL Stripping. He will document these attacks, providing insights into the execution and impact of these tactics.

Jordan - DoS and DDoS Simulations

Jordan will conduct Denial of Service (DoS) attacks and simulate Distributed Denial of Service (DDoS) attacks. His documentation will cover the methods used and the impacts on service availability, highlighting the potential damage such attacks can cause.

Alpha - Phishing and Social Engineering

Alpha will create phishing emails and utilize social engineering techniques to deliver malware. They will document the tactics used and the results of their phishing campaigns. Additionally, Alpha will explore and document various mitigation strategies to counter these attacks.

This comprehensive report highlights the critical need for robust cybersecurity measures to counteract the growing cyber-attack threat. Each attack demonstrated by hacking into vulnerable systems to execute Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks showcases the various methods attackers can employ to compromise systems and exploit vulnerabilities.

Objectives

- ✓ Demonstrate the ability to set up and configure virtual machines for penetration testing: Showcase proficiency in creating and configuring virtual environments that are isolated and safe for conducting penetration tests. This includes installing the necessary software and configuring initial settings. (Measure: Successfully set up and configure virtual machines for at least two testing scenarios).
- ✓ Apply penetration testing tools and techniques to identify and exploit vulnerabilities: Utilize Nmap, Gobuster, Nikto, Hydra, and Metasploit to conduct comprehensive penetration tests. Demonstrate the ability to use these tools to uncover and exploit security vulnerabilities effectively. (Measure: Use at least three tools per project and document findings).
- ✓ Document and report findings in a detailed and structured manner: Maintain thorough documentation of all methodologies, findings, and results throughout the penetration testing process. This includes writing detailed reports that outline each step taken, the tools used, and the outcomes of the tests. (Measure: Complete and submit a detailed report for each penetration testing project).
- ✓ Develop and implement mitigation strategies for identified vulnerabilities: Propose effective solutions to address security weaknesses identified during penetration testing. Where possible, implement these solutions and verify their effectiveness in mitigating the vulnerabilities. (Measure: Develop and test at least one mitigation strategy per identified vulnerability).

Tool Definitions and Their Functions

1. Controlled, Isolated Environment
 - Definition: A segregated setup where testing activities are conducted to prevent any impact on live systems.
 - Function: Provides a safe sandbox for ethical hacking activities, ensuring that live systems are not compromised during testing.
2. Nmap
 - Definition: Network Mapper, a powerful open-source network scanning tool.
 - Function: Scans networks to identify live hosts, open ports, and available services, creating a comprehensive map of the target network.
3. Gobuster
 - Definition: A tool used to brute-force URLs and DNS subdomains.
 - Function: Identifies hidden directories and files on the target WordPress site by attempting numerous URL variations, aiding in discovering concealed resources.
4. Wappalyzer
 - Definition: A browser extension and software tool that uncovers website technologies.
 - Function: Detects and reports the different technologies and software frameworks the target WordPress site employs, providing insights into its infrastructure.
5. Nmap Scripts
 - Definition: Predefined scripts within Nmap are used to automate various network scanning tasks.
 - Function: Automates the detection of vulnerabilities, such as outdated software versions, and security weaknesses like SQL injection and cross-site scripting.
6. Nikto
 - Definition: An open-source web server scanner.
 - Function: Scans web servers for vulnerabilities, including outdated software, misconfigurations, and potentially dangerous files, contributing to identifying security issues.
7. Python Scripts
 - Definition: Custom scripts written in Python for performing automated tasks.
 - Function: Used to execute brute-force attacks by automating the process of guessing login credentials and identifying weak passwords.
8. Hydra
 - Definition: A fast and flexible network login cracker.
 - Function: Conducts brute-force attacks against various protocols to guess login credentials, aiding in identifying weak access points.
9. PHP Script
 - Definition: A script written in PHP used for various web-related tasks.
 - Function: Can be used to establish a reverse shell, providing the attacker with remote control over the target system.

10. Metasploit

- Definition: A comprehensive penetration testing framework.
- Function: Utilized to develop and execute exploit code against a remote target machine, often used to establish a reverse shell for remote system control.

11. Kali Linux

- Definition: A Debian-based Linux distribution designed for digital forensics and penetration testing.
- Function: Provides a comprehensive suite of tools for ethical hacking, including network scanning, vulnerability assessment, and exploitation tools, all pre-installed and configured for immediate use.

12. Nano (Linux)

- Definition: A simple, user-friendly text editor for Unix-like operating systems.
- Function: Used for editing configuration files, scripts, and other text files directly from the command line, making it a convenient tool for quick modifications during penetration testing and system administration.

13. Ettercap

- Definition: A comprehensive suite for network protocol analysis and security auditing.
- Function: Facilitates man-in-the-middle attacks, allowing the interception and manipulation of network traffic for analysis or exploitation.

14. Wireshark

- Definition: A widely used network protocol analyzer.
- Function: Captures and interactively analyzes network traffic, helping identify anomalies, vulnerabilities, and security issues.

15. Social-Engineer Toolkit (SET)

- Definition: An open-source penetration testing framework specifically aimed at social engineering.
- Function: Automates a variety of social engineering attacks, including phishing, credential harvesting, and creating malicious payloads to exploit human vulnerabilities in security.

Introduction

With technology advancing at an unprecedented rate, the frequency of cyber-attacks is increasing. These attacks, which can take the form of Hacking, Man in the Middle (MITM), Denial of Service (DOS), and Phishing Emails, highlight the urgent need for prevention. This report will delve into each attack, its execution, and most importantly, the crucial prevention methods.

Purpose

The purpose of these attacks is to demonstrate the potential harm to your system. It's important to note that all these tests were conducted in a controlled environment with two virtual machines, ensuring that no attack could escape this scope. This controlled environment provides reassurance and ensures the validity of the results. These tests were purely educational and should not be used for other purposes.

Titled "Virtual Lab," this project involves each team member focusing on different exploitation scenarios. Responsibilities include:

- Setting up individual virtual machines.
- Installing the necessary software.
- Configuring initial settings to conduct specific network attacks.

Team Responsibilities:

Attack 1: Ivan – Hacking Mr. Robot.

Attack 2: Ozzy – Man-In-The-Middle (MITM)

Attack 3: Jordan - DoS and DDoS Simulations

Attack 4: Alpha - Phishing and Social Engineering

Attack 5: Largo - Mitigation Strategies

Hacking Mr. Robot

The first attack started with hacking into a vulnerable Vulnhub virtual machine called Mr. Robot, which hosts a WordPress site. Mr. Robot was made explicitly to practice pen-testing tools. The steps are as follows:

- Use Nmap to find live hosts, open ports, and available services.
- Use Gobuster and Wappalyzer to brute-force directories and identify technologies used by the target WordPress site
- Use Nikto to find vulnerabilities like outdated software, SQL injection, and cross-site scripting in web servers
- Use Python scripts and Hydra to guess login credentials and find weak passwords and access points
- Use a reverse shell or Metasploit to take control of Mr. Robot

Findings:

Finding	CVSS Score	Severity	Finding Name	Description	Recommendation
1	9	High	HTTP (80/tcp) - Apache HTTPD	Open ports 80 and 443 running Apache HTTPD, potential entry points	Ensure Apache is up-to-date and configure security headers
2	8	High	SSL Info	Missing security headers and outdated SSL configurations	Update SSL/TLS settings and add security headers
3	6	Medium	WordPress Plugins	Various plugins, including outdated versions	Regularly update all plugins and monitor for vulnerabilities
4	5	Medium	WordPress Themes	Multiple themes, including outdated versions	Update themes and remove unused ones
5	8	High	Configuration Issues	Missing security headers and outdated PHP version	Update server configurations and PHP version
6	9	Critical	Credentials Found	Username and password retrieved (elliott/ER28-0652)	Change all passwords and review user access controls
7	5	Low	Directories/Files	Various sensitive directories and files exposed	Restrict access to sensitive directories and files

Man in the Middle (MITM)

The second attack is creating an MITM attack between two systems. Attackers use man-in-the-middle attacks to harvest login credentials, personally identifiable information (PII), or other sensitive information and are, just like brute force attacks, used at the start of the cyber-attack lifecycle during the reconnaissance and exploitation stages. Address Resolution Protocol (ARP) poisoning and Domain Name System (DNS) spoofing are two common MITM attacks. The steps are as follows:

MITM-ARP Poisoning

- Use Nmap to find live hosts, open ports, and available services.
- Take note of the IP and Mac addresses
- Startup Wireshark to view and capture the packets
- Open and set Ettercap with the proper credentials to start an ARP Poisoning attack
- Run Ettercap and switch back to Wireshark to collect any findings from the attack

MITM-DNS Spoofing

- Edit the Ettercap config file (etter.conf) and set the values of “ec_uid” and “ec_gid” to 0
- Scroll down and remove ‘#’ from the “redir_command_on” and “redir_command_off” commands to activate them. Save and exit.
- Edit the Ettercap dns file (etter.dns) and scroll to the bottom.
- Add the domain name you intend to spoof (i.e., facebook.com being sent to your location), the associated A and PRT records(i.e., google.com redirects the victim to Microsoft.com), and your attacking IP address. Save and exit.
- Open Ettercap, stop unified sniffing and scan for hosts to modify the target list
- Add the target’s IP address and enable the “dns_spoof” plugin
- Click on “arp_cop” to report suspicious ARP activity and start the attack
- View your attack as the target gets redirected twice.

Denial of Service (DOS)

The third attack is creating a DOS attack to slow down a system. A Denial of Service (DOS) is an attack that overwhelms a system by sending numerous requests to disrupt the system's ability to function. One example of a DOS attack is a SYN flood. SYN flood sends request packets repeatedly to all open ports until the system fails.

The steps are as follows:

- Open Nmap and scan for nearby systems to see their IPs and open ports
- Take note of ipv4 and open port
- Open Metasploit
- Search for “synflood” and use “auxiliary/dos/tcp/synflood”
- Type in “options” and set RHOSTS to the target’s ipv4 and RPORT to the target’s open port
- Type in “exploit” to run the SYN flood attack
- Switch to your target VM and open Wireshark and Task Manager to view the packets being sent by the attack and the strain the system is taking

Phishing and Social Engineering

The fourth attack is creating a phishing email with the help of social engineering and a fake login page. Social Engineering is based on human interaction, where attackers use human emotions and tendencies against their victims. Phishing exploits are used to test employee vulnerability to fake/malicious emails. The steps are as follows:

- Carry out reconnaissance of a website to set up a fake login page and a target to get their credentials (i.e. GitHub)
- Open Social-Engineer Toolkit (SET) by typing “settoolkit” in your terminal
- Enter “2” for Website Attack Vectors
- Enter “3” for Credential Harvester Attack Method
- Enter “2” for Site Cloner
- Enter your IP address for SET to send back the captured credentials to you
- Enter the URL of the website’s login page you are replicating (i.e., <https://github.com/login>)
- Copy your IP from the previous step and create a convincing email for your target, asking them to click on the hyperlink (your IP) and login (to the fake login page)
- Once the target login to the fake page, SET will copy and display the target’s login credentials for you to use.

Mitigations

To prevent brute force credential harvesting, ensure you have a secure password, an antivirus installed, and fraud detection software installed. Your password should be firm and complex by containing uppercase, lowercase, numbers, symbols, and at least 12 characters long. Antivirus software will help flag and block malicious files and emails that can steal passwords. Fraud detection will monitor your network traffic and block any credential harvesting.

To prevent Man-in-the-Middle, using a virtual private network (VPN), multifactor authentication, and verifying signatures is recommended. VPN encrypts the data that goes through it and stops the MITM from infiltrating the network traffic. We use multi-factor authentication with at least two devices to authenticate the user when signing in and ensure that digital signatures match the message content by using a hash to ensure the message wasn't tampered with.

To prevent DOS/DDOS attacks, network protection, rate limiting, and a web application firewall (WAF) are recommended. A proper ZTNA solution to mitigate DDOS attacks protects the network as it doesn't require any ports to be opened as it proxies traffic to the enterprise network. Limit the number of requests a server will accept over a certain time window. A WAF can assist an organization's efforts to mitigate application-layer attacks. It stands between internet users and the organization's servers and policies requests for entrance.

Preventing phishing and social engineering involves awareness training. Educating employees on how social engineering is done through recognizing signs of manipulation and participating in social engineering simulations. Resisting the urge to click links in a suspicious email, visiting websites directly by typing them in a browser instead of clicking on them provided by the email, and not opening email attachments from unknown sources are three key tips.

Conclusion

This comprehensive report highlights the critical need for robust cybersecurity measures to counteract the growing cyber-attack threat. Each of the attacks demonstrated, from hacking into vulnerable systems to executing Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks, showcases the various methods attackers can employ to compromise systems and exploit vulnerabilities.

The controlled environment of the virtual lab allowed for a safe and educational exploration of these techniques, ensuring no real-world harm. By understanding the methods and execution of these attacks, we gain valuable insights into their prevention.

Key Takeaways:

- **Hacking Mr. Robot:** Highlighted the importance of keeping software updated, using strong passwords, and securing web applications against common vulnerabilities.
- **MITM Attacks:** Emphasized the need for strong encryption and network monitoring to detect and prevent unauthorized data interceptions.
- **DoS Attacks:** Demonstrated the impact of overwhelming a system's resources and underscored the necessity of implementing traffic management and mitigation strategies.
- **Phishing and Social Engineering:** Revealed how easily human factors can be exploited, reinforcing the importance of ongoing security awareness training for employees.