Internship Report

Prepared by: Simona Rumao 23E04-ST#IS#6248
Position: Cybersecurity Intern
Company: Supraja Technologies
Duration: Feb 2024 - July 2024
Date: 07 July 2024

INDEX

Introduction

This report documents my transformative journey as a Cybersecurity Intern at Supraja Technologies, structured across three pivotal phases aimed at equipping me with comprehensive cybersecurity skills and practical experience. Phase 1 laid the groundwork with foundational learning, Phase 2 immersed me in real-world tasks, and Phase 3 culminated in the development of the "USB Physical Security" project, showcasing my practical application of cybersecurity principles.

Company Overview

Supraja Technologies is a leading provider of cybersecurity solutions renowned for its commitment to safeguarding digital assets and enhancing security measures for clients. The company's expertise spans across proactive threat mitigation, incident response, and tailored security strategies to mitigate emerging cyber threats effectively.

Internship Objectives

Phase 1: Foundational Learning Phase 1 commenced with intensive foundational learning sessions, encompassing 31 video lectures covering essential cybersecurity concepts, tools, and methodologies. Using Kali Linux as a primary tool, I acquired proficiency in network scanning, vulnerability assessment, and penetration testing fundamentals.

Phase 2: Task Execution Transitioning into Phase 2, I applied acquired knowledge to execute diverse cybersecurity tasks. Utilizing tools such as Wireshark for network protocol analysis, Metasploit for exploitation, Nmap for network discovery, and Burp Suite for web application security testing, I honed my skills in identifying vulnerabilities and proposing mitigations.

Phase 3: Project Development In Phase 3, I undertook the development of the "USB Physical Security" project. This initiative focused on enhancing USB port security through user authentication using SQLite, enabling users to manage USB port access based on permissions while maintaining a comprehensive activity log for auditing purposes.

Tasks and Responsibilities

Task 1: SQL Injection Vulnerability Identification

- **Objective**: Find two websites vulnerable to login bypass using SQL injection payloads.
- **Process**: Conducted extensive research and used SQL injection techniques to test login forms on various websites.
- **Outcome**: Successfully identified two websites with SQL injection vulnerabilities and reported them.

Task 2: ClickJacking Attack

- **Objective**: Find a website vulnerable to ClickJacking attack and make a report.
- **Process**: Used ClickJacking techniques to test several websites and documented the findings.
- **Outcome**: Identified a vulnerable website and prepared a detailed report on the vulnerability.

Task 3: Local File Inclusion (LFI) Identification

- **Objective**: Find a website vulnerable to Local File Inclusion (LFI) and make a report.
- **Process**: Tested multiple websites for LFI vulnerabilities using various payloads.
- **Outcome**: Found a website with LFI vulnerability and documented the findings.

Task 4: Nessus Tool Network Scanning

- **Objective**: Perform different scans on the network using the Nessus tool and generate a report.
  - **a) Host Discovery Scan**
  - **b) Basic Network Scan**
- **Process**: Conducted scans using Nessus to identify network vulnerabilities.
- **Outcome**: Generated detailed reports for both scans, highlighting vulnerabilities and suggesting mitigations.

Task 5: Web Application Tests Scan

- **Objective**: Perform Web Application Tests Scan in the Nessus tool on the specified targets.
  - **a) http://testasp.vulnweb.com/**
  - **b) https://www.shoppersstop.com/**
- **Process**: Used Nessus to scan the specified websites for vulnerabilities.
- **Outcome**: Generated reports detailing the vulnerabilities found in the web applications.

Task 6: Acunetix Vulnerability Scanning

- **Objective**: Scan the specified targets using the Acunetix Vulnerability scanner.
    - **a) https://www.ebay.com/**
    - **b) https://shopping.rediff.com/**
- **Process**: Conducted vulnerability scans using Acunetix on the specified websites.
- **Outcome**: Provided detailed reports on the vulnerabilities identified.

Task 7: No Rate Limiting on Login OTP Page

- **Objective**: Perform No Rate Limiting on the login OTP page of the specified websites.
    - **a) https://www.freshbus.com/**
    - **b) https://nuego.in/**
    - **c) https://yolobus.in/**
- **Process**: Tested the OTP login pages for rate limiting vulnerabilities.
- **Outcome**: Identified vulnerabilities and prepared documentation on the findings.

Task 8: Parameter Tampering

- **Objective**: Perform Parameter(price) tampering on any two websites and prepare clear documentation.
- **Process**: Tested various websites for parameter tampering vulnerabilities and documented the process.
- **Outcome**: Successfully identified and documented vulnerabilities on two websites.

Task 9: Authentication Bypass Exploitation

- **Objective**: Perform Authentication Bypass Exploitation on any website and prepare clear documentation.
- **Process**: Used various techniques to bypass authentication on a targeted website.
- **Outcome**: Successfully bypassed authentication and documented the findings.

Task 10: Finding IP Webcams

- **Objective**: Find two IP webcams using Google Dorks and GHDB, and find the location of the IP address using the IP Geo Location Tool.
- **Process**: Utilized Google Dorks and GHDB to locate IP webcams and then used geolocation tools to identify their locations.
- **Outcome**: Successfully located and documented the IP webcams and their locations.

Task 11: Cloning Websites

- **Objective**: Using the HTTrack tool, clone any two websites.
- **Process**: Used HTTrack to clone the specified websites.
- **Outcome**: Successfully cloned two websites and documented the process.

Task 12: Sniffing Vulnerable Protocols

- **Objective**: Identify websites that have vulnerable protocols to sniff.
    - **a) FTP**
    - **b) POP3**
    - **c) HTTP**
- **Process**: Conducted sniffing tests to identify vulnerabilities in the specified protocols.
- **Outcome**: Identified vulnerable websites and documented the findings.

Task 13: ARP Poisoning Attack

- **Objective**: Perform the ARP Poisoning Attack on your local network and perform sniffing.
- **Process**: Conducted ARP poisoning on the local network and captured traffic.
- **Outcome**: Successfully performed the attack and documented the findings.

Task 14: Installation of Operating Systems in Virtual Box

- **Objective**: Generate a report on the installation of the Parrot Operating System and Ubuntu Operating System in Virtual Box.
- **Process**: Installed both operating systems in Virtual Box and documented the process.
- **Outcome**: Provided detailed installation reports for both operating systems.

Task 15: FTP Backdoor

- **Objective**: Perform an FTP Backdoor on a target website using the Metasploit tool.
- **Process**: Used Metasploit to exploit FTP backdoor vulnerabilities on a target website.
- **Outcome**: Successfully exploited the vulnerability and documented the findings.

Task 16: Email Spoofing Vulnerability

- **Objective**: Find two business mail IDs of any Pakistan organizations that are vulnerable to email spoofing attacks.
- **Process**: Researched and tested email IDs for spoofing vulnerabilities.
- **Outcome**: Identified and documented two vulnerable email IDs.

Task 17: Virus Creation and Scanning

- **Objective**: Create a virus and scan the file with the Virus Total tool. Make a report on it.
- **Process**: Created a virus file and scanned it using Virus Total.
- **Outcome**: Successfully identified the virus and reported the details.

Task 18: Trojan File Creation

- **Objective**: Create a trojan file using the NJRAT tool, scan the file with Virus Total, and report the details of security vendors who found it malicious.
- **Process**: Created a trojan file, scanned it, and documented the results.

- **Outcome**: Provided detailed findings on the trojan file.

Task 19: Vulnerable System Access

- **Objective**: Identify the hidden message in the README file, decrypt the secret data to get a link, download the OVA file, and gain access to the system.
    - **Method -1 - Crack the system password using OPH-Crack Tool and check the machine for files.**
    - **Method -2 - Perform scanning on the imported machine, check if it is vulnerable to any exploit, use the exploit to gain access, and check the machine for files.**
    - **Analyzing the Checksums: Check the files in the system, calculate the checksums, try to identify hidden data inside the tampered document, and identify the FLAG.**
- **Process**: Followed the steps to gain access to the vulnerable system and analyzed the checksums.
- **Outcome**: Successfully

Project: USB Physical Security

Overview: The "USB Physical Security" project aims to enhance USB port security by allowing users to disable and enable USB ports based on authentication. It includes the following features:

- **User Authentication:** Implemented using SQLite database for user management and authentication purposes.
- **USB Port Control:** Users can disable and enable USB ports based on their authentication status and permissions.
- **Activity Logging:** All activities related to enabling and disabling USB ports are logged in detail, providing an audit trail for security monitoring and compliance purposes.

Technologies Used:

- **Programming Languages:** [Specify the languages used, e.g., Python, JavaScript]
- **Database:** SQLite for user authentication and activity logging.
- **Security Measures:** [Describe any security measures implemented, e.g., encryption for sensitive data]

Outcome: The project successfully enhances USB port security within the organization, providing robust user authentication and detailed activity logging capabilities. It serves as a proactive measure against unauthorized data transfers via USB devices, thereby mitigating potential security risks.

Key Learnings

Key learnings from my internship encompassed both technical skills and professional development:

- **Technical Proficiency**: Mastery of cybersecurity tools and methodologies, from network analysis to penetration testing.
- **Project Management**: Experience in project lifecycle management, including scope definition, development, and deployment.
- **Collaborative Skills**: Effective teamwork and communication within multidisciplinary teams, essential for cybersecurity operations and project delivery.