Offense Project:
Exploit Demonstration Guidelines-IS493

2nd Semester 1446: 2024-2025 IS 493 Instructor: Dr. Abdulaziz Alajaji
Email: aalajaji@ksu.edu.sa

Organization

In this component of the course, students will be organized into groups, students will be organized into groups, at least (2), and maximum 3 students per group, to demonstrate an existing exploit (you are ***not*** expected to find a new novel exploit). Each group must identify an existing vulnerability with an existing exploit. Groups will be given about ten minutes to present and discuss their work with the rest of the class. In addition, the group will submit a project report explaining how the exploit works, software and systems involved, necessary steps to execute the exploit, and finally a proposed solution to prevent the exploit.

Project Setup & Timeline

- Each group is required to send an email to the instructor with their name, student IDs as soon aspossible, NO LATER than Feb 12th, 2025
- The final deadline for submitting project reports is Saturday May 3rd, 2025 midnight The presentations will be held on May 5th, 2025.
- The order of presentations will be randomly determined.
- Each Group MUST demonstrates a different vulnerability in Metasploitable 2. Once you have found a vulnerability that you can exploit, **RESERVE** it immediately (POST it in LMS in the discussion board). This will be on a first-come-first-serve bases. No two groups will be allowed to demonstrate the same vulnerability.

Resources

For this project, we will use a deliberately vulnerable Linux image called “Metasploitable 2”. The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. You can use VMWare to run the image.

Each group must select one vulnerability and exploit it. To exploit, you are expected to perform the necessary hacking activities (scanning, identifying vulnerabilities … etc.).

In order to perform the exploit, you will need an “attack” image. You can use “Kali Linux” as your attack machine. Kali Linux comes with all the tools that you would need to exploit the many vulnerabilities that exist in Metasploitable 2. Other resources can be used too. Examples include BeEF (Browser Exploitation Framework) for launching attacks against web browsers.

To recap:

- Use **Kali Linux** to find and exploit a vulnerability in **Metasploitable 2**.

Project report

- The report should discuss the following elements:
  - Vulnerability
  - How the exploit works
  - OS, Software involved
  - Network topology (if applicable)
  - Configuration
  - Proposed Solution
  - Screen shots from the different actions necessary for the exploit (scanning, execution, success … etc.)

Project presentation

- Each group is expected to demonstrate the exploit during the presentation
- Length: 7-8 minutes for presentation, plus 2-3 minutes Q&A session.
- Be prepared for questions about the exploit itself, the software involved, and the system configuration
- Evaluation mark is not necessary to be the same for all students in the same group.
- If for any reason any of your group members is not present, make sure you attend and perform the presentation.

Video Link: https://www.youtube.com/watch?v=0oOmU7IGSSE&list=PLEAkrOvgdk5RnMOqvQmMeAHl6UFJNiUcs https://www.youtube.com/watch?v=pre9yWxjjrk

https://www.youtube.com/watch?v=klNl67MT1Eo

Hint - Examples for Vulnerabilities

1. **vsftpd 2.3.4 Backdoor**
2. **UnrealIRCd 3.2.8.1 Backdoor**
3. **SQL Injection in DVWA**
4. **PHP Vulnerabilities (File Inclusion, RCE)**
5. **OpenSSH Authentication Bypass**
6. **Cross-Site Scripting (XSS) in OWASP Juice Shop**
7. **Insecure File Permissions (Various Services)**
8. **Django Default Credentials**
9. **Misconfigured NFS Shares**
10. **Remote Command Execution via Samba**
11. **Apache 2.2.8 Vulnerabilities (Including Directory Traversal)**
12. **Weak SSH Configurations (e.g., Allowing Root Login)**
13. **CVE-2010-3862: Linux Kernel Privilege Escalation**
14. **MySQL Authentication Bypass**
15. **PHPMyAdmin Default Credentials and Security Issues**
16. **Brute Force Attacks on OpenSSH**
17. **SNMP Community String Vulnerability**
18. **Insecure LDAP Configuration**

19. **Command Injection in various applications**
20. **Open Port Vulnerabilities**

Note: This is only a guide using a publicly available sources. The idea is to run the VM machine and explore on your own. Not every listed vulnerability is guaranteed to be useful, and you're free to use options not included in the list. You're also encouraged to try the latest version of Metasploitable. I hope you enjoy the thrill as well.

Structure for Each Report

For each vulnerability, consider the following structure:

- **Introduction**: Overview of the vulnerability.
- **Technical Details**: Description of how the vulnerability operates.
- **Exploitation**: Steps to successfully exploit the vulnerability.
- **Impact**: Consequences of exploitation and potential damage.
- **Mitigation and Prevention**: Best practices to secure against the vulnerability.