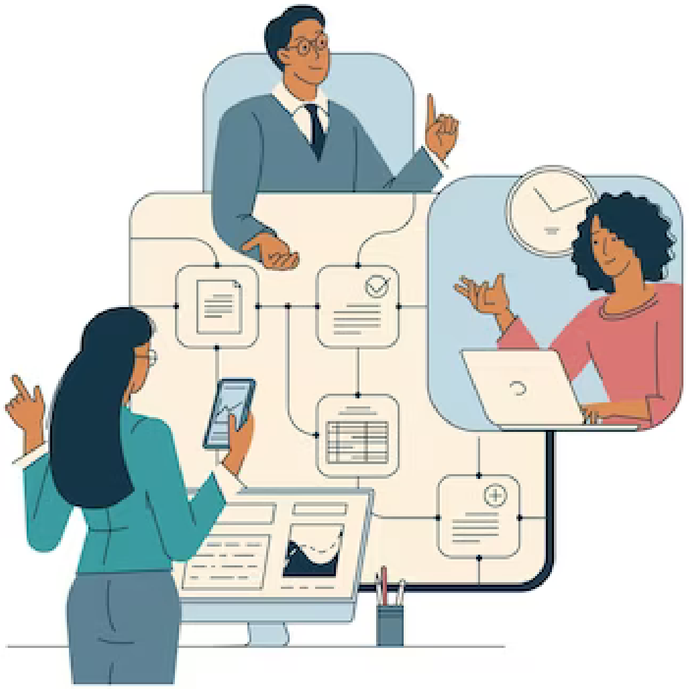
PENETRATION TESTING ON NETWORK PORT

Advisor: Chhim Bunchhun

Presentor: **Ly Sophavin**

FACULTY OF ENGINEERING

TABLE OF CONTENT



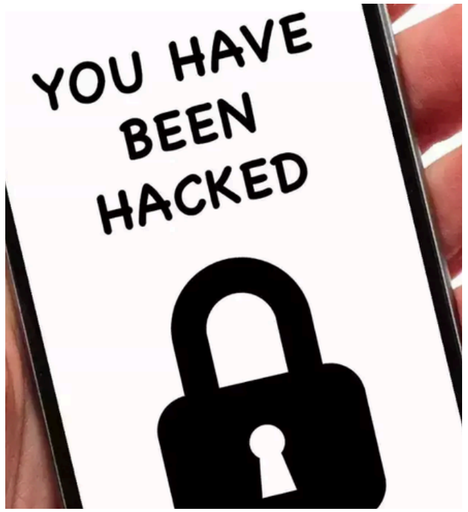
FACULTY OF ENGINEERING

1. INTRODUCTION

Nowadays, as web applications provide more functions, web vulnerabilities are also increasing. This project aims to demonstrate how these vulnerabilities work and how to prevent them to enhance security. It incorporates OWASP references and focuses on pentesting vulnerabilities in Metasploitable 2.

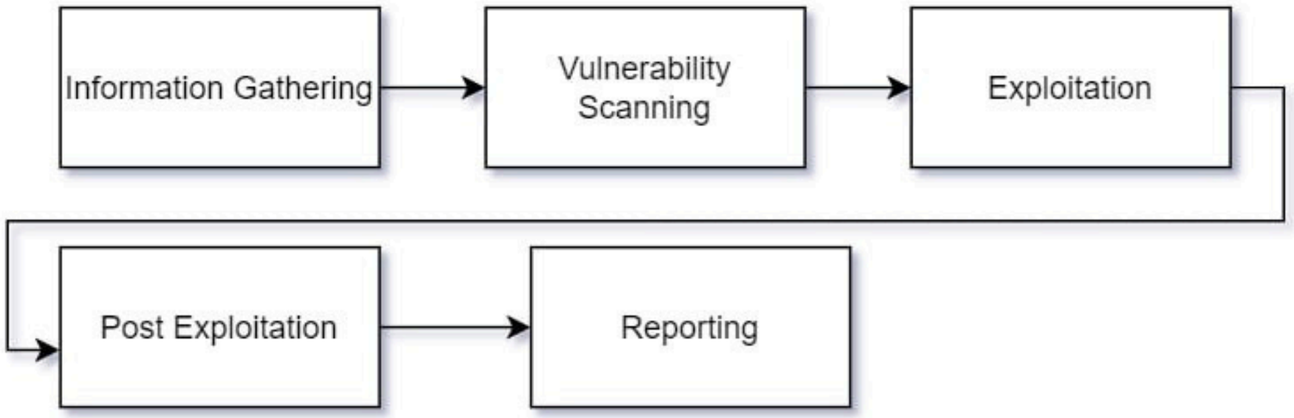
2. PROBLEMS

As organizations rely more heavily on technology, the complexity of IT infrastructures and applications has grown. This increase in complexity has led to more potential entry points for attackers.



FACULTY OF ENGINEERING

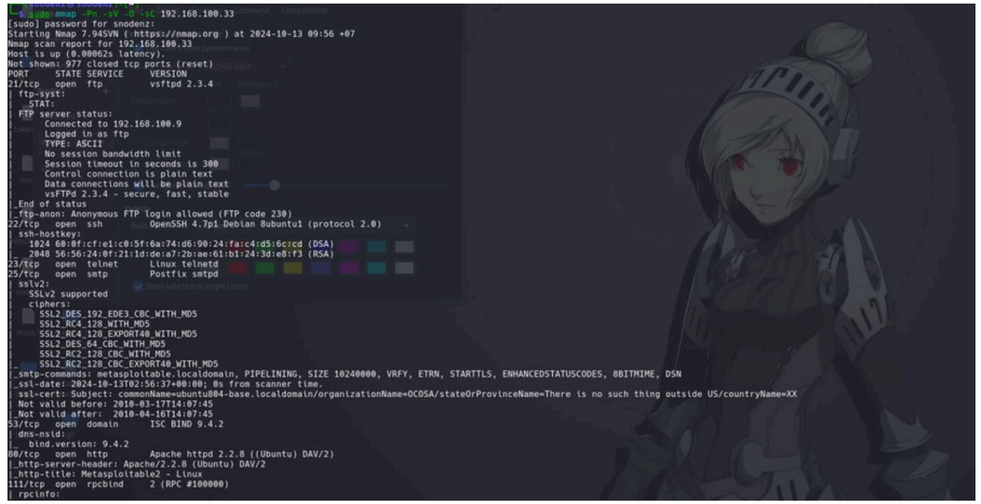
3 . METHODOLOGY



FACULTY OF ENGINEERING

1. INFORMATION GATHERING

Information gathering, also known as reconnaissance, is the process of collecting as much information as possible about the target system, network, or application, Here am using nmap to collect some open port



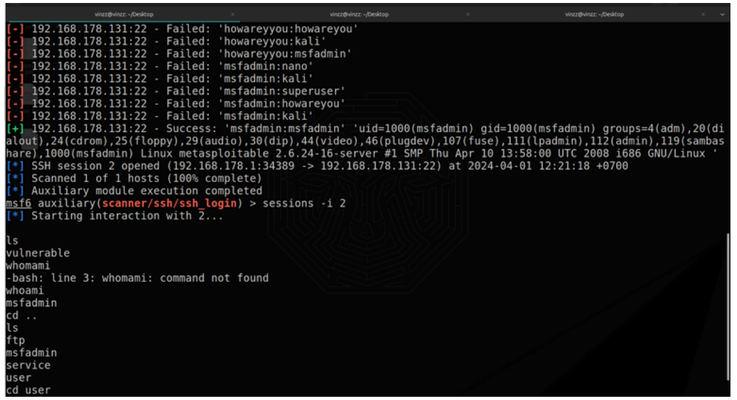
2. VULNERABILITY SCANNING

Vulnerability scanning identifies known vulnerabilities, lack of security controls, and common misconfiguration within systems on a network. Penetration testing simulates an attack to exploit weaknesses in order to prove the effectiveness of your network's security.

FACULTY OF ENGINEERING

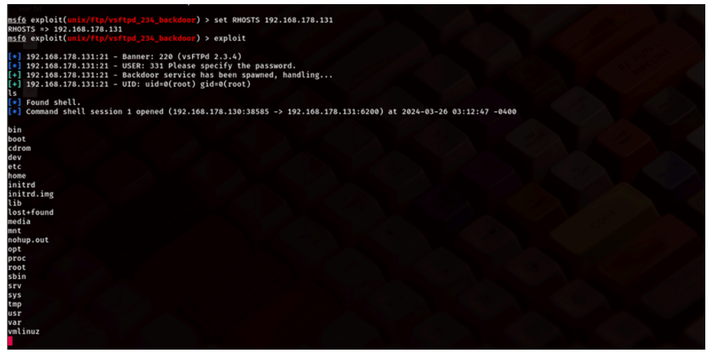
3. EXPLOITATION

The exploitation phase of a penetration test focuses on gaining access by bypassing security restrictions. If vulnerability analysis was done properly, this phase is a precise, planned effort to find entry points and high-value assets.



4. POST EXPLOITATION

Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network.



FACULTY OF ENGINEERING

5. REPORTING

This section outlines the goals of the Penetration Test and summarizes key findings. It is intended for those overseeing the security program and anyone affected by the identified threats.

4. TOOLS AND TECHNOLOGY

KALI

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

NMAP

Nmap (Network Mapper) is a free and open-source network scanning tool used for network discovery and security auditing. It's one of the most widely used tools for network reconnaissance and vulnerability assessment.

FACULTY OF ENGINEERING

METASPLOITABLE 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

METASPLOIT FRAMEWORK

The Metasploit Framework is an open-source penetration testing and exploitation toolkit developed by Rapid7, a cybersecurity company. It provides security professionals, ethical hackers, and penetration testers with a comprehensive platform for conducting security assessments, exploiting vulnerabilities, and testing defenses.

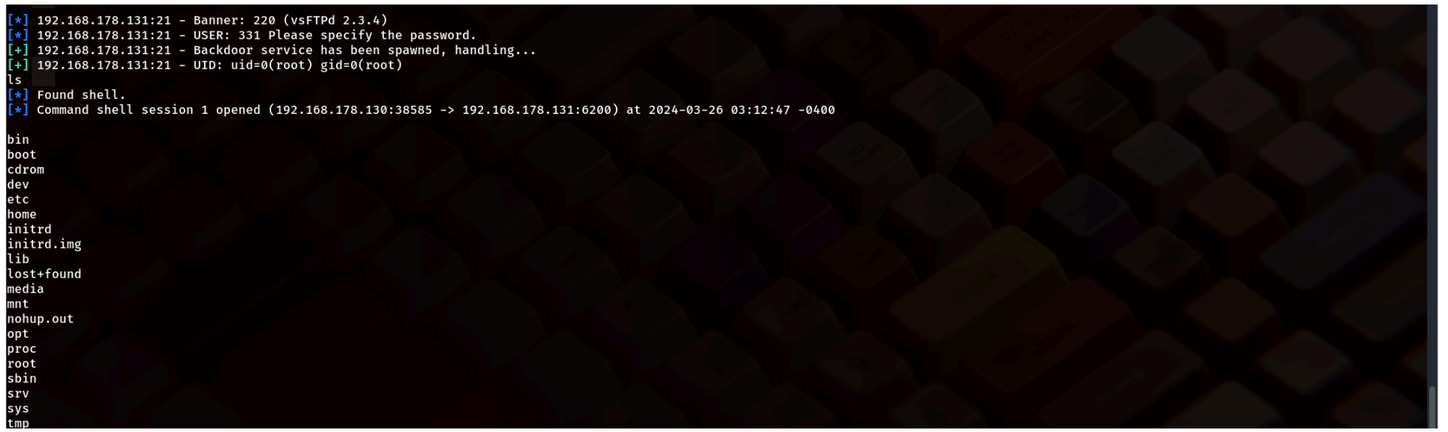
RAPID7

Metasploit

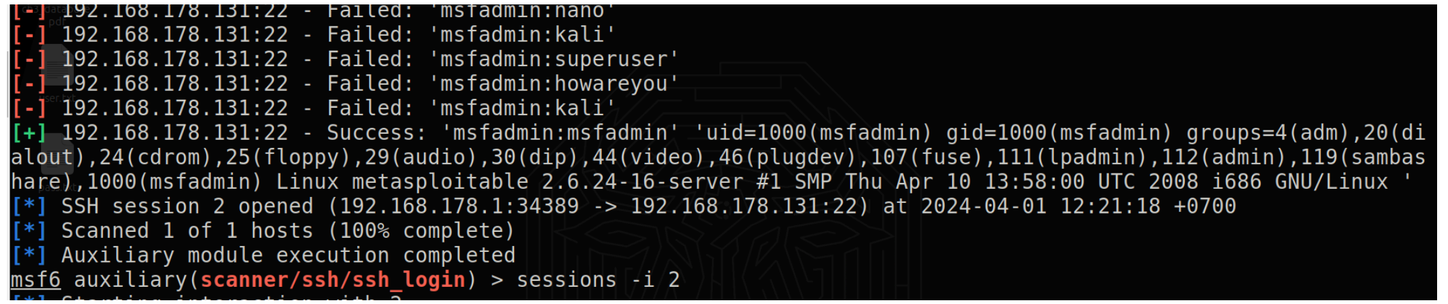
FACULTY OF ENGINEERING

5 . RESULT

FTP



SSH



SMB

```
[*] Started reverse TCP handler on 192.168.178.132:4444
[*] Command shell session 1 opened (192.168.178.132:4444 → 192.168.178.131:38277) at 2024-04-22 00:38:22 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

FACULTY OF ENGINEERING

5 .CONCLUSION

In conclusion, the penetration testing conducted on ports 21, 22, and 139 has provided valuable insights into the target system's security posture, highlighting areas of vulnerability and suggesting recommendations for improving security measures. Continued vigilance, regular security assessments, and proactive mitigation of identified risks are crucial for maintaining a robust defense against potential threats.

THANK YOU !