Assignment 2

I used a file in github, where I can't find any vulnerable windows xp machine.

I tried to get vm image file of windows xp vulnerable machine. But I couldn't make it.

But below is the process of same thing that how we need to perform a exploit in windows xp.

Objective: Use the Metasploit Framework to exploit a known vulnerability on a virtual machine (such as the MS08-067 vulnerability in Windows XP). Document the exploitation steps.

Penetration Testing - MS08-067 Exploit

Overview:

In this project, I performed a full penetration testing workflow targeting a vulnerable Windows XP system on a simulated internal network. After discovering the machine through Nmap scanning, I identified an exploitable vulnerability (MS08-067) using Nessus, then leveraged Metasploit to gain remote code execution and extract key files from the system.

Tools & Technologies:

- **Nmap** - Network Scanning and OS detection
- **OpenVAS** - Vulnerability Assessment
- **Metasploit** - Exploitation and post-exploitation
- **Kali Linux** - Attacker machine
- **Windows XP SP3** - Target machine

Objective / Scenario:

The goal was to simulate a real-world penetration test by identifying a vulnerable system, performing reconnaissance and enumeration, scanning for vulnerabilities, exploiting one, and retrieving proof of access by retreiving specified flags in the system.

Target IP: 11.11.0.13 **Operating System:** Windows XP SP3

Methodology

1. Network Scanning with Nmap

I followed a standard netwrok scanning procedure using Nmap on a Kali Linux virtual machine. Commands are listed below:

```
Nmap -sS -O -v 11.11.0.1/24
```

I combed through the list that was returned until I found the IP that was associated with the target WIndows XP machine. Below is the full report for the Windows XP system, including the ports and statuses.

Nmap scan report for 11.11.0.13

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows Netbios-ssn
445/tcp	open	Microsoft ds	Microsoft Windows XP Microsoft ds
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

Microsoft Windows XP SP3

2. Vulnerability Scanning with Nessus

Once I identified the system I wanted to exploit, I used Nessus to scan for vulnerabilities. There were 25 vulnerabilites on 11.11.0.13. I selected exploit: MS08-067 - Windows Server Service Crafted RPC Request Handling Remote Code. This vulnerability allows remote code execution by sending a specially crafted RPC request to the svchost.exe process on vulnerable Windows systems.

3. Exploitation with Metasploit

I started Metasploit and used the code below to begin the exploitation attempt:

```
use exploit/windows/smb/ms08_067_netapi
```

I specified the target IP I wanted to exploit:

```
set RHOST 11.11.0.13
```

then used the **Exploit** command to begin.

4. Post-Exploitation: File Retrieval

I navigated the file system using the shell commands listed below:

```
cd "Documents and Settings"

cd Administrator/Desktop

ls
```

Listed were three files:

flag0.txt

fruit.jpg

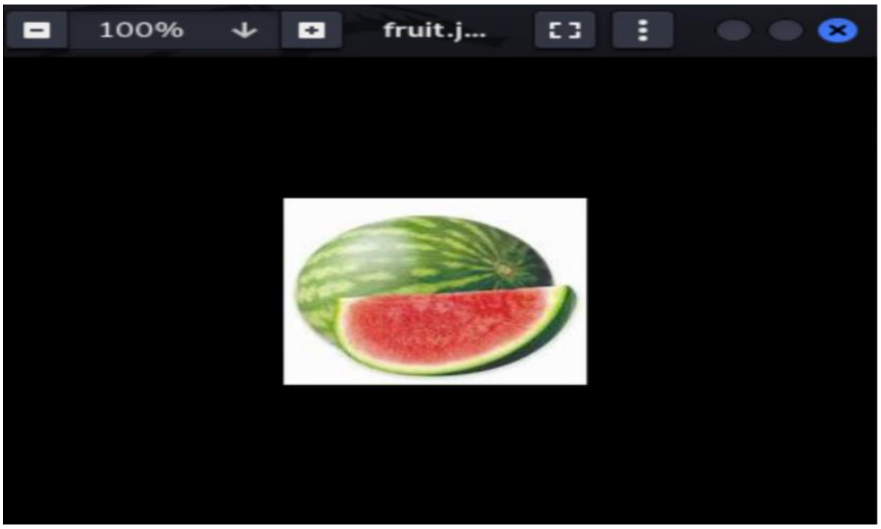
README.txt

I accessed all three using the cat command. The contents of the files will be listed below:

Flag0.txt: Gabaski

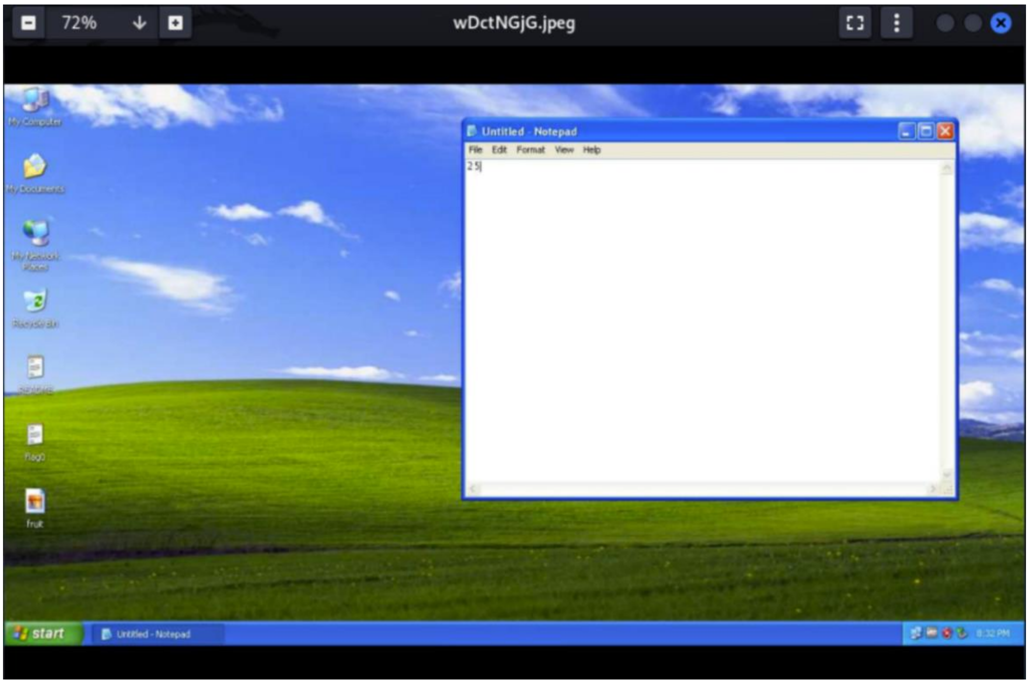
README.txt: Do not delete or add anything in this machine. Do not patch any vulnerabilites. Other people are using this machine for their project.

fruit.jpg:



I used the download command on the fruit photo and I used the screenshot command to take a screenshot of the

Administrator's desktop which is shown below:



25