# Penetration Testing Manifest

|  |  |
| --- | --- |
| Penetration Tester | Gregory Kukanich – UIN: 01078189 |
| Scanning periods | 2/15/2021 |
| Tools | Nmap 7.80; Metasploit Framework 5.0.70-dev; |
| Scope | Nmap scan was used to identify open ports and the services that were running on those ports. Using the information gathered from the scan about the services, plans for how to gain access to the system can be formulated. |
| Description | The purpose of this lab is to find vulnerable services running on a system and to use these vulnerabilities to gain access to the system. The impact is to demonstrate how these vulnerabilities can be catastrophic for a system by allowing unauthorized users a way to gain access to the system. |

**Penetration Test Lab Report**

**Why do we need to assign an internal IP address (i.e., behind NAT) for Metasploitable 2 Linux machine? What will happen if we assign a public IP to it?**

There are two reasons why we assign an internal IP address to Metasploitable 2. The first is so that we can connect to it from the other virtual machine we are using Kali Linux and the second reason and the more important one is that Metasploitable 2 is designed to contain numerous amounts of known vulnerabilities. If you were to assign Metasploitable 2 a public IP address and an attacker discovered this they could use the vulnerabilities shipped with Metasploitable 2 to gain access to your network. By only allowing Metasploitable 2 to have access to the local network you can still conduct penetration tests from another local system and not risk exposing your entire network to an attack.

**Executive Summary Scope**:

It is important to always ensure that your systems are safe and secure. A computer system that is vulnerable to attacks can be an entry point for an attacker to an entire network. Having open ports with outdated or vulnerable services running can be a way for an attacker to gain access to a system/network. In this report I detail the steps I took while performing reconnaissance of the system looking for vulnerabilities as well as the steps I took after to exploit the vulnerabilities that were found.

# Approach:

To start I performed an Nmap scan to identify what ports on the target system were open and what services were running on those ports. I did this using the following command “nmap -p1-65535 -A

Text

Description automatically generated10.0.2.4”.

Text

Description automatically generated

Text

Description automatically generated

Looking at the scan results there were a number of open ports discovered and some of these ports have vulnerable services running. For example, port 21 was open and was running a FTP server Vsftpd 2.3.4 which is vulnerable to a backdoor attack. Some of the other ports/services of interest were telnet on port 23 which is vulnerable to an attack that would return the banner for the system which includes the username and password for an account. Port 445 was running a version of samba that is vulnerable to a command execution attack and finally port 6667 is running a version of UnrealIRCd that contains a backdoor vulnerability.

Text

Description automatically generatedAfter analyzing the Nmap scan results I decided to focus my attention on the ports/vulnerabilities discussed above. I began my penetration testing with the Vsftpd service running on port 21. Using Metasploit Framework console (msfconsole) I searched for exploits for the Vsftpd service, the only vulnerability available in the msfconsole was “vsftpd\_234\_backdoor” this is an exploit for the same version of Vsftpd running on the target system. I set the host to the target machines IP address of “10.0.2.4”, I selected the payload to use and then used the “exploit” command in msfconsole to start the attack.

As you can see in the screenshot above the backdoor exploit was successful and I was able to establish a command shell session with the target system. I was able to access the root account of the system. If I were an actual attacker lots of harm could have been done. This is a huge vulnerability and a big risk for the system that needs to be fixed.

Graphical user interface, website

Description automatically generatedAfter a successful first attack I moved onto the next port/service of interest which was telnet running on port 23. Using an auxiliary module from the msfconsole I was able to retrieve a banner from the target system. This banner contained the Username/Password for a sudo privileged user.

With this login information I can now use telnet to connect to the system.

As seen above I was able to remotely connect and login to the msfadmin user with the credentials that were obtained using the msfconsole. From here I would again be able to wreak a lot of havoc on the target system as I can run commands as root.

# Text Description automatically generatedThe next port/service I attempted to exploit was port 6667 which was running UnrealIRCd. Using the msfconsole I searched for an exploit to use and decided on “unreal\_ircd\_3281\_backdoor”. After selecting this exploit, I again set the targets IP address as the host.

# 

# I then began to execute the exploit, after a short period msfconsole was able to establish a command shell session with the target system. I once again had access to the target system as the root user.

# Text Description automatically generated

# To show just how dangerous this vulnerability is I used the command shell that was opened to create a file named after myself in the /home directory of the target system.

# Graphical user interface Description automatically generated with medium confidence

# Above is the creation of the file from the command shell opened in msfconsole on Kali Linux. Below is another screenshot of the same file but from the target system just to show that I was in fact able to remotely connect and create a file.

# While this example was just the creation of an empty file in my name it shows what type of access, I was able to gain using the exploit found in the msfconsole.

# Text Description automatically generatedFinally I targeted one last port/service which was port 445 running samba. I again searched msfconsole for available exploits regarding samba and decided to use “usermap\_script” which will allow me to execute commands if successful.

# After again setting the target systems IP address as the host I began running the exploit for samba. Once again I was able to successfully create a command shell session as the root user on the target system. I created another empty file in the home directory to show the access I had gained to the system.

# Text Description automatically generated

# Text Description automatically generated

# As you can see from the screenshot above taken on the target system I was indeed able to create another empty file in the /home directory. There are now two different files I added while remotely accessing the system using the vulnerabilties discovered.

# Findings:

# The penetration testing that was conducted shows that the specified target system is extremely vulnerable to a wide range of different attacks as demonstrated in this report. These vulnerabilities could have catastrophic consequences if not fixed immediately. My recommendation to the IT department is to fix all of the vulnerabilities outlined in this report as well as to begin regularly conducting internal vulnerability scans of this system and any other systems. New techniques and exploits are developed every day and not keeping your systems security up to date can result in an attacker gaining unregulated access to a system or the entire network with dire consequences.