Notes from Exploring Vulnerabilities

Instructions

Make a copy of this document, rename it to "exploring-vulns-notes" and move it to your CSE 523 Google Docs collection. If at any point in this exercise you feel stuck, raise your hand and get some guidance. When you reach each GATE below, switch over to the Tracking Progress document and update your position. Try to be efficient with your time.

GATE 1

Overview

Today we will explore how to scan machines and networks in Metasploit. Keep detailed notes below (place your comments in between the provided horizontal lines); you will be referring to these in the future to do your work.

Part 1: Setting up your VMs

For this activity, you will be using the same network of two VMs in ONL that we have used for the previous few exercises. Boot up your cse523 Ubuntu virtual machine.

At this point, you can get started with the normal configuration steps for our VMs in ONL. If you need a reference, follow the instructions of exploring-msploit-notes to the point where `config.sh` has been run inside of each VM.

These two VMs will be referred to as VM1 and VM2 for the rest of the exercise. VM1 does not require any additional setup. VM2 needs to be configured to run as a VirtualBox container for Windows XP.

Log into VM2 with X-forwarding. Record VM2's data interface IP address:

Start virtualbox with:

```
sudo virtualbox
```

Click settings, then go to Network. Open the "Advanced" area of Adapter 1's settings. It should say that the adapter is attached to NAT.

After verifying this, click on "Port Forwarding". Add two new rule entries that sets the host port and guest port to 445 on both TCP and UDP. This VM setup emulates a single XP machine attached to a Linux router, where the smb ports are being forwarded. Next, close the Port Forwarding and Settings windows and start the Windows XP VM.

For the rest of the exercise, leave the VirtualBox windows open, and do nothing else in VM2's terminal window until instructed to do so. Open a new terminal window and log into VM1, and then record VM1's data interface IP address:

GATE 2

Part 2: Using nmap

Go to your VM1 terminal, and run nmap, a network scanner, with the following command (change the target IP address to match VM2):

```
sudo nmap -O -v -sV 192.168.1.1
```

Here are the details on the options:
-sV: Probe open ports to determine service/version info
-v: Increase verbosity level (use twice or more for greater effect)

Copy the nmap output you see below, between the two horizontal lines.

Now, start metasploit with the following command:

```
sudo msfconsole
```

After a few minutes of waiting for msfconsole to finish, use the following command to check your database status:

```
db_status
```

If the result is anything other than "[*] postgresql connected to msf3", then there is probably an issue with your database install, and you should contact the TA. Otherwise, continue on with:

```
db_nmap -O -v -sV 192.168.1.1
```

When the command is complete, enter `hosts` on the command line and copy the output below.

Now enter `services` on the command line and copy the output below.

GATE 3

Part 3: Refining our knowledge

It turns out we can easily learn more about our target machine. Use the following transcript as a guide at your own msfconsole window (using VM2’s IP as the target IP).

```
msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) > set RHOSTS 192.168.1.1
RHOSTS => 192.168.1.1
msf auxiliary(smb_version) > set SMBDirect false
SMBDirect => false
msf  auxiliary(smb_version) > run
```

When the command is finished running, enter `hosts` on the command line and copy the output below.

Now enter `services` on the command line and copy the output below.

To get out of the smb_version auxiliary module, enter `back` at the console.

GATE 4

Using your favorite search engine, find out what SMB is.
Briefly describe it here:

GATE 5

From the Metasploit documentation, find out what this command is doing:
(be sure you describe what the smb_version scanner does.)

```
msf > use auxiliary/scanner/smb/smb_version
```

Briefly describe it here:

GATE 6

Now that you know how to scan with metasploit, if you want to experiment some more on your own, you can use Google (or your favorite information search service) to find metasploit vulnerabilities that match the system and service versions you have identified. Keep in mind that you may have to add additional ports for exploits to work correctly. For example, in exploring-msploit-notes we had to add a port forwarding rule for 135 for it to work in ONL, and here we had to add a similar rule but for port 445.

COMPLETE