Lab 8: Armitage

Armitage provides an open source GUI front end to Metaploit and supports the security testing against a range of vulnerabilities. We will mainly be using your **Kali** instance and a **Windows 2003** target. We will take the basic steps of: Scan, Exploit and Gathering.

A Setting up

1. On Kali, first start the PostgreSQL database management and metasploit services:

```
service postgresql start
service metasploit start
```

2. Next run Armitage:

```
armitage
```

Look back at previous labs, can you find the following:

Double-click on **auxillary → exploit → browser → webview_addjavascriptinterface**

What is the version of Android that is affected by this vulnerability? What the parameters used with the exploit:

B Host discovery

3. Next we will try and discover some of the hosts on the network with an ARP sweep:

auxillary → scanner → discovery → arp_sweep

What is the generated Metasloit script (looking in the console window for the script generated): Which hosts did it discover, and what are their details:

3. For one of the hosts found (do not select 10.200.0.1), now do a port scan:

auxillary → scanner → portscan → tcp

What is the generated Metasloit script (looking in the console window for the script generated): Which ports did it discover:

4. Next we will try and discover some Windows instances. For this run the nbname scanner:

auxillary → scanner → nbname

What is the generated Metasloit script (looking in the console window for the script generated): Which hosts did it discover, and what are their details:

5. Next we will try and discover some Windows instances which are sharing with SMB. For this run the nbname scanner:

auxillary → scanner → smb_version

Define the SMB hosts on the network, and their operating system: Which port does SMB use?

6. Now for one of the Windows instances you have found, run a TCP scan just on that instance:

Auxillary → scanner → portscan → tcp

Next right-click on the host in the main windows, and select **services**. Which services are running (Figure 2):

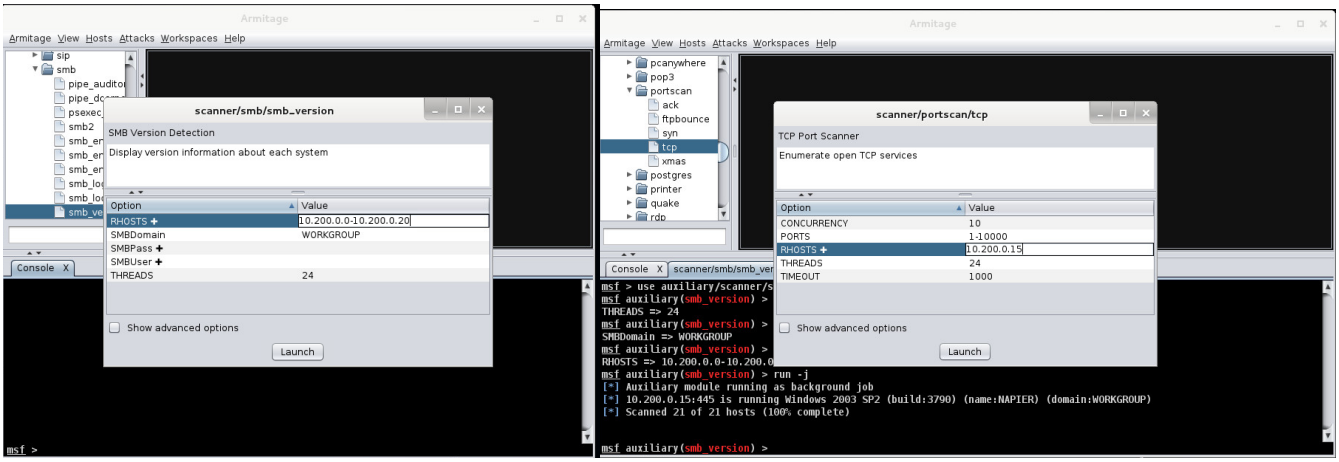

Figure 1:

C Running an Exploit

7. The SMB service on Windows 2003 can be susceptible to MS08-067. Select the following and run it against your Windows 2003 instance (Figure 2):

Exploit → windows → smb → ms08_067

Outline the MS08-067 vulnerability:

Which are the parameter used in the exploit, and outline its Metasploit script:

What indication that you get that the instance has been compromised:

How the icon on the main window changed? If so what does it look like?

8. Next run the Meterpreter Shell (Figure 3).

In the console window, can you type Meterpreter commands. If so, get the following information:

```
Getsystem:

Getuid:

Getsid:
```

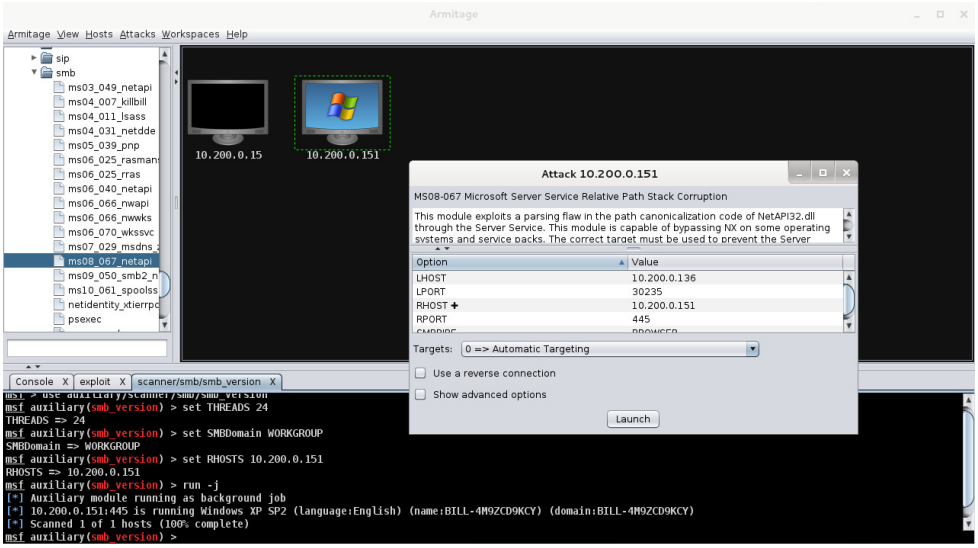

Figure 2: MS08-067

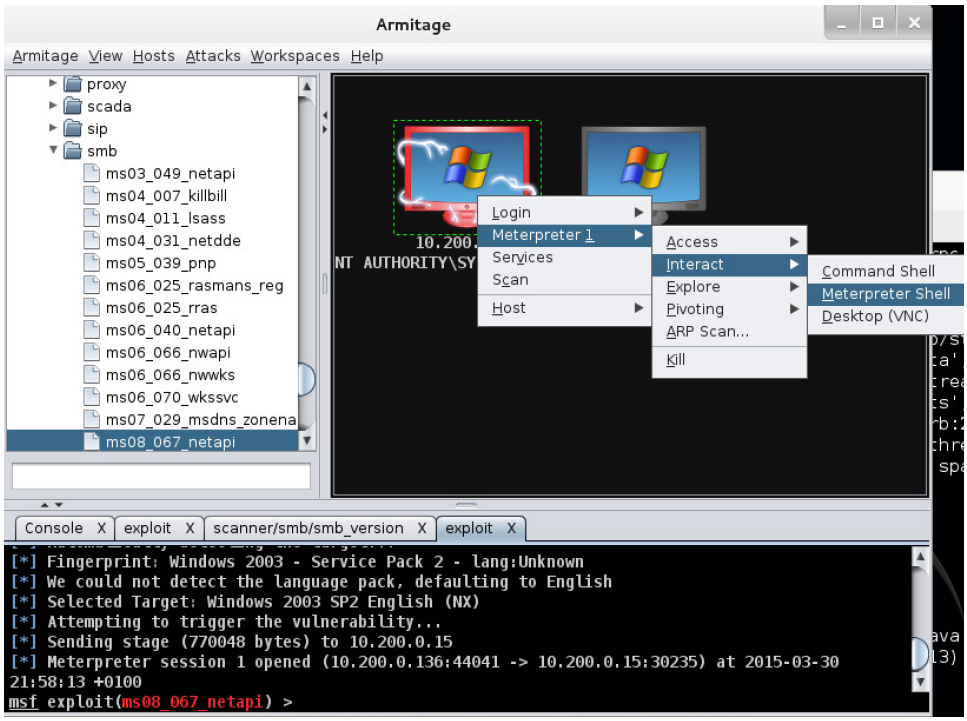

Figure 3: Running the Meterpreter Shell

9. Next we will grab the username database and use John the Ripper to crack them (Figure 4):

```
Hashdump
```

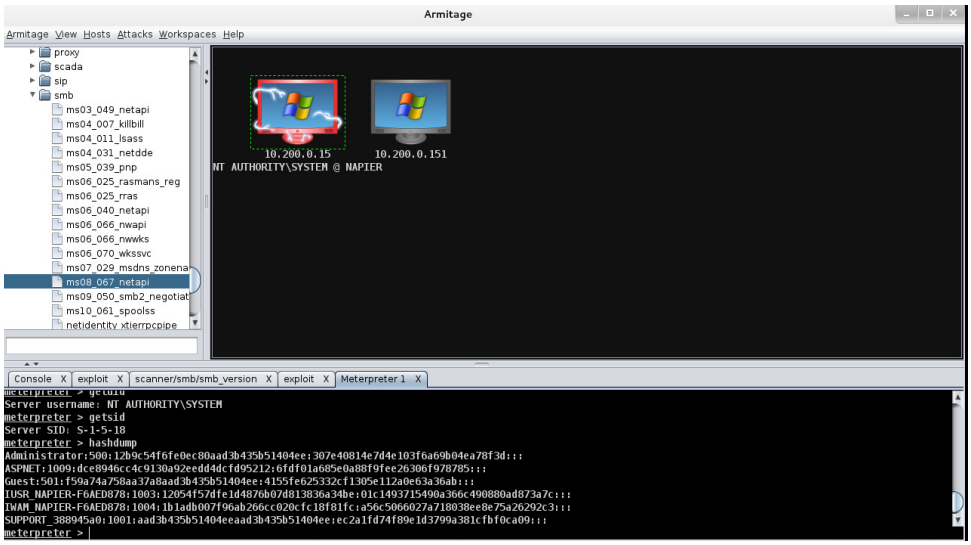

Figure 4: Hashdump

10. Get your lab partner to log into your Windows 2003 target. Now using the Administrator details for Windows 2003, connect to the server with psexec, perform the following:

Now right-click on the compromised Windows 2003 in Armitage, and capture a screen shot (left side of Figure 5). Was it successful?

Now right-click on the compromised Windows 2003 in Armitage, and Show the processes. What are some of the processes running:

Now right-click on the compromised Windows 2003 in Armitage, and browse the files. What are the folders in the top level of c:

Now right-click on the compromised Windows 2003 in Armitage, and capture key strokes. Ask your lab partner to key some keys and see if you can recover them: Which file was used to store the key strokes?

Now right-click on the compromised Windows 2003 in Armitage, and from Meterpreter -> Interact -> VNC. Armitage will tell you the IP address and port to connect to. Next open a terminal any enter the command:

vncviewer [IP]:port

Can you connect to the remote instance?

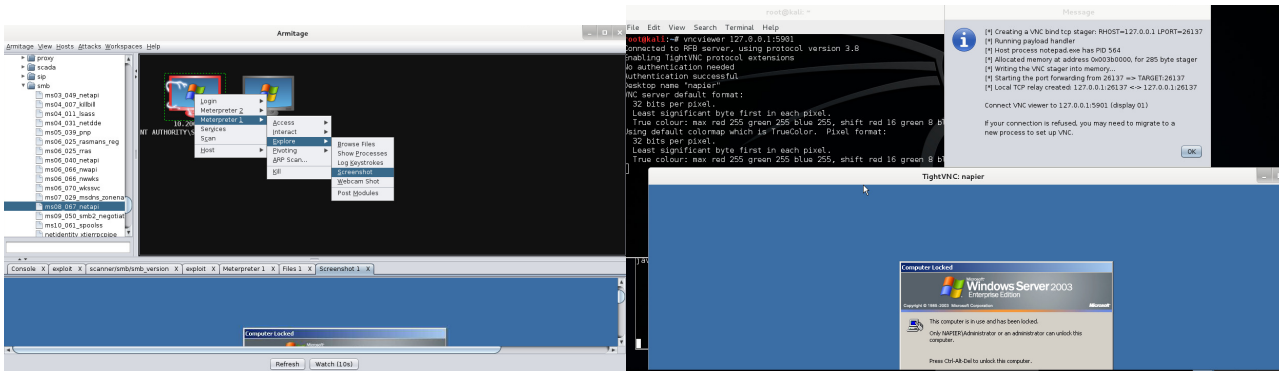

Figure 5: Screenshot and VNC Connection

D Gathering information

11. Next we can setup a compromise to determine the details of the instance. First run the following:

Post → Windows → Gatherer → CheckVM

Is the instance a virtual machine:

Run an ARP scan across 10.200.0.10 to 10.200.30 from the compromised instance:

Post → Windows → Gatherer → Arp_scanner

Which nodes and MAC addresses did it find:

Now run a netstat on the compromised node:

Post → Windows → Gatherer → tcpnetstat

Outline some of the ports that are open:

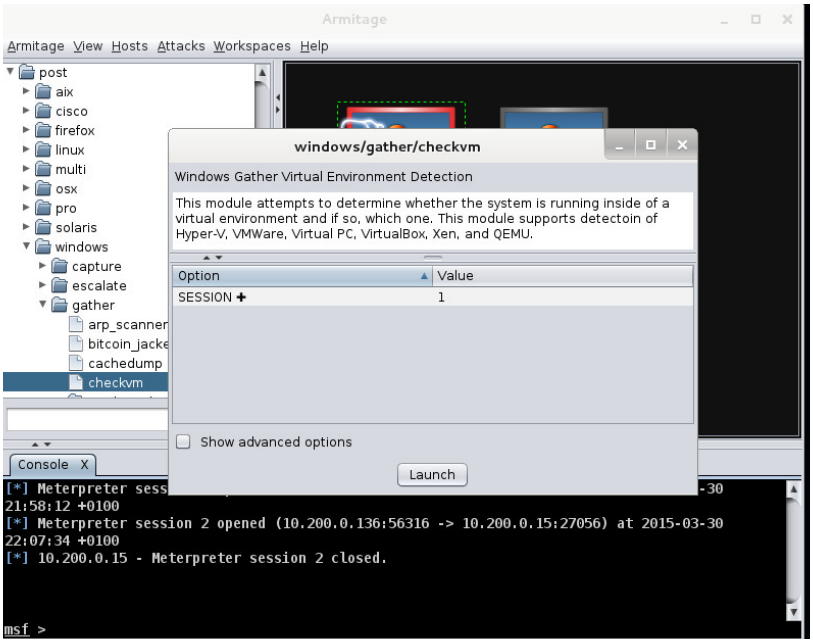

Figure 6: Check if VM

Next run the following and gather information:

Module	**Information gained**
Post/Windows/Gatherer/enum_ie	
post/windows/gather/credential_collector	
post/windows/manage/migrate	
post/windows/gather/dumplinks	
post/windows/gather/enum_applications	
post/windows/gather/enum_logged_on_users	
post/windows/gather/enum_shares	

post/windows/gather/usb_history	
post/windows/capture/keylog_recorder	

12. Next ask your lab partner to add a new user on the Windows 2003 instance, and see if you can delete it with:

post/windows/manage/delete_user

Complete the following if you did not complete it in the previous lab:

E Examining Firmware

There can be a great deal of information that can be gained from examining the firmware of a device. On Kali, download this firmware:

https://dl.dropboxusercontent.com/u/40355863/51.3.0.152.rar

First examine the firmware with binwalk:

```
binwalk 51.3.0.152.bin
```

Which folders are contained in the firmware:

Next, on Kali, extract to a ZIP file and then extract the image:

```
dd bs=1 skip=36  if=51.3.0.152.bin of=image.zip
unzip image.zip
```

Now find the daemon.v5.5 file in the folders created, and list its contents with:

```
cat daemon.v5.5
```

Can you locate the line with /etc/password?

Can you extract the /etc/password entry and use John the Ripper to determine the password:

Use the following commands to determine some information:

```
cat /proc/version
cat /proc/cpuinfo
```

OS Version:

CPU Type:

Find the ipcam.sh file and determine which processes it starts: