# CIS 480 Metasploit Project

|  |
| --- |
| * This is an individual assignment. * The due date is Tuesday, December 5, 2017 4:00 (sec01) /7:00 (sec76). * For this assignment, you will need to use Kali and Metasploitable2. * Follow the usual naming convention. |

# 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>
  + 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 in 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

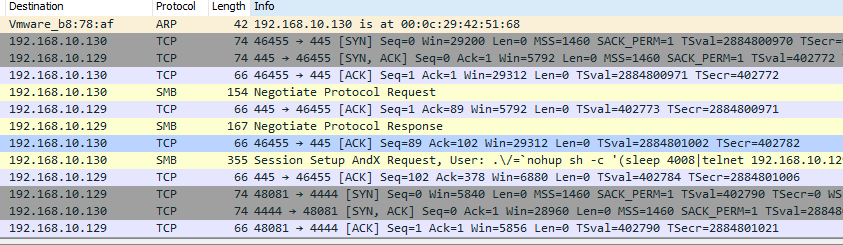
## Task 1 (10 points). Exploiting Samba, CVE20072447: Remote Command Injection

* 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.
* *If the requested screenshots are not provided, the grade for this task will be zero.*

1.1 (3 points) Explain Samba and the vulnerability associated with CVE 2007-2447.

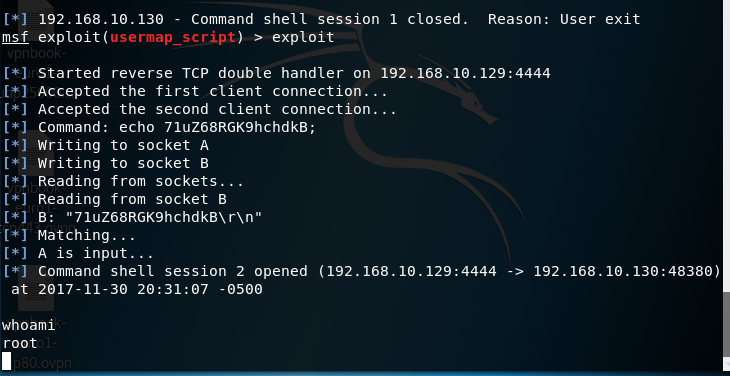
Samba is a free software that uses SMB (server message block protocol) to allow the ability to file share and remote print amongst computers in a network. The vulnerability allows remote attackers to exploit the usermap\_script and gain command shell root access to the machine.

1.2 (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 think the SMB packet with length 355 has the exploit code. This is because the info includes session setup and the user is a set of symbols and command string.

1.3 (3 points) Execute whoami (p. 24) and display the result in a screenshot.



## Task 2 (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.
* *If the requested screenshots are not provided, the grade for this task will be zero.*

2.1 (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 goal of this task is to exploit the shared file system on metasploitable. By following the steps associated with network file system protocal, rpcbind, and ssh daemons. You will be able to gain root access to metasploitables shared file system.

2.2 (3 points) Explain each of the following protocols and their roles in the task: NFS (network file system), rpcbind, and SSH.

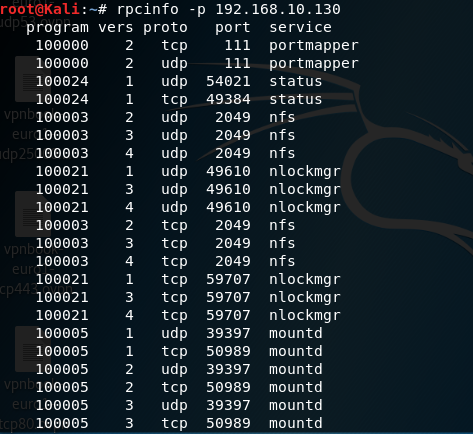
NFS is what makes the rest of the exploit possible. Showmount is used to know if the network file system is mountable to the world, which it is. Rpcbind directs client to proper port number to communicate with the requested service. This allows rpcinfo command to show all the RPC problems that are running. Once you create a ssh pair key and add it to the authorized\_keys file on metasploitable. You then can use the SSH command to gain root access to the shared file system on metasploitable.

2.3 (4 points) Interpret the following command lines. You have to explain all the switches associated with the commands as well. Display the results in screenshots.

(p. 14) rpcinfo -p 192.168.1.112

**rpcinfo:** shows all the rpc problems that are running on the server.

**-p:** Probe rpcbind on host using version 2 of the rpcbind protocol, and display a list of all registered RPC programs. If host is not specified, it defaults to the local host.



(p. 15) showmount -e 192.168.1.112

**showmount:** is used to know if the filesystem is mountable to the world by querying the state of the NFS server.

**-e:** prints a list of the files that are shared or exported.



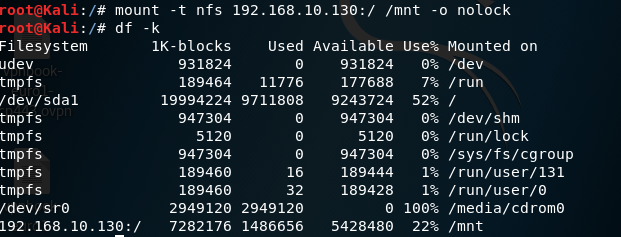
(p. 17) mount -t nfs 192.168.1.112:/ /mnt -o nolock

**mount:** to connect to the filesystem of metasploitable.

**-t:** file tree.

**nfs:** specify mounting nfs file system on host.

**/mnt –o nolock:** local mount point and specifies mount option nolock, which disables file locking.



(p. 19) ssh -i /root/.ssh/hacker\_rsa root@192.168.1.112

**ssh:** to start the ssh remote session.

**-i:** forces to use identity file where the key is read (hacker\_rsa)

**root@:** give yourself root access at the specified host.

