OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 – Password Cracking

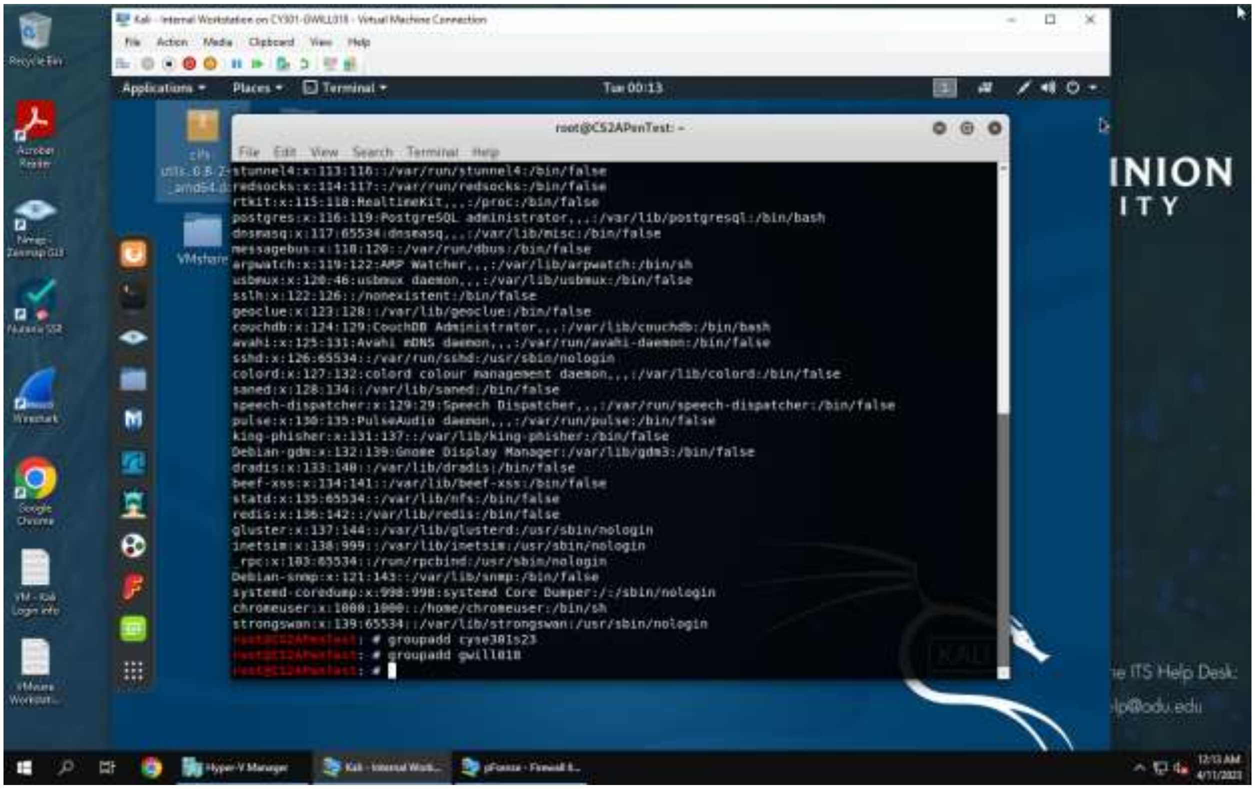
Gavin Williams

01230006

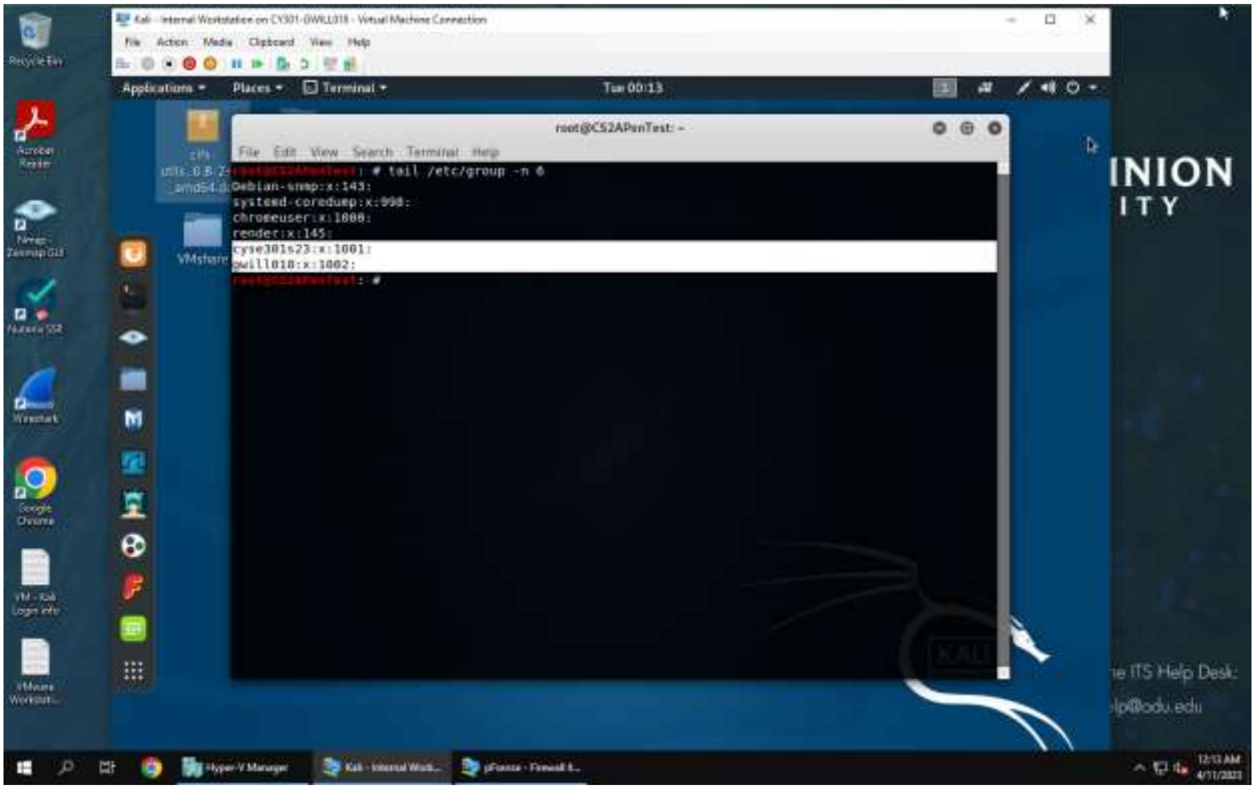
PART A

Task A: Linux Password Cracking (25 points)

1. 5 points. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.


Kali - Internal Workstation on CY301-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 00:13
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall &...

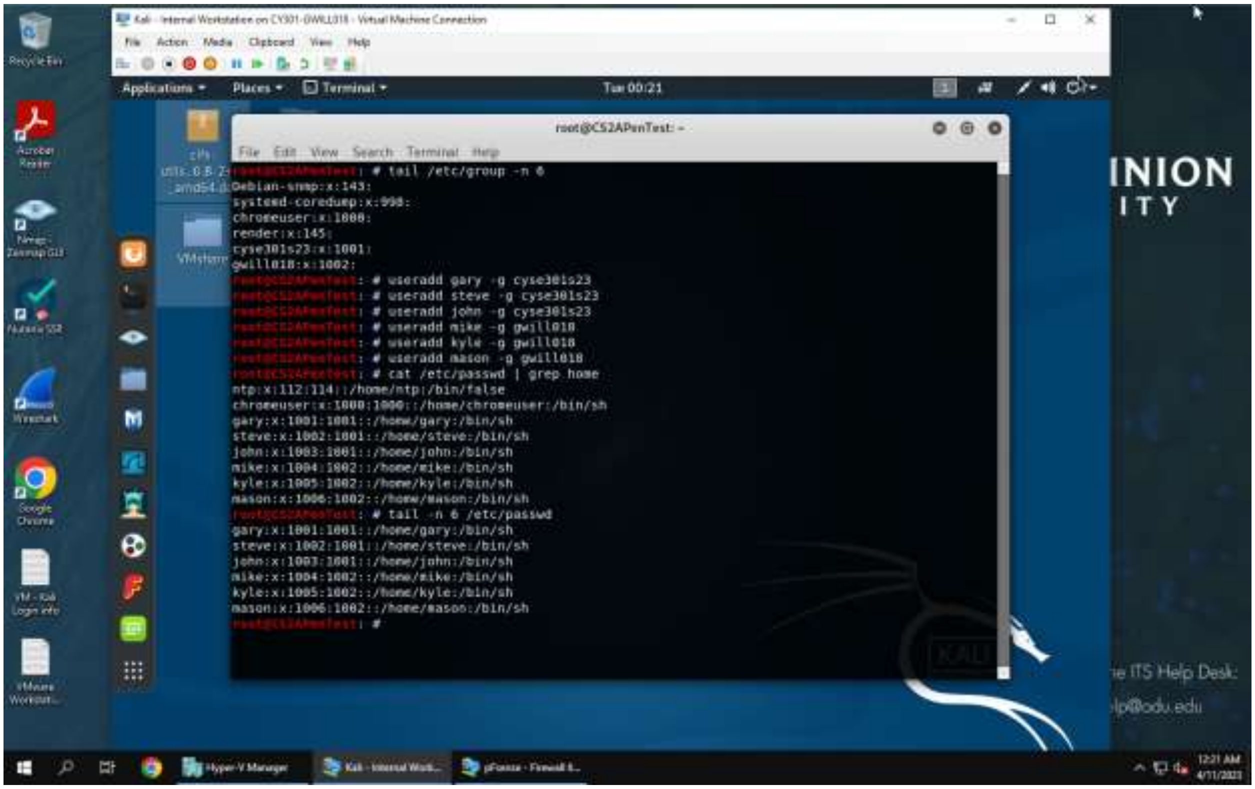
```
stunnel4:x:113:116::/var/run/stunnel4:/bin/false
redsocks:x:114:117::/var/run/redsocks:/bin/false
rtkit:x:115:118:RealtimeKit,,,:/proc:/bin/false
postgres:x:116:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
dnsmasq:x:117:65534:dnsmasq,,,:/var/lib/misc:/bin/false
messagebus:x:118:120::/var/run/dbus:/bin/false
arpwatch:x:119:122:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
sslh:x:122:126::/nonexistent:/bin/false
geoclue:x:123:128::/var/lib/geoclue:/bin/false
couchdb:x:124:129:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
avahi:x:125:131:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
sshd:x:126:65534::/var/run/sshd:/usr/sbin/nologin
colord:x:127:132:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:128:134::/var/lib/saned:/bin/false
speech-dispatcher:x:129:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:130:135:PulseAudio daemon,,,:/var/run/pulse:/bin/false
king-phisher:x:131:137::/var/lib/king-phisher:/bin/false
Debian-gdm:x:132:139:Gnome Display Manager:/var/lib/gdm3:/bin/false
dradis:x:133:140::/var/lib/dradis:/bin/false
beef-xss:x:134:141::/var/lib/beef-xss:/bin/false
statd:x:135:65534::/var/lib/nfs:/bin/false
redis:x:136:142::/var/lib/redis:/bin/false
gluster:x:137:144::/var/lib/glusterd:/usr/sbin/nologin
inetsim:x:138:999::/var/lib/inetsim:/usr/sbin/nologin
_rpc:x:103:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:121:143::/var/lib/snmp:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
chromeuser:x:1000:1000::/home/chromeuser:/bin/sh
strongswan:x:139:65534::/var/lib/strongswan:/usr/sbin/nologin
root@CS2APenTest:~# groupadd cyse301s23
root@CS2APenTest:~# groupadd gwill018
root@CS2APenTest:~# 
```



```
root@CS2APenTest:~# tail /etc/group -n 6
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301s23:x:1001:
gwill018:x:1002:
root@CS2APenTest:~#
```

Explanation: I created two groups using the commands; “groupadd cyse301s23” and “groupadd gwill018” and then to display the groups I used the command “tail /etc/group -n 6” to see the last 6 lines of /etc/group.

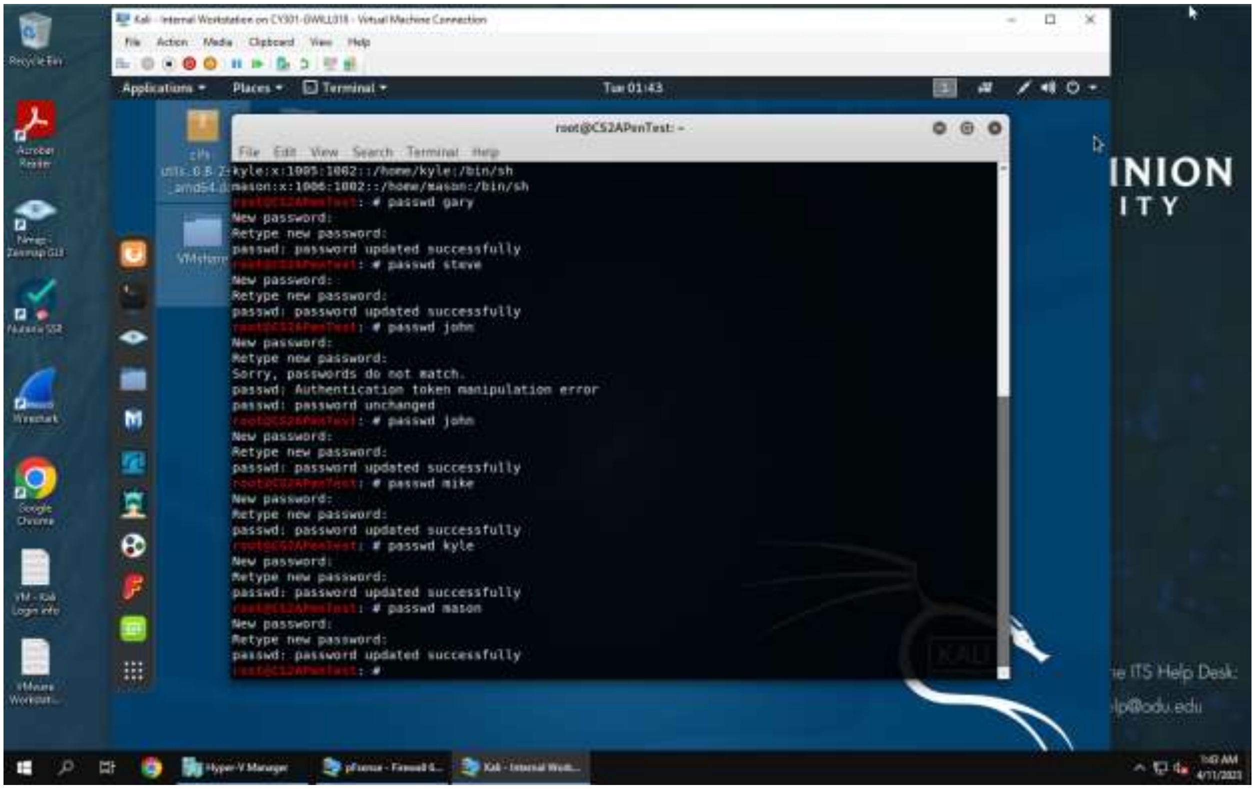
2. 5 points. Create and assign three users to each group. Display related UID and GID information of each user.



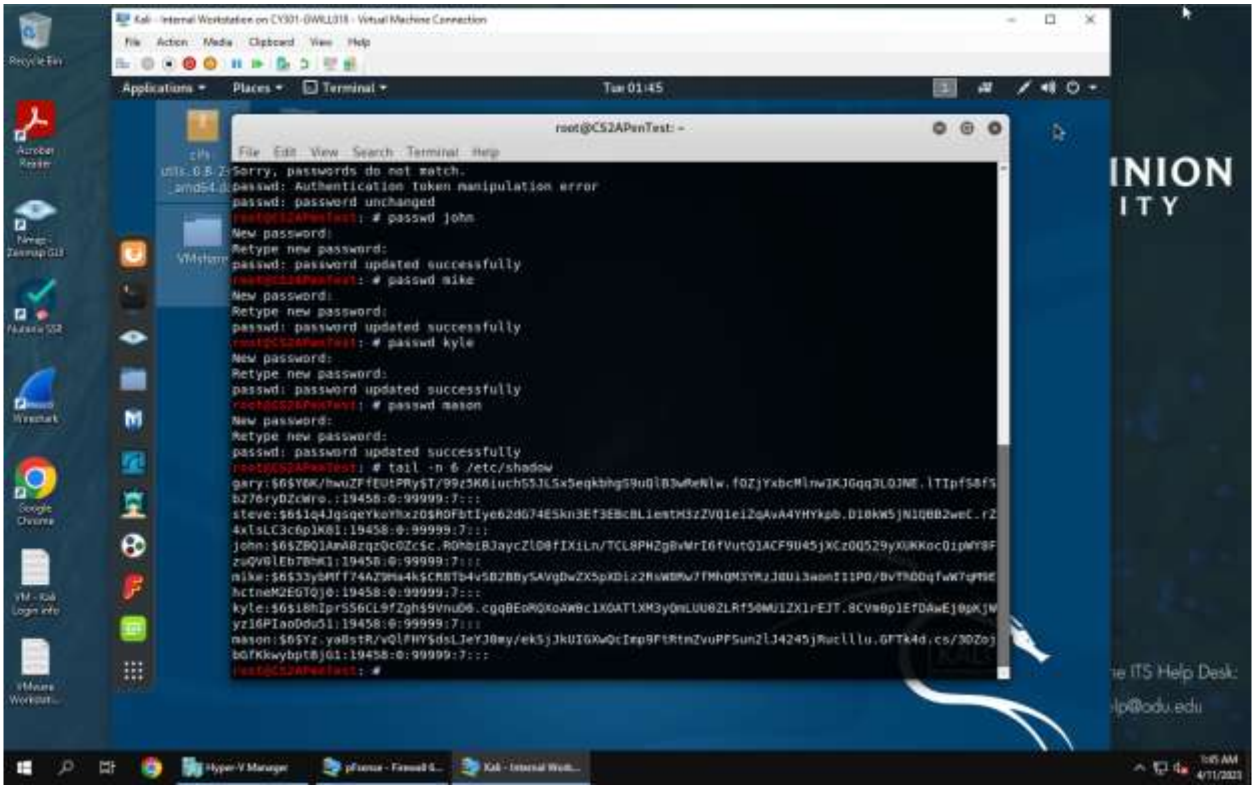
```
root@CS2APenTest:~# tail /etc/group -n 6
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301s23:x:1001:
gwill018:x:1002:
root@CS2APenTest:~# useradd gary -g cyse301s23
root@CS2APenTest:~# useradd steve -g cyse301s23
root@CS2APenTest:~# useradd john -g cyse301s23
root@CS2APenTest:~# useradd mike -g gwill018
root@CS2APenTest:~# useradd kyle -g gwill018
root@CS2APenTest:~# useradd mason -g gwill018
root@CS2APenTest:~# cat /etc/passwd | grep home
ntp:x:112:114::/home/ntp:/bin/false
chromeuser:x:1000:1000::/home/chromeuser:/bin/sh
gary:x:1001:1001::/home/gary:/bin/sh
steve:x:1002:1001::/home/steve:/bin/sh
john:x:1003:1001::/home/john:/bin/sh
mike:x:1004:1002::/home/mike:/bin/sh
kyle:x:1005:1002::/home/kyle:/bin/sh
mason:x:1006:1002::/home/mason:/bin/sh
root@CS2APenTest:~# tail -n 6 /etc/passwd
gary:x:1001:1001::/home/gary:/bin/sh
steve:x:1002:1001::/home/steve:/bin/sh
john:x:1003:1001::/home/john:/bin/sh
mike:x:1004:1002::/home/mike:/bin/sh
kyle:x:1005:1002::/home/kyle:/bin/sh
mason:x:1006:1002::/home/mason:/bin/sh
root@CS2APenTest:~#
```

Explanation: using the "useradd [name] -g [groupname]" command I was able to add 3 users to each group, for example "useradd gary -g cyse301s23" to add a new user gary to the cyse301s23 group. Then I was able to see the GID and UID of each user using the command "tail -n 6 /etc/passwd".

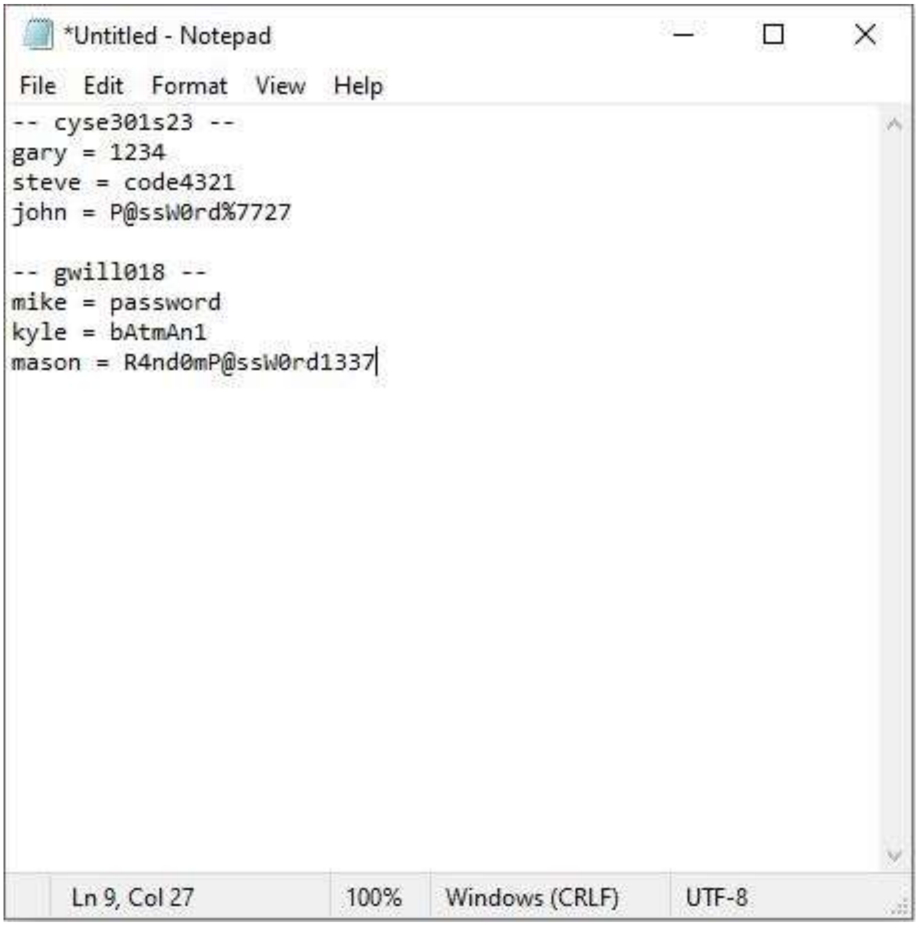
3. 5 points. Choose six new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords.


Kali - Internal Workstation on CY301-OWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 01:43
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pfSense - Firewall &...
Kali - Internal Work...

```
kyle:x:1005:1002::/home/kyle:/bin/sh
mason:x:1006:1002::/home/mason:/bin/sh
root@CS2APenTest:~# passwd gary
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd steve
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd john
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
root@CS2APenTest:~# passwd john
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd mike
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd kyle
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd mason
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~#
```


Kali - Internal Workstation on CY301-OWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 01:45
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pfSense - Firewall &...
Kali - Internal Work...

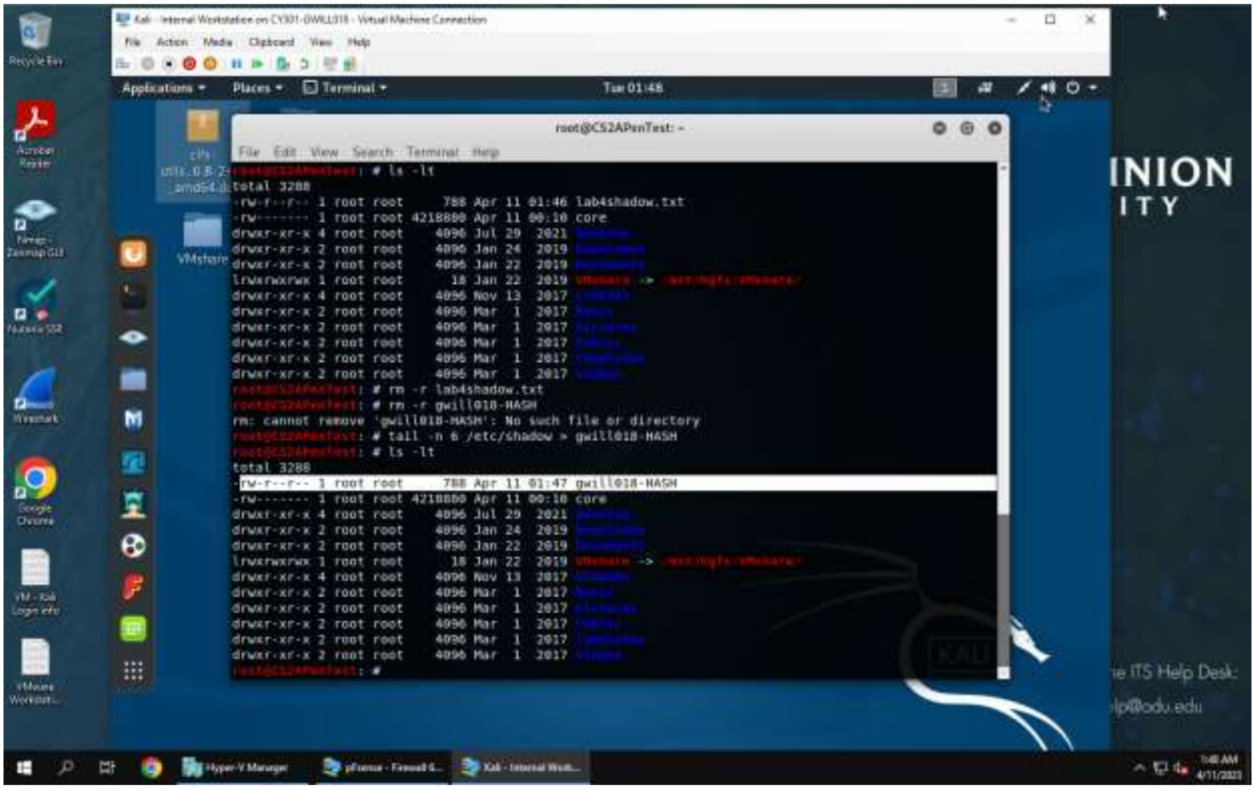
```
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
root@CS2APenTest:~# passwd john
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd mike
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd kyle
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd mason
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# tail -n 6 /etc/shadow
gary:$6$Y6K/hwuZFfEUtPRy$T/99z5K6iuch55JLSx5eqkbhgS9uQlB3wReNlw.fOZjYxbcMlnw1KJGqq3LQJNE.lTIpfS8fS
b276ryDZcWro.:19458:0:99999:7:::
steve:$6$1q4JgsqeYkoYhxzO$RDFbtIye62dG74ESkn3Ef3EBcBLiemtH3zZVQ1ei2qAvA4YHYkpb.D10kW5jN1QBB2weC.rZ
4xlsLC3c6plK01:19458:0:99999:7:::
john:$6$ZBQ1AmA8zqzQcOZc$c.ROhbiBJaycZlD8fIXiLn/TCL8PHZgBvWrI6fVutQ1ACF9U45jXCzOQ529yXUKKocQ1pWY8F
zuQV0lEb7BhK1:19458:0:99999:7:::
mike:$6$33yBMff74AZ9Ha4k$CR8Tb4vSB2BByS AVgDwZX5pXDiz2RsW8Rw7fMhQM3YRzJ8Ui3aonII1PO/BvTRDDqfwW7qM8E
hctneM2EGTQj0:19458:0:99999:7:::
kyle:$6$i8hIprS56CL9fZgh$9VnuD6.cgqBEoRQXoAW8c1XOATlXM3yOmLUU0ZLRf50WU1ZX1rEJT.8CVm0plEfDAwEj0pKjW
yz16PIaoDdu51:19458:0:99999:7:::
mason:$6$Yz.ya8stR/vQlFHY$dsLJeYJ0my/ekSjJkUIGXwQcImp9FtRtmZvuPFSun2lJ4245jRuclllu.GFTk4d.cs/3DZoj
bOfKkwybpt8jO1:19458:0:99999:7:::
root@CS2APenTest:~#
```



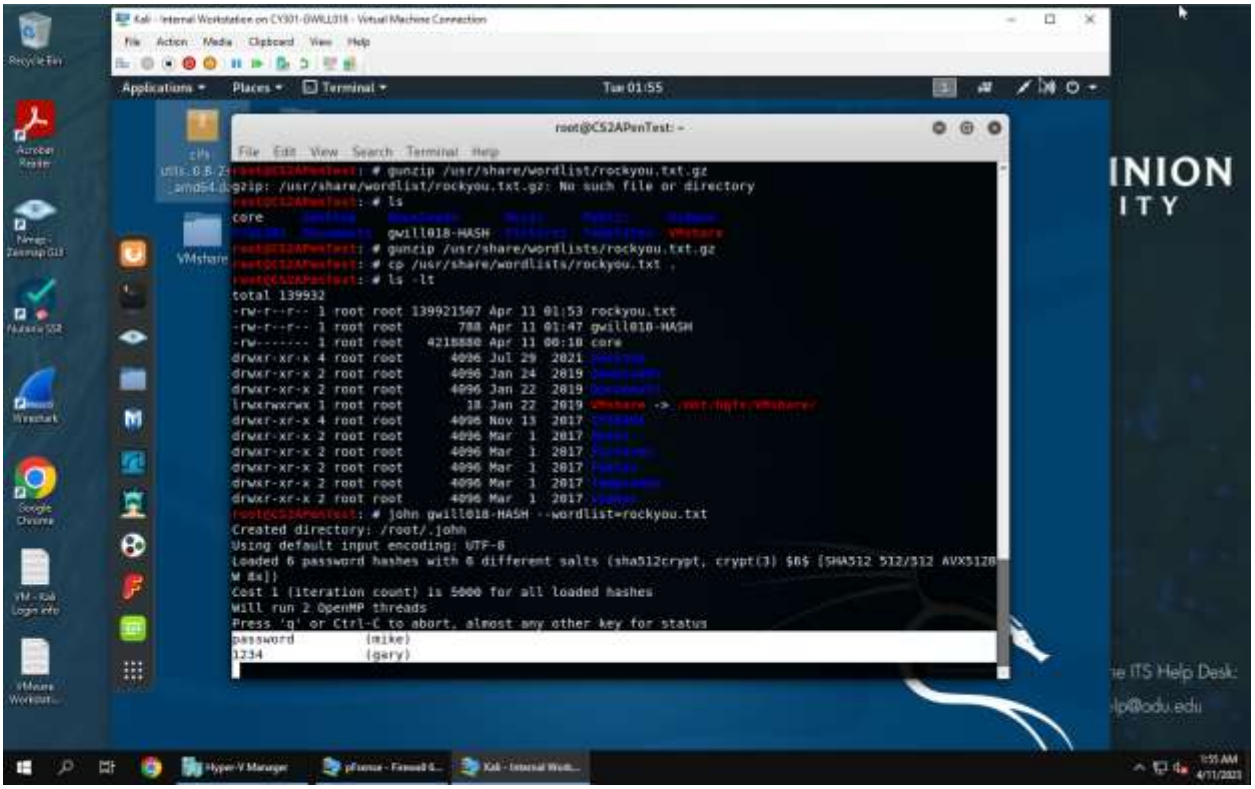
```
-- cyse301s23 --
gary = 1234
steve = code4321
john = P@ssW0rd%7727

-- gwill018 --
mike = password
kyle = bAtmAn1
mason = R4nd0mP@ssW0rd1337
```

Explanation: using the command “passwd [user]” I was able to create new passwords for each user (the password for each user is displayed in the Notepad file above). Then using the “tail -n 6 /etc/shadow” we can see the update user list with the password hashes next to each user.

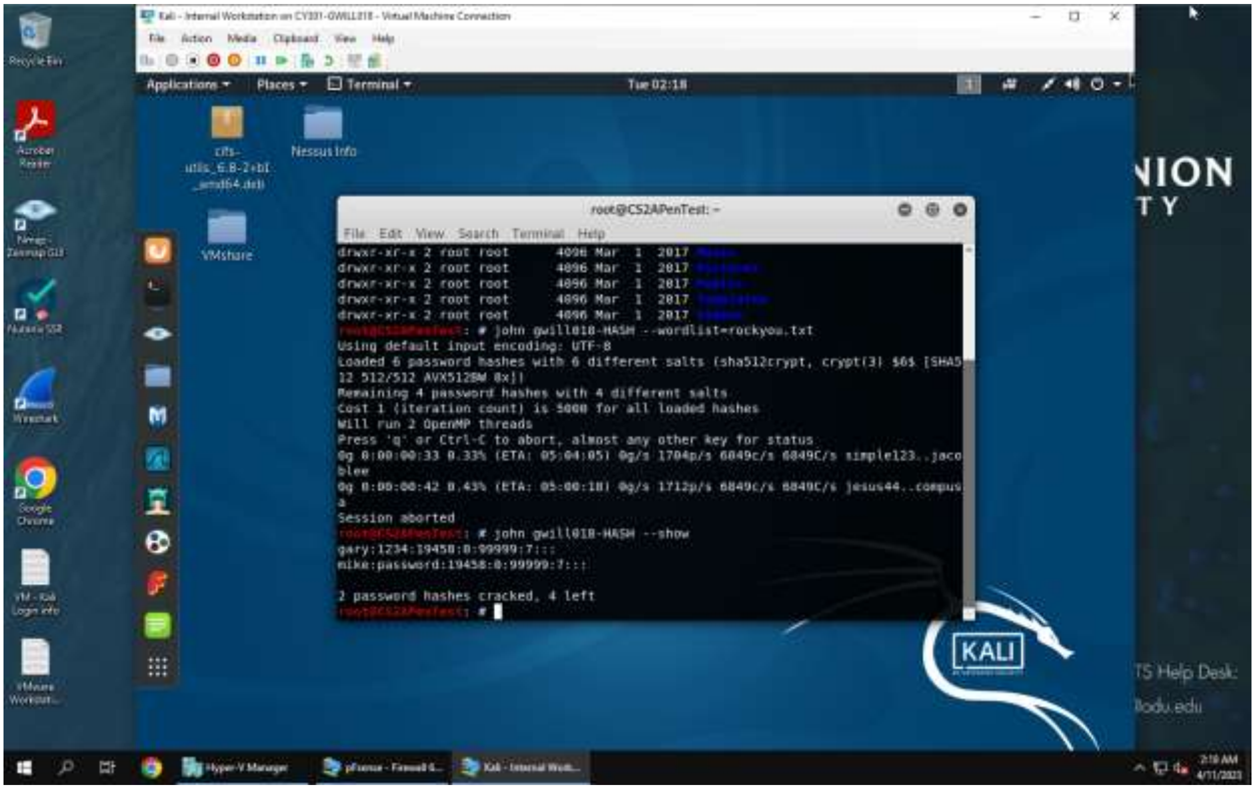
4. 5 points. Export all six users’ password hashes into a file named “YourMIDAS-HASH” (for example, pjiang-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.


Kali - Internal Workstation on CYS01-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 01:48
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
root@CS2APenTest:~# ls -lt
total 3288
-rw-r--r-- 1 root root     788 Apr 11 01:46 lab4shadow.txt
-rw------- 1 root root 4218880 Apr 11 00:10 core
drwxr-xr-x 4 root root    4096 Jul 29  2021 Desktop
drwxr-xr-x 2 root root    4096 Jan 24  2019 Downloads
drwxr-xr-x 2 root root    4096 Jan 22  2019 Documents
lrwxrwxrwx 1 root root      18 Jan 22  2019 VMshare -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root root    4096 Nov 13  2017 [illegible]
drwxr-xr-x 2 root root    4096 Mar  1  2017 Music
drwxr-xr-x 2 root root    4096 Mar  1  2017 Pictures
drwxr-xr-x 2 root root    4096 Mar  1  2017 Public
drwxr-xr-x 2 root root    4096 Mar  1  2017 Templates
drwxr-xr-x 2 root root    4096 Mar  1  2017 Videos
root@CS2APenTest:~# rm -r lab4shadow.txt
root@CS2APenTest:~# rm -r gwill018-HASH
rm: cannot remove 'gwill018-HASH': No such file or directory
root@CS2APenTest:~# tail -n 6 /etc/shadow > gwill018-HASH
root@CS2APenTest:~# ls -lt
total 3288
-rw-r--r-- 1 root root     788 Apr 11 01:47 gwill018-HASH
-rw------- 1 root root 4218880 Apr 11 00:10 core
drwxr-xr-x 4 root root    4096 Jul 29  2021 Desktop
drwxr-xr-x 2 root root    4096 Jan 24  2019 Downloads
drwxr-xr-x 2 root root    4096 Jan 22  2019 Documents
lrwxrwxrwx 1 root root      18 Jan 22  2019 VMshare -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root root    4096 Nov 13  2017 [illegible]
drwxr-xr-x 2 root root    4096 Mar  1  2017 Music
drwxr-xr-x 2 root root    4096 Mar  1  2017 Pictures
drwxr-xr-x 2 root root    4096 Mar  1  2017 Public
drwxr-xr-x 2 root root    4096 Mar  1  2017 Templates
drwxr-xr-x 2 root root    4096 Mar  1  2017 Videos
root@CS2APenTest:~#
```


Kali - Internal Workstation on CYS01-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 01:55
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
root@CS2APenTest:~# gunzip /usr/share/wordlist/rockyou.txt.gz
gzip: /usr/share/wordlist/rockyou.txt.gz: No such file or directory
root@CS2APenTest:~# ls
core         Desktop    Downloads      Music     Public     Videos
[illegible]  Documents  gwill018-HASH  Pictures  Templates  VMshare
root@CS2APenTest:~# gunzip /usr/share/wordlists/rockyou.txt.gz
root@CS2APenTest:~# cp /usr/share/wordlists/rockyou.txt .
root@CS2APenTest:~# ls -lt
total 139932
-rw-r--r-- 1 root root 139921507 Apr 11 01:53 rockyou.txt
-rw-r--r-- 1 root root       788 Apr 11 01:47 gwill018-HASH
-rw------- 1 root root   4218880 Apr 11 00:10 core
drwxr-xr-x 4 root root      4096 Jul 29  2021 Desktop
drwxr-xr-x 2 root root      4096 Jan 24  2019 Downloads
drwxr-xr-x 2 root root      4096 Jan 22  2019 Documents
lrwxrwxrwx 1 root root        18 Jan 22  2019 VMshare -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root root      4096 Nov 13  2017 [illegible]
drwxr-xr-x 2 root root      4096 Mar  1  2017 Music
drwxr-xr-x 2 root root      4096 Mar  1  2017 Pictures
drwxr-xr-x 2 root root      4096 Mar  1  2017 Public
drwxr-xr-x 2 root root      4096 Mar  1  2017 Templates
drwxr-xr-x 2 root root      4096 Mar  1  2017 Videos
root@CS2APenTest:~# john gwill018-HASH --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512B
W 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (mike)
1234             (gary)
```



Kali - Internal Workstation on CY331-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 02:18
root@CS2APenTest: ~
File Edit View Search Terminal Help
Nessus Info
VMshare
KALI
Hyper-V Manager
Kali - Internal Work...

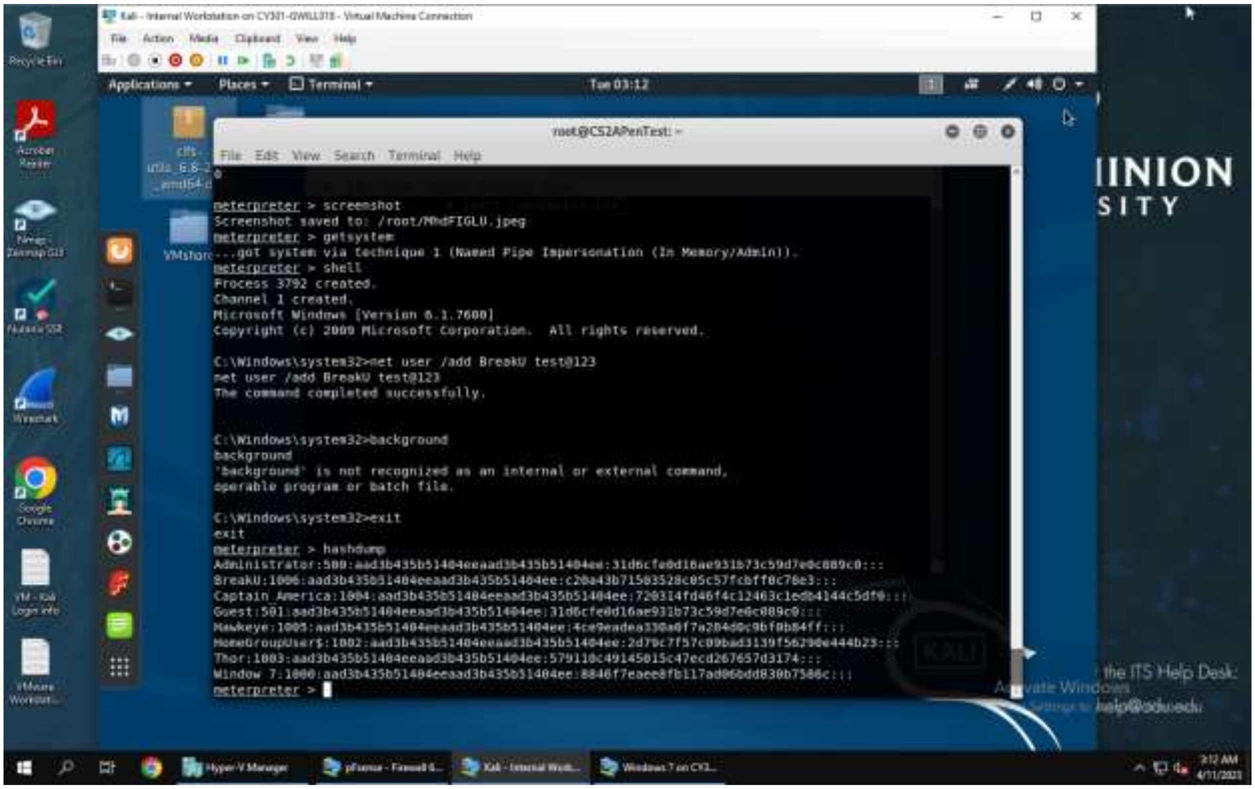
```
drwxr-xr-x 2 root root     4096 Mar  1  2017
drwxr-xr-x 2 root root     4096 Mar  1  2017
drwxr-xr-x 2 root root     4096 Mar  1  2017
drwxr-xr-x 2 root root     4096 Mar  1  2017
drwxr-xr-x 2 root root     4096 Mar  1  2017
root@CS2APenTest:~# john gwill018-HASH --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Remaining 4 password hashes with 4 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:33 0.33% (ETA: 05:04:05) 0g/s 1704p/s 6849c/s 6849C/s simple123..jacoblee
0g 0:00:00:42 0.43% (ETA: 05:00:18) 0g/s 1712p/s 6849c/s 6849C/s jesus44..compusa
Session aborted
root@CS2APenTest:~# john gwill018-HASH --show
gary:1234:19458:0:99999:7:::
mike:password:19458:0:99999:7:::

2 password hashes cracked, 4 left
root@CS2APenTest:~# 
```

Explanation: to crack the passwords of the users I had to first unzip and copy the word list that will be used for the password cracker. I did this using the commands; "gunzip /usr/share/wordlists/rockyou.txt.gz" and "cp /usr/share/wordlists/rockyou.txt .". Then I executed the password cracker to crack the hashes of each user saved in the file gwill018-HASH using the command "john gwill018-HASH --wordlist=rockyou.txt". Finally, I was able to see the cracked passwords using the command "john gwill018-HASH --show".

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM. Now, complete the following tasks:

1. 5 points. Display the password hashes by using the "hashdump" command in the meterpreter shell. Then

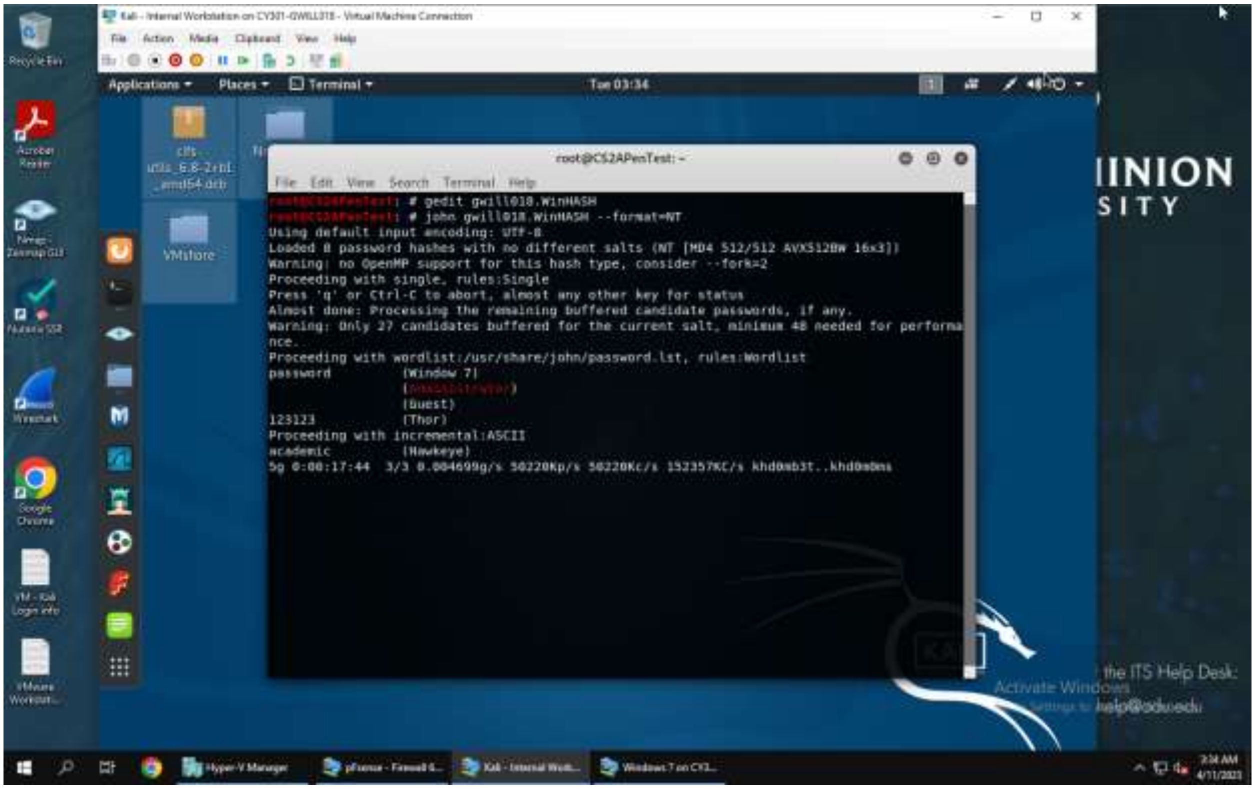


```
meterpreter > screenshot
Screenshot saved to: /root/MhdFIGLU.jpeg
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 3792 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user /add BreakU test@123
net user /add BreakU test@123
The command completed successfully.


C:\Windows\system32>background
background
'background' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
BreakU:1006:aad3b435b51404eeaad3b435b51404ee:c20a43b71583528c05c57fcbff0c78e3:::
Captain_America:1004:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb4144c5df0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hawkeye:1005:aad3b435b51404eeaad3b435b51404ee:4ce9eadea330a0f7a284d0c9bf0b84ff:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Thor:1003:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > 
```

Kali - Internal Workstation on CY301-GWILL018 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 03:12
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pFsense - Firewall &...
Kali - Internal Work...
Windows 7 on CY3...
3:12 AM
4/11/2023

Explanation: After gaining root access to the windows 7 machine through the kali VM I was able to use the "hashdump" command in the meterpreter shell to show me the hashed passwords for each user.

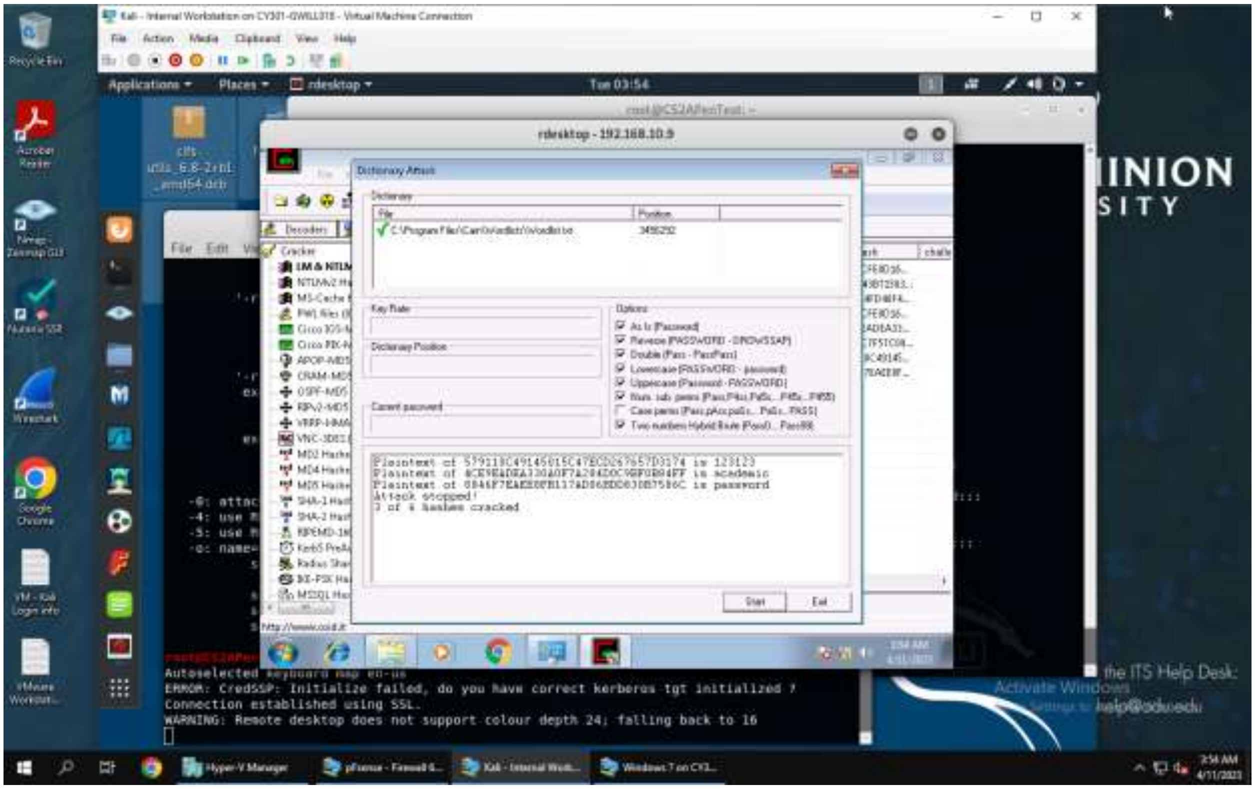
2. 10 points. Save the password hashes into a file named "your_midas.WinHASH" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).



```
root@CS2APenTest:~# gedit gwill018.WinHASH
root@CS2APenTest:~# john gwill018.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 27 candidates buffered for the current salt, minimum 48 needed for performa
nce.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password         (Window 7)
                 (Administrator)
                 (Guest)
123123           (Thor)
Proceeding with incremental:ASCII
academic         (Hawkeye)
5g 0:00:17:44  3/3 0.004699g/s 50220Kp/s 50220Kc/s 152357KC/s khd0mb3t..khd0m0ns
```

Explanation: I saved the hashes to "gwill018.WinHASH" I did this by copying the hashes and pasting them to a text file using the command "gedit gwill018.WinHASH". Then I used the command "john gwill018.WinHASH –format=NT" to crack the passwords. I let it run for a couple of minutes and found the password for the users; Thor, Window 7, and Hawkeye.

3. 10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).


Kali - Internal Workstation on CY301-GWLL01B - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places rdesktop
Tue 03:54
rdesktop - 192.168.10.9
Dictionary Attack
Start
Exit
2:54 AM
4/11/2023

Dictionary

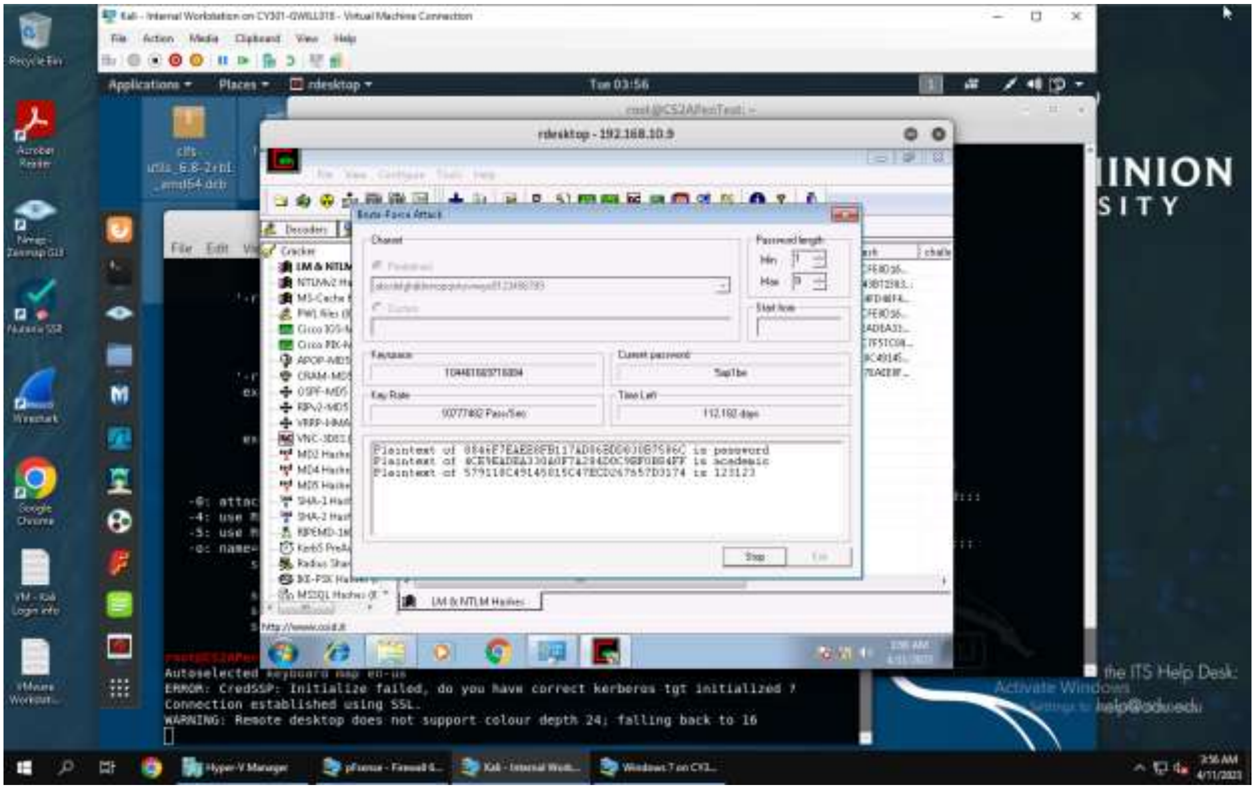
File	Position
✓ C:\Program Files\Cain\Wordlists\Wordlist.txt	3495292

Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- □ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0...Pass99)

```
Plaintext of 579110C49145015C47ECD267657D3174 is 123123
Plaintext of 8CE9EADEA330A0F7A284D0C9BF0B84FF is academic
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Attack stopped!
3 of 4 hashes cracked
```

```
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```


Kali - Internal Workstation on CY301-GWLL01B - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places rdesktop
Tue 03:56
rdesktop - 192.168.10.9
Brute-Force Attack
LM & NTLM Hashes
Stop
Exit
2:56 AM
4/11/2023

Charset: ● Predefined abcdefghijklmnopqrstuvwxyz0123456789 ○ Custom

Password length: Min 1 Max 9

Keyspace: 104461669716804

Current password: 5ap1be

Key Rate: 93077482 Pass/Sec

Time Left: 112.182 days

```
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Plaintext of 8CE9EADEA330A0F7A284D0C9BF0B84FF is academic
Plaintext of 579110C49145015C47ECD267657D3174 is 123123
```

```
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```

Explanation: I uploaded the Cain and Able program using the command "upload /root/CYSE301/Module\ IV-Password\Cracking/ca_setup.exe C:\\" to the Windows 7 VM and by connecting to it using remote desktop I was able to run it. The command I used to do this was "rdesktop -

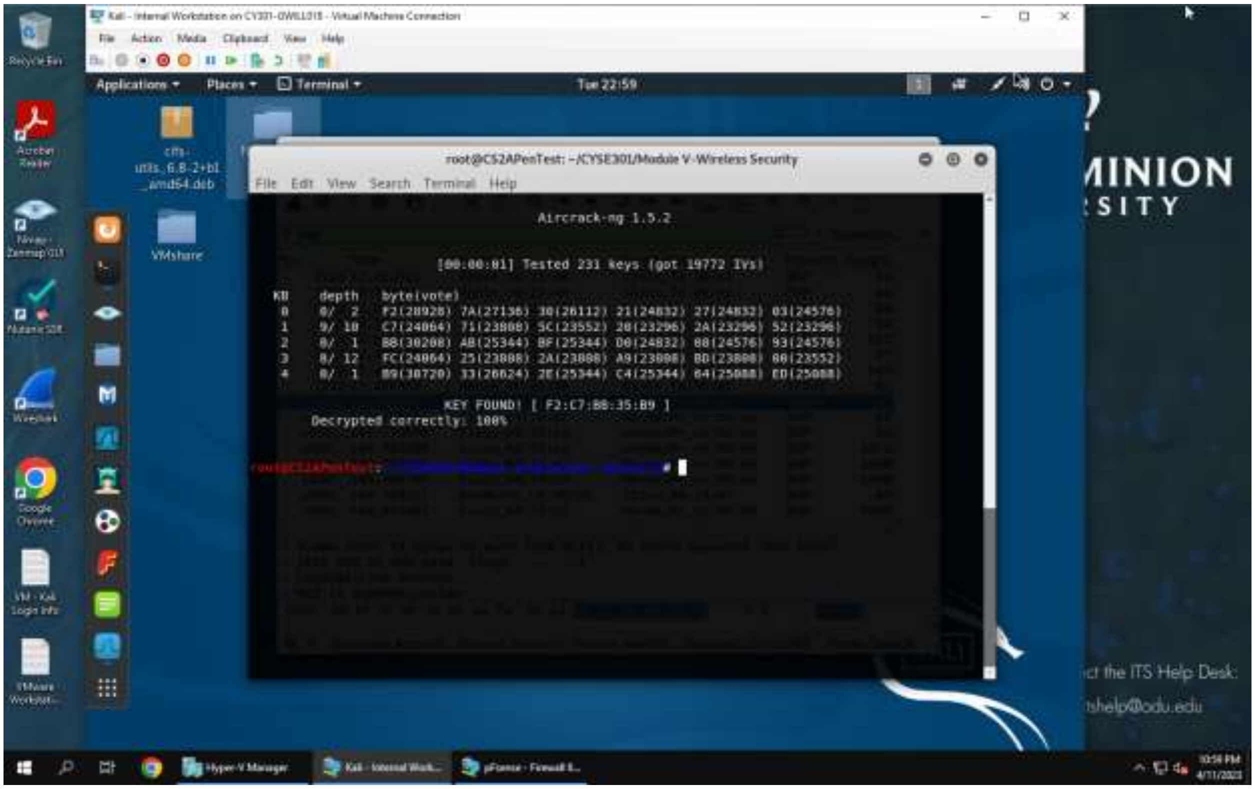
u ‘Window 7’ -p password 192.168.10.9”. Then by using the program I was able to crack the passwords using both Brute Force and a dictionary attack.

PART B

Task C: 20 points

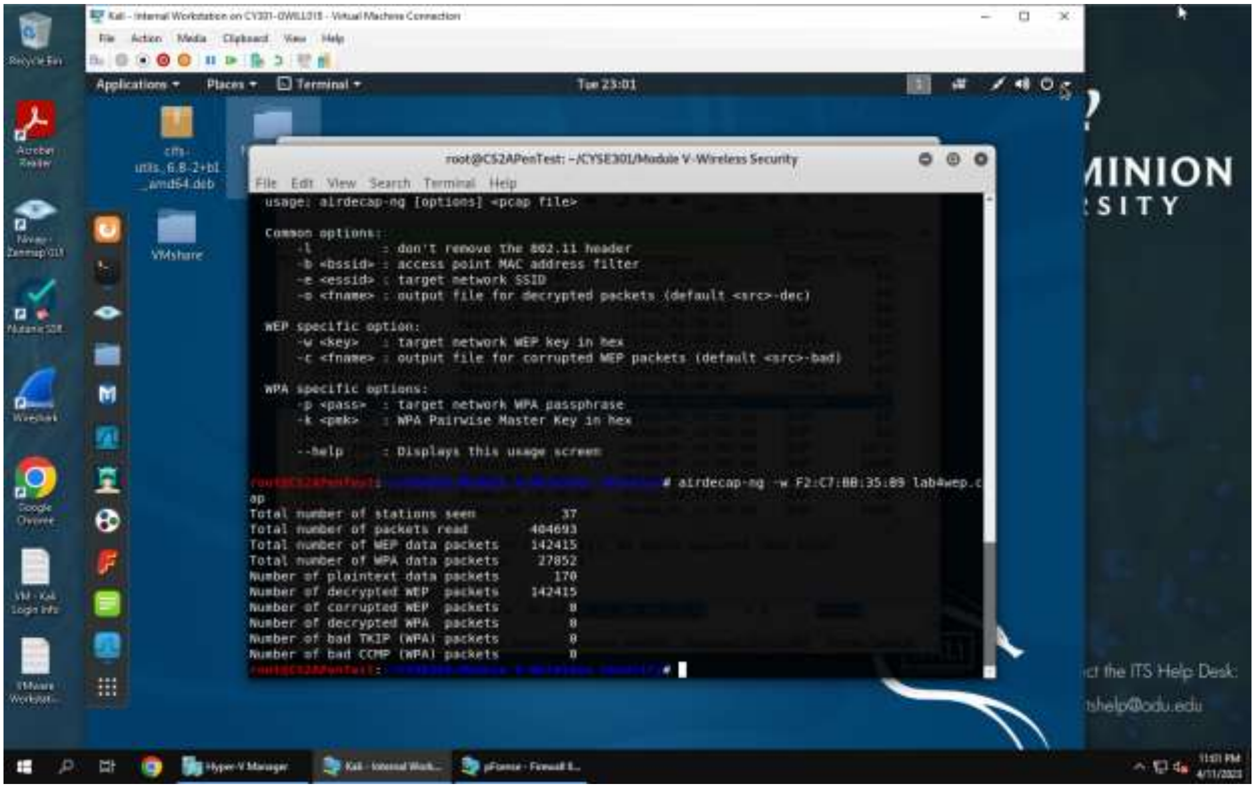
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)



root@CS2APenTest: ~/CYSE301/Module V-Wireless Security

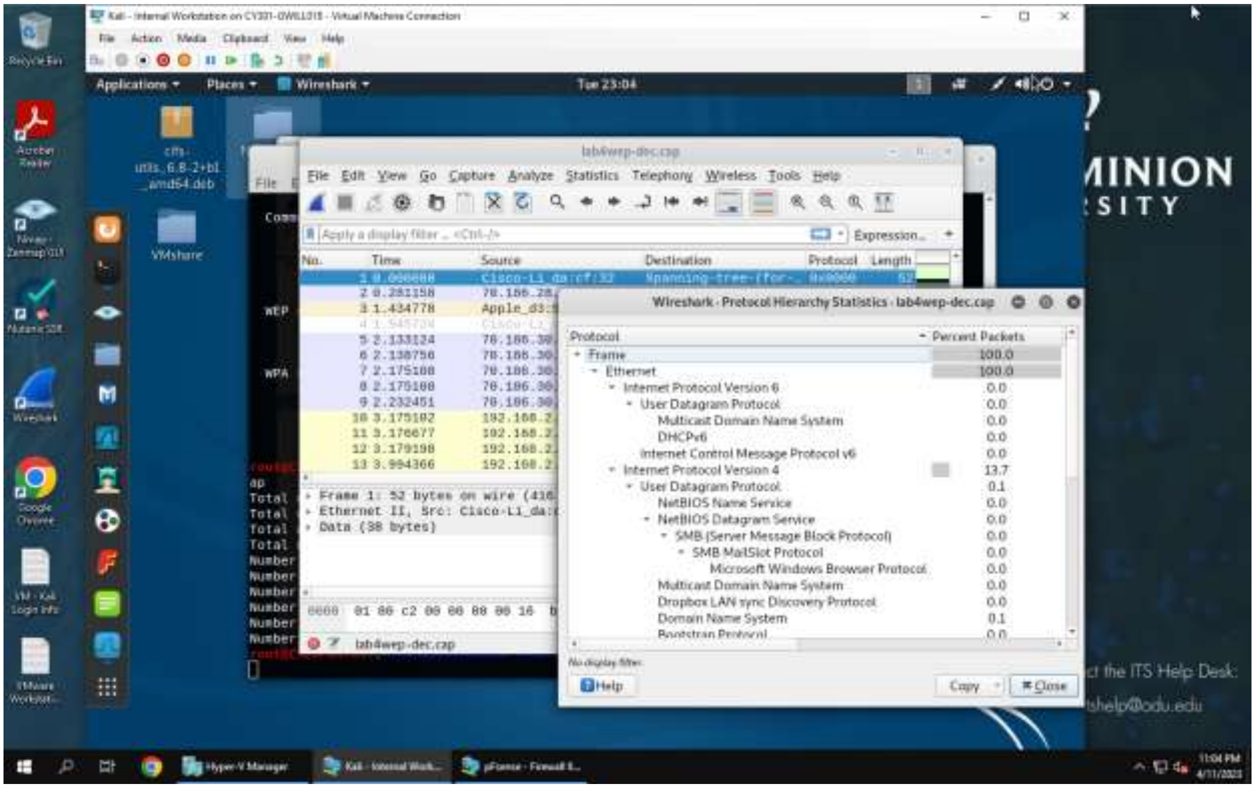
```
                              Aircrack-ng 1.5.2


                 [00:00:01] 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)
    1    9/ 10   C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296)
    2    0/  1   B8(30208) AB(25344) BF(25344) D0(24832) 88(24576) 93(24576)
    3    0/ 12   FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 80(23552)
    4    0/  1   B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088)

                      KEY FOUND! [ F2:C7:B8:35:B9 ]
	Decrypted correctly: 100%

root@CS2APenTest:[illegible]#
```



root@CS2APenTest: ~/CYSE301/Module V-Wireless Security

```
usage: airdecap-ng [options] <pcap file>

  Common options:
      -l         : don't remove the 802.11 header
      -b <bssid> : access point MAC address filter
      -e <essid> : target network SSID
      -o <fname> : output file for decrypted packets (default <src>-dec)

  WEP specific option:
      -w <key>   : target network WEP key in hex
      -c <fname> : output file for corrupted WEP packets (default <src>-bad)

  WPA specific options:
      -p <pass>  : target network WPA passphrase
      -k <pmk>   : WPA Pairwise Master Key in hex

      --help     : Displays this usage screen

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -w F2:C7:B8:35:89 lab4wep.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
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# 
```

Applications
Places
Terminal
Tue 23:01
Kali - Internal Workstation on CY301-OWILL015 - Virtual Machine Connection
File Action Media Clipboard View Help
File Edit View Search Terminal Help
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall E...
11:01 PM
4/11/2023



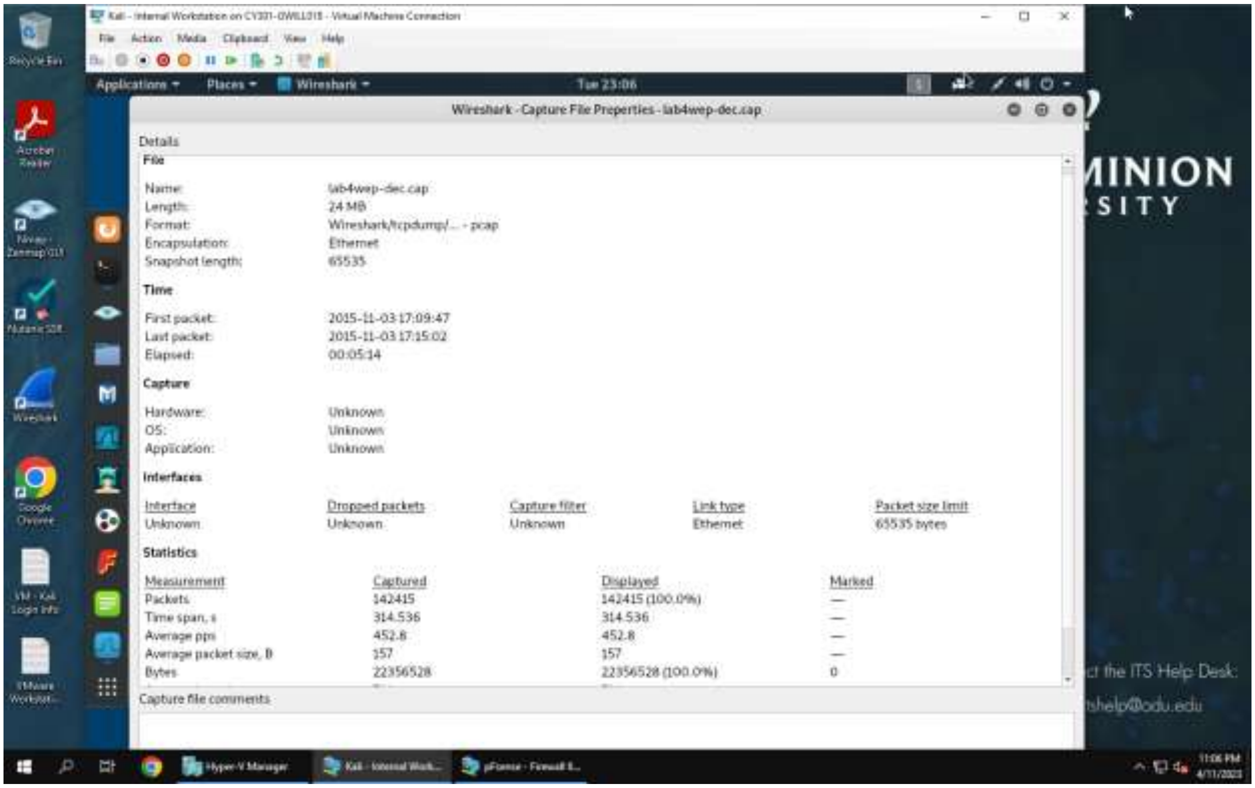
lab4wep-dec.cap

```
No.  Time        Source              Destination              Protocol  Length
  1 0.000000     Cisco-Li_da:cf:32   Spanning-tree-(for-…     0x0000    52
  2 0.281158     70.186.28.
  3 1.434778     Apple_d3:
  4 1.545724     Cisco-Li_
  5 2.133124     70.186.30.
  6 2.138756     70.186.30.
  7 2.175108     70.186.30.
  8 2.175108     70.186.30.
  9 2.232451     70.186.30.
 10 3.175102     192.168.2.
 11 3.176677     192.168.2.
 12 3.179198     192.168.2.
 13 3.994366     192.168.2.

› Frame 1: 52 bytes on wire (416
› Ethernet II, Src: Cisco-Li_da:c
› Data (38 bytes)

0000  01 80 c2 00 00 00 00 16
```

Wireshark · Protocol Hierarchy Statistics · lab4wep-dec.cap

```
Protocol                                              Percent Packets
▾ Frame                                                    100.0
  ▾ Ethernet                                               100.0
    ▾ Internet Protocol Version 6                            0.0
      ▾ User Datagram Protocol                               0.0
          Multicast Domain Name System                       0.0
          DHCPv6                                             0.0
        Internet Control Message Protocol v6                 0.0
    ▾ Internet Protocol Version 4                           13.7
      ▾ User Datagram Protocol                               0.1
          NetBIOS Name Service                               0.0
        ▾ NetBIOS Datagram Service                           0.0
          ▾ SMB (Server Message Block Protocol)              0.0
            ▾ SMB MailSlot Protocol                          0.0
                Microsoft Windows Browser Protocol           0.0
          Multicast Domain Name System                       0.0
          Dropbox LAN sync Discovery Protocol                0.0
          Domain Name System                                 0.1
          Bootstrap Protocol                                 0.0
```

No display filter.

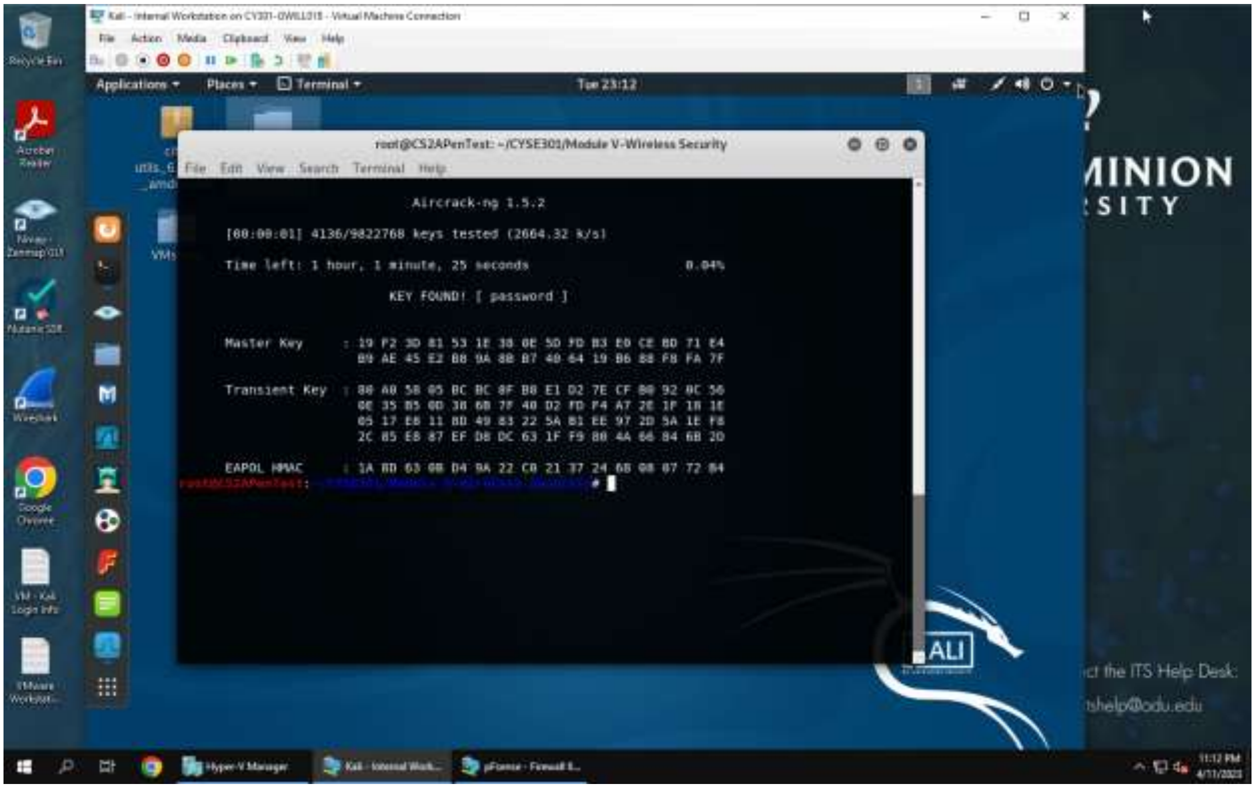

Kali - Internal Workstation on CY331-OWILL015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Wireshark ▾
Tue 23:06
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall E...

Wireshark - Capture File Properties - lab4wep-dec.cap

```
Details
File

Name:                 lab4wep-dec.cap
Length:               24 MB
Format:               Wireshark/tcpdump/... - pcap
Encapsulation:        Ethernet
Snapshot length:      65535

Time

First packet:         2015-11-03 17:09:47
Last packet:          2015-11-03 17:15:02
Elapsed:              00:05:14

Capture

Hardware:             Unknown
OS:                   Unknown
Application:          Unknown

Interfaces

Interface             Dropped packets     Capture filter     Link type     Packet size limit
Unknown               Unknown             Unknown            Ethernet      65535 bytes

Statistics

Measurement               Captured        Displayed              Marked
Packets                   142415          142415 (100.0%)        —
Time span, s              314.536         314.536                —
Average pps               452.8           452.8                  —
Average packet size, B    157             157                    —
Bytes                     22356528        22356528 (100.0%)      0

Capture file comments
```

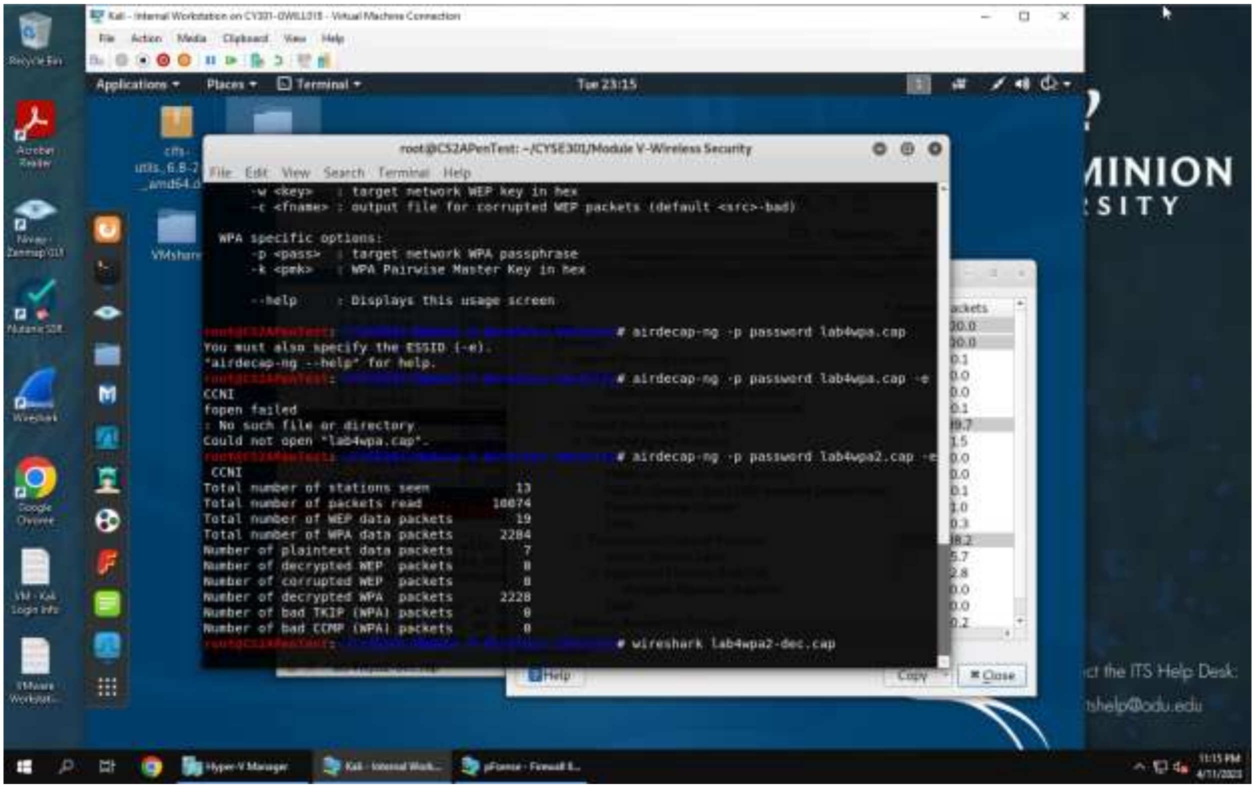
Explanation: I decrypted the lab4wep capture using the command "aircrack-ng lab4wep.cap" I was then able to select network 1 and find the key. With the key I was able to issue the command "airdecap-ng -w F2:C7:BB:35:B9 lab4wep.cap" then I was able to analyze the traffic in Wireshark using the command "wireshark lab4wep-dec.cap".

2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)



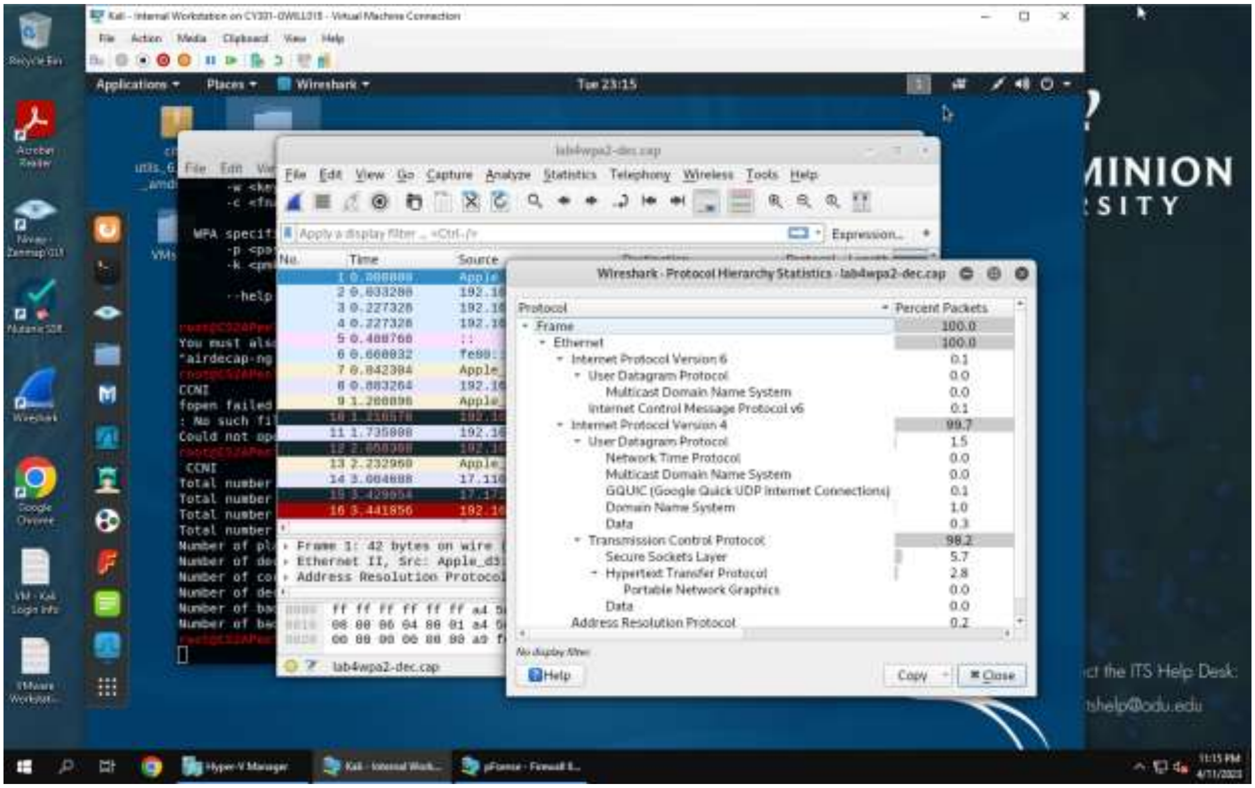
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security

```
                         Aircrack-ng 1.5.2

      [00:00:01] 4136/9822768 keys tested (2664.32 k/s)

      Time left: 1 hour, 1 minute, 25 seconds                    0.04%

                         KEY FOUND! [ password ]


      Master Key     : 19 F2 3D 81 53 1E 38 0E 5D FD B3 E0 CE 8D 71 E4
                       B9 AE 45 E2 B8 9A 8B B7 40 64 19 B6 88 F8 FA 7F

      Transient Key  : 80 A0 58 05 BC BC 8F B8 E1 D2 7E CF B0 92 0C 56
                       0E 35 B5 0D 38 6B 7F 40 D2 FD F4 A7 2E 1F 18 1E
                       05 17 E8 11 8D 49 83 22 5A B1 EE 97 2D 9A 1E F8
                       2C 85 E8 87 EF D8 DC 63 1F F9 B8 4A 66 84 6B 2D

      EAPOL HMAC     : 1A BD 63 0B D4 9A 22 C8 21 37 24 6B 08 07 72 84
root@CS2APenTest:[illegible]# 
```



root@CS2APenTest: ~/CYSE301/Module V-Wireless Security

```
      -w <key>    : target network WEP key in hex
      -c <fname>  : output file for corrupted WEP packets (default <src>-bad)

  WPA specific options:
      -p <pass>   : target network WPA passphrase
      -k <pmk>    : WPA Pairwise Master Key in hex

      --help      : Displays this usage screen

root@CS2APenTest:[illegible]# airdecap-ng -p password lab4wpa.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
root@CS2APenTest:[illegible]# airdecap-ng -p password lab4wpa.cap -e
CCNI
fopen failed
: No such file or directory
Could not open "lab4wpa.cap".
root@CS2APenTest:[illegible]# airdecap-ng -p password lab4wpa2.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
root@CS2APenTest:[illegible]# wireshark lab4wpa2-dec.cap
```



Wireshark · Protocol Hierarchy Statistics · lab4wpa2-dec.cap

Protocol	Percent Packets
Frame	100.0
Ethernet	100.0
Internet Protocol Version 6	0.1
User Datagram Protocol	0.0
Multicast Domain Name System	0.0
Internet Control Message Protocol v6	0.1
Internet Protocol Version 4	99.7
User Datagram Protocol	1.5
Network Time Protocol	0.0
Multicast Domain Name System	0.0
GQUIC (Google Quick UDP Internet Connections)	0.1
Domain Name System	1.0
Data	0.3
Transmission Control Protocol	98.2
Secure Sockets Layer	5.7
Hypertext Transfer Protocol	2.8
Portable Network Graphics	0.0
Data	0.0
Address Resolution Protocol	0.2

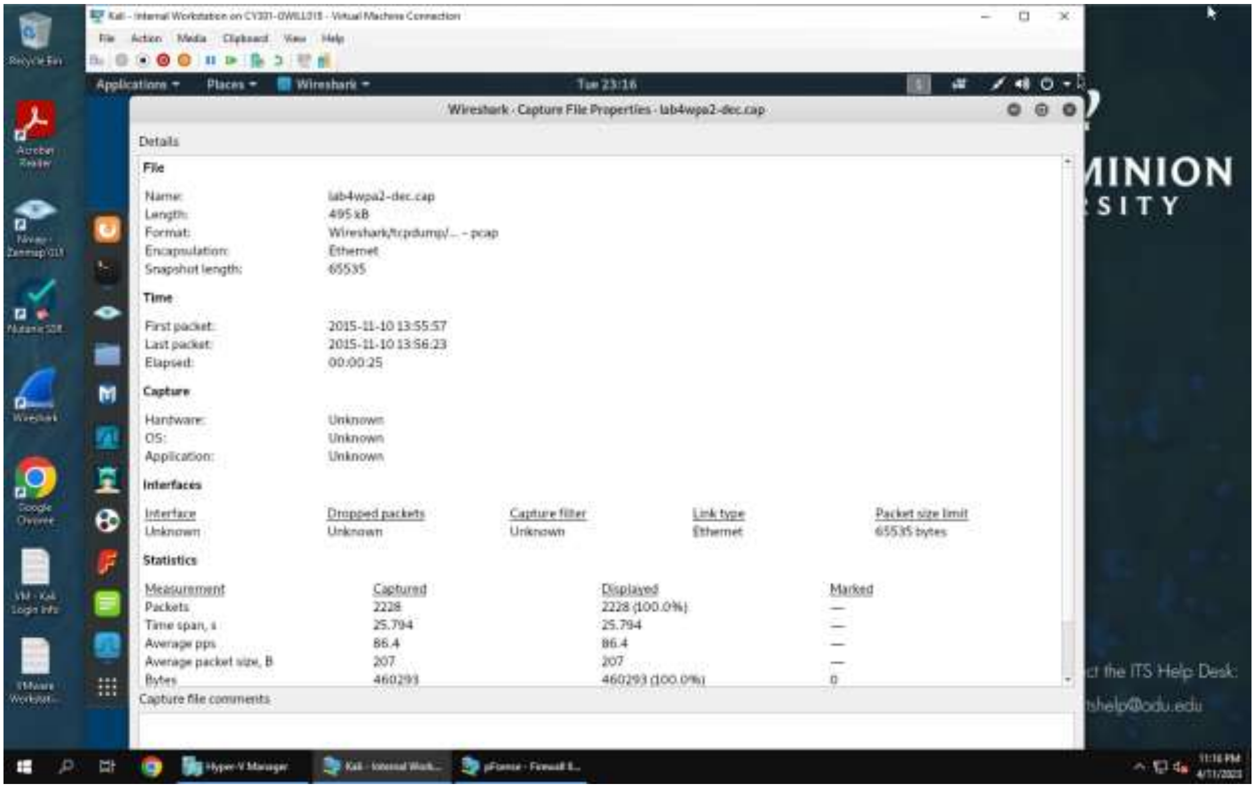
No display filter.

```
    -w <ke
    -c <fn

 WPA specif
    -p <pa
    -k <pm

    --help

You must als
"airdecap-ng
CCNI
fopen failed
: No such fi
Could not op
 CCNI
Total number
Total number
Total number
Total number
Number of pl
Number of de
Number of co
Number of de
Number of ba
Number of be
```

```
No.  Time       Source
 1 0.000000   Apple
 2 0.033280   192.16
 3 0.227328   192.16
 4 0.227328   192.16
 5 0.408768   ::
 6 0.660832   fe80::
 7 0.842384   Apple_
 8 0.883264   192.16
 9 1.280896   Apple_
10 1.316570   192.16
11 1.735808   192.16
12 2.008308   192.16
13 2.232960   Apple_
14 3.004808   17.110
15 3.429654   17.17
16 3.441856   192.16

Frame 1: 42 bytes on wire (
Ethernet II, Src: Apple_d3
Address Resolution Protocol

0000  ff ff ff ff ff ff a4 5
0010  08 00 06 04 00 01 a4 5
0020  00 00 00 00 00 00 a9 f
```

lab4wpa2-dec.cap

Kali - Internal Workstation on CY301-OWILL015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Tue 23:15
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Help
Copy
Close
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall t...
11:15 PM
4/11/2023



Wireshark · Capture File Properties · lab4wpa2-dec.cap

Details

File

Name: lab4wpa2-dec.cap
Length: 495 kB
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 65535

Time

First packet: 2015-11-10 13:55:57
Last packet: 2015-11-10 13:56:23
Elapsed: 00:00:25

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	2228	2228 (100.0%)	—
Time span, s	25.794	25.794	—
Average pps	86.4	86.4	—
Average packet size, B	207	207	—
Bytes	460293	460293 (100.0%)	0

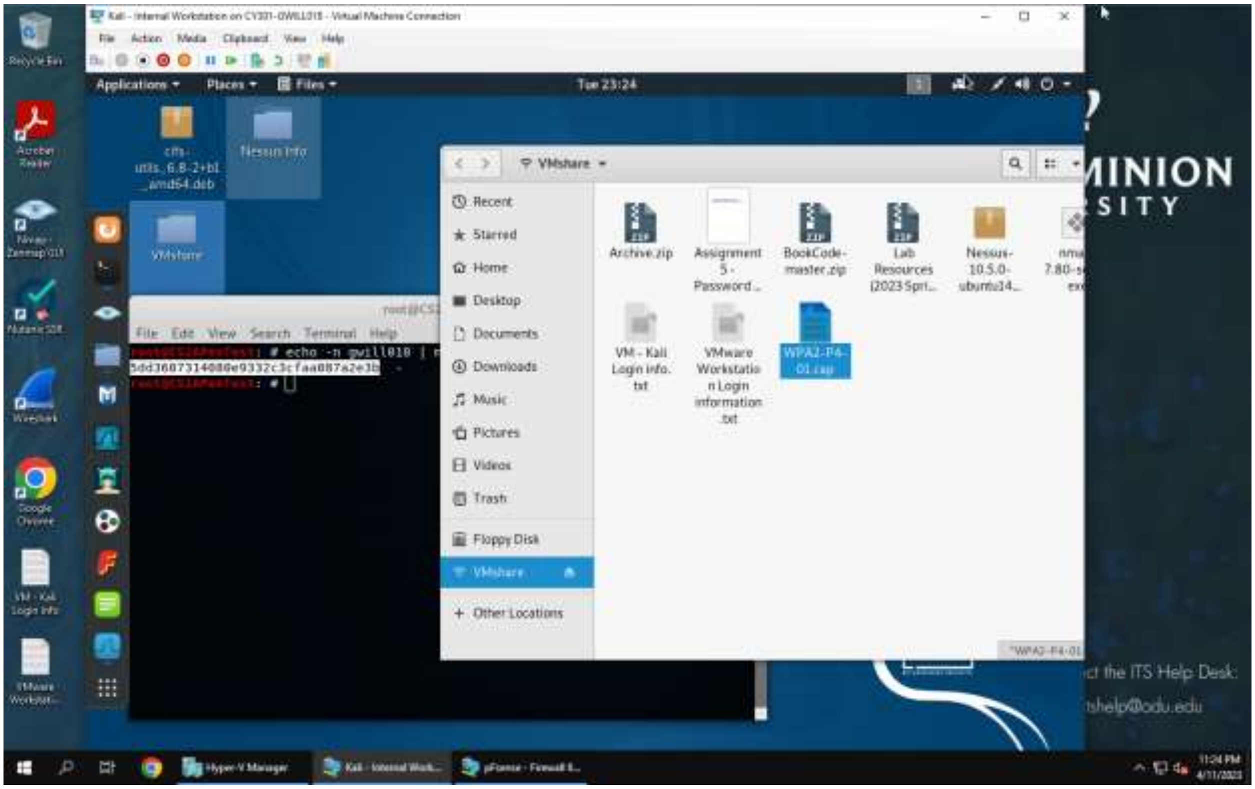
Capture file comments

Kali - Internal Workstation on CY301-OWILL015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Tue 23:16
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall t...
11:16 PM
4/11/2023

Explanation: to decrypt the wpa2 capture I first used the command "aircrack-ng lab4wpa2.cap -w rockyou.txt" then selected network 4 (CCNI) to find the key. Then I used the newly discovered password and the ESSID "CCNI" in the command "airdecap-ng -p password lab4wpa2.cap -e CCNI" to decrypt the capture. Finally, I was able to look over it in wireshark using the command "wireshark lab4wpa2-dec.cap"

Task D: 30 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for pjiang is e. Thus, I should pick up the file "WPA2-P5-01.cap."

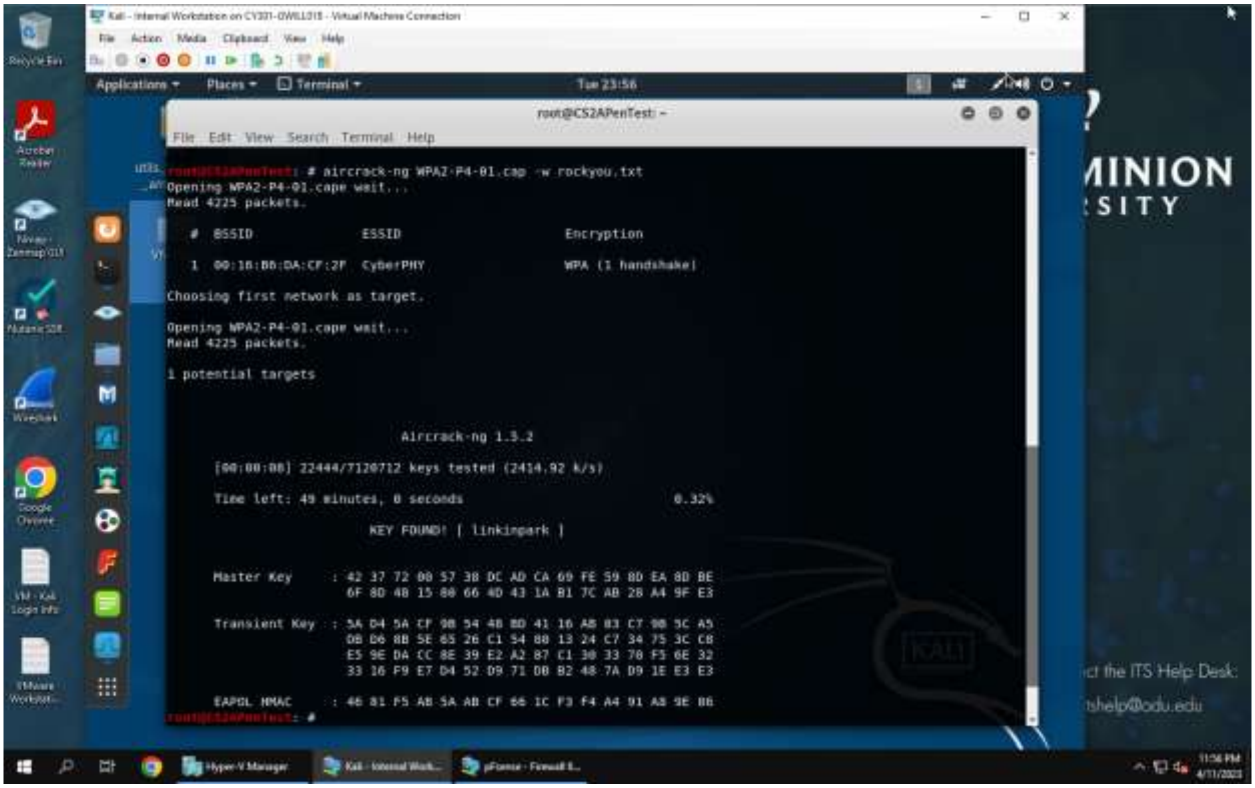


```
root@CS18PenTest:~# echo -n gwill018 | m
5dd3607314080e9332c3cfaa087a2e3b  -
root@CS18PenTest:~# 
```

Explanation: using the "echo -n gwill018 | md5sum" command I was able to find the corresponding wpa2 capture file, "WPA2-P4-01.cap". Then I simply copied it from its originally directory to the home directory.

Then complete the following steps:

1. Implement a dictionary attack and decrypt the traffic. - 20 points

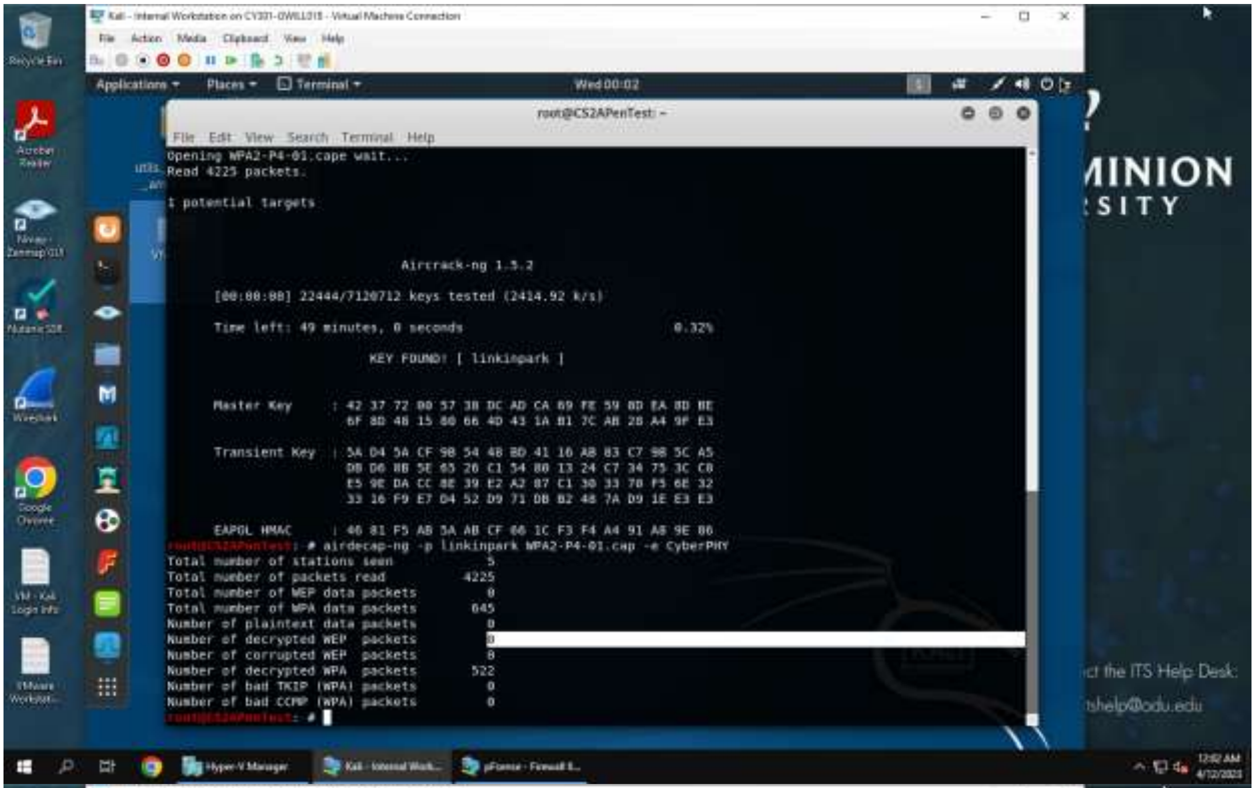


Kali - Internal Workstation on CY301-OWILL015 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Tue 23:56
root@CS2APenTest: ~
File Edit View Search Terminal Help

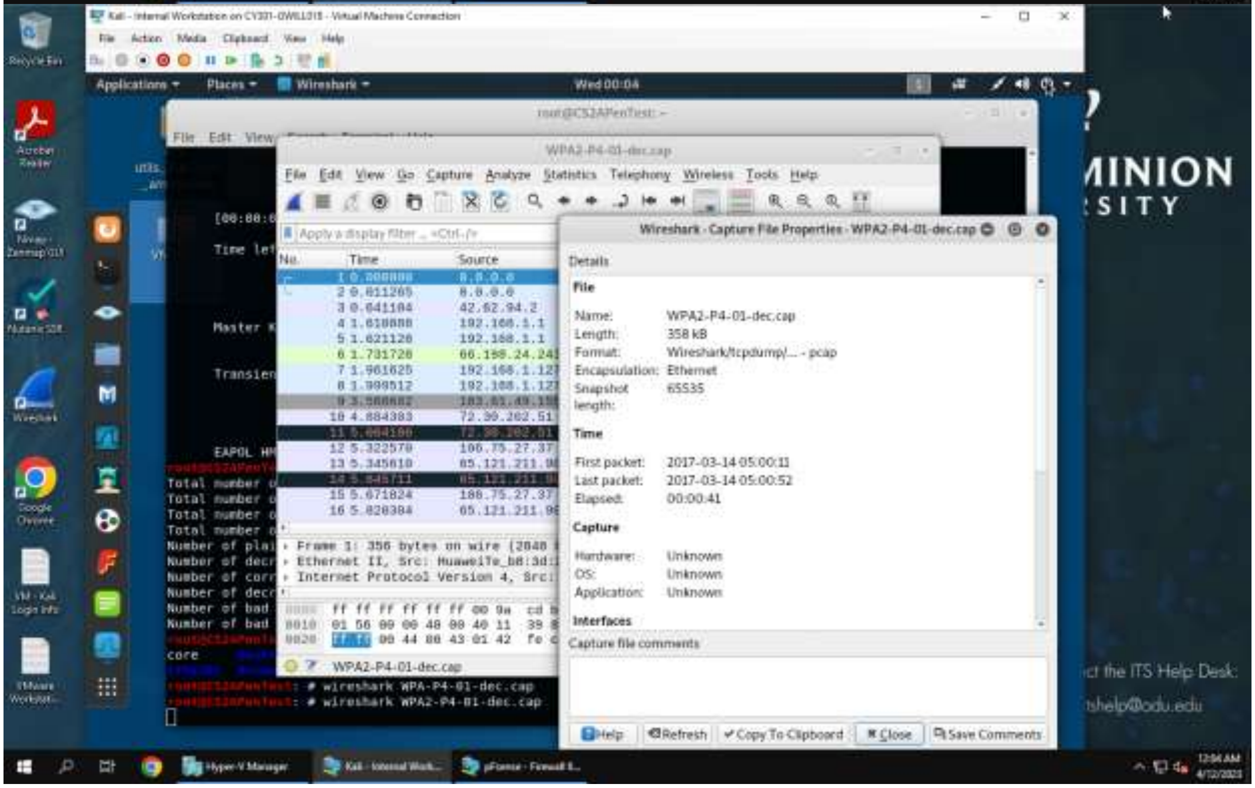
```
root@CS2APenTest:~# aircrack-ng WPA2-P4-01.cap -w rockyou.txt
Opening WPA2-P4-01.cape wait...
Read 4225 packets.

   #  BSSID              ESSID                     Encryption

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

Choosing first network as target.

Opening WPA2-P4-01.cape wait...
Read 4225 packets.

1 potential targets



                              Aircrack-ng 1.3.2

      [00:00:08] 22444/7120712 keys tested (2414.92 k/s)

      Time left: 49 minutes, 0 seconds                           0.32%

                          KEY FOUND! [ linkinpark ]


      Master Key     : 42 37 72 00 57 38 DC AD CA 69 FE 59 8D EA 8D BE
                       6F 8D 48 15 00 66 4D 43 1A B1 7C AB 28 A4 9F E3

      Transient Key  : 5A D4 5A CF 98 54 48 8D 41 16 AB 83 C7 98 5C A5
                       DB D6 8B 5E 65 26 C1 54 88 13 24 C7 34 75 3C C8
                       E5 9E DA CC 8E 39 E2 A2 87 C1 30 33 78 F5 6E 32
                       33 16 F9 E7 D4 52 D9 71 DB B2 48 7A D9 1E E3 E3

      EAPOL HMAC     : 46 81 F5 AB 5A AB CF 66 1C F3 F4 A4 91 A8 9E 86
root@CS2APenTest:~#
```

Explanation: I issued a dictionary attack to the capture using the command "aircrack-ng WPA2-P4-01.cap -w rockyou.txt", this gave me the key = linkinpark.

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -10 points



```
Opening WPA2-P4-01.cape wait...
Read 4225 packets.

1 potential targets



                               Aircrack-ng 1.5.2

      [00:00:00] 22444/7120712 keys tested (2414.92 k/s)

      Time left: 49 minutes, 0 seconds                          0.32%

                           KEY FOUND! [ linkinpark ]


      Master Key     : 42 37 72 00 57 38 DC AD CA 69 FE 59 0D EA 0D BE
                       6F 8D 48 15 80 66 4D 43 1A B1 7C AB 28 A4 9F E3

      Transient Key  : 5A D4 5A CF 98 54 48 BD 41 16 AB 83 C7 98 5C A5
                       DB D6 8B 5E 65 26 C1 54 80 13 24 C7 34 75 3C C8
                       E5 9E DA CC 8E 39 E2 A2 87 C1 30 33 78 F5 6E 32
                       33 16 F9 E7 D4 52 D9 71 DB B2 48 7A D9 1E E3 E3

      EAPOL HMAC     : 46 81 F5 AB 5A AB CF 06 1C F3 F4 A4 91 A8 9E 86
root@CS2APenTest:~# airdecap-ng -p linkinpark WPA2-P4-01.cap -e CyberPHY
Total number of stations seen            5
Total number of packets read          4225
Total number of WEP data packets         0
Total number of WPA data packets       645
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets       522
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
root@CS2APenTest:~#
```



```
No.  Time        Source
  1  0.000000    0.0.0.0
  2  0.011265    0.0.0.0
  3  0.041104    42.62.94.2
  4  1.610000    192.168.1.1
  5  1.621126    192.168.1.1
  6  1.731728    66.198.24.241
  7  1.961625    192.168.1.127
  8  1.999512    192.168.1.127
  9  3.566682    183.61.49.150
 10  4.884383    72.30.202.51
 11  5.004106    72.30.202.51
 12  5.322570    106.75.27.37
 13  5.345610    65.121.211.96
 14  5.845711    65.121.211.96
 15  5.671824    106.75.27.37
 16  5.820384    65.121.211.96

> Frame 1: 356 bytes on wire (2848 b
> Ethernet II, Src: HuaweiTe_b8:3d:1
> Internet Protocol Version 4, Src:

0000  ff ff ff ff ff ff 00 9a  cd b
0010  01 56 00 00 40 00 40 11  39 8
0020  ff ff 00 44 00 43 01 42  fe c
```

```
core
root@CS2APenTest:~# wireshark WPA-P4-01-dec.cap
root@CS2APenTest:~# wireshark WPA2-P4-01-dec.cap
```

Wireshark · Capture File Properties · WPA2-P4-01-dec.cap

Details

File

Name: WPA2-P4-01-dec.cap
Length: 358 kB
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 65535

Time

First packet: 2017-03-14 05:00:11
Last packet: 2017-03-14 05:00:52
Elapsed: 00:00:41

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Capture file comments

Explanation: I decrypted the traffic using the command "airdecap-ng -p linkinpark WPA2-P4-01.cap -e CyberPHY" (the argument -e CyberPHY specifies the ESSID). Then I was able to look at eh decrypted capture in wireshark using the command "wireshark WPA2-P4-01-dec.cap".

What I found in wireshark:

I was able to decrypt 522 packets, most of the packets were TCP packets, TCP made up 69.9% of the traffic. Other notable protocols were UDP at 29.7%, MSN Messenger Service at 10.9%, and SSL at 10.2. We can see that this traffic was captured in 2017 specifically March 14th at 5pm. I was able to gather 21 resolved addresses and the host names. Of these I can guess that a video was playing at the time of the capture as evidence from “182.95.153.10 hpcc-video.cnc.ccgslb.com.cn” and the Mp4 packets, I don’t know what this is exactly since when I put it into google it said it was unsecure. I can also see that they were running WordPress and Taobao which is a Chinese online shopping platform. The traffic could be from a google or android device since they are running Gstatic. I also found a service name HuaweiTe which is a Chinese video conferencing soft client that provides video, audio and content sharing for desktop and mobile. This could explain the Mp4 packets, and the Chinese shopping platform found in the traffic.