

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

Assignments #4 & #5 Password Cracking

---

Harold Vernon

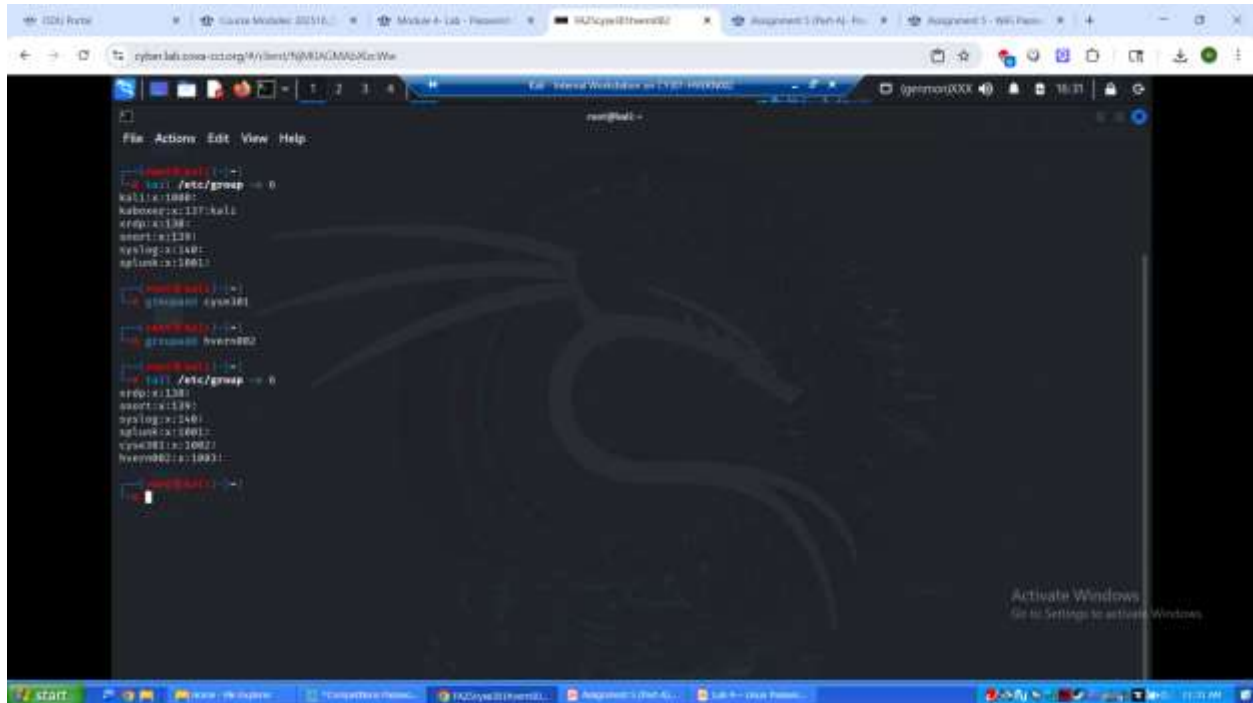
01265958

Below is the snippet of a sample lab report.

---

## TASK A

1. Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.

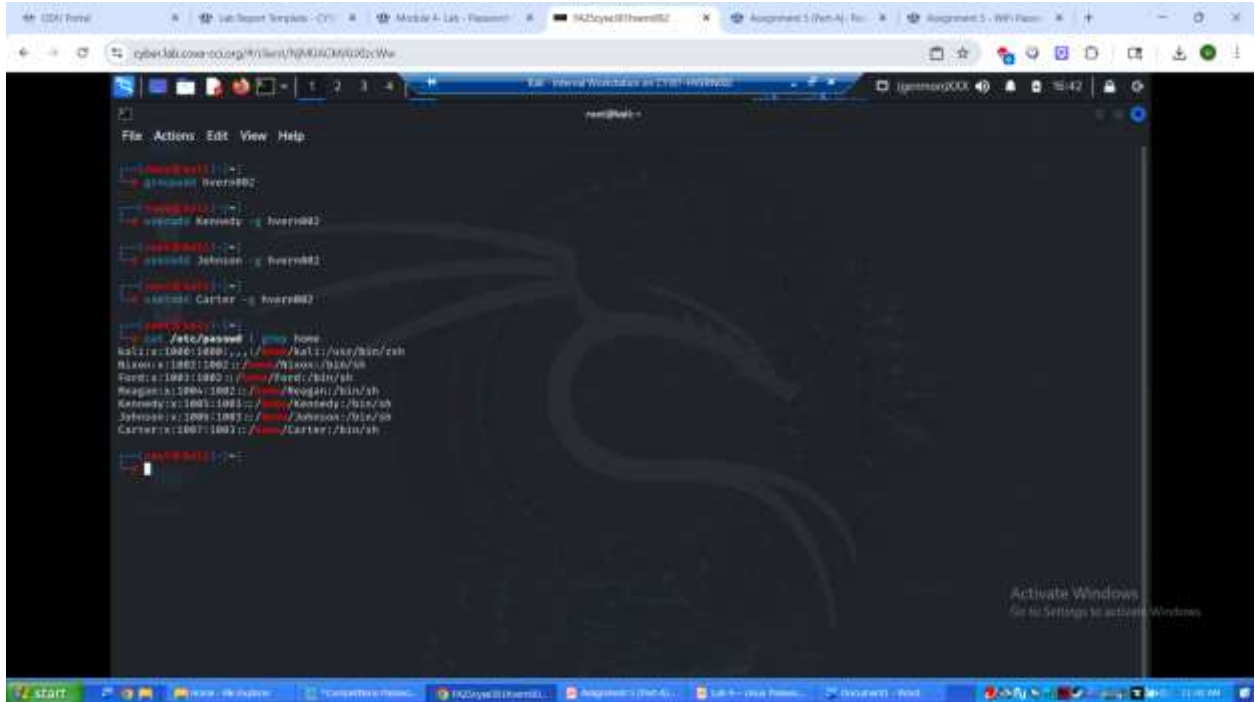


```
root@kali:~# groupadd cyse301
root@kali:~# groupadd hvern002
root@kali:~# cat /etc/group
root:x:1000:
kali:x:1000:
kuboseg:x:117:kali
krfp:x:138:
nsort:x:139:
nyslog:x:140:
nplink:x:1801:
root@kali:~# cat /etc/group
root:x:1000:
cyse301:x:1001:
hvern002:x:1002:
root@kali:~# cat /etc/group
root:x:1000:
kali:x:1000:
kuboseg:x:117:kali
krfp:x:138:
nsort:x:139:
nyslog:x:140:
nplink:x:1801:
cyse301:x:1001:
hvern002:x:1002:
```

### Explanation:

Above are the groups for the Internal Kali VM. “cyse301” and “hvern002” are visible as requested.

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



```
root@kali:~# cat /etc/passwd | grep home
kali:x:1000:1000::/home/kali:/usr/bin/zsh
Nixon:x:1001:1001::/home/Nixon:/bin/sh
Ford:x:1002:1002::/home/Ford:/bin/sh
Reagan:x:1003:1003::/home/Reagan:/bin/sh
Kennedy:x:1004:1004::/home/Kennedy:/bin/sh
Johnson:x:1005:1005::/home/Johnson:/bin/sh
Carter:x:1006:1006::/home/Carter:/bin/sh

root@kali:~# cat /etc/passwd | grep hvern02
hvern02:Kennedy:x:1007:1007::/home/hvern02:/bin/sh
hvern02:Johnson:x:1008:1008::/home/hvern02:/bin/sh
hvern02:Carter:x:1009:1009::/home/hvern02:/bin/sh
```

**Explanation:**

Above, the added users can be seen. “cyse301” contains the users Nixon, Ford, and Reagan while “hvern02” contains the users Kennedy, Johnson, and Carter.

- 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.



**Explanation:**

Above, the tail command has been run on the shadow file. The shadows of the six users' passwords can be seen. Their actual passwords are red (Nixon), Red38 (Ford), ?81R3D3L3PH4N7589RR! (Reagan), blue (Kennedy), Blue36 (Johnson), and ?71BLU3D0NK3Y575JC! (Carter.)

- Export all Three users' password hashes into a file named "YourMIDAS-HASH" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



**Explanation:**

Above are the results of the dictionary attack. In a realistic attack, the passwords red, blue, Red38, and Blue36 would not be secure. If an attacker is using John with the wrong hash, they could just as easily guess red or blue to access Nixon or Kennedy's account respectively.



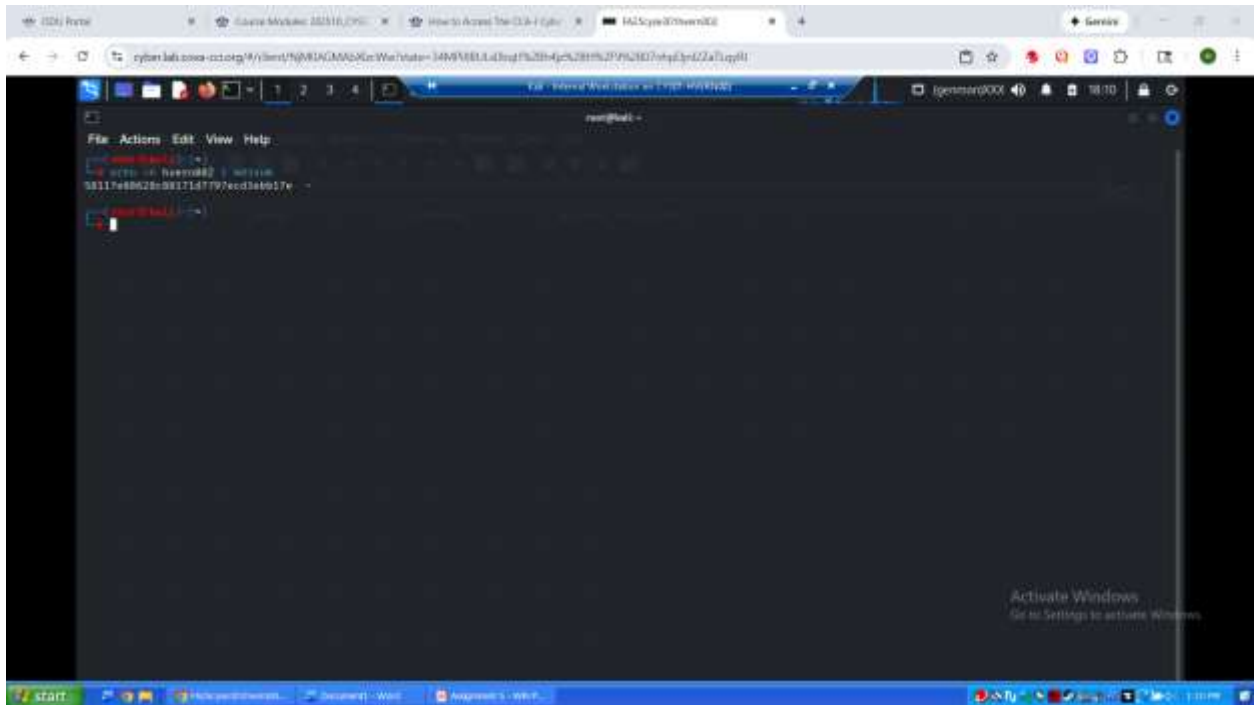
6. Decrypt the lab5wpa2-demo. cap file and perform a detailed traffic analysis.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	IDUs
- Frame	100.0	2228	100.0	460293	142 k	0	0	0	2228
- Ethernet	100.0	2228	6.8	31192	9,674	0	0	0	2228
- Internet Protocol Version 6	0.1	3	0.0	120	37	0	0	0	3
- User Datagram Protocol	0.0	1	0.0	8	2	0	0	0	1
- Multicast Domain Name System	0.0	1	0.1	278	86	1	278	86	1
- Internet Control Message Protocol v6	0.1	2	0.0	40	12	2	40	12	2
- Internet Protocol Version 4	99.7	2221	9.7	44420	13 k	0	0	0	2221
- User Datagram Protocol	1.5	33	0.1	264	81	0	0	0	33
- Network Time Protocol	0.0	1	0.0	48	14	1	48	14	1
- Multicast Domain Name System	0.0	1	0.0	114	35	1	114	35	1
- QUIC (Google Quick UDP Internet Connections)	0.1	2	0.3	1387	430	2	1387	430	2
- Domain Name System	1.0	22	0.2	939	291	22	939	291	22
- Data	0.3	7	0.3	1374	426	7	1374	426	7
- Transmission Control Protocol	98.2	2188	82.6	379997	117 k	1998	300797	93 k	2188
- Transport Layer Security	5.7	127	8.5	39288	12 k	127	39288	12 k	127
- Hypertext Transfer Protocol	2.8	62	14.2	65357	20 k	61	64032	19 k	62
- Portable Network Graphics	0.0	1	0.2	1060	328	1	1060	328	1
- Data	0.0	1	0.1	343	106	1	343	106	1
- Address Resolution Protocol	0.2	4	0.0	112	34	4	112	34	4

**Explanation:**

Above is the protocol hierarchy of the given packet. Due to the decryption carried out using the aircrack tool and rockyou wordlist for a dictionary attack, nearly all packets and their protocols are visible.

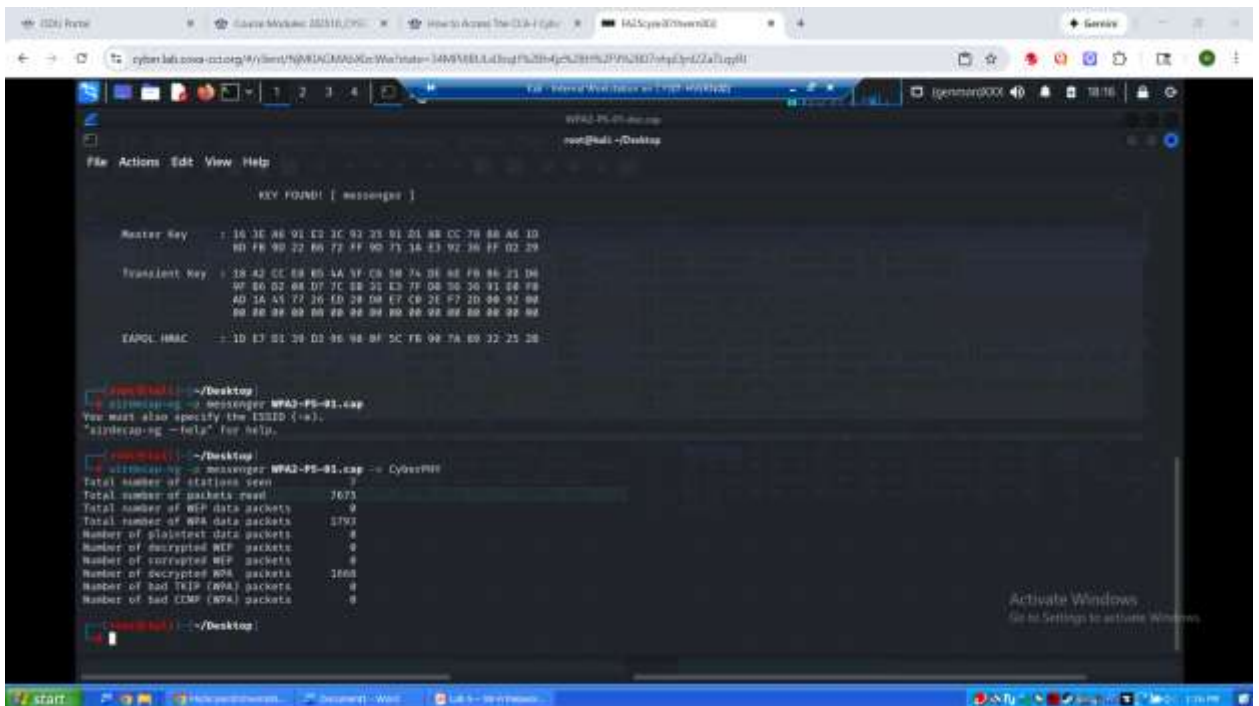
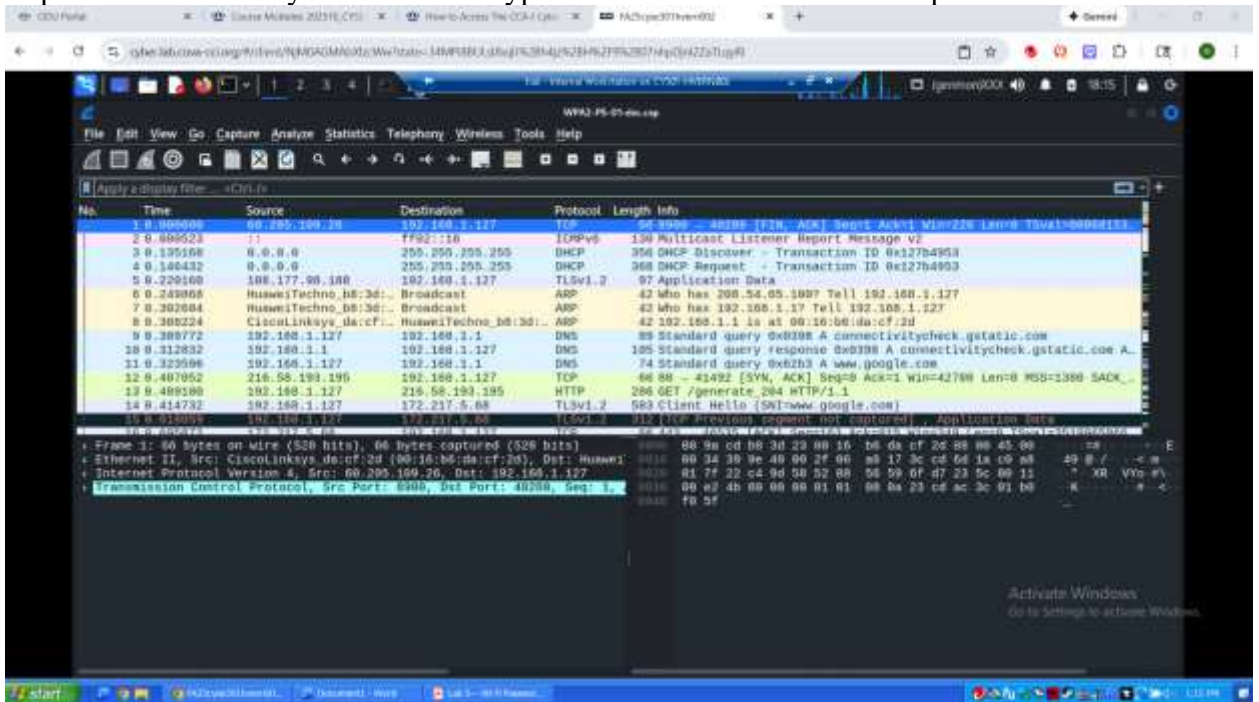
- Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID.



**Explanation:**

Since the last character of my MD5 is the letter E, I will be working with WPA2-P5-01.cap.

8. Implement a dictionary attack and decrypt the traffic in WPA2-P5-01.cap.



**Explanation:**

Above is the decrypted traffic of the given file and the command used to decrypt them after the successful dictionary attack.

- Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file (using wireshark).

The screenshot shows the 'Protocol Hierarchy Statistics' window in Wireshark. The table below represents the data shown in the window, detailing the percentage of packets and bytes, along with counts for various protocols.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PT
Frame	100.0	1668	100.0	613627	140 k	0	0	0	16
Ethernet	100.0	1668	3.8	23352	5,358	0	0	0	16
Internet Protocol Version 6	0.2	4	0.0	160	36	0	0	0	4
Internet Control Message Protocol v6	0.2	4	0.0	188	43	4	188	43	4
Internet Protocol Version 4	99.4	1658	5.4	33160	7,609	0	0	0	16
User Datagram Protocol	35.5	926	1.2	7408	1,700	0	0	0	95
Multicast Domain Name System	0.1	2	0.0	122	27	2	122	27	2
Internet Security Association and Key Management Protocol	0.1	1	0.1	488	111	1	488	111	1
GQUIC (Google Quick UDP Internet Connections)	41.9	699	46.8	287090	65 k	699	287090	65 k	66
Dynamic Host Configuration Protocol	0.1	2	0.1	640	146	2	640	146	2
Domain Name System	2.3	39	0.3	1803	413	39	1803	413	39
Data	11.0	183	13.5	82617	18 k	183	82617	18 k	18
Transmission Control Protocol	43.8	731	28.7	175926	40 k	624	87839	20 k	72
XTI	0.1	1	0.0	34	5	0	0	0	1
Malformed Packet	0.1	1	0.0	0	0	1	0	0	1
Transport Layer Security	2.9	48	2.1	12856	2,950	48	12856	2,950	48
MSN Messenger Service	1.9	31	7.3	44888	10 k	31	44888	10 k	31
Hypertext Transfer Protocol	1.5	25	4.4	27075	6,213	25	27075	6,213	25
Data	0.1	2	0.0	132	30	2	132	30	2
Internet Control Message Protocol	0.1	1	0.1	489	112	0	0	0	1
Internet Security Association and Key Management Protocol	0.1	1	0.1	453	103	1	453	103	1
Address Resolution Protocol	0.4	6	0.0	168	38	6	168	38	6

**Explanation:** Above is the traffic file's protocol hierarchy. A simple dictionary attack removed all security that existed around the packets on the file. This could be dangerous as it means that threat actors can easily access the information being sent over a network. It is best to use an encrypted key to prevent dictionary attacks. When encrypting the key, however, it is important to avoid using insecure algorithms such as WEP because those too can be cracked with aircrack and similar tools.