# CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking (Part A)

At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof. You need to use

#### Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svasta). Then display the corresponding group IDs.



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



3. **5 points.** 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.

```
<u>User1 password = password</u>
<u>User2 password = Passw0rd!</u>
User3 password = P@ss0rd545!
```

4. **5 points.** 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.

## root@kali)-[~] at mbrow-HASH user1:\$y\$j9T\$atDwwoB9fmIjN8QtKuz9d0\$Q60agOqa1SHA2Yz2F5MwtZtSsYSpPEtCjxmZJMxPQ v3:20048:0:99999:7::: user2:\$y\$j9T\$loXA/1w9zsgcqLotDMVvI/\$qowkZ0pYU6jzqlxKXLDRTA6yscmMQ5Dsoh90I2BPz 0C:20048:0:99999:7::: user3:\$y\$j9T\$8xTwoq7STHcfat9nUfZ.K0\$xrqgkdfY2lcopTRhH.eOi/UvZczzJq0jjfqc8bcrJ q5:20048:0:99999:7::: john -- format=crypt -- wordlist=rockyou.txt mbrow-HASH Using default input encoding: UTF-8 Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/6 41) Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh a512crypt]) 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 password (user1)

#### Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and establish a reverse shell connection with the **admin** privilege to the target Windows 7 VM. Then, create a list of 3 users with different passwords. [**10 Points**] Now, complete the following tasks in sequence:

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



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). 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.).



#### 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 lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)



KEY FOUND! [ F2:C7:BB:35:B9 ] Decrypted correctly: 100%
(root@kali)-[~//VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
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
(Touse have ) ["//Wishare/Lab Resources (2023 Spring)/Lab Resources/Module 5]

2. Decrypt the lab5wpa2-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

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 (39.56 k/s)
Time left: 4 days, 4 hours, 43 minutes, 47 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 89 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
<pre>void@Rall)-[~//VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]</pre>
s # BSSID ESSID Encryption
1       00:16:86:DA:CF:32       ccn1-test       WEP (0 IVs)         2       58:BF:EA:FA:38:B0       Unknown         3       58:BF:EA:FA:38:B0       Unknown         4       98:FC:11:7C:D0:C7       CCNI       WPA (1 handshake)         5       F4:7F:35:39:0A:A0       AccessODU       Unknown         6       F4:7F:35:39:0A:A1       Unknown         7       F4:7F:35:39:0A:A2       MonarchODU       Unknown         9       F4:7F:35:39:0A:A4       eduroam       Unknown
<pre>(root@kell)-[~//VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]</pre>
<pre>(root@kali)-[~//VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]</pre>
(rooter(all))-[~//VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]

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 svatsa is **8**. Thus, I should pick up the file "WPA2-P3-01.cap."

### MD5 of svatsa is fe2943715a4e07c670b242559f5974f8



You can find an online MD5 hash generator or the following command to get the hash of a text string,

0~3	WPA2-P1-01.cap			
4~5	WPA2-P2-01.cap			
6~8	WPA2-P3-01.cap			
9~B	WPA2-P4-01.cap			
C~F	WPA2-P5-01.cap			
L L L Z L L MDE E'L				

Last digit of your MD5 Filename

Then complete the following steps:

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. - 20 points



I will be choosing file WPA2-P4-01.cap

<pre>(root@kali)-[~//VMs     aircrack-ng WPA2-P4- Reading packets, please Opening WPA2-P4-01.cap Read 4225 packets.</pre>	share/Lab Resources 01.cap -w rockyou wait	s (2023 Sp txt	oring)/Lab Resources/M	odule 5]	<u>A</u>
# BSSID	ESSID		Encryption		
1 00:16:B6:DA:CF:2F	CyberPHY		WPA (1 handshake)		
Choosing first network a	is target.				
Reading packets, please Opening WPA2-P4-01.cap Read 4225 packets.	wait				
1 potential targets					
	Aircrack-ng	g 1.7			
[00:00:00] 579/103	03727 keys tested	(1821.54	k/s)		
Time left: 1 hour,	34 minutes, 16 se	conds	0.01%		
	KEY FOUND! [ lin	nkinpark ]			
(root @ kali)-[~//V airdecap-ng -p lin Total number of statio Total number of packet Total number of WEP da Total number of WPA da Number of plaintext da Number of decrypted WE Number of decrypted WE Number of bad TKIP (WP Number of bad CCMP (WP	Mshare/Lab Resour kinpark WPA2-P4-0 ns seen s read 4 ta packets ta packets ta packets P packets P packets A packets A packets A) packets A) packets	<b>ces (2023</b> <b>1.cap</b> - e 5 225 0 5 5 6 6 5 5 2 0 0 0 5 5 2 0 0 0 0 0 0 0 0 0 0 0 0 0	Spring)/Lab Resource CyberPHY	s/Module 5]	
(TOOL Kall)-[~//V	MShare/Lab Resour	ces (2023	Spring)/Lab Resource	s/Module 5]	