## CYSE 301: Cybersecurity Technique and Operations

Assignment M5: Wi-Fi Password Cracking

## Task A: 40 points

Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

Requirements:

- Decrypt the lab4wep.cap file (10 points) and perform a detailed traffic analysis (10 points)
- Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)

## Task B: 60 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 file "WPA2-P5-01.cap."

## MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

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

<pre>root@CS2APenTest:~# echo 5a618cdc3edffd8b4c661e7e root@CS2APenTest:~#</pre>	-n pjiang   md5sum 9b70cele -
Last digit of your MD5	Filename

	· ·····
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

The above files are zipped in a folder named "Lab Resources." You can locate zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under sub-folder "Wireless Traffic".



Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine in order to access it from the Kali VMs.

	> This PC > Local Disk (C:) > VMshare					🕎 Attacker Kali - Enternal Workstation on CV301-PIIAH001 - Virtual Machine Connection		
-		Nome	Date modified	Туре	Size	Fit     Action     Media     Cliphond     Verw     Heip       Bit     Ib     Ib     Ib     Ib     Ib     Ib     Ib       Applications     ID     Ib     Ib     Ib     Ib     Ib     Ib		
ess		Archive	11/5/2019 7:04 PM	Compressed (zipp	3 KB			
nts ; ds ;	*	BookCode-master	1/29/2020 4:19 PM	Compressed (zipp	100 KB	VMshare Nessus Info		
	A	🔞 nmap-7.80-setup	2/24/2020 10:11 AM	Application	26,292 KB			
	A	Jubuntu-18.04.3-desktop-amd64	2/12/2020 10:01 AM	Disc Image File	2,034,000 KB	🛇 Recent 🚯 👪 🗛 🔤 🔤 🎦		
	*	📄 VM - Kali Login info	6/23/2017 2:29 PM	Text Document	1 KB	The starred Archive.zip BookCode- nmap- ubuntu- VM - Kali VMware WPA2-P1-		
		VMware Workstation Login information	2/12/2020 10:06 AM	Text Document	1 KB	the master.zip 7.80-setup. 18.04.3- Login info. Workstatio 01.cap we desktop- txt n Login		
		WPA2-P1-01	3/14/2017 8:40 AM	Wireshark capture	300 KB	amd64.iso information .bt		
						D Documents		

Then complete the following steps:

- Implement a dictionary attack and find the password. 30 points
   Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points