OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

Assignment #5 – Password Cracking

Darren Pritchard 01241796

Password Cracking (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.



Explanation: Here we add both groups, one named cyse301s23 and the other named dprit002, my Midas ID.

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



Explanation: Here 6 users are created, with User1 through User3 assigned to cyse301s23, and User4 through User6 is assigned to dprit002.

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.



Explanation: As shown, this is after updating all 6 users with passwords ranging from very easy to very hard, with solarwinds123 being the easiest password, and the last password being a diceware passphrase using the EFF wordlist, which is the hardest.

EDIT: For the speed of the next step of the process, the password for User2 has been changed to "password".

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.



Explanation: This is the command used to export all 6 passwords to a file called "dprit002-HASH". You can see, in the background, that the file has been made in the home directory.



Explanation: After running the command "john dprit002-HASH –wordlist=rockyou.txt" for less than a minute, the password for User2, "password", is found.

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:



Explanation: Here we have the commands used in command prompt to create 3 users and their corresponding passwords.



Explanation: And here we see that all users have been made correctly.



Explanation: Rather than reinventing the wheel, I will be using the same method as the previous assignment to establish a reverse shell.



Explanation: And then to perform privilege escalation, we background the original session and use ms10_015_kitrap0d.

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



Explanation: This is after running hashdump, failing for some reason to directly write to a file named "dprit002.WinHASH" and just copy-pasting it to leafpad and saving the file as "dprit002.WinHASH."

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.).



explanation: After the VM getting deleted, I repeated all the steps but instead made all the passwords "password" for every user, hence there is only one hash to crack.

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.).

		Attaci	ker Kali - External Workstation on C	V301-DER/T002	- 8 × /		
oplications 👻 🛛 Places 👻	🗈 Terminal 👻		Sun 04:53			1,*	メ 🗤 🖰 -
			Terminal				000
Ello Edit Minu Con	rch Terminal Hele						
File Edit View Sear	Leasessaan	414	5276761776.02.25.22.	24.49 0400	pagafila cyc		
000113/0/1-X1WX	104050522004057015	111	5220701770-03-25 25:	24:46 -0400	pagerite.sys		
meterpreter > uploa	ad ca setup exe						
uploading : ca	a setup.exe -> ca set	tup.exe					
Uploaded 7.86 M	TIB of 7.86 MiB (100.	.0%): ca	a setup.exe -> ca set	up.exe			
uploaded : ca	<pre>setup.exe -> ca_set</pre>	tup.exe					
<pre>meterpreter > ls</pre>							
Listing: C:\							
			STRUCT DESIGNED THE D				
Mode	Size	Туре	Last modified		Name		
10777	(bishing the fu			0.100	+nl- ni-		
40777 FWXFWXFWX	8102	01F	2009-07-13 22:36:15	-0400	SRECYCLE.BIN		
1004444/111	4096	dir	2017-08-23 15:08:55	-0400	Boot		
40777/rwxrwxrwx	4050	dir	2009-07-14 00:53:55	-0400	Documents and Setti	DAS	
40777 / rwx rwx rwx	0	dir	2009-07-13 22:37:05	-0400	Perflogs	1193	
40555/r-xr-xr-x	4096	dir	2009-07-13 22:37:05	-0400	Program Files		
40777/rwxrwxrwx	4096	dir	2009-07-13 22:37:05	-0400	ProgramData		
40777/rwxrwxrwx	0	dir	2017-08-23 11:14:31	-0400	Recovery		
40777/rwxrwxrwx	8192	dir	2017-08-23 14:09:57	-0400	System Volume Infor	mation	
40777/rwxrwxrwx	0	dir	2017-08-23 11:44:42	-0400	Tools		
40555/r-xr-xr-x	4096	dir	2009-07-13 22:37:05	-0400	Users		
40777/rwxrwxrwx	16384	dir	2009-07-13 22:37:05	-0400	Windows		
100777/rwxrwxrwx	24	fil	2009-07-13 22:04:04	-0400	autoexec.bat		
100444/rr	383562	fil	2017-08-23 15:08:55	-0400	bootmgr		
100777/rwxrwxrwx	8244106	fil	2023-04-16 04:48:19	-0400	ca_setup.exe		
100666/rw-rw-rw-	10	fil	2009-07-13 22:04:04	-0400	config.sys		
60611570/r-xrwx	160714841537937391	111	5101854894-08-31 00:	01:04 -0400	pagefile.sys		
motorprotor > chall							
La Failed to snaw	shell with thread i	impersor	ation Retrying with	out it			
Process 2852 create	ed.	Luper 30	iscion. Acciping with	out It.			
Channel 4 created.							
Microsoft Windows	[Version 6.1.7600]						
Copyright (c) 2009	Microsoft Corporatio	on. All	l rights reserved.				
C:\>net user dprit@	002 password /add						
net user dprit002 p	assword /add						
The command complet	ed successfully.						
Culonet local second	administrations doubt	+002 (2)	14				
C: (>net localgroup	administrators dprit	1002 /ac	10				

explanation: after uploading ca_setup.exe we add my MIDAS as a user and elevate it to administratorlevel privileges



Explanation: me starting up rdesktop, yet failing to actually launch it for an absolutely unknown reason



explanation: due to repeated technical errors I just went to the windows 7 VM, logged in, installed CA. This is generally the same steps as what it would be otherwise, just not using rdesktop

	Mew Careligues Tools Help Brute-Force Attack			
Cracker	Charaet Predefined [abcdetghiklmoppet.rvwgs012345678	-	Password length Min 1	IT Hash
I NTLMU I MS-Cas I MS-Cas I WL fil I I Cisco II I MS-Cas I VICA I VICA	Control Keyrpace 8.1880514273234411E+024 Key Rate 7374622 Past/Sec	Time Left 351 988	v/H83	84067EAEE8F. 1D6CFE0016. D79C7F57C09 4F49C406510 4F49C406510 4F49C406510 846F7EAEE8F.
	, 1201 - CHITCH THE INF	-	Stop Eul	

Explanation: and this is me bruteforcing passwords

	· [bin] File View Con	nfigure Tools Help	9. «\) mai mai	164		0 7 i		
rome	AUTH RESET HT				cou 100 w			
-	Content Street Street	K 🖼 Sniffer 🥑 Cracker	Traceroute		CDU Wireless	D Query	Transie and the second	
≝⊅	Cracker	User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	
		Administrator	* empty *		* empty *	AAD3B435B51	31D6CFE0D16	
ŪΎ	MS_Cache Hacher	Cuert	* empty *		password	AAD38435851	21D6CEE0D16	
	PWI files (0)	HomeGroupUser	* empty *		empty	AAD38435851	2079C7E57C09	
	Cisco IOS-MD5 H	AUser1	* empty *	*	Password	AAD3B435B51	A4F49C406510.	
	Cisco PIX-MD5 Hi -	Duser2	* empty *	*	Password	AAD38435851	A4F49C406510	
	APOP-MD5 Hash	SUser3	* empty *	*	Password	AAD3B435B51	A4F49C406510	
	CRAM-MD5 Hash	🕄 Window 7	* empty *	*	password	AAD3B435B51	8846F7EAEE8F	
	OSPF-MD5 Hashe							
	RIPv2-MD5 Hashe							
	VRRP-HMAC Has							
	VNC-3DES (0)							
	MD4 Hashes (0)							
	MD5 Hashes (0)		N					
	SHA-1 Hashes (0)		43					
	B DIDEMD 160 Link							
	160 KIPEIVID-100 Hash	4	m				F.	
	Keins PreAuti Ha +	LM & NTLM Hashes						
1/1/8	1							
11	nttp://www.oxid.it						he.	
						2		

explanation: after restarting the bruteforce attack and starting from "password," thus automatically cracking all of the passwords at once

	Dictionary Attack			
70	Dictionary			1
and a C	File	Position		
Decoders	C.\Phogram Files\Cain\Wordlists\Wordlist	Lod		IT Hash
BIM&P				1D6CFE0D16
NTLM.	- Key Rate	Optiona		846F7EAEE8F
MS-Ca	1890086 Pass/Sec	P Asis Password		106CFE0016
Cisco H	Dictionary Position	Revenue PASSWORD	(DROWSSAP)	4F49C406510
Cisco P	3366016 (97%)	Investor Pater - Pater in P Lowerson Patchultin	D - persword!	4F49C406510
APOP-		P Uppergase (Password		4F49C406510
CRAM-	Current password	Vian, sub permi Pava.	PAGEPadia_PAtter_PAtter	846F7EAEE8F
+ OSPF-N		Two numbers Hotsid IIr	ute (Pauli Paul)	
+ VRRP-H				
VNC-3	Plaintext of 8846F7EAEE8FB1	17AD06BDD830B7586C is pa	ssword	
MD2 H	Plaintext of A4F49C406510BE	CAB6824EE7C30FD852 is Pa	ssword	
nd MD4 H				
SHA-1				
SHA SHA-2				
B RIPEME				
Kerb5 F				
- m		T	Rise 1	
million mail			Stop E.M.	

explanation: dictionary attack, using the wordlist.txt in CA

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)



explanation: after using aircrack-ng on lab4wep.cap and selecting network 1, which is the only WEP one, we get a key of F2:C7:BB:35:B9



explanation: And after using airdecap we have 142,415 decrypted WEP packets

Ethernet · 19 IPv4 · 91 IPv6 · 7 TCP · 238 UDP · 84 Address A * Address B Packets Bytes Packets A + B Bytes A + B Packets B + A Bytes B + A Ref 3 00:16:b6:da:cf:30 a4:5e:60:d3:93:65 7,984 8,069 k 6,283 7,895 k 1,701 174 k 0.0 00:16:b6:da:cf:30 24:e3:14:7f:66:11 11,511 9,001 k 6,254 8,568 k 5,257 4328 k 56. 00:16:b6:da:cf:32 01:80:c2:00:00:0 114 5,928 114 5,928 k 0	art Duration										
Address A< Address B	art Duration						UDP - 84	TCP · 238	v4 · 91 IPv6 · 7	IP	Ethernet - 19
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	ALC: AND ALCOIL	Rel Start	Bytes B → A	Packets B → A	Bytes A → B	Packets A → B	Bytes	Packets	Address B	-	Address A
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	1158 314.251	0.281158	174 k	1,701	7,895 k	6,283	8,069 k	7,984	a4:5e:60:d3:93:65	30	00:16:b6:da:cf:
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	18387 254.947	56.418387	432 k	5,257	8,568 k	6,254	9,001 k	11,511	24:e3:14:7f:66:11	30	00:16:b6:da:cf:
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	0000 307.999	0.000000	0	0	5,928	114	5,928	114	01:80:c2:00:00:00	32	00:16:b6:da:cf:
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	0590 276.55	37.980590	0	0	5,255 k	122,620	5,255 k	122,620	ff:ff:ff:ff:ff:ff	:7e	00:c0:ca:82:c3:
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	23711 0.0000	40.923711	46	1	0	0	46	1	a4:5e:60:d3:93:65	0:02	01:00:5e:00:00
01:00:5e:00:00:fb a4:5e:60:d3:93:65 26 5,290 0 0 26 5,290 40 01:00:5e:00:00:fb 24:e3:14:7f:66:11 8 696 0 0 8 696 59 24:e3:14:7f:66:11 ff:ff:ff:ff:ff 22 1,224 22 1,224 0 0 56 24:e3:14:7f:66:11 33:33:00:00:00:02 5 350 0 0 58 24:e3:14:7f:66:11 33:33:00:00:00:016 3 270 3 270 0 0 58 24:e3:14:7f:66:11 33:33:00:00:00:016 12 1,448 12 1,448 0 0 0 58 24:e3:14:7f:66:11 33:33:00:00:00:02 a4:5e:60:d3:93:65 2 220 0 0 2 20 33 33:33:00:00:00:02 a4:5e:60:d3:93:65 2 20 0 0 2 20 36 33:33:00:00:00:02 a4:5e:60:d3:93:65 28 6,426 0 0 0 33:33:00:00:00:02 a5:46:40 <td>0784 0.0722</td> <td>59.520784</td> <td>92</td> <td>2</td> <td>0</td> <td>0</td> <td>92</td> <td>2</td> <td>24:e3:14:7f:66:11</td> <td>0:02</td> <td>01:00:5e:00:00</td>	0784 0.0722	59.520784	92	2	0	0	92	2	24:e3:14:7f:66:11	0:02	01:00:5e:00:00
	5996 210.978	40.295996	5,290	26	0	0	5,290	26	a4:5e:60:d3:93:65):fb	01:00:5e:00:00
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	37856 233.647	59.587856	696	8	0	0	696	8	24:e3:14:7f:66:11	0:fb	01:00:5e:00:00
24:e3:14:7f:66:11 33:33:00:00:00:02 5 350 5 350 0 0 56. 24:e3:14:7f:66:11 33:33:00:00:00:16 3 270 3 270 0 0 58. 24:e3:14:7f:66:11 33:33:00:00:00:06 12 1,448 12 1,448 0 0 113. 33:33:00:00:00:00:16 a4:5e:60:d3:93:65 4 280 0 0 4 280 39. 33:33:00:00:00:01:6 a4:5e:60:d3:93:65 2 220 0 0 2 220 36. 33:33:00:00:00:01:6 a4:5e:60:d3:93:65 2 220 0 0 28 6,426 35. 33:33:00:00:00:02 f8:b1:56:c5:45:59 6 966 0 0 28 6,426 35. 33:33:00:01:00:02 f8:b1:56:c5:45:59 6 966 0 0 8. 34:5e:60:d3:93:65 f8:b1:56:c5:45:59 2 164 0 0 3. a4:5e:60:d3:93:65 f8:b1:56:c5:45:59 2 164 0 0 2 164 7.	9924 235.586	56.419924	0	0	1,224	22	1,224	22	hernet - 19 IPv4 - 91 IPv6 - 7 TCP - dress A × Address B Pack 16:b6:da:cf:30 a4:5e:60:d3:93:65 16:b6:da:cf:32 01:80:2:00:00:00 16:b6:da:cf:32 01:80:2:00:00:00 10:05:2:00:00:00 10:05:2:00:00:00 cc:ca:82:c3:7e ff:ff:ff:ff:ff:ff 11 00:5e:00:00:02 24:3e:60:d3:93:65 00:5e:00:00:02 00:5e:00:00:05 24:3e:60:d3:93:65 00:5e:00:00:00 00:5e:00:00:05 24:3e:14:7f:66:11 83:33:00:00:00:02 e3:14:7f:66:11 33:33:00:00:00:00 e3:14:7f:66:11 33:30:00:00:00:16 a4:5e:60:d3:93:65 33:00:00:00:16 a3:30:00:00:00:16 a4:5e:60:d3:93:65 33:00:00:00:16 33:00:00:00:16 a4:5e:60:d3:93:65 53:30:00:10:00:2 33:00:00:00:16 a4:5e:60:d3:93:65 53:30:00:10:00:2 s3:00:00:00:16 a4:5e:60:d3:93:65 55:5:45:59 5e:60:d3:93:65 ff:ff:ff:ff:ff:ff Image: State		
24:e3:14:7f:66:11 33:33:00:00:00:16 3 270 3 270 0 58. 24:e3:14:7f:66:11 33:33:00:00:00:16 12 1,448 12 1,448 0 0 11.33.33:00:00:00:00:16 32.00:00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:16 32.00:00:00:00:16 32.00:00:16 32.00:00:00:16 32.00:00:16<	7694 9.2314	56.517694	0	0	350	5	350	2 5	33:33:00:00:00:02	11	24:e3:14:7f:66:
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	6720 2.7307	58.136720	0	0	270	3	270	3	33:33:00:00:00:16	11	24:e3:14:7f:66:
33:33:00:00:00:02 a4:5e:60:d3:93:65 4 280 0 0 4 280 39 33:33:00:00:00:01 a4:5e:60:d3:93:65 2 220 0 0 2 220 36 33:33:00:00:00:01:6 a4:5e:60:d3:93:65 2 220 0 0 2 220 36 33:33:00:00:00:01:6 a4:5e:60:d3:93:65 28 6,426 0 0 28 6,426 35 33:33:00:01:00:02 f8:b1:56:c5:45:59 6 966 0 0 6 966 244 a4:5e:60:d3:93:65 ff:ff:ff:ff:ff:ff:ff:ff 56 6,340 56 6,340 0 0 3 a4:5e:60:d3:93:65 ff:ff:ff:ff:ff:ff:ff:ff 9 915 0 0 3 3	32442 179.403	113.932442	0	0	1,448	12	1,448	12	33:33:00:00:00:fb	11	24:e3:14:7f:66:
33:33:00:00:00:16 a4:5e:60:d3:93:65 2 220 0 0 2 220 36. 33:33:00:00:00:16 a4:5e:60:d3:93:65 28 6,426 0 0 28 6,426 33:33:00:00:10:00:16 a4:5e:60:d3:93:65 28 6,426 0 0 28 6,426 32:33:00:00:10:00:02 f8:b1:56:c5:45:59 6 966 0 0 6 966 24:44:5e:60:d3:93:65 f6:56:60:63:93:65 f6:56:60:63:93:65 f6:56:60:63:93:65 f6:56:60:63:93:65 f8:b1:56:c5:45:59 f6:46 0 0 0 33:45:e:60:d3:93:65 f8:b1:56:c5:45:59 f1:64 0 0 2 164 7.9 f8:b1:56:c5:45:59 f1:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:f	0469 4.396	39.890469	280	4	0	0	280	4	a4:5e:60:d3:93:65	0:02	33:33:00:00:00
33:33:00:00:00:1b a4:be:60:d3:93:65 28 6,426 0 0 28 6,426 35, 33:33:00:00:00:1c f8:b1:56:c5:45:59 6 966 0 0 6 966 24 a4:5e:60:d3:93:65 ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.	91134 3.0051	36.091134	220	2	0	0	220	2	a4:5e:60:d3:93:65	0:16	33:33:00:00:00
33:33:00:01:00:02 78:b1:56:c5:45:59 6 966 0 0 6 966 244 a4:5e:60:d3:93:65 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	09728 215.565	35.709728	6,426	28	0	0	6,426	28	a4:5e:60:d3:93:65	0:fb	33:33:00:00:00
a4:5e:60:d3:93:65 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	08894 62.979	244.208894	966 .	6	0	0	966	6	f8:b1:56:c5:45:59	0:02	33:33:00:01:00
a4:5e:60:03:93:65 ts:b1:56:c5:45:59 z 164 0 0 z 164 7.5 f8:b1:56:c5:45:59 ff:ff:ff:ff:ff 9 915 9 915 0 0 3.3	56// 310.96/	3.1/66//	0	0	6,340	56	6,340	56		5:65	a4:5e:60:d3:93
18:D1:20:C2:42:29 IT:IT:IT:IT:IT:IT:IT:IT:IT:IT:IT:IT:IT:I	7204 67.483	7.987204	164	2	015	0	164	2	18:D1:56:C5:45:59	5:05	a4:5e:60:d3:93
		Jiar JACE				,					10.02.00.00.10.
R									G		31
Name resolution Limit to display filter Absolute start time	Conversation T	Conv				osolute start time	At	splay filter	🗌 Limit to di	tion	Name resolut
Copy • Follow Stream.	Graph X	Grap	Follow Stream	Copy -							Help

explanation: And looking at the conversations in the decrypted cap file, we see the ethernet conversations that took place in this capture

			ashura C	totictics	Tolor	hony Mirolan	Tools Help					
					W	ireshark · Conve	sations · lab4w	ep-dec.cap			0	0
Ethernet - 19	IPv4 · 91	IPv6 ·	7 TCP	· 238	UDP -	84				à		
Address A	* Address B	3	Packets	Byte	es P	ackets $A \rightarrow B$	Bytes A → B	Packets $B \Rightarrow A$	Bytes $B \rightarrow A$	Rel Start	Duration	Bit
0.0.0.0	255.255.2	255.255		3	1,026	3	1,026	C	0	35.436838	20.9831	
1.1.1.1	192.168.2	.10		2	478	0	0	2	478	52.138789	6.3677	
8.8.8.8	192.168.2	.10		53 5	5,969	31	4,190	22	1,779	19.049155	194.8792	
12.188.251.151	192.168.2	.10		76	59 k	56	57 k	20	1,734	69.380486	32.2775	
17.110.229.150	192.168.2	.10		17	4,414	2	132	15	4,282	40.810597	63.0891	
17.154.66.120	192.168.2	.10		27	11 k	15	10 k	12	984	19.455781	2.4393	
17.154.66.125	192.168.2	.10		1	78	0	0	1	78	19.450661	0.0000	
17.155.127.222	192.168.2	.48		13	754	7	406	e	348	59.878149	4.8218	
17.155.127.223	192.168.2	.48		7	406	3	174	4	232	60.013316	4.2484	
17.167.138.20	192.168.2	.10		16	5,295	6	4,416	10	879	44.283237	0.6989	
17.167.139.39	192.168.2	.10	8	79	14 k	40	6,083	39	8,036	103.994884	37.9770	
17.167.139.91	192.168.2	.10		26 6	6,079	4	943	22	5,136	213.948837	0.4194	
17.167.192.128	192.168.2	.10		15	2,961	10	2,387	5	574	216.582723	1.9242	
17.167.192.176	192.168.2	.10		15 2	2,449	9	1,858	e	591	218.994369	0.5034	
17.167.194.148	192.168.2	.10		1	66	1	66	0	0	218.674884	0.0000	
17.172.232.11	192.168.2	10		13	2.182	3	344	10	1.838	40.596547	3.1541	
17.172.232.12	192.168.2	.10		2	108	0	0	2	108	40.891493	0.0000	
17.172.232.176	192.168.2	.48		29 6	6.588	13	3.335	16	3.253	302.862797	2.0691	
17.172.232.220	192.168.2	.48		6	412	2	148	4	264	302.890957	0.1812	
17,172,238,48	192,168,2	.48		25	7.232	11	3.072	14	4.160	113.187930	67.1762	
17,172,238,51	192,168,2	48		6	424	3	214		210	302.863821	0.1449	
17.172.239.43	192.168.2	.10		2	108	0	0	2	108	41.405090	0.0000	
17.172.239.62	192,168,2	.48		6	412	2	148	4	264	302.878669	0.1239	
1							2.1					
Name resolut		Limit t	o display	filter		Absolute start t	ime			1	Conversation	Ty
								Com	. Collour Ci		and I	* (1)
								Сору			arophine	- <u>C</u>

explanation: As we can see, much of this traffic is from 192.168.2.10

Applica	tions 🔻	Places 🕶	🔜 Wireshark 🔻	Sun 05:48		1 🗯	× 40) () -
			Wireshark - Res	solved Addresses · /root/CYSE301/Module V-Wireless Security/lab4wep-dec.cap	0		
	File E Image: Apple to the second seco	dit View Go	$\begin{array}{c} 220.243.235.10\\ 209.249.181.25\\ 70.186.30.27\\ 70.186.30.27\\ 70.186.28.21\\ 68.181.195.4\\ 23.229.176.66\\ 17.167.139.39\\ 108.160.172.225\\ 70.186.30.23\\ 112.90.86.16\\ 173.254.183.20\\ 17.172.239.130\\ 23.195.82.217\\ 141.85.166.61\\ 140.98.193.116\\ 17.174.2.5\\ 104.72.16.17\\ 17.167.138.20\\ 198.84.60.198\\ 223.252.199.5\\ 220.243.235.13\\ 173.194.121.58\\ 70.186.28.24\\ 17.172.239.106\\ 70.186.30.26\\ 70.186.30.26\\ 108.160.172.193\\ 104.72.29.195\\ 70.186.30.22\\ 83.167.185.35\\ \end{array}$	<pre>netease.video.ourdvs.com docs.netgear.com encrypted-tbn0.gstatic.com hpc-mirror.usc.edu technitium.com p19-keyvalueservice.icloud.com.akadns.net d.v.dropbox.com encrypted-tbn0.gstatic.com updatecenter.qq.com www.cacetech.com us-courier.push-apple.com.akadns.net e673.e9.akamaiedge.net www.upb.ro standards.ieee.org st14p02sa.guzzoni-apple.com.akadns.net e3191.dscc.akamaiedge.net p17-calendars.icloud.com.akadns.net packetstormsecurity.org music.163.com netease.video.ourdvs.com pagead46.1.doubleclick.net encrypted-tbn0.gstatic.com us-courier.push-apple.com.akadns.net encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com encrypted-tbn2.gstatic.com e6987.g.akamaiedge.net encrypted-tbn0.gstatic.com e6987.g.akamaiedge.net encrypted-tbn0.gstatic.com</pre>		Tell 0.6 Tell 192. 2.168.2.1 ITCP AC not capt 57 Tell 57 Tell 57 Tell 57 Tell 57 Tell 9:c2:00:0	xpression +
	0000 0010 0020 0030	01 80 c2 00 00 16 b6 da cf 30 80 02 a5 a5 a5 a5	83.167.185.35 17.172.232.170 17.173.66.101 174.35.27.77 17.172.232.197 17.172.232.197 17.172.238.48 17.172.232.220 70.186.28.27 17.249.105.246 17.172.239.12 173.194.121.57 70.186.28.23	<pre>beauty.klben.het us-courier.push-apple.com.akadns.net p48-buy.itunes-apple.com.akadns.net n2.panthercdn.com us-courier.push-apple.com.akadns.net us-courier.push-apple.com.akadns.net encrypted-tbn2.gstatic.com api.smoot-apple.com.akadns.net us-courier.push-apple.com.akadns.net encrypted-tbn2.gstatic.com api.smoot-apple.com.akadns.net us-courier.push-apple.com.akadns.net us-courier.push-apple.com.akadns.net us-courier.push-apple.com.akadns.net us-courier.push-apple.com.akadns.net encrypted-tbn2.gstatic.com </pre>	*		
	07	lab4wep-dec.ca		Show Show	ĸ	(100.0%)	Profile: Default

Explanation: And here we can see some of the resolved addresses, including music.163.com, apple.com, and dropbox.com

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



Explanation: Similar process to before, decrypting using the rockyou.txt dictionary and aircrack-ng



Explanation: After decrypting the traffic with airdecap, using the passphrase of "password" and the WPA ESSID



explanation: Resolved addresses of this traffic, mostly google plus traffic.



Explanation: Most of this traffic is also from 192.168.2.23

Film Field Aligna	Go Cantu		alura d	Chatletine	Talashanu Min	alare Toole H	do.					
					Wireshark · Co	nversations - lab	wpa2-dec.cap				0 (
Ethernet - 6	IPv4 - 40 1	Pv6 - 3	TCP	- 191	UDP · 28							
Address A	Address B	Pac	kets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	+ Bits/	s A
8.8.8.8	192.168.2.23		22	1,86	3	1 203	21	1,660	0.033280	23.2452	2	
128.82.112.29	192.168.2.23		1,110	305	k 14	3 192 k	967	113	6.316416	17.9094		
70.186.30.26	192.168.2.23		128	16	k .	4 1.916	124	14	4.200192	17.0169		
70.186.30.20	192.168.2.23		89	9,77	0 0	0 0	89	9,770	4.236032	16.8669	a	
70.186.30.25	192.168.2.23		151	14	k	3 1.099	148	131	4.231424	16.4680	0	
31.13.73.36	192.168.2.23		6	3,48	31	1 1.464	5	2,01	6.398848	14.9969		
104.90.71.242	192.168.2.23		20	3,77	3	2 1.580	18	2.193	6.400384	13.7235		
70.186.28.26	192.168.2.23		18	3,27	8	0 0	18	3.278	6.332800	13.2458	1	
104.90.92.117	192.168.2.23		55	9,31	8	3 4.542	52	4,776	6.359424	13.1152		
192.168.2.23	192.229.163.	25	29	2.42	4 2	2.424	0	(6.346112	13.0968	3	
74.125.29.95	192.168.2.23		13	1.32	6	0 0	13	1.326	6.359424	12.8577		
70.186.31.35	192.168.2.23		20	2.06	51	0 0	20	2.06	7.575552	12.5386	÷	
70.186.30.21	192.168.2.23		204	25	k	6.426	195	18	4.206336	10.8044		
70.186.30.22	192.168.2.23		11	1.85	5	1 666	10	1.189	4.207360	10.7978		
70.186.28.24	192.168.2.23		8	1.27	3	0 0	8	1.27	4.234496	10.7732		
70.186.28.20	192 168 2.23		26	4.15	7	0 0	26	4.15	4.246784	10.7594	i i	
31.13.73.7	192.168.2.23		17	4.15	0	2 2.928	15	1.22	7.910912	7.9340		
70.186.30.81	192.168.2.23		12	2.19	0	1 1.464	11	726	5 7.916032	7.9022		
192.168.2.1	192.168.2.23		6	27	6	0 0	6	276	0.227328	6,4476		
17.172.232.82	192.168.2.23		5	56	9	3 336	2	233	1,735808	2.1961		
17.110.226.165	192.168.2.23		8	98	5	1 135	7	850	3.004608	1.7875		
74.125.136.94	192.168.2.23		9	3,31	9	0 0	9	3,319	19.587328	1.3190		
173.194.205.95	192.168.2.23		22	4,70	4 1	0 0	22	4,704	20.175104	1.0901		
			-									
🗇 Name resoluti		Limit to	display	filter	Absolute st	art time				Convers	ation Ty	pes -
Help							Co	y + Follo	v Stream.		*0	lose
Theth							co	7 1 sette				tose

We can see here that while most of the time was spent in communication with 8.8.8.8 (google DNS) the next most communicated with address is 128.82.112.29

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." 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,

• The above files are zipped in a folder named "Lab Resources." You can locate the 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 the sub-folder "Wireless Traffic."

• Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine to access it from

the Kali VMs (you can use either Kali to complete the assignment).

Figure left: Windows Host Machine Figure right: VMshare folder on Kali Linux

Then complete the following steps:



Explanation: the MD5 of my MIDAS ID is as shown and ends in "b" so my file is "WPA2-P4-01.cap "

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



Explanation: after the dictionary attack we see the passphrase is linkinpark, rest in peace chester



explanation: after cracking

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored

from this encrypted traffic file. -10 points



Explanation: the suspicious traffic in this file mostly comes from 192.168.1.127 and seems to have a large number of destinations. In particular here I'm looking at the traffic to 70.186.29.17, though there are many other addresses that have been communicated with by 192.168.1.127.

Applications * Places *	Wireshark 🛪 Mon 03:23	1 🛋 🗡 🕫 🕘 👻
	Wireshark - Resolved Addresses - /root/WPA2-P4-01-dec.cap	
File Edit View Ge Image: Constraint of the second	<pre># Resolved addresses found in /root/WPA2-P4-01-dec.cap # Comments # No entries. # No entries. # No entries. # losts # 21 entries. 52.220.165.0 lb-im-11-1803639322.ap-southeast-1.elb.amazonaws.com 12.90.11.94 vzbfmbt.tcdn.qq.com 65.121.211.90 a474.srj1.atsarjp.net.ddba8b66.1.cn.akasrjpcn.net 172.217.5.65 googlehosted.l.googleusercontent.com 52.221.30.167 lb-im-11-1803639322.ap-southeast-1.elb.amazonaws.com 24.24.144.168 lb-im-11-1803639322.ap-southeast-1.elb.amazonaws.com 26.3205.149.88 m.qpic.on.tcdn.qq.com 172.217.4.131 ssl.gstatic.com 66.198.24.243 www.tabbao.com.danuoyi.tbcache.com 182.202.33.9 lb-im-11-1803639322.ap-southeast-1.elb.amazonaws.com 216.58.193.193 uwnthesis-files-wordpress-com.cdn.ampproject.org 183.60.48.166 vzbfmht.tcdn.qq.com 183.60.48.166 vzbfmht.tcdn.qq.com 183.60.48.166 vzbfmht.tcdn.qq.com 283.205.151.139 aeventlog.beacon.qq.com 183.36.153.16 hpc-video.cn.ccgslb.com.cn 283.205.149.254 m.qpic.on.tcdn.qq.com 283.205.149.254 m.qpic.on.tcdn.qq.com 283.205.149.254 m.qpic.on.tcdn.qq.com 283.205.149.85 m.qpic.qpic.qpic.qpic.qpic.qpic.qpic.qpic</pre>	Activate Windows Go to Settings to activate Windo
	✓ Show- Show- Scancel ✓ OK	1
Ø Z Transmission		i) Profile: Default

We can see here the resolved addresses in this capture file, seemingly a lot of interaction with AWS servers. Though, imaginably, it's probably because ODU uses AWS.

Page 100												
Ethernet · 2	IPv4 · 50	IPv6	TCP · 66	UDP - 39	D. J. L. A. D.	D	D. J. L. D. J.	0	0.10	D	. Disc	
Address A	Address t	477	Packets	Bytes	Packets A → B	Bytes A + B	Packets B + A	Bytes B → A	Reistart	Duration	- Bits/	5
42.02.94.2	102.168.1	127	22	2 0 8 0		2 22/		1 25	1 0.041104	40.1/3		
192.100.1.1 66 109 24 242	102 160 1	127	33	3,969	23	3,224	•	1 0	1.010888	30.7933	200	
66 108 24 234	192.100.1	127	3	643		100	5	1 20	10 137740	37.037:	es Form	
172 217 4 142	192.108.1	127	17	2 371	17	20.	1	5 50	10.13//40	22.4702		
60 20 200 140	192.100.1	127	15	3,2/1	13	4.015		0	19.903608	10.6268	2011 2011	
73 20 202 51	192.108.1	137		7,003		4,01	2	4 27	4 00 4303	19.0303	Kalini Kalini	
103 169 1 137	192.108.1	151 102		1002		0,750	c	4 27	0 4 4 6 4 7 1	16.7140	3	
172 217 4 122	203.205.	101.195	50	190	40	511	3	2 13	10 /02120	10.070		
102 169 1 127	216 59 10	12 202	10	5 902		1 010		4 4.09	7 17 740146	12 7240		
192 168 1 127	216 58 10	2 102	11	7 821		555	2	9 7.26	20 701114	11 0471		÷
192 168 1 127	216.58.19	3 195	24	25 k		720		7 74	20.924751	10.7916		
172 217 5 65	192 168 1	127	23	15 k	18	151		5 36	5 20 780362	10.650		
112 90 11 94	192.168.1	127	80	94 k	64	931	k i	6 90	8 943693	10.3354	0	
172 217 4 129	192 168 1	127	7	4 480	6	4 400	S	1 8	20 848975	9 7158		
192.168.1.127	205.204	101.107	9	845	5	576	5	4 26	32,757319	8.2811	10	
183,95,153,10	192,168,1	127	3	162	2	108	3	1 5	26,268816	6.4568	2	
31.13.69.195	192.168.1	127	6	605	2	140	5	4 46	5 32.104473	6.1674	í.	
60.205.109.26	192.168.1	127	2	171	ā	()	2 17	1 17.939094	6.1480	ā. —	
31.13.69.197	192.168.1	.127	3	810	2	637	7	1 17	3 21.483920	5.4203		
184.173.21.66	192.168.1	.127	30	10 k	20	9,172	2 1	1,14	6.281098	5.3518		
183.61.49.155	192.168.1	.127	4	272	2	140)	2 13	3.580682	5.3497		
192.168.1.127	203.205.	158.84	15	6,618	4	792	2	11 5,82	5 7.790602	5.3267		
<u>(</u>			•••								a ()	
		Limit	to display fil	ter	Absolute start	time				Conversati	on Type	\$ <i>.</i> :

Explanation: We see here that 192.168.1.127 spent the most time talking to 42.62.94.2, followed by 192.168.1.1, but 192.168.1.127 looks like it's talking to everyone. I think 192.168.1.127 was doing a thorough nmap scan of the network.