## OLD DOMINION UNIVERSITY

#### CYSE 301 Cybersecurity Techniques and Operations

# Assignment #5 Password Cracking

Bradley Hamilton 01240068 TASK A

1. Linux Password Cracking:



Figure 1 Groups being made with CYSE301s24 and MIDAS ID



Figure 2 Screenshot of Users being added to groups



Figure 3 Screenshot of groups listing users



Figure 4 Screenshot of individual password hashes



Figure 5 Screenshot of changing user passwords to easy, medium, and hard passwords



Figure 6 Screenshot cracking passwords using –format=crypt command



Figure 7 shows password being cracked for one of the users

Password cracking is very time consuming and the screenshot above shows one being cracked, the following screenshots show two others being revealed



Figure 8 second password revealed



Figure 9 Screenshot of third password cracked.

Task B



1. Windows Password Cracking:

Figure 10 Screenshot of new users created on Win 8 and reverse shell connection to Win 7 VM

💌 Taper Angewant HS - Updawe X Antigeneer S - Research Erst X STER Visual Lab Street	las 🔹 🧰 Gaskalivasa	t Rutal	<ul> <li>Siliseastetataantiit</li> </ul>	* ±		- 1	6
6 0 3 bit-connect.com/https://dit3/guarancie.idc.com/stg/guarancie/#/dem	t/Mag1AGMAbNacWhe					C ** G \$ 1	
E Windows Ton CYER-HAMMER Vinue Michael Connection	🕎 Attacker Kali - Enternal Work	Litation en C1301-B	1 × Hand Machine Cornectio	- 1 <u>1</u> × .			
b. 0 0 0 0 0 0 0 b b 2 0	Pile Actor Media Vie	ev Help					
	b 0 8 8 0 u P	<ul> <li>              日日         </li> </ul>					
	🔠 💷 🖿 🖪 🕸		E 3 4 E			🖬 (genman(XXX 🚯 🏦	8
Revenue Landouri					root@balk -		
AC	<b>1</b>	- 18		File Actions Edit View Help			
	Within Hours	1014 1-1	File Actions Edit View	1) stell		192.158.217.3:5525 → 19 2.168.217.2:52719 (192.1	
Choose the account you would like to change	COMPANY AND			12 shett		65.217.2) 192.168.217.3:5525 → 19	
50000			ising default input encoc. In password hashes loader			2.160.217.2:45518 (192.1 68.217.2)	
A Window 7 bradey				13 shell		192.168.217.3:5525 -* 19 2.168.217.2:8683 (103.16	
PL Advertised	Trash		sing default input encid	th shall		8.217.2) 100 (68 212.1:5535 → 10	
(MARKA)			oaded 6 password hashes bot 1 (algorithm Tildesc			2.168.217.2:52485 (192.1	
User1 User2 Standard Standard			ost 2 (algorithm specifi III rus 2 Open#P thream	15 meterpreter x86/window	IS WENDOWS7 WENDOW 7 B NEW	102.168.217.3:5525 → 10	
Pactword protected	0		receeding with single, i		- Contract	65.18.9)	
Many	File System		g gragtagt01 14.64% 1/3	mit explort( annue the firment			
User3 Sentecture Guest		and the second	g eleelestan us.30% 2/3	nais exploit (passion from hits pass			
Provod pritected	the second		arning: Only 17 candidat	[.] Started reverse TCP handler or	192.168.217.214444		
disease.			larning: Only 17 candidat	[4] UAC is Enabled, checking level [4] UAC is set to Default			
Whith is a see account	Home		Toceeding with wordList: 2345676 (user1)	<ul> <li>RypansillsC can bygats this sett</li> <li>Part of Administrators group?</li> </ul>	ing, continuing Continuing		
			g 8 80102145 8.65X 2/2 ( 7854022 (unirs)	I lalcoded the agent to the file	aveter		
(#2) (B) Security Canton	and the second se		g 0100 00100 1.60X 2/3 ( banaord] (usar2)	Meterpreter stager executable	73882 bytes long being upla	naded	
Gis to the main User Administration			g didb:09:31 0.215 2/2 (	Meterproter session 16 ogened	(192-108-217-3:4444 → 192	168.217.2:11724) ot 2024-07	
	VMshare		8 8:00:17:01 10.38% 273 8 8:00:17:58 11.175 273	-20 22-30-24 -0400			
			g 0:00:17:52 11.25% 2/3	BEIGHNIEIGE >		anna an	
Newson Attacker Gal. External Workstation on CVID. BHAMELA			g 0:00:20:36 13.80% 2/3	(ETA: 00:05-10) 0.002+30g/s 31.36p	5 70.31c/s 70.31C/s etak	socobor	
-Virtue Wachiae Contection	100		g 0:00:22:35 13:706 2/3	(ETA: 00:03:51) 0.001605g/s 28.67p	s 68.30c/s 68.30C/s beyond	e2 - jullane2	
	rilet.txt		g 0:00:28:04 19+026 2/3 )	(fir: en:er:12) 0.001/012/2 58/2300	\$ 68/320/3 68/120/1 WOLVER	inez - cthurniz	
States Larroy			1		Activ	ite Windows	
	Statuce Running					and the second se	
						S 6 11 000	
😫 🔎 💇 🚺 Hyper Y Managar 🔯 Attacker Kall - Educ 🎅 Windows 7 os CY1							2024
🚍 D H 🖿 🧕 🔹 🖉 🖉 🧕 🖉						318	PM

Figure 11 Screenshot of admin privileges from meterpreter

Admin access is needed to perform hashdump command on meterpreter.



Figure 12 Screenshot of hash dump being executed and grabbing all users from Win 7



Figure 13 Screenshot of retrieving rockyou.txt for password definitions



Figure 14 Screenshot of executing password cracking with rockyou.txt extracted.



Figure 15 Screenshot of password cracks of 4 users.

Win 7 has 'password' and 3 others are passwordless. The other 3 users were still not cracked after 1 hour of time elapsing.

### Task C



2. Decrypting WEP and WPA/WPA2:



Figure 16 Screenshot of opened demo file and filtering DNS packets

Figure 17 Screenshot of filtering arp packets

* = 4	lläkysellittenentii 🛛 🗴 +									-	a x
(C. 11)	C 😫 lab-connect.com-co.org	yhttps-6883/guiasmole.lab	она-оп тудинат	nole/#/client/Mzg1AGMAbXba	cillu					C 🎂 🔅 🕸	<b>4</b> ()
Process	File Actors Yew Help The Actors Yew Help	Kali - Internal Markstafin Nar Action Media	in on CY351-BHAMSH4 Tew Help IP 10 2 12 6	- Virtual Machine Connection				- c	1: X		
	ние чинечи Макери В Солт-вызмета	Na Na Vivisnare Jab	Sweps D File A	2 3 4 0 2 2 4 Elle Salt View So So So 1 1 6 6 0 6	nune Analyze Statistics ' I 🕅 🙆 🔍 ← →	latõngretenastas Telephon <u>y Wi</u> reless <u>T</u> ools A +€ →• <b>■1 ■</b>	5 <u>H</u> elp <b>0 0 0 1</b>		<b>-</b> 6	ION	
Array- Zermap GLI			9A2.P1 *C	to Time 2206 12.207458 2213 12.321611 2215 12.328690 2223 12.3092178 2227 12.413170 2296 12.419626 2232 12.426934	Source Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40 Apple_c8:21:40	Destination Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2 Cisco_fat3b:a2	Protocol Le EAP EAP TLSv1 TLSv1 TLSv1 TLSv1 TLSv1 TLSv1	sept me 41 Response, Protected EAP (EAP- 44 Response, Protected EAP (EAP- 44 Response, Protected EAP (EAP- 148 Capinalson, Protected EAP (EAP- 122 Client Key Exchange, Change ( 37 Application Data 143 Application Data		Y	
Nesat		C File System	at La station ab5wep at (a station station	1636, 140,755283 1636, 140,755283 1636, 140,772679 1636, 140,776299 1636, 140,796590 1636, 140,796785 1636, 140,796785	Cisco 04:7d:e2 Cisco 04:7d:e2 Cisco 04:7d:e2 Cisco 04:7d:e2 Cisco 04:7d:e2 Cisco 04:7d:e2 MonthelPrecis.c5:90.	MonimalPrecis_05.90: MonimalPrecis_05.90; MonimalPrecis_05.90; MonimalPrecis_05.90; MonimalPrecis_05.90; Cisco_04:74:e2	. ЕАР ЕАР ЕАР ЕАР ЕАР ЕАР ЕАР	44 Applebelow Long atta 48 Request, John Ling Cap (DAP-1 472 Request, Protected SAP (DAP-1 1948 Request, Protected SAP (DAP-1 1948 Request, Protected SAP (DAP-1 44 Response, Protected SAP (DAP-1 44 Response, Protected CAP (DAP-1 45 Response), Protected CAP (DAP-1 45 Response), Protected CAP (DAP-1 46 Response), Protected CAP (DAP-1 47 Respons			
		Home	0000000 ++ (x ++ (x tk_0thi ++ (x + (x capturi	TEEE 002 il QoS Dat Logical-Link Contro 002 JX Authonicati Extensible Authenti	a, Flags:T 1 cm cation Protocol	0020 0020 0030 0040 0040 0040	58 bf en fa 88 80 81 60 28 e1 de cf 2n 44 fe fa 8f	15:52 (5 00 05 06 05 05 05 05 05 05 06 05 0 00 25 05 05 05 05 05 05 05 05 05 05 05 05 05			
Villean Workhote		VMshare	1								
		Sotan Ranning	- 40	Constructions		<del>&gt;/</del> 10, 1	Province of	For technology help, contact	≡∎≙ the ITS	indows Help Desk:	
<b>1</b> P	2 🔒 🌍 🎁 Hypele V Man	agar 🔤 Attackar Kak - D	ister 🤤 Wirelowa	7 os CY2. 🧶 Kak-Tatinnal	Wak					· · · · · · · · · · · · · · · · · · ·	41 1226AM
a 🖬	바 🖿 🗿 🖷 🐠 🛷										7-26 PM

Figure 18 Screenshot of filtering eap packets



Figure 19 Screenshot of aircrack-ng command on WEP demo file



Figure 20 Screenshot of successfully finding key from aircrack



Figure 21 Screenshot of using the key to decrypt packets, all packets shown to be decrypted for WEP



Figure 22 Screenshot of Protocol Hierarchy for after decrypting packets for WEP



Figure 23 Screenshot of filtering eapol packets for WPA lab demo



Figure 24 Screenshot of aircrack used on WPA lab demo

WPA aircrack-ng requests a dictionary to be used, which rockyou.txt was the main one used.



Figure 25 Screenshot of password being shown after cracking with dictionary attack



Figure 26 Screenshot of inputting password and ESSID in order to decrypt packets



Figure 27 Screenshot of packets after decrypting

a Noo V Mireje	🕎 Kal - Internal Norkstation on CY301-BHAM	014 - Vitual Machine Connection				- a	×
File Action Year Help	file Action Media Easy Help						Sec.
🗢 🖈 🖉 📰 🖬 🖽							
Hype-V Minager	🕹 😂 = 1	2 3 4 🔤 🗄 💪		1.44		enmon(XCCX 🌒 🌲 🛢 0.43 🛔	A 6
CON-Semantia	Na						
		The Edit Mass des Castains Assesse Enstation Talanda Manhada Baseral Massela Talanda	na thister Taul	te Malan	-		
	Ultrana Internet			<b>7</b> 0	11-15-0		ION
	Auguste alpowepour	Protecol	Percent Packets	Packets	Percent Bytes	<b>C</b> +	
		Ethemet	100.0	2328	6.8		Y
		<ul> <li>Internet Protocol Version 6</li> </ul>	0,1	3	00	254 (258) 2567 Te11	
		Multicast Domain Name System	0.0		0.0	Ty 0x0000 ANY Pen	
	c Trash WPA2-P1-0	Internet Control Message Protocol v6	0.1	2	0.0	Seltation for fee	
	Che Che	Thermet Protocol Version 4     Tuber Datagram Protocol	15	33	9.7	ry 0x8000 PTR _ai	
		Network Time Protocol	0.0		0.0	[ACK] Seg=1 Ack=12	
	0	GQUIC (Google Guick UDP Internet Connection	0.1		0.3	254.265.2557 Tell	
	File System lab5wep-d	Domain Name System	1.0	22	0.2	[ACK] Seg=1 Ack=	
	Constanting Areastand	Transmission Control Protocol	98.2	2188	82.6	1 segments not cap	
		Transport Layer Security	57	127	8.5 14.2	Data	
	A DECEMBER OF A	Portable Network Graphics	0.0	1	0.2	ci3 \$3 65 28 86 88 81	
	Jacob Jabbarra 2	Data Address Resolution Protocol	0.0	1	0.1	d3 93 65 66 88 82 17 ff	
	Home anompar-	Party Contraction of Contract					
	and the second sec	We display then					
	VMshare Pockyou.tet		Cose Co	ey Prot	ocols - O'Help		
	Sec. Constant of the second se						
	- Whuil Madvine Econection	IsbSwpa2-demo-dec.cap		Packets:	2228 Displayed 222	8 (100.0%) Profile: Default	
	X X	0. 5	- 19	8 -			
		· · ·	1000.07			Acti	and Mindows
					For tec	nology help contest th	a ITS Halo Dask
	- F51878	and the second se			FOR ISC	mology help, conider m	e no neip Desk.

Figure 28 Screenshot of Protocol Hierarchy after decrypting packets

### TASK C

3. Decrypting WPA2-P1-01.cap



Figure 29 Screenshot with MD5SUM ending in 2 -> referencing WPA2-P1-01.cap file to decrypt



Figure 30 Screenshot with Wireshark referencing WPA2-P1-01.cap file to decrypt

* 1	illinyosiilliniuvalli 🔹 +			= 第)五
(e	C 😫 lab-connections-crime	Mtps-Bitt3/guaranzik.lab.ons-on.arg/guarannole/#/clant/Mtg1A/JMAbitadWa		C ** 9 * 1 i
Regretat	Bit Ingon Y Miresjen File Autors Yean Help In Process Discount of the State Helper Y Manager In Charlesauteriz	Image: Second Model         Test Control Model         Test Second           Test Second         Test Second         Test Second         Test Second           Image: Second Se	C (genmen)0000 🚯 🌲 🖻 0.47	
Activity Reside Targe-		File         File <th< td=""><td>Parallela- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:           Postelia- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Postelia- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela- Stap:         Parallela-</td><td>ION Y</td></th<>	Parallela- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:           Postelia- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Postelia- WA2-Fr-5tap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:         Parallela- Stap:           Bit Dot         22660 Stap:         Stap:         Parallela-	ION Y
HH - Kal Lagar (Pro- Vietnese) Vietnese)		W Waysing Stare	Postet: 2460. Displayed 2460 (000.0%)   Profile: Default	Tindows the ITS Help Deck
<b>11</b> / P	🗢 😰 👔 Hyper V Mer	ger 🧕 Attacker Kal - Edm 🤰 Windows 7 se CYL. 🎯 Kal - Internal Work		^ 😡 41 1347AM 7/28/2804
0 🖬	비 🗖 🧕 🖷 🍕			7547 PM

Figure 32 Screenshot with WPA2-P1-01.cap Protocol Hierarchy



Figure 33 Screenshot with aircrack-ng on WPA2-P1-01.cap which needs a dictionary attack



Figure 34 Screenshot shows dictionary attack with PASSWORD being the password



Figure 35 Screenshot shows implementation of the password and CyberPHY to decrypt packets



Figure 36 Screenshot shows Wireshark packets after decryption



Figure 37 Screenshot shows Wireshark Protocol Hierarchy after decryption



Figure 38 Screenshot shows Wireshark DNS filter after decryption



Figure 39 Screenshot shows Wireshark ARP filter after decryption



Figure 40 Screenshot shows Wireshark EAPOL filter after decryption

Decrypting the traffic was quite tedious, but after getting a grasp of the commands and utilizing it correctly, decrypting the traffic proved simple. When breaking the WPA/WPA2 down it seems as though they will require dictionary attacks in order to decrypt the packets in order to view what is within them. The screenshots provided shows the process step-by-step and provides a brief view into what the packets look like when encrypted and how they change after encryption. The best possible breakdown is looking at the protocol hierarchy and how more subcategories open, detailing what specifically is being sent across the network.

WPA/WPA2 shows that it has a stronger security and encryption of the packets and requires a little bit more work in order to figure out how to decrypt the packets in order to obtain information that is wanted. Furthermore, not all packets decrypt as only roughly 400 packets were during this process, so it would be safe to say that more protocols would need to be taken in order to access all of the data that is within the file.

This lab has been a great source of information regarding packet transmissions and how they are securely sent over the internet, but it also shows how they can be dissected in order to find information that is wanted. With the appropriate tools, much of the information can be found when cracking passwords or even figuring out wifi passwords that could be exploited by criminals and hackers.