Old Dominion University <u>CYSE 301 Cybersecurity Techniques and Operations</u>

<u>Assignment #5 – Password Cracking</u>

Ned Smith 01200384

Part One: Password Cracking

Task A: Linux Password Cracking

Group Creation



Explanation: I created two groups using the "groupadd" command, one named CYSE301s23 and the other named after my MIDAS ID.

User Creation



Explanation: I added six users, three to each of the groups, using the "useradd" command.

Password Creation



Explanation: Using the "passwd" command, I changed the passwords of each user to the following passwords:

User1: 321321 User2: abcd1234 User3: college User4: a1b2c3 User5: SuperRad100% User6: In2an3P4ssw0rd(*)

Task B: Windows Password Cracking

User Creation



Explanation: After gaining administrator privileges and establishing a reverse shell connection, I used the net user command to add three users, as well as their passwords, to the Windows 7 VM.

Question 1



Explanation: I used the hashdump command in the meterpreter shell to display the password hashes

Question 2



Explanation: Using the gedit command, I saved the hashes into a hash file. I then used John the Ripper to crack the three password hashes, with it finishing once it had cracked all three.

Question 3:

Dictionary Attack



Brute Force Attack



Explanation: Using the previously mentioned reverse shell connection and administrator privileges, I uploaded the Cain and Abel password-cracking tool to the Windows 7 VM and installed it through the remote desktop window. I then used the Cain and Abel tool to run a dictionary attack as well as a brute force attack, with both resulting in all three hashes being cracked.



Task C: Extra Credit

Explanation: I didn't save the initial steps leading up to cracking the hash originally, so the first screenshot is a recreation of how I saved the hashes in the hash file. Using a combination of the echo and cat commands, I wrote both hashes to the hash file called "ExtraCredit-HASH". I then used the format "raw-md5" with John the Ripper to crack the two passwords. The second screenshot is the original image showing that the passwords were cracked and displaying the two passwords, those being password and root. I don't have a screenshot of the original password-cracking session with John the Ripper, and it won't perform an additional one because the cracked hashes are saved by John the Ripper.

Part Two: Wi-fi Password Cracking

Task A:

Decrypt the lab4wep.cap file:









Explanation: Using the aircrack-ng command, I figured out that the first network is the one that needs to be targeted due to it using the WEP. After inputting "1" where it asks for the index, aircrack-ng was able to find the key, which was F2:C7:BB:35:B9. Now that I had the key, I used airdecap-ng, followed by -w along with the key to decrypt the traffic in the lab4wep.cap file. The decrypted traffic was saved into a file named lab4wep-dec.cap, which I then opened in wireshark to analyze the traffic.

Traffic Analysis





Explanation: The traffic starts off with various TCP SYN packets and HTTP packets being exchanged between various source IP addresses and the destination IP address of 192.168.2.10. There also seem to be a lot of unseen segments, Wireshark most likely couldn't figure out the specifics of the packet but knows it exists and was transferred. However, after a short amount of time, we can see that most of the packets being exchanged over the network are ARP packets, all sharing a source of Alfa_82:c3:7e and a destination of broadcast. The packets seem to be request packets asking about various IP addresses and trying to find their corresponding MAC addresses. While there are some HTTP and TCP packets interspersed between the ARP queries, most of the traffic occurring are ARP query packets.

Decrypt the lab4wpa2.cap file





Explanation: After opening the file and examining the encrypted traffic, I copied the rockyou.txt file into my current directory for it to be used in a dictionary attack. After that, I used aircrack-ng to attempt to crack the password using a dictionary attack with the rockyou.txt file as the wordlist. After choosing index 4 from the list of networks, due to it being the wpa format, the dictionary attack occurred, and the "password" key was found. After finding the password, I once use airdecap-ng along with the password and the ESSID of the network, which was CCNI. This allowed me to decrypt the packets, which were placed in a folder called lab4wpa2-dec.cap.

Traffic Analysis







Explanation: A big difference we can immediately notice between the traffic of the wpa2 file and the WEP file is the notable lack of ARP packets in the wpa2 file. While the wep file was mostly ARP query packets, this file has very few to the point where they are basically unnoticeable without filtering the traffic. Much of the traffic occurring over this file are DNS, TCP, and HTTP packets, with some noticeable transfers of UDP and ICMP packets here and there as well. We can also see that there are cases of TLS client hello packets, suggesting that some of the connections have achieved both TCP and TLS handshakes respectively. The lack of ARP packets seems to suggest that the MAC addresses are known this time around, or that they do not need to be found for some reason, but the practical nonexistence of them when compared to the WEP counterpart file is interesting.

Task B





Explanation: After figuring out which file I should use based on my MIDAS ID, I used aircrack-ng to perform a dictionary attack on the WPA2-P4-01.cap file using "rockyou.txt" as the wordlist file. After using that to crack the password (linkinpark), I then used airdecap-ng to decrypt the traffic, using the password I previously cracked along with the ESSID of CyberPHY. This allowed me to decrypt the traffic for analysis, which was saved in a file called WPA2-P4-01-dec.cap

Traffic Analysis

-						
	state Place 4	Western *	the 2	14	II # /40+	
	The Red Lines die 1	Comment Annual Theorem	weaters in the	and and	0.0.0	
	ANCAR		3		17	
				2.3.5		
and a second	and a state of the	Annual Control of Cont	Partness.	And and	La Captoren .	
	- 14 100000	1.8.8.8.1	100.003.000.000	No. P	The sale discover - framework of former-	
	3.9.945385	42.42.94.2	1007-1008-0-1077	110	IT AND . ADDED [PUR, ADD] Grant Avera and	
100	8.1.400488	107.106.1.0 107.168.1.5	1007.100.4.527 107.109.4.527	396	List Elandard mary response Berry's A sup-	
•	0.5.701728	00.100.04.043	- 103, 100, 1, 637	10.0	to be - peers (ris, and) heart acers with	
-	41.009122	1007.100.1.127	104.100.1.1	095	AT Mandard sarry Schull A ranter of per-	
	10 4.404300	72.00.000.00	101,140.1.127	10	This and - All an (Act) Sourt many miners)	
	11 1, 127178	594-75-37-57	10113041107	19	AN AND - AND TO LOCAL SHOPL ACTION AND TO AND	
	12 5, M/M 18	45.125.311.49	101.109.1.127	112	HE ALL - STORP [SCI] Ampl. MAYL SIMPLE	
	34.0.879839	47. 10. 11. 14	1007 100 3 107 1007 100 3 107	1091.3	ANY ADDITION THAT ANY	
2	17.8-2423080	104.170.22.00	1007 LOD 3. 117	10*	an and - many late many many many many	
0	10.6.40799	1000.173.21.86	100.100.3.527	16.	at Gardianation Date	
1	A determ	WALLARD CO.	HALFFOLD IN		18 LULE ADDRESS PROPERTY INCOMENTS 19410 - 14	
.	23 7.796127	240.005.150.44	587.148.3.127	104	Int an - Addes [POA, ACK] Indy'l Active methods	
	24 7, M09020	2011.2011.2107.010	1967 1868 - 1 - 127 1082 1868 - 1 - 127	10.0	ALL BR - SUMP [NCR] Septem Artic Marrie	
	34 ()457132	388,397,128,84	181,189,1,123	7(7#	to be - come [VDs, ACK] hep-2011 Alaris	
	DO D. DAMAS		Martine Aug		188 (10) Alter second segurite Carl Law	
111	Para-Letano	Street in the	COLUMN TWO IS NOT	1	atta new derrorsantation and Labora (and	
	30 6.201888	109.71.17.27	183, 188, 1-127	TLP	AN INC - MILLS [MAL MORE ADDING MEANING	
	the second		State of the state	100		
	store internation					In a failing is also by Western
	0 7 Amil 1 Am	in last added			Partner SJ. Distant SJ. 200 Ph. Partner Delay	
						And the local state of the second
			- Concerner	-		
			The subscription of the su			
Apple	ations+. Planes+	Breakars +	96m21		III # /40-	
	the last tree and	attent dealers (manufa	Designers diversed To	the below	0.0.0	
	AHAO D		2 * * 2 =			
	Conta e starte bier	4.40			E2 - Apresso, +	
	the field	Tanan A	Instrume	Patron	Langit Ma	
-	THE LOCK STREET	CONTRACTOR OF THE OWNER	the second s		and the second se	
	THE OF TRADE	144. P. 14. TL	101100-0.007	ROATE	The owner provides and the owner out the second of	
10.0	Contractor Contractor		Contract of the	1000 1000		
				19Han		
•				(interest		
				SHool B		
A 🛊 🔳 🕿				Hoolis		
				SEcol Sel		
	19 1/ 2010 19 1/ 2010 10 1/	MAR / M	100 Auto 2000 100 Au	Hoolin 2020		
					Bits Constraints Constraints Constraints Since Constraints Constraints Constraints Constraints Since Constraints	
2 0 E E E O O			101 All 1 Al		111.4 11.4 <t< td=""><td></td></t<>	
0 H 🖉 🖉 🖉 🖓 🕼	194 12 02000 194 12 020000 194 12 02000000000000000000000000000000000		2014 All 1 and 1 a			
🧌 🕴 🗉 🖬 🖉 🐘	120 12 02 000000 100 12 0000000 100 12 000000 100 12 000000000 100 12 00000000 100 12 00000000 100 12 00000000000000000000000000000000	10.1 1.00 1.0 10.1 2.00 1.0 10.0 0.00 1.0 10.1 2.00 1.0 10.1 2	2014 All A and A a			
2 0 II = I II 0 M I					11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	
2 0 II = = H 0 & I	100 01/0 02000 000 01/0 0200 000 0000000000000000000000000000		$\begin{array}{c} (1) & (1) & (1) & (1) \\$			
2 0 II = = H 0 K II I	10 01 01 01000000000000000000000000000		101 440.1 457 102 440.2 457 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 103 2.25 72 103 2.25 72 103 2.25 74 103 2.25 74 104 1.27 74 105 1.25 74 104 1.27 74 105 1.26 74 105 1.26 74 105 1.26 74 105 1.26 74 105 1.27 74		 III Construction of the second scale sca	
2 0 II 2 2 14 0 16 18 18 18	10 10<		101 440 457 102 440 5 557 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 102 2.25 72 103 2.25 72 104 2.25 72 105 2.25 72 104 2.25 72 105 2.25 72 104 2.25 72 105 2.25 72 104 2.25 72 105 2.25 72 104 2.25 72 105 2.25 72 104 72			
2 🕴 🖩 🗢 🖬 🖬 🖓 🐼 📑 📑 📰	10 10 <th10< th=""> 10 10 10<!--</td--><td></td><td>100 400 507 100 400 5.424 100 400 5.424 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 101 5.02 100 102 5.02 100 103 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02</td><td></td><td></td><td></td></th10<>		100 400 507 100 400 5.424 100 400 5.424 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 100 5.02 100 101 5.02 100 102 5.02 100 103 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02 100 104 5.02			
2 0 🖩 8 📑 14 0 🛝 📑 🔮	100 12 02 02 00000 100 12 02 00000 100 12 000000 100 12 00000 100 12 0000000 100 12 00000 100 12 000000 100 12 000000 100 12 000000 100 12 0000000 100 12 00000000000000000000000000000000				Interface Interface Interface Interface Interface Note Note <td< td=""><td></td></td<>	
27 0 E 2 0 14 0 18 0 E 11	100 100 <td></td> <td></td> <td></td> <td></td> <td></td>					
유 후 문 호 분 년 원 ស 📑 🖶			10 40 40 10 40 4 10 40 4 10 40 4 10 40 4 10 4 4 10 4 4 10 4 4 10 4 4 10 4 4 10 4 4 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 <t< td=""><td></td><td></td><td>Authorite Windows To an Anthony is a scheme Moneyman</td></t<>			Authorite Windows To an Anthony is a scheme Moneyman
A O II 2 2 14 0 16 10 10 10 10	10 10<		10 40 40 10 40 5 40 10 40 5 40 10 40 7 40 10 2 2 7 10 2 2 7 10 2 2 7 10 2 2 7 10 2 2 7 10 2 2 7 10 2 2 2 10 2 2 2 2 10 2 2 2 2 2 10 2 2 2 2 2 2 10 2 2 2 2 2 2 2 10 2 <td></td> <td></td> <td>Authoritetta Welvellineet Täivete Vellineitetta autoonid Ministerie</td>			Authoritetta Welvellineet Täivete Vellineitetta autoonid Ministerie
0 0 = 2 0 ii 0 0 00 0 0 0 0 0 0 0 0 0 0 0 0 0	Tot II Column 1 Image: State Sta	1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000 1000	10 400.4 4.01 100.4 400.2 4.01 100.4 400.2 4.01 100.4 400.2 4.01 100.4 4.01 <t></t>			- Accharate Websitement Ta da Samang Is activate Researce

Applement	· Paris ·					
		THE REPORT OF		115	4 /40+	
			HONG PRI	il de la de	0.0.0	
	Dat New St D	Auto Braites Daper	a Jacoburg House 3	10.00		
4	128.0	XC C			A	
1.000	h + Angling 10 Arr. 1	Con Ja			EI - Equinar, +	
1 Par	THE PR PROPERTY.	THE DESIGNATION.	the same is all	- Patent	All Mandard many reserve burld, 5 Tol	
	pho 38. Televito	112 217 5 20	382.388.1.127	107	1202 Add - ADDIT Servicitie	
	Phy 26, 781104	116.09.101.100	197.188.3.127	100	1242 445 - 88817 120-1200	
•	214 28. 198234	110.50,100.100	100, 000, 1, 117 100, 000, 1, 127	107	JTAR AN - MARY LANCES	
_	259 38.89500	128.59.291.180 172.217.8.45	100.100.1.127 100.100.1.127	004	TT ARE - DORLT LAWYED	
	200 28.014100	175.017.5.06	180.388.5.577	0.07	1002 440 - 42149 140-2000	
M	260-28.848075	170.017.4.329	107.108.1.1/7	100	TORY AND - AAMED LANCEDON	
	AT BUILDING	10111111111	100 000 1 107	Contract of	THE REAL PROPERTY OF THE PROPERTY OF THE REAL PROPE	
	253 39.040008 264 39.0400073	880.7.29.48	380, 988, 3, 337 189, 389, 1, 117	PLANE -	1011 A Calebrate and the set of the calebrate and the calebrate and the set of the set o	
	pain pie, medicine	048.7.79.41	107. 108. 1. 117 107. 108. 0. 117	10000	12114 Second and American Contractor and American Second	
	107 JR. ROOMEN	100.7.29.40	192.088.1.127	10041	The loss and law per per an an an and the	
6	ING IN ADDRESS	100.7.25.41	190.368.3.317	moster.	1114 March deer geer and seen and seen and seen	
F	TTY IN ATTRUS	445.7.09.41	140, 168, 1, 117 140, 168, 1, 117	1000	Lines when peer and user and user and and deal lines	
_	The part of the second	200.7.34.41	397 149 1 117	10000	DELLA COMPOSITION AND ADDRESS AND ADDRESS AND ADDRESS AND	
-	TTN JR BTRONS	388.3.29.45	387.388.3.377 387.388.1.377	MILLION COLUMN	1711 A TONOT AND	
	TVS 28 Shirts	345.1.05.41	280.388.5.527 181 188 1.417	wight.	1211 Control and and and the set and the set	
100	The law watched	105.3.28.41	192.348.1.117	REAM	Inter Charlose day any the lost and the start	
***	114 JR 8184124	111.1.28.41	287.044.1.317	40476	1014 New York and And New York And And And	
	THE PR. PROPERTY .	100.7.09.40	100.088.1.177	NO.	TALK CONTRACTOR AND	
	and the second of	400 X 10 X		and and	and a state of a state	
	WFAP. PR. 21. 40	CONCLUSION AND AND AND AND	10 M M M 15 19			
10.7	Pare Pares 10	i false		_	Particle 122 Displayed \$22,201,276; Northe Default	
	0	C 10 0 .	-			2 art fan - 4 art 1000 C
			Tel March Science	-	121 C	
Application of	Family B	Brenet P				
Applacement	Fact 1	manual *	the state	025 1.81.19	E # 240-	
3 Date	ter first fir ()	anne fraise frans	a Tanahang Brenes J	1. Million Million (199		
1 2 2	ри ун р. р. 1 / Ф. Ф .	1000000 100000 10000 100000 100000 10000 10000 100000	0001 0000000 1 Tonaton (1999) 2 Tonaton (1999)	1.81.09 	E 4 2405	
	pa pa pa p 1 d ⊕ D	The part of the second	100000 (00000) 1000000 (00000) 2 3 4 4 (2) (1)	0.00 R. Max.org M. M. M. M.	1 4 /4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0	
			Alian Metal Ana Solutions (Spream) - 2 H + (Spream)	A R. R. R.	1	
			2010 2 1 Stopheng (Spream 2) 2 Stopheng (Sp	21 1.41.09 4.4.4.4 2.21	1 4 7 4 0 4 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	
		1000 - 1000 1000 - 2000 1000	Contract of the second		1	
		The second	Destention 00041040 1 Nonphang Symmer 1 2 H = 1000 101.000 A = 1010		10 - 500 - 5	
		Control of Contr	WHALPAN WHAPAN WHAPAN WHAPAN WHAPAN WHAPAN WHAPAN WHAPAN WHAPAN			
		Comparison of the second				
		Control of the second se	Contraction Contracti		Comparison C	
		Control of the second se	Descent Descent 1 Nonpolece Symmet 1 Nonpolece Symmet 2 0 0 2 0 0 2 0 0 101 0.01 1.07 102 0.01 1.07 103 0.01 1.07 104 0.01 1.07 105 0.01 1.07 104 0.01 1.07 105 0.01 1.07 104 0.01 1.07 105 0.01 1.07 104 0.01 1.07 105 0.01 1.07 105 0.01 1.07 105 0.01 1.07 105 0.01 1.07		Comparison C	
		Alexandre (1998) Ale	NYAL PAO WHAL PAO 1 Tringelang (Eyrows T) 2 How et al. NH 100 AL 107		Comparison C	
		Control of the second se	Second		Comparison Compariso	
		Andrew Control of Control o	Contraction Contracti		Comparison C	
		Protect (1) Protect	Section Section 1 Templane Templane 2 0 0 2 0 0 2 0 0 2 0 0 1 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100<		Comparison C	
	Image: Section of the sectio	Andrew Constraints Andrew Constrain	Description Description 1 Nonpolence (Second Second Seco		Comparison Compariso	
		Alexandre - Constanting	NUMBER 1		Comparison Compariso	
		Control of the second se	Contraction (Contraction) Contraction (Contraction) Contraction (Contraction) Contraction (Contraction) Contraction C		Comparison C	
		Annual A	Section 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 1 100 101 0.01 102 0.01 103 0.01 104 0.01 105 0.01 102 0.01 103 0.01 104 0.01 105 0.01 104 0.01 105 0.01 104 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01 105 0.01		Constraints of the second	
		No. 00 No. 00 Party A Party A Party A No. 00 No. 00 Party A No. 00 <	Bit State Bit State 1 Nonpolence generation 2 0 0 2 0 0 3 0 0 3 0 0 1 0		Control (Control (Cont) (Control (Control (Control (Control (Control (Control (Control (
		Control of the second se	NYAL DATA WHAL DATA ''''''''''''''''''''''''''''''''''''		Control of the second sec	
		Control of the second se	Control of the second sec		Comparison C	
		Image: Solution of the second secon	Control of the second sec		Constant of the second se	
		Normality Normality Normality Normality	Control (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contro)		Control (Control (Contro) (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro)	Activate Wildowi Statuses and
		Image: Solution of the second secon	marking and a second seco		Compared a card of the compared and the compared and of the compared and of the compared and of the c	Activista Wildelman, Si de Samage de activide Ministeres
		Control of the second sec	Control (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contro)		Control of the second of	Activate Wildland Table school Planet



Explanation: We can easily see many similarities between the WPA2-P4-01-dec.cap and lab4wpa2-dec.cap files when analyzing the traffic of both files. When filtering for ARP packets we can once again see that there are none within this traffic file, and most of the file consists of DNS, TCP, and HTTP packets being exchanged. However, this file notably also contains many more instances of UDP packets as well as another packet type called MDNMS which I am not familiar with. Another interesting factor when analyzing this file is that some portions of the analysis contain numerous unseen segments in a row, especially more than the other files. I'm not sure if this is due to the file itself or maybe a malfunction with Wireshark, but it's interesting that this file is the smallest overall yet seems to contain the greatest quantity of unseen packets. This file also has a few examples of TLS client hello packets, again suggesting that some of the connections successfully completed both TCP and TLS handshakes across this wi-fi connection.