OLD DOMINION CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS Assignment #5 – PASSWORD CRACKING AUSTIN CUPP 01183567



A.1 Two groups are created. one is cyse301f22, and the other is acupp001 which is my midas ID.



A2. Created and assigned three users to each group with information displayed.



A3. Six new passwords chosen, from easy to hard, and assigned to the users I created.

Username and password below

User1: password

User2: p@ssword

User3: claudion125

User4: p455word

User5: pa55wordx

User6: p455wordxx



A4. All six users' password hashes are exported into a file named acupp001-HASH.txt. Then a dictionary attack is launched to crack the passwords. 3 passwords are cracked, user1, user2, and user4



B1. Password hashes are displayed by using the "hashdump" command in the meterpreter shell.



B2. Password hashes are saved into a file named acupp001.WinHASH in Kali Linux.

THE REST OF B2 IS ON THE NEXT PAGE

	🕎 Windows 🕎 Att.	acker Kali - External Workstation on CV301-ACUPP001 - Virtual Machine Connection —		Х	k
N	File Actio File	Action Media Clipboard View Help			
Recycle Bin					
	/ 🗋 Index c Appl	ications 🔻 Places 🔻 🗵 Terminal 👻 🚺 📲	x =)) () -	
L	$\leftrightarrow \rightarrow \mathbf{C}$	acupp001.WinHASH.txt - 🗆 × root@CS2APenTest: ~ -	×		
		File Edit Search Options Help inal Help			
Acrobat Reader	Index	Administrator:500:aad3b435b51404eeaad3b435b51404ee:31cbm -p windows/meterpreter/reverse_tcp lport=4444 l Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1 alc.exe HomeGroupUser\$:1002:aad3b435b51404eeaad3b435b51404ee: ed, choosing Msf::Module::Platform::Windows from t	host he p	1	ION
	<u>Name</u>	root@CS2APenTest: ~	00	0	Y
Nman -		File Edit View Search Terminal Help			
Zenmap GUI		Using default input encoding: UTF-8		-	
-	Apache/2.4	Loaded 7 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])			
		Proceeding with single, rules:Single			
Nutanix SSR		Press 'q' or Ctrl-C to abort, almost any other key for status			
Nuclinix Joh		Almost done: Processing the remaining buttered candidate passwords, it any. Warning: Only 26 candidates buffered for the current salt. minimum 48 needed for performance.			
		Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist			
		password (user1)			
Manada and	M	(Administrator)			
wiresnark		(Guest)			
		Proceeding with incremental:ASCII 4a 0:00:09:07 3/3 0.007312a/s 49658Kp/s 49658Kc/s 148974KC/s kcna2m4kcna2DX			
		Use the "showformat=NT" options to display all of the cracked passwords reliably			
		Session aborted			
Google Chrome	-	Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::			
		Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::			
		User1:password:1003:aad3b435b51404eeaad3b435b51404ee:88467/eaee8fb11/ad06bdd830b7586c::: Window 7:password:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::			
	F				
VM - Kali Login info		4 password hashes cracked, 3 left			
			λ.		
		(KALI)			
		ST OTRENIRE SECURITY		3	Help Desk:
VMware Workstati	calc (الله مالي
	3				uu.euu
	Charles Dannie Historie	ar V Managar			10:32 PM
\sim				\sim	11/22/2022

B2. John the ripper is run for 10 minutes to crack the passwords. 4 passwords were cracked, with 3 left.



B3. Uploaded the password cracking tool, Cain and Abel, to the remote Windows 7 VM.

B3 CONTINUES ONTO THE NEXT PAGE



B3. Cain and Able is installed via a remote desktop window.

B3 CONTIUES ONTO THE NEXT PAGE

	🕎 Windows 🕎 Attacker Kali - Exter	nal Workstation on CY301-ACUPP001 - Virtual Machir	ne Connection			- 🗆 X	k
	File Actio File Action Med	lia Clipboard View Help					
Recycle Bin							
	Applications -	Places 🔻 📕 rdesktop 🔻	Tue 2	3:45	1	₩ / •1) & •	
کم		rdeskt	op - 192.168.10.25		0	- D X	
Acrobat							
Reader					1.1		ION
	Recycle Bin	Brute-Force Attack					
P		Charset-		Password length			
Nmap -		• Predefined		Mín 7 🚊			
zenmap oor	s 🚺	abcdefghijklimnopqrstuvwxyz0123456789	•	Max 10 🕂	korboros tat i	nitialized	
1	Chrome	C Custom		Start from	Kerberos tyt I	AILIGUIZEU X	
8	•				24: falling bac	k to 16	
Nutanix SSR		Keyspace 3760616909315297	Current password		24, ruccing but		
		Key Rate	/ _/		cupp001 /add		
	M						5
Wireshark		Plaintant of 00/(E2E)EE0ED113	1104 PDD920 P7504C is see				5
		Plaintext of CED2992A3609ADFF	76D9E63B503F05C5D is p455	word			1. A.
		2 of 4 hashes cracked					
\mathbf{N}		8					6
Google Chrome	8					×	
				Start Exit			
	F //					NUMBER OF STREET	
VM - Kali						Connection	
Login info				11:45	ow 7 @ WINDOWS7	192.168.217.3	
	l 🚺 🚺		a mecerprocer	11/22	/2022 	192.168.217.3	
		**************************************	4444 -> 192.168.217.2:	49185 (192.168.10.25)			s Help Desk:
VMware Workstati		m in the second s	<u>sf5</u> exploit(<mark>windows/l</mark> o	cal/bypassuac) > 🗌	A	Activate Windows	,
. consections					6	o to setung to activate	Vahiech
	Chature Duranin						
۶ ج) 🛱 🎁 Hyper-V Manager	輿 pFsense - Firewall 6 🛛 👲 Windows 7 or	n CY3 👲 Attacker Kali - Exter.			,	11:45 PM
	A CONTRACT OF A		and the second sec				11/ 66/ 606

B3. Brute force attack is implemented to crack the passwords, 2 of 4 are cracked.

B3 CONTIUES ONTO THE NEXT PAGE

Recycle Bin	□ □ </th <th>I▶ 🔂 D 🔮 👬 aces ▼ 🔲 rdesktop ▼</th> <th>Tue 23:38</th> <th>1</th> <th>j≌ ≠ 40) (¹ +</th>	I▶ 🔂 D 🔮 👬 aces ▼ 🔲 rdesktop ▼	Tue 23:38	1	j≌ ≠ 40) (¹ +
لمر		rd	iesktop - 192.168.10.25	0 0	- 🗆 x
Acrobat Reader	Recycle Bin	Dictionary Attack Dictionary File C.\Program Files\Cain\Wordlists\Word	Position dist. txt 3456292		
Nutanix SSR	Socie Chrome Chrome N	Key Rate Dictionary Position Current password	Options Image: As Is (Password) Image: Password PassPass) Image: Double (Pass - Pass) Image: Double - Pass - Pass - Pass) Image: Double - Pass - Pa	kerberos tgt 24; falling ba	initialized ⊣j× nck to 16
Google Chrome	 ✓ ✓	Plaintext of 8846F7EAEE8F Plaintext of CED2992A3609 Attack stopped! 2 of 4 hashes cracked	B117AD06BDD830B7586C is password ADFF6D9E63B503F05C5D is p455word		
VM - Kali			Start Exit		Connection
Login info VMware Workstati			14444 -> 192.168.217.2:49185 (192.168.1 msf5 exploit(windows/local/bypassuac) >	11:38 PM 7 @ WINDOWS 11:22/2022 0.25)	7 192.168.217.3 7 192.168.217.3 Activate Windows
	Chelus Durnis	🔊 nFrance - Firewall 6 🛛 🚯 Window	ws 7 nn CV3 🚯 Attacker Kalis-Exter		Go to service Voluiedu

B3. Dictionary attack is implemented to crack the passwords, 2 of 4 are cracked.