CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Password Cracking (Part A)

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)

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.

Applications 👻	Places 🔻	🕞 Terminar 💾 💵	Attacker Kali -	External Workstation on CS301-KCOLE030	- 8 ×	1	,
			root@	CS2APenTest: ~	0 0	8	
	File Edit Vie	w Search Terminal H	eln				
VMs	root@CS2APen	Test: # useradd user	sl -a cvse30	1		~	
	root@CS2APen	Test: # useradd user	s2 -g cyse30	1			
	root@CS2APen	Test: # useradd user	s3 -g cyse30	1			
	root@CS2APen	Test: # useradd user	s4 -g Kcole0. s5 -g Kcole0.	30			
	root@CS2APen	Test: # useradd user	s6 -q Kcole0	30			
2		Test: # id users1	,				
	uid=1002(use	rs1) gid=1001(cyse30	1) groups=10	01(cyse301)			
	uid=1003(use	rs2) aid=1001(cvse30	1) aroups=10	01(cvse301)			
-	root@CS2APen	Test: # id users3	1, groups 10				
	uid=1004(use	rs3) gid=1001(cyse30	1) groups=10	01(cyse301)			
	root@CS2APen	Test: # id users4	(20) around (-1)	992 (Kcol e929)			
	root@CS2APen	Test:-# id users5	so) groups=1	002(RC0[2030)			
	uid=1006(use	rs5) gid=1002(Kcole0	30) groups=1	002(Kcole030)			
M	root@CS2APen	Test: # id users5	•				
	uid=1006(use	rs5) gid=1002(Kcole0	30) groups=1	002(Kcole030)			
	root@CS2APen	Test:-#					
	root@CS2APen	Test:-#					
*	root@CS2APen	Test:-#					
<u> </u>	root@CS2APen	Test: # Test: # id users6					
	uid=1007(use	rs6) gid=1002(Kcole0	30) groups=1	002(Kcole030)			
5	root@CS2APen	Test:-#					
-							Activ
7							Go to !
Applications 👻	Places 🔻	🖂 Termina 🗧 🕂 📶	Attacker Kali - I	External Workstation on CS301-KCOLE030	_ 8 × /	1	
	_	_					
10.4-6	Niner	a la fa					
VMSN	are Nessu	s inio					
				root@CS2APenTest:~	0.0	0	
				ioot@cszAFeiiiest.~	0		
5		File Edit View Sea	rch Terminal	Help			
		root@CS2APenTest:	≇ groupadd cy ≇ groupadd Ko	/Se301			
		root@CS2APenTest:-	# useradd use	erl-g cyse301			
		Usage: useradd [op	tions] LOGIN				
		useradd -D	[+:]				
		useradd -D	[options]				
		Options:					
		-b,base-dir B/	ASE_DIR	base directory for the h	ome directory of the		
		ht of a contra		new account	dimension		
M		btrts-subvo	DLUME-NOME MMENT	GECOS field of the new a	nome directory		
		-d,home-dir H	DME DIR	home directory of the new a	w account		
		-D,defaults		print or change default	useradd configuration		
		-e,expiredate	EXPIRE_DATE	expiration date of the n	ew account		
Š		-T,inactive I	NACTIVE	password inactivity perio	of the new account		
<u> </u>		g,giù unup		account	group of the new		
		-G,groups GRO	JPS	list of supplementary gr	oups of the new		
•				account			
-		-h,help	TR	display this help message	e and exit		Activ
<u>مر</u>		-K,SKEL SKEL		override /etc/login defs	defaults		Go to S

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



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 passwor

plications	👻 Places 👻 🕞 🛛	Terminat 🛨 📶	Attacker Kali - External Wo	orkstation on CS301-KCOLEC	030 <u>-</u> ×	1	, #	1
			root@CS2APen	Test: ~		000		
	File Edit View	Search Terminal H	lelp					
VM	Sroot@CS2APenTes1	:#lss						
	bash: lss: comma	and not found						
	root@CS2APenTest	: # ls						
	core Desktor							
			ublic Videos					
	root@CS2APenTest	: # cp /usr/shar	e/wordlists/rockyou	.txt.gz .				
	root@CS2APenTest	: # gunzip rocky	ou.txt.gz					
	FOOT@CS2APenTest	: # tall -no /et	c/shadow > Kcole030	.TXT				
	Created director	: # JohnTorma	π=επγρι κεστέσσο.τχ	i -wordlist=rock	you.txt			
	Using default in	y. /1000/.john	F-8					
	Loaded 6 passwor	d hashes with 6	different salts (cr	vot. generic crv	nt(3) [7/64])			
	Cost 1 (algorith	m [1:descrvpt 2:	md5crvpt 3:sunmd5 4	:bcrvpt 5:sha256	crvpt 6:sha512crvpt	1) is 6		
	for all loaded h	ashes		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				
	Cost 2 (algorith	nm specific itera	tions) is 5000 for	all loaded hashe	S			
	Will run 2 OpenM	1P threads						
	Press 'q' or Ctr	<pre>rl-C to abort, al</pre>	most any other key	for status				
	1234567	(users5)						
	123456	(users2)						
	1234	(users1)						
	3g 0:00:00:13 0.	02% (ETA: 01:20:	25) 0.2260g/s 202.5	p/s 716.2c/s 716	.2C/s my3kidsvict	orial		
	Use the "show"	option to displ	ay all of the crack	ed passwords rel	lably			
	Session aborted	, # john chou k						
	proot@c52APentest	: # jonn -snow M		Dictures /	ssb (
	armitage prop	Documents/	iohn/	nki/	Templates/			
	bash history	Downloads/	Kcole030 txt	profile	Videos/		Act	
	.bashrc	.emacs.d/	lesshst	Public/	viminfo		Act	Ivati
	cache/	aconf/	local/	rnd	VMshare		Go to	

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.

plications	🕶 Places 🕶 🕟	Terminal 💾 💷	Attacker Kali - External Wo	orkstation on CS301-KCOLE030	- 8 ×		1	, #	1
	File Edit View	Search Terminal Hel	root@CS2APen	Test: ~		• •	0		
VM	Subashrc .cache/ .config/ core CYSE301/ rootaCS2APenTes	<pre>.emacs.d/ .gconf/ .gnome/ .gnupg/ .ICEauthority t: # iohn -show Kcd</pre>	.lesshst .local/ .mozilla/ .msf4/ Music/ ble030.txt	Public/ .rnd rockyou.txt .selected_editor .smbcredentials	.viminfo VMshare .wget-hsts .zenmap/		^		
	.armitage/ .armitage.prop .bash_history .bashrc .cache/ .config/ core CYSE301/	Desktop/ Documents/ Downloads/ .emacs.d/ .gconf/ .gnome/ .gnupg/ .ICEauthority	.java/ .john/ Kcole030.txt .local/ .mozilla/ .msf4/ Music/ J0020.txt	Pictures/ .pki/ .profile Public/ .rnd rockyou.txt .selected_editor .smbcredentials	.ssh/ Templates/ Videos/ .viminfo VMshare .wget-hsts .zenmap/				
	armitage/ .armitage/prop. bash_history .bashrc .cache/ .config/ core CYSE301/ root@CS2APenTes users1:1234:198 users2:123456:1 users5:1234567:	<pre>t: # john -show kct Desktop/ Documents/ Downloads/ .emacs.d/ .gconf/ .gnupg/ .ICEauthority t: # john -show Kct 17:0:99999:7::: 9817:0:99999:7:::</pre>	.jova/ .john/] Kcole030.txt .lesshst .local/ .mozilla/ .msf4/ Music/ ble030.txt	Pictures/ .pki/ .profile Public/ .rnd rockyou.txt .selected_editor .smbcredentials	.ssh/ Templates/ Videos/ .viminfo VMshare .wget-hsts .zenmap/			Act	
	2 password bash	es cracked 3 left						Got	

Task B: Windows Password Cracking (25 points)

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



 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.).



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.).

				Attacker Kalı - I	External Workstation on CS.	SUT-KCOLEUSU -		$^{\sim}$ /	
Applicat	tions 🔻	Places 🔻	🗧 rdesktop 🔻		Thu 14:01				
	_		rd	lesktop - 192.168.1	0.9		0	8	
	2								×
F	Recycle Bin		Brute-Force Attack			-	3		
2			Charset			Password length		23	×
\$	Google		Predetined abcdefghijklmnopqrstuv vsyz012	23456789	Ţ	Max 16 ÷			6cfe ae93
	Chrome	🧭 Dec	C Custom			Start from		NT	d79c aee8
			Keyspace][Current password			31[31[aee8
		- 🦛 M	8.18605142737343	89E+024	kqOp	sca		2D'	
	PuTTY		Key Rate	/Sec	Time Left	010 ueare		884	
U U			110052501 033		2.00000				24-04-0
			Plaintext of 8846F7	EAEE8FB117AD06BI	DD830B7586C is pas	sword			
<u>1</u>	Cain							Þ):::
€		http://w	1			Stop Exit		1.	23:::
F									

			lli. 🕂	Attacker	Kali - External Wo	rkstation on CS301-KCOLE03	30 <u>-</u> ×	
Appli	cations 🔻 🛛	Places 🔻 🛛	🗕 rdesktop 👻			Thu 13:59		1
			ro	lesktop - 192.1	68.10.9		0 0	
	Recycle Bin	Dictionary A Dictionary File	xttack rogram Files\Cain\Wordlists\Word	flist, txt	Position 3456292		~	× • •
5	Google	Keu Bate			ions			6cfei≜ ae93
•	Chrome		Position	य य य य	As Is (Password) Reverse (PASSWC Double (Pass - Pas Lowercase (PASS))RD - DROWSSAP) sPass) vORD - password) ord - PASSWORD)		aee8 aee8
M	ΡυΤΤΥ		assword	<u>र</u> य	Num. sub. perms (F Case perms (Pass,p Two numbers Hybri	vass,P4ss,Pa5s,P45sP455) pAss,pa5s,PaSsPASS) id Brute (Pass0Pass99)		24-04-04 02:
	Cain	Plain Attack 1 of 3	text of 8846F7EAEE8F < stopped! 2 hashes cracked	B117AD06BDD8	30B7586C is	password		
•)23:::
F						Start Exit		
			00			••	1:59 PM 1:59 PM 4/4/2024	

Task C: Extra credit: (10 points)

Search the proper format in John the Ripper to crack the following **MD5** hashes (use the <u>--list=formats</u> option to list all supported formats). Show your steps and results.

- 1. 5f4dcc3b5aa765d61d8327deb882cf99
- 2. 63a9f0ea7bb98050796b649e85481845