OLD DOMINION UNIVERSITY CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS ASSIGNMENT #5 PASSWORD CRACKING

Clarence V. Kimbrell Jr. UIN 01207106

Task A Step 1.



These groups were added by using the groupadd command. Then followed what the group named selected for the assignment. Many additions can be added following the initial groupadd command. For this assignment the first group needed to be called cyse301f22 then the second one was then our own Midas ID which is ckimb002.

Task A Step 2.



In the next part of our assignment, we are instructed to add users. This can be done by using the useradd command. For my convenience, I created six users with names that start with the letter "J". After I created the users then added them to the groups created in the previous step. This was done by using the usermod command followed by which group I would like them to join and their name.

Task A Step 3.



Then in step three, we are assigned to create a password for each user. This was accomplished by using the passwd command. For Jimmy, the password is "orange". For Jack, the password is "1234". For Jim, the password is "orange123". For Jill, the password is "orange123!". For Josh, the password is "pear123" For James, the password is "Pear123!". I created these passwords with increasing difficulty and assigned them down the list of users.





To export all six users' password hashes, we need to create a file for them to be stored. First, we start with the touch command to create a file name our Midas which is ckimb002 then followed by "-HASH". Now we have a file that we can export the password hashes. This is done by using the tail command which reads off the last few lines in the file and the /etc/shadow command this is to display the hashes in the first place. Then we add the redirect ">" to the file of our choice which is ckimb002-HASH.



In this part of step 4 we had to unzip a word list file, this file contains thousands of commonly used passwords. Then we copied this file to our home directory to be able to access it much easier. Then we used the john the ripper program in the command line with the file we want to attack and with the wordlist file. Within seconds it was able to reveal three passwords.

Task B Step 1



When using meterpreter we can use the hashdump command to see the list of hashes on the target windows. These were the accounts created in the prerequisites to step 1. This was only available by establishing a reverse shell connection with admin privilege on the target windows.

Task B Step 2



In step two we are using john the ripper. In this case, we are asking it to use the hashes that were copied from windows 7. Then for us to see what the passwords are we have to use the --format=NT. After 10 minutes it was able to figure out the passwords used for the accounts created on the windows VM.

Task B Step 3

0	Tile Action Media Clipboard	n CY301-CKIMB002 - Virtual Machine Connection View Help			- 0 ×		
Recycle Bin	Applications • Places •	D 👻 🛍 ■ rdesktop 🕶	Wed 21:57		1 1 / 10 -		
2		Terminal		- 0 x			
Acrobat	File Copyr	root@CS2APen1	Test: -				
Reader	C:\W	rdesk	ctop - 192.168.10.9		อไ	INION	
	net LAutos	Protection datable				SITY	
Mmap -	NET LCOOP	Dictionary					
Zenmap GUI	I [USETWARN]	File	Position 4 3456292				
Nutanic SSR							
	C:\Wi Geogle net u Chrome	Key Rate	Options				
	M The c	Dictionary Position	Reverse (PASSWORD Double (Pass - PassPas	DROWSSAP)			
Wireshark	C:\Wi	<u>U</u>	Lowercase (PASSW0Ri Uppercase (Password	/ - password) /ASSWORD)		14 C	
	net 1 pluny The c	Current password	Case perms (Pass, A	4ss,Pa5s,P45sP455) JaSs,PaSsPASS)			
			V Two numbers Hybrid Bru	e (Pass0Pass99)		10 C	
Google Chrome	🔁 C: \Wi	Plaintext of 7CE21F17COAEE7F1 Plaintext of CA8E025E9893E8C1	4 nge				
	2 Cale	Attack stopped! 3 of 5 hashes cracked	SWOID		100 C 100		
104-106						100 B 100	
Login info						100 State 1	
		1		Start Exit Window	👷 🔣 KALI		
VMware				I his copy of Windows is not genu	ine avenues teconor	the ITS Help Desk:	
Workstati		🖻 📑 o 💽 🌄		P 🔂 🕩 12/7/2022.		nelp@odu.edu	

This first screenshot is using a dictionary attack using the cain and Abel program. We were able to complete this attack by using the default word list that is on the windows 7 VM. Within seconds it displays the passwords of the user accounts.

	Reference - External Workstation	on CY301-CKIMB002 - Virtual Machine Connection	×
	File Action Media Clipboard	View Help	
Recycle Bin			
	Applications • Places •	Terminal	
	File Charles Contract	Tanalad Hala	
Acrobat Reader	Copyr	root@CS2APenTest; • ×	UNION
	C:\WJ	rdesktop - 192.168.10.9	INION
e e e e e e e e e e e e e e e e e e e	The SERROF		SITY
Nmap - Zenmap GUI	NET LConne Recycle Bin		
	Luserwarni	Brute-Force Attack	
		Charleton Min 1 -	
Nutanic SSR		ebcdelghijdmoopgstuwwyo0123456789	
	net L Google	C Custom	
<u></u>	M The c	Li L	
Wireshark	C:\Wi	3760620109779060 gvguva	100 C
	net l puny	Key Rate Time Left 11090314 Pass/Sec 10.7525 years	
		Division of ORIGERETEREDUSTION DOCUMENTS of a summer	
Google Chrome	C: \Wi	Plaintext of CAECUSEPSICEDICEDCEDES3005306 is password Plaintext of ACECUSEPSICEDICEDCEDCEDAS3200546AD6 is 1234	
VM - Kali Login info		Stop Eat	
-		Windows 7	
		Build 7600 This capy of Windows is not genuine	the ITS Help Desk:
VMware Workstati			nelp@odu.edu

In this screenshot, we are using a brute force attack. This program allows for the customization of settings to allow quicker results. We selected the default letter and number choice and lowered the maximum number of characters to 10. Then nearly instantly found the passwords for the user accounts.