

LAB MANUAL ON PASSWORD CRACKING OF WINDOWS OPERATING SYSTEM



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

INTRODUCTION TO PASSWORD CRACKING	2
PASSWORD CRACKING TECHNIQUES	3
TOOL I: MIMIKATZ TOOL	4
GETTING HASH OF PASSWORD WITH MIMIKATZ TOOL	5
TOOL II: HASHCAT TOOL	16
RECOVERING PLAINTEXT FROM NTLM HASH WITH HASH	САТ
TOOL	16
COUNTERMEASURES	27
REFERENCES	29

MANUAL-4: PASSWORD **CRACKING OF** WINDOWS **OPERATING SYSTEM**

INTRODUCTION TO PASSWORD CRACKING

 Passwords are used to protect the system from an unauthorized access.

 Computers with Windows operating system stores password in Security Account Manager (SAM) file in the form of New Technology LAN Manager (NTLM) hash.

- Passwords are stored in the form of hash due to its irreversible property. This means that password in plaintext can be converted to hash but a hash can't be converted back to plaintext.
- Password cracking in Windows operating system is a process to recover passwords from a SAM file.

 The purpose of password cracking is to recover forgotten password. The forensic team can perform password cracking on a computer system to recover the data after getting the password.

 This is usually accomplished by recovering the passwords from data stored in the SAM file in the form of NTLM hash value.



Figure 1: Password Cracking

PASSWORD CRACKING TECHNIQUES

The password cracking techniques are discussed as follows:

 BRUTE FORCE: A brute force technique is an attempt to crack passwords using permutation and combination approach. This method takes a lot of time and memory consumption depending on the length and complexity of password.

 DICTIONARY: A dictionary technique is an attempt to store in-build passwords in a file known as dictionary. Instead of trying all combination of passwords, it creates a word-list of most common passwords and calculates the hash values while cracking the passwords. It will only able to crack the password if it is stored in dictionary file. This technique takes less time as compared to brute-force technique to crack the password.

• **RAINBOW TABLES**: This technique is same as dictionary, but instead of calculating hash vales during password cracking; it stores the in-built hash values of password in the tables. Thus, this technique takes less time as compared to brute-force and dictionary technique to crack the password.

TOOL I: MIMIKATZ TOOL

 The Mimikatz tool [1] was first developed in 2007 by Benjamin Delpy.

 Mimikatz is an open-source application and postexploitation Windows operating system tool that allows users to view authentication credentials.

 This tool provides hashes from SAM file of Windows operating system to users.

 Windows store password data in an NTLM hash. The forensics team can use Mimikatz tool to get the hash string and use hashcat tool to get plain text and pass it to the target computer to login.

GETTING HASH OF PASSWORD WITH MIMIKATZ TOOL

The NTLM hash of password can be accessed with mimikatz tool with following steps:

Step 1: Open Run box by clicking "Window + R" on keyboard and type "regedit" as shown in Figure 2 and Figure 3 respectively. Click "OK" to proceed.



Figure 2: Windows 10 operating system



Figure 3: Opening Windows registry file

Step 2: A Registry Editor file with SAM and SYSTEM folder will open as shown in Figure 4.

The SAM and SYSTEM files are located in *"C:\Windows\System32\config"* path as shown in Figure 5.

📑 Registry Editor				-	×
File Edit View Favorites Help					
Computer\HKEY_LOCAL_MACHINE\SYS	STEM				
> HKEY_CLASSES_ROOT	Name	Туре	Data		
> HKEY_CURRENT_USER	(Default)	REG_SZ	(value not set)		
HKEY_LOCAL_MACHINE					
SAM					
SECURITY					
> SOFTWARE					
SYSTEM					
> ActivationBroker					
> ControlSet001					
> CurrentControlSet					
> DriverDatabase					
HardwareConfig					
Keyboard Layout					
Maps					
MountedDevices					
> ResourceManager					
> ResourcePolicyStore					
RNG					
Select					
> Setup					
< Software >					



← → • ↑ 📘	C:\Wir	ndows\System32\config			
		Name	Date modified	Туре	Size
📌 Quick access		—	10 00 0010 10 00	51.6.1	
E Desktop	*	Journal	19-03-2019 10:22	Filefolder	
		🛃 RegBack	19-03-2019 10:22	File folder	
- Downloads	*	systemprofile	19-03-2019 10:22	File folder	
🛗 Documents	*	📑 TxR	20-11-2019 13:55	File folder	
Pictures	*	📄 BBI	20-11-2019 13:54	File	512 KB
course 1		BCD-Template	11-10-2019 05:28	File	28 KB
h Music			20-11-2019 13:57	File	39,936 KB
Videos		DEFAULT	20-11-2019 13:54	File	512 KB
E		DRIVERS	20-11-2019 13:59	File	4,096 KB
lesson on e Drive e Statement de Carlos e Carlos		ELAM	11-10-2019 04:29	File	32 KB
This PC		SAM	20-11-2019 13:54	File	64 KB
			20-11-2019 13:54	File	32 KB
3D Objects		SOFTWARE	20-11-2019 13:54	File	81,408 KB
📃 Desktop		SYSTEM	20-11-2019 13:54	File	13,312 KB

Figure 5: SAM and SYSTEM file

Step 3: These SAM and SYSTEM files can be accessed by registry editor after giving administrative permissions. Right click on the SAM file as shown in Figure 6. Then allow "Full Control" and "Read" by clicking the check box as shown in Figure 7.

📑 Registry Editor				_	×
File Edit View Favorites	lelp				
Computer\HKEY_LOCAL_MACH	NE\SAM\SAM				
Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_CURRENT_USER HKEY_CURRENT_USER HKEY_CURRENT_USER SAM SCONDOR SAM SCONDOR SAM SCONDOR SEC SON HARDWARE SAM SEC SON SEC SON HARDWARE SEC SON SEC SON HEV Export HKEY_ Copy Key	Name	Type REG_SZ REG_BINARY REG_BINARY	Data 0 09 00 01 00 00 00 00 00 00 00 00 00 00 03 00 01 00 01 0 fe ff 07		

Figure 6: Checking permissions of SAM file

Permissions for SAM				×
Security				
Group or user names:				
SYSTEM				
Administrators (CYBERSHWV	Adminis	trators)		
	Ad	ld	Remove	
Permissions for Administrators		Allow	Deny	
Full Control				
Read		\square		
Special permissions				
For special permissions or advance	d settin	gs,	Advanced	
Click Advanced.				
OK		Cancel	Apply	

Figure 7: Giving permissions to the SAM file

Step 4: Export the SAM file after giving the administrative permissions. Right click on the SAM file and click "Export" as shown in Figure 8. Save the file by giving file name as "SAM" and type as "Registry Hive Files" as shown in Figure 9.

📑 Registry Editor			– 🗆 X
File Edit View Favorites Help			
Computer\HKEY_LOCAL_MACHINE\SAM\SAM			
 HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE BCD0000000 HARDWARE SAM SEC SAM SCI New SOI New SOI Permissions Copy Key Name MountedDevices Permissions 	Type REG_SZ REG_BINARY U REG_BINARY	Data (value not set) 09 00 01 00 00 00 00 00 00 00 00 00 00 03 00 01 00 01 0 fe ff 07	
ResourcePolicyStore RNG			
 Select Setup 			

Figure 8: Exporting the SAM file

Export Regis	try File				×
Save in:	E Desktop		~	G 🕸 🖻 🛄 -	
Quick access	OneD)rive	2	NITTR	
Desktop	This F	ork		Libraries	
Libraries					
٢					
Network	File name:	SAM		~	Save
	Save as type:	Registration Files (*.reg)		~	Cancel
Export range All Selected bra	nch	Registration rules (reg) Registry Hive Files (*.*) Text Files (*.txt) Win9x/NT4 Registration File All Files	es (*.reg)		
HKEY_LC	DCAL_MACHINE\S/	AM\SAM			

Figure 9: Saving the SAM file

Step 5: In a similar fashion, right click on the SYSTEM file and give administrative permissions by allowing "Full Control" and "Read" after clicking the check box as shown in Figure 10.

Permissions for SYSTEM				×
Security				
Group or user names:				
SYSTEM				^
Administrators (CYBERSHW)	Administr	rators)		
Series (CYBERSHW\Users)				
<			>	~
	Add	I	Remove	
Permissions for Administrators		Allow	Deny	
Full Control				
Read		\checkmark		
Special permissions				
For special permissions or advance click Advanced.	ed setting	IS,	Advanced	
ОК	(Cancel	Арр	ły

Figure 10: Giving permissions to the SYSTEM file

Step 6: Export the SYSTEM file after giving the administrative permissions. Right click on SYSTEM file and click "Export" as shown in Figure 11. Save the file by giving file name as "SYSTEM" and type as "Registry Hive Files" as shown in Figure 12.

🔡 Registry Editor				-	×
File Edit View Favorites Help					
Computer\HKEY_LOCAL_MACHINE\SYS	STEM				
> HKEY_CLASSES_ROOT	Name	Туре	Data		
	赴 (Default)	REG_SZ	(value not set)		
BCD0000000					
> HARDWARE					
SAM					
> SOFTWARE					
SVSTEM	I				
Collapse					
New	>				
Find					
Delete					
Rename					
Export					
Permissions					
Copy Key Name					
Go to HKEY_CURRENT_US	ER				
<					

Figure 11: Exporting the SYSTEM file

Export Regist	try File				×
Save in:	Desktop		~	G 🕸 📂 🛄 -	
Quick access	OneDa	ive	2	NITTTR	
Desktop	This P	c		Libraries	
Libraries	Netwo	ork			
This PC					
Matura de					
Network	File name:	SYSTEM		~	Save
F	Save as type:	Registry Hive Files (*.*)		\sim	Cancel
All					
Selected bran HKEY_LO	nch CAL_MACHINE\SY	STEM			

Figure 12: Saving the SYSTEM file

Step 7: Download the "Mimikatz" tool by clicking the "mimikatz_trunk.zip" file from GitHub website as shown in Figure 13 and Figure 14.

Google	Iminikatz download Images Images	🌷 Q				
	🔍 All 🕨 Videos 🖽 News 🖾 Images 🧷 Shopping :	More Settings Tools				
	About 1,08,000 results (0.52 seconds)					
	Releases · gentilkiwi/mimikatz · GitHub https://github.com › gentilkiwi › mimikatz › releases • A little tool to play with Windows security. Contribute to gentilkiwi/m creating an account on GitHub.	imikatz development by				

Figure 13: Search Mimikatz tool



Figure 14: Download Mimikatz_trunk file from GitHub

<u>Step 8</u>: After downloading the file, unzip the "mimikatz_trunk.zip" file. Now go to: "C:/Downloads/mimikatz_trunk/x64/mimikatz" and left click twice on mimikatz file as shown in Figure 15.

	> Thi	s PC → Downloads → mimikatz_trunk	c → x64		
		Name	Date modified	Туре	Size
ess		🚳 mimidrv.sys	25-11-2019 12:22	System file	36 KB
	1	🥝 mimikatz	25-11-2019 12:22	Application	991 KB
ads	*	🖻 mimilib.dll	25-11-2019 12:22	Application exten	46 KB
ints	*				
	*				



Step 9: A prompt with a security warning will open as shown in Figure 16. Click on "Run" button to run the tool.

Open File	- Security War	ning	×
Do you	want to run ti	his file?	
	Name:	\NITTTR\Downloads\mimikatz trunk\x64\mimikatz.ex	e
	Publisher:	<u>Open Source Developer, Benjamin Delpy</u>	
	Type:	Application	
	From:	C:\Users\NITTTR\Downloads\mimikatz_trunk\x64\mim.	
		Run Cancel]
🗹 Alwa	ys ask before o	pening this file	
٢	While files fr harm your co <u>What's the ri</u>	om the Internet can be useful, this file type can potentiall omputer. Only run software from publishers you trust. <u>sk?</u>	у

Figure 16: Click "Run" button

Step 10: A command line prompt of Mimikatz tool will open as shown in Figure 17.

🥝 mimikatz 2	.2.0 x64 (oe.eo)		
.#####. .## ^ ##. ## / \ ## ## \ / ## '## v ##' '#####	<pre>mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47 "A La Vie, A L'Amour" - (oe.eo) /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)</pre>		Â
mimikatz #			
			\checkmark

Figure 17: Mimikatz command line

Step 11: Type "Isadump::sam /system:C:\Users\NITTTR\Desktop\SYSTEM /SAM:C:\Users\NITTTR\Desktop\SAM" command in command line prompt of Mimikatz tool. Press Enter. The command will show NTLM hash password of Windows operating system as shown in Figure 18.



Figure 18: Typing the command and getting NTLM hash

TOOL II: HASHCAT TOOL

- Hashcat tool [2] is an advanced password recovery tool.
- It had a proprietary code base until 2015, but now it is an open source tool and available in Kali Linux operating system.
- It recovers and provides plaintext of various hash such as LM, NTLM, MD5, SHA, and so on.

RECOVERING PLAINTEXT FROM NTLM HASH WITH HASHCAT TOOL

The Mimikatz tool provides NTLM hash of Windows operating system password. The password in plaintext from NTLM hash can be recovered with hashcat tool with following steps:

Step 1: Open Kali Linux operating system as shown in Figure 19.



Figure 19: Kali Linux operating system

Step 2: Copy the NTLM hash (recovered with Mimikatz tool, refer Figure 18) and store it in a file on Desktop as shown in Figure 20. Also, multiple NTLM hash can be stored in a file to get plaintext as shown in Figure 21.







Figure 21: Multiple NTLM hash in a file

Step 3: Search the password wordlist by browsing Google search engine as shown in Figure 22. Open the GitHub website and download the ZIP file as shown in Figure 23.



Figure 22: Search password wordlist

GitHub - berzerk0/Prob	able-Word	dlists: Versio	on 2 is live! Wordlists	sorted by probal	bility originally cre	ated for passwoi	rd generation and testing - make	sure your passwords ar
G password wordlist o	downlix	Ç GitHub	- berzerk0/Probal ×	+				
← → ⊂ ŵ		(i) 🔒 Gi	tHub, Inc. (US) htt	ps:// github.com /b	erzerk0/Probable	-Wordlists		♥ ☆
	wordlist	password	password-strength	password-safety	dictionary-attack	dictionary		
	-0- 26	9 commits	្ទ្រ 2 branche	s 🗇 0	packages		4 contributors	മൂ CC-BY-SA-4.0
	Branch: ma	aster - Ne	ew pull request				Find file	Clone or download -
	脑 berz	erk0 fix 404 or	line 53				Clone with HTTPS ??	
	Analy	Analysis-Files		Appeara	Appearances for some files		Use Git or checkout with SVN u	sing the web URL.
	Dictio	Dictionary-Style		Formattir	Formatting that you don't see until after pushir		https://github.com/berzer	k0/Probable-W 📴
💼 Re		Passwords		fix 404 or	n line 53		Download	ZIP

Figure 23: Download password wordlist

Step 4: Save and open the downloaded file as shown in Figure 24. Open the "Real-Passwords" folder to see the passwords wordlist as shown in Figure 25.

< >	🔂 Home Download	s Probable-Wts-m	aster 🔻		٩ 🗉	- E 0
🕲 Recent						
★ Starred						
🔂 Home						
Desktop	Analysis-Files	Changelog.md	Contributing.md	Dictionary-Style	Downloads.md	License.txt
Documents						
④ Downloads	Probable Wordlists					
🎜 Music						
n Pictures	ProbableWordlistLo go.png	README.md	Real-Passwords			

Figure 24: Password folder in downloaded file



Figure 25: Password wordlist

Step 5: Open any password wordlist (e.g., Top12Thousand-probable-v2.txt file) as shown in Figure 26. Copy the wordlist file on Desktop and rename as "pwdlist" as shown in Figure 27.

Open ▼	Top12Thousand-probable-v2.txt /Downloads/Probable-Wordlists-master/Real-Passwords	Save	
123456 password 123456789 12345678 12345 qwerty 123123 111111 abc123 1234567 dragon 1q2w3e4r sunshine 654321 master 1234 football 1234567890 00000 computer 666666 superman michael internet iloveyou			

Figure 26: Top 12 thousand most frequently used passwords

Applicatio	ons 🔻 🛛 Places	s ▼ 📳 Text Editor ▼		Wed 04:56				
		Open 👻 🖻	pwdlist ~/Desktop		Save	0	•	8
		123456						
	hash	password						
		123456789						
		12345678						
		12345						
		qwerty						
	and the second se	123123						
	pwdlist	111111						
		abc123						
		1234567						
		dragon						
		Iq2w3e4r						
*-	command	654221						
-	commente	mostor						
		1234						
		football						
		1234567890						
M		000000						
	hash (copy)	computer						
		666666						
2		superman						
		michael						
		internet						
		iloveyou						
		daniel						

Figure 27: Copy the wordlist file on Desktop

<u>Step 6</u>: In Kali Linux operating system, open the hashcat tool. Go to Applications-> Password attacks-> hashcat as shown in Figure 28.



Figure 28: Opening hashcat tool

Step 7: A terminal with usage of hashcat tool will open as shown in Figure 29. The tool states various hash modes which can be recovered as shown in Figure 30 and Figure 31. The NTLM hash has ID of 1000 as shown in Figure 31. The tool also shows various attack modes as shown in Figure 32.

le Edit View Search Terminal shcat - advanced password re age: hashcat [options] ha [Options] -	root@kali:~
le Edit View Search Terminal shcat - advanced password re age: hashcat [options] ha [Options] -	Help ecovery ash hashfile hccapxfile [dictionary mask directory
shcat - advanced password re age: hashcat [options] ha [Options] -	ecovery ash hashfile hccapxfile [dictionary mask directory
age: hashcat [options] ha [Options] -	ash hashfile hccapxfile [dictionary mask directory
[Options] -	
[Options] -	
ntions Short / Long	
	Type Description
Example	Type Description
	+++
m,hash-type	Num Hash-type, see references below
i -m 1000 aattack-mode	Num Attack-mode, see references below
-a 3	
V,version	Print version
h,help	Print help
quiet	Suppress output
hex-charset	Assume charset is given in hex
1	
nex-satt	Assume satt is given in nex
1.18	gure 29. Hashcat terminar
	root@kali:~ 🖨 💼 (
le Edit View Search Terminal	Hala
	Help
commas brain-sessio	n-whitelist=0x2ae611db
commas brain-sessio [Hash modes] -	Help on-whitelist=0x2ae611db
commas brain-sessio	Help on-whitelist=0x2ae611db
commas brain-sessio [Hash modes] - # Name	Help on-whitelist=0x2ae611db Category
commas brain-sessio [Hash modes] - # Name =====+===============================	help on-whitelist=0x2ae611db Category
commas brain-sessio [Hash modes] - # Name =====+===============================	Help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name =====+===============================	heip on-whitelist=0x2ae611db Category Raw Hash Raw Hash Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name ====================================	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash Raw Hash Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224	help pn-whitelist=0x2ae611db Category Raw Hash Raw Hash Raw Hash Raw Hash Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name ============= 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-384 1700 SHA2-384	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-512 17300 SHA2-324	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-512 17300 SHA3-224	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name ====================================	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-226 10800 SHA2-384 1700 SHA2-384 1700 SHA2-512 17300 SHA3-224 17400 SHA3-256 17500 SHA3-384 17600 SHA3-384	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-384 1700 SHA2-512 17300 SHA3-224 17400 SHA3-256 17500 SHA3-384 17600 SHA3-512 17700 Keccak-224	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-512 17300 SHA3-224 17400 SHA3-256 17500 SHA3-384 17600 SHA3-512 17700 Keccak-224 17800 Keccak-256	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name # Name 900 MD4 0 MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-512 17300 SHA3-224 17400 SHA3-256 17500 SHA3-224 17600 SHA3-384 17600 SHA3-512 17700 Keccak-224 17800 Keccak-256 17900 Keccak-384	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash
commas brain-sessio [Hash modes] - # Name # Name 900 MD4 0 MD5 5100 Half MD5 5100 Half MD5 100 SHA1 1300 SHA2-224 1400 SHA2-256 10800 SHA2-384 1700 SHA2-512 17300 SHA3-224 17400 SHA3-256 17500 SHA3-256 17500 SHA3-384 17600 SHA3-512 17700 Keccak-224 17800 Keccak-256 17900 Keccak-384 18000 Keccak-384	help on-whitelist=0x2ae611db Category Raw Hash Raw Hash

	root@kali: ~	000
File Edit	View Search Terminal Help	
16400	CRAM-MD5 Dovecot	HTTP, SMTP, LDAP Se
rver		
15000	FileZilla Server >= 0.9.55	FTP Server
11500	CRC32	Checksums
3000	LM	Operating Systems
1000	NTLM	Operating Systems
1100	Domain Cached Credentials (DCC), MS Cache	Operating Systems
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	Operating Systems
15300	DPAPI masterkey file v1	Operating Systems
15900	DPAPI masterkey file v2	Operating Systems
12800	MS-AzureSync PBKDF2-HMAC-SHA256	Operating Systems
1500	descrypt, DES (Unix), Traditional DES	Operating Systems
12400	BSDi Crypt, Extended DES	Operating Systems
500	md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5)	Operating Systems
3200	bcrypt \$2*\$, Blowfish (Unix)	Operating Systems
7400	sha256crypt \$5\$, SHA256 (Unix)	Operating Systems
1800	sha512crypt \$6\$, SHA512 (Unix)	Operating Systems
122	macOS v10.4, MacOS v10.5, MacOS v10.6	Operating Systems
1722	macOS v10.7	Operating Systems
7100	macOS v10.8+ (PBKDF2-SHA512)	Operating Systems
6300	AIX {smd5}	Operating Systems
6700	AIX {ssha1}	Operating Systems
6400	AIX {ssha256}	Operating Systems
6500	AIX {ssha512}	Operating Systems



Figure 32: Attack modes

<u>Step 8</u>: The basic examples regarding the usage of hashcat tool is shown in Figure 33.

	root@kali:~	0	• •
File Edit View Search Termi	nal Help		
1 Low 2 ms 2 Default 12 ms 3 High 96 ms 4 Nightmare 480 ms	Low Minimal Economic Noticeable High Unresponsive Insane Headless		
- [Basic Examples] -			
Attack- Hash- Mode Type ======+=====	 Example command +		====
======================================	hashcat -a 0 -m 400 example400.hash exam hashcat -a 0 -m 0 example0.hash example	nple.dio .dict -ı	ct r rul
Brute-Force MD5 Combinator MD5 e.dict	hashcat -a 3 -m 0 example0.hash ?a?a?a?a hashcat -a 1 -m 0 example0.hash example	a?a?a .dict e>	kampl
If you still have no idea w	what just happened, try the following pages	5:	
<pre>* https://hashcat.net/wiki/ * https://hashcat.net/faq/ root@kali:~#</pre>	#howtos_videos_papers_articles_etc_in_the	_wild	

Figure 33: Example of hashcat

Step 9: Write the command "hashcat -m 1000 -a 0 /root/Desktop/hash /root/Desktop/pwdlist --force" to recover the hash and "hashcat -m 1000 -a 0 /root/Desktop/hash /root/Desktop/pwdlist --force --show" to display the plaintext of NTLM hash as shown in Figure 34.

In this command, -m stands for hash mode (e.g., 1000 stands for NTLM hash, refer Figure 31) and -a stands for attack mode (e.g., 0 stands for straight attack, refer Figure 32). The

path to the hash file and wordlist file is also given in the command.

The plaintext of the NTLM hash is displayed in the Figure 34 and highlighted in red rectangular box. The plaintext of the NTLM hash is "password123".



Figure 34: Recover plaintext of NTLM hash

Step 10: Similarly, hashcat can recover plaintext of multiple hash file. Write the command "hashcat –m 1000 –a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force" to recover the hash and "hashcat –m 1000 –a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force -- show" to display the plaintext of multiple NTLM hash as shown in Figure 35.

The plaintext of the multiple NTLM hash is displayed in the Figure 35 and highlighted in red rectangular box. The

plaintext of the NTLM hash is "shweta123" "password123" respectively.	а	nd	
root@kali:~ File Edit View Search Terminal Help root@kali:~# hashcat -m 1000 -a 0 /root/Desktop/multiplehash /root/Desk stforce hashcat (v5.1.0) starting	• top/		8 Li ^
OpenCL Platform #1: The pocl project ====================================			
* Device #1: pthread-Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz, 1024/2231 atable, 1MCU INFO: All hashes found in potfile! Useshow to display them.	МВ	allo	рс
<pre>Started: Wed Mar 18 05:45:39 2020 Stopped: Wed Mar 18 05:45:39 2020 root@kali:~# hashcat -m 1000 -a 0 /root/Desktop/multiplehash /root/Desk stforceshow f5f03f250ecaceccc69568dee319637e:shweta123 a9fdfa038c4b75ebc76dc855dd74f0da:password123 root@kali:~# root@kali:~# root@kali:~#</pre>	top/	pwdl	Li

Figure 35: Recover plaintext of multiple NTLM hash

COUNTERMEASURES

The following countermeasures must be followed:

 Strong Passwords: Establish strong password using special characters, numbers, and lower and upper case alphabets.

• Minimum Password Length: The length of the password should be set to at least 14 characters. The long passwords are harder to crack than the short ones. • Dictionary words: Do not use dictionary words such as password, qwerty, abc123, etc. These passwords can be cracked easily with tools. Do not rely on similar looking characters such as: $3 \rightarrow E$, $5 \rightarrow S$, $! \rightarrow 1$. These words are also stored in dictionary.

 Minimum Password age: The users must change the password after some time (30 days). This will reduce the risk of password cracking.

 Stronger authentication method: Use stronger authentication methods such as enable Gmail one time password feature to login in a new device.

 Different passwords: Use different passwords for different device or websites.

 Sharing passwords: Do not share passwords with anyone or change password immediately after usage, if shared.

 Storing passwords: Avoid storing passwords in an unsecured location such as desktop or mobile phones. An attacker can access those passwords by hacking the device. Try to remember the passwords.

 Personal Information: Do not use personal information such as date of birth, pet names, vehicle number, etc. An attacker can easily guess the password by knowing personal details through social engineering.

REFERENCES

- [1] B. DELPY, "github," [Online]. Available: https://github.com/gentilkiwi/mimikatz/releases. [Accessed 21 February 2020].
- [2] Atom. [Online]. Available: https://tools.kali.org/password-attacks/hashcat. [Accessed 27 March 2020].