CS7339 HW3: Kali VM Install

Name: Bingying Liang
ID: 48999397

Oct 27 2023

Windows XP password hash files are attached so that you can begin attempting to crack them. The very basic description of the assignment is to try to collect as many username and password combinations as you can. 1 point will be given for each username, 1 point for each hash, and 2 points for each password.

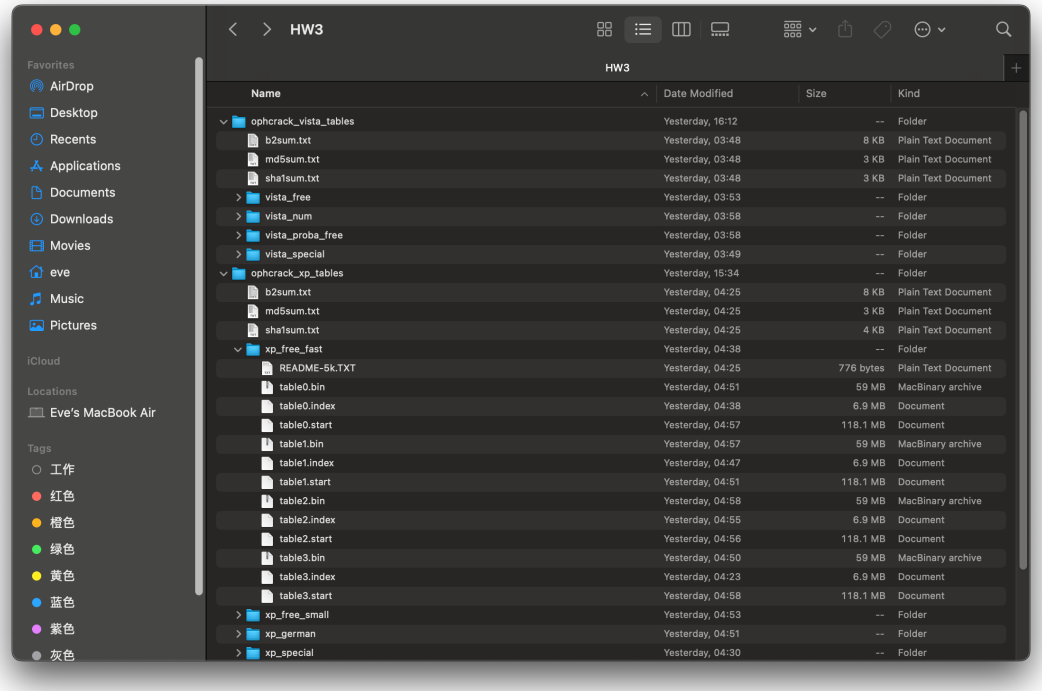
Remaining credit for 100 point total will be given for a 1 to 2 page write up on:

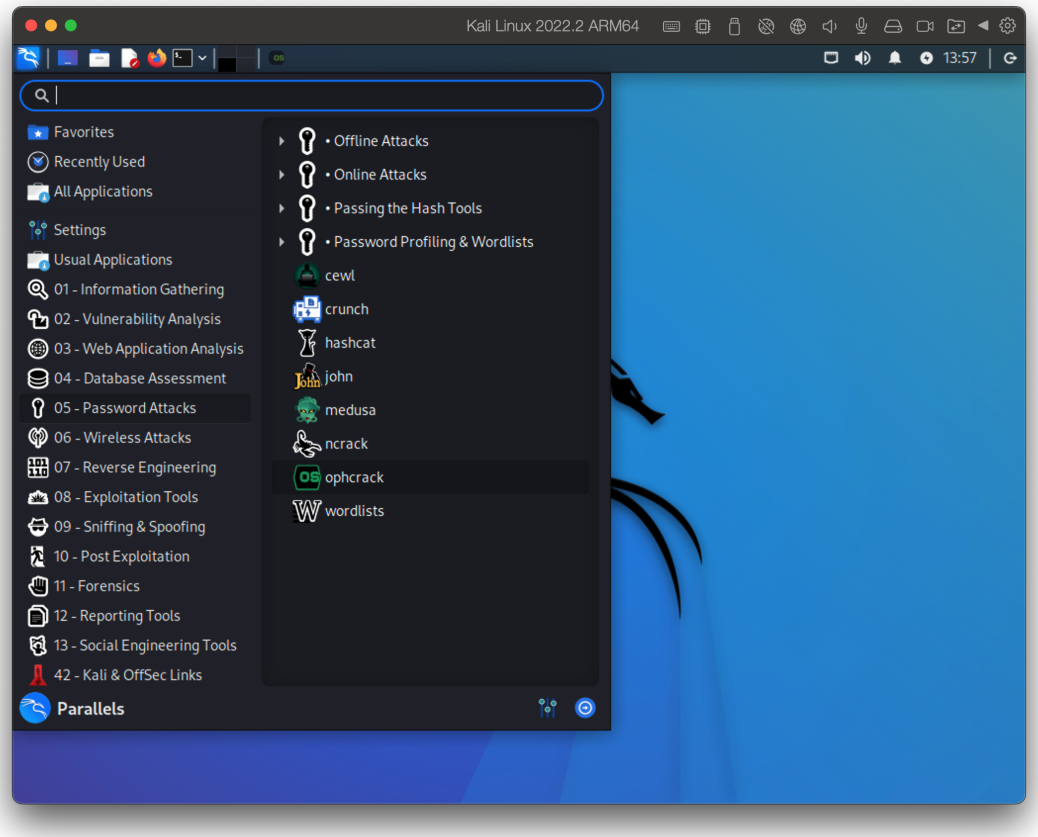
1. How you did it and what challenges you ran into.
2. How an attacker could obtain these files to steal the passwords in a live situation (i.e. - if you came across a physical XP system that was powered off or locked and you had to gain access to it).
3. What would be different if this was on a Windows 7 or newer system

1. How you did it and what challenges you ran into.

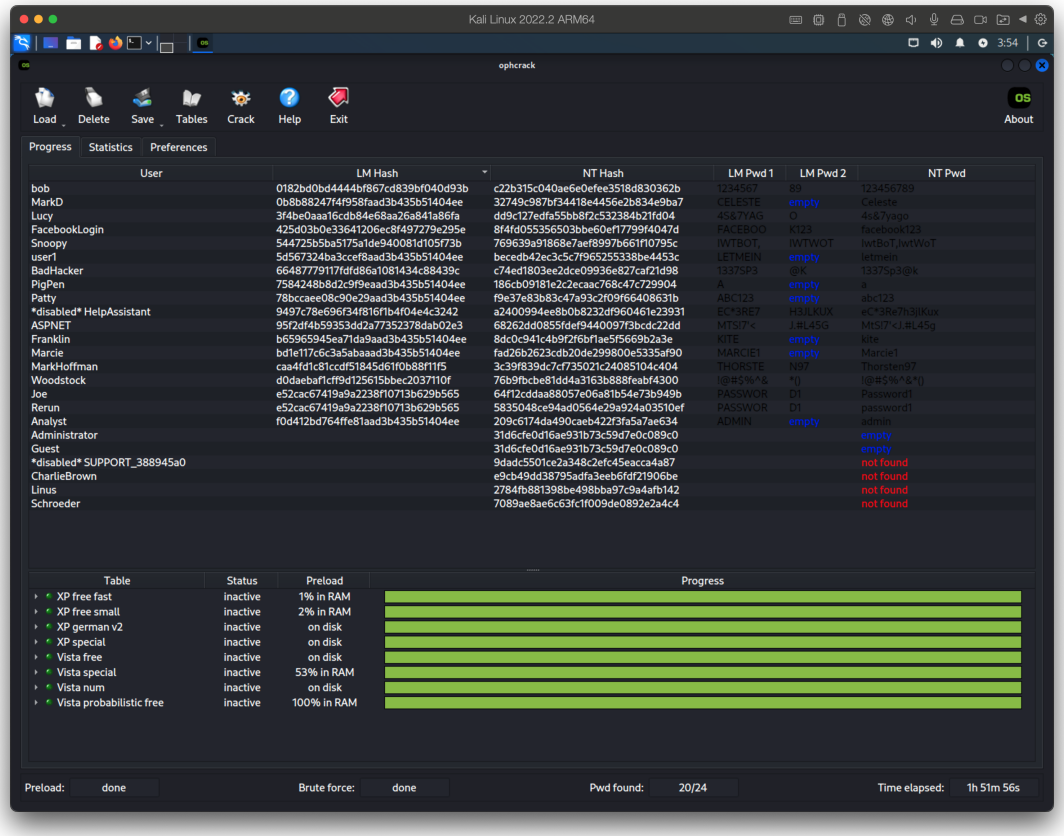
Solution:

(a) How I did it: I download tables from the ophcrack website and then use the virtual machine to use Kali OS. And then follow the instruction from the video which on the Canvas and the class.





And the result is show in the following, I also save the result in the result.csv file.



Result

0	500	Administrator		31d6cfe0d16ae931b73c59d7e0c089c0				1	0	0	empty	Bruteforce
1	501	Guest		31d6cfe0d16ae931b73c59d7e0c089c0				1	0	0	empty	Bruteforce
2	1000	*disabled* HelpAssistant	9497c78e696f34f816f1b4f04e4c3242	a2400994ee8b0b8232df960461e23931	EC*3RE7	H3JLKUX	eC*3Re7h3jlKux	1	3026	14	mixedalphanum+special	XP special/XP free fast
3	1002	*disabled* SUPPORT_388945a0		9dadc5501ce2a348c2efc45eacca4a87				0				
4	1004	ASPNET	95f2df4b59353dd2a77352378dab02e3	68262dd0855fdef9440097f3bcdc22dd	MTSl7'<	J.#L45G	MtSl7'<J.#L45g	1	2917	14	mixedalphanum+special	XP special/XP special
5	1005	Analyst	f0d412bd764ffe81aad3b435b51404ee	209c6174da490caeb422f3fa5a7ae634	ADMIN		admin	1	501	5	lowalpha	XP free fast/Bruteforce
6	1007	Joe	e52cac67419a9a2238f10713b629b565	64f12cddaa88057e06a81b54e73b949b	PASSWOR	D1	Password1	1	482	9	mixedalphanum	XP free fast/Bruteforce
7	1008	bob	0182bd0bd4444bf867cd839bf040d93b	c22b315c040ae6e0efee3518d830362b	1234567	89	123456789	1	481	9	num	Bruteforce/Bruteforce
8	1009	MarkHoffman	caa4fd1c81ccdf51845d61f0b88f11f5	3c39f839dc7cf735021c24085104c404	THORSTE	N97	Thorsten97	1	476	10	mixedalphanum	XP free small/Bruteforce
9	1010	MarkD	0b8b88247f4f958faad3b435b51404ee	32749c987bf34418e4456e2b834e9ba7	CELESTE		Celeste	1	475	7	mixedalpha	XP free small/Bruteforce
10	1011	CharlieBrown		e9cb49dd38795adfa3eeb6fdf21906be				0				
11	1012	Snoopy	544725b5ba5175a1de940081d105f73b	769639a91868e7aef8997b661f10795c	IWTBOT,	IWTWOT	IwtBoT,IwtWoT	1	3061	13	mixedalpha+special	XP special/XP free small
12	1013	BadHacker	66487779117fdfd86a1081434c88439c	c74ed1803ee2dce09936e827caf21d98	1337SP3	@K	1337Sp3@k	1	478	9	mixedalphanum+special	XP free fast/Bruteforce
13	1014	user1	5d567324ba3ccef8aad3b435b51404ee	becedb42ec3c5c7f965255338be4453c	LETMEIN		letmein	1	475	7	lowalpha	XP free small/Bruteforce
14	1015	Lucy	3f4be0aaa16cdb84e68aa26a841a86fa	dd9c127edfa55bb8f2c532384b21fd04	4S&7YAG	O	4s&7yago	1	729	8	lowalphanum+special	XP special/Bruteforce
15	1016	Linus		2784fb881398be498bba97c9a4afb142				0				
16	1017	FacebookLogin	425d03b0e33641206ec8f497279e295e	8f4fd055356503bbe60ef17799f4047d	FACEBOO	K123	facebook123	1	480	11	lowalphanum	XP free small/Bruteforce
17	1018	Woodstock	d0daebaf1cff9d125615bbec2037110f	76b9fbcbe81dd4a3163b888feabf4300	!@#$%^&	*()	!@#$%^&*()	1	669	10	special	Bruteforce/Bruteforce
18	1019	Patty	78bccaee08c90e29aad3b435b51404ee	f9e37e83b83c47a93c2f09f66408631b	ABC123		abc123	1	478	6	lowalphanum	XP free fast/Bruteforce
19	1020	PigPen	7584248b8d2c9f9eaad3b435b51404ee	186cb09181e2c2ecaac768c47c729904	A		a	1	0	1	lowalpha	Bruteforce/Bruteforce
20	1021	Schroeder		7089ae8ae6c63fc1f009de0892e2a4c4				0				
21	1022	Rerun	e52cac67419a9a2238f10713b629b565	5835048ce94ad0564e29a924a03510ef	PASSWOR	D1	password1	1	481	9	lowalphanum	Bruteforce/Bruteforce
22	1023	Marcie	bd1e117c6c3a5abaaad3b435b51404ee	fad26b2623cdb20de299800e5335af90	MARCIE1		Marcie1	1	476	7	mixedalphanum	XP free small/Bruteforce
23	1024	Franklin	b65965945ea71da9aad3b435b51404ee	8dc0c941c4b9f2f6bf1ae5f5669b2a3e	KITE		kite	1	3	4	lowalpha	Bruteforce/Bruteforce

(b) Challenges I ran into: When I choose the table to crack, I cannot use all of them at the same time, the software is failover. I have to crack them by one table, and then one by one. Another changllges is the some user cannot be cracked, the strong password cannot cracked by the tables.

2. How an attacker could obtain these files to steal the passwords in a live situation (i.e. - if you came across a physical XP system that was powered off or locked and you had to gain

access to it)

Solution:
An attacker might use the following way to obtain these files:

(a) Booting the system using an external device, such as a USB stick with a Linux distribution, circumvents operating system level security measures and provides direct access to the file system.

(b) Physically removing the hard drive and connecting it to another machine bypasses any OS-level passwords.

(c) If the user executes, malware or Trojans may be used to extract the hash file. And then can use another computer to crack it.

If I came across a physical XP system that was powered off or locked and you had to gain access to it I might booting the system using external device with USB which might provides direct access to the file system, and then I crack the password.

3. What would be different if this was on a Windows 7 or newer system

Solution:
To crack the password is much harder on a Windows 7 or newer system.

(a) Windows XP uses LM which is called LanManager and NTLM hashes. LM is vulnerable due to design flaws. Starting with Windows Vista, LM hashing is disabled by default.

(b) The introduction of User Account Control in Windows Vista adds an additional layer of security to restrict the permissions of applications without the consent of the user.

(c) BitLocker, introduced in Windows Vista, provides full disk encryption. This makes it harder for an attacker to access the file without the decryption key.

(d) Security Account Manager files are locked while the operating system is running, which makes it more challenging to extract hash values in real-time systems.

(e) Windows 10 adds Virtualization Security and certificate protection to provide stronger protection against attacks.