

Cyber Security

LAB-8

Mruganshi Gohel

B20CS014

Question: You must find at least three password brute-forcing tools and use them on your system. Make a report comparing them based on various factors such as type of attack, type of password able to track/guess, platform (windows, Linux, mac), time is taken, etc.

Also, include screenshots of your experiments in the report.

Ans.

the tools that I am going to use are :

- Aircrack-ng
- John the Ripper
- L0phtCrack

1. Aircrack-ng

Aircrack-ng is an open-source password-cracking tool primarily used to crack WEP and WPA/WPA2-PSK wireless networks. It can be run on Windows, Linux, and macOS platforms. Aircrack-ng uses a combination of dictionary and brute-force attacks to crack passwords. It has a fast cracking speed and supports multithreading. However, it is not effective against strong passwords and requires a high level of technical knowledge to use. It is used for password cracking, capturing packets, etc. It analyses incoming encrypted packets that come from wireless n/w and tries to attempt passwords using our brute-force cracking.

After downloading tool I went through some steps.

- start the wireless interface in the monitor mode

- Start airodump-ng on AP channel with filter for bssid to collect authentication handshake
- Use airplay-ng to deauthenticate the wireless client
- Run aircrack-ng to crack the pre-shared key using the authentication handshake

below is the full display of the steps

```
Read 139 packets.

# BSSID          ESSID          Encryption
1 00:11:22:00:00:00 test1          WPA (1 handshake)
2 00:11:22:00:00:01          WPA (0 handshake)

Index number of target network ? 1

Reading packets, please wait...
```

We use network 1 which is encrypted with WPA encryption and let aircrack-ng analyze the packets to crack the keys

```
Administrator: C:\WINDOWS\System32\cmd.exe
Read 139 packets.
1 potential targets

Aircrack-ng 1.7

[00:00:01] 2227/2294 keys tested (2270.58 k/s)

Time left: 0 seconds                                97.08%

KEY FOUND! [ 12345678 ]

Master Key      : 69 ED 1C 98 4B D8 E8 65 68 0E F8 14 03 F4 EB 4A
                  C3 41 D4 01 87 91 39 B0 9F 40 33 55 B5 EE E3 8C

Transient Key   : 15 B8 EA 23 57 CA 22 EC 29 2C 22 4F 09 41 F6 68
                  94 65 D3 15 05 FC AA 0A FC 4C 7B AB 66 20 86 97
                  91 86 FF 5F 61 CF 9D DC 96 20 43 8C 40 F8 CB 18
                  E7 74 AF 82 37 58 00 86 D9 46 41 A5 87 7B FC DA

EAPOL HMAC     : 61 59 36 A4 82 EB D3 56 4F 50 CE 6E 9A 10 F4 41
```

2. John the Ripper

John the Ripper is a free and open-source password-cracking tool that is used to perform dictionary and brute-force attacks. It is available for Windows, Linux, and macOS platforms. John the Ripper has a high success rate in cracking passwords, including strong passwords, and supports multiple cracking modes, including single and multi-mode.

After downloading the tool, I performed the following steps:

- Create a password file containing passwords to be cracked
- Run John the Ripper on the password file using a dictionary attack
- Run John the Ripper on the password file using a brute-force attack

to crack the passwords I ran the command

john --format=raw-MD5 "C:\Users\mruganshi\Desktop\passwords.txt"

Below is the result of the above steps:

```
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
Proceeding with incremental:ASCII
123456 (?)
1g 0:00:00.00 DONE 3/3 (2023-04-09 19:46) 1.742g/s 273919p/s 273919c/s 273919C/s 123456..mordee
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

analysis of the password that is cracked is:

password	0
incorrect	0
asdfghjkl	0
123456	1.7
Mruganshi12	>>10mins
Mruganshi&^561	>>40min (can say uncracked)

here first column shows the password I used to check and the second column shows the time tool took to crack.

3. L0phtCrack

L0phtCrack is a proprietary password-cracking tool that is used to perform dictionary and brute-force attacks. It is available for Windows platforms. L0phtCrack uses various techniques to crack passwords, **brute-force attacks**, and hybrid attacks.

When using a brute-force approach, L0phtCrack typically begins with shorter passwords and simpler character sets, and then progressively works up to longer passwords and more complex character sets. It may also use other techniques, such as wordlists or dictionary attacks, to speed up the process.

- ☒ **Quick Password Audit**
This method checks for passwords that you could find in a dictionary, with common permutations.
- ☐ **Common Password Audit**
This method checks for passwords that you could find in a dictionary, with many permutations.
This is followed by a 1 hour long brute-force attack using an alphanumeric+space character set.
- ☐ **Thorough Password Audit**
This method checks for passwords that you could find in a dictionary, with extensive permutations.
This is followed by an 6 hour long brute-force attack using a large ASCII character set.
- ☐ **Strong Password Audit**
This method starts with a 24 hour long brute-force attack using the entire ISO-8859-1 character set.
Then it checks for passwords that you could find in a dictionary, with all available permutations.
Use of a GPU-enabled machine is required. Audit may take several days to complete!

I used a **Common password Audit** which uses letters, and numbers in passwords (no special characters). It has a maximum character limit of 7.

- ☒ **Common Password Audit**
This method checks for passwords that you could find in a dictionary, with many permutations.
This is followed by a 1 hour long brute-force attack using an alphanumeric+space character set.
- ☐ **Thorough Password Audit**
This method checks for passwords that you could find in a dictionary, with extensive permutations.
This is followed by an 6 hour long brute-force attack using a large ASCII character set.
- ☐ **Strong Password Audit**
This method starts with a 24 hour long brute-force attack using the entire ISO-8859-1 character set.
Then it checks for passwords that you could find in a dictionary, with all available permutations.
Use of a GPU-enabled machine is required. Audit may take several days to complete!

Dictionary: wordlist-medium.txt, 253525 words. No length limit. 'Jumbo Plus' permutations set.

Brute Force: Letters, numbers, 7 character limit, 1 hour maximum.

	Username	NTLM Hash	NTLM Password	NTLM State	User Info	User Id
1	Administrator				(Built-in account for administering the computer/domain)	500
2	DefaultAccount				(A user account managed by the system.)	503
3	Guest				(Built-in account for guest access to the computer/domain)	501
4	HP	0AC69E26K9BFD135DE1E9E4B5A8E60E0		Not Cracked		1001
5	WDAGUtilityAccount	DCAEA96E5D24E8A175D6A37DC543900		Not Cracked	(A user account managed and used by the system for Windows Defender Application Guard ...)	504

here we can see that tool not able to crack some passwords and also check account status using the brute force method since my passwords were tough enough.

but in below image passwords has been cracked due to easy password had been used.

Schedule	2	Guest				Cracked: No Password Hash	501
Documentation	3	user1	8846F7EAXE8FB117AD06BDD830B7686C	password		Cracked (Dictionary:Fast): instantly	1001
System	4	user2	32ED87BDB5FDC5E9CBA88647376818D4	123456		Cracked (Dictionary:Fast): instantly	1002
Settings	5	user3	3B3E70A62518B4386538BDC089254858	wonderful		Cracked (Dictionary:Fast): instantly	1003
	6	user4	403FE014F97595A8070C59C8A9859180	abc789		Cracked (Dictionary:Fast): instantly	1004
	7	user5	34823259805A88A95E921F4F7E053334			Not Cracked	1005

Status: Pass 1/1 (NTLM): Elapsed Time: 0d0h0m1s Pass Time Left: 0d0h3m59s Max Time Left: 0d0h59m59s Speed: 5.062Mc/s

Overall, John the Ripper has the highest success rate in cracking passwords, followed by Aircrack-ng and L0phtCrack. However, Aircrack-ng is the most effective in cracking wireless network passwords, while L0phtCrack is the best tool for password policy auditing. The time taken to crack passwords varies depending on the complexity of the password and the type of attack used.