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

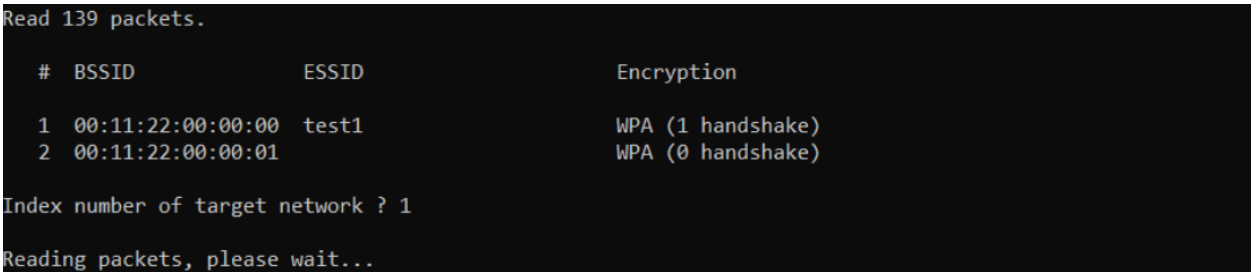
Aircrack-ng is an open-source password-cracking tool primarily used to crack WEP and WPA/WPA2-PSK wireless networks. It can be run on Windows, Linux, and macOS platforms. Aircrack-ng uses a combination of dictionary and brute-force attacks to crack passwords. It has a fast cracking speed and supports 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.

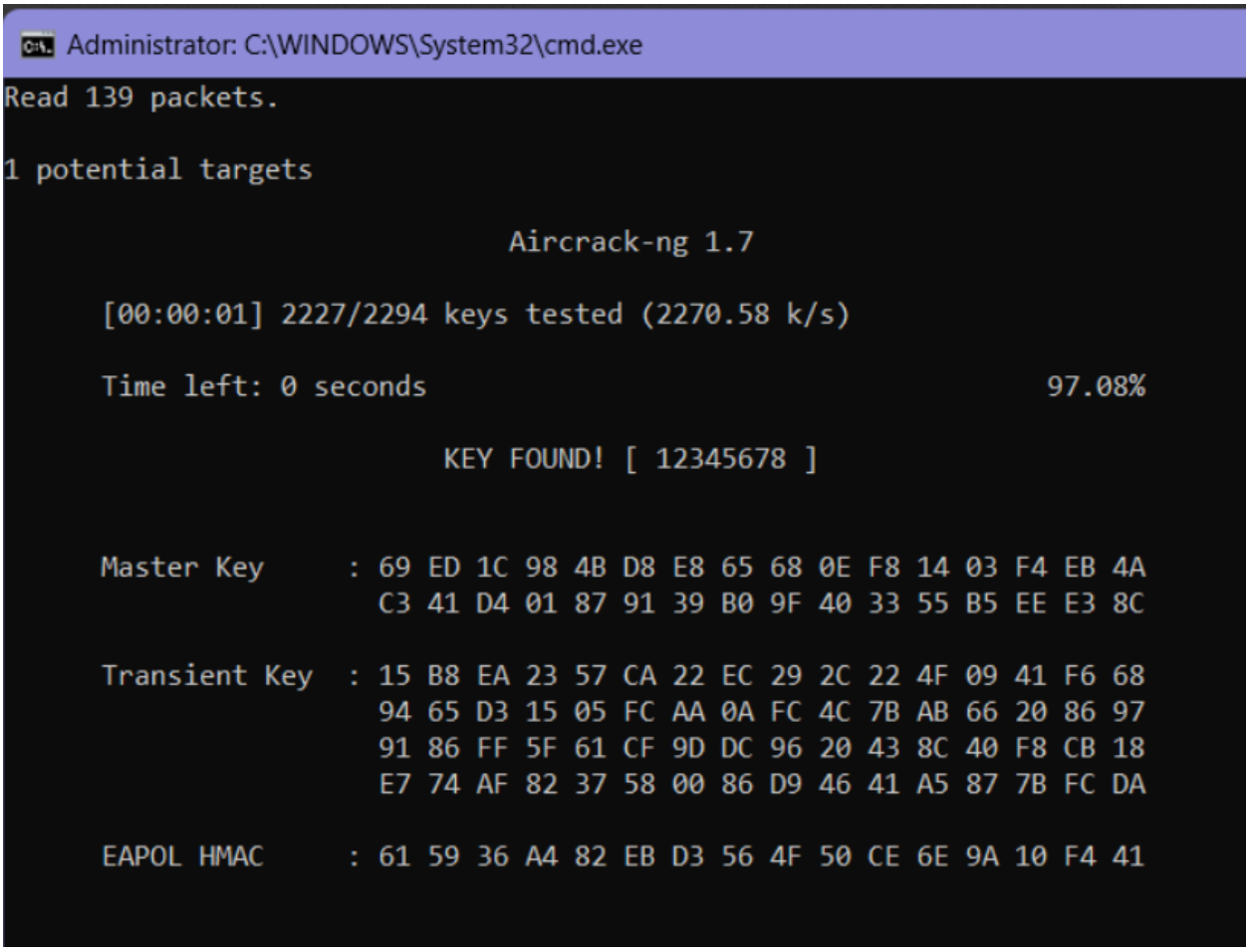
- start the wireless interface in the monitor mode

- 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



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



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.

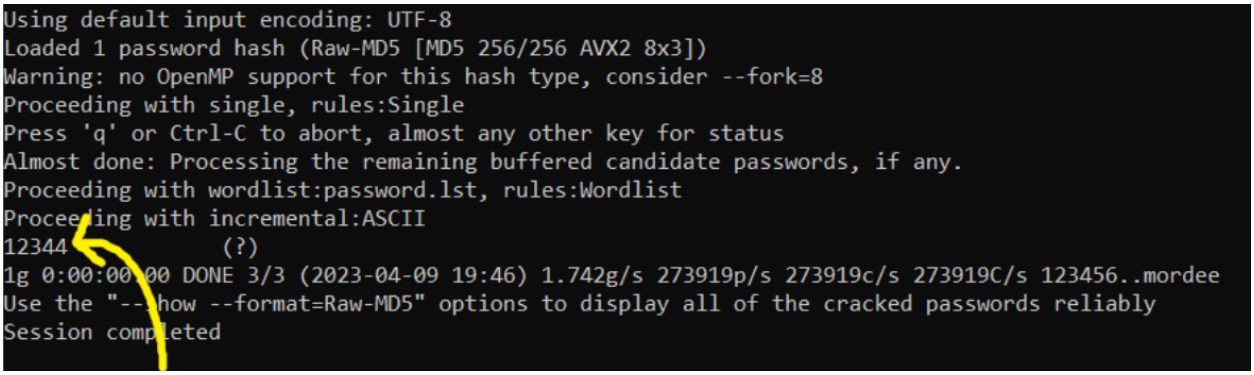
After downloading the tool, I performed the following steps:

- 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:



analysis of the password that is cracked is:

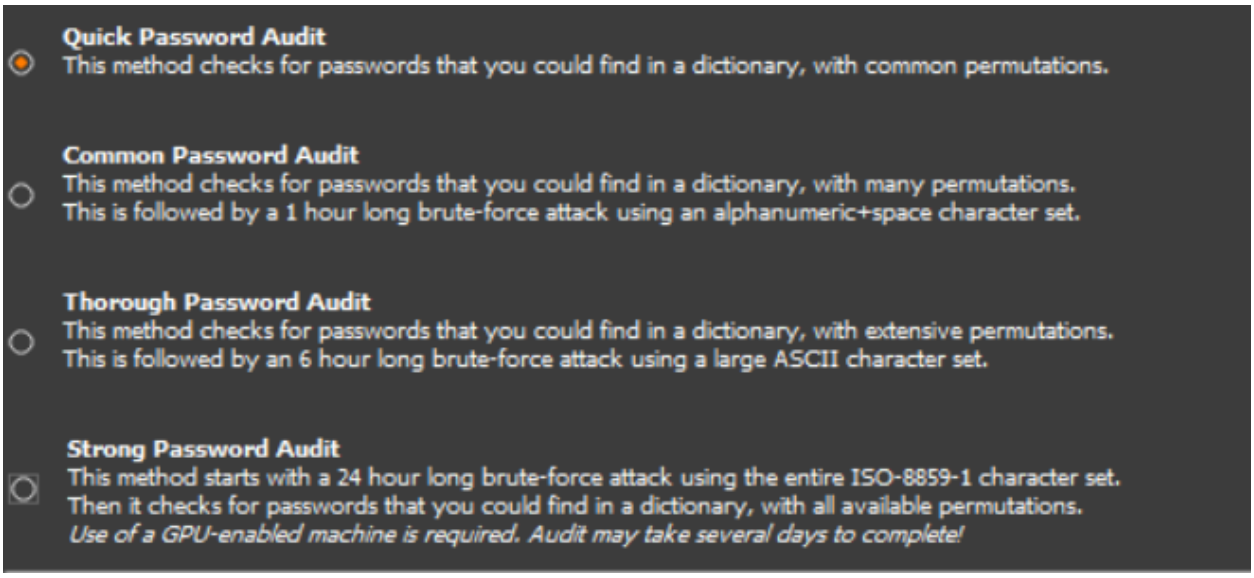
password	0
incorrect	0
asdfghjkl	0
123456	1.7
Mruganshi12	>>10mins
Mruganshi&^561	>>40min (can say uncracked)

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

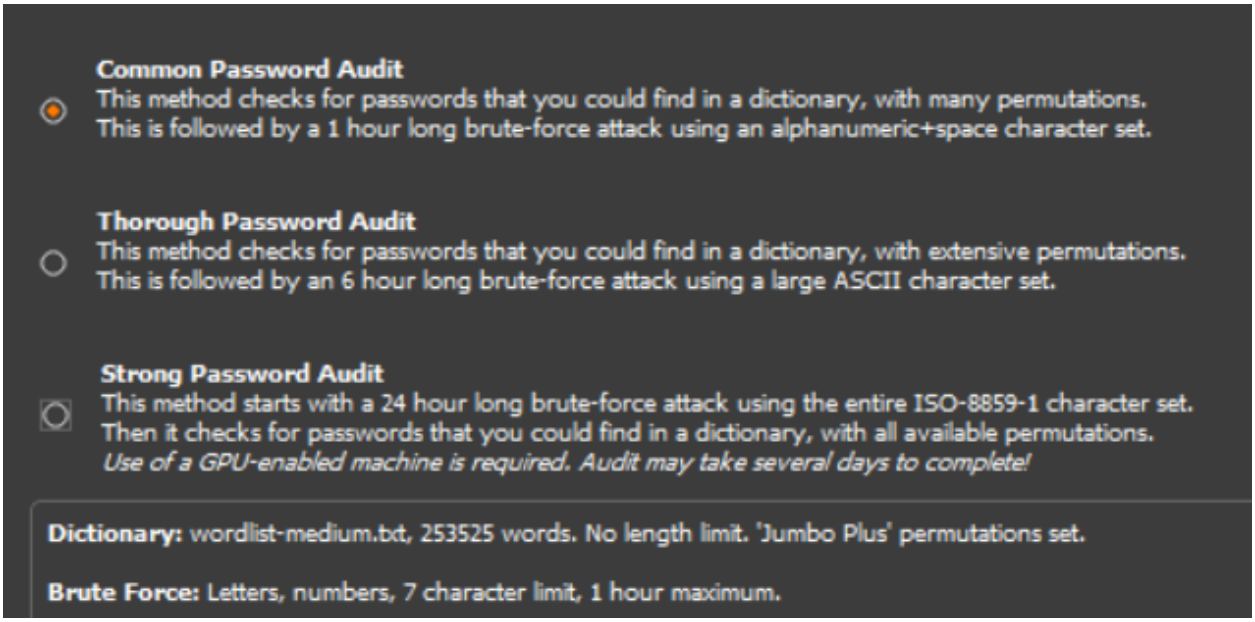
3. L0phtCrack

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 attack**s, 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.



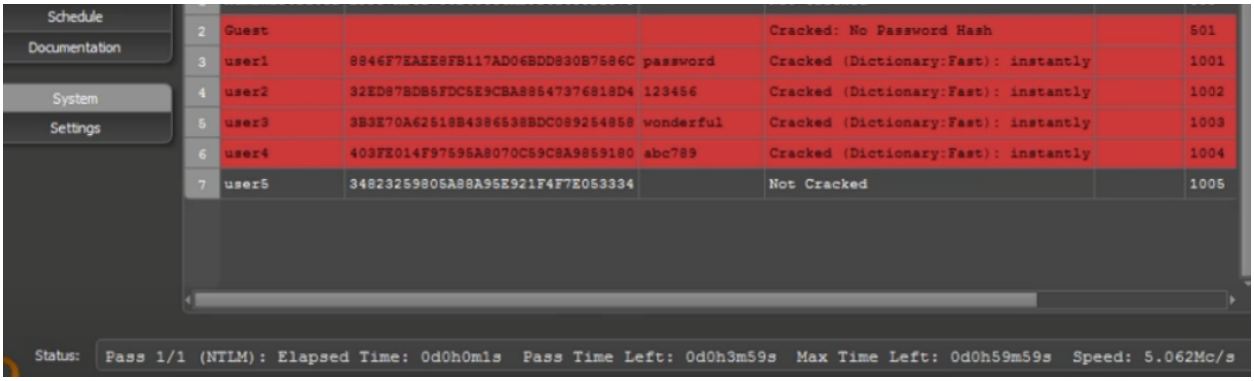
I used a **Common password Audit** which uses letters, and numbers in passwords (no special
characters). It has a maximum character limit of 7.



	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	0AC69E26E9BFD135DE1E9E4B5A8E60E0		Not Cracked		1001
5	WDAGUtilityAccount	DCAEA96E5D245E8A175D6A37DC543800		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.



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.