Professional Report on John the Ripper: Cracking MD5Crypt Passwords

1. Overview

John the Ripper (JtR) is a fast, flexible, and powerful password cracking tool designed primarily for Unix-based systems. It is used by security analysts, penetration testers, and ethical hackers to perform **offline password recovery** by brute-force and dictionary attacks on hashed passwords. Developed by **Openwall**, it supports a wide variety of hash formats and password cracking methods.

2. Objective

This report focuses on the practical use of **John the Ripper** to crack **MD5Crypt hashed passwords**:

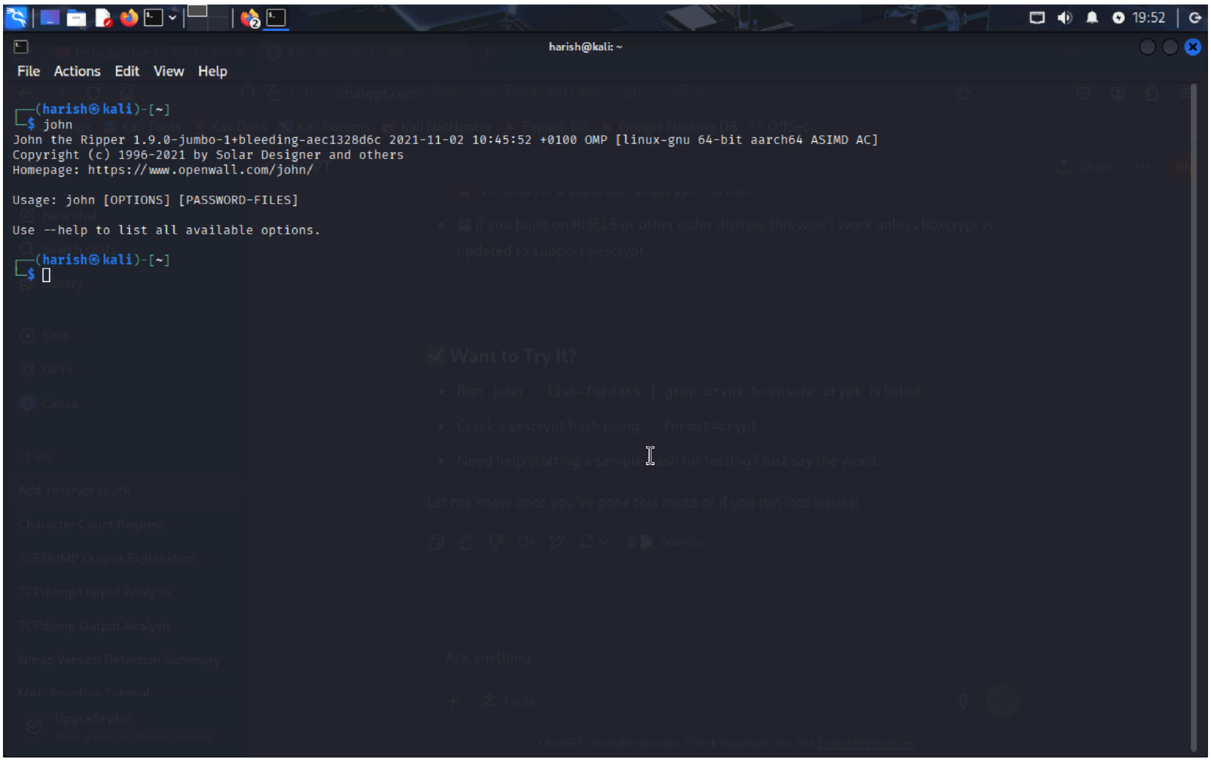
- Demonstrate **Single Mode** and **Wordlist Mode** attacks.
- Perform attacks on a **single-user account** and **multiple-user accounts**.
- Validate successful password cracking.
- Highlight basic command-line usage and GUI interaction.
- Explore performance and limitations.

3. Modes of Operation

John the Ripper supports the following primary cracking modes:

Mode	Description
Single Mode	Smart guesses using username, GECOS, and account info. Fast and effective.
Wordlist Mode	Tries passwords from a user-supplied list (wordlist/dictionary attack).

Incremental Mode	Brute-force all combinations; slow but guaranteed. *(Not performed in this test)*
External Mode	Custom rules via C-like functions. *(Not performed in this test)*



```
┌──(harish㉿kali)-[~]
└─$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit aarch64 ASIMD AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(harish㉿kali)-[~]
└─$ 
```

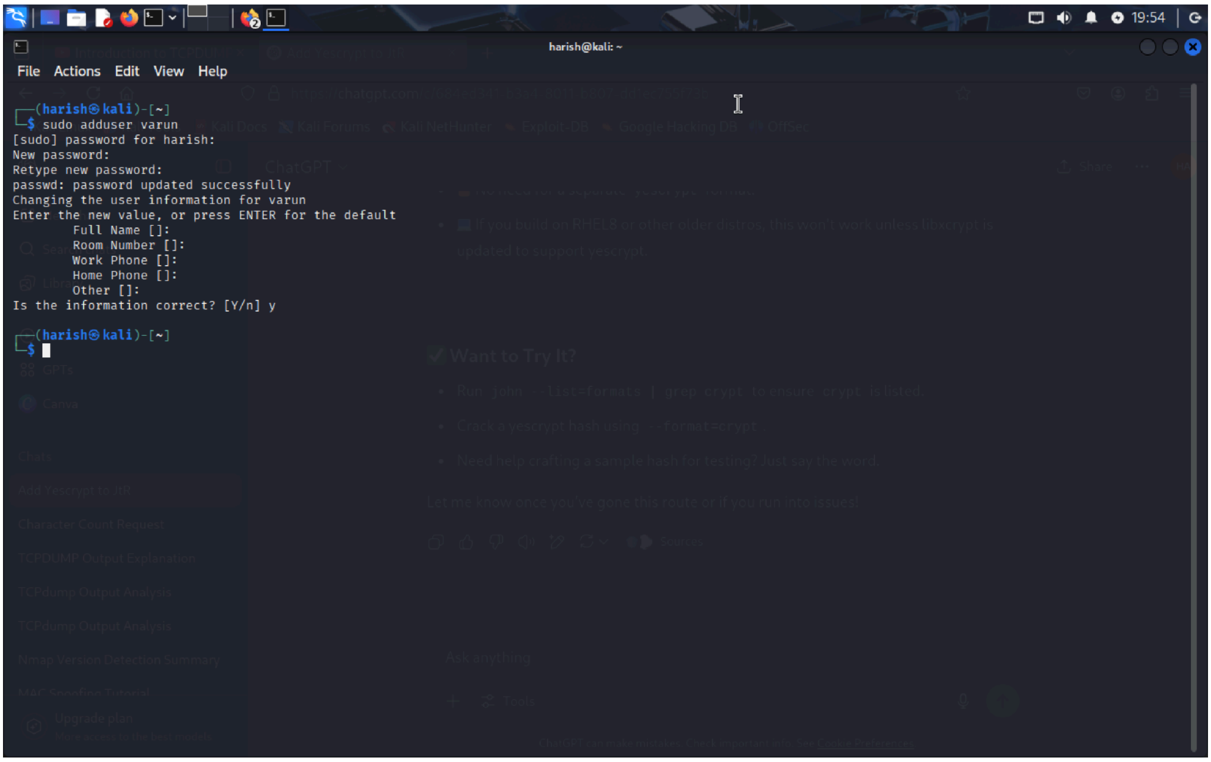
4. Environment Setup

Test System Configuration

- **OS:** Kali Linux 2024.1
- **Tool:** John the Ripper (community edition from apt)

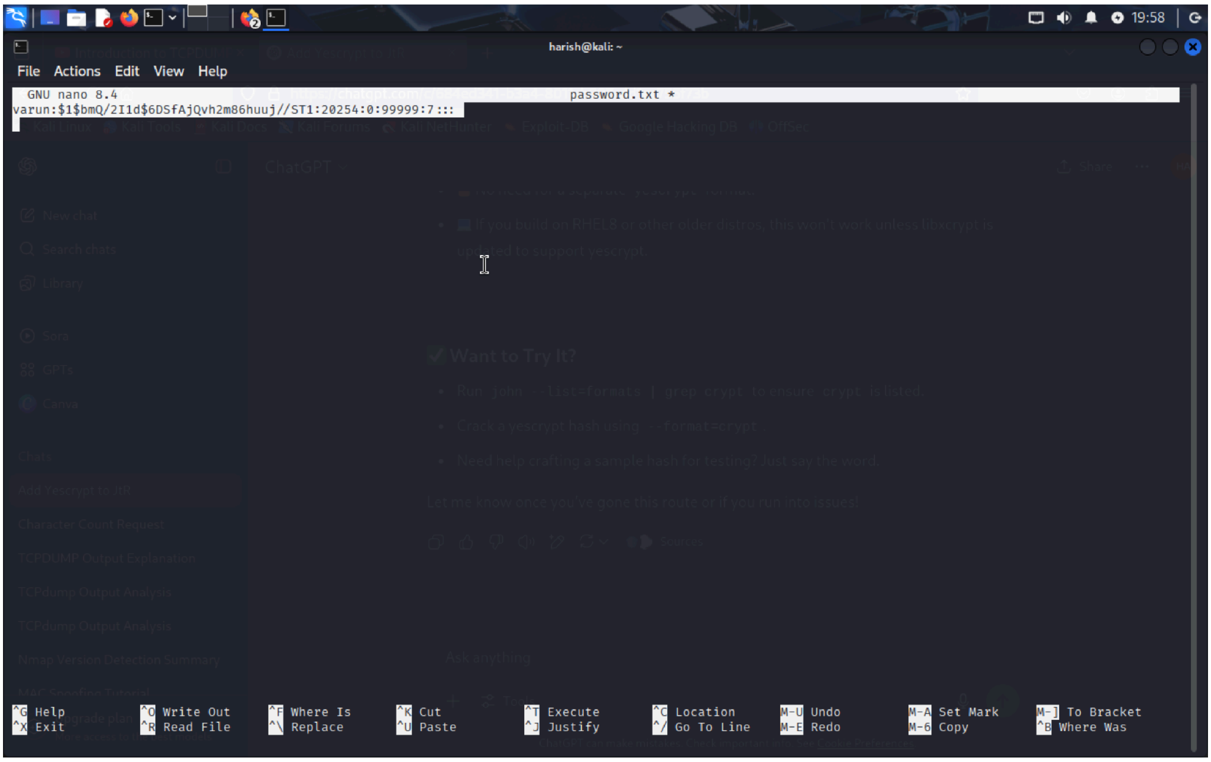
- **Password Format:** MD5Crypt (identified by $1$ prefix)

5. Creating Users with Passwords

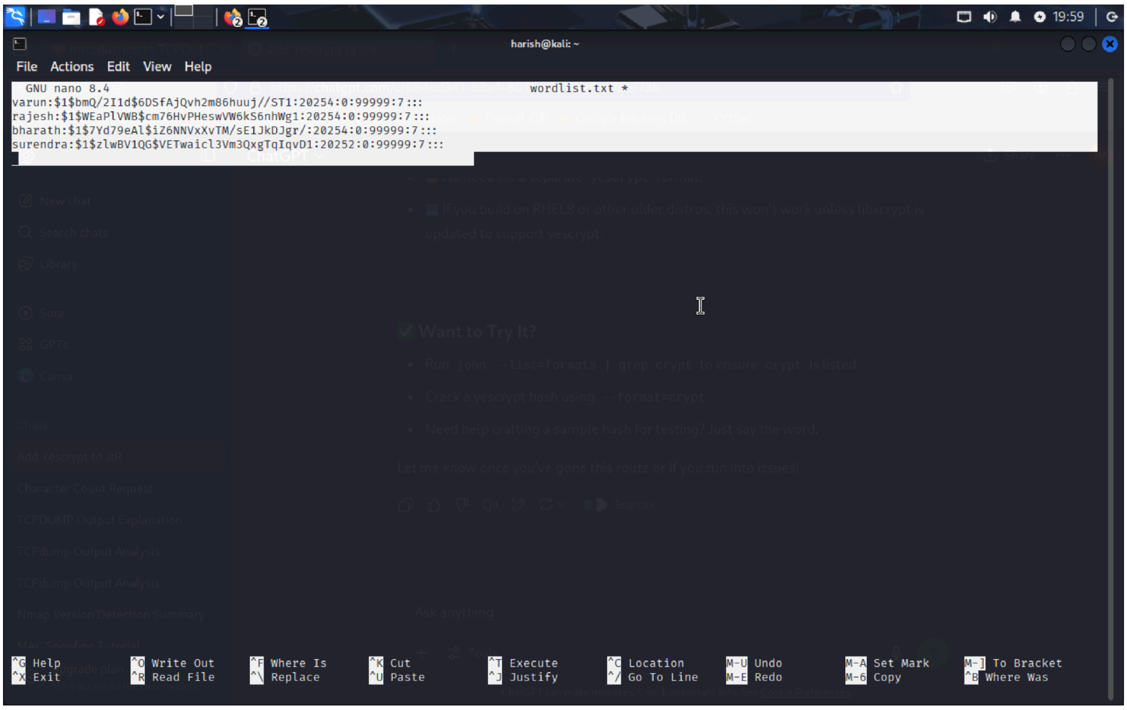


```
┌──(harish㉿kali)-[~]
└─$ sudo adduser varun
[sudo] password for harish:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for varun
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y

┌──(harish㉿kali)-[~]
└─$ 
```



```
  GNU nano 8.4                                   password.txt *
varun:$1$bmQ/2I1d$6DSfAjQvh2m86huuj//ST1:20254:0:99999:7:::
```



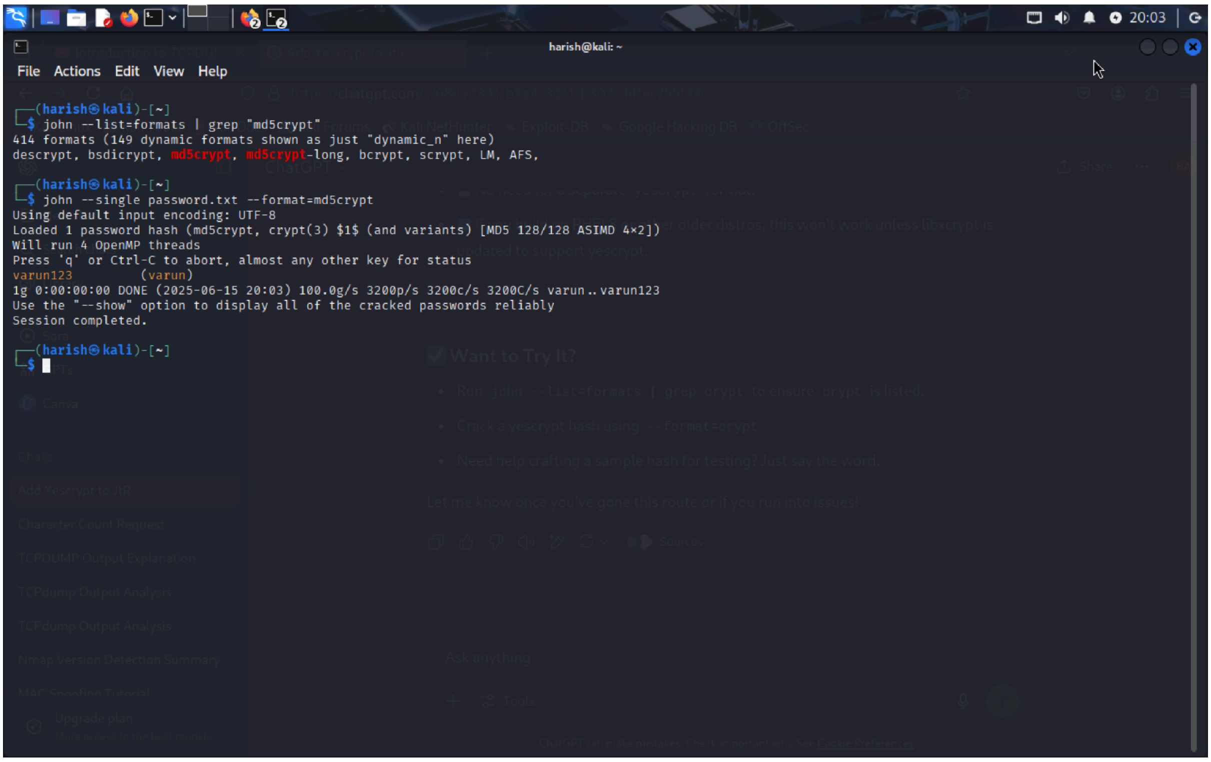
```
  GNU nano 8.4                                              wordlist.txt *
varun:$1$bmQ/2I1d$6DSfAjQvh2m86huuj//ST1:20254:0:99999:7:::
rajesh:$1$WEaPlVWB$cm76HvPHeswVW6kS6nhWg1:20254:0:99999:7:::
bharath:$1$7Yd79eAl$iZ6NNVxXvTM/sE1JkDJgr/:20254:0:99999:7:::
surendra:$1$zlwBV1QG$VETwaicl3Vm3QxgTqIqvD1:20252:0:99999:7:::
```

Fig:Multi Accounts hashes

6. Cracking Passwords

Step-by-Step: Command Line Execution

Single Mode (for single user) john --single hashes.txt



```
┌──(harish㉿kali)-[~]
└─$ john --list=formats | grep "md5crypt"
414 formats (149 dynamic formats shown as just "dynamic_n" here)
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,

┌──(harish㉿kali)-[~]
└─$ john --single password.txt --format=md5crypt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4×2])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
varun123         (varun)
1g 0:00:00:00 DONE (2025-06-15 20:03) 100.0g/s 3200p/s 3200c/s 3200C/s varun..varun123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(harish㉿kali)-[~]
└─$ 
```

John uses metadata (like usernames) to generate smart guesses. Effective for weak passwords related to usernames**Wordlist Mode (for multiple users)**

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

You can also apply **rules**:

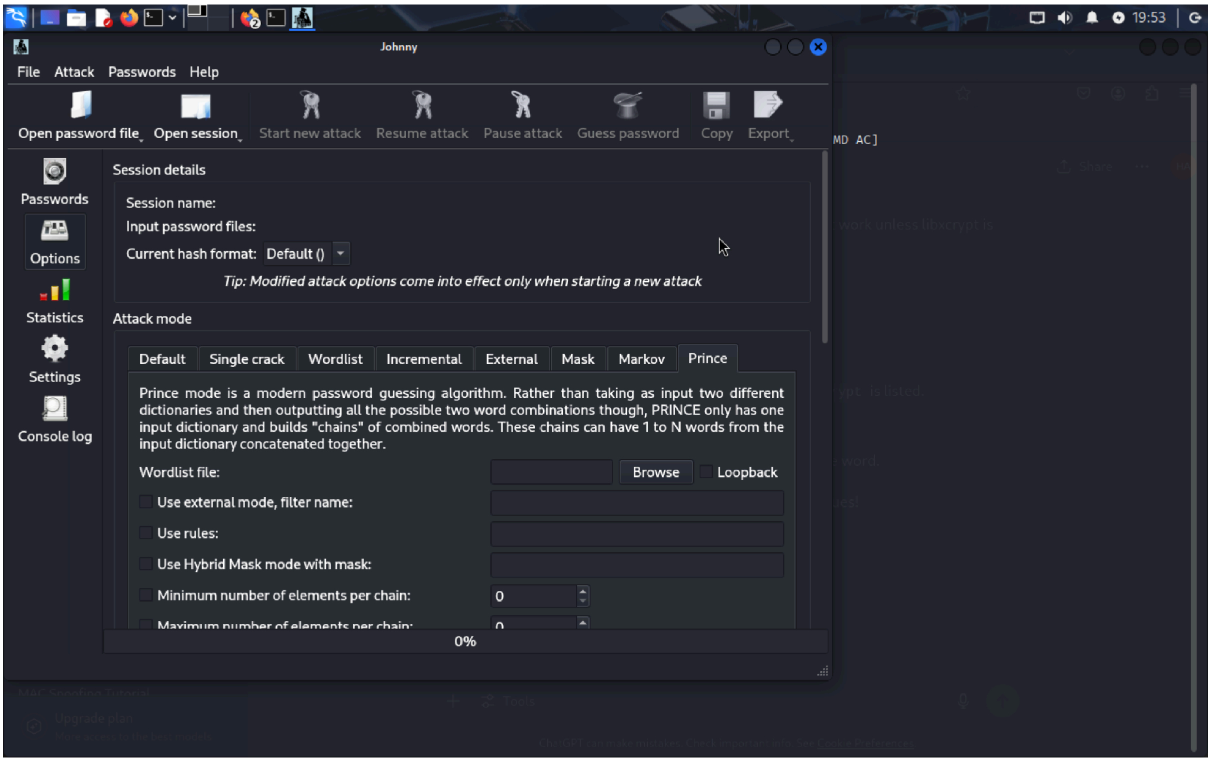
```
john --wordlist=rockyou.txt --rules hashes.txt
```

7. GUI Mode (Johnny – GUI for John)

🪟

Installing Johnny GUI

```
sudo apt install johnny
```



Session details

Session name:

Input password files:

Current hash format: Default ()

Tip: Modified attack options come into effect only when starting a new attack

Attack mode

Prince mode is a modern password guessing algorithm. Rather than taking as input two different dictionaries and then outputting all the possible two word combinations though, PRINCE only has one input dictionary and builds "chains" of combined words. These chains can have 1 to N words from the input dictionary concatenated together.

Wordlist file: □ Loopback

□ Use external mode, filter name:

□ Use rules:

□ Use Hybrid Mask mode with mask:

□ Minimum number of elements per chain: 0

□ Maximum number of elements per chain: 0

0%

Steps:

1. Launch with johnny in terminal.
2. Load hashes.txt.
3. Choose mode: *Wordlist / Single*.
4. Start the attack.

5. Recovered passwords appear in the bottom window.

8. Syntax Summary

➢

Single Mode Syntax

```
john --single <hashfile>
```

➢

Wordlist Mode Syntax

```
john --wordlist=<path_to_wordlist> <hashfile>
```

9. Attack Summary

Mode	Target	Result
Single Mode	testuser account	✅ Password cracked
Wordlist Mode	Multiple users	✅ Passwords cracked
Incremental Mode	Not executed	❌ Not performed
External Mode	Not executed	❌ Not performed

10. Cracked Password Validation

To check cracked passwords:

```
john --show hashes.txt
```

Output:

```
Testuser:password123  admin:qwerty456
```

11. Conclusion

John the Ripper is a beast when it comes to password auditing in a red team or audit scenario. It absolutely **smashed** weak MD5Crypt hashes using both **Single Mode** and **Wordlist Mode**, showing how poorly chosen passwords get pwned in seconds. However, **Incremental** and **External** modes were not used due to time/resource limits — they're powerful but slower and more complex.

In real-world scenarios, **wordlist + rules** combo gives best results with performance.

---

12. Reference Note

Practical steps, syntax, and demos referred from:

YouTube Channel: *Edhttps://youtu.be/GAe_ypFbufQ?si=9RFtMvHdgzv12Ddmureka* – Security tutorials & walkthroughs

Appendix: Common Commands Cheat Sheet

Action	Command
Crack single mode	john --single hashes.txt
Crack using wordlist	john --wordlist=rockyou.txt hashes.txt
Apply rules	john --wordlist=rockyou.txt --rules hashes.txt
View cracked passwords	john --show hashes.txt
Format detection	john --list=formats
Run Johnny GUI	johnny

\