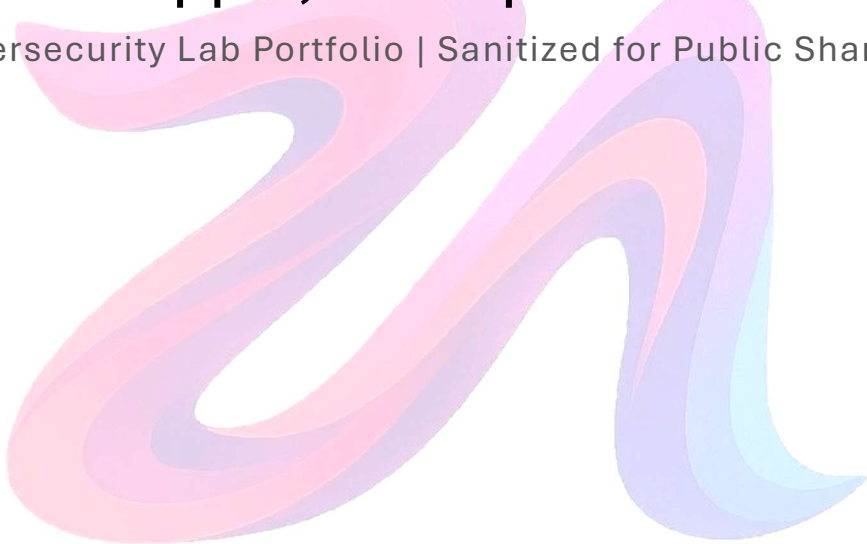


Password Cracking with Hashcat, John the Ripper, and Ophcrack

Cybersecurity Lab Portfolio | Sanitized for Public Sharing



Overview

This lab focused on ethical password cracking using industry-standard tools like Hashcat, John the Ripper, Ophcrack, and CrackStation. I targeted Windows NTLM and Linux SHA-512 hashes extracted from SYSTEM, SAM, and shadow files. Techniques included dictionary attacks, rainbow tables, and custom OSINT-based wordlists. This hands-on exercise reinforced my understanding of hash algorithms, cracking strategies, and the ethical considerations of using these tools in real-world security testing.

Tools Used

- Hashcat - GPU-accelerated cracking
- John the Ripper & Johnny GUI
- Ophcrack – Rainbow table cracking for NTLM
- CrackStation – Online has lookup
- CeWL – Custom wordlist generator
- Python (BeautifulSoup) – OSINT wordlist scraping
- Linux environment (Kali VM on VMWare Workstation)

Methods

- Extracted Windows NTLM hashes (SAM & SYSTEM files) and Linux SHA-512 hashes (shadow file).
- Verified and installed password-cracking tools (Hashcat, John, Ophcrack).
- Cracked NTLM hashes using Ophcrack with Vista rainbow tables and Crackstation.net.
- Used John the Ripper with rockyou.txt and SecLists wordlists for Linux SHA-512 hashes.
- Created custom wordlists using CeWL and Python BeautifulSoup scraping fandom wikis.
- Attempted advanced cracking with JTR Jumbo rules for mangling and OSINT-based lists.

Key Results

1. Cracking NTLM Password with Ophcrack

- Successfully cracked Dewey Crowe's Windows NTLM password: dewey!
- Technique: Rainbow tables (Vista free)\

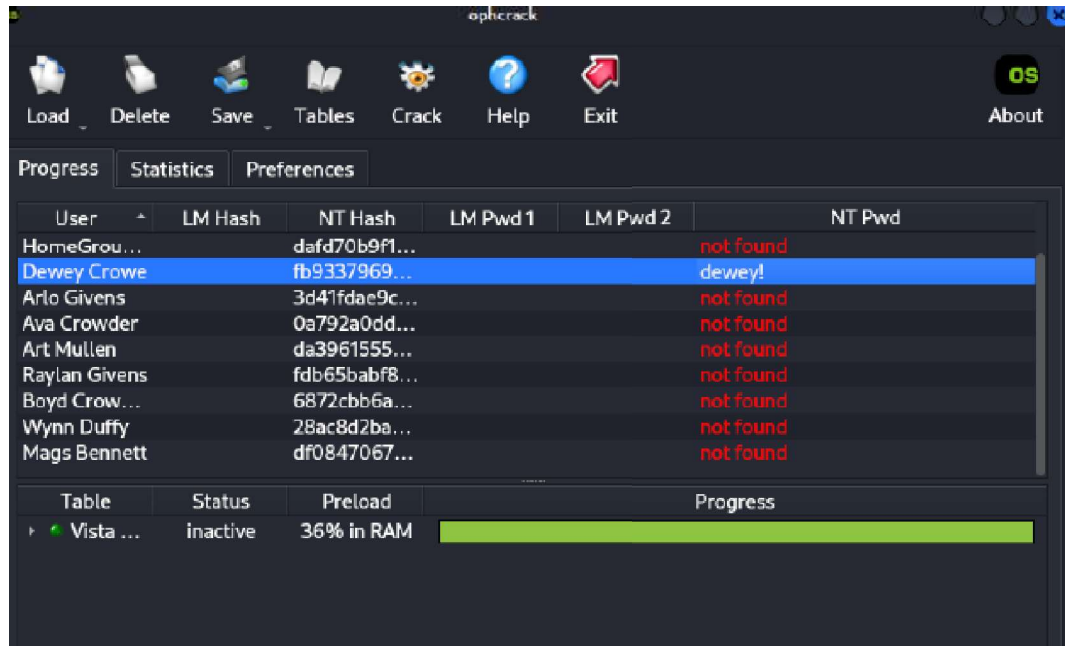


Figure 1 Ophcrack GUI showing cracked NTLM password. Usernames are part of lab environment and are not real accounts.

2. Cracking Linux SHA-512 Passwords with JTR

- Cracked two Linux passwords (Jahan and topiary) from shadow file using rockyou.txt.
- Command:
`john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt hashes.txt`

```

kali) [~/linux_hashes]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:11:37 6.83% (ETA: 04:59:48) 0g/s 1601p/s 12816c/s 12816C/s 131512..125603
0g 0:00:11:41 6.87% (ETA: 04:59:52) 0g/s 1600p/s 12816c/s 12816C/s 102030j..092961
0g 0:00:15:15 9.05% (ETA: 04:58:21) 0g/s 1586p/s 12696c/s 12696C/s nazininja..nature109
0g 0:00:15:17 9.07% (ETA: 04:58:20) 0g/s 1586p/s 12694c/s 12694C/s nasaa..nanook9
0g 0:00:15:20 9.09% (ETA: 04:58:24) 0g/s 1586p/s 12692c/s 12692C/s nadiab..nickle
0g 0:00:15:22 9.12% (ETA: 04:58:23) 0g/s 1585p/s 12691c/s 12691C/s mypassone1..mylife1995
0g 0:00:15:24 9.14% (ETA: 04:58:22) 0g/s 1585p/s 12690c/s 12690C/s myalize..muzaim
0g 0:00:15:25 9.14% (ETA: 04:58:26) 0g/s 1585p/s 12688c/s 12688C/s muzafarek1223..musabelliu0189
0g 0:00:15:26 9.16% (ETA: 04:58:22) 0g/s 1585p/s 12687c/s 12687C/s mummysboy1..muffi0
0g 0:00:15:28 9.18% (ETA: 04:58:22) 0g/s 1585p/s 12686c/s 12686C/s mrssprouse..mrbrownie45
0g 0:00:15:30 9.20% (ETA: 04:58:21) 0g/s 1585p/s 12684c/s 12684C/s mosnarak..morenita06
0g 0:00:15:52 9.41% (ETA: 04:58:29) 0g/s 1582p/s 12665c/s 12665C/s melinda1154..meisgay1
0g 0:00:15:53 9.42% (ETA: 04:58:26) 0g/s 1582p/s 12664c/s 12664C/s megan113..med1986
0g 0:00:15:55 9.44% (ETA: 04:58:26) 0g/s 1582p/s 12664c/s 12664C/s mckenziepickeral..mble1318
0g 0:00:21:13 12.82% (ETA: 04:55:18) 0g/s 1587p/s 12706c/s 12706C/s atimsa..astonpa
0g 0:00:21:15 12.84% (ETA: 04:55:18) 0g/s 1587p/s 12706c/s 12706C/s ashleyre..ash2112
Jahan (nandor)
1g 0:00:22:35 13.66% (ETA: 04:55:10) 0.000737g/s 1586p/s 12680c/s 12680C/s Chillen1..Callie9
1g 0:00:22:50 13.82% (ETA: 04:54:59) 0.000729g/s 1588p/s 12677c/s 12677C/s 948490..940122075503
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

```

Figure 2 John the Ripper cracking Linux SHA-512 hashes using rockyou.txt wordlist (sensitive details sanitized).

```

kali) [~/linux_hashes]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 7 password hashes with 7 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:40 0.42% (ETA: 05:13:18) 0g/s 1764p/s 12349c/s 12349C/s jordan28..280282
0g 0:00:00:44 0.46% (ETA: 05:13:07) 0g/s 1766p/s 12367c/s 12367C/s superm..jasons1
0g 0:00:19:35 13.92% (ETA: 04:53:37) 0g/s 1866p/s 13067c/s 13067C/s 842104..8321388
copyary (Lazlo)
1g 0:01:53:53 DONE (2025-04-12 04:26) 0.000146g/s 2098p/s 13050c/s 13050C/s !!!playboy!!!7..*7jVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

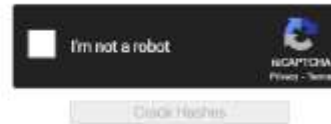
Figure 3 John the Ripper successfully cracking Linux SHA-512 hashes from a shadow file using the rockyou.txt wordlist with completion status (sensitive details sanitized).

3. Using CrackStation for Additional Matches

- Uploaded NTLM hashes to CrackStation.net, successfully cracked bad dad.
- All hashes and credentials shown are form a lab environment and do not represent real accounts.

Enter up to 20 non-salted hashes, one per line:

```
31d5c
31d66
da4d
fb93
3d41
8a79
da39
fdb6
6877
28ac
df08
```



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-haF, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL-4.1+ (sha1(sha1_bin)), jubev3.1BackupDefault

Hash	Type	Result
31d5cfe0d16ae931b73c59d7e0c089c0	NTLM	
31d5cfe0d16ae931b73c59d7e0c089c0	NTLM	
da4d78b9f13818154aab79fc6E60ed97	Unknown	Not found.
Fb937969addc609e155ff90277cd45f	NTLM	dewey!
3d41fd0e9c46f27defdb3b02ec84b7b	NTLM	bad dad
8a792e0dd4b28d356e26f487f2c90b12	Unknown	Not found.

Figure 4 CrackStation successfully resolving NTLM hashes from the lab, including “dewey!” and “bad dad”.

Discussion

This lab demonstrated the practical effectiveness of different cracking techniques, including rainbow tables for quick NTLM recovery and dictionary attacks for Linux hashes. It reinforced the value of password complexity and the role of OSINT in advanced cracking strategies. While custom wordlists and Jumbo rules didn't yield extra results, they laid the foundation for improving real-world cracking attempts. Challenges like VM storage constraints highlighted the importance of system prep in security labs.

Key Takeaways

- Cracked 4 passwords using Ophcrack, JTR, and CrackStation.
- Gained hands-on experience with rainbow tables, dictionary attacks, and custom wordlists.
- Learned ethical considerations and limitations of password-cracking tools.
- Reinforced Linux command-line proficiency and Python scripting basics for OSINT.