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)\

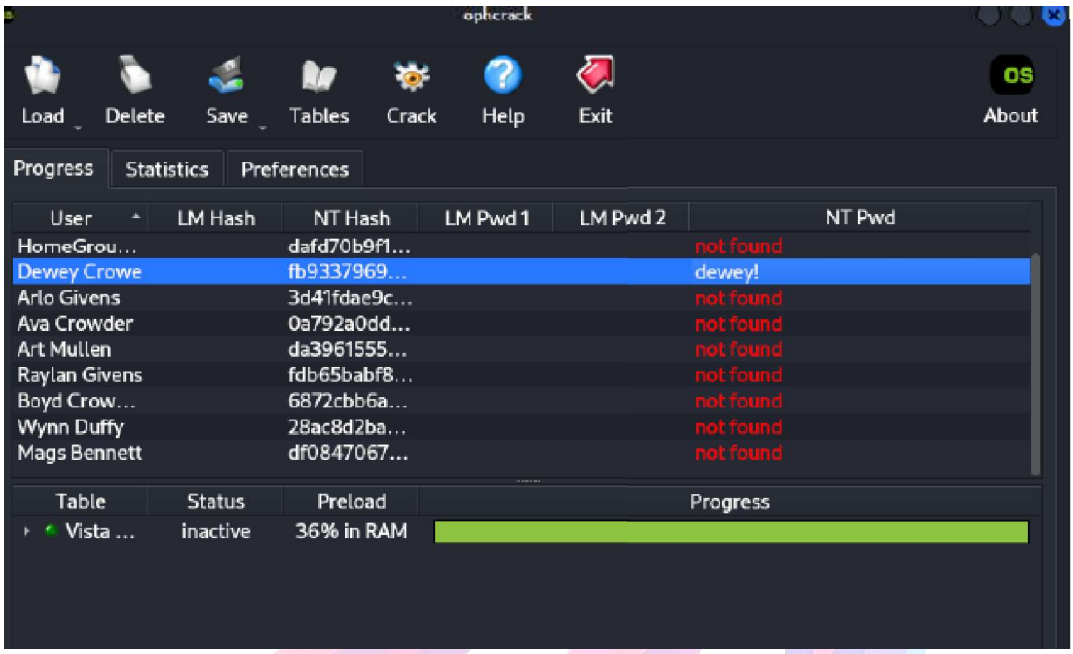

Figure 1 Ophcrack GUI showing cracked NTLM password. Usernames are part of lab environment and are not real accounts.

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

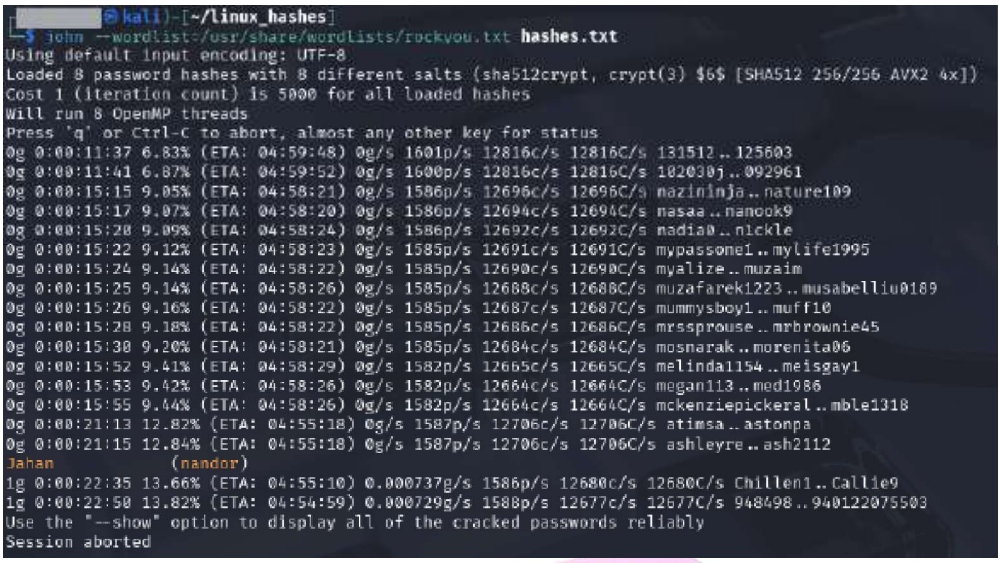

Figure 2 John the Ripper cracking Linux SHA-512 hashes using rockyou.txt wordlist (sensitive details sanitized).

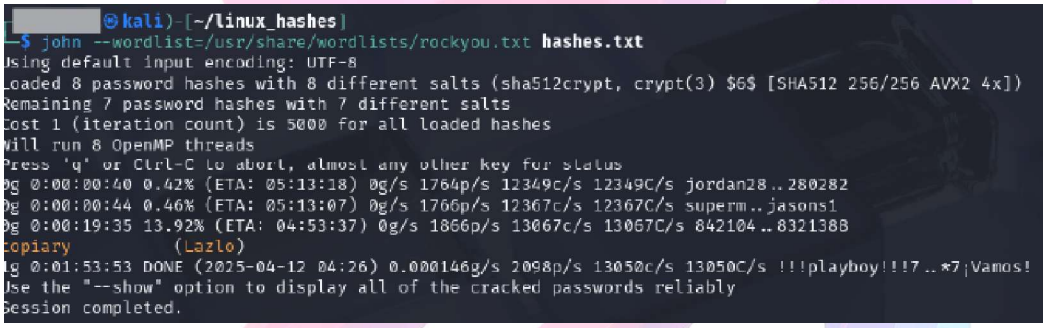

Figure 3 John the Ripper successfully cracking Linux SHA-512 hashes from a shadow file using the rockyou.txt wordlist with completion status (sensitive details sanitized).

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.

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.