Vinayak Mohan Bhujawadkar: (4020102) Abhishek Anil Nambiar: (4020125)

**EXPERIMENT NO. 7**

AIM: Perform the password audit on the Linux / Windows based system

Tools: Cain & Able, John the ripper, LCP Password Auditing tools for Windows. THEORY: Password auditing is a crucial security practice aimed at assessing the strength and integrity of passwords within an organization's or individual's digital environment. This process involves systematically examining password-related factors, such as complexity, length, and adherence to security policies. The primary objective is to identify vulnerabilities and potential weaknesses that could be exploited by malicious actors. Password auditing tools and techniques help pinpoint common or easily guessable passwords, as well as those exposed in data breaches. By conducting regular password audits, organizations can enforce stronger password policies, educate users on best practices, and enhance overall cybersecurity, reducing the risk of unauthorized access and data breaches.

This is not the only way John finds a password. You can also customize John based on your requirements. For example, you can specify the password format using the — — format flag.

In this article, we will first install John followed by a walkthrough of the different modes you can use. We will then use John to crack passwords for three different use cases — a Windows password, a Linux password, and a zip file password.

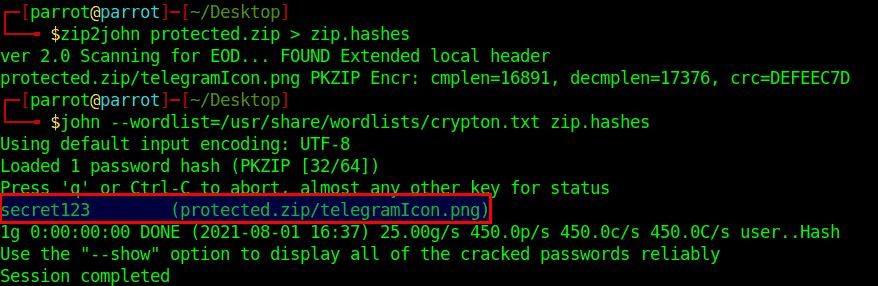


STEPS:

1. Generate hash of any password using online hashing tools.
2. Copy the hash into a .txt file.
3. Use this command to find the password:

zip2john protected.zip>zip.hashes

john –wordlist=/usr/share/wordlists/crypton.txt zip.hashes



CONCLUSION: Thus, we have successfully performed password auditing using JohnTheRipper