‹ Dashboard

Why Password Cracking?

Protecting confidential information is one of the biggest problems in the computer industry. Advancements in technology have created new ways of authenticating users and protecting systems against unauthorized access. However, for protecting passwords, password hashing (or salted hashing) is still the preferred way. Similarly, sensitive files are still encrypted with a password known to the user.

During pentesting or red teaming, it is very common to come across password hashes and protected files. It is, therefore, essential for a security professional to know the tools and techniques that can be used to crack these passwords.

Prerequisites

- Basic knowledge of computers
- Familiarity with the Linux Operating System

What will you learn?

In this section, you will learn to crack password hashes and recover passwords for encrypted files of different types (e.g. ZIP, PDF, MS Word) using Hashcat and John The Ripper (JTR). Each lab is supported by PDF and video solutions to help the students understand the approach.

Sub-sections/topics to be covered:

Basics (Hashes)

Password hashing is the process of passing a plaintext password to a one-way function (hash function) that generates a hexadecimal string of a fixed length called a password hash. This function is chosen in such a manner that getting a hash from a plaintext password is very efficient while recovering the plaintext password from the hash is very difficult. Hence, the name “one-way function”. Password hashing serves as the last defense against the attacker because, even after getting his hands on the username and password hashes, the attacker still has to recover the plaintext passwords in order to use the credentials. In these labs, various types of hashes are provided along with the Hashcat tool. The user has to crack the given hash and recover the plaintext password.

Basics (File Password)

Once the attacker has access to storage media like hard disks, USB drives and cloud storage, the files stored on that media become accessible to him. In order to put one more layer of defense in such cases, the sensitive files are encrypted. In most cases, a password known to the legitimate user/owner is used to derive a long key and this key is then used to encrypt the file. However, if the password used to protect the file is weak, it becomes susceptible to dictionary and mask/pattern-based attacks. In this section, different types of encrypted files are provided along with tools, Hashcat and John The Ripper (JTR). The user has to recover the passwords for these files.