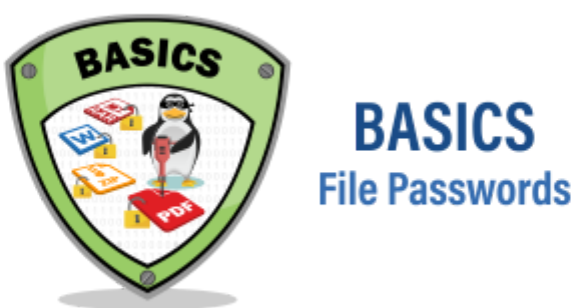

Once the attacker has access to storage media like hard disks, USB drives and cloud storage, the files stored on that media become accessible to him. In order to put one more layer of defense in such cases, the sensitive files are encrypted. In most cases, a password known to the legitimate user/owner 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.

What will you learn?

- Recovering passwords for different types of encrypted files using Hashcat and John The Ripper.

References:

1. Hashcat (https://hashcat.net/hashcat/)
2. John The Ripper (https://www.openwall.com/john/)

Labs Covered:

- Cracking RAR Archives
  Crack the password for an encrypted RAR archive by launching a dictionary attack using Hashcat or John The Ripper.

- Cracking PKZIP Archives
  Crack the password for an encrypted PKZIP archive by launching a dictionary attack using John The Ripper.

- Cracking 7z Archives
  Crack the password for an encrypted 7z archive by launching a mask-based brute-force attack using Hashcat or John The Ripper.

- Cracking SSH known_hosts File
  Use an open-source 3rd party python tool to convert the known_host entry into Hashcat compatible format and then recover the IP address stored in it using Hashcat.

- Cracking MS Word .docx
  Crack the password for an encrypted MS Word .docx file by launching a dictionary attack using Hashcat or John The Ripper.

- Cracking MS Word .doc
  Crack the password for an encrypted MS Word .doc file by launching a dictionary attack using Hashcat or John The Ripper.

- Cracking PDF (PDF 1.1-1.3)
  Crack the password for an encrypted PDF file by launching a dictionary attack using Hashcat or John The Ripper.

- Cracking PDF (PDF 1.4-1.6)
  Crack the password for an encrypted PDF file by launching a dictionary attack using Hashcat or John The Ripper.

- Cracking Private Key Passphrase
  Crack the password for an encrypted private key by launching a dictionary attack using John The Ripper.

Cracking PKZIP Archives

Start

Cracking 7z Archives

Start

Cracking SSH known_hosts File

Start

Cracking MS Word .docx

Start

Cracking MS Word .doc

Start

Cracking PDF (PDF 1.1-1.3)

Start

Cracking PDF (PDF 1.4-1.6)

Start

Cracking Private Key Passphrase

Start