**H5 September2023!**

**x) Read or watch and summarize**

**Schneier 2015: Applied Cryptography: 2.3 One-Way Functions**

A hash function in cryptography scrambles data to encrypt it, making it unreadable without specialized keys or difficult hacking techniques. They are used in pseudorandom generators, authentication of messages and digital signatures.

- Creating a one-way function is simple, but returning the computational function to its initial input is very hard.

- In terms of mathematics, there is no evidence to support either the existence or the formation of one-way functions

- We are unable to decrypt a message encrypted with one-way functions, hence they are useless. Utilize a different method for public key encryption.

- Trapdoor one-way is a one-way function that can be reversed using a secret formula. If you know the secret, that is.

**2.4 One-Way Hash Functions**.

- Numerous aliases include message digest, compression function, and contraction function.

- Compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and modification detection code (MDC) are other names for the one-way hash function. is crucial to contemporary cryptography and a foundational element for many protocols.

-In one-way hash function, Input = pre-image and output = hash value. Where it hard to guess the pre-image for a certain hash value.

- Message Authentication Code (MAC) and Data Authentication Code (DAC) are one-way function work with a secret key.

- It functions like a fingerprint by taking an input and producing a fixed-length output (hash value).

**Särökaari 2018:** **Phishing through email (video summary)**

**-** Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source.

- Phishing is an attempt to steal personal information or break in to online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already used.

- Attackers exploit curiosity to make receiver click on the link or attachment, which may include malicious attachments or forwards to malicious sites.

- Why people fall for phishing tricks as per research because they through that the sender is legitimate or message is an expectation thought the known sender.

- Using common email and name is a good technique in phishing.

**Protection**

- Sender Policy Framework (SPF) is an Email validation system, along with checking the sender IP is white listed IP or expected IP.

- Domain Keys Identified Mail (DKIM), an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain.

- Malware and spam filtering, which blocks or allows content across entire web domains based on DNS queries. DNS filtering takes more of a blunt hammer approach to blocking sites.

- URL whitelisting and web filtering tools, only known domains are allowed to send messages

- Greylisting is a method of defending e-mail users against spam.

**a) Install Hashcat**

By using below commands, I installed Hashcat on my machine.

sudo apt-get update

sudo apt-get -y install hashid hashcat wget

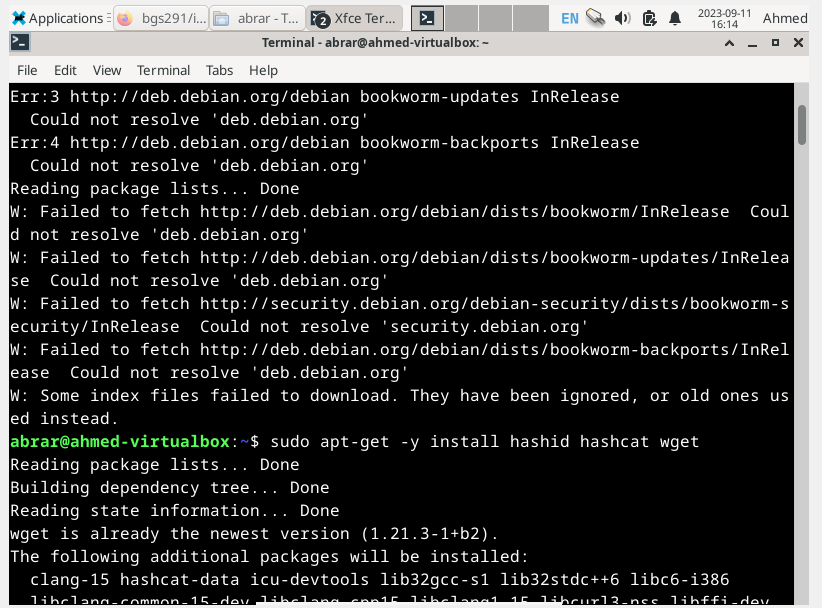
mkdir hashed

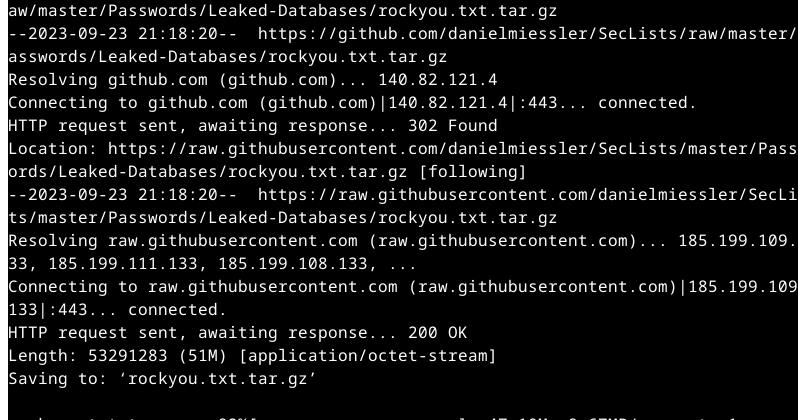
cd hashed

$ wget https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz

$ tar xf rockyou.txt.tar.gz

$ rm rockyou.txt.tar.gz

****



Installed. Done

**b) Crack this hash: 8eb8e307a6d649bc7fb51443a06a216f**

I got this error.

**c) Gone phising**