Cheatsheets / **Introduction To Ethical Hacking**

Evading & Computing

Cryptography

Cryptography is the process of encrypting and decrypting data in order to keep that data safe when storing or transmitting it.

- **Encryption** is a way of *hiding* data by converting it to an encoded format.
- **Decryption** is a way of *revealing* encrypted data by decoding it from its encoded format.

Symmetric Vs. Asymmetric Encryption

Ciphers can be symmetric or asymmetric.

- **Symmetric** encryption uses the *same* key to encrypt and decrypt information.
- **Asymmetric** encryption uses a *public* key to encrypt data and a different *private* key to decrypt data.

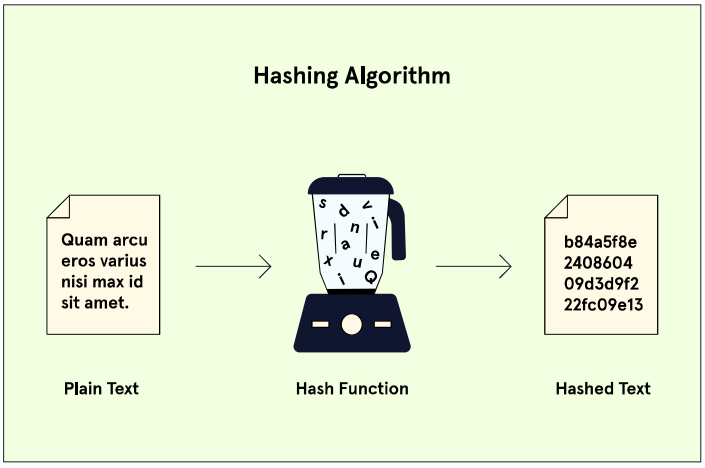
Asymmetric ciphers can be slower than symmetric ciphers but have additional use-cases in authentication and non-repudiation.

Hashing

Hashing is a *one-way process* that takes data of any size and represents it as a *unique* hash value of a fixed size. No matter how large or complex your file is, hashing provides a fast, reliable way to compare files and verify their authenticity.

Hashing lets you check if two pieces of information are the same, without knowing what the information itself actually is.

Hashing can be used to store sensitive data in a *secure* way.



Ephemeral Keys

Ephemeral keys are keys that are *discarded after being generated and used*.
This means that there is little benefit to an attacker who steals the key because the key quickly becomes useless!

Cryptography, Confidentiality, and Integrity

Cryptography is a powerful tool for maintaining both confidentiality and integrity. Powerful ciphers prevent unauthorized parties from accessing information without the appropriate key, while cryptographic hashing algorithms make it easy to see if information has been altered, maliciously or otherwise.

Cryptography Isn't Perfect

Given enough time, *any encryption can be broken using brute force*. The ciphers we use today are designed to take an extremely long time to be cracked, but computing power is always growing.
Design flaws can allow a cipher to be cracked much faster than would be possible using brute force alone.
Cryptography needs to be implemented and applied correctly to work. Strong ciphers are useless if the key is easily stolen, or the data they encrypt is stored in plaintext elsewhere.

Firewalls

Firewalls are hardware or software that filter network traffic, according to a set of rules. If you want to evade a firewall, you'll need to make your suspicious network traffic look like legitimate network traffic.

Intrusion Detection Systems

Intrusion Detection Systems are a type of hardware or software that monitors activity within a network, and looks for evidence of malicious or prohibited activity. In order to evade them, you need to avoid creating evidence that the IDS will flag as suspicious. This means not creating known Indicators of Compromise during your activity.

Honeypots

Honeypots are decoy computers/networks, designed to entice intruders and keep them distracted. Conducting careful reconnaissance before you act will help you avoid falling into honeypots.

How are Firewalls evaded

Firewalls are evaded by making your network traffic look legitimate.

how are IDSs are evaded

Intrusion Detection Systems (IDSs) are evaded by not creating known indicators of compromise during your activity.

How are honeypots evaded

Honeypots are evaded by taking your time and conducting good reconnaissance before acting.

Print Share