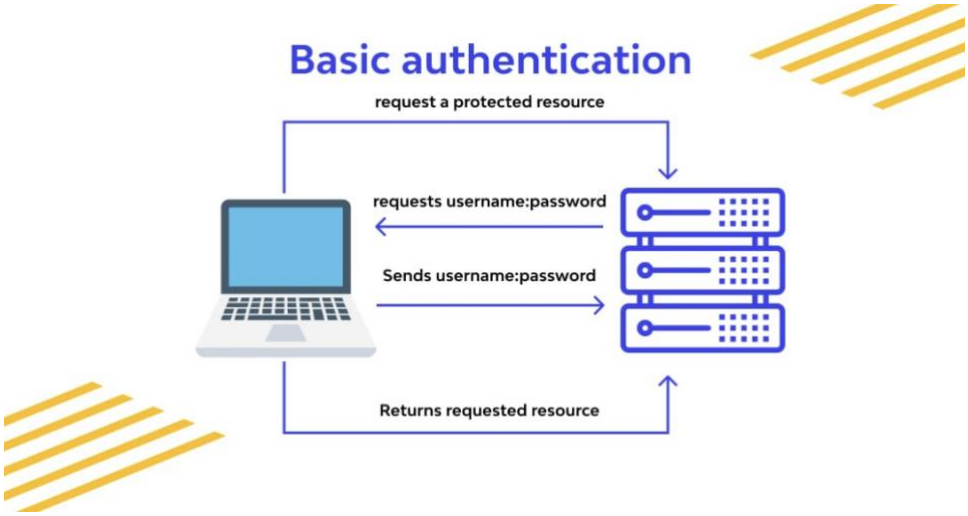
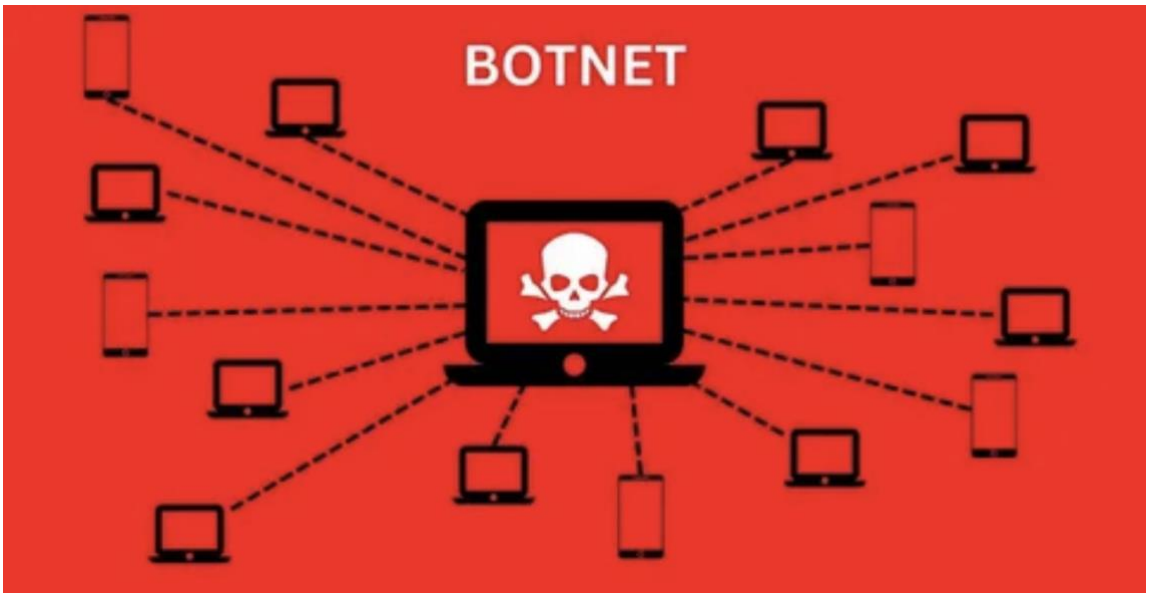
Authentication

This is one of the common cyber security terms. Authentication is the process of identifying someone's or something's identity, making sure that something is true, genuine, or valid. This can be carried out either by a PIN/password, retina scan, or biometric scan, sometimes even a combination of these things.



Botnet

A combination of the words “robot” and “network”, a botnet is a network of devices (computers, routers, etc.) that have been infected with a malicious code and can be operated continuously to create malicious security operations. These attacks can be of any type including click fraud, Bitcoin mining, sending spam e-mails, and Dos/DDoS attacks.



Data Breach

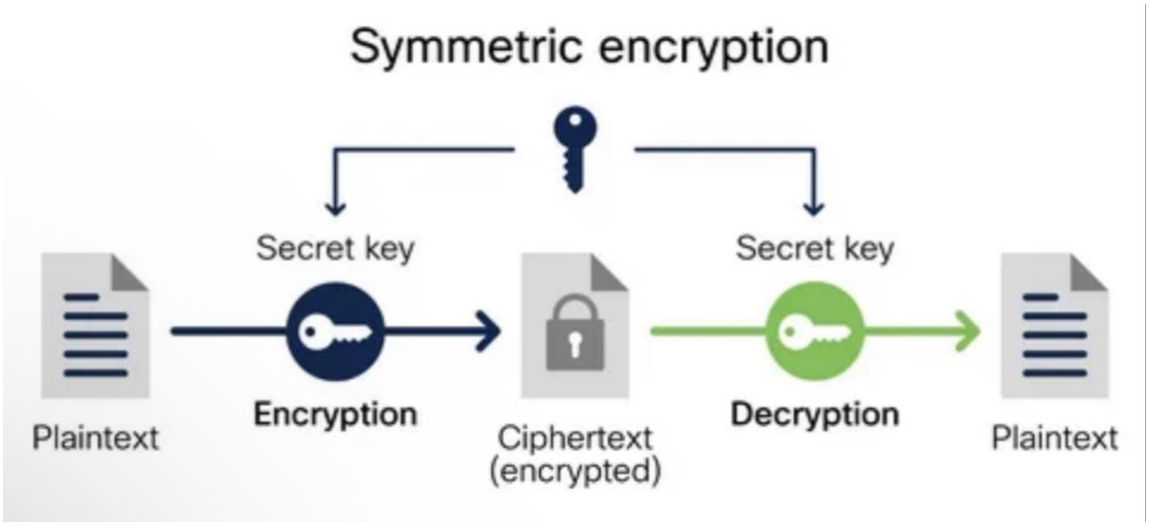
A data breach is one of the basic cybersecurity terms that is the result when a hacker successfully attacks the Business, government, and individual, gaining control of its network, system, server, or database and exposing its data, usually personal data such as Credit Card numbers, Bank Account numbers, Username passwords, Social Security numbers, and more.

DDoS

DDoS is short for Distributed Denial of Service, and this attack makes the availability disappear from the CIA triad. This malicious attack utilizes multiple sources to generate a lot of traffic to disrupt the normal traffic of a targeted service, server, or network. The overwhelming Internet traffic to the target or its surrounding infrastructure locks up the system and forces it to temporarily stay unavailable.

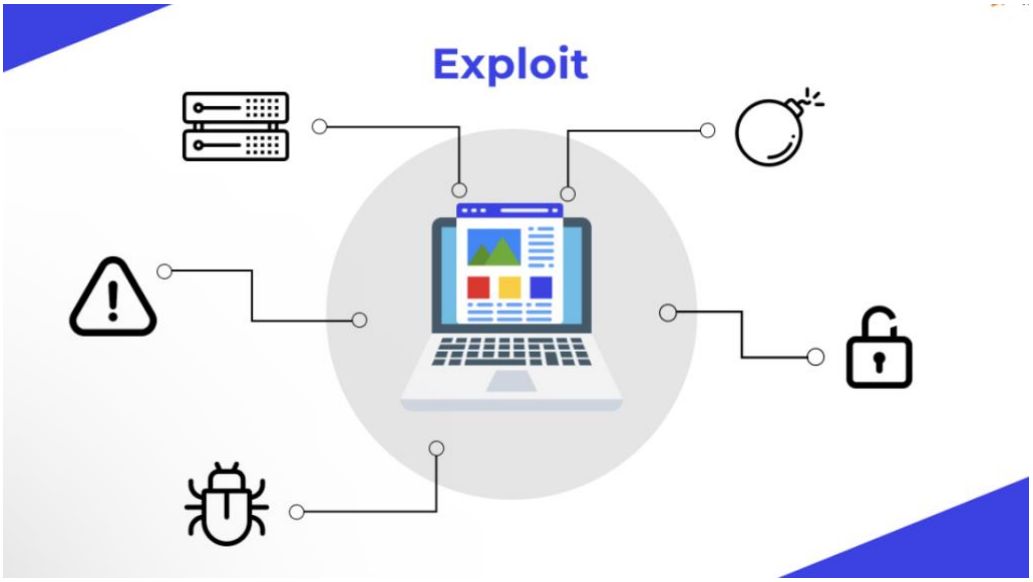
Encryption

Encryption is the technique by which any kind of information can be converted into a secret form that conceals the actual meaning of the information. It helps protect confidential information and sensitive & critical data and can improve the security of communication.



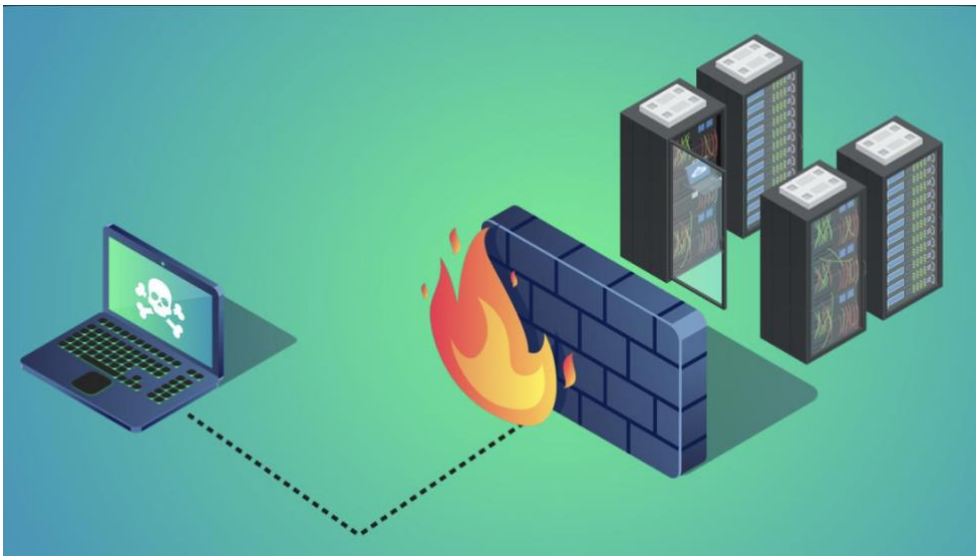
Exploit

An exploit is a code or program developed to find and take advantage of a security flaw or vulnerability in an application, network, or computer system, typically for malicious purposes such as installing malware.



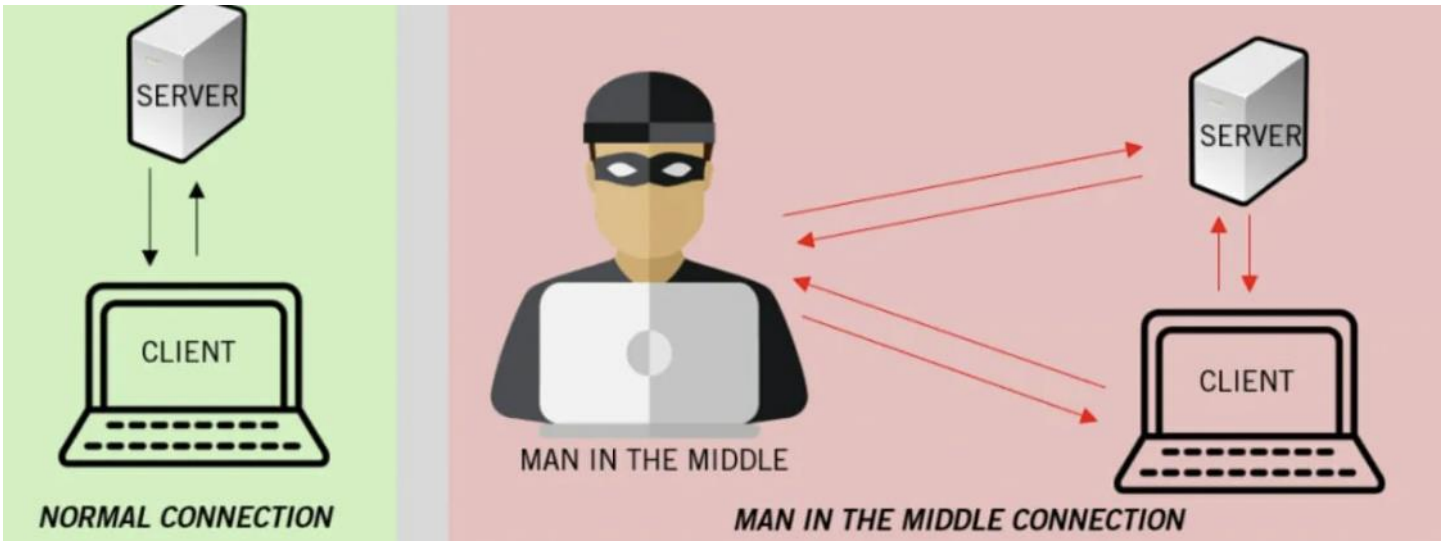
Firewall

Firewalls can be in the form of software or hardware, monitors, and filters inbound and outbound network traffic based on an organization's created security policies.



Man in the Middle Attack

A man in the middle (MITM) attack is a widespread term for when an adversary positions himself in a conversation happening between a user and an application or even between a computer and router and listens to all the data transmitted between them and in most cases, the adversary is also able to crack the encryption.



Phishing

Phishing is a sort of social engineering attack often used to steal user data, including login credentials and credit card numbers. It happens when an attacker, masquerading as a trusted entity, deceives a victim into clicking on an email, instant message, or text message.

The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

Trojan Horse

Yet another type of malware, this one is a misleading computer program that looks innocent but contains malicious code or program within that allows the bad actor to hack into your system via a backdoor, allowing them to compromise your computer.