Security Fundamnetals

CIA Triad: Confidentiality → only authorized users should be able to access data.
Integrity: Data should not be tampered/modified by unauthorized users (correct and authentic).
Availability: The network/systems should be accessible and operational to unauthorized users.
Vulnerability: any potential that can compromise the CIA of a system/info.
Exploit: something that can potentially be used (technique) to exploit the vulnerability.
Threat: a potential of a vulnerability (window) to be exploited (rock) (combined together to break into the house).
Mitigation Technique: something that can protect against threats, should be implemented everywhere a vulnerability can be exploited as switches, routers, hosts,…., can involve preventing unauthorized people from getting physical access to a device by keeping them on a secure rack behind a secure door,.. etc.

Denial of Service (DOS) attack: DoS attacks threaten the availability of a system as TCP SYN flood:
→ the attacker sends countless TCP SYN messages to the target, the target replies with a SYN ack that doesn't reach the attacker due to its spoofed IP address, the incomplete connections fill up the target's connection table leading to the target not being able to make legitimate TCP connections.
DDOS (Distributed DoS): the attacker infects as many target computers with malware and uses them all to initiate a DoS attack, the group of infected computers is called a botnet.
Spoofing: to use a fake source address (IP or MAC), involved in numerous attacks (not a single kind) as DHCP exhaustion: an attacker uses spoofed mac addresses to flood DHCP discover messages, the target server's DHCP pool becomes full, resulting in a DoS to other devices that won't be able to get an IP address.
(while offering an IP address in DHCP it's not assigned to other devices).
Reflection/Amplification attacks:the attacker sends traffic to a reflector and spoofs the src address of its packet using the target's IP, so the reflector sends replies to the target IP resulting in DoS, it becomes amplification when a small amount of traffic sent by the attacker triggers a large amount of traffic to be sent from the reflector to the target.
Man in the Middle: the attacker places himself between the src and dest to eavesdrop on communications or modify traffic before reaching dest as ARP spoofing/poisoning → the target sends a broadcast ARP request, the attacker sends an ARP reply after the legitimate replier so it overwrites the legitimate ARP entry, so any message sent to server will be forwarded to the attacker instead who can inspect/modify messages then forward them to the server.
Reconnaissance attacks: gathering publicly available information about a target for future attacks as nslookup to learn IP of a website or WHOIS query to learn emails, phone numbers, physical addresses,… etc.
Malware: Viruses → infect other software (a host program), can spread as the software is shared by users, typically corrupt or modify files on the target computer. Worms → don't require a host program, they are standalone and able to spread on their own without user interaction, can congest the network and their payload can cause additional harm to target devices. Trojan Horses: harmful software disguised as legitimate one, spread through user interaction as opening email attachments or downloading a file from the internet.
Social Engineering Attacks: target people by involving psychological manipulation to make the target reveal confidential information or perform some action as: Phishing → fraudulent emails appear to come from a legitimate business and containing links to a fraudulent website that seems legitimate , include spear phishing: a more targeted form aims at employees of a certain company, whaling: targeted at high-profile individuals as company president.
Vishing: Phishing over the phone. **Smishing**: Phishing using SMS text messages.
Watering hole: attacks compromise sites that the target victim frequently visits, placing a malicious link on a website that the target trusts.
Tailgating: entering restricted, secured areas by simply walking in behind an authorized personas hey enter.
Password related attacks: by guessing, Dictionary attack through running through a list/dictionary of common words/ passwords to find the targets password, Brute Force attack.
Strong passwords: at least 8 characters, a mixture of upper and lowercase letters, a mixture of letters and numbers, one or more special characters, changed regularly.

Multi Factor Authentication: something you know as a username/password combination, a PIN, something you have as a notification that appears on your phone through an authenticator app or a badge that is scanned, something you are as biometrics.

Digital certificate: to prove the identity of the certificate holder to verify that websites being accessed are legitimate. Entities send a CSR (Certificate Signing Request) to a certificate authority CA to generate and sign the certificate.

Authentication, Authorization and Accounting (AAA): a framework for controlling and monitoring users of a computer system as a network.
Authentication: verifying a user's identity. Authorization: granting the user the appropriator access and permissions.
Accounting: recording the user's activities on the system as logging.
ISE (Identity Services Engine): is Cisco AAA server.
RADIUS: an open standard protocol uses UDP ports 1812,1813.
TACACS+: a cisco proprietary uses TCP port 49.

Security Program Elements: User Awareness programs to make employees aware of potential security threats and risks.
User training programs: more formal, conducted for new employees and on intervals.
Physical access control: protects equipment and data from potential attackers by only allowing authorizes users into protected areas such as network closets or data centers, using multi factor locks.