Encryption
Example: When you send an email, the message is encrypted by your email provider using a key that is only known to you and the recipient. This implies that the message can only be read and decrypted by the intended recipient.

Exploit
Example: In 2017, a software vulnerability known as "Heartbleed" was discovered that could be exploited to steal data from websites. Attackers were able to read the memory of impacted servers through the Heartbleed exploit, which may have contained passwords and other sensitive data.

Enumeration
Example: To scan a network and find every device connected to it, an attacker could use a program such as Nmap.

Footprinting
Example: To find out information about a target organization, an attacker could use a tool like Shodan.

Flooding
Example: To overwhelm a server with SYN packets, an attacker could utilize a tool similar to SYNflood. SYN packets are the first part of a TCP connection handshake.

Firewall
Example: A firewall is a piece of software or hardware that can be configured to block unauthorized traffic from entering a network like CISCO ASA 5505

Fork Bomb
An example of a fork bomb is a piece of code that forks itself repeatedly, or makes many copies of itself.

Fuzzing
Example: To test a software program's ability to handle exceptions, fuzzers are tools that feed random input to it. Software vulnerabilities that an attacker could exploit can be found using fuzzing.

Hardening
Example: Closing unused ports, disabling unnecessary services, and installing security updates.

Hash Function
Example: SHA256, MD5, NTLM etc

Honey Pot

Example: Deploying a decoy server to mimic vulnerabilities and attract potential attackers for monitoring and analysis.

HIPAA
Example: Inorder to ensure HIPAA Compliance Implementing encryption and access controls to protect patient health information