Types of Attacks

- **Reconnaissance:** attacker gathers information about computer network to evade security controls.
- **Fuzzers:** the attacker attempts to uncover security loopholes in a program, operating system, or network by feeding it with massive random data entry to block it.
- **Analysis:** a type of intrusion that penetrates web applications through ports (for example, port scans), emails (for example, spam), and web scripts (for example, HTML files).
- **Backdoor:** a stealthy technique to avoid normal authentication to ensure unauthorized remote access to a device.
- **Exploit:** a sequence of instructions that exploits a flaw (vulnerability) caused by involuntary or unsuspected behavior on a host or network.
- **Generic:** a technique that attempts against block encryption using a hash function for collision regardless of encryption settings.
- **Shellcode:** attacker penetrates a small piece of code from shell to control the compromised machine.
- **Worm:** the attack replicates malicious script to spread it to other computers. Often, it uses a computer network to spread, depending on security flaws in the destination computer.
- **DoS:** an intrusion that disrupts computer resources, often through memory, to be extremely busy to prevent unauthorized requests from accessing a device.