•Birthday attack: Cryptographic attack that exploits the mathematics behind the birthday problem in the probability theory forces collisions within hashing functions.
•Brute force attacks: continually tries different inputs to achieve a predefined goal. Brute force is defined as “trying every possible combination until the correct one is identified".
•Buffer overflow: Too much data is put into the buffers that make up a stack. Common attack vector used by hackers to run malicious code on a target system.
•cross-site scripting: refers to an attack where a vulnerability is found on a web site that allows an attacker to inject malicious code into a web application
•Dictionary attacks: Files of thousands of words are compared to the user’s password until a match is found.
•DNS poisoning: Attacker makes a DNS server resolve a host name into an incorrect IP address
•Fraggle attack: A DDoS attack type on a computer that floods the target system with a large amount of UDP echo traffic to IP broadcast addresses.
•pharming: redirects a victim to a seemingly legitimate, yet fake, web site
•Phishing: type of social engineering with the goal of obtaining personal information, credentials, credit card number, or financial data. The attackers lure, or fish, for sensitive data through various different methods
•Ping of Death: A DoS attack type on a computer that involves sending malformed or oversized ICMP packets to a target.
•replay attack: a form of network attack in which a valid data transmission is maliciously or fraudulently repeated with the goal of obtaining unauthorized access.
•Replay Attack: an attacker capturing the traffic from a legitimate session and replaying it to authenticate his session
•session hijacking: If an attacker can correctly predict the TCP sequence numbers that two systems will use, then she can create packets containing those numbers and fool the receiving system into thinking that the packets are coming from the authorized sending system. She can then take over the TCP connection between the two systems.
•Side-channel attacks: Nonintrusive and are used to uncover sensitive information about how a component works, without trying to compromise any type of flaw or Weakness. A noninvasive attack is one in which the attacker watches how something works and how it reacts in different situations instead of trying to “invade” it with more intrusive measures. side-channel attacks are fault generation, differential power analysis, electromagnetic analysis, timing, and software attacks.
•Smurf attack: A DDoS attack type on a computer that floods the target system with spoofed broadcast ICMP packets.
•Social engineering: An attacker falsely convinces an individual that she has the necessary authorization to access specific resources.
•Spoofing at Logon: attacker can use a program that presents to the user a fake logon screen, which often tricks the user into attempting to log on
•SYN flood: DoS attack where an attacker sends a succession of SYN packets with the goal of overwhelming the victim system so that it is unresponsive to legitimate traffic.
•(TOC/TOU) attack: Attacker manipulates the “condition check” step and the “use” step within software to allow for unauthorized activity.
•War dialing: war dialer inserts long list of phone numbers into war dialing program in hopes of finding modem to gain unauthorized access.
•Wormhole attack: This takes place when an attacker captures packets at one location in the network and tunnels them to another location in the network for a second attacker to use against a target system.
•Denial-Of-Service (Dos) Attack: An attacker sends multiple service requests to the victim’s computer until they eventually overwhelm the system, causing it to freeze, reboot, and ultimately not be able to carry out regular tasks.
•Man-In-The-Middle Attack: An intruder injects herself into an ongoing dialog between two computers so she can intercept and read messages being passed back and forth. These attacks can be countered with digital signatures and mutual authentication techniques.
•Mail Bombing: This is an attack used to overwhelm mail servers and clients with unrequested e-mails. Using e-mail filteringand properly configuring e-mail relay functionality on mail servers can be used to protect against this type of DoS attack.
•Teardrop: This attack sends malformed fragmented packets to a victim. The victim’s system usually cannot reassemble the packets correctly and freezes as a result. Countersues to this attack are to patch the system and use ingress filtering to detect these packet types.