Common Attacks

Virus: A piece of malicious code that can take many forms and serve many purposes. Needs a host in which to live, and an action by the user to spread.

Worm: Similar to a virus, but does not need a host and is self replicating

Logic Bomb: A type of malicious code that lays dormant until a logical event occurs

Trojan Horse: One program (usually some type of malicious code) masquerades as another. Common means of distributing Back Door Programs

Back Door Programs: A Program that allows access (often administrative access) to a system that bypasses normal security controls. Examples are NetBus, Back Orifice, SubSeven

Salami: Many small attacks add up to equal a large attack

Data Diddling: Altering/Manipulating data, usually before entry

Sniffing: Capturing and Viewing packets through the use of a protocol analyzer. Best defense: Encryption

Session Hijacking: Where an attacker steps in between two hosts and either monitors the exchange, or often disconnects one. Session hijacks are types of Man in the Middle attacks. Encryption prevents sniffing and mutual authentication would prevent a session hijack

Wardialing: An attack on a RAS (Remote Access Server) where the attacker tries to find the phone number that accepts incoming calls. RAS should be set to use caller ID (can be spoofed), callback (best), and configured so that modem does not answer until after 4 calls.

Dos Denial of Service: The purpose of these attacks is to overwhelm a system and disrupt its availability

DDoS Distributed Denial of Service: Characterized by the use of Control Machines (Handlers) and Zombies (Bots) An attacker uploads software to the control machines, which in turn commandeer unsuspecting machines to perform an attack on the victim. The idea is that if one machine initiating a denial of service attack, then having many machines perform the attack is better.

Ping of Death: Sending a Ping Packet that violates the Maximum Transmission Unit (MTU) size—a very large ping packet.

Ping Flooding: Overwhelming a system with a multitude of pings.

Tear Drop: Sending Malformed packets which the Operating System does not know how to reassemble. Layer 3 attack

Buffer Overflow: Attacks that overwhelm a specific type of memory on a system—the buffers. Is best avoided with input validation

Bonk : Similar to the Teardrop attack. Manipulates how a PC reassembles a packet and allows it to accept a packet much too large.

Land Attack: Creates a “circular reference” on a machine. Sends a packet where source and destination are the same.

Syn Flood: Type of attack that exploits the three way handshake of TCP. Layer 4 attack. Stateful firewall is needed to prevent

Smurf: Uses an ICMP directed broadcast. Layer 3 attack. Block distributed broadcasts/ICMP on routers

Fraggle: Similar to Smurf, but uses UDP instead of ICMP. Layer 4 attack. Block distributed broadcasts on routers