Managing Incident Response



The *SYN flood attack* is a common DoS attack. It disrupts the standard three-way handshake used by TCP to initiate communication sessions.

Smurf and fraggle attacks are both DoS attacks. A smurf attack is another type of flood attack, but it floods the victim with Internet Control Message Protocol (ICMP) echo packets instead of with TCP SYN packets.

When standard security practices are used, smurf attacks are rarely a problem today. Fraggle attacks are similar to smurf attacks. However, instead of using ICMP, a fraggle attack uses UDP packets over UDP ports 7 and 19

**Botnets**

Botnets are quite common today. The computers in a botnet are like robots (often called zombies) and will do whatever attackers instruct them to do. A bot herder is typically a criminal who controls all the computers in the botnet via one or more command and control servers. Computers often join a botnet after being infected with some type of malicious code or malicious software.

A ping-of-death attack employs an oversized ping packet. Ping packets are normally 32 or 64 bytes, though different operating systems can use other sizes. The ping-of-death attack changed the size of ping packets to over 64 KB, which was bigger than many systems could handle. When a system received a ping packet larger than 64 KB, it resulted in a problem.

**Teardrop**

In a teardrop attack , an attacker fragments traffic in such a way that a system is unable to put data packets back together. Large packets are normally divided into smaller fragments when they’re sent over a network, and the receiving system then puts the packet fragments back together into their original state. However, a teardrop attack mangles these packets in such a way that the system cannot put them back together.

**Land Attacks**

A *land attack* occurs when the attacker sends spoofed SYN packets to a victim using the victim’s IP address as both the source and destination IP address. This tricks the system into constantly replying to itself and can cause it to freeze, crash, or reboot.

**War Dialing**

War dialing means using a modem to search for a system that accepts inbound connection attempts. A war dialer might be a typical computer with a modem attached and running war dialer software, or it can be a stand-alone device. In either case, war dialers systematically dial phone numbers and listen for computer carrier tones

**Sabotage**

Employee *sabotage* is a criminal act of destruction or disruption committed against an organization by an employee. It can become a risk if an employee is knowledgeable enough about the assets of an organization

**Espionage**

Espionage is the malicious act of gathering proprietary, secret, private, sensitive, or confidential information about an organization. Attackers often commit espionage with the intent of disclosing or selling the information to a competitor or other interested organization.

***Honeypots* are individual computers created as a trap for intruders. A *honeynet* is two or more networked honeypots used together to simulate a network**

Pseudo flaws are false vulnerabilities or apparent loopholes intentionally implanted in a system in an attempt to tempt attackers. They are often used on honeypot systems to emulate well-known operating system vulnerabilities

A padded cell system is similar to a honeypot, but it performs intrusion isolation using a different approach. When an IDS detects an intruder, that intruder is automatically transferred to a padded cell. The padded cell has the look and feel of an actual network, but the attacker is unable to perform any malicious activities or access any confidential data from within the padded cell.

The padded cell is a simulated environment that offers fake data to retain an intruder’s interest, similar to a honeypot. However, the IDS transfers the intruder into a padded cell without informing the intruder that the change has occurred.

**Whitelisting identifies a list of applications authorized to run on a system, and blacklisting identifies a list of applications that are not authorized to run on a system.**

**Egress Monitoring**

*Egress monitoring* refers to monitoring outgoing traffc to prevent data exfiltration, which is the unauthorized transfer of data outside the organization. Some common methods used to prevent data exfiltration are using data loss prevention techniques…