CTS2134
Introduction to Networking

Module 08:
Network Security

Denial of Service (DoS)

DoS (Denial of Service) attack impacts system availability by flooding the target system with traffic or by exploiting a system flaw. The goal is to make a service or device unavailable to respond to legitimate requests.

- A Distributed Denial of Service (DDoS) attack uses zombies (slave computers) to multiply the number of attacks directed at the target.
- A Distributed Reflective Denial of Service (DRDoS) uses an amplification network to increase the severity of the attack.

Smurf

A **Smurf** attack is a form of DRDoS attack that spoofs the source address in ICMP packets. The attack requires an attacker system, an amplification network, and a victim computer or network.

- Sends ICMP packets that spoof the source address of the target.

Many personal firewalls block all ICMP protocol messages in response to these attacks.

Virus

A virus is a program that attempts to damage a computer system and replicate itself to other computer systems.

- Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions.
- Often focuses on destruction or corruption of data.
- Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book.

Worm

A worm is a self-replicating program that uses the network to replicate itself to other systems.

- A worm can negatively impact network traffic just in the process of replicating itself
- Introduced into the system through a vulnerability in a system or a network.
- Infects one system and spreads to other systems on the network.
- Can install a backdoor in the infected computer, allowing an attacker to remotely access the system.

Man-in-the-middle

A man-in-the-middle attack is used to intercept information passing between two communication partners.

- Commonly used to steal online bank credentials, personal and business information.
- An attacker inserts himself in the communication flow between the client and server and the client is fooled into authenticating the attacker, while the attacker intercepts and/or modifies the data in transit.

Rogue access point

A rogue access point is an unauthorized access point added to a network that is configured to mimic a valid access point.

- An attacker with access to the wired network installs a wireless access point that provides a method for remotely accessing the network.
- The access point is configured to prompt for credentials, allowing the attacker to steal those credentials or connect to the valid wireless access point.

Social Engineering

Social engineering exploits human nature by convincing someone to reveal information or perform an activity. Relies on the attacker gaining or exploiting the trust of and individual.

Examples of social engineering include:

- *Dumpster diving*
- *Shoulder surfing*
- *Piggybacking*
- *Eavesdropping*
- *Masquerading*
- *Phishing (*uses e-mail and a spoofed Web site to gain sensitive information)

Hoax viruses are spoofed e-mails that ask for information or ask for tasks to be performed (such as delete a file or go to a Web site and enter sensitive information).

Countermeasures Facts

A **countermeasure** is an action or a control put into place that eliminates/reduces the effects of an attack.

•Apply patches and updates to systems, particularly updates related to security issues

•Implement strong physical security to control access to your facilities and your network.

•Specific countermeasures for various types of attacks

- Automated attacks
- Malware
- Man-in-the-middle attacks
- Social engineering

Firewall Facts

A **firewall** is a device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules (ACLs).

- A network-based firewall inspects traffic as it flows between networks.
- A host-based firewall inspects traffic received by a host
- Firewalls use filtering rules, sometimes called **access control lists** (ACLs), to identify allowed and blocked traffic.
- A common method of using firewalls is to identify various network **zones** (based on users or computers that have similar access needs).
    - A demilitarized zone (**DMZ**) is a buffer network that sits between the private network and an un-trusted network (such as the Internet).

Firewall Types

Packet filtering firewall (layer 3)

- Examines information in the IP packet header

Circuit-level proxy (layer 5)

- Makes decisions about which traffic to allow based on sessions.

Application level gateway (layer 7)

- Filters based on information contained in the data portion of a packet.
  - Proxy server (can shield or hide a private network)

Common Ports

The TCP/IP protocol stack uses **port numbers** (logical connections at the transport layer) to determine what protocol incoming traffic should be directed to.

Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN):

- Well known ports (0 to 1023): Assigned to common protocols and services.
- Registered ports (1024 to 49151): Assigned to specific services.
- Dynamic ports (49,152 to 65,535): Used by any service on an ad hoc basis. Ports are assigned when a session is established, and released when the session ends.

VPN Facts

A virtual private network (**VPN**) is a network that uses encryption to allow IP traffic to travel securely over a non-trusted TCP/IP network.

- VPNs work by using a **tunneling protocol** *(NNTP, L2TP, IPSec, or SSL)*
- VPNs establish a security association between the two tunnel endpoints

VPNs can be implemented in the following ways:

- **Host-to-host**: Two hosts establish a secure channel and communicate directly.
- **Site-to-site**: Routers on the edge of each site establish a VPN.
- **Remote access**: A server on the edge of a network is configured to accept VPN connections from individual hosts.

VPN Facts

PPTP (Point-to-Point Tunneling Protocol)

- Uses standard authentication protocols (CHAP or PAP)
- Supports TCP/IP only
- Uses Microsoft Point-to-Point Encryption
- Is supported by most operating systems and servers
- L2TP is making PPTP obsolete.

L2TP (Layer Two Tunneling Protocol)

- Can use certificates for authentication
- Uses IPSec for encryption (requires certificates)
- Supports multiple protocols (not just IP)
- Not supported by older operating systems

VPN Facts

IPSec (Internet Protocol Security) provides authentication and encryption, and can be used in conjunction with L2TP or by itself as a VPN solution.

IPSec includes two protocols that provide different features.

- Authentication Header (AH) provides authentication features. If you use only AH, data is *not encrypted.*
- Encapsulating Security Payload (ESP) provides data encryption.

IPSec uses either digital certificates or pre-shared keys

Secure Sockets Layer (SSL)

SSL is used to secure traffic generated by IP protocols such as HTTP, FTP, and e-mail. SSL can also be used as a VPN solution, typically in a remote access scenario.

- Authenticates the server to the client using public key cryptography and digital certificates.
- Encrypts the entire communication session.
- Uses port 443, a port that is often already opened in most firewalls.
- Implementations that use SSL for VPN tunneling include Microsoft's SSTP and Cisco‘s SSL VPN.