Lesson Proper for Week 7

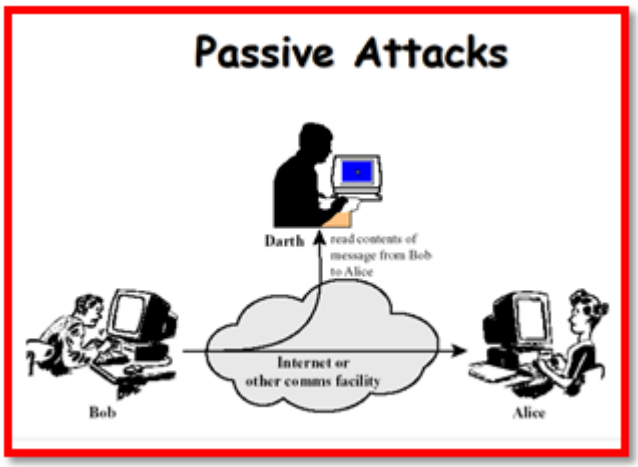
NETWORK ATTACKS AND NETWORK SECURITY THREATS

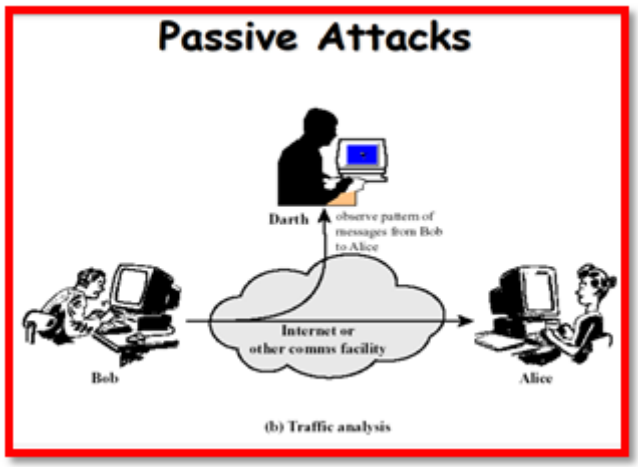
Network attack

An attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.

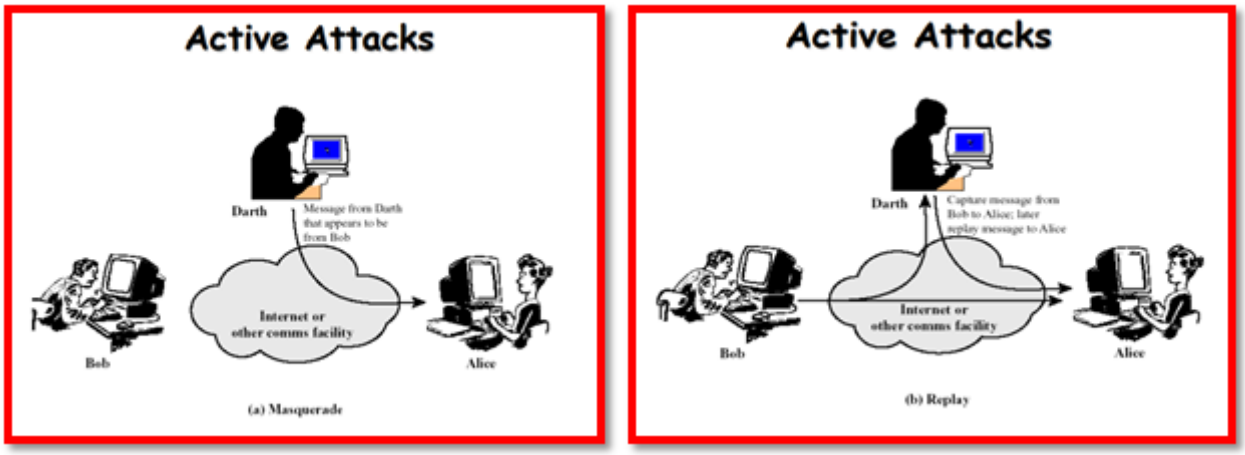
There are two main types of network attacks:

1. Passive: Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.





2. Active: Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.



Types of attacks if you do not have a security plan in place:

1. Eavesdropping:

Majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic.

When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

2. Data Modification:

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver.

3. Identity Spoofing (IP Address Spoofing):

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data.

4. Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password

5. Denial-of-Service Attack

Denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

o Send invalid data to applications or network services, which causes abnormal termination or behaviour of the applications or services.

o Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.

o Block traffic, which results in a loss of access to network resources by authorized users.

6. Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information.

We distinguish network attacks from several other types of attacks:

§ **Endpoint attacks**—gaining unauthorized access to user devices, servers or other endpoints, typically compromising them by infecting them with malware.

§ **Malware attacks**—infecting IT resources with malware, allowing attackers to compromise systems, steal data and do damage. These also include ransomware attacks.

§ **Vulnerabilities, exploits and attacks**—exploiting vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.

§ **Advanced persistent threats—**these are complex multilayered threats, which include network attacks but also other attack types.

Network Protection Best Practices

1. Segregate Your Network

A basic part of avoiding network security threats is dividing a network into zones based on security requirements. This can be done using subnets within the same network, or by creating Virtual Local Area Networks (VLANs), each of which behaves like a complete separate network. Segmentation limits the potential impact of an attack to one zone, and requires attackers to take special measures to penetrate and gain access to other network zones.

2. Regulate Access to the Internet via Proxy Server

Do not allow network users to access the Internet unchecked. Pass all requests through a transparent proxy, and use it to control and monitor user behavior. Ensure that outbound connections are actually performed by a human and not a bot or other automated mechanism. Whitelist domains to ensure corporate users can only access websites you have explicitly approved.

3. Place Security Devices Correctly

Place a firewall at every junction of network zones, not just at the network edge. If you can't deploy full-fledged firewalls everywhere, use the built-in firewall functionality of your switches and routers. Deploy anti-DDoS devices or cloud services at the network edge. Carefully consider where to place strategic devices like load balancers – if they are outside the Demilitarized Zone (DMZ), they won't be protected by your network security apparatus.

4. Use Network Address Translation

Network Address Translation (NAT) lets you translate internal IP addresses into addresses accessible on public networks. You can use it to connect multiple computers to the Internet using a single IP address. This provides an extra layer of security, because any inbound or outgoing traffic has to go through a NAT device, and there are fewer IP addresses which makes it difficult for attackers to understand which host they are connecting to.

5. Monitor Network Traffic

Ensure you have complete visibility of incoming, outgoing and internal network traffic, with the ability to automatically detect threats, and understand their context and impact. Combine data from different security tools to get a clear picture of what is happening on the network, recognizing that many attacks span multiple IT systems, user accounts and threat vectors.

6. Use Deception Technology

No network protection measures are 100% successful, and attackers will eventually succeed in penetrating your network. Recognize this and place deception technology in place, which creates decoys across your network, tempting attackers to "attack" them, and letting you observe their plans and techniques. You can use decoys to detect threats in all stages of the attack lifecycle: data files, credentials and network connections.

◄ Preliminary Activity for Week 7

Jump to...

Analysis, Application, and Exploration for Week 7 ►

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 1
Network Attacks: Detection, Analysis & Counter...
Participants
General
06 - Preliminary Examination
07 Network Attacks
Preliminary Activity for Week 7
Lesson Proper for Week 7
Analysis, Application, and Exploration for Week 7
Generalization for Week 7
Evaluation for Week 7
Assignment for Week 7
Ojt/Practicum 1
Social And Professional Issues
System Integration And Architecture 2
Courses

Fair Warning

Activities

- Assignments
- Forums
- Quizzes
- Resources