Attacks on Networks

- Threat actors place a high priority on targeting networks in their attacks
- Exploiting a single network vulnerability can expose hundreds or thousands of devices
- Attacks that target a network or a process that relies on a network include:
  - Interception attacks
  - Layer 2 attacks
  - DNS attacks
  - Distributed denial of service attacks
  - Malicious codding and scripting attacks

CENGAGE

Interception Attacks (1 of 5)

- **Man-in-the-Middle (MITM)**
  - In an MITM, a threat actor is positioned in a communication between two parties
  - The goal of an MITM attack is to eavesdrop on the conversation or impersonate one of the parties
- A typical MITM attack has two phases:
  - The first phase is intercepting the traffic
  - The second phase is to decrypt the transmissions

Interception Attacks (2 of 5)

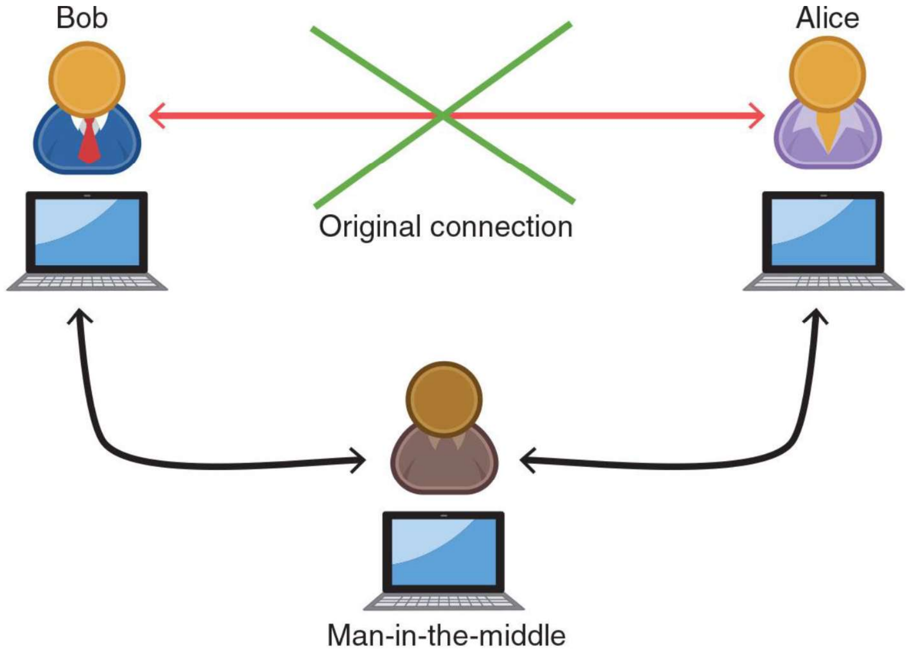


Figure 8-1 MITM attack

Figure 8-1 MITM attack

Interception Attacks (3 of 5)

- Session Replay
  - A *replay* attack makes a copy of a legitimate transmission before sending it to the recipient
  - Attacker uses the copy at a later time
  - Example: capturing logon credentials
- Threat actors use several techniques for stealing an active session ID:
  - Network attacks (hijacks and altered communication between two users)
  - Endpoint attacks (cross-site scripting, Trojans, and malicious JavaScript coding)

Interception Attacks (4 of 5)

- Man-in-the-Browser (MITB)
  - A **man-in-the-browser (MITB)** attack intercepts communication between parties to steal or manipulate the data
    - It occurs between a browser and the underlying computer
- A MITB attack usually begins with a Trojan infecting the computer and installing an “extension” into the browser configuration
  - When the browser is launched the extension is activated
  - Extension waits for a specific webpage in which a user enters information such as account number and password for a financial institution
  - When users click “Submit” the extension captures all the data from the fields on the form
    - May even modify some of the data

Interception Attacks (5 of 5)

- Man-in-the-Browser (MITB) (continued)
  - Advantages to a MITB attack:
    - Most MITB attacks are distributed through a Trojan browser extension making it difficult to recognize that malicious code has been installed
    - An infected MITB browser might remain dormant for months until triggered by the user visiting a targeted website
    - MITB software resides exclusively within the web browser, making it difficult for standard anti-malware software to detect it

Layer 2 Attacks (1 of 2)

- The OSI reference model separates networking steps into a series of seven *layers*
  - Within each layer, different networking tasks are performed that cooperate with the tasks in the layers immediately above and below it
- Layer 2, the Data Link Layer, is responsible for dividing the data into packets
  - A compromise at Layer 2 can affect the entire communication
- Address Resolution Protocol Poisoning
  - If the IP address for a device is known but the MAC address is not, the sending computer sends an **Address Resolution Protocol (ARP)** packet to determine the MAC address
  - MAC addresses are stored in an ARP cache for future reference
  - ARP poisoning
    - Relies upon MAC spoofing, which is imitating another computer by means of changing the MAC address

CENGAGE

Layer 2 Attacks (2 of 2)

- Media Access Control Attacks
  - Other attacks manipulate MAC addresses through spoofing
  - Two common attacks involving spoofing MAC addresses are MAC cloning and MAC flooding
  - In a **MAC cloning attack**, threat actors discover a valid MAC address of a device connected to a switch
    - They spoof the MAC address on and the switch changes its MAC address table to reflect the MAC address with the port to which the attacker’s device is connected
  - A **MAC flooding attack** is another attack based on spoofing, MAC cloning, and the MAC address table of a switch
    - A threat actor overflows the switch with Ethernet packets that have been spoofed so that every packet contains a different source MAC address

CENGAGE

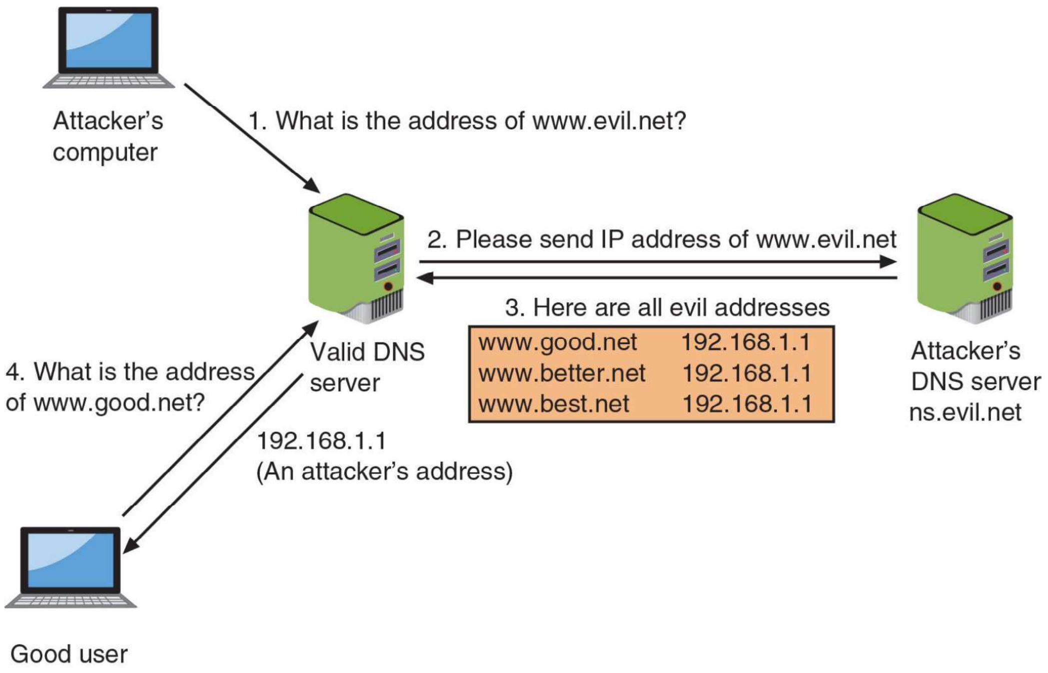
DNS Attacks (1 of 3)

- *Domain Name System (DNS)* is a hierarchical name system for matching computer names and IP addresses
  - A DNS-based attack substitutes a DNS address so that the computer is silently redirected to a different device
  - A successful DNS attack has two consequences:
    - *URL redirection*
    - *Domain reputation*
  - Attacks using DNS include DNS poisoning and DNS hijacking
- DNS Poisoning
  - **DNS poisoning** modifies a local lookup table on a device to point to a different domain
  - Two locations for DNS poisoning
    - Local host table
    - External DNS server

DNS Attacks (2 of 3)

- DNS Hijacking
  - **DNS hijacking** is intended to infect an external DNS server with IP addresses that point to malicious sites
  - DNS hijacking has the advantage of redirecting all users accessing the server
  - Attackers attempt to exploit a protocol flaw and convince the authentic DNS server to accept fraudulent DNS entries sent from the attackers' DNS server
  - If the DNS server does not correctly validate DNS responses to ensure they have come from an authoritative source, it stores the fraudulent entries locally and serves them to users
    - Spreading them to other DNS servers

DNS Attacks (3 of 3)


Attacker's computer
1. What is the address of www.evil.net?
2. Please send IP address of www.evil.net
3. Here are all evil addresses
Valid DNS server
Attacker's DNS server ns.evil.net
4. What is the address of www.good.net?
192.168.1.1 (An attacker's address)
Good user

www.good.net	192.168.1.1
www.better.net	192.168.1.1
www.best.net	192.168.1.1

Figure 8-5 DNS server poisoning

Figure 8-5 DNS server poisoning

Distributed Denial of Service Attack

- A *denial of service* (*DoS*) attack is a deliberate attempt to prevent authorized users from accessing a system by overwhelming it with requests
- Most DoS attacks today are **distributed denial of service (DDoS)**
  - Using hundreds or thousands of devices flooding the server with requests
- The devices participating in a DDoS attack are infected and controlled by threat actors so that users are completely unaware that their endpoints are part of a DDoS attack

CENGAGE

Malicious Coding and Scripting Attacks (1 of 3)

- Some network attacks come from malicious software code and scripts
- These attacks use PowerShell, Visual Basic for Applications, the coding language Python, and the Linux/UNIX Bash
- **PowerShell** is a task automation and configuration management framework from Microsoft
  - Administrative tasks are performed by cmdlets, which are specialized .NET classes that implement a specific operation
  - PowerShell allows attackers to inject code from the PowerShell environment into other processes without first storing any malicious code on the hard disk
    - Commands can then be executed while bypassing security protections and leave no evidence behind

Malicious Coding and Scripting Attacks (2 of 3)

- **Visual Basic for Applications (VBA)**
  - VBA is an event-driven Microsoft programming language
  - VBA is most often used to create macros, which are used to automate a complex task or a repeated series of tasks
  - Macros date back to late 1990s but continue to be a key attack vector
  - Due to the impact of macro malware, Microsoft has implemented several protections:
    - *Protected View*
    - *Trusted Documents*
    - *Trusted Location*

Malicious Coding and Scripting Attacks (3 of 3)

- Python
  - **Python** is a popular programming language that can run on several OS platforms
  - There are several best practices to follow when using Python so that the code does not contain vulnerabilities:
    - Use the latest version of Python
    - Stay current on vulnerabilities within Python
    - Be care when formatting strings in Python
    - Download only vetted Python libraries
- Bash
  - **Bash** is the command language interpreter for the Linux/UNIX OS
  - *Bash scripting* is using Bash to create a script
  - Exploits have taken advantage of vulnerabilities in Bash

Knowledge Check Activity 1

In which type of attack is the threat actor positioned between two parties and alters the transmission to eavesdrop or impersonate one of the parties?

a. MITB

b. MAC cloning

c. MITM

d. Session replay

Knowledge Check Activity 1: Answer

In which type of attack is the threat actor positioned between two parties and alters the transmission to eavesdrop or impersonate one of the parties?

Answer: c. MITM

In a man-in-the-middle (MITM) attack, a threat actor is positioned between two parties with the goal of eavesdropping or impersonating a party. In an MITM attack, the transmission is altered whereas in a session replay attack, a copy is made of a legitimate transmission for the purpose of replaying it later.