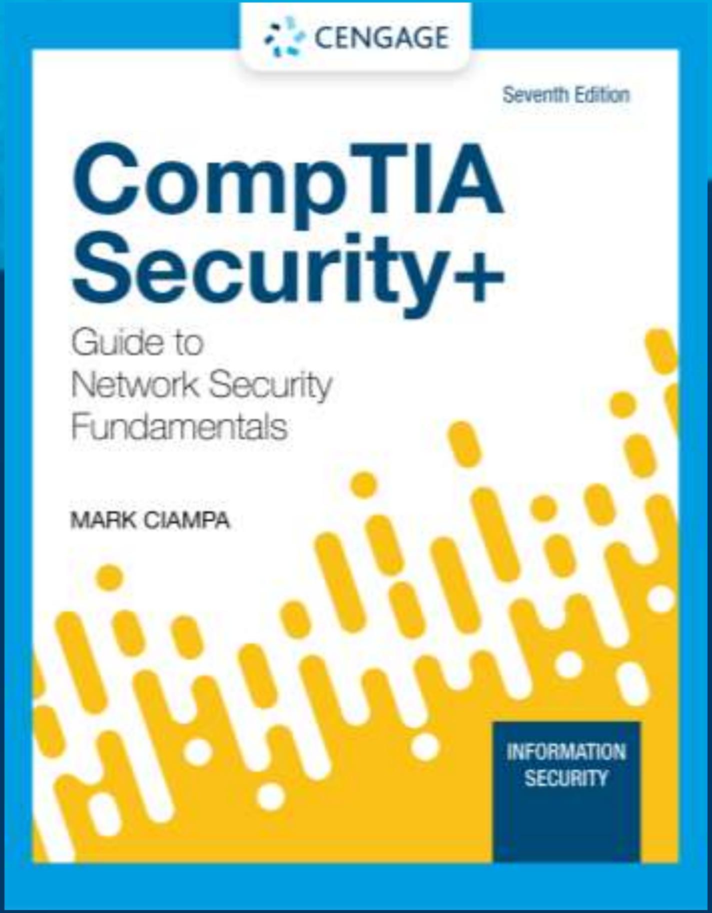


CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 8: Networking Threats, Assessments, and Defenses

Module Objectives

By the end of this module, you should be able to:

1. Describe the different types of networking-based attacks

2. List the different network assessment tools

3. Explain how physical security defenses can be used

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

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)

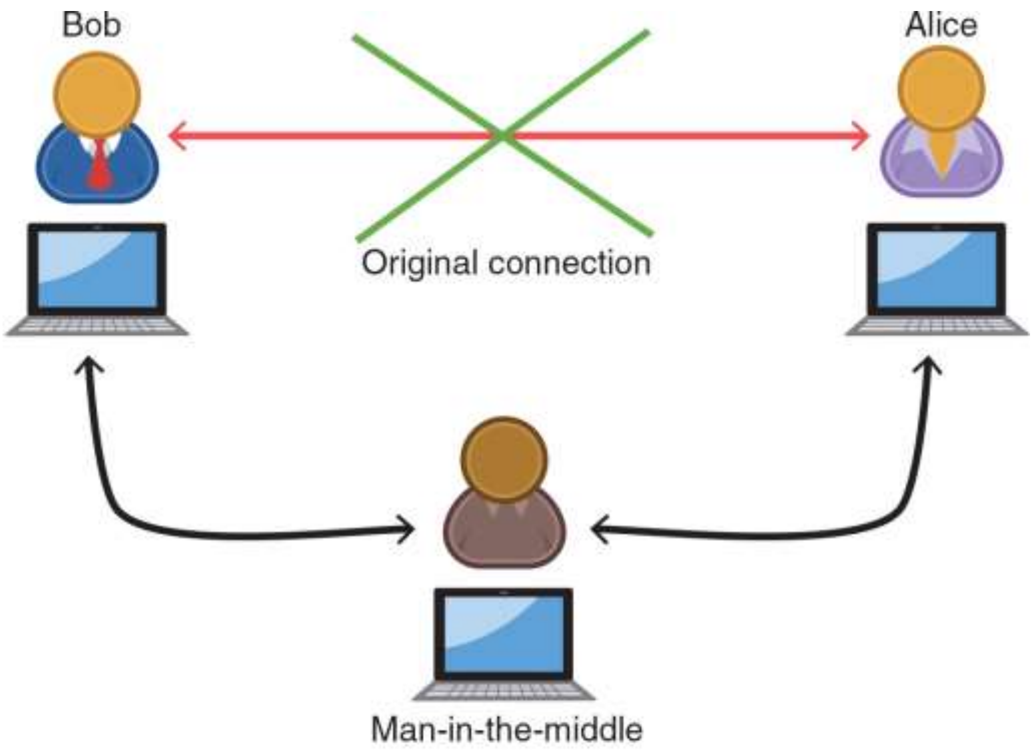


Figure 8-1 MITM attack

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

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

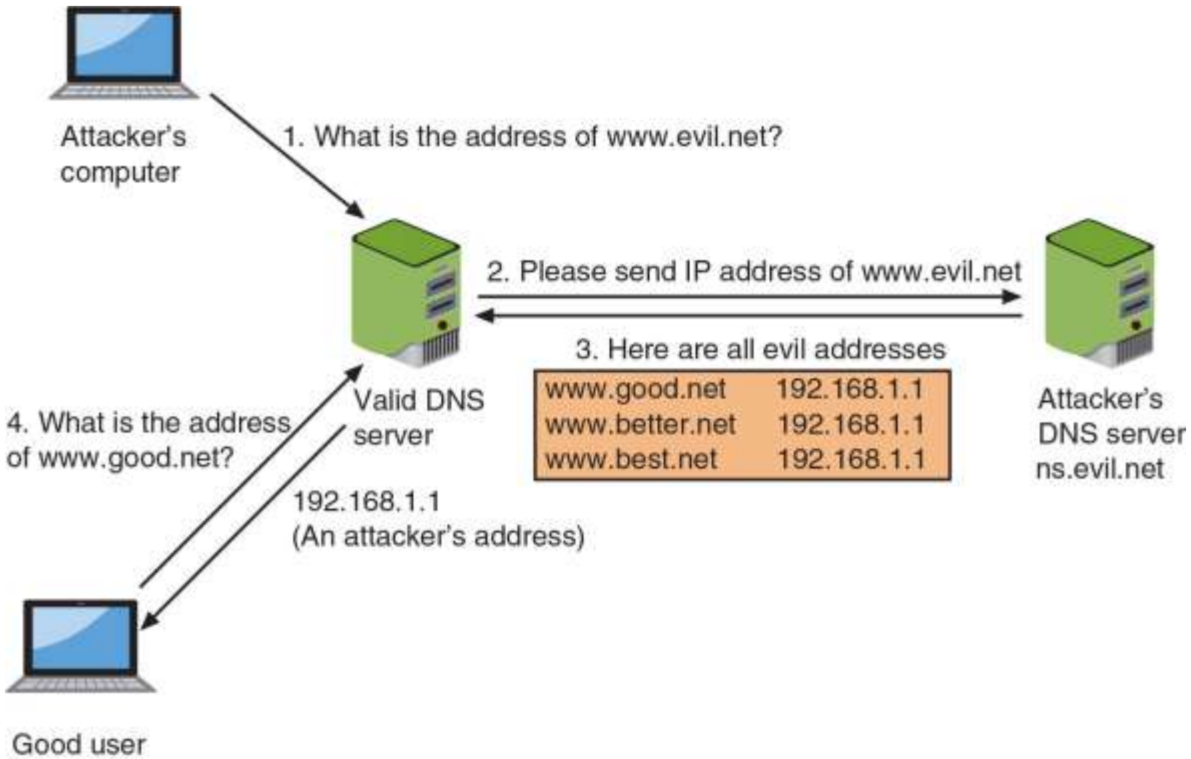
DNS Attacks (1 of 3)

- *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

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.

Tools for Assessment and Defense

- Several assessment tools determine the strength of a network
- Other tools can be used to create a stronger network defense
- Both types of tools can be categorized into network reconnaissance and discovery tools, Linux file manipulation tools, and packet capture and replay tools

Network Reconnaissance and Discovery Tools

Name	Source	Description
theHarvester	Kali Linux	Provides information about email accounts, user names, and hostnames/subdomains from different public sources
dnsenum	Kali Linux	List DNS information of a domain
sn1per	XeroSecurity	Penetration testing tool
Cuckoo	Cuckoo	Automated malware analysis system
Nessus	Tenable	Vulnerability assessment tool
scanless	Vesche	Tool for using websites to perform port scan
nmap	Nmap	Network discovery and security auditing

Linux File Manipulation Tools

Tool name	Description	Example
head	Display the first 10 lines of a file	*head etc/snort/snort.conf*
tail	Display the last 10 lines of a file	*tail etc/snort/snort.conf*
cat	Display an entire file	*cat etc/snort/snort.conf*
grep	Search for keyword	*grep apache1*
chmod	Change file permissions	*chmod 774 rules*
logger	Add content to syslog file	*logger comment*

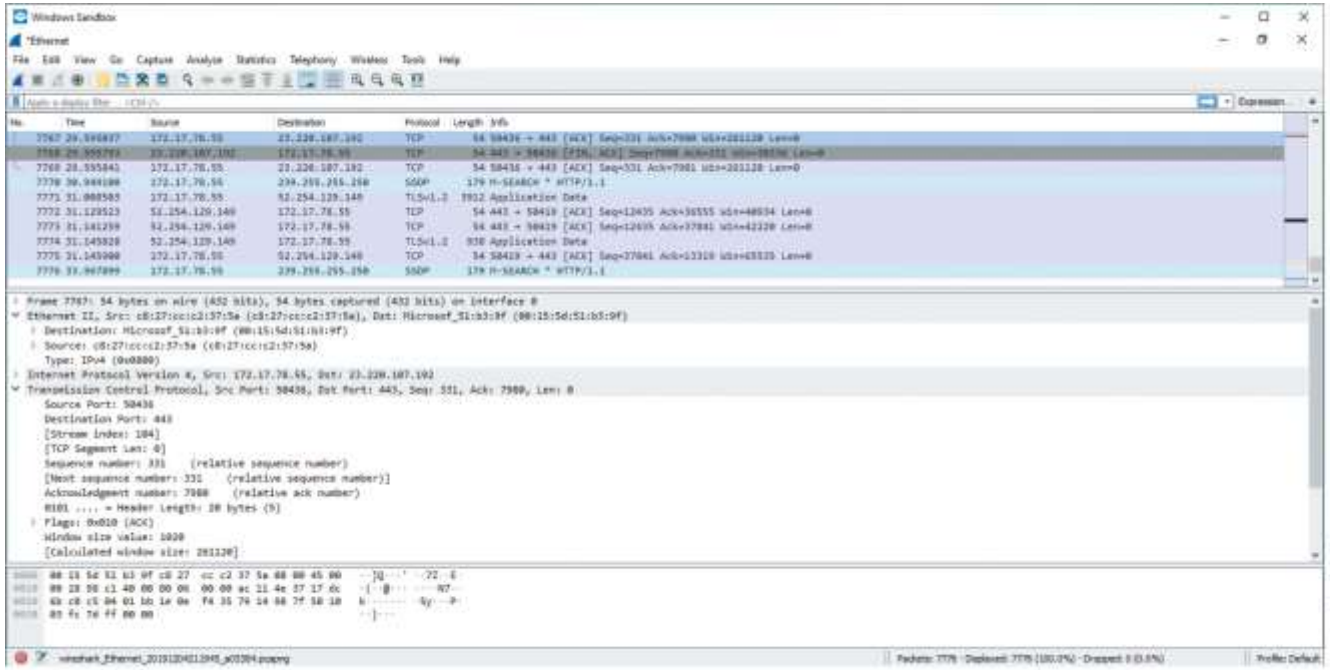
Scripting Tools

- Scripting tools are used to create scripts that facilitate tasks
- PowerShell is one of the most powerful scripting tools
- Scripts can also be created when using Secure Shell (SSH)
- **OpenSSL** is another tool that supports scripting
  - It is a cryptography library that offers open source applications of the TLS protocol

Packet Capture and Replay Tools (1 of 2)

- Collecting and analyzing data packets that cross a network can provide valuable information
- Packet analysis typically examines the entire contents of the packet, which can be used extensively for security
    - It can detect unusual behavior that could indicate the presence of malware, search for unusual domains or IP address endpoints, and discover regular connections to a threat actor’s command and control (C&C) server
- **Wireshark** is a popular GUI packet capture and analysis tool
- **Tcpdump** is a command-line packet analyzer
- **Tcpreplay** is a tool for editing packets and then “replaying” the packets back onto the network to observe their behavior

Packet Capture and Replay Tools (2 of 2)


Windows Sandbox
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time       Source           Destination      Protocol Length Info
 7767 29.595837  172.17.78.55     23.220.107.192   TCP        54 58436 → 443 [ACK] Seq=331 Ack=7980 Win=261120 Len=0
 7768 29.595793  23.220.107.192   172.17.78.55     TCP        54 443 → 58436 [FIN, ACK] Seq=7980 Ack=331 Win=30720 Len=0
 7769 29.595841  172.17.78.55     23.220.107.192   TCP        54 58436 → 443 [ACK] Seq=331 Ack=7981 Win=261120 Len=0
 7770 30.944100  172.17.78.55     239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
 7771 31.008503  172.17.78.55     52.254.129.140   TLSv1.2  3912 Application Data
 7772 31.129523  52.254.129.140   172.17.78.55     TCP        54 443 → 58419 [ACK] Seq=12435 Ack=36555 Win=40534 Len=0
 7773 31.141259  52.254.129.140   172.17.78.55     TCP        54 443 → 58419 [ACK] Seq=12435 Ack=37841 Win=42320 Len=0
 7774 31.145828  52.254.129.140   172.17.78.55     TLSv1.2   938 Application Data
 7775 31.145900  172.17.78.55     52.254.129.140   TCP        54 58419 → 443 [ACK] Seq=37841 Ack=13319 Win=65535 Len=0
 7776 33.967899  172.17.78.55     239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
```

```
> Frame 7767: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
v Ethernet II, Src: c8:27:cc:c2:37:5a (c8:27:cc:c2:37:5a), Dst: Microsoft_51:b3:9f (00:15:5d:51:b3:9f)
  > Destination: Microsoft_51:b3:9f (00:15:5d:51:b3:9f)
  > Source: c8:27:cc:c2:37:5a (c8:27:cc:c2:37:5a)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.17.78.55, Dst: 23.220.107.192
v Transmission Control Protocol, Src Port: 58436, Dst Port: 443, Seq: 331, Ack: 7980, Len: 0
    Source Port: 58436
    Destination Port: 443
    [Stream index: 104]
    [TCP Segment Len: 0]
    Sequence number: 331    (relative sequence number)
    [Next sequence number: 331    (relative sequence number)]
    Acknowledgment number: 7980    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 1020
    [Calculated window size: 261120]
```

```
0000  00 15 5d 51 b3 9f c8 27  cc c2 37 5a 08 00 45 00   ..]Q...' ..7Z..E.
0010  00 28 50 c1 40 00 80 06  00 00 ac 11 4e 37 17 dc   .(P.@... ....N7..
0020  6b c0 e4 44 01 bb 1e 0e  f4 35 79 14 88 7f 50 10   k..D.... .5y...P.
0030  03 fc 7d ff 00 00                                  ..}...
```

wireshark_Ethernet_20191204211945_a03384.pcapng | Packets: 7776 · Displayed: 7776 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Wireshark Software

Figure 8-7 Wireshark packet capture and analysis tool

Figure 8-7 Wireshark packet capture and analysis tool

Knowledge Check Activity 2

Which of the following is a GUI tool that it used to capture and analyze packets?

a. Tcpdump

b. PowerShell

c. Tcpreplay

d. Wireshark

Knowledge Check Activity 2: Answer

Which of the following is a GUI tool that it used to capture and analyze packets?

Answer: d. Wireshark

Wireshark is a GUI packet capture and analysis tool. Tcpdump is a command-line packet analyzer, Tcprelay is used to edit and replay packets, and PowerShell is a scripting tool.

Physical Security Controls

- Physical security involves preventing a threat actor from physically accessing the network
- Physical security controls include:
    - External perimeter defenses
    - Internal physical security controls
    - Computer hardware security

External Perimeter Defenses (1 of 2)

- Industrial camouflage is an attempt to make the physical presence of a building as nondescript as possible
- When camouflage is not possible, external perimeter defenses must be used
- Barriers
  - Barriers acts as passive security devices
  - **Fencing** is usually a permanent structure to keep unauthorized personnel out
    - It is usually accompanied by signage that explains the area is restricted
  - A **barricade** is generally designed to block the passage of traffic but not designed to keep out individuals
  - A **bollard** is a short but sturdy vertical post that is used as a vehicular traffic barricade to prevent a car from ramming into a secured area

External Perimeter Defenses (2 of 2)

- Personnel
  - Human security guards who patrol and monitor restricted areas are most often used as an active security defense
  - In settings that require a higher level of protection, two security guards may be required
  - Some guards are responsible for monitoring activity captured by video surveillance cameras that transmit a signal to a specific and limited set of receivers called closed circuit television (CCTV)
  - Drones, also called unmanned aerial vehicles (UAVs), include cameras for monitoring activity
  - Robot sentries that patrol and use CCTV with object detection are increasingly being used in public areas
- Sensors
  - To supplement the work of security guards, sensors can be placed in strategic locations to alert guards by generating an audible alarm of an unexpected or unusual action

Internal Physical Security Controls (1 of 5)

- Internal physical access security controls include:
  - Locks
  - Secure areas
  - Protected cable distribution
  - Fire suppression
- Locks
  - Physical locks require a key or other device to open doors or cabinets
  - **Electronic locks** use buttons that must be pushed in the proper sequence to open the door
  - *Smart locks* use a smartphone to send a code via wireless Bluetooth to open a door
  - *Fingerprint locks* have a pad that scans a user’s fingerprint

Internal Physical Security Controls (2 of 5)

- Secure Areas
  - A **demilitarized zone (DMZ)** in cybersecurity is an area that separates threat actors from defenders
  - A *mantrap* is designed as an air gap to separate a nonsecure area from a secured area (see Figure 8-11 on the following slide)
    - A mantrap device monitors and controls two interlocking doors to a vestibule
  - Another area that must be secured is the data center that houses the on-premises network, server, and storage equipment

Internal Physical Security Controls (3 of 5)

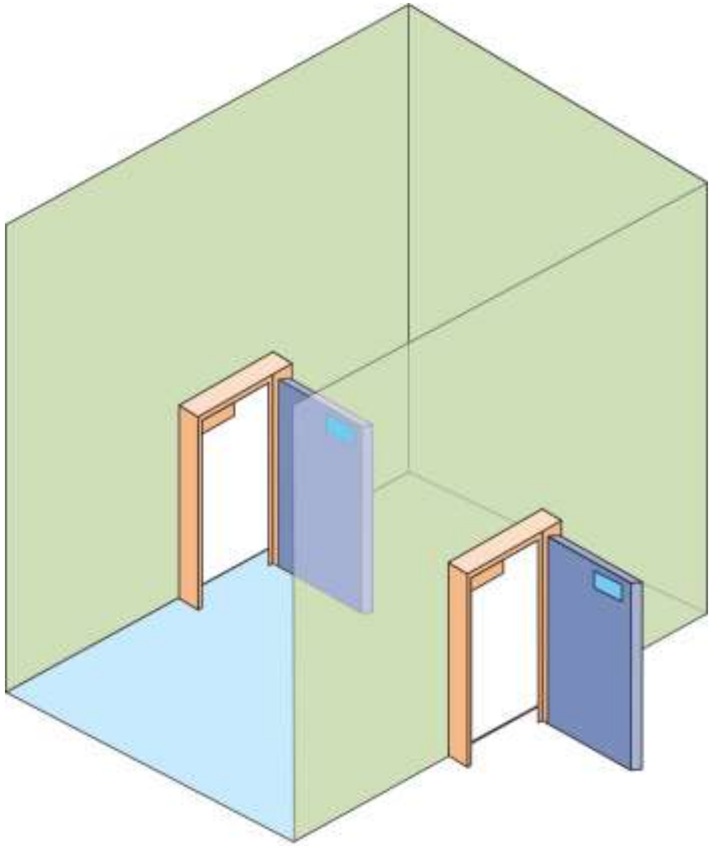


Figure 8-11 Mantrap

Figure 8-11 Mantrap

Internal Physical Security Controls (4 of 5)

- Protected Cable Distribution
  - A **protected cable distribution (PDS)** is a system of cable conduits used to protect classified information that is being transmitted between two secure areas
  - Two types of PDS are commonly used:
    - In a *hardened carrier PDS*, the data cables are installed in a conduit constructed of special electrical metallic tubing and all connections between segments are permanently sealed with welds or special sealants
    - In an *alarmed carrier PDS*, the carrier system is deployed with specialized optical fibers in the conduit that can sense acoustic vibrations that occur when an intruder attempts to gain access to cables

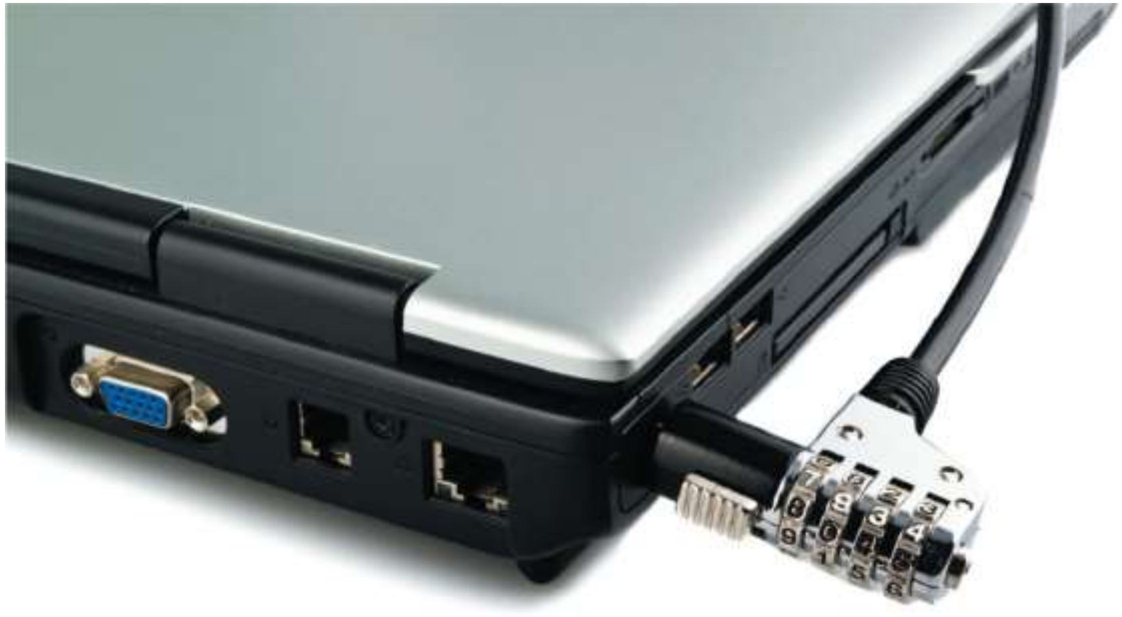
Internal Physical Security Controls (5 of 5)

- Fire Suppression
  - In a data center containing electronic equipment, using water or a handheld fire extinguisher is not recommended because it can contaminate equipment
  - Stationary fire suppression systems are integrated into the building’s infrastructure and release fire suppressant
    - Systems can be classified as:
      - Dry chemical systems that disperse a fine, dry powder over the fire
      - Clean agent systems that extinguish a fire by reducing heat, removing or isolating oxygen, or inhibiting the chemical reaction

Computer Hardware Security (1 of 2)

- Computer hardware security is the physical security that involves protecting endpoint hardware
- A **cable lock** can be inserted into the security slot of a portable device to secure the device
- For storage, a laptop can be placed in a safe or a **vault**
  - These can be prewired for electrical power as well as wired network connections
- Computer systems, printers, and similar electronic devices emit electromagnetic fields, which can result in interference (called *electromagnetic interference* or *EMI*)
  - Electromagnetic spying can be defined as picking up electromagnetic fields and reading data that is producing them
  - A Faraday cage is a metallic enclosure that prevents entry or escape of an electromagnetic field. A Faraday cage can prevent electromagnetic spying and remote wiping of electronic devices.

Computer Hardware Security (2 of 2)



O.Bellini/Shutterstock.com

Figure 8-13 Cable lock

Figure 8-13 Cable lock

Knowledge Check Activity 3

What can be used to secure electronic devices from electromagnetic spying and shield them from EMI?

a. Demilitarized zone

b. PDS

c. Faraday cage

d. Mantrap

Knowledge Check Activity 3: Answer

What can be used to secure electronic devices from electromagnetic spying and shield them from EMI?

Answer: c. Faraday cage

A Faraday cage is a metallic enclosure that prevents the entry or escape of an electromagnetic field.

Self-Assessment

Consider the three learning objectives of this module:

1. Describe the different types of networking-based attacks

2. List the different network assessment tools

3. Explain how physical security defenses can be used

For each objective, write two or three sentences explaining what you learned about each of these objectives from reading the module and performing the exercises.

Summary (1 of 2)

- Some attacks are designed to intercept network communications
  - Man-in-the-middle and replay attacks are examples
- Some types of attacks inject “poison” into a normal network process to facilitate an attack
- DNS poisoning modifies a local lookup table on a device to point to a different domain, which is usually a malicious DNS server controlled by a threat actor that will redirect traffic to a website designed to steal user information or infect the device with malware
- Several successful network attacks come from malicious software code and scripts
- There are several different assessment tools for determining the strength of a network
- Collecting and analyzing data packets that cross a network can provide a wealth of valuable information

Summary (2 of 2)

- An often-overlooked consideration when defending a network is physical security: preventing a threat actor from physically accessing the network is as important as preventing the attacker from accessing it remotely
- While barriers act as passive devices to restrict access, personnel are considered active security elements
- In the event that unauthorized personnel defeat external perimeter defenses, they should then face internal physical access security
- A demilitarized zone (DMZ) is an area that separates threat actors from defenders (also called a physical air gap)