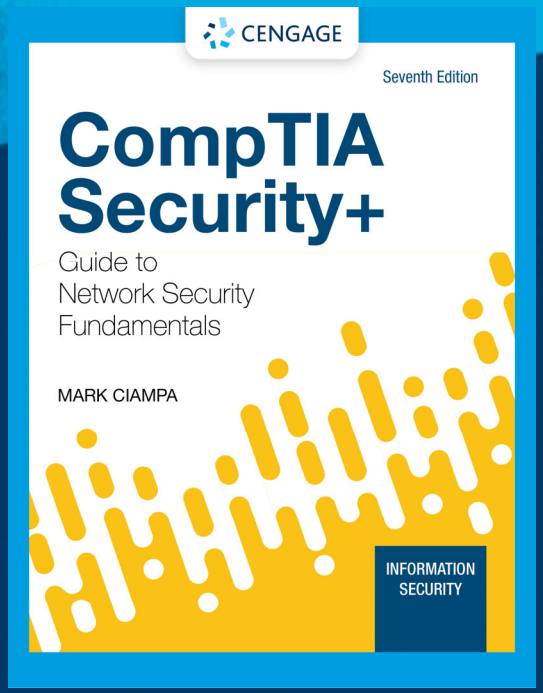


Module 8: Networking Threats, Assessments, and Defenses

Module Objectives

- By the end of this module, you should be able to:
  - Describe the different types of networking-based attacks
  - List the different network assessment tools
  - 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

- **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

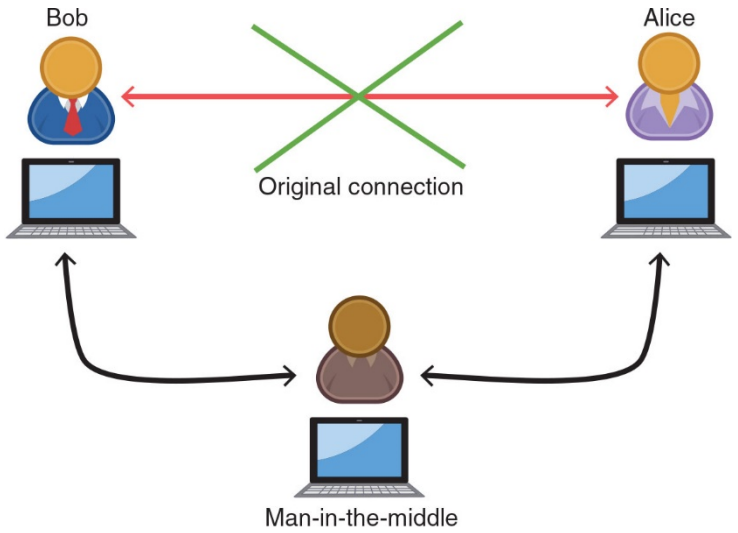


Figure 8-1 MITM attack

Interception Attacks (contd.)

- **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 (contd.)

- **Man-in-the-Browser (MITB) attack**
  - Intercepts communication between parties to steal or manipulate the data
    - Occurs between a browser and the underlying computer
  - 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 (contd.)

- **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
      - Makes it difficult for standard anti-malware software to detect it

Layer 2 Attacks

- The OSI reference model
  - Separates networking steps into a series of seven *layers*
  - Within each layer, different networking tasks are performed
    - Cooperate with the tasks in the layers immediately above and below it

https://ipwithease.com/network-vulnerabilities-and-the-osi-model/

Layer 2 Attacks

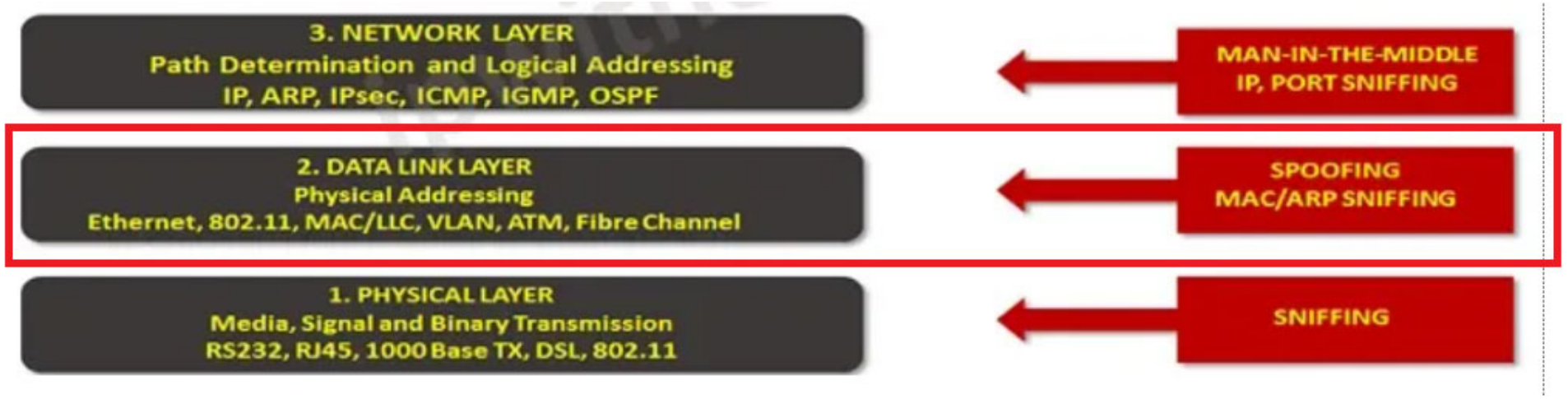
Away	Application Layer	**A**ll
Pizza	Presentation Layer	**P**eople
Sausage	Session Layer	**S**eem
Throw	Transport Layer	**T**o
Not	Network Layer	**N**eed
Do	Data Link Layer	**D**ata
Please	Physical Layer	**P**rocessing

Layer 2 Attacks

- Layer 2, the Data Link Layer
  - Responsible for dividing the data into packets
  - A compromise at Layer 2 can affect the entire communication

Away	Application Layer	All
Pizza	Presentation Layer	People
Sausage	Session Layer	Seem
Throw	Transport Layer	To
Not	Network Layer	Need
Do	Data Link Layer	Data
Please	Physical Layer	Processing

- **Attacks**
  - **Address Resolution Protocol Poisoning**
  - **Media Access Control Attacks**



Layer 2 Attacks

- **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

- **Address Resolution Protocol 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
    - MAC cloning
    - MAC flooding

- **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
- **MAC flooding attack**
  - **A**nother 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

OSI MODEL LAYERS	TYPES OF ATTACK
7. APPLICATION LAYER Network Process to Application DNS, WWW, HTTP, SMTP, Telnet, FTP	EXPLOIT USER ID/PASSWORD SNIFFING
6. PRESENTATION LAYER Data Representation and Encryption	PHISHING SSL/TLS SESSION SNIFFING
5. SESSION LAYER Inter Host Communication Session Establishment in TCP, SIP, RTP, RPC	HIJACKING TELNET & FTP SNIFFING
4. TRANSPORT LAYER End to End connection and reliability TCP, UDP, SSL, TLS	RECONNAISSANCE/DOS TCP SESSION SNIFFING/PORT SNIFFING
3. NETWORK LAYER Path Determination and Logical Addressing IP, ARP, IPsec, ICMP, IGMP, OSPF	MAN-IN-THE-MIDDLE IP, PORT SNIFFING
2. DATA LINK LAYER Physical Addressing Ethernet, 802.11, MAC/LLC, VLAN, ATM, Fibre Channel	SPOOFING MAC/ARP SNIFFING
1. PHYSICAL LAYER Media, Signal and Binary Transmission RS232, RJ45, 1000 Base TX, DSL, 802.11	SNIFFING

3

https://ipwithease.com/network-vulnerabilities-and-the-osi-model/

DNS Attacks

- **Domain Name System (DNS)**
  - *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
  - DNS hijacking

DNS Attacks

- **Domain Name System (DNS)**
  - *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
    - DNS hijacking

DNS Attacks

- **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 Hijacking**
  - 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

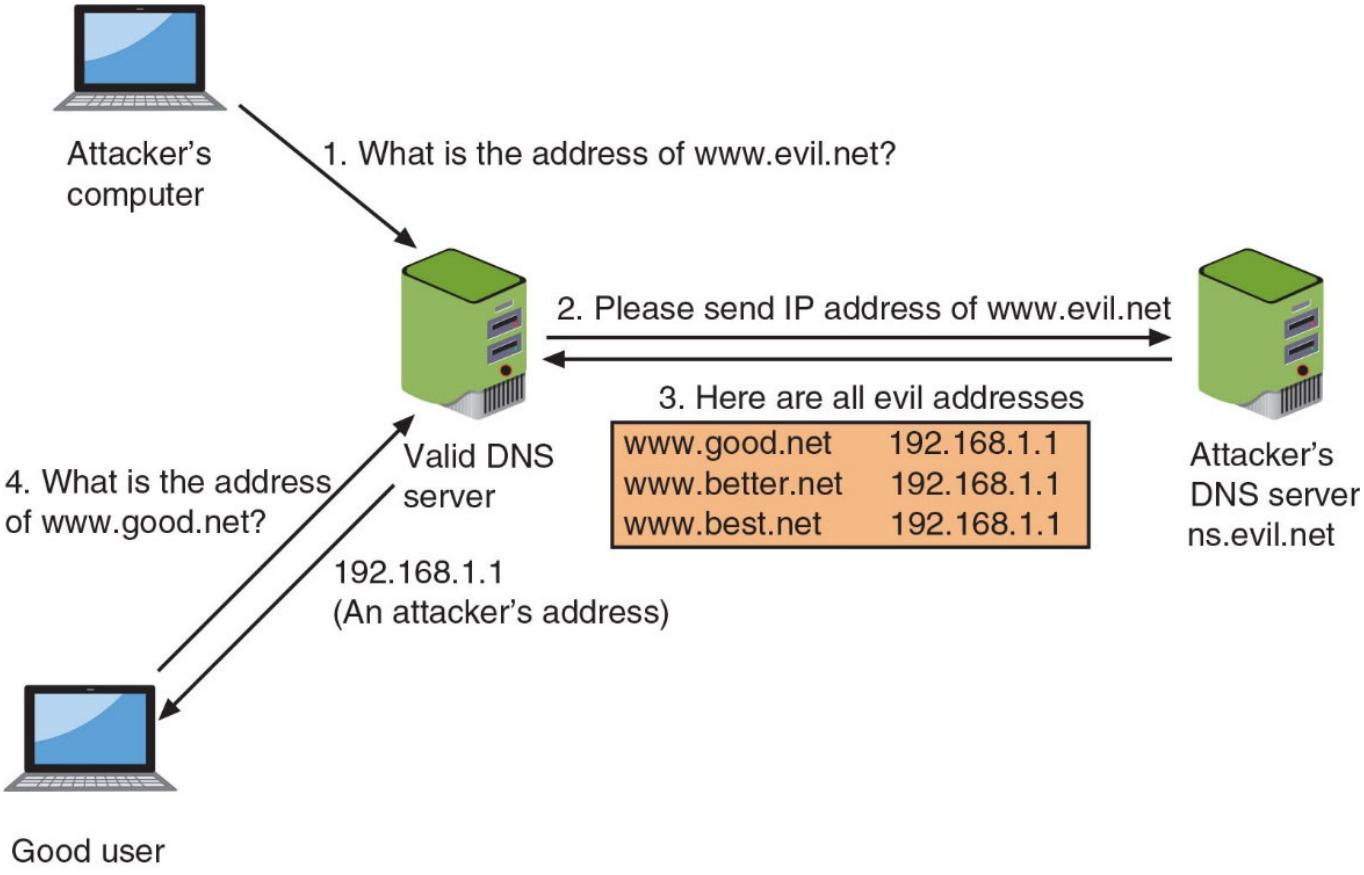


Figure 8-5 DNS server poisoning

- Figure 8-5 DNS server poisoning

Distributed Denial of Service Attack

- **Denial of service (DoS) attack**
  - 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
  - Users are completely unaware that their endpoints are part of a DDoS attack

Malicious Coding and Scripting Attacks

- Some network attacks come from malicious software code and scripts
  - PowerShell
  - Visual Basic for Applications
  - Python
  - Linux/UNIX Bash

- **PowerShell**
  - A task automation and configuration management framework from Microsoft
  - Administrative tasks are performed by cmdlets
    - Specialized .NET classes that implement a specific operation
  - 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)**
  - An event-driven Microsoft programming language
  - Most often used to create macros, which are used to automate a complex task or a repeated series of tasks
  - Due to the impact of macro malware, Microsoft has implemented several protections:
    - *Protected View*
    - *Trusted Documents*
    - *Trusted Location*

Malicious Coding and Scripting Attacks

- **Bash**
  - 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

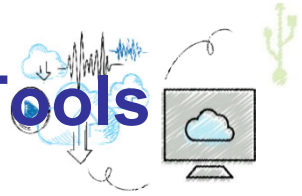
- **Python**
  - A popular programming language that can run on several OS platforms
  - Several best practices to follow when using Python so that the code does not contain vulnerabilities:
    - Use the latest version of Python
    - Stay current on vulnerabilities within Python
    - Be care when formatting strings in Python
    - Download only vetted Python libraries

Tools for Assessment and Defense

- **Tools Purpose**
  - Determine the strength of a network
  - Create a stronger network defense

- **Tools Categorization**
  - Network reconnaissance and discovery tools
  - Linux file manipulation tools
  - 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

Packet Capture and Replay Tools

- 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
  - Can detect unusual behavior:
    - Indicate the presence of malware
    - Search for unusual domains or IP address endpoints
    - Discover regular connections to a threat actor's command and control (C&C) server
- **Wireshark**
  - A popular GUI packet capture and analysis tool
- **Tcpdump**
  - A command-line packet analyzer
- **Tcpreplay**
  - A tool for editing packets and then "replaying" the packets back onto the network to observe their behavior

Physical Security Controls

- **Physical security**
  - 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

- 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**
  - Acts as passive security devices

  - **Fencing**
    - Permanent structure to keep unauthorized personnel out
    - Usually accompanied by signage that explains the area is restricted
  - **Barricade**
    - Designed to block the passage of traffic but not designed to keep out individuals
  - **Bollard**
    - 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

- **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**
    - Unmanned aerial vehicles (UAVs), include cameras for monitoring activity
  - **Robot sentries**
    - Patrol and use CCTV with object detection are increasingly being used in public areas
- **Sensors**
  - Supplement the work of security guards
  - Pplaced in strategic locations to alert guards by generating an audible alarm of an unexpected or unusual action

Internal Physical Security Controls

- 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

- **Secure Areas**
  - A **demilitarized zone (DMZ)** in cybersecurity
    - An area that separates threat actors from defenders
  - ***A mantrap***
    - *D*esigned as an air gap to separate a nonsecure area from a secured area
    - 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

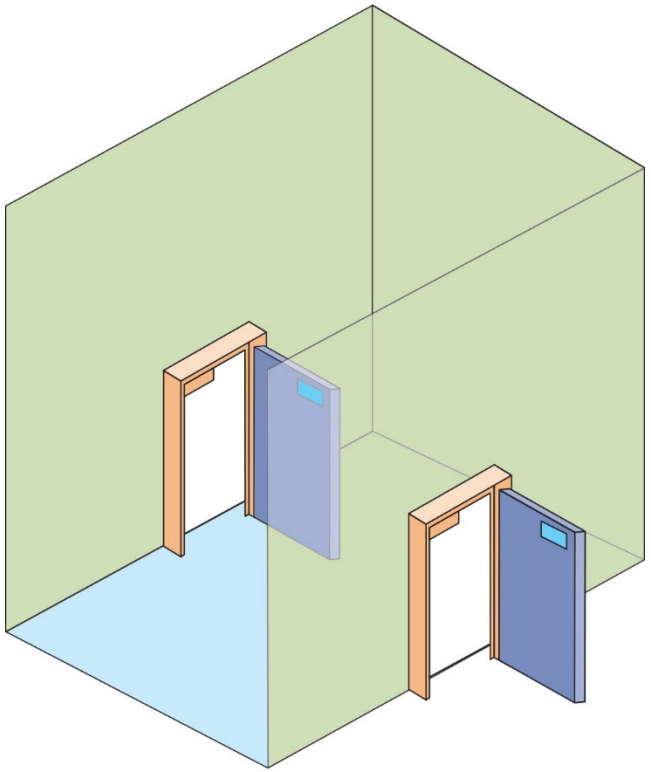


Figure 8-11 Mantrap

Internal Physical Security Controls

- **Protected Cable Distribution System**
  - A system of cable conduits used to protect classified information that is being transmitted between two secure areas
  - **Two types of PDS**
    - **Hardened carrier PDS**
      - *D*ata cables are installed in a conduit constructed of special electrical metallic tubing
      - All connections between segments are permanently sealed with welds or special sealants
    - **Alarmed carrier PDS**
      - *T*he carrier system is deployed with specialized optical fibers in the conduit
      - Sense acoustic vibrations that occur when an intruder attempts to gain access to cables

Internal Physical Security Controls

- **Fire Suppression**
  - In a data center containing electronic equipment, using water or a handheld fire extinguisher is not recommended
    - It can contaminate equipment

- **Stationary fire suppression systems**
  - Integrated into the building's infrastructure and release fire suppressant
  - Can be classified as:
    - **Dry chemical systems**
      - Disperse a fine, dry powder over the fire
    - **Clean agent systems**
      - Extinguish a fire by reducing heat, removing or isolating oxygen, or inhibiting the chemical reaction

Computer Hardware Security

- **Computer hardware security**
  - Physical security that involves protecting endpoint hardware
- **Cable lock**
  - 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 Hardware Security

- **Electromagnetic interference or EMI**
  - Computer systems, printers, and similar electronic devices emit electromagnetic fields, which can result in interference
  - Electromagnetic spying can be defined as picking up electromagnetic fields and reading data that is producing them

- **A Faraday cage**
  - Metallic enclosure that prevents entry or escape of an electromagnetic field.
  - Prevent electromagnetic spying and remote wiping of electronic devices.

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)

LAYER	PROTOCOL DATA UNIT (PDU)	DESCRIPTION	PROTOCOL SUPPORTED	EXAMPLES OF ATTACK	IMPACT OF ATTACK
Application Layer (7)	Data	End-user protocol.	FTP, HTTP, POP3 and SMTP.	HTTP GET and HTTP POST.	During an attack, no user are able to access network resources.
Presentation Layer (6)	Data	Encrypt and Decrypt data format at both ends.	Protocols Compression & Encryption	Attackers use SSL to tunnel HTTP attacks to target the server.	Affected systems stop accepting SSL connections or automatically restart.
Session Layer (5)	Data	Establishment, termination, and sync of session.	PAP, NetBIOS, L2TP, L2F, PPTP, RPC.	Telnet DDoS-attacker.	Disable management operations.
Transport Layer (4)	Segment	Error free and reliable transmission between hosts.	TCP & UDP.	SYN Flood, Smurf Attack.	Connection limits of hosts.
Network Layer (3)	Packet	Routing and Switching information to different networks.	IP, ICMP, ARP and routing protocol.	Layer 3 infrastructure DDoS attack.	Affect on network bandwidth and impose extra load on the firewall.
Data Link Layer (2)	Frame	Handles how the transfer is accomplished over the physical layer.	ATM, CDP, Ethernet, FDDI, Frame Relay, HDLC, IEEE 802, IEEE 802.11, PPP, MPLS, UDLD.	MAC flooding.	Disrupts the sender to receiver flow of data flooding across all ports.
Physical Layer (1)	Bits	Limited to cables, jacks, and hubs	100 Base-T & 1000 Base-X, Hubs, patch panels, & RJ45 Jacks.	Alter data bits.	Data destroyed.
					https://ipwithease.com

https://ipwithease.com/network-vulnerabilities-and-the-osi-model/