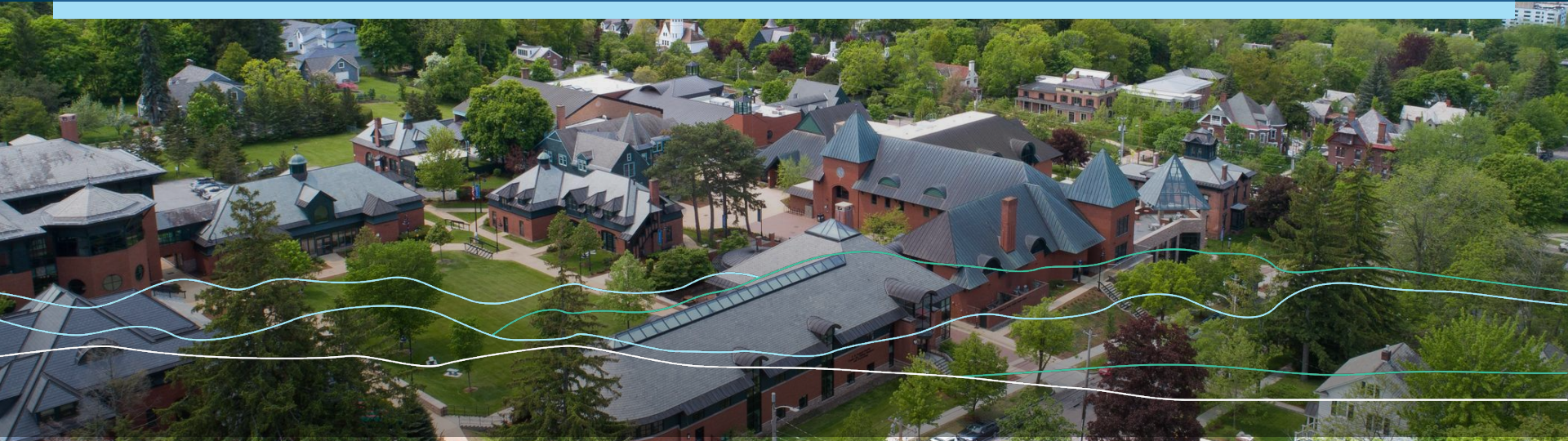


CHAMPLAIN COLLEGE



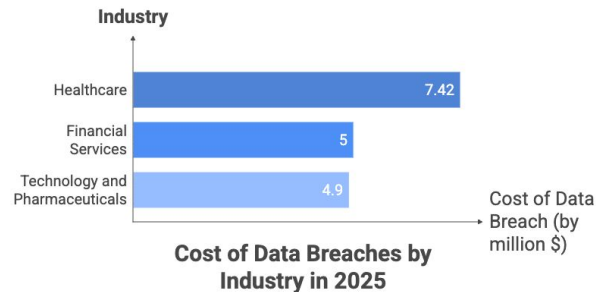
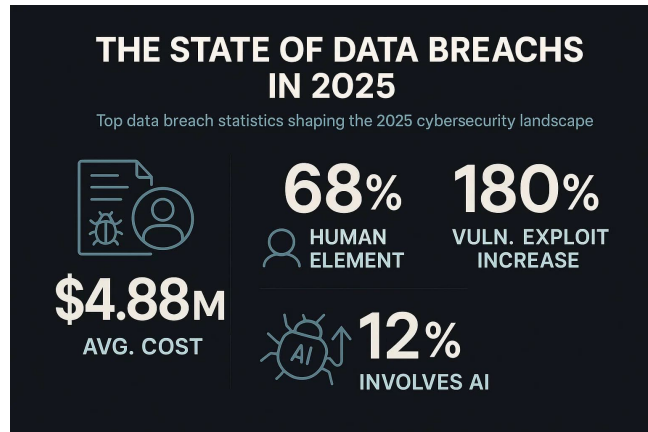
Mod 10 – Network Security

SEC-110



Why Network Security Matters

- **More devices = more vulnerabilities**
 - Every connected device can be a target
- **Security vs convenience**
 - Easier access often means weaker protection
- **Real-world impact**
 - **Data breaches:** personal info can be stolen or exposed
 - **Financial losses:** downtime and recovery can cost millions
 - **Privacy violations:** personal data can be exposed or misused



Real world network breach

Allianz Life Insurance (2025)

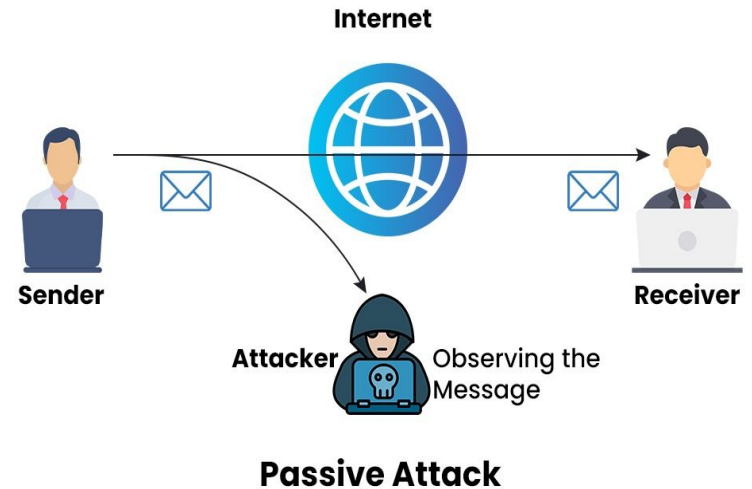
- A third-party cloud vendor was hacked, exposing personal data of most of Allianz Life's 1.4 million US customers.
 - **Cause:** Vendor-level breach
 - **Impact:** Data exposure, customer privacy risk
 - **Lesson:** Even secure companies can be vulnerable through partners



Common Network Threats

Passive Attacks: monitoring network traffic without changing it.

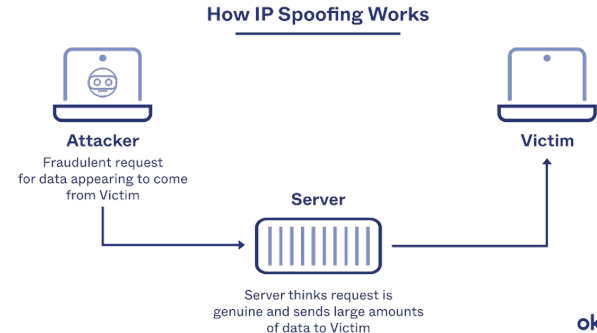
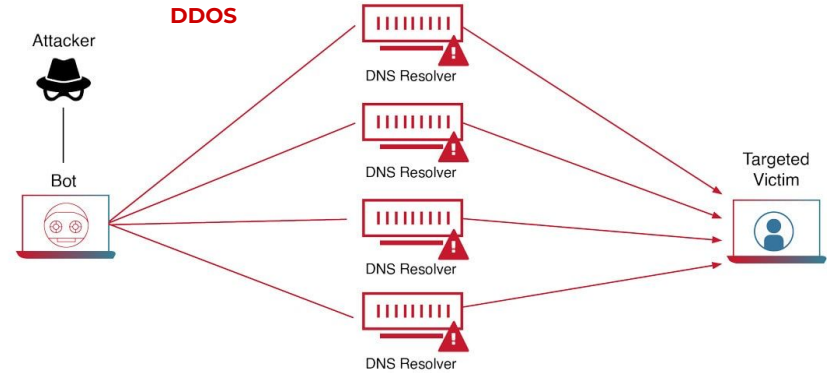
- **Packet Sniffing:** capturing data using tools like Wireshark
- **Traffic Analysis:** Studying communication patterns to gather intel
- **Man-in-the-middle attacks:** intercepting and possibly altering private communications



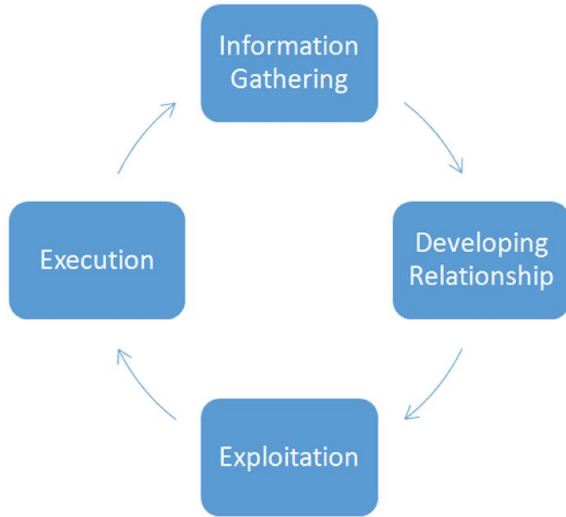
Common Network Threats

Active Attacks

- **Denial of Service (DoS):**
Overwhelming network resources
- **Distributed DoS (DDoS):** Using multiple compromised systems
- **IP spoofing:** Faking an IP address to impersonate another device
- **Session hijacking:** Taking over someone else's active login session



Common Network Threats



Social Engineering: Tricking people into giving up sensitive info.

- **Phishing** - Fake emails or sites steal login data
- **Pretexting** - Pretending to be someone trustworthy to get info

Network Vulnerabilities



- **Unencrypted communications** (data sent in plaintext)
- **Weak Authentication** (Default passwords, poor access controls)
- **Unpatched systems** (known security flaws not fixed)
- **Misconfigured devices** (routers, switches, firewalls set up incorrectly)

Security at Each OSI Layer

Physical Layer Security (Layer 1)

- Physical access controls (locked server rooms, cable protection)
- Wireless security concerns (signal interception, rogue access points)
- Cable tapping (direct access to network cables)

PHYSICAL LAYER

1

— Transmits raw bit stream over the physical medium

Security at Each OSI Layer

Data Link Layer Security (Layer 2)

- MAC address spoofing: Changing device identifiers
- ARP poisoning: Corrupting address resolution tables
- VLAN security: Isolating network segments



— Defines the format of data on the network

Security at Each OSI Layer

Network Layer Security (Layer 3)

- IP address spoofing: Faking packet source addresses
- Routing attacks: Manipulating network paths
- ICMP attacks: Using ping and traceroute maliciously



— Decides which physical path the data will take

Security at Each OSI Layer

Transport Layer Security (Layer 4)

- Port scanning: Finding open services
- TCP hijacking: Taking over connections
- UDP flooding: Overwhelming connectionless services



— Transmits data using transmission protocols including TCP and UDP

Security at Each OSI Layer

Upper Layers (5-7)

- Application vulnerabilities: Web apps, email, file sharing
- Exploitation: Taking advantage of design flaws
- Malware delivery: Using legitimate protocols to spread threats



— Human-computer interaction layer, where applications can access the network services



— Ensures that data is in a usable format and is where data encryption occurs

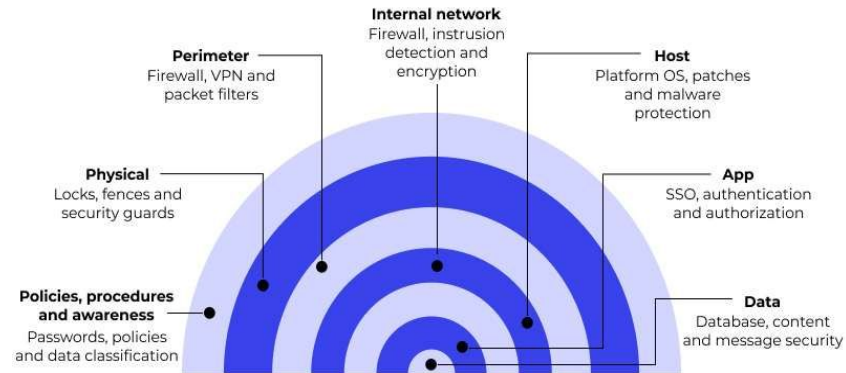


— Maintains connections and is responsible for controlling ports and sessions

Network Defense Strategies

Defense in Depth

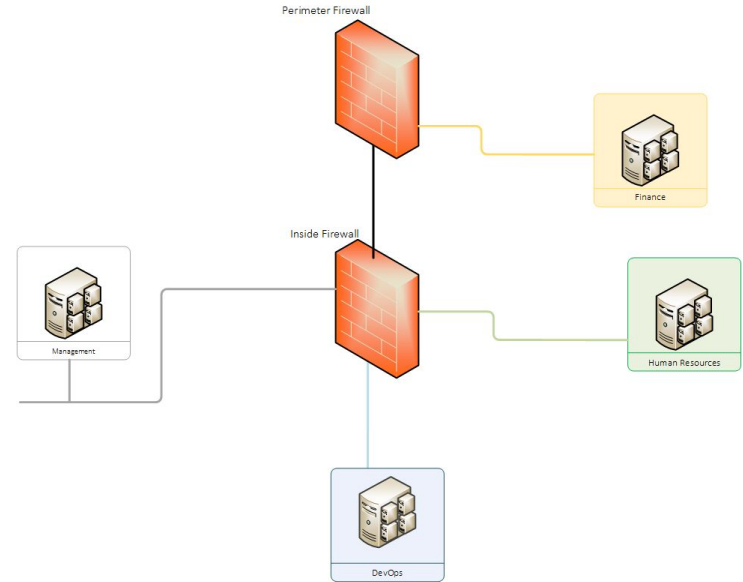
- Multiple security layers: No single point of failure
- Redundant controls: Backup security measures
- The security onion: Peeling back layers of protection



Network Defense Strategies

Network Segmentation

- DMZ (Demilitarized Zone): Separating public and private networks
- VLANs: Virtual network isolation
- Subnetting for security: Limiting broadcast domains and access



Network Defense Strategies

Access Controls

- Authentication: Proving identity (passwords, certificates, biometrics)
- Authorization: Determining permissions
- Accounting: Logging and monitoring access

MULTI-FACTOR AUTHENTICATION



Access Control



Broken Access Control

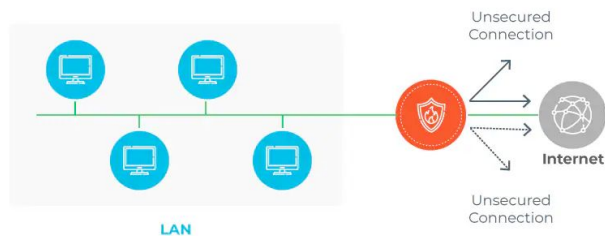


Network Defense Strategies

Firewalls

- Packet filtering: Examining individual packets
- Stateful inspection: Tracking connection states
- Application layer filtering: Deep packet inspection
- Firewall rules: Allow, deny, and logging policies

Hardware Firewall

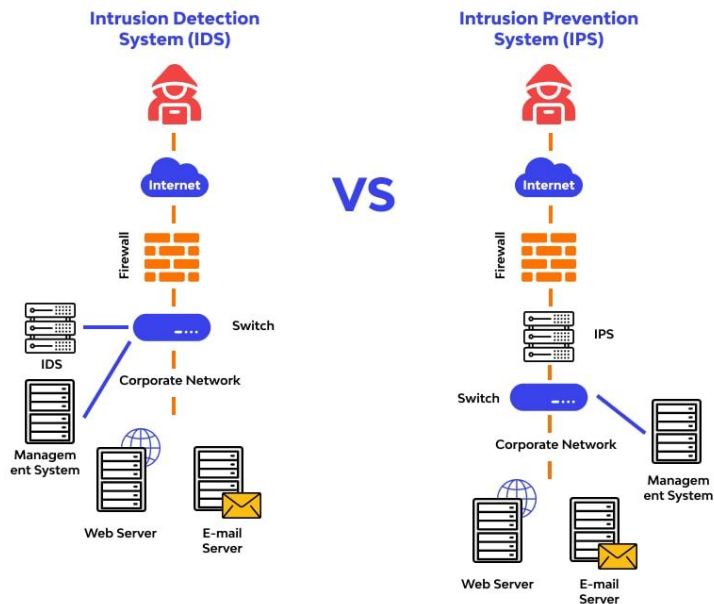


Software Firewall



Network Defense Strategies

Intrusion Detection and Prevention



- Network IDS: Monitoring for suspicious traffic patterns
- Host-based IDS: Watching individual systems
- Signature-based detection: Known attack patterns
- Anomaly-based detection: Unusual behavior identification

Encryption and Secure Protocols

Cryptography Basics

- **Symmetric encryption:**
Same key for
encrypt/decrypt
- **Asymmetric encryption:**
Public/private key pairs
- **Hashing:** One-way data
integrity verification
- **Digital signatures:**
Proving authenticity and
integrity

Secure Network Protocols

- Replacing Insecure
Protocols
 - HTTP → HTTPS
(SSL/TLS encryption)
 - Telnet → SSH (Secure
Shell)
 - FTP → SFTP/FTPS
(Secure file transfer)
 - SMTP → SMTPS (Secure
email)

Secure Protocol Example

Wireshark analysis of insecure protocol:

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcpstream eq 10

No.	Time	Source	Destination	Protocol	Length	Info
139	2.576953	192.168.1.127	[REDACTED]	HTTP/1.1	549	POST
141	2.579090	[REDACTED]	192.168.1.127	HTTP/1.1	549	POST
2190	39.646171	192.168.1.127	[REDACTED]	HTTP	426	GET /

Referer: http://[REDACTED]/auth\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

\r\n

[Full request URI: http://[REDACTED]/api/v1/auths/signin]

File Data: 76 bytes

JavaScript Object Notation: application/json

- Object
 - Member: email
 - [Path with value: /email:ThisIs@MyEmail.InPlaintext]
 - [Member with value: email:ThisIs@MyEmail.InPlaintext]
 - String value: ThisIs@MyEmail.InPlaintext
 - Key: email
 - [Path: /email]
 - Member: password
 - [Path with value: /password:superdupersecurepassword]
 - [Member with value: password:superdupersecurepassword]
 - String value: superdupersecurepassword

Wireshark analysis of secure protocol:

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcpstream eq 10

No.	Time	Source	Destination	Protocol	Length	Info
235	4.046264	192.168.1.127	31.13.66.48	TLSv1.2	257	Application Data
236	4.046342	192.168.1.127	31.13.66.48	TLSv1.2	853	Application Data
237	4.046375	192.168.1.127	31.13.66.48	TLSv1.2	85	Application Data

> Frame 235: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits) on interface 0

> Ethernet II, Src: Intel_a4:1e:38 (d0:65:78:a4:1e:38), Dst: Calix_78:72:72 (08:00:27:78:72:72)

> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 31.13.66.48

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 243

Identification: 0x9205 (37381)

010. = Flags: 0x2, Don't Fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.127

Destination Address: 31.13.66.48

[Stream index: 13]

> Transmission Control Protocol, Src Port: 19496, Dst Port: 443, Seq: 1, Win: 0, Len: 0

> Transport Layer Security

- TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 198
 - Encrypted Application Data [..]: fb15e175fad9a804683ee5e4a02cfeb23
 - [Application Data Protocol: Hypertext Transfer Protocol]

Encryption and Secure Protocols

VPNs (Virtual Private Networks)

- **Site-to-site VPNs:**
Connecting office locations
- **Remote access VPNs:**
Secure connections for remote workers
- **Tunneling protocols:**
IPSec, L2TP, OpenVPN

WiFi Security

- **WEP weaknesses:** Easily broken encryption
- **WPA/WPA2:** Stronger wireless protection
- **WPA3:** Latest wireless security standard
- **Enterprise vs. Personal:**
Different authentication methods