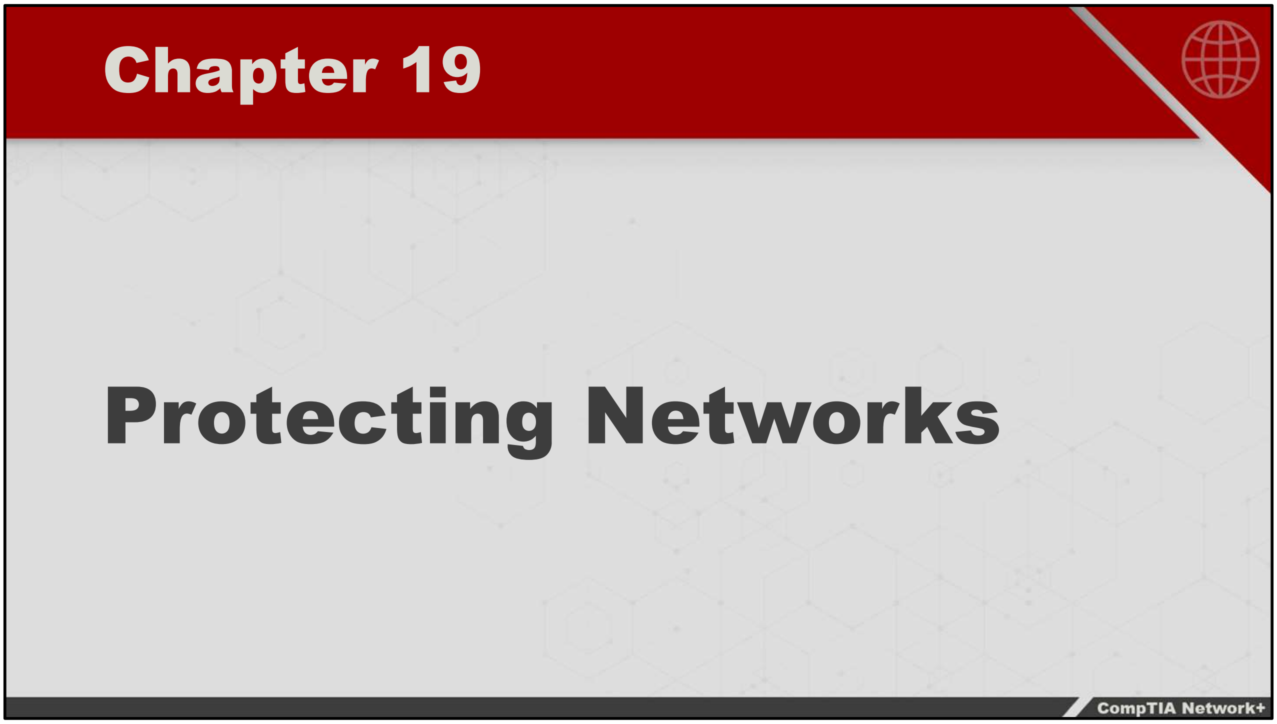
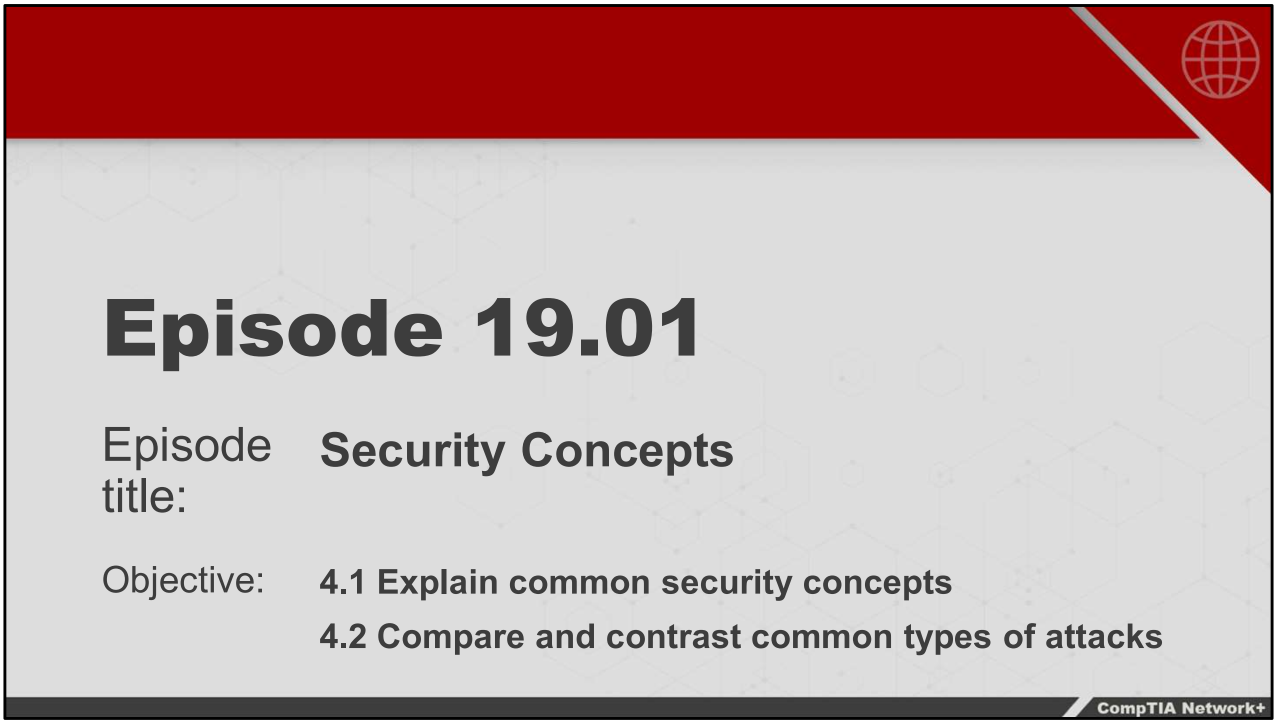


Chapter 19

Protecting Networks

CompTIA Network+

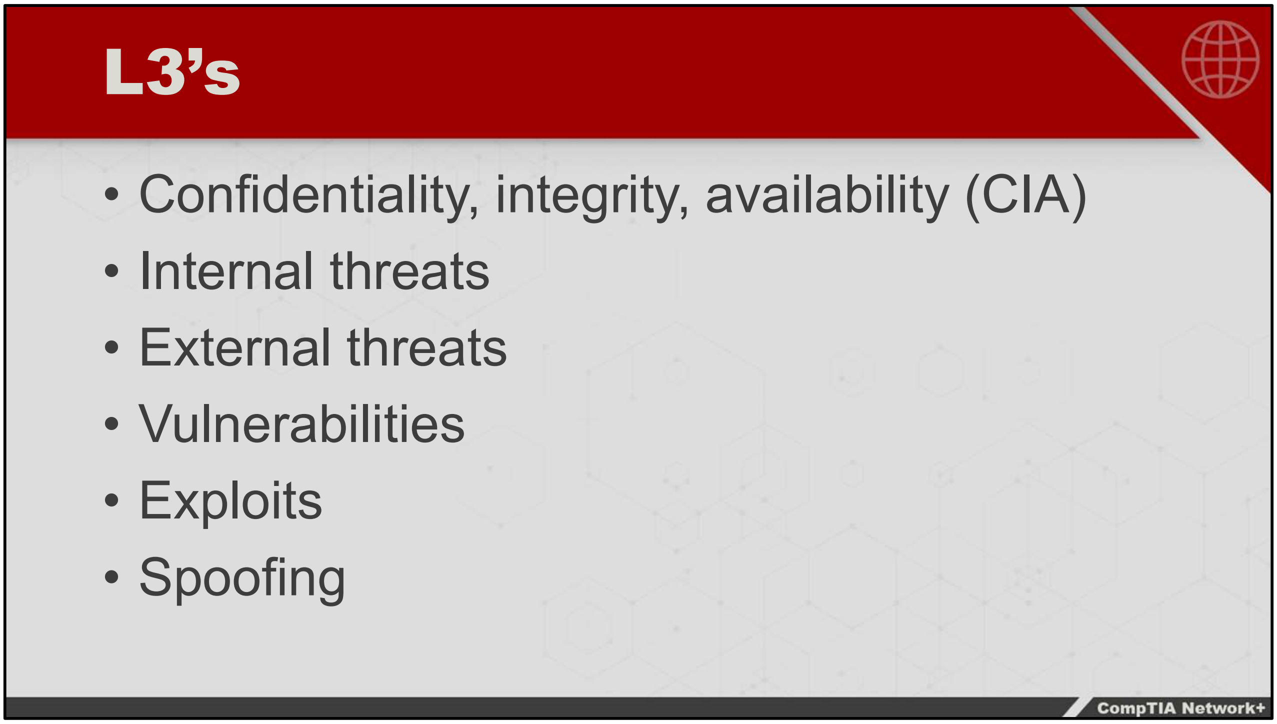


Episode 19.01

Episode title: **Security Concepts**

Objective: **4.1 Explain common security concepts**

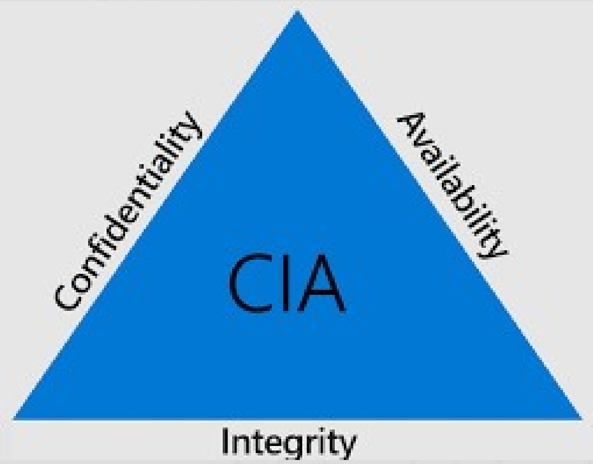
4.2 Compare and contrast common types of attacks

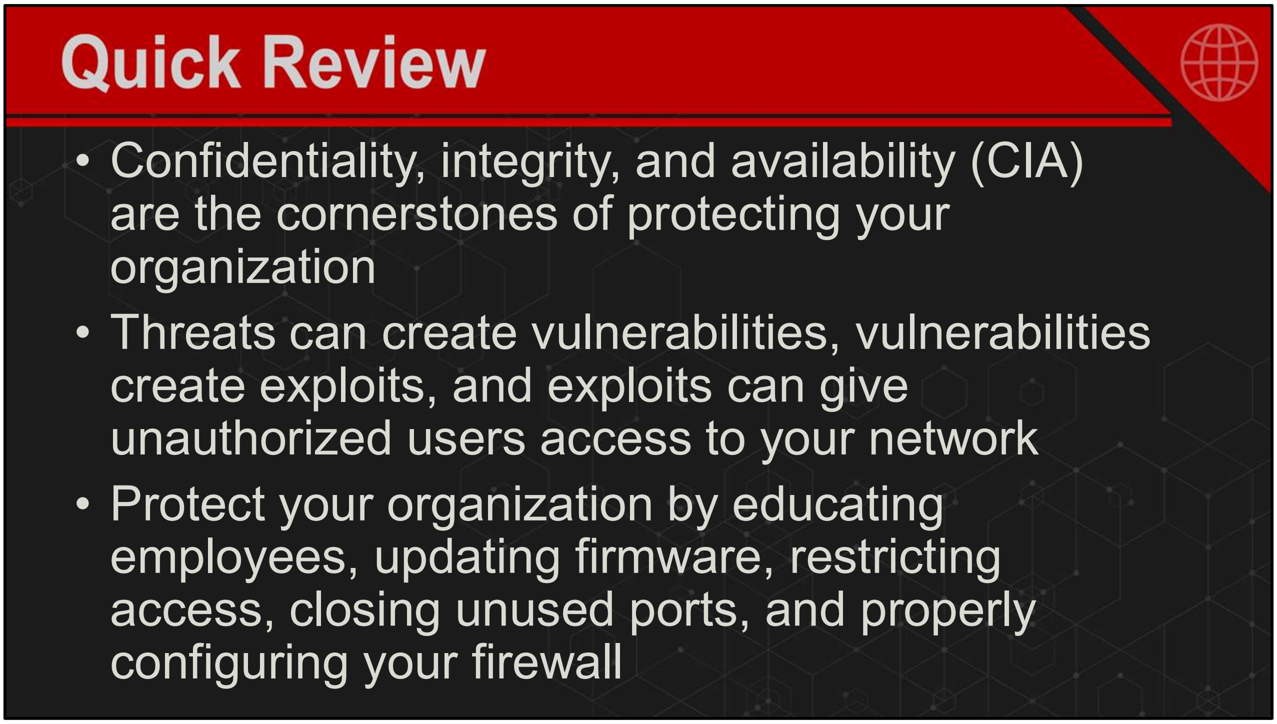


L3’s

- Confidentiality, integrity, availability (CIA)
- Internal threats
- External threats
- Vulnerabilities
- Exploits
- Spoofing

19.01 Graphic





Quick Review

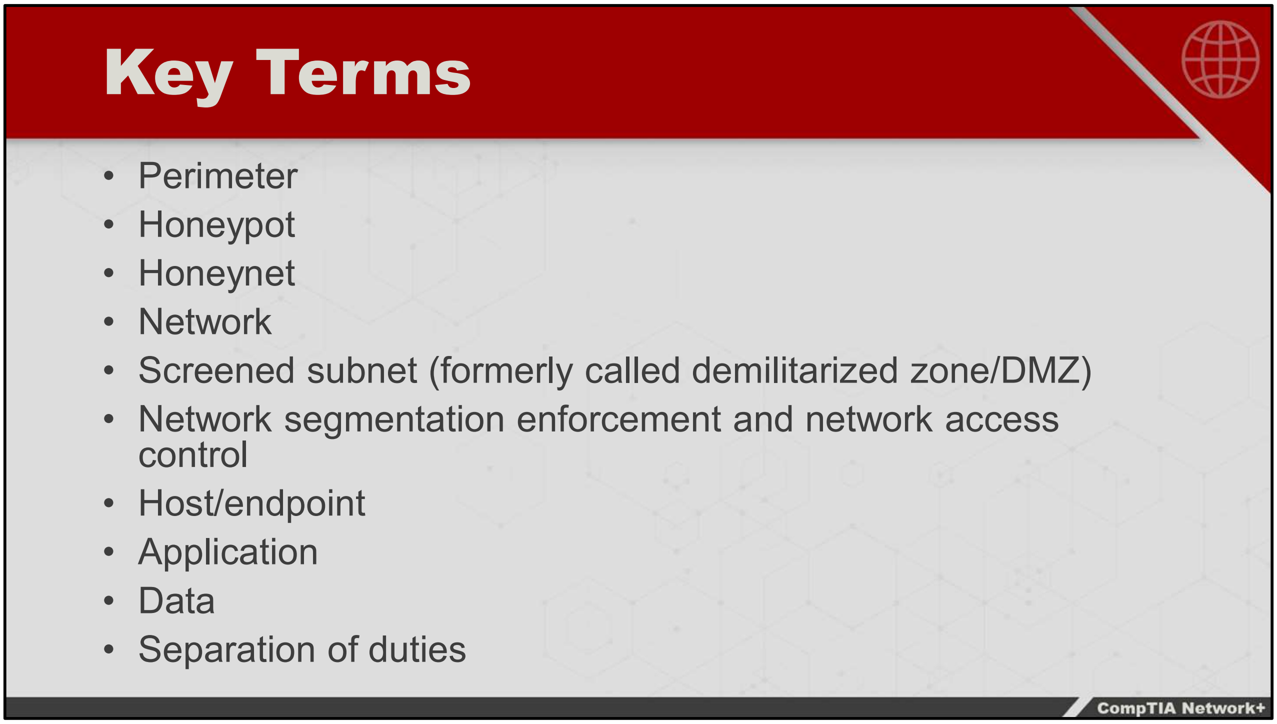
- Confidentiality, integrity, and availability (CIA) are the cornerstones of protecting your organization
- Threats can create vulnerabilities, vulnerabilities create exploits, and exploits can give unauthorized users access to your network
- Protect your organization by educating employees, updating firmware, restricting access, closing unused ports, and properly configuring your firewall

Episode 19.02

Episode title: **Defense in Depth**

Objective: **4.1 Explain common security concepts**

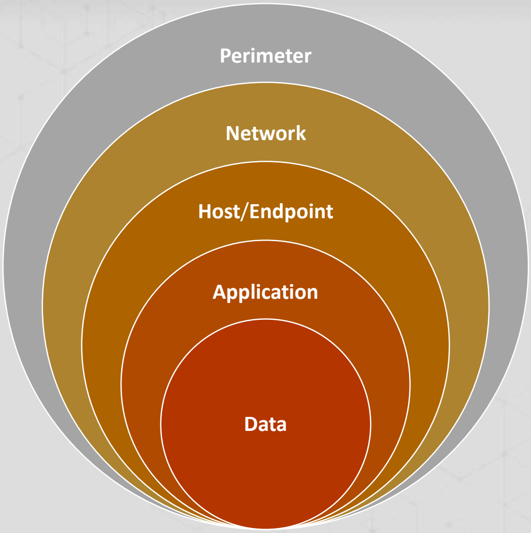
CompTIA Network+



Key Terms

- Perimeter
- Honeypot
- Honeynet
- Network
- Screened subnet (formerly called demilitarized zone/DMZ)
- Network segmentation enforcement and network access control
- Host/endpoint
- Application
- Data
- Separation of duties

Defense in Depth



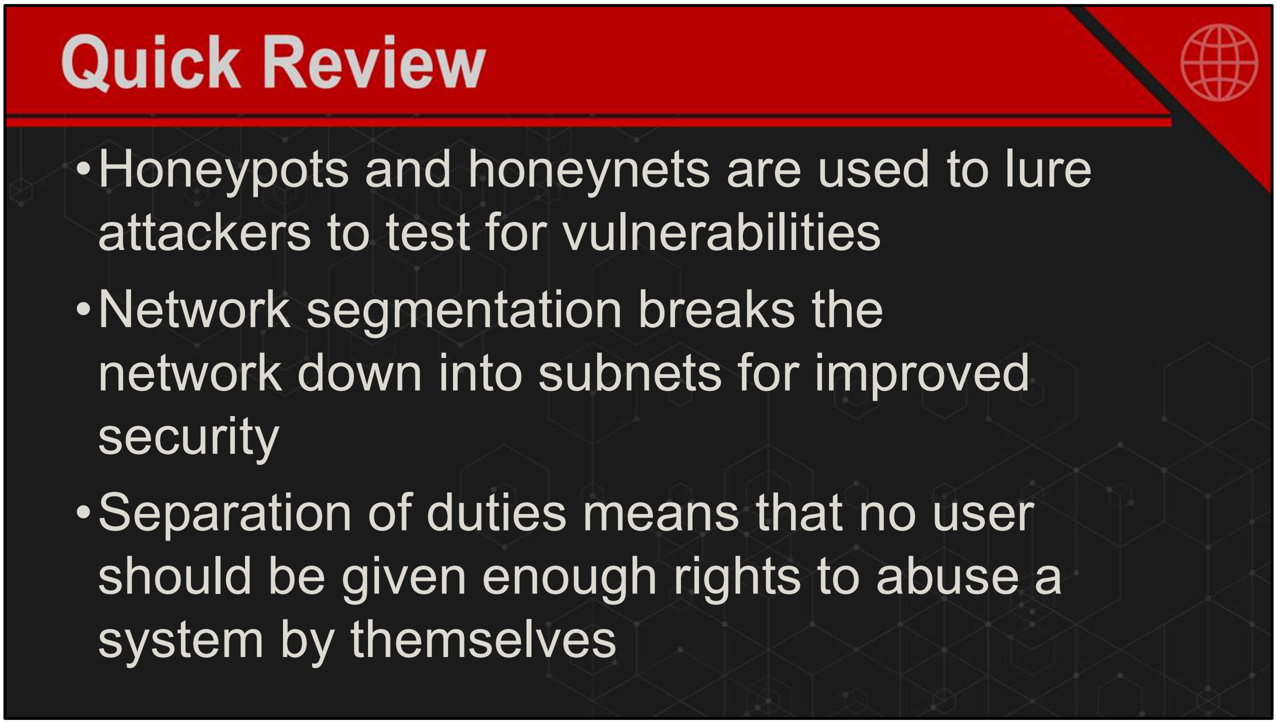
Perimeter

Network

Host/Endpoint

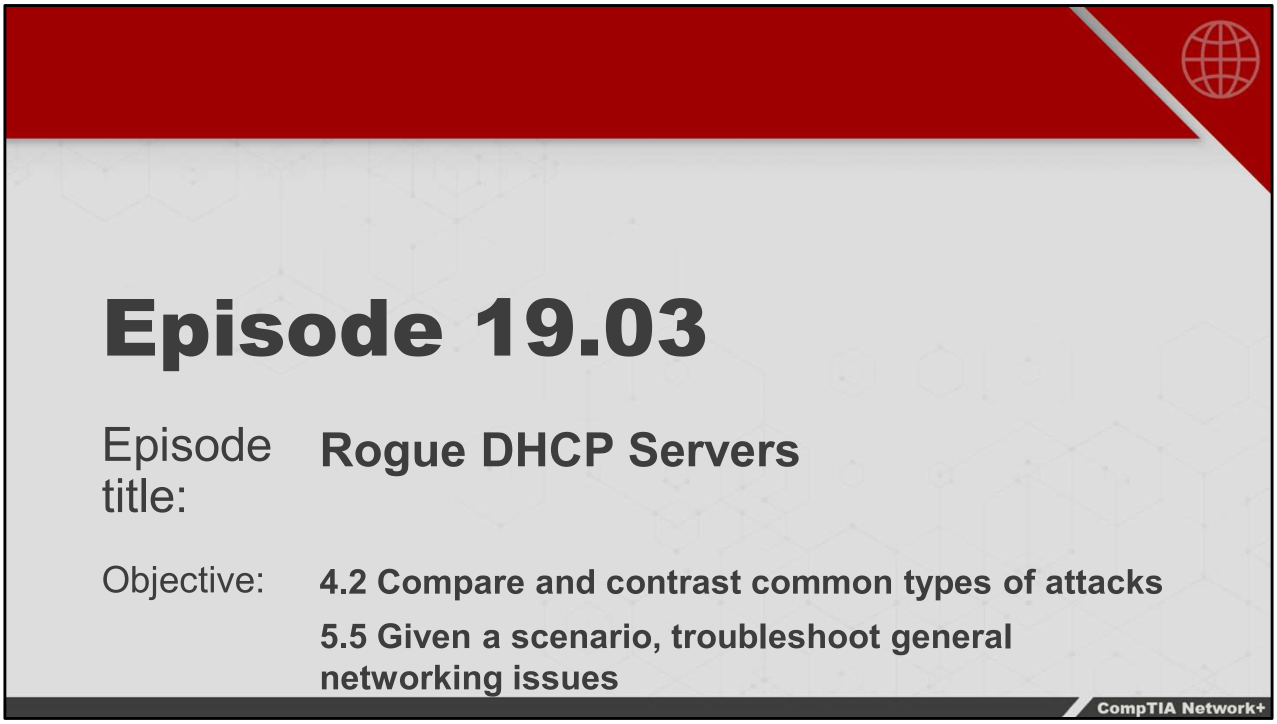
Application

Data



Quick Review

- Honeypots and honeynets are used to lure attackers to test for vulnerabilities
- Network segmentation breaks the network down into subnets for improved security
- Separation of duties means that no user should be given enough rights to abuse a system by themselves



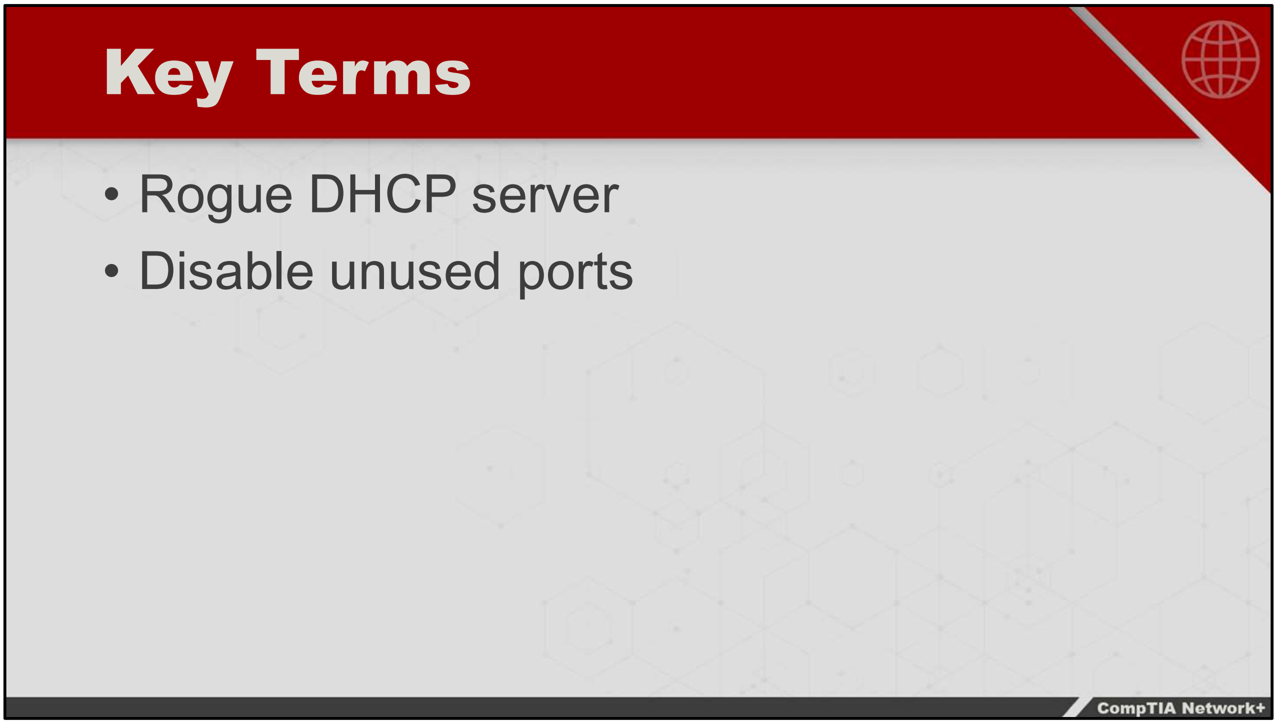
Episode 19.03

Episode title: **Rogue DHCP Servers**

Objective: **4.2 Compare and contrast common types of attacks**

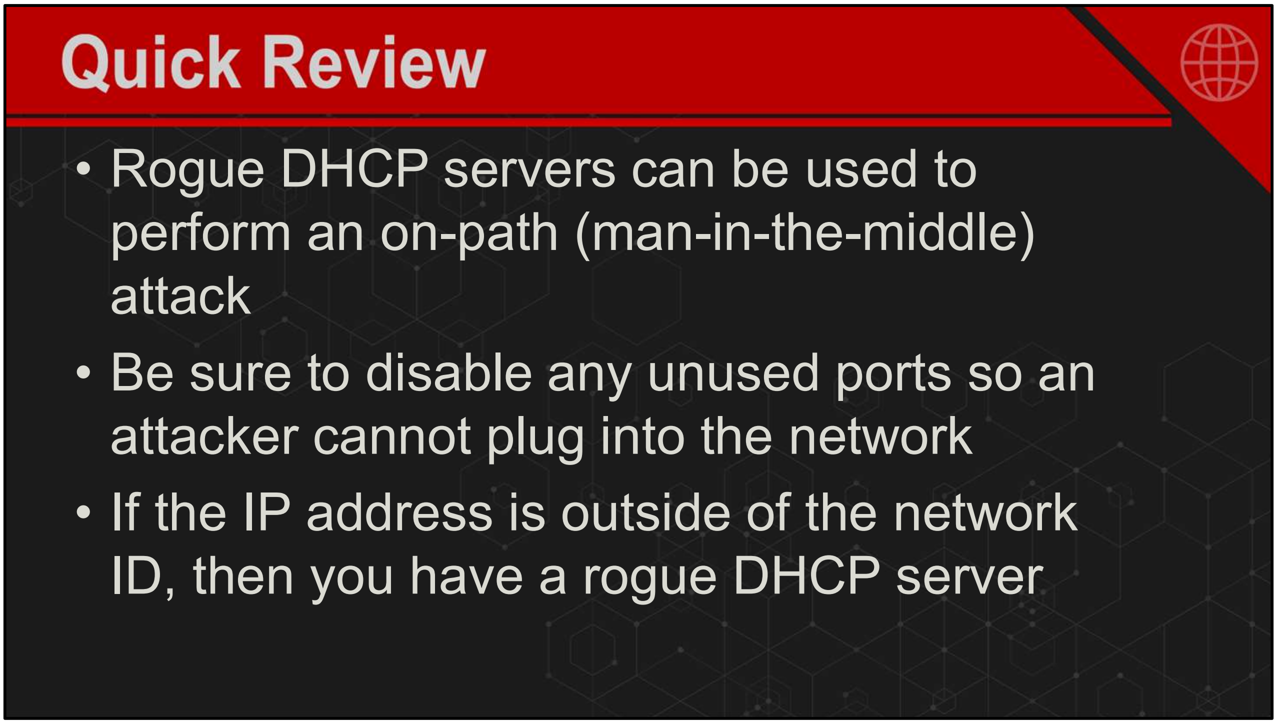
5.5 Given a scenario, troubleshoot general networking issues

CompTIA Network+



Key Terms

- Rogue DHCP server
- Disable unused ports



Quick Review

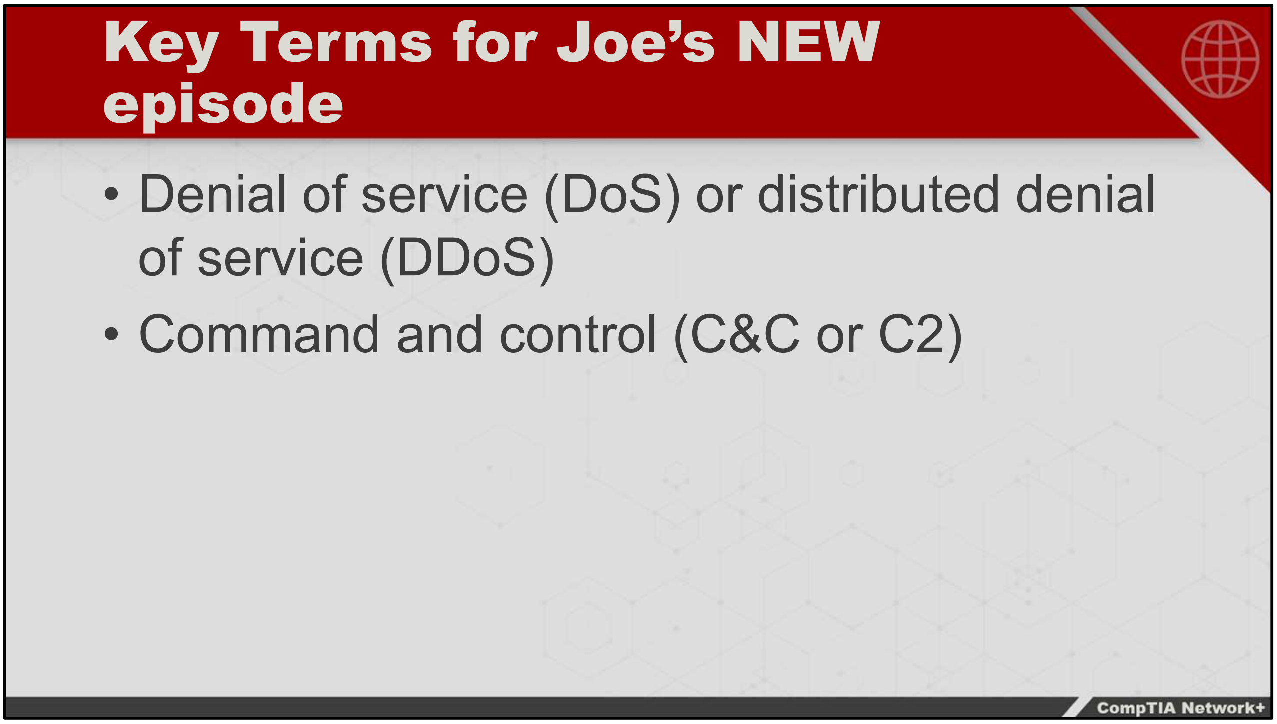
- Rogue DHCP servers can be used to perform an on-path (man-in-the-middle) attack
- Be sure to disable any unused ports so an attacker cannot plug into the network
- If the IP address is outside of the network ID, then you have a rogue DHCP server

Episode 19.04

Episode title: **Denial of Service (DoS)**

Objective: **4.2 Compare and contrast common types of attacks**

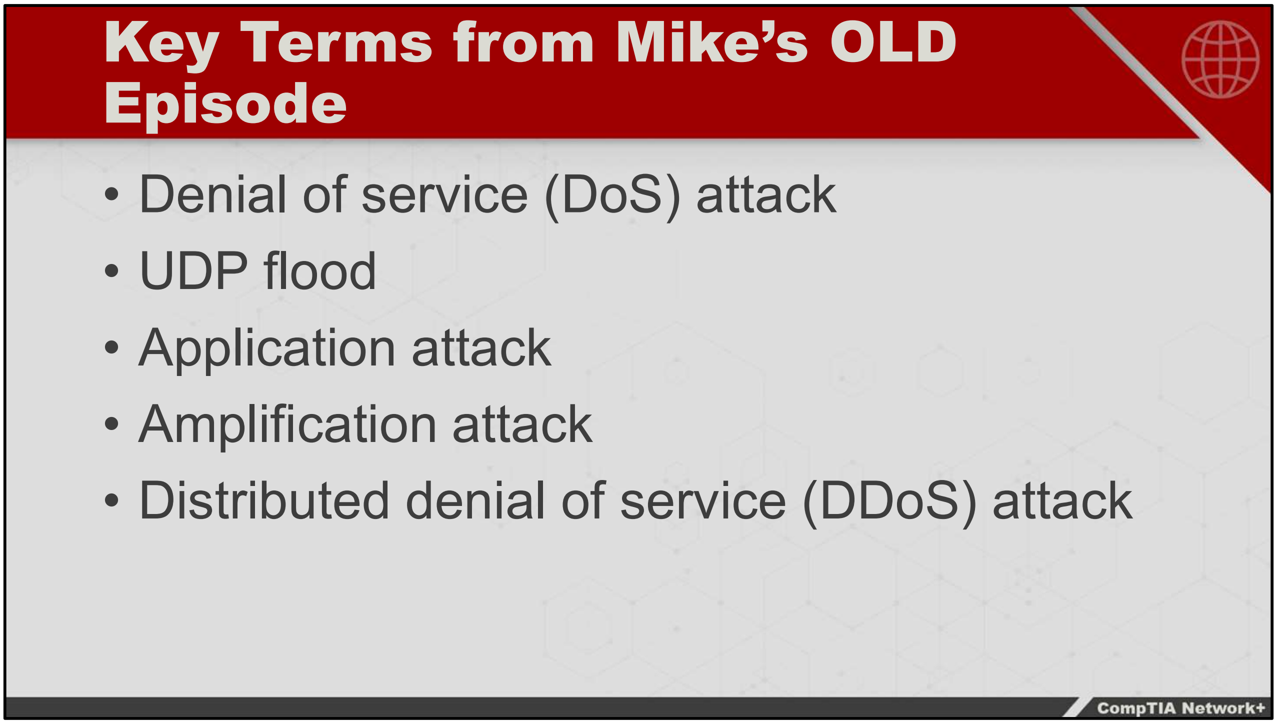
CompTIA Network+



Key Terms for Joe’s NEW episode

- Denial of service (DoS) or distributed denial of service (DDoS)
- Command and control (C&C or C2)

CompTIA Network+

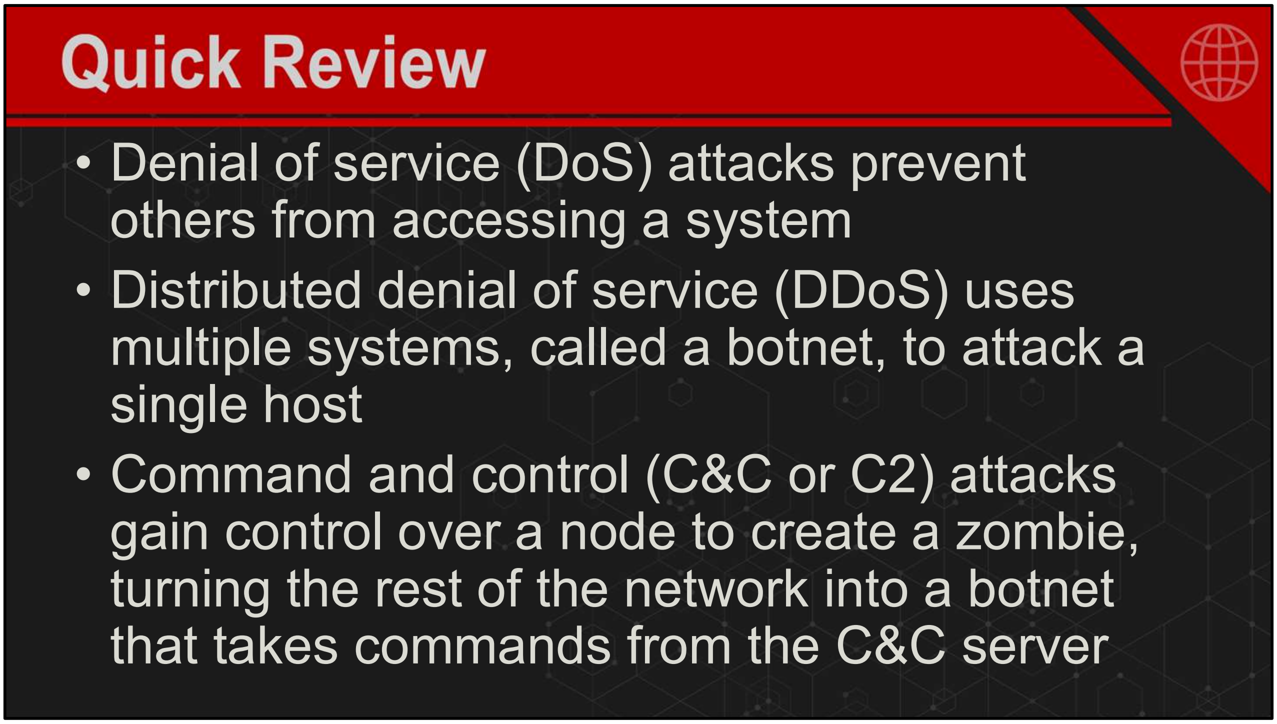


Key Terms from Mike's OLD Episode

- Denial of service (DoS) attack
- UDP flood
- Application attack
- Amplification attack
- Distributed denial of service (DDoS) attack

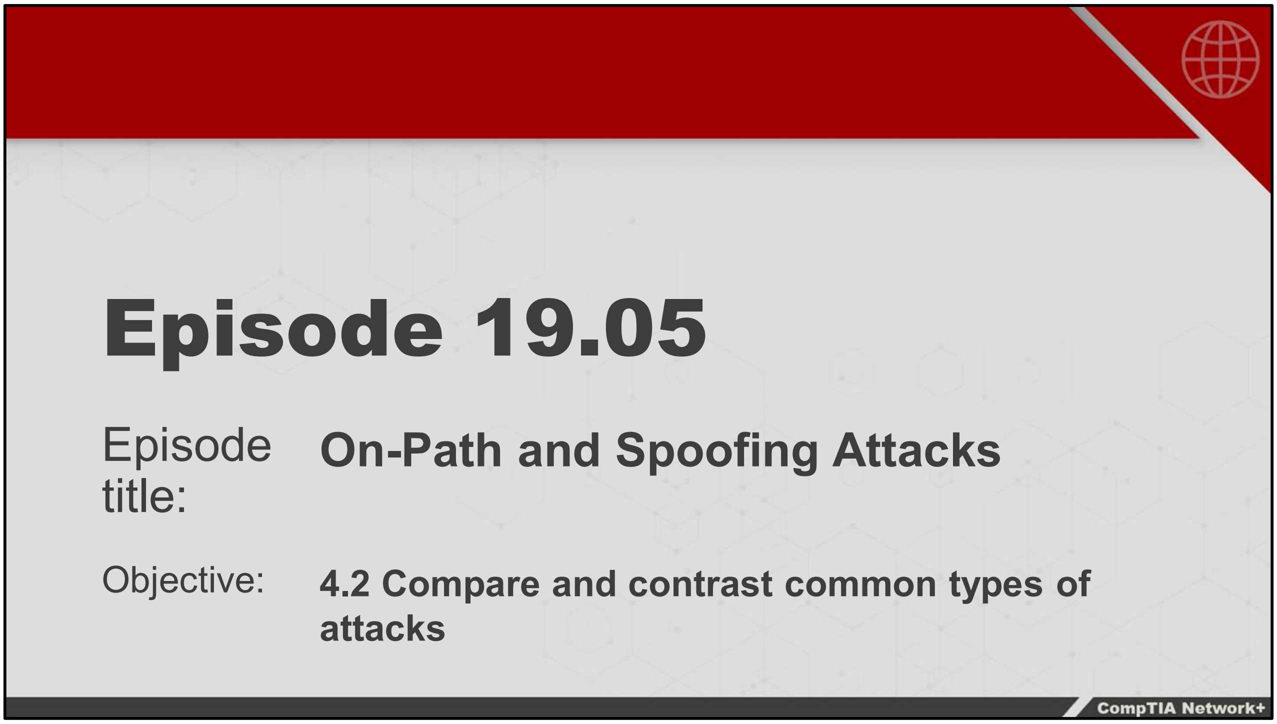
Denial of Service (DoS) Attack

- DoS attack types
  - Volume attack
  - Protocol attack
  - Application attack



Quick Review

- Denial of service (DoS) attacks prevent others from accessing a system
- Distributed denial of service (DDoS) uses multiple systems, called a botnet, to attack a single host
- Command and control (C&C or C2) attacks gain control over a node to create a zombie, turning the rest of the network into a botnet that takes commands from the C&C server

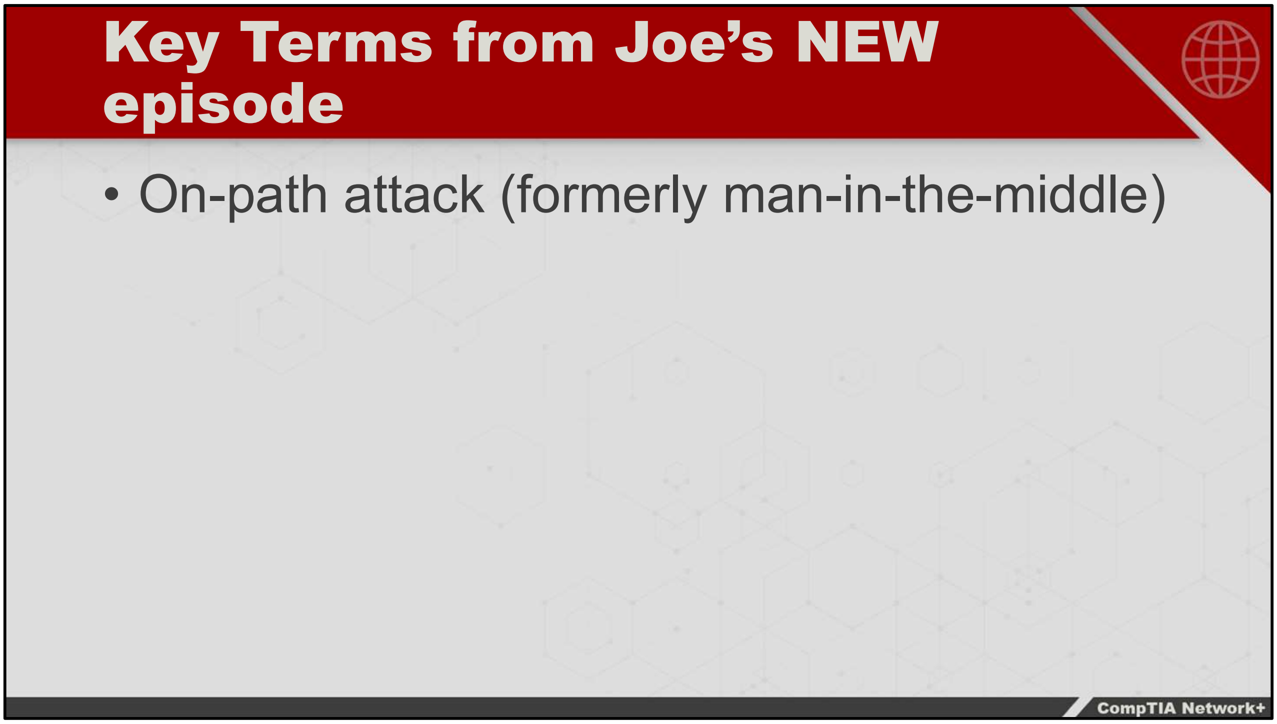


Episode 19.05

Episode title: **On-Path and Spoofing Attacks**

Objective: **4.2 Compare and contrast common types of attacks**

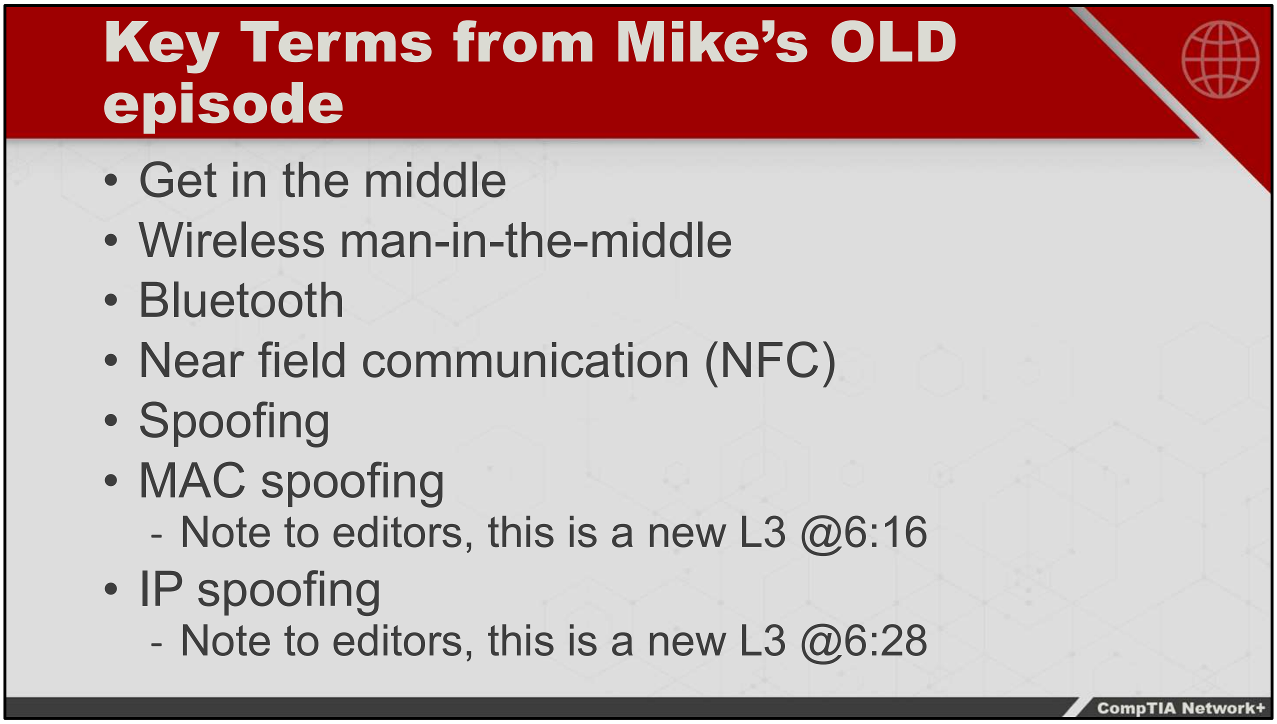
CompTIA Network+



Key Terms from Joe’s NEW episode

- On-path attack (formerly man-in-the-middle)

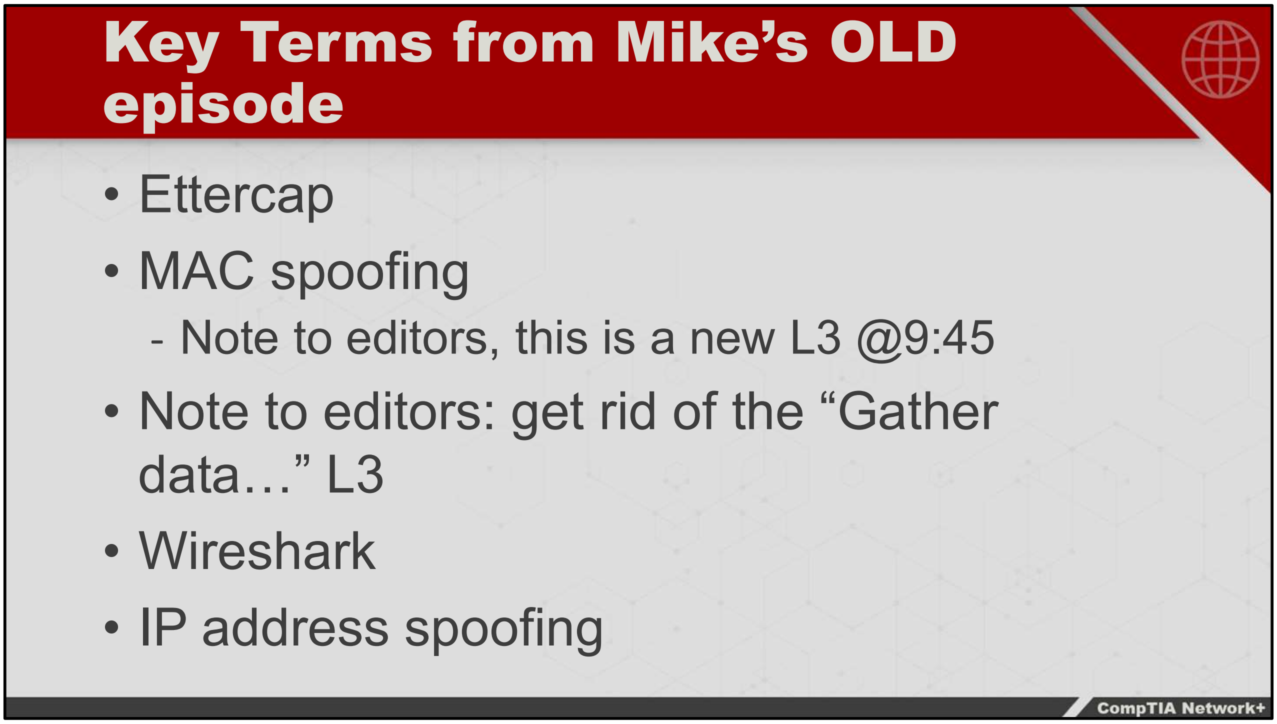
CompTIA Network+



Key Terms from Mike’s OLD episode

- Get in the middle
- Wireless man-in-the-middle
- Bluetooth
- Near field communication (NFC)
- Spoofing
- MAC spoofing
  - Note to editors, this is a new L3 @6:16
- IP spoofing
  - Note to editors, this is a new L3 @6:28

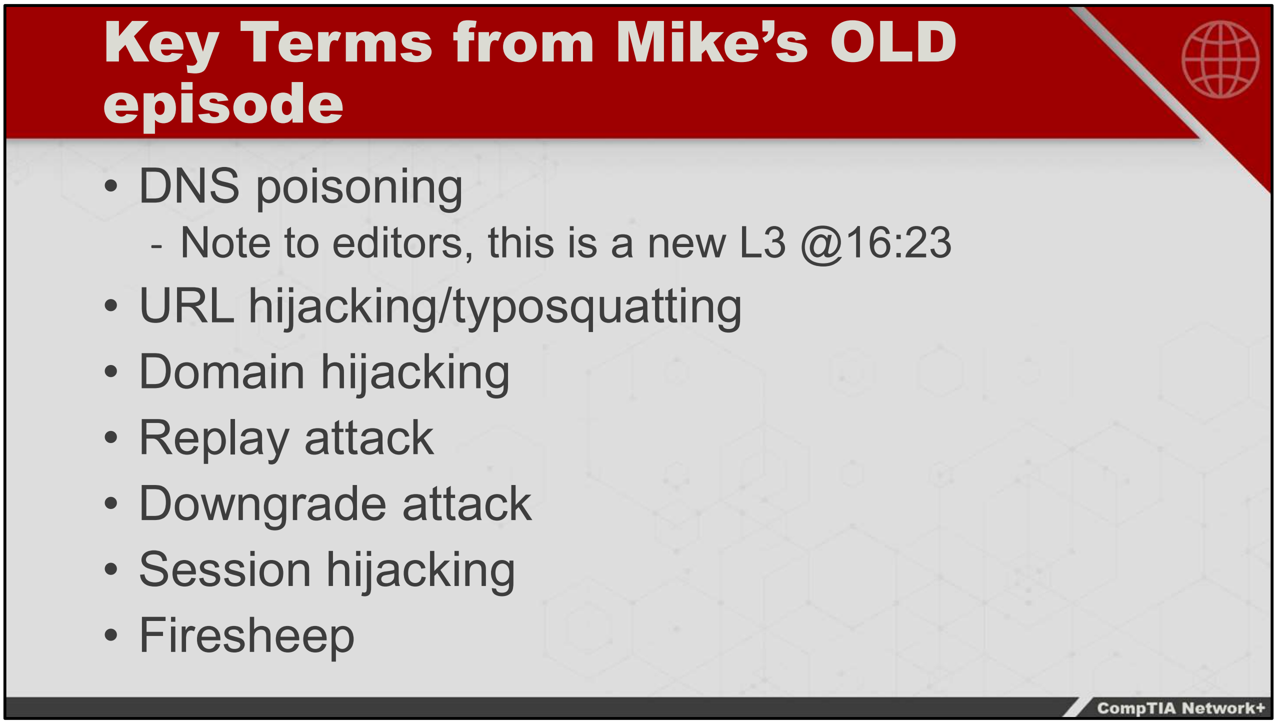
CompTIA Network+



Key Terms from Mike’s OLD episode

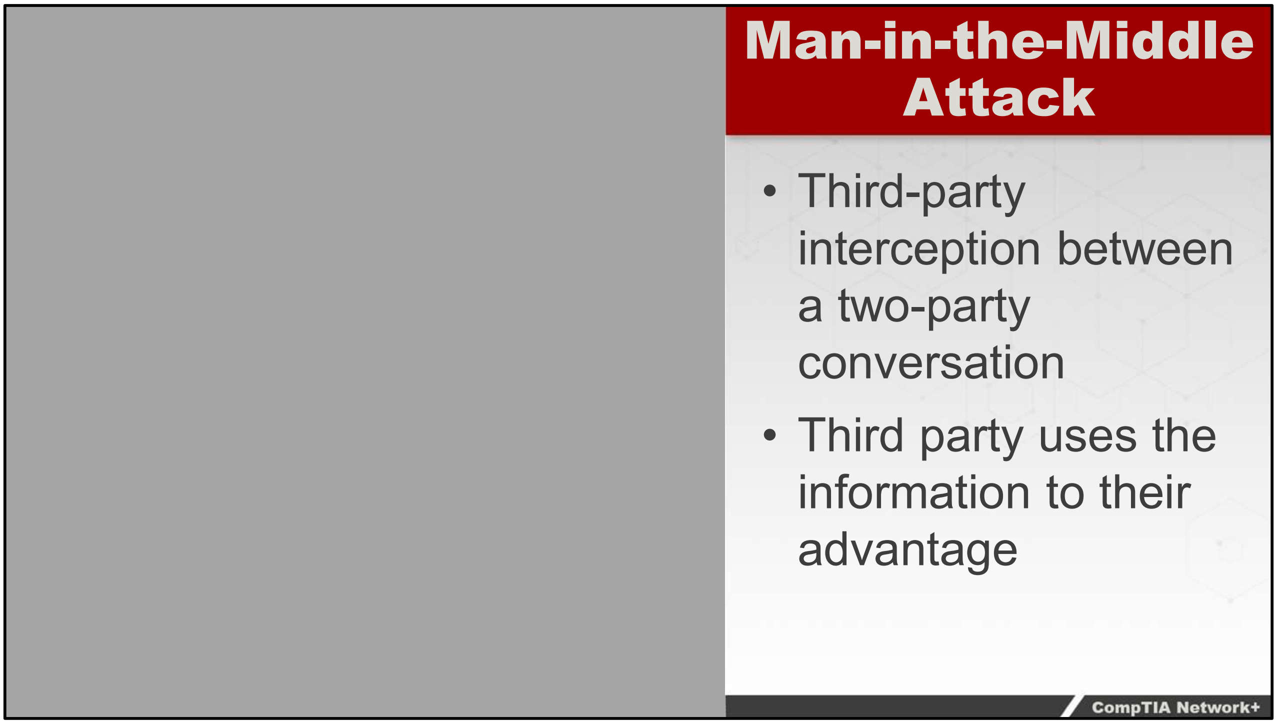
- Ettercap
- MAC spoofing
  - Note to editors, this is a new L3 @9:45
- Note to editors: get rid of the “Gather data…” L3
- Wireshark
- IP address spoofing

CompTIA Network+



Key Terms from Mike's OLD episode

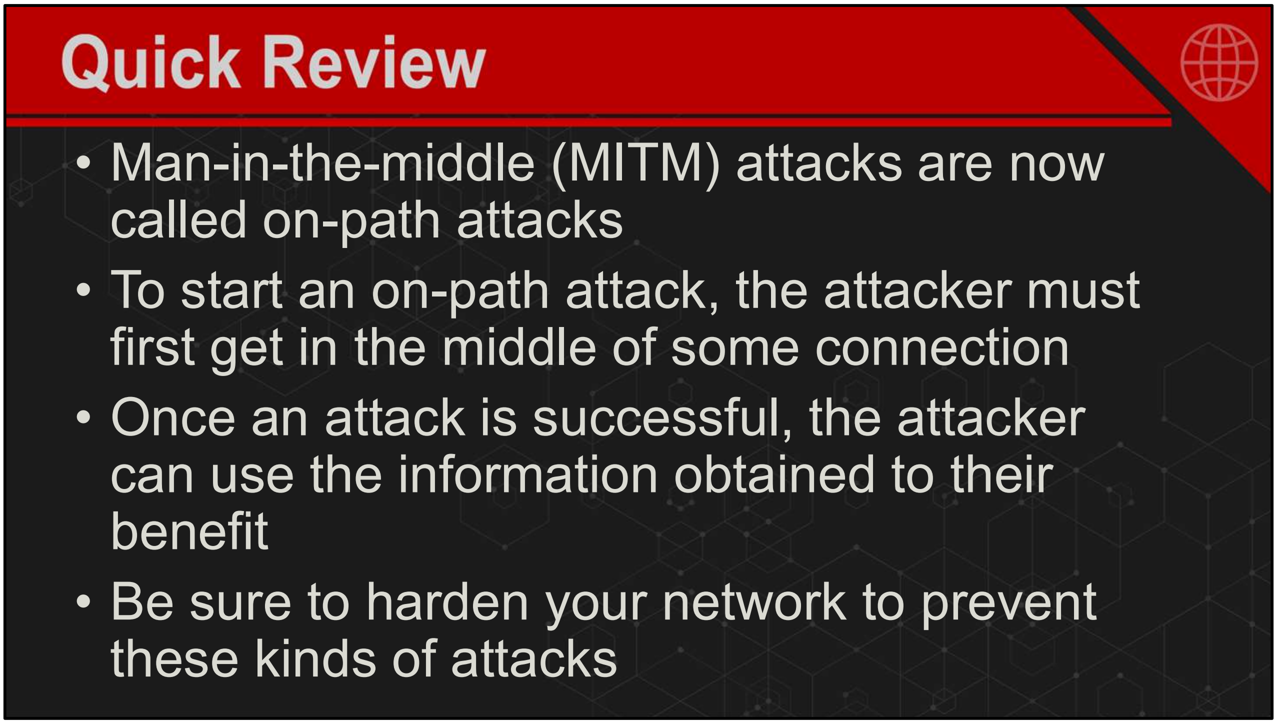
- DNS poisoning
  - Note to editors, this is a new L3 @16:23
- URL hijacking/typosquatting
- Domain hijacking
- Replay attack
- Downgrade attack
- Session hijacking
- Firesheep



Man-in-the-Middle Attack

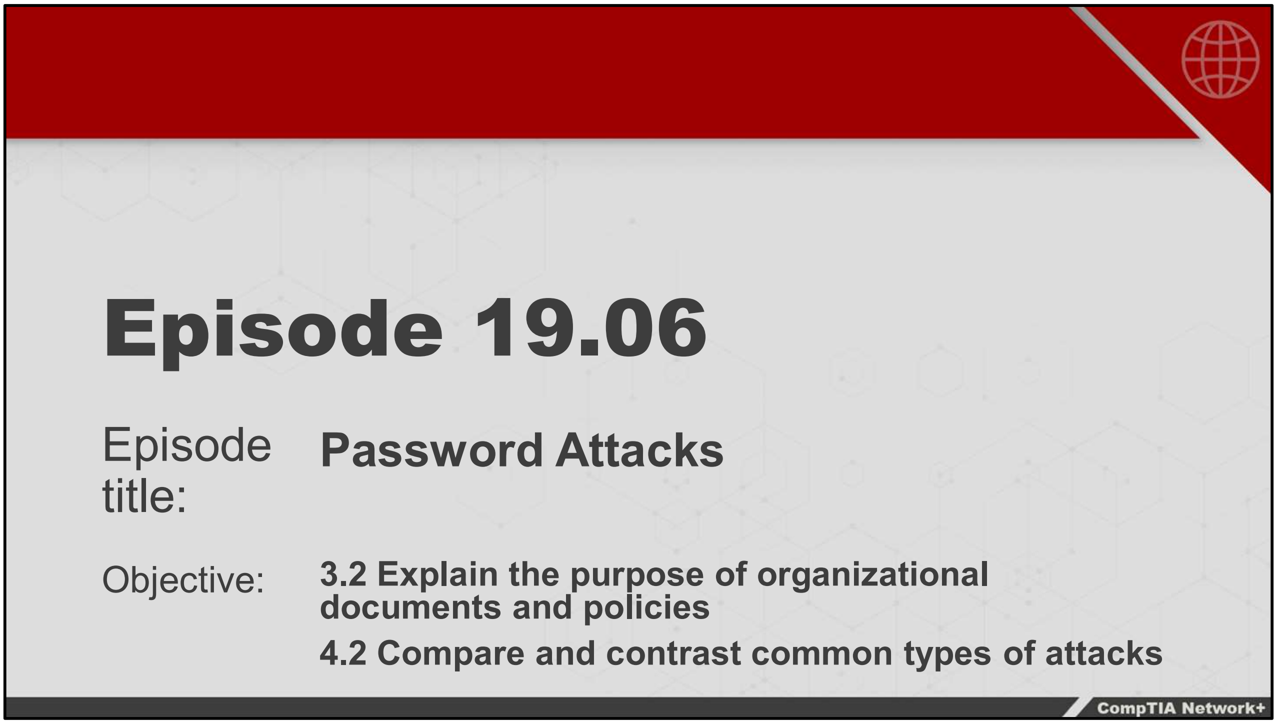
- Third-party interception between a two-party conversation
- Third party uses the information to their advantage

CompTIA Network+



Quick Review

- Man-in-the-middle (MITM) attacks are now called on-path attacks
- To start an on-path attack, the attacker must first get in the middle of some connection
- Once an attack is successful, the attacker can use the information obtained to their benefit
- Be sure to harden your network to prevent these kinds of attacks



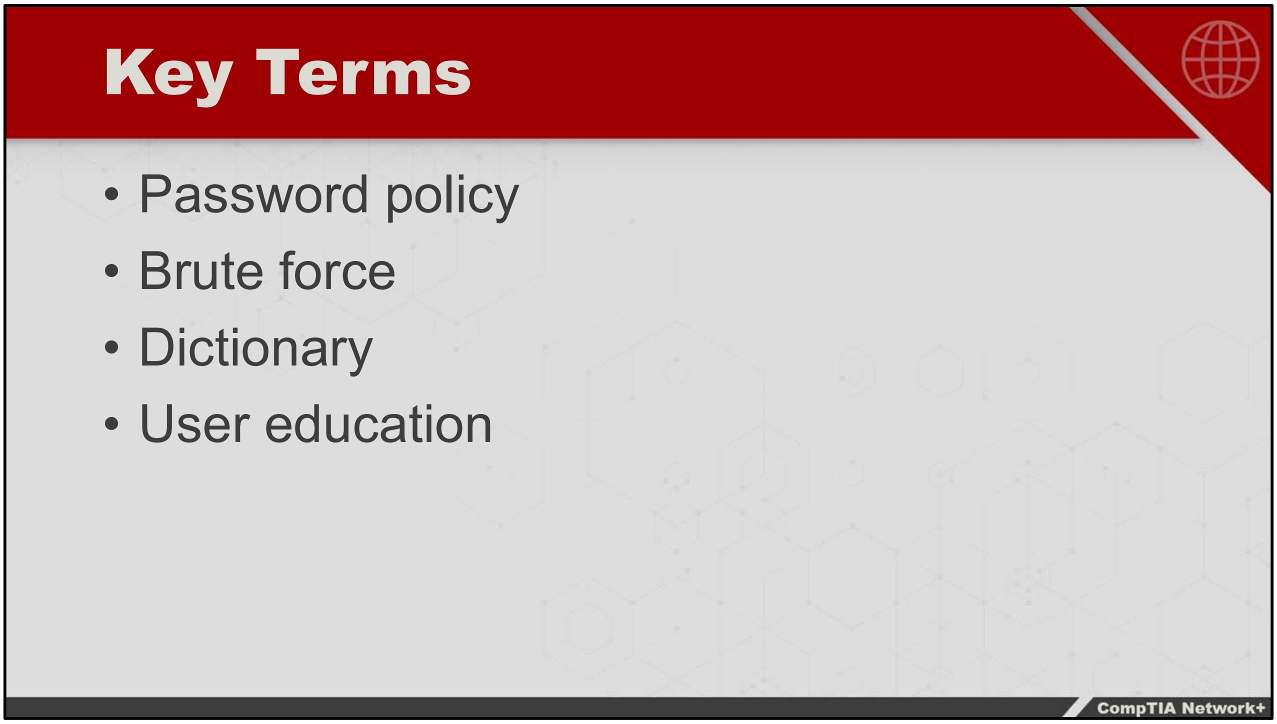
Episode 19.06

Episode title: **Password Attacks**

Objective: **3.2 Explain the purpose of organizational documents and policies**

4.2 Compare and contrast common types of attacks

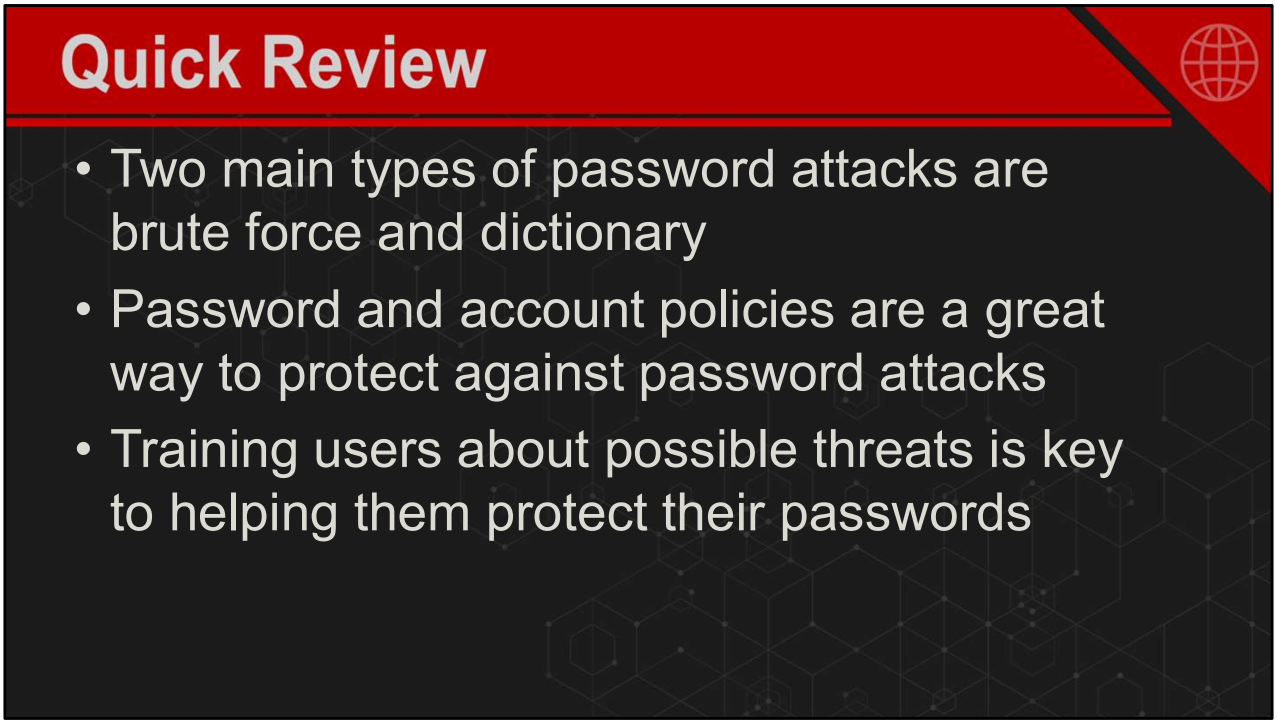
CompTIA Network+



Key Terms

- Password policy
- Brute force
- Dictionary
- User education

CompTIA Network+



Quick Review

- Two main types of password attacks are brute force and dictionary
- Password and account policies are a great way to protect against password attacks
- Training users about possible threats is key to helping them protect their passwords

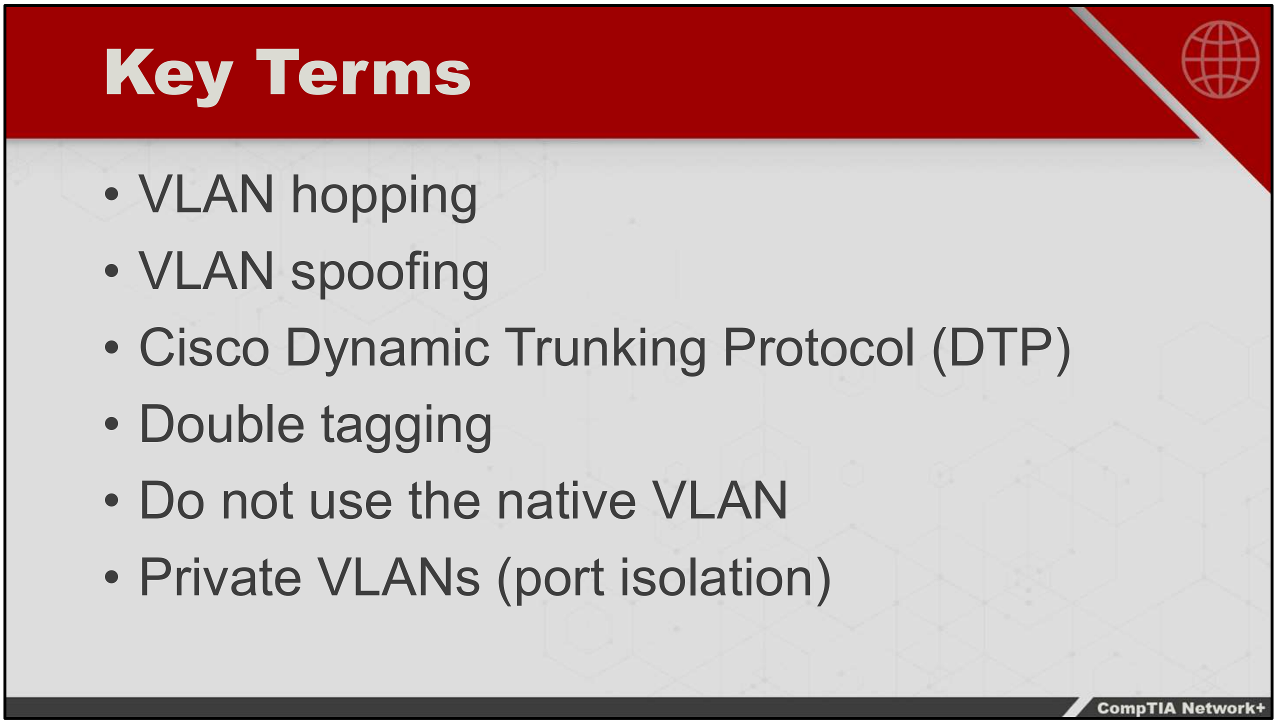
Episode 19.07

Episode title: **VLAN Hopping**

Objective: **2.3 Given a scenario, configure and deploy common Ethernet switching features**

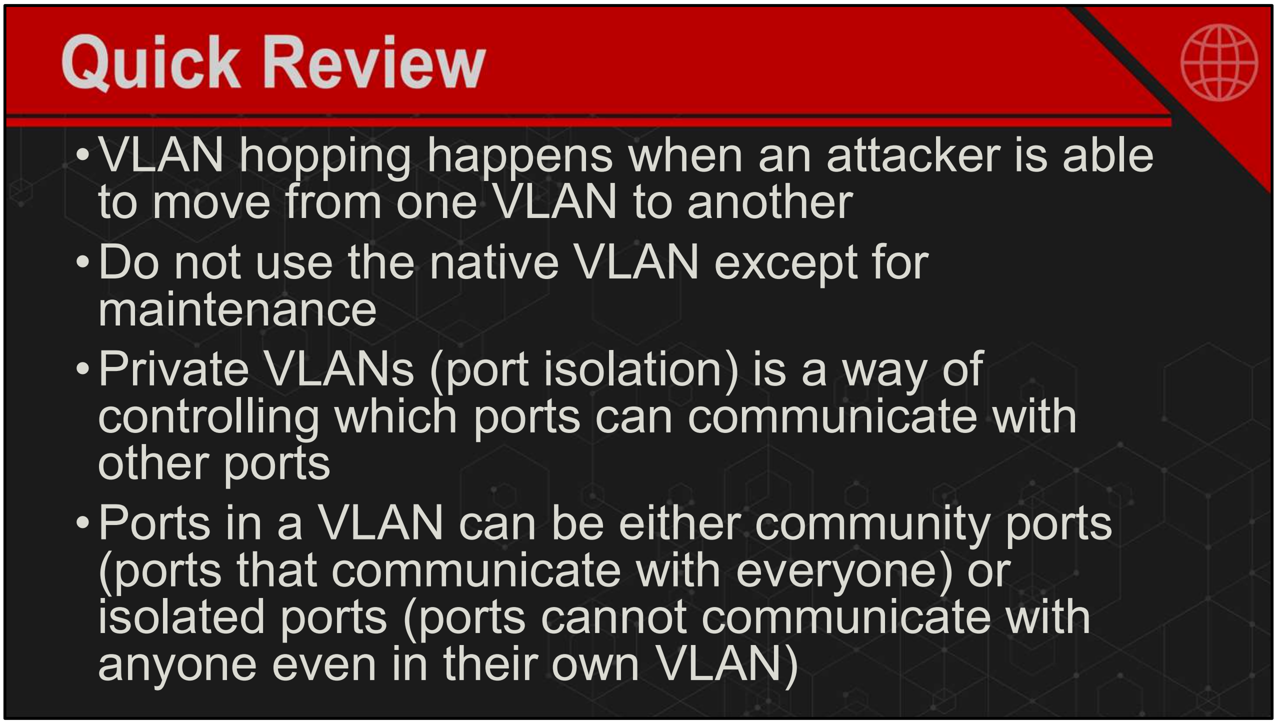
4.2 Compare and contrast common types of attacks

CompTIA Network+



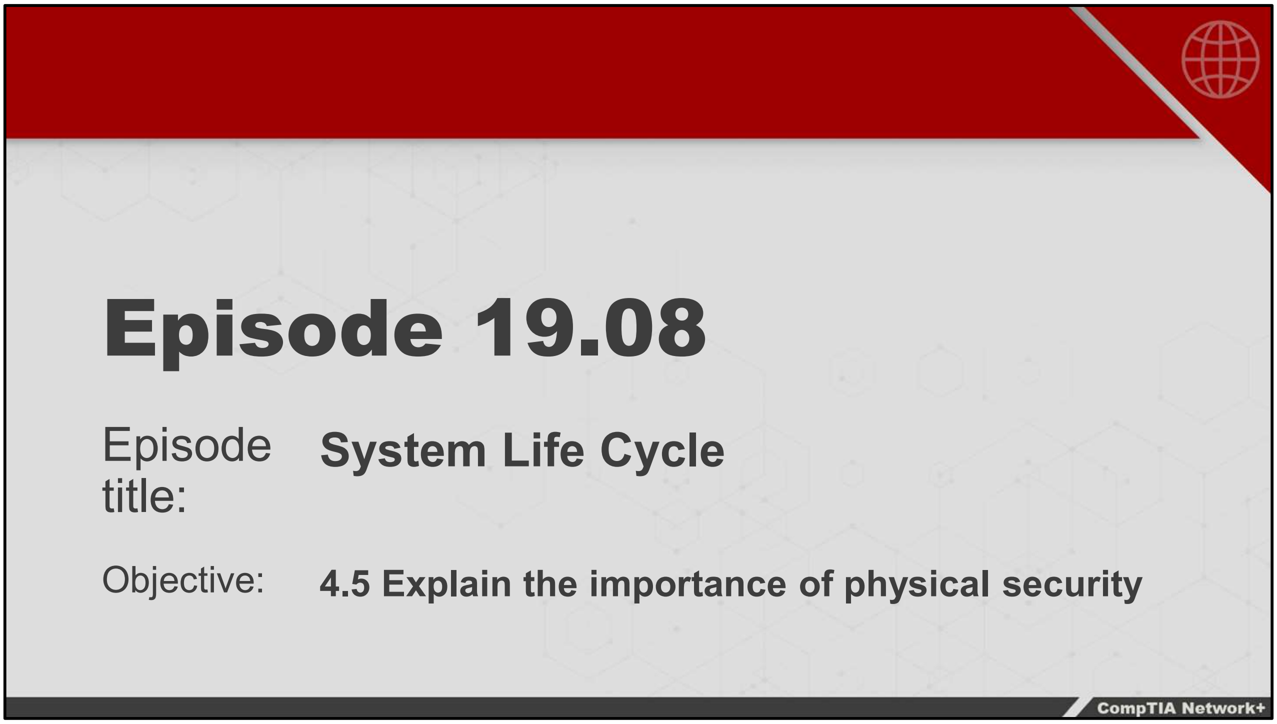
Key Terms

- VLAN hopping
- VLAN spoofing
- Cisco Dynamic Trunking Protocol (DTP)
- Double tagging
- Do not use the native VLAN
- Private VLANs (port isolation)



Quick Review

- VLAN hopping happens when an attacker is able to move from one VLAN to another
- Do not use the native VLAN except for maintenance
- Private VLANs (port isolation) is a way of controlling which ports can communicate with other ports
- Ports in a VLAN can be either community ports (ports that communicate with everyone) or isolated ports (ports cannot communicate with anyone even in their own VLAN)

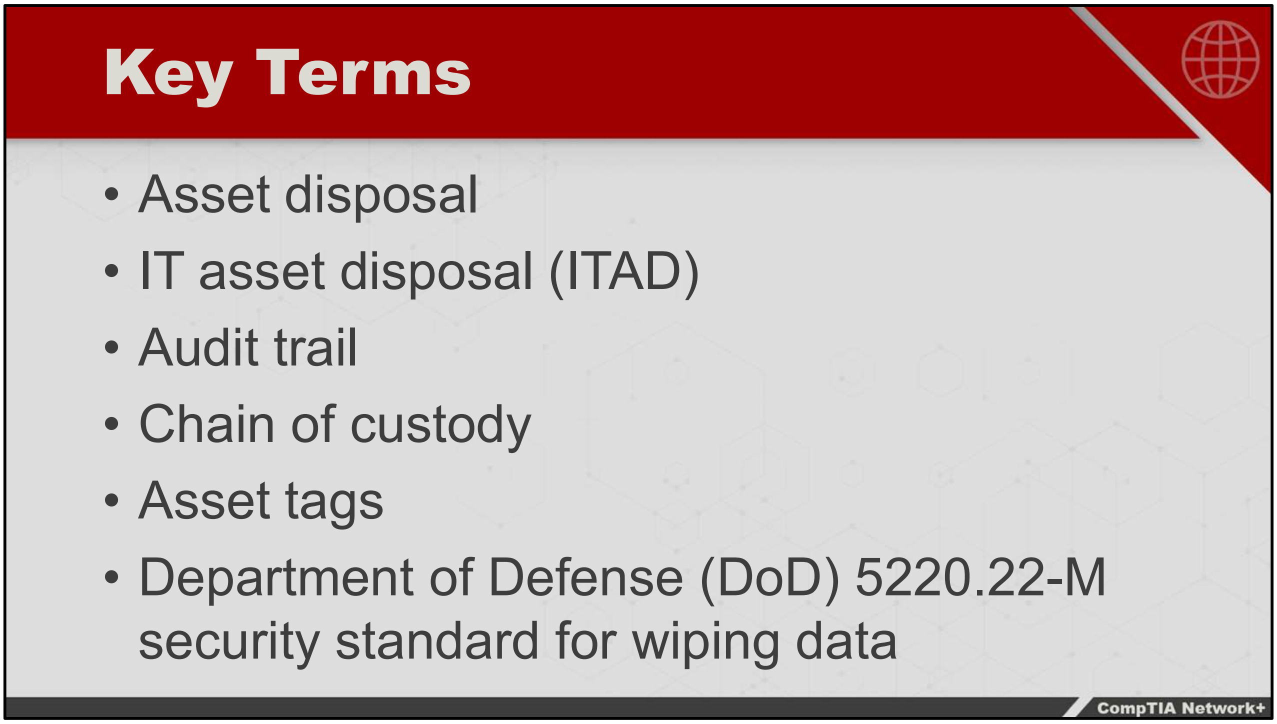


Episode 19.08

Episode title: **System Life Cycle**

Objective: **4.5 Explain the importance of physical security**

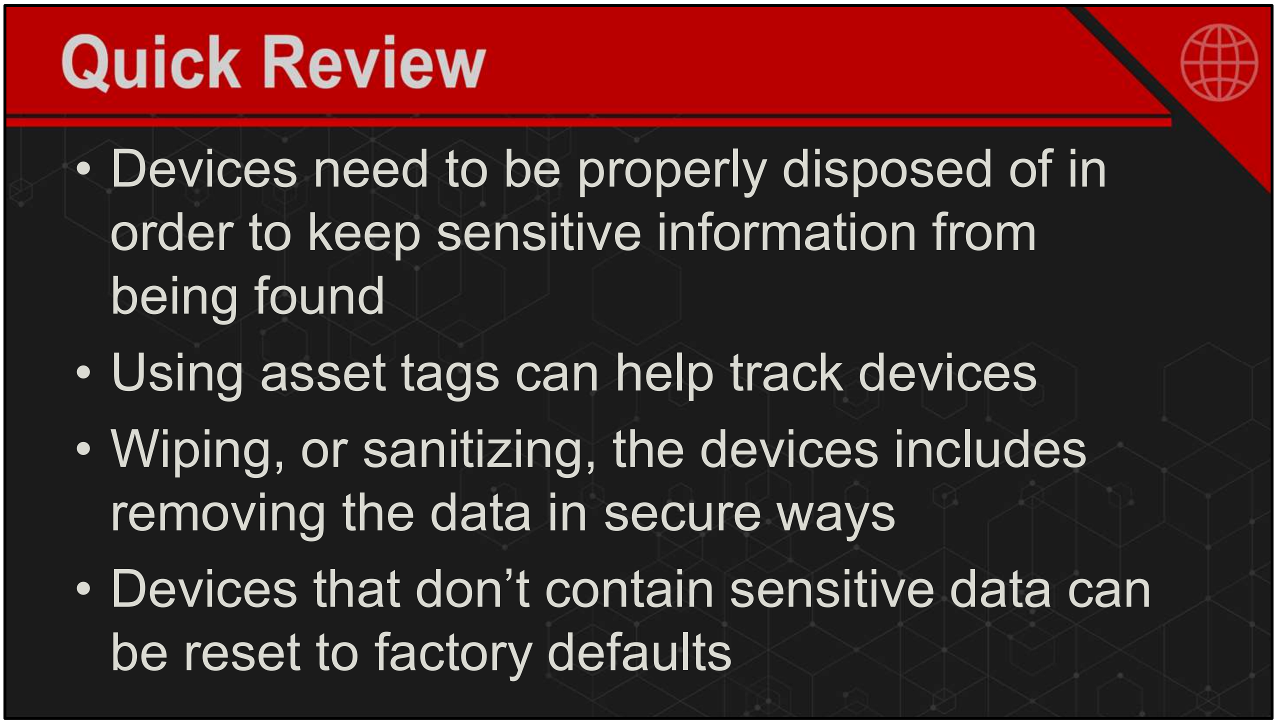
CompTIA Network+



Key Terms

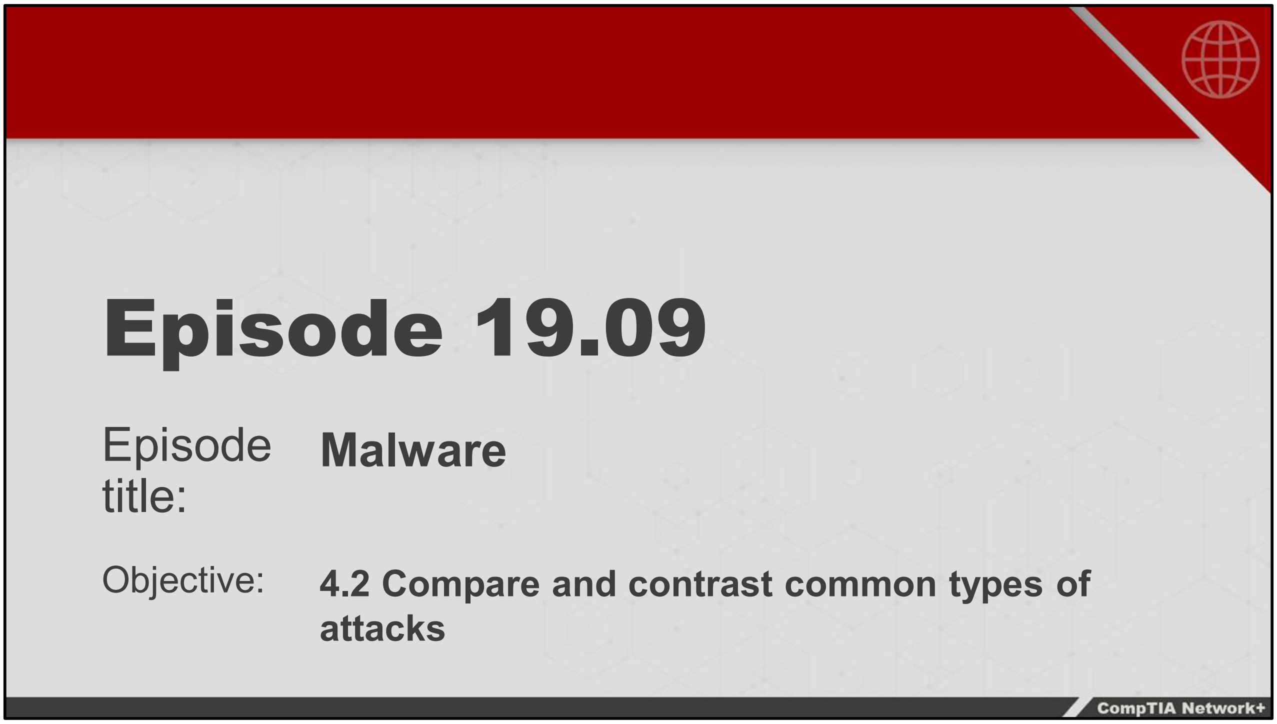
- Asset disposal
- IT asset disposal (ITAD)
- Audit trail
- Chain of custody
- Asset tags
- Department of Defense (DoD) 5220.22-M security standard for wiping data

CompTIA Network+



Quick Review

- Devices need to be properly disposed of in order to keep sensitive information from being found
- Using asset tags can help track devices
- Wiping, or sanitizing, the devices includes removing the data in secure ways
- Devices that don’t contain sensitive data can be reset to factory defaults

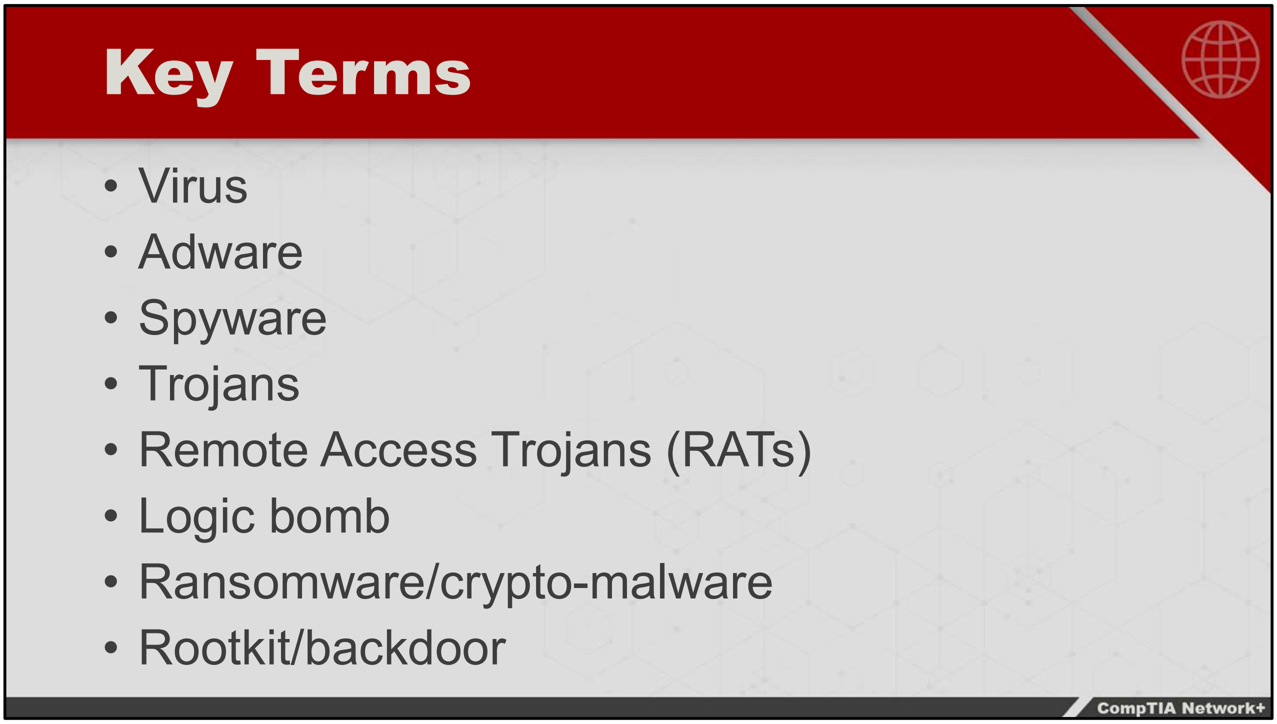


Episode 19.09

Episode title: **Malware**

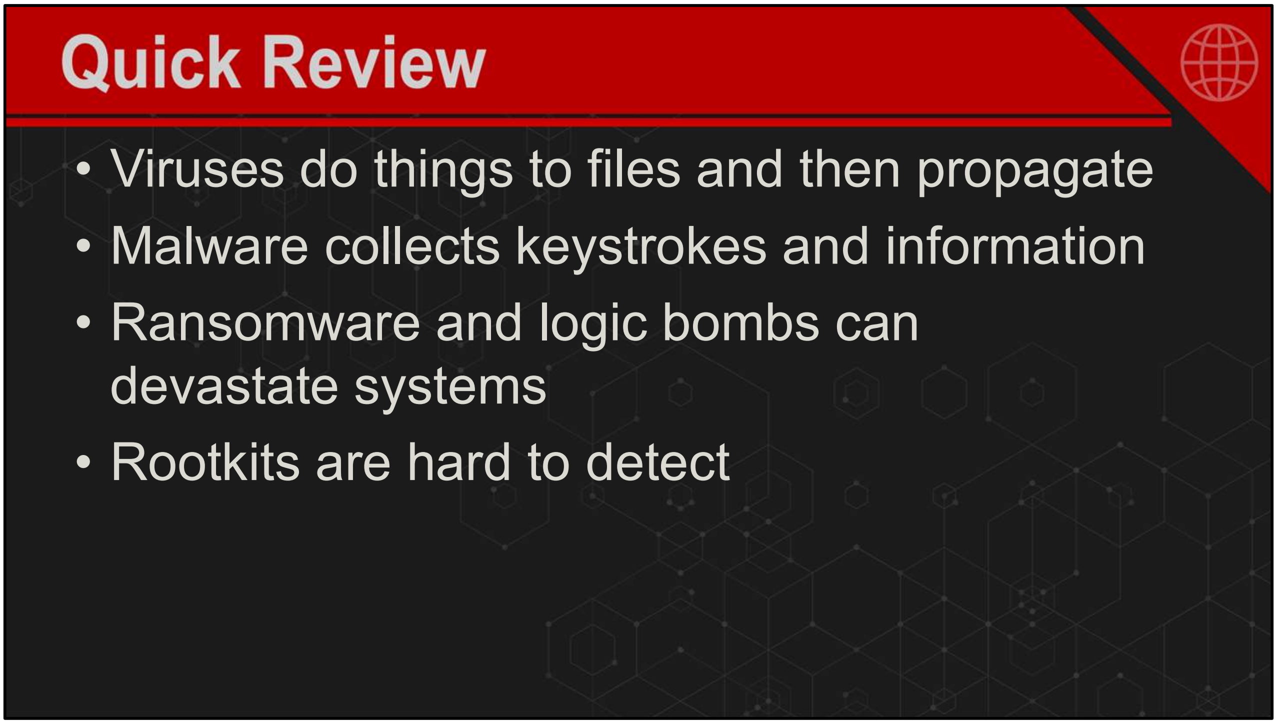
Objective: **4.2 Compare and contrast common types of attacks**

CompTIA Network+



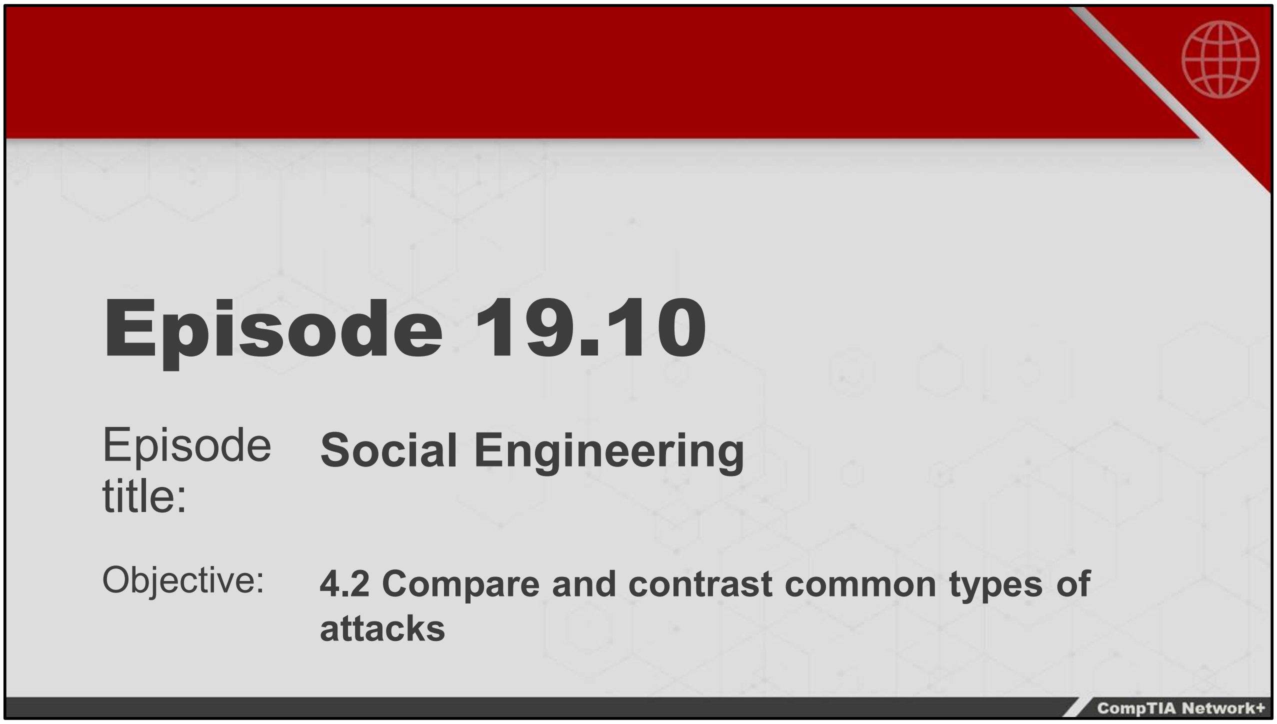
Key Terms

- Virus
- Adware
- Spyware
- Trojans
- Remote Access Trojans (RATs)
- Logic bomb
- Ransomware/crypto-malware
- Rootkit/backdoor



Quick Review

- Viruses do things to files and then propagate
- Malware collects keystrokes and information
- Ransomware and logic bombs can devastate systems
- Rootkits are hard to detect

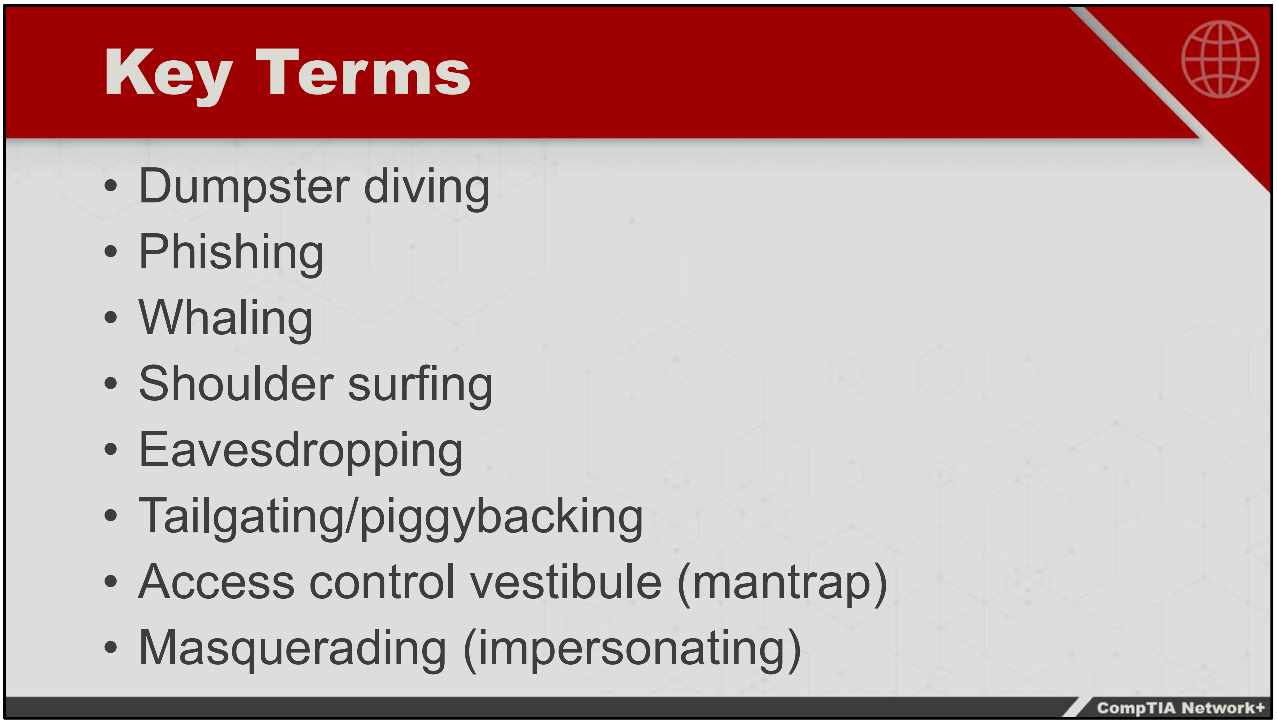


Episode 19.10

Episode title: **Social Engineering**

Objective: **4.2 Compare and contrast common types of attacks**

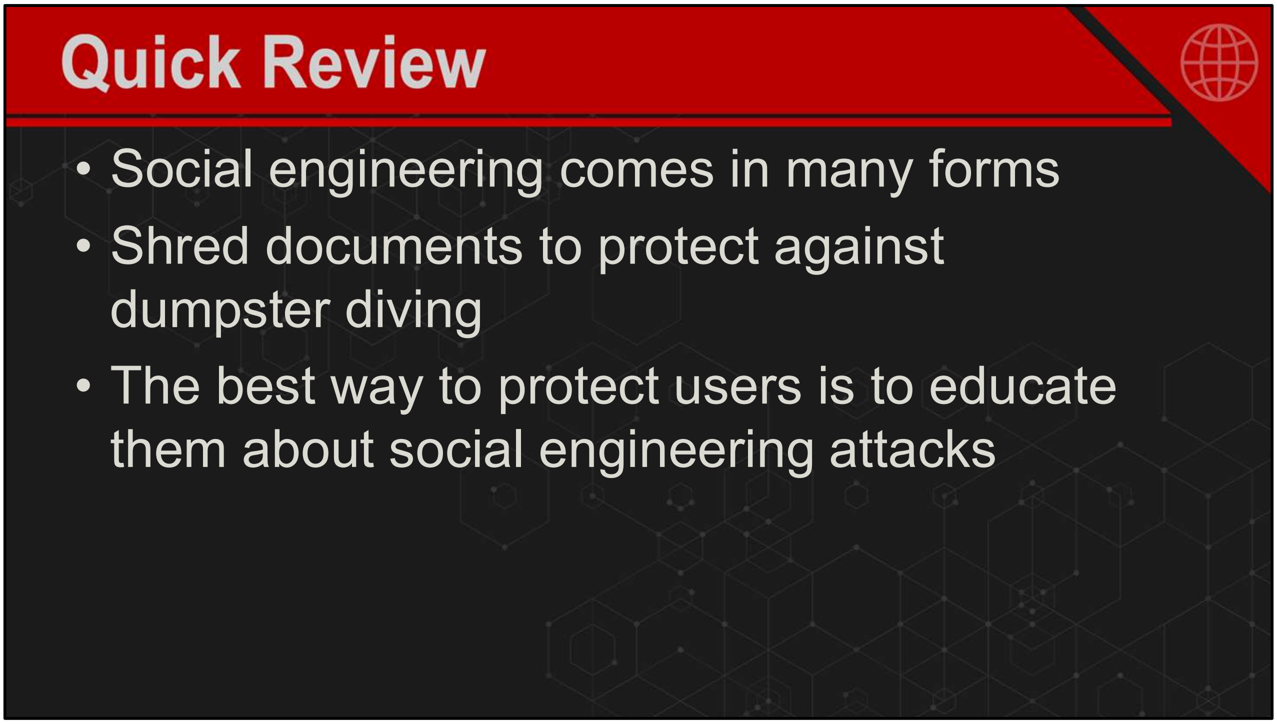
CompTIA Network+



Key Terms

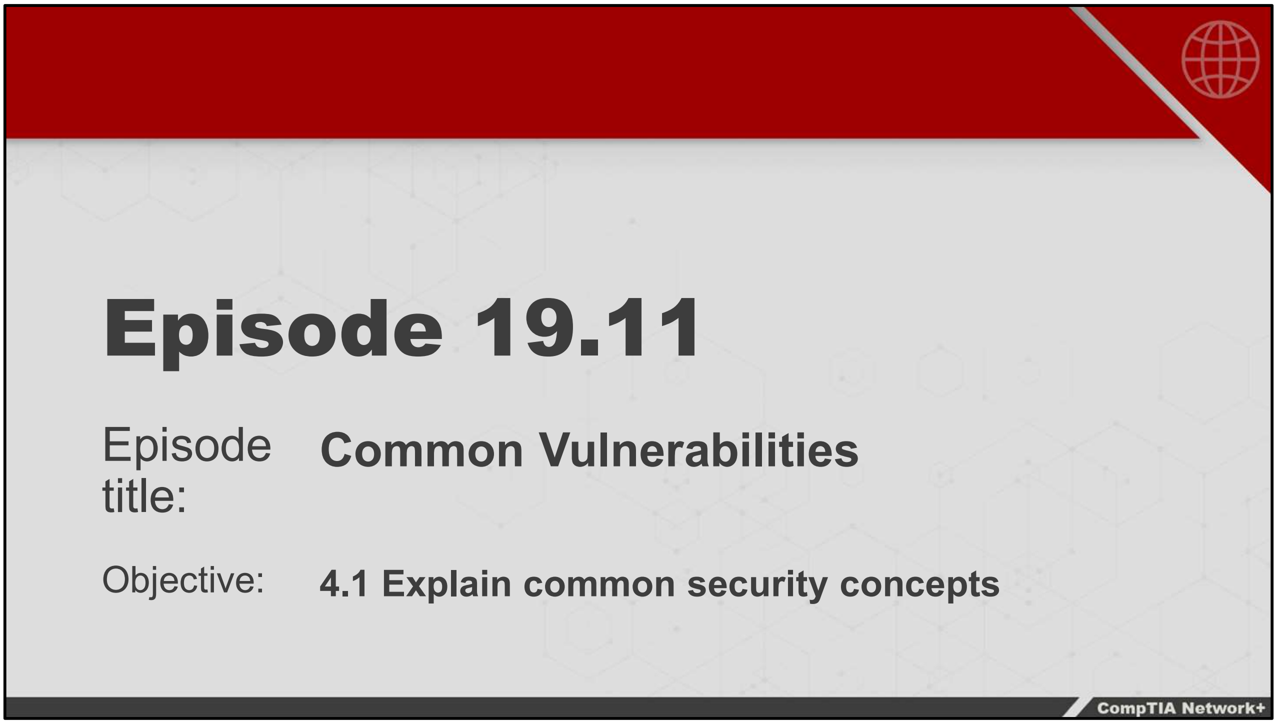
- Dumpster diving
- Phishing
- Whaling
- Shoulder surfing
- Eavesdropping
- Tailgating/piggybacking
- Access control vestibule (mantrap)
- Masquerading (impersonating)

CompTIA Network+



Quick Review

- Social engineering comes in many forms
- Shred documents to protect against dumpster diving
- The best way to protect users is to educate them about social engineering attacks

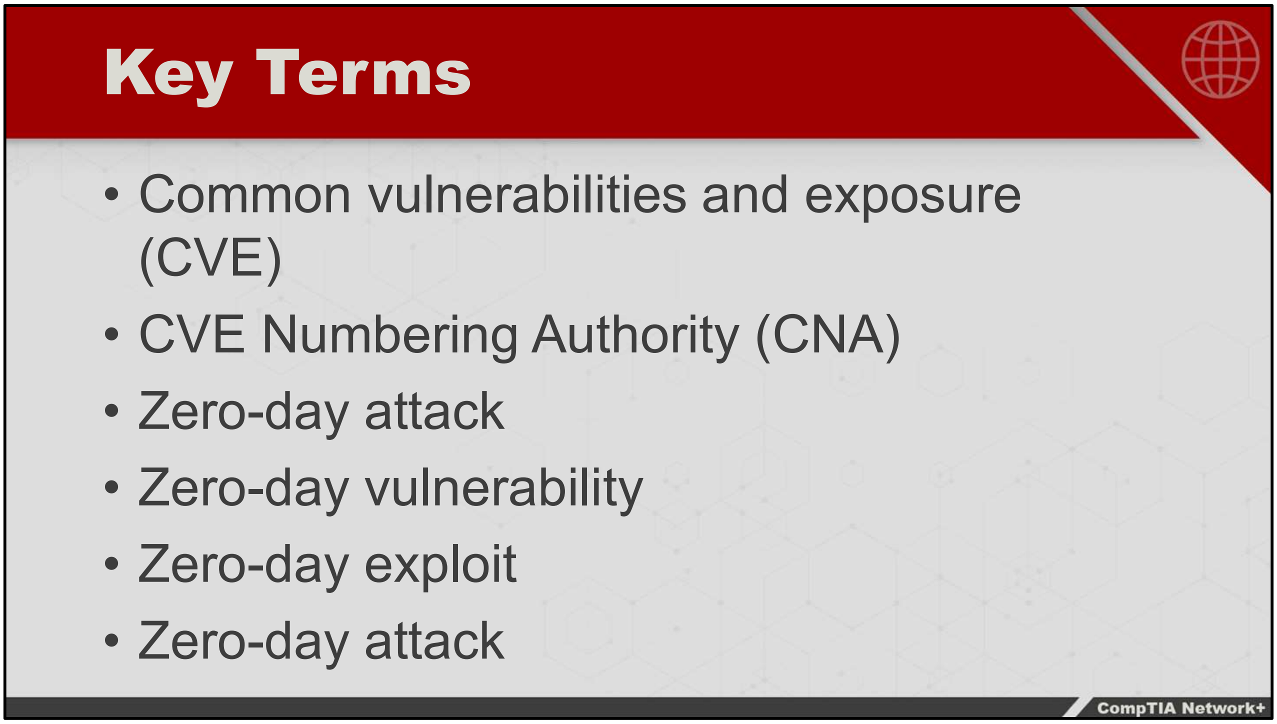


Episode 19.11

Episode title: **Common Vulnerabilities**

Objective: **4.1 Explain common security concepts**

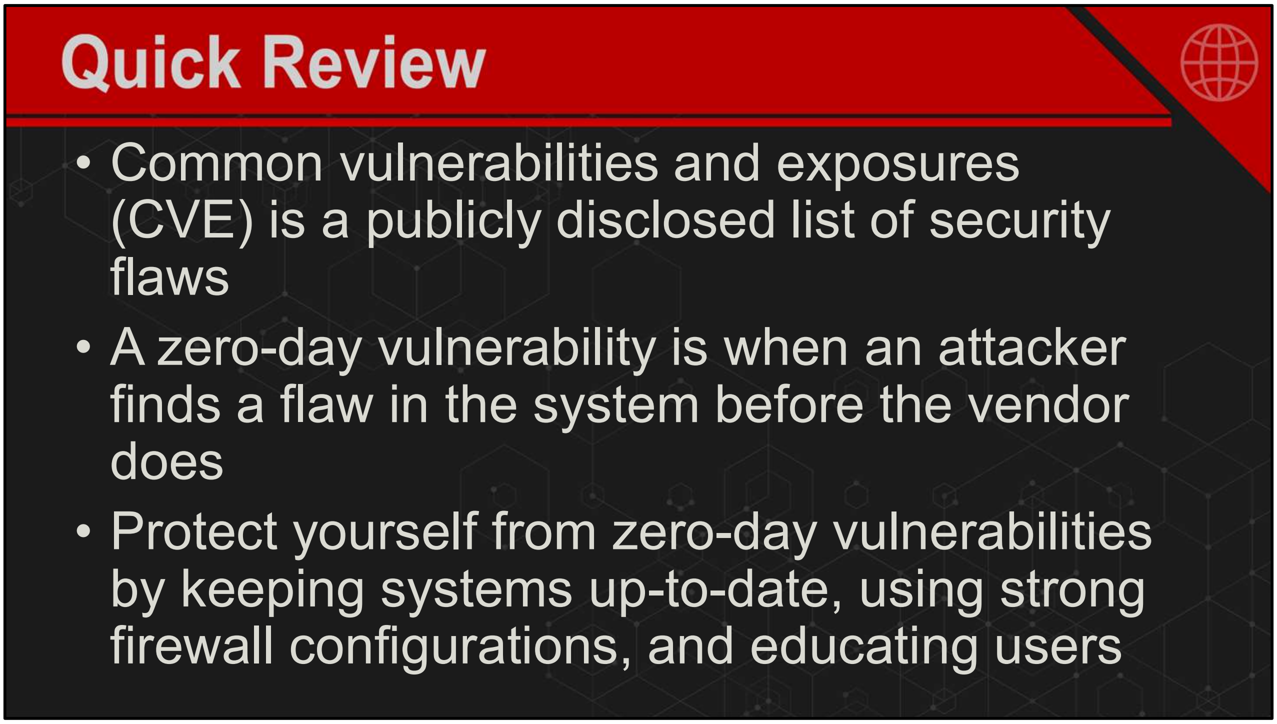
CompTIA Network+



Key Terms

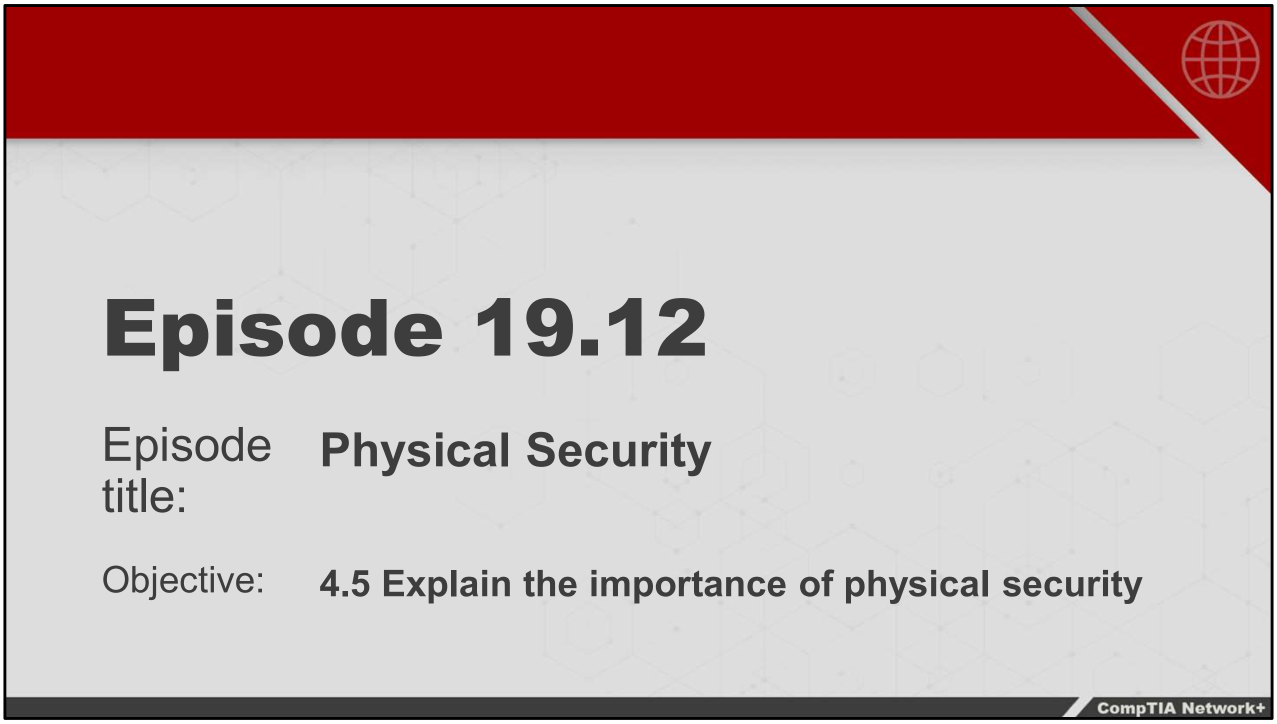
- Common vulnerabilities and exposure (CVE)
- CVE Numbering Authority (CNA)
- Zero-day attack
- Zero-day vulnerability
- Zero-day exploit
- Zero-day attack

CompTIA Network+



Quick Review

- Common vulnerabilities and exposures (CVE) is a publicly disclosed list of security flaws
- A zero-day vulnerability is when an attacker finds a flaw in the system before the vendor does
- Protect yourself from zero-day vulnerabilities by keeping systems up-to-date, using strong firewall configurations, and educating users

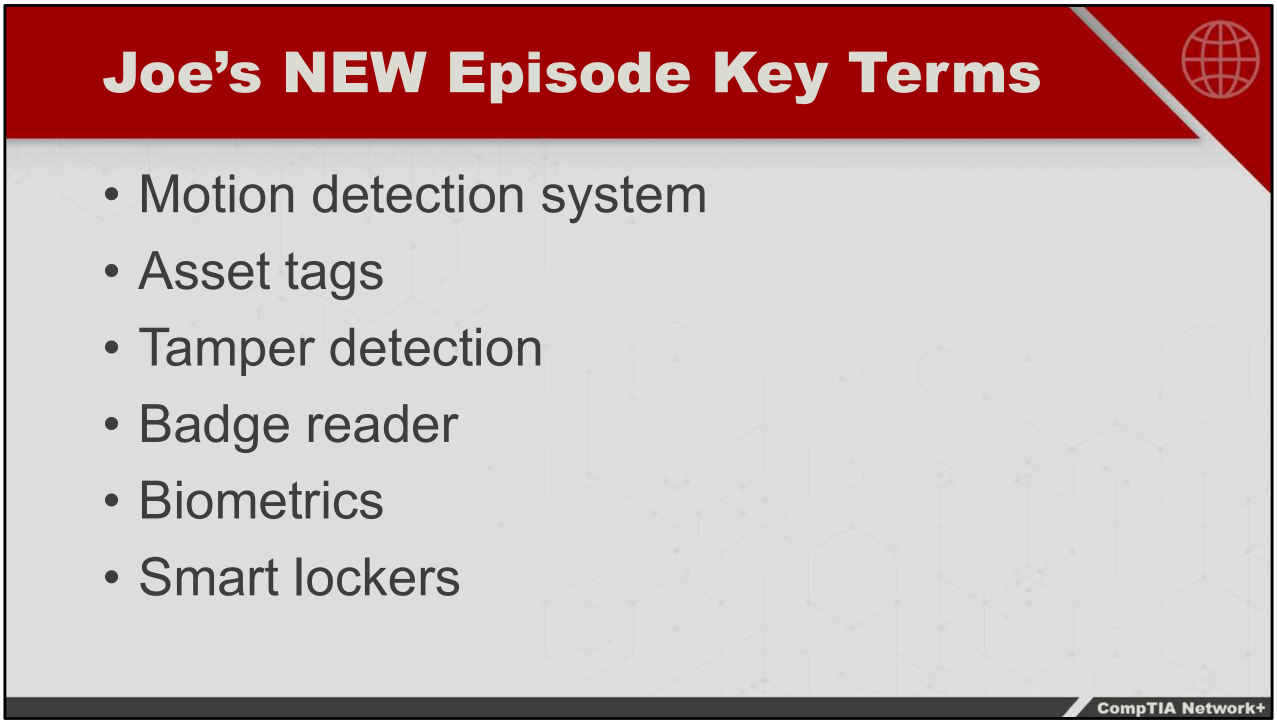


Episode 19.12

Episode title: **Physical Security**

Objective: **4.5 Explain the importance of physical security**

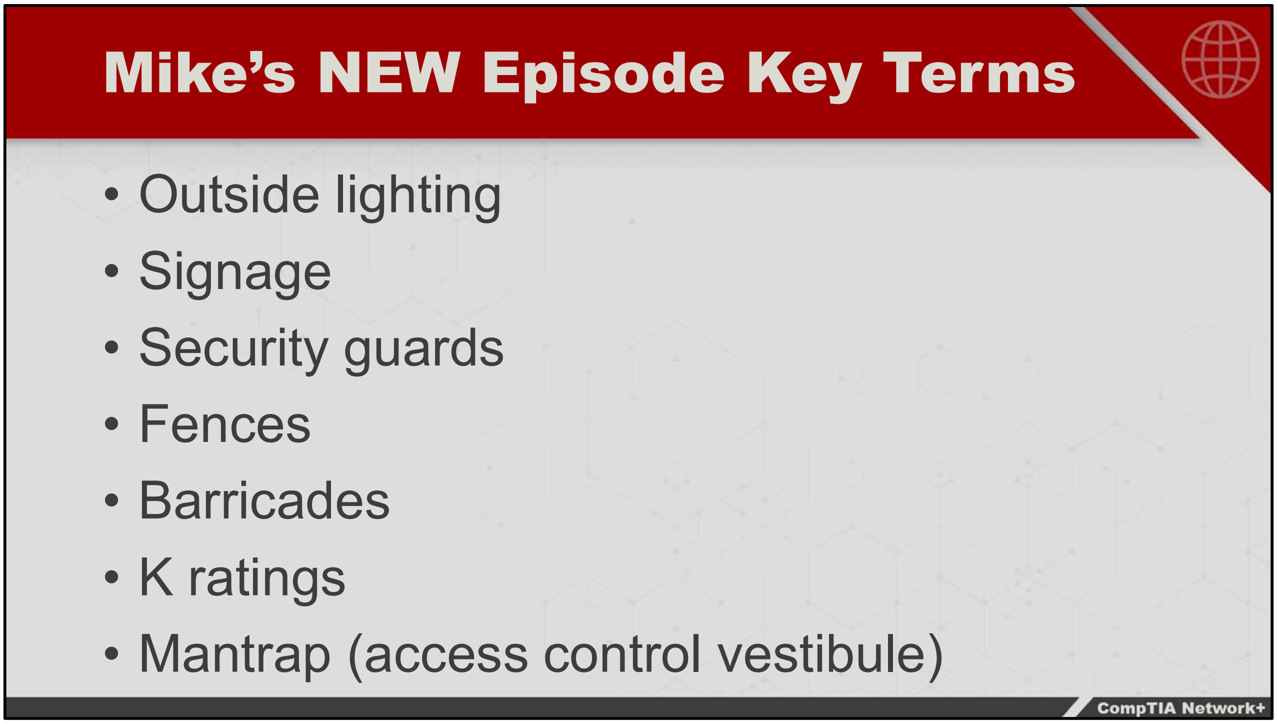
CompTIA Network+



Joe’s NEW Episode Key Terms

- Motion detection system
- Asset tags
- Tamper detection
- Badge reader
- Biometrics
- Smart lockers

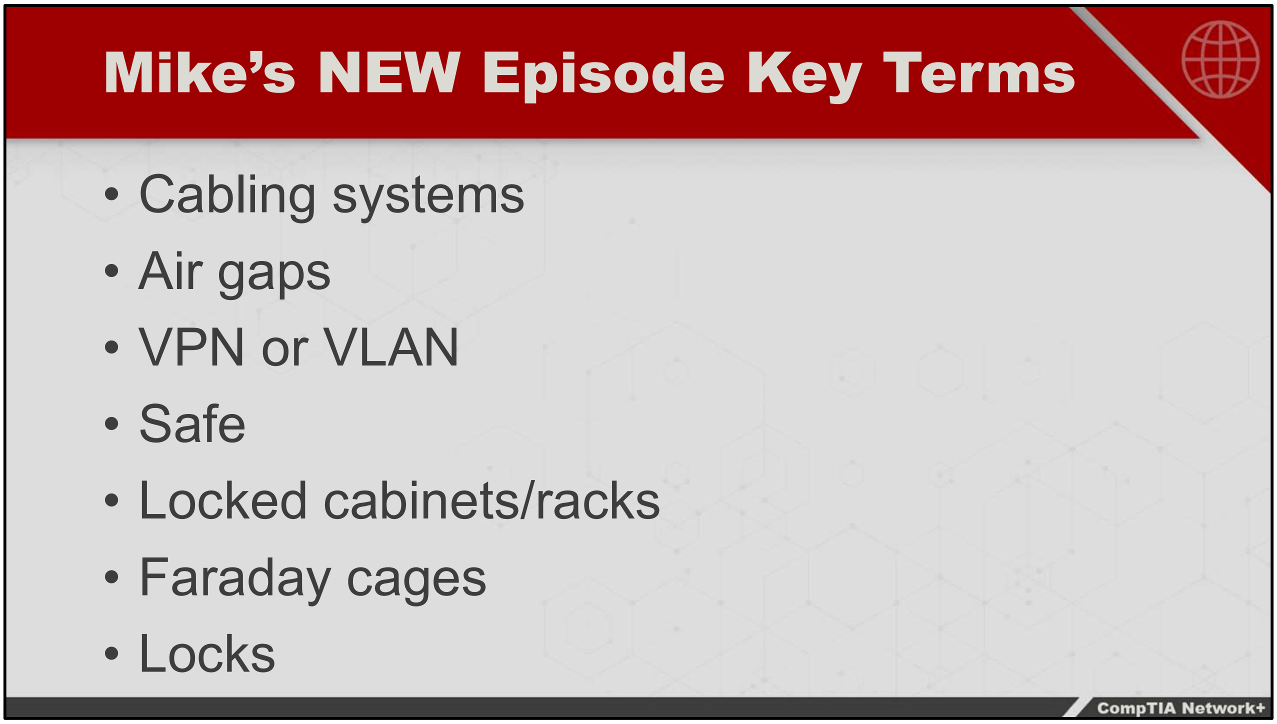
CompTIA Network+



Mike's NEW Episode Key Terms

- Outside lighting
- Signage
- Security guards
- Fences
- Barricades
- K ratings
- Mantrap (access control vestibule)

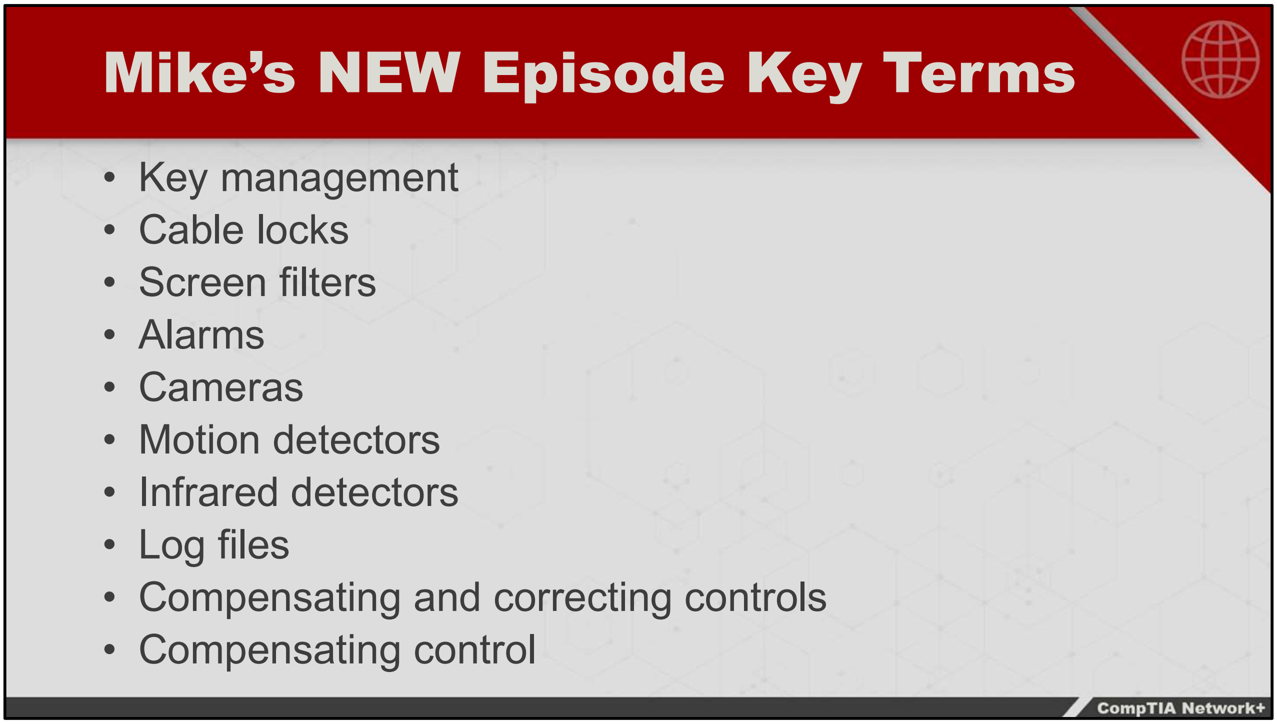
CompTIA Network+



Mike's NEW Episode Key Terms

- Cabling systems
- Air gaps
- VPN or VLAN
- Safe
- Locked cabinets/racks
- Faraday cages
- Locks

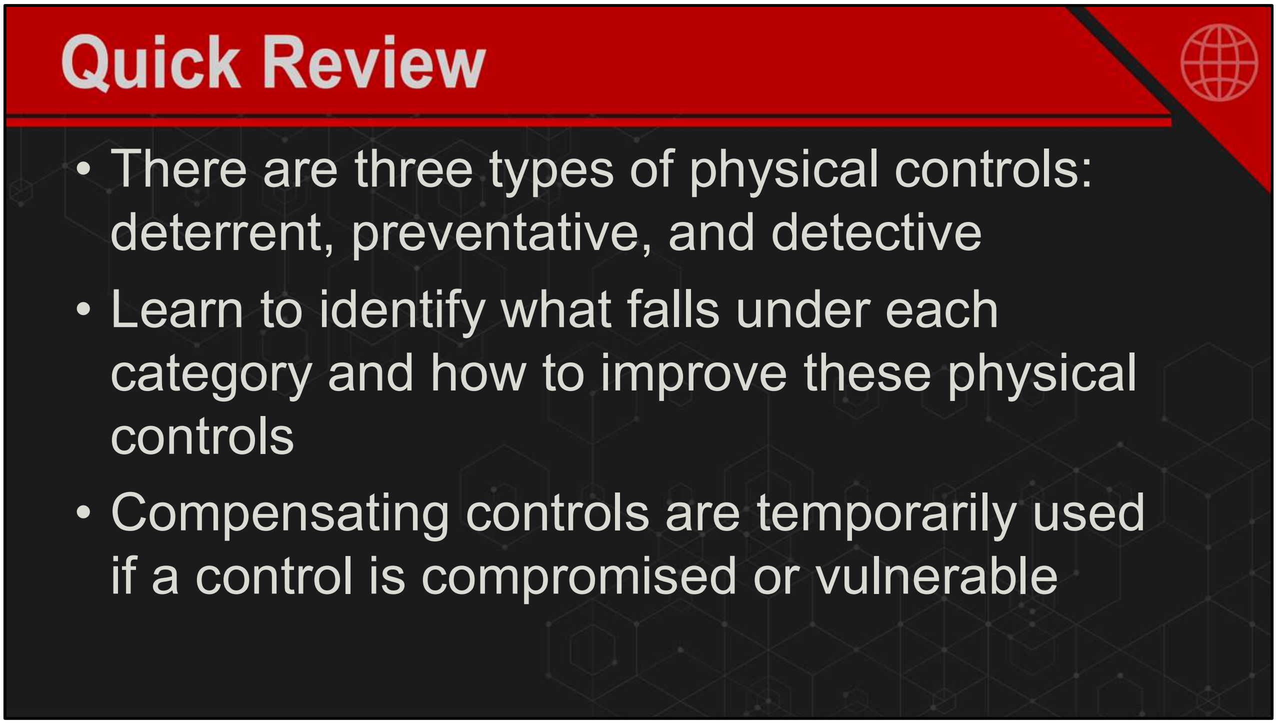
CompTIA Network+



Mike’s NEW Episode Key Terms

- Key management
- Cable locks
- Screen filters
- Alarms
- Cameras
- Motion detectors
- Infrared detectors
- Log files
- Compensating and correcting controls
- Compensating control

CompTIA Network+



Quick Review

- There are three types of physical controls: deterrent, preventative, and detective
- Learn to identify what falls under each category and how to improve these physical controls
- Compensating controls are temporarily used if a control is compromised or vulnerable

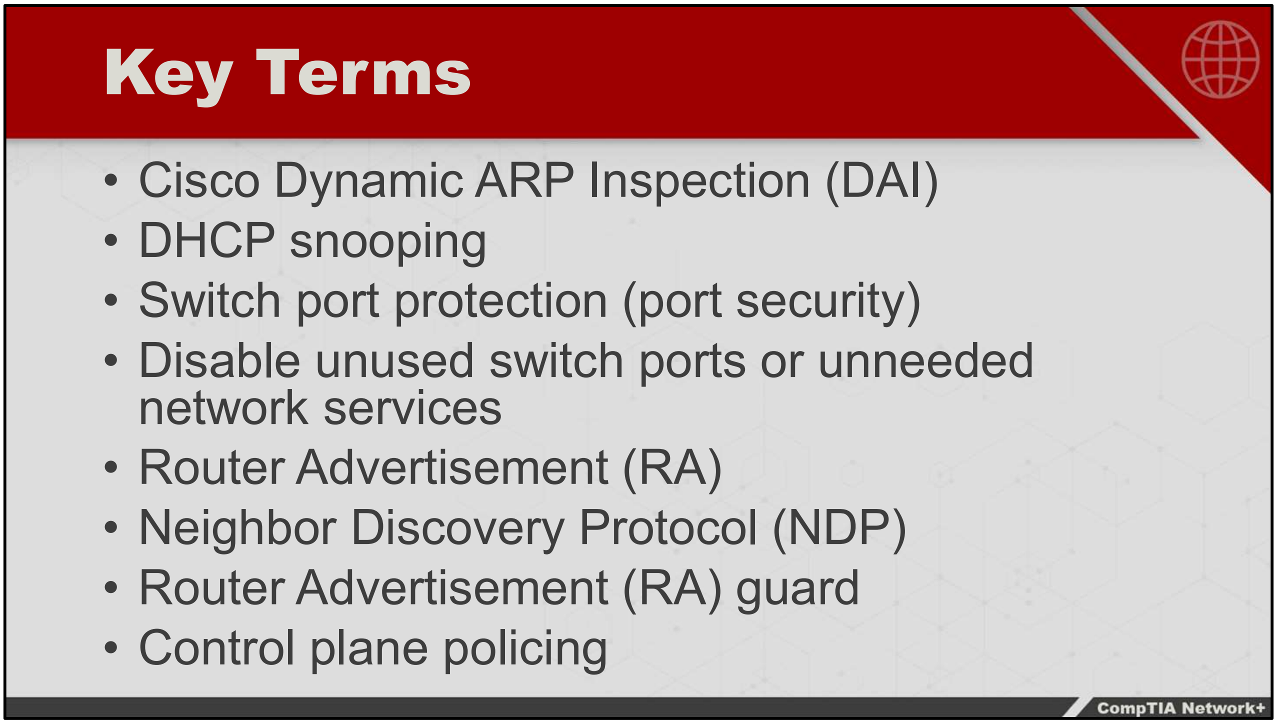
Episode 19.13

Episode title: **Network Hardening**

Objective: **2.3 Given a scenario, configure and deploy common Ethernet switching features**

4.3 Given a scenario, apply network hardening techniques

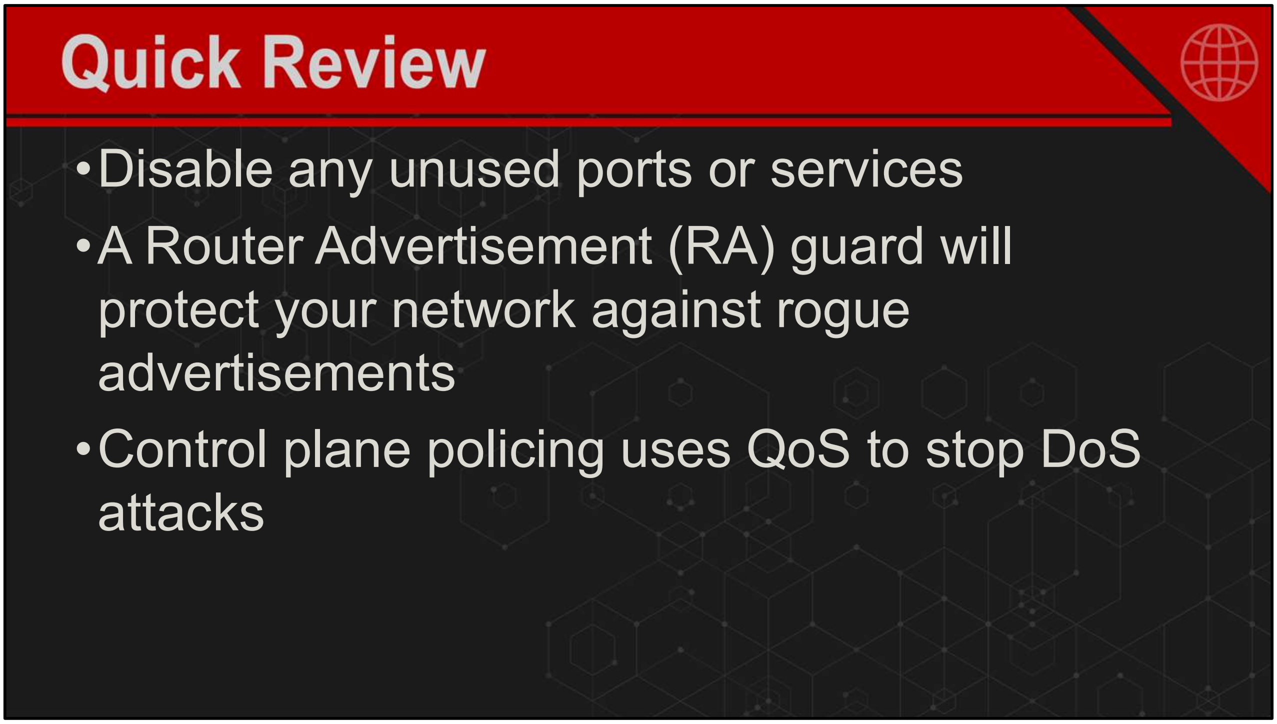
CompTIA Network+



Key Terms

- Cisco Dynamic ARP Inspection (DAI)
- DHCP snooping
- Switch port protection (port security)
- Disable unused switch ports or unneeded network services
- Router Advertisement (RA)
- Neighbor Discovery Protocol (NDP)
- Router Advertisement (RA) guard
- Control plane policing

CompTIA Network+



Quick Review

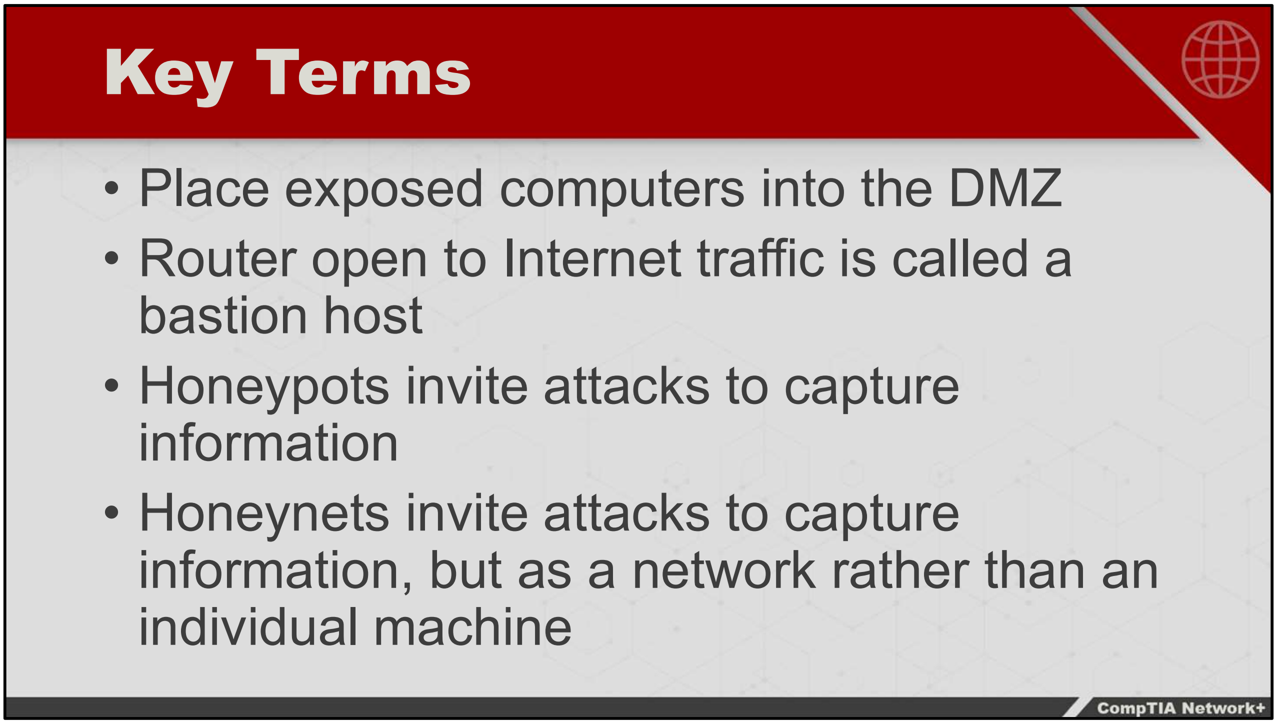
- Disable any unused ports or services
- A Router Advertisement (RA) guard will protect your network against rogue advertisements
- Control plane policing uses QoS to stop DoS attacks

Episode 19.14

Episode title: **Demilitarized Zone (DMZ)**

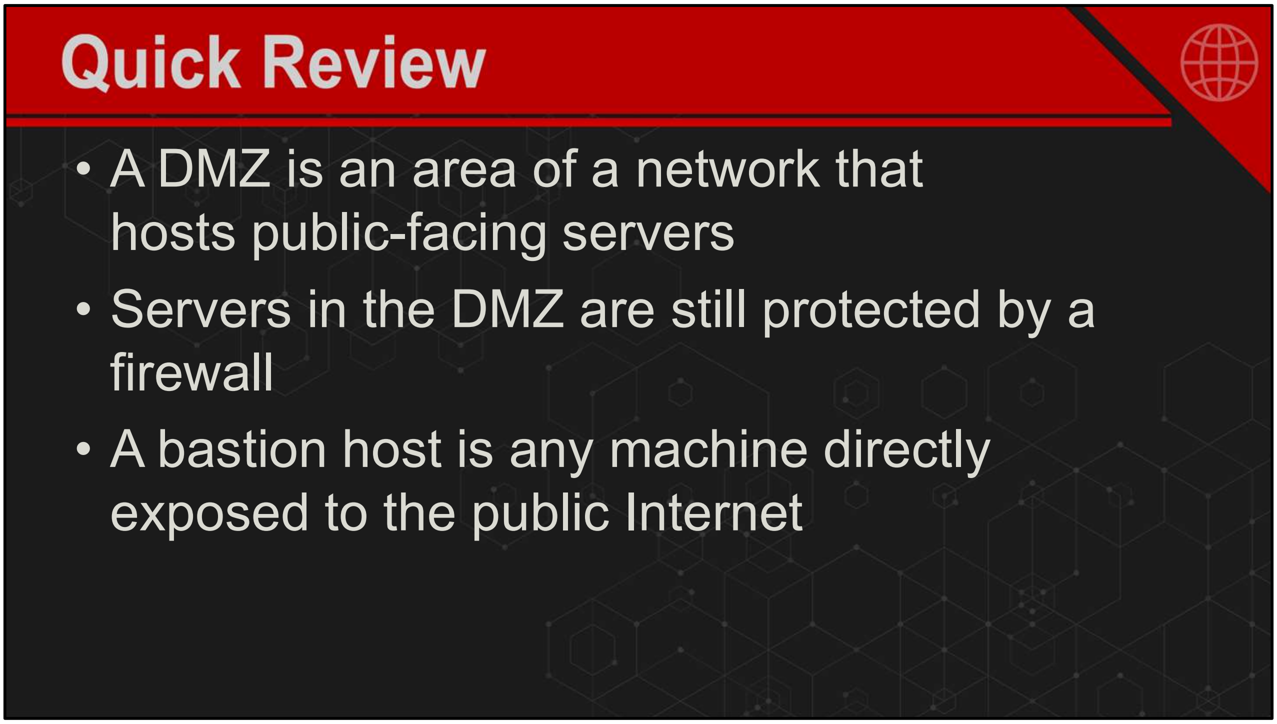
Objective: **4.1 Explain common security concepts**

CompTIA Network+



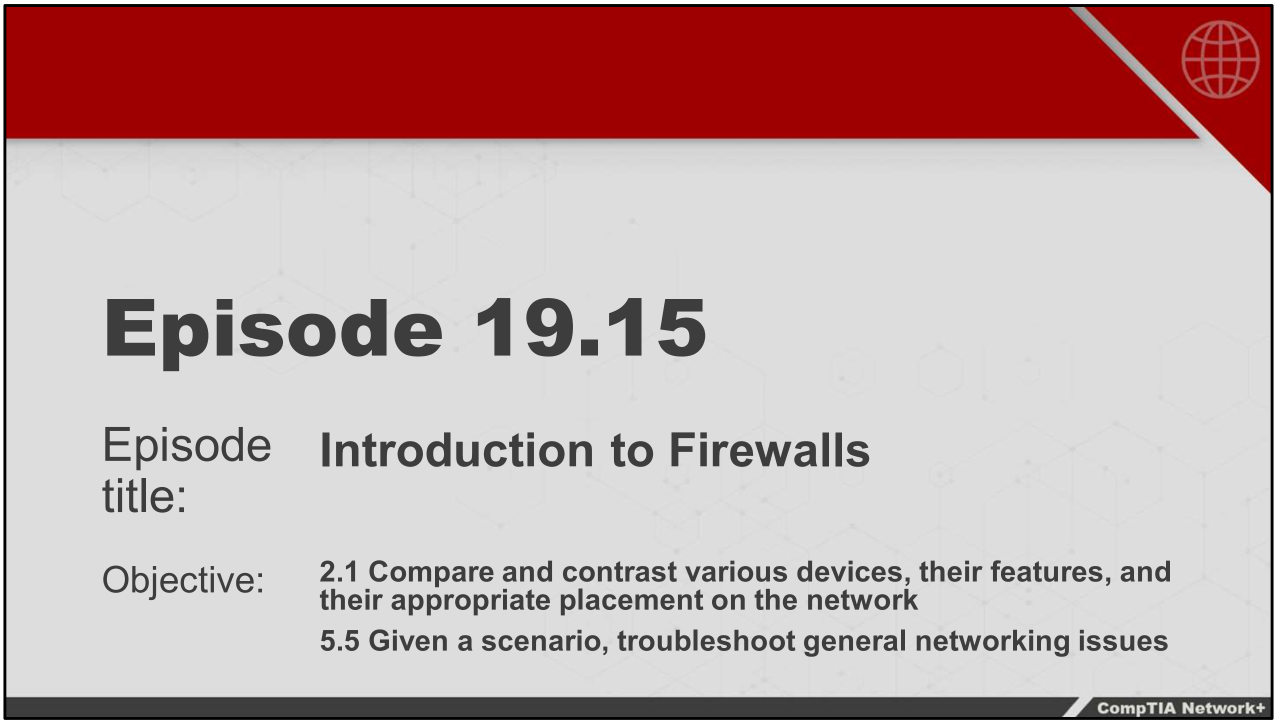
Key Terms

- Place exposed computers into the DMZ
- Router open to Internet traffic is called a bastion host
- Honeypots invite attacks to capture information
- Honeynets invite attacks to capture information, but as a network rather than an individual machine



Quick Review

- A DMZ is an area of a network that hosts public-facing servers
- Servers in the DMZ are still protected by a firewall
- A bastion host is any machine directly exposed to the public Internet



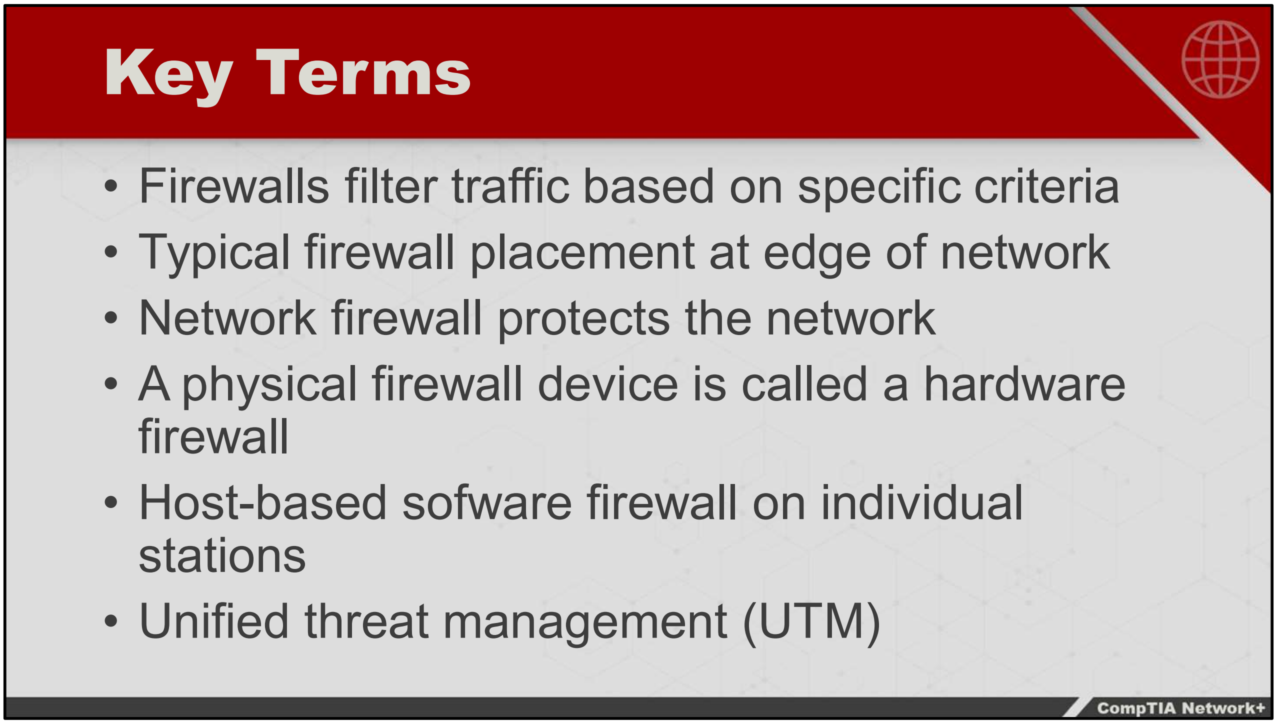
Episode 19.15

Episode title: **Introduction to Firewalls**

Objective: **2.1 Compare and contrast various devices, their features, and their appropriate placement on the network**

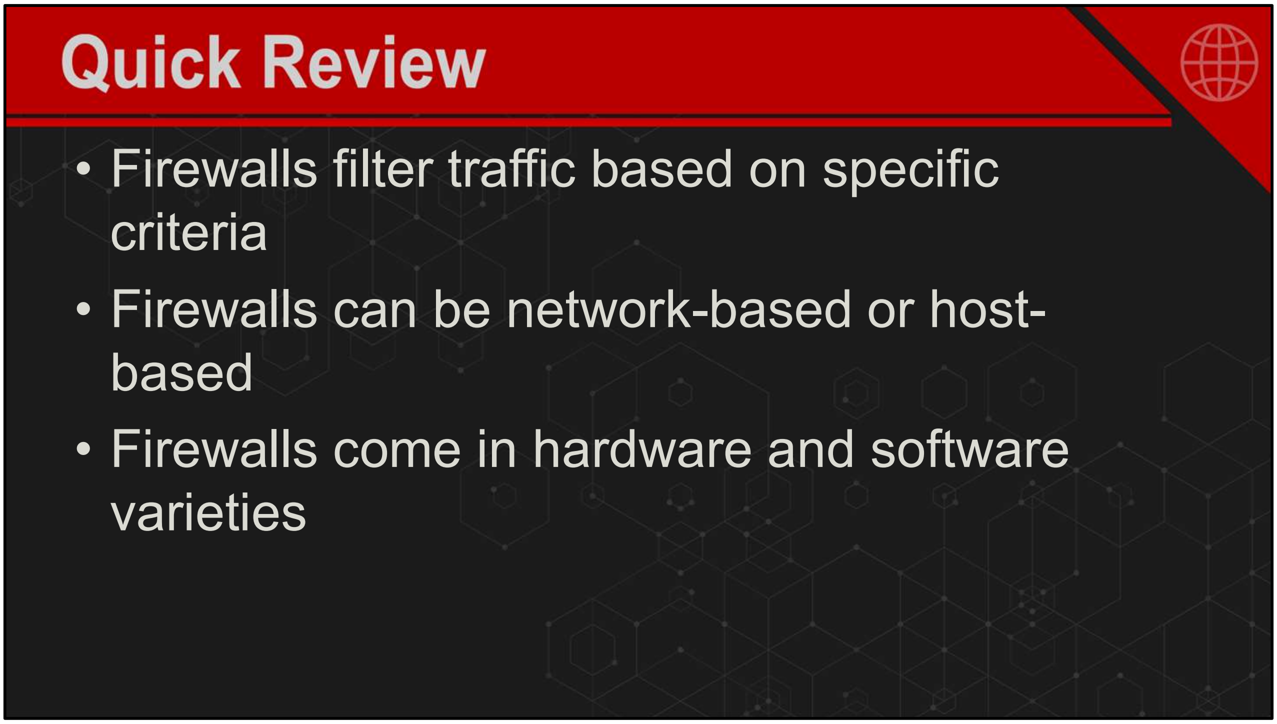
5.5 Given a scenario, troubleshoot general networking issues

CompTIA Network+



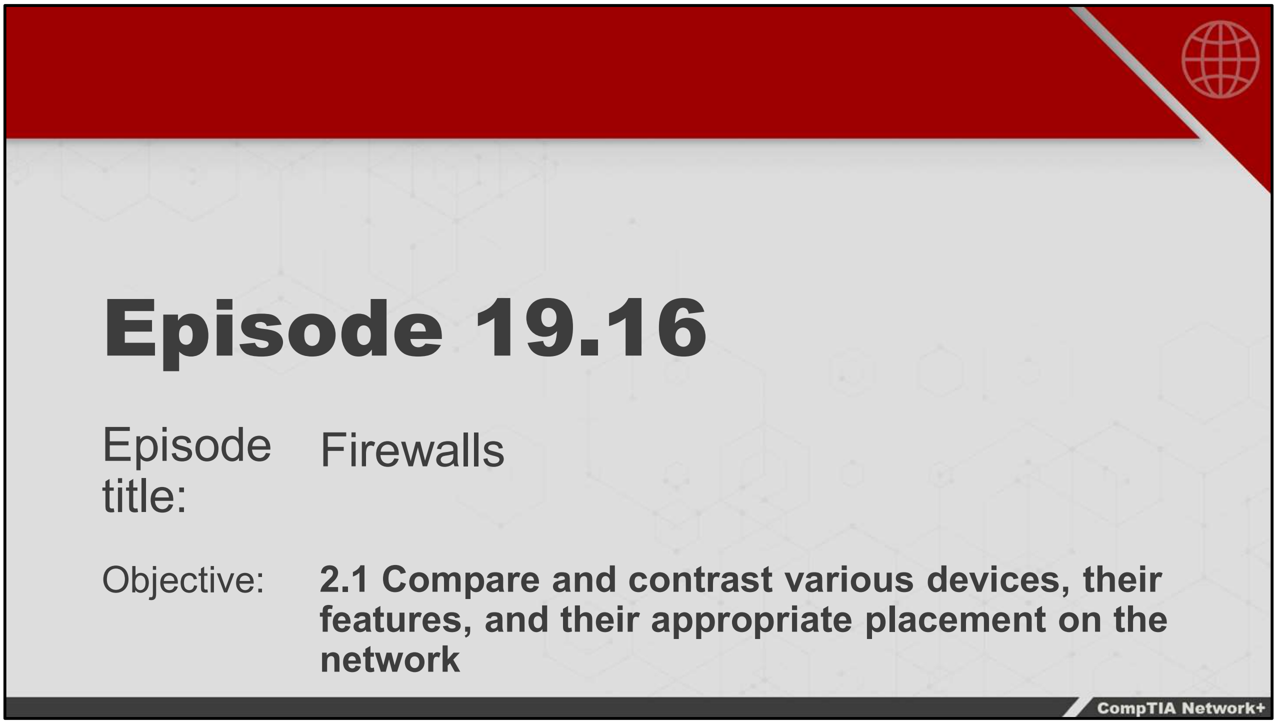
Key Terms

- Firewalls filter traffic based on specific criteria
- Typical firewall placement at edge of network
- Network firewall protects the network
- A physical firewall device is called a hardware firewall
- Host-based sofware firewall on individual stations
- Unified threat management (UTM)



Quick Review

- Firewalls filter traffic based on specific criteria
- Firewalls can be network-based or host-based
- Firewalls come in hardware and software varieties

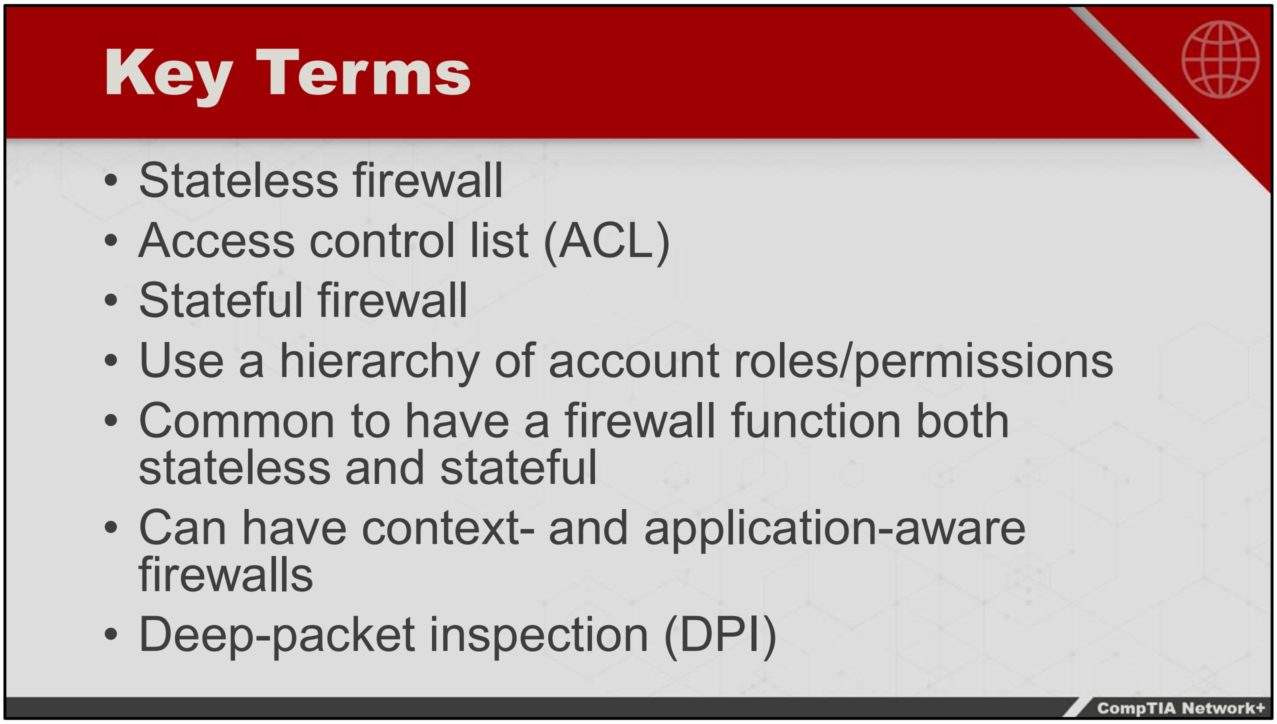


Episode 19.16

Episode title: Firewalls

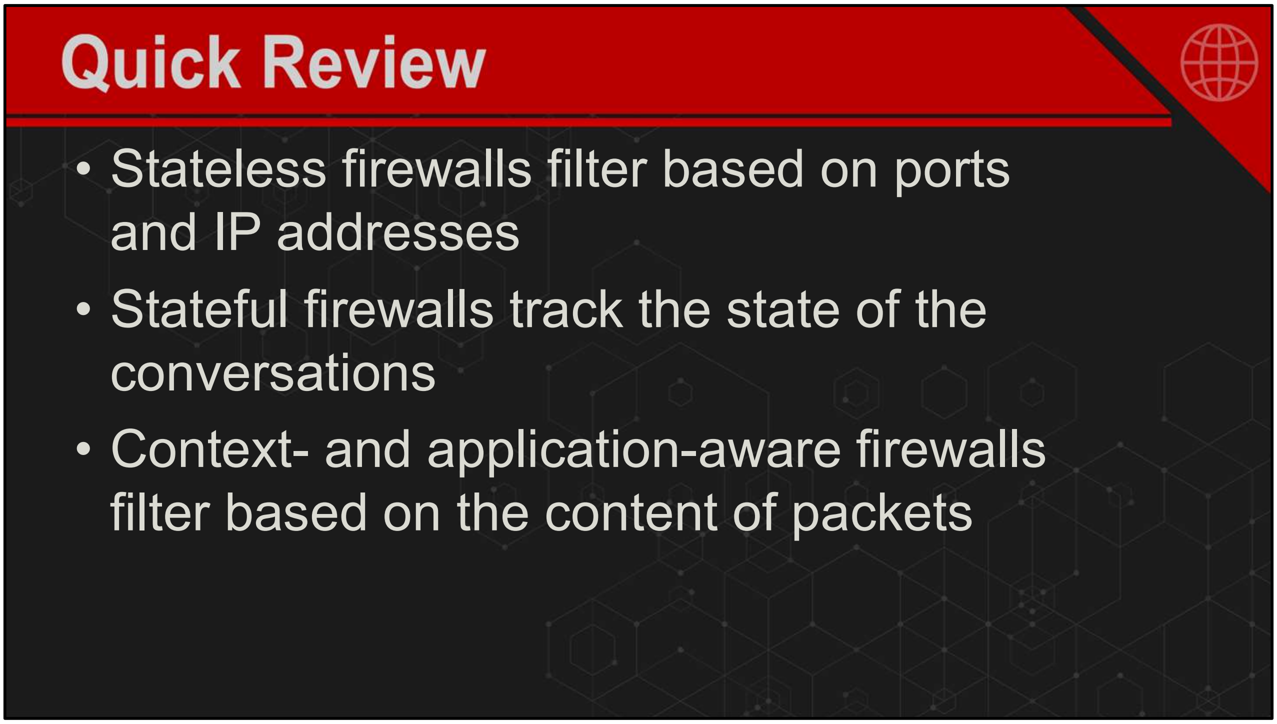
Objective: **2.1 Compare and contrast various devices, their features, and their appropriate placement on the network**

CompTIA Network+



Key Terms

- Stateless firewall
- Access control list (ACL)
- Stateful firewall
- Use a hierarchy of account roles/permissions
- Common to have a firewall function both stateless and stateful
- Can have context- and application-aware firewalls
- Deep-packet inspection (DPI)



Quick Review

- Stateless firewalls filter based on ports and IP addresses
- Stateful firewalls track the state of the conversations
- Context- and application-aware firewalls filter based on the content of packets