Chapter 10

Chapter 10

Episode 10.01

Episode title: **Making TCP/IP Secure**

Objective: **4.1 Explain common security concepts**

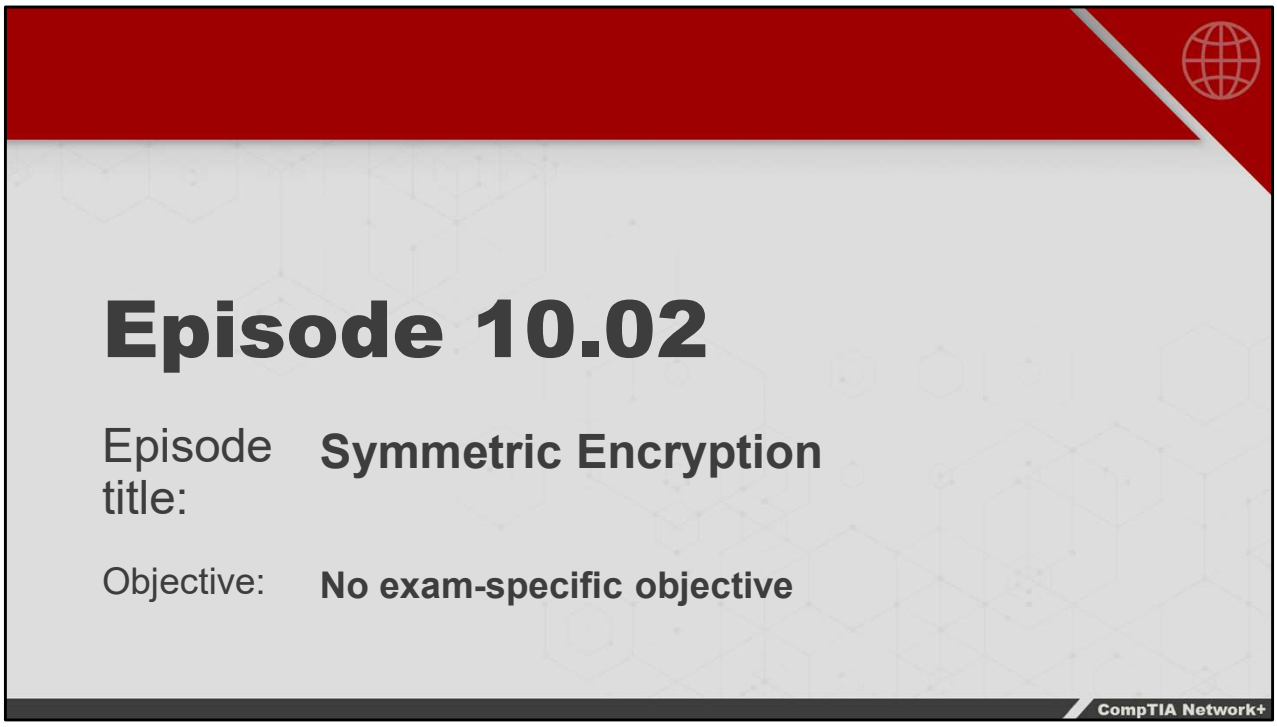
CompTIA Network+

Key Terms

- Encryption
- Non-repudiation
- Availability
- Authorization and authentication

Quick Review

- Security can be broken into three areas: confidentiality, integrity, and availability
- Confidentiality can be addressed through encryption
- Confidentiality and integrity must be balanced with availability

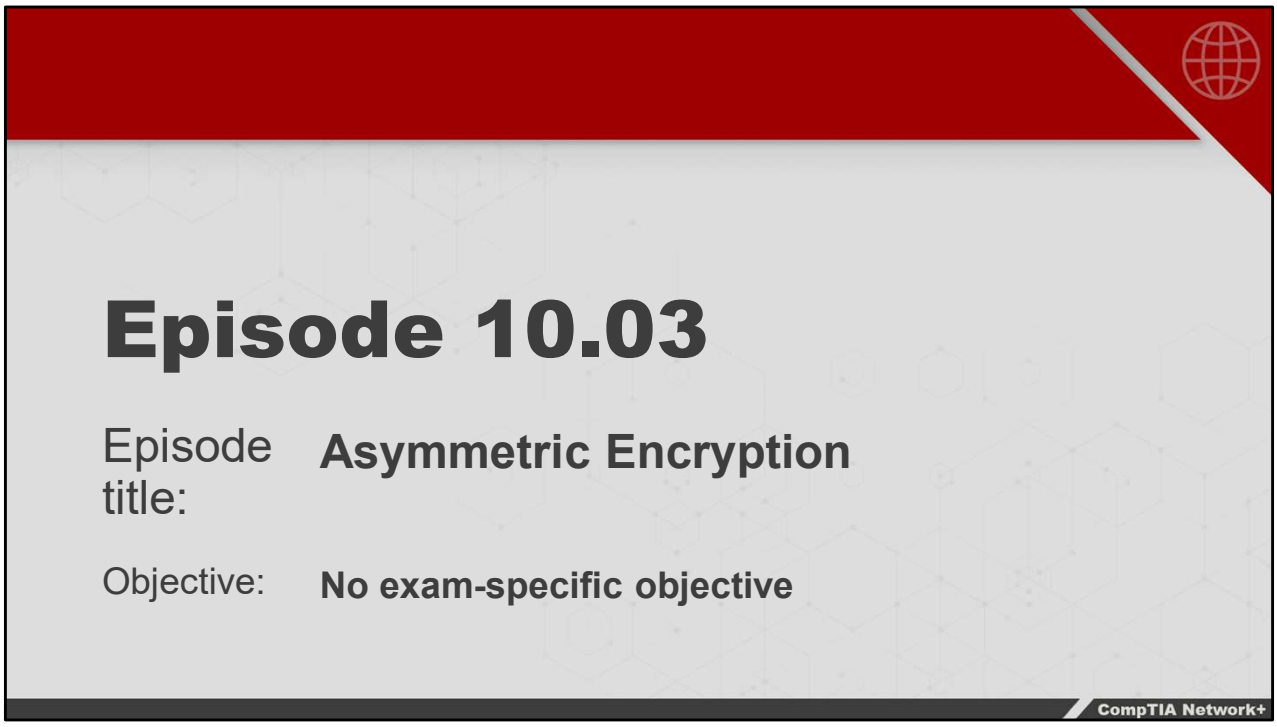

Episode 10.02
Episode title:
Symmetric Encryption
Objective:
No exam-specific objective
CompTIA Network+

Key Terms

- Ilovemikemeyersnetworkplus
- Caesar Cypher
- Algorithms
- Cleartext
- Key
- Cyphertext
- Symmetric Encryption

Quick Review

- Cleartext is any unencrypted data
- Algorithms use keys to encrypt cleartext into cyphertext
- An algorithm that uses the same key to encrypt and decrypt is symmetric encryption


Episode 10.03
Episode title:
Asymmetric Encryption
Objective:
No exam-specific objective
CompTIA Network+

Key Terms

- Asymmetric encryption
- Public key
- Private key
- Public keys only encrypt
- Private keys only decrypt
- A private key and its associated public key is a key pair

Key Terms

- Public keys are distributed so others can send you encrypted data
- Key exchange

Quick Review

- Asymmetric encryption uses a public and a private key
- Public keys encrypt, private keys decrypt
- For two people to communicate, they must exchange public keys


Episode 10.04
Episode title:
Cryptographic Hashes
Objective:
No exam-specific objective
CompTIA Network+

Key Terms

- Hash
- A hash algorithm creates a fixed-size hash value
- Hashes are used to verify data integrity
- MD5 and SHA-1

Quick Review

- Hashes are used for verifying data, not for encryption
- Hash values are always fixed in size
- Two common hashes are MD5 and SHA-1


Episode 10.05
Episode title:
Identification
Objective:
4.1 Explain common security concepts
CompTIA Network+

Key Terms

- Identification
- Authentication
- Authorization

Multifactor Authentication (MFA)

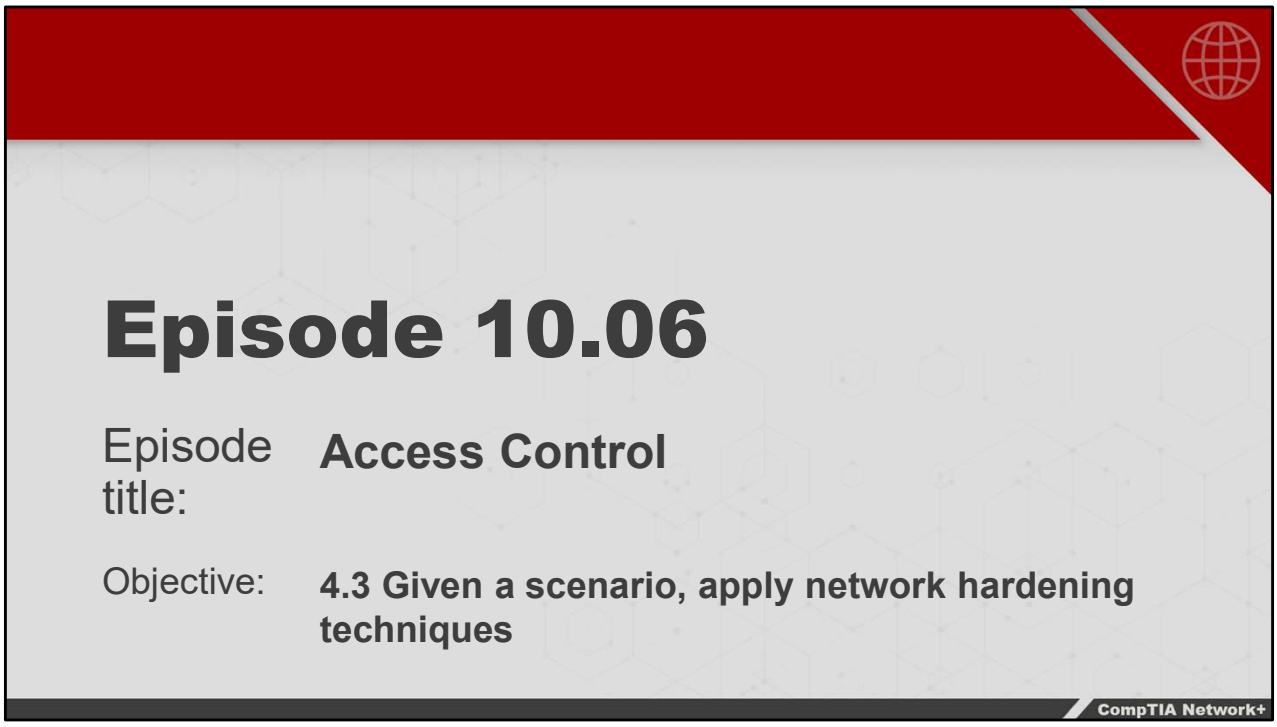
- Using more than one factor of authentication
- Factors
  - Something you know
  - Something you have
  - Something you are

Authentication Attributes

- Something you do
- Something you exhibit
- Someone you know
- Somewhere you are

Quick Review

- Identification is claiming an identity
- Authentication is proving that identity
- Authorization is permitting specific actions once a user has been authenticated
- Authentication factors include something you know, have, or are
- Authentication attributes include something you do, exhibit, know, or somewhere you are


Episode 10.06
Episode title:
Access Control
Objective:
4.3 Given a scenario, apply network hardening techniques
CompTIA Network+

Key Terms

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Users -> groups -> rights and permissions

Quick Review

- Mandatory access control (MAC) uses labels
- Discretionary access control (DAC) gives the creators control over permissions
- Role-based access control (RBAC) uses groups


Episode 10.07
Episode title: AAA
Objective: 4.1 Explain common security concepts
CompTIA Network+

Key Terms

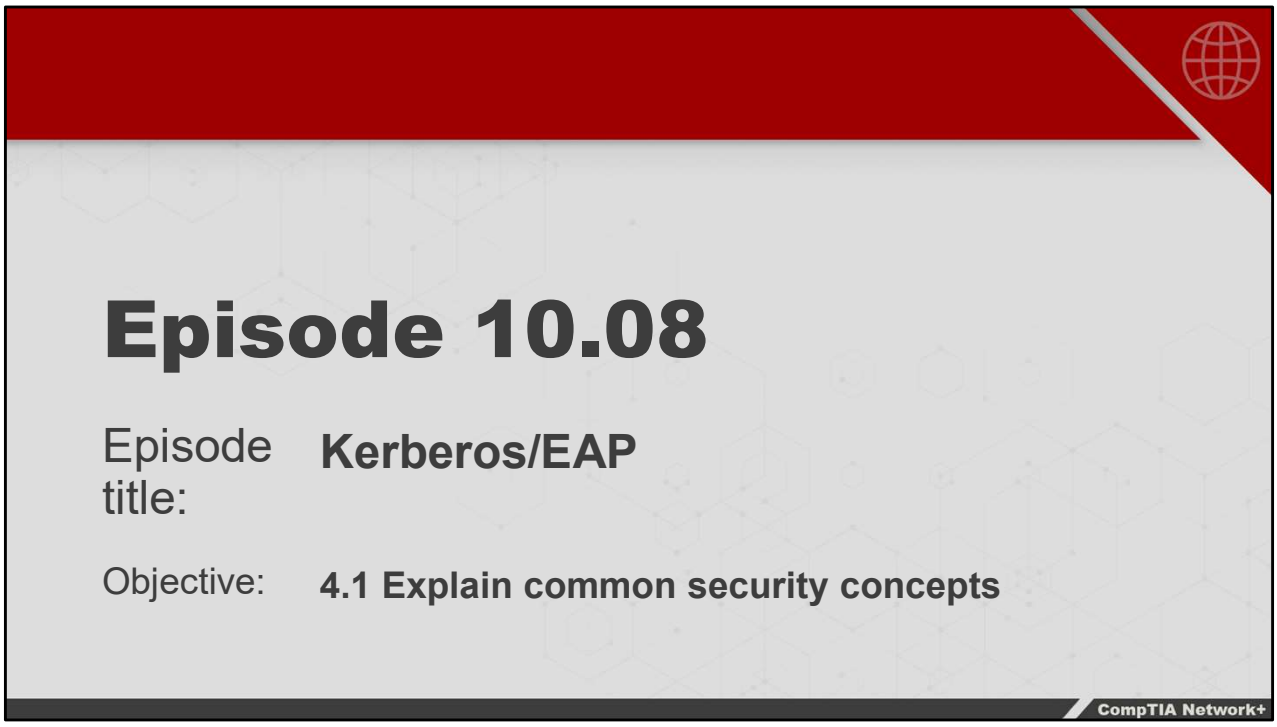
- RADIUS Server
- RADIUS Client
- RADIUS Supplicant
- RADIUS Database
- RADIUS uses UDP ports 1812-1813 or UDP ports 1645-1646
- RADIUS provides AAA—authentication, authorization, and accounting

Key Terms

- TACACS+
- TACACS+ uses TCP port 49

Quick Review

- A RADIUS client is an intermediary agent between a RADIUS supplicant and a RADIUS server
- A RADIUS database of authenticated users and passwords may reside outside the RADIUS server
- RADIUS uses UDP ports 1812-1813 or UDP ports 1645-1646, and TACACS+ uses TCP port 49


Episode 10.08
Episode title:
Kerberos/EAP
Objective:
4.1 Explain common security concepts
CompTIA Network+

Key Terms

- Kerberos
- Key Distribution Center
- Authentication Server
- Ticket Granting Service
- Ticket Granting Ticket (TGT)
- Time stamps are important in Kerberos
- Kerberos is a Microsoft proprietary technology

Key Terms

- Extensible Authentication Protocol (EAP)
- EAP pre-shared key (EAP PSK)
- Protected Extensible Authentication Protocol (PEAP)
- EAP MD5
- EAP TLS
- EAP TTLS

Quick Review

- Kerberos handles authentication and authorization for wired networks
- Kerberos relies heavily on time stamps
- EAP enables flexible authentication


Episode 10.09
Episode title:
Single Sign-on
Objective:
4.1 Explain common security concepts
CompTIA Network+

Key Terms

- LAN uses Windows Active Directory
- Federated systems
- Security Assertion Markup Language (SAML)
- Service provider (SP)

Quick Review

- For local area networks, use Windows Active Directory for single sign-on
- SAML is used to manage multiple apps using a single account
- SSOcircle provides a variety of service provider (SP) samples

Episode 10.10

Episode title: **Certificates and Trust**

Objective: **5.5 Given a scenario, troubleshoot general networking issues**

CompTIA Network+

Key Terms

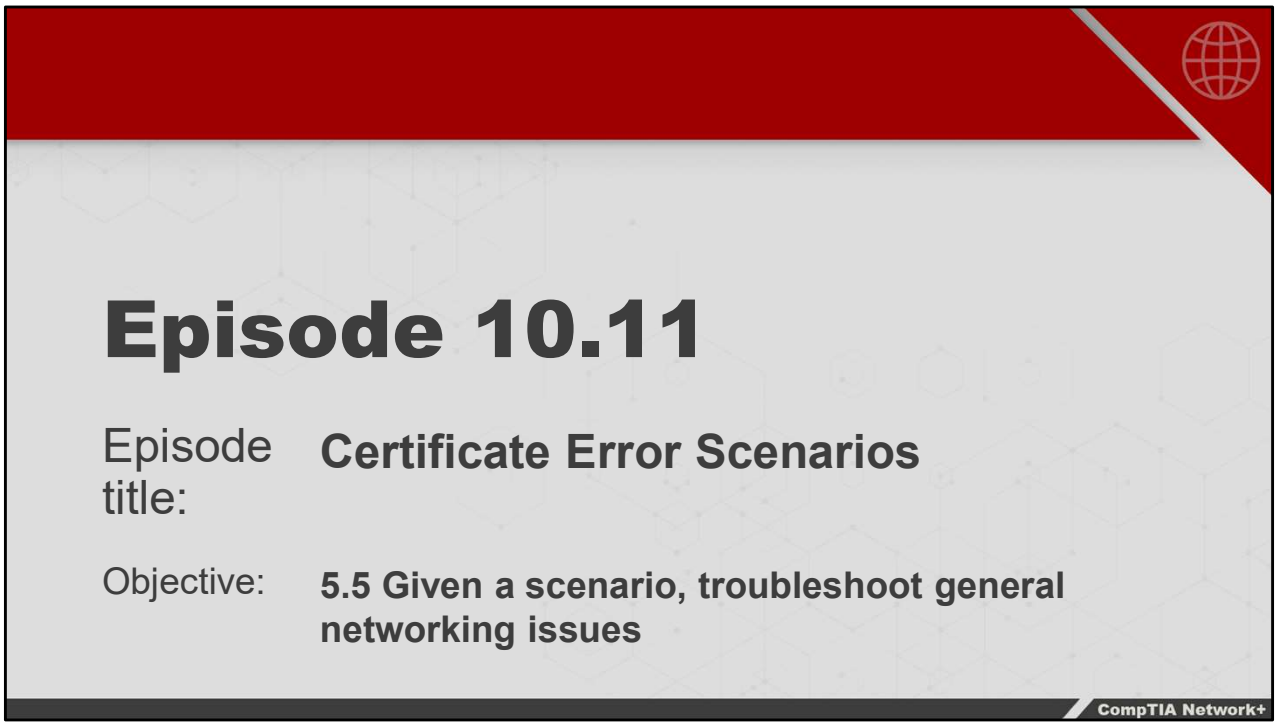
- Public/private key pair
- Key exchange
- Either key in a private and public pair can be the public key
- Digital certificates
- Generate your own certificates
- Unsigned certificate

Key Terms

- Web of trust
- Web of trust requires lots of maintenance
- Public key infrastructure (PKI)

Quick Review

- Certificates include a public key and at least one digital signature
- Web of trust uses a web of mutually trusting peers
- Public key infrastructure uses a hierarchical structure with root servers


Episode 10.11
Episode title:
Certificate Error Scenarios
Objective:
5.5 Given a scenario, troubleshoot general networking issues
CompTIA Network+

Key Terms

- No Key Terms for this Episode

Quick Review

- A self-signed certificate can throw a 443 error, as the certificate has not been issued by a certificate authority
- An expired certificate can be viewed, then fixed either by getting a new certificate from its issuer or accepting the certificate in its current state
- The setting to query OCSP to confirm the current validity of certificates is a good security setting