Chapter 28

Essential Security Practices

Episode 28.01

Episode title: **Threats**

Objective: 2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities

L3s

- 2:07 - Objective term - Man-in-the-middle (on-path) attack
- 3:30 - Objective term - Spoofing
- 4:26 - Objective term - Denial of Service (DoS)
- 5:25 - Objective term - Distributed Denial of Service (DDoS)
- 5:51 - Zombie
- 6:46 - Objective term - Zero day
- 7:47 - Objective term - Renamed system files
- 8:13 - Objective term - Disappearing files

L3s

- Evil twin attack
- Insider threat
- SQL injection attack
- Cross-site scripting or XXS attack
- Business email compromise (BEC)
- Supply chain attack

SQL Injection Attacks

Types of attacks

- In-band
- Error based
- Out-of-hand
- Time-based blind

XSS Attacks

Types of attacks

- Stored (persistent)
- Reflected (non-persistent)
- Document Object Model (DOM) - based

Supply Chain Attacks

Happens at any point in the supply pipeline

- Objective/ Goals
  - Financial gain
  - Espionage
  - Politics
  - Disruption
- Targets examples
  - Specific organization
  - Industry
  - Content-delivery network

Episode 28.02

Episode title: **Dealing with Threats**

Objective: 2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities

L3s

- 0:47 - Objective term - Patch your system!
- 1:43 - Objective term - Run anti-malware and antivirus
- 1:58 - Objective term - Run a host-based software firewall
- 2:41 - Intrusion detection systems (IDS)
- 3:43 - Intrusion prevention systems (IPS)
- 5:02 - Endpoint management
- 5:55 - Objective term - Unified Threat Management (UTM)
- Test Access Point (TAP)

L3s

- Passive TAPs
- Active TAPs
- Compliance
- Non-compliant

Episode 28.03

Episode title: **Physical Security**

Objective: 2.1 Summarize various security measures and their purposes.

L3s

1:35 - Objective term - Security guard
2:00 - Objective term - Mantrap (access control vestibule)
2:41 - Objective term - Locking doors
2:51 - Objective term - Need a key
2:53 - Entry control roster

L3s

- 3:25 - Objective term - Badge reader
- 3:26 - RFID-chips embedded in badges
- 3:54 - Objective term - Smart card
- 4:12 - Objective term - Biometric scanners/locks
- 4:52 - Objective term - Cable locks to secure hardware

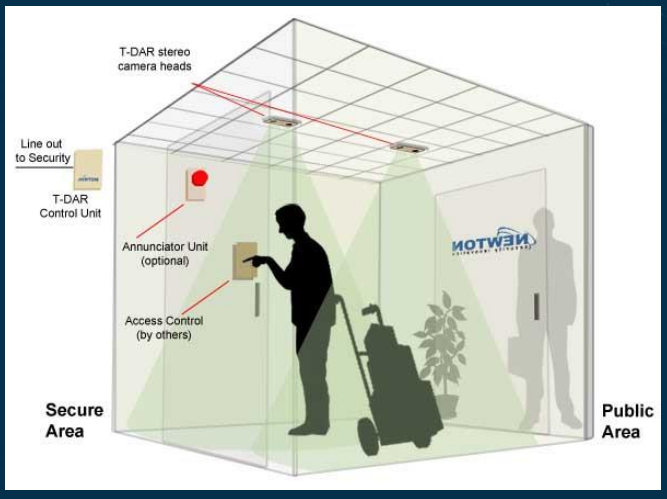
L3s

- 5:20 - Objective term - Server lock
- 5:50 - Objective term - USB locks
- 6:26 - Privacy screens
- 7:05 - Objective term - Key fobs
- 7:15 - Objective term - Hardware token/ Hardware Security Module HSM

L3s

- Bollards
- Video surveillance
- Motion detection
- Security alarm system
- Fence

Mantrap (Access Control Vestibule)



Source: https://www.newtonsecurityinc.com/datacenter_landing.html

Episode 28.04

Episode title: **Passwords and Authentication**

Objective: 2.7 Given a scenario, apply workstation security options and hardening techniques

L3s

- 0:55 - Hash
- 3:37 - Objective term - Brute-force
- 5:44 - Objective term - Dictionary attack
- 7:16 - Rainbow tables
- 9:09 - Objective term - Password best practices
- 9:13 - Objective term - 1. Set strong passwords

L3s

- 9:16 - Objective term - Make complex passwords with upper- and lowercase letters and use different character types
- 9:36 - Objective term - Looooong passwords
- 10:37 - Objective term - 2. Password expiration
- 10:54 - Objective term - (Also...make sure your employees aren't taping their passwords to their monitors...)

L3s

- 1:22 - Objective term - 3. Require screensavers with password login on desktops
- 11:49 - Objective term - 4. Require lock screens with passwords on mobile devices
- 12:20 - Objective term - 5. BIOS/UEFI passwords
- 12:36 - 6. Require passwords everywhere!
- 13:01 - Objective term - 7. Multifactor authentication (MFA)

L3s

- Data at rest
- Access control
- Passwords should be unique to each application
- Complex control requirements
- Password manager

Passwords

Passwords should be unique to each application

- Requirements
  - Include a length greater than 8 characters
  - Mix choice of character types
  - Should not contain PII or common phrases
  - The most common password is “password.”

Episode 28.05

Episode title: **Multifactor Authentication (MFA)**

Objective:

1.1 Summarize various security measures and their purposes.

2.1 Summarize various security measures and their purposes.

2.2 Given a scenario, configure and apply basic Microsoft Windows OS Security settings

L3s

- 0:15 - Objective term - Multifactor authentication (MFA)
- 0:21 - Something you know
- 0:49 - Two-factor authentication (2FA)
- 0:55 - Something you have
- 1:06 - Objective term - Hardware token
- 1:13 - Objective term - Authenticator application
- 1:36 - Something you are

L3s

- 1:40 - Objective term - Biometrics such as fingerprint, palmprint, or retinal scanners
- 1:54 - Objective term - Facial recognition
- 1:59 - Somewhere you are
- 2:11 - Objective term - Supervisory Control and Data Acquisition (SCADA)
- 3:17 - Objective term - OS login options include facial recognition, fingerprint recognition, and personal identification number (PIN)

L3s

- One-Time Password (OTP)
- Physical token
- Protect email
- Digital voice calls
- SMS authentication
- Passwordless authentication
- Windows Hello
- Security lighting
- Magnetometers


OTP Physical Token
21436587

Email Security:

- Use strong passwords
- Implement MFA
- Be cautious with unknow senders
- Be cautious of attachments
- Be cautious of imbedded links
- Consider encryption
- Avoid using public hot-spots
- Training is critical

Authentication

The process of verifying identity before granting access

Users must prove who they are:

- Something you know (password)
- Something you have (token)
- Something you are (fingerprint)
- Something you can do (signature)

Physical Security

Security lighting protects property and people by deterring intruders and ensuring visibility

- Continuous: Fixed lights with overlapping coverage
- Standby: Motion-activated
- Portable: Supplemental, movable lights
- Emergency: Backup lighting used during power failures

Email Security:

Learn to recognize:

- Phishing
- Whaling
- Vishing
- Other social engineering tactics