

CompTIA Network+ Exam N10-008

Lesson 17



Explaining Organizational and Physical Security Concepts

Objectives

- Explain organizational documentation and policies
- Explain physical security methods
- Compare and contrast Internet of Things devices

Lesson 17

Topic 17A

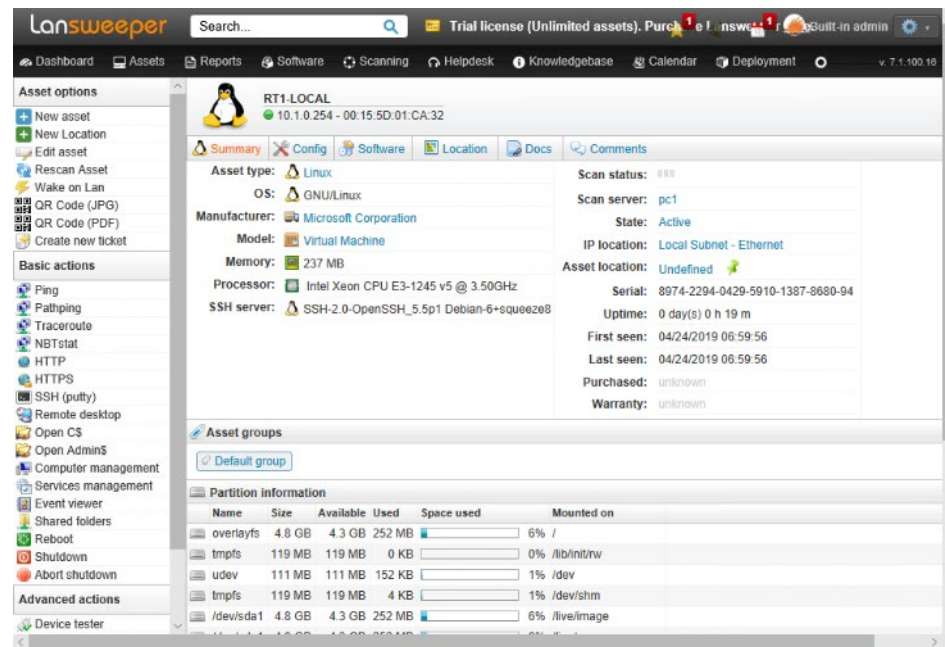
Explain Organizational Documentation and Policies

Operating Plans and Procedures

- Configuration management
 - Assets and configuration items
 - Baselines
- Change management
 - Reactive versus proactive
 - Change request and approval
- Standard Operating Procedures (SOPs)

System Life Cycle Plans and Procedures

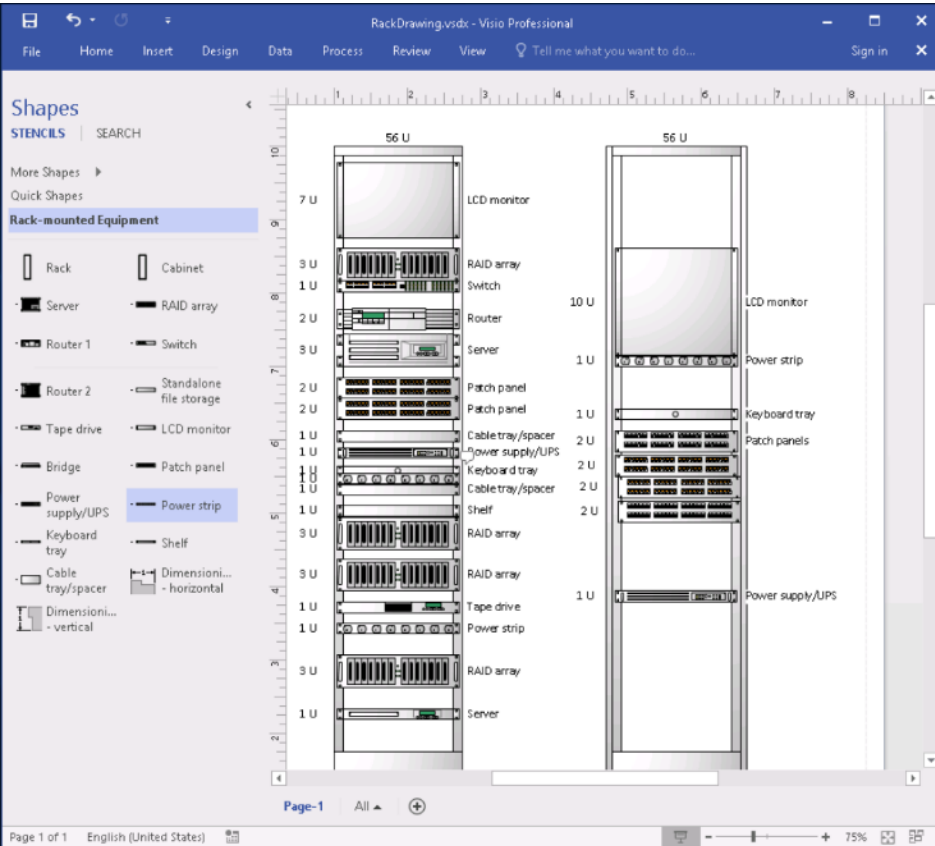
- Audit report
 - Identify and record assets
- Assessment report
 - Evaluate configuration/performance
 - Compare to baselines
- System life cycle
 - Acquisition, deployment, use, and decommissioning



Physical Network Diagrams

- Floor plan
 - Detailed scale diagram
- Wiring diagram
 - Illustrate and document cable termination
- Distribution frame
 - Port IDs
 - Main versus intermediate distribution frames (MDF versus IDF)
- Site survey report



















Rack Diagrams



- Rack format
 - Standard 19" width
 - 1.75" U multiples in height
- Stencils
- Position of appliances
- Label network and power ports
- Configuration and asset information

Logical versus Physical Network Diagrams

- Diagram types
 - Detailed physical plans
 - Schematics
- Constrain to single OSI layer per diagram
 - PHY (Physical layer)
 - Data Link (layer 2)
 - Logical (IP/layer 3)
 - Application
- Standard icons

Icon	Device	Icon	Device	Icon	Device
	Hub		Content Switch		IP Phone
	Access Point		Modem		Firewall
	Bridge		CSU/DSU		Router
	Basic Switch		PBX		Wireless Router
	Layer 3 Switch		Broadband Router		Router/Firewall
	Multilayer Switch		Cable Modem		Security Appliance

Security Response Plans and Procedures

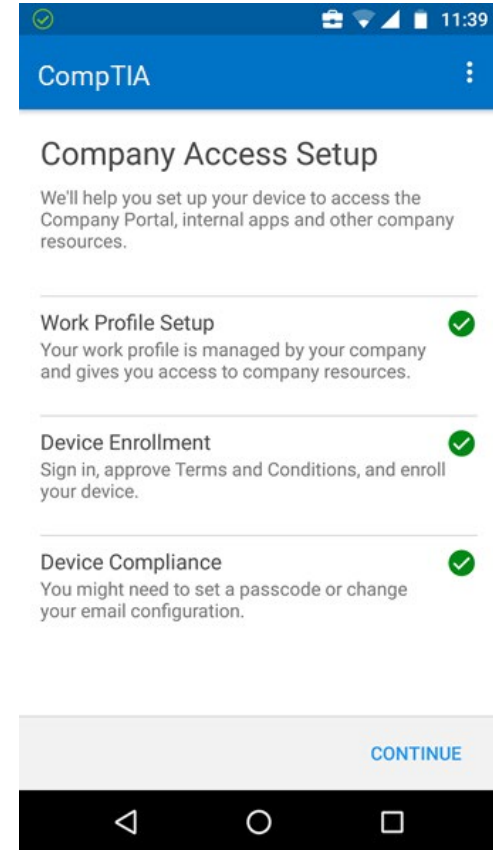
- Incident response plan
 - Categorize incident types, such as data breach, malware/intrusion detection, denial of service (DoS), ...
 - Restoring security versus preserving evidence
- Disaster recovery plan
 - Identify major incident scenarios
- Business continuity plan
 - Identify and prioritize functions for investment in fault tolerance/redundancy
 - Business impact analysis (BIA)
 - IT contingency planning (ITCP)

Hardening and Security Policies

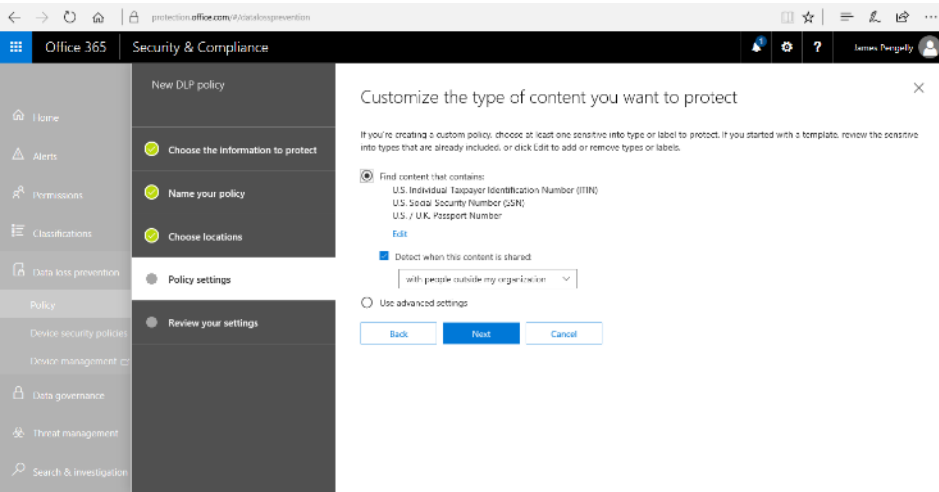
- Security policy types
- Human Resources (HR)-led policies
 - Onboarding
 - Offboarding

Usage Policies

- Password policy
 - User behavior
 - System-enforced selection and change rules
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policies
 - BYOD versus corporate owned
 - Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)



Data Loss Prevention



- Risks from data breach
- Data loss prevention (DLP) software
 - Scan file and data stores
 - Match confidential and personal/sensitive data
 - Control access, copying, and printing

Remote Access Policies

- Ensure remote devices and network connections do not create vulnerabilities
 - Malware protection and patching of remote hosts
 - Protection of credentials
 - Protection for data processed off-site
 - Treat remote hosts and networks as untrusted


Common Agreements

- Service Level Agreement (SLA) requirements
- Non-Disclosure Agreement (NDA)
 - Legal basis for protecting information assets
 - Used in employment contracts and between companies
- Memorandum of Understanding (MoU)

Review Activity: Documentation and Policies

- Operating Plans and Procedures
- System Life Cycle Plans and Procedures
- Physical Network Diagrams and Rack Diagrams
- Logical versus Physical Network Diagrams
- Security Response Plans and Procedures
- Hardening and Security Policies
- Usage Policies
- Data Loss Prevention
- Remote Access Policies
- Common Agreements

Assisted Lab: Develop Network Documentation

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

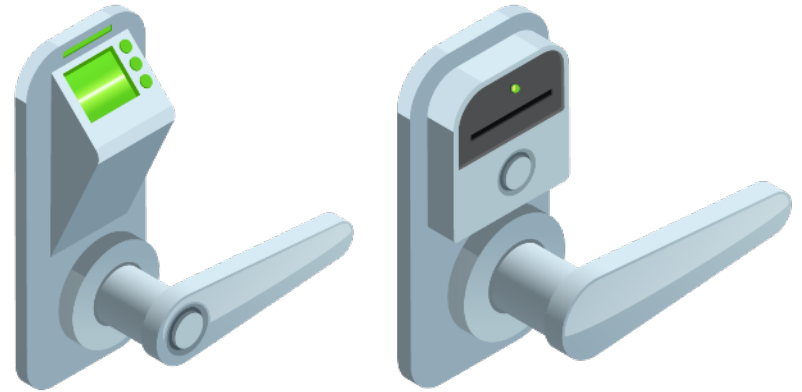
Lesson 17

Topic 17B

Explain Physical Security Methods

Badges and Site Secure Entry Systems

- Access control hardware
 - Badge reader
 - Biometric
- Access control vestibule
 - Prevent tailgating and piggybacking
 - Turnstile
 - “Mantrap”



Physical Security for Server Systems



- Locking racks
 - Lock whole rack
 - Bracket/shelf locks
- Locking cabinets
- Smart lockers
 - Smart card/biometric lock
 - Sensors to detect add/remove

Detection-Based Devices

- Surveillance systems and security guards
- Cameras
 - Fixed versus Pan-Tilt-Zoom (PTZ)
 - Focal length
 - Closed Circuit Television (CCTV) coax networks
 - IP camera data and PoE networks
- Asset tags
 - Link asset to database/configuration management
 - Radio Frequency ID (RFID) monitored tags



Alarms and Tamper Detection

- Alarm types
 - Circuit/tamper detection
 - Motion detection
- Alarms for rack systems and chassis intrusion
- Tamper detection for cabling
 - Protected Distribution System (PDS)

Asset Disposal

- Factory reset/configuration wipe
 - Remove accounts and passwords
 - Remove configuration information
 - Remove licensing keys and registration
- Data remnants and media sanitization
 - Physical destruction
 - Overwriting and HDDs versus SSDs
 - Secure Erase (SE)
 - Instant Secure Erase (ISE)

Employee Training

- Security awareness
 - Incident reporting
 - Site security
 - Data and credential handling
 - Social engineering, malware, and other threat awareness
- Role-based training



Review Activity: Physical Security Methods

- Badges and Site Secure Entry Systems
- Physical Security for Server Systems
- Detection-Based Devices
- Alarms and Tamper Detection
- Asset Disposal
- Employee Training

Lesson 17

Topic 17C

Compare and Contrast Internet of Things Devices

Internet of Things

- Consumer-grade smart devices
 - Hub versus device functions
- Physical access control systems and smart buildings

ICS/SCADA

- Industrial control systems (ICS) and the AIC triad
- Workflow and process automation systems
 - Power suppliers, water suppliers, health services, telecommunications, and national security services
 - Programmable logic controller (PLC)
 - Mechanical devices and sensors
 - Human-machine interface (HMI)
- Supervisory Control and Data Acquisition (SCADA)
 - ICS distributed over large areas
 - Control software running on PCs
 - Cellular communications

IoT Networks

- Operational Technology (OT) networks
 - Serial data or industrial Ethernet
 - Require deterministic, low-latency delivery over bandwidth
- Cellular networks
 - Deterministic, low-latency versions of 4G/5G
- Z-Wave and Zigbee
 - Wireless mesh for home automation devices

Placement and Security

- Consumer-grade smart devices
 - Vendor assessment
 - Risks from shadow IT
- Smart buildings
 - Isolate management traffic from data networks
 - Include in configuration management/assessments
- ICS/SCADA
 - Isolate/monitor connections to data networks

Review Activity: Internet of Things Devices

- Internet of Things
- ICS/SCADA
- IoT Networks
- Placement and Security

CompTIA Network+ Exam N10-008

Lesson 17



Summary