CompTIA Security + - Certification Outline

Filename: comptia-secplussy0501-0-0-outline
Title: Security + Certification Outline
Subtitle: CompTIA Security+ (SY0-502)

Domains	Percentage
Threats, Attacks and Vulerabilities	21%
Technologies and Tools	22%
Architecture and Design	15%
Identity and Access Management	16%
Risk Manangement	14%
Cryptography and PKI	12%

- Install and Configure Security on:
  - Applications
  - Networks
  - Devices

- Perform:
  - Threat Analysis
  - Incident Response
  - Awareness and operations (Operate with in the policies or standards)
  - Perform tasks supporting: Confidentiality, Integrity, Availability

---

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

filename:comptia-secplussy0501-1-1-determining_types_of_malware
Title: Determining Types of Malware
Subtitle: CompTIA Security+ (SY0-501)

1.1 Determining Types of Malware

- Given a scenario, analyze indicators of compromise and determine the type of malware
  - Viruses
  - Crypto-malware
  - Ransomware
  - Worm
  - Spyware
  - Bots
  - RAT(Remote Access Trojan)
  - Logic bomb
  - Backdoor

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-2-types_of_attacks
Title: Types of Attacks
Subtitle: CompTIA Security+ (SY0-501)

1.2 Types of Attacks

- 1.2 Compare and contrast types of attacks.
  - Social engineering
    - Phishing
    - Spear phishing
    - Whaling
    - Vishing
    - Tailgating
    - Impersonation
    - Dumpster diving
    - Shoulder surfing
    - Hoax
    - Watering hole attack
    - Principles (reasons for effectiveness)

        - Authority
        - Intimidation
        - Consensus
        - Scarcity
        - Familiarity
        - Trust
        - Urgency
    - Application/service attacks o DoS
        - DDoS
        - Man-in-the-middle
        - Buffer overflow
        - Injection
        - Cross-site scripting
        - Cross-site request forgery
        - Privilege escalation
        - ARP poisoning
        - Amplification
        - DNS poisoning
        - Domain hijacking
        - Man-in-the-browser
        - Zero day
        - Replay
        - Pass the hash
        - Hijacking and related attacks
            - Clickjacking
            - Session hijacking
            - URL hijacking
            - Typo squatting
        - Driver manipulation
            - Shimming
            - Refactoring
        - MAC spoofing
        - IP spoofing
    - Wireless attacks
        - Replay
        - IV
        - Evil twin
        - Rogue AP
        - Jamming
        - WPS
        - Bluejacking
        - Bluesnarfing
        - RFID
        - NFC
        - Disassociation
    - Cryptographic attacks
        - Birthday
        - Known plain text/cipher text o Rainbow tables
        - Dictionary
        - Brute force
            - Online vs. offline
        - Collision
        - Downgrade
        - Replay
        - Weak implementations

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-3-threat_vector_types_and_attributes
Title: Threat Vector Types and Attributes
Subtitle: CompTIA Security+ (SY0-501)

1.3 Threat Vector Types and Attributes

- 1.3 Explain threat actor types and attributes.
    - Types of actors
        - Script kiddies
        - Hacktivist
        - Organized crime
        - Nation states/APT
        - Insiders

        - Competitors
    - Attributes of actors
        - Internal/external
        - Level of sophistication
        - Resources/funding
        - Intent/motivation
    - Use of open-source intelligence

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-4-penetration_testing_concepts
Title: Penetration Testing Concepts
Subtitle: CompTIA Security+ (SY0-501)

1.4 Penetration Testing Concepts

- 1.4 Explain penetration testing concepts.
    - Active reconnaissance
    - Passive reconnaissance
    - Pivot
    - Initial exploitation
    - Persistence
    - Escalation of privilege
    - Black box
    - White box
    - Gray box
    - Pen testing vs. vulnerability scanning

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-5-vulnerability_scanning_concepts
Title: Vulnerability scanning concepts
Subtitle: CompTIA Security+ (SY0-501)

1.5 Vulnerability Scanning Concepts

- 1.5 Explain vulnerability scanning concepts
    - Passively test security controls
    - Identify vulnerability
    - Identify lack of security controls
    - Identify common misconfigurations
    - Intrusive vs. non-intrusive
    - Credentialed vs. non-credentialed
    - False positive

CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-6-impact_of_various_vulnerabilities
Title: Impact of Various Vulnerabilities
Subtitle: CompTIA Security+ (SY0-501)

1.6 Impact of Various Vulnerabilities

- 1.6 Explain the impact associated with types of vulnerabilities
    - Race conditions
    - Vulnerabilities due to:
        - End-of-life systems
        - Embedded systems
        - Lack of vendor support
    - Improper input handling
    - Improper error handling
    - Misconfiguration/weak configuration
    - Default configuration
    - Resource exhaustion
    - Untrained users
    - Improperly configured accounts
    - Vulnerable business processes
    - Weak cipher suites and implementations

- Memory/buffer vulnerability
  - Memory leak
  - Integer overflow
  - Buffer overflow
  - Pointer dereference
  - DLL injection
- System
- Architecture/design weaknesses
- New threats/zero day
- Improper certificate and key management

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-1-hardware_and_software_organizational_security
Title: Hardware and Software Orgranizational Security
Subtitle: CompTIA Security+ (SY0-501)

2.1 Hardware and Software Orgranizational Security

- 2.1 Install and configure network components, both hardware- and software-based, to support organizational security
  - Firewall
    - ACL
    - Application-based vs. network-based o Stateful vs. stateless
    - Implicit deny
  - VPN concentrator
    - Remote access vs. site-to-site
    - IPSec
      - Tunnel mode
      - Transportmode
      - AH
      - ESP
    - Split tunnel vs. full tunnel
    - TLS
    - Always-on VPN
  - NIPS/NIDS
    - Signature-based
    - Heuristic/behavioral
    - Anomaly
    - Inline vs. passive
    - In-band vs. out-of-band
    - Rules
    - Analytics
      - False positive
      - False negative
  - Router
    - ACLs
    - Antispoofing Switch
    - Port security
    - Layer 2 vs. Layer 3
    - Loop prevention
    - Flood guard
  - Proxy
    - Forward and reverse proxy
    - Transparent
    - Application/multipurpose
  - Load balancer
    - Scheduling
      - Affinity
      - Round-robin
    - Active-passive
    - Active-active
    - Virtual IPs
    - SSID
    - MAC filtering
    - Signal strength
    - Band selection/width
    - Antenna types and placement
    - Fat vs. thin
    - Controller-based vs. standalone
  - SIEM
    - Aggregation

        - Correlation
        - Automated alerting and triggers
        - Time synchronization
        - Event deduplication
        - Logs/WORM
    - DLP
        - USB Blocking
        - Cloud-based
        - Email
    - NAC
        - Dissolvable vs. permanent
        - Host health checks
        - Agent vs. agentless
    - Mail gateway
        - Spam filter
        - DLP
        - Encryption
    - Bridge
    - SSL/TLS accelerators
    - SSL decryptors
    - Media gateway
    - Hardware security module

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-2-software_based_security_posture_assessment
Title: Software-based Security Posture Assessment
Subtitle: CompTIA Security+ (SY0-501)

2.2 Software-based Security Posture Assessment

- 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
    - Protocol analyzer
    - Network scanners
        - Rogue system detection
        - Network mapping
    - Wireless scanners/cracker
    - Password cracker
    - Vulnerability scanner
    - Configuration compliance scanner
    - Exploitation frameworks
    - Data sanitization tools
    - Steganography tools
    - Honeypot
    - Backup utilities
    - Banner grabbing
    - Passive vs. active
    - Command line tools
        - ping
        - netstat
        - tracert
        - nslookup/dig
        - arp
        - ipconfig/ip/ifconfig
        - tcpdump
        - nmap
        - netcat

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-3-troubleshoot_common_security_issues
Title: Troubleshoot Common Security Issues
Subtitle: CompTIA Security+ (SY0-501)

2.3 Troubleshoot Common Security Issues

- 2.3 Given a scenario, troubleshoot common security issues.
    - Unencrypted credentials/clear text
    - Logs and events anomalies Permission issues
    - Access violations

    - Certificate issues Data exfiltration Misconfigured devices
        - Firewall
        - Content filter
        - Access points
    - Weak security configurations
    - Personnel issues
        - Policy violation
        - Insider threat
        - Social engineering
        - Social media
        - Personal email
    - Unauthorized software
    - Baseline deviation
    - License compliance violation (availability/integrity)
    - Asset management
    - Authentication issues

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-4-analyze_and_interpret_output_from_security_technologies
Title: Analyze and Interpret Output from Security Technologies
Subtitle: CompTIA Security+ (SY0-501)

2.4 Analyze and Interpret Output from Security Technologies

- 2.4 Given a scenario, analyze and interpret output from security technologies.
    - HIDS/HIPS
    - Antivirus
    - File integrity check
    - Host-based firewall
    - Application whitelisting
    - Removable media control
    - Advanced malware tools
    - Patch management tools
    - UTM
    - DLP
    - Data execution prevention
    - Web application firewall

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-5-deploy_mobile_security
Title: Deploy Mobile Security
Subtitle: CompTIA Security+ (SY0-501)

2.5 Deploy Mobile Security

- 2.5 Given a scenario, deploy mobile devices securely.
    - Connection methods
        - Cellular
        - WiFi
        - SATCOM
        - Bluetooth
        - NFC
        - ANT
        - Infrared
        - USB
    - Mobile device management concepts
        - Application management
        - Content management
        - Remote wipe
        - Geofencing
        - Geolocation
        - Screen locks
        - Push notification services
        - Passwords and pins
        - Biometrics
        - Context-aware authentication
        - Containerization
        - Storage segmentation

        - Full device encryption
    - Enforcement and monitoring for:
        - Third-party app stores
        - Rooting/jailbreaking
        - o Sideloading
        - Custom firmware
        - Carrier unlocking
        - Firmware OTA updates
        - Camera use
        - SMS/MMS
        - External media
        - USB OTG
        - Recording microphone
        - GPS tagging
        - WiFi direct/ad hoc
        - Tethering
        - Payment methods
    - Deployment models
        - BYOD
        - COPE
        - CYOD
        - Corporate-owned
        - VDI

        CompTIA Security + 2.0 Technologies and Tools

        ==========

Filename: comptia-secplussy0501-2-6-implement_secure_protocol
Title: Implement Secure Protocol
Subtitle: CompTIA Security+ (SY0-501)

2.6 Implement Secure Protocols

- Given a scenario, implement secure protocols
    - Protocols
        - DNSSEC
        - SSH
        - S/MIME
        - SRTP
        - LDAPS
        - FTPS
        - SFTP
        - SNMPv3
        - SSL/TLS
        - HTTPS
        - Secure POP/IMAP
    - Use cases
        - Voice and video
        - Time synchronization o Email and web
        - File transfer
        - Directory services
        - Remote access
        - Domain name resolution
        - Routing and switching
        - Network address allocation
        - Subscription services

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-1-best_practices_and_secure_configuration_guides
Title: Best Practices and Secure Configuration Guides
Subtitle: CompTIA Security+ (SY0-501)

3.1 Best Practices and Secure Configuration Guides

- 3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.
    - Industry-standard frameworks and reference architectures o Regulatory
        - Non-regulatory
        - National vs. international
        - Industry-specific frameworks
    - Benchmarks/secure configuration guides
        - Platform/vendor-specific guides

        - Web server
        - Operating system
        - Application server
        - Network infrastructure devices
      - General purpose guides
    - Defense-in-depth/layered security
      - Vendor diversity
      - Control diversity
        - Administrative
        - Technical
    - User training

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-2-secure_network_architecture_concepts
Title: Secure Network Architecture Concepts
Subtitle: CompTIA Security+ (SY0-501)

3.2 Secure Network Architecture Concepts

- 3.2 Given a scenario, implement secure network architecture concepts.
  - Zones/topologies
    - DMZ
    - Extranet
    - Intranet
    - Wireless
    - Guest
    - Honeynets
    - NAT
    - Adhoc
  - Segregation/segmentation/isolation
    - Physical
    - Logical (VLAN)
    - Virtualization
    - Air gaps
  - Tunneling/VPN
    - Site-to-site
    - Remote access
  - Security device/technology placement
    - Sensors
    - Collectors
    - Correlation engines
    - Filters
    - Proxies
    - Firewalls
    - VPN concentrators
    - SSL accelerators
    - Load balancers
    - DDoS mitigator
    - Aggregation switches
    - Taps and port mirror
  - SDN

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-3-secure_system_design
Title: Secure System Design
Subtitle: CompTIA Security+ (SY0-501)

3.3 Secure System Design

- 3.3 Given a scenario, implement secure systems design.
  - Hardware/firmware security o FDE/SED
    - TPM
    - HSM
    - UEFI/BIOS
    - Secure boot and attestation o Supply chain
    - Hardware root of trust
    - EMI/EMP
  - Operating systems

        - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile OS
        - Patch management
        - Disabling unnecessary ports and services
        - Least functionality
        - Secure configurations
        - Trusted operating system
        - Application whitelisting/blacklisting
        - Disable default accounts/passwords
    - Peripherals
        - Wireless keyboards
        - Wireless mice
        - Displays
        - WiFi-enabled MicroSD cards
        - Printers/MFDs
        - External storage devices
        - Digital cameras

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-4-secure_staging_deployment_concepts
Title: Secure Staging Deployment Concepts
Subtitle: CompTIA Security+ (SY0-501)

3.4 Secure Staging Deployment Concepts

- 3.4 Explain the importance of secure staging deployment concepts
    - Sandboxing
    - Environment
        - Development
        - Test
        - Staging
        - Production
    - Secure baseline
    - Integrity measurement

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-5-security_implications_of_embedded_systems
Title: Security Implications of Embedded Systems
Subtitle: CompTIA Security+ (SY0-501)

3.5 Security Implications of Embedded Systems

- 3.5 Explain the security implications of embedded systems.
    - SCADA/ICS
    - Smart devices/IoT
        - Wearable technology
        - Home automation
    - HVAC
    - SoC
    - RTOS
    - Printers/MFDs
    - Camera systems
    - Special purpose
        - Medical devices
        - Vehicles
        - Aircraft/UAV

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-6-security_implications_of_embedded_systems
Title: Secure Application Development and Deployment
Subtitle: CompTIA Security+ (SY0-501)

3.6 Secure Application Development and Deployment

- 3.6 Summarize secure application development and deployment concepts
  - Development life-cycle models
    - Waterfall vs. Agile
  - Secure DevOps
    - Security automation
    - Continuous integration
    - Baselining
    - Immutable systems
    - Infrastructure as code
  - Version control and change management
  - Provisioning and deprovisioning
  - Secure coding techniques
    - Proper error handling
    - Proper input validation
    - Normalization
    - Stored procedures
    - Code signing
    - Encryption
    - Obfuscation/camouflage
    - Code reuse/dead code
    - Server-side vs. client-side execution and validation
    - Memory management
    - Use of third-party libraries and SDKs
    - Data exposure
  - Code quality and testing
    - Static code analyzers
    - Dynamic analysis (e.g., fuzzing)
    - Stress testing
    - Sandboxing
    - Model verification
  - Compiled vs. runtime code

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-7-cloud_and_virtualization_concepts
Title: Cloud and Virtualization Concepts
Subtitle: CompTIA Security+ (SY0-501)

3.7 Cloud and Virtualization Concepts

- 3.7 Summarize cloud and virtualization concepts.
  - Hypervisor
    - TypeI
    - Type II
    - Application cells/containers
  - VM sprawl avoidance
  - VM escape protection
  - Cloud storage
  - Cloud deployment models
    - SaaS
    - PaaS
    - IaaS
    - Private
    - Public
    - Hybrid
    - Community
  - On-premise vs. hosted vs. cloud
  - VDI/VDE
  - Cloud access security broker
  - Security as a Service

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-8-using_resiliency_and_automation_to_reduce_risk
Title: Using Resiliency and Automation to Reduce Risk
Subtitle: CompTIA Security+ (SY0-501)

3.8 Using Resiliency and Automation to Reduce Risk

- 3.8 Explain how resiliency and automation strategies reduce risk.
  - Automation/scripting
    - Automated courses of action
    - Continuous monitoring
    - Configuration validation
  - Templates
  - Master image
  - Non-persistence
    - Snapshots
    - Revert to known state
    - Rollback to known configuration
    - Live boot media
  - Elasticity
  - Scalability
  - Distributive allocation
  - Redundancy
  - Fault tolerance
  - High availability
  - RAID

CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-9-importance_of_security_controls
Title: Importance of Physical Security
Subtitle: CompTIA Security+ (SY0-501)

3.9 Importance of Physical Security

- 3.9 Explain the importance of physical security controls.
  - Lighting
  - Signs
  - Fencing/gate/cage
  - Security guards
  - Alarms
  - Safe
  - Secure cabinets/enclosures
  - Protected distribution/Protected cabling
  - Airgap
  - Mantrap
  - Faraday cage
  - Lock types
  - Biometrics
  - Barricades/bollards
  - Tokens/cards
  - Environmental controls
    - HVAC
    - Hot and cold aisles
    - Fire suppression
  - Cable locks
  - Screen filters
  - Cameras
  - Motion detection
  - Logs
  - Infrared detection
  - Key management

CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-1-identity_and_access_management_concepts
Title: Identity and Access Managements Concepts
Subtitle: CompTIA Security+ (SY0-501)

4.1 Identity and Access Managements Concept

- 4.1 Compare and contrast identity and access management concepts.
  - Identification, authentication, authorization and accounting (AAA)
  - Multifactor authentication

        - Something you are
        - Something you have
        - Something you know
        - Somewhere you are
        - Something you do
    - Federation
    - Single sign-on
    - Transitive trust

CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-2-identity_and_access_services
Title: Identity and Access Services
Subtitle: CompTIA Security+ (SY0-501)

4.2 Identity and Access Services

- 4.2 Given a scenario, install and configure identity and access services
    - LDAP
    - Kerberos
    - TACACS+
    - CHAP
    - PAP
    - MSCHAP
    - RADIUS
    - SAML
    - OpenID Connect
    - OAUTH
    - Shibboleth
    - Secure token
    - NTLM

CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-3-identity_and_access_management_controls
Title: Identity and Access Management Controls
Subtitle: CompTIA Security+ (SY0-501)

4.3 Identity and Access Management Controls

- 4.3 Given a scenario, implement identity and access management controls.
    - Access control models
        - MAC
        - DAC
        - ABAC
        - Role-based access control
        - Rule-based access control
    - Physical access control
        - Proximity cards
        - Smart cards
    - Biometric factors
        - Fingerprint scanner
        - Retinal scanner
        - Iris scanner
        - Voice recognition
        - Facial recognition
        - False acceptance rate
        - False rejection rate
        - Crossover error rate
    - Tokens
        - Hardware
        - Software
        - HOTP/TOTP
    - Certificate-based authentication
        - PIV/CAC/smart card
        - IEEE 802.1x
    - File system security
    - Database security

CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-4-common_account_management_practices
Title: Common Account Management Practices
Subtitle: CompTIA Security+ (SY0-501)

4.4 Common Account Management Practices

- 4.4 Given a scenario, differentiate common account management practices.
  - Account types
    - User account
    - Shared and generic accounts/credentials
    - Guest accounts
    - Service accounts
    - Privileged accounts
  - General Concepts
    - Least privilege
    - Onboarding/offboarding
    - Permission auditing and review
    - Usage auditing and review
    - Time-of-day restrictions
    - Recertification
    - Standard naming convention
    - Account maintenance
    - Group-based access control
    - Location-based policies
  - Account policy enforcement
    - Credential management
    - Group policy
    - Password complexity o Expiration
    - Recovery
    - Disablement
    - Lockout
    - Password history
    - Password reuse
    - Password length

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-1-policies_plans_and_procedures
Title: Policies, Plans, and Procedures
Subtitle: CompTIA Security+ (SY0-501)

5.1 Policies, Plans, and Procedures

- 5.1 Explain the importance of policies, plans and procedures related to organizational security.
  - Standard operating procedure
  - Agreement types
    - BPA
    - SLA
    - ISA
    - MOU/MOA
  - Personnel management
    - Mandatory vacations
    - Job rotation
    - Separation of duties
    - Clean desk
    - Background checks
    - Exit interviews
    - Role-based awareness training
      - Data owner
      - System administrator
      - System owner
      - User
      - Privileged user
      - Executive user
    - NDA
    - Onboarding
    - Continuing education
    - Acceptable use policy/rules of behavior

        - Adverse actions
            - General security policies
            - Social media networks/applications
            - Personal email

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-2-impact_business_analysis
Title: Impact Business Analysis
Subtitle: CompTIA Security+ (SY0-501)

5.2 Impact Business Analysis

- 5.2 Summarize business impact analysis concepts.
    - MTBF
    - MTTR
    - Mission-essential functions
    - Identification of critical systems
    - Single point of failure
    - Impact
        - Life
        - Property
        - Safety
        - Finance
        - Reputation
    - Privacy impact assessment
    - Privacy threshold assessment

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-3-risk_management_processes_and_concepts
Title: Risk Management Processes and Concepts
Subtitle: CompTIA Security+ (SY0-501)

5.3 Risk Management Processes and Concepts

- 5.3 Explain risk management processes and concepts.
    - Threat assessment
        - Environmental
        - Manmade
        - Internal vs. external
    - Risk assessment
        - SLE
        - ALE
        - ARO
        - Asset value
        - Risk register
        - Likelihood of occurrence
        - Supply chain assessment
        - Impact
        - Quantitative
        - Qualitative
        - Testing
            - Penetration testing authorization
            - Vulnerability testing authorization
        - Risk response techniques
            - Accept
            - Transfer
            - Avoid
            - Mitigate
    - Change management

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-4-incident_response_procedures
Title: Incident Response Procedures
Subtitle: CompTIA Security+ (SY0-501)

5.4 Incident Response Procedures

- 5.4 Given a scenario, follow incident response procedures.
  - Incident response plan
    - Documented incident types/category definitions
    - Roles and responsibilities
    - Reporting requirements/escalation
    - Cyber-incident response teams
    - Exercise
  - Incident response process
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery
    - Lessons learned

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-5-basic_concepts_of_forensics
Title: Basic Concepts of Forensics
Subtitle: CompTIA Security+ (SY0-501)

5.5 Incident Response Procedures

- 5.5 Summarize basic concepts of forensics.
  - Order of volatility
  - Chain of custody
  - Legal hold
  - Data acquisition
    - Capture system image
    - Network traffic and logs
    - Capture video
    - Record time offset
    - Take hashes
    - Screenshots
    - Witness interviews
  - Preservation
  - Recovery
  - Strategic intelligence/counterintelligence gathering
    - Active logging
  - Track man-hours

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-6-disaster_recovery_and_business_continuity
Title: Disaster Recovery and Business Continuity
Subtitle: CompTIA Security+ (SY0-501)

5.6 Disaster Recovery and Business Continuity

- 5.6 Explain disaster recovery and continuity of operation concepts.
  - Recovery sites o Hot site
    - Warm site
    - Cold site
  - Order of restoration
  - Backup concepts o Differential
    - Incremental
    - Snapshots
    - Full
  - Geographic considerations
    - Off-site backups
    - Distance
    - Location selection
    - Legal implications
    - Data sovereignty
  - Continuity of operation planning
    - Exercises/tabletop
    - After-action reports

        - Failover
        - Alternate processing sites
        - Alternate business practices

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-7-types_of_controls
Title: Types of Controls
Subtitle: CompTIA Security+ (SY0-501)

5.7 Types of Controls

- 5.7 Compare and contrast various types of controls.
    - Deterrent
    - Preventive
    - Detective
    - Corrective
    - Compensating
    - Technical
    - Administrative
    - Physical

CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-8-data_security_and_privacy_practices
Title: Data Security and Privacy Practices
Subtitle: CompTIA Security+ (SY0-501)

5.8 Data Security and Privacy Practices

- 5.8 Given a scenario, carry out data security and privacy practices.
    - Data destruction and media sanitization o Burning
        - Shredding
        - Pulping
        - Pulverizing
        - Degaussing
        - Purging
        - Wiping
    - Data sensitivity labeling and handling
        - Confidential
        - Private
        - Public
        - Proprietary
        - PII
        - PHI
    - Data roles
        - Owner
        - Steward/custodian
        - Privacy officer
    - Data retention
    - Legal and compliance

CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-1-basic_concepts_of_cryptography
Title: Data Security and Privacy Practices
Subtitle: CompTIA Security+ (SY0-501)

6.1 Basic Concepts of Cryptography

- 6.1 Compare and contrast basic concepts of cryptography
    - Symmetric algorithms
    - Modes of operation
    - Asymmetric algorithms
    - Hashing
    - Salt, IV, nonce
    - Elliptic curve
    - Weak/deprecated algorithms

    - Key exchange
    - Digital signatures
    - Diffusion
    - Confusion
    - Collision
    - Steganography
    - Obfuscation
    - Stream vs. block
    - Key strength
    - Session keys
    - Ephemeral key
    - Secret algorithm
    - Data-in-transit
    - Data-at-rest
    - Data-in-use
    - Random/pseudo-random number generation
    - Key stretching
    - Implementation vs. algorithm selection
        - Crypto service provider
        - Crypto modules
    - Perfect forward secrecy
    - Security through obscurity
    - Common use cases
        - Low power devices
        - Low latency
        - High resiliency
        - Supporting confidentiality
        - Supporting integrity
        - Supporting obfuscation
        - Supporting authentication
        - Supporting non-repudiation
        - Resource vs. security constraints

CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-2-cryptography_algorithms_basics
Title: Data Security and Privacy Practices
Subtitle: CompTIA Security+ (SY0-501)

6.2 Cryptography Algorithms Basics

- 6.2 Explain cryptography algorithms and their basic characteristics.
    - Symmetric algorithms o AES
        - DES
        - 3DES
        - RC4
        - Blowfish/Twofish
    - Cipher modes
        - CBC
        - GCM
        - ECB
        - CTM
        - Stream vs. block
    - Asymmetric algorithms
        - RSA
        - DSA
        - Diffie-Hellman
    - Groups
    - DHE
    - ECDHE
        - Elliptic curve
        - PGP/GPG
    - Hashing algorithms
        - MD5
        - SHA
        - HMAC
        - RIPEMD
    - Key stretching algorithms
        - BCRYPT
        - PBKDF2
    - Obfuscation

        - XOR
        - ROT13
        - Substitution ciphers

CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-3-wireless_security
Title: Wireless Security
Subtitle: CompTIA Security+ (SY0-501)

6.3 Wireless Security

- 6.3 Given a scenario, install and configure wireless security settings.
    - Cryptographic protocols
        - WPA
        - WPA2
        - CCMP
        - TKIP
    - Authentication protocols
        - EAP
        - PEAP
        - EAP-FAST
        - EAP-TLS
        - EAP-TTLS
        - IEEE 802.1x
        - RADIUS Federation
    - Methods
        - PSK vs. Enterprise vs. Open
        - WPS
        - Captive portals

CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-4-public_key_infrastructure
Title: Public Key Infrastructure
Subtitle: CompTIA Security+ (SY0-501)

6.4 Public Key Infrastructure

- 6.4 Given a scenario, implement public key infrastructure.
    - Components
        - CA
        - Intermediate CA
        - CRL
        - OCSP
        - CSR
        - Certificate
        - Public key
        - Private key
        - Object identifiers (OID)
    - Concepts
        - Online vs. offline CA
        - Stapling
        - Pinning
        - Trust model
        - Key escrow
        - Certificate chaining
    - Types of certificates
        - Wildcard
        - SAN
        - Code signing
        - Self-signed
        - Machine/computer
        - Email
        - User
        - Root
        - Domain validation
        - Extended validation
    - Certificate formats
        - DER

- PEM
- PFX
- CER
- P12
- P7B