TestOut®

TestOut Security Pro – English 6.0.x

Objective Mappings:

TestOut Security Pro
CompTIA Security+ SY0-501

Revised: 2017-10-10

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Security Pro Objective

Section	Title	Objectives
1.0	**Introduction**	
1.1	Security Overview	
1.2	Using the Simulator	
2.0	**Security Basics**	
2.1	Understanding Attacks	1.3 Explain threat actor types and attributes. Types of actors o Script kiddies o Hacktivist o Organized crime o Nation states/APT o Insiders o Competitors Attributes of actors o Internal/external o Level of sophistication o Resources/funding o Intent/motivation Use of open-source intelligence 1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot
2.2	Defense Planning	3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides. Defense-in-depth/layered security

		o Vendor diversity o Control diversity ▪ Administrative ▪ Technical o User training
2.3	Access Control	4.1 Compare and contrast identity and access management concepts. Identification, authentication, authorization and accounting (AAA) Multifactor authentication o Something you are o Something you have o Something you know o Somewhere you are o Something you do Transitive trust 4.4 Given a scenario, differentiate common account management practices. General Concepts o Least privilege 5.1 Explain the importance of policies, plans and procedures related to organizational security. Personnel management o Job rotation o Separation of duties
2.4	Cryptography Basics	6.1 Compare and contrast basic concepts of cryptography. Steganography
2.5	Network Monitoring	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer

		Network scanners
2.6	Incident Response	5.4 Given a scenario, follow incident response procedures. Incident response plan o Documented incident types/category definitions o Roles and responsibilities o Reporting requirements/escalation o Cyber-incident response teams o Exercise Incident response process o Preparation o Identification o Containment o Eradication o Recovery o Lessons learned 5.5 Summarize basic concepts of forensics. Order of volatility Chain of custody Legal hold Data acquisition o Capture system image o Network traffic and logs o Capture video o Record time offset o Take hashes o Screenshots o Witness interviews Preservation Recovery Strategic intelligence/counterintelligence gathering o Active logging Track man-hours

3.0	Policies, Procedures, and Awareness	
3.1	Security Policies	4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity 5.1 Explain the importance of policies, plans and procedures related to organizational security. Agreement types o SLA Personnel management o Mandatory vacations o Job rotation o Background checks o Exit interviews o Continuing education o Acceptable use policy/rules of behavior o Adverse actions General security policies o Personal email 5.2 Summarize business impact analysis concepts. MTBF MTTR Impact o Life o Property o Safety o Finance o Reputation Privacy impact assessment Privacy threshold assessment 5.3 Explain risk management processes and concepts. Change management

		5.8 Given a scenario, carry out data security and privacy practices. Data sensitivity labeling and handling o PII Data retention Legal and compliance
3.2	Risk Management	5.3 Explain risk management processes and concepts. Threat assessment o Environmental o Manmade o Internal vs. external Risk assessment o SLE o ALE o ARO o Asset value o Risk register o Likelihood of occurrence o Supply chain assessment o Impact o Quantitative o Qualitative o Testing ▪ Penetration testing authorization ▪ Vulnerability testing authorization o Risk response techniques ▪ Accept ▪ Transfer ▪ Avoid ▪ Mitigate
3.3	Business Continuity	5.3 Explain risk management processes and concepts. Risk assessment o Risk response techniques ▪ Accept ▪ Transfer

		▪ Avoid ▪ Mitigate 5.6 Explain disaster recovery and continuity of operation concepts. Recovery sites o Hot site o Warm site o Cold site Order of restoration Backup concepts o Differential o Incremental o Snapshots o Full Geographic considerations o Off-site backups o Distance o Location selection o Legal implications o Data sovereignty Continuity of operation planning o Exercises/tabletop o After-action reports o Failover o Alternate processing sites o Alternate business practices
3.4	Manageable Network Plan	3.3 Given a scenario, implement secure systems design. Operating systems o Patch management
3.5	Social Engineering	1.2 Compare and contrast types of attacks. Social engineering o Phishing o Spear phishing o Whaling

		o Vishing o Tailgating o Impersonation o Dumpster diving o Shoulder surfing o Hoax o Watering hole attack o Principles (reasons for effectiveness) ▪ Authority ▪ Intimidation ▪ Consensus ▪ Scarcity ▪ Familiarity ▪ Trust ▪ Urgency
3.6	App Development and Deployment	3.6 Summarize secure application development and deployment concepts. Development life-cycle models o Waterfall vs. Agile
3.7	Employee Management	5.1 Explain the importance of policies, plans and procedures related to organizational security. Standard operating procedure Personnel management o Mandatory vacations o Job rotation o Separation of duties o Clean desk o Background checks o Exit interviews o Role-based awareness training ▪ Data owner ▪ System administrator ▪ System owner ▪ User ▪ Privileged user ▪ Executive user o NDA

		o Onboarding o Continuing education o Acceptable use policy/rules of behavior o Adverse actions General security policies o Social media networks/applications o Personal email
3.8	Mobile Devices	2.5 Given a scenario, deploy mobile devices securely. Mobile device management concepts o Remote wipe o Screen locks o Passwords and pins o Storage segmentation o Full device encryption
3.9	Third-Party Integration	4.4 Given a scenario, differentiate common account management practices. General Concepts o Onboarding/offboarding 5.1 Explain the importance of policies, plans and procedures related to organizational security. Agreement types o BPA o SLA o ISA o MOU/MOA Personnel management o Onboarding
4.0	**Physical**	
4.1	Physical Threats	2.7 Compare and contrast physical security and environmental controls

Physical security
- Hardware locks
- Mantraps
- Video Surveillance
- Fencing
- Proximity readers
- Access list
- Proper lighting
- Signs
- Guards
- Barricades
- Biometrics
- Protected distribution (cabling)
- Alarms
- Motion detection

Control types
- Deterrent
- Preventive
- Detective
- Compensating
- Technical
- Administrative

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
Mantrap
Lock types
Biometrics
Barricades/bollards
Tokens/cards
Cameras
Motion detection
Logs
Infrared detection

		Key management
4.2	Device Protection	2.7 Compare and contrast physical security and environmental controls. Physical security o Hardware locks o Proximity readers o Protected distribution (cabling) o Alarms o Motion detection
4.3	Network Infrastructure Protection	1.2 Compare and contrast types of attacks. Application/service attacks o DNS poisoning o Domain hijacking o Man-in-the-browser 3.2 Given a scenario, implement secure network architecture concepts. SDN
4.4	Environmental Controls	2.7 Compare and contrast physical security and environmental controls Environmental controls o HVAC o Fire suppression o EMI shielding o Hot and cold aisles o Environmental monitoring o Temperature and humidity controls 3.9 Explain the importance of physical security controls. Airgap Environmental controls

		o HVAC o Hot and cold aisles o Fire suppression
5.0	**Perimeter**	
5.1	Recon and Denial	1.2 Compare and contrast types of attacks. Application/service attacks o DoS o DDoS 1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot Initial exploitation Ports Persistence Escalation of privilege Black box White box Gray box Pen testing vs. vulnerability scanning
5.2	Spoofing and Poisoning	1.2 Compare and contrast types of attacks. Application/service attacks o Man-in-the-middle o ARP poisoning o DNS poisoning o Domain hijacking o Replay o Hijacking and related attacks ▪ Session hijacking o MAC spoofing

		o IP spoofing
5.3	Security Appliances	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Proxy NAC Mail gateway o Spam filter 3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o DMZ o Extranet o Intranet o Wireless o Guest o Honeynets o Ad hoc Security device/technology placement o Filters o Proxies
5.4	Demilitarized Zones (DMZ)	3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o DMZ
5.5	Firewalls	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Firewall o ACL o Application-based vs. network-based o Stateful vs. stateless o Implicit deny

		2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Firewall 2.4 Given a scenario, analyze and interpret output from security technologies. Host-based firewall 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Filters o Proxies o Firewalls
5.6	Network Address Translation (NAT)	3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o NAT
5.7	Virtual Private Networks (VPN)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. VPN concentrator o Remote access vs. site-to-site o IPSec ▪ Tunnel mode ▪ Transport mode ▪ AH ▪ ESP o Split tunnel vs. full tunnel o TLS o Always-on VPN 3.2 Given a scenario, implement secure network architecture concepts. Tunneling/VPN o Site-to-site

		o Remote access Security device/technology placement o VPN concentrators
5.8	Web Threat Protection	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Proxy o Forward and reverse proxy o Transparent o Application/multipurpose Mail gateway o Spam filter o DLP o Encryption 2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Content filter 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Filters o Proxies
5.9	Network Access Control (NAC)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. NAC o Dissolvable vs. permanent o Host health checks o Agent vs. agentless
5.10	Wireless Overview	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Access point

		o SSID o MAC filtering o Signal strength o Band selection/width o Antenna types and placement o Fat vs. thin o Controller-based vs. standalone Bridge 3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o Wireless o Ad hoc 6.3 Given a scenario, install and configure wireless security settings. Cryptographic protocols o WPA o WPA2 o CCMP o TKIP Authentication protocols o EAP o PEAP o EAP-FAST o EAP-TLS o EAP-TTLS o IEEE 802.1x o RADIUS Federation Methods o PSK vs. Enterprise vs. Open o WPS o Captive portals
5.11	Wireless Attacks	1.2 Compare and contrast types of attacks. Wireless attacks o Replay o IV o Evil twin

		o Rogue AP o Jamming o WPS o Bluejacking o Bluesnarfing o RFID o NFC o Disassociation
5.12	Wireless Defenses	1.6 Explain the impact associated with types of vulnerabilities. Misconfiguration/weak configuration Default configuration 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Access point o SSID o MAC filtering o Signal strength o Band selection/width o Antenna types and placement o Fat vs. thin o Controller-based vs. standalone 2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Access points 6.3 Given a scenario, install and configure wireless security settings. Authentication protocols o EAP o PEAP o EAP-FAST o EAP-TLS o EAP-TTLS o IEEE 802.1x o RADIUS Federation

		Methods o PSK vs. Enterprise vs. Open
6.0	**Network**	
6.1	Network Threats	1.6 Explain the impact associated with types of vulnerabilities. Untrained users 3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Physical o Logical (VLAN) 5.3 Explain risk management processes and concepts. Threat assessment o Internal vs. external
6.2	Network Device Vulnerabilities	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware. Backdoor 1.2 Compare and contrast types of attacks. Application/service attacks o Privilege escalation 3.3 Given a scenario, implement secure systems design. Operating systems o Disable default accounts/passwords Given a scenario, differentiate common account management practices. Account policy enforcement

		o Password complexity
6.3	Network Applications	3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services
6.4	Switch Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o ARP poisoning o MAC spoofing
6.5	Switch Security	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security o Layer 2 vs. Layer 3 o Loop prevention o Flood guard Access point o MAC filtering 3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Logical (VLAN) Security device/technology placement o Filters o Aggregation switches
6.6	Using VLANs	3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation

		o Logical (VLAN)
6.7	Router Security	1.6 Explain the impact associated with types of vulnerabilities. Misconfiguration/weak configuration Default configuration 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Router o ACLs o Antispoofing
6.8	Intrusion Detection and Prevention	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. NIPS/NIDS o Signature-based o Heuristic/behavioral o Anomaly o Inline vs. passive o In-band vs. out-of-band o Rules o Analytics ▪ False positive ▪ False negative
6.9	Vulnerability Assessment	1.4 Explain penetration testing concepts. Ports 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 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Network scanners o Rogue system detection o Network mapping Wireless scanners/cracker Password cracker Vulnerability scanner Command line tools o ping 3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services o Secure configurations
6.10	Protocol Analyzers	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer
6.11	Remote Access	2.6 Given a scenario, implement secure protocols. Protocols

		o SNMPv3 o SSL/TLS Use cases o Remote access 4.2 Given a scenario, install and configure identity and access services. TACACS+ CHAP PAP MSCHAP RADIUS
6.12	Network Authentication	4.2 Given a scenario, install and configure identity and access services. LDAP Kerberos SAML OpenID Connect OAUTH Shibboleth Secure token NTLM
6.13	Penetration Testing	1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot Initial exploitation Ports Persistence Escalation of privilege Black box White box Gray box Pen testing vs. vulnerability scanning

		5.3 Explain risk management processes and concepts. Risk assessment o Testing ▪ Penetration testing authorization ▪ Vulnerability testing authorization
6.14	Virtual Networking	3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Virtualization 3.7 Summarize cloud and virtualization concepts. Hypervisor o Type I o Type II o Application cells/containers VM sprawl avoidance VM escape protection VDI/VDE
6.15	Software-Defined Networking (SDN)	3.2 Given a scenario, implement secure network architecture concepts. SDN
6.16	Cloud Services	3.7 Summarize cloud and virtualization concepts. Cloud storage Cloud deployment models o SaaS o PaaS o IaaS o Private o Public o Hybrid o Community

		On-premise vs. hosted vs. cloud VDI/VDE Cloud access security broker Security as a Service
7.0	**Host**	
7.1	Malware	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware. Viruses Crypto-malware Ransomware Worm Trojan Rootkit Keylogger Adware Spyware Bots RAT Logic bomb Backdoor
7.2	Password Attacks	1.2 Compare and contrast types of attacks. Cryptographic attacks o Birthday o Known plain text/cipher text o Rainbow tables o Dictionary o Brute force ▪ Online vs offline o Collision o Downgrade o Replay o Weak implementations

		2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer Network scanners o Rogue system detection o Network mapping Wireless scanners/cracker Password cracker 4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity
7.3	Windows System Hardening	2.4 Given a scenario, analyze and interpret output from security technologies. Patch management tools Web application firewall 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Firewalls 3.3 Given a scenario, implement secure systems design. Operating systems o Patch management o Trusted operating system
7.4	Hardening Enforcement	3.3 Given a scenario, implement secure systems design. Operating systems o Secure configurations 4.4 Given a scenario, differentiate common account management practices. General Concepts

		o Group-based access control Account policy enforcement o Group policy
7.5	File Server Security	3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services o Least functionality 4.4 Given a scenario, differentiate common account management practices. General Concepts o Least privilege
7.6	Linux Host Security	1.4 Explain penetration testing concepts. Ports 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security 3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services
7.7	Embedded Systems	1.6 Explain the impact associated with types of vulnerabilities. Vulnerabilities due to: o Embedded systems 3.5 Explain the security implications of embedded systems SCADA/ICS

		Smart devices/IoT o Wearable technology o Home automation HVAC SoC RTOS Printers/MFDs Camera systems Special purpose o Medical devices o Vehicles o Aircraft/UAV
7.8	Log Management	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. SIEM o Aggregation o Correlation o Automated alerting and triggers o Time synchronization o Event deduplication o Logs/WORM 2.3 Given a scenario, troubleshoot common security issues. Logs and events anomalies
7.9	Audits	4.4 Given a scenario, differentiate common account management practices. General Concepts o Permission auditing and review o Usage auditing and review
7.10	Email	5.1 Explain the importance of policies, plans and procedures related to organizational security. General security policies o Personal email

		6.4 Given a scenario, implement public key infrastructure. Types of certificates o Email
7.11	BYOD Security	2.5 Given a scenario, deploy mobile devices securely. Deployment models o BYOD o COPE o CYOD o Corporate-owned o VDI
7.12	Mobile Device Management	2.5 Given a scenario, deploy mobile devices securely. Connection methods o Cellular o WiFi o SATCOM o Bluetooth o NFC o ANT o Infrared o USB Mobile device management concepts o Application management o Content management o Remote wipe o Geofencing o Geolocation o Screen locks o Push notification services o Passwords and pins o Biometrics o Context-aware authentication o Containerization o Storage segmentation o Full device encryption Enforcement and monitoring for: o Third-party app stores

		o Rooting/jailbreaking o Sideloading o Custom firmware o Carrier unlocking o Firmware OTA updates o Camera use o SMS/MMS o External media o USB OTG o Recording microphone o GPS tagging o WiFi direct/ad hoc o Tethering o Payment methods Deployment models o BYOD 3.3 Given a scenario, implement secure systems design. Operating systems o Types ▪ Mobile OS
7.13	Host Virtualization	3.7 Summarize cloud and virtualization concepts. Hypervisor o Type I o Type II o Application cells/containers VDI/VDE
8.0	**Application**	
8.1	Access Control Models	4.1 Compare and contrast identity and access management concepts. Transitive trust 4.3 Given a scenario, implement identity and access management controls.

		Access control models o MAC o DAC o ABAC o Role-based access control o Rule-based access control
8.2	Authentication	4.1 Compare and contrast identity and access management concepts. Multifactor authentication o Something you are o Something you have o Something you know o Somewhere you are o Something you do Single sign-on 4.3 Given a scenario, implement identity and access management controls. Biometric factors o Fingerprint scanner o Retinal scanner o Iris scanner o Voice recognition o Facial recognition o False acceptance rate o False rejection rate o Crossover error rate
8.3	Authorization	4.3 Given a scenario, implement identity and access management controls. File system security 4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control

8.4	Web Application Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o Buffer overflow o Injection o Cross-site scripting o Cross-site request forgery o Zero day o Hijacking and related attacks ▪ Clickjacking ▪ Session hijacking ▪ URL hijacking ▪ Typo squatting o Driver manipulation ▪ Shimming ▪ Refactoring 1.6 Explain the impact associated with types of vulnerabilities. Memory/buffer vulnerability o Integer overflow o Buffer overflow o DLL injection New threats/zero day
8.5	Internet Browsers	
8.6	Application Development	2.4 Given a scenario, analyze and interpret output from security technologies. Application whitelisting Data execution prevention 3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services o Least functionality o Secure configurations o Application whitelisting/blacklisting

		3.4 Explain the importance of secure staging deployment concepts. Sandboxing Environment o Development o Test o Staging o Production Secure baseline Integrity measurement 3.6 Summarize secure application development and deployment concepts. Secure DevOps o Security automation o Continuous integration o Baselining o Immutable systems o Infrastructure as code Secure coding techniques o Proper error handling o Proper input validation o Normalization o Stored procedures o Code signing o Encryption o Obfuscation/camouflage o Code reuse/dead code o Server-side vs. client-side execution and validation o Memory management o Use of third-party libraries and SDKs o Data exposure Code quality and testing o Static code analyzers o Dynamic analysis (e.g., fuzzing) o Stress testing o Sandboxing o Model verification
8.7	Active Directory Overview	

8.8	Windows Domain Users and Groups	4.4 Given a scenario, differentiate common account management practices. Account types o User account o Shared and generic accounts/credentials o Guest accounts o Service accounts o Privileged accounts
8.9	Linux Users	4.4 Given a scenario, differentiate common account management practices. Account types o User account o Shared and generic accounts/credentials o Guest accounts o Service accounts o Privileged accounts
8.10	Linux Groups	
8.11	Linux User Security	4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity o Expiration o Password history o Password reuse o Password length
8.12	Group Policy Overview	4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control Account policy enforcement o Group policy
8.13	Hardening Authentication 1	4.4 Given a scenario, differentiate common account management practices.

		General Concepts o Group-based access control Account policy enforcement o Group policy o Password complexity o Expiration o Recovery o Disablement o Lockout o Password history o Password reuse o Password length
8.14	Hardening Authentication 2	3.9 Explain the importance of physical security controls. Tokens/cards 4.3 Given a scenario, implement identity and access management controls. Physical access control o Smart cards Certificate-based authentication o PIV/CAC/smart card
9.0	**Data**	
9.1	Data Management	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Data sanitization tools 5.8 Given a scenario, carry out data security and privacy practices. Data destruction and media sanitization o Burning o Shredding o Pulping o Pulverizing o Degaussing

		o Purging o Wiping Data sensitivity labeling and handling o Confidential o Private o Public o Proprietary o PII o PHI Data roles o Owner o Steward/custodian o Privacy officer Data retention Legal and compliance
9.2	Advanced 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 o Crypt service provider o Crypt modules Perfect forward secrecy Security through obscurity Common use cases o Low power devices o Low latency o High resiliency o Supporting confidentiality o Supporting integrity o Supporting obfuscation o Supporting authentication o Supporting non-repudiation o Resource vs. security constraints
9.3	Cryptography Implementations	3.3 Given a scenario, implement secure systems design. Hardware/firmware security o TPM o HSM 5.1 Explain the importance of policies, plans and procedures related to organizational security. General security policies o Social media networks/applications o Personal email 6.1 Compare and contrast basic concepts of cryptography. Digital signatures 6.2 Explain cryptography algorithms and their basic characteristics. Asymmetric algorithms o PGP/GPG 6.4 Given a scenario, implement public key infrastructure. Types of certificates

		o Email Certificate formats o PEM
9.4	Cryptographic Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o Man-in-the-middle o Replay Cryptographic attacks o Birthday o Known plain text/cipher text o Dictionary o Brute force ▪ Online vs. offline o Replay o Weak implementations
9.5	Symmetric Encryption	6.1 Compare and contrast basic concepts of cryptography. Symmetric algorithms Modes of operation Hashing Salt, IV, nonce Weak/deprecated algorithms Stream vs. block Key strength Secret algorithm Key stretching 6.2 Explain cryptography algorithms and their basic characteristics. Symmetric algorithms o AES o DES o 3DES o RC4 o Blowfish/Twofish Cipher modes o CBC o ECB

		o Stream vs. block Hashing algorithms o MD5 o SHA o HMAC o RIPEMD Key stretching algorithms o BCRYPT o PBKDF2
9.6	Asymmetric Encryption	6.1 Compare and contrast basic concepts of cryptography. Modes of operation Asymmetric algorithms Elliptic curve Weak/deprecated algorithms Key exchange Digital signatures Key strength Session keys Ephemeral key Secret algorithm Data-in-transit Data-at-rest Data-in-use Perfect forward secrecy Common use cases o Supporting confidentiality o Supporting integrity o Supporting authentication o Supporting non-repudiation o Resource vs. security constraints 6.2 Explain cryptography algorithms and their basic characteristics. Asymmetric algorithms o RSA o DSA o Diffie-Hellman ▪ Groups ▪ DHE ▪ ECDHE

		o Elliptic curve o PGP/GPG
9.7	File Encryption	6.2 Explain cryptography algorithms and their basic characteristics. Symmetric algorithms o AES o DES o 3DES Asymmetric algorithms o RSA o DSA o Elliptic curve o PGP/GPG
9.8	Public Key Infrastructure (PKI)	6.4 Given a scenario, implement public key infrastructure. Components o CA o CRL o OCSP o CSR o Certificate o Public key o Private key Concepts o Online vs. offline CA o Key escrow
9.9	Hashing	6.1 Compare and contrast basic concepts of cryptography. Hashing Collision 6.2 Explain cryptography algorithms and their basic characteristics. Hashing algorithms o MD5 o SHA

		o HMAC o RIPEMD
9.10	Data Transmission Security	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. VPN concentrator o IPSec ▪ Tunnel mode ▪ Transport mode ▪ AH ▪ ESP o TLS 2.6 Given a scenario, implement secure protocols. Protocols o SSH o LDAPS o FTPS o SSL/TLS o HTTPS Use cases o Email and web o File transfer o Directory services
9.11	Data Loss Prevention (DLP)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. DLP o USB blocking o Cloud-based o Email 2.3 Given a scenario, troubleshoot common security issues. Data exfiltration

		2.4 Given a scenario, analyze and interpret output from security technologies. DLP
9.12	Redundancy	3.8 Explain how resiliency and automation strategies reduce risk. Elasticity Scalability Distributive allocation Redundancy Fault tolerance High availability RAID 5.2 Summarize business impact analysis concepts. RTO/RPO MTBF MTTR Mission-essential functions Identification of critical systems Single point of failure 5.6 Explain disaster recovery and continuity of operation concepts. Recovery sites o Hot site o Warm site o Cold site Order of restoration Geographic considerations o Off-site backups o Distance o Location selection o Legal implications o Data sovereignty
9.13	Backup and Restore	3.8 Explain how resiliency and automation strategies reduce risk. Templates

		Master image Non-persistence o Snapshots o Revert to known state o Rollback to known configuration o Live boot media 5.6 Explain disaster recovery and continuity of operation concepts. Backup concepts o Differential o Incremental o Snapshots o Full
9.14	Cloud Storage	3.7 Summarize cloud and virtualization concepts. Cloud access security broker

Objective Mapping: TestOut Security Pro Objective to LabSim Section

#	Domain	Module.Section
1.0	**Access Control and Identity Management**	
1.1	Create, Modify, and Delete User Profiles Manage Windows Domain Users and Groups o Create, rename, and delete users and groups o Assign users to appropriate groups o Lock and unlock user accounts o Change a user's password Manage Linux Users and Groups o Create, rename, and delete users and groups o Assign users to appropriate groups o Lock and unlock user accounts o Change a user's password o Configure password aging Manage Windows Local Users and Groups o Restrict use of local user accounts Restrict use of common access accounts	8.3, 8.8, 8.9, 8.10. 8.12, 8.13, 8.14
1.2	Harden Authentication Configure Domain GPO Account Policy to enforce a robust password policy Configure the Domain GPO to control local administrator group membership and administrator password Disable or rename default accounts, such as Guest and Administrator Configure the Domain GPO to enforce User Account Control Configure a GPO for smart card authentication for sensitive resources Configure secure remote access Implement centralized authentication	5.9 6.11 8.2, 8.12. 8.13, 8.14
1.3	Manage Certificates Approve, deny, and revoke certificate requests	9.8

	Configure Domain GPO Kerberos settings	
2.0	**Policies, Procedures, and Awareness**	
2.1	Promote Information Security Awareness Traveling with Personal Mobile Devices Exchanging content between home and work Storing personal information on the internet Using social networking sites Using SSL encryption Using email best practices Password management Photo/GPS integration Information security Auto-lock and passcode lock	3.5, 3.8 5.4 7.10, 7.11 9.3, 9.10
2.2	Evaluate Information Risk Perform risk calculation Risk avoidance, transference, acceptance, mitigation, and deterrence	3.2, 3.3 4.3
2.3	Maintain Hardware and Software Inventory	4.2
3.0	**Physical Security**	
3.1	Harden Data Center Physical Access Implement access rosters Use visitor identification and control Protect doors and windows Implement physical intrusion detection systems	4.1 6.7

3.2	Harden Mobile Devices (iPad) Apply updates Set Autolock Enable passcodes Configure network security settings	3.8 5.5 7.12
3.3	Harden Mobile Devices (Laptop) Set a BIOS password Set a login password Implement full disk encryption	5.5 7.12
4.0	**Perimeter Defenses**	
4.1	Harden the Network Perimeter (using a Cisco Network Security Appliance) Change the default user name and password Configure a firewall Create a DMZ Configure NAT Configure VPN Implement web threat protection	5.2, 5.4, 5.5, 5.6, 5.7, 5.8 6.2 8.4
4.2	Secure Wireless Devices and Clients Change the default user name, password, and administration limits Implement WPA2 Configure enhanced security o MAC filtering o SSID cloaking o Power control Disable Network Discovery	5.10, 5.12

5.0	Network Defenses	
5.1	Harden Network Devices (Using a Cisco Small Business Switch) Change the default user name and password on network devices Use secure passwords Shut down unnecessary services and ports Implement port security Remove unsecure protocols (FTP, telnet, rlogin, rsh) Implement access lists, deny everything else Run latest iOS version Turn on logging with timestamps Segment traffic using VLANs	2.11 5.12 6.2, 6.5, 6.6, 6.7, 6.9 7.2, 7.5, 7.6, 7.9 8.3, 8.11, 8.13
5.2	Implement Intrusion Detection/Prevention (Using a Cisco Network Security Appliance) Enable IPS protection for a LAN and DMZ Apply IPS signature updates Configure IPS policy	5.3
6.0	**Host Defenses**	
6.1	Harden Computer Systems Against Attack Configure a GPO to enforce workstation/server security settings Configure Domain GPO to enforce Windows Firewall use Configure Domain Servers GPO to remove unneeded services (such as file and printer sharing) Protect against spyware and unwanted software using Windows Defender Configure NTFS permissions for secure file sharing	7.3, 7.4, 7.5 8.12
6.2	Implement Patch Management/System Updates Configure Windows Update Apply the latest Apple software updates	7.3

6.3	Perform System Backups and Recovery	9.13
7.0	**Application Defenses**	
7.1	Implement Application Defenses Configure a GPO to enforce Internet Explorer settings Configure a GPO for application whitelisting Enable Data Execution Prevention (DEP) Configure web application security Configure parental controls to enforce web content filtering Configure secure browser settings Configure secure email settings Configure virtual machines and switches	6.3, 6.5, 6.10, 6.14 7.4, 7.10, 7.13 8.5, 8.6 9.3, 9.5, 9.6
7.2	Implement Patch Management/Software Updates Configure Microsoft Update	7.3
8.0	**Data Defenses**	
8.1	Protect and Maintain the Integrity of Data Files Implement encryption technologies Perform data backups and recovery Implement redundancy and failover mechanisms	5.12 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.12, 9.13
8.2	Protect Data Transmissions Across Open, Public Networks Encrypt data communications Implement secure protocols Remove unsecure protocols	5.4, 5.12 7.4 8.5 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.10

9.0	Audits and Assessments	
9.1	Implement Logging and Auditing Configure Domain GPO audit policy Configure Domain GPO for event logging	7.8, 7.9
9.2	Review Security Logs and Violation Reports, Implement Remediation	7.8, 7.9 8.1
9.3	Review Audit Reports, Implement Remediation	7.9
9.4	Review Vulnerability Reports, Implement Remediation	7.9

Objective Mapping: LabSim Section to CompTIA SY0-501 Objective

TestOut Section	Title	CompTIA Security+ Objective
1.0	**Introduction**	
1.1	Security Overview	
1.2	Using the Simulator	
2.0	**Security Basics**	
2.1	Understanding Attacks	1.3 Explain threat actor types and attributes. Types of actors o Script kiddies o Hacktivist o Organized crime o Nation states/APT o Insiders o Competitors Attributes of actors o Internal/external o Level of sophistication o Resources/funding o Intent/motivation Use of open-source intelligence 1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot

2.2	Defense Planning	3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides. Defense-in-depth/layered security o Vendor diversity o Control diversity ▪ Administrative ▪ Technical o User training
2.3	Access Control	4.1 Compare and contrast identity and access management concepts. Identification, authentication, authorization and accounting (AAA) Multifactor authentication o Something you are o Something you have o Something you know o Somewhere you are o Something you do Transitive trust 4.4 Given a scenario, differentiate common account management practices. General Concepts o Least privilege 5.1 Explain the importance of policies, plans and procedures related to organizational security. Personnel management o Job rotation o Separation of duties
2.4	Cryptography Basics	6.1 Compare and contrast basic concepts of cryptography. Steganography

2.5	Network Monitoring	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer Network scanners
2.6	Incident Response	5.4 Given a scenario, follow incident response procedures. Incident response plan o Documented incident types/category definitions o Roles and responsibilities o Reporting requirements/escalation o Cyber-incident response teams o Exercise Incident response process o Preparation o Identification o Containment o Eradication o Recovery o Lessons learned 5.5 Summarize basic concepts of forensics. Order of volatility Chain of custody Legal hold Data acquisition o Capture system image o Network traffic and logs o Capture video o Record time offset o Take hashes o Screenshots o Witness interviews Preservation Recovery Strategic intelligence/counterintelligence gathering o Active logging Track man-hours

3.0	Policies, Procedures, and Awareness	
3.1	Security Policies	4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity 5.1 Explain the importance of policies, plans and procedures related to organizational security. Agreement types o SLA Personnel management o Mandatory vacations o Job rotation o Background checks o Exit interviews o Continuing education o Acceptable use policy/rules of behavior o Adverse actions General security policies o Personal email 5.2 Summarize business impact analysis concepts. MTBF MTTR Impact o Life o Property o Safety o Finance o Reputation Privacy impact assessment Privacy threshold assessment 5.3 Explain risk management processes and concepts.

		Change management 5.8 Given a scenario, carry out data security and privacy practices. Data sensitivity labeling and handling o PII Data retention Legal and compliance
3.2	Risk Management	5.3 Explain risk management processes and concepts. Threat assessment o Environmental o Manmade o Internal vs. external Risk assessment o SLE o ALE o ARO o Asset value o Risk register o Likelihood of occurrence o Supply chain assessment o Impact o Quantitative o Qualitative o Testing ▪ Penetration testing authorization ▪ Vulnerability testing authorization o Risk response techniques ▪ Accept ▪ Transfer ▪ Avoid ▪ Mitigate
3.3	Business Continuity	5.3 Explain risk management processes and concepts. Risk assessment o Risk response techniques

		▪ Accept ▪ Transfer ▪ Avoid ▪ Mitigate 5.6 Explain disaster recovery and continuity of operation concepts. Recovery sites o Hot site o Warm site o Cold site Order of restoration Backup concepts o Differential o Incremental o Snapshots o Full Geographic considerations o Off-site backups o Distance o Location selection o Legal implications o Data sovereignty Continuity of operation planning o Exercises/tabletop o After-action reports o Failover o Alternate processing sites o Alternate business practices
3.4	Manageable Network Plan	3.3 Given a scenario, implement secure systems design. Operating systems o Patch management
3.5	Social Engineering	1.2 Compare and contrast types of attacks. Social engineering o Phishing

		o Spear phishing o Whaling o Vishing o Tailgating o Impersonation o Dumpster diving o Shoulder surfing o Hoax o Watering hole attack o Principles (reasons for effectiveness) ▪ Authority ▪ Intimidation ▪ Consensus ▪ Scarcity ▪ Familiarity ▪ Trust ▪ Urgency
3.6	App Development and Deployment	3.6 Summarize secure application development and deployment concepts. Development life-cycle models o Waterfall vs. Agile
3.7	Employee Management	5.1 Explain the importance of policies, plans and procedures related to organizational security. Standard operating procedure Personnel management o Mandatory vacations o Job rotation o Separation of duties o Clean desk o Background checks o Exit interviews o Role-based awareness training ▪ Data owner ▪ System administrator ▪ System owner ▪ User ▪ Privileged user

		▪ Executive user o NDA o Onboarding o Continuing education o Acceptable use policy/rules of behavior o Adverse actions General security policies o Social media networks/applications o Personal email
3.8	Mobile Devices	2.5 Given a scenario, deploy mobile devices securely. Mobile device management concepts o Remote wipe o Screen locks o Passwords and pins o Storage segmentation o Full device encryption
3.9	Third-Party Integration	4.4 Given a scenario, differentiate common account management practices. General Concepts o Onboarding/offboarding 5.1 Explain the importance of policies, plans and procedures related to organizational security. Agreement types o BPA o SLA o ISA o MOU/MOA Personnel management o Onboarding
4.0	**Physical**	

4.1	Physical Threats	2.7 Compare and contrast physical security and environmental controls Physical security o Hardware locks o Mantraps o Video Surveillance o Fencing o Proximity readers o Access list o Proper lighting o Signs o Guards o Barricades o Biometrics o Protected distribution (cabling) o Alarms o Motion detection Control types o Deterrent o Preventive o Detective o Compensating o Technical o Administrative 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 Mantrap Lock types Biometrics Barricades/bollards Tokens/cards Cameras Motion detection

		Logs Infrared detection Key management
4.2	Device Protection	2.7 Compare and contrast physical security and environmental controls. Physical security o Hardware locks o Proximity readers o Protected distribution (cabling) o Alarms o Motion detection
4.3	Network Infrastructure Protection	1.2 Compare and contrast types of attacks. Application/service attacks o DNS poisoning o Domain hijacking o Man-in-the-browser 3.2 Given a scenario, implement secure network architecture concepts. SDN
4.4	Environmental Controls	2.7 Compare and contrast physical security and environmental controls Environmental controls o HVAC o Fire suppression o EMI shielding o Hot and cold aisles o Environmental monitoring o Temperature and humidity controls 3.9 Explain the importance of physical security controls.

		Airgap Environmental controls o HVAC o Hot and cold aisles o Fire suppression
5.0	**Perimeter**	
5.1	Recon and Denial	1.2 Compare and contrast types of attacks. Application/service attacks o DoS o DDoS 1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot Initial exploitation Ports Persistence Escalation of privilege Black box White box Gray box Pen testing vs. vulnerability scanning
5.2	Spoofing and Poisoning	1.2 Compare and contrast types of attacks. Application/service attacks o Man-in-the-middle o ARP poisoning o DNS poisoning o Domain hijacking o Replay o Hijacking and related attacks

		▪ Session hijacking o MAC spoofing o IP spoofing
5.3	Security Appliances	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Proxy NAC Mail gateway o Spam filter 3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o DMZ o Extranet o Intranet o Wireless o Guest o Honeynets o Ad hoc Security device/technology placement o Filters o Proxies
5.4	Demilitarized Zones (DMZ)	3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o DMZ
5.5	Firewalls	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Firewall o ACL o Application-based vs. network-based o Stateful vs. stateless

		o Implicit deny 2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Firewall 2.4 Given a scenario, analyze and interpret output from security technologies. Host-based firewall 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Filters o Proxies o Firewalls
5.6	Network Address Translation (NAT)	3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o NAT
5.7	Virtual Private Networks (VPN)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. VPN concentrator o Remote access vs. site-to-site o IPSec ▪ Tunnel mode ▪ Transport mode ▪ AH ▪ ESP o Split tunnel vs. full tunnel o TLS o Always-on VPN 3.2 Given a scenario, implement secure network architecture concepts.

		Tunneling/VPN o Site-to-site o Remote access Security device/technology placement o VPN concentrators
5.8	Web Threat Protection	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Proxy o Forward and reverse proxy o Transparent o Application/multipurpose Mail gateway o Spam filter o DLP o Encryption 2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Content filter 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Filters o Proxies
5.9	Network Access Control (NAC)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. NAC o Dissolvable vs. permanent o Host health checks o Agent vs. agentless

5.10	Wireless Overview	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Access point o SSID o MAC filtering o Signal strength o Band selection/width o Antenna types and placement o Fat vs. thin o Controller-based vs. standalone Bridge 3.2 Given a scenario, implement secure network architecture concepts. Zones/topologies o Wireless o Ad hoc 6.3 Given a scenario, install and configure wireless security settings. Cryptographic protocols o WPA o WPA2 o CCMP o TKIP Authentication protocols o EAP o PEAP o EAP-FAST o EAP-TLS o EAP-TTLS o IEEE 802.1x o RADIUS Federation Methods o PSK vs. Enterprise vs. Open o WPS o Captive portals

5.11	Wireless Attacks	1.2 Compare and contrast types of attacks. Wireless attacks o Replay o IV o Evil twin o Rogue AP o Jamming o WPS o Bluejacking o Bluesnarfing o RFID o NFC o Disassociation
5.12	Wireless Defenses	1.6 Explain the impact associated with types of vulnerabilities. Misconfiguration/weak configuration Default configuration 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Access point o SSID o MAC filtering o Signal strength o Band selection/width o Antenna types and placement o Fat vs. thin o Controller-based vs. standalone 2.3 Given a scenario, troubleshoot common security issues. Misconfigured devices o Access points 6.3 Given a scenario, install and configure wireless security settings. Authentication protocols o EAP

		o PEAP o EAP-FAST o EAP-TLS o EAP-TTLS o IEEE 802.1x o RADIUS Federation Methods o PSK vs. Enterprise vs. Open
6.0	**Network**	
6.1	Network Threats	1.6 Explain the impact associated with types of vulnerabilities. Untrained users 3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Physical o Logical (VLAN) 5.3 Explain risk management processes and concepts. Threat assessment o Internal vs. external
6.2	Network Device Vulnerabilities	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware. Backdoor 1.2 Compare and contrast types of attacks. Application/service attacks o Privilege escalation 3.3 Given a scenario, implement secure systems design.

		Operating systems o Disable default accounts/passwords Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity
6.3	Network Applications	3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services
6.4	Switch Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o ARP poisoning o MAC spoofing
6.5	Switch Security	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security o Layer 2 vs. Layer 3 o Loop prevention o Flood guard Access point o MAC filtering 3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Logical (VLAN) Security device/technology placement o Filters

		o Aggregation switches
6.6	Using VLANs	3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Logical (VLAN)
6.7	Router Security	1.6 Explain the impact associated with types of vulnerabilities. Misconfiguration/weak configuration Default configuration 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Router o ACLs o Antispoofing
6.8	Intrusion Detection and Prevention	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. NIPS/NIDS o Signature-based o Heuristic/behavioral o Anomaly o Inline vs. passive o In-band vs. out-of-band o Rules o Analytics ▪ False positive ▪ False negative

6.9	Vulnerability Assessment	1.4 Explain penetration testing concepts. Ports 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 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Network scanners o Rogue system detection o Network mapping Wireless scanners/cracker Password cracker Vulnerability scanner Command line tools o ping 3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services o Secure configurations

6.10	Protocol Analyzers	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer
6.11	Remote Access	2.6 Given a scenario, implement secure protocols. Protocols o SNMPv3 o SSL/TLS Use cases o Remote access 4.2 Given a scenario, install and configure identity and access services. TACACS+ CHAP PAP MSCHAP RADIUS
6.12	Network Authentication	4.2 Given a scenario, install and configure identity and access services. LDAP Kerberos SAML OpenID Connect OAUTH Shibboleth Secure token NTLM
6.13	Penetration Testing	1.4 Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot Initial exploitation

		Ports Persistence Escalation of privilege Black box White box Gray box Pen testing vs. vulnerability scanning 5.3 Explain risk management processes and concepts. Risk assessment o Testing ▪ Penetration testing authorization ▪ Vulnerability testing authorization
6.14	Virtual Networking	3.2 Given a scenario, implement secure network architecture concepts. Segregation/segmentation/isolation o Virtualization 3.7 Summarize cloud and virtualization concepts. Hypervisor o Type I o Type II o Application cells/containers VM sprawl avoidance VM escape protection VDI/VDE
6.15	Software-Defined Networking (SDN)	3.2 Given a scenario, implement secure network architecture concepts. SDN
6.16	Cloud Services	3.7 Summarize cloud and virtualization concepts.

		Cloud storage Cloud deployment models o SaaS o PaaS o IaaS o Private o Public o Hybrid o Community On-premise vs. hosted vs. cloud VDI/VDE Cloud access security broker Security as a Service
7.0	**Host**	
7.1	Malware	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware. Viruses Crypto-malware Ransomware Worm Trojan Rootkit Keylogger Adware Spyware Bots RAT Logic bomb Backdoor
7.2	Password Attacks	1.2 Compare and contrast types of attacks. Cryptographic attacks o Birthday o Known plain text/cipher text o Rainbow tables o Dictionary o Brute force

		▪ Online vs offline o Collision o Downgrade o Replay o Weak implementations 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer Network scanners o Rogue system detection o Network mapping Wireless scanners/cracker Password cracker 4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity
7.3	Windows System Hardening	2.4 Given a scenario, analyze and interpret output from security technologies. Patch management tools Web application firewall 3.2 Given a scenario, implement secure network architecture concepts. Security device/technology placement o Firewalls 3.3 Given a scenario, implement secure systems design. Operating systems o Patch management o Trusted operating system
7.4	Hardening Enforcement	3.3 Given a scenario, implement secure systems design. Operating systems

		o Secure configurations 4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control Account policy enforcement o Group policy
7.5	File Server Security	3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services o Least functionality 4.4 Given a scenario, differentiate common account management practices. General Concepts o Least privilege
7.6	Linux Host Security	1.4 Explain penetration testing concepts. Ports 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. Switch o Port security 3.3 Given a scenario, implement secure systems design. Operating systems o Disabling unnecessary ports and services
7.7	Embedded Systems	1.6 Explain the impact associated with types of vulnerabilities. Vulnerabilities due to:

		o Embedded systems 3.5 Explain the security implications of embedded systems SCADA/ICS Smart devices/IoT o Wearable technology o Home automation HVAC SoC RTOS Printers/MFDs Camera systems Special purpose o Medical devices o Vehicles o Aircraft/UAV
7.8	Log Management	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. SIEM o Aggregation o Correlation o Automated alerting and triggers o Time synchronization o Event deduplication o Logs/WORM 2.3 Given a scenario, troubleshoot common security issues. Logs and events anomalies
7.9	Audits	4.4 Given a scenario, differentiate common account management practices. General Concepts o Permission auditing and review o Usage auditing and review

7.10	Email	5.1 Explain the importance of policies, plans and procedures related to organizational security. General security policies o Personal email 6.4 Given a scenario, implement public key infrastructure. Types of certificates o Email
7.11	BYOD Security	2.5 Given a scenario, deploy mobile devices securely. Deployment models o BYOD o COPE o CYOD o Corporate-owned o VDI
7.12	Mobile Device Management	2.5 Given a scenario, deploy mobile devices securely. Connection methods o Cellular o WiFi o SATCOM o Bluetooth o NFC o ANT o Infrared o USB Mobile device management concepts o Application management o Content management o Remote wipe o Geofencing o Geolocation o Screen locks o Push notification services o Passwords and pins o Biometrics

		o Context-aware authentication o Containerization o Storage segmentation o Full device encryption Enforcement and monitoring for: o Third-party app stores o Rooting/jailbreaking o Sideloading o Custom firmware o Carrier unlocking o Firmware OTA updates o Camera use o SMS/MMS o External media o USB OTG o Recording microphone o GPS tagging o WiFi direct/ad hoc o Tethering o Payment methods Deployment models o BYOD 3.3 Given a scenario, implement secure systems design. Operating systems o Types ▪ Mobile OS
7.13	Host Virtualization	3.7 Summarize cloud and virtualization concepts. Hypervisor o Type I o Type II o Application cells/containers VDI/VDE
8.0	**Application**	

8.1	Access Control Models	4.1 Compare and contrast identity and access management concepts. Transitive trust 4.3 Given a scenario, implement identity and access management controls. Access control models o MAC o DAC o ABAC o Role-based access control o Rule-based access control
8.2	Authentication	4.1 Compare and contrast identity and access management concepts. Multifactor authentication o Something you are o Something you have o Something you know o Somewhere you are o Something you do Single sign-on 4.3 Given a scenario, implement identity and access management controls. Biometric factors o Fingerprint scanner o Retinal scanner o Iris scanner o Voice recognition o Facial recognition o False acceptance rate o False rejection rate o Crossover error rate
8.3	Authorization	4.3 Given a scenario, implement identity and access management controls. File system security

		4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control
8.4	Web Application Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o Buffer overflow o Injection o Cross-site scripting o Cross-site request forgery o Zero day o Hijacking and related attacks ▪ Clickjacking ▪ Session hijacking ▪ URL hijacking ▪ Typo squatting o Driver manipulation ▪ Shimming ▪ Refactoring 1.6 Explain the impact associated with types of vulnerabilities. Memory/buffer vulnerability o Integer overflow o Buffer overflow o DLL injection New threats/zero day
8.5	Internet Browsers	
8.6	Application Development	2.4 Given a scenario, analyze and interpret output from security technologies. Application whitelisting Data execution prevention

3.3 Given a scenario, implement secure systems design.

Operating systems
- Disabling unnecessary ports and services
- Least functionality
- Secure configurations
- Application whitelisting/blacklisting

3.4 Explain the importance of secure staging deployment concepts.

Sandboxing
Environment
- Development
- Test
- Staging
- Production

Secure baseline
Integrity measurement

3.6 Summarize secure application development and deployment concepts.

Secure DevOps
- Security automation
- Continuous integration
- Baselining
- Immutable systems
- Infrastructure as code

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

		o Dynamic analysis (e.g., fuzzing) o Stress testing o Sandboxing o Model verification
8.7	Active Directory Overview	
8.8	Windows Domain Users and Groups	4.4 Given a scenario, differentiate common account management practices. Account types o User account o Shared and generic accounts/credentials o Guest accounts o Service accounts o Privileged accounts
8.9	Linux Users	4.4 Given a scenario, differentiate common account management practices. Account types o User account o Shared and generic accounts/credentials o Guest accounts o Service accounts o Privileged accounts
8.10	Linux Groups	
8.11	Linux User Security	4.4 Given a scenario, differentiate common account management practices. Account policy enforcement o Password complexity o Expiration o Password history o Password reuse o Password length

8.12	Group Policy Overview	4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control Account policy enforcement o Group policy
8.13	Hardening Authentication 1	4.4 Given a scenario, differentiate common account management practices. General Concepts o Group-based access control Account policy enforcement o Group policy o Password complexity o Expiration o Recovery o Disablement o Lockout o Password history o Password reuse o Password length
8.14	Hardening Authentication 2	3.9 Explain the importance of physical security controls. Tokens/cards 4.3 Given a scenario, implement identity and access management controls. Physical access control o Smart cards Certificate-based authentication o PIV/CAC/smart card
9.0	**Data**	
9.1	Data Management	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

		Data sanitization tools 5.8 Given a scenario, carry out data security and privacy practices. Data destruction and media sanitization o Burning o Shredding o Pulping o Pulverizing o Degaussing o Purging o Wiping Data sensitivity labeling and handling o Confidential o Private o Public o Proprietary o PII o PHI Data roles o Owner o Steward/custodian o Privacy officer Data retention Legal and compliance
9.2	Advanced 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 o Crypt service provider o Crypt modules Perfect forward secrecy Security through obscurity Common use cases o Low power devices o Low latency o High resiliency o Supporting confidentiality o Supporting integrity o Supporting obfuscation o Supporting authentication o Supporting non-repudiation o Resource vs. security constraints
9.3	Cryptography Implementations	3.3 Given a scenario, implement secure systems design. Hardware/firmware security o TPM o HSM 5.1 Explain the importance of policies, plans and procedures related to organizational security. General security policies o Social media networks/applications o Personal email 6.1 Compare and contrast basic concepts of cryptography.

		Digital signatures 6.2 Explain cryptography algorithms and their basic characteristics. Asymmetric algorithms o PGP/GPG 6.4 Given a scenario, implement public key infrastructure. Types of certificates o Email Certificate formats o PEM
9.4	Cryptographic Attacks	1.2 Compare and contrast types of attacks. Application/service attacks o Man-in-the-middle o Replay Cryptographic attacks o Birthday o Known plain text/cipher text o Dictionary o Brute force ▪ Online vs. offline o Replay o Weak implementations
9.5	Symmetric Encryption	6.1 Compare and contrast basic concepts of cryptography. Symmetric algorithms Modes of operation Hashing Salt, IV, nonce Weak/deprecated algorithms Stream vs. block Key strength Secret algorithm

		Key stretching 6.2 Explain cryptography algorithms and their basic characteristics. Symmetric algorithms o AES o DES o 3DES o RC4 o Blowfish/Twofish Cipher modes o CBC o ECB o Stream vs. block Hashing algorithms o MD5 o SHA o HMAC o RIPEMD Key stretching algorithms o BCRYPT o PBKDF2
9.6	Asymmetric Encryption	6.1 Compare and contrast basic concepts of cryptography. Modes of operation Asymmetric algorithms Elliptic curve Weak/deprecated algorithms Key exchange Digital signatures Key strength Session keys Ephemeral key Secret algorithm Data-in-transit Data-at-rest Data-in-use Perfect forward secrecy Common use cases o Supporting confidentiality o Supporting integrity

		- Supporting authentication
		- Supporting non-repudiation
		- Resource vs. security constraints
		
		6.2 Explain cryptography algorithms and their basic characteristics.
		
		Asymmetric algorithms
		- RSA
		- DSA
		- Diffie-Hellman
		  - Groups
		  - DHE
		  - ECDHE
		- Elliptic curve
		- PGP/GPG

9.7	File Encryption	6.2 Explain cryptography algorithms and their basic characteristics. Symmetric algorithms - AES - DES - 3DES Asymmetric algorithms - RSA - DSA - Elliptic curve - PGP/GPG
9.8	Public Key Infrastructure (PKI)	6.4 Given a scenario, implement public key infrastructure. Components - CA - CRL - OCSP - CSR - Certificate - Public key - Private key Concepts - Online vs. offline CA

		o Key escrow
9.9	Hashing	6.1 Compare and contrast basic concepts of cryptography. Hashing Collision 6.2 Explain cryptography algorithms and their basic characteristics. Hashing algorithms o MD5 o SHA o HMAC o RIPEMD
9.10	Data Transmission Security	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. VPN concentrator o IPSec ▪ Tunnel mode ▪ Transport mode ▪ AH ▪ ESP o TLS 2.6 Given a scenario, implement secure protocols. Protocols o SSH o LDAPS o FTPS o SSL/TLS o HTTPS Use cases o Email and web o File transfer o Directory services

9.11	Data Loss Prevention (DLP)	2.1 Install and configure network components, both hardware- and software-based, to support organizational security. DLP o USB blocking o Cloud-based o Email 2.3 Given a scenario, troubleshoot common security issues. Data exfiltration 2.4 Given a scenario, analyze and interpret output from security technologies. DLP
9.12	Redundancy	3.8 Explain how resiliency and automation strategies reduce risk. Elasticity Scalability Distributive allocation Redundancy Fault tolerance High availability RAID 5.2 Summarize business impact analysis concepts. RTO/RPO MTBF MTTR Mission-essential functions Identification of critical systems Single point of failure 5.6 Explain disaster recovery and continuity of operation concepts. Recovery sites o Hot site o Warm site

		o Cold site Order of restoration Geographic considerations o Off-site backups o Distance o Location selection o Legal implications o Data sovereignty
9.13	Backup and Restore	3.8 Explain how resiliency and automation strategies reduce risk. Templates Master image Non-persistence o Snapshots o Revert to known state o Rollback to known configuration o Live boot media 5.6 Explain disaster recovery and continuity of operation concepts. Backup concepts o Differential o Incremental o Snapshots o Full
9.14	Cloud Storage	3.7 Summarize cloud and virtualization concepts. Cloud access security broker

Objective Mapping: CompTIA SY0-501 Objective to LabSim Section

#	CompTIA Security+ (SY0-501) Objective	TestOut Module.Section
1.0	**Threats, Attacks and Vulnerabilities**	
1.1	Given a scenario, analyze indicators of compromise and determine the type of malware. Viruses Crypto-malware Ransomware Worm Trojan Rootkit Keylogger Adware Spyware Bots RAT Logic bomb Backdoor	6.2 7.1
1.2	Compare and contrast types of attacks. Social engineering: o Phishing o Spear phishing o Whaling o Vishing o Tailgating o Impersonation o Dumpster diving o Shoulder surfing o Hoax o Watering hole attack o Principles (reasons for effectiveness) ▪ Authority ▪ Intimidation	3.5 4.3 5.1, 5.2, 5.11 6.2, 6.4 7.2 8.4 9.4

- Consensus
- Scarcity
- Familiarity
- Trust
- Urgency

Application/service attacks

- 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

	o Disassociation Cryptographic attacks o Birthday o Known plain text/cipher text o Rainbow tables o Dictionary o Brute force ▪ Online vs. offline o Collision o Downgrade o Replay o Weak implementations	
1.3	Explain threat actor types and attributes. Types of actors o Script kiddies o Hacktivist o Organized crime o Nation states/APT o Insiders o Competitors Attributes of actors o Internal/external o Level of sophistication o Resources/funding o Intent/motivation Use of open-source intelligence	2.1
1.4	Explain penetration testing concepts. Active reconnaissance Passive reconnaissance Pivot Initial exploitation Ports Persistence Escalation of privilege Black box	2.1 5.1 6.9, 6.13 7.6

	White box Gray box Pen testing vs. vulnerability scanning	
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	6.9
1.6	Explain the impact associated with types of vulnerabilities. Race conditions Vulnerabilities due to: o End-of-life systems o Embedded systems o 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 o Memory leak o Integer overflow o Buffer overflow o Pointer dereference o DLL injection System sprawl/undocumented assets Architecture/design weaknesses New threats/zero day	5.12 6.1, 6.7 7.7 8.4

	Improper certificate and key management	
2.0	**Technologies and Tools**	
2.1	Install and configure network components, both hardware- and software-based, to support organizational security. Firewall o ACL o Application-based vs. network-based o Stateful vs. stateless o Implicit deny VPN concentrator o Remote access vs. site-to-site o IPSec ▪ Tunnel mode ▪ Transport mode ▪ AH ▪ ESP o Split tunnel vs. full tunnel o TLS o Always-on VPN NIPS/NIDS o Signature-based o Heuristic/behavioral o Anomaly o Inline vs. passive o In-band vs. out-of-band o Rules o Analytics ▪ False positive ▪ False negative Router o ACLs o Antispoofing Switch o Port security o Layer 2 vs. Layer 3 o Loop prevention	5.3, 5.5, 5.7, 5.8, 5.9, 5.10, 5.12 6.5, 6.7, 6.8, 6.9 7.6, 7.8 9.10, 9.11

- Flood guard

Proxy
- Forward and reverse proxy
- Transparent
- Application/multipurpose

Load balancer
- Scheduling
  - Affinity
  - Round-robin
- Active-passive
- Active-active
- Virtual IPs

Access point
- 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	
2.2	Given a scenario, use appropriate software tools to assess the security posture of an organization. Protocol analyzer Network scanners o Rogue system detection o 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 o ping o netstat o tracert o nslookup/dig o arp o ipconfig/ip/ifconfig o tcpdump o nmap o netcat	2.5 6.9, 6.10 7.2
2.3	Given a scenario, troubleshoot common security issues. Unencrypted credentials/cleartext Logs and events anomalies Permission issues Access violations Certificate issues Data exfiltration Misconfigured devices	5.5, 5.8, 5.12 7.8 9.11

	o Firewall o Content filter o Access points Weak security configurations Personnel issues o Policy violation o Insider threat o Social engineering o Social media o Personal email Unauthorized software Baseline deviation License compliance violation (availability/integrity) Asset management Authentication issues	
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	5.5 7.3 8.6 9.11
2.5	Given a scenario, deploy mobile devices securely. Connection methods o Cellular o WiFi o SATCOM o Bluetooth o NFC	3.8 5.10 7.11, 7.12

- 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
- 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

2.6	Given a scenario, implement secure protocols. Protocols o DNSSEC o SSH o S/MIME o SRTP o LDAPS o FTPS o SFTP o SNMPv3 o SSL/TLS o HTTPS o Secure POP/IMAP Use cases o Voice and video o Time synchronization o Email and web o File transfer o Directory services o Remote access o Domain name resolution o Routing and switching o Network address allocation o Subscription services	6.11 9.10
2.7	Compare and contrast physical security and environmental controls. Environmental controls o HVAC o Fire suppression o EMI shielding o Hot and cold aisles o Environmental monitoring o Temperature and humidity controls Physical security o Hardware locks o Mantraps o Vide o Surveillance	4.1, 4.2, 4.4

	o Fencing o Proximity readers o Access list o Proper lighting o Signs o Guards o Barricades o Biometrics o Protected distribution (cabling) o Alarms o Motion detection Control types o Deterrent o Preventive o Detective o Compensating o Technical o Administrative	
3.0	**Architecture and Design**	
3.1	Explain use cases and purpose for frameworks, best practices and secure configuration guides. Industry-standard frameworks and reference architectures o Regulatory o Non-regulatory o National vs. international o Industry-specific frameworks Benchmarks/secure configuration guides o Platform/vendor-specific guides ▪ Web server ▪ Operating system ▪ Application server ▪ Network infrastructure devices o General purpose guides Defense-in-depth/layered security o Vendor diversity o Control diversity ▪ Administrative ▪ Technical	2.2

	o User training	
3.2	Given a scenario, implement secure network architecture concepts. Zones/topologies o DMZ o Extranet o Intranet o Wireless o Guest o Honeynets o NAT o Ad hoc Segregation/segmentation/isolation o Physical o Logical (VLAN) o Virtualization o Air gaps Tunneling/VPN o Site-to-site o Remote access Security device/technology placement o Sensors o Collectors o Correlation engines o Filters o Proxies o Firewalls o VPN concentrators o SSL accelerators o Load balancers o DDoS mitigator o Aggregation switches o Taps and port mirror SDN	4.3 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.10 6.1, 6.5, 6.6, 6.14, 6.15 7.3
3.3	Given a scenario, implement secure systems design. Hardware/firmware security	3.4 6.2, 6.3, 6.9 7.3, 7.4, 7.5, 7.6, 7.12

	o FDE/SED o TPM o HSM o UEFI/BIOS o Secure boot and attestation o Supply chain o Hardware root of trust o EMI/EMP Operating systems o Types ▪ Network ▪ Server ▪ Workstation ▪ Appliance ▪ Kiosk ▪ Mobile OS o Patch management o Disabling unnecessary ports and services o Least functionality o Secure configurations o Trusted operating system o Application whitelisting/blacklisting o Disable default accounts/passwords Peripherals o Wireless keyboards o Wireless mice o Displays o WiFi-enabled MicroSD cards o Printers/MFDs o External storage devices o Digital cameras	8.6 9.3
3.4	Explain the importance of secure staging deployment concepts. Sandboxing Environment o Development o Test o Staging o Production Secure baseline	8.6

	Integrity measurement	
3.5	Explain the security implications of embedded systems. SCADA/ICS Smart devices/IoT o Wearable technology o Home automation HVAC SoC RTOS Printers/MFDs Camera systems Special purpose o Medical devices o Vehicles o Aircraft/UAV	7.7
3.6	Summarize secure application development and deployment concepts. Development life-cycle models o Waterfall vs. Agile Secure DevOps o Security automation o Continuous integration o Baselining o Immutable systems o Infrastructure as code Version control and change management Provisioning and deprovisioning Secure coding techniques o Proper error handling o Proper input validation o Normalization o Stored procedures o Code signing o Encryption o Obfuscation/camouflage o Code reuse/dead code	3.6 8.6

	o Server-side vs. client-side execution and validation o Memory management o Use of third-party libraries and SDKs o Data exposure Code quality and testing o Static code analyzers o Dynamic analysis (e.g., fuzzing) o Stress testing o Sandboxing o Model verification Compiled vs. runtime code	
3.7	Summarize cloud and virtualization concepts. Hypervisor o Type I o Type II o Application cells/containers VM sprawl avoidance VM escape protection Cloud storage Cloud deployment models o SaaS o PaaS o IaaS o Private o Public o Hybrid o Community On-premise vs. hosted vs. cloud VDI/VDE Cloud access security broker Security as a Service	6.14, 6.16 7.13 9.14
3.8	Explain how resiliency and automation strategies reduce risk. Automation/scripting o Automated courses of action o Continuous monitoring	9.12, 9.13

	o Configuration validation Templates Master image Non-persistence o Snapshots o Revert to known state o Rollback to known configuration o Live boot media Elasticity Scalability Distributive allocation Redundancy Fault tolerance High availability RAID	
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 o HVAC o Hot and cold aisles o Fire suppression Cable locks Screen filters Cameras Motion detection	4.1, 4.4 8.14

	Logs Infrared detection Key management	
4.0	**Identity and Access Management**	
4.1	Compare and contrast identity and access management concepts. Identification, authentication, authorization and accounting (AAA) Multifactor authentication o Something you are o Something you have o Something you know o Somewhere you are o Something you do Federation Single sign-on Transitive trust	2.3 8.1, 8.2
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	6.11, 6.12

4.3	Given a scenario, implement identity and access management controls. Access control models o MAC o DAC o ABAC o Role-based access control o Rule-based access control Physical access control o Proximity cards o Smart cards Biometric factors o Fingerprint scanner o Retinal scanner o Iris scanner o Voice recognition o Facial recognition o False acceptance rate o False rejection rate o Crossover error rate Tokens o Hardware o Software o HOTP/TOTP Certificate-based authentication o PIV/CAC/smart card o IEEE 802.1x File system security Database security	8.1, 8.2, 8.3, 8.14
4.4	Given a scenario, differentiate common account management practices. Account types o User account o Shared and generic accounts/credentials o Guest accounts o Service accounts o Privileged accounts General Concepts o Least privilege	3.9 6.2 7.2, 7.4, 7.5, 7.9 8.3, 8.8, 8.9, 8.11, 8.12, 8.13

	o Onboarding/offboarding o Permission auditing and review o Usage auditing and review o Time-of-day restrictions o Recertification o Standard naming convention o Account maintenance o Group-based access control o Location-based policies Account policy enforcement o Credential management o Group policy o Password complexity o Expiration o Recovery o Disablement o Lockout o Password history o Password reuse o Password length	
5.0	**Risk Management**	
5.1	Explain the importance of policies, plans and procedures related to organizational security. Standard operating procedure Agreement types o BPA o SLA o ISA o MOU/MOA Personnel management o Mandatory vacations o Job rotation o Separation of duties o Clean desk o Background checks o Exit interviews o Role-based awareness training ▪ Data owner	2.3 3.1, 3.7, 3.9 7.10 9.3

	▪ System administrator ▪ System owner ▪ User ▪ Privileged user ▪ Executive user o NDA o Onboarding o Continuing education o Acceptable use policy/rules of behavior o Adverse actions General security policies o Social media networks/applications o Personal email	
5.2	Summarize business impact analysis concepts. RTO/RPO MTBF MTTR Mission-essential functions Identification of critical systems Single point of failure Impact o Life o Property o Safety o Finance o Reputation Privacy impact assessment Privacy threshold assessment	3.1 9.12
5.3	Explain risk management processes and concepts. Threat assessment o Environmental o Manmade o Internal vs. external Risk assessment o SLE	3.1, 3.2, 3.3 6.1, 6.13

	o ALE o ARO o Asset value o Risk register o Likelihood of occurrence o Supply chain assessment o Impact o Quantitative o Qualitative o Testing ▪ Penetration testing authorization ▪ Vulnerability testing authorization o Risk response techniques ▪ Accept ▪ Transfer ▪ Avoid ▪ Mitigate Change management	
5.4	Given a scenario, follow incident response procedures. Incident response plan o Documented incident types/category definitions o Roles and responsibilities o Reporting requirements/escalation o Cyber-incident response teams o Exercise Incident response process o Preparation o Identification o Containment o Eradication o Recovery o Lessons learned	2.6
5.5	Summarize basic concepts of forensics. Order of volatility Chain of custody	2.6

	Legal hold Data acquisition o Capture system image o Network traffic and logs o Capture video o Record time offset o Take hashes o Screenshots o Witness interviews Preservation Recovery Strategic intelligence/counterintelligence gathering o Active logging Track man-hours	
5.6	Explain disaster recovery and continuity of operation concepts. Recovery sites o Hot site o Warm site o Cold site Order of restoration Backup concepts o Differential o Incremental o Snapshots o Full Geographic considerations o Off-site backups o Distance o Location selection o Legal implications o Data sovereignty Continuity of operation planning o Exercises/tabletop o After-action reports o Failover o Alternate processing sites o Alternate business practices	3.3 9.12, 9.13

5.7	Compare and contrast various types of controls. Deterrent Preventive Detective Corrective Compensating Technical Administrative Physical	4.1
5.8	Given a scenario, carry out data security and privacy practices. Data destruction and media sanitization o Burning o Shredding o Pulping o Pulverizing o Degaussing o Purging o Wiping Data sensitivity labeling and handling o Confidential o Private o Public o Proprietary o PII o PHI Data roles o Owner o Steward/custodian o Privacy officer Data retention Legal and compliance	3.1 9.1
6.0	**Cryptography and PKI**	

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 o Crypt service provider o Crypt modules Perfect forward secrecy Security through obscurity Common use cases o Low power devices o Low latency o High resiliency o Supporting confidentiality o Supporting integrity o Supporting obfuscation o Supporting authentication o Supporting non-repudiation o Resource vs. security constraints	2.4 9.2, 9.3, 9.5, 9.6, 9.9

6.2	Explain cryptography algorithms and their basic characteristics. Symmetric algorithms o AES o DES o 3DES o RC4 o Blowfish/Twofish Cipher modes o CBC o GCM o ECB o CTM o Stream vs. block Asymmetric algorithms o RSA o DSA o Diffie-Hellman ▪ Groups ▪ DHE ▪ ECDHE o Elliptic curve o PGP/GPG Hashing algorithms o MD5 o SHA o HMAC o RIPEMD Key stretching algorithms o BCRYPT o PBKDF2 Obfuscation o XOR o ROT13 o Substitution ciphers	9.3, 9.5, 9.6, 9.7. 9.9
6.3	Given a scenario, install and configure wireless security settings. Cryptographic protocols o WPA	5.10, 5.12

	o WPA2 o CCMP o TKIP Authentication protocols o EAP o PEAP o EAP-FAST o EAP-TLS o EAP-TTLS o IEEE 802.1x o RADIUS Federation Methods o PSK vs. Enterprise vs. Open o WPS o Captive portals	
6.4	Given a scenario, implement public key infrastructure. Components o CA o Intermediate CA o CRL o OCSP o CSR o Certificate o Public key o Private key o Object identifiers (OID) Concepts o Online vs. offline CA o Stapling o Pinning o Trust model o Key escrow o Certificate chaining Types of certificates o Wildcard o SAN o Code signing o Self-signed o Machine/computer	7.10 9.8

	o Email o User o Root o Domain validation o Extended validation Certificate formats o DER o PEM o PFX o CER o P12 o P7B	