CompTIA Security+ Detailed Mapping

SY0-401 vs SY0-501

Executive Summary

- An estimated 25% change exists between SY0-401 and SY0-501.
- The range of topics is similar but several topics are explored in more detail; there is more content to cover. For example, some SY0-401 objectives are broken down into multiple SY0-501 objectives to expand coverage of the same topic.
- Interestingly, SY0-501 objectives cover *lower* Bloom's taxonomy layers than SY0-401.
    - SY0-401 objectives focused on *analyzing* (Layer 4) – intermediate skills and entry-level
    - SY0-501 focuses on *applying* (Layer 3) – entry-level skills
- SY0-501 objectives cover mostly lower-level learning objectives through *knowledge, comprehension*, and *application*. The SY0-401 exam covered the more intermediate *analysis* level. Analysis is now found in intermediate-level certifications, such as CompTIA Cybersecurity Analyst (CSA+).
- The updated exam focuses more on attacks, risk management and hands-on skills using technologies and tools. The domains were re-ordered and re-named to reflect better ID organization and emphasis of industry cybersecurity trends, as determined in the Security+ SY0-501 Job Task Analysis (JTA).
- In general, there is more content to cover, but the exam questions focus on applying technology (Layer 3) instead of previously more-difficult analysis (Layer 4) skills.

Exam Information

	SY0-401	SY0-501
Number of questions	Max of 110	TBD
Duration	90 minutes	TBD
Format	Multiple choice and performance-based questions	Multiple choice with performance-based questions
Delivery	Pearson VUE	Pearson VUE
Exam Fee	$320	$320
Number of exam objectives	33	37

Exam Overview Comparison

SY0-401	SY0-501
The CompTIA Security+ certification is a vendor-neutral, internationally recognized credential used by organizations and security professionals around the globe to validate foundation level security skills and knowledge. Candidates are encouraged to use this document to help prepare for CompTIA Security+ SY0-401, which measures necessary skills for IT security professionals. Successful candidates will have the knowledge required to: • Identify risk • Participate in risk mitigation activities • Provide infrastructure, application, information and operational security • Apply security controls to maintain confidentiality, integrity and availability • Identify appropriate technologies and products • Troubleshoot security events and incidents • Operate with an awareness of applicable policies, laws and regulations	The CompTIA Security+ certification is a vendor-neutral credential. The CompTIA Security+ exam is an internationally recognized validation of foundation-level security skills and knowledge, and is used by organizations and security professionals around the globe. The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.

Sample Job Roles

SY0-401	SY0-501
Security or Systems Administrator	Systems Administrator
Network Administrator	Network Administrator
Security Specialist/Administrator	Security Administrator
Security Consultant	Junior IT Auditor/Penetration Tester

Domain Comparison

SY0-401 Domains		SY0-501 Domain Equivalent	
1.0 Network Security	20%	2.0 Technologies and Tools	22%
2.0 Compliance and Operational Security	18%	5.0 Risk Management	14%
3.0 Threats and Vulnerabilities	20%	1.0 Threats, Attacks and Vulnerabilities	21%
4.0 Application, Data and Host Security	15%	3.0 Architecture and Design	15%
5.0 Access Control and Management	15%	4.0 Identity and Access Management	16%
6.0 Cryptography	12%	6.0 Cryptography and PKI	12%

Summary

CompTIA expects a smooth transition from SY0-401 to SY0-501. The purpose of the exam has not changed. Security+ continues to provide the universal baseline for entry-level cybersecurity skills needed throughout the globe. SY0-501 provides the latest technology and industry job skills to mirror the changing world of cybersecurity skills. It is anticipated that Security+ will continue to raise the standard for cybersecurity professionals worldwide.

Objective by Objective Mapping (starts on next page)

Objective Comparison

SY0-401	SY0-501
1.1 Implement security configuration parameters on network devices and other technologies. • Firewalls • Routers • Switches • Load balancers • Proxies • Web security gateways • VPN concentrators • NIDS and NIPS - Behavior-based - Signature-based - Anomaly-based - Heuristic • Protocol analyzers • Spam filter • UTM security appliances - URL filter - Content inspection - Malware inspection • Web application firewall vs. network firewall • Application aware devices - Firewalls - IPS - IDS - Proxies	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 o Dissolvable vs. permanent o Host health checks o Agent vs. agentless • Mail gateway o Spam filter o DLP o Encryption • Bridge • SSL/TLS accelerators • SSL decryptors • Media gateway • Hardware security module
1.2 Given a scenario, use secure network administration principles.	

• Rule-based management • Firewall rules • VLAN management • Secure router configuration • Access control lists • Port security • 802.1x • Flood guards • Loop protection • Implicit deny • Network separation • Log analysis • Unified threat management	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 o Dissolvable vs. permanent o Host health checks o Agent vs. agentless • Mail gateway o Spam filter o DLP o Encryption • Bridge • SSL/TLS accelerators • SSL decryptors • Media gateway • Hardware security module
1.3 Explain network design elements and components. • DMZ • Subnetting • VLAN • NAT • Remote access • Telephony • NAC • Virtualization • Cloud computing - PaaS - SaaS	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

- IaaS - Private - Public - Hybrid - Community • Layered security/defense in depth	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
1.4 Given a scenario, implement common protocols and services. • Protocols - IPSec - SNMP - SSH - DNS - TLS - SSL - TCP/IP - FTPS - HTTPS - SCP - ICMP - IPv4	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

- IPv6 - iSCSI - Fibre Channel - FCoE - FTP - SFTP - TFTP - TELNET - HTTP - NetBIOS • Ports - 21 - 22 - 25 - 53 - 80 - 110 - 139 - 143 - 443 - 3389 • OSI relevance	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
1.5 Given a scenario, troubleshoot security issues related to wireless networking. • WPA • WPA2 • WEP • EAP • PEAP • LEAP • MAC filter • Disable SSID broadcast • TKIP • CCMP	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

• Antenna placement • Power level controls • Captive portals • Antenna types • Site surveys • VPN (over open wireless)	o IEEE 802.1x o RADIUS Federation • Methods o PSK vs. Enterprise vs. Open o WPS o Captive portals
2.1 Explain the importance of risk related concepts. • Control types - Technical - Management - Operational • False positives • False negatives • Importance of policies in reducing risk - Privacy policy - Acceptable use - Security policy - Mandatory vacations - Job rotation - Separation of duties - Least privilege • Risk calculation - Likelihood - ALE - Impact - SLE - ARO - MTTR - MTTF - MTBF • Quantitative vs. qualitative • Vulnerabilities • Threat vectors • Probability/threat likelihood	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 ▪ 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

• Risk avoidance, transference, acceptance, mitigation, deterrence • Risks associated with cloud computing and virtualization • Recovery time objective and recovery point objective	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
2.2 Summarize the security implications of integrating systems and data with third parties. • On-boarding/off-boarding business partners • Social media networks and/or applications • Interoperability agreements - SLA - BPA - MOU - ISA • Privacy considerations • Risk awareness • Unauthorized data sharing • Data ownership • Data backups • Follow security policy and procedures	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

• Review agreement requirements to verify compliance and performance standards	o Control diversity ▪ Administrative ▪ Technical o User training 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 ▪ 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

2.3 Given a scenario, implement appropriate risk mitigation strategies. • Change management • Incident management • User rights and permissions reviews • Perform routine audits • Enforce policies and procedures to prevent data loss or theft • Enforce technology controls - Data Loss Prevention (DLP)	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 • Change management
2.4 Given a scenario, implement basic forensic procedures. • Order of volatility • Capture system image • Network traffic and logs • Capture video • Record time offset • Take hashes • Screenshots	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

• Witnesses • Track man hours and expense • Chain of custody • Big Data analysis	o Record time offset o Take hashes o Screenshots o Witness interviews • Preservation • Recovery • Strategic intelligence/counterintelligence gathering o Active logging • Track man-hours
2.5 Summarize common incident response procedures. • Preparation • Incident identification • Escalation and notification • Mitigation steps • Lessons learned • Reporting • Recovery/reconstitution procedures • First responder • Incident isolation - Quarantine - Device removal • Data breach • Damage and loss control	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 Explain the importance of security related awareness and training. • Security policy training and procedures • Role-based training • Personally identifiable information • Information classification - High - Medium - Low - Confidential - Private	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

- Public • Data labeling, handling and disposal • Compliance with laws, best practices and standards • User habits - Password behaviors - Data handling - Clean desk policies - Prevent tailgating - Personally owned devices • New threats and new security trends/alerts - New viruses - Phishing attacks - Zero-day exploits • Use of social networking and P2P • Follow up and gather training metrics to validate compliance and security posture	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 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
2.7 Compare and contrast physical security and environmental controls. • Environmental controls - HVAC - Fire suppression - EMI shielding - Hot and cold aisles - Environmental monitoring - Temperature and humidity 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	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 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

- Compensating - Technical - Administrative	• 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 • Logs • Infrared detection • Key management 5.7 Compare and contrast various types of controls. • Deterrent • Preventive • Detective • Corrective • Compensating • Technical • Administrative • Physical
2.8 Summarize risk management best practices. • Business continuity concepts - Business impact analysis - Identification of critical systems and components - Removing single points of failure - Business continuity planning and testing - Risk assessment	3.8 Explain how resiliency and automation strategies reduce risk. • Automation/scripting o Automated courses of action o Continuous monitoring o Configuration validation • Templates • Master image • Non-persistence o Snapshots

- Continuity of operations - Disaster recovery - IT contingency planning - Succession planning - High availability - Redundancy - Tabletop exercises • Fault tolerance - Hardware - RAID - Clustering - Load balancing - Servers • Disaster recovery concepts - Backup plans/policies - Backup execution/frequency - Cold site - Hot site - Warm site	o Revert to known state o Rollback to known configuration o Live boot media • Elasticity • Scalability • Distributive allocation • Redundancy • Fault tolerance • High availability • RAID 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

2.9 Given a scenario, select the appropriate control to meet the goals of security. • Confidentiality - Encryption - Access controls - Steganography • Integrity - Hashing - Digital signatures - Certificates - Non-repudiation • Availability - Redundancy - Fault tolerance - Patching • Safety - Fencing - Lighting - Locks - CCTV - Escape plans - Drills - Escape routes - Testing controls	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 • Logs • Infrared detection • Key management
3.1 Explain types of malware. • Adware • Virus • Spyware • Trojan • Rootkits • Backdoors	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware. • Viruses • Crypto-malware • Ransomware • Worm • Trojan

• Logic bomb • Botnets • Ransomware • Polymorphic malware • Armored virus	• Rootkit • Keylogger • Adware • Spyware • Bots • RAT • Logic bomb • Backdoor
3.2 Summarize various types of attacks. • Man-in-the-middle • DDoS • DoS • Replay • Smurf attack • Spoofing • Spam • Phishing • Spim • Vishing • Spear phishing • Xmas attack • Pharming • Privilege escalation • Malicious insider threat • DNS poisoning and ARP poisoning • Transitive access • Client-side attacks • Password attacks - Brute force - Dictionary attacks - Hybrid - Birthday attacks - Rainbow tables • Typo squatting/URL hijacking	1.2 Compare and contrast types of attacks. • Application/service attacks o DoS o DDoS o Man-in-the-middle o Buffer overflow o Injection o Cross-site scripting o Cross-site request forgery o Privilege escalation o ARP poisoning o Amplification o DNS poisoning o Domain hijacking o Man-in-the-browser o Zero day o Replay o Pass the hash o Hijacking and related attacks ▪ Clickjacking ▪ Session hijacking ▪ URL hijacking ▪ Typo squatting o Driver manipulation ▪ Shimming ▪ Refactoring

• Watering hole attack	o MAC spoofing o IP spoofing • 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
3.3 Summarize social engineering attacks and the associated effectiveness with each attack. • Shoulder surfing • Dumpster diving • Tailgating • Impersonation • Hoaxes • Whaling • Vishing • Principles (reasons for effectiveness) - Authority - Intimidation - Consensus/social proof - Scarcity - Urgency - Familiarity/liking - Trust	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

3.4 Explain types of wireless attacks. • Rogue access points • Jamming/interference • Evil twin • War driving • Bluejacking • Bluesnarfing • War chalking • IV attack • Packet sniffing • Near field communication • Replay attacks • WEP/WPA attacks • WPS 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
3.5 Explain types of application attacks. • Cross-site scripting • SQL injection • LDAP injection • XML injection • Directory traversal/command injection • Buffer overflow • Integer overflow • Zero-day • Cookies and attachments • Locally Shared Objects (LSOs) • Flash cookies • Malicious add-ons • Session hijacking • Header manipulation • Arbitrary code execution/	1.2 Compare and contrast types of attacks. • Application/service attacks o DoS o DDoS o Man-in-the-middle o Buffer overflow o Injection o Cross-site scripting o Cross-site request forgery o Privilege escalation o ARP poisoning o Amplification o DNS poisoning o Domain hijacking o Man-in-the-browser o Zero day o Replay o Pass the hash o Hijacking and related attacks

3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques. • Monitoring system logs - Event logs - Audit logs - Security logs - Access logs • Hardening - Disabling unnecessary services - Protecting management interfaces and applications - Password protection - Disabling unnecessary accounts • Network security - MAC limiting and filtering - 802.1x - Disabling unused interfaces and unused application service ports - Rogue machine detection • Security posture - Initial baseline configuration - Continuous security monitoring - Remediation • Reporting - Alarms - Alerts - Trends • Detection controls vs. prevention controls - IDS vs. IPS - Camera vs. guard	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 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

3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities. • Interpret results of security assessment tools • Tools - Protocol analyzer - Vulnerability scanner - Honeypots - Honeynets - Port scanner - Passive vs. active tools - Banner grabbing • Risk calculations - Threat vs. likelihood • Assessment types - Risk - Threat - Vulnerability • Assessment technique - Baseline reporting - Code review - Determine attack surface - Review architecture - Review designs	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
3.8 Explain the proper use of penetration testing versus vulnerability scanning. • Penetration testing - Verify a threat exists - Bypass security controls - Actively test security controls - Exploiting vulnerabilities	1.4 Explain penetration testing concepts. • Active reconnaissance • Passive reconnaissance • Pivot • Initial exploitation • Persistence • Escalation of privilege

• Vulnerability scanning - Passively testing security controls - Identify vulnerability - Identify lack of security controls - Identify common misconfigurations - Intrusive vs. non-intrusive - Credentialed vs. non-credentialed - False positive • Black box • White box • Gray box	• Black box • 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 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 • Change management
4.1 Explain the importance of application security controls and techniques. Fuzzing • Secure coding concepts - Error and exception handling - Input validation • Cross-site scripting prevention • Cross-site Request Forgery (XSRF) prevention • Application configuration baseline (proper settings) • Application hardening • Application patch management • NoSQL databases vs. SQL databases • Server-side vs. client-side validation	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 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
4.2 Summarize mobile security concepts and technologies. • Device security - Full device encryption - Remote wiping - Lockout - Screen locks - GPS - Application control - Storage segmentation - Asset tracking - Inventory control - Mobile device management - Device access control - Removable storage - Disabling unused features • Application security - Key management - Credential management - Authentication - Geo-tagging - Encryption - Application whitelisting - Transitive trust/authentication • BYOD concerns - Data ownership - Support ownership - Patch management - Antivirus management - Forensics - Privacy - On-boarding/off-boarding - Adherence to corporate policies - User acceptance	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

- Architecture/infrastructure considerations - Legal concerns - Acceptable use policy - On-board camera/video	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 o COPE o CYOD o Corporate-owned o VDI
4.3 Given a scenario, select the appropriate solution to establish host security. • Operating system security and settings • OS hardening • Anti-malware - Antivirus - Anti-spam - Anti-spyware - Pop-up blockers • Patch management • Whitelisting vs. blacklisting applications • Trusted OS • Host-based firewalls • Host-based intrusion detection • Hardware security - Cable locks - Safe - Locking cabinets • Host software baselining • Virtualization - Snapshots	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 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)

- Patch compatibility - Host availability/elasticity - Security control testing - Sandboxing	• Asset management • Authentication issue 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 3.3 Given a scenario, implement secure systems design. • Hardware/firmware security 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
4.4 Implement the appropriate controls to ensure data security. • Cloud storage • SAN • Handling Big Data • Data encryption - Full disk - Database - Individual files - Removable media - Mobile devices • Hardware-based encryption devices - TPM - HSM - USB encryption - Hard drive • Data in transit, data at rest, data in use • Permissions/ACL • Data policies	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

- Wiping - Disposing - Retention - Storage	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 o COPE o CYOD o Corporate-owned o VDI 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 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

4.5 Compare and contrast alternative methods to mitigate security risks in static environments. • Environments - SCADA - Embedded (printer, smart TV, HVAC control) - Android - iOS - Mainframe - Game consoles - In-vehicle computing systems • Methods - Network segmentation - Security layers - Application firewalls - Manual updates - Firmware version control - Wrappers - Control redundancy and diversity	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 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
5.1 Compare and contrast the function and purpose of authentication services. • RADIUS • TACACS+ • Kerberos • LDAP • XTACACS • SAML • Secure LDAP	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
5.2 Given a scenario, select the appropriate authentication, authorization or access control. • Identification vs. authentication vs. authorization • Authorization	4.4 4.1 Compare and contrast identity and access management concepts. • Identification, authentication, authorization and accounting (AAA)

- Least privilege - Separation of duties - ACLs - Mandatory access - Discretionary access - Rule-based access control - Role-based access control - Time of day restrictions • Authentication - Tokens - Common access card - Smart card - Multifactor authentication - TOTP - HOTP - CHAP - PAP - Single sign-on - Access control - Implicit deny - Trusted OS • Authentication factors - Something you are - Something you have - Something you know - Somewhere you are - Something you do • Identification - Biometrics - Personal identification verification card - Username • Federation • Transitive trust/authentication	• 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 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
5.3 Install and configure security controls when performing account management, based on best practices. • Mitigate issues associated with users with multiple account/ roles and/or shared accounts • Account policy enforcement - Credential management - Group policy - Password complexity - Expiration - Recovery - Disablement - Lockout - Password history - Password reuse - Password length - Generic account prohibition • Group-based privileges • User-assigned privileges • User access reviews • Continuous monitoring	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

	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 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
6.1 Given a scenario, utilize general cryptography concepts. • Symmetric vs. asymmetric • Session keys • In-band vs. out-of-band key exchange	6.1 Compare and contrast basic concepts of cryptography. • Symmetric algorithms • Modes of operation • Asymmetric algorithms

• Fundamental differences and encryption methods - Block vs. stream • Transport encryption • Non-repudiation • Hashing • Key escrow • Steganography • Digital signatures • Use of proven technologies • Elliptic curve and quantum cryptography • Ephemeral key • Perfect forward secrecy	• 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 Crypto service provider o Crypto 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

6.2 Given a scenario, use appropriate cryptographic methods. • WEP vs. WPA/WPA2 and pre-shared key • MD5 • SHA • RIPEMD • AES • DES • 3DES • HMAC • RSA • Diffie-Hellman • RC4 • One-time pads • NTLM • NTLMv2 • Blowfish • PGP/GPG • Twofish • DHE • ECDHE • CHAP • PAP • Comparative strengths and performance of algorithms • Use of algorithms/protocols with transport encryption - SSL - TLS - IPSec - SSH - HTTPS • Cipher suites - Strong vs. weak ciphers • 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 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

- PBKDF2 - Bcrypt	
6.3 Given a scenario, use appropriate PKI, certificate management and associated components. • Certificate authorities and digital certificates - CA - CRLs - OCSP - CSR • PKI • Recovery agent • Public key • Private key • Registration • Key escrow • Trust models	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 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
	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
	1.6 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 • Improper certificate and key management
	3.4 Explain the importance of secure staging deployment concepts. • Sandboxing • Environment o Development o Test o Staging o Production • Secure baseline • Integrity measurement