نام دوره : متخصص امنیت اطلاعات در شبکه های کامپیوتری ***CompTIA- Security+***			
مشخصات دوره	**تعداد ساعت :** ۴۰	**پیش نیاز :** آشنایی کامل با مفاهیم شبکه + Network	**تعداد ترم :** ۱
مخاطبین دوره	علاقه مندان ورود به دنیای امنیت اطلاعات ، شبکه و مسئول امنیت اطلاعات سازمان ها		
شرح دوره	دوره Security+ تعاریف و متدهای فنی و مدیریتی در حوزه امنیت فن آوری ارتباطات و اطلاعات را پوشش می دهد.به عبارت دیگر با توجه به دید جامع و کلی این دوره می توان آن را به مدیران حوزهICT بعنوان یک دوره آموزش تکمیلی و به علاقه مندان و متخصصین بعنوان مرحله اول ورود به مباحث تخصصی امنیت ICT توصیه نمود.		
آنچه در این دوره می آموزیم:	مفاهیم اساسی امنیت اطلاعات شناسایی خطرات و حملات بر علیه شبکه آشنایی با زیرساخت های امنیتی و ارتباطات شبکه (استراتژی انواع حملات) سیستم های تشخیص , پیشگیری و جلوگیری از نفوذ پیاده سازی و نگهداری شبکه های امن (پروتکل LDAP) امن سازی شبکه و محیط های پیرامون استاندارد ها ؛ روش ها و اصول اولیه رمز نگاری مدیریت آسیب پذیری شبکه پیاده سازی طرح امنیت شبکه با استفاده از پروتکل های امن (... , SSL , IPSec , VPN)		
ترم های دوره	***SY0-301 : CompTIA Security+***		

1.0 Network Security

1.1 Explain the security function and purpose of network devices and technologies

- Firewalls
- Routers
- Switches
- Load Balancers
- Proxies
- Web security gateways
- VPN concentrators
- NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic)
- Protocol analyzers
- Sniffers
- Spam filter, all-in-one security appliances
- Web application firewall vs. network firewall
- URL filtering, content inspection, malware inspection

1.2 Apply and implement 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
- Prevent network bridging by network separation
- Log analysis

1.3 Distinguish and differentiate network design elements and compounds

- DMZ
- Subnetting
- VLAN
- NAT
- Remote Access
- Telephony
- NAC
- Virtualization
- Cloud Computing ○ Platform as a Service ○ Software as a Service
- Infrastructure as a Service

1.4 Implement and use common protocols

- IPSec
- SNMP
- SSH DNS
- TLS SSL
- TCP/IP FTPS
- HTTPS
- SFTP
- SCP
- ICMP
- IPv4 vs. IPv6

1.5 Identify commonly used default network ports

- FTP
- SFTP
- FTPS TFTP
- TELNET
- HTTP
- HTTPS
- SCP
- SSH
- NetBIOS

1.6 Implement wireless network in a secure manner

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
- SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls

2.0 Compliance and Operational Security

2.1 Explain risk related concepts

- Control types Technical Management Operational
- False positives
- 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
- Quantitative vs. qualitative
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated to Cloud Computing and Virtualization

2.2 Carry out appropriate risk mitigation strategies

- Implement security controls based on risk
- Change management Incident management
- User rights and permissions reviews
- Perform routine audits
- Implement policies and procedures to prevent data loss or theft

2.3 Execute appropriate incident response procedures

- Basic forensic procedures ○ Order of volatility Capture system image Network traffic and logs Capture video Record time offset Take hashes Screenshots Witnesses Track man hours and expense
- Damage and loss control
- Chain of custody
- Incident response: first responder

2.4 Explain the importance of security related awareness and training

- Security policy training and procedures
- Personally identifiable information
- Information classification: Sensitivity of data (hard or soft)
- 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
- Threat awareness New viruses Phishing attacks Zero days exploits
- Use of social networking and P2P

2.5 Compare and contrast aspects of business continuity

- Business impact analysis
- Removing single points of failure
- Business continuity planning and testing
- Continuity of operations
- Disaster recovery
- IT contingency planning
- Succession planning

2.6 Explain the impact and proper use of environmental controls

- HVAC
- Fire suppression
- EMI shielding
- Hot and cold aisles
- Environmental monitoring
- Temperature and humidity controls
- Video monitoring

2.7 Execute disaster recovery plans and procedures

- Backup / backout contingency plans or policies
- Backups, execution and frequency
- Redundancy and fault tolerance Hardware
  RAID
  Clustering Load balancing Servers
- High availability
- Cold site, hot site, warm site
- Mean time to restore, mean time between failures, recovery time objectives and recovery point objectives

2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)

3.0 Threats and Vulnerabilities

3.1 Analyze and differentiate among types of malware

- Adware
- Virus
- Worms
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets

3.2 Analyze and differentiate among 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

3.3 Analyze and differentiate among types of social engineering attacks

- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing

3.4 Analyze and differentiate among types of wireless attacks

- Rogue access points
- Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- IV attack
- Packet sniffing

3.5 Analyze and differentiate among types of application attacks

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- Directory traversal/command injection
- Buffer overflow
- Zero day
- Cookies and attachments
- Malicious add-ons
- Session hijacking
- Header manipulation

3.6 Analyze and differentiate among types of mitigation and deterrent techniques

Manual bypassing of electronic controls Failsafe/secure vsfailopen
Monitoring system logs Event logs Audit logs

- Security logs Access logs

Physical security Hardware locks Mantraps Video surveillance
Fencing Proximity readers Access list
Hardening Disabling unnecessary services

- Protecting management interfaces and applications Password protection Disabling unnecessary accounts Port security MAC limiting and filtering
- 802.1x Disabling unused ports

Security posture Initial baseline configuration Continuous security monitoring

- remediation

Reporting ○ Alarms Alerts Trends
Detection controls vs. prevention controls IDS vs. IPS

- Camera vs. guard

3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities

- Vulnerability scanning and interpret results
- Tools ○ Protocol analyzer Sniffer Vulnerability scanner Honeypots Honeynets Port scanner
- Risk calculations Threat vs. likelihood
- Assessment types Risk Threat Vulnerability
- Assessment technique Baseline reporting Code review Determine attack surface Architecture
- Design reviews

3.8 Within the realm of vulnerability assessments, 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
- Vulnerability scanning Passively testing security controls Indentify vulnerability Indentify lack of security controls Indentify common misconfiguration
- Black box
- White box
- Gray box

4.0 Application, Data and Host Security

4.1 Explain the importance of application security

- 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

4.2 Carry out appropriate procedures to establish host security

- Operating system security and settings
- Anti-malware Anti-virus Anti-spam Anti-spyware Pop-up blockers Host-based firewalls
- Patch management
- Hardware security Cable locks Safe Locking cabinets
- Host software baselining
- Mobile devices Screen lock Strong password Device encryption Remote wipe/sanitation Voice encryption ○ GPS tracking
- Virtualization

4.3 Explain the importance of data security

- Data Loss Prevention (DLP)
- Data encryption Full disk
  - Database
  - Individual files
  - Removable media Mobile devices
- Hardware based encryption devices TPM HSM
  - USB encryption Hard drive
- Cloud computing

5.0 Access Control and Identity Management

5.1 Explain the function and purpose of authentication services

- RADIUS
- TACACS
- TACACS+
- Kerberos
- LDAP
- XTACACS

5.2 Explain the fundamental concepts and best practices related to authentication, authorization and access control

- Identification vs. authentication
- Authentication (single factor) and authorization
- Multifactor authentication
- Biometrics
- Tokens
- Common access card
- Personal identification verification card
- Smart card
- Least privilege
- Separation of duties
- Single sign on
- ACLs
- Access control
- Mandatory access control
- Discretionary access control
- Role/rule-based access control
- Implicit deny
- Time of day restrictions
- Trusted OS
- Mandatory vacations
- Job rotation

5.3 Implement appropriate security controls when performing account management

- Mitigates issues associated with users with multiple account/roles
- Account policy enforcement

  Password complexity Expiration Recovery

  Length Disablement Lockout Group based

  privileges User assigned privileges

6.0 Cryptography

6.1 Summarize general cryptography concepts

- Symmetric vs. asymmetric
- 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

6.2 Use and apply appropriate cryptographic tools and products

- WEP vs. WPA/WPA2 and preshared key
- MD5 SHA
- RIPEMD
- AES DES
- 3DES
- HMAC
- RSA
- RC4
- One-time-pads
- CHAP PAP
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- Whole disk encryption
- Two Fish
- Comparative strengths of algorithms
- Use of algorithms with transport encryption SSL TLS IPsec SSH
- HTTPS

6.3 Explain the core concepts of public key infrastructure

- Certificate authorities and digital certificates CA CRLs
- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models

6.4 Implement PKI, certificate management and associated components

- Certificate authorities and digital certificates ○ CA ○ CRLs
- PKI
- Recovery agent
- Public key
- Private keys
- Registration
- Key escrow
- Trust models