Course Content Summary
ITN 260 – Network Security Basics (3 Credits)

The TNCC Cybersecurity Program Web page is located at: http://tncc.edu/programs/cyber-security

Course Description:
Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers; risk management, network security policy, and security training. Includes the give security keys, confidentiality integrity, availability, accountability and auditability. Lecture 3 hours per week.

Statement of Purpose:
The purpose of this course is to instill the basics of network security (aka “information assurance”) as well as provide a resource to assist students who are pursuing CompTIA’s Security+ certification. The textbook for this course maps directly to the CompTIA Security+ certification exam objectives and outcomes. This course also includes content, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA’s Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites / Corequisites:
ITN 109, ITN 154 and ITN 155, or a verified current CompTIA Network+ or Cisco CCENT certification.

Required Text:

Course Objectives:
Upon successful completion of this course, the student will have a working knowledge of:

A. Network security basics, security architecture, and security models.
B. Network security planning, risk management and policy
C. Network security vulnerabilities, attacks and attack characteristics
D. Network security defensive technologies
E. Network security administration and organization
F. Legal, privacy and ethical issues
Course Content:

1.0 Network security basics
2.0 Compliance and Operational Security
3.0 Threats and Vulnerabilities
4.0 Application, Data, and Host Security
5.0 Access Control and Identity Management
6.0 Cryptography

Student Learning Outcomes:

1.0 Network Security

1.1 Implement security configuration parameters on network devices and other technologies. [IA5]

- 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

1.2 Given a scenario, use secure network administration principles. [SA14]

- 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

1.3 Explain network design elements and components. (CD7a)

- DMZ
- Subnetting
- VLAN
- NAT
- Remote Access
- Telephony
- NAC
- Virtualization
- Cloud Computing
  - Platform as a Service
  - Software as a Service
  - Infrastructure as a Service
  - Private
  - Public
  - Hybrid
  - Community
- Layered security / Defense in depth

1.4 Given a scenario, implement common protocols and services. (SA14)

- Protocols
  - IPSec
  - SNMP
  - SSH
  - DNS
  - TLS
  - SSL
  - TCP/IP
  - FTPS
  - HTTPS
- SCP
- ICMP
- IPv4
- IPv6
- iSCSI
- Fibre Channel
- FCoE
- FTP
- SFTP
- TFTP
- TELNET
- HTTP
- NetBIOS

- Ports
  - 21, 22, 25, 53, 80, 110, 139, 143, 443, 3389

- OSI relevance

1.5 Given a scenario, troubleshoot security issues related to wireless networking. (IT7)

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
- Disable SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls
- Captive portals
- Antenna types
- Site surveys
- VPN (over open wireless)
2.0 Compliance and Operational Security

2.1 Explain the importance of risk related concepts. (FS4) (SA16)

- 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
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated with Cloud Computing and Virtualization
- Recovery time objective and recovery point objective
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
- Review agreement requirements to verify compliance and performance standards

2.3 Given a scenario, implement appropriate risk mitigation.

- Change management
- Incident management
- User rights and permissions reviews
- Perform routine audits
- Enforce policies and procedures to prevent data loss
- Enforce technology controls
  - Data Loss Prevention (DLP)

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
- Witnesses
- Track man hours and expense
- Chain of custody
- Big Data analysis

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
  o Quarantine
  o Device removal
• Data breach
• Damage and loss control

2.6 Explain the importance of security related awareness and training.

• Security policy training and procedures
• Role-based training
• Personally identifiable information
• Information classification
  o High, Medium, Low
  o Confidential, Private, Public
• Data labeling, handling and disposal
• Compliance with laws, best practices and standards
• User habits
  o Password behaviors
  o Data handling
  o Clean desk policies
  o Prevent tailgating
  o Personally owned devices
• New threats and new security trends/alerts
  o New viruses
  o Phishing attacks
  o Zero-day exploits
• Use of social networking and P2P
• Follow up and gather training metrics to validate compliance and security posture

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 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

2.8 Summarize risk management best practices. (SA12)

• Business continuity concepts
  o Business impact analysis
  o Identification of critical systems and components
  o Removing single points of failure
  o Business continuity planning and testing
  o Risk assessment
  o Continuity of operations
  o Disaster recovery
  o IT contingency planning
  o Succession planning
  o High availability
  o Redundancy
  o Tabletop exercises

• Fault tolerance
  o Hardware
  o RAID
  o Clustering
  o Load balancing
  o Servers
• Disaster recovery concepts
  o Backup plans/policies
  o Backup execution/frequency
  o Cold site
  o Hot site
  o Warm site

2.9 Given a scenario, select the appropriate control to meet the goals of security. *(IA10)*

• Confidentiality
  o Encryption
  o Access controls
  o Steganography

• Integrity
  o Hashing
  o Digital signatures
  o Certificates
  o Non-repudiation

• Availability
  o Redundancy
  o Fault tolerance
  o Patching

• Safety
  o Fencing
  o Lighting
  o Locks
  o CCTV
  o Escape plans
  o Drills
  o Escape routes
  o Testing controls
3.0 Threats and Vulnerabilities

3.1 Explain types of malware. (IA1) (CT4b)

- Adware
- Virus
- Spyware
- Trojan
- Rootkits
- Backdoors
- Logic bomb
- Botnets
- Ransomware
- Polymorphic malware
- Armored virus

3.2 Summarize various types of attacks. (CT4a) (CT4c) (CT4d)

- 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
• Watering hole attack

3.3 Summarize social engineering attacks and the associated effectiveness with each attack. (CT6)

• Shoulder surfing
• Dumpster diving
• Tailgating
• Impersonation
• Hoaxes
• Whaling
• Vishing
• Principles (reasons for effectiveness)
  o Authority
  o Intimidation
  o Consensus/Social proof
  o Scarcity
  o Urgency
  o Familiarity/liking
  o Trust

3.4 Explain types of wireless attacks. (CT4c)

• 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

3.5 Explain types of application attacks. (CT4c) (CT4e)

• Cross-site scripting
• SQL injection
• LDAP injection
• XML injection
• Directory traversal/command injection
• Buffer overflow
• Integer overflow
• Zero-day
• Cookies and attachments
• LSO (Locally Shared Objects)
• Flash Cookies
• Malicious add-ons
• Session hijacking
• Header manipulation
• Arbitrary code execution / remote code execution

3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.

(IA5) (SA1) (SA6) (SA7) (SA9) (SA10) (SA12) (SA13)

• Monitoring system logs
  o Event logs
  o Audit logs
  o Security logs
  o Access logs

• Hardening
  o OS installation methods*
  o Disabling unnecessary services
  o OS Service Packs and Updates
  o Protecting management interfaces and applications
  o Password protection
  o Disabling unnecessary accounts
  o File System and Hard Drives

• Network security
  o MAC limiting and filtering
    o 802.1x
    o Disabling unused interfaces and unused application service ports
  o Rogue machine detection

• Security posture
  o Initial baseline configuration
  o Continuous security monitoring
  o Remediation

• Reporting
  o Alarms
  o Alerts
  o Trends

• Detection controls vs. prevention controls
  o IDS vs. IPS
  o Camera vs. guard
3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities. (IA2) (IA3) (CT4f) (CD9)

- 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

3.8 Explain the proper use of penetration testing versus vulnerability scanning. (IA3)

- Penetration testing
  - Verify a threat exists
  - Bypass security controls
  - Actively test security controls
  - Exploiting vulnerabilities
- 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
4.0 Application, Data and Host Security

4.1 Explain the importance of application security controls and techniques. (FS7) (IA4)

- 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
- System development life-cycle

4.2 Summarize mobile security concepts and technologies. (IT3) (CT8) (PL10)

- 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
4.3 Given a scenario, select the appropriate solution to establish host security. (SA11) (SA15)

- Operating system security and settings
- OS hardening
- Anti-malware
  - Antivirus
  - Anti-spam
  - Anti-spyware
  - Pop-up blockers
- Patch management
- White listing vs. black listing applications
- Trusted OS
- Host-based firewalls
- Host-based intrusion detection
- Hardware security
  - Cable locks
  - Safe
  - Locking cabinets
- Host software baselining
- Virtualization
  - Snapshots
  - Patch compatibility
  - Host availability/elasticity
  - Security control testing
  - Sandboxing

4.4 Implement the appropriate controls to ensure data security. (IA7) (SA16)

- 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
  - Wiping
  - Disposing
  - Retention
  - Storage

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
5.0 Access Control and Identity Management

5.1 Compare and contrast the function and purpose of authentication services.

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- Secure LDAP

5.2 Given a scenario, select the appropriate authentication, authorization or access control.

(IA9) (IA11) (FS4) (CD2a) (SA4) (SA8)

- Identification vs. authentication vs. authorization
- Authorization
  - 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
5.3 Install and configure security controls when performing account management, based on best practices. *(SA2) (SA3)*

- 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
6.0 Cryptography

6.1 Given a scenario, utilize general cryptography concepts. (IC1) (CD2a) (IA6)

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- 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

6.2 Given a scenario, use appropriate cryptographic methods. (IC1) (IC3) (IA6)

- WEP vs. WPA/WPA2 and preshared 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
  o SSL
  o TLS
  o IPSec
  o SSH
  o HTTPS
• Cipher suites
  o Strong vs. weak ciphers
• Key stretching
  o PBKDF2
  o Bcrypt

6.3 Given a scenario, use appropriate PKI, certificate management and associated components.
   (IC2a) (IC2b) (IA6)
   • Certificate authorities and digital certificates
     o CA
     o CRLs
     o OCSP
     o CSR
   • PKI
   • Recovery agent
   • Public key
   • Private key
   • Registration
   • Key escrow
   • Trust models
### CAE2Y Knowledge Unit Domain Index

<table>
<thead>
<tr>
<th>Course Content KU Indicator</th>
<th>CAE2Y KU Full Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD</td>
<td>Basic Data Analysis</td>
</tr>
<tr>
<td>BS</td>
<td>Basic Scripting</td>
</tr>
<tr>
<td>CD</td>
<td>Cyber Defense</td>
</tr>
<tr>
<td>CT</td>
<td>Cyber Threats</td>
</tr>
<tr>
<td>FS</td>
<td>Fundamental Security Design Principles</td>
</tr>
<tr>
<td>IA</td>
<td>Information Assurance Fundamentals</td>
</tr>
<tr>
<td>IC</td>
<td>Introduction to Cryptography</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology System Components</td>
</tr>
<tr>
<td>NC</td>
<td>Networking Concepts</td>
</tr>
<tr>
<td>PL</td>
<td>Policy legal Ethics and Compliance</td>
</tr>
<tr>
<td>SA</td>
<td>Systems Administration</td>
</tr>
</tbody>
</table>

**NOTE:** the number following the KU Indicator represents the KU Domain topic as shown in the KU mapping matrix (Excel file).

* Indicates student review lab required before implementation of following topics.