COURSE SYLLABUS

LAST REVIEW Fall 2022

COURSE TITLE Computer and Network Security

COURSE NUMBER CRTE 0203

DIVISION Career and Technical Education

DEPARTMENT CRTE

CIP CODE 11.1006

CREDIT HOURS 3

CONTACT HOURS/WEEK Class: 1 Lab: 4

PREREQUISITES None

COURSE DESCRIPTION
This course is an introduction to the basic concepts, of computer and network security. Students will learn the knowledge and skills required to identify risk and participate in risk mitigation activities, provide infrastructure, application, operational and information security, apply security controls to maintain confidentiality, integrity and availability, identify appropriate technologies and products, and operate with an awareness of applicable policies, laws and regulations.

PROGRAM ALIGNMENT
This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit:
https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Students will be able to configure a router and a switch for basic functionality
2. Students will be able to configure, monitor and troubleshoot access controls lists for various addressing methods
3. Students will be able to build, maintain and troubleshoot server hardware and software technologies
4. Students will be able to explain and enforce basic concepts of computer network security

TEXTBOOKS
http://kckccbookstore.com/

METHODS OF INSTRUCTION
A variety of instructional methods may be used depending on content area. These include but are not limited to: lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE
I. Network Security

A. Implement security configuration parameters on network devices and other technologies.
    1. Firewalls
    2. Routers
    3. Switches
    4. Load Balancers
    5. Proxies
    6. Web security gateways
    7. VPN concentrators
    8. NIDS and NIPS
        a. Behavior based
        b. Signature based
        c. Anomaly based
        d. Heuristic
    9. Protocol analyzers
    10. Spam filter
    11. UTM security appliances
        a. URL filter
        b. Content inspection
        c. Malware inspection
    12. Web application firewall vs. network firewall
    13. Application aware devices
        a. Firewalls
        b. IPS
        c. IDS
        d. Proxies
B. Given a scenario, use secure network administration principles.
    1. Rule-based management
    2. Firewall rules
    3 VLAN management
    4. Secure router configuration
    5. Access control lists
    6. Port Security
    7. 802.1x
    8. Flood guards
    9. Loop protection
    10. Implicit deny
    11. Network separation
    12. Log analysis
    13. Unified Threat Management
C. Explain network design elements and components.
    1. DMZ
    2. Subnetting
    3. VLAN
    4. NAT

5. Remote Access
6. Telephony
7. NAC
8. Virtualization
9. Cloud Computing
    a. Platform as a Service
    b. Software as a Service
    c. Infrastructure as a Service
    d. Private
    e. Public
    f. Hybrid
    g. Community
10. Layered security / Defense in depth

D. Given a scenario, implement common protocols and services.

1. Protocols
    a. IPSec
    b. SNMP
    c. SSH
    d. DNS
    e. TLS
    f. SSL
    g. TCP/IP
    h. FTPS
    i. HTTPS
    j. SCP
    k. ICMP
    l. IPv4
    m. IPv6
    n. iSCSI
    o. Fibre Channel
    p. FCoE
    q. FTP
    r. SFTP
    s. TFTP
    t. TELNET
    u. HTTP
    v. NetBIOS
2. Ports
    a. 21
    b. 22
    c. 25
    d. 53
    e. 80
    f. 110
    g. 139

h. 143
i. 443
j. 3389

3. OSI relevance

E. Given a scenario, troubleshoot security issues related to wireless networking.

1. WPA
2. WPA2
3. WEP
4. EAP
5. PEAP
6. LEAP
7. MAC filter
8. Disable SSID broadcast
9. TKIP
10. CCMP
11. Antenna Placement
12. Power level controls
13. Captive portals
14. Antenna types
15. Site surveys
16. VPN (over open wireless)

II. Compliance and Operational Security

A. Explain the importance of risk related concepts.

1. Control types
    a. Technical
    b. Management
    c. Operational
2. False positives
3. False negatives
4. Importance of policies in reducing risk
    a. Privacy policy
    b. Acceptable use
    c. Security policy
    d. Mandatory vacations
    e. Job rotation
    f. Separation of duties
    g. Least privilege
5. Risk calculation
    a. Likelihood
    b. ALE
    c. Impact
    d. SLE
    e. ARO
    f. MTTR

g. MTTF
h. MTBF

6. Quantitative vs. qualitative
7. Vulnerabilities
8. Threat vectors
9. Probability / threat likelihood
10. Risk-avoidance, transference, acceptance, mitigation, deterrence
11. Risks associated with Cloud Computing and Virtualization
12. Recovery time objective and recovery point objective

B. Summarize the security implications of integrating systems and data with third parties.

1. On-boarding/off-boarding business partners
2. Social media networks and/or applications
3. Interoperability agreements
    a. SLA
    b. BPA
    c. MOU
    d. ISA
4. Privacy considerations
5. Risk awareness
6. Unauthorized data sharing
7. Data ownership
8. Data backups
9. Follow security policy and procedures
10. Review agreement requirements to verify compliance and performance standards

C. Given a scenario, implement appropriate risk mitigation strategies.

1. Change management
2. Incident management
3. User rights and permissions reviews
4. Perform routine audits
5. Enforce policies and procedures to prevent data loss or theft
6. Enforce technology controls
    a. Data Loss Prevention (DLP)

D. Given a scenario, implement basic forensic procedures.

1. Order of volatility
2. Capture system image
3. Network traffic and logs
4. Capture video
5. Record time offset
6. Take hashes
7. Screenshots
8. Witnesses
9. Track man hours and expense
10. Chain of custody

11. Big Data analysis

E. Summarize common incident response procedures.
1. Preparation
2. Incident identification
3. Escalation and notification
4. Mitigation steps
5. Lessons learned
6. Reporting
7. Recovery/reconstitution procedures
8. First responder
9. Incident isolation
    a. Quarantine
    b. Device removal
10. Data breach
11. Damage and loss control

F. Explain the importance of security related awareness and training.
1. Security policy training and procedures
2. Role-based training
3. Personally identifiable information
4. Information classification
    a. High
    b. Medium
    c. Low
    d. Confidential
    e. Private
    f. Public
5. Data labeling, handling and disposal
6. Compliance with laws, best practices and standards
7. User habits
    a. Password behaviors
    b. Data handling
    c. Clean desk policies
    d. Prevent tailgating
    e. Personally owned devices
8. New threats and new security trends/alerts
    a. New viruses
    b. Phishing attacks
    c. Zero-day exploits
9.Use of social networking and P2P
10. Follow up and gather training metrics to validate compliance and security posture

G. Compare and contrast physical security and environmental controls.
1. Environmental controls
    a. HVAC
    b. Fire suppression
    c. EMI shielding

d. Hot and cold aisles
e. Environmental monitoring
f. Temperature and humidity controls

2. Physical security
    a. Hardware locks
    b. Mantraps
    c. Video Surveillance
    d. Fencing
    e. Proximity readers
    f. Access list
    g. Proper lighting
    h. Signs
    i. Guards
    j. Barricades
    k. Biometrics
    l. Protected distribution (cabling)
    m. Alarms
    n. Motion detection
3. Control types
    a. Deterrent
    b. Preventive
    c. Detective
    d. Compensating
    e. Technical
    f. Administrative

H. Summarize risk management best practices.

1. Business continuity concepts
    a. Business impact analysis
    b. Identification of critical systems and components
    c. Removing single points of failure
    d. Business continuity planning and testing
    e. Risk assessment
    f. Continuity of operations
    g. Disaster recovery
    h. IT contingency planning
    i. Succession planning
    j. High availability
    k. Redundancy
    l. Tabletop exercises
2. Fault tolerance
    a. Hardware
    b. RAID
    c. Clustering
    d. Load balancing
    e. Servers

3. Disaster recovery concepts
    a. Backup plans/policies
    b. Backup execution/frequency
    c. Cold site
    d. Hot site
    e. Warm site

I. Given a scenario, select the appropriate control to meet the goals of security.
1. Confidentiality
    a. Encryption
    b. Access controls
    c. Steganography
2. Integrity
    a. Hashing
    b. Digital signatures
    c. Certificates
    d. Non-repudiation
3. Availability
    a. Redundancy
    b. Fault tolerance
    c. Patching
4. Safety
    a. Fencing
    b. Lighting
    c. Locks
    d. CCTV
    e. Escape plans
    f. Drills
    g. Escape routes
    h. Testing controls

III. Threats and Vulnerabilities

A. Explain types of malware
1. Adware
2. Virus
3. Spyware
4. Trojan
5. Rootkits
6. Backdoors
7. Logic bomb
8. Botnets
9. Ransomware
10. Polymorphic malware
11. Armored virus

B. Summarize various types of attacks.
1. Man-in-the-middle
2. DDoS

3. DoS
4. Replay
5. Smurf attack
6. Spoofing
7. Spam
8. Phishing
9. Spim
10. Vishing
11. Spear phishing
12. Xmas attack
13. Pharming
14. Privilege escalation
15. Malicious insider threat
16. DNS poisoning and ARP poisoning
17. Transitive access
18. Client-side attacks
19. Password attacks
    a. Brute force
    b. Dictionary attacks
    c. Hybrid
    d. Birthday attacks
    e. Rainbow tables
20. Typo squatting/URL hijacking
21. Watering hole attack

C. Summarize social engineering attacks and the associated effectiveness with each attack.
1. Shoulder surfing
2. Dumpster diving
3. Tailgating
4. Impersonation
5. Hoaxes
6. Whaling
7. Vishing
8. Principles (reasons for effectiveness)
    a. Authority
    b. Intimidation
    c. Consensus/Social proof
    d. Scarcity
    e. Urgency
    f. Familiarity/liking
    g. Trust

D. Explain types of wireless attacks.
1. Rogue access points
2. Jamming/Interference
3. Evil twin

4. War driving
5. Bluejacking
6. Bluesnarfing
7. War chalking
8. IV attack
9. Packet sniffing
10. Near field communication
11. Replay attacks
12. WEP/WPA attacks
13. WPS attacks

E. Explain types of application attacks.
1. Cross-site scripting
2. SQL injection
3. LDAP injection
4. XML injection
5. Directory traversal/command injection
6. Buffer overflow
7. Integer overflow
8. Zero-day
9. Cookies and attachments
10. LSO (Locally Shared Objects)
11. Flash Cookies
12. Malicious add-ons
13. Session hijacking
14. Header manipulation
15. Arbitrary code execution / remote code execution

F. Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
1. Monitoring system logs
    a. Event logs
    b. Audit logs
    c. Security logs
    d. Access logs
2. Hardening
    a. Disabling unnecessary services
    b. Protecting management interfaces and applications
    c. Password protection
    d. Disabling unnecessary accounts
3. Network security
    a. MAC limiting and filtering
    b. 802.1x
    c. Disabling unused interfaces and unused application service ports
    d. Rogue machine detection
4. Security posture
    a. Initial baseline configuration

b. Continuous security monitoring
c. Remediation

5. Reporting
    a. Alarms
    b. Alerts
    c. Trends
6. Detection controls vs. prevention controls
    a. IDS vs. IPS
    b. Camera vs. guard

G. Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities .

1. Interpret results of security assessment tools
2. Tools
    a. Protocol analyzer
    b. Vulnerability scanner
    c. Honeypots
    d. Honeynets
    e. Port scanner
    f. Passive vs. active tools
    g. Banner grabbing
3. Risk calculations
    a. Threat vs. likelihood
4. Assessment types
    a. Risk
    b. Threat
    c. Vulnerability
5. Assessment technique
    a. Baseline reporting
    b. Code review
    c. Determine attack surface
    d. Review architecture
    e. Review designs

H. Explain the proper use of penetration testing versus vulnerability scanning.

1. Penetration testing
    a. Verify a threat exists
    b. Bypass security controls
    c. Actively test security controls
    d. Exploiting vulnerabilities

2. Vulnerability scanning
    a. Passively testing security controls
    b. Identify vulnerability
    c. Identify lack of security controls
    d. Identify common misconfigurations
    e. Intrusive vs. non-intrusive

f. Credentialed vs. non-credentialed
g. False positive
3. Black box
4. White box
5. Gray box

IV. Application, Data and Host Security

A. Explain the importance of application security controls and techniques.
1. Fuzzing
2. Secure coding concepts
a. Error and exception handling
b. Input validation
3. Cross-site scripting prevention
4. Cross-site Request Forgery (XSRF) prevention
5. Application configuration baseline (proper settings)
6. Application hardening
7. Application patch management
8. NoSQL databases vs. SQL databases
9. Server-side vs. Client-side validation

B. Summarize mobile security concepts and technologies.
1. Device security
a. Full device encryption
b. Remote wiping
c. Lockout
d. Screen-locks
e. GPS
f. Application control
g. Storage segmentation
h. Asset tracking
i. Inventory control
j. Mobile device management
k. Device access control
l. Removable storage
m. Disabling unused features
2. Application security
a. Key management
b. Credential management
c. Authentication
d. Geo-tagging
e. Encryption
f. Application whitelisting
g. Transitive trust/authentication
3. BYOD concerns
a. Data ownership
b. Support ownership
c. Patch management

d. Antivirus management
e. Forensics
f. Privacy
g. On-boarding/off-boarding
h. Adherence to corporate policies
i. User acceptance
j. Architecture/infrastructure considerations
k. Legal concerns
l. Acceptable use policy
m. On-board camera/video

C. Given a scenario, select the appropriate solution to establish host security.
1. Operating system security and settings
2. OS hardening
3. Anti-malware
    a. Antivirus
    b. Anti-spam
    c. Anti-spyware
    d. Pop-up blockers
4. Patch management
5. White listing vs. black listing applications
6. Trusted OS
7. Host-based firewalls
8. Host-based intrusion detection
9. Hardware security
    a. Cable locks
    b. Safe
    c. Locking cabinets
10. Host software baselining
11. Virtualization
    a. Snapshots
    b. Patch compatibility
    c. Host availability/elasticity
    d. Security control testing
    e. Sandboxing

D. Implement the appropriate controls to ensure data security.
1. Cloud storage
2. SAN
3. Handling Big Data
4. Data encryption
    a. Full disk
    b. Database
    c. Individual files
    d. Removable media
    e. Mobile devices
5. Hardware based encryption devices

a. TPM
b. HSM
c. USB encryption
d. Hard drive

6. Data in-transit, Data at-rest, Data in-use
7. Permissions/ACL
8. Data policies
    a. Wiping
    b. Disposing
    c. Retention
    d. Storage

E. Compare and contrast alternative methods to mitigate security risks in static environments.

1. Environments
    a. SCADA
    b. Embedded (Printer, Smart TV, HVAC control)
    c. Android
    d. iOS
    e. Mainframe
    f. Game consoles
    g. In-vehicle computing systems
2. Methods
    a. Network segmentation
    b. Security layers
    c. Application firewalls
    d. Manual updates
    e. Firmware version control
    f. Wrappers
    g. Control redundancy and diversity

V. Access Control and Identity Management

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

1. RADIUS
2. TACACS+
3. Kerberos
4. LDAP
5. XTACACS
6. SAML
7. Secure LDAP

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

1. Identification vs. authentication vs. authorization
2. Authorization
    a. Least privilege
    b. Separation of duties

c. ACLs
d. Mandatory access
e. Discretionary access
f. Rule-based access control
g. Role-based access control
h. Time of day restrictions

3. Authentication
    a. Tokens
    b. Common access card
    c. Smart card
    d. Multifactor authentication
    e. TOTP
    f. HOTP
    g. CHAP
    h. PAP
    i. Single sign-on
    j. Access control
    k. Implicit deny
    l. Trusted OS
4. Authentication factors
    a. Something you are
    b. Something you have
    c. Something you know
    d. Somewhere you are
    e. Something you do
5. Identification
    a. Biometrics
    b. Personal identification verification card
    c. Username
6. Federation
7. Transitive trust/authentication

C. Install and configure security controls when performing account management, based on best practices.

1. Mitigate issues associated with users with multiple account/roles and/or shared accounts
2. Account policy enforcement
    a. Credential management
    b. Group policy
    c. Password complexity
    d. Expiration
    e. Recovery
    f. Disablement
    g. Lockout
    h. Password history
    i. Password reuse

j. Password length
k. Generic account prohibition
3. Group based privileges
4. User assigned privileges
5. User access reviews
6. Continuous monitoring

VI. Cryptography

A. Given a scenario, utilize general cryptography concepts.
1. Symmetric vs. asymmetric
2. Session keys
3. In-band vs. out-of-band key exchange
4. Fundamental differences and encryption methods
5. Transport encryption
6. Non-repudiation
7. Hashing
8. Key escrow
9. Steganography
10. Digital signatures
11. Use of proven technologies
12. Elliptic curve and quantum cryptography
13. Ephemeral key
14. Perfect forward secrecy

B. Given a scenario, use appropriate cryptographic methods.
1. WEP vs. WPA/WPA2 and preshared key
2. MD5
3. SHA
4. RIPEMD
5. AES
6. DES
7. 3DES
8. HMAC
9. RSA
10. Diffie-Hellman
11. RC4
12. One-time pads
13. NTLM
14. NTLMv2
15. Blowfish
16. PGP/GPG
17. TwoFish
18. DHE
19. ECDHE
20. CHAP
21. PAP
22. Comparative strengths and performance of algorithms

23. Use of algorithms/protocols with transport encryption
    a. SSL
    b. TLS
    c. IPSec
    d. SSH
    e. HTTPS
24. Cipher suites
    a. Block vs. stream
25. Key stretching
    a. PBKDF2
    b. Bcrypt

C. Given a scenario, use appropriate PKI, certificate management and associated components.
1. Certificate authorities and digital certificates
    a. CA
    b. CRLs
    c. OCSP
    d. CSR
2. PKI
3. Recovery agent
4. Public key
5. Private key
6. Registration
7. Key escrow
8. Trust models

COURSE LEARNING OUTCOMES AND COMPETENCIES

Upon successful completion of this course, the student will:

A. *Analyze, configure and discuss network security.*
1. Implement security configuration parameters on network devices.
2. Utilize network security principles.
3. Explain network design elements and components.
4. Implement common protocols, ports and services.
5. Troubleshoot security issues related to wireless networks.

B. *Analyze, configure and discuss compliance and operational security.*
6. Explain the importance of risk related concepts.
7. Summarize the risk related to integrating data with third parties.
8. Implement appropriate risk mitigation strategies.
9. Implement basic forensic procedures.
10. Summarize common incident response procedures.
11. Compare and contrast physical security and environmental controls.
12. Summarize risk management best practices.

C. *Analyze and explain types of threats and vulnerabilities.*
13. Explain types of malware.
14. Summarize various types of network attacks.
15. Summarize types of social engineering attacks.
16. Summarize types of application attacks.
17. Analyze types of mitigation and deterrent techniques.
18. Utilize appropriate tools and techniques to discover security threats and vulnerabilities.
19. Compare and contrast penetration testing and vulnerability scanning.

D. Analyze application, data and host security.
20. Explain the importance of application security controls.
21. Summarize mobile security concepts.
22. Select appropriate solutions to establish host security.
23. Implement controls to ensure data security.
24. Compare and contrast methods to mitigate security risks.

E. Analyze access control methods.
25. Compare and contrast functions and purposes of authentication services.
26. Determine the appropriate authentication.

F. Discuss cryptography.
27. Utilize general cryptography concepts and methods.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor's course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook
https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog
https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.