<table>
<thead>
<tr>
<th>Course Competency</th>
<th>Learning Outcomes</th>
</tr>
</thead>
</table>
| **Competency 1:** The student will demonstrate an understanding of network defensive concepts by: | • Numbers / Data  
• Critical thinking  
• Computer / Technology Usage  
• Information Literacy |
| 1. Discussing strategies to minimize exposure.  
2. Describing security concepts applicable to network infrastructure, including defense in depth, compartmentalization, least privilege, weakest link, hierarchically trusted components and protection, mediated access, accountability and traceability.  
3. Describing the features of network security architecture, including: administrative, technical and physical controls; Confidentiality, Integrity and Availability (CIA) of data; security policies and operations; risk analysis and management; and security life cycle.  
4. Describing access control methods, including passwords, card keys, biometrics, access control lists (ACLs), and authentication, authorization, and accounting (AAA).  
5. Describing network defensive technologies, including firewalls, DMZ, VPN, proxy servers, honeypots, intrusion detection systems (IDS) and intrusion prevention systems (IPS).  
6. Describing encryption concepts, methods, techniques and applications. |
1. Describing the categories of hackers, cybercriminals and other adversaries, their motivations, profiles, and common targets.
2. Describing logical and physical weaknesses in computers and networks as well as weaknesses in policies, procedures and practices of an organization and its personnel.
3. Explaining vulnerability windows (from 0-day to patch availability)
4. Describing the vulnerabilities inherent in network devices, protocols, and services, and the methods used to exploit them.
5. Describing how viruses, Trojan horses, spyware, worms, phishing, denial of service (DOS) attacks, control system attacks, and malicious software invade and infect a network.
6. Identifying common attacks and threat vectors, including cognitive threats via social media, social engineering, cell phone and consumer electronics exploits, man-in-the-middle and replay attacks, website compromises, virtualization exploits, memory scraping, hardware hacking, and IPv6-based attacks.
7. Describing vulnerabilities and threats to wireless and mobile networks.

**Competency 3:** The student will demonstrate an understanding of network security policies by:

1. Describing the laws and regulations that require organizations to protect their network systems and confidential information from cyberattack.
2. Explaining how security policies are used to: control network implementation; control access to the network (internally and externally), balance security restrictions with business operations; model user behavior; comply with government regulations; provide for criminal prosecution and civil litigation; establish disaster recovery procedures; set standards for handling abnormalities and security incidents; etc.
3. Assembling an Incident Response (IR) plan, based on best practices for: preparation,
identification, containment, eradication, recovery, and review of lessons learned.

4. Describing communication methods used within an organization and with law enforcement during security incidents and disruptions.
5. Describing procedures for responding to security issues, business disruption and disasters.
6. Describing methods to train, communicate and enforce security policies with end users.
7. Drafting a network security policy for the network of a given organization.

**Competency 4:** The student will demonstrate an understanding of the implementation of network defenses by:

1. Designing a network in compliance with a given security policy for an organization, and specifying the devices required including: hardened gateways; firewalls; IDS and IPS; honeypot; proxy servers; VLANs with port security; and Network Address Translation, DNS, Syslog, authentication and other servers.
2. Prescribing physical security controls for the assets and resources of a network.
3. Implementing a hardware firewall device and enabling the firewall on a host computer.
4. Implementing a DMZ with a public server.
5. Implementing a Virtual Private Network (VPN) server, with authentication, encryption and security protocols.
6. Implementing an IDS, a proxy server and a honeypot behind the firewall.
7. Configuring computers, servers and network devices for secure operations, including updating, patching and hardening the operating systems and their applications.
8. Describing the best practices for mitigating the vulnerabilities of wireless networks.
9. Troubleshooting a network’s defenses including security devices and services.
10. Performing a network security audit and the documenting the results.
**Competency 5:** The student will demonstrate an understanding of network monitoring by:

1. Performing network mapping
2. Describing the signatures of malicious system activity, including: overflow attack, cache poisoning, password cracking attack, data theft, denial of service (DOS) attack, session hijack, man-in-the-middle attack, and web site attacks.
3. Describing incidents, disruptions, and other unusual activities that trigger IR protocols.
4. Describing methods used by hackers and other adversaries to avoid detection.
5. Describing the operation of network intrusion detection and prevention systems.
6. Deploying open source IDS and IPS tools, including Snort, Suricata, OSSEC and Bro IDS.
7. Performing traffic analysis to detect signatures of malicious activity and other anomalies.
8. Analyzing data from logs and other sources to aid in the detection of security incidents.

**Competency 6:** The student will demonstrate an understanding of responding to network attacks by:

1. Outlining common attacks against the network
2. Describing the use of an Incident Response (IR) plan during a network attack.
3. Describing countermeasures, controls, and procedures for responding to network attacks.
4. Detecting, analyzing and documenting malicious system activity, including: overflow attack, cache poisoning, password cracking attack, data theft, denial of service (DOS) attack, session hijack, man-in-the-middle attack, and web site attacks.
5. Responding to a network attack by implementing procedures for containment, mitigation, protection of assets, preservation of evidence, eradication of malicious content, system recovery, and communication with authorities.
6. Collecting data and evidence from logs and other resources.
7. Restoring services and processes, and performing disaster recovery procedures.

Updated Spring 2021
<table>
<thead>
<tr>
<th>Course Competency 7: The student will demonstrate an understanding of workplace skills and professionalism by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Describing the roles of the network security professional in a business enterprise.</td>
</tr>
<tr>
<td>2. Describing methods of logging incidents and reporting problem resolution.</td>
</tr>
<tr>
<td>3. Presenting and following oral and written instructions.</td>
</tr>
<tr>
<td>4. Demonstrating self-motivation and responsibility to complete an assigned task.</td>
</tr>
<tr>
<td>5. Choosing appropriate actions in situations requiring effective time management.</td>
</tr>
<tr>
<td>6. Applying principles and techniques for being a productive, contributing member of a team.</td>
</tr>
<tr>
<td>7. Identifying and discussing intellectual property rights and licensing issues.</td>
</tr>
<tr>
<td>8. Identifying and discussing issues contained within professional codes of conduct.</td>
</tr>
<tr>
<td>9. Using appropriate communication skills, courtesy, manners, and dress in the workplace.</td>
</tr>
<tr>
<td>10. Documenting problems and solutions in service reports and maintaining support records.</td>
</tr>
<tr>
<td>11. Explaining the methods and best practices of interviewing end users to determine the symptoms and probable causes of system problems.</td>
</tr>
</tbody>
</table>

8. Reviewing and reporting lessons learned after a security breach.