Course Description

CTS2314 | Network Defense and Countermeasures | 4.00 credits

In this course, students will take an in-depth look at network defense concepts and techniques. Coverage includes network defensive concepts; policy development; problem solving; and implementation of firewalls, DMZ, VPN, IDS, NAT and proxy servers. Prerequisites: CTS1120 and CTS1134.

Course Competencies:

Competency 1: The student will demonstrate an understanding of network defensive concepts by:

1. Describing security concepts applicable to network infrastructure, including defense in depth, compartmentalization, least privilege, the weakest link, hierarchically trusted components and protection, mediated access, accountability, and traceability.
2. 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.
3. Describing access control methods, including passwords, card keys, biometrics, access control lists (ACLs), and authentication, authorization, and accounting (AAA).
4. Describing network defensive technologies, including firewalls, DMZ, VPN, proxy servers, honeypots, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
5. Describing encryption concepts, methods, techniques, and applications.

Competency 2: The student will demonstrate an understanding of network vulnerabilities and attack vectors by:

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 and weaknesses in policies, procedures, and practices of an organization and its personnel.
3. Describing the vulnerabilities inherent in network devices, protocols, and services and the methods used to exploit them.
4. Describing how viruses, Trojan horses, spyware, worms, phishing, denial of service (DOS) attacks, control system attacks, and malicious software invade and infect a network.
5. 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.
6. 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 cyberattacks.
2. Explaining how security policies are used to control network implementation, 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. Perform a network security audit and document the results.

Competency 5: The student will demonstrate an understanding of network monitoring by:

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

Competency 6: The student will demonstrate an understanding of network penetration testing by:

1. Describing and modeling the ethics of a licensed Penetration Tester.
2. Describing the tools and techniques used for penetration testing, including packet sniffers, port scanners, vulnerability scanners, and other assessment tools.
3. Installing scanning and vulnerability testing software, including Nmap, Nessus, Tcpdump, Wireshark, Snort, Netcat, Hashcat, and Metasploit.
4. Testing network perimeter defense mechanisms to evaluate boundaries.
5. Performing network reconnaissance and enumeration to identify targets, services, operating systems, applications, trust relationships, permissions, and user accounts.
6. Deploying proprietary and open-source tools to test for network vulnerabilities.
7. Deploying and using exploitation and vulnerability validation tools.
8. Evaluating network vulnerabilities and the degree of information exposure and network control an attacker could achieve after successfully exploiting such vulnerabilities.
9. Performing an intrusion attack to gain unauthorized access to a network system and compromising it.
10. Documenting the results of penetration testing in a formal
11. report with recommendations for hardening network defenses against discovered vulnerabilities and security gaps.

Competency 7: The student will demonstrate an understanding of responding to network attacks by:

1. Describing the use of an Incident Response (IR) plan during a network attack.
2. Describing countermeasures, controls, and procedures for
3. responding to network attacks.
4. Detecting, analyzing, and documenting malicious system activity, including overflow attacks, cache

poisoning, password cracking attacks, data theft, denial of service (DOS) attacks, session hijacks, man-in-the-middle attacks, and website 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.
8. Reviewing and reporting lessons learned after a security breach.

Competency 8: The student will demonstrate an understanding of basic network forensics by:

1. Describe the phases of forensic analysis and the activities performed in each phase.
2. Describing the forensic and evidentiary considerations when determining containment.
3. Describe the types and sources of data collected for forensic analysis.
4. Explain the various forms of data and the associated collection and retrieval tools for the OSI model's application, transport, network, and data link layers.
5. Explaining the processes by which data is collected for analysis.
6. Describing the role of system events and process logs in data collection.
7. Describing the processes associated with preserving forensic evidence.
8. Managing evidentiary data in an electronic environment.
9. Describing how the chain of custody can be maintained for
10. evidence collected during a forensic analysis effort.

Competency 9: The student will demonstrate an understanding of workplace skills and professionalism by:

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

Learning Outcomes:

1. Information Literacy
2. Social Responsibility
3. Communication
4. Computer / Technology Usage
5. Critical Thinking
6. Ethical Issues