TITLE:	Cybersecurity Essentials	
GRADE LEVEL:	Grades9-12	
ISBN:	9781635635539	
PUBLISHER:	Goodheart-Willcox Publisher	

ALIGNMENT
FLORIDA DEPARTMENT OF EDUCATION
NEXT GENERATION SUNSHINE STATE
STANDARDS FOR CYBERSECURITY ESSENTIALS

BENCHMARK CODE		STRAND / STANDARD / BENCHMARK	LESSONS WHERE STANDARD/BENCHMARK IS DIRECTLY ADDRESSED IN MAJOR TOOL (MOST IN-DEPTH COVERAGE LISTED FIRST) - Include the student edition and teacher edition with the page numbers of lesson, a link to lesson, or other identifier for easy lookup by reviewers.		
CTE Standards and Benchmarks			FS-M/LA	NGSSS-Sci	CORRELATING PAGES
40.0	Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges. - The student will be able to:				
	40.01	Explain the various elements that make up the security taxonomy used by the U.S. Computer Emergency Readiness Team (CERT).			35-38
	40.02	Describe the challenges associated with achieving and maintaining computer security.			41-43, 46-56
	40.03	Discuss the range of potential consequences of various forms of security breaches.			41-43, 46-56
	40.04	Describe various defense mechanisms, techniques, and methodologies (e.g., antivirus, anti-malware, protocol analyzers and scans, analyzing email			15-16, 45
	40.05	Compare and contrast mechanisms employed in passive and active cyber attacks.			41-46
	40.06	Describe the difference between an inside and an outside attack.			11-15
	40.07	Describe vulnerabilities associated with each element of the CIA Triad.			34-35
	40.08	Explain the differences between hardware, software, data, and network assets susceptible to cyber attack.			271-281, 392-394, 405-411, 494-495
	40.09	Describe the tools and technologies used in cybersecurity.			15-16
	40.10	Define intrusion detection and discuss its role in cybersecurity (e.g., HIDS and NIDS).			307-308
	40.11	Explain what is meant by the term countermeasures (e.g., NIPS and HIPS).			23-27
	40.12	Describe the role recovery plays in cybersecurity (e.g., Business Continuity Plan).			508-513
41.0	Demonstrate an understanding of common information and computer system security vulnerabilities. - The student will be able to:				
	41.01	Describe the basic categories of vulnerabilities associated with cybersecurity (i.e., hardware, software, network, human, physical, and organizational).			428
	41.02	Describe the ways in which various social networks are cybersecurity targets.			15-16
	41.03	Describe footprinting and explain how it is used to reveal system vulnerabilities.			166-167
	41.04	Explain why default values and technical controls are points of vulnerability and describe the hardening efforts being taken by government and industry.			41-45
	41.05	Describe the process of port scanning and explain why it is so prevalent in cybersecurity.			428
	41.06	Describe what is meant by password strength and explain its relationship to vulnerability.			88-89
	41.07	Distinguish between a weak and a strong password.			88-89
	41.08	Describe some of the ways in which intruders are able to cover their tracks.			50-54
	41.09	Describe the circumstances under which a computer system is vulnerable to a denial of service attack.			272
42.0	Demonstrate an understanding of common cyber attack mechanisms, their consequences, and motivation for their use. - The student will be able to:			SC.912.N.1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7; 2.2; 2.4; 2.5; 3.1; 3.2; 3.5; 4.1; 4.2	
	42.01	Describe spoofing as an attack mechanism and discuss its consequences and common motivating factors for its use.			41-45
	42.02	Describe the introduction of malware or spyware as an attack mechanism and discuss its consequences and common motivating factors for its use.			41-45
	42.03	Describe the use of grayware as an attack mechanism and discuss its consequences and common motivating factors for its use.			5
	42.04	Describe the use of computer viruses or worms as an attack mechanism and discuss its consequences and common motivating factors for its use.			12, 41-42
	42.05	Describe Logic Bombs as an attack mechanism and discuss its consequences and common motivating factors for its use.			42

CTE Standards and Benchmarks			FS-M/LA	NGSSS-Sci	CORRELATING PAGES
	42.06	Describe botnet and rootkit as an attack mechanism and discuss its consequences and common motivating factors for its use.			43, 204
	42.07	Describe the introduction of a Trojan horse as an attack mechanism and discuss its consequences and common motivating factors for its use.			41
	42.08	Describe DNS poisoning as an attack mechanism and discuss its consequences and common motivating factors for its use.			164, 289
	42.09	Describe buffer overflow as an attack mechanism and discuss its consequences and common motivating factors for its use.			392
	42.10	Understand the risk associated with a zero-day exploit.			46
	42.11	Understand risks associated with P2P networking including the Gnutella protocol and Torrents.			271-281
43.0	Be able to identify and explain the following different kinds of cryptographic algorithms. - The student will be able to:				
	43.01	Demonstrate the use and purpose of hashing functions.			365-366
	43.02	Demonstrate the use and purpose of symmetric keys.			356
	43.03	Demonstrate the use and purpose of asymmetric keys.			357
	43.04	Demonstrate the use and purpose of Kerberos.			82
44.0	Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity. - The student will be able to:				
	44.01	Network steganographic methods (e.g., WLAN).			359, 557
	44.02	Digital steganographic methods (e.g., image encryption, audio, mimic functions, video, packet manipulation).			262-269, 359, 557
45.0	Understand how cryptography and digital signatures address the following security concepts. - The student will be able to:				
	45.01	Provide examples of confidentiality.			35
	45.02	Provide examples of integrity.			35, 567
	45.03	Provide examples of authentication.			73
	45.04	Provide examples of non-repudiation.			35
	45.05	Provide examples of access control.			77-78
46.0	Understand and be able to explain the following concepts of PKI (Public Key Infrastructure). - The student will be able to:				
	46.01	Provide examples of certificates (e.g., policies, practice statements).			368-370
	46.02	Provide examples of revocation.			368-374
	46.03	Provide examples of trust models.			366-374
47.0	Demonstrate an understanding of certificates and their role in cybersecurity. - The student will be able to:				
	47.01	Describe the role of a Certificate Authority (CA).			368
	47.02	Describe Registration Authority (RA) and its relevance to security certificates.			368-374
	47.03	Compare and contrast SSL/TSL X.509-compliant certificates with PGP-compliant certificates.			368-374
	47.04	Describe the events that make up the lifecycle of a certificate.			368-374
	47.05	Describe how root certificate distribution works.			371
48.0	Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation. - The student will be able to:				
	48.01	Define intrusion.			307-308
	48.02	Describe the classes of intruders (i.e., masquerader, misfeasor, clandestine user).			307-308
	48.03	Describe what is meant by a hacker and discuss their role in cybersecurity.			5
	48.04	Compare and contrast the "black hat", "white hat", "blue hat", and "grey hat" hacker cultures (i.e., computer criminal versus computer security			5
	48.05	Describe various techniques used by hackers to achieve intrusion.			307-308

CTE Standards and Benchmarks			FS-M/LA	NGSSS-Sci	CORRELATING PAGES
49.0	Demonstrate an understanding of Intrusion Detection Systems (IDS). - The student will be able to:			SC.912.N.1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7; 2.2; 2.4; 2.5; 3.1; 3.2; 3.5; 4.1; 4.2; SC.912.P.10.1; 10.2; 10.4; 10.10; 10.14;	
	49.01	Describe the three logical components that comprise and IDS (i.e., sensors, analyzers, user interface).			307-308
	49.02	Explain how user behavior relates to the detection of an intruder.			307-308
	49.03	Describe the essential requirements for any IDS.			307-308
50.0	Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature). - The student will be able to:				
	50.01	Describe anomaly detection, specifically threshold and profile-based approaches.			307-308
	50.02	Describe the types of audit records employed in intrusion detection (i.e., native, detection-specific).			196-199
	50.03	Describe signature detection, specifically rule-based anomaly and penetration identification approaches.			78, 419
51.0	Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature). - The student will be able to:				
	51.01	Describe the primary approach for intrusion detection in a network.			307-308
	51.02	Compare and contrast inline and passive sensors.			424
	51.03	Discuss typical placement of sensors in a network-based IDS environment and explain the rationale for each.			424
52.0	Demonstrate an understanding of IDS applications. - The student will be able to:			SC.912.N.1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7; 2.2; 2.4; 2.5; 3.1; 3.2; 3.5; 4.1; 4.2	
	52.01	Describe the operation, typical activities, and outputs of an intrusion detection system.			307-308
	52.02	Describe some of the limitations of intrusion detection systems.			307-308
	52.03	Differentiate between an intrusion detection system (passive) and an intrusion prevention (reactive) system.			424
	52.04	Compare and contrast several of the intrusion detection systems available on the current market.			424
53.0	Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques. - The student will be able to:				
	53.01	Describe the process of monitoring/detecting port scanning attacks and associated patterns.			428
	53.02	Explain how the monitoring and analysis of network traffic can be used to detect intrusion.			428
	53.03	Utilize network monitoring and analysis tools to detect intrusion and anomalies.			428
54.0	Demonstrate an understanding of firewalls and other means of intrusion prevention. - The student will be able to:				
	54.01	Describe the purpose and limitations of firewalls.			206-211
	54.02	Describe the four types of firewalls (i.e., packet filtering, stateful inspection, application-level gateway, circuit-level gateway).			206-208
	54.03	Describe the use of honeypots as an intrusion prevention technique.			310
	54.04	Explain how security policies are used to prevent intruders.			34-38
	54.05	Explain how Access Control Lists (ACLs) are used to prevent intrusion.			78-79
55.0	Demonstrate an understanding of vulnerabilities unique to virtual computing environments. - The student will be able to:				
	55.01	Describe the limitations of traffic monitoring within virtual networks.			428
	55.02	Discuss the primary vulnerability of virtual operating systems.			293, 296
	55.03	Describe the "hypervisor" and explain its role in securing a virtual environment.			19
56.0	Demonstrate an understanding of social engineering and its implications to cybersecurity. - The student will be able to:				
	56.01	Define social engineering and describe its role in cybersecurity.			50-56
	56.02	Discuss common mechanisms that constitute social engineering (e.g., phishing, baiting, quid pro quo, pretexting).			50-56
	56.03	Describe the variety of attacks targeting the human element.			50-56

CTE Standards and Benchmarks			FS-M/LA	NGSSS-Sci	CORRELATING PAGES
	56.04	Describe countermeasures that can be used to counter social engineering attacks.			50-56
57.0	Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability. - The student will be able to:				
	57.01	Discuss the three over-arching security design principles (i.e., only necessary, simple, ease of use).			34-38
	57.02	Describe the principle of least privilege as it relates to computer security.			34-38
	57.03	Describe the principle of separation of duties as it relates to computer security.			78, 170
	57.04	Describe the principle of defense in depth as it relates to computer security.			36
	57.05	Describe the principle of fail secure or fail safe and false positive or false negative as it relates to computer security.			205
	57.06	Describe the principle of economy of mechanism as it relates to computer security.			34-38
	57.07	Describe the principle of complete mediation as it relates to computer security.			34-38
	57.08	Describe the principle of open design as it relates to computer security.			34-38
	57.09	Describe the principle of least common mechanism as it relates to computer security.			34-38
	57.10	Describe the principle of psychological acceptability as it relates to computer security.			34-38
	57.11	Describe the principle of leveraging existing components as it relates to computer security.			34-38
	57.12	Describe the principle of weakest link as it relates to computer security.			34-38
	57.13	Describe the principle of single point of failure as it relates to computer security.			515
58.0	Demonstrate the importance of health, safety, and environmental management systems in organizations and their importance to organizational performance and				
	58.01	Describe personal and jobsite safety rules and regulations that maintain safe and healthy work environments.			567-571, 57
	58.02	Explain emergency procedures to follow in response to workplace accidents.			568-569
	58.03	Create a disaster and/or emergency response plan.			588-589
59.0	Demonstrate leadership and teamwork skills needed to accomplish team goals and objectives. - The student will be able to:				
	59.01	Employ leadership skills to accomplish organizational goals and objectives.			569
	59.02	Establish and maintain effective working relationships with others in order to accomplish objectives and tasks.			568-569
	59.03	Conduct and participate in meetings to accomplish work tasks.			569-570
	59.04	Employ mentoring skills to inspire and teach others.			569-570
60.0	Explain the importance of employability skill and entrepreneurship skills. - The student will be able to:				
	60.01	Identify and demonstrate positive work behaviors needed to be employable.			567-571
	60.02	Develop personal career plan that includes goals, objectives, and strategies.			574-576
	60.03	Examine licensing, certification, and industry credentialing requirements.			571-574
	60.04	Maintain a career portfolio to document knowledge, skills, and experience.			574-576
	60.05	Evaluate and compare employment opportunities that match career goals.			574-576
	60.06	Identify and exhibit traits for retaining employment.			567-571
	60.07	Identify opportunities and research requirements for career advancement.			574-576
	60.08	Research the benefits of ongoing professional development.			574-576
	60.09	Examine and describe entrepreneurship opportunities as a career planning option.			574-576
	60.10	Understand the concept of hashing functions.			84
	60.11	Implement the use of symmetric keys.			356

CTE Standards and Benchmarks			FS-M/LA	NGSSS-Sci	CORRELATING PAGES
	60.12	Implement the use of asymmetric Keys.			357
	60.13	Understand Kerberos and when it should be implemented.			82
	60.14	Understand how to use network steganographic methods (e.g., VOIP, WLAN).			359, 557
	60.15	Understand how to use digital steganographic methods (e.g., image encryption, audio, mimic functions, video, packet manipulation).			359, 557
	60.16	Explain the importance of the C.I.A. model (Confidentiality, Integrity and Authentication).			34-35
	60.17	Explain the importance of integrity.			35
	60.18	Explain the importance of authentication.			35
	60.19	Understand non-repudiation.			35
	60.20	Implement access control.			78-79
	60.21	Utilize certificates.			368-374
	60.22	Check a certificate for revocation.			371
	60.23	Differentiate between one-way and two-way trust models.			225