Curriculum Map Overview

Career, Technical & Agricultural Education
Cluster: Information Technology
Course Name: Advanced CyberSecurity (11.48200)

Course Description: Advanced Cybersecurity is designed to provide students the advanced concepts and terminology of cybersecurity. The course explores the field of cybersecurity with updated content including new innovations in technology and methodologies. It builds on existing concepts introduced in Introduction to Cybersecurity and expands into malware threats, cryptography, organizational security, and wireless technologies.

Unit #	Unit Title	Timeframe (Suggested) (MS- 18 weeks; HS- 36 weeks
1	Employability Skills	Ongoing
2	CyberSecurity Ethics and the Law	3 Weeks
3	Malware Threats	4 Weeks
4	Threats and Vulnerability Analysis	4 Weeks
5	Advanced Cryptography	4 Weeks
6	Advanced Communication/Wireless Security	4 Weeks
7	Organizational Security	3 Weeks
8	Contingency Planning	3 Weeks
9	Security Analysis, Testing, and Evaluation	4 Weeks
10	Risk Management	3 Weeks
11	Basic Network Security Methods	4 Weeks
12	Career Portfolios	Ongoing
13	CTSOs	Ongoing

Unit 1 – Employability Skills							
DISCOVER: Top 10 Employability skills for young people video				**DISCUSS: What does "Professionalism" mean?**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Visit employment websites. Review the employability skills required for the job.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
Ongoing	**Explore how related student organizations are integral parts of career and technology education courses through leadership development, school and community service projects, entrepreneurship development, and competitive events.** 10.1 Explain the goals, mission and objectives of SkillsUSA. 10.2 Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development. 10.3 Explore the competitive events related to the content of this course and the required competencies, skills, and knowledge for each related event for individual, team, and chapter competitions.	1. How can CTSO prepare me for the workforce? 2. How can I show case my talents and abilities in CTSO? 3. What service-learning opportunities are available through CTSO? 4. Why should I join a CTSO?	I can dress for success. I can communicate professionally. I can write a professional essay. I am capable of giving a successful job interview.	Employability, SkillsUSA, Community Service, Leadership, Career, CTSO Career Technical Student Organizations, Professional Image, Communication	Life Maps Mock Interviews Right Way/Wrong Way Skits No-Hands Cup Stacking Challenge Time-Management Challenge Listen and Recap	Pre Test w/ Answer Key Post Test w/ Answer Key Work Ethic Progress Check 1 Work Ethic Progress Check 2	Top 10 Employability Skills Developing Mock Interview Questions Youtube – mock interview videos

Unit 2 – CyberSecurity Ethics and the Law							
DISCOVER: "*Ethics is knowing the difference between what you have the right to do and what is the right thing to do.*" - Unknown				**DISCUSS: Can you hack a network and still be ethical?**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Research individuals such as Edward Snowden and Reality Winner. Were they right or wrong in what they did?**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
2 Weeks	**Explore concepts of cybersecurity related to legal and ethical decisions. The following elements should be integrated throughout the content of this course.** 2.1 Describe the threats to a computer network, methods of avoiding attacks, and options in dealing with virus attacks. 2.2 Investigate potential abuse and unethical uses of computers and networks. 2.3 Explain the consequences of illegal, social, and unethical uses of information technologies. 2.4 Discuss computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and ethics pertaining to scanned and downloaded clip art images, photographs, documents, video, recorded sounds and music, trademarks, and other elements for use in Web publications.	1. What are some common methods for preventing attacks of a networking? 2. Discuss ways that crimes can be prevented in the workplace. 3. Name laws associated with computers crimes and the penalty for breaking the law	1. I can explain the ways a network can be attacked. 2. I can describe how to prevent workplace attacks. 3. I can discuss computer crime laws.	information security, confidentiality, integrity, availability, authentication, authorization, accounting, non-repudiation, defense in depth, white hat, ethical hacker, black hat, script kiddie, hacktivist, organized crime, advanced persistent threat (APT)	Professor Messer: Security Frameworks (3 Videos) Security Policies Fact Sheet Computer Ethics Jeopardy Game (multiple versions) Quizlet Live Computer Ethics Game (24 Terms)	Unit 03 Pretest Bank Unit 03 Posttest Bank Unit 03 Progress Check 1 Unit 03 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 3 – Malware Threats							
DISCOVER: "*Wannacry is the Stuxnet of Ransomware*" — James Scott				**DISCUSS: Name your top 5 malware prevention techniques.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: You are a computer forensics technician, name the devices, tools and applications you would use for your cell phone as evidence.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Investigate concepts of malware threats.** 3.1 Analyze and differentiate among types of malware. 3.2 Identify malware code, including strings. 3.3 Demonstrate skill in handling malware. 3.4 Demonstrate skill in preserving evidence integrity according to standard operating procedures or national standards.	1. How do the different types of malware affect a computer or network? 2. Discuss the steps in handling malware on a computer. 3. Name devices used in preserving evidence and how each function.	1. I can explain how malware attacks a network. 2. I can explain how to handle malware found on a computer. 3. I can name devices used in preserving evidence.	malware, virus, worm, Trojan horse, remote access Trojan (RAT), ransomware, spyware, adware, grayware, rootkit, spam, threat vector, attack vector, typosquatting, botnet, zombie, active interception, privilege escalation, backdoors, logic bomb, time bomb, open mail relay	Malware Jeopardy game (multiple versions) Professor Messor: Malware (9 Videos) Malware Fact Sheet Quizlet Live Malware Game (42 Terms)	Unit 04 Pretest Bank Unit 04 Posttest Bank Unit 04 Progress Check 1 Unit 04 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 4 – Threats and Vulnerability Analysis							
DISCOVER: ***"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers."*** **– Chris Pirillo**				**DISCUSS: Without giving personal information, describe a breach you or someone close to you had and how could it have been prevented.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Install Wireshark on a computer at home. Attempt to determine the IP addresses of computers sending you data.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Demonstrate how to analyze and react to various threats and vulnerabilities.** 4.1 Analyze and differentiate among types of network attacks (e.g., virus, worms, trojans, etc.). 4.2 Distinguish between different social engineering attacks (e.g., baiting, phishing/spear phishing, pretexting/ blagging, tailgating, quid pro quo, etc.). 4.3 Distinguish between reconnaissance/footprinting, infiltration, network breach, network exploitation, and attack for effects (e.g., deceive, disrupt, degrade, and destroy). 4.4 Demonstrate an understanding of DoS/DDoS, session hijacking, HTTP spoofing, DNS attacks, switch attacks, man-in-the-middle (MITM) attacks, and cross site scripting, and drive-by-attacks.	1. Compare and contrast the different malware attacks. 2. Compare and contrast the different social engineering attacks. 3. Compare and contrast the different network attacks.	1. I can explain how various malware attacks occur. 2. I can explain how various social engineering attacks occur. 3. I can explain how various network attacks occur.	pretexting, diversion theft, phishing, spear phishing, whaling, vishing, hoax, shoulder surfing, eavesdropping, dumpster diving, baiting, piggybacking, tailgating, mantrap, watering hole attack, Faraday cage, denial-of-service (DoS), ping flood, Smurf attack, Fraggle, SYN flood, flood guard, Ping of Death, teardrop attack, permanent DoS attack, fork bomb, distributed denial-of-service (DDoS), DNS amplification attack, spoofing, phishing, TCP/IP hijacking, man-in-the-middle (MITM), man-in-the-browser (MITB), watering hole attack, replay attack, DNS poisoning, pharming, ARP poisoning	Professor Messer: Attack Types (28 Videos) Understanding Attacks Fact Sheet Recon and Denial Fact Sheet Spoofing and Poisoning Fact Sheet Quizlet Live Network Threats Game Quizlet Live Network Vulnerabilities Game	Unit 05 Pretest Bank Unit 05 Posttest Bank Unit 05 Progress Check 1 Unit 05 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 5 – Advanced Cryptography							
DISCOVER: ***"Cryptography is the ultimate form of non-violent direct action."*** **— Julian Assange**				**DISCUSS: Use a cipher to encrypt your first or middle name. Post it. Attempt to unencrypt it. Post the answer and give the cypher used.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Find a website that offers free steganography services and try it for yourself.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Apply advanced principles of cryptology.** 5.1 Use and apply appropriate cryptographic tools and products. 5.2 Demonstrate knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]) and implement PKI, certificate management, and associated components. 5.3 Install and view a digital certificate. 5.4 Understand and master process to enroll for digital certificates. 5.5 Renew, revoke, backup, and restore public and private key certificates.	1. How do you apply cryptography to steganography? 2. How do you create a public key infrastructure for a small business? 3. Describe the process of enrolling a digital certificate. 4. Explain the process of asymmetric key certification	1. I can create cryptographic solutions. 2. I can build a Public Key Infrastructure. 3. I can discuss the key certification process. 4. I can enroll a digital certificate.	cryptography, encryption, cipher, algorithms, key, private key, public key, symmetric key algorithm, stream cipher, block cipher, asymmetric key algorithm, public key cryptography, digital signature, certificate, steganography, one-time pad, hash, hash function, one-way function, cryptographic hash functions, pass the hash, birthday attack, key stretching, public key infrastructure (PKI), certificates, X.509, wildcard certificate, certificate authority (CA), one-to-one mapping, many-to-one mapping, registration authority (RA), certificate revocation list (CRL), Online Certificate Status Protocol (OCSP), key escrow, key recovery agent	Advanced Cryptography (11 Activities) Cryptography Jeopardy games (multiple versions) Professor Messer: Cryptography (11 Videos) Advanced Cryptography Fact Sheet Escape the Room Activity	Unit 06 Pretest Bank Unit 06 Posttest Bank Unit 06 Progress Check 1 Unit 06 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 6 – Advanced Communication/Wireless Security							
DISCOVER: ***"If you use a cell phone - as I do - your wireless carrier likely has records about your physical movements going back months, if not years."*** **-Al Franken**				**DISCUSS: Look around the room. Name the strengths and weaknesses of the wireless networks in the classroom.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Install Wireshark on a wireless computer at home. Use it to determine the security level and encryption you are using.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Apply advanced communications and wireless security techniques.** 6.1 Implement wireless networks in a secure manner. 6.2 Analyze and differentiate among types of wireless attacks. 6.3 Configure a wireless Access Point (WPA, WPA-2). 6.4 Demonstrate use of InSSIDer and Netstumbler on wireless communications. 6.5 Demonstrate knowledge of Virtual Private Network (VPN) security and configure Virtual Private Network (VPN).	1. Configure wireless security on a wireless access point. 2. Compare and contrast the different wireless attacks. 3. Detect and analysis wireless networks using InSSIDer and Netstumbler. 4. Analysis and configure a VPN on a sample network.	1. I can configure wireless security on a WAP. 2. I can differentiate different wireless attacks. 3. I can use InSSIDer and Netstumbler to find wireless networks. 4.I can configure a VPN.	default account, privilege escalation, backdoor, electromagnetic interference (EMI), radio frequency interference (RFI), crosstalk, data emanation, Faraday cage, TEMPEST, wiretapping, butt set, protected distribution system (PDS), service set identifier (SSID), rogue AP, evil twin, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP), pre-shared key (PSK), Wireless Transport Layer Security (WTLS), Wi-Fi Protected Setup (WPS), MAC filtering, AP isolation, war-driving, war-chalking, IV attack, Wi-Fi disassociation attack, bluejacking, bluesnarfing	Wireless Security Jeopardy game (multiple versions) Professor Messer: Wireless Security (3 Videos) Professor Messer: Public Key Infrastructure (4 Videos) Wireless Security Overview Fact Sheet Public Key Infrastructure (PKI) Fact Sheet	Unit 07 Pretest Bank Unit 07 Posttest Bank Unit 07 Progress Check 1 Unit 07 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 7 – Organizational Security							
DISCOVER: ***"If you spend more time on coffee than on IP security, you will be hacked. What's more, you deserve to be hacked."*** **– Richard Clarke WH CS Adv.**				**DISCUSS: Using the information in this unit, create an acceptable use policy for something in your house. Get the OK from your teacher before starting.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Using the following website: Templates. Create a security for a technology in your house.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
3 Weeks	**Implement organizational security techniques.** 7.1 Explain the impact and proper use of environmental controls. 7.2 Explain the importance of security-related awareness and training. 7.3 Install environmental controls through Basic Input/Output System (BIOS). 7.4 Write organizational security policies (email, wireless, etc.).	1. How can environmental controls be used to improve network operations? 2. What are the best security policies for a business scenario?	1. I can write a security policy. 2. I can build a security policy and awareness solution. 3. I can build an environmental controls solution.	change management, separation of duties, acceptable use policy (AUP), mandatory vacations, onboarding, due diligence, due care, due process, personally identifiable information (PII), service-level agreement (SLA), memorandum of understanding (MoU), interconnection security agreement (ISA), incident response, incident management, first responders, chain of custody	Business Continuity Fact Sheet Professor Messer: Incident Response (2 Videos) Professor Messer: Forensics (2 Videos) Incident Response Fact Sheet Quizlet Live Business Continuity Game (31 Terms)	Unit 08 Pretest Bank Unit 08 Posttest Bank Unit 08 Progress Check 1 Unit 08 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 8 – Contingency Planning							
DISCOVER: ***"The biggest problem in incident response is understanding how the business is using its servers, its data, and who has access."*** **— Incident Response panel at SecureWorld Chicago**				**DISCUSS: Given a scenario, discuss incident response options for the company.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: What is your contingency plan for when you lose the data on your cell phone? How would you strengthen that plan?**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
3 Weeks	**Implement contingency planning (incident response and disaster recovery) techniques.** 8.1 Demonstrate knowledge of incident response and handling methodologies. 8.2 Demonstrate knowledge of incident categories, incident responses, and timelines for responses and compare and contrast aspects of business continuity. 8.3 Demonstrate the ability to capture volatile memory contents. 8.4 Perform imaging functions, such as operating system, network, and software configurations. 8.5 Restore a machine from a known good backup.	1. Can you demonstrate knowledge of a sample business incident response program? 2. Can you demonstrate the process of incident response given a scenario? 3. Can you demonstrate the process of capturing volatile memory given a scenario? 4. Can you backup and restore an operating system?	1. I can describe and discuss a sample incident response program. 2. I can apply an incident response program to a small business. 3. I can backup and restore an image.	single point of failure, surge, spike, sag, brownout, blackout, redundant power supply, uninterruptible power supply (UPS), backup generator, standby generator, RAID 1, disk duplexing, RAID 5, RAID 6, RAID 10, redundant ISP, cluster, failover clusters, load-balancing clusters, hot site, warm site, cold site, full backup, incremental backup, differential backup, 10 tape rotation, grandfather-father-son, Towers of Hanoi, snapshot backup, disaster recovery plan (DRP), business impact analysis (BIA), recovery time objective (RTO), recovery point objective (RPO)	Redundancy Fact Sheet Professor Messer: Resiliency and Automation (2 Videos) Business Continuity Fact Sheet Quizlet Live Contingency Planning Game (58 Terms)	Unit 09 Pretest Bank Unit 09 Posttest Bank Unit 09 Progress Check 1 Unit 09 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 9 – Security Analysis, Testing, and Evaluation							
DISCOVER: "*When it comes to Cybersecurity, nothing is more important that the facts. Are you secure? Yes or no*." – Matthew Blanco				**DISCUSS: List the devices that have internet access. Which vulnerability application would you use to test the device?**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Install Wireshark on a computer. Determine your security level for that computer.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Perform security analysis, as well as testing and evaluation.** 9.1 Analyze and differentiate among types of mitigation and deterrent techniques. 9.2 Implement assessment tools and techniques to discover security threats and vulnerabilities. 9.3 Demonstrate skill in conducting vulnerability scans and recognizing vulnerabilities in security systems (e.g., Nessus, Nmap, Retina). 9.4 Demonstrate knowledge of packet-level analysis in order to install and view packet sniffer. 9.5 Perform secure data destruction (e.g., Secure Erase, BCWipe).	1. How do you know when to use packet tracing, vulnerability scanning and penetration testing? 2. How do you install Nmap and perform a vulnerability scan? 3. How do you install Wireshark and view basic packet data?	1. I can use Wireshark to obtain packet data. 2. I can use Nmap to scan a computer for vulnerabilities. 3. I can determine what software to use to scan a network.	vulnerability, passive reconnaissance, active reconnaissance, vulnerability management, vulnerability assessment, penetration testing, network mapping, vulnerability scanning, port scanner, banner grabbing, protocol analyzer	Vulnerability Assessment Fact Sheet Protocol Analyzers Fact Sheet Penetration Testing Fact Sheet Professor Messer: Penetration Testing (1 Video) Professor Messer: Vulnerability Scanning (1 Video)	Unit 10 Pretest Bank Unit 10 Posttest Bank Unit 10 Progress Check 1 Unit 10 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 10 – Risk Management							
DISCOVER: ***"Sense and deal with problems in their smallest state, before they grow bigger and become fatal."*** **- Pearl Zhu**				**DISCUSS: Using what you have learned, perform a risk assessment on your cell phone. Post your results.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Continuing with the discussion topic, what mitigation methods are you using? Explain your answer.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
2 Weeks	**Implement risk management techniques for personal computer and network systems.** 10.1 Explain risk-related concepts. 10.2 Perform a risk assessment. 10.3 Identify mitigations for risks from risk assessment. 10.4 Conduct appropriate risk mitigation strategies.	1. How does a business identify risk? 2. Discuss what a risk analysis accomplishes. 3. Discuss what a business can do to mitigate risk. 4. Differentiate between the types of risk mitigation strategies.	1. I can conduct a risk assessment. 2. I can apply the appropriate risk mitigation strategy. 3. I can explain the concept of risk in a business.	risk, risk management, information assurance (IA), risk transference, risk avoidance, risk reduction, risk acceptance, residual risk, risk assessment, risk register, qualitative risk assessment, risk mitigation, quantitative risk assessment, mean time between failures (MTBF)	Risk Management Jeopardy Games (multiple versions) Professor Messer: Risk Management (1 Video) Risk Management Fact Sheet Quizlet Live Computer and Network Security Game	Unit 11 Pretest Bank Unit 11 Posttest Bank Unit 11 Progress Check 1 Unit 11 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 11 – Basic Network **Security Methods**							
DISCOVER: ***"Every time I say something that's extremely truthful out loud, it literally breaks the Internet"*** **– Kanye West**				**DISCUSS: Consider 5 applications you use on your cell phone; describe the protocols those apps use during communication.**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Develop a training program for your family members to train them to use their cell phones securely.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
4 Weeks	**Demonstrate how to work with advanced methods of cybersecurity.** 11.1 Apply and implement secure network administration principles. 11.2 Demonstrate knowledge of how network services and protocols interact to provide network communications to securely implement and use common protocols. 11.3 Identify commonly used default network ports. 11.4 Set up a Network Address Translation (NAT) device. 11.5 Spoof a Media Access Control (MAC) address. 11.6 Configure Virtual Private Network (VPN). 11.7 Configure a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).	1. How do ports function for the transmission and receiving of data? 2. Which ports are used for the most common network services? 3. How does NAT function and configure it for a network? 4. How does a VPN function and configure it for a network?	1. I can identify common network ports. 2. I can configure NAT for a network. 3. I can configure VPN for a network. 4. I can explain how ports function in data transmission. 5. I can use Nmap to scan for open ports.	File Transfer Protocol (FTP), Secure Shell (SSH), Telnet, Simple Mail Transfer Protocol (SMTP), Trivial File Transfer Protocol (TFTP), Hypertext Transfer Protocol (HTTP), Kerberos, Post Office Protocol v3 (POP3), NetBIOS, Internet Message Access Protocol (IMAP), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Layer 2 Tunneling Protocol (L2TP), Point to Point Tunneling Protocol (PPTP), RADIUS, RDP, Domain Name Service (DNS)	Tablets of Stone Activity Professor Messer: Secure Protocols (1 Video) Quizlet Live Network Protocols Game (65 Terms) Quizlet Live Secure Protocols Game (68 Terms) Network Protocols Fact Sheet	Unit 12 Pretest Bank Unit 12 Posttest Bank Unit 12 Progress Check 1 Unit 12 Progress Check 2	TestOut.com Security Plus Cert Guide Examcompass CompTIA Practice Exams SY0-501 Exam Objectives

Unit 12 – Online Portfolios							
DISCOVER: Organize personal online career portfolio for specific career interests.				**DISCUSS:**			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Consider watching competition videos related to both organizations. Feel free to ask questions at any time.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
Ongoing	**12.1 Review and update résumé to reflect new knowledge and skills master and additional work experience.** **12.2 Organize folders within the portfolio to reflect specific careers of interest, including résumé, targeted cover letter, and artifacts relevant to the specific career.** **12.3 Update all current items in the portfolio.** **12.4 Identify and upload additional industry-appropriate artifacts reflective of mastered skills throughout this course.** **12.5 Polish all entries in the online career portfolio to ensure accuracy and professionalism as expected from employers.** **12.6 Conduct a job search and share the appropriate folder with the potential employer.**	1. How would you tailor a resume to a specific career placement? 2. How do you write a targeted cover letter? 3. What examples can you provide (types of media) that will support your claims of experience in certain areas? 4. How can I improve my resume to make it more appealing to the employer?	1. I can explain the goals, mission and objectives of a job search. 2. I can dress for success and communicate professionally. 3. I can organzine an online portfolio.	Employability, resume, portfolio, interview, professionalism, media types.	Maintain Online Portfolio with ongoing assignments.	Each activity/task is a assessment at the same time for and during the competition.	Youtube.com

Unit 13 – Career & Technical Student Organization (CTSO)							
DISCOVER: Introduction to CyberPatriot and SkillsUSA Framework				**DISCUSS:** CyberPatriot is the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.			
DEMONSTRATE: Refer to Activities/Tasks/Assessments				**DEEPEN: Consider watching competition videos related to both organizations. Feel free to ask questions at any time.**			
Timeframe	**Standards (Priority/Supporting)**	**Essential Questions**	**Learning Targets**	**Vocabulary**	**Activities/Tasks**	**Assessments**	**Suggested Resources**
Ongoing	**Explore how related student organizations are integral parts of career and technology education courses through leadership development, school and community service projects, entrepreneurship development, and competitive events.** 10.1 Explain the goals, mission and objectives of SkillsUSA. 10.2 Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development. 10.3 Explore the competitive events related to the content of this course and the required competencies, skills, and knowledge for each related event for individual, team, and chapter competitions.	1. How can CTSO prepare me for the workforce? 2. How can I show case my talents and abilities in CTSO? 3. What service-learning opportunities are available through CTSO? 4. Why should I join a CTSO?	1. I can explain the goals, mission and objectives of CTSO. 2. I can explain how participating in CTSO will promote lifelong learning responsibilities for community service and professional development. 3. I can dress for success and communicate professionally.	Employability, CyberPatriot, SkillsUSA, Community Service, Leadership, Career, CTSO Career Technical Student Organizations, Professional Image, Communication	Attend Exhibition Round 1 Attend Exhibition Round 2 Attend the Cyberpatriot Training Round Attend the Cyberpatriot Sneak Preview Attend the Cyberpatriot Practice Round	Each activity/task is a assessment at the same time for and during the competition.	CyberPatriot SkillsUSA Youtube.com