Virginia Cyber Range Courseware Catalog Index and Descriptions

	COURSE: Ethics for the Cyber Age
Ethics for the Cyber Age	This course explores social, ethical, and policy issues of information technology developments by covering concerns that challenge today's cyber workforce. Selected course topics include the following: Classic Theories in Ethical Studies, Privacy and Personal Information (PPI) exposure, Manifestation of Human Rights in the Information Age, Intellectual Property, Computer Crime, Social Responsibilities of Modern Corporations, and Professional Ethics for Cyber Workers. The controversial questions raised at the end of case studies, together with chapter exercises, provide opportunities for students to express their viewpoints. Students will improve their critical thinking skills by going through case analysis and discussions. This course aims to prepare students to enter the future cybersecurity workforce, introducing them to and stressing the importance of the non-technical aspects of cybersecurity. In this way, students will better evaluate complex issues and defend their conclusions with facts, sound values, and rational arguments. There are two modules in this course: Module A: Ethical Theories Module B: Ethical Issues in Today's Organizations & Professional Codes of Ethics
Module A: Ethical Theories	This first module of the Ethics for the Cyber Age course focuses on Classic Ethical Theories that provide moral guidelines to individuals who need assistance in approaching cyber concerns in a thoughtful manner. This module lays the knowledge foundation for students who do not have much exposure to the subject matter and provides an overview of major social and ethical concerns that have short-term and long-term effects on how people perceive, use and interpret Information Technology. Instructors may use this module as a standalone learning unit.
Lesson A1: An Overview of Ethics in Cyber Age	This lesson describes ethical issues and concerns that emerged from the rapidly changing cyber technologies. Students will learn classic theories rooted in ethics, psychology, and social psychology that offer the basic grounding for practitioners to ethically assess, evaluate, and justify their course of action in daily situations.
Lesson A2: Kantianism	This lesson introduces Kantianism as a major workable theory that sheds light on today's ethical dilemmas. Both strengths and constraints of Kant's framework are discussed with examples provided concerning the application of Kantianism for typical ethical judgment in a computing environment.
Lesson A3: Consequentialism	This lesson introduces another popular workable theory - Consequentialism - that sheds light on today's ethical issues. The core concepts of Consequentialism are discussed, along with its variants, strengths, and constraints. Examples are provided concerning the application of Consequentialism for ethical judgment in the real world.
Lesson A4: Social Contract Theory & Principle of Justice	This lesson introduces Social Contract Theory & Principles of Justice as important ethical judgment theories that focus on the concepts of morally binding agreements and the principles of justice. Both strengths and constraints of this framework are discussed. Examples are provided to showcase how the theory and the principle can be useful for today's ethical appraisal needs.
Lesson A5: Just Consequentialism	This lesson introduces a combinative ethical framework Just Consequentialism. Coined by James Moor (1999), this framework has influenced many policies by addressing the complementary aspects of Just and Consequentialism, especially in the computing ethics area.
Module B: Ethical Issues in Today's Organizations and Professional Codes of Ethics	This second module, the last half of the Ethics for the Cyber Age course, looks into practical issues that impact established ethical standards and befuddle today's information workers and organizations. Issues such as data privacy, intellectual property, and social responsibility have long existed, whereas artificial intelligence and evolving professional codes of ethics are relatively new. Drawing upon the theoretical knowledge provided in Module A, students can explain the rationale supporting their ethical decisions related to real-world situations.
Lesson B1: Data, Privacy, and Government	This lesson discusses the concept of privacy as a right, its connection to the Constitution, and some of the key concerns related to real-world practices. Legislative regulations, intelligence gathering strategies, and approaches are also discussed.
Lesson B2: Intellectual Property	This lesson discusses the concept of intellectual property as a right, its connection to traditional perceptions of property rights, and some of the key concerns related to real-world practices. Viable measures of intellectual property protection are also discussed.
Lesson B3: Professional Codes of Ethics for IT Workers	This lesson discusses the role of a Code of Ethics for today's information workers, how it may exert impacts on organizations, and tools that are created to enhance professionalism and ethical behaviors. The Enron Scandal case is used to illustrate the detrimental effects of eroded ethics within an organization.
Lesson B4: Artificial Intelligence & Ethics	This lesson focuses on the concepts and technologies associated with Artificial Intelligence (AI), as well as ethical concerns.
Lesson B5: Social Responsibility	This lesson discusses the concepts revolving around social responsibility, its forms, requirements, and innovative ways the IT industry can give back to society.
	COURSE: Computer Systems Security for Non-Engineering Majors
Computer Systems Security for Non-Engineering Majors	This course is a three-module introductory survey course that will provide non-engineers the basic concepts and terminology required to enable an interdisciplinary workforce. Students will learn the basics of how computers and networks operate, with the focus on providing information that will allow students to understand various security risks and ways to defend against vulnerabilities. An introduction to coding concepts will be included.
Module A: How a Computer Works	This is the first module of the Computer Systems Security for Non-Engineering Majors course. Computer use is required of almost all professions in today's technological world and yet how they work is mysterious. This module starts from electrons and transistors and builds up to the major components of a computer. It spends a significant portion of the time describing binary logic since that is fundamental to understanding a computer. With the knowledge gained in this course, a student will be able to describe how a computer works and will be able to understand the importance of various characteristics of the computer.
Lesson A1: Digital Logic 1	Understanding digital logic is essential to understanding how a computer works. This lesson will provide an introduction to binary numbers and digital logic.
Lesson A2: Digital Logic 2	This lesson builds on the previous lecture (Lesson A1: Digital Logic 1) by showing how digital logic can be used to perform mathematical operations. This is central to a true understanding of how a computer works.
Lesson A3: Physical Implementation	This lesson builds on the previous lecture (Lesson A2: Digital Logic 2) by showing how digital logic can be used to perform mathematical operations. This lesson links these logic gates to the transistors used to implement them.
Lesson A4: Clocked Logic	In this lesson, we will introduce clocked logic which uses the binary logic that we've learned in the preceding section to do sequential calculations. After understanding clocked logic, the student will basically understand how math is implemented on a computer.
Lesson A5: Parts of a Computer	This lesson will go over parts of the computer to provide an understanding of what each of the larger components of the computer does.
Module B: How Software Works	This is the second module of Computer Systems Security For Non-Engineering Majors. This module provides some instruction on the writing of code, but is primarily focused on how the code works. Fundamentals of coding and memory handling are included. Some security implications of these low-level memory operations are discussed.
Lesson B1 Operating System	This first lesson in the "How Software Works" module describes what an operating system is and what it does. Software usually describes programs that are running in an operating system. The operating system is itself software that provides developers with a good platform for developing compatible programs.
Lesson B2: Bash	In this lesson, students will learn about programming in a basic scripting language, BASH. In this shell language, they will be introduced to the for-loop, while-loop, and if-then programming constructs. They will learn about how these scripted commands can either be input directly into the terminal, or saved in shell script files.
Lesson B3: Python	In this lesson, students will continue to enhance their scripting knowledge by learning to write scripts in python.
Lesson B4: Compiler	In this lesson, students will learn about an example compiled language and how that language gets converted to assembly language and then machine language. They will also learn about the difference between the stack and heap memory.
Lesson B5: Stack Heap	In this lesson, students will learn about how variables and functions are stored during the execution of a program.
Module C: How Networks Work	This is the third module of the Computer Systems Security For Non-Engineering Majors course. This module provides some instruction on Hyper-text Markup Language, LAMP, docker containers, and other components of networks and how they work. Some security implications of these low-level operations are discussed.
Lesson C1: Web Server	This first lesson in the How Networks Work module starts with a topic that is familiar to most people: websites. Most Internet users are primarily consumers of content, or if they produce content, it is through social media or platforms provided by others. This lesson provides knowledge of the fundamental building blocks of hosting web content and the ability to host a website on your local machine.

Lesson C2: Web Server Security	This is the second lesson of this module. It builds heavily on the first lesson on how to create a webserver. This lesson shows how a user steals information from users of your webserver. It also shows how an injection attack could be used to compromise the webserver.
Lesson C3: Rates and Diffie	In this third lesson of the How Networks Work module, students will learn some of the Internet's design considerations concerning latency and throughput. We will also introduce a basic type of cryptography called residual number system (RNS) cryptograph and a basic example of key exchange: Diffie Hellman.
Lesson C4: Cyber-Physical Systems Security	This lesson is meant to be a fun conclusion to this three-module series. Instead of digging into a lot of technical details, this lesson discusses cybersecurity and adds some considerations specific to cyber-physical systems. While cybersecurity concerns can be categorized as confidentiality, integrity, and availability, the concerns related to cyber-physical systems can be more complex.
	COURSE: Cyber Basics
Cyber Basics	This course aims to provide a basic and broad overview of cybersecurity, helping the student to understand correct and safe online behavior and increase their interest in cybersecurity and careers in the cybersecurity workforce. In this course, we will explore various cybersecurity topics to include networking and network security tools, cryptography (ciphers, keys, digital signatures, hashes, encryption protocols, etc.), hacking basics (network reconnaissance and scanning, password cracking, and exploiting web application vulnerabilities), and the legal and ethical considerations of cybersecurity activities. There is a total of seven modules in this course, but only the first six are meant to be taught to the students. The additional seventh module (Module G) is provided as a resource for the prospective teacher.
Module A: Introduction to Linux	Module A of the Cyber Basics course (aka GenCyber) contains a collection of introductory hands-on Linux labs for students to become familiar with the Linux OS as well as many of the tools used in cybersecurity. LABS: Introduction to the Linux Terminal and Understanding Directories Linux Applications and Other Tools Introduction to the Linux User Accounts, Groups, and Permissions Linux Networking and Command Line Tools Introduction to Networking Introduction to Wireshark
Laboratory Exercise A1: Introduction to the Linux Terminal and Understanding Directories	This laboratory exercise will provide a fundamental understanding of the Linux Terminal (also referred to as the command-line), a powerful tool for all cyber security professionals. The terminal allows a user to manipulate files, create users, and run terminal programs to perform certain tasks. For the purposes of this lab, we will be focusing on the Linux filesystem and directories.
Laboratory Exercise A2: Linux Applications and other tools	In this exercise, we will explore some various tools in the Linux operating system. Though Kali Linux comes preloaded with many tools for security practice, it is like all other operating systems with web browser applications and text editors. These tools, however, can serve every security personnel in some administrative way.
Laboratory Exercise A3: Introduction to Linux User Accounts, Groups, and Permissions	This lesson will provide an introduction into Linux user accounts. By the end of this lesson, you should be comfortable creating, deleting, and managing, user accounts. Groups and Permissions will also be introduced.
Laboratory Exercise A4: Linux Networking and Command Line Tools	This laboratory exercise will expand your understanding of the Linux Terminal (sometimes called the “shell”, command-line, or CLI) and introduction to a powerful set of tools all cyber security professionals should fully embrace. Linux and UN*X based operating systems are comprised of thousands of “many small tools that do one thing well,” as the saying goes – a realization that only more seasoned experts fully appreciate. This “many small tools” concept is the foundation of the UN*X philosophy, and if fully embraced, greatly amplifies the user's ability to perform very complex operations. It represents much of the hidden power Linux users have access to. For the purposes of this lab, we will be focusing on learning more Linux command line tools and how they work together to provide simple yet powerful functionality.
Laboratory Exercise A5: Introduction to Networking	In this lesson, the student will learn the fundamentals of networking. The student will use the Linux operating system as a tool to understand networking concepts. By now, the student should understand the Internet, ethernet connections, and Wi-Fi. By the end of this lesson, the student should understand how machines communicate with each other in a network.
Laboratory Exercise A6: Introduction to Wireshark	In this lesson, the student will be introduced to Wireshark, a very useful tool that covers a very important network forensics concept – reading and understanding networking traffic. Wireshark (software known as a packet analyzer) allows you to view pieces of data (called packets) in real-time as they go in and out of a system and can be saved as packet capture (pcap or cap) files. In this exercise, the student will be analyzing packet capture files as well as capturing live network traffic in real-time.
Module B: Introduction to Cybersecurity and Virtualization	Module B of the Cyber Basics course (aka GenCyber) covers introductory level cybersecurity topics. In the first lesson, it provides a very high-level and basic overview of cybersecurity. During the remaining lessons, it walks the student through hands-on installation of virtualization software and a Linux operating system on a virtual machine (VM). Additionally, the student is exposed to, and gains confidence using, rudimentary Linux commands and tasks. At the end of this module, the student should have a basic understanding of cybersecurity and the skills to install and use virtualization software. This module prepares the student for follow-on modules in the Cyber Basics course.
Lesson B1: Introduction to and Overview of Cybersecurity	This lesson provides an introduction and overview of cyberspace and cybersecurity. We will explore the fundamental principles of cybersecurity, i.e. confidentiality, integrity and availability. We also explore some common threats to information security and look at basic security fundamentals to understand how we can secure our systems and networks better.
Lesson B2: System Preparation: Virtualization and Linux OS Installation	This lesson provides the steps to download and install free open-source virtualization software on a computer (laptop); in this lesson we use Oracle’s VirtualBox. It then provides instructions on how to create a new virtual machine using this software and then walks through the steps to install a Linux operating system on it.
Lesson B3: Introduction to Kali Linux and the Command Line	This lesson familiarizes the student with a Linux user interface and provides hands-on experience in a UNIX-based environment to gain familiarity with basic UNIX commands and tasks.
Lesson B4: Windows Command Line	This lesson familiarizes the student with the Windows user interface and basic Windows commands and tasks.
Module C: Networking	This is the second module in the Cyber Basics course (aka GenCyber). It provides basic definitions related to networking (NIC, LAN, WAN, WAP, internet, etc.) and describes basic network devices. It explains the pros/cons between wired and wireless network topographies. It also gives a brief overview and history of the global internet. It familiarizes the student with layered networking models (TCP/IP & OSI), the client-server networking model, and some basic tools for network defense, specifically firewalls (network and host-based) and intrusion detection/prevention systems. It provides them with a basic understanding of networking concepts for both UNIX/Linux and Windows environments and network services (DNS, web servers, FTP, SSH, etc.). Additionally, it provides some hands-on experience with a network protocol analyzer software tool (Wireshark) and Windows firewall settings and rules. Upon completion of this module, the student will have a rudimentary understanding of how networks work and be familiar with some basic tools to defend them.
Lesson C1: Introduction to Network Concepts	This lesson provides basic definitions related to networking and describes basic network devices. It gives examples of wired and wireless network topographies and encourages students to consider advantages and disadvantages of network model. It also describes local area and wide area networks, and also gives a brief overview and history of the global internet. Finally, this lesson introduces basic network security devices and discusses how they might be deployed in a network.
Lesson C2: Network Fundamentals	This lesson familiarizes the student with layered networking models (TCP/IP & OSI) and exposes them to basic networking concepts for both UNIX/Linux and Windows environments. Additionally, it provides hands-on experience with a network protocol analyzer software tool (Wireshark) used to examine network traffic.
Lesson C3: Network Services (Daemons)	This lesson familiarizes the student with client-server networking model and provides them with a basic understanding of network services such as the Domain Name Service, web servers, file transfer protocol (FTP) and secure shell (SSH).
Lesson C4: Network Security Tools	This lesson familiarizes the student with the basic tools for network defense, specifically firewalls (network and host-based) and intrusion detection/prevention systems. Additionally, it provides some hands-on experience with Windows firewall settings and rules.
Lesson C5: Introduction to Wireshark	This lesson familiarizes the student with Wireshark, a network protocol analyzer. This tool allows students to capture and analyze network traffic in real time, as well as opening saved network packet capture data for analysis after-the-fact. Most network incident response involves analyzing saved network traffic to determine whether, when, and how a specific device on the network might have been compromised.

Module D: Cryptography	This is the third module in the Cyber Basics course (aka GenCyber). It begins by providing the student with a bit of the evolution of cryptography and cryptographic systems, exposing them to several cipher techniques. We then look at basic threats to confidentiality and explain how cryptography can help to ensure confidentiality, discussing the cryptography process and symmetric versus asymmetric cryptography. The module introduces the student to several critical pieces and parts of modern cryptography to include cryptographic algorithms, cryptographic hash functions, key exchange, key management (private and public keys), PKI, and digital signatures. Additionally, the module provides the student with some hands-on experience with cryptography using online tools and exposure to techniques for encrypting and decrypting files.
Lesson D1: Introduction and Evolution	This lesson introduces the student to cryptography and cryptographic systems and exposes them to several cipher techniques. Additionally, it provides hands-on experience with a few of these techniques.
Lesson D2: Modern Cryptography	This lesson familiarizes the student with basic threats to confidentiality and explains how cryptography can help to ensure confidentiality via PAIN (Privacy, Authentication, Integrity, and Non-repudiation). This lesson also explains the cryptography process and discusses symmetric versus asymmetric cryptography, looking at several pieces and parts of modern cryptography to include key exchange, key management (private and public keys), PKI, and digital signatures. Finally, it provides the student with several examples of cryptographic algorithms and explains cryptographic hash functions and their uses.
Lesson D3: Hands-on Cryptography	This lesson provides the student with some hands-on experience with cryptography using online tools to solve simple cryptographic problems. It also exposes the student to techniques for encrypting and decrypting files on a Linux system. For this lesson, we assume the instructor has provisioned accounts for his or her students in the Virginia Cyber Range and has added the Laboratory Exercise D3: Introduction to Cryptography Lab to their course. The instructor should have copies of the lab hand-out from the courseware repository.
Laboratory Exercise D3: Introduction to Cryptography Lab	This introductory lab has students learn how to use both symmetric and asymmetric encryption at the Linux command line. This exercise includes an encryption primer and an introduction to symmetric encryption using the Linux utility ccrpyt. It also has students use the Linux gpg utility to create a public/private key pair, as well as encrypt and decrypt a file using public-key cryptography.
Lesson D4: Encryption Protocols	This lesson introduces the student to several encryption protocols and their uses with other protocols.
Module E: Hacking	This is the fourth module in the Cyber Basics course (aka GenCyber). This module familiarizes the student with techniques for passive and active network reconnaissance to include sweeping, scanning, OS finger printing, banner grabbing, war-dialing and war-driving. It then looks at how passwords are stored (hashes) and how attacks on user password hashes are carried out. During the password cracking lesson, the students actually get some hands-on experience with a free, open source password cracking tool. Finally, the module moves on to how web servers have evolved and introduces the student to the various web application vulnerabilities resulting from this evolution. Again, students get some hands-on experience by attacking web applications using a known vulnerable website with vulnerable applications.
Lesson E1: Reconnaissance and Scanning	This lesson familiarizes the student with techniques for passive and active network reconnaissance to include sweeping, scanning, OS finger printing, banner grabbing, war-dialing and war-driving.
Laboratory Exercise E1: Reconnaissance and Network Scanning Lab	This introductory lab has students scanning a small network subnet using nmap to identify live hosts and open ports. Targets include three virtual machines: a web server, a vulnerable Samba server, and an FTP server, as well as other open network ports. It teaches Linux utilities for reconnaissance and scanning such as whois, ifconfig, and nmap with various command-line switches.
Lesson E2: Hands-on with Password Audits	This lesson provides the student with a basic understanding of how passwords are stored (hashes) and how attacks on user password hashes are carried out. Additionally, students get some hands-on experience with a free, open source password cracking tool, i.e. John the Ripper. This lesson includes a hands-on exercise in the Virginia Cyber Range. If instructors would like to have students complete the exercise, they should have requested an account and had a course created for them. They should upload their student list to the course and prepare the exercise entitled 'Laboratory Exercise E2: Introduction to Password Auditing Lab' and download the lab document from the courseware repository.
Laboratory Exercise E2: Introduction to Password Auditing	This introductory lab has students conducting a password audit using John the Ripper, a free open source password cracking software tool, on a Linux computer.
Lesson E3: Web Application Vulnerabilities	This lesson provides the student with a basic understanding of how web servers have evolved and introduces them to the various web application vulnerabilities resulting from this evolution. Throughout the lesson, students get some hands-on experience attacking web applications using a known vulnerable website with vulnerable applications. These attacks include SQL Injection, Command Injection, and Cross Site Scripting (XSS). This lesson includes two hands-on exercises in the Virginia Cyber Range. This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course. They should upload their student list to the course and prepare the exercise entitled ' Laboratory Exercise E3: Web Application Security: SQL Injection Lab' and 'Laboratory Exercise E3: Web Application Security: Command Injection Lab' and download the lab documents from the courseware repository.
Laboratory Exercise E3: Web Application Security: SQL Injection Lab	This introductory lab has students using simple SQL injection to attempt to gain unauthorized access to data on an intentionally vulnerable web server. The lab document includes a brief SQL primer so that students understand enough to exploit simple SQL injection attacks, followed by an introduction to DVWA and its SQL Injection page for testing injection techniques.
Laboratory Exercise E3: Web App Penetration Security: Command Injection Lab	This introductory lab has students using simple command injection to attempt to gain unauthorized access to data on an intentionally vulnerable web server. The lab document includes a brief primer on command injection and an introduction to DVWA and its command injection tab so students can use command injection to answer a series of lab questions.
Module F: Legal and Ethics	This is the fifth module in the Cyber Basics course (aka GenCyber). This module stimulates discussion and gets students thinking about the importance of ethical behavior when engaging in cybersecurity activities. It looks at Acceptable Use Policies, various case studies, and existing codes of ethics/conduct in industry today. It also presents the student with several recent case studies on cybersecurity activities (national and international) and allows them to explore and discuss the legal, ethical and privacy considerations of each case.
Lesson F1: Ethics and Cybersecurity Education	This lesson discusses the importance of ethical behavior when engaging in cybersecurity activities. It looks at Acceptable Use Policies, various case studies, and existing codes of ethics/conduct in industry today.
Lesson F2: Case Studies: Cybersecurity Law, Ethics, and Privacy	This lesson presents the student with several recent case studies on cybersecurity activities (national and international) and allows them to explore and discuss the legal, ethical and privacy considerations of each case.
Module G: Teacher Resources	This is the sixth and final module in the Cyber Basics course (aka GenCyber). This module is a resource and reference for high school teachers (or other educators) using parts or all of the material from the Cyber Basics course. These are tools and resources that can assist the teacher in getting students excited about and engaged in cyber education. It discusses several topics to include starting a cybersecurity "hacking" club, cybersecurity competitions, getting guest speakers in the field of cybersecurity, Hacker Con events, the Maker Movement, and Hackerspaces. Additionally, it provides a listing of various free online cybersecurity educational tools and resources suitable for use by high school teachers in their classrooms.
Lesson G1: Getting Students Engaged in Cyber Education	This lesson is a resource tool and reference for high school teachers to get students excited about and engaged in cyber education. It discusses several topics to include starting a cybersecurity "hacking" club, cybersecurity competitions, getting guest speakers in the field of cybersecurity, Hacker Con events, the Maker Movement, and Hackerspaces.
Lesson G2: Awesome (mostly Free) Online Tools	This lesson introduces various free online cybersecurity educational tools and resources for use by high school teachers in their classrooms.
	COURSE: Cyber-Physical Industry

Cyber-Physical Industry	The goal of this course is to familiarize the student with the elements of automated production systems from both traditional and modern (cyber-physical) perspectives, reflecting the long (20-40 year) asset lifecycles commonly seen in large manufacturing plants in both discrete and process industries. Traditional industrial control systems (ICS) were built from mechanical and electrotechnical devices in closed (air-gapped) systems, but information technologies and communication protocols are central to modern control systems. Although this increases efficiency, and can reduce waste and costs, these changes have made the infrastructures more vulnerable to external attack. Safety and ergonomics are often drivers of automation, but in the era of wide-scale cyber-physical systems, both physical and cognitive ergonomics play a key role: even in highly automated systems, humans are still required to rapidly integrate and interpret information. Confusion (which can be brought about by both physical and cognitive impairments) can be costly, dangerous, and increase an organization's vulnerability to attack. As a result, this course will familiarize the student with the terms, definitions, and architecture of Industrial Control Systems (ICS) from the joint perspectives of quality management and cybersecurity. Using hazards, risks, vulnerabilities, threats, and impacts as the basis for understanding, we will explore conceptual frameworks and analytical tools for understanding and managing aspects of cyber-physical industry based on new research. This course is not a deep dive into specific tools, protocols, vulnerabilities, or exploits, but will help the student navigate the industrial environment and its expanding ecosystem of connected components. This course is broken into four logical modules: Module A: Introduction to Industrial Control Systems Module B: Critical Infrastructure & Smart Cities Module C: Managing Security, Safety, and Risk Module D: Physical and Cognitive Ergonomic
Module A: Introduction to Industrial Control Systems	This is the first module in the Cyber-Physical Industry course; however, it can be taught as a standalone module. The purpose of this module is to introduce students to concepts associated with system assets and system operations in industrial control systems. The material is approached from the perspective of quality management, which aims to discover and describe all processes, participants, and interactions to ensure that an industrial system meets its strategic and operational goals. This module provides a high-level introduction to the industrial environment to prepare students for more in-depth work in industrial networks, ICS protocols, and PLC programming.
Lesson A1: Quality, Innovation, & Cybersecurity	This lesson focuses on foundational concepts that will help students understand production systems from a quality systems perspective.
Lesson A2: Mechanization & Automation	This lesson focuses on mechanization and automation: core concepts underlying the existence of all industrial control systems.
Lesson A3: Control Systems from Ancient Times to Present	This lesson explains what control systems are, how they work (at a high level), how they have evolved since ancient times, and how "Industry 4.0" emerged.
Lesson A4: Key Concepts in ICS and Cyber-Physical Systems	This lesson describes the components of an ICS (including RTU, PLC, PAC, SCADA, HMI, SIS, DCS) and their inter-relationships.
Lesson A5: Control Systems in Discrete Manufacturing & Process Industries	This lesson explains how control systems differ depending upon whether a plant is manufacturing units of a product (cars, books, phones) or volumes of a product (beverages, beer, pharmaceuticals).
Lesson A6: Concepts in PLC Programming	This lesson introduces the student to programming concepts in ladder logic for Programmable Logic Controllers (PLCs); an understanding the functions of PLCs can help with securing and protecting the processes they control. This lesson will prepare students for hands-on courses in PLC programming.
Lesson A7: Evolution of HMIs to VR/AR and Augmented Human	This lesson describes the history and future of Human-Machine Interfaces (HMIs) in the industrial context, including virtual reality (VR), augmented reality (AR), mixed reality (MR), diminished reality (DR), wearables, bio-signal HMIs, and the "Augmented Human."
Module B: Critical Infrastructure & Smart Cities	This is the second module in the Cyber-Physical Industry course; however, it can be taught as a standalone module. The purpose of this module is to introduce students to the current concept of critical infrastructure, the sectors of the economy that are currently managed as critical infrastructure, and the vision for how critical infrastructure will evolve as "smart cities" grow and develop.
Lesson B1: Critical Infrastructure Sectors	This lesson describes critical infrastructure sectors, which depend on industrial control systems (ICS) while making production systems (and other critical infrastructure sectors) possible.
Lesson B2: From M2M to IoT	This lesson explains how machine-to-machine (M2M) communications, which have been critical for ICS performance for decades, lay the groundwork for the Internet of Things (IoT).
Lesson B3: Asset Management	This lesson introduces asset management, a critical enterprise activity for most industrial operations, and explains why IoT is a focal element in the next generation of asset management systems.
Lesson B4: Commercial Building Automation	This lesson describes the components of commercial Building Automation Systems (BAS), a very common implementation of industrial control systems (ICS), and related security issues.
Lesson B5: Smart Cities	This lesson introduces smart grids and smart cities, emphasizing the enabling technologies which originated in ICS and M2M, and the new challenges associated with cyber-physical infrastructure risk.
Lesson B6: Participatory Sensing	This lesson introduces participatory sensing (PS), systems in which individuals serve as monitor points within their own communities to provide resources that are only available as the result of distributed data collection.
Lesson B7: Seasteading	This lesson provides an introduction to seasteading, an extreme future vision for "platform-as-a-service" smart cities to support radical innovation in all areas of technology and society.
Module C: Managing Security, Safety, and Risk	This is the third module in the Cyber-Physical Industry course; however, it can be taught as a standalone module. The purpose of this module is to introduce students to an integrated perspective on security, safety, and risk that has quality management at its center.
Lesson C1: Security, Safety, Risk, & Quality Systems	This lesson describes the relationships between systems, standards, and guidance for security, safety, quality, and risk management. Commonly implemented standards from national and international standards organizations are introduced.
Lesson C2: Risks, Threats, and Vulnerabilities	This lesson introduces the concepts of risk, threats, vulnerabilities, and capabilities from the process perspective of industrial control systems.
Laboratory Exercise C2: Risk Analysis & Prioritization	This lab exercise introduces a quantitative approach to risk analysis using Failure Mode Effects Analysis (FMEA) and Risk Priority Number (RPN), and analytical methods for prioritization (ANOVA). It applies concepts learned during Lesson 3B in Module 3: Managing Security, Safety, and Risk of the Cyber-Physical Industry course.
Lesson C3: The NIST Cybersecurity Framework (CSF)	This lesson describes the NIST Cybersecurity Framework (NIST CSF), which provides risk-based guidance for cybersecurity management.
Laboratory Exercise C3: The NIST Cybersecurity Framework	This lab exercise addresses cybersecurity critical infrastructure and risk management by introducing the NIST Cybersecurity Framework (CSF) and how it is applied. It applies concepts learned during Lesson 3C in Module 3: Managing Security, Safety, and Risk of the Cyber-Physical Industry course.
Lesson C4: The Baldrige Cybersecurity Excellence Builder (BCEB)	This lesson describes the Baldrige Cybersecurity Excellence Builder (BCEB), which provides process-based guidance for assessment of cybersecurity risk management programs.

Laboratory Exercise C4: Baldrige Cybersecurity Excellence Builder (BCEB)	This lab introduces the student to the Baldrige Cybersecurity Excellence Builder (BCEB), a self-assessment tool to help organizations assess how effectively they are implementing the NIST Cybersecurity Framework (NIST CSF). It applies concepts learned during Lesson 3D in Module 3: Managing Security, Safety, and Risk of the Cyber-Physical Industry course. Even though it was designed to be compatible with the CSF, it can also be used for organizations that use other approaches to cybersecurity operations and risk management. This exercise will helps the student : Become familiar with the Criteria for Performance Excellence from the Malcolm Baldrige National Quality Awards (MBNQA) program Become familiar with the cybersecurity-related criteria that the BCEB adds to MBNQA, and how they are designed to work together Apply ADLI (Approach-Deployment-Learning-Integration) to BCEB process categories Apply LeTCI (Levels-Trends-Comparison-Integration) to BCEB results category
Lesson C5: The Cybersecurity Capability Maturity Models (*-C2M2)	This lesson explains how to use the Cybersecurity Capability Maturity Model (C2M2) family as a quick self-assessment tool. Although developed for critical infrastructure, it can be applied in any industry.
Lesson C6: Hazard Analysis	This lesson explains hazard analysis, a technique often employed in the process industries, to understand and mitigate process risk. Hazard analyses can provide critical input for cybersecurity risk management.
Laboratory Exercise C6: Hazard Analysis with PHA/What-If and HAZOP	This lab explores hazard analysis, a family of techniques often employed in the process industries to understand and mitigate process risk. It applies concepts learned during Lesson 3F in Module 3: Managing Security, Safety, and Risk of the Cyber-Physical Industry course.
Lesson C7: Supply Chain Disruption	This lesson explains the concept of supply chain risk management, which is used to increase resilience to supply chain disruption, and introduces an assessment tool for diagnosing supply chain vulnerabilities and capabilities.
Lesson C8: Quality Costs	This lesson introduces the concept of quality costs, which can be used to understand how resources are allocated, prioritizing activities, budgeting activities, and determining whether improvements have yielded a financial benefit.
Laboratory Exercise C8: Quality Costs	This lab exercise introduces the concept of quality costs and shows you how to analyze and interpret quality cost data for a hypothetical organization that uses the NIST Cybersecurity Framework for risk management, and has designed its cost accounting system around the structure of the Framework Core. It applies concepts learned during Lesson 3H in Module 3: Managing Security, Safety, and Risk of the Cyber-Physical Industry course.
Module D: Physical and Cognitive Ergonomics	This is the fourth and final module in the Cyber-Physical Industry course; however, it can be taught as a standalone module. The purpose of this module is to introduce students to physical and cognitive ergonomics (human factors), and explain why this discipline is so critical for cybersecurity management. The lessons relate musculoskeletal, metabolic, environmental, and cognitive aspects of performance to contextual risk. The lessons learned are applied to design for safe, secure, reliable Human-Machine Interfaces (HMIs) in industrial environments. Finally, common research methods used to determine whether improvements have or have not occurred as a result of training or other interventions are explained, with practical examples.
Lesson D1: The Relationship Between Ergonomics and Cybersecurity	This lesson explains why ergonomics (human factors) is critical for cybersecurity.
Lesson D2: Biomechanical Risks	This lesson explains potential physical stressors on operators working in an industrial environment where carrying and lifting objects is required, and how they can be managed and mitigated.
Lesson D3: Metabolic and Environmental Risks	This lesson explains potential physical risks for operators working in an extreme industrial environment where exertion may be required, and how those risks can be managed and mitigated.
Lesson D4: Cognitive Risks	This lesson provides tools and heuristics based on principles in cognitive science that can be used to design and improve Human-Machine Interfaces (HMIs) for ease of use.
Laboratory Exercise D4: Hicks Law and the Nature of Choice	This lab exercise explores the Hicks-Hyman Law (sometimes referred to as simply Hicks Law). It applies concepts learned during Lesson 4D in Module 4: Physical and Cognitive Ergonomics of the Cyber-Physical Industry course.
Laboratory Exercise D4: Fitts Law	This lab exercise explores Fitts Law, which states that response time will be the smallest when the distance to a target is small, and the size of the target is large. It applies concepts learned during Lessons 4D/4G in Module 4: Physical and Cognitive Ergonomics of the Cyber-Physical Industry course.
Lesson D5: Characterizing the Context: Learning and Situation Awareness	This lesson provides tools and constructs for operators so that they can quickly make the best decisions – especially in dangerous circumstances.
Lesson D6: Designing Safe & Secure HMIs	This lesson provides up-to-date guidance on how to design HMIs that are safe, secure, reliable, and effective.
Laboratory Exercise D6: Designing Safe & Secure HMIs	In this exercise, students use Situation Awareness (SA), Gestalt Principles, design affordances, and CIA-for-HMI to design the Human-Machine Interface (HMI) for a cyber-physical system (one that will brew and serve pots of coffee). It applies concepts learned during Lessons 4E/4F in Module 4: Physical and Cognitive Ergonomics of the Cyber-Physical Industry course.
Lesson D7: Research Methods in Ergonomics	This lesson illustrates the most common parametric and nonparametric statistical tests used to determine whether interventions improve human factors and HMI issues in production systems environments.
	COURSE: Introduction to Cybersecurity for High School Students and K12 Educators

Introduction to Cybersecurity for High School Students and K12 Educators	The goal of this course is to provide high school students and educators an introduction to the technological aspects of cyber security with hands on practice. This foundational course covers the following category of topics: legal and ethical issues; foundational knowledge required for cybersecurity and for hands on practice including: using the Linux command line, basics of computer networking and basics of web technology; steps in hacking including reconnaissance and exploits; cryptography; secure design of systems, and hardening operating systems. For educators, the course includes a topic on resources available to help teach cybersecurity. The course consists of five modules: Module A: Teaching Cybersecurity Module B: Cyber Ethics and Law Module C: Foundations of Cybersecurity Module D: Anatomy of an Attack Module E: Cyber Defense and Cryptography
Module A: Teaching Cybersecurity	This is the first module in the Introduction to Cybersecurity for High School Students and K12 Educators course. It addresses the following: Strategies to motivate middle/high school students to take the course. Disclaimers and agreements that students and their legal guardians must agree to before taking the course. Commonwealth of Virginia state recommended syllabi for high schools and competencies. Standard certification exams that high school students can apply for. The topics covered in a foundational course including a wide array of pre-requisite knowledge to learn cybersecurity: using Linux and windows command line, basic networking concepts, mathematics for cryptography, and the backbone of the Internet: HTML and client-side scripting. Textbooks available to incorporate into a classroom. Type of labs and tools available for teachers. At the end of this module, teachers will have a basic understanding on what is involved to get started in teaching cybersecurity. They will also have knowledge on what topics a fundamental security course will cover.
Lesson A1: Creating Cyber Awareness: Strategies to Motivate Students	The purpose of this lesson is to provide instructors with a brief set of tools they can use to motivate students about the need to study cybersecurity. The lesson is purposefully short to ensure students remain attentive.
Lesson A2: Foundational Cybersecurity Curriculum: Overview	The purpose of this lesson is to provide instructors with a basic idea of what topics are covered in a foundational cybersecurity course. There are several syllabi for a foundational course. K12 educators are urged to read two such resource: Commonwealth of Virginia Department of Education's Pathway to Cybersecurity careers and CompTIA Security+ certification syllabus.
Module B: Cyber Ethics and Law	This is the second module in the Introduction to Cybersecurity for High School Students and K12 Educators course. It addresses the following: Laws including copyright laws with respect to cyber Ethical issues At the end of this module, participants will have a basic understanding of copyright laws and ethical issues facing them in cyber.
Lesson B1: Cyber Ethics	This lesson introduces the student to the concept of cyber ethics. This introduction includes the ACM Code of Ethics as well as other professional ethical codes of conduct.
Lesson B2: Copyright and Fair Use	The purpose of this lesson is to provide a first introduction to the concept of Intellectual Property through a discussion of Copyright. The discussion includes the Fair Use exceptions to Copyright.
Lesson B3: Cyber Law	The purpose of this lesson is to provide a very basic introduction to Cyber Law while at the same time expanding the introduction to Intellectual Property.
Lesson B4: Responsibility and Cyber Decision Making	The purpose of this lesson is to introduce the concept of levels of responsibility (i.e. role, causal, blameworthy, liability) and then apply those concepts to some example scenarios.
Module C: Foundations of Cybersecurity	Cybersecurity requires foundational knowledge from a wide array of topics including: mathematics, coding, networking, web-technologies, operating systems and complex software applications such as database management systems. Clearly, an introductory course cannot cover all these topics. The goal of this third module in the Introduction to Cybersecurity for High School Students and K12 Educators course is more modest: it focuses on the key technologies that form the backbone of both the Internet and the computing infrastructures in most organizations: computer networking and web-technologies (e.g., HTML, client side scripts). Knowledge in this area will help students get hands-on experience in cybersecurity appropriate for an introductory course. When it comes to hands-on exercises, Linux is the de-facto OS platform for educators and cybersecurity experts alike. This is primarily because many open source tools in cybersecurity are available on Linux platforms. Teachers can create hands on lab exercises on a shoe-string budget using these tools. Hence, this module starts with a lesson that introduces the Linux command line, followed by a tour of the Kali Linux OS distribution – a Linux distribution that is packaged with more tools than most experts can handle! The last two lessons cover the basics of networking and web-technologies.
Lesson C1: Using the Linux Command Line	Linux is the de-facto operating system (OS) standard in cybersecurity mainly because of the availability of many open-source tools. Learning how to use the Linux command line is a skill that will help students perform different hands-on experiments in cybersecurity including: vulnerability assessments, penetration tests, and apply cyber-defense techniques. This skill will also reduce the learning curve in using other such command line tools including Windows Powershell™. By learning how to use Linux, educators can develop hands on labs that use open-source software tools on shoe-string budgets. This lesson will introduce the Linux command line to accomplish various tasks including: traversing the Linux directory structure, searching for specific data within file names or file content, and recording and parsing results.
Lesson C2: Setting up a Kali Linux Lab	This lesson plan is primarily designed for students who are educators and wish to setup their own security lab. Students will get a quick tour on how to setup a basic security lab. Students will also get a tour of Kali Linux OS distribution that has several tools that educators can use to create new projects.
Lesson C3: Basics of Computer Networking	This lesson covers the basics of networking required in later modules to perform reconnaissance, understand network-based exploits and understand concepts of network defense.
Lesson C4: Basics of the Web: HTML & Javascript	In this lesson, students gain a rudimentary understanding of how websites work and the difference between HTML and dynamic HTML with the use of client-side scripts.

Module D: Anatomy of an Attack	In this fourth module of the Introduction to Cybersecurity for High School Students and K12 Educators course, the lessons will describe the steps an attacker would take when attacking a computing infrastructure. The module covers the first 2 steps in the 4-step process including: reconnaissance and exploits. Students will work on the Kali Linux box associated with the course in the [[organization.name]].
Lesson D1: Reconnaissance	Studying hacking is an important aspect of cybersecurity. It helps security experts measure how vulnerable their computer networks are and the effectiveness of their defensive techniques. In this lesson, we will enumerate the four steps that form the anatomy of an attack. Next, we will start digging deeper by discussing the first step of a hack: reconnaissance.
Lesson D2: Exploits	In this lesson, we will survey technological exploits including buffer overflows, cross site scripting and SQL Injection. Students will get hands on experience with an assessment involving a social media site seeded with vulnerabilities.
Module E: Cyber Defense and Cryptography	This is the fifth and final module in the Introduction to Cybersecurity for High School Students and K12 Educators course and it has as four lessons. The first is a short lesson on the key categories of cyber defense and aspects of technological defense. The second lesson introduces the types of cryptography and their application. The third lesson is on secure design and coding standards and can be used by instructors in classes where students understand basic programming concepts. The fourth and final lesson focusses on hardening operating systems, especially Linux-based systems. For Windows-based systems, this fourth lesson directs instructors to follow the curriculum of the Air Force Association's CYBERPATRIOT competition.
Lesson E1: Securing Computing Infrastructure	This lesson is short, but lays the foundation for the rest of the lessons and modules. It introduces the three categories of cyber defense and enumerates key technological defense techniques.
Lesson E2: Cryptography	This lesson covers the theory behind three types of cryptography: symmetric key (or secret-key), public-key and secure hash functions. The purpose of these three types is also discussed. Students will learn that cryptography is a crucial component in securing data for confidentiality and integrity.
Lesson E3: Secure Design and Coding	Secure design principles provide guidance on how to secure computer networks and software applications against attacks and when attacked, how to limit the damage caused by the attacks. This lesson discusses key secure design principles. The lesson also covers secure coding techniques to develop applications that are resilient to attacks.
Lesson E4: Hardening Operating Systems	In this lesson students, will apply secure design principles to harden operating systems. The lesson can be used as a lead-in to the Air Force Association's CYBERPATRIOT training material.
	COURSE: Introduction to Hands-On Cybersecurity Attack and Defense
Introduction to Hands-On Cybersecurity Attack and Defense	This course aims to provide a hands-on perspective of common cybersecurity attacks, explain their mechanisms so that students can learn how to mitigate their impacts, discuss why these attacks pose constant threats to netizens, and introduce tools, techniques, and processes used to put us in a better position in the battle against cyber crimes. Computer crime is an area of study that is rapidly growing in today's socio-technical environment. Both profit and non-profit organizations have increasingly emphasized the importance and visibility of cybersecurity. With the easy access and use of malicious computing tools, people can commit crimes with and against computers. There is a growing need for a future IT workforce to be equipped with the skills to investigate and respond to these threats. Hence, this course will introduce the topics of cybersecurity attacks and defense. Students will be exposed to different aspects of malicious software, system intrusions, and ways in which to detect and protect digital assets. The course content is dedicated to explain and showcase popular cybersecurity practices and concepts. Real world examples and hands-on labs will assist the students in learning about the malicious tools and techniques commonly used by hackers to exploit a victim system. Having a good understanding of these tools and techniques allows students to design and develop coping strategies as well as actionable plans to safeguard the computer information systems they are defending. There are three modules in this course: Module A: Introduction to Cybersecurity Concepts and Practices Module B: Cybersecurity Threats & Attacks Module C: Managing Cybersecurity Defense
Module A: Introduction to Cybersecurity Concepts and Practices	This is the first module in the Introduction to Hands-On Cybersecurity Attack and Defense course and it focuses on cybersecurity concepts and principles. It lays the knowledge foundation for students who don't have much experience in the subject matter. It aims to provide an overview of major factors that have distinct impacts on cybersecurity, including software, hardware, network, and people. As a high-level introduction, this module prepares students for hands-on work that illustrates the applications of malicious software and techniques (e.g., Keylogger), as well as defense (e.g., encryption).
Lesson A1: A Quick View of Cybersecurity Trends	This lesson aims to provide an overview of the current trending challenges, crimes, and technologies related to cybersecurity. Students will learn basic security concepts, issues and terms that help them better understand the course materials later.
Lesson A2: General Cybersecurity Concepts	This lesson focuses on the foundational knowledge of cybersecurity concepts, principles, and models. Some of the topics are technical while others are operational or managerial.
Lesson A3: Operational and Organizational Cybersecurity	This lesson covers basic aspects of physical concerns and environmental issues related to cybersecurity.
Lesson A4: The Role of People	This lesson discusses the role of people in cybersecurity.
Lesson A5: Hiding Information and Cybersecurity	This lesson discusses the concept of encryption in the context of cybersecurity, including Public Key Infrastructure (PKI), which is one of the most important building blocks of online transaction providing nonrepudiation, confidentiality, privacy, integrity/consistency, and authentication.
Lesson A6: Network Fundamentals and Cybersecurity	This lesson focuses on the technologies, processes, and methods of transmitting data (0s and 1s) across the network. Learning how networks operate is a critical prerequisite to understand cybersecurity issues.

Module B: Cybersecurity Threats & Attacks	This is the second module in the Introduction to Hands-On Cybersecurity Attack and Defense course and it focuses on various types of cyber attacks. Students will be exposed to the forms, mechanisms, and characteristics of some of the most frequently seen online threats. The module also discusses common techniques used by intruders who go after personal and business data that are private and confidential. This module can be used as a standalone unit. There are four hands-on labs in this module to engage students with malicious computer programs, which provide them with unique experience of understanding the process of initiating cyber attacks.
Lesson B1: An Overview of Cyber Attacks I	This lesson aims to provide an overview of cyber-attack instances and their mechanisms. Students will obtain a basic understanding of how these attacks take place in a real-world perspective. The learning outcomes of this lesson directly feed into the next lesson – An Overview of Cyber-Attacks II.
Lesson B2: An Overview of Cyber Attacks II	This lesson is an extension of lesson 2A - An Overview of Cyber Attacks I. It focuses on some of the most popular online threat instances, and provides an in-depth view in terms of how they work and respond strategies. The hands-on lab allows students to simulate a DDoS attack.
Lesson B3: Malicious Websites	This lesson discusses a common online threat – malicious websites as well as their variants. An in-depth view in terms of their characteristics and coping strategies are provided, followed by the methods and tools used to identify suspicious websites. A hands-on lab is provided for students who can create a malicious website using SET.
Lesson B4: Malware Analysis	In this lesson, the student learns about the nature of malware in terms of its properties, methods/tools of analysis, and responding strategies. The students will also learn how to place a malware file in the victim's computer using a hands-on lab exercise, allowing them to walk through multiple procedures including earning victim's trust, tricking the victim to activate the payload, and establish a backward connection.
Lesson B5: OSINT	This lesson focuses on a well-known social engineering technique – Open Source Intelligence, which aims to gather information on a target for future exploitation. This public information gathering approach has been constantly used by some of the most significant and successful hacking endeavors, including international cyber espionage.
Module C: Managing Cybersecurity Defense	This is the third module in the Introduction to Hands-On Cybersecurity Attack and Defense course and it presents several defending concepts and practices of cybersecurity. Students will be exposed to the forms, mechanisms, and characteristics of host-level and network-based defense techniques. The module also discusses some common tools used by cybersecurity professionals responding to threat incidents and attempting to recover from cyber intrusions. This module can be used as the standalone unit. There are four hands-on labs in this module to engage students with defending techniques.
Lesson C1: System Hardening	This lesson focuses on hardening exercises that help us to enhance security protection at the host and network levels. Discussion includes hardening options, the pros and cons, and various tools used for hardening purposes. Two labs are provided to engage students with hands-on experience.
Lesson C2: Web Application Security	This lesson provides an introduction to two popular attacks aimed at vulnerable web application servers (i.e. XSS and SQL Injection). Examples are provided to present an insider look of how these attacks function. It is important to raise the awareness of web app vulnerabilities as our society is increasingly relying on IoT, Cloud computing, and Big Data.
Lesson C3: Pretty Good Privacy (PGP) & Steganography	This lesson provides an introduction to two popular encryption applications: PGP and Steganography. Students gain hands-on experience of using these tools in labs. The importance of encrypted data/information transmission is covered. In addition to data privacy, other important characteristics of secured data transmission are also discussed (e.g., nonrepudiation, authentication, and so forth).
Lesson C4: Vulnerability Assessment & Host Forensics	This lesson covers two important topics in managing cybersecurity defense: Vulnerability Assessment and Host-based Forensics. Processes and approaches are discussed pertaining to host-level forensics and general vulnerability assessment. These approaches are also compared and contrasted in terms of their advantages and disadvantages. In the end, the students should gain a good grasp of how to conduct an entry-level forensic investigation.
Lesson C5: Recovering from a Hack	This lesson discusses the overall steps (five) cybersecurity professionals follow to recover from actual hacks. These steps can be carried out to respond to various levels of attacks. It also covers common approaches assessing the scale of a hack and some of the tools needed.
	COURSE: Cyber Intelligence: Analyzing Cyber Adversaries and Threats
Cyber Intelligence: Analyzing Cyber Adversaries and Threats	Cyber intelligence is the collection and analysis of information about cyber adversaries' (also known as hackers, cyber threat actors) motivations, capabilities, geopolitical aspirations and activities in the cyber and physical domains to support decision making about cyber security. Students use analytical methodologies, risk assessment models, and cyber security frameworks to develop common vocabulary to support technical and managerial discussions about cyber threats. Using cyber intelligence tools and methodologies such as the intelligence cycle and cyber kill chain, students assess an organization's internal and external environments to generate cyber threats matrix, harvest open source information about adversaries, analyze diverse data and conduct basic technical as well as strategic analyses of cyber threats and adversaries. Using the results of the analysis, students write analytical reports and present briefings for management. The course focuses on organizations' cyber threats and cyber adversaries. This course is organized around the intelligence cycle which is a planning process based on requirements, information gathering, analysis, and generation of finished intelligence product (i.e., briefing, alert, report). The intelligence cycle has been adapted to cyber security. The course is broken into the following modules which reflect a logical process for introducing cyber intelligence to assessing cyber security threats to organizations and their cyber adversaries: Module A: Overview of Cyber Threats Module B: Introduction to Cyber Intelligence Module C: Intelligence Cycle and Cyber Intelligence Module D: Cyber Threat Intelligence Cycle (CTIC): Intel Requirement, Environment, & Collection Module E: Cyber Threat Intelligence Cycle (CTIC): Processing & Analysis Module F: Cyber Threat Intelligence Cycle (CTIC): Production & Dissemination
Module A: Overview of Cyber Threats	This is the first module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to trends and challenges in cyber threats. The material is approached from the perspective of what are examples of cyber threats, how are they impacting on cyber security and how are we responding. This module provides a high-level introduction to cyber intelligence to prepare students for opportunities as cyber analysts and/or cyber intelligence specialists in industry and government.

Lesson A1: Overview of Cyber Threats	This lesson covers summary of current state of cyber security, trends, and challenges in cyber threats. It provides examples of common cyber threats, associated threat trends, and impact.
Lesson A2: Introduction to Protecting the Networks	This lesson provides a high-level introduction to protecting computer networks such as the ones at work and/or at home. It highlights different ways to protect networks (e.g., firewall, password, cyber security awareness training). It introduces a Defense-in-Depth (DID) approach that utilizes multi-layered network defense techniques.
Module B: Introduction to Cyber Intelligence	This is the second module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to the emerging discipline of cyber intelligence. The material is approached from the perspective of what are examples of sophisticated cyber threats and how are they driving businesses to consider an intelligence-driven approach to cyber security called cyber intelligence. This module provides a high-level introduction to cyber intelligence and adversaries to make students aware of opportunities as cyber analysts in industry and government.
Lesson B1: Cyber Intelligence	This lesson provides a high-level introduction to the emerging intelligence-driven discipline called cyber intelligence. Cyber intelligence is the collection analysis of information to identify, track, and predict cyber adversaries (e.g., hackers) capabilities, intentions, and activities that can be used to inform decision making.[1] Cyber intelligence focuses on holistic and analytic aspects of cyber threats while cyber security focuses on technical aspects. [1] Cyber Intelligence Tradecraft Project. Software Engineering Institute (SEI), CMU, 2013. https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf
Lesson B2: Introduction to Cyber Adversaries	In cyber intelligence, the emphasis is on understanding the adversary. This lesson provides a high-level introduction to types of cyber adversaries and their motivations. It introduces the concept of advanced persistent threat (APT) which is a highly focused attack using advanced techniques and methods. Techniques and methods are called tradecraft.
Module C: Intelligence Cycle and Cyber Intelligence	This is the third module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to the emerging discipline of cyber intelligence that uses the intelligence cycle to conduct analysis and support decision making. The material is approached from the perspective of the intelligence cycle as a planning process for asking questions, gathering data/information, analysis, and dissemination. In some ways, the intelligence cycle is similar to the research process and the scientific method of inquiry. In reference to cyber threats, some of the major questions are who are the cyber adversaries who may want to attack your organization, what are their motivations, what are their capabilities such as tactics, techniques, and procedures (TTPs), and what may they do next? This module provides a high-level introduction to a process called the intelligence cycle. Intelligence cycle is used by different intelligence organizations such as CIA (US), MI6 (UK), and ASIS (Australia). It is a planning process for generating intelligence to support making decisions about how to protect the countries. Although the intelligence cycle is used to answer questions about threats associated with intelligence organizations, law enforcement, military, and industry, now it is being adapted to cyber security threats. Exploring the intelligence cycle to analyze questions about cyber threats and adversaries prepares students for opportunities as cyber analysts and/or cyber intelligence specialists in industry, academic, and government.
Lesson C1: Intelligence Cycle (Planning Process for Knowledge Acquisition)	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the intelligence cycle (planning process for knowledge acquisition). The lesson is approached from the perspective of the intelligence cycle as a planning process for asking questions, gathering data/information, analysis, and dissemination. In some ways, the intelligence cycle is similar to the research process and the scientific method of inquiry. In reference to cyber threats, the intelligence cycle is being used to analyze threats and cyber adversaries. The intelligence cycle is being applied to cyber threats in order to find answers to the following questions: Who are the cyber adversaries who may want to attack your organization; what are their motivations; what are their capabilities such as tactics, techniques, and procedures (TTPs); and, what may they do next?
Lesson C2: Usage of Intelligence Cycle	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence (intel) that uses the intel cycle (planning process for knowledge acquisition). The lesson is approached from the perspective of the intel cycle as a planning process for asking questions, gathering data, analysis, and dissemination. The intel cycle is used in many areas such as the intelligence organizations (e.g., FBI), industry (TMZ Celebrity Gossip), military (e.g., US Army Command), and law enforcement (NYC Police Department). This lesson introduces the concept that the intel cycle is being applied to cyber security industry to identify and analyze threat trends and adversaries' motivations, tactics, and intentions.
Module D: Cyber Threat Intelligence Cycle (CTIC): Intel Requirement, Environment, & Collection	This is the fourth module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to an emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC) to analyze threats and cyber adversaries to support decision making. The material is approached from the perspective of CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. In reference to cyber threats, some of the major questions are: Who are the cyber adversaries who may want to attack your organization? What are their motivations? What are their capabilities such as tactics, techniques, and procedures (TTPs), and what may they do next? This module provides a high-level introduction to a process called the CTIC. It is a planning process for generating threat intelligence to support making decisions about cyber threats and adversaries. Exploring the CTIC to analyze questions about cyber threats and adversaries prepares students for opportunities as cyber analysts and/or cyber intelligence specialists in industry, academic, and government
Lesson D1: CTIC: Intel Requirement	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Its first step is intelligence requirements.
Lesson D2: CTIC: Environment	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Its second step is environment which includes the internal (e.g., looking inward such as in the organization) and external (e.g., geopolitical issue).
Lesson D3: CTIC: Collection	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence (intel) that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Its third step is collection which includes data identification, searching, and collecting information to provide insight on environment and intel requirement.
Module E: Cyber Threat Intelligence Cycle (CTIC): Processing & Analysis	This is the fifth module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC) to analyze threats and cyber adversaries to support decision making. The material is approached from the perspective of CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. In reference to fourth step, some questions are how is cyber threat data and information processed? What is meant by blacklisted IP addresses? What services are provided in a commercial threat intelligence platform? How can threat intelligence be used to identify cyber adversaries and their capabilities? How does one use the Diamond Model and cyber kill chain methodologies? This module provides a high-level introduction to CTIC and its fourth step (processing and analysis). It is a planning process for generating threat intelligence to support making decisions about cyber threats and adversaries. Exploring the CTIC to analyze questions about cyber threats and adversaries prepares students for opportunities as cyber analysts and/or cyber intelligence specialists in industry, academic, and government.
Lesson E1: CTIC: Processing	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Although its fourth step is Processing & Analysis, this lesson focuses on processing.
Lesson E2: CTIC: Analysis	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Although its fourth step is Processing & Analysis, this lesson focuses on analysis.

Lesson E3: CTIC: Analysis (cont)	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. Although its fourth step is Processing & Analysis, this lesson describes analysis.
Module F: Cyber Threat Intelligence Cycle (CTIC): Production & Dissemination	This is the sixth module in the Cyber Intelligence: Analyzing Cyber Adversaries and Threats course. The purpose of this module is to introduce students to the emerging discipline of cyber intelligence that uses the Cyber Threat Intelligence Cycle (CTIC) to analyze threats and cyber adversaries to support decision making. The material is approached from the perspective of CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. In reference to the fifth step, some questions are what is the production and dissemination of cyber threat intelligence? What is meant by cyber threat intelligence consumer? What is the difference between a SIEM and SOC? What is attribution? This module provides a high-level introduction to CTIC and its fifth step. It is a planning process for generating threat intelligence to support making decisions about cyber threats and adversaries. Exploring the CTIC to analyze questions about cyber threats and adversaries prepares students for opportunities as cyber analysts and/or cyber intelligence specialists in industry, academic, and government.
Lesson F1: CTIC: Production and Dissemination	This lesson provides a high-level introduction to the emerging discipline of cyber intelligence (intel) that uses the Cyber Threat Intelligence Cycle (CTIC). The lesson is approached from the perspective of the CTIC as an intel-driven planning process for asking questions, gathering data/information, analysis, and dissemination. CTIC is an adaptation of the intelligence cycle which has been applied to cyber threat. The lesson focuses on production and dissemination which is the fifth step in CTIC.
	MODULE: Introduction to Digital Forensics
Module: Introduction to Digital Forensics	This module on digital forensics will familiarize you with forensics terminology and approaches, along with hands-on experience with a variety of forensic tools used by investigators to conduct incident response, find evidence of criminal behavior, and examine the effects of malware infection. The module will focus on Windows forensics and will use a Linux-based forensic workstation for hands-on analysis. Tools for conducting forensic examinations using a Windows system will also be introduced. You should leave this workshop with a good understanding of the tools and techniques used to conduct forensic examinations of digital systems.
Lesson 1: Introduction to Digital Forensics	This lesson provides an introduction and overview of digital forensics. We will explore some of the tools and software that can be used to conduct forensic investigations and introduce various computer forensics topics such as filesystem and browser forensics, Windows Registry forensics, log analysis, memory forensics, and network forensics. We also explore a methodology for digital forensics analysis, various types of forensic artifacts, and important legal considerations on this topic.
Lesson 2: Windows Filesystem and Browser Forensics	This lesson provides an overview of the Windows filesystem and relevant forensic artifacts. It includes coverage of tools and techniques for browser, recycle bin, app, and LNK file forensics, as well as specific pieces of information that might be discovered during an analysis of these file system elements.
Laboratory Exercise 2A: Browser Forensics and Recycle Bin Analysis	This exercise provides hands-on experience applying concepts learned during Lesson 2: Windows Filesystem and Browser Forensics in the Digital Forensics Module. Students will use tools on the SANS SIFT Workstation Linux distribution to examine partial Windows file system images and find browser and recycle bin artifacts.
Lesson 3: Windows Registry Forensics	This lesson delves into the Windows Registry and those features that can be relevant to a forensic investigation.
Laboratory Exercise 3A: Windows Registry Forensics Analysis	This exercise provides hands-on experience applying concepts learned during Lesson 3: Windows Registry Forensics in the Digital Forensics Module. Students will use tools on the SANS SIFT Workstation Linux distribution to examine Windows Registry artifacts from a partial file system image.
Lesson 4: Memory Forensics	In this lesson, we explore memory forensics and how related artifacts can assist in digital forensic analysis. We will learn tools for capturing memory images on live systems and virtual machines and get hands-on experience analyzing memory images.
Laboratory Exercise 4A: Memory Forensics Analysis	This exercise provides hands-on experience applying concepts learned during Lesson 4: Memory Forensics in the Digital Forensics Module. Students will use tools on the SANS SIFT Workstation Linux distribution to examine a Windows memory image for various forensic artifacts.
Lesson 5: Windows Logs and Log Analysis	In this lesson we explore Windows log formats and learn tools and techniques for log file analysis.
Lesson 6: Network Forensics	Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Network forensics is a relative new field of forensic analysis. In this lesson, we will introduce the concept of network forensics and explore tools and techniques used for this purpose.
Laboratory Exercise 6A: Network Forensics	This exercise provides hands-on experience applying concepts learned during Lesson 6: Network Forensics in the Introduction to Digital Forensics Module. Students will use tools on the SANS SIFT Workstation Linux distribution to examine packet capture files for forensics evidence.
	COURSE: Cyber Security Advanced Ethical Hacking
Cyber Security Advanced Ethical Hacking	

Module A: Introduction to Ethical Hacking	This module covers an introduction to Ethical Hacking and an overview of the course. This is a third-year advanced high school course. Students should have at least one cybersecurity class, knowledge of networks, and basic computer science skills before taking this course. The module covers attack phases, threats, attack vectors, penetration testing tools, laws/ethics, and the basics of using the Cyber Range. NOTE: This is the first of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking; this module. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson A1: Introduction to Ethical Hacking	In this lesson, students will learn about Ethical Hacking and related certifications. It is designed to be an introduction to Ethical Hacking course, covering prerequisites, course expectations, a brief network recap, and Ethical Hacking as a career. In the lesson, students will research careers in Ethical Hacking using online resources.
Lesson A2: Attack Phases, Threats, and Attack Vectors	For this lesson, students will examine the latest news in cybersecurity by examining the newest exploits, reading white papers, and looking for security podcasts.
Lesson A3: Overview of Penetration Testing	In this lesson, students will learn about the basics of penetration testing. In the lab exercise, students will use the Cyber Range to review Nmap scanning with an emphasis on penetration methodology and simple reporting.
Lesson A4: Laws and Ethics	In this lesson, students will learn about the laws and ethics of hacking. Students will examine EC-Councils Code of Ethics, watch videos about cybersecurity issues, and read articles in which they will examine and respond to ethical issues in cybersecurity.
Lesson A5: Getting to know the Cyber Range	For this lesson, students will learn how to use the Cyber Range. A Kali Linux virtual machine (VM) will be used to complete basic tasks so that students become acclimated to the environment. Topics covered are how to login to the course, change the terminal settings, use the man tool, and how to separate programs from the terminal. This is largely a review for experienced Cyber Range users.
Module B: Reconnaissance	This module covers the first stage of an attack. Reconnaissance is the stage where an attacker will gather as much information as possible about their target before they exploit a system. Much of the module will cover OSINT or open source intelligence. Topics include passive and active footprinting, competitive intelligence gathering, whois/rdap lookups, website cloning, and email tracking and harvesting. NOTE: This is the second of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance; this module. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson B1: Passive and Active Footprinting	In this lesson, students will learn about the first phase of an attack: reconnaissance. The lesson walks the student through the basics of passive and active footprinting. Students will also complete passive footprinting tasks in a hands-on lab. NOTE: For this lesson, we will use the Cyber Range: Cyber Basics (2020.12) Kali Linux environment to perform passive footprinting on a target.
Lesson B2: Competitive Intelligence	In this lesson, students will use the Cyber Range Kali Linux environment to perform passive competitive intelligence on a target using web services.
Lesson B3: Whois/RDAP Lookup	In this lesson, students will use the Cyber Range Kali Linux environment to perform a WHOIS lookup on a target.
Lesson B4: Website Cloning	In this lesson, students will learn how to clone a website with wget and HTTrack using the Cyber Range Kali Linux environment. Students will inspect the elements of a webpage, locate submission boxes in HTML code, and reveal saved passwords in submission boxes.
Lesson B5: Email Tracking and Harvesting	In this lesson, students will learn how to track email locations by examining email headers, and harvest emails using the Kali Linux and Windows environments.

Module C: Scanning and Enumeration	This module covers phase two of an attack. Scanning and enumeration is the phase where the attacker begins to “touch” the systems. Attackers will scan networks to discover live hosts and open port. They will then enumerate the live hosts and ports to discover services, machine names, and other network resources. In this module, students will complete the scanning and enumeration phase using hands-on labs using the Cyber Range. Topics include: advanced port scanning, scanning and enumeration, vulnerability scanning, advanced enumeration, and subnet scanning. NOTE: This is the third of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration; this module. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson C1: Extra Advanced Port Scanning	In this lesson, students will learn about the second phase of an attack: scanning and enumeration. The lesson walks the student through advanced port scanning with nmap and Metasploit. NOTE: For this lesson, we will use the Cyber Range Kali Linux with Metasploitable (2018) environment.
Lesson C2: Scanning and Enumeration	In this lesson, students will learn about the second phase of an attack: scanning and enumeration. The lesson walks the student through advanced scanning with Netcat, Nmap, cURL, Wget, and Netstat. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux with Metasploitable (2020.09) environment.
Lesson C3: Vulnerability Scanning	In this lesson, students will learn about the second phase of an attack: scanning and enumeration. The lesson walks the student through vulnerability scanning with Nessus, Metasploit, and Nikto. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux with Metasploitable (2020.09) environment.
Lesson C4: Advanced Enumeration	In this lesson, students will learn more advanced scanning and enumeration. The lesson walks the student through several enumeration techniques using Kali Linux. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux with Metasploitable (2020.09) environment.
Lesson C5: Subnet Scanning	In this lesson, students will complete a subnet scan using Masscan. During the scan Wireshark will be used for packet analysis and Htop will be used to monitor PC performance. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux with Metasploitable (2020.09) environment.
Module D: Sniffing, IDS, and Firewall Evasion	This module covers sniffing protocols, TCPDump, Wireshark, IDS evasion techniques, spoofing, and packet creation. Sniffing and IDS/firewall evasion will usually occur during the first three phases of an attack. In the recon phase, sniffing a web app/site can provide information that is useful in an attack. In the scanning and enumeration phase, evading IDS and spoofing are commonly used techniques. During phase 3, sniffing can be used to obtain credentials or discover other misconfigurations that allow unauthorized access to devices. NOTE: This is the fourth of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module 1 is titled Introduction to Ethical Hacking. Module 2 is titled Reconnaissance. Module 3 is titled Scanning and Enumeration. Module 4 is titled Sniffing, IDS, and Firewall Evasion; this module. Module 5 is titled System Hacking. Module 6 is titled Web Apps and Data Servers. Module 7 is titled Web Apps and Data Servers Part 2. Module 8 is titled Natas. Module 9 is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson D1: Sniffing and Evasion Tools	In this lesson, students will learn how to sniff networks and analyze domains for security flaws. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux environment with Metasploitable (2020.09).
Lesson D2: TCPDump and Wireshark	In this lesson, students will learn how to use TCPDump and Wireshark to capture, read, and filter packets. NOTE: For this lesson, we will use the Cyber Range’s Kali Linux with Metasploitable (2020.09) environment.
Lesson D3: Evading Detection Systems	For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2020.09) environment to evade detection systems using Nmap and Metasploit.
Lesson D4: IP and MAC Spoofing	For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2020.09) and the Kali Linux and Vulnerable Windows 7(64bit) VMs (2020.09) environments to spoof IP and MAC addresses.
Lesson D5: Packet Creation and Netcat	For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2020.09) and the Kali and Vulnerable Windows7(64bit) VMs (2020.09) environments to create custom packets with Scapy and a reverse shell in Netcat/Ncat.

Module E: System Hacking	This module covers the creation of internal network attacks, cracking authentications, hiding backdoors in applications, performing denial of services attacks, and customizing the bash terminal. Students will learn how to analyze data collected in the first two phases to gain access to a system. The fourth phase of an attack will be covered as well. Students will learn how to maintain persistent access once a system is compromised (post exploitation). In lesson four, students will be challenged to complete tasks where knowledge of previously learned material will be necessary; gaps will be left intentionally in the instructions. In the final lesson, students will modify the bash terminal for the customization of ethical hacking tools. NOTE: This is the fifth of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking; this module. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson E1: Creating Attacks with Metasploit	For this lesson, students will use the Cyber Range: Kali Linux and Vulnerable Windows 7(64bit) VMs (2020.09) environment to create and deploy exploits. They will simulate a web application file upload attack by creating a simple webserver to upload the exploit. Once the Window VM has a meterpreter session, students will escalate privileges using Metasploit's local exploits. They will then sniff traffic, dump hashes, and place a keylogger.
Lesson E2: Cracking Authentications	For this lesson, students will use the Cyber Range: Kali Linux and Vulnerable Windows 7(64bit) VMs (2020.09) environment to crack authentications using Hydra, Hashcat, John the Ripper and online tools. Students will be immersed in the addictive cryptographic cracking arena that is essential to becoming an ethical hacker.
Lesson E3: Wrapping Backdoors into Applications	For this lesson, students will use the Cyber Range: Kali Linux and Vulnerable Windows 7(64bit) VMs (2020.09) environments to create a backdoor and wrap it in another application. In addition, students will learn the techniques used by social engineers to get payloads deployed onto a victim's computer.
Lesson E4: Denial of Service Attacks	In this lesson, students will learn about DoS attacks, their creation and their mitigation. Additionally, students will use the Cyber Range: Kali Linux and Vulnerable Windows 7(64bit) VMs (2020.09) environment to create a denial-of-service (DoS) attack against the remote desktop protocol.
Lesson E5: Customizing Tools	This lesson focuses on the customization of the Bash terminal where many hacking tools will be accessed. By learning how to set up and modify specific Bash files, students will be able to customize their command line tools, which increases the efficiency needed in order to complete tasks in a timely manner. Additionally, students will use the Cyber Range: Cyber Basics (2020.12) to customize the Bash terminal and set up the system to quickly modify and create aliases in a hands-on exercise.
Module F: Web Apps and Data Servers	This module covers the basics of web application security testing. Students will learn how to install and configure several web application tools, and how to install a web application into a Docker container. In the last lesson of this module students will learn about the basics of cross site scripting and its impact on organizations that are vulnerable. The goal of this module is to have students understand how to manually examine and modify HTTP requests and responses to discover vulnerabilities. NOTE: This is the sixth of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers; this module. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson F1: Web App Recon Tools	In this lesson, students will learn about the tools available to complete web application reconnaissance. Additionally, students will use the Cyber Range: Cyber Basics (2020.12) environment to install several tools that will be used in later lessons.
Lesson F2: Web App Recon	For this lesson, students will use the Cyber Range: Cyber Basics (2020.12) environment to discover subdomains, directories, and files. Students will also install a vulnerable web application in Docker.
Lesson F3: Web App Manual Recon with Burp	For this lesson, students will understand how web requests and responses in a web application play a role in its security. They will learn how to define a target scope, refine a site map, manipulate requests, and analyze responses. Using the Cyber Range: Cyber Basics (2020.12) environment in a hands-on exercise, they will learn how to complete manual web application reconnaissance using Burp Suite.
Lesson F4: Manual Web App Vulnerability Testing	In this lesson, students will learn how to manually test a web application for vulnerabilities using Burp Suite, spider a website and analyze the data for sensitive data exposure, and examine the OWASP Top 10 to better understand common impactful vulnerabilities.
Lesson F5: Cross Site Scripting Basics	In this lesson, students will understand how to test a web application for cross site scripting (XSS). They will learn how to execute XSS attacks at different levels of security on two separate web applications. The focus of the lab exercise is on reflected and DOM (Document Object Model)-based XSS.

Module G: Web Apps and Data Servers Part 2	This module covers several web application security vulnerabilities in depth. Students will learn several techniques: how to exploit a system vulnerable to SQL injection, how to exploit a stored cross-site scripting vulnerability, how to scan an application to discover its vulnerabilities, and how to gain a shell from a file upload vulnerability. In addition, they will learn about post-exploitation techniques once a successful shell on a web application has been achieved. NOTE: This is the seventh of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2; this module. Module H is titled Natas. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson G1: SQL Injection	In this lesson, students will understand how to test a web application for SQL injection. They will learn how to execute error-based and UNION-based SQL injection using Burp Suite, SQLmap, and manual methods on the OWASP Juice Shop web application.
Lesson G2: Broken Authentication and In Depth SQLi	In this lesson, students will use the Cyber Range: Cyber Basics (2018) environment to learn how to manually execute SQL injections to retrieve personally identifiable information, discover account credentials, and modify shopping carts. In the lecture, students will learn about the global cyber war and its impact, and examine cybersecurity careers.
Lesson G3: Stored Cross Site Scripting	In this lesson, students will learn the basics of stored XSS and how to analyze code to determine if a site is vulnerable to stored XSS. Students will then exploit Stored XSS from an attacker's perspective using the Browser Exploitation Framework.
Lesson G4: Web App And Vulnerability Scanning	In this lesson, students will learn about the Web Application Vulnerability stack and its layers to better understand a web applications attack surface. The focus then turns to the web app architecture and its importance when scanning. In the lesson exercise, students will use the Cyber Range: Cyber Basics (2018) environment to learn how to complete vulnerability scanning using Nikto, SkipFish, and Zed Attack Proxy (ZAP). In addition, students will examine the benefits of Extensions/Add-ons and WhatWeb when determining what is running on a web application/site.
Lesson G5: Web App Shells	In this lesson students create and spawn a web application shell in DVWA using a file upload vulnerability. They further explored the DVWA shell and attempted to better understand how the system works. They learn how to spawn a bash terminal inside a DVWA shell and navigate the application file system. Using the spawned terminal shell they will learn to view running processes. Finally, students will learn several ways to enumerate and further explore a MySql database once a shell is established.
Module H: Natas	This module covers several web application security vulnerabilities in depth with a focus on using Python and the Sublime Text editor to exploit vulnerabilities. Using the OverTheWire website “Natas,” students will complete challenges in a progressive capture the flag (CTF) game. Some knowledge of Python will be beneficial; however, it is not required to complete the labs. NOTE: This is the eighth of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module A is titled Introduction to Ethical Hacking. Module B is titled Reconnaissance. Module C is titled Scanning and Enumeration. Module D is titled Sniffing, IDS, and Firewall Evasion. Module E is titled System Hacking. Module F is titled Web Apps and Data Servers. Module G is titled Web Apps and Data Servers Part 2. Module H is titled Natas; this module. Module I is titled Advanced Social Engineering. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson H1: Natas Level 0-6	In this lesson, students will understand how to test for web-based vulnerabilities using Python, Sublime Text and Natas. Natas is an educational open source CTF challenge hosted on overthewire.org. Students will be introduced to script writing using the requests and re Python modules. Using scripting basics, students will parse information from the web and analyze the information. The lab exercise drives home and is key in the student's mastering of the learning objectives.
Lesson H2: Natas Level 6-10	In this lesson, students will learn new skills by setting up the Sublime Text editor with Python and using it to test web applications. Using the Brigante VM environment, students will be presented with progressive challenges from the OverTheWire website (Natas) in which they will use previously learned skills to find the CTF flags. This lesson covers natas levels 6-10. Students will learn to exploit a local file inclusion vulnerability, a directory traversal vulnerability, a cryptographic vulnerability and a command injection vulnerability.
Lesson H3: Natas Level 10-13	In this lesson, students will learn new skills by setting up the Sublime Text editor with Python and using it to test web applications. Using the Brigante VM environment students will be presented with progressive challenges from the OverTheWire website (Natas) in which they will use previously learned skills to find the CTF flags. This lesson covers levels 10-13. Students will learn to exploit a command injection vulnerability, bypassed character filters, decoded weak encryption and exploited a PHP file upload vulnerability.
Lesson H4: Natas Level 13-16	In this lesson, students will learn new skills by setting up the Sublime Text editor with Python and using it to test web applications. Using the Brigante VM environment, students will be presented with progressive challenges from the OverTheWire website (Natas) in which they will use previously learned skills to find the Capture the Flag (CTF) flags. This lesson covers levels 13-16. Students will learn to exploit a file upload service, an SQL injection vulnerability, and a blind SQL injection vulnerability.
Lesson H5: Natas Level 16-19	In this lesson, students will learn new skills by setting up the Sublime Text editor with Python and using it to test web applications. Using the Brigante VM environment students will be presented with progressive challenges from the OverTheWire website (Natas) in which they will use previously learned skills to find the CTF flags. This lesson covers levels 16-19. Students will learn to exploit a command injection vulnerability, a timed SQL injection vulnerability, and hijack a session with a brute force technique.

Module I: Advanced Social Engineering	This module covers Advanced Social Engineering. Students will learn about and examine the attack cycle of social engineering, social engineering history, and its most notorious professionals. In the lab exercises, they will complete social engineering tasks that lead to the exploitation of systems through spoofing, credential harvesting, and phishing. NOTE: This is the ninth of 18 modules in the Cyber Security Advanced Ethical Hacking course. Module 1 is titled Introduction to Ethical Hacking. Module 2 is titled Reconnaissance. Module 3 is titled Scanning and Enumeration. Module 4 is titled Sniffing, IDS, and Firewall Evasion. Module 5 is titled System Hacking. Module 6 is titled Web Apps and Data Servers. Module 7 is titled Web Apps and Data Servers Part 2. Module 8 is titled Natas. Module 9 is titled Advanced Social Engineering; this module. As each module is completed, it will be posted. We are working diligently to get the remaining 9 modules and course published.
Lesson I1: Pretexting And Spoofing	In this lesson, students will learn about pretexting and spoofing attacks. In the lesson exercise, students learn how to spoof a phone number and use pretexting to convince individuals to provide personal information.
Lesson I2: Email Spoofing	In this lesson, students will learn about SMTP vulnerabilities and email spoofing techniques.
Lesson I3: Harvesting Credentials	In this lesson, students will learn about credential harvesting techniques. Students will then perform three techniques: website cloning, LLMNR, and MimiKatz in the lab exercise.
Lesson I4: Creating Social Engineering Exploits	In this lesson, students will learn about social engineering (SE) tactics, the SE attack cycle, and examine engagements in Social Engineering. In the lesson exercise, students will create a PowerShell script that can be used in a social engineering attack.
Lesson I5: Spear Phishing	In this lesson, students will learn about social engineering psychology, manipulation tactics, and how to create a spear phishing exploit using the social engineering toolkit.
	COURSE: Introduction to the Command Line Interface
Introduction to the Command Line Interface	This is a ten-module course with the goal to provide students with an introduction to the Linux operating system command line interface (CLI). Each module includes several hands-on lab exercises that allows students to practice navigating around the CLI and use Linux commands. These can all be completed in the Cyber Range virtual environment. Modules: Module A: Basics of using the Command Line Interface Module B: Working with Files and Directories Module C: Working with Users and Groups Module D: Working with Linux Commands Module E: Working with Processes and Services Module F: Editing Files Module G: Processing Text Files Module H: Networking Module I: Installing software Module J: Secure Shell (SSH)
Module A: Basics of Using the Command Line Interface	The purpose of this module is to introduce students to the basics of using the Command Line Interface (CLI) in Linux to perform tasks. NOTE: This is the first of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface; this module. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson A1: Bash Basics	In this lesson, the student will learn the basics of using the Linux Command Line Interface (CLI), also known as the terminal.
Lesson A2: Moving Around the CLI	In this lesson, the student will learn the basics of moving around on the Linux Command Line Interface (CLI), also known as the terminal.

Module B: Working with Files and Directories	The purpose of this module is to introduce students to the basics of working with files and directories in the Linux file system. NOTE: This is the second of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories; this module. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson B1: The Linux File System	In this lesson, the student will learn the basics of the Linux File System.
Lesson B2: File System Shortcuts	In this lesson, the student will learn the basics of the Linux File System Shortcuts.
Lesson B3: Listing Files	In this lesson, the student will learn the basics of the listing files in the Linux File System.
Lesson B4: Making Files and Directories	In this lesson, the student will learn the basics of Making Files and Directories in the Linux File System.
Lesson B5: Removing Files and Directories	In this lesson, the student will learn how to remove files and directories in the Linux file system.
Lesson B6: File and Directory Permissions	In this lesson, the student will learn how to set file and directory permissions in the Linux file system.
Lesson B7: Copying and Moving Files and Directories	In this lesson, the student will learn how to copy and move files and directories in the Linux file system.
Lesson B8: Finding Files and Directories	In this lesson, the student will learn how to find files and directories in the Linux file system.
Lesson B9: Zipping and Unzipping Files	In this lesson, the student will learn how to zip and unzip files in the Linux file system.
Lesson B10: File Links	In this lesson, the student will learn how file links are used in the Linux file system.
Lesson B11: File Information	In this lesson, the student will learn how to find file information in the Linux file system.
Module C: Working with Users and Groups	The purpose of this module is to introduce students to the basics of working with users and groups in the Linux file system. NOTE: This is the third of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups; this module. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson C1: Types of Users	In this lesson, the student will learn the different types of users on a Linux system.
Lesson C2: Working with User Accounts	In this lesson, the student will learn how to work with user accounts on a Linux system.
Lesson C3: Working with Groups	In this lesson, the student will learn how to work with groups on a Linux system.
Lesson C4 Modifying Users	In this lesson, students will learn how to modify users on a Linux system.

Module D: Working with Linux Commands	The purpose of this module is to introduce students to the basics of working with Linux commands. NOTE: This is the fourth of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands; this module. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson D1: Identifying Commands	This lesson will demonstrate how to identify commands on a Linux system.
Lesson D2: Getting Help	In this lesson, the student will learn how to get help with commands on a Linux system.
Lesson D3: Command Aliases	In this lesson, the student will learn how to use command aliases on a Linux system.
Lesson D4: Command Redirection	In this lesson, the student will learn how to use command redirection on a Linux system.
Lesson D5: Command Quotes	In this lesson, the student will learn how to use quotes with commands on a Linux system.
Lesson D6: Command Expansion	In this lesson, the student will learn how to use command expansion on a Linux system.
Lesson D7: Controlling Commands	In this lesson, the student will learn how to use control commands on a Linux system.
Module E: Working with Processes and Services	The purpose of this module is to introduce students to the basics of working with processes and services on a Linux system. NOTE: This is the fifth module of the ten-module Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services; this module. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson E1: Working with Processes	In this lesson, the student will learn how to work with processes on a Linux system.
Lesson E2: Working with Services	In this lesson, the student will learn how to work with services on a Linux system.
Module F: Editing Files	The purpose of this module is to introduce students to the basics of editing files on a Linux system. NOTE: This is the sixth of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files; this module. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson F1: Using Nano	In this lesson, the student will learn how to use the Nano text editor on a Linux system.
Lesson F2: Using Vi Part 1	In this lesson, the student will learn how to use the Vi text editor on a Linux system.

Lesson F3: Using Vi Part 2	In this lesson, the student will learn how to use the Vi text editor on a Linux system.
Lesson F4: Using Vi Part 3	In this lesson, the student will learn how to use the Vi text editor on a Linux system.
Module G: Processing Text Files	The purpose of this module is to introduce students to the basics of viewing and parsing text files on a Linux system. NOTE: This is the seventh of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files; this module. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson G1: Viewing Text Files	In this lesson, the student will learn how to use Linux commands to view a file from the CLI.
Lesson G2: Parsing Text Files	In this lesson, the student will learn how to use Linux commands to view a file from the CLI.
Module H: Networking	The purpose of this module is to introduce students to the basics of networking on a Linux system. NOTE: This is the eighth of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking; this module. Module I is titled Installing Software. Module J is titled Secure Shell (SSH).
Lesson H1: Networking Interfaces	This lesson will demonstrate how to use Linux commands to view the network interface information.
Lesson H2: Testing Network Connectivity	In this lesson, the student will learn how to use Linux commands to test network connectivity from the CLI.
Lesson H3: Name Resolution	In this lesson, the student will learn how to use Linux commands to perform name resolution from the CLI.
Module I: Installing Software	The purpose of this module is to introduce students to the basics of installing software on a Linux system. NOTE: This is the ninth of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software; this module. Module J is titled Secure Shell (SSH).
Lesson I1: Advanced Packaging Tool	In this lesson, the student will learn how to use Linux commands to install, remove, and upgrade software packages.
Lesson I2: Debian Package Manager	In this lesson, the student will learn how to use the dpkg command to install and remove software packages.

Module J: Secure Shell (SSH)	The purpose of this module is to introduce students to the basics of using Secure Shell (SSH) for secure remote connections to a Linux server. NOTE: This is the tenth of 10 modules in the Introduction to the Command Line Interface course. Module A is titled Basics of using the Command Line Interface. Module B is titled Working with Files and Directories. Module C is titled Working with Users and Groups. Module D is titled Working with Linux Commands. Module E is titled Working with Processes and Services. Module F is titled Editing Files. Module G is titled Processing Text Files. Module H is titled Networking. Module I is titled Installing Software. Module J is titled Secure Shell (SSH); this module.
Lesson J1: Secure Shell (SSH)	In this lesson, the student will learn how to use the Linux command line to create secure remote connections with the ssh and sftp commands.
Lesson J2: Secure Shell (SSH) with Certificates	In this lesson, the student will learn how to use the Linux command line to create secure remote connections with the ssh and sftp commands using public key certificates.
	MODULE: Penetration Testing Using Kali Linux
Penetration Testing Using Kali Linux	The purpose of this module is to introduce students to the use of Kali Linux to perform a penetration test against a target system in a controlled lab environment. The material is approached from the perspective of what an actual penetration tester would do in a real-life penetration testing scenario. This module contains the following nine labs and provides a hands-on introduction to penetration testing to prepare students for opportunities as penetration testers or red team members in industry and government: RECOMMENDED: Complete labs in order
Lesson/Laboratory Exercise 1: Reconnaissance	This lab will demonstrate the use of the route command to obtain network information and the use of nmap and Zenmap to map a network.
Lesson/Laboratory Exercise 2: Enumeration	This lab will demonstrate the use of various Tools, Techniques, and Procedures for the enumeration of hosts discovered on a network. In network penetration testing, enumeration is the act of examining or observing a specific host or target to generate a list of services and ports for possible exploitation. A penetration tester will use enumeration to locate ports, services, and software versions for possible exploit during the penetration test. The student should have completed the previous lab in the Penetration Testing Using Kali Linux module: Reconnaissance.
Lesson/Laboratory Exercise 3: Vulnerability Scanning	This lab will demonstrate the use of various Tools, Techniques, and Procedures to complete a vulnerability scan of hosts discovered on a network. The student should have completed the previous two labs in the Penetration Testing Using Kali Linux module: Reconnaissance and Enumeration.
Lesson/Laboratory Exercise 4: Exploitation	This lab will demonstrate the use of various Tools, Techniques, and Procedures to complete the exploitation of a target host based upon a known vulnerability. The student should have completed the previous three labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, and Vulnerability Scanning.
Lesson/Laboratory Exercise 5: Post-Exploitation	This lab will demonstrate the use of various Tools, Techniques, and Procedures to complete post-exploitation activities of a target host that has already been exploited. The student should have completed the previous four labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, Vulnerability Scanning, and Exploitation.
Lesson/Laboratory Exercise 6: Exfiltration	This lab will demonstrate the use of various Tools, Techniques, and Procedures to exfiltrate data from a target host that has already been exploited. Now that we have access setup with ssh (see previous lab), it is time to exfiltrate the passwords from the system. Even though we now have an account with root level access, it is always a good idea to see if we can get access to other accounts. Other systems may use accounts located on this system and we can always use additional accounts as backups should our newly created account be discovered and deleted. The student should have completed the previous five labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, Vulnerability Scanning, Exploitation, and Post-Exploitation.
Lesson/Laboratory Exercise 7: Password Cracking	This lab will demonstrate the use of various Tools, Techniques, and Procedures to crack passwords exfiltrated from a target host that has already been exploited. The student should have completed the previous six labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, Vulnerability Scanning, Exploitation, Post-Exploitation, and Exfiltration.
Lesson/Laboratory Exercise 8: Creating a Backdoor	This lab will demonstrate the use of various Tools, Techniques, and Procedures to create a backdoor on the target host that has already been exploited. The student should have completed the previous seven labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, Vulnerability Scanning, Exploitation, Post-Exploitation, Exfiltration, and Password Cracking.
Lesson/Laboratory Exercise 9: Cleaning Up	The last step of a penetration test is cleaning up all of the changes made to the target system. This lab will demonstrate the use of various Tools, Techniques, and Procedures to clean up the target host that has been exploited. The student should have completed the previous eight labs in the Penetration Testing Using Kali Linux module: Reconnaissance, Enumeration, Vulnerability Scanning, Exploitation, Post-Exploitation, Exfiltration, Password Cracking, and Creating a Backdoor.