Syllabi Cybersecurity Program

CYSE 100: Introduction to Information Security and Assurance

Course Description

This course helps students take a proactive, realistic, and holistic approach to assess cyber threats and implementing countermeasures. It provides students with basic knowledge and skills in the fundamental theories and practices of cybersecurity. This course also provides a basic introduction to all aspects of cybersecurity, including core concepts, technology and skills, latest attacks and countermeasures, policy and procedures, communications security, network security, security management, legal issues, political issues, and technical issues.

Required Textbook

“Computer Security Fundamentals”, By Chuck Easttom, 4th Edition. ISBN-13: 9780135774731

Reference Textbook

“Elementary Information Security” By Richard E Smith., Third Edition, ISBN- 9781284153040

Course Objectives

Students who complete this course should be able to perform the following tasks:

1. Understand the basic principles of information security
2. Understand the broad set of technical, social & political aspects of information security
3. Understand the modern concepts in cybersecurity attacks and prevention methods
4. Identify main tradeoffs between different cybersecurity-related interests (e.g., between economics and security levels; between law enforcement and civil liberties; between private interests and public interests).
5. Identify and define challenges to understand secure procedures to protect information
6. Suggest approaches to maintain a reasonable state of information security and to address breaches effectively, ethically, and according to law.

Topics Covered:

1. Introduction to Computer Security
2. Networks and the Internet
3. Cyber Stalking, Fraud, and Abuse
4. Denial of Service Attacks
5. Malware
6. Techniques Used by Hackers
7. Industrial Espionage in Cyberspace
8. Encryption
9. Computer Security Technology
10. Security Policies
11. Network Scanning and Vulnerability Scanning
12. Cyber Terrorism and Information Warfare
13. Cyber Detective
14. Introduction to Forensics
15. Cybersecurity Engineering

CYSE 110: Ethics in Cybersecurity and Cyberlaw

Course Description
This course offers an accessible introduction to the topic of cybersecurity ethics consisting of three parts. Part I introduces the field of ethics, philosophy, and philosophy of science, ethical frameworks, and the notion of ethical hacking. Part II applies these frameworks to issues within the field of cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyber-ethics in relation to military affairs. Part III concludes by exploring current codes of ethics used in cybersecurity.

Required Textbook
Cybersecurity, Introduction, By Mary Manjikian, 2018, Published by Routledge. ISBN-13: 978-1138717497

Reference Textbook
Cybersecurity Law, By Jeff Kosseff, 2019, Published by Wiley and Sons. ISBN-13: 978-1119517207
Other Readings as Assigned by Instructor

Course Objectives
Students who complete this course should be able to perform the following tasks:

1. Describe steps for carrying out ethical penetration testing, describe ethical hacking principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.
2. Identify concepts such as ethics, morals, character, ethical principles, and ethical relativism.
3. Demonstrate an understanding of the importance of ethical issues that emerge from the widespread use of information technology.
4. Identify appropriate and ethical behaviors, legal standards, rights, restrictions, and moral duties when accessing technology systems, digital media, and information technology within the context of today's society.
5. Demonstrate an understanding of the ethical issues associated with confidentiality and privacy as they relate to information technology.
6. Provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology, and data.
7. Evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking

Topics Covered:

1. What is ethics
2. Three ethical frameworks
3. The ethical hacker
4. The problem of privacy
5. The problem of surveillance
6. The problem of piracy
7. The problem of cyberwarefare

CYSE 130: IT System Component Security

Course Description
This course provides students with a basic understanding of an information technology system's core components and their roles in system operation. It also covers high-level introduction of endpoint protection, storage devices, system architectures, alternative environments, network security components, intrusion detection and prevention systems, incident response, software security, configuration management. It also focuses on vulnerability scanning, vulnerability windows, physical and environmental security concerns, Internet of Things, and cyber defense.

Required Textbook

“Fundamentals of Information System Security, Third Edition”,
Author: Davin Kim and Michael G. Solomon.
Publisher: John and Bartlett Learning.
ISBN-13: 978-1284116458

Course Objectives
Students who complete this course should be able to perform the following tasks:

1. Describe different Network Security Components (Data Loss Prevention, VPNs / Firewalls)
2. Understand different System Architectures (Virtualization / Containers, Cloud)
3. Describe the hardware components of modern computing environments and their individual functions.
4. Describe different components of a network components.
5. Describe the basic security implications of modern computing environments.
6. Understand the Federal, State and Local Cyber Defense partners/structures.
7. Properly use the Vocabulary associated with cybersecurity.

Topics Covered:

1. Information Systems Security
2. The Internet of Things Is Changing How We Live
3. Malicious Attacks, Threats, and Vulnerabilities
4. The Drivers of the Information Security Business
5. Access Controls
6. Security Operations and Administration
7. Auditing, Testing, and Monitoring
8. Risk, Response, and Recovery
9. Cryptography
10. Networks and Telecommunications
11. Malicious Code and Activity
12. Information Security Standards
13. Information Systems Security Education and Training
14. Information Security Professional Certifications
15. U.S. Compliance Laws

CYSE 200: Network Security

Course Description
This course provides a comprehensive overview of fundamental network security concepts, techniques, and issues such as types of cyber-attacks, attacker profiles, and hardware/software defense solutions. It includes fundamental principles and basic concepts of data communications and networking, the various network components. It also enables students to build a comprehensive security strategy and differentiate between intrusion prevention and intrusion detection systems.

Required Textbook
Computer Security Principles and Practice, 4th Edition, Publisher Pearson Edition 2018, ISBN-10:0-13-479410-9

Course Objectives
Students who complete this course should be able to perform the following tasks:

1. Describe different Network Security Components (Data Loss Prevention, VPNs / Firewalls)
2. Understand different System Architectures (Virtualization / Containers, Cloud)
3. Describe the hardware components of modern computing environments and their individual functions.
4. Describe different components of a network components.
5. Describe the basic security implications of modern computing environments.
6. Understand the Federal, State and Local Cyber Defense partners/structures.
7. Properly use the Vocabulary associated with cybersecurity

Topics Covered:

1. Network Technologies
2. Network Layers
3. Network Security Goals
4. Categories of Network Attacks
5. Defending Against Network Attacks
6. Remote Access Security
7. Firewalls
8. Virtual Private Network
9. Intrusion Detection and Prevention (IDS/IPS)

CYSE 220: Introduction to Cryptography

Course Description

This course is an introduction to modern cryptography describing basic principles of cryptography and general cryptanalysis. It covers the concepts of symmetric encryption and authentication, as well as public key encryption, digital signatures, and key establishment. It also includes common examples and uses of cryptographic schemes, including the AES, RSA-OAEP, the Digital Signature Algorithm, and the basic Diffie-Hellman key establishment protocol.

Required textbook:

"Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC Press, 2nd edition.

Objectives

Students who complete this course should be able to perform the following tasks:

1. implement and cryptanalyze classical ciphers.
2. describe modern private-key cryptosystems and ways to cryptanalyze them.
3. describe modern public-key cryptosystems and ways to cryptanalyze them.
4. explain basic mathematical concepts underlying modern cryptography
5. describe the field of cryptography and its relation to security.

Topics Covered:

1. Introduction and classical cryptography
2. Private-key encryption
3. Message authentication codes
4. Hash functions and applications
5. Practical constructions of symmetric-key primitives
6. Theoretical constructions of symmetric-key primitives
7. Number theory and cryptographic hardness assumptions
8. Algorithms for factoring and computing discrete logarithms
9. Key management and the public-key revolution
10. Public key encryption
11. Advanced topics in public-key encryption

CYSE 230 Introduction to Computer and Mobile Forensics

Course Description:
This course presents methods to properly conduct a computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. The provides an overview of digital investigations and data recovery with emphasis on data presentation techniques and chain-of-evidence procedures. Current computer forensics tools are presented along with controls required for digital evidence acquisition.

Required Textbook:
- Guide to Computer Forensics and Investigations – Sixth Edition, by Phillips, Nelson, & Steuart. (Cengage Learning / Course Technology, Boston, MA, 2019)

Reference Textbook:
- Access Data Forensics Training Manual – Copyright 2019, Access Data Group, LLC.

Objectives
Upon completion of this course, students will be able to:

1. Describe how to conduct a computer forensic investigation and complete a case
2. Determine the best data acquisition method, then perform, and validate a data acquisition using the appropriate tools and techniques
3. Describe how to identify, secure, catalog, and store digital evidence
4. Explain the Microsoft DOS & Windows file structures and describe how to retrieve digital evidence from those file structures
5. Differentiate, validate, and use various computer forensics software tools to analyze various forms of digital evidence
6. Analyze and repair graphic files using the appropriate software tools and techniques
7. Describe network forensics and differentiate various network forensic tools and techniques
8. Analyze various types of emails and email file headers
9. Describe mobile forensics and differentiate various mobile forensic tools and techniques
10. Create professional reports for forensic investigations
11. Prepare and provide Expert Witness Testimony for computer forensic investigations
12. Apply ethics and professional codes of conduct to computer forensic investigations and to Expert Witness testimony

Topics Covered:

1. Understanding the digital forensics profession and investigation
2. The investigator's office and laboratory
3. Data acquisition
4. Processing crime and incident scenes
5. Working with windows and CLI systems
6. Current digital forensics tools
7. Linux and Macintosh file systems
8. Recovering graphics files
9. Digital forensics analysis validation
10. Virtual machine forensics, live acquisition, and network forensics
11. e-mail and social media investigations
12. mobile device forensics and the internet of anything
13. cloud forensics

CYSE 275: Principles of Cybersecurity and Security Management

Course Description
This course covers the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. It includes the topics related to Administering a Secure Network, understanding the basic and core concepts of information security, identifying different types of cyber-attacks including, Malware and Social Engineering Attacks, Networking and Server Attacks.

Required Text
- "Security+ Guide to Network Security Fundamentals 6th Edition" Author: Mark Ciampa, PhD, Publisher: Cengage Learning ISBN 978-1-337-28878-1"

Course Objectives:

1. At the completion of the course, the student will be able to:
2. Describe various concepts in network defense.
3. Describe various network vulnerabilities and attacks.
4. Describe client-side attacks and Web application attacks such as cross scripting, SQL, XML, and command injection attacks.
5. Apply security knowledge to implement network defense measures, such as IDS/IPS, firewalls and VPNs.
6. Use network monitoring and mapping tools for network traffic analysis and network defense.
7. List the steps for hardening systems and networks and securing applications and data.
8. Administer a secure network in terms of network protocols and network design principles.
9. Describe and configure wireless network security.
10. Describe access control fundamentals, models, and best practices.
11. Define and evaluate authentication methods and technologies
12. Compare and evaluate encryption solutions.
13. Apply cryptography solutions to data and communication protection.
14. Describe and configure DMZs and proxy servers.
15. Identify and evaluate network security controls, solutions, and tools.
16. Create and evaluate network policy and operational procedures for network hardening and defense.

Topics Covered:

1. Introduction to security
2. Malware and social engineering attacks
3. Basic cryptography
4. Advanced cryptography and PKI
5. Networking and server attacks
6. Network security devices design, and technology
7. Administering a secure network
8. Wireless network security
9. Client and application security
10. Mobile and embedded device security
11. Authentication and account management
12. Access management
13. Vulnerability assessment and data security
14. Business continuity
15. Risk mitigation

CYSE210: Computer Data Communication, Networking Protocols and Management

Course Description

This course covers topics closely related to the Computer Network Fundamentals and more importantly it will prepare the students for the COMPTIA Network+ Certification. This course will enable the students to understand the TCP/IP protocols and their functions in addition to the lab sessions where they will have a hands-on experience on how to create, review, update, and troubleshoot different network topologies, and secure the network infrastructure. The lab sessions will also learn the command line network administration tools, configuring and setting different network security tools. Moreover, they will be able to learn and apply the best network security policies and practices to support the business continuity plans.

COURSE MATERIAL:
Text CompTIA Network+ N10-007 Cert Guide, Deluxe Edition
Author Anthony Sequeira, Michael D. Taylor
ISBN-13: 978-0-7897-5982-5

Note: The textbook CompTIA Network+ N10-007 Hands-on Lab Simulator software included free on the companion website that accompanies this book.

Title: TestOut Network Pro
ISBN: 978-1-935080-43-5
Pricing Code: 14-232TA
Available at http://www.testout.com/resources/student-resources/student-purchase

Course Objectives:

Upon completion of this course, students will be able to:

1. Describe fundamental networking concepts including network architecture, components, topologies, protocols, services, connection technologies, and the OSI and TCP/IP models.
2. Identify and describe cables and connectors including twisted pair, coaxial, fiber optic, and wiring implementation.
3. Select, install, and connect networking devices such as network adapters, media converters and routers.
4. Describe Ethernet architecture, specifications, and connecting devices.
5. Explain network implementation including IP addressing and assignment, DNS name resolution, routing, NAT, subnetting, and data communication format.
6. Describe wireless networking standards, configuration, and security issues.
7. Analyze TCP connections and explain wide area networks technologies, services and structure, internet connectivity and remote access.
8. Describe network security, authentication, firewalls, VPNs, detection and prevention and secure protocols.
9. Explain and analyze network management, documentation, monitoring and optimization.
10. Analyze and troubleshoot network communication, connections, IP configuration, name resolution, switching and routing.
11. Use tools for network mapping, monitoring, and troubleshooting and packet tracing and analysis.
12. Apply knowledge of network technologies to design and construct a working network.

Topics Covered:

1. Computer Network Fundamentals
2. The OSI Reference Model
3. Network Components
4. Ethernet Technology
5. IPv4 and IPv6 Addresses
6. Routing IP Packets
7. Wide Area Networks (WANs)
8. Wireless Technologies

9. Network Optimization
10. Command-Line Tools
11. Network Management
12. Network Security
13. Network Policies and Best Practices
14. Network Troubleshooting
15. Final Preparation

CYSE 310 Cybersecurity Planning, Operation, and Incident response Management

Course Description

This course addresses the basic Cybersecurity planning techniques, the different components of cybersecurity operations, the purpose of incident response management systems. Moreover, it enables the students to learn the application of cybersecurity planning, the main properties of cybersecurity Operation, and how Incident management helps in resolving issues related to different cyber threats in the daily operation and administration of enterprise computer systems. It also describes ethical considerations, as per the (ISC)2 code of ethics guidelines and provides a clear understanding of the information security principles and how an SSCP candidate must be able to apply them in all situations. Additional topics to be covered include privacy, least privilege, non-repudiation, and the separation of duties.

Course Materials

The Cyber Intelligence Handbook: An Authoritative Guide for the C-Suite, IT Staff, and Intelligence Team

By David M. Cooney Jr. (Author), Muireann O'Dunlaing (Editor), Mark McGibbon (Foreword)

Course Objectives

Students who complete this course should be able to perform the following tasks:

1. Explain the purpose of different cybersecurity technologies
2. Evaluate current, commonplace threats in the context of a cybersecurity investigation
3. Develop skills, knowledge and understanding focused on how cyber security professionals respond to a cyberattack.
4. Apply legally defensible practices to a cyber security investigation
5. Investigate evidence from a cyber security incursion
6. Understand the full spectrum of Cybersecurity Operation

Topics Covered:

1. Planning Cybersecurity Strategies
2. Full Spectrum of Cybersecurity Operation (CND, CNE, CNA, and CNO)
3. Effective Cybersecurity Operation
4. Incident Response Techniques and Management
5. Understanding Intelligence
6. Understand Threats
7. Understand your needs
8. The simplified cyber intelligence process
9. Sustaining and improving cyber intelligence capabilities

CYSE 320: Reverse Engineering and Malware Analysis

Course Description

This course offers a systematic approach to reverse engineering with plenty of hands-on exercises and real-world examples. Students will use the reverse engineering tools to thwart potential threats to stop hackers in their tracks. This course also covers the static and dynamic analysis of malware, Malware functionalities and Persistence, Code injections and hooking, Malware Obfuscation Techniques. Students will learn how to hunt and detect Malwares using Memory forensics.

This course also covers the static and dynamic analysis of malware, Malware functionalities and Persistence, Code injections and hooking, Malware Obfuscation Techniques. Students will learn how to hunt and detect Malwares using Memory forensics,

Course Textbook
- "Practical Reverse Engineering, X64, X86, Windows Kernel, reversing tools and Obfuscation", By
  Authors: Bruce Dang, Alexandre Gazet, and Elias Bachaalany, ISBN-13: 978-1118787311
- "Learning Malware Analysis: Explore the Concepts, tools, and techniques to analyze and investigate
  Windows Malware." Author: Monnappa K A, ISBN: 978-1-78839-250-1

Course Objectives:
Students who complete this course should be able to perform the following tasks:

1. Recognize and understand the characteristics of various malware, motivations of creators, and impacts on recipients.
2. Describe the manner that malware propagates, becomes resident and executes.
3. Analyze how malware interacts with any associated networks, identifying the type of information being targeted.
4. Demonstrate the ability to use various tools and techniques to safely perform static and dynamic analysis of software (or malware) of potentially unknown origin, including obfuscated malware, to fully understand the software's functionality.
5. Apply testing methodologies to build test cases that demonstrate the existence of vulnerabilities in software (or malware).
6. Recognize and understand the anti-disassembly, anti-debugging, and anti-VM techniques that are incorporated by the attacker to impede the analysis and reversing of malware.

7. Formulate Indicators of Compromise (IoCs) from malware samples to aid in threat intelligence efforts.
8. Demonstrate ethical behavior appropriate to security-related technologies.

Topics Covered:

1. Practical Reverse Engineering of Cyber-attacks
2. Malware Analysis Techniques
3. Early identification of targeted resources
4. Techniques to investigate Malwares
5. The importance of ethical behavior
6. Building testing cases to implement reverse engineering practices
7. Formulating indicators of targeted critical infrastructure resources
8. x86 and x64
9. ARM
10. The Windows Kernel
11. Debugging and Automation
12. Obfuscation

CYSE 355 Cybersecurity Tools and Risk Management

Course Description

This course provides basic introduction to cybersecurity tools. It covers the properties of cybersecurity tools, types, and motives of cyber-attacks. This course also describes the security life cycle, framework, and different security models. It also includes research cybersecurity issues in the modern era.

Required Textbook:
Information Assurance Handbook: Effective Computer Security and Risk Management Strategies
by Corey Schou, Steven Hernandez
Released September 2014
Publisher(s): McGraw-Hill
ISBN: 9780071826310

Course Objectives:

Upon completion of this course, students will be able to:

1. Define key terms and fundamental concepts of cyber defense used for system security.
2. Identify and describe information security vulnerabilities, threats, attacks, and risks.
3. Apply risk assessment methods to information security risk analysis.
4. Define and differentiate confidentiality, integrity, availability, access, identification, authentication authorization, audit, non-repudiation, and privacy.
5. Describe security life cycle, frameworks, and security models.
6. Explain intrusion detection and prevention systems and technology.
7. Describe access control models (MAC, DAC, BRAC) and authentication methods.
8. Identify system vulnerabilities and risks and corresponding security technologies and methods.
9. Use tools for vulnerability scanning and analysis.
10. Identify and evaluate information security tools, controls, and mechanisms.
11. Describe data security mechanisms and fundamentals of cryptography.
12. Evaluate business continuity planning and disaster recovery planning in a security framework.
13. Identify and describe key laws, ethics, and professional communities in information security.

Topics Covered:

1. The Need for Information Security
2. Concepts in Information Security
3. Assets, Threats, Vulnerabilities, Risks, and Controls
4. Security Professionals and Organizations
5. Information Security management System
6. Implementing Information Security Strategy into Current Practices, Regulations, and Plans
7. Approaches to Implementing Information Security
8. Organizational Structure for Managing Information Security
9. Asset Management
10. Information Security Risk Management
11. Information Security Policy
12. Human Resource Security
13. Certification, Accreditation, and Assurance
14. Information Security in System Development

15. Physical and Environmental Security Controls
16. Information Security Awareness, Training, and Education
17. Preventive Tools and Techniques
18. Access Control
19. Information Security Monitoring Tools and Methods
20. Information Security Measurements and Metrics
21. Information Security Incident Handling
22. Computer Forensics
23. Business Continuity
24. Backup and Restoration

CYSE 410: Threat Intelligence and Cyber Defense

Course Description:

This course prepares students to be aware of network attack strategies and common countermeasures and prepare students to use various penetration testing tools to analyze networks for vulnerabilities. It also enables the students to exploit vulnerabilities and weaknesses in various systems and Knowledge of these vulnerabilities also helps students to understand how to counter these vulnerabilities and improve network security. This Course prepares the students to be a certified ethical hacker (CEH) and penetration tester.

Required Book:
- Ethical Hacking: The Ultimate Guide to Using Penetration Testing to Audit and Improve the Cybersecurity of Computer Networks for Beginners, Including Tips on Social Engineering.
- CEH Certified Ethical Hacker Bundle, Fourth Edition 4th Edition, MAT WALKER, ISBN-13: 9781260455267 ISBN-10: 1260455262

Course Objectives:
Students who complete this course should be able to perform the following tasks:

1. Grasp the step-by-step methodology and tactics that hackers use to penetrate network systems
2. Understand the finer nuances of trojans, backdoors, and countermeasures
3. Get a better understanding of IDS, firewalls, honeypots, and wireless hacking
4. Master advanced hacking concepts, including mobile device, and smartphone hacking, writing virus codes, exploit writing & reverse engineering and corporate espionage.
5. Gain expertise on advanced concepts such as advanced network packet analysis, securing IIS & Apache web servers, Windows system administration using PowerShell, and hacking SQL and Oracle databases
6. Cover the latest developments in mobile and web technologies including Android, iOS, BlackBerry, Windows Phone, and HTML 5
7. Learn advanced log management for information assurance and allow you to manage information security with more clarity
8. Understand how to Prevents malicious hackers from entering the system through the identified loopholes.
9. Learn How to Erase all traces of the hack after checking the system for any vulnerability.

Topics Covered:

1. Best Practices of Threat Intelligent
2. Network attack strategies and common countermeasures fighting against companies
3. Applying various penetration testing tools
4. Assess computer system security by using penetration testing techniques.
5. Scan, Test and Hack secure systems and applications,
6. Methodology and tactics that hackers use to penetrate network systems
7. Advanced hacking concepts (Including mobile device, and smartphone hacking, writing virus codes, exploit writing)
8. Reverse engineering and corporate espionage.
9. Prevention of malicious hackers from entering the system through the identified loopholes.
10. Erasing all traces of the hack after checking the system for any vulnerability.
11. Ethical hacking defined
12. War on the internet
13. engineer's mind
14. The almighty EULA
15. the danger of defaults
16. John Deere
17. Copyright and how to protect copyright
18. YouTube content ID

CYSE 420 Cloud Computing Security

Course Description:

This course provides an overview of cloud computing essentials such as cloud computing models, services, the establishment of cybersecurity fundamentals, and data segregation security. It also covers and discusses cloud security and privacy, trust baselines, and the major components of cloud infrastructure. Moreover, it focuses on risk analysis by describing how to manage risk on the cloud, the role of risk management on cloud security, and securing cloud risk management processes. It finally discusses the best practices to secure critical infrastructure, including cloud-based access control policies, key management, and security architectures.

Required Text

Cloud Computing Security: Foundations and Challenges 1st Edition
Author John R. Vacca

Cloud computing environment and security technologies, so no single textbook can cover it all. Class notes will be provided for all topics covered.

Course Objectives:

Students who complete this course should be able to perform the following tasks:

1. Compare and select the viable cloud services and deployment techniques.
2. Analyze the trade-offs between deploying applications in the cloud and over the local infrastructure.
3. Compare the advantages and disadvantages of various cloud computing platforms.
4. Deploy applications over commercial cloud computing infrastructures such as Amazon Web Services,
5. Windows Azure, and Google AppEngine.
6. Program data intensive parallel applications in the cloud.
7. Analyze the performance, scalability, and availability of the underlying cloud technologies and software.
8. Identify security and privacy issues in cloud computing.
9. Identify and enforce cloud access control management techniques.
10. Explain recent research results in cloud computing and identify their pros and cons.

Topics Covered:

1. Cloud computing essentials and architectures (Cloud computing Characteristics, computing models, computing services)
2. Cloud security, privacy, and trust baselines
3. Identify the known threats, risks, vulnerabilities, and privacy issues associated with Cloud based IT services
4. Examining the security of major components of cloud infrastructure
5. Security vulnerability with cloud computing services (SaaS, PaaS, and IaaS)
6. Security issues with major characteristics of Cloud Computing
7. Security issues with cloud deployment services (Private, Public, Hybrid, Community)
8. Risk and Trust Assessment within the cloud operation
9. Managing risk on the cloud computing environment
10. The role of risk management on cloud security
11. Securing cloud risk management processes
12. Specification and enforcement of access policies in emerging scenarios
13. Cryptographic key management for data protection
14. Cloud security access control (Distributed Access Control)
15. Cloud Security Key Management: (Cloud Users Control)

CYSE 430: Secure Software Engineering

Course Description:
This course will enable students to identify and understand common software vulnerabilities and threats by exposing them to secure programming concepts, techniques, and preventative measures. Students will get some hands-on experience in the effective use of design patterns for secure code. This course is also designed to enable a student to take a proactive approach to software security. This course also provides expert perspectives and techniques to build security-compliant software by considering threats and vulnerabilities early in the development cycle. Additional topics to be covered include risk management and security testing.

Required Book:
Security for Software Engineers, By James Helfrich. CRC Press. ISBN: 978-1-138-58382-5

Course Objectives
Upon completion of this course, students will be able to:

1. Articulate the need for secure programming techniques
2. Identify and understand common software vulnerabilities and threats
3. Define secure programming concepts, techniques, and preventative measures
4. Identify key characteristics of secure code
5. Demonstrate effective use of design patterns for secure code by testing, editing, and debugging programs using secure programming techniques

Topics Covered:

1. Importance of security in software development
2. Proactive approaches to Software security
3. Identifying Common software vulnerabilities and threats
4. Techniques to help ensure the security of essential software by considering threats and vulnerabilities
5. Defining secure programming concepts, techniques, and preventative measures,
6. Secure software development best practices
7. Secure software development standards
8. Secure development Benefits
9. Identifying key characteristics of secure code.
10. Effective use of design patterns for secure code
11. Building software programs that help get security the first time.
12. Detecting and improving software developers' practices which cause security problems
13. Determining an acceptable level of risk, developing security tests, and plugging security holes

CYSE 440: Principles and Practices of Network Defense and Applied Network Monitoring

Course Description

This course equips students with the right tools for data collection, detecting malicious activity, and performing the intrusion detection analysis. This course follows the three stages of the network security monitoring cycle: collection, detection, and analysis. This course will describe how to define multiple analysis frameworks that can be used for performing network security monitoring investigations in a structured and systematic manner.

Course Textbook:

- “Applied Network Security Monitoring”, by Chris Sanders and Jason Smith, ISBN-13:978-0124172081
- “Network Defense and Countermeasures, Principle and practice”, by Chuck Easttom II, ISBN-13: 978-0789759962

Objectives

Students who complete this course should be able to perform the following tasks:

1. Discusses the proper methods for planning and executing an NSM data collection strategy
2. Understand and Apply the three main phases of Applied Network Monitoring (Data Collection, Threat Monitoring, and Threat Detection)
3. Describe Applied collection framework which is used for making decisions regarding what data should be collected using a risk-based approach
4. Define what Network Security Monitoring and is relevance in the modern security landscape
5. Describe the packet string (PSTR)and its usefulness during NSM analytics process
6. Describe the importance of full packet capturing of Data and examine different tools that allow full capture of PCAP data.
7. Describe threat detection mechanisms and identify indicators of compromises and signatures.
8. Describe the relation between detection mechanisms and indicators of compromises.
9. Describe the different types of detection techniques including Reputation-based Detection, Signature-Based Detection, Anomaly-Based Detection
10. Discuss the importance and application of canary honeypots as a threat detection tool.
11. Enhance the ability to interpret and decipher packet data that represents the network communication during Packet Analysis.

Topics Covered:

1. The Practice of Applied Network Security Monitoring
2. Planning Data Collection
3. The Sensor Platform
4. Session Data
5. Full Packet Capture Data
6. Packet String Data
7. Detection Mechanisms, Indicators of Compromise, and Signatures
8. Reputation-Based Detection
9. Signature-Based Detection with Snort and Suricata
10. The Bro Platform
11. Anomaly-Based Detection with Statistical Data
12. Using Canary Honeypots for Detection
13. Packet Analysis
14. Friendly and Threat Intelligence
15. The Analysis Process

CYSE 480: Advanced Info Security Assurance and Risk Control

Course Description:

This course provides the fundamental broad concepts reviews of the entire field of information security and assurance. The purpose of the course is to provide students with a comprehensive overview of the field of information security assurance and risk control. This course covers different security models and frameworks, risk management, access control mechanisms, understanding and implementation of intrusion detection and protection tools. This course also discusses and describe the underlying foundations of modern cryptosystems, examining both security personnel and security of personnel, and describing the ongoing technical and administrative evaluation and maintenance of the information security system.

Required Textbook:
Title: Principles of Information Security, 6th Edition.
Authors: Michael E. Whitman & Herbert J. Mattord
Publisher: Cengage Learning
ISBN: 9781337102063

Course Objectives
Upon completion of this course, students will be able to:

1. Define key terms and fundamental concepts of cyber defense used for system security.
2. Identify and describe information security vulnerabilities, threats, attacks, and risks.
3. Apply risk assessment methods to information security risk analysis.
4. Define and differentiate confidentiality, integrity, availability, access, identification, authentication authorization, audit, non-repudiation, and privacy.
5. Describe security life cycle, frameworks, and security models.
6. Explain intrusion detection and prevention systems and technology.
7. Describe access control models (MAC, DAC, BRAC) and authentication methods.
8. Identify system vulnerabilities and risks and corresponding security technologies and methods.
9. Use tools for vulnerability scanning and analysis.
10. Identify and evaluate information security tools, controls, and mechanisms.
11. Describe data security mechanisms and fundamentals of cryptography.
12. Evaluate business continuity planning and disaster recovery planning in a security framework.
13. Identify and describe key laws, ethics, and professional communities in information security.

Topics Covered:

1. Introduction to Information Security.
2. The Need for Security.
3. Legal, Ethical, and Professional Issues in Information Security.
4. Planning for Security.
5. Access control models (MAC, DAC, RBAC) and authentication methods.
6. Risk Management.
7. security life cycle, frameworks, and security models.
8. Security Technology: Firewalls, VPNs, and Wireless.
9. Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools.
10. Cryptography.
11. Physical Security.
12. Evaluation of Business Continuity and Disaster Recovery Planning in a Security Framework
13. Implementing Information Security.
14. Security and Personnel.
15. Information Security Maintenance and eDiscovery.

CYSE 498 Cybersecurity Capstone I

Course Description
This course covers the first part of the Cybersecurity Capstone course work. Students are expected to work with their project advisor (instructor) to come up with a cybersecurity project topic, prepare a white paper of their project review, project plan, design, and the presentation of prototype, and the direction and expectation of the remaining project work.

Course Objectives:

Students who complete this course should be able to perform the following tasks:

1. Demonstrate a knowledge of research techniques and literature survey skills by investigating the feasibility of a proposed project and its societal implications.
2. Know how to plan, propose, and prepare to implement a new project in the discipline.
3. Demonstrate communication skills and public speaking skills through written and oral presentations
4. Learn proposal development skills to initiate an application-oriented or research-based project in the discipline.

Topics Covered:

1. Learning new topics and vocabularies by employing proven research techniques. (Students learn new vocabularies in diverse research fields.)
2. Understanding the current state-of-the-art in the discipline by finding relevant information, knowledge, and learning resources to make the planning project successful.
3. Planning and proposing a new project using sound analysis and design principles in visualizing the project.
4. Learn to find, read, and summarize. relevant technical literature.
5. Writing the project proposal and understanding standard procedures of footnoting, referencing, and symbol usage in a technical paper.
6. Skillful communication skills. (Enhance the ability to skillfully communicate on a technical subject to an audience less knowledgeable than the author by providing rich evidence to the senior project.)

CYSE 499 Cybersecurity Capstone II

Course Description
This course covers the second and major part of the Cybersecurity Capstone course work and it is the continuation of CYSE 498. Students are expected to work with their project advisor (instructor) to complete the cybersecurity project by discussing their research result, achievement, challenges, limitations, any other future work. They are expected to submit the final research paper.

Course Objectives:

Students who complete this course should be able to perform the following tasks:

1. Design and develop a cybersecurity-oriented or research-based project of significant complexity in the discipline.
2. Understand the professional, ethical, and social aspects of cybersecurity design and principles.
3. Prepare a presentation, oral or written (including poster) of their project and deliver to an audience of faculty and peers.

Topics Covered:

1. Learn how to write a polished research paper by following IEEE or ACM research paper templates.
2. Understanding standard procedures of footnoting, referencing, and symbol usage
3. Writing a comprehensive project report.
4. Skillful communication (Enhance the ability to skillfully communicate on a technical subject to an audience less knowledgeable than the author by providing rich evidence to the senior project.)