# ITS 222 Enterprise Security

| | |
|---|---|
| Rubric: ITS | Term: Fall 2022 |
| Number: 222 | Credits: 3 |
| Section: 01 | Lecture: MC 25 MW 11:00-11:50 AM |
| CRN: 72158 & 74338 | Lab: MC 25 Tuesday 11:00AM – 12:20 PM |

### Instructor Information

Name: Jeff Arends

Email: jeffrey.arends@mso.umt.edu

Office: MC 324

Office Hours (or by appointment):

| Day | Hours |
|---|---|
| Monday | 2-3 PM |
| Tuesday | 2-3 PM |
| Wednesday | 2-3 PM |
| Thursday | 2-3 PM |
| Friday | By Appointment |

### Course Description

Examination of general information technology security concepts. Topics include access control, authentication, attack methods, remote access, web security, wireless networks, cryptography, internal infrastructure security, and external attacks. Security procedures, organizational policies, risk management and disaster recovery addressed.

Aligns with Center for Academic Excellence Knowledge Units:

- Cyber Foundations
- Cyber Principles
- Cyber Threats
- Cyber Security Planning
- Security Program Management
- Risk Analysis
- Basic Cryptography

### Course Outcomes

1. Cybersecurity fundamentals

a. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
b. Define the principles of Cybersecurity.
c. Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
d. Properly use the Vocabulary associated with cybersecurity

2. Attacks, Threats, and Defense
   a. Describe different types of attacks and their characteristics.
   b. Describe potential system attacks and the actors that might perform them.
   c. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
   d. Describe appropriate measures to be taken should a system compromise occur.
   e. Analyze common security failures and identify specific design principles that have been violated.
   f. Given a specific scenario, identify the design principles involved or needed.
3. Security Planning
   a. Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms
   b. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk
   c. Examine the placement of security functions in a system and describe the strengths and weaknesses
   d. Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.
   e. Develop system specific plans for:
      i. The protection of intellectual property
      ii. The implementation of access controls
      iii. Patch and change management
   f. Apply their knowledge to develop a security program, identifying goals, objectives and metrics
   g. Apply their knowledge to effectively manage a security program.
   h. Assess the effectiveness of a security program.
4. Risk Analysis
   a. Describe how risk relates to a system security policy.
   b. Describe various risk analysis methodologies
   c. Evaluate and categorize risk
      i. with respect to technology
      ii. with respect to individuals, and
      iii. in the enterprise, and recommend appropriate responses.
   d. Select the optimal methodology based on needs, advantages and disadvantages.
5. Outline and explain the roles of personnel in planning and managing security, including:
   a. Board of Directors
   b. Senior Management
   c. Chief Information Security Officer (CISO)
   d. IT Management (CIO, IT Director, etc)
   e. Functional Area Management
   f. Information Security personnel
   g. End users

6. Basic Cryptography
    a. Students will be able to identify the elements of a cryptographic system.
    b. Students will be able to describe the differences between symmetric and asymmetric algorithms.
    c. Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
    d. Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.

| Unit | Chapter | KU Topics | Labs: |
|---|---|---|---|
| Security Basics | Security Essentials Chapter 1 | • Vulnerabilities and Risk management (include backups and recovery)<br>• Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy<br>• Security Life-Cycle<br>• Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)<br>• Legal Issues associated with cyber threats | Lab 1: Lavender_2022: Security Reports, Lab 2: Lavender_2022: Compliance, Lab 3: Lavender_2022 CIS Framework |
| Defining the Threats | Security Essentials Chapter 2 | • Threats and Adversaries (threat actors, malware, natural phenomena)<br>• The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)<br>• Types of Attacks (and vulnerabilities that enable them)<br>• Motivations and Techniques<br>• Threat Information Sources (e.g., CERT)<br>• Common Attacks<br>• Social Engineering<br>• Attack surfaces / vectors, and trees<br>• Password guessing / cracking<br>• Backdoors / trojans / viruses / wireless attacks<br>• Sniffing / spoofing / session hijacking<br>• Denial of service / distributed DOS / BOTs<br>• MAC spoofing / web app attacks / 0-day exploits<br>• Advanced Persistent Threat (APT)<br>• Attack Timing (within x minutes of being attached to the net)<br>• Covert Channels | Lab 1: Lavender_2022: Free Antimalware, Lab 2: Lavender_2022, Macros, Lab 3: Lavender_2022: Weak Configurations |
| Security Evaluation Techniques | Security Essentials Chapter 3 | • Malicious activity detection / forms of attack<br>• Events that indicate an attack is/has happened | Lab 1: Lavender_2022: Nessus Vulnerability Scanning, Lab 2: |

| | | | |
|---|---|---|---|
| | | | Lavender_2022: Performance Monitoring, Lab 3: Lavender_2022: Syslog, Lab 4: Lavender: Event logging with PowerShell |
| Access Management | Security Essentials Chapter 4 | • Access Control Models (MAC, DAC, RBAC, Lattice)<br>• Managing the implementation of access controls | Lab 1: Lavender_2022: Local Password Policy, Lab 2: Lavender_2022: NTFS and Combined NTFS Share Permissions |
| Physical Security | Security Essentials Chapter 5 | • Insider problem<br>• Layering (Defense in depth) | Lab 1: Lavender_2020: Implementing Security Controls, Lab 2: Lavender_2022: Viewing and recovering Deleted Files |
| Host and Server Security | Security Essentials Chapter 6 | • Appropriate Countermeasures<br>• Managing patch and change control<br>• | Lab 1: Lavender_2022: Windows Services, Lab 2: Lavender_2022: Secure Workstation Policies |
| Application and Development Security | Security Essentials Chapter 7 | • Session Management<br>• Exception Management<br>• Security Mechanisms (e.g., Identification/Authentication, Audit) | Lab 1: OWASP Questions, Lab 2: Juice Shop |
| Soft Skills | Security Essentials Chapter 19 | • Ethics (Ethics associated with cybersecurity profession)<br>Legal Issues associated with cyber threats | Project: Promoting Cybersecurity Awareness |
| Device Security | Security Essentials Chapter 8 | | Lab 1: Lavender_2022: Drive Encryption |
| CLI | Security Essentials Chapter 11 | • | Lab1: Lavender_2022: |

|  |  |  |  |
|---|---|---|---|
|  |  |  | System Management with Windows PowerShell |
| Basic Cryptography | Security Essentials Chapter 9 & 10 | • Common cryptographic uses<br>○ Security Functions (data protection, data integrity, authentication, non-repudiation)<br>○ Block vs. stream data<br>○ Digital Signatures (Authentication)<br>• Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)<br>• Integrity checking<br>• For protecting authentication data<br>• Collision resistance<br>• Symmetric Cryptography (DES, Twofish)<br>• Public Key Cryptography (Diffie-Hellman, RSA, ECC, ElGamal, DSA)<br>• Public Key Infrastructure<br>• Certificates<br>• Key Management (creation, exchange/distribution)<br>• Cryptography in practice<br>• Common Cryptographic Protocols<br>• DES -> AES (evolution from DES to AES)<br>• Cryptographic Modes (and their strengths and weaknesses)<br>• Cryptographic standards (FIPS 140 series)<br>• Cryptographic failures<br>• Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)<br>• Applications of Cryptography and PKI<br>• Implementation failures<br>• Data Security (in transmission, at rest, in processing) | Lab 1: Lavender_2022: Symmetric Encryption, Lab 2: Lavender_2022: Asymmetric Encryption, Lab 3: Lavender_2022: Viewing Web Security and Certificate Information |
| Secure Networks: Design and Admin | Security Essentials Chapter 12 & 13 | • Separation (of domains/duties)<br>• Isolation<br>• Encapsulation<br>• Modularity<br>• Simplicity of design (Economy of Mechanism)<br>• Minimization of implementation (Least Common Mechanism)<br>• Open Design<br>• Complete Mediation<br>• Layering (Defense in depth)<br>• Least Privilege<br>• Fail Safe Defaults / Fail Secure<br>• Least Astonishment (Psychological Acceptability)<br>• Minimize Trust Surface (Reluctance to trust)<br>• Usability | Lab 1: Lavender_2022: Using iptables, Lab 2: Lavender_2022: Ping Sweep |

| | | | |
|---|---|---|---|
| | | • Trust relationships | |
| Wireless Networks | Security Essentials Chapter 14 | | Lab 1: Lavender_2022: Analyzing Wireless Activity Packets |
| The Cloud | Security Essentials Chapter 15 | | Lab 1: Lavender_2022: Combatting VM Sprawl |
| Governance and Risk | Security Essentials Chapter 16 & 18 | • Measuring the effectiveness of a security program (metrics).<br>• Roles and Responsibilities of the Security Organization<br>• Security Policies.<br>○ Compliance with Applicable Laws and Regulations<br>○ Security best practices and frameworks.<br>• Security Baselining<br>• Program Monitoring and Control<br>• Awareness, Training and Education<br>• Security program addresses:<br>○ Physical Security<br>○ Personnel Security<br>○ System and Data Identification<br>○ System security plans.<br>○ Configuration and Patch management<br>○ System Documentation<br>○ Incident Response Program<br>○ Disaster Recovery Program.<br>○ Certification and Accreditation<br>• Basic Risk Assessment Risk Assessment/Analysis Methodologies<br>• Risk Measurement and Evaluation Methodologies<br>• Risk Management Models<br>• Risk Management Processes<br>• Risk Mitigation Economics<br>• Risk Transference/Acceptance/Mitigation<br>• Communication of Risk<br>• Broad coverage of the cybersecurity Common Body of Knowledge (CBK) and how it affects planning and management.<br>• Differentiate and provided examples of Operational, Tactical, and Strategic Planning and Management<br>• Examine C-Level Functions which impact cybersecurity.<br>• Making cybersecurity a strategic essential (part of core organizational strategy)<br>• Identify requirements and create plans for Business Continuity / Disaster Recovery | Lab 1: Lavender_2022: Evaluating User Training, Lab 2: Lavender_2022: Use Training through Interactive Labs, Lab 3: Lavender_2022: Business impact analysis, Lab 4: Lavender_2022: RAID Systems |

|  |  |  |  |
|---|---|---|---|
|  |  | • Planning for protection of intellectual property<br>• Legal issues |  |
| Incident Response | Security Essentials Chapter 17 | • Develop processes and procedures for incident response | Lab 1: Lavender_2022: Incident Response and Digital Forensics, Lab 2: Lavender_2022: Metadata |

## Resources

Textbook: Security Essentials. 2022. Linda K. Lavender. Published by G-W Publishing. ISBN: 978-1-64564-637-2 (printed textbook)/ 978-1-64564-639-6 (printed lab manual). (referred to as Lavender_2022)

## Grading:

Grading is based on a simple point accumulation (i.e. score). Any score above the passing score will get at least a C.

Grading Categories:

- Exams: There will be one midterm exam and one comprehensive final exam. These must be taken at the scheduled time except with prior approval or extenuating circumstances.
- Homework: Homework will consist of labs assigned in Moodle. Homework is graded in the following manner: Mostly complete (more than 85% complete) = full credit; Partial Credit (less between half complete and 85% complete) = 60% credit; Incomplete (Missing or less than 50% complete) = no credit). Homework will not be graded in detail. If you have questions about homework please ask those questions in lab or in the forum.
- Projects: There will be multiple projects during the semester representing larger tasks. Each project will explain the criteria by which it will be graded and due dates.
- Quizzes: Quizzes are graded automatically in moodle.

Due Dates and Late Policy. Different than prior semesters I have decided to implement a strict deadline policy as allowing late work tends to cause a domino affect of missing assignments. As such, the due date for all assignments are set to a Wednesday (designated in Moodle). Every day after Wednesday 10% is deducted from the total possible points for the assignment. After the following Sunday, the assignment is no longer accepted. In other words, make every effort to turn in work on time or risk losing credit for the assignment. Extenuating circumstances and prior consent are the only means to extend the deadlines.

## Disability Statement

The University of Montana assures equal access to instruction through collaboration between students with disabilities, instructors, and the Office for Disability Equity (ODE). If you anticipate or experience barriers based on disability, please contact the ODE at: (406) 243-2243, ode@umontana.edu, or visit www.umt.edu/disability for more information. Retroactive accommodation requests will not be honored, so please, do not delay. As your instructor, I will work with you and the ODE to implement an effective accommodation, and you are welcome to contact me privately if you wish.

**Scholarly Conduct**

- All students must practice academic honesty. Academic misconduct is subject to an academic penalty by the course instructor and/or a disciplinary sanction by the University. All students need to be familiar with the Student Conduct Code.
- Plagiarism, cheating, or direct use of online resources without proper attribution will result in a deduction of points no less than 20% of the total points for the assignment to a zero on the assignment at the instructor's discretion.
- All students are expected to respect the opinions and dignity of all members of the class and act in a dignified manner.
- Every effort will be made to accommodate disabilities. Please inform me of any issues.

**Safety Considerations:** Given the current circumstances with COVID-19 please keep in mind the following:

- Please wear a mask within the classroom.
- Cleaning kits are available. Please make use of these and clean your space at the start of class and the end of class.
- Please avoid congregating before or after class.
- Please sit in the same seat for all semester.
- Food and drink are strongly discouraged within classrooms.
- If you feel sick stay home and attend class remotely