**MST Course – Cybersecurity Fundamentals**

**Lecture: Distance Education**

**Instructor:** Dr. Sihua Shao
**Office:** Workman 209
**Phone:** 575-835-5932
**E-mail:** sihua.shao@nmt.edu

**Course Description:**
Cybersecurity Fundamentals is a comprehensive course tailored for high-school level teachers, empowering them with the necessary knowledge and skills to instruct students on safeguarding internet-connected systems from vulnerabilities and cyber-attacks. The course delves into a range of topics, such as cybercrimes, cyber ethics, Linux basics, networking technologies, essential cybersecurity terminology, an introduction to hacking, cryptography principles and applications, social engineering attacks, penetration testing, and vulnerability assessment tools. Additionally, the course incorporates hands-on practice using Kali Linux OS to reinforce the concepts covered in the lectures.

**Course Learning Outcomes**:
Upon successfully completing this course, students will be able to:

- Gain a solid understanding of cyber ethics and relevant cyber laws.
- Master basic Linux OS commands and acquire basic knowledge of network technologies.
- Familiarize themselves with key cybersecurity and hacking terminology.
- Apply basic ciphers, encryption techniques, and steganography in cybersecurity.
- Configure and utilize various social engineering tools within the Kali Linux OS.
- Conduct ethical penetration tests in compliance with relevant laws and guidelines.
- Employ widely-used tools for conducting introductory vulnerability assessments.

**MST Program Learning Outcomes**: https://nmt.edu/academics/psych-ed/graduate.php

**Lectures:**

- Chapter 1: Legal and Ethical Issues in Cybersecurity
- Chapter 2: Linux Basics
- Chapter 3: Networking Technology Basics
- Chapter 4: Essential Cybersecurity Terminology
- Chapter 5: Introduction to Hacking
- Chapter 6: Cryptography Principles and Applications
- Chapter 7: Social Engineering Attacks
- Chapter 8: Penetration Testing
- Chapter 9: Vulnerability Assessment

**Homework**:
A total of nine homework assignments will be given, with one corresponding to each chapter topic. Homework submissions should be in PDF format via Canvas by the specified deadline. If students cannot meet a deadline, they must contact the instructor immediately.

**Lab**:
A total of nineteen labs will be conducted throughout the course, with one to three labs dedicated to each chapter topic. Lab submissions will be made through the NICE Challenge Webportal (https://portal.nice-challenge.com/login). Instructors are responsible for reserving labs, and each reservation can span a maximum of two days. To complete a lab, students are required to send a lab reservation request to the instructor (sihua.shao@nmt.edu), specifying the lab and preferred dates (e.g., request for Backdoor/Trojan Lab 1 on Feb. 1 and Feb. 2). Discussions on the lab requirements can be initiated in the lab reservation request. Students may attempt each lab multiple times, with only their highest score counting toward the final grade. Personalized and constructive feedback is provided for labs through Zoom meetings.

**Project**:
One course project will be assigned, requiring students to create their own syllabus based on the material covered throughout the course. Project submissions should be in PDF format via Canvas by the specified deadline. If students cannot meet the deadline, they must contact the instructor immediately.

**Grading**:

- Homework: 40%
- Lab: 40%
- Course Project: 20%

| | | | |
|---|---|---|---|
| A | 90-100 | C | 70-72 |
| A- | 86-89 | C- | 66-69 |
| B+ | 83-85 | D+ | 63-65 |
| B | 80-82 | D | 60-62 |
| B- | 76-79 | F | <60 |
| C+ | 73-75 | | |

## Modular Course Schedules

### Chapter 1. Legal and Ethical Issues in Cybersecurity (HW1)

| | |
|---|---|
| Module 1.1: Understanding Cybercrime | In this module, we will discuss the definition, history, and various types of cybercrime. We will examine the challenges in defining and prosecuting cybercrime and why it necessitates a separate category. Additionally, we will outline current cybercrime trends and suggest several strategies to combat cybercrime effectively. |
| Module 1.2: Addressing Ethical Issues in Cybersecurity | In this module, we will explore the distinctions between law and ethics, as well as between religion and ethics. We will identify non-universal ethical principles and discuss ethical pluralism. Through consequence-based and rule-based ethical principles, we will learn how to assess situations for ethical issues in the context of cybersecurity. |

| | |
|---|---|
| Module 1.3: Analyzing Incidents with Ethical Considerations | In this module, we will review multiple case studies to understand how ethics influence professional actions in cybersecurity. Each case study is designed to highlight specific ethical points, such as use of computer services, privacy rights, fraud, and ethics of hacking or cracking. |
| Module 1.4: Ethical Hacking, Certification, and Cyber Laws | In this module, we will define ethical hacking and discuss common terminology used to differentiate between regular hackers and ethical hackers. We will present certification exams available for ethical hackers and explore the legal aspects of ethical hacking in the context of diverse cyber laws across different jurisdictions. |

**Chapter 2. Linux Basics (HW2)**

| | |
|---|---|
| Module 2.1: Linux Overview and File System Exploration | In this module, we will introduce the Linux OS, discussing its use cases, advantages compared to other operating systems, and the Linux command line. We will use the Linux command line to navigate the filesystem, including working with directories and text files, reading files, and moving/copying files. |
| Module 2.2: Linux Command Line | In this module, we will delve deeper into the Linux command line, exploring options/flags, superuser privileges, searching for strings and files, changing file ownership and permissions, and writing to the system's log. |
| Module 2.3: Labs | In this module, one lab will be covered: i) Display Matrix lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 3. Networking Technology Basics (HW3)**

| | |
|---|---|
| Module 3.1: Understanding Key Networking Terminology | In this module, we will introduce essential networking terminology, including network interface, local area network (LAN), wide area network (WAN), packet, host, hub, switch, router, protocols, ports, MAC address, IP address, domain name system (DNS), etc. |
| Module 3.2: Exploring the Open Systems Interconnection (OSI) Model | In this module, we will delve into the 7-layer OSI model, covering the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer. A brief comparison to the 4-layer TCP/IP model will also be discussed. |
| Module 3.3: TCP/IP Network Architecture | In this module, we will concentrate on the TCP/IP architecture. We will explore how the layers work together under the TCP/IP network protocols. To better understand how packets are routed in the internet layer, IP addressing and subnet addressing will be discussed. |
| Module 3.4: Labs | In this module, two labs will be covered: i) ip/ifconfig lab and ii) Wireshark lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will |

| | |
|---|---|
| | be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 4. Essential Cybersecurity Terminology (HW4)**

| | |
|---|---|
| Module 4.1: Introduction to Cybersecurity, Challenges, and Careers | In this module, we will provide an overview of cybersecurity and briefly discuss its challenges. We will address commonly recognized major cybersecurity issues and introduce careers in the cybersecurity field, including real job opportunities with job titles, descriptions, and salaries. |
| Module 4.2: Understanding Cyber Attacks | In this module, we will present three different types of hackers: white hat, gray hat, and black hat hackers. We will also introduce the fundamentals of attack analysis and discuss the top 10 cyber attacks in today's internet environment. Towards the end of this module, we will introduce some tools for combating attacks. |
| Module 4.3: Email, Passwords, and Cloud Security | In this module, we will engage in extensive discussions on email exchange mechanisms and password creation. We will learn how to identify compromised emails and how to strengthen our passwords. Additionally, we will provide a high-level analysis of the pros and cons of cloud services. |
| Module 4.4: Labs | In this module, two labs will be covered: i) Passwords lab and ii) Denial of Service Attack lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 5. Introduction to Hacking (HW5)**

| | |
|---|---|
| Module 5.1: Introduction to Hacking | In this module, we will provide a brief overview of hacking history, from the first documented use of the term "hacking" to the latest trends. We will clarify commonly used terms related to hacking, such as cracking, phreaking, spoofing, and Denial of Service (DoS). Additionally, we will discuss the various types of hackers and their motivations. |
| Module 5.2: Exploring Different Types of Malwares | In this module, we will introduce various types of malware, including viruses, worms, ransomware, crypto-malware, trojan horses, backdoors, RATs, rootkits, keyloggers, adware/spyware, botnets, and logic bombs. We will also suggest protective measures against malware. |
| Module 5.3: Understanding Attack Surface Basics | In this module, we will present the fundamentals of attack surfaces, encompassing types, measurements, and scopes of interactions. We will cover interactions through wireless channels using multiple examples. Furthermore, we will discuss the four-point process for analyzing porosity and its analogy to examining a sick person. |

| | |
|---|---|
| Module 5.4: Labs | In this module, three labs will be covered: i) Backdoor/Trojan lab 1 - Reverse HTTP, ii) Backdoor/Trojan lab 2 - Reverse TCP, and iii) Keylogger lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 6. Cryptography Principles and Applications (HW6)**

| | |
|---|---|
| Module 6.1: Cryptography Concepts and Related Attacks | In this module, we will introduce the concepts of encryption, authentication, digital signatures, and public key infrastructure. Additionally, we will discuss various attacks against encryption schemes. |
| Module 6.2: Cryptography Systems, Hash Functions, and Cryptographic Protocols | In this module, we will present two fundamental types of cryptographic systems: symmetric key encryption and asymmetric key encryption. We will also explore the operating principles, properties, examples, and applications of hash functions. Furthermore, we will examine the messages and steps involved in cryptographic protocols. |
| Module 6.3: Simple Encryption Models and Block Ciphers | In this module, we will learn about simple ciphers, such as Caesar Cipher, Transposition Cipher, Exclusive OR Cipher, and Vernam Cipher. We will also discuss the definition of block ciphers, attacks related to block ciphers, and some classic block cipher algorithms. |
| Module 6.4: Labs | In this module, three labs will be covered: i) Pass the Hash lab, ii) Dictionary Attack lab, and iii) Brute Force and Rainbow Table lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 7. Social Engineering Attacks (HW7)**

| | |
|---|---|
| Module 7.1: Understanding Social Engineering | In this module, we will introduce the definition and applications of social engineering. We will also discuss the social engineering life cycle and the type of tools used in social engineering attack. |
| Module 7.2: Information Collection and Social Engineering Attacks | In this module, we will explore both technical and non-technical information collection methods, as well as classic social engineering attacks such as phishing, pretexting, baiting, quid pro quo, and tailgating. We will also learn how to identify common social engineering attacks. |
| Module 7.3: Social Engineering Tools and Mitigation | In this module, we will examine three categories of social engineering tools: physical tools, software tools, and phone tools. We will also learn how to mitigate social engineering attacks. |

| | |
|---|---|
| Module 7.4: Labs | In this module, three labs will be covered: i) Credentials Harvester Attack lab, ii) Phishing Attack lab, and iii) Clickjacking Attack lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 8. Penetration Testing (HW8)**

| | |
|---|---|
| Module 8.1: Ethical Hacking Basics and Penetration Test Phases | In this module, we will discuss the general models and steps employed by ethical hackers during penetration tests. Additionally, we will briefly introduce the four phases of a penetration test, with an emphasis on Phase I – Reconnaissance, and Phase II – Scanning. |
| Module 8.2: Phase III – Exploitation and Privilege Escalation | In this module, we will concentrate on Phase III – Exploitation. After gathering sufficient information in Phases I and II, the ethical hacker attempts to take control of a system during the Exploitation phase. We will explore one aspect of exploitation – privilege escalation, along with concepts such as authentication, access control, and account types. |
| Module 8.3: Exploitation Tools, Examples, and Post-Exploitation Phase | In this module, we will conclude our discussion of the Exploitation phase by examining commonly used tools and presenting various exploitation examples. Following the completion of the final informal phase, Phase IV – Post-Exploitation and Maintaining Access, a detailed and comprehensive summary report will be generated. |
| Module 8.4: Labs | In this module, two labs will be covered: i) Privilege Escalation lab and ii) Local Area Network (LAN) Sniffing lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |

**Chapter 9. Vulnerability Assessment (HW9)**

| | |
|---|---|
| Module 9.1: Introduction to Vulnerability Assessment Basics | In this module, we will define vulnerability assessment (VA) and discuss its benefits. We will also introduce VA-related terms such as false positives and false negatives. The four general steps of VA will be presented along with instructive examples. Additionally, we will delve into vulnerability scanning and its various types. |
| Module 9.2: Evaluating Vulnerability Assessment Tools | In this module, we will delve into the key metrics and criteria frequently employed to assess the effectiveness of VA tools. Discussion will encompass vulnerability service tools and testing methods. We will further differentiate between two types of VA service tools, specifically those designed for static code analysis and those tailored for dynamic program analysis. |

| | |
|---|---|
| Module 9.3: Popular Vulnerability Assessment Tools | In this module, we will introduce some of the most frequently used VA tools, such as network/port scanners and vulnerability scanners. We will elaborate on widely used VA tools, including Wireshark, SolarWinds, NMAP, and Nessus, with extensive examples. We will also provide URLs for downloading certain VA tools that are not pre-installed on the Kali Linux operating system. |
| Module 9.4: Web Application Vulnerabilities and Secure Configurations | In this module, we will examine cases of exploiting web application vulnerabilities, such as code injection, cross-site scripting, and cross-site request forgery. We will delve into network instruction detection and prevention policies, along with their respective rules. Finally, we will tackle system hardening and secure deployments, covering these subjects through high-level concepts. |
| Module 9.5: Labs | In this module, three labs will be covered: i) SQL Injection lab, ii) Cross-Site Scripting (XSS) lab, and iii) Command Injection lab. Students will be guided through each step, with checkpoints provided for evaluating their progress. Lab exercises will be available on the NICE Challenge platform, utilizing an HTML5 web console for practice. |