MST Course – Cybersecurity Fundamentals
Fall, 2022
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 developed to prepare primarily high-school level teachers to deliver a course that uses Kali Linux OS to teach the basics of protecting Internet-connected systems from passive vulnerabilities as well as cyber-attacks. Topics include definitions of fundamental cybersecurity terminologies, what to hack and how to hack, principles and applications of cryptography, different forms of social engineering attack, how to perform penetration tests as an ethical hacker, and the basics of vulnerability assessments.

Course Learning Outcomes:
After completion of this course, students are expected to be able to:

- Identify the definition of cybersecurity, cyber ethics, and cyber-attacks
- Identify different categories of hackers and understand vulnerabilities
- Learn the simple ciphers, simple encryption models, and steganography
- Identify the definition of social engineering and introduce the social engineering tool in Kali Linux system.
- Perform penetration test according to ethical hacking laws
- Use the common tools to perform introductory vulnerability assessment

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

Lectures:

- Chapter 1: Cybersecurity Terms and Definitions
- Chapter 2: Hacking
- Chapter 3: Cryptograph
- Chapter 4: Social Engineering
- Chapter 5: Penetration Testing
- Chapter 6: Vulnerability Assessment

Homework:
There will be a total of 6 homework with 1 homework assigned to each chapter. The submission of homework will be done via Canvas as PDF files. Homework must be submitted by the posted deadline. If you are unable to meet a deadline, get in touch with the instructor immediately.

Lab:
There will be a total of 18 labs with 3 labs assigned to each chapter. The submission of labs will be done via NICE Challenge Webportal (https://portal.nice-challenge.com/login). Lab reservation must be done by the instructor. Each lab reservation can only span two days. To complete the labs, you

need to send an email to the instructor (sihua.shao@nmt.edu) to request for the reservation. In the request, specify the lab and dates (e.g., request for Backdoor/Trojan Lab 1 on Feb. 1 and Feb. 2).

Project:
There will be one course project. The project requires you to design your own syllabus based on the materials covered in the course. The submission of project will be done via Canvas as PDF files. Project must be submitted by the posted deadline. If you are unable to meet a deadline, get in touch with 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. Introduction to Cybersecurity (HW1)

Module 1.1: Defining Cybersecurity and Challenges of Cybersecurity	In this module, we will introduce what cybersecurity is and challenges of cybersecurity briefly. To achieve cybersecurity, the students will understand the current technology (hardware and software), programming languages and operating systems, social influences, legal and ethical issues and public policies.
Module 1.2: Cyber Crime, Cyber Ethics and Cybersecurity Career	This module will help students understand what cybercrime is. It covers the nature of cybercrime, some of the impacts, and cyber ethics. Most of the subtopics here should be discussion-based and will be more impactful to students if they are allowed to research some of the examples and information themselves. We will also introduce the career in the cybersecurity field. We will show some real job opportunities for cybersecurity which include the job title, job description, and the salary. Top 5 areas where cyber security skills are needed will also be talked about.
Module 1.3: Cyber Attacks	In this module, we will tell students who a hacker is. Three different types hackers will be introduced white hat hacker, gray hat hacker and black hat hacker. The attack analysis process will be also introduced. We will also talk about the top 10 cyber-attacks in today's internet environment. Some tools for fighting attacks will be introduced at last of this module.
Module 1.4: Passwords	In this module, we will introduce some password cracking methods and how to choose a good password, and how to be more cyber secure.
Module 1.5: Labs	In this module, we will go over three labs – i) Display Matrix lab, ii) IP- Ifconfig lab, and iii) Passwords lab, step by step with checkpoints

	provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.

Chapter 2. Hacking (HW2)

Module 2.1: Introduction to Hacking	In the first module, we will briefly introduce the history of the hacking, from the first documented use of the word "hacking" to the most recent hacking patterns. The commonly used terms that are similar to hacking will be clarified, such as cracking, phreaking, spoofing, and Denial of Service (DoS). We will also discuss different types of hackers and their various hacking motivations.
Module 2.2: What to Hack (Malware)	In the second module, we will briefly introduce the different types of malwares, such as viruses, worms, ransomware, crypto-malware, trojan horse, backdoor, RATs, rootkit, keylogger, adware/spyware, botnets and, logic bomb. Protections against malware will be suggested.
Module 2.3: What to Hack (Email, Password, and Cloud)	In the third module, extensive discussions will be performed on the mechanism of email exchange and password formation. We will learn how to identify the compromised email and how to strengthen our passwords. In addition, a high-level analysis of the pros and cons of cloud services will be covered.
Module 2.4: How to Hack.	In the fourth module, we will introduce the basis of attack surface, including types, measure, and scope of interactions. The interaction through wireless channels will be covered with multiple paradigms. Four-point process analyzing porosity and its analogy to analyzing a sick person will be discussed. Moreover, we will cover IP address, fundamental Linux terminal commands, and ping command-based detection and attacks.
Module 2.5: Labs	In the fifth module, we will go over three labs – i) backdoor attack using reverse HTTP, ii) backdoor attack using reverse TCP, and iii) javascript keylogger attack, step by step with checkpoints provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.

Chapter 3. Cryptography (HW3)

Module 3.1: History of Cryptography and Components of a Cryptosystem	In this module, we will introduce the history of cryptography briefly, talk about some components of a cryptosystem such as plaintext, encryption algorithm, cipher, decryption algorithm, encryption key and decryption key. Cryptography is a method of protecting information from unauthorized users using codes or ciphers. When we send the encrypted message, the original message will be read or processed by only the intended user(s).
Module 3.2: Simple	In this module, we will introduce Caesar Cipher, Whitfield Diffie and

Encryption Models.	Martin Hellman Model, Transposition Cipher, Vernam or Exclusive OR Cipher and Vigenere Cipher.
Module 3.3: Types of Cryptography Systems and Protocols for Secure Communication	In this module, we will introduce two fundamental types of cryptographic systems. One is Symmetric Key Encryption. Another one is Asymmetric Key Encryption. We will also talk some challenges to contemporary encryption. After that, we will introduce three common encryption methods. They are hashing, digital signatures and digital certificates. We also will introduce TCP/IP, HTTP, HTTPS, Pretty Good Privacy (PGP), Secure Multipurpose Internet Mail Extension (S-MIME), Secure Socket Layer (SSL), Secure file transfer protocol (SFTP) and Data Encryption Standards (DES).
Module 3.4: Steganography	In this module, the student will learn what Steganography is. Steganography literally means covered writing. Steganography takes one piece of data and hides it within another object (message, image, or other file).
Module 3.5: Labs	In this module, we will go over three labs – i) Pass the Hash lab, ii) Dictionary Attack lab, and iii) Brute Force and rainbow table lab, step by step with checkpoints provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.

Chapter 4. Social Engineering (HW4)

Module 4.1: Definitions of Social Engineering	In this module, we will introduce what social engineering is briefly. Both dictionary and internet definitions for social engineering will be talked.
Module 4.2: Why Use Social Engineering	In this module, we will introduce the social engineering life cycle and what a social engineering attack looks like. The students will also know how to spot an attack.
Module 4.3: Social Engineering Attacks	In this module, we will introduce some of popular social engineering attacks such as phishing, pretexting, baiting, quid pro quo and tailgating. We also will talk about some solution for these attacks.
Module 4.4: Policies and Training	In this module, the students will learn some basic rules for making a security policy for business. The students will also know how important the security to all of employees for a company.
Module 4.5: Labs	In this module, we will go over three labs – i) Credentials Harvester Attack lab by using social engineering tools, ii) Phishing Attack lab by using social engineering tools, and iii) Clickjacking Attack lab by using social engineering tools, step by step with checkpoints provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.

Chapter 5. Ethical Hacking and Penetration Testing (HW5)

Module 1: Ethical Hacker Basics and Phases of a Penetration Test.	In the first module, we will introduce the definition of ethical hacking and some commonly used terminologies to distinguish a regular hacker and an ethical hacker. We will cover the general models adopted and steps followed by an ethical hacker for a penetration test. We will also briefly introduce the four phases in a penetration test with further discussions about Phase I – Reconnaissance and Phase II – Scanning.
Module 2: Phase III – Exploitation (e.g., Privilege Escalation)	In the second module, we will focus on Phase III – Exploitation. Once enough information is collected in Phase I & II, in Exploitation phase, the ethical hacker attempts to gain the control over a system. We will cover one paradigm of exploitation – privilege escalation, with the concepts of authentication, access control, and account types.
Module 3: Exploitation Tools, Examples, and Post Exploitation Phase.	In the third module, we will wrap up the discussions on Exploitation phase with some commonly used tools. We will also enumerate several exploitation examples. After completing the last informal phase, Phase IV – Post Exploitation and Maintaining Access, a thorough and comprehensive summary report will be generated.
Module 4: Certification, Cyber Laws, and Risk Assessment.	In the fourth module, we will introduce the certification tests for ethical hackers. We will also discuss the legality of ethical hacking and geographically diverse cyber laws with two case studies. The application of penetration test, such as risk assessment, will be covered.
Module 5: Labs	In the fifth module, we will go over three labs – i) analyze packets using wireshark, ii) local area network (LAN) sniffing, and iii) privilege escalation, step by step with checkpoints provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.

Chapter 6. Vulnerability Assessment (HW6)

Module 1: Vulnerability Assessment Basics.	In the first module, we will introduce the definition and benefits of vulnerability assessment (VA). VA terms - false positive and false negative will also be introduced. Four general VA steps will be discussed with some instructive examples. Further discussion will be provided about vulnerability scanning and types.
Module 2: VA Tools Evaluation.	In the second module, we will introduce the criteria and critical metrics that are generally utilized to evaluate the performance of a VA tool. We will also discuss the vulnerability services tools and test. Two types of service tools will be covered with one focusing on static code analysis and the other focusing on dynamic program analysis.
Module 3: Common VA Tools.	In the third module, we will introduce some commonly used VA tools, network/port scanners, and vulnerability scanners. Popular VA tools will be discussed with comprehensive examples, such as Wireshark, SolarWinds, NMAP, and Nessus. URLs for download will be provided for some VA tools that are not pre-installed in Kali Linux OS.

Module 4: Vulnerability examples and secure configurations.	In the fourth module, we will introduce examples of leveraging the vulnerability of web applications, such as code injection, cross-site scripting, and cross-site request forgery. Network instruction detection and prevention policies and rules will be discussed. System hardening and secure deployments will be covered with high-level concepts.
Module 5: Labs	In the fifth module, we will go over three labs – i) setup Damn Vulnerable Web Application (DVWA) and try different SQL injection commands, ii) try different cross-site scripting (XSS) commands to bypass server access control under DVWA, and iii) try different command injection to read files located on webserver under DVWA step by step with checkpoints provided for student evaluations. Practices of the labs will be offered on the NICE challenge platform using HTML5 web console.