

Cyber Security tools and Technologies

Mid term syllabus

Book: Computer Security Fundamentals

Chapter 1 (Introduction to Computer Security)

- ❖ Introduction
- ❖ How Seriously Should You Take Threats to Network Security?
- ❖ Identifying Types of Threats (seven broad classes)
- ❖ Assessing the Likelihood of an Attack on Your Network
- ❖ Basic Security Terminology
- ❖ Concepts and Approaches
- ❖ How Do Legal Issues Impact Network Security?
(excluded)

Chapter 2 (Networks and the Internet)

1. Introduction
2. Network Basics
3. How the Internet Works
4. History of the Internet (excluded)
5. Basic Network Utilities
6. Other Network Devices
7. Advanced Network Communication Topics

Chapter 5 (Malware)

1. Introduction
2. VIRUSES
3. TROJAN HORSES
4. The Buffer-Overflow Attack (excluded)
5. SPYWARE
6. Other Forms of Malware
7. Detecting and Eliminating Viruses and Spyware

Forum: TryHackMe

Nmap

1. **Nmap Live Host Discovery** room: all tasks and related concepts

Pre Security

❖ **Module 1:** *Introduction To Cyber Security*

1. Intro to Offensive Security.
2. Intro to Defensive Security.
3. Careers in Cyber

Module 2: *Network Fundamentals*

1. What's networking?
2. Intro to LAN
3. OSI Model
4. Packets and Frames

Pre Security

❖ **Module 3:** *How the Web Works*

1. DNS in detail
2. HTTP in detail
3. How websites work

Module 4: *Linux Fundamentals*

1. Linux Fundamentals Part 1

Other Material

Slides

- ❖ **Slides shared on GCR**
- ❖ **Research article titled (shared on GCR)**
 - From information security to cyber security