

# Cyber Security tools and Technologies

Final Syllabus

# **Book**

# **Computer Security**

# **Fundamentals**

# Chapter 1: Introduction to Computer Security

- ❖ **Included:** From Section 1 Till Section 6 (Concepts and Approaches)
- ❖ **Excluded:** Section 7 onward

# Chapter 2: Networks and the Internet

- ❖ **Included:** Section 1 to 3, and Sections 5 – 7
- ❖ **Excluded:** Section 4

# Chapter 5: Malware

- ❖ **Included:** Full Chapter

# Chapter 6: Techniques Used by Hackers

- ❖ Introduction
- ❖ Basic Terminology
- ❖ The Reconnaissance Phase
- ❖ Actual Attacks
- ❖ Malware Creation
- ❖ Penetration Testing

# Chapter 7: Industrial Espionage in Cyberspace

- ❖ Introduction
- ❖ What is Industrial Espionage?
- ❖ Information as an Asset
- ❖ Real-world Examples Of Industrial Espionage
- ❖ How Does Espionage Occur?
- ❖ Protecting Against Industrial Espionage
- ❖ Spear Phishing

# Chapter 9: Computer Security Technology

- ❖ Introduction
- ❖ Virus Scanners
- ❖ Firewalls
- ❖ Antispyware
- ❖ IDSs
- ❖ SSL/TLS
- ❖ WiFi Security

# Chapter 11: Network Scanning and Vulnerability Scanning

- ❖ Introduction
- ❖ Basics of Assessing a System
- ❖ Securing Computer Systems

**Forum: TryHackMe**



# Nmap Module

1. Nmap Live Host Discovery
2. Nmap Basic Port Scanning
3. Nmap Advanced Port Scanning
4. Nmap Post Port Scans
  - ✓ Task 1: Introduction
  - ✓ Task 2: Service Detection
  - ✓ Task 3: OS Detection and Traceroute

# Pre security path

- ✓ Sec 1: Intro to Cyber Security (separate module as well)
  - ✓ Intro to Offensive security
  - ✓ Intro to Defensive security
  - ✓ Careers in Cyber
- ✓ Sec 2: Network Fundamentals – Complete
- ✓ Sec 3: How the Web Works – Complete
- ✓ Sec 4: Linux Fundamentals – Complete
- ✓ Sec 5: Windows Fundamentals – Complete

# Vulnerability Research Module

- ✓ Part 1: **Vulnerabilities 101**
  - ✓ Task 2: Intro to Vulnerabilities
  - ✓ Task 3: Scoring vulnerabilities Overview
    - ✓ Frameworks: CVSS & VPR
  - ✓ Task 4: Vulnerability databases (overview)
  - ✓ Task 5: An example of finding a Vulnerability

**Other Material**

**Slides / Notes shared on GCR**

# Week 9: Notes / Slides

## **Topic 1: Certified Information Systems Security Professional (CISSP):**

- ❖ CISSP: Security Domains for Cyber Analyst
- ❖ Managing Threats, Risks and Vulnerabilities
- ❖ Frameworks and Controls
  - Cyber Threat Framework
  - ISO/IEC 27001 Framework
  - Controls

# Week 9: Notes / Slides

## **Topic 2: Software Security**

- ❖ Overview
- ❖ EU General Data Protection Regulation requirements for software
- ❖ Classification of vulnerabilities
- ❖ Detection of vulnerabilities

# Week 12: Sniffers

## **Sniffers: Chapter/Module 9 of Certified Ethical Hacker (CEH) Study Guide v12**

✓ Notes/ Slides

# Week 14: Sniffers

## **NIST Cybersecurity Framework (CSF)**

✓ **Notes/ Slides**



# Research Articles

❖ **A1: Title:** Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle

- Abstract
- Sec 1: Introduction
- Sec 5: Table 1: Reconnaissance Tools (Nmap)

❖ **A2: Title:** Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey

- Abstract
- Sec 1: Introduction
- Sec 2: Existing Surveys And Our Contributions