Cybersecurity Fundamentals

Course Overview:

This course is the introductory class for cybersecurity certification (CompTIA Security + and CEH-EC Council). Students will master the fundamental concepts and learn different tools of the trade to become an active cyber defender. Students will use Kali Linux and its various cybersecurity applications such as Metasploit, crack passwords using Hydra, and execute social engineering attacks. Students will also learn how to defend against various forms of attacks from configuring firewalls, activating intrusion detection systems, and learn about how cryptography can keep data and transmission safe.

Grade Level: High School and Above

Time Required to Complete this Course: 120 to 150 Hours.

Prerequisites: No

Requirements: Windows PC / 8 GB RAM / Internet Connection / VM Capable (PC should not be greater than 10 years old).

Course Layout

This course is laid out in the following structure:

- **Instructional videos** (these are where students will acquire a lot of their information). They can watch these videos as many times as they want.
- **Checkpoints:** this is a great way to assess quickly what they have learned. They are often provided in H5P format.
- **Activities:** These should count as grades and they vary greatly from one another). Some activities will ask students to acquire information that were not directly presented to them.
- **Quizzes:** These are summative assessments thrown into parts of the chapter as necessary. Quizzes are set to auto grading.
- **Projects:** Generally, these are large, time consuming assignments designed to get students to create artifacts. Often, finishing these projects will require knowledge acquired outside of the classroom.

Course Breakdown

Unit 1: Introduction to Ethical Hacking

Objectives / Topics Covered	• Cyber Attack • Different Types of Cyber Attacks • Passive Attacks • Active Attacks • Hacking • Hacker Categories • Essential Terminologies in Cyber World
Activities	• Activity 1: Flipbook • Activity 2: Steps of Hacking • Activity 3: Top 10 Hackers
Assessments	• 3 Quizzes
Project 1	• Case study on a Movie
Exam Preparation	• Overview of Security

Environment Setup

Setting up the Virtual Machine	• Virtual Box Download • Download Windows Machine • Download Kali Linux • How to use Kali Linux

Unit 2: Who am I

Objectives / Topics Covered	• Digital Identity • Identity Spoofing • IP Address • Spoofing Attacks
Activities	• Activity 1: DNS Server • Activity 2: Email Spoofing • Activity 3: SMS Spoofing • Activity 4: VPN

Assessments	• 3 Quizzes
Project 2	• Losing Your Digital Identity
Exam Preparation	• Social Engineering
Tools and Media	• Command Prompt • Whatismyip.com • Facebook • Instagram • Email

Unit 3: We are everywhere & nowhere

Objectives / Topics Covered	• Reconnaissance • Types of Reconnaissance • How Search Engine Works • Google Dorks • Recon NG • Using Maltego • Using PhoneInfoga • Email Spoofing
Activities	• Activity 1: Searching for Password List • Activity 2: Recon NG • Activity 3: Get Some Numbers
Assessments	• 3 Quizzes
Project 3	• IOT Boundaries
Exam Preparation	• Physical Security
Tools and Media	• Shodan.io, Kali Linux, Maltego

Unit 4: Now you can see me

Objectives / Topics Covered	• Active Reconnaissance • Networking Scanning Process • TCP and IP • Ping Command, ICMP and TTL

	• IP Scanners
Activities	• Activity 1: TCP/IP Attacks • Activity 2: Defender Mode
Assessments	• 3 Quizzes
Project 4	• Network Security
Tools and Media	• Angry IP Scanner, Hping Tool, Zenmap Tool

Unit 5: Cryptography

Objectives / Topics Covered	• Cryptography • Encryption Definition • Symmetric & Asymmetric Encryption • Basic Algorithms • Encoding • Hashing and Salting • Stenography
Activities	• Activity 1: Caesar Cipher • Activity 2: Base46 • Activity 3: AES • Activity 4: RSA • Activity 5: Hashing Collisions
Assessments	• 3 Quizzes
Project 5	• Substitution Cipher
Exam Preparation	• Cryptography
Tools and Media	• Base64encode.org, nano editor, python hash generator, 7 zip, devglan.com, Putty Gen

Unit 6: Let's Break

Objectives / Topics Covered	• Decoding • Decryption • Cracking Windows Password from Boot • Tradition Password patterns

	• Brute force in depth • Dictionary Attack
Activities	• Activity 1: Base64 Decoding • Activity 2: Password Combinations
Assessments	• 1 Quiz
Project 6	• Cracking RSA
Exam Preparation	• Public Key Infrastructure
Tools and Media	• Base64encode.org, base64 guru, Hydra,

Unit 7: The Trojan Games

Objectives / Topics Covered	• Virus, Worms, Trojan Horse • Creating Malware • Ransomware • Intrusion Detection System
Activities	• Activity 1: Virus / Worm Signatures • Activity 2: Antivirus vs. IDS
Assessments	• 2 Quizzes
Project 7	• Design a Defense
Exam Preparation	• Malware
Tools and Media	• ZLogger, The Zoo Malware Repository, Darkcomet, Poison IVY,ardamax keylogger, Wanna cry ransomware case study

Unit 8: MITM

Objectives / Topics Covered	• ARP Concepts • SSL STRIP • TCP Dump • TCP Flooding Attack • Introduction to Wireshark • Man in the Middle Attack
Activities	• Activity 1: MITM

	• Activity 2: Wireshark
Assessments	• 2 Quizzes
Project 8	• The 'Syn' Food
Exam Preparation	• Risk Assessment
Tools and Media	• Wireshark, Tcpdump, Ettercap

Unit 9: Put on a Happy Face

Objectives / Topics Covered	• Phishing Attacks • Introduction to Social Engineering • MS Office • Dynamic Data Exchange • Website Attack Vectors
Activities	• Activity 1: MS Office Exploit • Activity 2: PDF Exploit • Activity 3: Phishing • Activity 4: SMS Spoofing
Assessments	• 1 Quiz
Project 9	• Social Engineering
Tools and Media	• SEE KIT, Kali Linux, Metasploit Framework, msf console

Unit 10: Happy Neighbour Wi-Fi

Objectives / Topics Covered	• Wi-Fi Basics and Protocols • Wireless Access Points and Wi-Fi Routers • IEEE • Different Types of Wi-Fi Networks • Sniffing • Types of Wi-Fi Authentication • WEP Cracking • WPA-2 Cracking
Activities	• Activity 1: Your Wireless Router

Assessments	• 1 Quiz
Project 10	• Hacking Wi-Fi Networks
Tools and Media	• net stumber, aircrack, Kali Linux

Unit 11: Secure Ending

Objectives / Topics Covered	• Windows Hardening • Securing Windows • User Privileges • Anti-Virus
Activities	• Activity 1: Windows Hardening
Assessments	• 1 Quiz
Project 11	• Operating System Security
Tools and Media	• McAfee antivirus, Malware bytes