
EC-Council C|EH v13
Certified Ethical Hacker v13
Instructor Guide

Agenda

01 What is CEH

02 CEH Training schedule and exam information

03 How to access course related material

04 Class Minimum requirements, basic lab setup requirements, and lab setup environment

05 Live sites to try hacks

06 What is EC-COUNCIL CYBERQ

07 What should you ensure before going to Class

08 How to Teach CEH

09 Where to get help

Agenda 01

What Is CEH

What is CEH Program?

- CEH is a comprehensive **ethical hacking** and **information systems security auditing** program focusing on latest security threats, advanced attack vectors and practical real time demonstration of latest **hacking techniques**, methodologies, tools, tricks and security measures

- A program developed by **subject matter experts** from all over the world and are constantly updated to ensure that the students are exposed to the latest advances in the space

What is CEH Program?

A Comprehensive Encyclopedia of Attack Vectors and Hacking Techniques

- More than **1250** illustrated instructor slides
- More than **3500** pages of comprehensive student manual
- More than **1850** pages of lab manual covering detailed lab scenarios and instructions
- A repository of more than **3500** hacking and security tools

What is CEH Program?

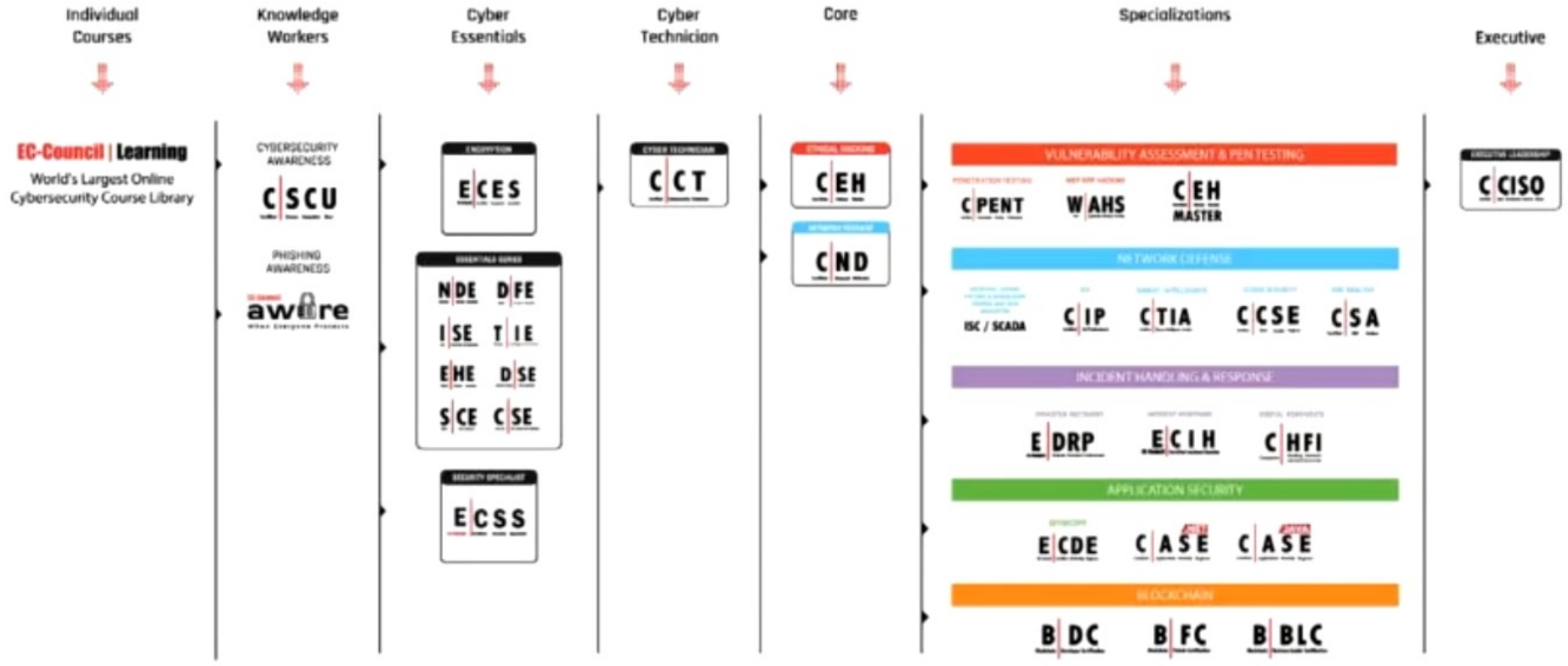
A lab intensive program

- Every learning objective is demonstrated using labs
- Complex and advanced labs to emphasize the learning objectives
- More than **50%** of training time is dedicated to labs
- **91** Core Labs and **130** Self-study Labs available separately as the **CEH Self Study Upgrade Lab Pack**
- Lab setup simulates real-life networks and platforms

Where Does CEH Fits in EC-Council Career Path?

EC-Council
Building A Culture Of Security

Cybersecurity Learning Track



CEH Mapping to NICE 2.0

Compliance with National Initiative for Cybersecurity Education (NICE) in the work role category "PROTECTION and DEFENSE (PD)"

CEH maps 100 percent to three important **Work Roles** under NICE framework's **PROTECTION and DEFENSE** work role category.

- **Defensive Cybersecurity (PD-WRL-001)**

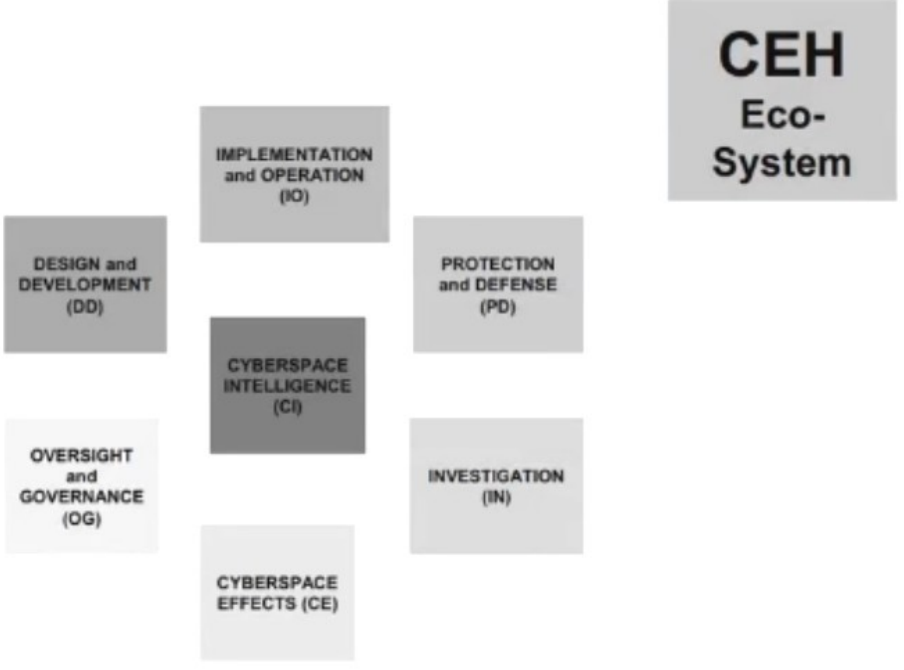
  Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

- **Threat Analysis (PD-WRL-006)**

  Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.

- **Vulnerability Analysis (PD-WRL-007)**

  Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.



https://www.nist.gov

CEH Mapping to DoD Cyber Workforce Framework Work Roles

Work Role	Work Role ID	Work Role Description
Warning Analyst	**141**	Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.
Cyber Defense Analyst	**511**	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Research & Development Specialist	**661**	Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
Vulnerability Assessment Analyst	**541**	Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

CEH Course Outline

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT and OT Hacking
19. Cloud Computing
20. Cryptography

What will Student Learn?

Students going through CEH training will learn:

- Key issues plaguing the information security world, hacking methodologies and frameworks, information security controls, and information security laws and standards
- Different types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- Different types of vulnerability assessment and vulnerability assessment tools
- System hacking methodology
- Different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures
- Various packet sniffing techniques and sniffing countermeasures
- Social engineering techniques, identity theft, and countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures

What will Student Learn?

Students going through CEH training will learn:

- Firewall, IDS, IPS, honeypot, NAC, and endpoint evasion techniques, evasion tools, and countermeasures
- Different types of web server, web application, and web API attacks, hacking methodology, hacking tools, and countermeasures
- SQL injection attacks, injection methodology, evasion techniques, and SQL injection countermeasure
- Different types of wireless encryption, wireless threats, wireless hacking methodology, wireless hacking tools, Wi-Fi security tools, and countermeasures
- Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools
- Different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures
- Various cloud computing technologies, cloud computing threats, attacks, hacking methodology (AWS, Microsoft Azure, Google Cloud, and container hacking), and security techniques and tools
- Different types of encryption algorithms, cryptography tools, applications of cryptography, cryptography attacks, and cryptanalysis tools
- AI-driven ethical hacking

Agenda 02

CEH Training Schedule and Exam Information

Training Information

- Title of the Course: **Ethical Hacking and Countermeasures**
- Version: **13**
- Training Duration: **5 Days (40 Hours)**
- Training Timing: **9:00 AM to 5:00 PM**
- Delivery Mode:
  - **Instructor-led Training (ILT)**
  - **iWeek (Synchronous Online Learning)**
  - **iLearn (Asynchronous Online Learning)**
  - **CodeRed (Asynchronous Online Learning)**

Target Audience

- Ethical Hackers
- Information Security Analyst/Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Information Security Professionals/Officers
- Information Security/IT Auditors
- Risk/Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers
- Anyone who is concerned about the integrity of the network infrastructure

Note: The CEHv13 is an advanced security training program. Proper preparation is required before conducting the CEH class

Training Sessions

SESSIONS	START	END	DURATION (MINUTES)
Morning Session	9:00 AM	10:45 AM	105
Break	10:45 AM	11:00 AM	15
Noon Session	11:00 AM	12:30 PM	90
Lunch Break	12:30 PM	1:30 PM	60
Afternoon Session	1:30 PM	2:45 PM	75
Break	2:45 PM	3:00 PM	15
Evening Session	3:00 PM	5:00 PM	120

- **Total Session Time/Day in Hours: 6.30**
- **Total Session Time in 5 Days in Minutes: 1950**

Training Session: Day 1

Start	End	Time in Minutes	Module
9:00	9:10	10	Module 00: Student Introduction
9:10	9:50	40	Module 01: Introduction to Ethical Hacking
9:50	10:30	40	Module 02: Footprinting and Reconnaissance
10:30	10:45	15	Classroom Exercise for Module 02
10:45	11:00		Break
11:00	12:00	60	Classroom Exercise for Module 02
12:00	12:30	30	Module 03: Scanning Networks
12:30	1:30		Lunch Break
1:30	1:35	5	Module 03: Scanning Networks
1:35	2:45	70	Classroom Exercise for Module 03
2:45	3:00		Break
3.00	3.30	30	Module 04: Enumeration
3.30	4.30	60	Classroom Exercise for Module 04
4.30	4.50	20	Module 05: Vulnerability Analysis
4:50	5:00	10	Classroom Exercise for Module 05

Training Session: Day 2

Start	End	Time in Minutes	Module
9:00	9:25	25	Classroom Exercise for Module 05
9:25	10:45	80	Module 06: System Hacking
10:45	11:00		Break
11:00	11:20	20	Module 06: System Hacking
11:20	12:30	70	Classroom Exercise for Module 06
12.30	1.30		Lunch Break
1.30	2.40	70	Classroom Exercise for Module 06
2:40	2:45	5	Module 07: Malware Threats
2:45	3:00		Break
3:00	3:45	45	Module 07: Malware Threats
3.45	4.45	60	Classroom Exercise for Module 07
4.45	5.00	15	Module 08: Sniffing

Training Session: Day 3

Start	End	Time in Minutes	Module
9:00	9:20	20	Module 08: Sniffing
9:20	10:00	40	Classroom Exercise for Module 08
10:00	10:30	30	Module 09: Social Engineering
10:30	10:45	15	Classroom Exercise for Module 09
10:45	11:00		Break
11:00	11:05	5	Classroom Exercise for Module 09
11:05	11:35	30	Module 10: Denial-of-Service
11:35	12:05	30	Classroom Exercise for Module 10
12:05	12:30	25	Module 11: Session Hijacking
12:30	1:30		Lunch Break
1:30	1:35	5	Module 11: Session Hijacking
1:35	2:10	35	Classroom Exercise for Module 11
2:10	2:45	35	Module 12 Evading IDS, Firewalls, and Honeypots
2:45	3:00		Break
3:00	3:15	15	Module 12 Evading IDS, Firewalls, and Honeypots
3:15	4:15	60	Classroom Exercise for Module 12
4:15	5:00	45	Module 13: Hacking Web Servers

Training Session: Day 4

Start	End	Time in Minutes	Module
9:00	9:45	45	Classroom Exercise for Module 13
9:45	10:45	60	Module 14: Hacking Web Applications
10:45	11:00		Break
11:00	11:45	45	Module 14: Hacking Web Applications
11:45	12:30	45	Classroom Exercise for Module 14
12.30	1.30		Lunch Break
1.30	2:10	40	Classroom Exercise for Module 14
2:10	2:45	35	Module 15: SQL Injection
2:45	3:00		Break
3.00	3:10	10	Module 15: SQL Injection
3:10	3:45	35	Classroom Exercise for Module 15
3:45	4:20	35	Module 16: Hacking Wireless Networks
4:20	4:35	15	Classroom Exercise for Module 16
4:35	5:00	25	Module 17: Hacking Mobile Platforms

Training Session: Day 5

Start	End	Time in Minutes	Module
9:00	9:30	30	Module 17: Hacking Mobile Platforms
9:30	10:15	45	Classroom Exercise for Module 17
10:15	10:45	30	Module 18: IoT and OT Hacking
10:45	11:00		Break
11:00	11:35	35	Module 18: IoT and OT Hacking
11:35	12:15	40	Classroom Exercise for Module 18
12:15	12:30	15	Module 19: Cloud Computing
12:30	1:30		Lunch Break
1:30	2:40	70	Module 19: Cloud Computing
2:40	2:45	5	Classroom Exercise for Module 19
2:45	3:00		Break
3:00	3:35	35	Classroom Exercise for Module 19
3:35	4:15	40	Module 20: Cryptography
4:15	5:00	45	Classroom Exercise for Module 20

Instructors may alter the structure of the course and the timings to meet their requirements.

Exam Information

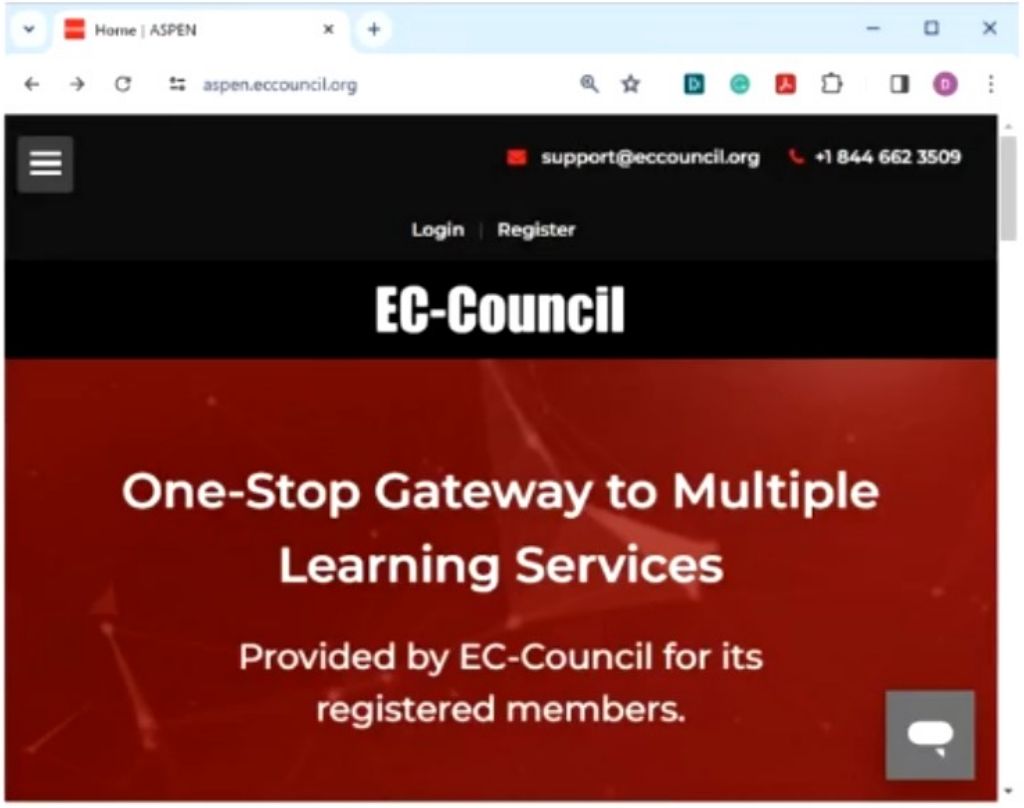
1. Exam Title: Certified Ethical Hacker
2. Exam Code: 312-50 (ECC Exam Portal) / 312-50 (VUE)
3. Number of Questions: 125
4. Duration: 4 hours
5. Availability: ECC Exam Portal / VUE
6. Passing Score: Please refer https://cert.eccouncil.org/faq.html
7. Test Format: Multiple Choice
8. The training center / instructor will advise you about the exam schedule and voucher details

Agenda 03

How to Access Course related Material

What is Aspen?

- Aspen is a **one-step gateway to multiple portals**, **products**, and **services** provided by EC-Council for its registered members
- You can download instructor slides, lab setup guide, e-courseware, lab manuals, and tools at ***https://aspen.eccouncil.org***

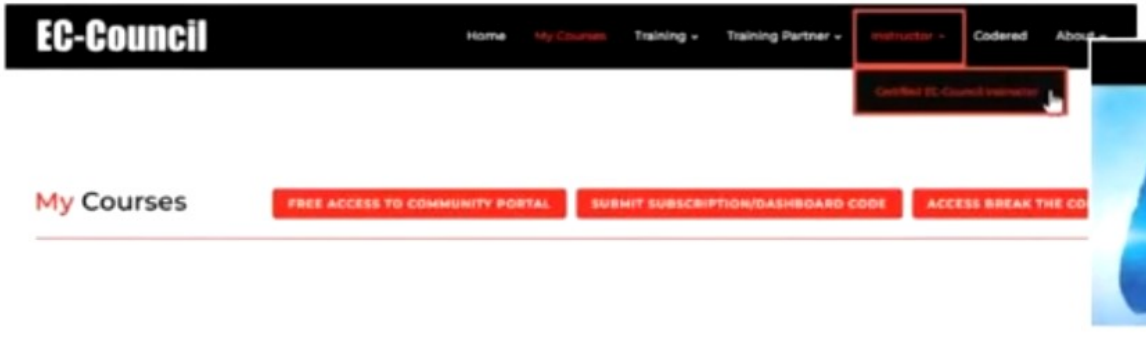


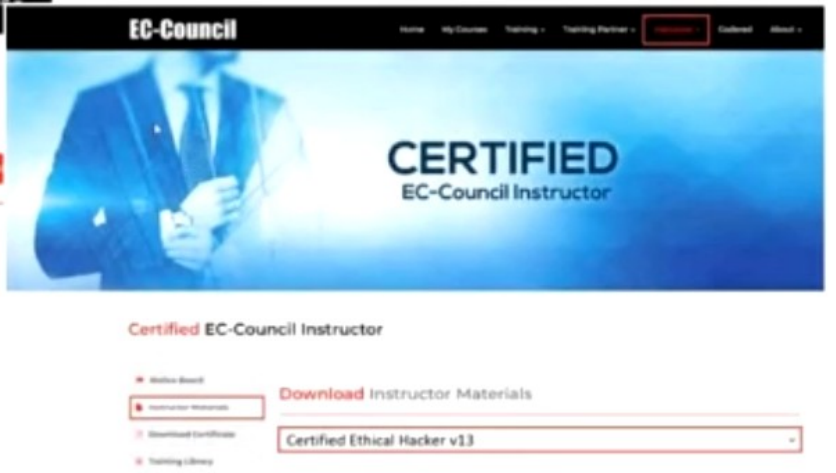
Accessing CEI Material

1. Log in to the **Aspen** portal and click the **Certified EC-Council Instructor** option from the **Instructor** menu

2. Click **Instructor Materials** in the side menu and select **Certified Ethical Hacker v13** from drop-down menu

3. Download your **Instructor Slides**, **Courseware**, **Tools**, and **Lab Setup Guide**





Agenda 04

Class Minimum Requirements, Basic Lab Setup Requirements, and Lab Setup Environment

Minimum Requirements

- Intel Core i5 or equivalent CPU with a minimum CPU speed of 3.2 GHz
- Minimum of 8 GB RAM (16 GB recommended)
- Hard disk, 500 GB or higher and 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- One network adapter (minimum of a 10/100 NIC, but a 10/100/1000 is preferred)
- Monitor (minimum requirement is a 17-inch LCD monitor)
- Mouse or compatible pointing device and a sound card with amplified speakers
- Internet access
- Two Wireless Network adapter (PCI or USB)*

Basic Lab Setup Requirements

- Any Windows/Linux/macOS operating system capable of running VMware Workstation Pro v17.5.2 or later version
- CEH Tools downloadable from the Aspen portal
- Microsoft Windows 11 Enterprise or Professional (64-bit) with full patches applied
- Microsoft Windows Server 2022 Standard Edition (64-bit) with full patches applied
- Microsoft Windows Server 2019 Standard Edition (64-bit) with full patches applied
- Parrot Security (MATE) v6.0 (64 bit) with full patches applied
- Android 8.1-r6 (64-bit) with full patches applied
- Ubuntu 22.04.3 (64 bit) with full patches applied
- Adobe Acrobat Reader DC or later version
- WinRAR v6.10 or later version
- Web browsers: Internet Explorer, Firefox, and Chrome
- Word, Excel, and PowerPoint viewers, preferably Microsoft Office 2016 or Open Office
- WampServer 3.3.5 or later version
- Java Runtime Environment v8u321 or later version
- Microsoft Visual C++ packages
- MSSQL Server Express 2022
- Notepad++ v8.6.5 or later version
- Linksys adapter
- WinPcap and Npcap

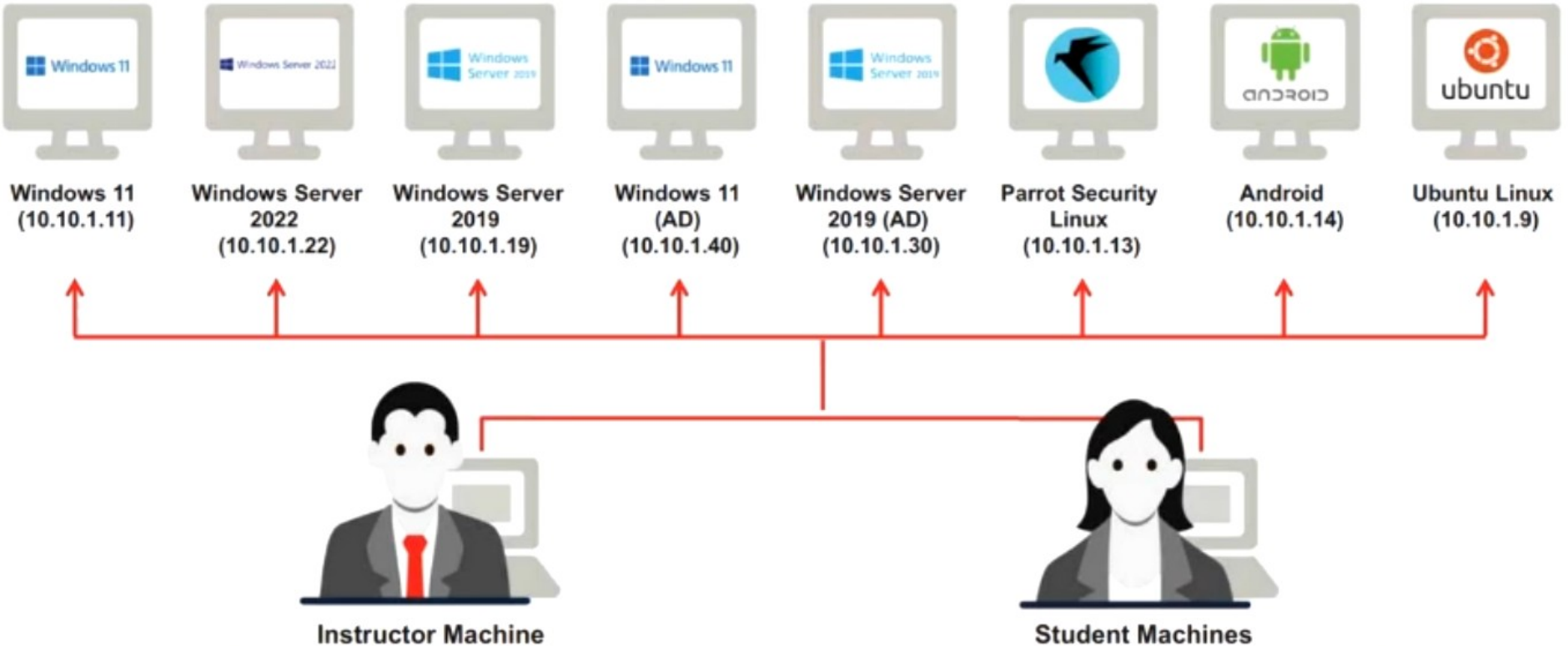
Note: Please check the **Lab Setup Guide** available in **Instructors Area** at https://aspen.eccouncil.org for detailed lab setup instructions

Basic Lab Setup Requirements

- You must sign up for OpenAI services and add a payment method for the OpenAI API keys for ShellGPT. You will be required to provide your credit card information. Follow the below steps to do this:

  1. Visit the OpenAI platform (**https://platform.openai.com**) and sign up or log in to your existing account
  2. Once logged in, click the profile icon at the top-right, click **Your profile** option, and navigate to the **Billing** section
  3. Under **Billing** section, go to **Payment methods** and click **Add payment method** to add a payment method
  4. Go to **Overview** and click **Add to credit balance**
  5. Enter the minimum amount, i.e., **$5** for **Amount to add**, and click **continue**. Please refer **https://openai.com/api/pricing/** for API pricing details
  6. Click **Confirm payment** and complete the transaction to add the credit balance

Lab Environment



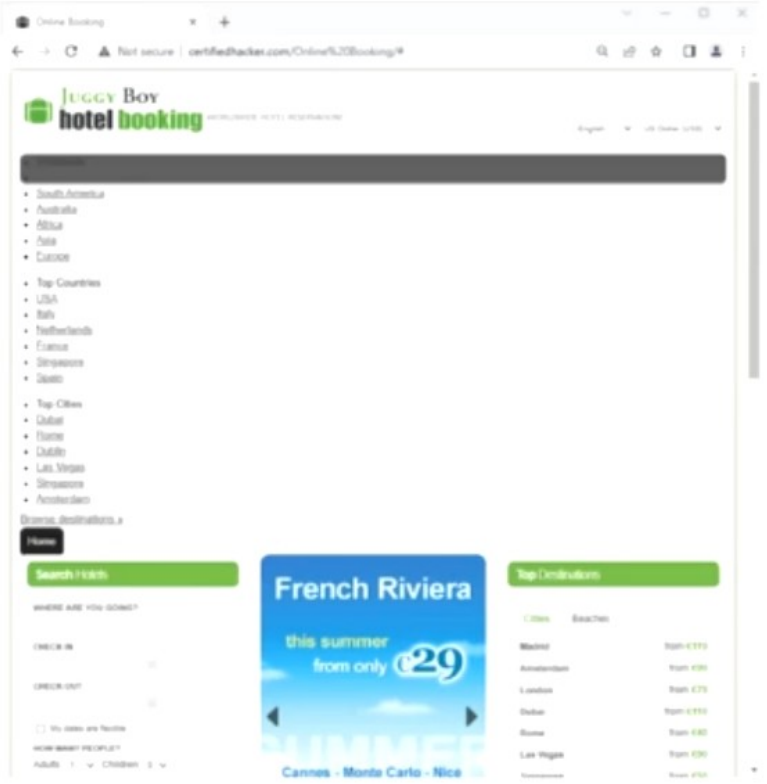
Instructor and Student Machine Operating System: Any Operating System Capable of Running VMware (Fully Patched)

Agenda 05

Live Sites to Try Hacks

Live Sites to Try Hacks

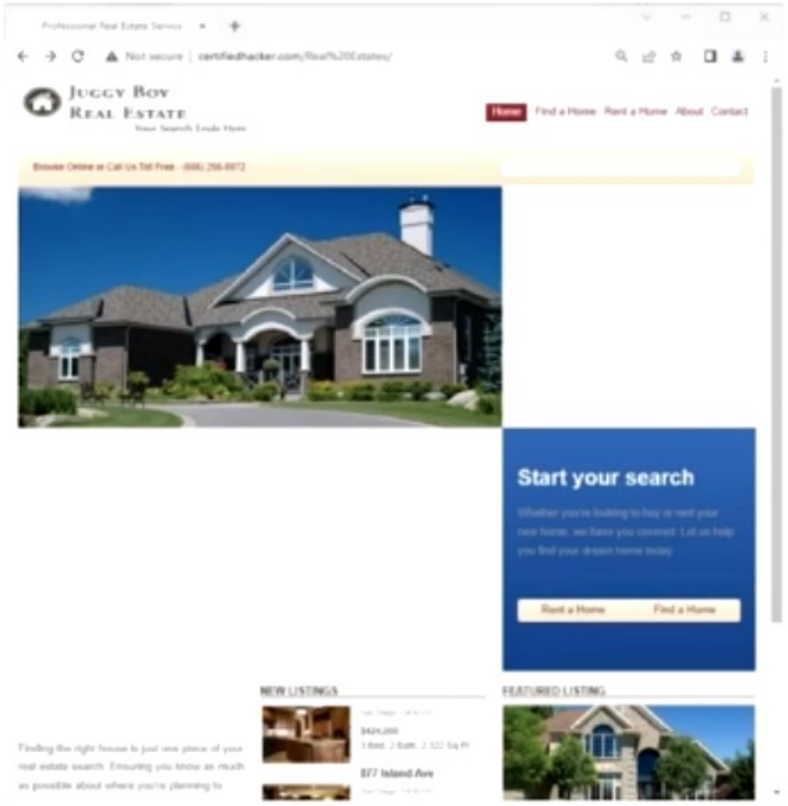
http://certifiedhacker.com/P-folio



http://certifiedhacker.com/Online Booking

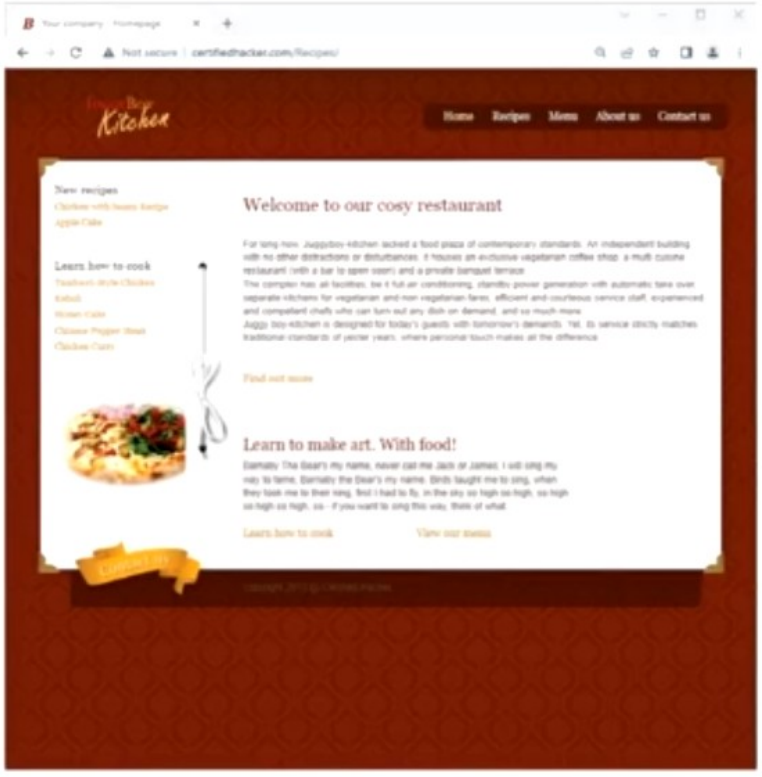
Live Sites to Try Hacks

http://certifiedhacker.com/corporate-learning-website/01-homepage.html



http://certifiedhacker.com/Real Estates

Live Sites to Try Hacks

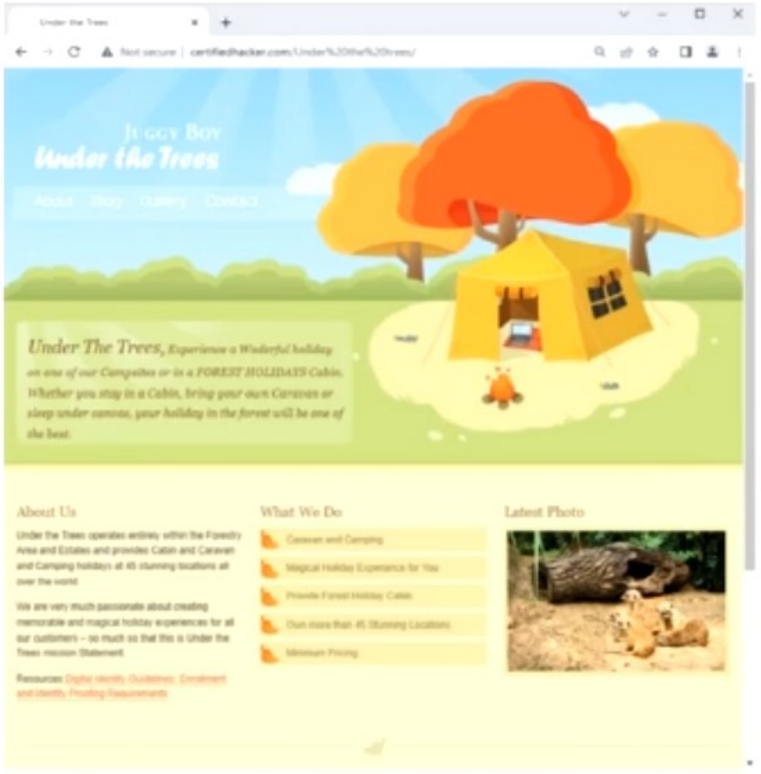


http://certifiedhacker.com/Recipes

http://certifiedhacker.com/Social Media

Live Sites to Try Hacks

http://certifiedhacker.com/Turbo Max



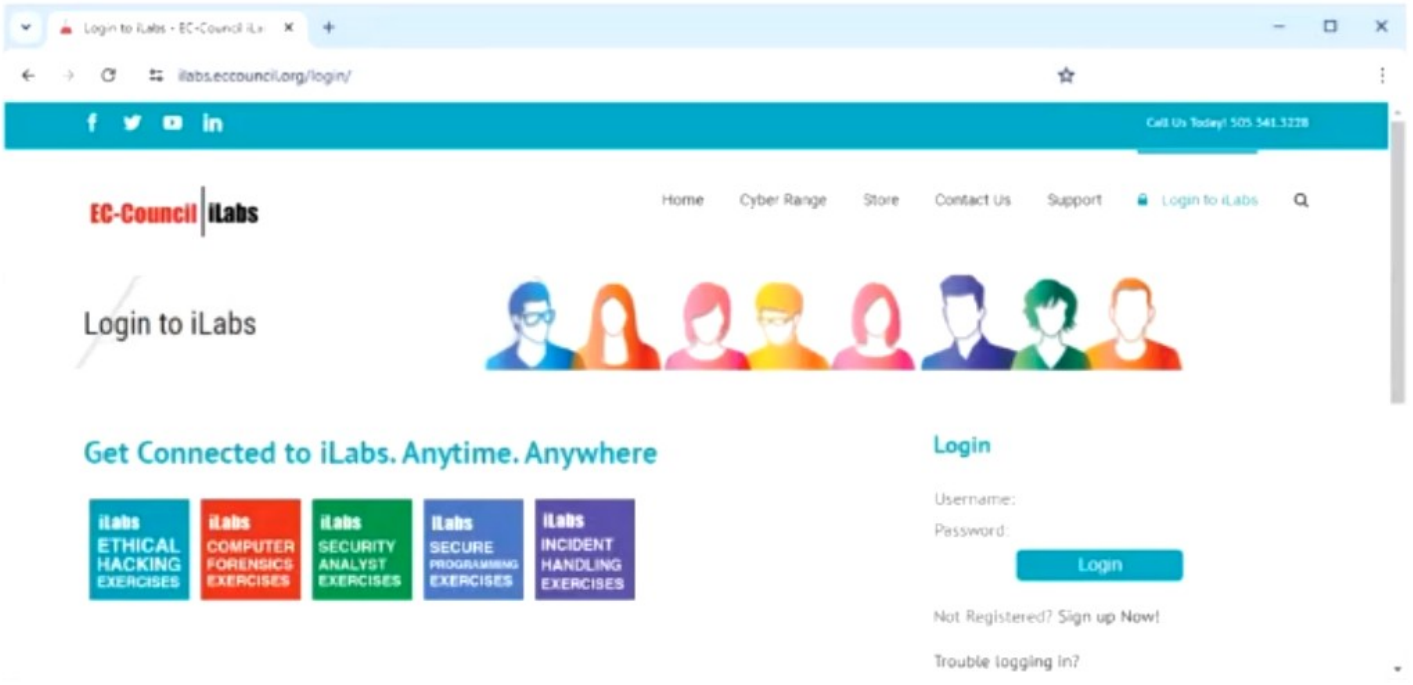
http://certifiedhacker.com/Under the trees

Agenda 06

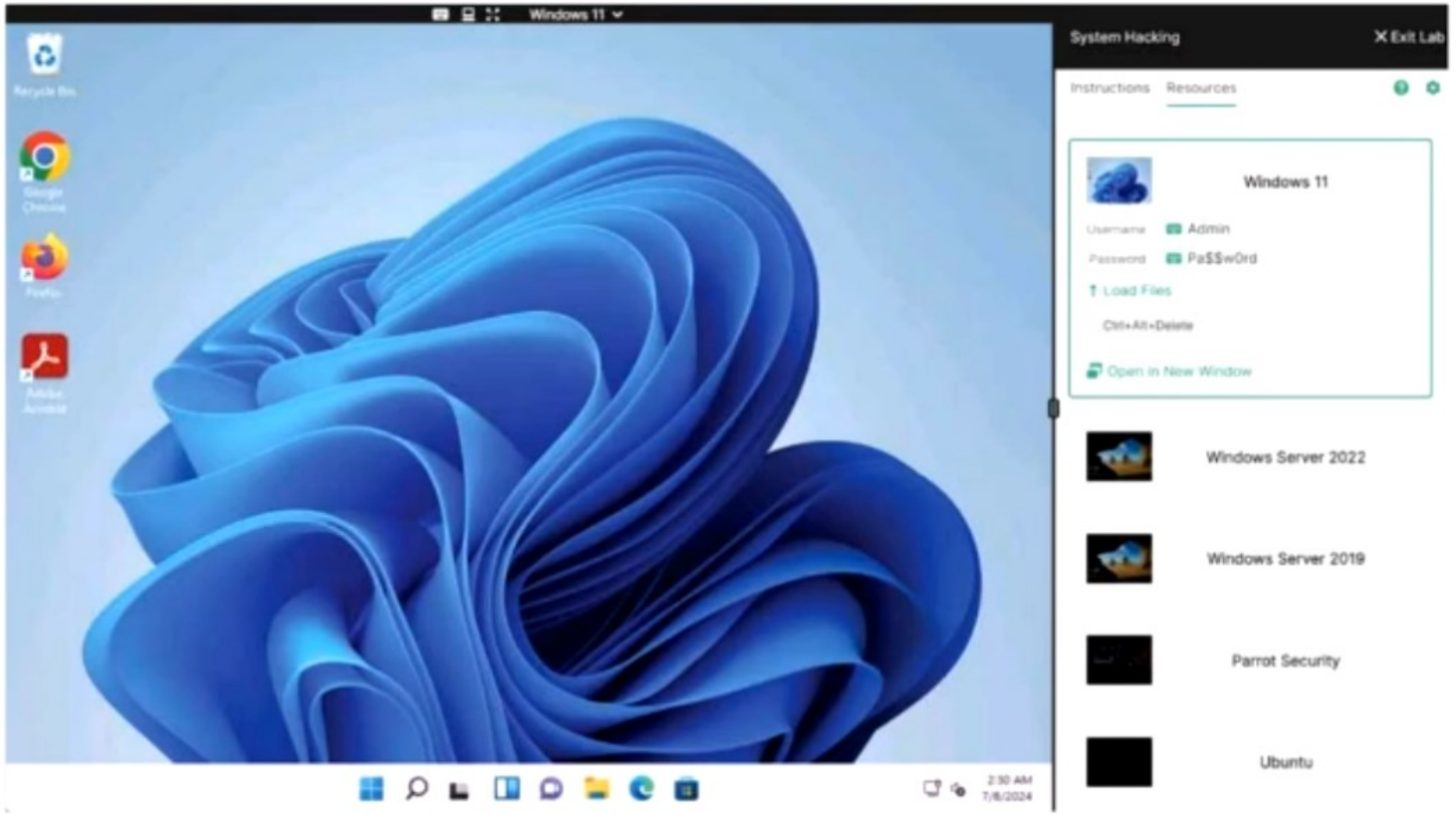
What Is EC-COUNCIL CYBERQ

EC-Council iLabs

The iLabs is a subscription-based service that allows students to logon to a **virtualized remote machine** to perform various exercises featured in the **CEHv13 Lab Manuals**

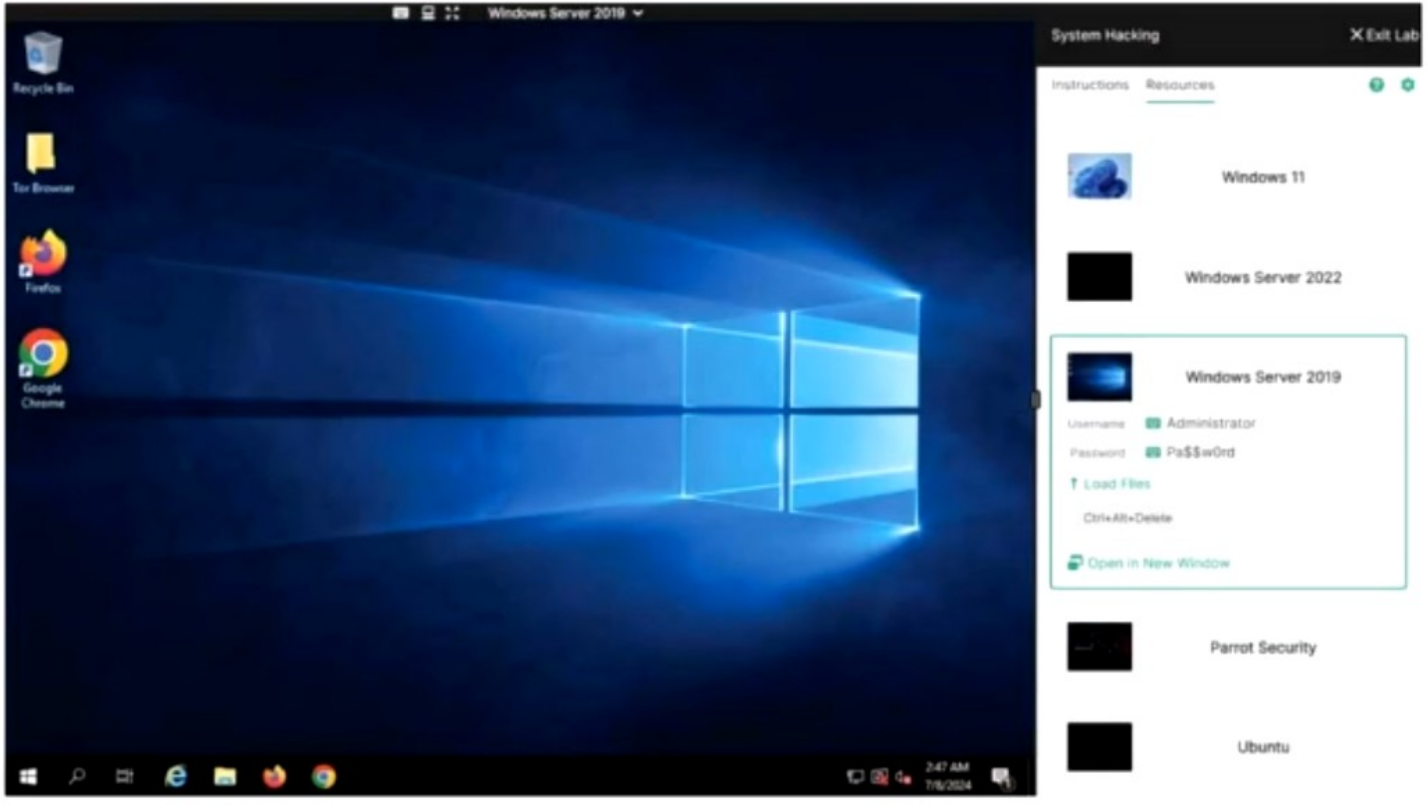


Windows 11 Machine in iLabs

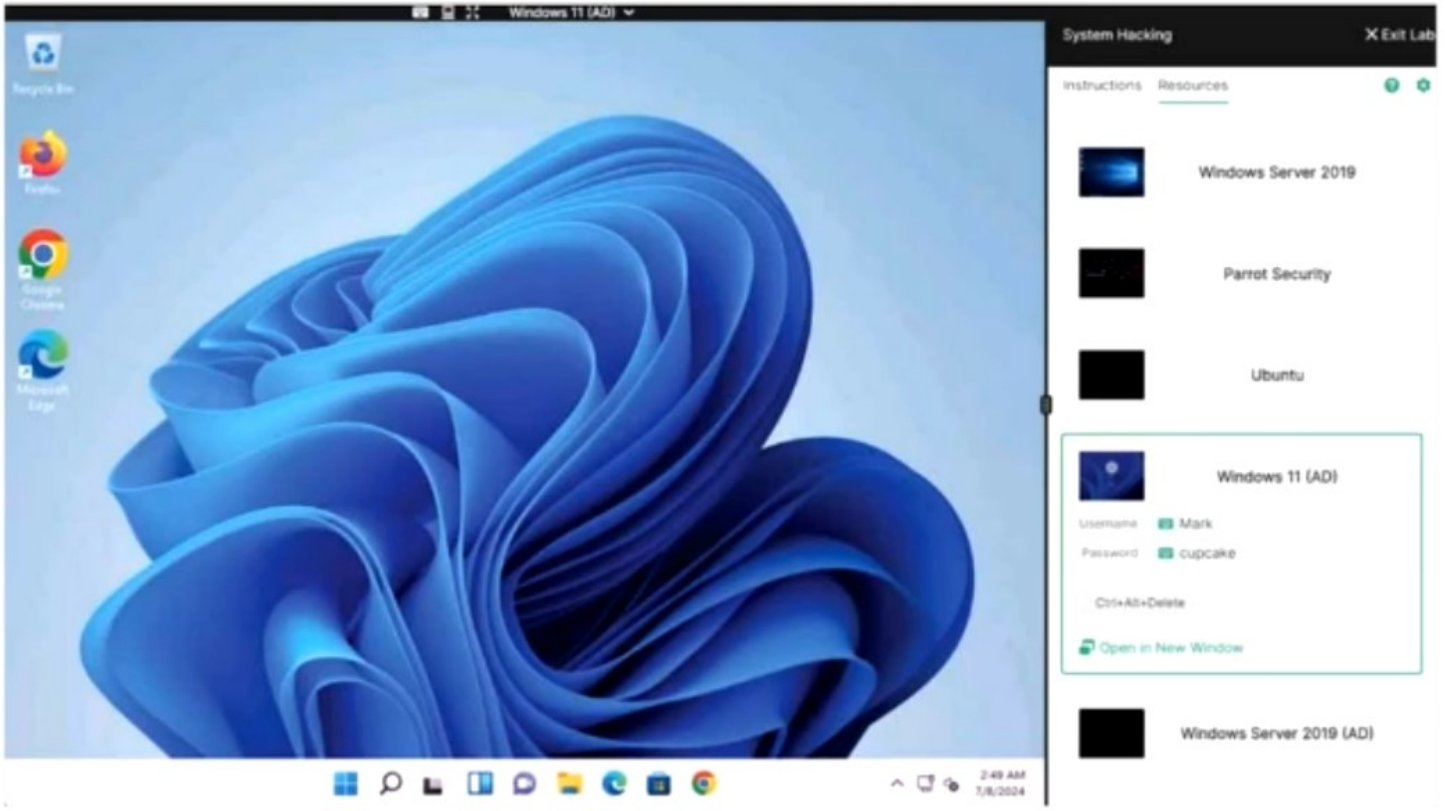


Windows Server 2022 Machine in iLabs

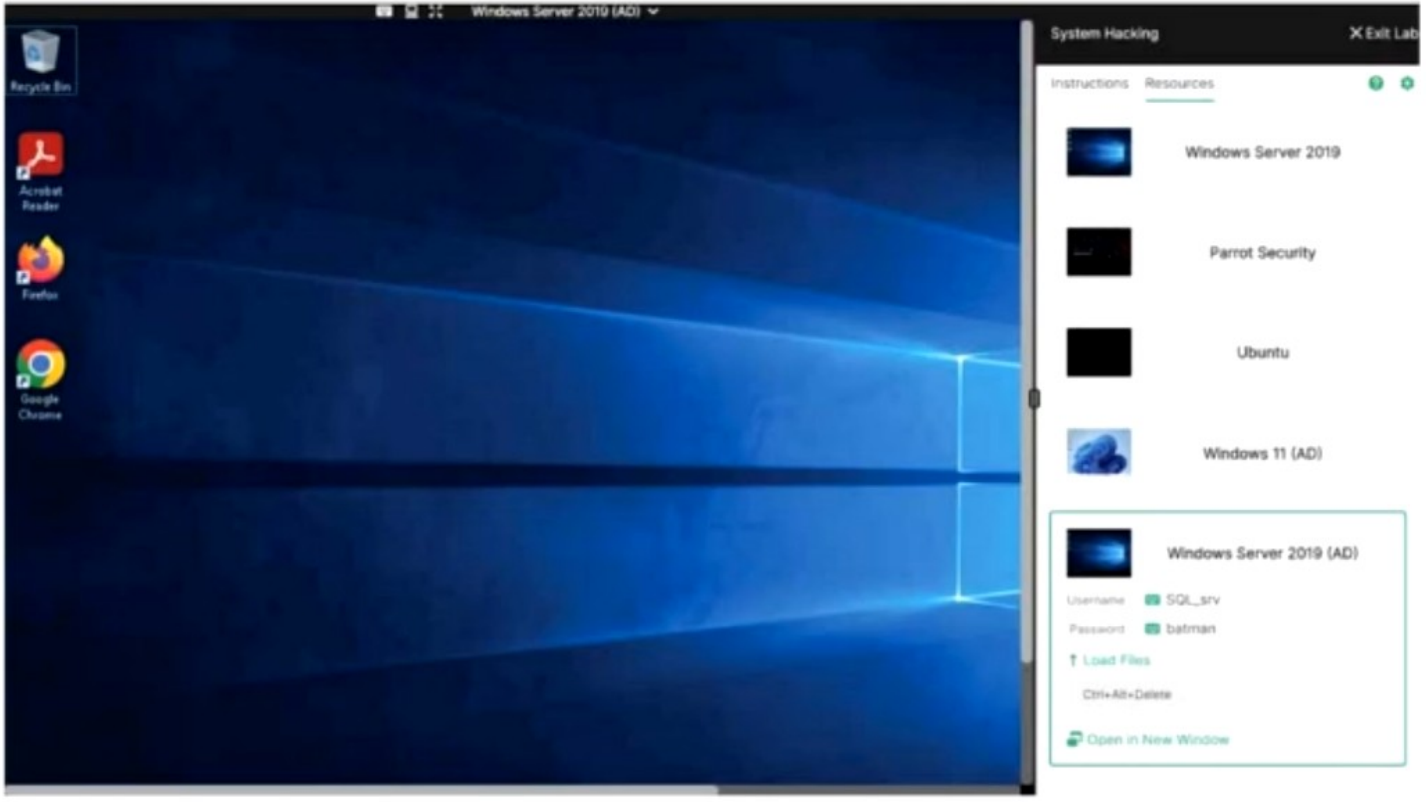
Windows Server 2019 Machine in iLabs



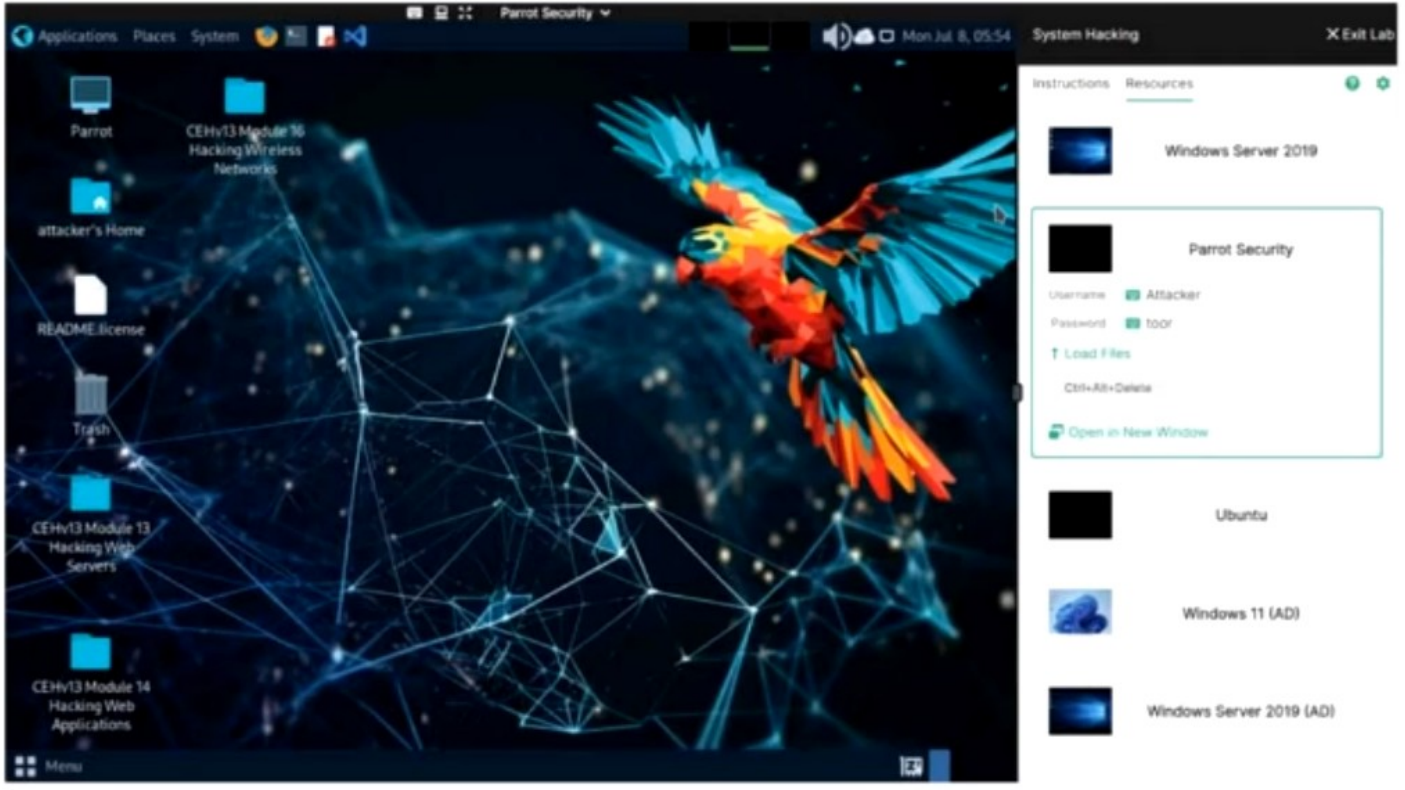
Windows 11 (AD) Machine in iLabs



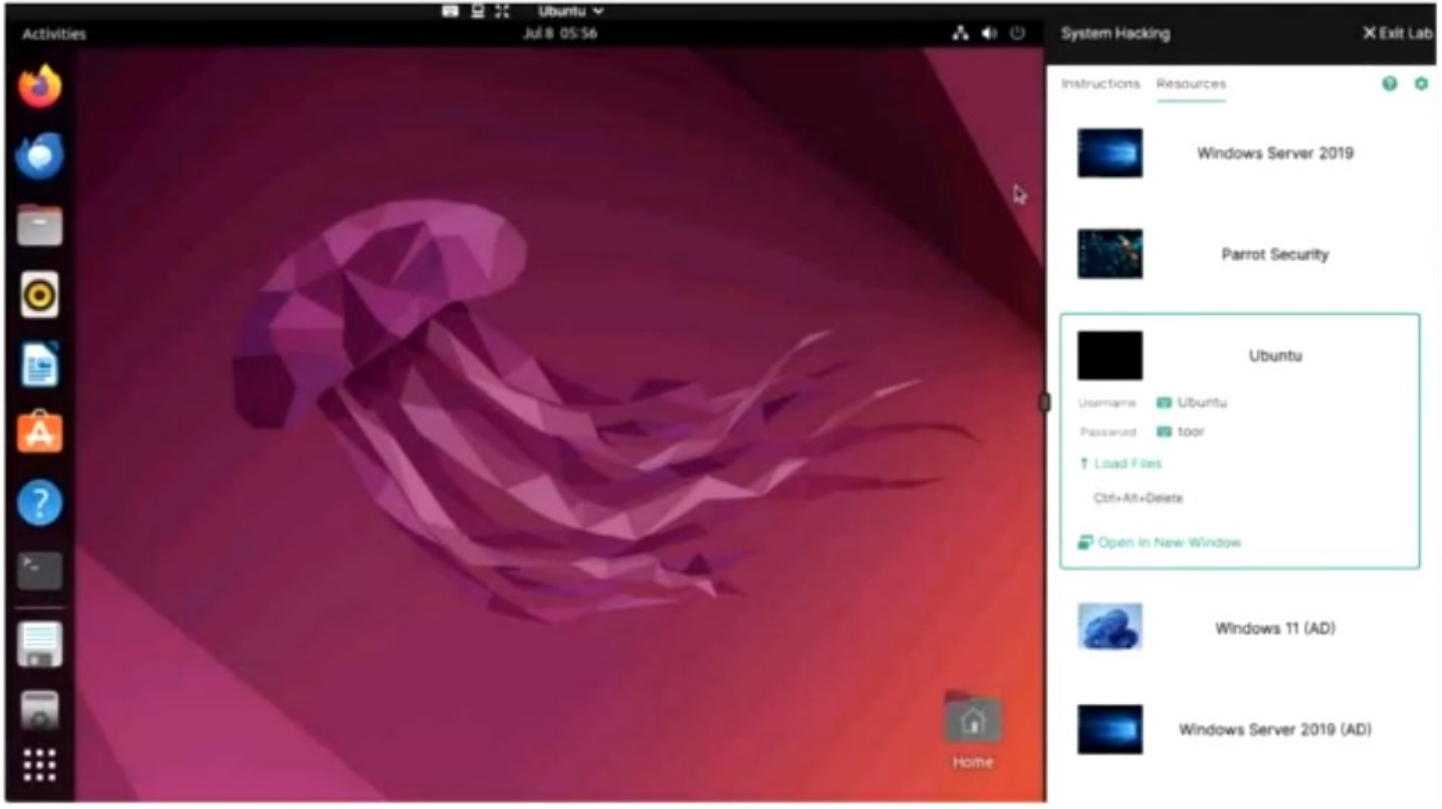
Windows Server 2019 (AD) Machine in iLabs



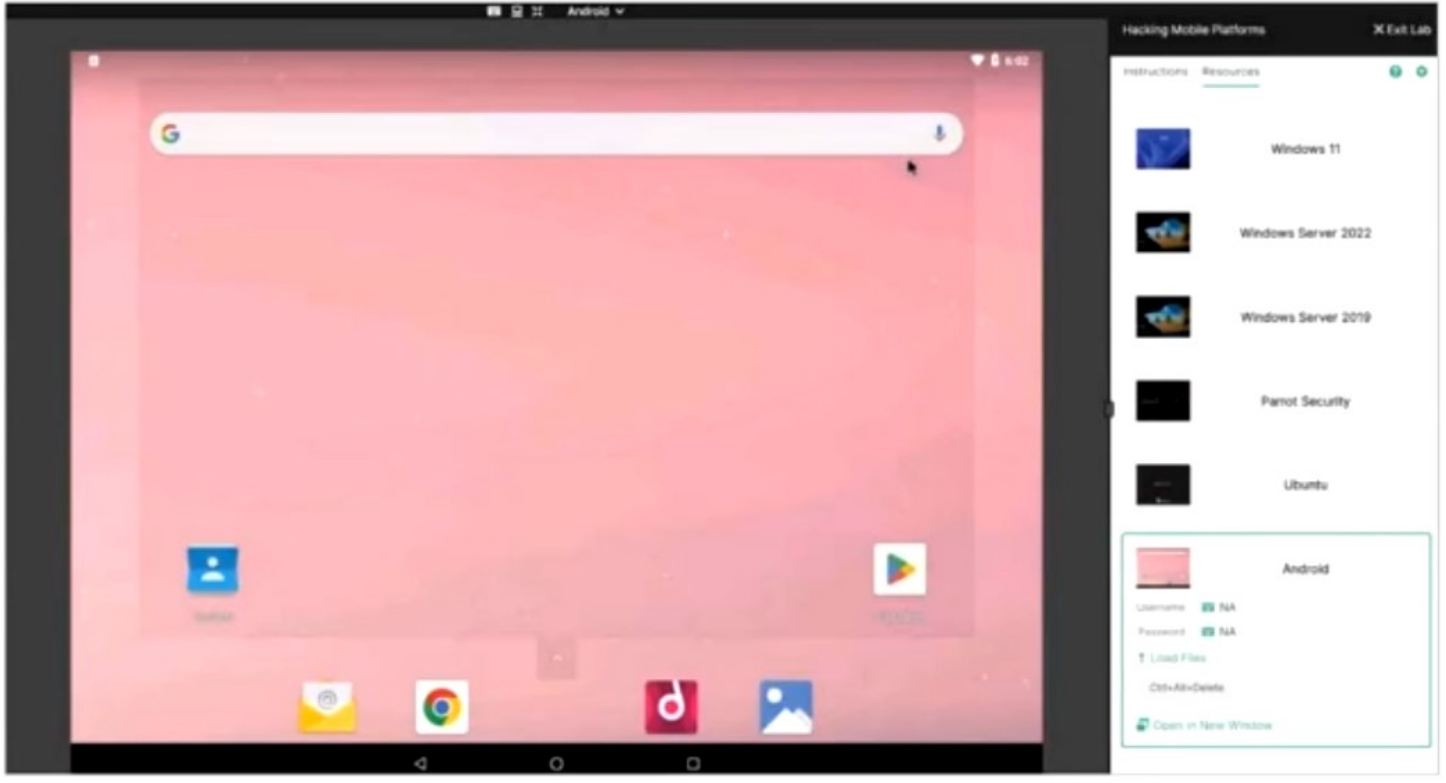
Parrot Security Machine in iLabs



Ubuntu Linux Machine in iLabs



Android Machine in iLabs



EC-Council iLabs Benefits

Student Benefits

- Fully Automated Lab Environment
- Unlimited Access over Subscription Term
- Simple clientless connection through web browser
- Fully loaded with Windows 11 (64-bit), Windows Server 2022 (64-bit), Windows Server 2019 (64-bit), Parrot Security, Ubuntu, and Android Operating Systems
- **Labs can be performed at 24x7 from anywhere!**

Instructor/ATC Benefits

- No more difficult Lab Setup
- No Software licensing Fees
- No Hardware to maintain
- Full Controls to reset or re-spin systems live
- Instant recovery

Agenda 07

What Should You Ensure Before Going to Class

Prepare Well !!!

- Please note that this is a **proposed course structure** for the CEHv13 course.
- While most instructors have their own style, this document is **meant to be a guide** from which instructors can understand EC-Council's vision.
- Instructors **MUST be certified in the CEHv13** PRIOR to the delivery of the program.
- Instructors must have **access to all course material**, including instructor slides, courseware, tools, lab setup guide, and supporting material available in ASPEN before going to the class
- Instructors must practice the labs before going to the class and must be **proficient in the usage of iLabs**.
- Several labs in the **Exercise** slides are marked as **Self-study**. These labs are available for students to practice on their own. Self-study labs are available separately as the **CEH Self Study Upgrade Lab Pack**.

Agenda 08

How to Teach CEH

Module 00

Student Introduction

Student Introduction

- Welcome the students to the **course** and **introduce yourself**
- Provide a brief overview of your **background** to establish credibility
- **Ask students to introduce themselves** and provide their background, experience, and expectations from the course
- Ask the students if they have **Linux** and **C++** programming experience
- **Write your name on the whiteboard corner** and do not erase this for the duration of the class so that the students will know your name
- Inform the students in your class what is required for the **CEH course**. Describe the **contents of the course materials**

Student Introduction

- Tell the students that this is a hands-on class and **50%** of class time will be spent on practicals/demonstrations

- Tell the students about the **modules that will be covered in the class** and also explain the CEH exam and the process of taking it

- You can give information to the students on **when the exam will be conducted**, **the cost of the exam**, **the total number of questions**, **the passing score**, etc. (consult with the training center regarding the exam delivery, they might have a prepaid exam voucher)

- Give them the link of the live website to hack for testing purposes in the class which is ***http://www.certifiedhacker.com*** (Write this information on the corner of the whiteboard)

Module 01

Introduction to Ethical Hacking

What is Covered in Module 01?

The module briefs about **information security**, **hacking methodologies and frameworks**; and **hacking concepts**

Addresses the pre-requisites to become an ethical hacker and also the **scope and limitations of ethical hacking**

Discusses various **information security controls** such as Information Assurance (IA), Defense-in-Depth, risk management, cyber threat intelligence, threat modeling, incident management, AI/ML, etc.

Discusses various **information security laws and standards**

How to Teach this Module?

- Discuss various elements of **information security**
- Discuss **classification of attacks**
- Explain the **hacking concepts** and Different **hacker classes**
- Discuss **necessity**, **scope**, and **limitations** of ethical hacking
- Explain various **hacking methodologies and frameworks**
- Discuss **CEH ethical hacking** framework
- Explain the importance of **risk management**
- Discuss **cyber threat intelligence** and **threat modeling**
- Discuss the **incident management** process
- Explain the role of **artificial intelligence** and **machine learning** in cyber security
- Discuss various **information security laws and standards**

Exercise

This module does not contain any hands-on exercise.

Module 02

Footprinting and Reconnaissance

What is Covered in Module 02?

- Discusses **footprinting** concepts
- Briefs on various **footprinting methodologies**, such as footprinting through search engines, Whois footprinting, DNS footprinting, etc.
- Provides an assessment of various footprinting tasks using **advanced tools** and **AI** to collect information regarding a target system or network
- Discusses various **footprinting countermeasures** to defend against footprinting attacks

How to Teach this Module?

- Discuss various **footprinting** concepts
- Discuss footprinting through **search engines**
- Explain footprinting through **Internet research services**
- Discuss footprinting through **social networking sites**
- Explain **Whois Footprinting**
- Discuss **DNS footprinting**
- Explain **network footprinting**
- Discuss **email footprinting**
- Discuss footprinting through **social engineering**
- Demonstrate footprinting tasks using **advanced tools** and **AI**
- Show how to **create** and **run custom Python scripts** to automate footprinting tasks with AI
- Discuss various **footprinting countermeasures**

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Footprinting Through Search Engines
  - 1.1: Gather Information using Advanced Google Hacking Techniques
  - 1.2: Gather Information from Video Search Engines (Self-study)
  - 1.3: Gather Information from FTP Search Engines (Self-study)
  - 1.4: Gather Information from IoT Search Engines (Self-study)
- **Lab 02:** Perform Footprinting Through Internet Research Services
  - 2.1: Find the Company's Domains, Sub-domains and Hosts using Netcraft and DNSDumpster
  - 2.2: Gather Personal Information using PeekYou Online People Search Service (Self-study)
  - 2.3: Gather Information using Deep and Dark Web Searching (Self-study)
  - 2.4: Determine Target OS Through Passive Footprinting (Self-study)
- **Lab 03:** Perform Footprinting Through Social Networking Sites
  - 3.1: Gather Personal Information from Various Social Networking Sites using Sherlock
- **Lab 04:** Perform Whois Footprinting
  - 4.1: Perform Whois Lookup using DomainTools
- **Lab 05:** Perform DNS Footprinting
  - 5.1: Gather DNS Information using nslookup Command Line Utility and Online Tool
  - 5.2: Gather Information of Subdomain and DNS Records using SecurityTrails (Self-study)
  - 5.3: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon (Self-study)

Exercise

Demonstrate the following labs

- **Lab 06:** Perform Network Footprinting
  - 6.1: Locate the Network Range (Self-study)
  - 6.2: Perform Network Tracerouting in Windows and Linux Machines
- **Lab 07:** Perform Email Footprinting
  - 7.1: Gather Information About a Target by Tracing Emails using eMailTrackerPro
  - 7.2: Gather information About a Target Email using Holehe (Self-study)
- **Lab 08:** Perform Footprinting using Various Footprinting Tools
  - 8.1: Footprinting a Target using Recon-ng
  - 8.2: Footprinting a Target using Maltego (Self-study)
  - 8.3: Footprinting a Target using FOCA (Self-study)
  - 8.4: Footprinting a Target using OSINT Framework (Self-study)
  - 8.5: Footprinting a Target using OSINT.SH (Self-study)
  - 8.6: Footprinting a Target using Web Check (Self-study)
- **Lab 09:** Perform Footprinting using AI
  - 9.1: Footprinting a Target using Shellgpt

Module 03

Scanning Networks

What is Covered in Module 03?

- Discusses **network scanning concepts**
- Provides an assessment of various **scanning tools** used to collect information regarding **hosts**, **ports**, and **services** in a network
- Briefs on **scanning methodology** used to identify the **hosts**, **ports**, **services**, and **OS** in a network
- Discusses various techniques to **scan beyond IDS and firewall**
- Explains various **network scanning countermeasures**

How to Teach this Module?

- Discuss the **network scanning** concepts
- Show various **tools used** to scan the network
- Illustrate various scanning techniques for **host discovery**
- Discuss various scanning techniques for **port and service discovery**
- Explain various scanning techniques for **banner grabbing/OS fingerprinting**
- Show how to perform host discovery, port scanning, service version discovery, and **OS discovery with AI**
- Discuss various **IDS/firewall evasion** techniques
- Explain how to use **proxies** for an attack
- Discuss various types of **anonymizers**
- Explain how to **defend** against various scanning techniques
- Discuss various **IP spoofing detection** techniques

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Host Discovery
  - 1.1: Perform Host Discovery using Nmap
  - 1.2: Perform Host Discovery using Angry IP Scanner (Self-study)
- **Lab 02:** Perform Port and Service Discovery
  - 2.1: Perform Port and Service Discovery using MegaPing (Self-study)
  - 2.2: Perform Port and Service Discovery using NetScanTools Pro (Self-study)
  - 2.3: Perform Port Scanning using sx Tool (Self-study)
  - 2.4: Explore Various Network Scanning Techniques using Nmap
  - 2.5: Explore Various Network Scanning Techniques using Hping3 (Self-study)
  - 2.6: Scan a Target Network using Rustscan (Self-study)
- **Lab 03:** Perform OS Discovery
  - 3.1: Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark (Self-study)
  - 3.2: Perform OS Discovery using Nmap Script Engine (NSE)

Exercise

Demonstrate the following labs

- **Lab 04:** Scan beyond IDS and Firewall
  - 4.1: Scan beyond IDS/Firewall using various Evasion Techniques
  - 4.2: Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall (Self-study)
  - 4.3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond the IDS/Firewall (Self-study)
- **Lab 05:** Perform Network Scanning using Various Scanning Tools
  - 5.1: Scan a Target Network using Metasploit
- **Lab 06:** Perform Network Scanning using AI
  - 6.1: Scan a Target using ShellGPT

Module 04

Enumeration

What is Covered in Module 04?

- This module explains the **process of extracting** usernames, machine names, network resources, shares, and services from a system
- Describes various **enumeration techniques** for protocols and services such as NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, etc.
- Illustrates the enumeration tools that can be used to **extract the data**
- Discusses various **enumeration countermeasures** to defend against enumeration attacks

How to Teach this Module?

1. Discuss the **concept of enumeration**

2. Explain the various techniques for **enumeration** such as NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Unix/Linux, and SMB

3. Illustrate various **tools to enumerate** NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Unix/Linux, and SMB

4. Show how to create and run custom scripts to automate network **enumeration tasks with AI**

5. Explain **how to defend** against various enumerations attacks

Exercise

Demonstrate the following labs

- **Lab 01:** Perform NetBIOS Enumeration
  - 1.1: Perform NetBIOS Enumeration using Windows Command-Line Utilities
  - 1.2: Perform NetBIOS Enumeration using NetBIOS Enumerator (Self-study)
  - 1.3: Perform NetBIOS Enumeration using an NSE Script (Self-study)
- **Lab 02:** Perform SNMP Enumeration
  - 2.1: Perform SNMP Enumeration using snmp-check (Self-study)
  - 2.2: Perform SNMP Enumeration using SoftPerfect Network Scanner (Self-study)
  - 2.3: Perform SNMP Enumeration using SnmpWalk
  - 2.4: Perform SNMP Enumeration using Nmap (Self-study)
- **Lab 03:** Perform LDAP Enumeration
  - 3.1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)
  - 3.2: Perform LDAP Enumeration using Python and Nmap (Self-study)
- **Lab 04:** Perform NFS Enumeration
  - 4.1: Perform NFS Enumeration using RPCScan and SuperEnum

Exercise

Demonstrate the following labs

- **Lab 05:** Perform DNS Enumeration
  - 5.1: Perform DNS Enumeration using Zone Transfer
  - 5.2: Perform DNS Enumeration using DNSSEC Zone Walking (Self-study)
  - 5.3: Perform DNS Enumeration using Nmap (Self-study)
- **Lab 06:** Perform SMTP Enumeration
  - 6.1: Perform SMTP Enumeration using Nmap
- **Lab 07:** Perform RPC, SMB, and FTP Enumeration
  - 7.1: Perform RPC and SMB Enumeration using NetScanTools Pro (Self-study)
  - 7.2: Perform SMB Enumeration using SMBeagle (Self-study)
  - 7.3: Perform RPC, SMB, and FTP Enumeration using Nmap (Self-study)
- **Lab 08:** Perform Enumeration using Various Enumeration Tools
  - 8.1: Enumerate Information using Global Network Inventory
  - 8.2: Enumerate Information from Windows and Samba Hosts using Enum4linux (Self-study)
- **Lab 09:** Perform Enumeration using AI
  - 9.1: Scan a Target using ShellGPT

Module 05

Vulnerability Analysis

What is Covered in Module 05?

- Discusses **vulnerability assessment concepts**
- Explains **vulnerability classification** and **assessment types**
- Briefs the working of **vulnerability assessment tools**
- Discusses how to generate and analyze **vulnerability assessment reports**

How to Teach this Module?

1. Discuss about **vulnerability classification**
2. Explain the importance of **vulnerability scoring systems**
3. Discuss the **vulnerability management life cycle**
4. Explain how to perform **vulnerability research**
5. Describe **vulnerability scanning** and **analysis**
6. Explain various **types of vulnerability scanning**
7. Illustrate various **tools** used to conduct **vulnerability assessment**
8. Demonstrate how to perform a vulnerability assessment using **AI-powered vulnerability assessment tools**
9. Show how to perform a vulnerability assessment using a **Python script with AI**
10. Explain how to generate and analyze **vulnerability assessment reports**

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Vulnerability Research with Vulnerability Scoring Systems and Databases
  - 1.1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)
  - 1.2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE) (Self-study)
  - 1.3: Perform Vulnerability Research in National Vulnerability Database (NVD) (Self-study)
  - 1.4: Perform Vulnerability Research using Searchsploit (Self-study)
  - 1.5: Perform Vulnerability Research using Vuldb (Self-study)
- **Lab 02:** Perform Vulnerability Assessment using Various Vulnerability Assessment Tools
  - 2.1: Perform Vulnerability Analysis using OpenVAS
  - 2.2: Perform Vulnerability Scanning using Nessus (Self-study)
  - 2.3: Perform Vulnerability Scanning using Sniper (Self-study)
- **Lab 03:** Perform Vulnerability Analysis using AI
  - 3.1: Perform Vulnerability Analysis using ShellGPT

Module 06

System Hacking

What is Covered in Module 06?

- Describes the CEH system hacking process which is classified into four stages: **gaining access** (by cracking passwords and exploiting vulnerabilities), **escalating privileges**, **maintaining access** (executing applications, hiding files, and establishing persistence), and **clearing logs** (covering tracks)

- Explains the **hacking tools** (exploitation tools, keyloggers, spywares, and rootkits, etc.) that aid the hacking process

- Presents the **countermeasures** that can be applied at every stage to prevent an attack on the system

How to Teach this Module?

- Explain how passwords are stored in **Windows SAM**
- Discuss **NTLM** and **Kerberos authentication** process
- Discuss various **password attacks**
- Illustrate various **tools** used to crack the password
- Explain various **vulnerability exploitation techniques**
- Demonstrate various **AI-powered vulnerability exploitation tools**
- Discuss various **privilege escalation techniques** and how to defend against it
- Discuss various techniques to create and maintain **remote access to the system**
- Discuss various **keystroke loggers** and **spywares**
- Explain how to defend against **keyloggers** and **spywares**
- Discuss various types of **rootkits** and explain how they work
- Explain various techniques used for **detecting rootkits**
- Explain how to **create NTFS streams** and how to defend against it
- Illustrate the working of **steganography** and discuss its various types
- Explain various **steganalysis methods** and **steganography detection tools**
- Explain various techniques to **establish persistence**
- Discuss various techniques to **hide the evidence of compromise (clearing logs)**

Exercise

Demonstrate the following labs

- **Lab 01:** Gain Access to the System
  - 1.1: Perform Active Online Attack to Crack the System's Password using Responder
  - 1.2: Perform Active Online Attack to Crack the System's Password using NTLM Theft (Self-study)
  - 1.3: Audit System Passwords using L0phtCrack (Self-study)
  - 1.4: Find Vulnerabilities on Exploit Sites (Self-study)
  - 1.5: Exploit Client-Side Vulnerabilities and Establish a VNC Session (Self-study)
  - 1.6: Gain Access to a Remote System using Reverse Shell Generator
  - 1.7: Gain Access to a Remote System using Image File Dropper (Self-study)
  - 1.8: Perform Buffer Overflow Attack to Gain Access to a Remote System
- **Lab 02:** Perform Privilege Escalation to Gain Higher Privileges
  - 2.1: Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities (Self-study)
  - 2.2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter (Self-study)
  - 2.3: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys
  - 2.4: Perform SSH-bruteforce Attack and Escalate Privileges by Exploiting Client-Side Vulnerabilities (Self-study)
  - 2.5: Escalate Privileges to Gather Hashdump using Mimikatz (Self-study)

Exercise

Demonstrate the following labs

- **Lab 03:** Maintain Remote Access and Hide Malicious Activities
  - 3.1: User System Monitoring and Surveillance using Spyrix
  - 3.2: Hide Files using NTFS Streams (Self-study)
  - 3.3: Image Steganography using OpenStego and StegOnline (Self-study)
  - 3.4: Maintain Persistence by Abusing Boot or Logon Autostart Execution (Self-study)
  - 3.5: Maintain Persistence by Modifying Registry Run Keys
  - 3.6: Gain Access using Havoc and Maintain Persistence using SharPersist (Self-study)
  - 3.7: Maintain Domain Persistence by Exploiting Active Directory Objects (Self-study)
  - 3.8: Privilege Escalation and Maintain Persistence using WMI (Self-study)
- **Lab 04:** Clear Logs to Hide the Evidence of Compromise
  - 4.1: View, Enable, and Clear Audit Policies using Auditpol (Self-study)
  - 4.2: Clear Windows Machine Logs using Various Utilities
  - 4.3: Clear Linux Machine Logs using the BASH Shell
  - 4.4: Hiding Artifacts in Windows and Linux Machines (Self-study)
- **Lab 05:** Perform Active Directory (AD) Attacks using various tools
  - 5.1: Perform AD Attacks using Various Tools
- **Lab 06:** Perform System Hacking using AI
  - 6.1: Perform System Hacking using ShellGPT

Module 07

Malware Threats

What is Covered in Module 07?

- Discusses various **malware and APT concepts**
- Discusses **Trojan**, **viruses**, and **worm** concepts (their types, and how they infect files/systems)
- Explains **fileless malware** concepts
- Discusses **AI-based malware** concepts
- Explains the static and dynamic **malware analysis process**
- Discusses various **countermeasures** to defend against malware attacks
- Lists **anti-malware tools**

How to Teach this Module?

- Explain **malware** and discuss various malware propagation techniques
- Explain **potentially unwanted applications (PUAs)** and adware
- Discuss **APT lifecycle** and **characteristics** of APT
- Explain **how hackers use Trojan to infect the systems**
- Discuss various **types of Trojans**
- Explain the **working of virus** and indications of virus attack
- Discuss various **types of viruses** and explain how they infect the system
- Explain **how hackers use virus to infect the systems**
- Discuss about **computer worms**
- Explain **how hackers use worm to infect the systems**
- Discuss various **fileless malware threats**
- Discuss the working of **AI-based malware and its techniques**
- Explain the **working of fileless malware** and fileless malware **obfuscation techniques**
- Discuss the static and dynamic **malware analysis procedure**
- Explain **how to detect virus** using various techniques
- Explain **how to defend** against Trojans, backdoors, viruses, worms and fileless malware
- Illustrate various **anti-malware tools** and **AI-powered malware detection and analysis tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Gain Access to the Target System using Trojans
  - 1.1: Gain Control over a Victim Machine using the njRAT RAT Trojan
  - 1.2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs (Self-study)
  - 1.3: Create a Trojan Server using Theef RAT Trojan (Self-study)
- **Lab 02:** Infect the Target System using a Malware
  - 2.1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System
  - 2.2: Create a Ransomware using Chaos Ransomware Builder and Infect the Target System (Self-study)
- **Lab 03:** Perform Static Malware Analysis
  - 3.1: Perform Malware Scanning using Hybrid Analysis
  - 3.2: Perform a Strings Search using BinText (Self-study)
  - 3.3: Identify Packaging and Obfuscation Methods using PEid (Self-study)
  - 3.4: Analyze ELF Executable File using Detect It Easy (DIE)
  - 3.5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer (Self-study)
  - 3.6: Extract and Analyze PE Headers using Pestudio (Self-study)
  - 3.7: Perform Malware Disassembly using IDA and OllyDbg
  - 3.8: Analyze Executable Files using capa (Self-study)
  - 3.9: Perform Malware Disassembly using Ghidra (Self-study)

Exercise

Demonstrate the following labs

- **Lab 04:** Perform Dynamic Malware Analysis
  - 4.1: Perform Port Monitoring using TCPView and CurrPorts
  - 4.2: Perform Process Monitoring using Process Monitor
  - 4.3: Perform Registry Monitoring using Reg Organizer (Self-study)
  - 4.4: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol (Self-study)
  - 4.5: Perform Files and Folder Monitoring using PA File Sight (Self-study)
  - 4.6: Perform Device Driver Monitoring using DriverView and Driver Reviver (Self-study)
  - 4.7: Perform DNS Monitoring using DNSQuerySniffer (Self-study)

Module 08

Sniffing

What is Covered in Module 08?

- Briefs about the **basic concepts of sniffing network** and various types of sniffing
- Discusses various **sniffing techniques** such as MAC attacks, DHCP attacks, ARP poisoning, spoofing, DNS poisoning, etc.
- Features various **sniffing tools** and explains how an attacker hacks a network using them
- Discusses on how to **defend against various sniffing attacks**
- Explains various **sniffing detection methods** and **tools**

How to Teach this Module?

- Define the term **sniffing** and explain various **types of sniffing**
- Describe **MAC attacks** and how to defend against MAC attacks
- Explain various **DHCP attacks** and how to defend against DHCP attacks
- Explain various threats of **ARP poisoning** and **exhibit tools** used to perform this attack
- Discuss **how to defend** against ARP poisoning and how to detect ARP spoofing
- Explain various **spoofing attacks** and exhibit tools used to perform this attack
- Discuss **how to defend** against spoofing attacks
- Elaborate various **DNS poisoning** techniques and explain in detail how to secure against them
- Demonstrate various **sniffing tools** and show how an attacker sniffs a network using them
- Discuss how to **defend against sniffing**
- Explain **sniffing detection techniques** and tools used to detect sniffing attempts

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Active Sniffing
  - 1.1: Perform MAC Flooding using macof
  - 1.2: Perform a DHCP Starvation Attack using Yersinia
  - 1.3: Perform ARP Poisoning using arpspoof (Self-study)
  - 1.4: Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel (Self-study)
  - 1.5: Spoof a MAC Address using TMAC and SMAC (Self-study)
  - 1.6: Spoof a MAC Address of Linux Machine using macchanger (Self-study)
- **Lab 02:** Perform Network Sniffing using Various Sniffing Tools
  - 2.1: Perform Password Sniffing using Wireshark
  - 2.2: Analyze a Network using the Omnipeek Network Protocol Analyzer (Self-study)
- **Lab 03:** Detect Network Sniffing
  - 3.1: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network
  - 3.2: Detect ARP Poisoning using the Capsa Network Analyzer (Self-study)

Module 09

Social Engineering

What is Covered in Module 09?

- Introduces social engineering concepts and various **attack phases**
- Describes the different **types of social engineering techniques** with examples
- Explains various types of **insider threats**
- Explains in detail how **impersonation on social engineering sites** is carried out
- Briefs how attackers obtain and exploit **personally identifiable information** and authenticate themselves, in order to impersonate victim
- Lists various social engineering, insider threats, and **identity theft countermeasures**

How to Teach this Module?

- Explain what is **social engineering** and its phases
- Discuss the **common targets** of social engineering attack
- Explain various **types of social engineering techniques (human-based, computer-based, mobile-based)** with examples and tools
- Discuss various types of **insider threats**
- Illustrate how **impersonation** on social engineering sites is carried out
- Demonstrate how to perform **impersonation using AI**
- Describe what is **identity theft** and how to steal identity?
- Discuss social engineering, insider threats, and **identity theft countermeasures**
- Demonstrate the **anti-phishing tools** to detect phishing emails and websites
- Illustrate common social engineering tactics and prevention strategies

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Social Engineering using Various Techniques
  - 1.1: Sniff Credentials using the Social-Engineer Toolkit (SET)
  - 1.2: Sniff Credentials using Dark-Phish (Self-study)
- **Lab 02:** Detect a Phishing Attack
  - 2.1: Detect Phishing using Netcraft
  - 2.2: Detect Phishing using PhishTank (Self-study)
- **Lab 03:** Social Engineering using AI
  - 3.1: Craft Phishing Emails with ChatGPT

Module 10

Denial-of-Service

What is Covered in Module 10?

1. Explains **DoS/DDoS concepts** and various **attack techniques**
2. Discusses **Botnets** and scanning methods for finding vulnerable machines
3. Explains various **techniques to perform DoS** and **DDoS attacks**
4. Demonstrates various **DoS/DDoS attack tools**
5. Discusses various countermeasures to **detect**, **prevent**, and **mitigate DoS/DDoS attacks**
6. Illustrates various **DoS/DDoS protection tools**

How to Teach this Module?

- Explain **DoS** and **DDoS attack concepts**
- Describe **Bots** and **Botnets** with the use of examples
- Explain the typical **Botnet setup**
- Describe some of the common **DoS/DDoS attack techniques**
- Showcase **tools** and **techniques** used to demonstrate DoS/DDoS attacks
- Explain various techniques to **detect**, **prevent**, and **mitigate** DoS/DDoS attacks
- Discuss various **countermeasures** to defend DoS/DDoS attacks
- Explain various techniques to **defend against Botnets**
- Demonstrate various **DoS/DDoS protection tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Perform DoS and DDoS Attacks using Various Techniques
  - 1.1: Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit (Self-study)
  - 1.2: Perform a DoS Attack on a Target Host using hping3 (Self-study)
  - 1.3: Perform a DDoS Attack using HOIC (Self-study)
  - 1.4: Perform a DDoS Attack using LOIC (Self-study)
  - 1.5: Perform a DDoS Attack using PyDDos and PyFloodder (Self-study)
  - 1.6: Perform a DDoS attack using ISB and UltraDDOS-v2 tools
  - 1.7: Perform a DDoS Attack using Botnet
- **Lab 02:** Detect and Protect Against DoS and DDoS Attacks
  - 2.1: Detect and Protect against DDoS Attack using Anti DDoS Guardian

Module 11

Session Hijacking

What is Covered in Module 11?

- This module explains **session hijacking concepts**
- Discusses about **application** and **network-level session hijacking**
- Explains various **session hijacking tools**
- Explains **countermeasures** to prevent session hijacking attacks

How to Teach this Module?

1. Explain various **session hijacking concepts** and **process**
2. Explain the difference between **spoofing** and **hijacking**
3. Discuss various **application-level session hijacking** attacks
4. Discuss various **network-level session hijacking** attacks
5. Showcase various **tools** used to perform session hijacking
6. Illustrate various **session hijacking detection tools**
7. Discuss the **countermeasures** to defend against session hijacking attacks
8. Explain various **approaches to prevent session hijacking attacks**
9. Explain various **approaches to prevent MITM attacks**
10. Explain **IPsec architecture** and modes of IPsec

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Session Hijacking
  - 1.1: Hijack a Session using Caido
  - 1.2: Intercept HTTP Traffic using bettercap (Self-study)
  - 1.3: Intercept HTTP Traffic using Hetty
- **Lab 02:** Detect Session Hijacking
  - 2.1: Detect Session Hijacking using Wireshark

Module 12

Evading IDS, Firewalls, and Honeypots

What is Covered in Module 12?

- This module gives an introduction to **IDS**, **IPS**, and **firewall** and their types
- Demonstrates various **IDS**, **IPS**, and **firewall solutions**
- Describes various **IDS** and **firewall evasion** techniques
- Explains various **NAC** and **endpoint security evasion** techniques
- Discusses **honeypot concepts** and **honeypot detection techniques**
- Discusses the **countermeasures** to defend against IDS/firewall and endpoint security evasion

How to Teach this Module?

1. Describe briefly about **Intrusion Detection System (IDS)** and their placement
2. Discuss about **Intrusion Prevention System (IPS)**
3. Discuss how an IDS detects an intrusion
4. Explain **firewall**, **firewall architecture** and its **types**
5. Demonstrate **Snort** and its rules
6. List various **IDS**, **IPS**, and **firewall solutions**
7. Discuss various techniques to **evade IDS** and **firewall**
8. Discuss various techniques to **evade NAC** and **endpoint security**
9. Discuss the **concepts of honeypots**, **types of honeypots**, and **honeypot solutions**
10. Explain how to **detect honeypots**
11. Discuss the **countermeasures** to defend against IDS/firewall evasion
12. Discuss the **countermeasures** to defend against endpoint security evasion

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Intrusion Detection using Various Tools
  - 1.1: Detect Intrusions using Snort
  - 1.2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL (Self-study)
  - 1.3: Detect Malicious Network Traffic using HoneyBOT (Self-study)
  - 1.4: Deploy Cowrie Honeypot to Detect Malicious Network Traffic
- **Lab 02:** Evade IDS/Firewalls using Various Evasion Techniques
  - 2.1: Bypass Firewall Rules using HTTP/FTP Tunneling (Self-study)
  - 2.2: Bypass Antivirus using Metasploit Templates (Self-study)
  - 2.3: Bypass Firewall through Windows BITSAdmin

Module 13

Hacking Web Servers

What is Covered in Module 13?

1. Explains **web server concepts**
2. Explains various key **web server attack techniques**
3. Demonstrates **web server attack methodology** and **tools**
4. Explains **countermeasures** to prevent web server attacks
5. Illustrates various **web server security tools**

How to Teach this Module?

1. Explain various **web server security issues**
2. Explain the architecture of **Apache**, **IIS**, and **Nginx** web servers
3. Discuss the vulnerabilities of **Apache**, **IIS**, and **Nginx** web servers
4. Discuss various **attacks on web server**
5. Explain various phases of **web server attack methodology**
6. Showcase various **techniques for hacking a web server using AI**
7. Explain methods used to **detect web server hacking attempts**
8. Discuss the various **countermeasures** to defend against web server attacks
9. Illustrate various **web server security tools**
10. Demonstrate various **web server pen testing tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Footprint the Web Server
  - 1.1: Information Gathering using Ghost Eye (Self-study)
  - 1.2: Perform Web Server Reconnaissance using Skipfish (Self-study)
  - 1.3: Footprint a Web Server using Netcat and Telnet
  - 1.4: Enumerate Web Server Information using Nmap Scripting Engine (NSE)
  - 1.5: Uniscan Web Server Fingerprinting in Parrot Security (Self-study)
- **Lab 02:** Perform a Web Server Attack
  - 2.1: Crack FTP Credentials using a Dictionary Attack
  - 2.2: Exploit the MSSQL Service using xp_cmdshell Function (Self-study)
  - 2.3: Gain Access to Target Web Server by Exploiting Log4j Vulnerability
- **Lab 03:** Perform a Web Server Hacking using AI
  - 3.1: Perform webserver footprinting and attacks using ShellGPT

Module 14

Hacking Web Applications

What is Covered in Module 14?

1. Explains **web application concepts**
2. Lists and explains various **web application threats** and **attacks**
3. Explains **web application hacking methodology** and **tools**
4. Discusses **web API** and **webhooks** concepts
5. Discusses **web application security** and **countermeasures** to defend against web application attacks

How to Teach this Module?

- Give a brief introduction about **web applications** and **how web applications work**
- Discuss the importance of **web services**
- List and explain various **web application threats** with examples
- Describe the **web application hacking methodology**
- Demonstrate various techniques for hacking **web applications using AI**
- Explain the **web API** and **webhooks** concepts
- Discuss the **web API security risks** and **vulnerabilities**
- Explain the **web API hacking methodology**
- Discuss the **best practices** for securing API and webhooks
- Explain the **web application security testing** methods
- Discuss the **web application fuzz testing** and **source code review**
- Explain how to perform **AI-powered fuzz testing** and application security testing
- Explain various **encoding schemes** used to prevent web application attacks
- Discuss how to perform **application whitelisting** and **blacklisting**
- Discuss various **countermeasures** to defend a web application attacks
- Demonstrate various **web application security testing tools** and **firewalls**

Exercise

Demonstrate the following labs

- **Lab 01:** Footprint the Web Infrastructure
  - 1.1: Perform Web Application Reconnaissance using Nmap and Telnet
  - 1.2: Perform Web Application Reconnaissance using WhatWeb (Self-study)
  - 1.3: Perform Web Spidering using OWASP ZAP
  - 1.4: Detect Load Balancers using Various Tools (Self-study)
  - 1.5: Identify Web Server Directories using Various Tools (Self-study)
  - 1.6: Perform Web Application Vulnerability Scanning using SmartScanner
  - 1.7: Identify Clickjacking Vulnerability using ClickjackPoc (Self-study)
- **Lab 02:** Perform Web Application Attacks
  - 2.1: Perform a Brute-force Attack using Burp Suite
  - 2.2: Perform Parameter Tampering using Burp Suite (Self-study)
  - 2.3: Identify XSS Vulnerabilities in Web Applications using PwnXSS (Self-study)
  - 2.4: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications (Self-study)
  - 2.5: Perform Cross-Site Request Forgery (CSRF) Attack (Self-study)
  - 2.6: Perform Remote Code Execution (RCE) Attack
  - 2.7: Enumerate and Hack a Web Application using WPScan and Metasploit (Self-study)
  - 2.8: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server (Self-study)
  - 2.9: Exploit a File Upload Vulnerability at Different Security Levels (Self-study)
  - 2.10: Perform JWT Token Attack (Self-study)

Exercise

Demonstrate the following labs

- **Lab 03:** Detect Web Application Vulnerabilities using Various Web Application Security Tools
  - 3.1: Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner
- **Lab 04:** Perform Web Application Hacking using AI
  - 4.1: Perform Web Application Hacking using ShellGPT

Module 15

SQL Injection

What is Covered in Module 15?

1. Discusses **SQL Injection concepts**
2. Explains various **types of SQL injection attacks** with examples
3. Explains **SQL injection methodology**
4. Explains various **evasion techniques**
5. Explains **countermeasures** to prevent SQL injection attacks
6. Demonstrates various **SQL injection detection tools**

How to Teach this Module?

- Give a brief introduction about **SQL injection attack**
- Give various examples on how a **web application is vulnerable** to SQL injection attacks
- List and explain different **types of SQL injection** attacks
- Discuss various phases of **SQL injection methodology** and how to perform **SQL injection using AI**
- Explain various **evasion techniques**
- Discuss various **countermeasures** to defend SQL injection attacks
- Illustrate various SQL injection **detection techniques** and **tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Perform SQL Injection Attacks
  - 1.1: Perform an SQL Injection Attack on an MSSQL Database (Self-study)
  - 1.2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap
  - 1.3: Perform an SQL Injection to Launch File Inclusion Attack on bWAPP (Self-study)
- **Lab 02:** Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools
  - 2.1: Detect SQL Injection Vulnerabilities using OWASP ZAP
  - 2.2: Detect SQL Injection Vulnerabilities using Ghauri (Self-study)
- **Lab 03:** Perform SQL Injection using AI
  - 3.1: Perform SQL Injection using ShellGPT

Module 16

Hacking Wireless Networks

What is Covered in Module 16?

1. This module explains **wireless concepts**
2. Discusses the **types of wireless encryption** and their working
3. Lists and explains various **wireless threats**
4. Describes **wireless hacking methodology**
5. Discusses how to **defend against wireless attacks**
6. Illustrates various **wireless security tools**

How to Teach this Module?

- Explain **wireless networks** and different forms of wireless networks
- Give a brief introduction about various available **wireless standards** and **Wi-Fi authentication modes**
- Describe the **types of wireless encryption** and their working
- Discuss various **wireless threats**
- Discuss various phases of **wireless hacking methodology**
- Demonstrate how to **crack Wi-Fi encryption**
- Discuss how to defend against Wi-Fi encryption cracking
- Discuss the various **countermeasures** to defend against wireless attacks
- Illustrate various **wireless security tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Footprint a Wireless Network
  - 1.1: Find Wi-Fi Networks in Range using Sparrow-wifi (Self-study)
- **Lab 02:** Perform Wireless Traffic Analysis
  - 2.1: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark
- **Lab 03:** Perform Wireless Attacks
  - 3.1: Find Hidden SSID using MDK (Self-study)
  - 3.2: Crack a WPA2 Network using Aircrack-ng
  - 3.3: Create a Rogue Access Point to Capture Data Packets (Self-study)

Module 17

Hacking Mobile Platforms

What is Covered in Module 17?

1. This module discusses **anatomy of a mobile attack** in detail and explores app sandboxing issues
2. Discusses **Android OS concepts** briefly and demonstrates **hacking Android OS** using various tools
3. Discusses **iOS concepts** briefly and demonstrates **jailbreaking and hacking** iOS using various tools
4. Explains about **mobile device management** and solutions for mobile device management
5. Provides brief knowledge on **mobile security guidelines** and lists various **mobile security tools**

How to Teach This Module?

- Explain various **mobile platform risks** and **anatomy of a mobile attack**
- Discuss **security issues** arising from App stores
- Explain various **mobile platform attacks** with example
- Describe **Android OS architecture** and demonstrate **Android rooting** using various tools
- Illustrate **hacking Android OS** using various hacking tools
- Discuss working of various **Android malware**
- **Discuss** guidelines for **securing Android devices** and demonstrate various **Android security tools**
- Explain **iOS architecture** and showcase tools and techniques to **jailbreak iOS**
- Illustrate **hacking iOS** using various hacking tools
- Discuss various **iOS malware** and guidelines for **securing iOS devices**
- Demonstrate various **iOS device security tools**
- Discuss about the **mobile device management** and solutions for mobile device management
- Illustrate various guidelines for **BYOD security**
- Discuss various **mobile security guidelines** and illustrate various **mobile security tools**

Exercise

Demonstrate the following labs

- **Lab 01:** Hack Android Devices
  - 1.1: Hack an Android Device by Creating Binary Payloads using Parrot Security (Self-study)
  - 1.2: Harvest Users' Credentials using the Social-Engineer Toolkit (Self-study)
  - 1.3: Launch a DoS Attack on a Target Website using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform (Self-study)
  - 1.4: Exploit the Android Platform through ADB using PhoneSploit-Pro
  - 1.5: Hack an Android Device by Creating APK File using AndroRAT
- **Lab 02:** Secure Android Devices using Various Android Security Tools
  - 2.1: Secure Android Devices from Malicious Apps using AVG

Module 18

IoT and OT Hacking

What is Covered in Module 18?

1. This module gives an introduction to **IoT concepts**
2. Briefs about various **IoT attacks** and security problems
3. Discusses the **IoT hacking methodology** and various **IoT hacking tools**
4. Discusses various **countermeasures** to prevent IoT hacking
5. Illustrates various **IoT device management solutions**
6. Explains various **OT concepts**
7. Briefs about various **OT attacks** and security problems
8. Discusses the **OT hacking methodology** and various **OT hacking tools**
9. Discusses various **countermeasures** to prevent OT hacking
10. Discusses various **international OT security organizations**

How to Teach this Module?

- Give a brief introduction to **IoT concepts**
- Explain various **IoT attack surface areas** and vulnerabilities
- List and explain various **IoT threats**, attacks, and malware
- Explain the **IoT hacking methodology**
- Demonstrate various **IoT hacking tools**
- Explain various **countermeasures** to prevent IoT hacking
- Discuss **secure practices** for IoT application development
- Discuss the IoT device management and its solutions

- Give a brief introduction to **OT concepts**
- Explain various **OT challenges** and security problems
- List and explain various **OT vulnerabilities** and **threats**
- Discuss various **OT attacks** and **OT malware**
- Explain the **OT hacking methodology**
- Explain various **countermeasures** to prevent OT hacking
- Discuss how to **secure IT/OT environment**
- Discuss various **international OT security organizations**

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Footprinting using Various Footprinting Techniques
  - 1.1: Gather Information using Online Footprinting Tools
- **Lab 02:** Capture and Analyze IoT Device Traffic
  - 2.1: Capture and Analyze IoT Traffic using Wireshark
- **Lab 03:** Perform IoT Attacks
  - 3.1: Hacking into VoIP based device (Self-study)
  - 3.2: Perform Replay Attack on CAN Protocol

Module 19

Cloud Computing

What is Covered in Module 19?

1. Briefs about the basic **concepts of cloud computing**
2. Explains the importance of **container technology** and **serverless computing** in cloud environment
3. Lists and explains various **cloud computing threats** and **attacks**
4. Illustrates **hacking cloud** using tools
5. Briefs about various **cloud computing security** considerations
6. Discusses various **cloud security tools controls**

How to Teach this Module?

- Define the term **cloud computing** and explain the **types of cloud computing services**
- Discuss cloud vs. **fog computing** vs. **edge computing**
- Discuss **container technology** concepts
- Explain **Docker**, **Kubernetes**, and **serverless computing** concepts
- Discuss various **risks** and **threats to cloud computing**
- Explain various **cloud computing attacks**
- Discuss the **cloud hacking methodology**
- Discuss how to **hack AWS**, **Azure**, and **Google Cloud environments** using tools
- Discuss **best practices** for securing cloud, container, Docker, Kubernetes, and serverless computing environments
- Explain various **cloud security controls**
- Discuss the importance of **zero trust networks**
- Explain the role of **Cloud Access Security Broker (CASB)** in cloud security

Exercise

Demonstrate the following labs

- **Lab 01:** Perform Reconnaissance
  - 1.1: Azure Reconnaissance with AADInternals
- **Lab 02:** Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools
  - 2.1: Enumerate S3 Buckets using lazys3 (Self-study)
  - 2.2: Enumerate S3 Buckets using Grayhatwarfare (Self-study)
  - 2.3: Enumerate S3 Buckets using Cloudbrute (Self-study)
- **Lab 03:** Exploit S3 Buckets
  - 3.1: Exploit Open S3 Buckets using AWS CLI
  - 3.2: Exploit Open S3 Buckets using Bucket Flaws (Self-study)
- **Lab 04:** Perform Privilege Escalation to Gain Higher Privileges
  - 4.1: Enumeration for Privilege Escalation using Cloudfox (Self-study)
  - 4.2: Escalate IAM User Privileges by Exploiting Misconfigured User Policy
- **Lab 05:** Perform vulnerability assessment on docker images
  - 5.1: Vulnerability Assessment on Docker Images using Trivy

Module 20

Cryptography

What is Covered in Module 20?

1. This module gives an introduction to **cryptography concepts**
2. Explains various **encryption algorithms** and **hashing algorithms**
3. Lists and features various **cryptography tools**
4. Discusses **applications of cryptography**
5. Briefs various **cryptanalysis methods** and **cryptography attacks**
6. Explains how to **defend against cryptographic attacks**

How to Teach this Module?

1. Explain **cryptography concepts**, types of cryptography, and their function
2. Explain the **symmetric encryption algorithms**
3. Explain the **asymmetric encryption algorithms**
4. Discuss various **hashing algorithms** and **message digest function calculators**
5. Demonstrate the function of **hardware-based encryption**, **quantum cryptography**, and various **cryptography tools**
6. Discuss **applications of cryptography**
7. Discuss **Public Key Infrastructure (PKI)** and its components
8. Discuss **email** and **disk encryption**
9. Explain various **cryptanalysis methods** and list various **cryptanalysis tools**
10. Discuss various **countermeasures** to defend against cryptographic attacks

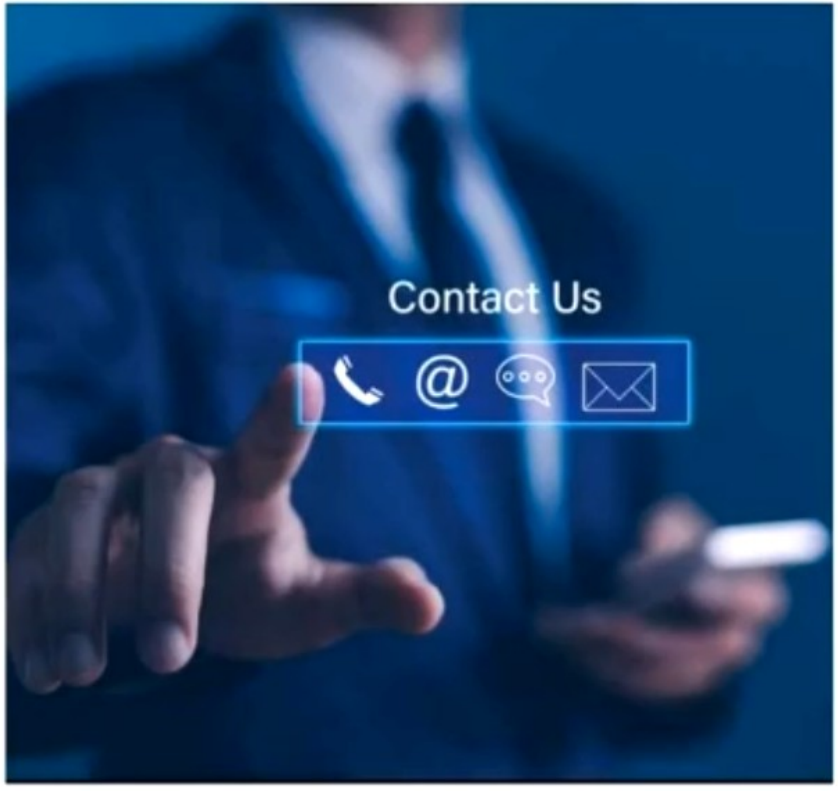
Exercise

Demonstrate the following labs

- **Lab 01:** Encrypt the Information using Various Cryptography Tools
  - 1.1: Perform Multi-layer Hashing using CyberChef
  - 1.2: Calculate MD5 Hashes using MD5 Calculator (Self-study)
  - 1.3: Calculate MD5 Hashes using HashMyFiles (Self-study)
  - 1.4: Perform File and Text Message Encryption using CryptoForge
  - 1.5: Encrypt and Decrypt Data using BCTextEncoder (Self-study)
- **Lab 02:** Create a Self-Signed Certificate
  - 2.1: Create and Use Self-signed Certificates
- **Lab 03:** Perform Email Encryption
  - 3.1: Perform Email Encryption using RMail (Self-study)
  - 3.2: Perform Email Encryption using Mailvelope (Self-study)
- **Lab 04:** Perform Disk Encryption
  - 4.1: Perform Disk Encryption using VeraCrypt
  - 4.2: Perform Disk Encryption using BitLocker Drive Encryption (Self-study)
  - 4.3: Perform Disk Encryption using Rohos Disk Encryption (Self-study)
- **Lab 05:** Perform Cryptanalysis using Various Cryptanalysis Tools
  - 5.1: Perform Cryptanalysis using CrypTool (Self-study)
- **Lab 06:** Perform Cryptography using AI
  - 6.1: Perform Cryptographic Techniques using ShellGPT

Agenda 09

Where to get help



- For any Aspen account issue, courseware and other CEI material access, contact: aspensupport@eccouncil.org
- You can open a support ticket from your Aspen account, or
- Get chat support (24x5)

Instructor Presentation

EC-Council
Official Curricula

EC-Council C|EH v13

Certified Ethical Hacker

EC-Council

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

NOTICE TO THE READER

Table of Contents

Table of Contents


EC-Council
CEH
Module
00
Welcome to Certified Ethical Hacker Class!
Student Introduction

What is CEH Program?

CEH is a comprehensive **ethical hacking** and **information systems security auditing** program focusing on latest security threats, advanced attack vectors and practical real time demonstration of latest **hacking techniques**, methodologies, tools, tricks and security measures

A program developed by **subject matter experts** from all over the world and are constantly updated to ensure that the students are exposed to the latest advances in the space

CEHv13 Course Outline

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT and OT Hacking
19. Cloud Computing
20. Cryptography

What will you Learn?

Students going through CEH training will learn:

- Key issues plaguing the information security world, hacking methodologies and frameworks, information security controls, and information security laws and standards
- Different types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- Different types of vulnerability assessment and vulnerability assessment tools
- System hacking methodology
- Different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures
- Various packet sniffing techniques and sniffing countermeasures
- Social engineering techniques, identity theft, and countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures

What will you Learn?

Students going through CEH training will learn:

- Firewall, IDS, IPS, honeypot, NAC, and endpoint evasion techniques, evasion tools, and countermeasures
- Different types of web server, web application, and web API attacks, hacking methodology, hacking tools, and countermeasures
- SQL injection attacks, injection methodology, evasion techniques, and SQL injection countermeasure
- Different types of wireless encryption, wireless threats, wireless hacking methodology, wireless hacking tools, Wi-Fi security tools, and countermeasures
- Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools
- Different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures
- Various cloud computing technologies, cloud computing threats, attacks, hacking methodology (AWS, Microsoft Azure, Google Cloud, and container hacking), and security techniques and tools
- Different types of encryption algorithms, cryptography tools, applications of cryptography, cryptography attacks, and cryptanalysis tools
- AI-driven ethical hacking

CEH Class Speed

1. The CEH class is **extremely fast paced**

2. It is highly recommended that candidates pursuing this course have a fundamental understanding of **operating systems**, **file systems**, **computer networks**, **TCP/IP protocols**, **information security controls**, basic network troubleshooting, data leakage, data backup, and risk management

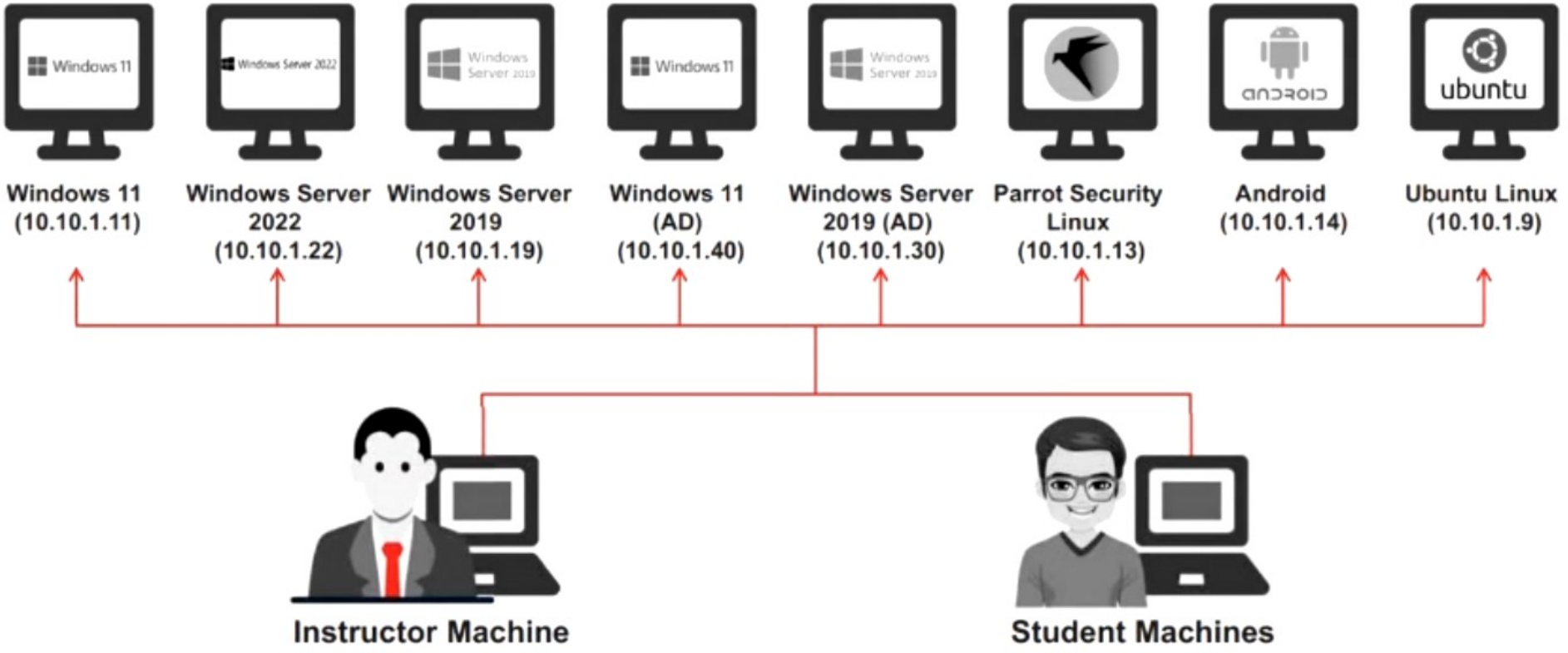
3. There are tons of hacking **tools** and hacking **technologies** covered in the curriculum.
The instructor **WILL NOT** be able to demonstrate **ALL** the tools in this class

4. The students are required to **practice with the tools** not demonstrated in the class on their own

Lab Sessions

1. Lab Sessions are designed to **reinforce** the classroom sessions
2. The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
3. There are tons of labs in the lab manual. Please practice these labs back at home
4. You can also subscribe to CEH CyberQ, a cloud-based virtual lab platform, at a cost to **practice CEH labs 24x7 from anywhere**

Advanced Lab Environment



Instructor and Student Machine Operating System: Any Operating System Capable of Running VMware (Fully Patched)

CEHv13 Exam Information

1. Exam Title: Certified Ethical Hacker
2. Exam Code: 312-50 (ECC Exam Portal) / 312-50 (VUE)
3. Number of Questions: 125
4. Duration: 4 hours
5. Availability: ECC Exam Portal / VUE
6. Passing Score: Please refer https://cert.eccouncil.org/faq.html

- ✓ The training center / instructor will advise you about the exam schedule and voucher details
- ✓ This is a difficult exam and requires extensive knowledge of CEH Core Modules

Let's Start Hacking!