# KnowledgeWoods
## Education . Training . Consulting

**Global Standard**
Aligned to Global Standards

**HD Quality Audio/Video Sessions**

**Storyline Driven Learning**

**Course end Assessment**

**Email Based Query Support**

**24/7 Access**

# Certified Ethical Hacker (CEH) v8

**Estimated Duration (30 Hrs.)**

**skillsoft**

**PMI** Registered Education Provider — Project Management Institute

**Microsoft Partner** — Silver Project and Portfolio Management — Silver Learning

**PRINCE2** — APPROVED EXAMINATION ORGANIZATION

**ITIL** — TRAINING ORGANIZATION — ACCREDITED BY PEOPLECERT

**PEARSON** — VUE-Authorized Test Center

## Certified Ethical Hacker (CEH) v8: Hacking and Penetration Testing

**Duration: 1.5 Hour**

- Match types of information security threats to examples
- Put the phases of a hacking attack in order
- Put the steps for creating and implementing security policies into the correct order
- Identify ways to assess the effectiveness of security policies and procedures
- Determine the type of penetration test to perform in a given situation
- Identify factors to consider when outsourcing penetration testing
- Identify effective penetration testing techniques in a given scenario

## Certified Ethical Hacker (CEH) v8: Footprinting and Reconnaissance

**Duration: 1.5 Hour**

- Recognize the purpose of footprinting
- Identify methods used to mirror a web site
- Match the competitive intelligence information you can obtain with the web site you use to obtain it
- Identify social engineering techniques
- Differentiate between footprinting tools
- Identify footprinting techniques and tools

## Certified Ethical Hacker (CEH) v8: Network Scanning

**Duration: 1.5 Hour**

- Dentify the purposes of network scanning
- Match the type of scan with its description
- Match the network scanning tool to its purpose
- Identify tools used to hide an attacker's identity
- Identify methods used to bypass censorship
- Identify the methods performed as part of scanning penetration testing
- Identify the techniques and tools used in network scanning

### Certified Ethical Hacker (CEH) v8: Enumeration and Cryptography

**Duration: 1.5 Hour**

- Recognize the steps of the enumeration phase of an attack
- Match the tool to the type of hosts it can enumerate
- Match the enumeration tool to the network protocol it operates over
- Match the enumeration countermeasure to the protocol it protects
- Identify characteristics of symmetric and asymmetric encryption
- Match the encryption algorithm to its characteristics
- Match the components of public key infrastructure to their descriptions
- Match the attack on cryptographic systems to its description
- Recognize the characteristics of the enumeration phase of an attack and countermeasures to take against enumeration

### Certified Ethical Hacker (CEH) v8: System Hacking

**Duration: 2 Hour**

- Match the stage of system hacking to the technique or exploit used
- Identify the characteristics of types of password attacks
- Match the lm/ntlm version to its attributes
- Identify the countermeasures against keylogging
- Identify countermeasures against spyware
- Match the method of rootkit detection with its description
- Identify the types of files that can have hidden messages added using least significant bit insertion
- Identify the tools used to cover the tracks of an intruder
- Identify the techniques and tools used in system hacking

### Certified Ethical Hacker (CEH) v8: Malware Hacking

**Duration: 2 Hour**

- Recognize techniques for getting trojans to evade antivirus software
- Match the trojan to its type
- Identify the purpose of specific trojans
- Identify the tools used to detect trojans by scanning for suspicious open ports
- Identify trojan countermeasures
- Recognize the definition and characteristics of a virus
- Identify the characteristics of a worm
- Identify the purpose and characteristics of sheep dip
- Identify and counter types of malware

## Certified Ethical Hacker (CEH) v8: Sniffing

**Duration: 1.5 Hour**

- Match each type of sniffing to its descriptions
- Match dhcp attacks with their descriptions and countermeasures
- Differentiate between arp attack tools and countermeasures
- Identify dns poisoning attacks
- Identify the countermeasures against sniffing
- Identify sniffing attacks and countermeasures

## Certified Ethical Hacker (CEH) v8: Social Engineering

**Duration: 0.5 Hour**

- Recognize social engineering
- Match social engineering activities to their types
- Identify the risks of social engineering through impersonation
- Identify social engineering countermeasures
- Identify social engineering techniques and countermeasures

## Certified Ethical Hacker (CEH) v8: Denial of Service and Session Hijacking

**Duration: 1 Hour**

- Identify permanent denial-of-service attacks
- Identify hardware botnet tools
- Identify which type of filtering defends against botnets and ddos
- Match the type of session hijacking attack to its characteristics
- Identify application-level hijacking attacks
- Identify true statements about ipsec
- Identify the characteristics of and countermeasures to denial-of-service and session hijacking attacks

## Certified Ethical Hacker (CEH) v8: Hacking Web Servers

**Duration: 1.5 Hour**

- Identify reasons why web servers are often compromised
- Differentiate between different types of web server attacks
- Recognize web server identification tools
- Identify precautionary steps to take to protect against web server attacks
- Sequence the steps you would perform to complete a penetration test on your web servers
- Identify web server hacking techniques and countermeasures against them

## Certified Ethical Hacker (CEH) v8: Hacking Web Applications

**Duration: 1.5 Hour**

- Identify common attack vectors for web applications
- Identify command injection attacks
- Match the layer to the web service attack type that can be performed at that layer
- Match the hacking activity to the stage in the web application hacking methodology
- Match the web application hacking countermeasure to the type of attack it helps defend against
- Determine what you test for at which stage of web application penetration
- Identify web application hacking techniques and tools and how to counter them

## Certified Ethical Hacker (CEH) v8: SQL Injection

**Duration: 1.5 Hour**

- Identify correct statements about sql injection
- Recognize characteristics of methods of testing for sql injection vulnerabilities
- Identify the characteristics of sql databases
- Identify the characteristics of sql injection tools
- Identify the characteristics of sql injection countermeasure tools
- Identify and counter sql injection techniques and tools

### Certified Ethical Hacker (CEH) v8: Hacking Wireless Networks

**Duration: 1.5 Hour**

- Identify wireless security standards
- Match the type of wireless attack to an example
- Identify wireless hacking discovery and analysis tools
- Identify types of wireless hacking attacks
- Identify types of bluetooth attacks
- Recognize the characteristics of wireless ips tools
- Identify wireless network hacking techniques and tools and how to counter them

### Certified Ethical Hacker (CEH) v8: Hacking Mobile Platforms

**Duration: 1.5 Hour**

- Identify mobile attack vectors
- Match android hacking tools to their descriptions
- Identify best practices for keeping an android device secure
- Identify best practices for making your ios device more secure
- Identify the countermeasures for attacks on windows os devices
- Identify countermeasures used to protect against attacks on blackberry devices
- Identify the best practices used to protect all mobile devices from attack
- Identify methods of mobile device attacks and how to counter them

### Certified Ethical Hacker (CEH) v8: Evading IDS, Firewalls, and Honeypots

**Duration: 1.5 Hour**

- Identify a honeypot
- Identify intrusion detection tools
- Identify types of attacks
- Recognize firewall evasion tools
- Identify firewall penetration testing techniques
- Identify tools and techniques used to evade ids, firewalls, and honeypots

### Certified Ethical Hacker (CEH) v8: Buffer Overflow

**Duration: 1 Hour**

- Identify types of buffer overflow
- Sequence the steps in a buffer overflow attack
- Sequence the steps for testing for a stack overflow vulnerability
- Recognize countermeasures against buffer overflow attacks
- Identify buffer overflow attack methodology and tools, and how to counter them