



# Certified Ethical Hacker





Cybersecurity  
Certification Prep Day 1



# Class Objectives

---

By the end of class today, students will be able to:

-  Explain what the Certified Ethical Hacker Exam is and which Info Sec fields would benefit from obtaining the certification.
-  List the requirements, prerequisites and details of the exam.
-  List the Domains covered in the exam that have/haven't been covered previously in our class
-  Complete a practice test

# Introduction to CEH

# What is a Certified Ethical Hacker?

---

## According to the **EC-Council**\*

- A skilled professional who understands how to look for weaknesses and vulnerabilities in target systems.
- Uses the same knowledge and tools as a malicious hacker in a lawful and legitimate manner to assess the security posture of a target system.

\* **EC-Council** is an organization that certifies qualified applicants in various e-business and infosec security skills.

- They provide testing and certification for CEH as well as more advanced certifications for ECSA (Certified SEcurity Analyst) and LPT (Licensed Penetration Tester)

# Introduction to CEH Certification

---

What are some jobs that may require the CEH certification?

- Penetration Testing
- Red Team/ Blue Team
- Ethical Hackers
- Security Specialists
- Information Security Analysts
- Security or Systems Administrators
- Application Security Engineers
- Vulnerability Management

# Introduction to CEH Certification

---

What will you learn with the certification?

- Footprinting and Reconnaissance
- Scanning and Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking
- Wireless Network Platforms
- IoT Hacking
- Cloud Computer
- Cryptography

# When should you consider taking the CEH Exam

---

While CEH is considered an entry-level exam and certification, the applicant must complete one of three credentials to take the exam:



Attended training at an Accredited Training Center



Completed iClass, through EC-Council's learning portal



Completed Self Study, after an application and proof of two years relevant Info Sec experience is provided



Without two years of experience, you can also request consideration based on educational background

# CEH Specs

---

The CEH Certification is obtained through passing the CEH V10 version of the Exam.



There are 125 multiple-choice questions on the exam.



The exam lasts 4 hours.



The cost of the exam is \$500.



The exam is vendor-neutral.



# How is the Exam Graded?

---

According to **EC-Council**:

EC-Council Exams are provided in multiple forms (i.e. different question banks).

- Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts
- ensures that each of our exams not only have academic rigor but also have "real world" applicability.

EC-Council also has a process to determine the difficulty rating of each question .

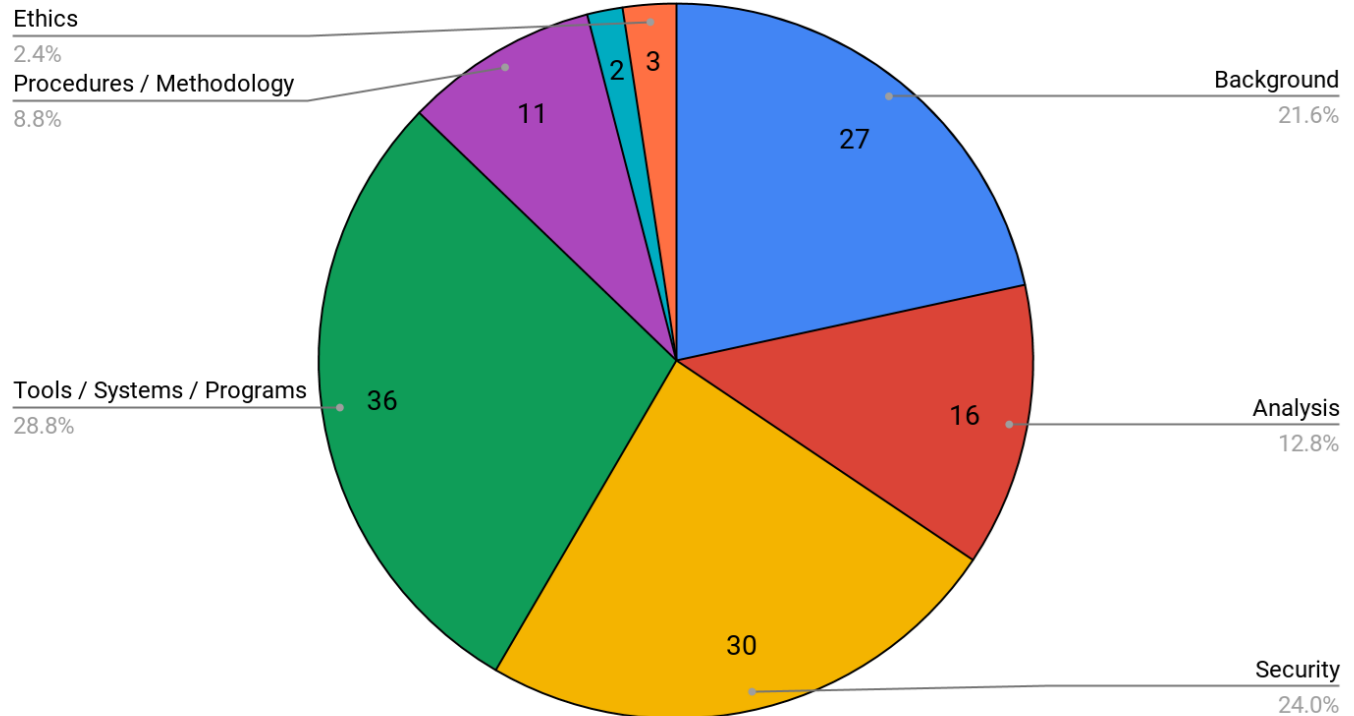
- The individual rating contributes to an overall "Cut Score" for each exam form.
- To ensure each form has equal assessment standards, cut scores are set on a "per exam form" basis. Depending on which exam form is challenged, cut scores can range from 60% to 85%."

# Domain Breakdown

# CEH Topics Breakdown

1. Background
2. Analysis / Assessment
3. Security
4. Tools/ Systems/ Programs
5. Procedures/ Methodology
6. Regulations / Policy
7. Ethics









Breakdown of Domains Covered on CEH



# Domain 1: Background

---

## Subtopics Included:

-  Networking technologies
-  Web technologies
-  System technologies
-  Communication Protocols
-  Malware Operations
-  Mobile technologies
-  Telecommunications Technologies
-  Backups and archiving



# Domain 1: Background

---

## Subtopics Covered In-Class:

-  Networking technologies - **Networking 101, Networking Security**
-  Web technologies - **Cyber 101, Web Development**
-  System technologies - **Cyber 101, Networking 101, Operating Systems**
-  Communication Protocols- **Networking 101, Networking Security**
-  Malware Operations- **Penetration Testing, Web Vulnerabilities**
-  Mobile technologies- **Not Covered**
-  Telecommunications Technologies- **Not Covered**
-  Backups and archiving- **Not Covered**



# Sample Question #1

---

Which of these options is the most secure procedure for strong backup tapes?

1. In a climate controlled facility offsite.
2. Inside the data center for faster retrieval in a fireproof safe.
3. In a cool dry environment.
4. On a different floor in the same building.



# Sample Question #1

---

Which of these options is the most secure procedure for strong backup tapes?

1. **In a climate controlled facility offsite.**
2. Inside the data center for faster retrieval in a fireproof safe.
3. In a cool dry environment.
4. On a different floor in the same building.



## Sample Question #2

---

Which of the following is the greatest threat posed by backups?

1. An un-encrypted backup can be misplaced or stolen.
2. A back is incomplete because no verification was performed.
3. A backup is the source of Malware or illicit information.
4. A backup is unavailable during disaster recovery.





## Sample Question #2

---

Which of the following is the greatest threat posed by backups?





1. **An un-encrypted backup can be misplaced or stolen.**
2. A back is incomplete because no verification was performed.
3. A backup is the source of Malware or illicit information.
4. A backup is unavailable during disaster recovery.



# Domain 2: Analysis and Assessment

---

Subtopics Included:

-  Data Analysis
-  System Analysis
-  Risk Assessment
-  Technical assessment methods



# Domain 2: Analysis and Assessment

---

Subtopics Covered in Class:



Data Analysis - **SIEMS**



System Analysis - **Operating Systems, SIEMS**



Risk Assessment - **Not Covered**



Technical assessment methods - **Not Covered**



# Sample Question #1

---

In Risk Management, how is the term “likelihood” related to the concept of "threat?"

1. Likelihood is the probability that a vulnerability is a threat-source.
2. Likelihood is a possible threat-source that may exploit a vulnerability.
3. Likelihood is the likely source of a threat that could exploit a vulnerability.
4. Likelihood is the probability that a threat-source will exploit a vulnerability.



# Sample Question #1

---

In Risk Management, how is the term “likelihood” related to the concept of "threat?"

1. Likelihood is the probability that a vulnerability is a threat-source.
2. Likelihood is a possible threat-source that may exploit a vulnerability.
3. Likelihood is the likely source of a threat that could exploit a vulnerability.
4. **Likelihood is the probability that a threat-source will exploit a vulnerability.**



## Sample Question #2

---

*Threats x Vulnerabilities* is referred to as the:

1. Threat assessment
2. Disaster recovery formula
3. BIA equation
4. Risk equation



# Sample Question #2

---

*Threats x Vulnerabilities* is referred to as the:

1. Threat assessment
2. Disaster recovery formula
3. BIA equation
4. **Risk equation**



## Sample Question #3

---

\_\_\_\_\_ is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosures, denial of service, or modification of data.

1. Threat
2. Attack
3. Risk
4. Vulnerability





## Sample Question #3

---

\_\_\_\_\_ is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosures, denial of service, or modification of data.








1. **Threat**
2. Attack
3. Risk
4. Vulnerability



# Domain 3: Security

---

## Subtopics Included:

-  Systems security controls
-  Application/file server
-  Firewalls
-  Cryptography
-  Network Security
-  Physical Security
-  Threat Modeling
-  Verification procedures

-  Social Engineering
-  Vulnerability Scanners
-  Security policy implications
-  Privacy/ confidentiality
-  Biometrics
-  Wireless access technology
-  Trusted Networks
-  Vulnerabilities



# Domain 3: Security


---

## Subtopics Covered In-Class:

 Systems security controls - **Network Security**

 Application/file server - **Web Vulnerabilities**

 Firewalls - **Network Security**


 Cryptography - **Cryptography**

 Network Security - **Network Security**

 Physical Security - **Not Covered**

 Threat Modeling - **GRC**


 Verification procedures - **SIEMS**

 Social Engineering - **Penetration Testing**

 Vulnerability Scanners - **Penetration Testing**

 Security policy implications - **Penetration Testing**

 Privacy/ confidentiality - **Penetration Testing**

 Biometrics - **Not Covered**

 Wireless access technology - **Not Covered**

 Trusted Networks - **Not Covered**

 Vulnerabilities - **Web Vulnerabilities, Penetration Testing**



# Sample Question #1

---

Which of the following tools can be used for passive OS fingerprinting?

1. tcpdump
2. ping
3. nmap
4. Tracert



# Sample Question #1

---

Which of the following tools can be used for passive OS fingerprinting?

1. **tcpdump**
2. ping
3. nmap
4. Tracert



## Sample Question #2

---

Which of the following is a low-tech way of gaining unauthorized access to systems?

1. Sniffing
2. Social engineering
3. Scanning
4. Eavesdropping



## Sample Question #2

---

Which of the following is a low-tech way of gaining unauthorized access to systems?

1. Sniffing
2. **Social engineering**
3. Scanning
4. Eavesdropping



## Sample Question #3

---

Which of the following statements is TRUE?

1. Sniffers operation on Layer 3 of the OSI model
2. Sniffers operation on Layer 2 of the OSI model
3. Sniffers operation on the Layer 1 of the OSI model
4. Sniffers operation on both Layer 2 & Layer 3 of the OSI model





## Sample Question #3

---

Which of the following statements is TRUE?










1. Sniffers operation on Layer 3 of the OSI model
2. **Sniffers operation on Layer 2 of the OSI model**
3. Sniffers operation on the Layer 1 of the OSI model
4. Sniffers operation on both Layer 2 & Layer 3 of the OSI model












# Domain 4: Tools / Systems Programs

---

## Subtopics Included:

-  Network /host-based infusion
-  Network sniffers
-  Access control mechanisms
-  Cryptography Techniques
-  Programming Languages
-  Scripting Languages
-  Boundary protection appliances
-  Networking topologies
-  Subnetting



















-  Port Scanning
-  Domain Name System
-  Routers/modems/switches
-  Vulnerability scanners
-  Vulnerability management
-  Operating environments
-  Antivirus Systems
-  Log analysis tools
-  Exploitation tools



# Domain 4: Tools / Systems Programs

---

## Subtopics Included:

-  Network /host-based infusion- **Net 101, NetSec**
-  Network sniffers- **Net 101, NetSec**
-  Access control mechanisms- **Not Covered**
-  Cryptography Techniques - **Cryptography**
-  Programming Languages - **Python**
-  Scripting Languages- **Web Development**
-  Boundary protection appliances - **Net Sec**
-  Networking topologies - **Net 101, NetSec**
-  Subnetting - **Not covered**
-  Port Scanning - **NetSec**
-  Domain Name System - **Networking 101**
-  Routers/modems/switches - **Networking 101**
-  Vulnerability scanners - **Penetration Testing**
-  Vulnerability management - **Pentest, Web Vulns**
-  Operating environments - **Linux / Windows OS**
-  Antivirus Systems - **Network Security**
-  Log analysis tools - **SIEM**
-  Exploitation tools - **Pentest**



# Sample Question #1

---

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

1. Jack the ripper
2. Nessus
3. Tcpdump
4. Ethereal



# Sample Question #1

---

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

1. Jack the ripper
2. Nessus
3. **Tcpdump**
4. Ethereal



## Sample Question #2

---

What does a firewall check to prevent particular ports and applications from getting packets into an organizations?

1. Transport layer port numbers and application layer headers
2. Network layer headers and the session layer port numbers
3. Application layer port numbers and the transport layer headers
4. Presentation layer headers and the session layer port numbers



## Sample Question #2

---

What does a firewall check to prevent particular ports and applications from getting packets into an organizations?

1. **Transport layer port numbers and application layer headers**
2. Network layer headers and the session layer port numbers
3. Application layer port numbers and the transport layer headers
4. Presentation layer headers and the session layer port numbers



# Take a Break!

---














The following domains  
were *not* covered in class...

# Domain 5: Procedures and Methodology

---

## Subtopics Included:

-  Public Key Infrastructure (PKI)
-  Security Architecture
-  Service-Oriented Architecture
-  Information security design
-  N-tier application design
-  TCP/IP networking
-  Security testing methodology



# Sample Question #1

---

A Regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

1. Move the financial data to another server on the same IP subnet
2. Place a front-end web server in a demilitarized zone that only handles external web traffic
3. Issue new certificates to the web servers from the root certificate authority
4. Require all employees to change their passwords immediately



# Sample Question #1

---

A Regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

1. **Move the financial data to another server on the same IP subnet**
2. Place a front-end web server in a demilitarized zone that only handles external web traffic
3. Issue new certificates to the web servers from the root certificate authority
4. Require all employees to change their passwords immediately



## Sample Question #2

---

You've just been hired to perform a pentest on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk. What is one of the first things you should do when starting this job?

1. Start the wireshark application to start sniffing network traffic.
2. Establish attribution to suspected attackers.
3. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
4. Interview all employees in the company to rule out possible insider threats.



## Sample Question #2

---

You've just been hired to perform a pentest on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk. What is one of the first things you should do when starting this job?

1. Start the wireshark application to start sniffing network traffic.
2. Establish attribution to suspected attackers.
3. **Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.**
4. Interview all employees in the company to rule out possible insider threats.



## Domain 6: Regulation / Policy

---

This section of the exam tests knowledge of major information security regulations and evaluations of corporation's security policies.

Sample Question:

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such as audit?

1. Port scanner
2. Protocol analyzer
3. Vulnerability scanner
4. Intrusion Detection System

## Domain 6: Regulation / Policy

---

This section of the exam tests knowledge of major information security regulations and evaluations of corporation's security policies.

Sample Question:

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such as audit?

1. Port scanner
2. Protocol analyzer
3. **Vulnerability scanner**
4. Intrusion Detection System



## Domain 7: Ethics

---

This section of the exam tests knowledge of how to behave appropriately in situations that you may encounter as an ethical hacker.

Sample Question:

Which of the following statements regarding ethical hacking is incorrect?

1. Testing should be remotely performed offsite.
2. Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the organizations IT system.
3. Ethical hacking should not involve writing to or modifying the target systems.
4. An organization should use ethical hackers who do not sell hardware/software or other consulting services.

## Domain 7: Ethics

---

This section of the exam tests knowledge of how to behave appropriately in situations that you may encounter as an ethical hacker.

Sample Question:

Which of the following statements regarding ethical hacking is incorrect?

1. Testing should be remotely performed offsite.
2. **Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the organizations IT system.**
3. Ethical hacking should not involve writing to or modifying the target systems.
4. An organization should use ethical hackers who do not sell hardware/software or other consulting services.



## Activity: Practice Quiz

In this activity, you will complete a practice CEH exam.

The purpose of this review is not to achieve a perfect score. It should be used as an opportunity to find less competent areas that you should focus on studying and preparing for.

Exam sent via Slack.

**Suggested Time:**  
1 hour

