CEH and CISSP

Cybersecurity

Certification Prep Day 3

Class Objectives

By the end of class, you will be able to:

- Prepare for the CEH exam.
- Understand the requirements of the CISSP exam.
- Correctly answer CEH and CISSP practice questions.

The first half of today's class will focus on the CEH and CISSP exams and the types of questions they contain.

The second half of the class will be a fun quiz competition using Kahoot.

CEH

What is CEH?

According to **EC-Council**:

The Certified Ethical Hacker (CEH) program is the most comprehensive ethical hacking course on the globe to help information security professionals grasp the fundamentals of ethical hacking.

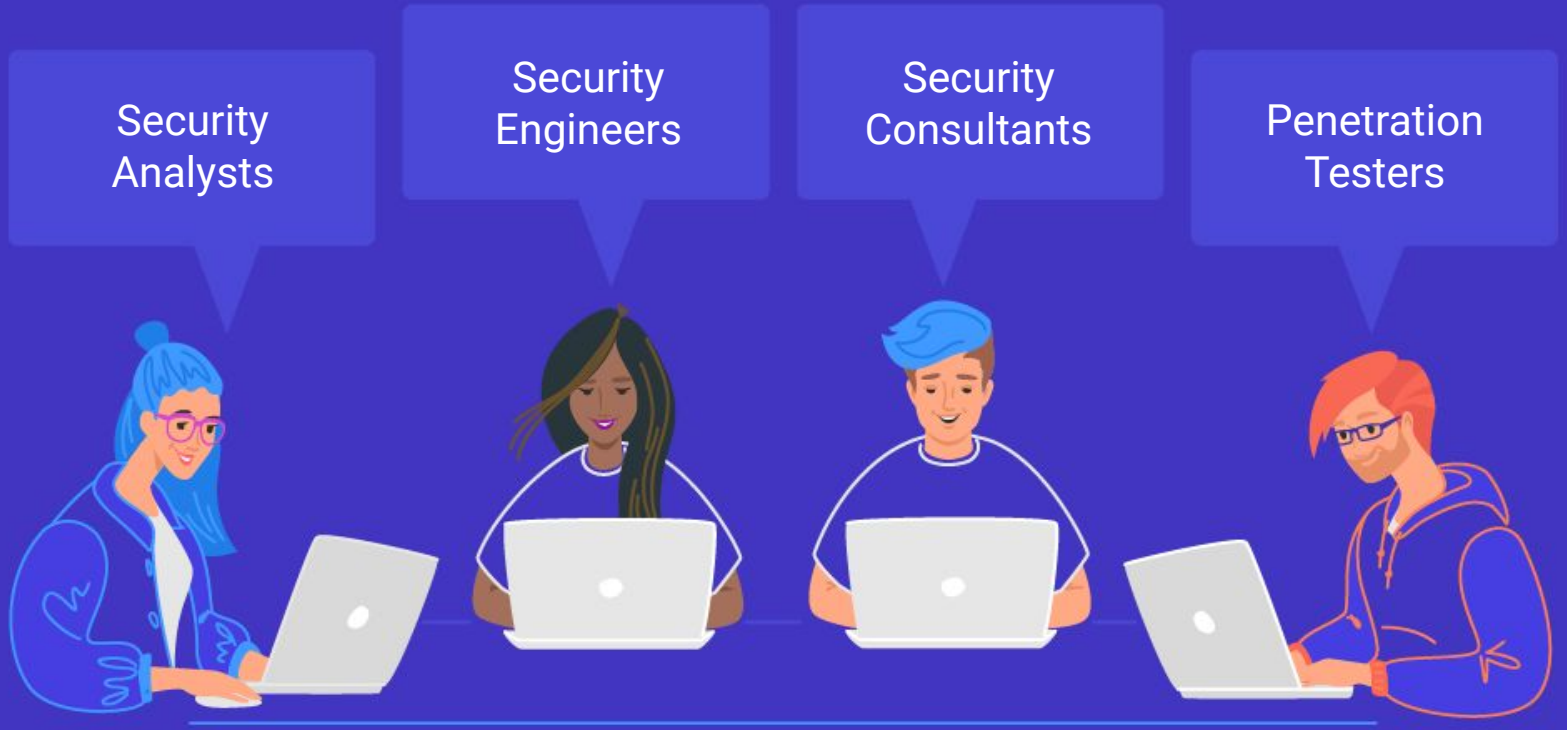
The course outcome helps you become a professional who systematically attempts to inspect network infrastructures with the consent of its owner to find security vulnerabilities which a malicious hacker could potentially exploit.

The course helps you assess the security posture of an organization by identifying vulnerabilities in the network and system infrastructure to determine if unauthorized access is possible.

As of early 2020, there were almost 12,000 infosec job openings desiring a CEH certification.

CEH Roles

Jobs requiring CEH certifications include:



CEH Exam Topics Breakdown

Domain Distribution

01 Background

02 Analysis and Assessment

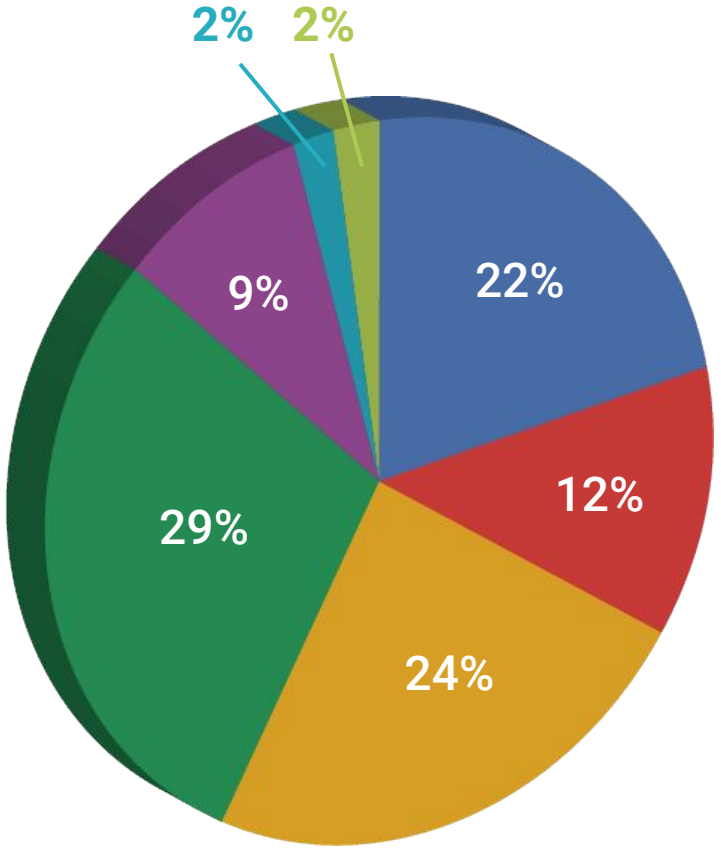
03 Architecture and Security

04 Tools, Systeems, and Programs

05 Procedures and Methodology

06 Regulation and Policy

07 Ethics

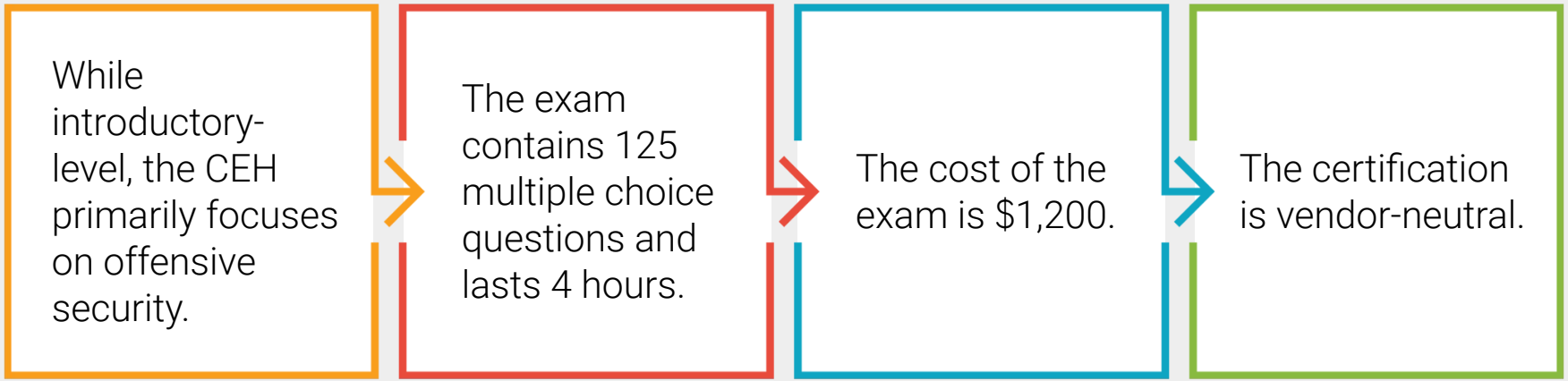


CEH Exam Topics Breakdown

Domain Distribution		Topics include:
01	Background	Communication protocols (HTTP, FTP), telecommunication technologies, backups and archiving
02	Analysis and Assessment	Data analysis, risk assessments
03	Architecture and Security	Firewalls, cryptography, vulnerabilities, systems security controls
04	Tools, Systeems, and Programs	Port scanning (Nmap), vulnerability scanning (Nessus), network sniffers (Wireshark)
05	Procedures and Methodology	Security testing methodologies, network routing, security architecture
06	Regulation and Policy	Behavioral requirements for ethical hackers in accordance with laws and policies
07	Ethics	Behaving ethically as an offensive security professional

CEH Specs

The CEH certification is obtained by passing the EC-Council administered CEH exam.



CEH Exam Prerequisites

Depending on your experience, you can prepare for the exam in two ways:

01 With Experience

If you currently have two years of information security experience, you can self-study for the exam without any formal training.

- Your eligibility must be approved by EC-Council with an Exam Eligibility Form.

02 Without Experience

If you do not have two years of information security experience, you will be required to take official EC-Council training for $850.

- Online and in-person courses are available.

CEH Tips

01 Memorize the most common ports and protocols.

02 Use free resources provided by EC-Council, e.g.: **CEH Exam Blueprint**

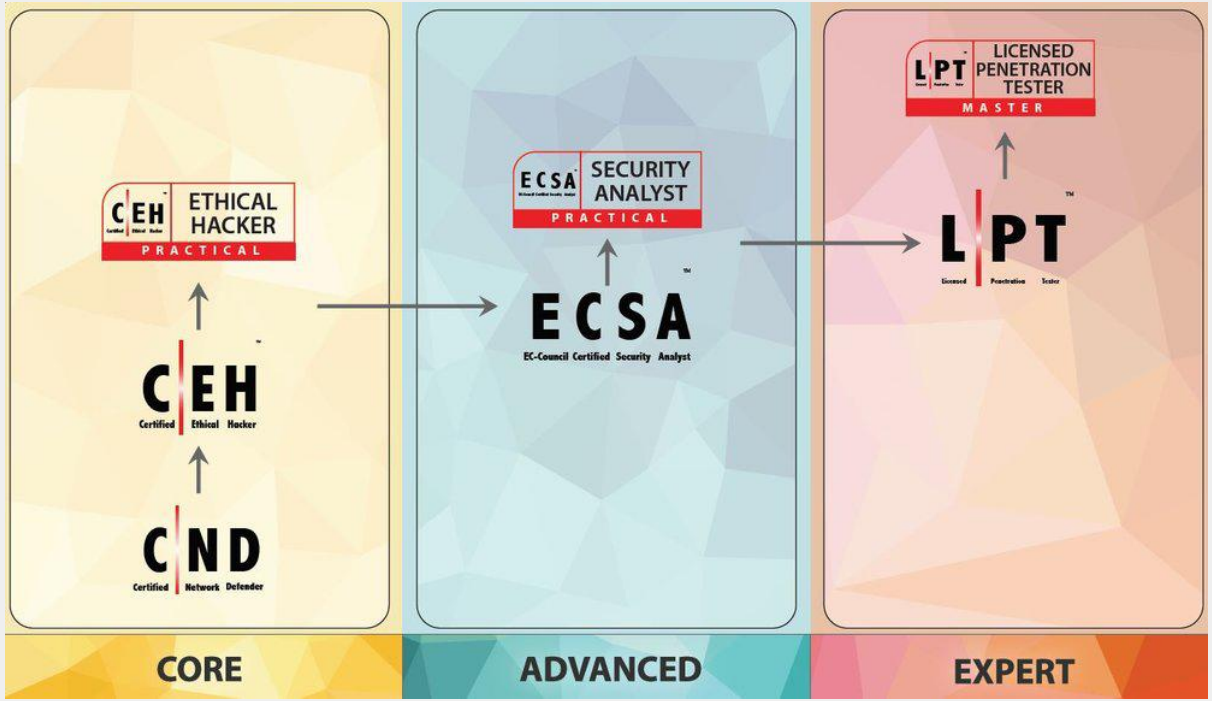
03 Consider taking the EC-Council's one-week boot camp course to prepare for the exam.

04 The exam is multiple choice, but practicing with hacking tools in virtual environments will help you understand each tool's purpose.

(Source)

EC-Council's Other Offerings

The EC-Council offers more advanced hands-on ethical hacker certifications to complete after CEH.



(Source)

Example Question:

A denial of service or DOS attack is a type of cyberattack where a malicious individual makes system resources unavailable.

This is often accomplished by flooding the system with erroneous requests.

Acme Corp is an organization that just experienced a DOS attack, which of the following is a symptom of this attack?

A. Acme Corp's database that contains salary information was modified to provide certain individuals higher salaries.
B. Acme Corp's customers are now reporting an error message when trying to access the Acme Corp homepage.
C. A hacker accessed a copy of Acme Corp's employee list and SSNs.
D. A hacker was able to successfully launch a SQL injection attack.

Example Question:

A denial of service or DOS attack is a type of cyberattack where a malicious individual makes system resources unavailable.

This is often accomplished by flooding the system with erroneous requests.

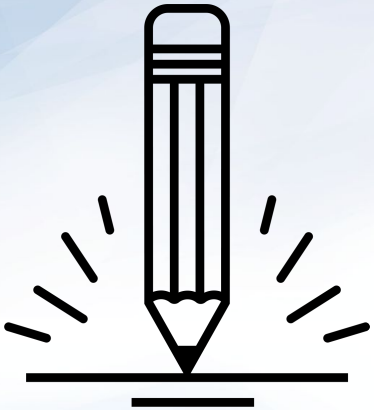
Acme Corp is an organization that just experienced a DOS attack, which of the following is a symptom of this attack?

A. Acme Corp's database that contains salary information was modified to provide certain individuals higher salaries.

B. **Acme Corp's customers are now reporting an error message when trying to access the Acme Corp homepage.**

C. A hacker accessed a copy of Acme Corp's employee list and SSNs.

D. A hacker was able to successfully launch a SQL injection attack.



Activity: CEH Practice Quiz

In this activity, you will complete sample CEH exam questions.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

CISSP

Certified Information Systems Security Professional (CISSP)

As an advanced certification, many professionals do not attempt this exam until they've worked in information security for several years.

As of early 2020, CISSP was the most desired certification, with around

54,5000

listing it as desired or required.

Per (ISC)², the average salary for CISSP jobs is

$131,030

More than

129,000

professionals hold the CISSP certification.

What is CISSP?

According to **(ISC)²**:

CISSP®

> The CISSP is ideal for information security professionals seeking to prove their understanding of cybersecurity strategy and hands-on implementation.
>
> It shows you have the advanced knowledge and technical skills to design, develop and manage an organization's overall security posture.

Jobs requiring **CISSP** certifications may include:

CISSP Exam Topics Breakdown

01 Security and Risk Management

02 Asset Security

03 Security Architecture and Engineering

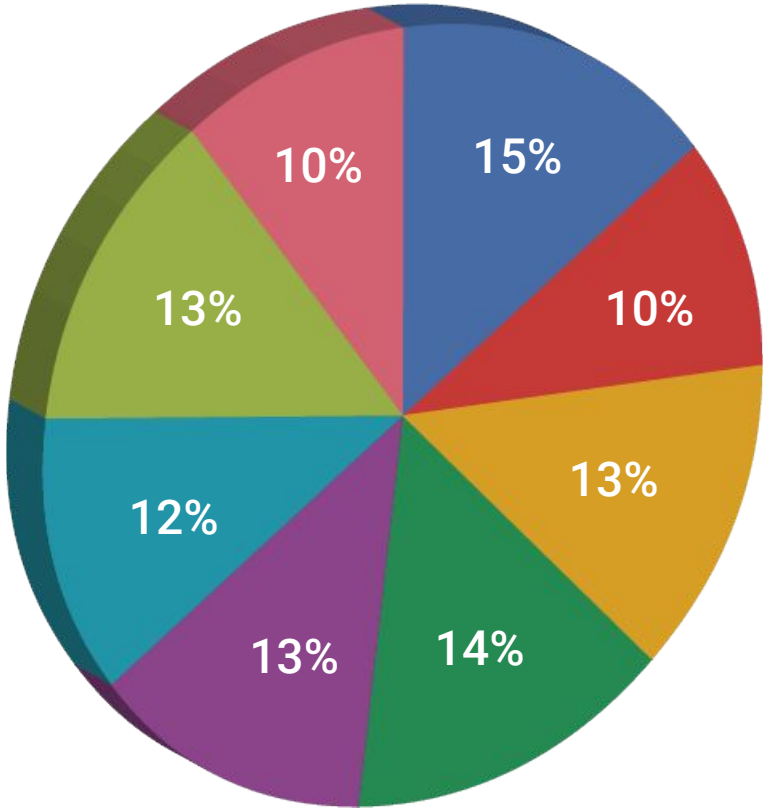
04 Communication and Network Security

05 Identity Access and Management

06 Assessment and Testing

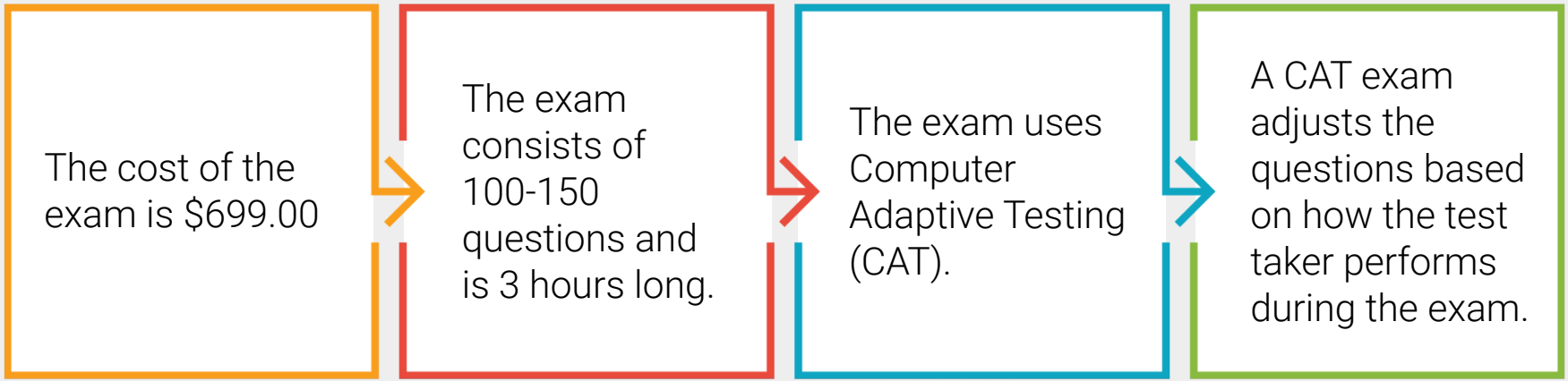
07 Security Operations

08 Software Development Security



Domain Distribution		Topics include:
01	Security and Risk Management	Confidentiality, integrity, and availability, business continuity
02	Asset Security	Data security controls, identifying and classifying information and assets
03	Security Architecture and Engineering	Vulnerabilities in web-based, mobile, and embedded systems, secure design principles
04	Communication and Network Security	Secure network components and architecture
05	Identity Access and Management	Physical and logical access security, identification and authentication of services and devices
06	Assessment and Testing	Security control testing, security audits
07	Security Operations	Incident management, disaster recovery plans
08	Software Development Security	Security in the software development lifecycle, security of acquired software

CISSP Specs


The cost of the exam is $699.00
The exam consists of 100-150 questions and is 3 hours long.
The exam uses Computer Adaptive Testing (CAT).
A CAT exam adjusts the questions based on how the test taker performs during the exam.

CISSP Exam Prerequisites

Depending on your experience, you can prepare for the exam in two ways:

01 CISSP Credentials

If you have five years of information security experience in two of the eight domains listed, you can register to take the exam. One year can be replaced with relevant completed education.

- After passing the exam, you have nine months to complete your endorsement, in which an (ISC)² certified professional attests to your professional experience.
- Once the endorsement is approved by (ISC)² , you will be granted your CISSP credentials.

02 Associate CISSP Credentials

If you do not have the five years of information security experience in two of the eight domains listed, you can still take the exam.

- After passing the exam, you will be granted an Associate CISSP certification.
- Once you have met the professional requirements of five years in two of the eight domains, you can begin the endorsement process.

Example Question:

An organization with 130 employees using symmetric encryption is considering moving to asymmetric encryption. How would this affect their number of keys?

A. 260 more keys
B. 8,000 fewer keys
C. 5,605 more keys
D. 8,125 fewer keys

Example Question:

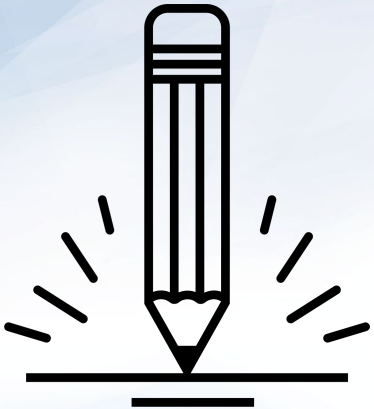
An organization with 130 employees using symmetric encryption is considering moving to asymmetric encryption. How would this affect their number of keys?

A. 260 more keys
B. 8,000 less keys
C. 5,605 more keys
D. **8,125 less keys**

Symmetric Formula = n(n - 1)/2
130 * 129 / 2 = **8385**

Asymmetric Formula = n * 2
130 * 2 = **260**

Difference:
8385 - 260 = **(D) 8125 fewer keys**



Activity: CISSP Practice Quiz

In this activity, you will complete sample CISSP exam questions.

Suggested Time:
7 Minutes

Time’s Up! Let’s Review.

Now we will take part in a fun and challenging competition using

Kahoot! Rules and Guidelines

- There are a total of 30 CEH and CISSP questions.
- Points are not deducted for incorrect answers.
- You have two minutes to answer each question.
- If you are competing as a team, select a team captain to answer the questions.
- Points are awarded for correct answers and for how quickly you answer the questions compared to your classmates.
- **Note:** If your class is currently online, it will be easier if each student competes individually.

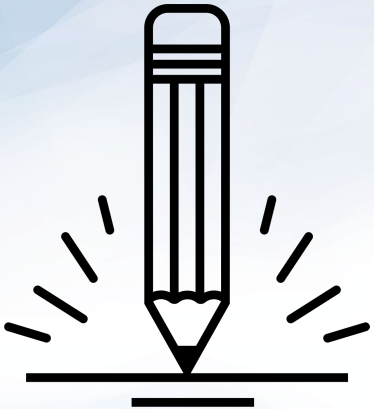
(kahoot.com)

Kahoot! Rules and Guidelines

- There will be 15 CEH questions and 15 CISSP questions.
- You can use all available resources: books, the internet, class notes, etc.
- Any issues will be decided by the judges (the TAs and/or instructor).

  Issues may include:
  - Answer disputes
  - Frozen or lagging computers
  - Kahoot issues
- The team or individual with the most points at the end of 30 questions will be declared the winner!

(kahoot.com)



Activity: Kahoot Challenge

Now we'll begin the competition!


The End.