



Surveying the Cyberspace

Cybersecurity
Cybersecurity 101 Day 3



Class Objectives

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



Consider roles and career pathways within the cybersecurity space.



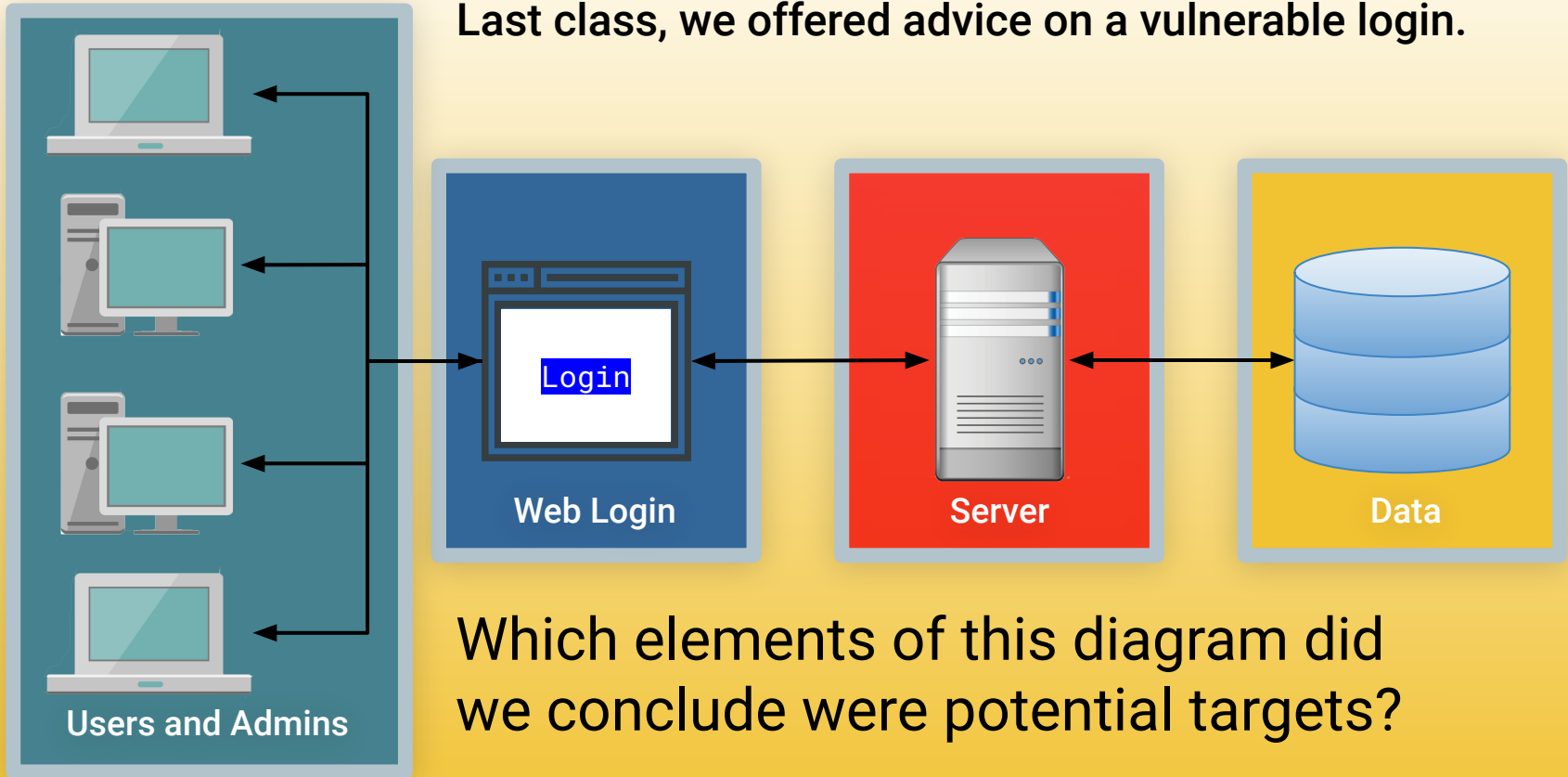
Explain the landscape of certifications available to security professionals.



Explore what the Security+ exam is and which infosec pathways benefit from the certification.

Quick Review

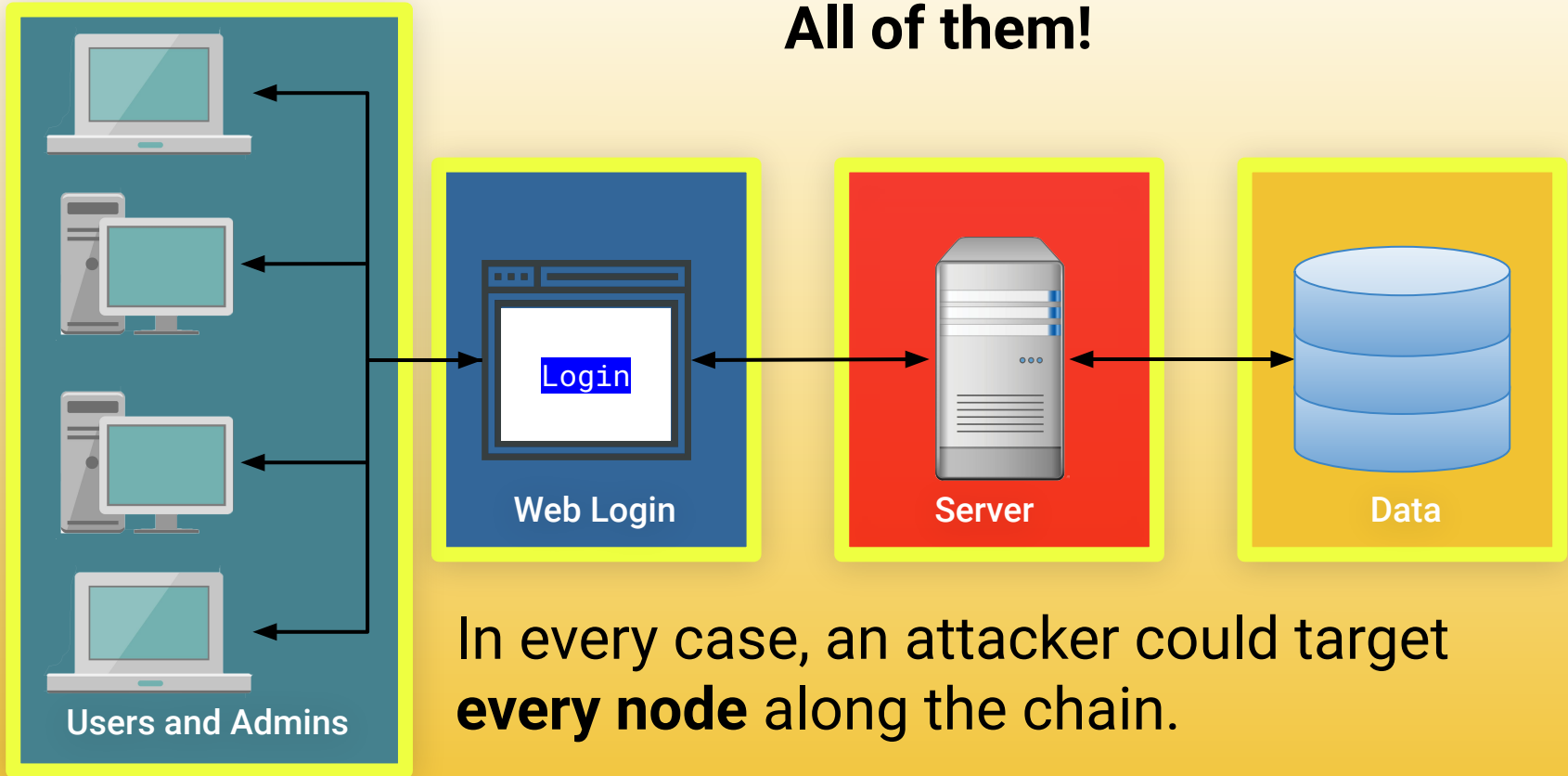
Last class, we offered advice on a vulnerable login.



Which elements of this diagram did we conclude were potential targets?

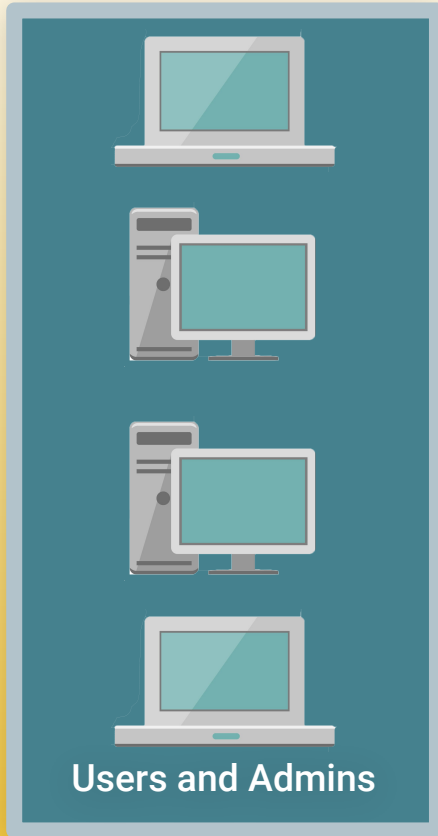
Quick Review

All of them!



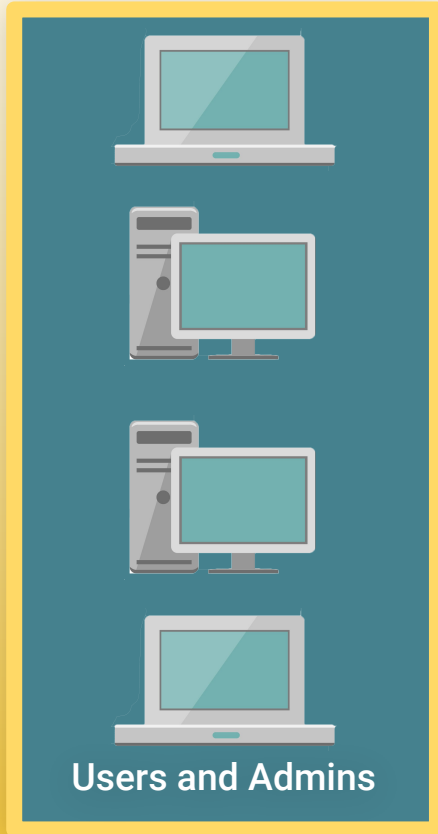
In every case, an attacker could target **every node** along the chain.

Quick Review



Name three user attacks.

Quick Review



Name three user attacks.

Social engineering

Credential reuse

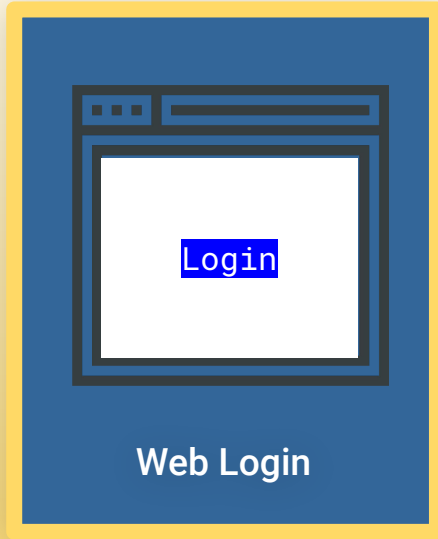
Malware attacks

Man in the middle

Packet sniffing

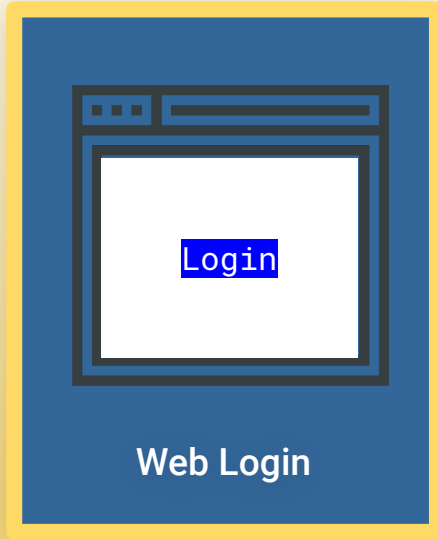
Computer theft

Quick Review



Name one website attack.

Quick Review



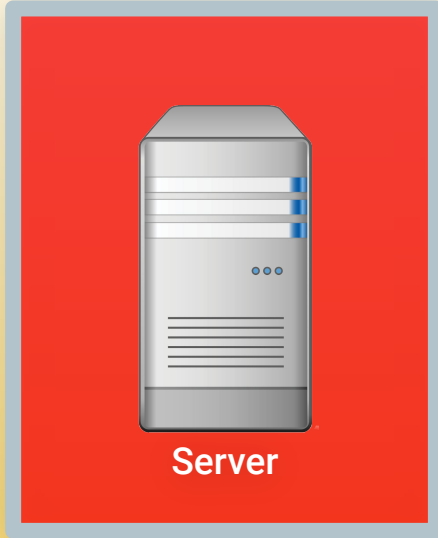
Name one website attack.

Brute force attacks

Code injection

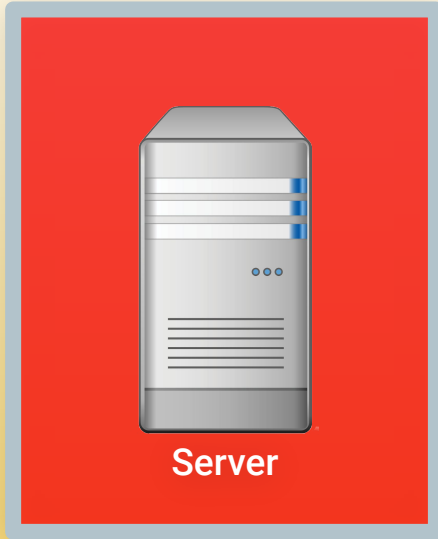
Session stealing

Quick Review



Name one server attack.

Quick Review

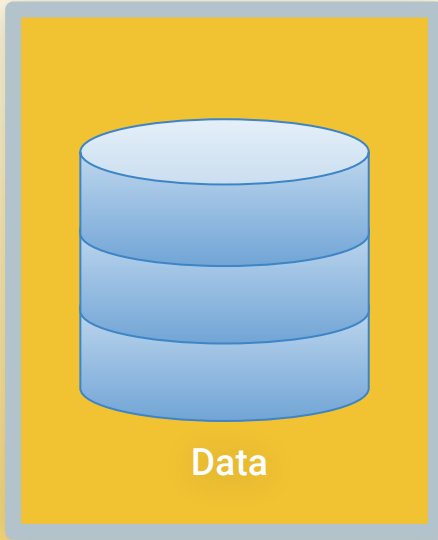


Name one server attack.

OS exploits

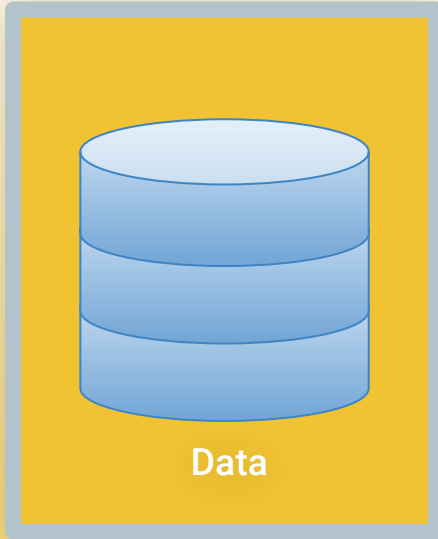
Code injection

Quick Review



Name one database attack.

Quick Review



Name one database attack.

Default credentials

Unpatched database

Lack of segregation

Quick Review

User Attacks

Social engineering

Phishing attacks

Credential reuse

Malware attacks

Man in the middle

Packet sniffing

Computer theft

Web Attacks

Brute force attacks

Code injection

Faulty sessions

Server Attacks

OS exploit

Malicious software

Database Attacks

Default credentials

Unpatched database

Lack of segregation

**Name three
risk mitigation
options.**

Quick Review

Name three risk mitigation options.

1. Educate all users on dangers of phishing and social engineering.
2. Ensure passwords are truly unique to website (require characters atypical of other websites).
3. Ensure users are using multi-factor authentication (login + phone confirmation).
4. Ensure administrators can only access the network from a secure location (on premises).
5. Ensure passwords used are *strong* (alphanumeric + symbols).
6. Ensure login fields do *not* accept any code insertions.
7. Ensure users are immediately signed off when browser is closed.
8. Ensure all servers are routinely patched against latest known vulnerabilities.
9. Ensure physical access to servers is protected by multiple forms of authentication.
10. Ensure that all data stored in the database is encrypted and cannot be read without additional login information.
11. Ensure that all cloud security platforms follow best practices for security implementation.

Cybersecurity Domains



Providing advice on ***getting started in digital security*** is similar to providing advice on *getting started in medicine*.

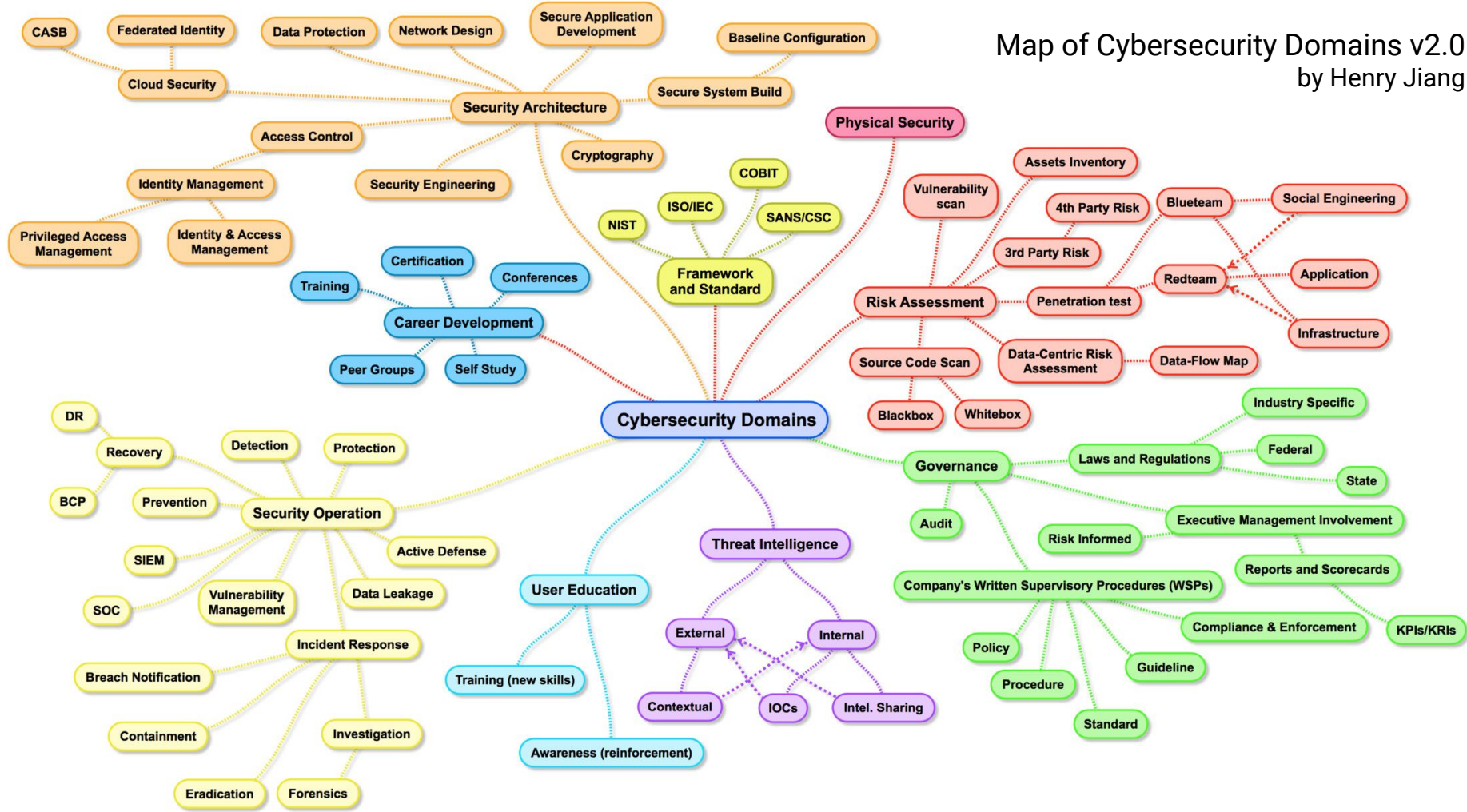
If you ask a neurosurgeon, he or she may propose some sort of experiment with dead frog legs and batteries. If you ask a dermatologist, you might get advice on protection from the sun whenever you go outside. Asking a “security person” will likewise result in many different responses, depending on the individual’s background and tastes.



—Tao Security’s ***Richard Bejtlich***
on entering the cybersecurity field

Map of Cybersecurity Domains v2.0

by Henry Jiang



Cybersecurity Domains



Security architecture: Security design that addresses the requirements and potential risks of a given scenario or environment. It also specifies when and where to apply security controls.



Security operations: Process of identifying, containing, and remediating threats on behalf of a company or organization.



Governance: Framework for managing performance and risk, oversight of compliance and control responsibilities, and defining the cyber mission by mapping the structure, authority, and processes to create an effective program.

Cybersecurity Domains



Physical security: Protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage. Includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.



Threat intelligence: Research and analyzation of evidence-based knowledge regarding an existing or emerging menace.



Career development: Training of future cybersecurity professionals.

Cybersecurity Domains



Risk assessment: Analyzing what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk is.



User education: Teaching users how to protect themselves from cyberattacks by informing them of risks, exploits, and external threats, and the skills needed to combat common attacks.



Frameworks and standards: Creation of new security frameworks and practices for professionals to follow.



Activity: Career and Pathway Research

In this activity, we will begin to research security careers and pathways in depth.

Suggested Time:
10 Minutes





Share your answers.

Sample (Entry Level) Cybersecurity Titles

Knowing which job titles and job types are entry-level is the first step in pursuing a career in the space. Try to identify with positions are entry-level.

Security Analyst	Security Operations Center (SOC) Analyst	Security Engineer	Systems Engineer
Cyber Threat Analyst	Cyber Defense Analyst	Incident Response Analyst	Intelligence Analyst
Information Assurance Technician	Risk Analyst	Forensics Investigator	Systems Administrator
Network Engineer	IT Auditor	Application Security Engineer	Penetration Tester
Information Analyst	Systems Security Analyst	IT Specialist	Web Engineer - Application Security

Cyber Fields by the Numbers

According to a report from Frost and Sullivan and (ISC)², there will be **more than 1.5 million unfilled cybersecurity positions by 2020**.

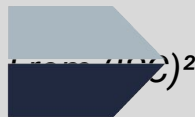
From ISACA:



53% of organizations take up to 6 months to find qualified cybersecurity candidates.



Cybersecurity jobs grew three times faster than IT jobs between 2010 and 2014.

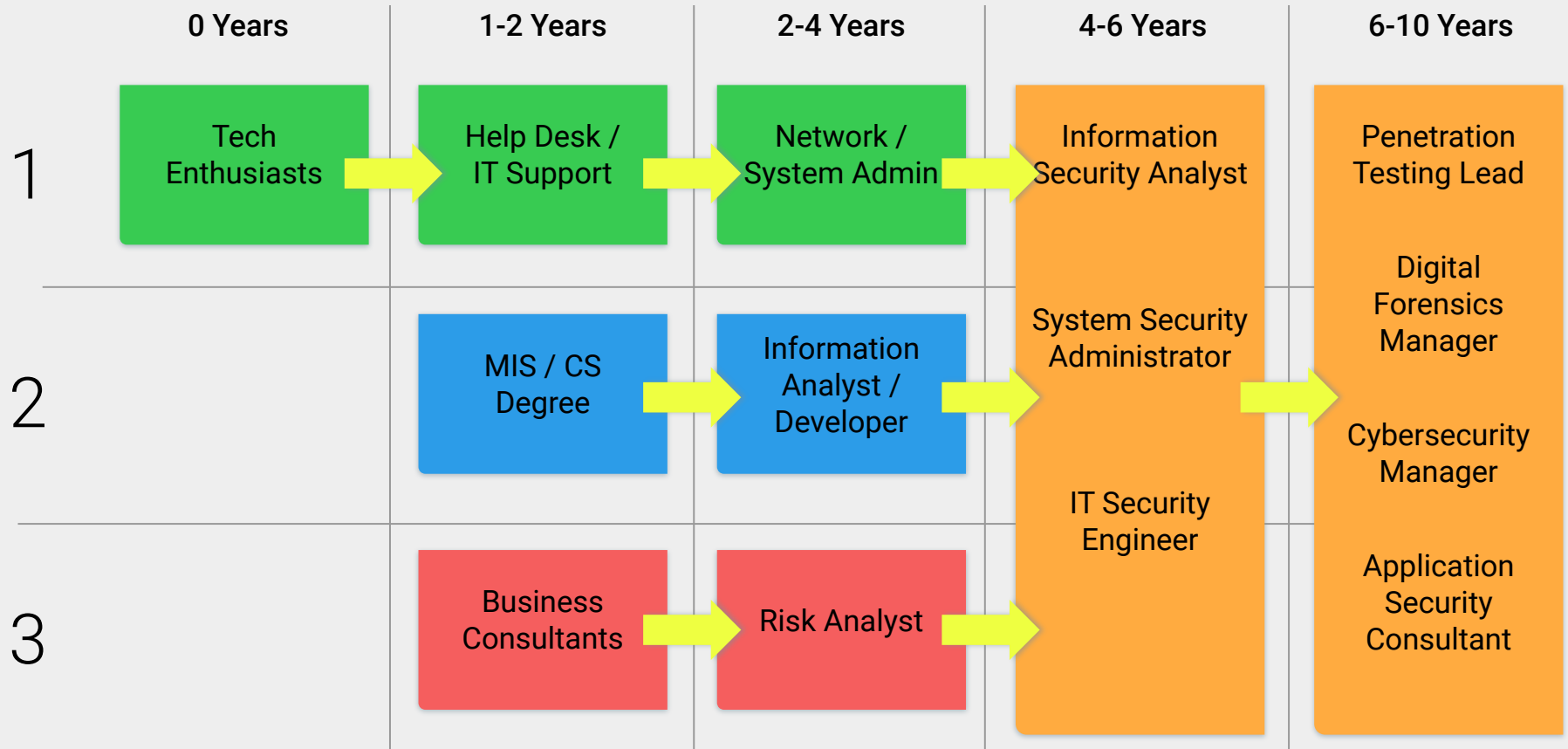


84% of organizations believe half or fewer of its applicants for open security jobs are qualified.



A full 87% of all cybersecurity professionals started their careers doing something different.

Career Context (Common Pathways)



Career Services Department

In class, we will tie concepts and skills in our program to career outcomes and roles. Outside of the classroom, the **Career Services** team will do the practical, hard work, helping you get a new role or promotion.

There are several career milestones for you to complete in Bootcamp Spot.

- You have access to them all now and can submit milestones whenever you want.
- However, you will need to submit at least one milestone in order to unlock Career Services.
- One of the milestones, an updated, polished resume, will be a requirement in one of our later homework assignments, but you can submit this earlier if you want.
- Review the slides on Becoming Employer Competitive, Working with Your Profile Coach, and Working with Your Career Director.



A close-up, high-angle photograph of a computer keyboard. The central focus is a large, white, rectangular key with rounded corners. On this key, there is a dark blue icon of a coffee cup with three wavy lines above it representing steam. Below the icon, the word "Break" is printed in a dark blue, serif font. The key is set against a light-colored, textured keyboard surface. Surrounding the main key are other keys, including one with a double quote symbol to the left and one with a dash/slash symbol to the right, all slightly out of focus.

Break

Security Certifications

Security Certifications

As the demand for cybersecurity careers grows, employers frequently use certification as a measure of employee **qualifications** and **training** when hiring.


CompTIA certifies **Security+** and **PenTest+**.

EC Council certifies **CEH** and **ECIH**.

(ISC)² certifies **CISSP** and **SSCP**.

Offensive Security certifies **OSCP** and **OSWP**.

GIAC certifies **GPEN** and **GCIH**.



Today, we'll do
a deeper review of
CompTIA's Security+
certification
and exam.



Activity: Certification Landscape

Let's take a quick look at this list of over 100 professional security certifications.

Go to:

en.wikipedia.org/wiki/List_of_computer_security_certifications

Suggested Time:
3-5 minutes



Of the 100+ certifications,
today we'll focus on one
of the most in-demand:

Security+



What is a Security+?

According to **CompTIA**, Security+:



Is the first security certification that IT professionals should earn.



Establishes core knowledge required for any cybersecurity role.



Provides a springboard to intermediate-level cyber jobs.



Incorporates hands-on troubleshooting to ensure practical security problem-solving.

CompTIA (Computing Technology Industry Association) is a non-profit trade organization that certifies qualified applicants in various information technology skills.



Provides testing and certification for Security+, Network+, CASP+, and PenTest+.

As of February 2021, the
average annual pay for an
information security analyst
in the United States was
\$99,944.



At Which Point in Your Career Should You Take The Exam?

Security+ is considered an **entry-level exam**. The skills we'll learn in this course will offer strong foundations for many topics covered on the exam.

However, the Sec+ exam is broad and will require additional knowledge in areas that aren't covered in this program.

The **CompTIA CertMaster** tool will provide the material needed to close these gaps and master the exam.



Why Don't We Cover Everything on the Sec+ Exam?

This course focuses on providing relevant practical experience of the most common and useful concepts, tools, and technologies used in security and networking. *It is not a test prep course.*

Some topics on the Security+ exam are not covered in this course because they are highly specific, and relevant only to certain subfields of cybersecurity.

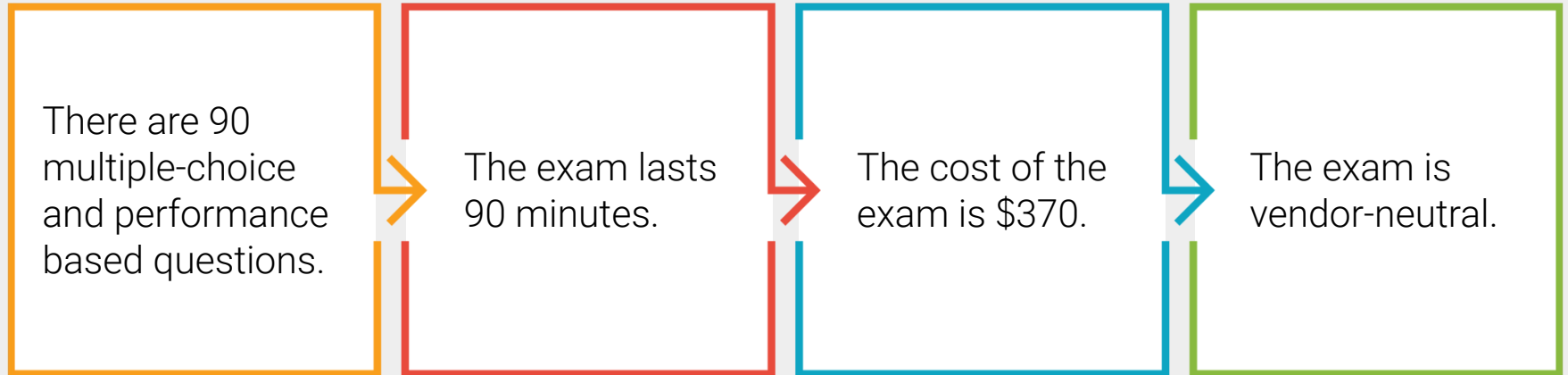
➤ While this course and exam share many overlapping topics, more niche topics covered on the exam will require additional study.

➤ **For example**, the TACACS+ protocol appears on the Security+ exam, but it is only used by engineers who work specifically with Cisco devices.



Security+ Specs

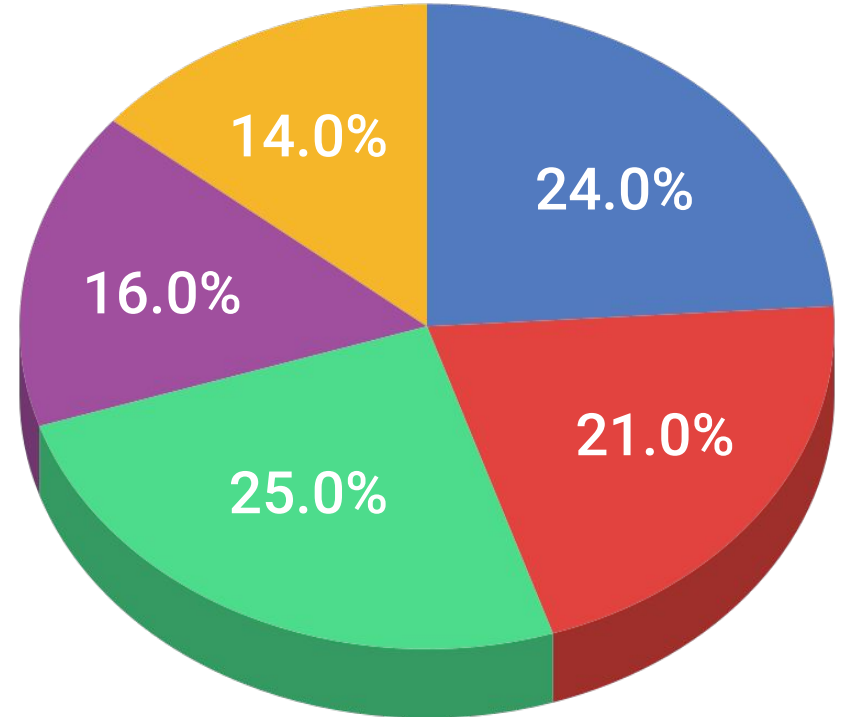
The Security+ Certification is obtained by passing the CompTIA-administered Security+ exam.



Security+ Exam Topics Breakdown

Domain Distribution

- 01 Attacks, Threats and Vulnerabilities
- 02 Architecture and Design
- 03 Implementation
- 04 Operations and Incident Response
- 05 Governance, Risk and Compliance



Question Formatting



There are two types
of questions on the
Security+ exam:
multiple choice and
performance based.

Example Question: Multiple Choice

Which of the following describes a logic bomb?

1. A program that performs a malicious activity at a specific time or after triggering an event.
2. A type of malicious code similar to a virus whose primary purpose is to duplicate itself and spread, while not necessarily internally damaging or destroying resources.
3. A program that appears to be a legitimate application, utility, game, or screen saver that performs malicious activities surreptitiously.
4. A program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the system where it is found.



Example Question: Multiple Choice

Which of the following describes a logic bomb?

1. A program that performs a malicious activity at a specific time or after triggering an event.
2. A type of malicious code similar to a virus whose primary purpose is to duplicate itself and spread, while not necessarily internally damaging or destroying resources.
3. A program that appears to be a legitimate application, utility, game, or screen saver that performs malicious activities surreptitiously.
4. A program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the system where it is found.



Example Question: Performance Based

Scenario: You are responsible for security at a small organization and have been tasked with implementing a security policy. Place the actions of organizing a security policy in their appropriate order. Note that there are five options, but you need to choose four.

Step 1 _____ > Step 2 _____ > Step 3 _____ > Step 4 _____

Possible choices:

- Obtain support and commitment from management.
- Analyze risks to security.
- Secure budgeting.
- Review, test, and update procedures.
- Implement appropriate controls.



Example Question: Performance Based

Scenario: You are responsible for security at a small organization and have been tasked with implementing a security policy. Place the actions of organizing a security policy in their appropriate order. Note that there are five options, but you need to choose four.

Step 1 _____ > Step 2 _____ > Step 3 _____ > Step 4 _____

Step 1: Obtain support and commitment from management.

Step 2: Analyze risks to security.

Step 3: Implement appropriate controls.

Step 4: Review, test, and update procedures.



Other Sample PBQs

You are in charge of creating an incident response process for your company. Match the procedures (*not mentioned in this example*) with the correct phases of the IR plan.

The phases are:

**Preparation,
Identification/Detection,
Analysis, Containment,
Eradication, Recovery**

You are in charge of deploying public key infrastructure (PKI) into your environment, and for this you need to have a good foundation in cryptographic technology. Drag the appropriate terminology to the function it's used for.

The terms are:

**Public key, Private key, Hash,
Digital signature**

You need to perform a business impact analysis (BIA) for a set of critical servers as part of a risk management push by your company. Organize the steps of a BIA in their proper order.

The steps are:


Identify threats, Remediate risk, Assign risk to each function or asset, Identify critical functions or processes, Identify assets and resources

CertMaster Practice Tool

CompTIA CertMaster Practice Tool


The practice tool takes a “question-first” approach to test prep.

Practice questions are organized according to the six domains covered in the exam.



These questions are divided into **subcategories** for different topics and tools within the domain.

CertMaster is an **adaptive knowledge assessment** tool.



Based on results of practice questions, CertMaster determines which categories you’ve mastered and which need more practice.

Next, we'll take a look at some of the Domain 1 subtopics and take some practice questions.

Try not to feel overwhelmed by the amount of information we're about to cover. You're not expected to learn all of this material today.

Rather, we want to give you a taste of the content covered on the exam.



Domain 1: Sub-Modules in CertMaster

Within this domain are five sub-modules:

1.1

Given a scenario, analyze indicators of compromise and determine the type of malware.

1.2

Compare and contrast types of attacks.

1.3

Explain threat actor types and attributes.

1.4

Explain penetration testing concepts.

1.5

Explain vulnerability scanning concepts.

Let's review **threat actor types**, to prepare for questions in sub-module 1.3:



Activity: Security+ Sample Questions

In this activity, you will work through Module 1.3 of the CertMaster Practice tool.

Suggested Time:
10 minutes



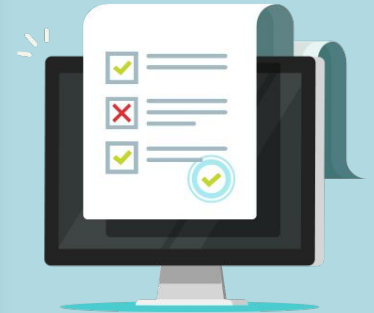


Time's Up! Let's Review.

Question 1:

Which of the following threat actors or threat actor groups is most likely to have the best funding to hire and sustain a group of cybercriminals?

1. Nation states
2. Organized crime
3. Script kiddies
4. Hacktivist groups



Question 1:

Which of the following threat actors or threat actor groups is most likely to have the best funding to hire and sustain a group of cybercriminals?

1. Nation states
2. Organized crime
3. Script kiddies
4. Hactivist groups

Extended Explanation:

- Nation states have tax revenues, backing from large companies, and/or wealthy benefactors who fund malicious activities.
- Well-funded, organized crime does not have the resources of an entire nation behind them.
- Script kiddies do not have any funding because they are typically young and inexperienced and do not qualify for any backing.
- Hactivist groups might have minor funding from opposing viewpoint factions but the funding is not significant nor comparable to nation states.



Question 2:

Which feature of insider threat actors makes them especially dangerous to an organization?

1. They will launch attacks using advanced persistent threats (APTs) to continuously compromise the system.
2. They are opposed to the organization's political or ideological goals.
3. They use prebuilt or canned programs for attacks.
4. They have unrestricted access to sensitive data and information.



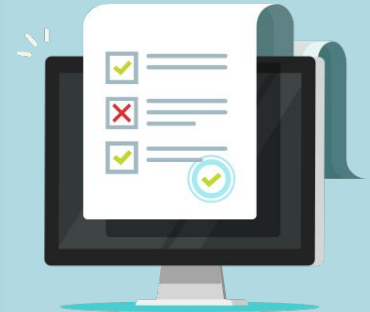
Question 2:

Which feature of insider threat actors makes them especially dangerous to an organization?

1. They will launch attacks using advanced persistent threats (APTs) to continuously compromise the system.
2. They are opposed to the organization's political or ideological goals.
3. They use prebuilt or canned programs for attacks.
4. They have unrestricted access to sensitive data and information.

Extended Explanation

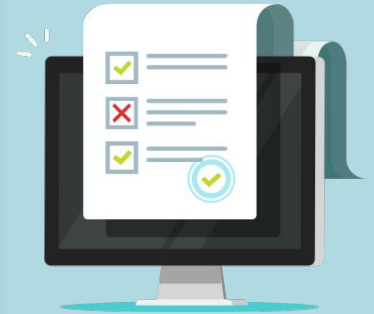
- Insider actors are dangerous because they have unrestricted access to sensitive data and information. That data can then be easily stolen or leaked by someone with appropriate access.
- Insiders prefer to stay in stealth mode and an APT will give away their intent.
- A hacktivist would oppose the organization's political or ideological goals. Insiders would never reveal this oppositional nature.
- Script kiddies use prebuilt or canned programs for attacks. Such attacks would likely give away the insider's position and intent.



Question 3:

Of the several types of threat actors, which one is a novice with little experience as a cybercriminal?

1. Hacktivist
2. Insider
3. Script kiddie
4. Competitor



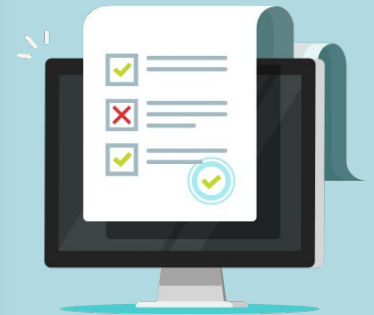
Question 3:

Of the several types of threat actors, which one is a novice with little experience as a hacker?

1. Hacktivist
2. Insider
3. Script kiddie
4. Competitor

Extended Explanation

- Script kiddies have very limited knowledge of security but use automated tools, such as scripts, to hack systems.
- A hacktivist is a hacker who gains access to systems or other resources to disrupt operations based on ideological differences with the target.
- An insider is someone who hacks internal systems in a company who has or had access to restricted materials.
- A competitor may attempt to hack, compromise, or sabotage another company or an individual's work to gain a competitive edge.



Question 4:

Which threat actor is most likely to be highly skilled in launching attacks involving advanced persistent threats (APTs) against targets?

1. Script kiddie
2. Nation state
3. Insider
4. Organized crime



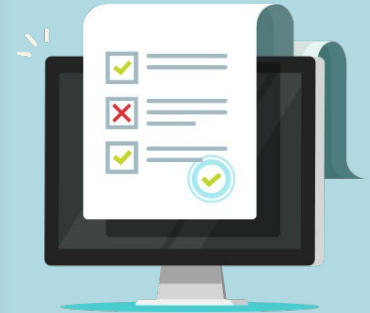
Question 4:

Which threat actor is most likely to be highly skilled in launching attacks involving advanced persistent threats (APTs) against targets?

1. Script kiddie
2. Nation state
3. Insider
4. Organized crime

Extended Explanation

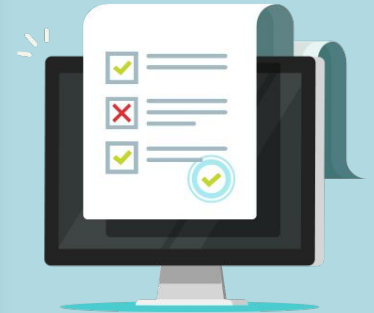
- A nation state has the most sophisticated and highly skilled cybercriminals available for launching APTs.
- Script kiddies are not highly skilled nor capable of launching APTs against targets.
- An insider can be highly skilled but does not use APTs because these would give away their positions and intent.
- Organized crime rings are highly skilled but they do not launch APTs against a target.



Question 5:

A group known as Takedown hacked into your political action committee website and defaced it. Which type of threat actor is most likely responsible for the attack?

1. Hacktivist
2. Script kiddie
3. Competitor
4. Insider



Question 5:

A group known as Takedown hacked into your political action committee website and defaced it. Which type of threat actor is most likely responsible for the attack?

1. Hacktivist
2. Script kiddie
3. Competitor
4. Insider

Extended Explanation

- Takedown is a hacktivist group. Its motivations seem political and it is interested in defacing websites of groups with opposing viewpoints.
- Script kiddies typically don't deface websites, but instead use scripts and applications to break into systems with known vulnerabilities.
- Although a malicious insider might have the ability to deface the site, it's unlikely they would. Insiders usually exfiltrate data rather than deface sites.
- It's unlikely that a competitor would deface the site. They'd more likely look for a list of donors or other sensitive information.



Question 6:

What aspect of cybercrime often motivates script kiddies to hack into systems or into a company?

1. Confidential company information
2. Financial motivation and ability to sell information
3. Collaboration with government and other agencies
4. Bragging rights, publicity, or other form of notoriety



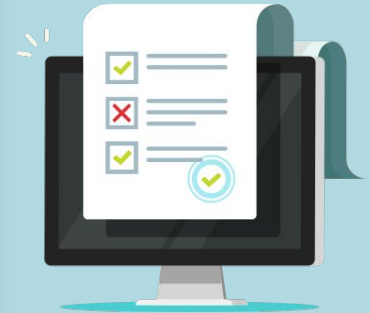
Question 6:

What aspect of cybercrime often motivates script kiddies to hack into systems or into a company?

1. Confidential company information
2. Financial motivation and ability to sell information
3. Collaboration with government and other agencies
4. Bragging rights, publicity, or other form of notoriety

Extended Explanation

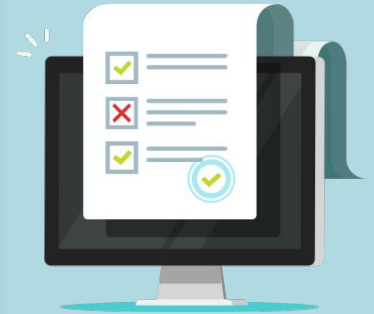
- Script kiddies generally just want to be able to tell their friends that they have hacked some company or want their names mentioned on the news.
- Script kiddies are not generally profit seekers because they do not have the resources to acquire or sell items.
- Script kiddies are not involved with government entities or agencies and therefore do not seek this type of information or activity.
- Private or secret information motivates insiders to become threats. Script kiddies do not gain profits by having access to private or secret information.



Question 7:

Which of the following motivates a hacktivist to perpetrate a website defacing or an informational breach?

1. Financial gain
2. Reputational damage to the target
3. Military tactics and political upheaval
4. Bragging right or other form of notoriety



Question 7:

Which of the following motivates a hacktivist to perpetrate a website defacing or an informational breach?

1. Financial gain
2. Reputational damage to the target
3. Military tactics and political upheaval
4. Bragging right or other form of notoriety

Extended Explanation

- Hacktivists are interested in damaging or exposing their ideological opposition but not generally for monetary gain or other accolades.
- Hacktivists are primarily concerned with damaging the reputations of their targets.
- Hacktivists have no interest in military tactics or political upheaval. Their interest is purely ideological.
- A boost in recognition is only important to script kiddies who want to show off to friends or rival script kiddie groups.



We covered a lot this week!

Don't be overwhelmed.

You were introduced new methods of thinking, new tools, and new areas of professional and technical exploration.

As we progress through this course, the skills learned this week will be fortified and expanded upon.