Certifications and Security+

Cybersecurity

Cybersecurity 101 Day 3

© 2020 Trilogy Education Services, Inc.

Class Objectives

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

Explain the landscape of certifications available to security professionals.

Articulate what the Security+ exam is and what InfoSec fields would benefit from obtaining the certification.

Answer sample practice questions from the Security+ exam.

Let’s do a quick review!

Quick Review

Last class, we introduced a framework that captures the fundamental goal of information security.

What was the framework?

Quick Review

The framework that captures the fundamental goal of information security:

The CIA Triad

Quick Review

What are the three elements of the CIA triad?

Quick Review

The three elements of the CIA triad are:

- **Availability**
- **Integrity**
- **Confidentiality**

Quick Review

Define each of the three elements in the context of information security:

Confidentiality
Integrity
Availability

Quick Review

Confidentiality:

Ensuring sensitive information is protected from reaches of unauthorized persons.

Integrity:

Protecting information from being modified or tampered by unauthorized persons.

Availability:

Ensuring that all operating systems, equipment, and data are functioning correctly and accessible by those who need it.

Quick Review

Provide an example of how each of the three elements can be adversely affected:

Confidentiality

Integrity

Availability

Quick Review

Confidentiality:

Banking breach releases credit card info into the public.

Integrity:

Student modifies official grades for himself and his friends.

Availability:

Hackers disable a website through a denial of service attack.

Research Presentations

Activity: Research Presentations

Last class, we introduced a number of threats for you to explore. In this activity, you will present your group research.

Make sure to send your presentations to the instructor via Slack.

Suggested Time:
1 Hour 30 Minutes

Homework Review: Research Discussions

1. What is this threat? (or what *was* it?)
2. What damage has it done?
3. What steps can or have been taken to mitigate?

Emotet	**Zealot Campaign**	**Digmine**	**Triton**	**BadRabbit**
Disakil	**Finfisher**	**Thrip**	**Orangeworm**	**Ploutus ATM Malware**
Gh0st RAT	**Trickbot**	**Necurs**	**BlankSlate**	**CVE-20170199**

Vulnerability, Exploits, and Threat Actors


40:00
Break

Security Certifications

Security Certifications

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

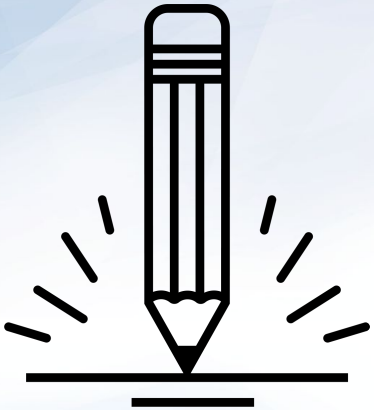
CompTIA certifies **Security+**, PenTest.

EC Council certifies CEH and ECIH.

ISC² certifies CISSP, SSCP.

Offensive Security certifies OSCP and OSWP.

GIAC certifies GPEN and GCIH.



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+:

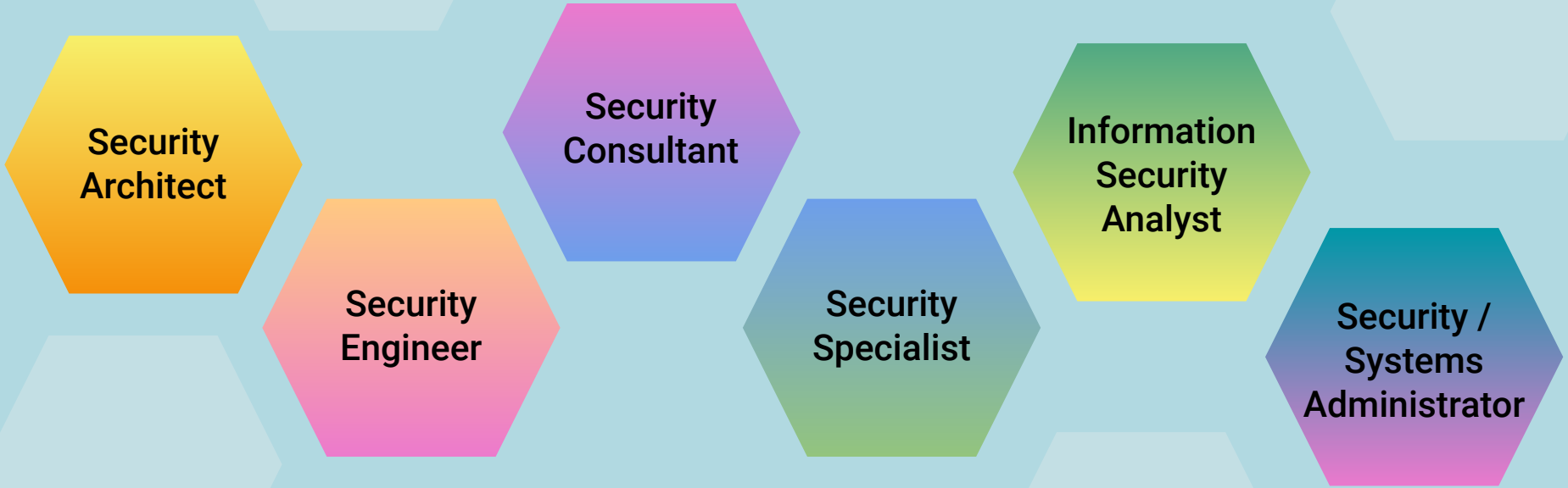
- Is the first security certification that IT professionals should earn.
- Establishes core knowledge required for any cybersecurity roles.
- Provides a springboard to intermediate-level cyber jobs.
- Incorporates hands-on troubleshooting to ensure practical security problem-solving.

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

- They provide testing and certification for the Security+ and other Cyber and IT fields like Network+, CASP+, CompTIA PenTest+.

Introduction to Security+ Certification

What are some jobs that may require the **Security+** certification?



As of December 2019, the average annual pay for an information security analyst in the United States is

$98,735.

Stat Reference: https://www.ziprecruiter.com/Salaries/Information-Security-Analyst-Salary

When 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?

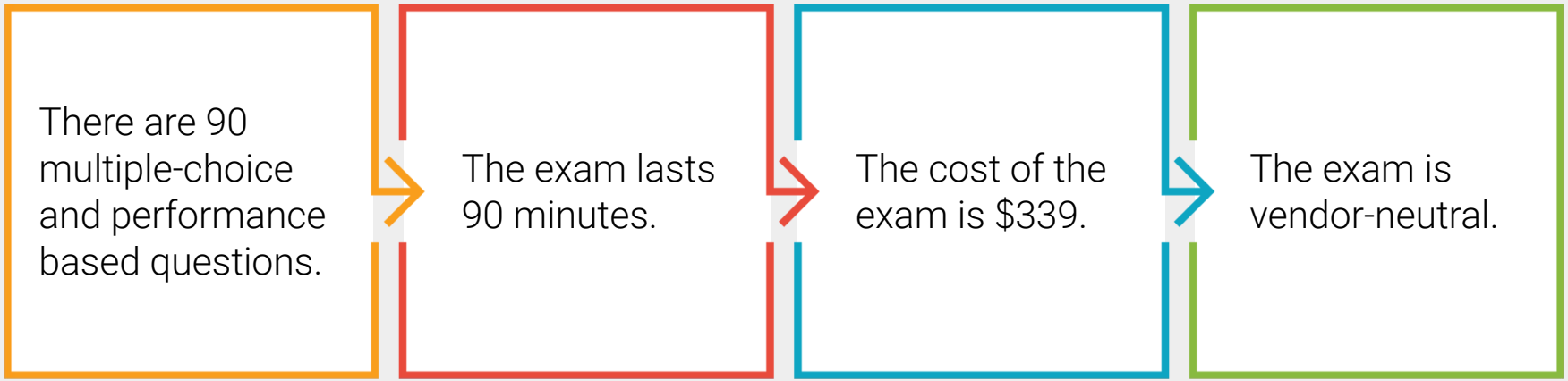
This course focuses on providing relevant hands-on experience of the most prominent and useful concepts, tools, and technologies used in security and networking. *It is not a test prep course*.

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.

- Therefore, while this course and exam share many overlapping coverage of topics, more niche topics that the exam covers will require additional study.
- **For example**, the TACACS+ protocol appears on the Security+ exam, but only engineers who work specifically with Cisco devices will use it.

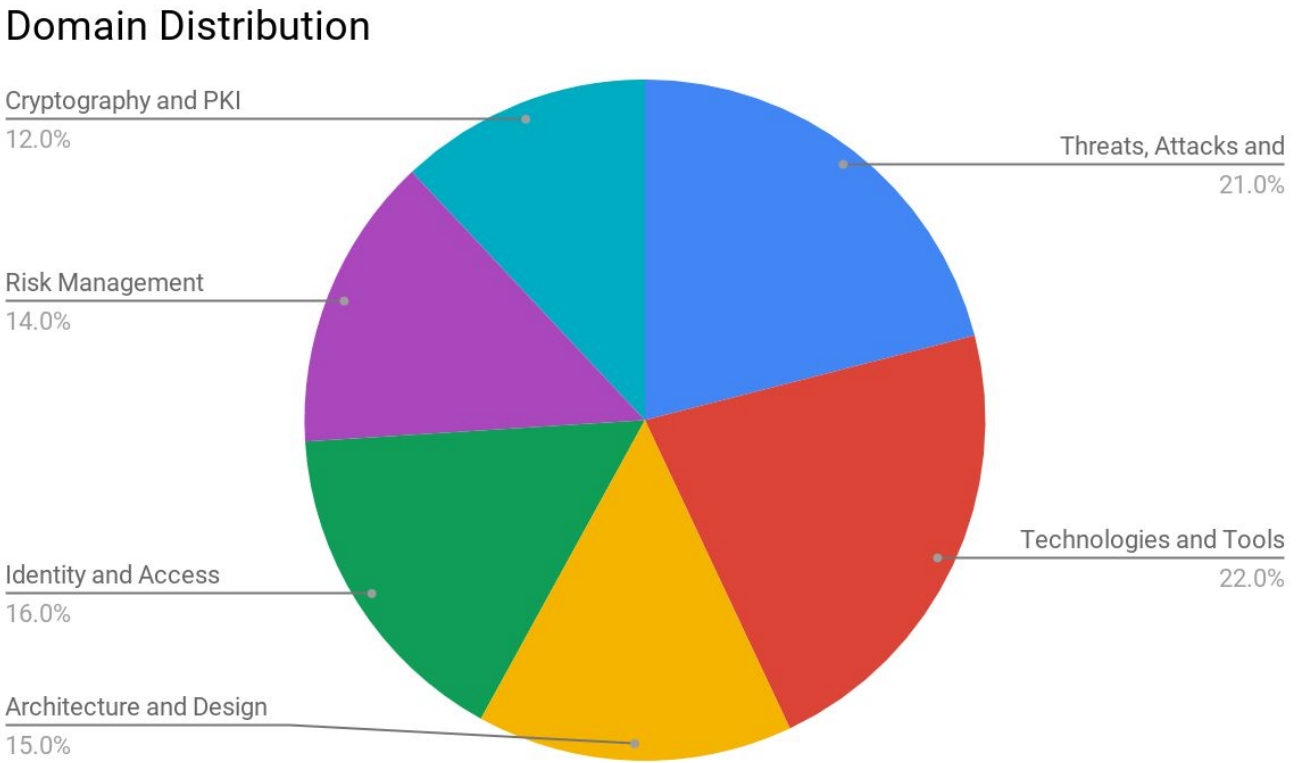
Security+ Specs

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



Security+ Exam Topics Breakdown

1. Threats, Attacks, and Vulnerabilities
2. Technologies and Tools
3. Architecture and Design
4. Identity and Access Management
5. Risk Management
6. Cryptography and PKI



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 different domains covered in the exam.

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

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

- Based on your results of practice questions, CertMaster will determine which categories you mastered and which categories need more practice.

Domain 1:
Threats, Attacks and Vulnerabilities

Domain 1: Threats, Attacks and Vulnerabilities

Subtopics and Examples Included:

- **Malware Types:** Ransomware, Trojans, Adware
- **Social Engineering:** Phishing, Vishing
- **Application Attacks:** DDOS, Cross Site Scripting, DNS Poisoning
- **Wireless Attacks:** Bluejacking, Evil Twin
- **Cryptographic Attacks:** Birthday Attack, Rainbow Tables
- **Threat Actors:** Script Kiddies, Hacktivists
- **Vulnerability Scanning:** ID-ing Misconfigurations, lack of security controls
- **Vulnerability Types:** Improper Input Handling, Improper Error Handling

Domain 1: Sample Question #1

A system being investigated is found to have had several of its core operating system files modified, but no traces of malware are found. What type of attack is this and how was it able to avoid detection?

1. The system is infected with a Trojan. It is able to avoid detection by operating in kernel mode and blocking attempts to detect it.
2. The system is infected with a rootkit. It is able to avoid detection by operating in kernel mode and blocking attempts to detect it.
3. The system has been compromised with an exploit framework. The attack is not detectable because it has migrated to another process.
4. The system has been compromised with an APT attack. It is not detectable as malware because the attacker is controlling the system directly.

Domain 1: Sample Question #1

A system being investigated is found to have had several of its core operating system files modified, but no traces of malware are found. What type of attack is this and how was it able to avoid detection?

1. The system is infected with a Trojan. It is able to avoid detection by operating in kernel mode and blocking attempts to detect it.
2. The system is infected with a rootkit. It is able to avoid detection by operating in kernel mode and blocking attempts to detect it.
3. The system has been compromised with an exploit framework. The attack is not detectable because it has migrated to another process.
4. The system has been compromised with an APT attack. It is not detectable as malware because the attacker is controlling the system directly.

Domain 1: Sample Question #2

Of a vulnerability, threat, exploit, and risk, which would be assessed by likelihood and impact?

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

Domain 1: Sample Question #2

Of a vulnerability, threat, exploit, and risk, which would be assessed by likelihood and impact?

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

Domain 1: Sample Question #3

In which stage of the “kill chain” does a threat actor first gain access to a resource on the target network?

1. Exploit
2. Reconnaissance
3. Installation
4. Command and Control

Domain 1: Sample Question #3

In which stage of the “kill chain” does a threat actor first gain access to a resource on the target network?

1. Exploit
2. Reconnaissance
3. Installation
4. Command and Control

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

Don't 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 that is covered in 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:

Threat Actors: External

There are various external threat actors:

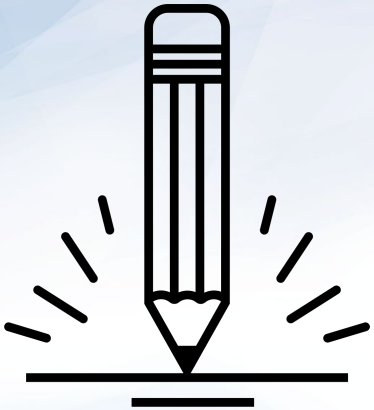
- The Lone Hacker (Black Hat / Script kiddies)
- Organized Cyber Crimes
- Nation State / Advanced Persistent Threat (APT)
- Hacktivists
- Competitor

Threat Actors: Inside Threats

Inside threats are affiliated with the organization: staff, partners, stakeholders, etc.

- Motivations include: sabotage, revenge, financial or business gains.
- Inside actors are more likely to bypass **technical controls**, meaning strong **operational** and **management controls** are needed to mitigate threats, such as:
  - Comprehensive on and off-boarding
  - Mandatory vacations
  - User awareness / training
  - Principle of least privilege

We'll dive into this topic when we learn about governance, risk and compliance.



Activity: Threat Actor Type Questions

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

(Question sheets shared by instructor.)

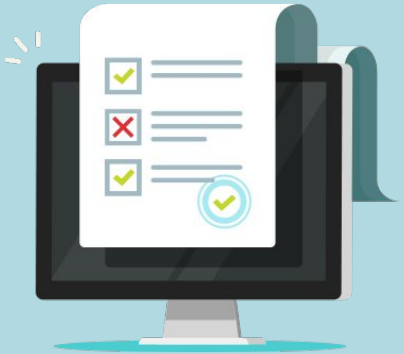
Suggested Time:
10 minutes

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 hackers?

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 hackers?

1. Nation states
2. Organized crime
3. Script kiddies
4. Hacktivist 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.
- Hacktivist 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 have unrestricted access to sensitive data and information.
2. They oppose the organization's political or ideological goals.
3. They launch advanced persistent attacks (APTs) against their own organization.
4. They use canned threat programs to launch their attacks.

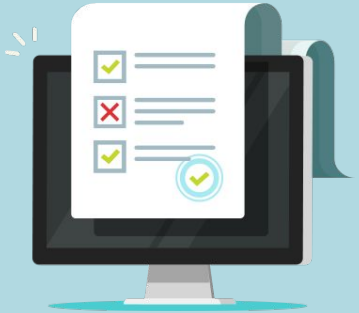
Question 2:

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

1. They have unrestricted access to sensitive data and information.
2. They oppose the organization's political or ideological goals.
3. They launch advanced persistent attacks (APTs) against their own organization.
4. They use canned threat programs to launch their attacks.

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.
- The insider would 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. An insider 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 hacker?

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

Question 3:

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

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

Extended Explanation

- Script kiddies use prebuilt or canned programs for attacks. Such attacks would likely give away the insider's position and intent.
- 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.
- The insider would 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. An insider would never reveal this oppositional nature.

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 hackers available for launching APTs.
- A script kiddies is not highly skilled nor capable of launching APTs against targets.
- An insider can be highly skilled but does not use APTs because it 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 those who have opposing viewpoints from their own.
- Script kiddies typically do not deface websites, but instead use scripts and applications to break into systems or applications with known vulnerabilities.
- Although a malicious insider might have the ability to deface the site, it’s unlikely they would do so. 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 only want to be able to tell their friends that they have hacked some company or hear their names on the news.
- Script kiddies are not generally profit seekers because they do not have the resources for acquisition or the sale of these 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 opposites 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.

Viruses and Worms

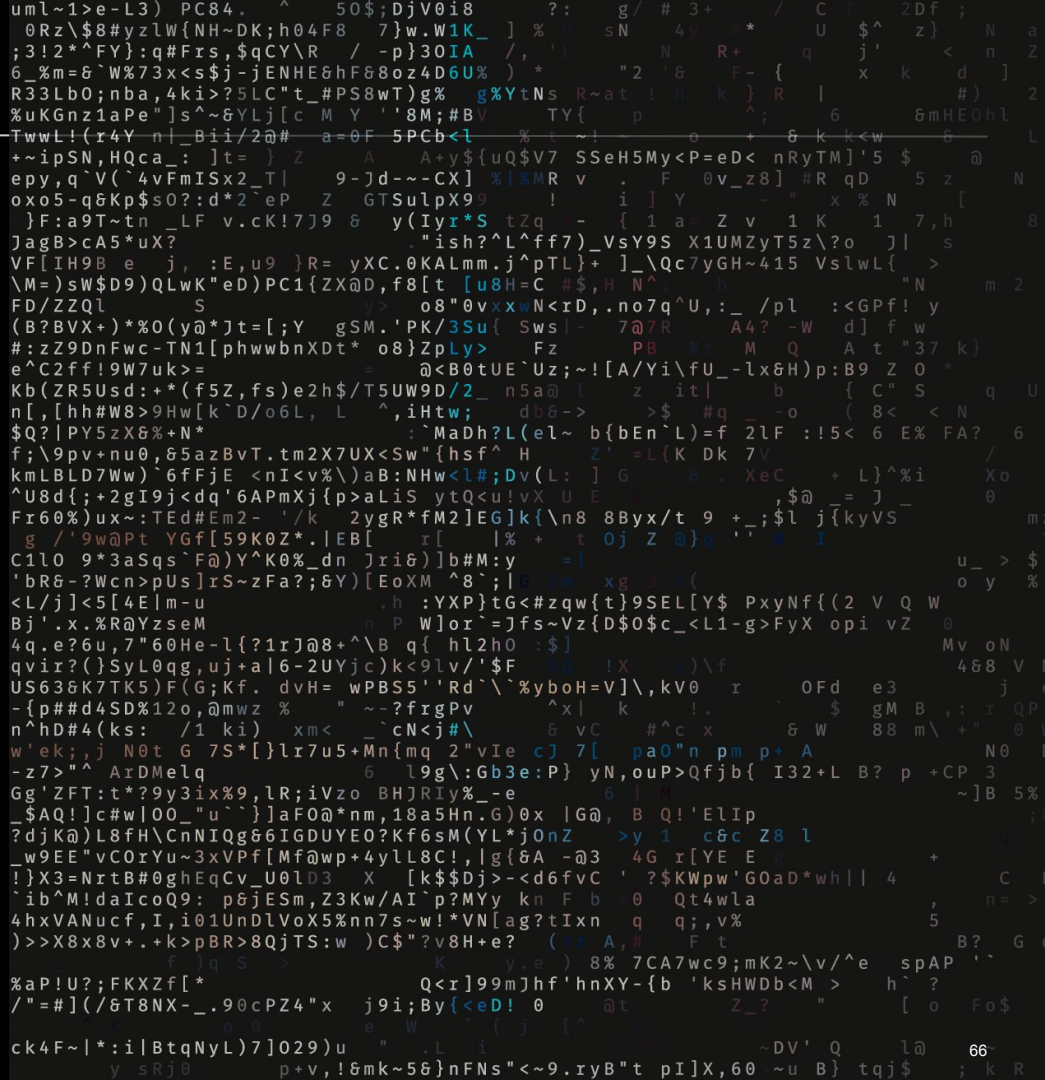
The Security+ Exam covers common types of malware and malware attacks.

We'll begin by looking at viruses and worms.

Viruses

A virus is a program that copies itself onto another computer systems.

- When the user runs the infected application, the virus also runs and copies itself onto *other* applications on the system as well.



Viruses

Viruses can damage the infected hosts in the following ways:

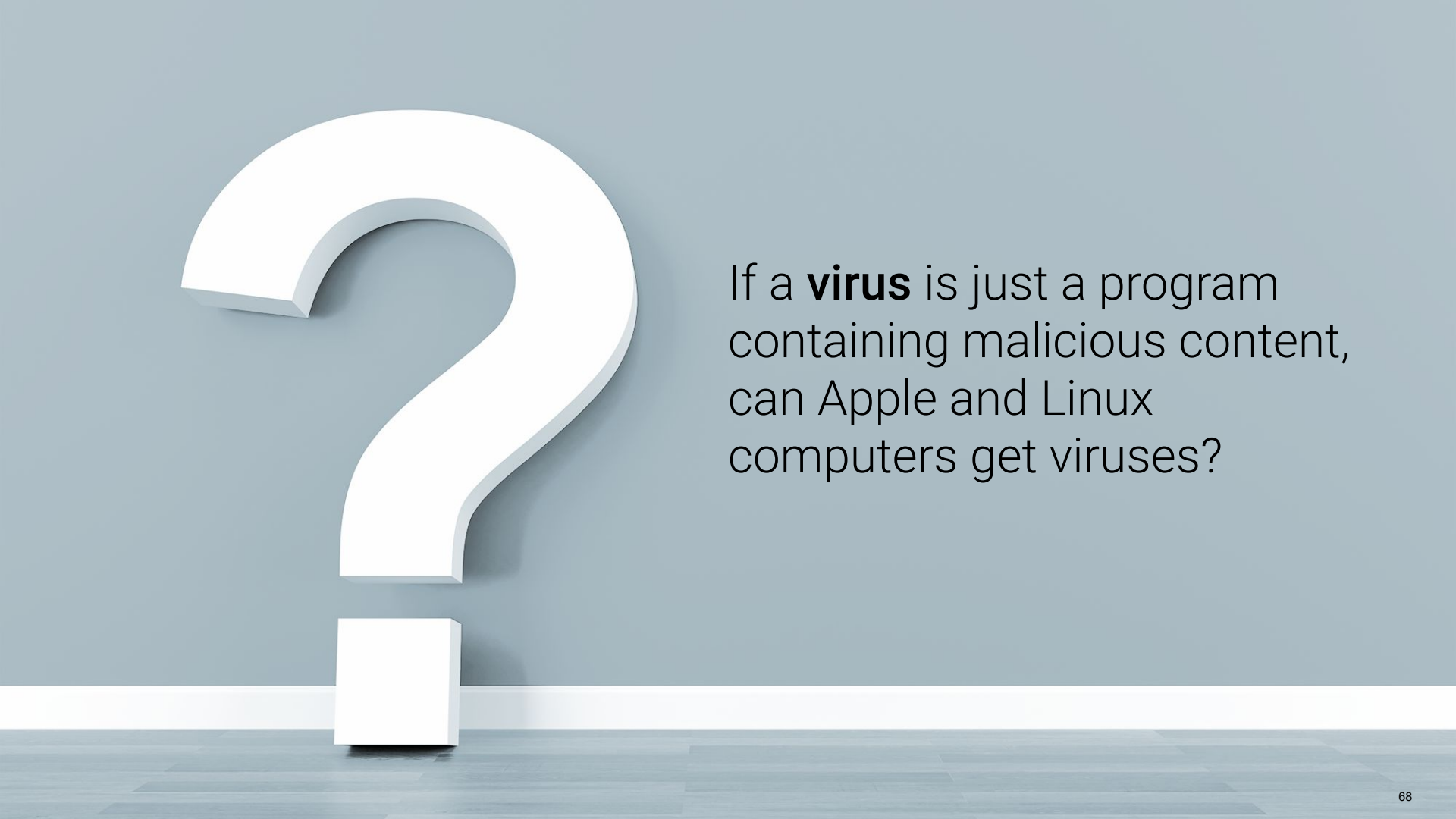
Slowing down the host by using up a computer's resources, such as **CPU** and **RAM**.

Denial of Service Attacks (DoS):

Shutting down the host by using up *all* of its resources or destroying essential files.

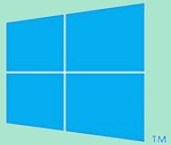
Ransomware:

"Scrambling" data on the host so that users can't read it, and demanding money to "unscramble" it.


If a **virus** is just a program containing malicious content, can Apple and Linux computers get viruses?

Viruses on Different Operating Systems

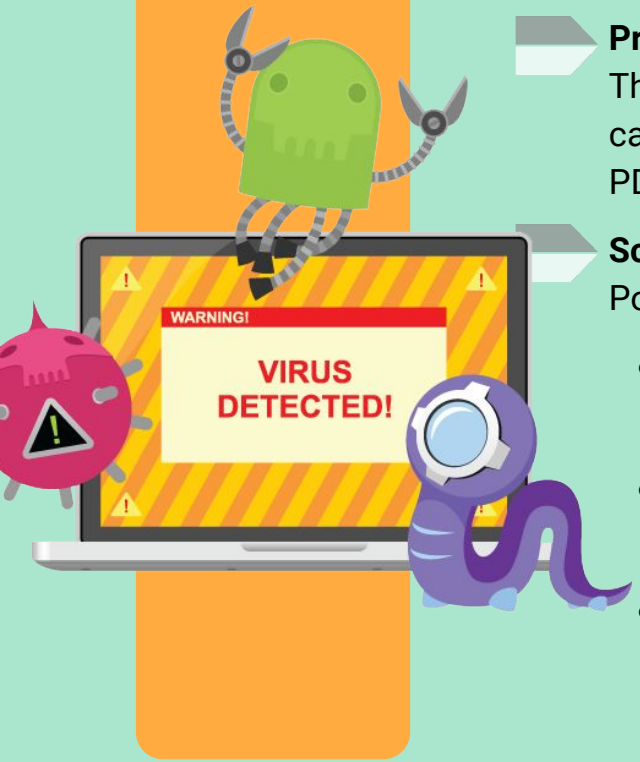
Every operating system is prone to viruses:



- Windows machines are the most widely used operating systems worldwide, so they are more prone to viruses.
  - Virus writers tend to target the most prominent machines, to boost the spread of their viruses.

- Windows are additionally more vulnerable, because their users often operate machines with administrator privileges.
  - Therefore, programs will download without asking the user.
  - Mac and Linux users are low-privileged and non-administrator by default.

Virus Types



Boot sector viruses attack the operating system, specifically the disk boot sector information, the partition table, and sometimes the file system.

Program viruses are code that insert themselves into executable programs. The virus becomes active once the program runs. These executable objects can be embedded or attached within other file types such as Word docs and PDFs.

Script viruses are written in a scripting language, such as JavaScript or PostScript.

- Script viruses are dangerous because they can be embedded in web pages or PDF files, making them harder to detect.
- When a user opens the web page or PDF file, the software that loads the page or PDF will read and run the virus code.
- Since the virus was contained in a “normal” web page or PDF document, users typically won’t realize that they’ve been infected.

Virus Types

Macro viruses are written in the same macro language used for software programs, such as Microsoft Word.

- Since they are focused on an application and not an operating system, they can generally infect any computer running any operating system.
- When executed, they can infect every other document on a user's computer.

Multipartite viruses use both boot sector and executable file infection methods to spread themselves.

Viruses

All virus types need to infect a host file, which can be distributed in a number of ways, such as on a disk, a network, or as an email or message attachment.

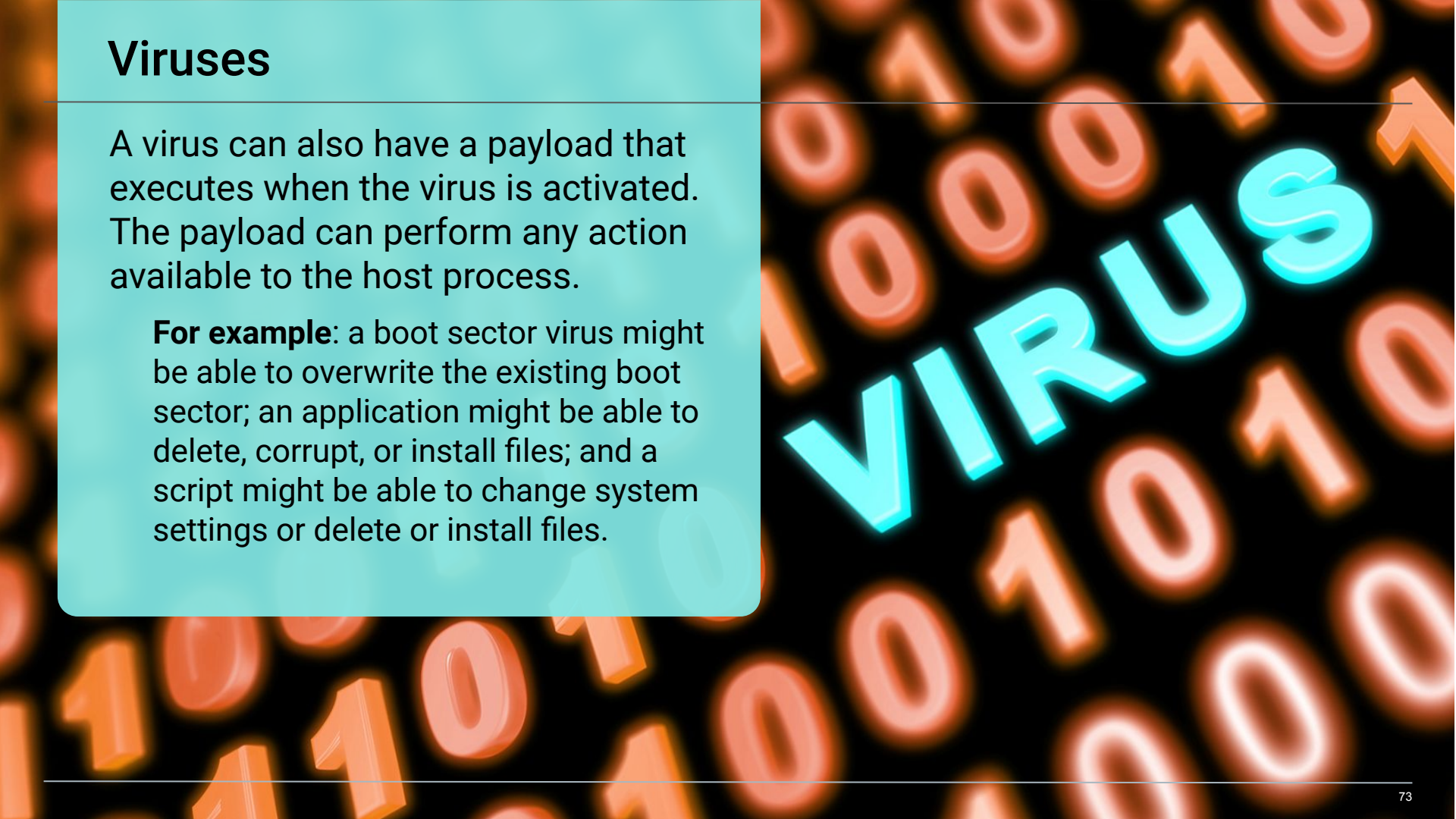
For example: Email attachment viruses, which are usually program or macro viruses hosted in an attached file, can use the infected victim's list of email contacts to spoof the sender's address when replicating.

Alex's computer is infected with a virus. Lindsey's email address is in his address book. The virus on Alex's computer can spoof Lindey's email address and send an infected email to a third person, Jeremy.

Viruses

A virus can also have a payload that executes when the virus is activated. The payload can perform any action available to the host process.

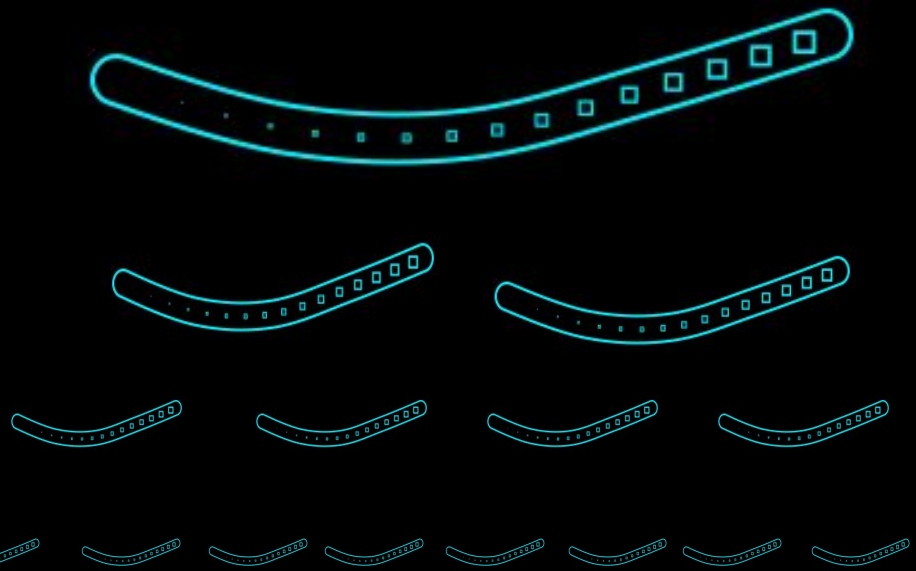
For example: a boot sector virus might be able to overwrite the existing boot sector; an application might be able to delete, corrupt, or install files; and a script might be able to change system settings or delete or install files.



Worms

A **worm** is a *self-replicating* program. It is considered a **memory-resident virus**. A worm does not need to attach itself to an executable file and instead can replicate over network resources.

- Worms usually target vulnerabilities in an application and will quickly consume network bandwidth as the replicate.
- They can also crash an operating system or server application, via a DoS attack.
- Like viruses, worms can have a payload that perform further malicious actions.



Viruses vs. Worms

It can be easy to confuse worms and viruses. **Make sure you know the difference.**

01 Viruses

- A virus attaches itself to a host.
- A virus requires an **activation mechanism**, meaning something has to be executed for the virus to take effect.

02 Worms

- Once on a computer, a worm **does not need human interaction** to activate.
- A worm **automatically replicates** itself and can travel across computer networks without human interaction.

1. Since viruses and worms are merely programming scripts, is every OS vulnerable?
2. A _____ needs a host mechanism to spread.
3. Is a virus self-replicating?
4. *True or False*: Once on a computer, a worm does not need human interaction to activate.
5. *True or False*: Worms replicate by themselves.

1. Since viruses and worms are merely programming scripts, is every OS vulnerable? **YES**
2. A _____ needs a host mechanism to spread.
3. Is a virus self-replicating?
4. *True or False*: Once on a computer, a worm does not need human interaction to activate.
5. *True or False*: Worms replicate by themselves.

1. Since viruses and worms are merely programming scripts, is every OS vulnerable? **YES**
2. A **VIRUS** needs a host mechanism to spread.
3. Is a virus self-replicating?
4. *True or False*: Once on a computer, a worm does not need human interaction to activate.
5. *True or False*: Worms replicate by themselves.

1. Since viruses and worms are merely programming scripts, is every OS vulnerable? **YES**
2. A **VIRUS** needs a host mechanism to spread.
3. Is a virus self-replicating? **NO**
4. *True or False*: Once on a computer, a worm does not need human interaction to activate.
5. *True or False*: Worms replicate by themselves.

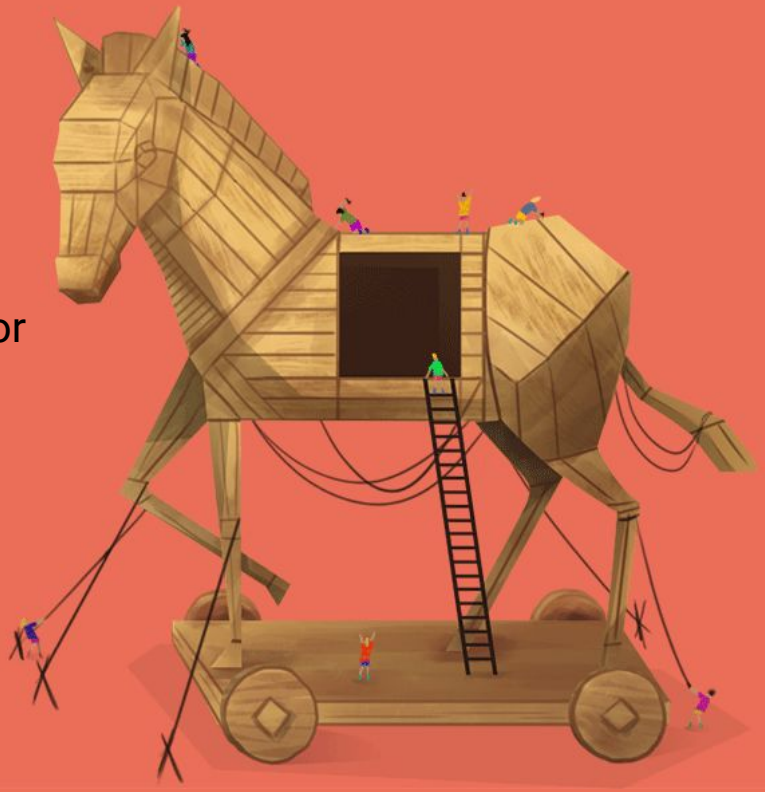
1. Since viruses and worms are merely programming scripts, is every OS vulnerable? **YES**
2. A **VIRUS** needs a host mechanism to spread.
3. Is a virus self-replicating? **NO**
4. *True or False*: Once on a computer, a worm does not need human interaction to activate. **TRUE**
5. *True or False*: Worms replicate by themselves.

1. Since viruses and worms are merely programming scripts, is every OS vulnerable? **YES**
2. A **VIRUS** needs a host mechanism to spread.
3. Is a virus self-replicating? **NO**
4. *True or False*: Once on a computer, a worm does not need human interaction to activate. **TRUE**
5. *True or False*: Worms replicate by themselves. **TRUE**

Trojans and RATs

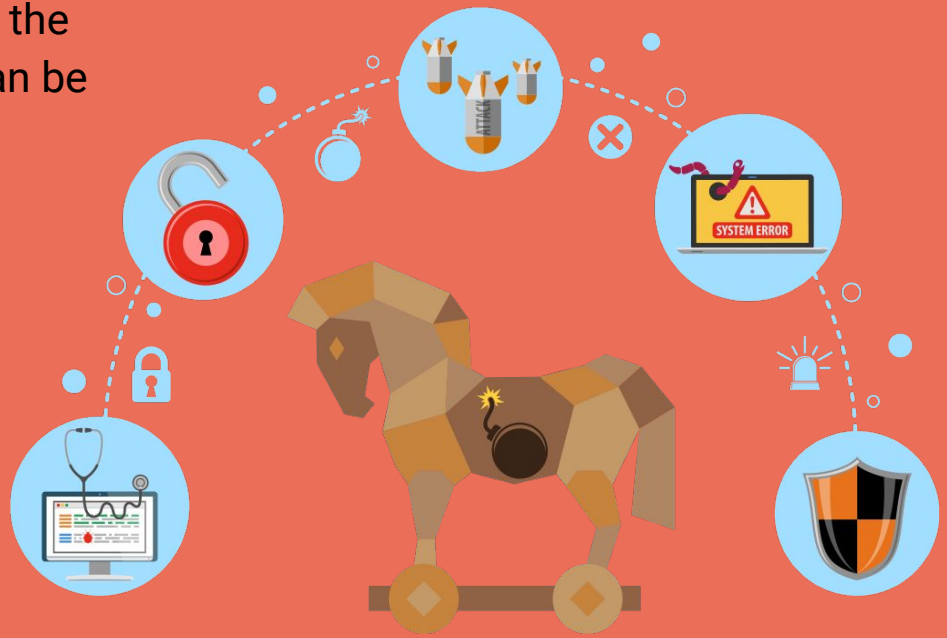
Trojans and RATs

- A **Trojan** is a program that typically hides within something else. They can be embedded within a downloadable object, such as a game or screensaver.
- **Remote Access Trojans (RAT)** function as backdoor applications. Once this Trojan backdoor is installed, the attacker can access the victim's computer and install files and software on it.
    - The RAT needs to establish a covert channel from the victim's host to a Command and Control (C2 or C&C) host or network operated by the attacker. Identifying a network connection is usually the best indicator that a RAT has compromised a victim's computer.



Trojans and RATs

- When the attacker is able to send remote commands to the victim's computer, the computer is called a **zombie**. This can be used for many purposes, such as downloading additional malicious programs.
- **Botnets** are two or more zombie computers that are remotely controlled by an attacker.



Spyware, Adware, and Keyloggers

- **Spyware** is a program that gains a foothold into the victim's system, and can be installed with or without the user's knowledge. They monitor user activity and send the information to an external source.
- **Keyloggers** actively attempt to steal confidential information by capturing the keystrokes of the victim. Keyloggers are considered a type of spyware, as they are hidden on the remote computer system and used to discreetly capture the victims information.

- **Adware** is any type of software or browser plugin that displays or downloads advertisements via pop-ups. Some can act like spyware, for example, by tracking websites that a user visits.

Backdoors

- **Backdoors** are remote access methods that are installed without the user knowing.
  - These installations can occur if the user has unknowingly installed malware, such as a Trojan.

Backdoors can also be created in different ways:

- Programmers create backdoors in software application for testing and development, but do not always remove them when the application is deployed.
- Some software or hardware misconfigurations can give unauthorized users access.
  - **For example**: A router can remain configured with the default administrative password.

Rootkits

Some Trojans appear as a running service. These service names are typically configured to be similar to real services in order to avoid detection.

Rootkits are a type of backdoor that are more difficult to detect and remove. They remain undetected by:

- Changing core system files and programming interfaces. The local shell processes can’t show their presence if run from an infected machine.
- Using tools that clean system logs.

They are installed into the kernel of an operating system, which means that they can infect a machine through a corrupted device driver or kernel patch.

While less effective, some rootkits can operate in user mode, meaning that they can replace key utilities or less-privileged drivers.

Vulnerabilities, Exploits, and Risks

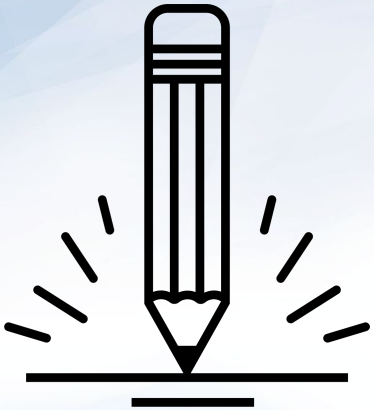
Vulnerabilities are weaknesses that can be exploited by an attacker.

- One broad category are zero-day vulnerabilities. These occur when software or hardware is not 100% secure.

Exploits are how actors attack computer systems. They can be malware or scripts that disrupt the normal flow of the computer.

Risks can include known kept vulnerabilities.

- These vulnerabilities are kept because it would either cost the business too much to protect against them, or the business would not be able to operate without the risk.
- Risks can be reduced, but it's impossible to fully remove all risks in an organization.
- Organizations have a formula to calculate risks: **Risk = Likelihood × Impact**.



Activity: Indicators of Compromise Questions

In this activity, you will work through Module 1.1 of the CertMaster Practice.

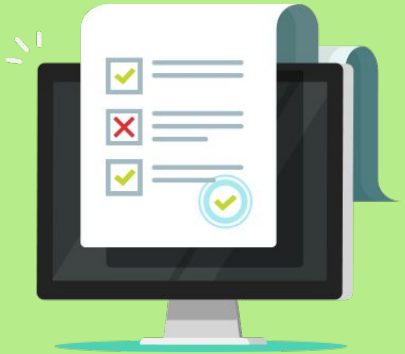
(Question sheets will be shared by instructor.)

Suggested Time:
10 minutes

Question 1:

Which of the following is a type of a classic virus that infects executable files, and upon execution of an infected file, infects other files?

1. Macro viruses
2. Metamorphic viruses
3. File-infecting or classic viruses
4. Crypto-malware



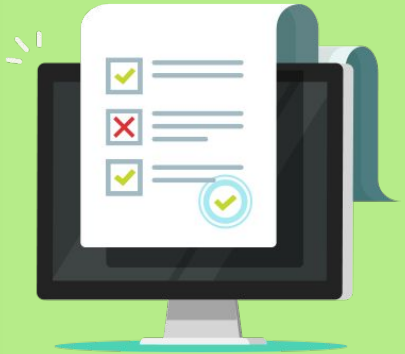
Question 1:

Which of the following is a type of a classic virus that infects executable files, and upon execution of an infected file, infects other files?

1. Macro viruses
2. Metamorphic viruses
3. File-infecting or classic viruses
4. Crypto-malware

Extended Explanation

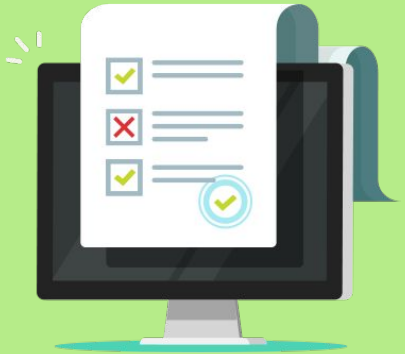
- File-infecting or classic viruses infect executable files, and upon execution of an infected file, the viruses spread to other executable.
- Macro viruses only affect documents of a specific type, such as DOC or DOCX files, and not executable files.
- Metamorphic viruses are very complex viruses in that they can infect executable of different operating systems and they change code with each infection. This is not classic virus behavior.
- Crypto-malware is not a virus, but a type of ransomware in which the attacker has encrypted a victim's files and demanded a ransom to have them unencrypted.



Question 2:

A network administrator suspects that several computers on the network have been compromised by malware because of the large numbers of TCP connections to a single IP address. Upon checking the IP address' origin, the administrator finds that it belongs to a major political action committee. Which type of malware has infected this network?

1. Botnet
2. Trojan horse
3. Ransomware
4. Adware



Question 2:

A network administrator suspects that several computers on the network have been compromised by malware because of the large numbers of TCP connections to a single IP address. Upon checking the IP address' origin, the administrator finds that it belongs to a major political action committee. Which type of malware has infected this network?

1. Botnet
2. Trojan horse
3. Ransomware
4. Adware

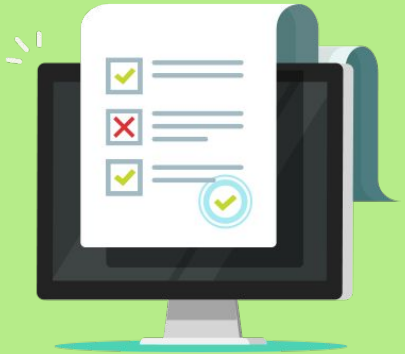
Extended Explanation

- A botnet infects multiple computers on a network in order to attack a target to halt its operation through a Distributed Denial of Service (DDoS) attack.
- A Trojan horse is hidden malware that causes damage to a system or gives an attacker a platform for monitoring and/or controlling a system. Its purpose is to remain stealthy and not reveal itself via network connections to an outside source.
- Ransomware has a single purpose: to extort money from its victims. It will not create connections from the infected computer to any third party target.
- Adware is noisy, annoying, and disruptive but does not make multiple network connections to a target in order to bring it down from a DDoS attack.

Question 3:

A user found that their personal data had been exfiltrated from their computer by a malicious program that they clicked on several weeks ago. Which type of malware infected the user's system?

1. Zombie
2. Spyware
3. Virus
4. Trojan horse



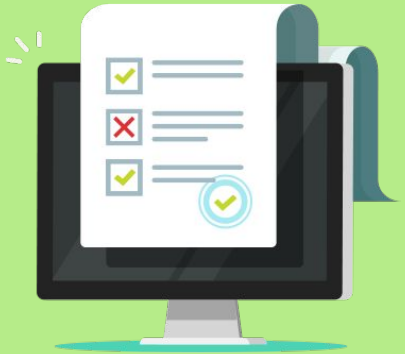
Question 3:

A user found that their personal data had been exfiltrated from their computer by a malicious program that they clicked on several weeks ago. Which type of malware infected the user's system?

1. Zombie
2. Spyware
3. Virus
4. Trojan horse

Extended Explanation

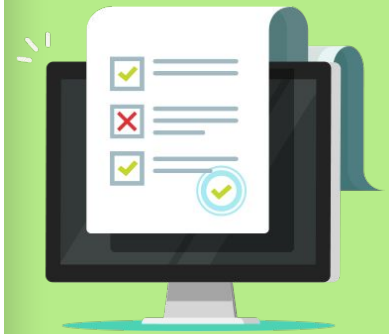
- The user was infected by spyware, whose purpose is to exfiltrate user data to an external location.
- A zombie is not a malware infection, but a computer connected to the Internet that has been compromised by an attacker and can be used to perform malicious tasks under remote direction.
- A virus typically disrupts user productivity by disabling services and programs or entire systems, but does not exfiltrate data.
- Trojan horses cause direct damage to a system or network of systems by allowing the Trojan writer to monitor or control a system that is inside the infected network.



Question 4:

A malicious actor has contacted multiple individuals at a company over multiple months in order to convince unsuspecting users to execute a malicious file on their systems. By doing so, the actor could covertly gain control of those systems and establish a presence inside the network. Which type of malware was the actor attempting to have the users execute?

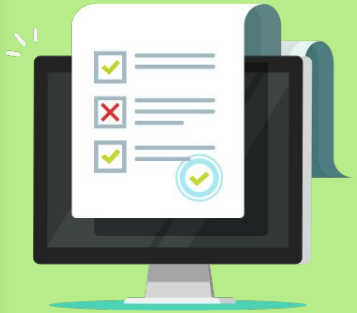
1. Virus
2. Adware
3. Spyware
4. Trojan horse



Question 4:

A malicious actor has contacted multiple individuals at a company over multiple months in order to convince unsuspecting users to execute a malicious file on their systems. By doing so, the actor could covertly gain control of those systems and establish a presence inside the network. Which type of malware was the actor attempting to have the users execute?

1. Virus
2. Adware
3. Spyware
4. Trojan horse



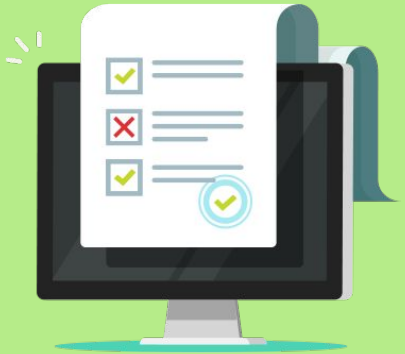
Extended Explanation

- The malicious actor (caller) is using social engineering tactics to have the victims execute a Trojan horse so that he or she can gain control of at least one computer inside the target network. This could be by sending the victims a file and requesting they open it.
- A virus wouldn't give the actor control of any computer, but would allow him or her to disrupt productivity.
- Adware wouldn't give the actor control, but could possibly allow them to exfiltrate data.
- Spyware wouldn't give the actor control, but would allow them to exfiltrate data.

Question 5:

Which of the following is an example of evidence that a system has been infected with some type of malware?

1. Anti-virus update notifications
2. Email being routed to a spam folder
3. Unsolicited pop-up advertisements
4. Windows updates notifications



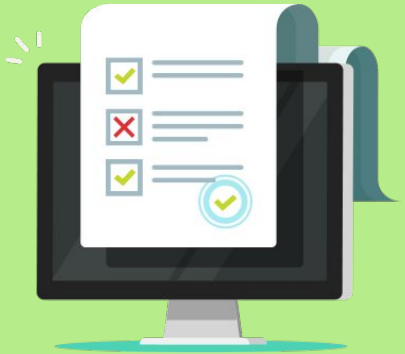
Question 5:

Which of the following is an example of evidence that a system has been infected with some type of malware?

1. Anti-virus update notifications
2. Email being routed to a spam folder
3. Unsolicited pop-up advertisements
4. Windows updates notifications

Extended Explanation

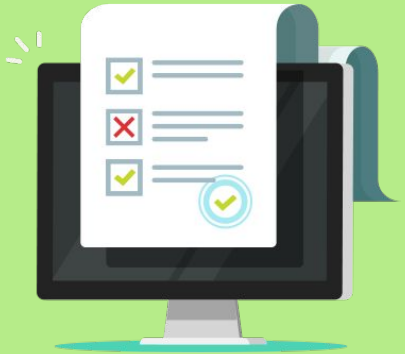
- Malware can generate unsolicited pop-up advertisements. These advertisements direct users to clandestine websites that can steal information or infest their system with more malware.
- Normal notifications for anti-virus updates are not unusual.
- Email that is routed to the junk or spam folder means that the email's spam filter is working correctly.
- Normal notifications for Windows updates are expected and not unusual.



Question 6:

A rootkit is a particularly dangerous type of malware. What makes it so dangerous?

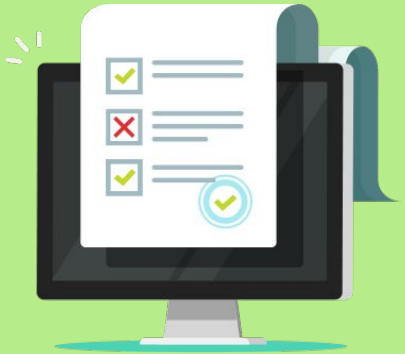
1. It takes control of a system at the lowest levels while attempting to hide from detection.
2. It attaches to files and spread from one computer to another.
3. It generates unsolicited advertisements that direct users to sites infected with malware.
4. It records all keystrokes made by a user, exposing that user's passwords.



Question 6:

A rootkit is a particularly dangerous type of malware. What makes it so dangerous?

1. It takes control of a system at the lowest levels while attempting to hide from detection.
2. It attaches to files and spread from one computer to another.
3. It generates unsolicited advertisements that direct users to sites infected with malware.
4. It records all keystrokes made by a user, exposing that user's passwords.



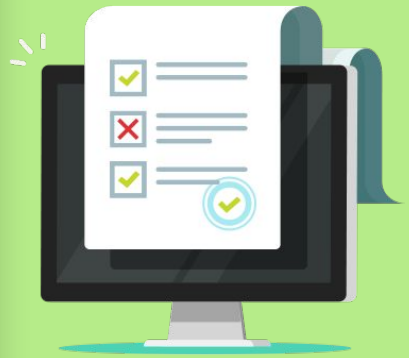
Extended Explanation

- A rootkit is so dangerous because it is designed to hide from normal detection methods. Rootkits attempt to integrate at the "root" or lowest level of a computer system, providing access to an attacker. Once an attacker has administrative privileges, they can further mask their activities, making detection nearly impossible.
- Viruses attach to files and spread from one computer to another.
- Adware generates unsolicited advertisements that direct users to sites infected with malware.
- Keyloggers record all keystrokes made by a user, exposing that user's passwords.

Question 7:

What is the major benefit to an attacker using a so-called backdoor attack?

1. The backdoor can be opened and closed at will.
2. The backdoor automatically guarantees privileged system access.
3. An attacker can set up fake entry points.
4. The backdoor helps the attacker break into a target's infrastructure without being discovered.



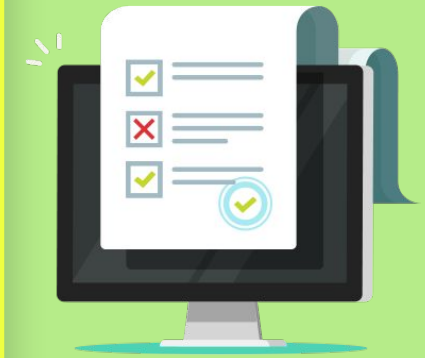
Question 7:

What is the major benefit to an attacker using a so-called backdoor attack?

1. The backdoor can be opened and closed at will.
2. The backdoor automatically guarantees privileged system access.
3. An attacker can set up fake entry points.
4. The backdoor helps the attacker break into a target's infrastructure without being discovered.

Extended Explanation

- Backdoors, which can exist for legitimate remote access, can also allow attackers into a network without discovery.
- The backdoor cannot be opened and closed at will. If the attacker closes the backdoor, he or she no longer has access.
- Backdoors are legitimate passages into a system or network and there is no need to set up fake entry points, which would be discovered.
- Backdoors typically only provide access to a single point of entry, such as a single server, and not all access nor privileged access is guaranteed.



We just covered a lot!

Don’t feel overwhelmed.

By the time you receive your Certmaster Practice Tool later in the course, you will be more prepared to answer questions and learn about other domains.