



# Security + Certification






Cybersecurity  
Review Week Day 1



# Class Objectives

---

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

-  Understand the landscape of certifications available to security professionals.
-  Describe the Security+ exam and the InfoSec fields that would benefit from obtaining the certification.
- 
  - Understand the requirements, pre-requisites and details of the Security+ exam.
-  Use the **Certmaster Practice** tool to prepare for the Security+ exam.
-  List the domain topics covered in the exam that we have and have not covered previously in our class.

# 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.

**ISC<sup>2</sup>** certifies CISSP, SSCP.

**Offensive Security** certifies OSCP and OSWP.

**GIAC** certifies GPEN and GCIH.



Today, we'll take a closer look at CompTIA's Security + certification and exam.



## Certification Landscape

Check out this list of over 100 Professional Security Certifications!

[https://en.wikipedia.org/wiki/List\\_of\\_computer\\_security\\_certifications](https://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  
them:

**Security +**

# Introduction to Security +

# What is a Security +?

---

According to **CompTIA**, Security + :

- Is an early security certification IT professionals could 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 an 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 certifications?

- Security Architects
- Security Engineers
- Security Consultants
- Security Specialists
- Information Security Analyst
- Security / Systems Administrator



As of May 30, 2019, the average annual pay for an Information Security Analyst in the United States is **\$98,735**.

# Introduction to Security + Certification

---

What are some skills that the Security + certification endorses?



Threats, Attacks, and Vulnerabilities



Technologies and Tools



Architecture and Design



Identity and Access Management



Risk Management



Cryptography and PKI

# When Should You Take The Exam?

---

Security + is considered an entry-level exam. The skills that you've learned in this course have provided a strong foundation for you to take the exam.

However, the Sec+ exam is broad and will require additional knowledge in areas that we've chosen not to cover in this program.

The CompTIA CertMaster tool will provide the necessary coverage needed to cover the gaps and master the exam.

# Why Do We Not 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.

Some topics on the Security+ exam are not covered in this course because they are highly specific, and relevant in 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 ever use it.

# Security + Specs

---

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



There are 90 multiple-choice and performance based questions.



The exam lasts 90 minutes.



The cost of the exam is \$339.

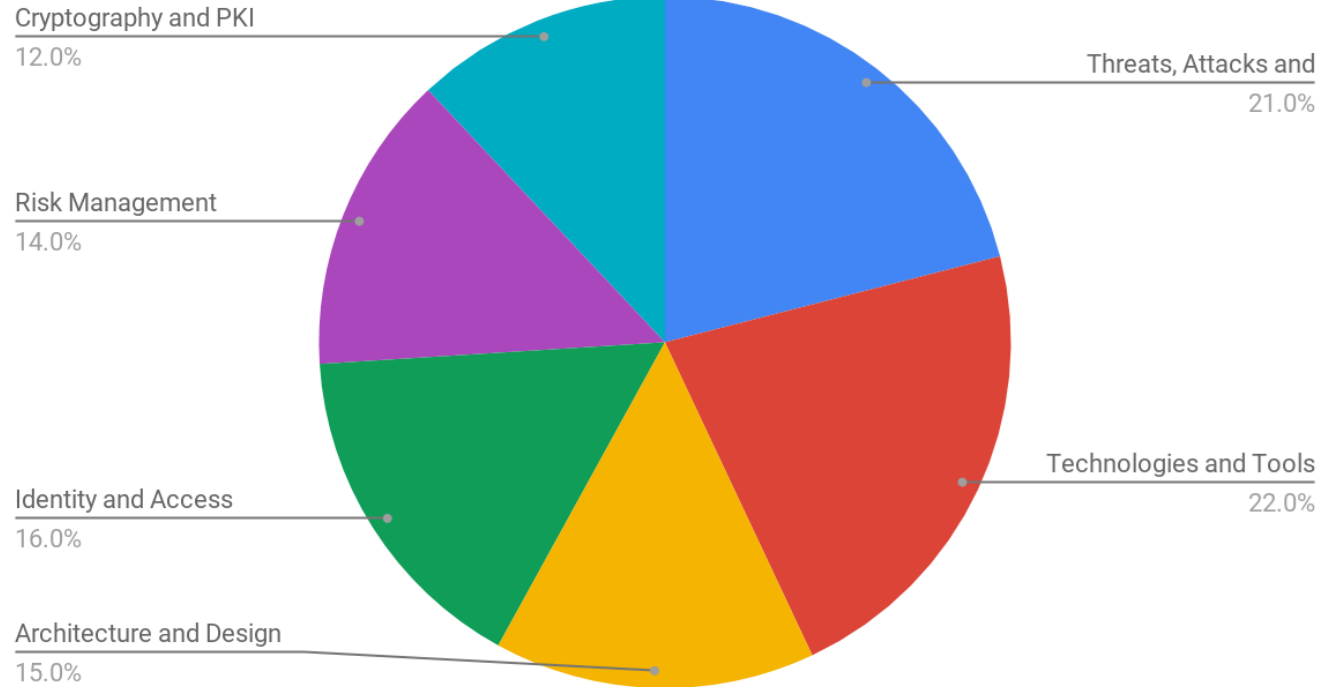


The exam is vendor-neutral.

# 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

Domain Distribution



# 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** that comprise of different topics and tools within the domain.

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

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



# Instructor Demonstration

CertMaster Tool

# 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 with the function its used for. Terms are **public key, private key, hash, digital signature**.
- You need to perform a Business Impact Analysis for a set of critical servers as part of a risk management push by your company. Organize the steps of a Business Impact Analysis (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**

# Domain Breakdown

# 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: Threats, Attacks and Vulnerabilities

---

## Subtopics:

-  Malware Types: Ransomware, Trojans, Adware - **Cyber 101, Incident Response**
-  Social Engineering: Phishing, Vishing - **Cyber 101, Incident Response, PenTesting**
-  Application Attacks: DDOS, Cross Site Scripting, DNS Poisoning - **Cyber 101, IR, Web Vulnerabilities**
-   Wireless Attacks: Bluejacking, Evil Twin - **Not Covered**
-   Cryptographic Attacks: Birthday Attack, Rainbow Tables - **Cryptography**
-   Threat Actors: Script Kiddies, Hacktivists - **Cyber 101, Incident Response, PenTesting**
-   Vulnerability Scanning: ID-ing Misconfigurations - **Operating Systems, PenTesting, Web Vulns**
-   Vulnerability Types: Improper Input Handling Improper Error Handling - **(Same as above)**



# 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.



# 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.



## 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



## 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





## 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



## 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: Sub-modules in CertMaster

---

Within this domain are five sub-modules:

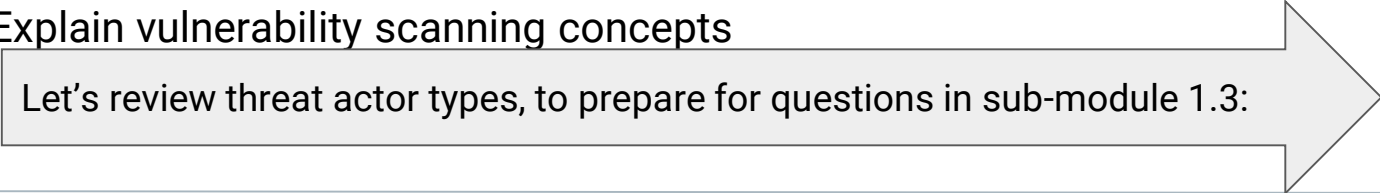
**1.1** Given a scenario, analyze indicators of compromise and determine the type of malware.

**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 deeper during our Governance, Risk and Compliance week.

# The Kill Chain

---

The kill chain highlights general stages of an attack on a system's security:

1. **Planning and scoping:** Attacker determines method and resources they need
2. **Reconnaissance and discovery:** Attacker learns about the target's organization and security system. Includes both passive information gathering and active scanning.
3. **Weaponization:** Attacker uses exploit to gain access.
  - a. **Exploit:** running code on a target system to gain elevated privilege
  - b. **Callback:** a secret channel is established to an external command and Control network
  - c. **Tool download:** Tools are installed to pivot and maintain access to the system.
4. **Post-exploitation** and lateral discovery: Once a pivot is established, attackers scan to learn more about network topography.
5. **Action on objectives:** Attacker performs data exfiltration to copy information. (Motivations for attack may vary)
6. **Retreat:** Attack either maintains APT or retreats from network and removing any trace of their presence.



## Your Turn: CertMaster Practice 1.3

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

Don't worry about finishing the whole module. Get acquainted with the types of adaptive questions that you encounter in the next 10 minute timeframe.

**Suggested Time:**  
10 minutes



# 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 so 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. Hactivist 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 so 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.

# Take a Break!

---



# Viruses and Worms

The Security + Exam covers common types of malware and malware attacks.  
We'll begin coverage by looking at viruses and worms.



# Viruses

---

A virus is a program that copies itself on to other 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 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.
- Shutting down the host by using up *all* of its resources or destroying essential files. This is called a *Denial of Service (DoS)* attack.
- "Scrambling" data on the host, so that users can't read it, and demanding money to "unscramble" it. Such viruses are called *ransomware*.



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

# Viruses on Different Operating Systems

---

Since a virus is just a program, it can infect any OS: Apple, Linux, Windows, etc.

- 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 the user 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.

**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 regular ways like on a disk, on a network, or as an attachment through an email or messaging system.

- **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. See scenario below:

Alex's computer is infected with a virus. In his address book, he has Michael's email address. The virus on Adam's computer can spoof Lindsey's email address and send an infected email to a third person, Jeremy.

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 can be 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 they will quickly consume network bandwidth as they replicate.
- They can also crash an operating system or server application, via a DoS attack.
- Like viruses, worms can have a payload that performs 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.
- A virus is known for having .bat file extension interaction.

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.

# 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.
- A victim's computer is referred to as a **zombie** when the attacker is able to send remote commands to the victim's computer. This can be used for many purposes, such as downloading additional malicious programs.
- **Botnets** are two or more zombie computers that are being 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 can be viewed as 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, such as:

- If programmer creates backdoors in software application for testing and development but then does not removed them when the application is deployed.
- Some software or hardware misconfigurations can give unauthorized users access.
  - **For example:** a router can be left configured with the default administrative password.

# Rootkits

---

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

# Rootkits

---

Some Trojans can often appear as a running service to avoid detection.

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

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

They are installing 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 which means 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 of vulnerabilities are zero-day vulnerabilities which occur when software or hardware that is released is not 100% secure. These are then the first vulnerabilities found within an application.

**Exploits** are the way attackers attack computer systems. They can be malware or scripts that disrupt the normal flow of the computer.

**Risks** can include known kept vulnerabilities.

- The reason why these vulnerabilities are kept, are because it would either cost the business too much to protect against or the business would not be able to operate without this risk.
- There are ways to reduce risks, but it is never possible to 100 percent fully remove all risks in an organization.
- Organizations have a formula to calculate risks which is  $\text{Risk} = \text{Likelihood} \times \text{Impact}$ .



## Your Turn: CertMaster Practice 1.1

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

Don't worry about finishing the whole module. Get acquainted with the types of adaptive questions that you encounter in the next 10 minute timeframe.

**Suggested Time:**



# 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. File-infecting or classic viruses
3. Metamorphic 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. File-infecting or classic viruses
3. Metamorphic 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 executables.
- 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 executables 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. Trojan horse
2. Botnet
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. Trojan horse
2. Botnet
3. Ransomware
4. Adware

- 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. Virus
3. Spyware
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. Virus
3. **Spyware**
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.

# Security + Domains Continued

# 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

## Domain Distribution

Cryptography and PKI

12.0%

Risk Management

14.0%

Identity and Access

16.0%

Architecture and Design

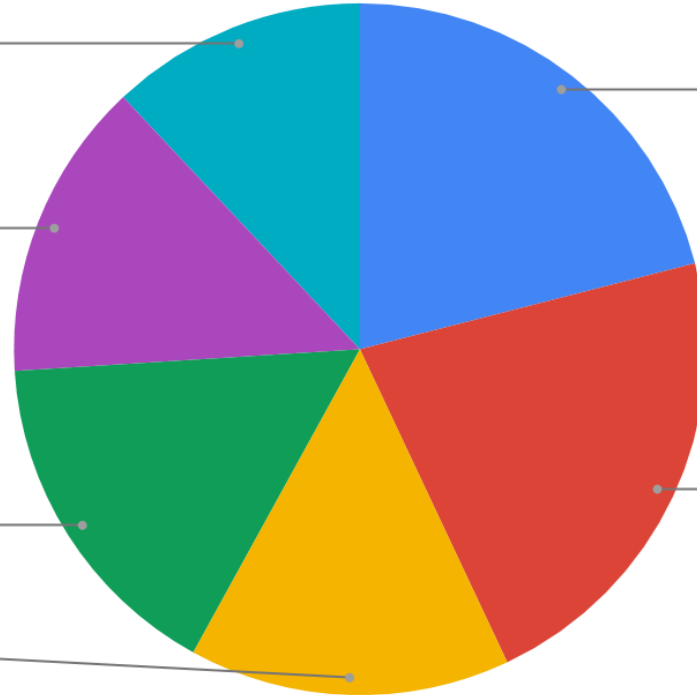
15.0%

Threats, Attacks and

21.0%

Technologies and Tools







22.0%



# Domain 2: Technologies and Tools

---

## Subtopics Included:







-  Network Devices: Routers, Switches, VPN
-  Security Devices: Firewalls, NIDS, SIEMS
-  Security Tools: Vulnerability and Network Scanners, Password Crackers
-  Command Line Tools: ping, tracert
-  Mobile Device Security: Jailbreaking, Sideloaded, BYOD
-  Secure Protocols: SSH, SFTP, SSL/TLS



# Domain 2: Technologies and Tools

---

## Subtopics Covered In-Class:

-  Network Devices: Routers, Switches, VPN - **Network Security, Networks 101**
-  Security Devices: Firewalls, NIDS, SIEMS - **Net Sec, Net 101, SIEMS, Incident Response**
-  Security Tools: Vuln and Network Scanners, Password Crackers - **Cryptography, PenTesting, Net Sec**
-  ☐ Command Line Tools: ping, tracert - **Command Line, PenTesting, Networks 101, Linux**
-  ☐ Mobile Device Security: Jailbreaking, Sideloaded, BYOD - **Not Covered**
-  ☐ Secure Protocols: SSH, SFTP, SSL/TLS - **Networking 101**





# Sample Question #1

---

To protect corporate data on devices that are decommissioned after end of life, which of the following tools should be used during the decommission process?

1. Data leakage prevention tools
2. Protocol analyzer
3. Data sanitization tools
4. Data Mining Tools



# Sample Question #1

---

To protect corporate data on devices that are decommissioned after end of life, which of the following tools should be used during the decommission process?

1. Data leakage prevention tools
2. Protocol analyzer
3. **Data sanitization tools**
4. Data Mining Tools



## Sample Question #2

---

A security analyst has been asked to determine if there are any weaknesses in a new hardware device that the operations engineering department needs to monitor on the manufacturing line.

To determine if there are any software, network, or security issues with this new device, which tool would you use?

1. Vulnerability scanner
2. Port scanner
3. Host scanner
4. Explicit scanner



## Sample Question #2

---

A security analyst has been asked to determine if there are any weaknesses in a new hardware device that the operations engineering department needs to monitor on the manufacturing line.

To determine if there are any software, network, or security issues with this new device, which tool would you use?

1. **Vulnerability scanner**
2. Port scanner
3. Host scanner
4. Explicit scanner



## Sample Question #2

---

For which purpose do most organizations implement data loss prevention (DLP) technologies?

1. To prevent employees from executing malicious code
2. To maintain backup copies of valuable data
3. To protect the corporate network when performing malware analysis
4. To prevent insiders from leaking sensitive data



## Sample Question #2

---

For which purpose do most organizations implement data loss prevention (DLP) technologies?






1. To prevent employees from executing malicious code
2. To maintain backup copies of valuable data
3. To protect the corporate network when performing malware analysis
4. **To prevent insiders from leaking sensitive data**



# Domain 3: Architecture and Design

---

## Subtopics Included:






-  Topologies: Extranet, Intranet, DMX, VLANs
-  Network Placement: Load Balancers, DDOS Mitigators
-  Operating Systems: Various OS's, Patch Management, Secure Configurations
-  Peripherals: Mice, Keyboards, Printers
-  Embedded Systems: SCADA, IOT



# Domain 3: Architecture and Design

---

## Subtopics Covered In-Class:

-  Topologies: Extranet, Intranet, DMX, VLANs - **Net Sec, Networks 101**
-  Network Placement: Load Balancers, DDOS Mitigators - **Net Sec, Net 101, IR**
-  Operating Systems: Various OS's, Patch Management - **PenTesting, OS, Linux**
-  Peripherals: Mice, Keyboards, Printers - **Not Covered**
-  Embedded Systems: SCADA, IOT - **Not Covered**





# Sample Question #1

---

A security manager has been tasked with finding a solution for remote users to be able to connect to the corporate network securely. The solution must also support at least 500 simultaneous users.

Which solution does the manager decide to implement on the network?

1. A perimeter router
2. A stateful firewall
3. A wireless access point
4. A virtual private network (VPN) concentrator



# Sample Question #1

---

A security manager has been tasked with finding a solution for remote users to be able to connect to the corporate network securely. The solution must also support at least 500 simultaneous users.

Which solution does the manager decide to implement on the network?

1. A perimeter router
2. A stateful firewall
3. A wireless access point
4. **A virtual private network (VPN) concentrator**



## Sample Question #2

---

The system administration team needs to implement a security solution for all computers on the network that ensures data security for the data stored on individual hard drives.

1. Password-protected folders
2. Software-based full disk encryption
3. Mandatory strong login passwords
4. Hardware-based full disk encryption



## Sample Question #2

---

The system administration team needs to implement a security solution for all computers on the network that ensures data security for the data stored on individual hard drives.

1. Password-protected folders
2. Software-based full disk encryption
3. Mandatory strong login passwords
4. **Hardware-based full disk encryption**



## Sample Question #3

---

Consider different types of locks for securing a data center server room. Which lock is the most secure?

1. Retina scanner
2. Combination lock
3. Electronic keycard
4. Padlock



## Sample Question #3

---

Consider different types of locks for securing a data center server room. Which lock is the most secure?

1. **Retina scanner**
2. Combination lock
3. Electronic keycard
4. Padlock



# Domain 4: Cryptography

---

## Subtopics Included:



Concepts: Symmetric / Asymmetric, Hashing, Steganography



Algorithm types: AES, DES, RC4, MD5, RSA



Cipher Modes: CBC, ECB



Protocols: WPA, EAP, TKIP








Certificates: CA, Intermediate CA, Self-Signed, Public / Private Keys



# Domain 4: Cryptography

---

## Subtopics Included:

-  Concepts: Symmetric / Asymmetric, Hashing, Steganography
-  Algorithm types: AES, DES, RC4, MD5, RSA
-  Cipher Modes: CBC, ECB
-  Protocols: WPA, EAP, TKIP
-  Certificates: CA, Intermediate CA, Self-Signed, Public / Private Keys



All topics were covered in our Cryptography Unit.





# Sample Question #1

---

Other than an obfuscation technique to protect the code, which method do programmers use to guarantee that their code has not been tampered with?

1. Limited data exposure
2. A digital signature
3. Encryption
4. Input validation



# Sample Question #1

---

Other than an obfuscation technique to protect the code, which method do programmers use to guarantee that their code has not been tampered with?

1. Limited data exposure
2. **A digital signature**
3. Encryption
4. Input validation



## Sample Question #2

---

Why was the Advanced Encryption Standard (AES) algorithm developed?

1. To offer an alternative to the Data Encryption Standard (DES)
2. To offer an alternative to Blowfish
3. To offer an alternative to the One Time Pad
4. To replace the Data Encryption Standard (DES)



## Sample Question #2

---

Why was the Advanced Encryption Standard (AES) algorithm developed?

1. To offer an alternative to the Data Encryption Standard (DES)
2. To offer an alternative to Blowfish
3. To offer an alternative to the One Time Pad
4. **To replace the Data Encryption Standard (DES)**



## Sample Question #3

---

A webmaster creates a certificate signing request (CSR) and needs to send it to a third-party service to receive the corresponding certificate. What is the third-party service generally known as?

1. The registration authority (RA)
2. The object identifier (OID)
3. The identity provider (IdP)
4. The certificate authority (CA)



## Sample Question #3

---

A webmaster creates a certificate signing request (CSR) and needs to send it to a third-party service to receive the corresponding certificate. What is the third-party service generally known as?





1. The registration authority (RA)
2. The object identifier (OID)
3. The identity provider (IdP)
4. **The certificate authority (CA)**



# Domain 5: Identity and Access Management

---

## Subtopics Included:

-  Concepts: SSO, MFA, Federated, Least Privilege
-  Access Control Models: MAC, Rule-Based, Role-Based
-  Biometric Factors
-  Tokens: Hard/ Soft



We'll focus on this topic in a later Sec + Review session and during our GRC week.



# Sample Question #1

---

You have been asked to provide single sign-on (SSO) capabilities for all your systems. What does this mean?

1. You provide each user with a single, unique sign-on for each system.
2. You can only sign on to a single system at one time and must sign out completely before you access a different system.
3. Signing on to any system gives you access to everything you need
4. Each system can only be signed on to once per day.





# Sample Question #1

---

You have been asked to provide single sign-on (SSO) capabilities for all your systems. What does this mean?

1. You provide each user with a single, unique sign-on for each system.
2. You can only sign on to a single system at one time and must sign out completely before you access a different system.
3. **Signing on to any system gives you access to everything you need**
4. Each system can only be signed on to once per day.



# Sample Question #2

---

Which of the following is NOT an example of a “something you are” access control mechanism?

1. Facial recognition
2. Proximity Cards
3. Fingerprint Scans
4. Voice recognition



# Sample Question #2

---

Which of the following is NOT an example of a “something you are” access control mechanism?

1. Facial recognition
2. **Proximity Cards**
3. Fingerprint Scans
4. Voice recognition



# Sample Question #3

---

Which resource is protected through the use of permissions such as read, write, and execute?

1. LAN
2. Server Room
3. Active Directory
4. File System



# Sample Question #3

---

Which resource is protected through the use of permissions such as read, write, and execute?










1. LAN
2. Server Room
3. Active Directory
4. **File System**



# Domain 6: Risk Management

---

## Subtopics Included:










-  Agreement Types: BPA, SLA, ISA
-  Personnel Management: Job Rotations, Separation of Duties, Awareness Training
-  Business Impact Analysis: MTTR, RPO, RTO, Single Point of Failure
-  Concepts and Processes: Threat Assessment, Risk Assessment, Change Management
-  Incident Response
-  Forensics: Chain of Custody, Data Acquisition
-  Disaster Recovery: Recovery Sites, Tabletop exercises
-  Data Destruction
-  Data Sensitivity Labelling: Confidential, PII, PHI



# Domain 6: Risk Management

---

**Every topic besides Agreement Types will be covered in the GRC unit.**

-  Agreement Types: BPA, SLA, ISA
-  Personnel Management: Job Rotations, Separation of Duties, Awareness Training
-  Business Impact Analysis: MTTR, RPO, RTO, Single Point of Failure
-  Concepts and Processes: Threat Assessment, Risk Assessment, Change Management
-  Incident Response
-  Forensics: Chain of Custody, Data Acquisition
-  Disaster Recovery: Recovery Sites, Tabletop exercises
-  Data Destruction
-  Data Sensitivity Labelling: Confidential, PII, PHI



# Sample Question #1

---

How do standard operating procedures (SOPs) reduce risk?

1. By combining technical and administrative controls into practical solutions.
2. By setting up automated procedures according to a standard.
3. By setting regulatory standards with which industries must comply.
4. By providing step-by-step instructions that detail how to implement components of a policy.





# Sample Question #1

---

How do standard operating procedures (SOPs) reduce risk?

1. By combining technical and administrative controls into practical solutions
2. By setting up automated procedures according to a standard
3. By setting regulatory standards with which industries must comply
4. **By providing step-by-step instructions that detail how to implement components of a policy**



## Sample Question #2

---

Failover is an important concept to include in which action plan?

1. Business continuity plan (BCP)
2. Incident response plan (IRP)
3. After-action report (AAR)
4. Disaster recovery plan (DRP)



# Sample Question #2

---

Failover is an important concept to include in which action plan?

1. **Business continuity plan (BCP)**
2. Incident response plan (IRP)
3. After-action report (AAR)
4. Disaster recovery plan (DRP)



## Sample Question #3

---

What is the purpose of taking screenshots while performing forensic procedures on a system?

1. The screenshots are hashes of the data shown on the screen.
2. There may be traces of evidence in the screenshots that need to be examined further.
3. These screenshots can be assembled into a video of the procedure.
4. It provides the court with proof of the use of valid computer forensic methods while extracting evidence.



# Sample Question #3

---

What is the purpose of taking screenshots while performing forensic procedures on a system?

1. The screenshots are hashes of the data shown on the screen.
2. There may be traces of evidence in the screenshots that need to be examined further.
3. These screenshots can be assembled into a video of the procedure.
4. **It provides the court with proof of the use of valid computer forensic methods while extracting evidence.**





Any Questions?