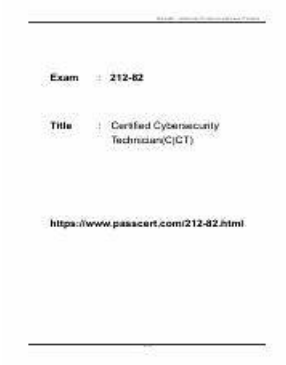
New 212-82 Dumps Free - Vce 212-82 Format


Exam : 212-82

Title : Certified Cybersecurity Technician(C|CT)

https://www.passcert.com/212-82.html

What's more, part of that TestPassed 212-82 dumps now are free: https://drive.google.com/open?id=1PGSCLUaf-oFVmfoXqslJSoAhgUdXvuL7

Are you worried about insufficient time to prepare the exam? Do you have a scientific learning plan? Maybe you have set a series of to-do list, but it's hard to put into practice for there are always unexpected changes during the 212-82 exam. Here we recommend our 212-82 test prep to you. With innovative science and technology, our study materials have grown into a powerful and favorable product that brings great benefits to all customers. Under the support of our 212-82 Study Materials, passing the 212-82 exam won't be an unreachable mission.

The CCT certification is an entry-level certification that is ideal for professionals who are starting their career in cybersecurity. 212-82 exam covers topics such as threat assessment, vulnerability assessment, risk management, and incident response. Certified Cybersecurity Technician certification also covers the basics of cybersecurity, such as firewalls, intrusion detection systems, and virtual private networks. Certified Cybersecurity Technician certification is recognized globally, and it is a valuable credential for IT professionals who are looking to advance their careers in cybersecurity. Certified Cybersecurity Technician certification is also a great way to demonstrate to employers that a candidate has the necessary skills to protect their organization's digital assets.

ECCouncil 212-82 Exam provides an opportunity for individuals to demonstrate their knowledge and skills in cybersecurity. Certified Cybersecurity Technician certification is recognized by employers around the world as a mark of excellence in cybersecurity. Certified Cybersecurity Technician certification provides individuals with a competitive advantage in the job market and opens up many career opportunities in the field of cybersecurity.

>> New 212-82 Dumps Free <<

Exam Questions for the ECCouncil 212-82 - Master Your Certification

Journey

Each ECCouncil certification exam candidate know this certification related to the major shift in their lives. ECCouncil Certification 212-82 Exam training materials TestPassed provided with ultra-low price and high quality immersive questions and answersdedication to the majority of candidates. Our products have a cost-effective, and provide one year free update. Our certification training materials are all readily available. Our website is a leading supplier of the answers to dump. We have the latest and most accurate certification exam training materials what you need.

The main objective of the ECCouncil 212-82 (Certified Cybersecurity Technician) certification exam is to train the candidates to secure, protect and defend their organizations' systems and networks against potential cyber-attacks. 212-82 exam covers a wide range of topics such as intrusion detection, vulnerability assessment, and remediation, network and application security, incident response, and data privacy. The candidates will learn how to use various cybersecurity tools such as firewalls, antivirus, and IDS/IPS systems to secure their organizations' systems from potential cyber threats.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q110-Q115):

NEW QUESTION # 110
Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.
Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

- A. Do not leave the device as it is if it is ON
- B. Turn the device ON if it is OFF
- C. Never record the screen display of the device
- D. Make sure that the device is charged

Answer: A,B,D

Explanation:
Turn the device ON if it is OFF, do not leave the device as it is if it is ON, and make sure that the device is charged are some of the points that Shawn must follow while preserving the digital evidence in the above scenario. Digital evidence is any information or data stored or transmitted in digital form that can be used in a legal proceeding or investigation. Digital evidence can be found on various devices, such as computers, mobile phones, tablets, etc. Preserving digital evidence is a crucial step in forensic investigation that involves protecting and maintaining the integrity and authenticity of digital evidence from any alteration or damage.
Some of the points that Shawn must follow while preserving digital evidence are:
* Turn the device ON if it is OFF: If the device is OFF, Shawn must turn it ON to prevent any data loss or encryption that may occur when the device is powered off. Shawn must also document any password or PIN required to unlock or access the device.
* Do not leave the device as it is if it is ON: If the device is ON, Shawn must not leave it as it is or use it
* for any purpose other than preserving digital evidence. Shawn must also disable any network connections or communication features on the device, such as Wi-Fi, Bluetooth, cellular data, etc., to prevent any remote access or deletion of data by unauthorized parties.
* Make sure that the device is charged: Shawn must ensure that the device has enough battery power to prevent any data loss or corruption that may occur due to sudden shutdown or low battery. Shawn must also use a write blocker or a Faraday bag to isolate the device from any external interference or signals.
Never record the screen display of the device is not a point that Shawn must follow while preserving digital evidence. On contrary, Shawn should record or photograph the screen display of the device to capture any relevant information or messages that may appear on the screen. Recording or photographing the screen display of the device can also help document any changes or actions performed on the device during preservation.

NEW QUESTION # 111
TechTonic, a leading software solution provider, is incorporating stringent cybersecurity measures for their Windows-based server farm. Recently, it noticed a series of unauthorized activities within its systems but could not trace back tot he origins. The company Intends to bolster Its monitoring capabilities by comprehensively analyzing Windows system logs. Which strategy should TechTonic prioritize to gain an insightful and effective analysis of its Windows logs, aiming to trace potential intrusions?

- A. Focus solely on logs from critical servers, assuming other logs are less consequential.
- B. Implement a centralized logging server and analyze logs using pattern-detection algorithms.
- C. Set up monitoring only for Windows Event Log IDs commonly associated with security breaches.

- D. Routinely back up logs every week and conduct a monthly manual review to detect anomalies.

Answer: B

NEW QUESTION # 112
An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.
Identify the VPN topology employed by Brandon in the above scenario.

- A. Hub-and-Spoke VPN topology
- B. Full-mesh VPN topology
- C. Star topology
- D. Point-to-Point VPN topology

Answer: A

Explanation:
A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied.
The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

NEW QUESTION # 113
Calvin spotted blazing flames originating from a physical file storage location in his organization because of a Short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large are a. Which of the following firefighting systems did Calvin use in this scenario?

- A. Sprinkler system
- B. Smoke detectors
- C. Fire detection system
- D. Fire extinguisher

Answer: D

Explanation:
Fire extinguisher is the firefighting system that Calvin used in this scenario. A firefighting system is a system that detects and suppresses fire in a physical location or environment. A firefighting system can consist of various components, such as sensors, alarms, sprinklers, extinguishers, etc. A firefighting system can use various agents or substances to suppress fire, such as water, foam, gas, powder, etc. A fire extinguisher is a portable device that contains an agent or substance that can be sprayed or discharged onto a fire to extinguish it . A fire extinguisher can be used to curb fire in the initial stage and prevent it from spreading over a large area . In the scenario, Calvin spotted blazing flames originating from a physical file storage location in his organization because of a short circuit. In response to the incident, he used a fire suppression system that helped curb the incident in the initial stage and prevented it from spreading over a large area. This means that he used a fire extinguisher for this purpose. A fire detection system is a system that detects the presence of fire by sensing its characteristics, such as smoke, heat, flame, etc., and alerts the occupants or authorities about it . A sprinkler system is a system that consists of pipes and sprinkler heads that release water onto a fire when activated by heat or smoke. A smoke detector is a device that senses smoke and emits an audible or visual signal to warn about fire.

NEW QUESTION # 114
Elliott, a security professional, was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network, Elliott monitored the firewall logs to detect evolving threats And attacks; this helped in ensuring firewall security and addressing network issues beforehand.
In which of the following phases of firewall implementation and deployment did Elliott monitor the firewall logs?

- A. Configuring
- B. Deploying
- C. Managing and maintaining
- D. Testing

Answer: C

Explanation:
Managing and maintaining is the phase of firewall implementation and deployment in which Elliott monitored the firewall logs in the above scenario. A firewall is a system or device that controls and filters the incoming and outgoing traffic between different networks or systems based on predefined rules or policies. A firewall can be used to protect a network or system from unauthorized access, use, disclosure, modification, or destruction.Firewall implementation and deployment is a process that involves planning, installing, configuring, testing, managing, and maintaining firewalls in a network or system.Managing and maintaining is the phase of firewall implementation and deployment that involves monitoring and reviewing the performance and effectiveness of firewalls over time.Managing and maintaining can include tasks such as updating firewall rules or policies, analyzing firewall logs , detecting evolving threats or attacks , ensuring firewall security , addressing network issues , etc. In the scenario, Elliott was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network, Elliott monitored the firewall logs to detect evolving threats and attacks; this helped in ensuring firewall security and addressing network issues beforehand.
This means that he performed managing and maintaining phase for this purpose. Deploying is the phase of firewall implementation and deployment that involves installing and activating firewalls in the network or system according to the plan. Testing is the phase of firewall implementation and deployment that involves verifying and validating the functionality and security of firewalls before putting them into operation. Configuring is the phase of firewall implementation and deployment that involves setting up and customizing firewalls according to the requirements and specifications.

NEW QUESTION # 115
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of TestPassed 212-82 dumps from Cloud Storage: https://drive.google.com/open?id=1PGSCLUaf-oFVmfoXqslJSoAhgUdXvuL7