Free Questions for 212-82 by certscare

Shared by Riley on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

Options:

A- white@hat

B- red@hat

C- hat@red

D- blue@hat

Answer:

C

Explanation:

hat@red is the FTP credential that was stolen using Cain and Abel in the above scenario. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. FTP requires a username and a password to authenticate the client and grant access to the server . Cain and Abel is a tool that can perform various network attacks, such as ARP poisoning, password cracking, sniffing, etc. Cain and Abel can poison the machine and fetch the FTP credentials used by the admin by intercepting and analyzing the network traffic . To validate the credentials that were stolen using Cain and Abel and read the file flag.txt, one has to follow these steps:

Navigate to the Documents folder of Attacker-1 machine.

Double-click on Cain.exe file to launch Cain and Abel tool.

Click on Sniffer tab.

Click on Start/Stop Sniffer icon.

Click on Configure icon.

Select the network adapter and click on OK button.

Click on + icon to add hosts to scan.

Select All hosts in my subnet option and click on OK button.

Wait for the hosts to appear in the list.

Right-click on 20.20.10.26 (FTP server) and select Resolve Host Name option.

Note down the host name as ftpserver.movieabc.com

Click on Passwords tab.

Click on + icon to add items to list.

Select Network Passwords option.

Select FTP option from Protocol drop-down list.

Click on OK button.

Wait for the FTP credentials to appear in the list.

Note down the username as hat and the password as red

Open a web browser and type ftp://hat:red@ftpserver.movieabc.com

Press Enter key to access the FTP server using the stolen credentials.

Navigate to flag.txt file and open it.

Read the file content.

Question 2

Question Type: MultipleChoice

RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.

Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

Options:

A- 2

B- 4

C- 3

D- 5

Answer:

C

Explanation:

3 is the number of files present in the folder in the above scenario. A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system or network. A RAT can be used to steal sensitive data, spy on user

activity, execute commands, install other malware, etc. To initiate a remote connection using thief client, one has to follow these steps:

Navigate to the thief folder located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

Double-click on thief.exe file to launch thief client.

Enter 20.20.10.26 as IP address of server.

Enter 1234 as port number.

Click on Connect button.

After establishing connection with server, click on Browse button.

Navigate to Desktop folder on server.

Count number of files present in folder.

The number of files present in folder is 3, which are:

Sensitive corporate docs.docx

Sensitive corporate docs.pdf

Sensitive corporate docs.txt

Question 3

Question Type: **MultipleChoice**

Cassius, a security professional, works for the risk management team in an organization. The team is responsible for performing various activities involved in the risk management process. In this process, Cassius was instructed to select and implement appropriate controls on the identified risks in order to address the risks based on their severity level.

Which of the following risk management phases was Cassius instructed to perform in the above scenario?

Options:

A- Risk analysis

B- Risk treatment

C- Risk prioritization

D- Risk identification

Answer:

B

Explanation:

Risk treatment is the risk management phase that Cassius was instructed to perform in the above scenario. Risk management is a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that can affect an organization's objectives, assets, or operations. Risk management phases can be summarized as follows: risk identification, risk analysis, risk prioritization, risk treatment, and risk monitoring . Risk identification is the risk management phase that involves identifying and documenting potential sources, causes, events, and impacts of risks. Risk analysis is the risk management phase that involves assessing and quantifying the likelihood and consequences of risks. Risk prioritization is the risk management phase that involves ranking risks based on their severity level and determining which risks need immediate attention or action. Risk treatment is the risk management phase that involves selecting and implementing appropriate controls or strategies to address risks based on their severity level . Risk treatment can include avoiding, transferring, reducing, or accepting risks. Risk monitoring is the risk management phase that involves tracking and reviewing the performance and effectiveness of risk controls or strategies over time.

Question 4

Question Type: MultipleChoice

Kasen, a cybersecurity specialist at an organization, was working with the business continuity and disaster recovery team. The team initiated various business continuity and discovery activities in the organization. In this process, Kasen established a program to restore both the disaster site and the damaged materials to the pre-disaster levels during an incident.

Which of the following business continuity and disaster recovery activities did Kasen perform in the above scenario?

Options:

A- Prevention

B- Resumption

C- Response

D- Recovery

Answer:

D

Explanation:

Recovery is the business continuity and disaster recovery activity that Kasen performed in the above scenario. Business continuity and disaster recovery (BCDR) is a process that involves planning, preparing, and implementing various activities to ensure the continuity of critical business functions and the recovery of essential resources in the event of a disaster or disruption. BCDR activities can be categorized into four phases: prevention, response, resumption, and recovery . Prevention is the BCDR phase that involves identifying and mitigating potential risks and threats that can cause a disaster or disruption. Response is the BCDR phase that involves activating the BCDR plan and executing the immediate actions to protect people, assets, and operations during a disaster or disruption. Resumption is the BCDR phase that involves restoring the minimum level of services and functions required to resume normal business operations after a disaster or disruption. Recovery is the BCDR phase that involves restoring both the disaster site and the damaged materials to the pre-disaster levels during an incident.

Question 5

Question Type: **MultipleChoice**

Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media.

Identify the method utilized by Ruben in the above scenario.

Options:

A- Sparse acquisition

B- Bit-stream imaging

C- Drive decryption

D- Logical acquisition

Answer:

B

Explanation:

Bit-stream imaging is the method utilized by Ruben in the above scenario. Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

Question 6

Question Type: **MultipleChoice**

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.)

Options:

A- Never record the screen display of the device

B- Turn the device ON if it is OFF

C- Do not leave the device as it is if it is ON

D- Make sure that the device is charged

Answer:

B, C, 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.

Question 7

Question Type: MultipleChoice

Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.

In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

Options:

A- Investigation process

B- Investigation objectives

C- Evidence information

D- Evaluation and analysis process

Answer:

B

Explanation:

Investigation objectives is the section of the forensic investigation report where Arabella recorded the "nature of the claim and information provided to the officers" in the above scenario. A forensic investigation report is a document that summarizes the findings and conclusions of a forensic investigation. A forensic investigation report typically follows a standard template that contains different sections covering all the details of the crime and the investigation process. Investigation objectives is the section of the forensic investigation report that describes the purpose and scope of the investigation, the nature of the claim and information provided to the officers, and the questions or issues to be addressed by the investigation. Investigation process is the section of the forensic investigation report that describes the steps and methods followed by the investigators, such as evidence collection, preservation, analysis, etc. Evidence information is the section of the forensic investigation report that lists and describes the evidence obtained from various sources, such as devices, media, witnesses, etc. Evaluation and analysis process is the section of the forensic investigation report that explains how the evidence was evaluated and analyzed using various tools and techniques, such as software, hardware, etc.

Question 8

Question Type: MultipleChoice

Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.

Which of the following rules of evidence was discussed in the above scenario?

Options:

A- Authentic

B- Understandable

C- Reliable

D- Admissible

Answer:

D

Explanation:

Admissible is the rule of evidence discussed in the above scenario. A rule of evidence is a criterion or principle that determines whether a piece of evidence can be used in a legal proceeding or investigation. Admissible is a rule of evidence that states that the evidence must be relevant, reliable, authentic, and understandable to be accepted by a court or a jury . Admissible also means that the evidence must be obtained legally and ethically, without violating any laws or rights. In the scenario, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury, which means that he has followed the admissible rule of evidence. Authentic is a rule of evidence that states that the evidence must be original or verifiable as genuine and not altered or tampered with. Understandable is a rule of evidence that states that the evidence must be clear and comprehensible to the court or jury and not ambiguous or confusing. Reliable is a rule of evidence that states that the evidence must be consistent and trustworthy and not based on hearsay or speculation.