212-82^{Q&As}

212-82$^{Q\&As}$

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/212-82.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Identify a machine in the network with 5SH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the tile\'s content as the answer. The credentials tor SSH login are sam/adm(admin@123.

A. sam@bob

B. bob2@sam

C. sam2@bob D. bobt@sam

Correct Answer: D

Explanation: bob1@sam is the file\'s content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command nmap -p 22 192.168.0.0/24 will scan the network range 192.168.0.0/24 for port 22 and display the results2. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command ssh sam@192.168.0.10 will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@1233. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine\'s file system. For example, the command find / -name flag.txt will search for the file flag.txt from the root directory (/) and display its location4. To enter the file\'s content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command cat /home/sam/flag.txt will display the content of the file flag.txt located in /home/sam/ directory5. The screenshot below shows an example of performing these steps: ![Screenshot of performing these steps] References: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]

QUESTION 2

An loT device placed in a hospital for safety measures has sent an alert to the server. The network traffic has been captured and stored in the Documents folder of the "Attacker Machine-1". Analyze the loTdeviceTraffic.pcapng file and identify the command the loT device sent over the network.

A. Tempe_Low

B. Low_Tem p e

C. High_Tcmpe

D. Temp_High

Correct Answer: D

Explanation: The loT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the loTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark4. The command Temp_High can be seen in the data field of the UDP packet sent from the loT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03. The screenshot below shows the packet details5: References: Wireshark User\'s Guide, [loTdeviceTraffic.pcapng]

QUESTION 3

A company decided to implement the cloud infrastructure within its corporate firewall 10 secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. Which of the following types of cloud deployment models did the company implement in this scenario?

A. Multi cloud

B. Public cloud

C. Private cloud

D. Community cloud

Correct Answer: C

Explanation: Private cloud is the type of cloud deployment model that the company implemented in this scenario. Cloud computing is a model that provides on-demand access to shared and scalable computing resources, such as servers, storage, networks, applications, etc., over the internet or a network. Cloud computing can have different types based on its service or deployment model. A cloud deployment model defines how and where the cloud infrastructure and services are hosted and accessed . A cloud deployment model can have different types, such as public cloud, private cloud, hybrid cloud, community cloud, etc. A private cloud is a type of cloud deployment model that provides exclusive access to cloud infrastructure and services to a single organization or entity . A private cloud can be hosted within or outside the organization\\\'s premises and managed by the organization or a third-party provider . A private cloud can be used to secure sensitive data from external access and maintain full control over the corporate data . In the scenario, the company decided to implement the cloud infrastructure within its corporate firewall to secure sensitive data from external access. The company invested heavily in creating a cloud architecture within its premises to manage full control over its corporate data. This means that the company implemented a private cloud for this purpose. A multi- cloud is not a type of cloud deployment model, but a term that describes a strategy that uses multiple public or private clouds from different providers for different purposes or functions . A public cloud is a type of cloud deployment model that provides open access to cloud infrastructure and services to multiple organizations or entities over the internet . A public cloud can be hosted and managed by a third-party provider that owns and operates the cloud infrastructure and services . A community cloud is a type of cloud deployment model that provides shared access to cloud infrastructure and services to multiple organizations or entities that have common interests or goals

QUESTION 4

Jordan, a network administrator in an organization, was instructed to identify network- related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

A. Time exceeded message

B. Destination unreachable message

C. Unreachable networks

D. Network cable is unplugged

Correct Answer: B

Explanation: Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems1.

References: Destination Unreachable Message

QUESTION 5

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.

A. 2

B. 4

C. 3

D. 5

Correct 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