CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.geekcert.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence. Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup

B. Creating a backdoor

C. Exploiting an arbitrary code execution exploit

D. Moving laterally to a more authoritative server/service

Correct Answer: B

QUESTION 2

A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online.

Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.

B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.

C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.

D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Correct Answer: C

QUESTION 3

A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.

Which of the following BEST describes the type of malware the solution should protect against?

A. Worm

B. Logic bomb

C. Fileless

D. Rootkit

Correct Answer: C

Reference: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

QUESTION 4

A security administrator is setting up a virtualization solution that needs to run services from a single host. Each service should be the only one running in its environment. Each environment needs to have its own operating system as a base but share the kernel version and properties of the running host. Which of the following technologies would best meet these requirements?

A. Containers

B. Type 1 hypervisor

C. Type 2 hypervisor

D. Virtual desktop infrastructure

E. Emulation

Correct Answer: A

Containers are the most suitable technology for the scenario described by the security administrator. They allow each service to run in its own isolated environment with its own filesystem and processes while sharing the host\\'s kernel. This meets the requirement of having separate OS environments for each service but leveraging the common properties and kernel version of the host system, ensuring efficient resource utilization and isolation between services.

QUESTION 5

A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices: Which of the following mobile configuration settings is the mobile administrator verifying?

```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
10,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

A. Service set identifier authentication

B. Wireless network auto joining

C. 802.1X with mutual authentication

D. Association MAC address randomization

Correct Answer: D

CAS-004 PDF Dumps CAS-004 Exam Questions CAS-004 Braindumps