CAS-003^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A company is concerned about disgruntled employees transferring its intellectual property data through covert channels. Which of the following tools would allow employees to write data into ICMP echo response packets?

A. Thor

B. Jack the Ripper

C. Burp Suite

D. Loki

Correct Answer: D

QUESTION 2

A company is not familiar with the risks associated with IPv6. The systems administrator wants to isolate IPv4 from IPv6 traffic between two different network segments. Which of the following should the company implement? (Select TWO)

A. Use an internal firewall to block UDP port 3544.

B. Disable network discovery protocol on all company routers.

C. Block IP protocol 41 using Layer 3 switches.

D. Disable the DHCPv6 service from all routers.

E. Drop traffic for ::/0 at the edge firewall.

F. Implement a 6in4 proxy server.

Correct Answer: DE

QUESTION 3

Given the code snippet below:

```
#include <stdio.h>                                           3 / 4
#include <stdlib.h>
int main(void) {
  char username[8];
  printf("Enter your username: ");
  gets(username)
  printf("\n";
if (username == NULL) {
  printf("you did not enter a username\n";
}
it strcmp(username, "admin") {
  printf("%s","Admin user, enter your physical token value: ");
// rest of conditional logic here has been snipped for brevity
} else [
printf ("Standard user, enter your password: ");
// rest of conditional logic here has been snipped for brevity
}
}
```

Which of the following vulnerability types in the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.

B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.

C. Hardcoded usernames with different code paths taken depend on which user is entered.

D. Format string vulnerability is present for admin users but not for standard users.

Correct Answer: B

QUESTION 4

A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks

B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches

C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use

D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions

E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication

F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Correct Answer: CD

QUESTION 5

Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
  Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
  IPv4 Address................ : 172.30.0.28
  Subnet Mask................. : 255.255.0.0
  Default Gateway............. : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

A. Allow 172.30.0.28:80 -> ANY

B. Allow 172.30.0.28:80 -> 172.30.0.0/16

C. Allow 172.30.0.28:80 -> 172.30.0.28:443

D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Correct Answer: B

CAS-003 PDF Dumps   CAS-003 VCE Dumps   CAS-003 Braindumps