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:

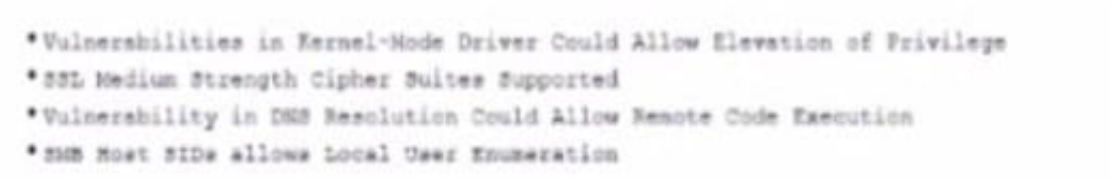
https://www.pass4itsure.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:



Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker

B. Port scanner

C. Account enumerator

D. Exploitation framework

Correct Answer: A

QUESTION 2

A MSSP has taken on a large client that has government compliance requirements. Due to the sensitive nature of communications to its aerospace partners, the MSSP must ensure that all communications to and from the client web portal are secured by industry-standard asymmetric encryption methods. Which of the following should the MSSP configure to BEST meet this objective?

A. ChaCha20

B. RSA

C. AES256

D. RIPEMD

Correct Answer: B

QUESTION 3

A company recently migrated all its workloads to the cloud and implemented a transit VPC with a managed firewall. The cloud infrastructure implements a 10.0.0.0/16 network, and the firewall implements the following ACLs:

```
FROM UNTRUST TO TRUST
10 PERMIT TCP FROM 0.0.0.0/0 ANY TO 10.0.0.0/16 80,443
20 PERMIT TCP FROM 192.168.1.0/24 ANY TO 10.0.10.0/24 22

FROM TRUST TO UNTRUST
10 PERMIT IP FROM 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY
```

The Chief Information Security Officer wants to monitor relevant traffic for signs of data exfiltration. Which of the following should the organization place in its monitoring tool to BEST detect data exfiltration while reducing log size and the time to search logs?

A. FROM UDP 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY

B. FROM TCP 10.0.0.0/16 80,443 TO 0.0.0.0/0 ANY

C. FROM TCP 0.0.0.0/0 ANY TO 10.0.0.0/16 80,443,22

D. FROM IP 10.0.0.0/16 ANY TO 0.0.0.0/0 ANY

E. FROM IP 0.0.0.0/0 ANY TO TCP 0.0.0.0/0 ANY

F. FROM UDP 0.0.0.0/0 ANY TO 0.0.0.0/0 ANY

Correct Answer: B

QUESTION 4

DRAG DROP

A vulnerability scan with the latest definitions was performed across Sites A and B.

INSTRUCTIONS

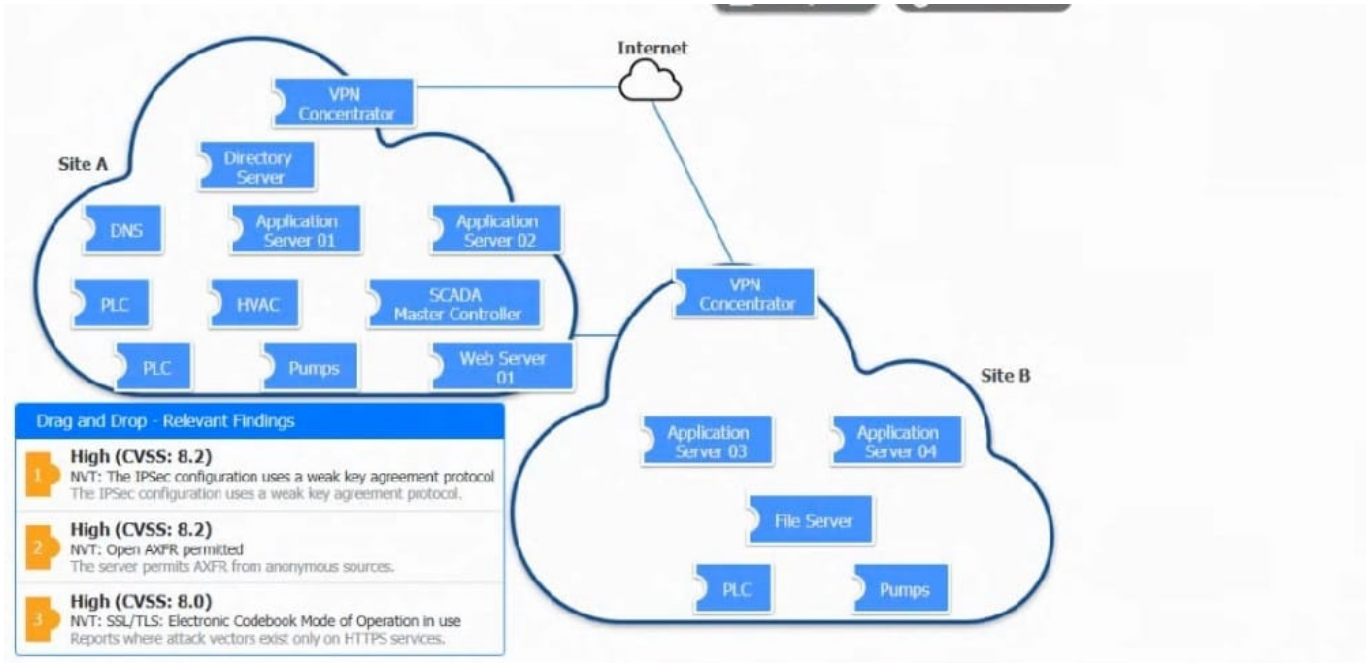
Match each relevant finding to the affected host.

After associating the finding with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

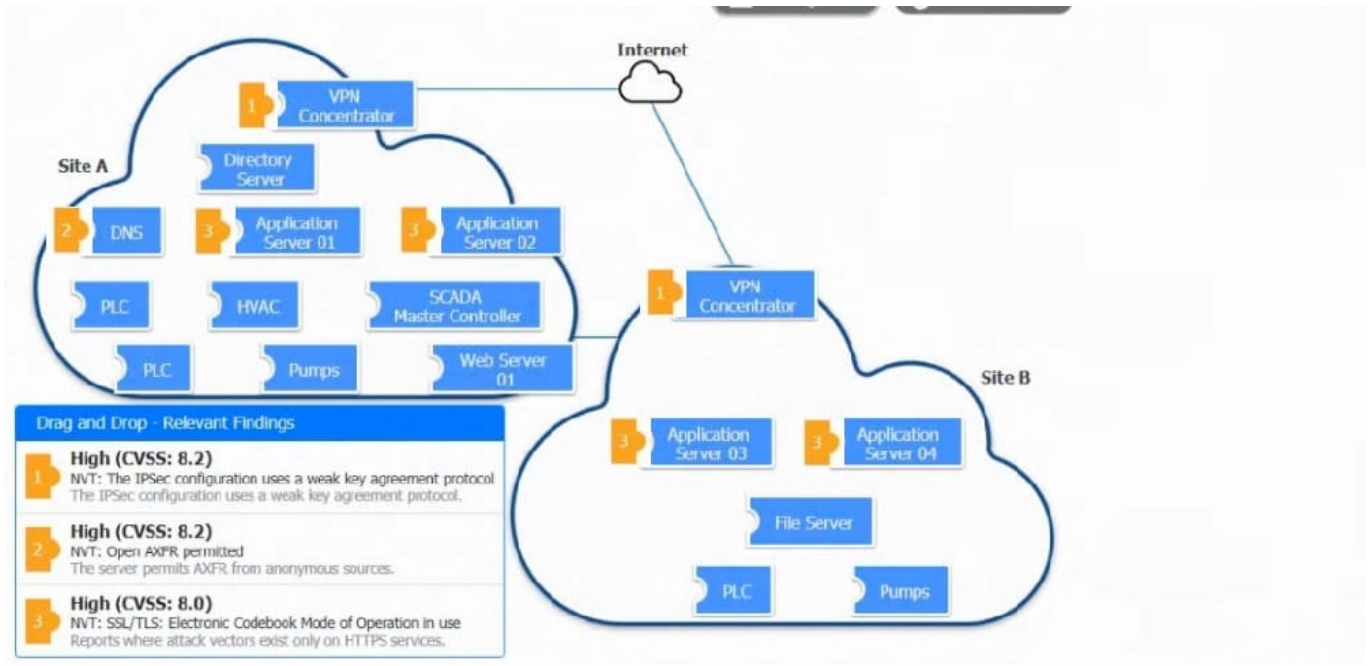
Each finding may be used more than once.

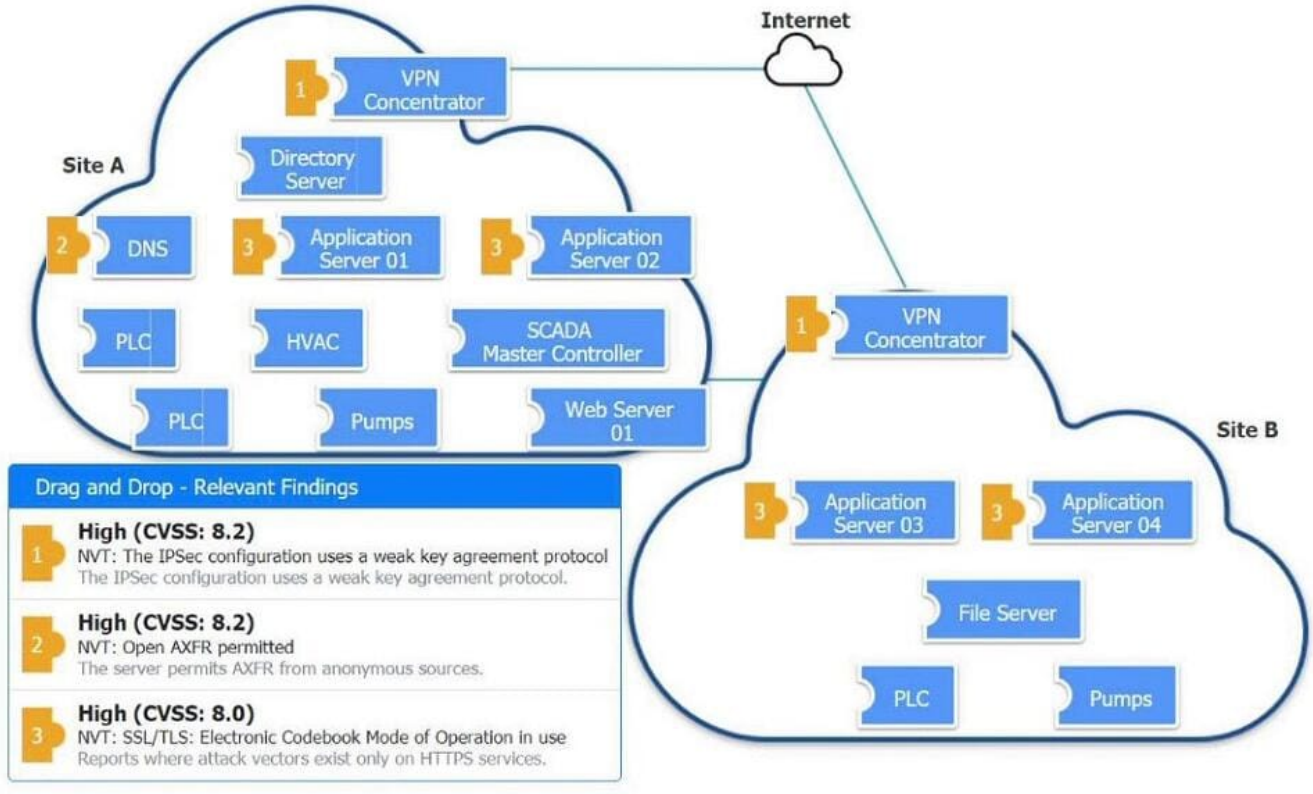
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Correct Answer:





QUESTION 5

A company recently acquired a SaaS provider and needs to integrate its platform into the company\\'s existing infrastructure without impact to the customer\\'s experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider\\'s systems shows multiple critical vulnerabilities attributed to very old and outdated Oss.

Which of the following solutions would prevent these vulnerabilities from being introduced into the company\\'s existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs

B. Migrate the services to new systems with a supported and patched OS.

C. Patch the systems to the latest versions of the existing OSs

D. Install anti-malware. HIPS, and host-based firewalls on each of the systems

Correct Answer: B