CS0-001 Q&As

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The development team recently moved a new application into production for the accounting department. After this occurred, the Chief Information Officer (CIO) was contacted by the head of accounting because the application is missing a key piece of functionality that is needed to complete the corporation\\'s quarterly tax returns. Which of the following types of testing would help prevent this from reoccurring?

A. Security regression testing

B. User acceptance testing

C. Input validation testing

D. Static code testing

Correct Answer: B

QUESTION 2

A security administrator uses FTK to take an image of a hard drive that is under investigation. Which of the following processes are used to ensure the image is the same as the original disk? (Choose two.)

A. Validate the folder and file directory listings on both.

B. Check the hash value between the image and the original.

C. Boot up the image and the original systems to compare.

D. Connect a write blocker to the imaging device.

E. Copy the data to a disk of the same size and manufacturer.

Correct Answer: BC

QUESTION 3

A security analyst\\'s daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst\\'s support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?

A. Updating the ACL

B. Conducting backups

C. Virus scanning

D. Additional log analysis

Correct Answer: C

QUESTION 4

As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select two.)

A. Timing of the scan

B. Contents of the executive summary report

C. Excluded hosts

D. Maintenance windows

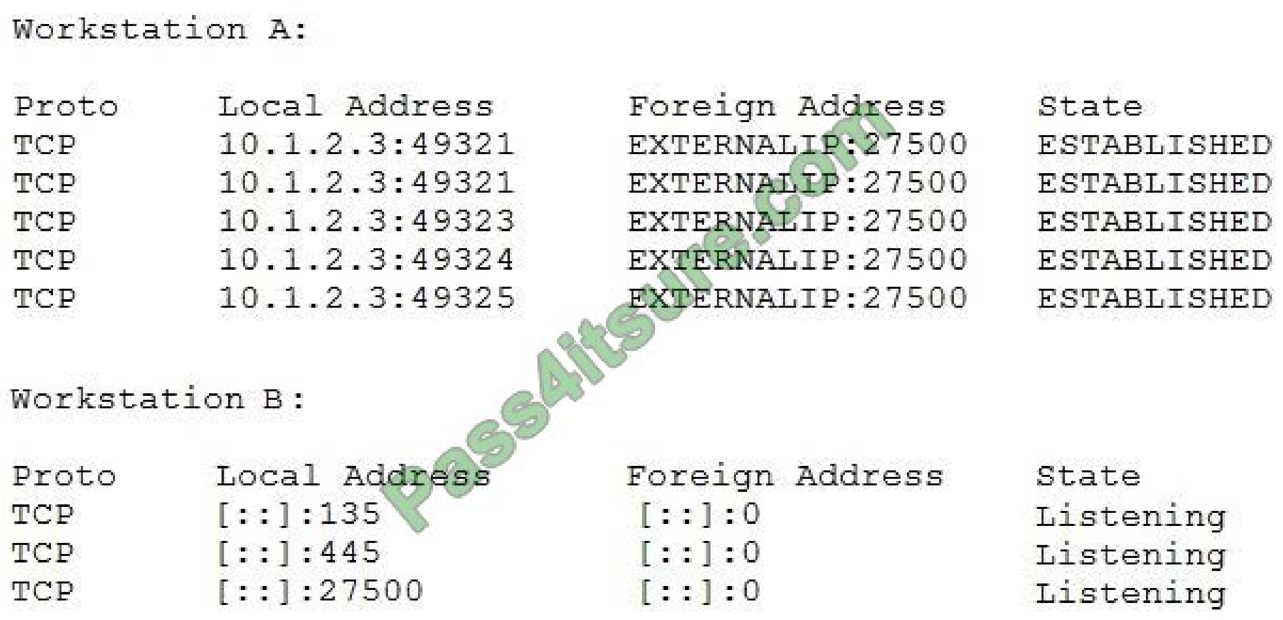
E. IPS configuration

F. Incident response policies

Correct Answer: AC

QUESTION 5

A newly discovered malware has a known behavior of connecting outbound to an external destination on port 27500 for the purposes of exfiltrating data. The following are four snippets taken from running netstat ?n on separate Windows workstations:

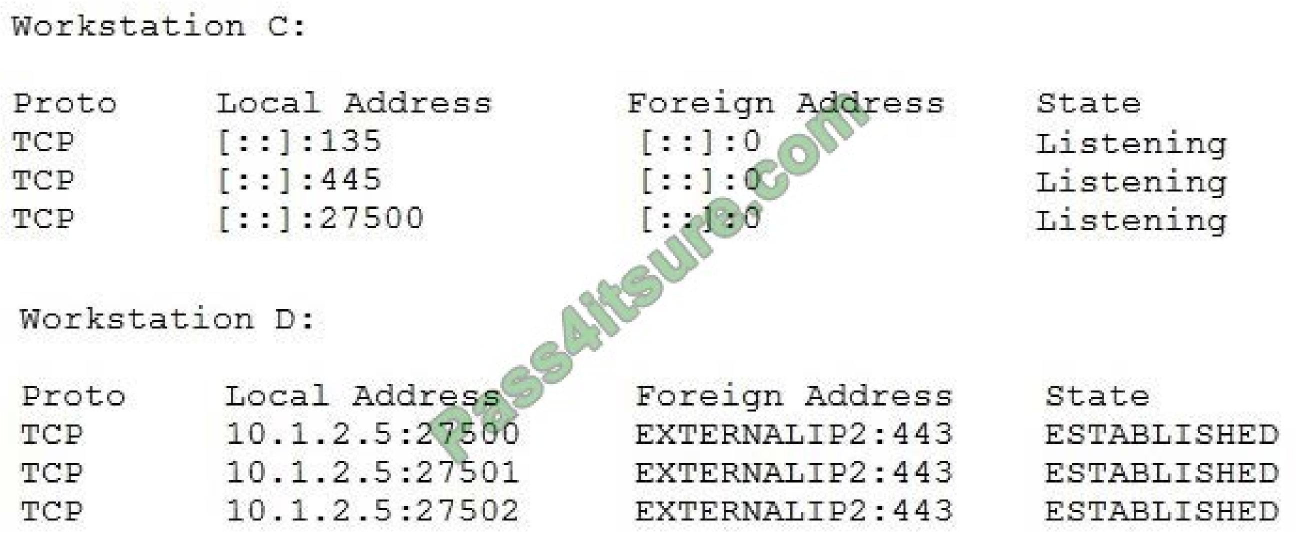


```
Workstation A:

Proto     Local Address         Foreign Address       State
TCP       10.1.2.3:49321        EXTERNALIP:27500      ESTABLISHED
TCP       10.1.2.3:49321        EXTERNALIP:27500      ESTABLISHED
TCP       10.1.2.3:49323        EXTERNALIP:27500      ESTABLISHED
TCP       10.1.2.3:49324        EXTERNALIP:27500      ESTABLISHED
TCP       10.1.2.3:49325        EXTERNALIP:27500      ESTABLISHED

Workstation B:

Proto     Local Address         Foreign Address       State
TCP       [::]:135               [::]:0               Listening
TCP       [::]:445               [::]:0               Listening
TCP       [::]:27500             [::]:0               Listening
```



```
Workstation C:

Proto     Local Address        Foreign Address     State
TCP       [::]:135             [::]:0              Listening
TCP       [::]:445             [::]:0              Listening
TCP       [::]:27500           [::]:0              Listening

Workstation D:

Proto     Local Address        Foreign Address     State
TCP       10.1.2.5:27500       EXTERNALIP2:443     ESTABLISHED
TCP       10.1.2.5:27501       EXTERNALIP2:443     ESTABLISHED
TCP       10.1.2.5:27502       EXTERNALIP2:443     ESTABLISHED
```

Based on the above information, which of the following is MOST likely to be exposed to this malware?

A. Workstation A

B. Workstation B

C. Workstation C

D. Workstation D

Correct Answer: A

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

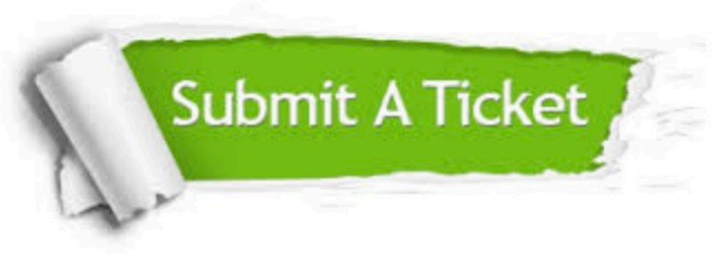
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4itsure.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.