1T6-540

Advanced Troubleshooting with InfiniStream Network Mgmt

Q&A

DEMO Version

Important Note
Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the http://www.chinatag.com website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

Question No: 1 Applications that use ephemeral ports on both sides of a connection are difficult to mine, because:

A. The ephemeral ports cannot be predicted
B. They all use the same port, TCP/1024
C. The well-known ports cannot be predicted
D. The ephemeral ports can be predicted but the port pairings are always different

Answer: A

Question No: 2 Mining FTP frames for both the Control and Data connections is difficult, because:

A. The server listens on TCP/20 and on ephemeral addresses that are difficult to predict.
B. The server listens on TCP/21 and multiple addresses that cannot be predicted.
C. The server listens on TCP/21 and ephemeral ports that are difficult to predict.
D. Many implementations of FTP exist that use varying well-known ports.

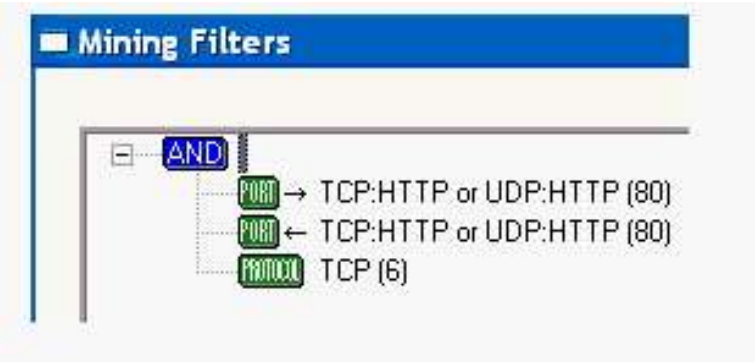
Answer: C

Question No: 3 Which of the following is NOT typically associated with network security auditing?

A. Inspection of passwords
B. Examining a network for signs of misuse
C. Troubleshooting network application efficiency
D. Looking for conformance to policy

Answer: C

Question No: 4 Consider this illustration of a data mining filter. What is wrong with it?



A. The filter only allows packets that are sent to HTTP servers on their well-known port. It would only show commands without replies. This filter is incomplete.
B. The filter only allows packets that are both to and from the well-known port TCP/80 (HTTP). Both source and destination port cannot be 80. Nothing would pass the filter.
C. It would also allow UDP packets to and from port 80 (HTTP), which does not make sense, since HTTP is a TCP-based protocol.
D. Nothing. It will capture normal data to and from TCP/80 (HTTP) servers.

Answer: B

Question No: 5 The easiest way to identify data for further analysis is to _____.

A. create an alias
B. group multiple protocols together
C. sort on port number
D. select all ephemeral ports

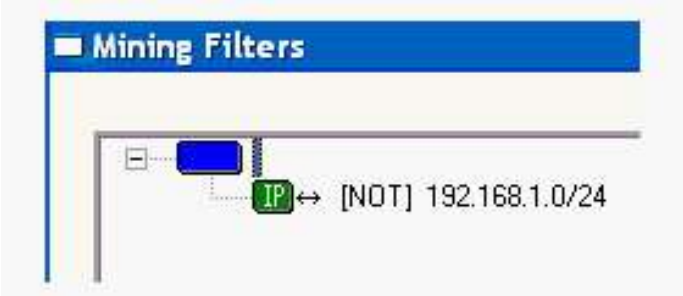
Answer: C

Question No: 6 A one to many relationship is indicative of:

A. Backdoors
B. Clients sending email to a relay server
C. Password guessing
D. Peer-to-Peer

Answer: D

Question No: 7 Consider this mining filter. Which description most accurately describes what it does?



A. It includes all packets to and from network 192.168.1.0/24.
B. It includes all packets that have sources and destinations within network 192.168.1.0/24.
C. It includes all packets that are not to or from network 192.168.1.0/24.
D. Nothing. No packets would pass this filter.

Answer: C

Question No: 8 Time duration and speed are _____.

A. primary limitations of mining and analysis
B. not relevant to InfiniStream
C. only related to Expert analysis
D. relevant, but secondary issues

Answer: A

Question No: 9 For testing, it is useful to convert your _____ into _____.

A. data / units of measurement
B. hypothesis / an if-then statement
C. hypothesis / a conclusion
D. conclusion / if-then statement

Answer: B

Question No: 10 Maintaining a baseline can aid in detecting bandwidth denial of service attacks by:

A. Listing status codes associated with denial of service.
B. Revealing significant changes in protocol activity and bandwidth through comparison.
C. Showing ports known to be associated with bandwidth denial of service.
D. Listing source IP addresses know to send denial of service attacks.

Answer: B