Exam Code: 1T6-540

Exam Name: Advanced Troubleshooting with InfiniStream Network Mgmt

Vendor: Network General Corp

Version: DEMO

Part: A

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

Correct Answers: A

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.

Correct Answers: C

3: Which of the following is NOT typically associated with network security auditing?

A.Inspection of passwords

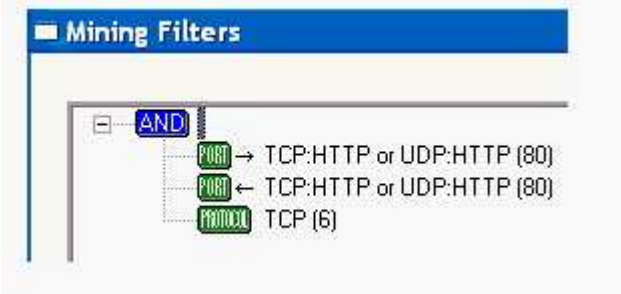
B.Examining a network for signs of misuse

C.Troubleshooting network application efficiency

D.Looking for conformance to policy

Correct Answers: C

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.

Correct Answers: B

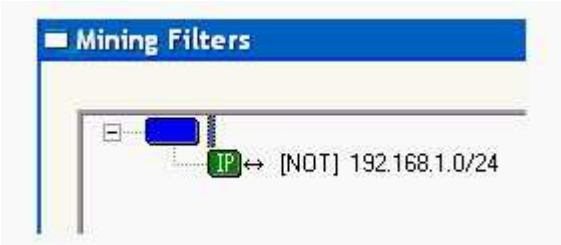
5: The easiest way to identify data for further analysis is to _____.

A.create an alias

B.group multiple protocols together
C.sort on port number
D.select all ephemeral ports
Correct Answers: C

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
Correct Answers: D

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.
Correct Answers: C

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
Correct Answers: A

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
Correct Answers: B

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.

Correct Answers: B

11: To see user names sent to an FTP server, you should view _____.
A.the Expert Service layer objects
B.the Expert Application layer objects
C.the Advanced tab in the mining interface (Quick Select)
D.the Names tab in the mining interface (Quick Select)
Correct Answers: B

12: Most Remote Procedure Calls (RPCs) listen on _____ ports?
A.all well-known ports
B.any port below 512
C.dynamically assigned ports, usually below port 1024
D.dynamically assigned ports, usually above port 1023
Correct Answers: D

13: In order to mine DHCP client addressing problems, it would be best to mine _____.
A.RDP and its associated port
B.Bootpc and Bootps (DHCP) and the last known address of the client
C.the last known address of the client
D.the port on the server that the client was attempting to reach
Correct Answers: B

14: Consider this mining filter. Which description most accurately describes what it does?

A.It includes packets in either direction only between network 192.168.1.0/24 and network 10.2.1.0/24.
B.It includes packets sent from network 192.168.1.0/24 to network 10.2.1.0/24.
C.It includes packets in either direction between network 192.168.1.0/24 and other all other networks, except 10.2.1.0/24.
D.Nothing. No packets would pass this filter.
Correct Answers: A

15: Reviewing initial data and noting significant trends is part of a process used to _____.
A.testing a hypothesis
B.isolate an application for conversion
C.profile network usage
D.all of the above

Correct Answers: C

16: If you have captured network traffic and misuse of a network is uncovered, it is usually best to:
A.Confront the individual and record your conversation.
B.Hand the information over to a network security officer or manager.
C.Take the initiative and perform your own investigation.
D.Not inform anyone.
Correct Answers: B

17: Remote Procedure Calls may change their listening port number when the service is disabled and restarted.
A.TRUE
B.FALSE
Correct Answers: A

18: Which of the following uses Remote Procedure Calls?
A.Grep
B.Linux and Unix
C.Windows
D.VLANs
E.DNS
Correct Answers: B C

19: A list of up to 10 of the last file names accessed on an FTP server may be viewed _____.
A.in the data mining interface (Quick Select) on Files tab
B.in the data mining interface (Quick Select) by creating a custom tab and adding a Files column
C.in the analysis interface in an Expert Application layer object
D.in the analysis interface in an Expert Service layer object
Correct Answers: D

20: While troubleshooting firewall issues, it is useful to compare:
A.Stream data on the inside, since anything blocked will be on the inside.
B.Stream data on the outside, since anything blocked will be on the outside.
C.Stream data on the inside and outside of the firewall to see what is getting through.
D.None of the above.
Correct Answers: C