Question 1

In what order are filters evaluated as data flows through the Decoder?

Options:

A- Feeds. Network Rules. LUA Parsers. Application Rules. BPF

B- Feeds. Network Rules. BPF. Application Rules, LUA Parsers

C- Network Rules. Feeds. Application Rules. BPF, LUA Parsers

D- BPF. Network Rules. LUA Parsers. Feeds. Application Rules

Answer:

D

Question 2

Which device index file should you use to create new meta keys?

Options:

A- index-user, xml

B- index-default xml

C- index-<device> xml

D- index-<device>-custom xml

Answer:

D

Question 3

Question Type: MultipleChoice

Logging in to NetWitness via RAM requires which of the following to succeed'?

Options:

A- PAM User Authentication

B- NSS Group Authentication

C- PAM User Authentication and Group Mapping

D- Kerberos Authentication

Answer:

A

Question 4

Question Type: MultipleChoice

What is the definition of an RSA NetWitness ad hoc feed?

Options:

A- A feed that is deployed one time on one or more Decoders

B- A feed that is deployed once on three or more Decoders

C- A feed that is deployed on no more than three Decoders once

D- A feed that is deployed on one or more Decoders at least three times

Answer:

A

Question 5

Question Type: **MultipleChoice**

What are the two types of device index files available in RSA NetWitness?

Options:

A- index xml and index.orig.xml

B- index-rsa.txt and index-custom txt

C- index-rsa.xml and index-custom xml

D- index-<device> xml and index-<device>-custom xml

Answer:

D

Question 6

Question Type: MultipleChoice

To run a report you need to create which of the following?

Options:

A- View

B- Alert

C- Report rule

D- Schedule

Answer:

C

Question 7

When adding a data source to the ESA device. RSA recommends using only the

Options:

A- Concentrator

B- Decoder

C- Log Collector

D- Archiver

Answer:

A

Question 8

Which of the following statements about Health and Wellness Policies is false?

Options:

A- Policies can be defined by NW administrators

B- Out-of-the-box policies are enabled by default

C- Out-of-the-box policies can be edited by NW administrators

D- Out-of-the-box policies are provided for most NW services

Answer:

C

Question 9

Question Type: MultipleChoice

The RSA NetWitness Reporting Engine provides visibility into captured data via which of the following mechanisms?

Options:

A- static and/or dynamic analysis

B- alerts, reports and charts

C- community and/or sandbox analysis

D- ad hoc, schedules, and/or auto-run features

Answer:

C