Free Questions for 500-285 by go4braindumps

Shared by Cash on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What does packet latency thresholding measure?

Options:

A- the total elapsed time it takes to process a packet

B- the amount of time it takes for a rule to process

C- the amount of time it takes to process an event

D- the time span between a triggered event and when the packet is dropped

Answer:

A

Question 2

Question Type: MultipleChoice

Which feature of the preprocessor configuration pages lets you quickly jump to a list of the rules associated with the preprocessor that you are configuring?

Options:

A- the rule group accordion

B- a filter bar

C- a link below the preprocessor heading

D- a button next to each preprocessor option that has a corresponding rule

Answer:

C

Question 3

Question Type: **MultipleChoice**

A one-to-many type of scan, in which an attacker uses a single host to scan a single port on multiple target hosts, indicates which port scan type?

Options:

A- port scan

B- portsweep

C- decoy port scan

D- ACK scan

Answer:

B

Question 4

Question Type: **MultipleChoice**

Which statement represents detection capabilities of the HTTP preprocessor?

Options:

A- You can configure it to blacklist known bad web servers.

B- You can configure it to normalize cookies in HTTP headers.

C- You can configure it to normalize image content types.

D- You can configure it to whitelist specific servers.

Answer:

B

Question 5

Question Type: MultipleChoice

Controlling simultaneous connections is a feature of which type of preprocessor?

Options:

A- rate-based attack prevention

B- detection enhancement

C- TCP and network layer preprocessors

D- performance settings

Answer:

A

Question 6

Question Type: MultipleChoice

What does the whitelist attribute value "not evaluated" indicate?

Options:

A- The host is not a target of the whitelist.

B- The host could not be evaluated because no profile exists for it.

C- The whitelist status could not be updated because the correlation policy it belongs to is not enabled.

D- The host is not on a monitored network segment.

Answer:

A

Question 7

Question Type: MultipleChoice

Which option is a remediation module that comes with the Sourcefire System?

Options:

A- Cisco IOS Null Route

B- Syslog Route

C- Nmap Route Scan

D- Response Group

Answer:

A

Question 8

Question Type: MultipleChoice

Correlation policy rules allow you to construct criteria for alerting on very specific conditions. Which option is an example of such a rule?

Options:

A- testing password strength when accessing an application

B- limiting general user access to administrative file shares

C- enforcing two-factor authentication for access to critical servers

D- issuing an alert if a noncompliant operating system is detected or if a host operating system changes to a noncompliant operating system when it was previously profiled as a compliant one

Answer:

D

Question 9

Question Type: **MultipleChoice**

Which statement is true concerning static NAT?

Options:

A- Static NAT supports only TCP traffic.

B- Static NAT is normally deployed for outbound traffic only.

C- Static NAT provides a one-to-one mapping between IP addresses.

D- Static NAT provides a many-to-one mapping between IP addresses.

Answer:

C

Question 10

Question Type: MultipleChoice

Which interface type allows for VLAN tagging?

Options:

A- inline

B- switched

C- high-availability link D. passive

Answer:

B

Question 11

Question Type: MultipleChoice

Which Sourcefire feature allows you to send traffic directly through the device without inspecting it?

Options:

A- fast-path rules

B- thresholds or suppressions

C- blacklist

D- automatic application bypass

Answer:

A