Vendor: Palo Alto Networks

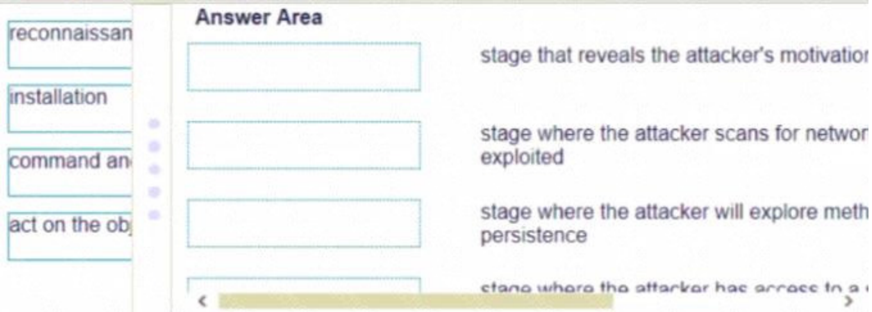
Exam Code: PCNSA

Exam Name: Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)

Version: 13.01

Q & As: 218

QUESTION 1
DRAG DROP
Match the cyber-attack lifecycle stage to its correct description.



reconnaissan
installation
command an
act on the obj

Answer Area

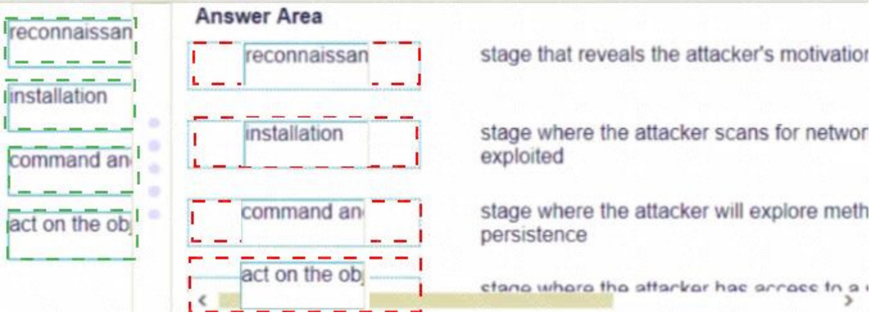
stage that reveals the attacker's motivatior

stage where the attacker scans for networ exploited

stage where the attacker will explore meth persistence

stage where the attacker has access to a

Correct Answer:



reconnaissan
installation
command an
act on the obj

Answer Area

reconnaissan	stage that reveals the attacker's motivatior
installation	stage where the attacker scans for networ exploited
command an	stage where the attacker will explore meth persistence
act on the obj	stage where the attacker has access to a

QUESTION 2
Which the app-ID application will you need to allow in your security policy to use facebook-chat?

A. facebook-email
B. facebook-base
C. facebook
D. facebook-chat

Correct Answer: BD

QUESTION 3
Which type of address object is "10 5 1 1/0 127 248 2"?

A. IP subnet
B. IP wildcard mask
C. IP netmask
D. IP range

Correct Answer: B

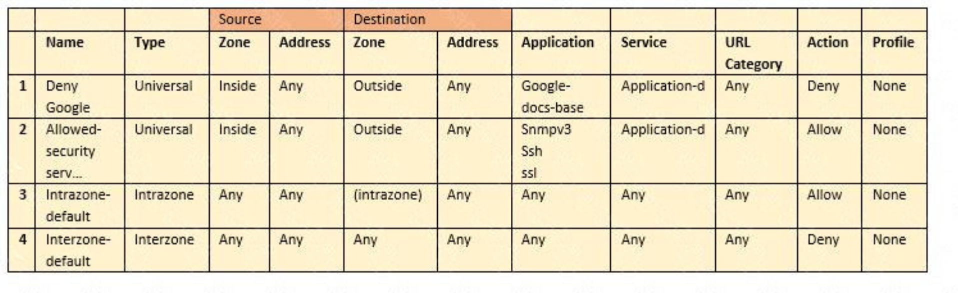
QUESTION 4
You must configure which firewall feature to enable a data-plane interface to submit DNS queries

on behalf of the control plane?

A. Admin Role profile
B. virtual router
C. DNS proxy
D. service route

Correct Answer: A

QUESTION 5
Based on the security policy rules shown, ssh will be allowed on which port?



			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. any port
B. same port as ssl and snmpv3
C. the default port
D. only ephemeral ports

Correct Answer: C

QUESTION 6
An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

A. Security policy rule
B. ACC global filter
C. external dynamic list
D. NAT address pool

Correct Answer: A
Explanation:
You can use an address object of type IP Wildcard Mask only in a Security policy rule.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses

IP Wildcard Mask
Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1.

Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

QUESTION 7
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

A. override
B. authorization
C. authentication
D. continue

Correct Answer: A

QUESTION 8
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

A. Add zones attached to interfaces to the virtual router
B. Add interfaces to the virtual router
C. Enable the redistribution profile to redistribute connected routes
D. Add a static routes to route between the two interfaces

Correct Answer: D

QUESTION 9
URL categories can be used as match criteria on which two policy types? (Choose two.)

A. authentication
B. decryption
C. application override
D. NAT

Correct Answer: AB

QUESTION 10
An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

A. Reset-server
B. Block
C. Deny
D. Drop

Correct Answer: D

QUESTION 11
An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

A. vulnerability protection profile applied to outbound security policies