Free Questions for 350-701 by certscare

Shared by Taylor on 07-06-2022

For More Free Questions and Preparation Resources

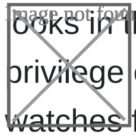
Check the Links on Last Page

Question 1

Question Type: DragDrop

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

Image not found or type unknown
Image not found or type unknown



Explanation: Cisco Tetration platform studies the behavior of the various processes and applications in the workload, measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its basic building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and watches for them. The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

Cisco Tetration platform studies the behavior of the various processes and applications in the workload,

measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By

studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its basic building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and watches for them.

The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:

+ Shell code execution: Looks for the patterns used by shell code.

+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.

+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).

+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.

+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.

+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.

+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the

Tetration Analytics platform.

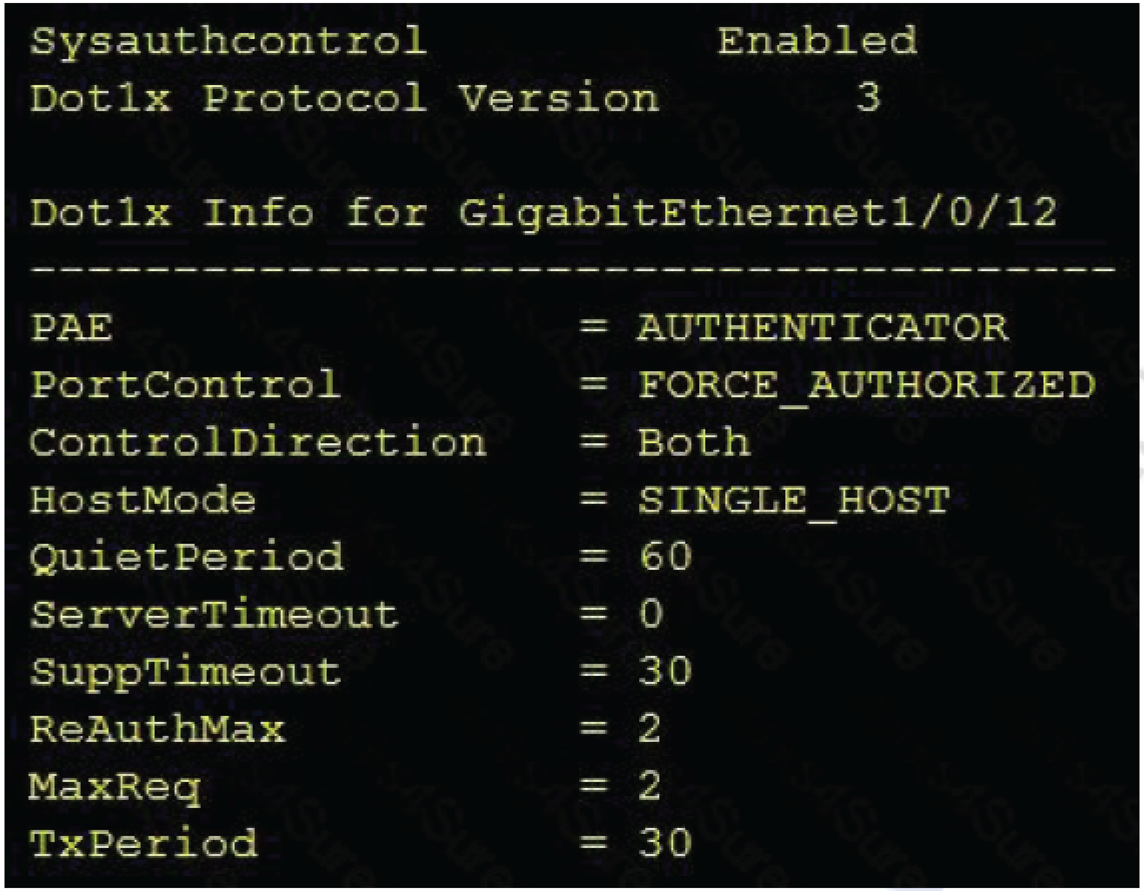
Explanation: Cisco Tetration platform studies the behavior of the various processes and applications in the workload, measuring them against known bad behavior sequences. It also factors in the process hashes it collects. By studying various sets of malwares, the Tetration Analytics engineering team deconstructed it back into its basic building blocks. Therefore, the platform understands clear and crisp definitions of these building blocks and watches for them. The various suspicious patterns for which the Cisco Tetration platform looks in the current release are: + Shell code execution: Looks for the patterns used by shell code. + Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree. + Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts. Using these, it can detect Meltdown, Spectre, and other cache-timing attacks. + Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping). + User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods. + Interesting file access: Cisco Tetration platform can be armed to look at sensitive files. + File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user. + Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform. Reference: https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-740380.html

Answer:

Question 2

Question Type: **MultipleChoice**

Refer to the Exhibit:



```
Sysauthcontrol                Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet1/0/12
--------------------------------------
PAE                      = AUTHENTICATOR
PortControl              = FORCE_AUTHORIZED
ControlDirection         = Both
HostMode                 = SINGLE_HOST
QuietPeriod              = 60
ServerTimeout            = 0
SuppTimeout              = 30
ReAuthMax                = 2
MaxReq                   = 2
TxPeriod                 = 30
```

Which command was used to display this output?

Options:

A) show dotlx all

B) show dotlx

C) show dotlx all summary

D) show dotlx interface gil/0/12

Answer:

A

Question 3

Question Type: **MultipleChoice**

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

Options:

A) The attack is fragmented into groups of 16 octets before transmission.

B) The attack is fragmented into groups of 8 octets before transmission.

C) Short synchronized bursts of traffic are used to disrupt TCP connections.

D) Malformed packets are used to crash systems.

E) Publicly accessible DNS servers are typically used to execute the attack.

Answer:

B, D

Question 4

Question Type: **MultipleChoice**

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

Options:

A) asset inventory management

B) allowed application management

C) Active Directory group policy management

D) network device management

E) critical device management

Answer:

A, B

Question 5

Question Type: MultipleChoice

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

Options:

A) biometric factor

B) time factor

C) confidentiality factor

D) knowledge factor

E) encryption factor

Answer:

A, D

Question 6

Question Type: **MultipleChoice**

Which two capabilities does TAXII support? (Choose two.)

Options:

A) exchange

B) pull messaging

C) binding

D) correlation

E) mitigating

Answer:

B, C