210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

QUESTION 1

What mechanism does the Linux operating system provide to control access to files?

A. privileges required

B. user interaction

C. file permissions

D. access complexity

Correct Answer: C

QUESTION 2

Which value in profiling servers in a system is true?

A. it can identify when network performance has decreased

B. it can identify servers that have been exploited

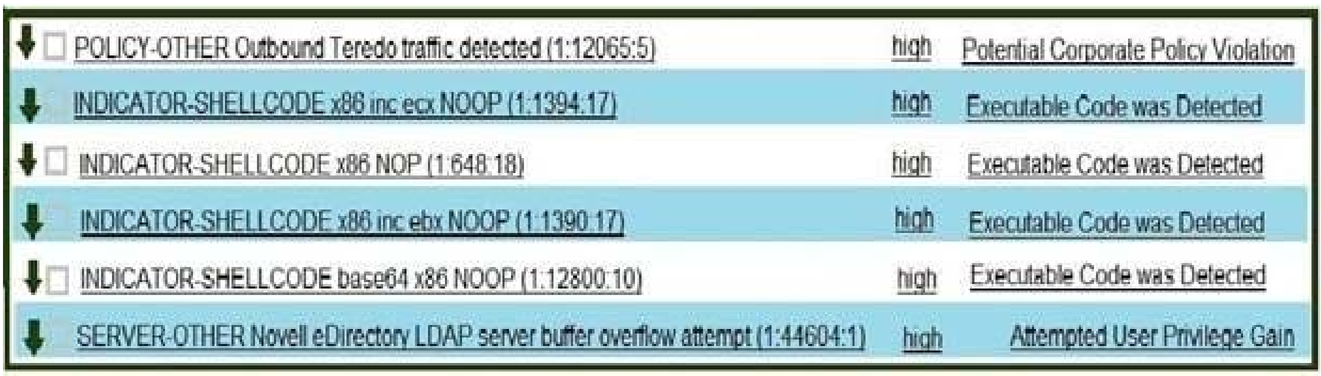
C. it can identify when network ports have been connected

D. it can protect the address space of critical hosts.

Correct Answer: B

QUESTION 3

Refer to exhibit. Which option is the logical source device for these events?



☐ POLICY-OTHER Outbound Teredo traffic detected (1:12065:5)	high	Potential Corporate Policy Violation
INDICATOR-SHELLCODE x86 inc ecx NOOP (1:1394:17)	high	Executable Code was Detected
☐ INDICATOR-SHELLCODE x86 NOP (1:648:18)	high	Executable Code was Detected
INDICATOR-SHELLCODE x86 inc ebx NOOP (1:1390:17)	high	Executable Code was Detected
☐ INDICATOR-SHELLCODE base64 x86 NOOP (1:12800:10)	high	Executable Code was Detected
SERVER-OTHER Novell eDirectory LDAP server buffer overflow attempt (1:44604:1)	high	Attempted User Privilege Gain

A. web server

B. NetFlow collector

C. proxy server

D. IDS/IPS

Correct Answer: D

QUESTION 4

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2?

A. instigator

B. precursor

C. online assault

D. trigger

Correct Answer: B

QUESTION 5

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

A. so that everyone knows the local time

B. to ensure employees adhere to work schedule

C. to construct an accurate timeline of events when responding to an incident

D. to guarantee that updates are pushed out according to schedule

Correct Answer: C

QUESTION 6

Choose the option that best describes NIST data integrity

A. use only sha-1

B. use only md5

C. you must hash data and backup and compare hashes

D. no need to hash data and backup and compare hashes

Correct Answer: C

QUESTION 7

What is the definition of availability accord to CVSSv3 framework?

A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.

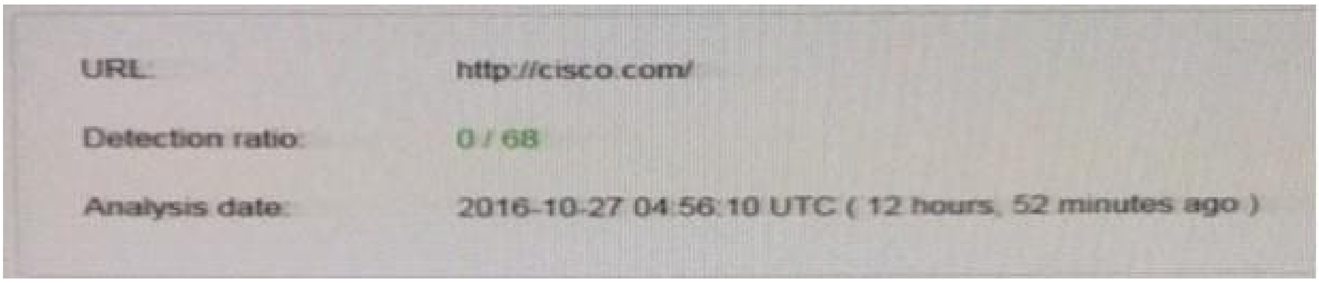
B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.

C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

Correct Answer: C

QUESTION 8

Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?



URL: http://cisco.com/

Detection ratio: 0 / 68

Analysis date: 2016-10-27 04:56:10 UTC (12 hours, 52 minutes ago)

A. The website has been marked benign on all 68 checks.

B. The threat detection needs to run again.

C. The website has 68 open threats.

D. The website has been marked benign on 0 checks.

Correct Answer: A

QUESTION 9

What is Data mapping used for? (Choose two)

A. data accuracy (integrity)

B. data availability

C. data normalization

D. data confidentiality

E. data visualisation

Correct Answer: AE

QUESTION 10

Which string matches the regular expression r(ege)+x?

A. rx

B. regeegex

C. r(ege)x

D. rege+x

Correct Answer: B

QUESTION 11

Which feature is used to find possible vulnerable services running on a server?

A. CPU utilization

B. security policy

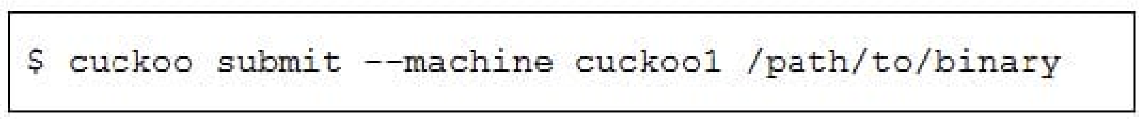
C. temporary internet files

D. listening ports

Correct Answer: D

QUESTION 12

Refer to the exhibit.



```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Which event is occurring?

A. A URL is being evaluated to see if it has a malicious binary.

B. A binary on device cuckoo1 is being submitted for evaluation.

C. A binary named “submit” is running on cuckoo1.

D. A binary is being submitted to run on device cuckoo1.

Correct Answer: D

QUESTION 13

Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario?

A. deterministic

B. exploratory

C. probabilistic

D. descriptive

Correct Answer: A

QUESTION 14

Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

A. data analytics

B. asset attribution

C. threat actor attribution

D. evidence collection

Correct Answer: A

QUESTION 15

Which CVSS Attach Vector metric value means that the vulnerable component is not bound to the network stack and the path of the attacker is via read/write/execute capabilities?

A. network

B. physical

C. local

D. adjacent

Correct Answer: C

Reference: https://www.first.org/cvss/specification-document