Cisco 210-250 Exam

Volume: 65 Questions

Question No: 1
Which definition of a fork in Linux is true?

A. daemon to execute scheduled commands

B. parent directory name of a file pathname

C. macros for manipulating CPU sets

D. new process created by a parent process

Answer: C

Question No: 2
Which identifier is used to describe the application or process that submitted a log message?

A. action

B. selector

C. priority

D. facility

Answer: D

Question No: 3
Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

A. NTP

B. HTIP

C. DNS

D. SSH

Answer: C

Question No: 4
Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation

B. tunneling

C. timing attack

D. resource exhaustion

Answer: A

Question No: 5
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IPS phones?

A. replay

B. man-in-the-middle

C. dictionary

D. known-plaintext

Answer: B

Question No: 6
Which definition of permissions in Linux is true?

A. rules that allow network traffic to go in and out

B. table maintenance program

C. written affidavit that you have to sign before using the system

D. attributes of ownership and control of an object

Answer: A

Question No: 7
Which definition describes the main purpose of a Security Information and Event Management solution?

A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats

B. a monitoring interface that manages firewall access control lists for duplicate firewall filtering

C. a relay server or device that collects then forwards event logs to another log collection device

D. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture

Answer: D

Question No: 8
If a web server accepts input from the user and passes it to a bash shell, to which attack method is it vulnerable?

A. input validation

B. hash collision

C. command injection

D. integer overflow

Answer: B

Question No: 9
Which security monitoring data type is associated with application server logs?

A. alert data

B. statistical data

C. session data

D. transaction data

Answer: A

Question No: 10
Which two terms are types of cross site scripting attacks? (Choose two)

A. directed

B. encoded

C. stored

D. reflected

E. cascaded

Answer: CD

Question No: 11
Which two actions are valid uses of public key infrastructure? (Choose two)

A. ensuring the privacy of a certificate

B. revoking the validation of a certificate

C. validating the authenticity of a certificate

D. creating duplicate copies of a certificate

E. changing ownership of a certificate

Answer: AC

Question No: 12
Which definition of a process in Windows is true?

A. running program

B. unit of execution that must be manually scheduled by the application

C. database that stores low-level settings for the OS and for certain applications

D. basic unit to which the operating system allocates processor time

Answer: C

Question No: 13
Which tool is commonly used by threat actors on a webpage to take advantage of the software vulnerabilities of a system to spread malware?

A. exploit kit

B. root kit

C. vulnerability kit

D. script kiddie kit

Answer: A

Question No: 14
Which encryption algorithm is the strongest?

A. AES

B. CES

C. DES

D. 3DES

Answer: A

Question No: 15
In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully?

A. ACK

B. SYN, ACK

C. RST

D. PSH, ACK