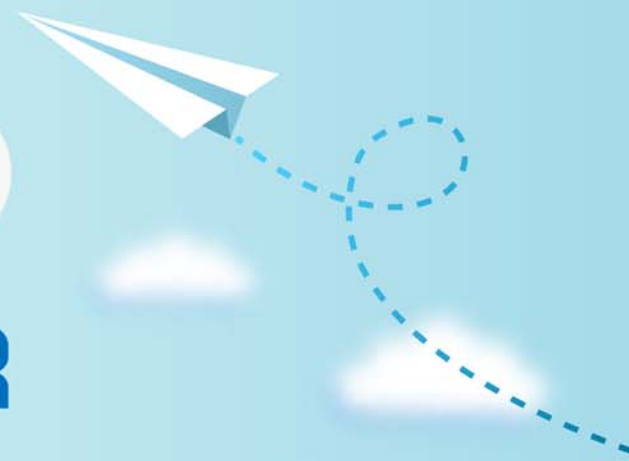


CERTPARK

QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



Exam : 210-250

**Title : Understanding Cisco
Cybersecurity
Fundamentals**

Version : DEMO

- 1.Which definition of a fork in Linux is true?
- A. daemon to execute scheduled commands
 - B. parent directory name of a file path name
 - C. macros for manipulating CPU sets
 - D. new process created by a parent process

Answer: D

- 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

Explanation:

Reference: <https://www.tutorialspoint.com/unix/unix-system-logging.htm>

- 3.Which protocol is expected to have a user agent, host, and referrer header in a packet capture?
- A. NTP
 - B. HTTP
 - C. DNS
 - D. SSH

Answer: B

- 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: C

Explanation:

Reference: https://books.google.by/books?id=KlWLSddtAWsC&pg=PA58&lpg=PA58&dq=timing+attack+performing+actions+slower+than+normal+to+prevent+detection&source=bl&ots=9qu7ywV-mX&sig=_9lwcDDq-WNaYIEeP7Vkr0MPAOE&hl=en&sa=X&redir_esc=y#v=onepage&q=timing%20attack%20performing%20actions%20slower%20than%20normal%20to%20prevent%20detection&f=false

- 5.Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?
- A. replay
 - B. man-in-the-middle
 - C. dictionary
 - D. known-plaintext

Answer: B