Cisco CCNA Certification 210-255 Exam

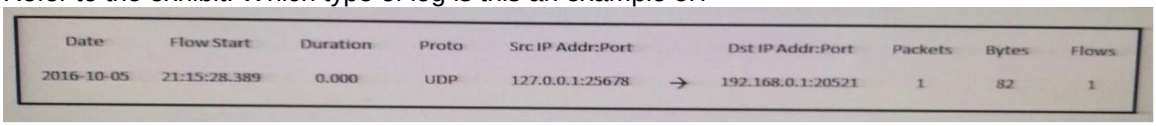
- **Vendor: Cisco**
- **Exam Code: 210-255**
- **Exam Name: Implementing Cisco Cybersecurity Operations (SECOPS)**

QUESTION 1
Which option can be addressed when using retrospective security techniques?

A. if the affected host needs a software update
B. how the malware entered our network
C. why the malware is still in our network
D. if the affected system needs replacement

Answer: A

QUESTION 2
Refer to the exhibit. Which type of log is this an example of?



Date	Flow Start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2016-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	192.168.0.1:20521	1	82	1

A. IDS log
B. proxy log
C. NetFlow log
D. syslog

Answer: A

QUESTION 3
Which option is a misuse variety per VERIS enumerations?

A. snooping
B. hacking
C. theft
D. assault

Answer: B

QUESTION 4
In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

A. determining the number of attackers that are associated with a security incident
B. ascertaining the number and types of vulnerabilities on your network
C. identifying the extent that a security incident is impacting protected resources on the network
D. determining what and how much data may have been affected
E. identifying the attackers that are associated with a security incident

Answer: DE

QUESTION 5
Which regular expression matches "color" and "colour"?

A. col[0-9]+our
B. colo?ur
C. colou?r
D.]a-z]{7}

Answer: C

QUESTION 6
Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. preparation
B. detection and analysis
C. containment, eradication, and recovery
D. post-incident analysis

Answer: B

QUESTION 7
Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

A. URL
B. hash
C. IP address
D. destination port

Answer: C

QUESTION 8
Which data type is protected under the PCI compliance framework?

A. credit card type
B. primary account number
C. health conditions
D. provision of individual care

Answer: C

QUESTION 9
Which kind of evidence can be considered most reliable to arrive at an analytical assertion?

A. direct
B. corroborative
C. indirect
D. circumstantial
E. textual

Answer: A

QUESTION 10
Which of the following is not a metadata feature of the Diamond Model?

A. Direction
B. Result
C. Devices

D. Resources

Answer: C

QUESTION 11
Which of the following has been used to evade IDS and IPS devices?

A. SNMP
B. HTTP
C. TNP
D. Fragmentation

Answer: D

QUESTION 12
Which of the following can be identified by correlating DNS intelligence and other security events? (Choose two.)

A. Communication to CnC servers
B. Configuration issues
C. Malicious domains based on reputation
D. Routing problems

Answer: AC

QUESTION 13
Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a security operations center (SOC)?

A. Cisco CloudLock
B. Cisco's Active Threat Analytics (ATA)
C. Cisco Managed Firepower Service
D. Cisco Jasper

Answer: B

QUESTION 14
Which of the following is not an example of weaponization?

A. Connecting to a command and control server
B. Wrapping software with a RAT
C. Creating a backdoor in an application
D. Developing an automated script to inject commands on a USB device

Answer: A

QUESTION 15
Which of the following are core responsibilities of a national CSIRT and CERT?

A. Provide solutions for bug bounties
B. Protect their citizens by providing security vulnerability information, security awareness training, best practices, and other information

C. Provide vulnerability brokering to vendors within a country
D. Create regulations around cybersecurity within the country

Answer: B

QUESTION 16

……