QUESTION 30
When you are researching a Windows operating system vulnerability (such as CVE-2016-7211), which organization can provide detailed information about the specific vulnerability?

A. Institute of Electrical and Electronics Engineers (IEEE)
B. Control Objectives for Information and Related Technologies (COBIT)
C. National Institute of Standards and Technology (NIST)
D. International Organization for Standardization (ISO)

Answer: C

QUESTION 31
Which property of a cryptographic hash algorithm is desirable?

A. collision resistance
B. reversibility
C. nondeterminism
D. rainbow tables

Answer: A

QUESTION 32
Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context
B. session
C. laptop
D. firewall logs
E. threat actor

Answer: AE

QUESTION 33
Which regular expression matches "color" and "colour"?

A. colo?ur
B. col[0-8]+our
C. colou?r
D. col[0-9]+our

Answer: C

QUESTION 34
A user received a malicious attachment but did not run it.
Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Answer: D

QUESTION 35
Which process is used when IPS events are removed to improve data integrity?

A. data availability
B. data normalization
C. data signature
D. data protection

Answer: B

QUESTION 36
An investigator is examining a copy of an ISO file that is stored in CDFS format.
What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

QUESTION 37
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

QUESTION 38
Refer to the exhibit. In which Linux log file is this output found?

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

A. /var/log/authorization.log

B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

Answer: D

QUESTION 39
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

QUESTION 40
Which type of data typically consists of connection level, application-specific records generated from network traffic?

A. location data
B. statistical data
C. alert data
D. transaction data

Answer: B

QUESTION 41
What are three key components of a threat-centric SOC? (Choose three.)

A. people
B. compliances
C. processes
D. regulations
E. technologies

Answer: ACE

QUESTION 42
An analyst is investigating an incident in a SOC environment.
Which method is used to identify a session from a group of logs?

A. sequence numbers
B. IP identifier
C. 5-tuple
D. timestamps

Answer: C