QUESTION 56
Refer to the exhibit. Which event is occurring?

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

A. A binary named "submit" is running on VM cuckoo1.
B. A binary is being submitted to run on VM cuckoo1
C. A binary on VM cuckoo1 is being submitted for evaluation
D. A URL is being evaluated to see if it has a malicious binary

Answer: C

QUESTION 57
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: B

QUESTION 58
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining
D. due diligence

Answer: A

QUESTION 59
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.
Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

A. signatures
B. host IP addresses
C. file size
D. dropped files
E. domain names

Answer: BE

QUESTION 60
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

Answer: D

QUESTION 61
One of the objectives of information security is to protect the CIA of information and systems.
What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

Answer: D

QUESTION 62
What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Answer: B

QUESTION 63
What is personally identifiable information that must be safeguarded from unauthorized access?

A. date of birth
B. driver's license number
C. gender
D. zip code

Answer: B

QUESTION 64
How does an SSL certificate impact security between the client and the server?

A. by enabling an authenticated channel between the client and the server

B. by creating an integrated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server

Answer: D

QUESTION 65
Which type of exploit normally requires the culprit to have prior access to the target system?

A. local exploit
B. denial of service
C. system vulnerability
D. remote exploit

Answer: A

QUESTION 66
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 67
Which type of data consists of connection level, application-specific records generated from network traffic?

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

Answer: A

QUESTION 68
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application
D. data link

Answer: C

QUESTION 69
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

A. NetScout
B. tcpdump
C. SolarWinds
D. netsh

Answer: B