- Vendor: CompTIA
- Exam Code: SY0-601
- Exam Name: CompTIA Security+ Certification Exam
- New Updated Questions from Braindump2go (Updated in June/2022)

QUESTION 656
A DBA reports that several production server hard drives were wipes over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?

A. Logic Bomb
B. Ransomware
C. Fileless virus
D. Remote access Trojans
E. Rootkit

Answer: A

QUESTION 657
Digital signatures use asymmetric encryption. This means the message is encrypted with:

A. the senders private key and decrypted with the senders' public key
B. the senders public key and decrypted with the senders' private key
C. the senders private key and decrypted with the recipient's public key
D. the senders public key and decrypted with the recipient's private key

Answer: A

QUESTION 658
A help desk technician receives a phone call from someone claiming to be a part of the organizations cybersecurity incident response team. The caller asks the technician to verify networks internal firewall IP address. Which of the following is the technicians BEST course of action?

A. direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.
B. ask for the callers name, verify the persons identity in the email directory, and provide the requested information over the phone.
C. write down the phone number of the caller if possible, the name of the person requesting the information. Hang-up, and notify the organizations cybersecurity officer
D. request the caller send an email for identity verification and provide the requested information via email to the caller.

Answer: C

QUESTION 659
An employee received a word processing file that was delivered as an email attachment. The subject line and email content enticed the employee to open the attachment.
Which of the following attack vectors BEST matches this malware?

A. embedded Python code
B. Macro-enabled file
C. Bash scripting
D. Credential-harvesting website

Answer: B

QUESTION 660
Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media retention policy?

A. putting security/antitamper tape over USB ports. Keylogging the port numbers and regularly inspecting the ports.
B. implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
C. placing systems into locked key-controlled containers with no access to the USB ports.
D. installing an endpoint agent to detect connectivity of USB and removable media

Answer: B

QUESTION 661
The SOC for a large MSSP in a meeting to discuss the lessons learned from a recent incident that took much too long to resolve. This type of incident has become more common over weeks and is consuming large amounts of the analysts time due to manual tasks being performed. Which of the following solutions should the SOC consider to BEST improve its response time?

A. configure a NIDS appliance using a Switched Port Analyzer
B. collect OSINT and catalog the artifacts in a central repository
C. implement a SOAR with customizable playbooks
D. install a SIEM with community-driven threat intelligence

Answer: C

QUESTION 662
A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. a search of the WAF logs reveals the following output:

```
172.16.1.3/ 10.10.1.1/ web/ permit and log
```

A. XSS attack
B. SQLi attack
C. Replay attack
D. XSRF attack

Answer: A

QUESTION 663
Which of the following is an example of transference of risk?

A. purchasing insurance

B. patching vulnerable servers
C. retiring outdated applications
D. Application owner risk sign-off

Answer: A

QUESTION 664
A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

A. SSO
B. IDS
C. MFA
D. TPM

Answer: C

QUESTION 665
A tax organization is working on a solution to validate the online submission of documents. The solution should be carried on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

A. user certificate
B. self-signed certificate
C. computer certificate
D. root certificate

Answer: C

QUESTION 666
During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

A. the forensic investigator forgot to run a checksum on the disk image after creation
B. the chain of custody form did not note time zone offsets between transportation regions
C. the computer was turned off, and a RAM image could not be taken at the same time
D. the hard drive was not properly kept in an antistatic bag when it was moved.

Answer: D

QUESTION 667
A security analyst needs to be able to search and correlate logs from multiple sources in a single tool. Which of the following would BEST allow a security analyst to have this ability?

A. SOAR
B. SIEM
C. Log collectors
D. Network-attached storage

Answer: C

QUESTION 668
The chief information security officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data which of the following would be BEST for the third-party vendor to provide the CISO?

A. GDPR compliance attestation
B. cloud security alliance materials
C. SOC 2 type 2 report
D. NIST RMP workbooks

Answer: C

QUESTION 669
A company labeled some documents with the public sensitivity classification. This means the documents can be accessed by:

A. employees of other companies and the press
B. all members of the department that created the documents
C. only the company's employees and those listed in the document
D. only the individuals listed in the documents

Answer: C

QUESTION 670
Which of the following explains why RTO is included in a BIA?

A. it identifies the amount of allowable downtime for an application or system
B. it prioritizes risks so the organization can allocate resources appropriately.
C. it monetizes the loss of an asset and determines a break even point for risk mitigation
D. it informs the backup approach so that the organization can recover data to a known time

Answer: C

QUESTION 671
A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance has degraded. Which of the following MOST likely explains this behavior?

A. DNS poisoning
B. MAC flooding
C. DDoS attack
D. ARP poisoning

Answer: C