- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 1148
A coding error has been discovered on a customer-facing website. The error causes each request to return confidential PHI data for the incorrect organization. The IT department is unable to identify the specific customers who are affected. As a result, all customers must be notified of the potential breach. Which of the following would allow the team to determine the scope of future incidents?

A. Intrusion detection system
B. Database access monitoring
C. Application fuzzing
D. Monthly vulnerability scans

Answer: B

QUESTION 1149
A systems engineer wants to leverage a cloud-based architecture with low latency between network- connected devices that also reduces the bandwidth that is required by performing analytics directly on the endpoints. Which of the following would BEST meet the requirements? (Choose two.)

A. Private cloud
B. SaaS
C. Hybrid cloud
D. IaaS
E. DRaaS
F. Fog computing

Answer: AB

QUESTION 1150
A systems engineer is setting up a RADIUS server to support a wireless network that uses certificate authentication. Which of the following protocols must be supported by both the RADIUS server and the WAPs?

A. CCMP
B. TKIP
C. WPS
D. EAP

Answer: D

QUESTION 1151

A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
- Protection from power outages
- Always-available connectivity in case of an outage
The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

A. Lease a telecommunications line to provide POTS for dial-up access.
B. Connect the business router to its own dedicated UPS.
C. Purchase services from a cloud provider for high availability.
D. Replace the business's wired network with a wireless network.

Answer: C

QUESTION 1152
A systems engineer is configuring a wireless network. The network must not require installation of third- party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS
B. EAP-TTLS
C. EAP-FAST
D. EAP-MD5
E. PEAP

Answer: A

QUESTION 1153
A security operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

Answer: C

QUESTION 1154
An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

Answer: A

QUESTION 1155
Joe, an employee, knows he is going to be fired in three days. Which of the following is Joe?

A. An insider threat
B. A competitor

C. A hacktivist
D. A state actor

Answer: A

QUESTION 1156
Which of the following BEST describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible
B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations
C. Implementing elliptic curve cryptographic algorithms with true random numbers
D. The use of NDAs and policy controls to prevent disclosure of company secrets

Answer: B

QUESTION 1157
Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.
B. Users need to authenticate for each resource they access.
C. It requires an organization to configure federation.
D. The authentication is transparent to the user.

Answer: A

QUESTION 1158
An intruder sniffs network traffic and captures a packet of internal network transactions that add funds to a game card. The intruder pushes the same packet multiple times across the network, which increments the funds on the game card. Which of the following should a security administrator implement to BEST protect against this type of attack?

A. An IPS
B. A WAF
C. SSH
D. An IPSec VPN

Answer: D

QUESTION 1159
Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

Answer: B

QUESTION 1160
After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service

D. NTP server

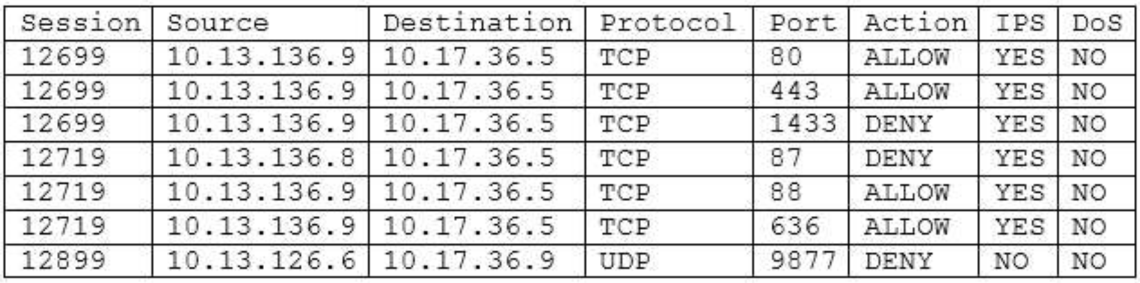
Answer: D

QUESTION 1161
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer: D

QUESTION 1162
The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9, and the destination IP is 10.17.36.5. The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:



Session	Source	Destination	Protocol	Port	Action	IPS	DoS
12699	10.13.136.9	10.17.36.5	TCP	80	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	443	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	1433	DENY	YES	NO
12719	10.13.136.8	10.17.36.5	TCP	87	DENY	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	88	ALLOW	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	636	ALLOW	YES	NO
12899	10.13.126.6	10.17.36.9	UDP	9877	DENY	NO	NO

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5.
B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.
C. Request the network team to turn off IPS for 10.13.136.8 going to 10.17.36.5.
D. Request the application team to reconfigure the application and allow RPC communication.

Answer: C

QUESTION 1163
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

Answer: A