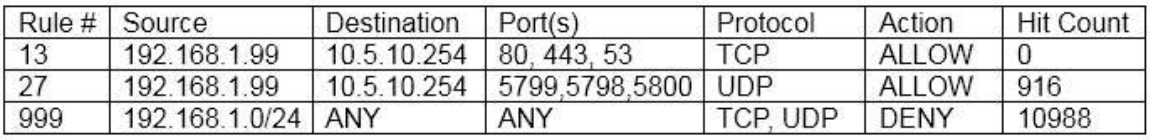
- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 1164
After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:



Rule #	Source	Destination	Port(s)	Protocol	Action	Hit Count
13	192.168.1.99	10.5.10.254	80, 443, 53	TCP	ALLOW	0
27	192.168.1.99	10.5.10.254	5799,5798,5800	UDP	ALLOW	916
999	192.168.1.0/24	ANY	ANY	TCP, UDP	DENY	10988

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled.
B. The VLAN is not trunked properly.
C. There is a policy violation for DNS lookups.
D. The firewall policy is misconfigured.

Answer: D

QUESTION 1165
A security analyst is performing a BIA. The analyst notes that in a disaster, failover systems must be up and running within 30 minutes. The failover systems must use backup data that is no older than one hour. Which of the following should the analyst include in the business continuity plan?

A. A maximum MTTR of 30 minutes
B. A maximum MTBF of 30 minutes
C. A maximum RTO of 60 minutes
D. A maximum RPO of 60 minutes
E. An SLA guarantee of 60 minutes

Answer: D

QUESTION 1166
A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud

Answer: D

QUESTION 1167
An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

Answer: A

QUESTION 1168
A malicious actor recently penetrated a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

QUESTION 1169
Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws

Answer: B

QUESTION 1170
An attacker is able to capture the payload for the following packet:
IP 192.168.1.22:2020 10.10.10.5:443
IP 192.168.1.10:1030 10.10.10.1:21
IP 192.168.1.57:5217 10.10.10.1:3389
During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and using those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on across multiple servers.

Answer: C

QUESTION 1171
A forensics analyst is investigating a hard drive for evidence of suspected illegal activity. Which of the following should the analyst do FIRST?

A. Create a hash of the hard drive.
B. Export the Internet history.
C. Save a copy of the case number and date as a text file in the root directory.
D. Back up the pictures directory for further inspection.

Answer: A

QUESTION 1172
Which of the following is a passive method to test whether transport encryption is implemented?

A. Black box penetration test
B. Port scan
C. Code analysis
D. Banner grabbing

Answer: D

QUESTION 1173
The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: File format not recognized. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware
B. Polymorphic virus
C. Rootkit
D. Spyware

Answer: A

QUESTION 1174
Ann, a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot- up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann's computer?

A. The hard drive is falling, and the files are being corrupted.
B. The computer has been infected with crypto-malware.
C. A replay attack has occurred.
D. A keylogger has been installed.

Answer: B

QUESTION 1175
A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Choose two.)

A. Geofencing
B. Video surveillance
C. Protected cabinets
D. Mantrap
E. Key exchange
F. Authorized personnel signage

Answer: CD

QUESTION 1176
A system uses an application server and database server. Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server. Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).
The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit. Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.
B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.
C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

Answer: A

QUESTION 1177
A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices for corporate use must opt in to the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading
B. Full device encryption
C. Application management
D. Containerization

Answer: D

QUESTION 1178
A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. A bot
B. A fileless virus
C. A logic bomb
D. A RAT

Answer: A

QUESTION 1179
A systems administrator is auditing the company's Active Directory environment. It is quickly noted that the username "company\bsmith" is interactively logged into several desktops across the organization. Which of the following has the systems administrator MOST likely come across?

A. Service account
B. Shared credentials

C. False positive
D. Local account

Answer: B