- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in April/2021)**

QUESTION 1336
A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:

```
$ history
    ifconfig -a
    netstat -n
    pskill 1788
    pskill 914
    mkdir /tmp/1
    mount -u ada101 /tmp/1
    cp /tmp/1/* ~/1/
    umount /tmp/1
    ls -al 1/1/
    apt-get update
    apt-get upgrade
    clear
```

Given this output, which of the following security issues has been discovered?

A. A misconfigured HIDS
B. A malware installation
C. A policy violation
D. The activation of a Trojan

Answer: B

QUESTION 1337
During certain vulnerability scanning scenarios, it is possible for the target system to react in unexpected ways. This type of scenario is MOST commonly known as:

A. intrusive testing
B. a buffer overflow
C. a race condition
D. active reconnaissance

Answer: A

QUESTION 1338

An organization prefers to apply account permissions to groups and not individual users, but allows for exceptions that are justified. Some systems require a machine-to-machine data exchange and an associated account to perform this data exchange. One particular system has data in a folder that must be modified by another system. No user requires access to this folder; only the other system needs access to this folder. Which of the following is the BEST account management practice?

A. Create a service account and apply the necessary permissions directly to the service account itself
B. Create a service account group, place the service account in the group, and apply the permissions on the group
C. Create a guest account and restrict the permissions to only the folder with the data
D. Create a generic account that will only be used for accessing the folder, but disable the account until it is needed for the data exchange
E. Create a shared account that administrators can use to exchange the data, but audit the shared account activity

Answer: A

QUESTION 1339
A user attempts to send an email to an external domain and quickly receives a bounce-back message. The user then contacts the help desk stating the message is important and needs to be delivered immediately. While digging through the email logs, a systems administrator finds the email and bounce- back details:
Your email has been rejected because it appears to contain SSN information. Sending SSN information via email to external recipients violates company policy.
Which of the following technologies successfully stopped the email from being sent?

A. DLP
B. UTM
C. WAF
D. DEP

Answer: A

QUESTION 1340
Which of the following controls does a mantrap BEST represent?

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

Answer: C

QUESTION 1341
A security administrator has created a new group policy object that utilizes the trusted platform module to compute a hash of system files and compare the value to a known-good value. Which of the following security concepts is this an example of?

A. Integrity measurement
B. Secure baseline
C. Sandboxing
D. Immutable systems

Answer: A

QUESTION 1342

A network administrator wants to gather information on the security of the network servers in the DMZ. The administrator runs the following command:
Telnet www.example.com 80
Which of the following actions is the administrator performing?

A. Grabbing the web server banner
B. Logging into the web server
C. Harvesting cleartext credentials
D. Accessing the web server management console

Answer: A

QUESTION 1343
Which of the following should be implemented to stop an attacker from interacting with the hypervisor through another guest?

A. Containers
B. VM escape protection
C. Security broker
D. Virtual desktop

Answer: B

QUESTION 1344
An internal intranet site is required to authenticate users and restrict access to content to only those who are authorized to view it. The site administrator previously encountered issues with credential spoofing when using the default NTLM setting and wants to move to a system that will be more resilient to replay attacks. Which of the following should the administrator implement?

A. NTLMv2
B. TACACS+
C. Kerberos
D. Shibboleth

Answer: C

QUESTION 1345
A security consultant is analyzing data from a recent compromise. The following data points are documented:
- Access to data on share drives and certain networked hosts was lost after an employee logged in to an interactive session as a privileged user.
- The data was unreadable by any known commercial software.
- The issue spread through the enterprise via SMB only when certain users accessed data.
- Removal instructions were not available from any major antivirus vendor.
Which of the following types of malware is this an example of?

A. RAT
B. Ransomware
C. Backdoor
D. Keylogger
E. Worm

Answer: B

QUESTION 1346
An organization handling highly confidential information needs to update its systems. Which of the following is the BEST method to prevent data compromise?

A. Wiping
B. Degaussing
C. Shredding
D. Purging

Answer: C

QUESTION 1347
A security administrator is working with the human resources department to classify data held by the company. The administrator has determined the data contains a variety of data types, including health information, employee names and addresses, trade secrets, and confidential customer information. Which of the following should the security administrator do NEXT?

A. Apply a predefined set of labels from government sources to all data within the company
B. Create a custom set of data labels to group the data by sensitivity and protection requirements
C. Label sensitive data according to age to comply with retention policies
D. Destroy company information that is not labeled in compliance with government regulations and laws

Answer: B

QUESTION 1348
A security administrator has been conducting an account permissions review that has identified several users who belong to functional groups and groups responsible for auditing the functional groups' actions. Several recent outages have not been able to be traced to any user. Which of the following should the security administrator recommend to preserve future audit log integrity?

A. Enforcing stricter onboarding workflow policies
B. Applying least privilege to user group membership
C. Following standard naming conventions for audit group users
D. Restricting audit group membership to service accounts

Answer: C

QUESTION 1349
Joe, a new employee, discovered a thumb drive with the company's logo on it while walking in the parking lot. Joe was curious as to the contents of the drive and placed it into his work computer. Shortly after accessing the contents, he noticed the machine was running slower, started to reboot, and displayed new icons on the screen. Which of the following types of attacks occurred?

A. Social engineering
B. Brute force attack
C. MITM
D. DoS

Answer: A

QUESTION 1350
In the event of a security incident, which of the following should be captured FIRST?

A. An external hard drive
B. System memory
C. An internal hard drive
D. Network interface data

Answer: B

QUESTION 1351
A security analyst receives the following output:

Time	Action	Host	File Name	User
12/15/2017	Policy: Endpoint USB Transfer - Blocked	Host1	Q3-Financials.PDF	User1

Which of the following MOST likely occurred to produce this output?

A. The host-based firewall prevented an attack from a Trojan horse
B. USB-OTG prevented a file from being uploaded to a mobile device
C. The host DLP prevented a file from being moved off a computer
D. The firewall prevented an incoming malware-infected file

Answer: C

QUESTION 1352
Which of the following BEST explains "likelihood of occurrence"?

A. The chance that an event will happen regardless of how much damage it may cause
B. The overall impact to the organization once all factors have been considered
C. The potential for a system to have a weakness or flaw that might be exploited
D. The probability that a threat actor will target and attempt to exploit an organization's systems

Answer: D

QUESTION 1353
When choosing a hashing algorithm for storing passwords in a web database, which of the following is the BEST explanation for choosing HMAC-MD5 over simple MD5?

A. HMAC provides hardware acceleration, thus speeding up authentication
B. HMAC adds a transport layer handshake, which improves authentication
C. HMAC-MD5 can be decrypted faster, speeding up performance
D. HMAC-MD5 is more resistant to brute forcing

Answer: B

QUESTION 1354
Given the following:

```
> md5.exe file1.txt
> AD1FAB103773DC6A1E6021B7F503A210
> md5.exe file2.txt
> AD1FAB103773DC6A1E6021B7F503A210
```

Which of the following concepts of cryptography is shown?

A. Collision
B. Salting
C. Steganography
D. Stream cipher

Answer: B

QUESTION 1355
A law firm wants to protect its customers' individual information, which is stored at a remote facility, from inadvertently

being compromised through a violation of the security objectives. Which of the following BEST describes the customer information that is being stored at this facility?

A. Trade secrets
B. Personal health information
C. Proprietary
D. Confidential

Answer: D

QUESTION 1356
A technician wants to configure a wireless router at a small office that manages a family-owned dry cleaning business. The router will support five laptops, personal smartphones, a wireless printer, and occasional guests. Which of the following wireless configurations is BEST implemented in this scenario?

A. Single SSID with WPA2-Enterprise
B. 802.1X with a guest VLAN
C. Dual SSID with WPA2-PSK
D. Captive portal with two-factor authentication

Answer: C

QUESTION 1357
A systems administrator just issued the `ssh-keygen -t rsa` command on a Linux terminal. Which of the following BEST describes what the `rsa` portion of the command represents?

A. A key generation algorithm
B. A hashing algorithm
C. A public key infrastructure type
D. A certificate authority type

Answer: A

QUESTION 1358
A newly hired Chief Security Officer (CSO) is reviewing the company's IRP and notices the procedures for zero-day malware attacks are being poorly executed, resulting in the CSIRT failing to address and coordinate malware removal from the system. Which of the following phases would BEST address these shortcomings?

A. Identification
B. Lessons learned
C. Recovery
D. Preparation
E. Eradication

Answer: B

QUESTION 1359
A security analyst has identified malware that is propagating automatically to multiple systems on the network. Which of the following types of malware is MOST likely impacting the network?

A. Virus
B. Worm
C. Logic bomb
D. Backdoor

Answer: B

QUESTION 1360
An organization allows the use of open-source software as long as users perform a file integrity check on the executables and verify the file against hashes of known malware. A user downloads the following files from an open-source website:

FILE NAME	MD5
webserver_81.exe	1e39 2210 faec 6ae4 243f 22cd 33da 62e4
opendatabase_43.exe	2f36 12e0 123c 52e2 1a3e 10ae 23bb 72a3
webserver_82.exe	2f40 3221 33ad 8f34 1032 1adc 13ef 51a4
opendatabase_44.exe	2a22 10ac 36ac 7789 10af 12aa 23aa 51e6

After submitting the hashes to the malware registry, the user is alerted that 2f40 3221 33ad 8f34 matches a known malware signature. The organization has been running all of 1032 1adc 13ef 51a4 the above software with no known issues. Which of the following actions should the user take and why?

A. Download and run the software but notify the organization's cybersecurity office. The malware registry has a false positive since the software has been running without any issues.
B. Do not run any of the software and notify the organization's cybersecurity office. The open-source website has been compromised, and none of the software can be trusted.
C. Download and run only webserver_82.exe and opendatabase_44.exe and notify the organization's cybersecurity office. Legacy versions of the software have been compromised.
D. Do not run webserver_82.exe and notify the organization's cybersecurity office. The software is malware.

Answer: D

QUESTION 1361
An administrator needs to protect five websites with SSL certificates. Three of the websites have different domain names, and two of the websites share the domain name but have different subdomain prefixes. Which of the following SSL certificates should the administrator purchase to protect all the websites and be able to administer them easily at a later time?

A. One SAN certificate
B. One Unified Communications Certificate and one wildcard certificate
C. One wildcard certificate and two standard certificates
D. Five standard certificates

Answer: A

QUESTION 1362
A security administrator begins assessing a network with software that checks for available exploits against a known database, using both credentials and external scripts. A report will be compiled and used to confirm patching levels. This is an example of:

A. penetration testing
B. fuzzing
C. static code analysis
D. vulnerability scanning

Answer: D

QUESTION 1363
While testing a new application, a developer discovers that the inclusion of an apostrophe in a username causes the application to crash. Which of the following secure coding techniques would be MOST useful to avoid this problem?

A. Input validation
B. Code signing
C. Obfuscation
D. Encryption

Answer: A

QUESTION 1364
A company recently contracted a penetration testing firm to conduct an assessment. During the assessment, the penetration testers were able to capture unencrypted communication between directory servers. The penetration testers recommended encrypting this communication to fix the vulnerability. Which of the following protocols should the company implement to close this finding?

A. DNSSEC
B. SFTP
C. Kerberos
D. LDAPS

Answer: D

QUESTION 1365
Which of the following are disadvantages of full backups? (Choose three.)

A. They rely on other backups for recovery
B. They require the most storage
C. They demand the most bandwidth
D. They have the slowest recovery time
E. They are impossible in virtual environments
F. They require on-site storage
G. They are time-consuming to complete

Answer: BDG

QUESTION 1366
A security analyst performs a vulnerability scan on the local network. Several items are flagged on the report as being critical issues. The security analyst researches each of the vulnerabilities and discovers that one of the critical issues on the report was mitigated in a previous scan. Which of the following MOST likely happened?

A. A patch was removed
B. A false positive occurred
C. The tool has a high crossover error rate
D. A necessary service was not running

Answer: B