- **Vendor:** CompTIA
- **Exam Code:** SY0-601
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2021)**

Visit Braindump2go and Download Full Version SY0-601 Exam Dumps

QUESTION 336
A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs
B. Common Vulnerabilities and Exposures
C. Static code analysis
D. Non-credentialed scans

Answer: C

QUESTION 337
A user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides. Which of the following authentication concepts are in use?

A. Something you know, something you have, and somewhere you are
B. Something you know, something you can do, and somewhere you are
C. Something you are, something you know, and something you can exhibit
D. Something you have, somewhere you are, and someone you know

Answer: A

QUESTION 338
A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at https://www.company.com. A security analyst then examines the user's Internet usage logs and observes the following output:

```
date; username; url;destinationport; responsecode
2020-03-01; userann; http: //www.company.org/;80;302
2020-03-01; userann: http: //www.company.org/secure_login/;80;
200 2020-03-01; userann:http: //www.company.org/dashboard/;80;200
```

Which of the following has MOST likely occurred?

A. Replay attack
B. SQL injection
C. SSL stripping
D. Race conditions

Answer: A

QUESTION 339
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage.
Which of the following is MOST likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

QUESTION 340
A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS.
Which of the following is the MOST likely attack type?

A. Request forgery
B. Session replay
C. DLL injection
D. Shimming

Answer: A

QUESTION 341
Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

A. Production
B. Test
C. Research and development
D. PoC
E. UAT
F. SDLC

Answer: BE

QUESTION 342
A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support.
Which of the following should the administrator employ to meet these criteria?

A. Implement NAC.
B. Implement an SWG.
C. Implement a URL filter.
D. Implement an MDM.

Answer: B

QUESTION 343
An information security officer at a credit card transaction company is conducting a framework- mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

A. ISO
B. PCI DSS
C. SOC
D. GDPR
E. CSA
F. NIST

Answer: BD

QUESTION 344
Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers' accounts. Which of the following should be implemented to prevent similar situations in the future?

A. Ensure input validation is in place to prevent the use of invalid characters and values.
B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.
C. Configure the web application firewall to look for and block session replay attacks.
D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

Answer: A

QUESTION 345
To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic.
Which of the following solutions would BEST accomplish this objective?

A. Install a hypervisor firewall to filter east-west traffic.
B. Add more VLANs to the hypervisor network switches.
C. Move exposed or vulnerable VMs to the DMZ.
D. Implement a zero-trust policy and physically segregate the hypervisor servers.

Answer: B

QUESTION 346
A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees.
Which of the following controls should the company consider using as part of its IAM strategy? (Select TWO).

A. A complex password policy
B. Geolocation
C. An impossible travel policy
D. Self-service password reset
E. Geofencing
F. Time-based logins

Answer: AB

QUESTION 347
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day.
Which of the following VPN solutions would BEST support the new office?

A. Always On
B. Remote access
C. Site-to-site
D. Full tunnel

Answer: C

QUESTION 348
A security analyst has been reading about a newly discovered cyber attack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

A. Security research publications
B. The MITRE ATT&CK framework
C. The Diamond Model of Intrusion Analysis
D. The Cyber Kill Chain

Answer: B

QUESTION 349
Which of the following is the correct order of volatility from MOST to LEAST volatile?

A. Memory, temporary filesystems, routing tables, disk, network storage
B. Cache, memory, temporary filesystems, disk, archival media
C. Memory, disk, temporary filesystems, cache, archival media
D. Cache, disk, temporary filesystems, network storage, archival media

Answer: B

QUESTION 350
After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

A. Disabling guest accounts
B. Disabling service accounts
C. Enabling network sharing
D. Disabling NetBIOS over TCP/IP
E. Storing LAN manager hash values
F. Enabling NTLM

Answer: AD

QUESTION 351
Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

A. WPA3
B. AES
C. RADIUS

D. WPS

Answer: D

QUESTION 352
Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing

Answer: C

QUESTION 353
A500 is implementing an insider threat detection program, The primary concern is that users may be accessing confidential data without authorization. Which of the fallowing should be deployed to detect a potential insider threat?

A. A honeyfile
B. A DMZ
C. ULF
D. File integrity monitoring

Answer: A

QUESTION 354
The website http://companywebsite.com requires users to provide personal information including security responses, for registration. Which of the following would MOST likely cause a date breach?

A. LACK OF INPUT VALIDATION
B. OPEN PERMISSIONS
C. UNSCECURE PROTOCOL
D. MISSING PATCHES

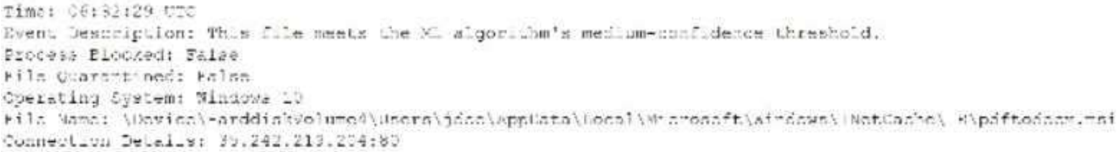
Answer: A

QUESTION 355
A security analyst needs to find real-time data on the latest malware and IoCs. Which of the following would BEST describes the solution the analyst should pursue?

A. Advisories and bulletins
B. Threat feeds
C. Security news articles
D. Peer-reviewed content

Answer: B

QUESTION 356
An end user reports a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-digit number ta an IP address once a day. The only resent log entry regarding the user's computer is the following:



```
Time: 06:32:29 UTC
Event Description: This file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows\INetCache\IE\pdftodocx.msi
Connection Details: 35.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed 2 PUP from a web browser.
B. 4 bot on the computer is rule forcing passwords against a website.
C. A hacker Is attempting to exfilltrated sensitive data.
D. Ransomwere is communicating with a command-and-control server.

Answer: A