A. advisories and bulletins
B. threat feeds
C. security news articles
D. peer-peviewed content

Correct Answer: B

QUESTION 346
A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation, which improves conditions, but performance degrades again after a few days The administrator runs an analysis tool and sees the following output:

The administrator terminates the timeAttend.exe, observes system performance over the next few days and notices that the system performance does not degrade Which of the following issues is MOST likely occurring?

A. DLL injection
B. API attack
C. Buffer overflow
D. Memory leak

Correct Answer: B

QUESTION 347
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production
B. Test
C. Staging
D. Development

Correct Answer: B

QUESTION 348
The board of doctors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?

A. Transference
B. Avoidance
C. Mitigation
D. Acknowledgement

Correct Answer: A

QUESTION 349
Remote workers in an organization use company-provided laptops with locally installed

applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public. Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE
B. TPM
C. HIDS
D. VPN

Correct Answer: A

QUESTION 350
A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

A. Installing WAPs with strategic placement
B. Configuring access using WPA3
C. Installing a WIDS
D. Enabling MAC filtering
E. Changing the WiFi password every 30 days
F. Reducing WiFi transmit power throughout the office

Correct Answer: BD

QUESTION 351
A security monitoring company offers a service that alerts ifs customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?

A. STIX
B. The dark web
C. TAXII
D. Social media
E. PCI

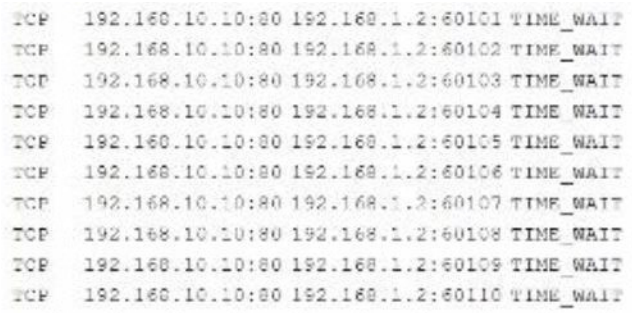
Correct Answer: B

QUESTION 352
A company wants to deploy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describe these systems?

A. DNS sinkholes
B. Honepots
C. Virtual machines
D. Neural network

Correct Answer: A

QUESTION 353
A security analyst is reviewing the following output from a system:



Which of the following is MOST likely being observed?

A. ARP palsoning
B. Man in the middle
C. Denial of service
D. DNS poisoning

Correct Answer: C

QUESTION 354
When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

Correct Answer: D

QUESTION 355
Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing
B. Salting
C. Integrity
D. Digital signature

Correct Answer: A
Explanation:
https://www.digitalocean.com/community/tutorials/how-to-verify-downloaded-files

Confidentiality = Encryption
Integrity = Hashing
Availability = Redundancy/Resilience

QUESTION 356
A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Choose two.)

A. The order of volatility

B. ACRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

Correct Answer: AE

QUESTION 357
A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents. Which of the following backup types should be used?

A. Snapshot
B. Differential
C. Cloud
D. Full
E. Incremental

Correct Answer: A

QUESTION 358
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.

Correct Answer: D

QUESTION 359
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework

Correct Answer: D

QUESTION 360
A security analyst has been asked by the Chief Information Security Officer to:

- develop a secure method of providing centralized management of infrastructure
- reduce the need to constantly replace aging end user machines
- provide a consistent user desktop experience

Which of the following BEST meets these requirements?

A. BYOD
B. Mobile device management
C. VDI
D. Containerization

Correct Answer: B

QUESTION 361
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.

Correct Answer: B

QUESTION 362
An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model. Which of the following BEST describes the configurations the attacker exploited?

A. Weak encryption
B. Unsecure protocols
C. Default settings
D. Open permissions

Correct Answer: C

QUESTION 363
A website developer who is concerned about theft of the company's user database warns to protect weak passwords from offline brute-force attacks. Which of the following be the BEST solution?

A. Lock accounts after five failed logons
B. Precompute passwords with rainbow tables
C. Use a key-stretching technique
D. Hash passwords with the MD5 algorithm

Correct Answer: A

QUESTION 364
A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely