CompTIA

CAS-003 Exam

CompTIA Advanced Security Practitioner Exam

Thank you for Downloading CAS-003 exam PDF Demo

You can also Buy our CAS-003 Premium Full Version

https://www.certkillers.net/Exam/CAS-003

Version: 12.0

Question: 1

A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.
Which of the following is the BEST solution?

A. Use an entropy-as-a-service vendor to leverage larger entropy pools.
B. Loop multiple pseudo-random number generators in a series to produce larger numbers.
C. Increase key length by two orders of magnitude to detect brute forcing.
D. Shift key generation algorithms to ECC algorithms.

Answer: A

Question: 2

A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

Question: 3

A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

Answer: A

Question: 4

The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.
Which of the following BEST meets the needs of the board?

A. KRI:- Compliance with regulations- Backlog of unresolved security investigations- Severity of threats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basisKPI:- Time to resolve open security items- % of suppliers with approved security control frameworks- EDR coverage across the fleet- Threat landscape rating
B. KRI:- EDR coverage across the fleet- Backlog of unresolved security investigations- Time to patch critical issues on a monthly basis- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors
C. KRI:- EDR coverage across the fleet- % of suppliers with approved security control framework- Backlog of unresolved security investigations- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations- Time to patch critical issues on a monthly basis- Severity of threats and vulnerabilities reported by sensors
D. KPI:- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors- Threat landscape ratingKRI:- Time to resolve open security items- Backlog of unresolved security investigations- EDR coverage across the fleet- Time to patch critical issues on a monthly basis

Answer: A

Question: 5

The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.
Which of the following would be the MOST cost-effective solution to meet the company's needs?

A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
D. Hire an experienced, full-time information security team to run the startup company's information

security department.

Answer: C

Question: 6

As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

A. the collection of data as part of the continuous monitoring program.
B. adherence to policies associated with incident response.
C. the organization's software development life cycle.
D. changes in operating systems or industry trends.

Answer: A

Question: 7

A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

A. Custom firmware with rotating key generation
B. Automatic MITM proxy
C. TCP beacon broadcast software
D. Reverse shell endpoint listener

Answer: B

Question: 8

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder
Torrentz

My TAX.xls
Consultancy HR Manual.doc
Camera: SM-G950F
Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

A. MicroSD in not encrypted and also contains personal data.
B. MicroSD contains a mixture of personal and work data.
C. MicroSD in not encrypted and contains geotagging information.
D. MicroSD contains pirated software and is not encrypted.

Answer: A

Question: 9

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:
Access to a number of applications, including internal websites
Access to database data and the ability to manipulate it
The ability to log into Linux and Windows servers remotely
Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

A. VTC
B. VRRP
C. VLAN
D. VDI
E. VPN
F. Telnet

Answer: D,E

Question: 10

A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

A. SaaS
B. PaaS
C. IaaS
D. Hybrid cloud
E. Network virtualization

Answer: B

Question: 11

During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories
B. Security requirements traceability matrix
C. Software development lifecycle
D. Data design diagram
E. Roles matrix
F. Implementation guide

Answer: F

Question: 12

An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security
B. Rogue device detection
C. Bluetooth
D. GPS

Answer: D

Question: 13

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

A. Reconfigure the firewall to block external UDP traffic.
B. Establish a security baseline on the IDS.

C. Block echo reply traffic at the firewall.
D. Modify the edge router to not forward broadcast traffic.

Answer: B

Question: 14

An administrator is working with management to develop policies related to the use of the cloud-based resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?
A. MDM
B. Sandboxing
C. Mobile tokenization
D. FDE
E. MFA

Answer: A

Question: 15

Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company. Which of the following should the systems administrator do to BEST address this problem?

A. Add an ACL to the firewall to block VoIP.
B. Change the settings on the phone system to use SIP-TLS.
C. Have the phones download new configurations over TFTP.
D. Enable QoS configuration on the phone VLAN.

Answer: B

Question: 16

A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:
TCP 80 open
TCP 443 open
TCP 1434 filtered
The penetration tester then used a different tool to make the following requests:
GET / script/login.php?token=45$MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF
Which of the following tools did the penetration tester use?

A. Protocol analyzer
B. Port scanner
C. Fuzzer
D. Brute forcer
E. Log analyzer
F. HTTP interceptor

Answer: C

Question: 17

A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.
Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.
B. Research industry best practices and latest RFCs.
C. Undertake an external vulnerability scan and penetration test.
D. Conduct a threat modeling exercise.

Answer: D

Question: 18

In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.
Which of the following strategies should the engineer recommended be approved FIRST?

A. Avoid
B. Mitigate
C. Transfer
D. Accept

Answer: B

Question: 19

A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.
Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

A. Install and configure an IPS.
B. Enforce routine GPO reviews.
C. Form and deploy a hunt team.
D. Institute heuristic anomaly detection.
E. Use a protocol analyzer with appropriate connectors.

Answer: A,D

Question: 20

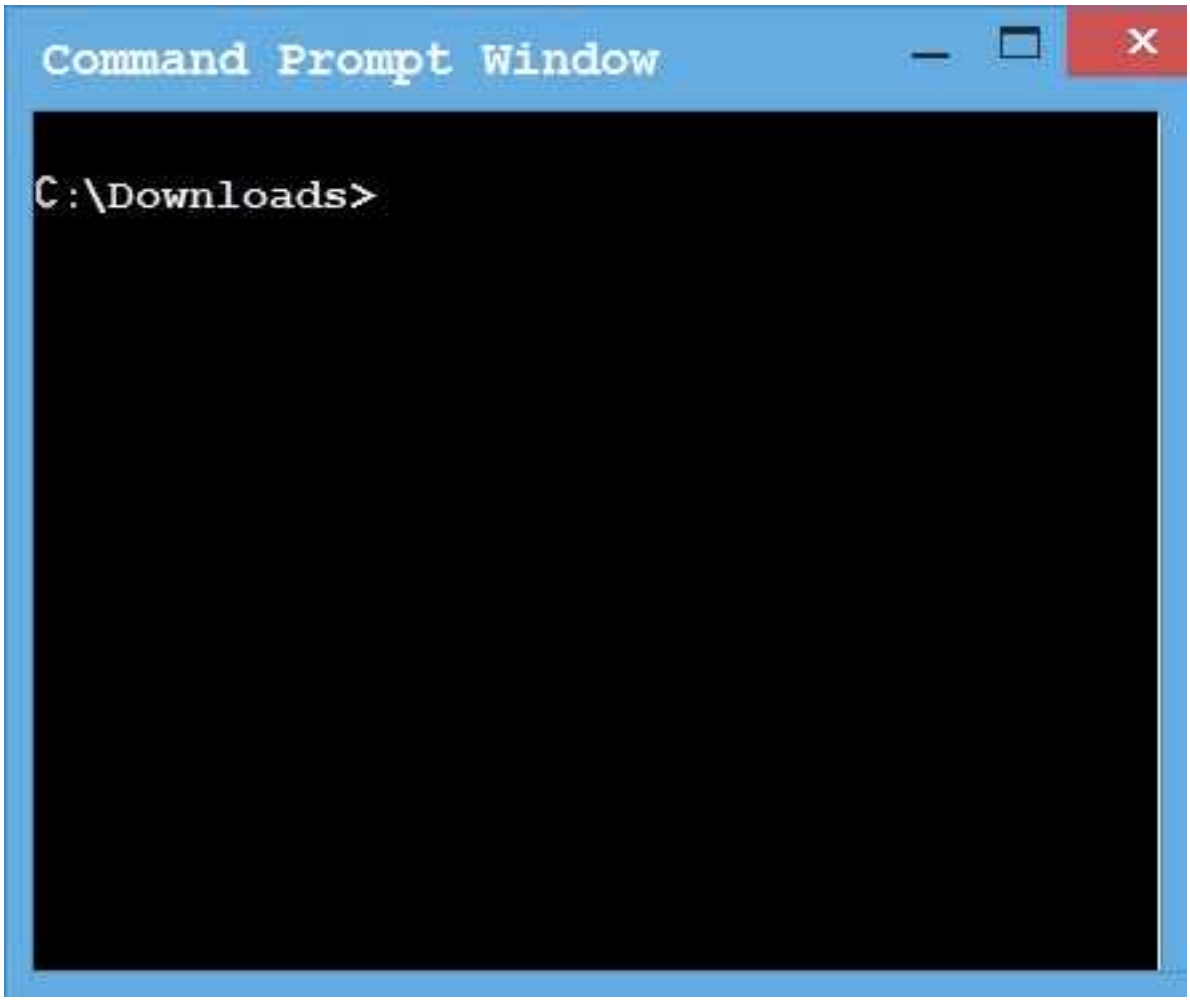
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.
Which of the following procedures should the security responder apply to the situation? (Choose two.)

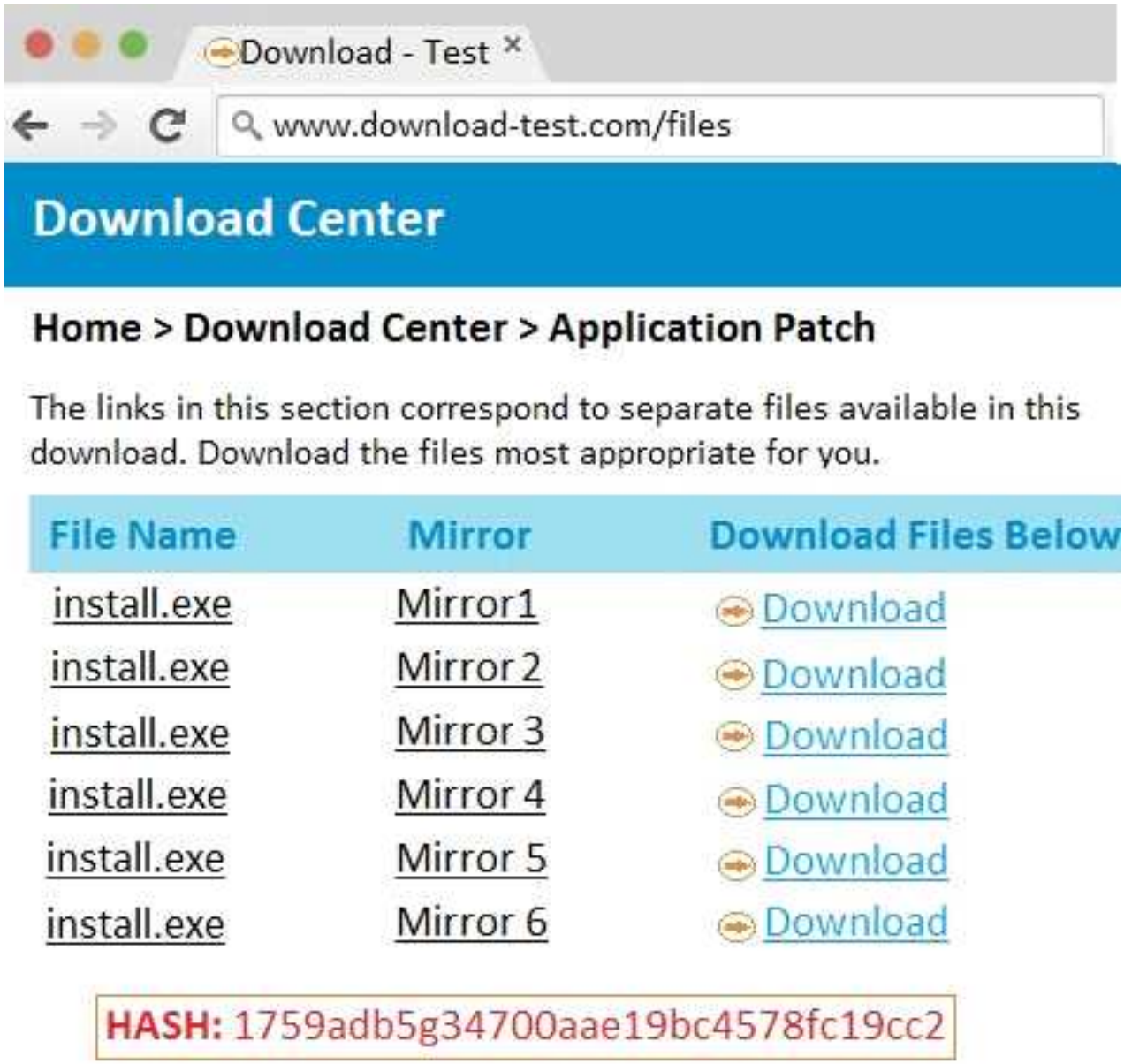
A. Contain the server.
B. Initiate a legal hold.
C. Perform a risk assessment.
D. Determine the data handling standard.
E. Disclose the breach to customers.
F. Perform an IOC sweep to determine the impact.

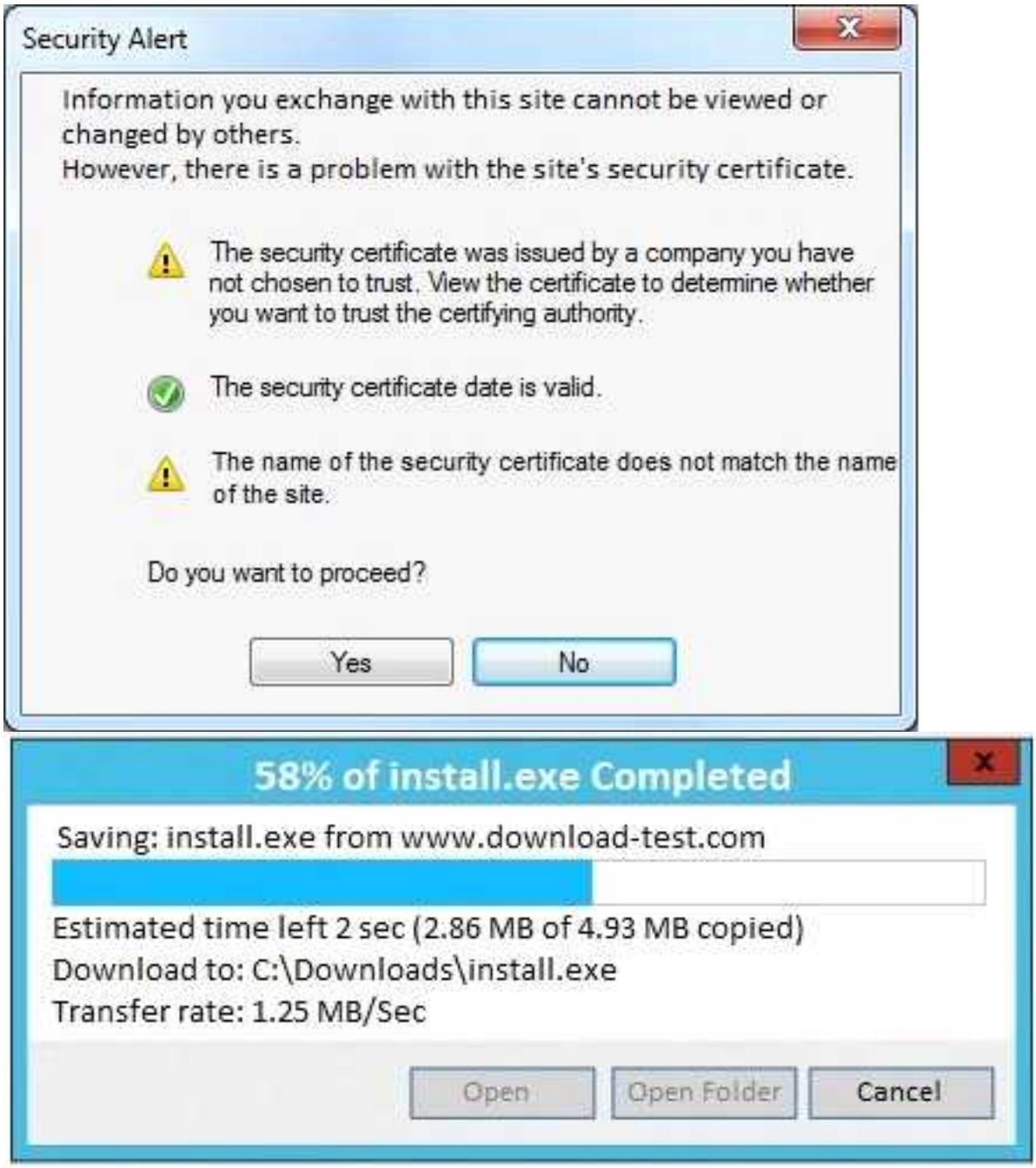
Answer: B,F

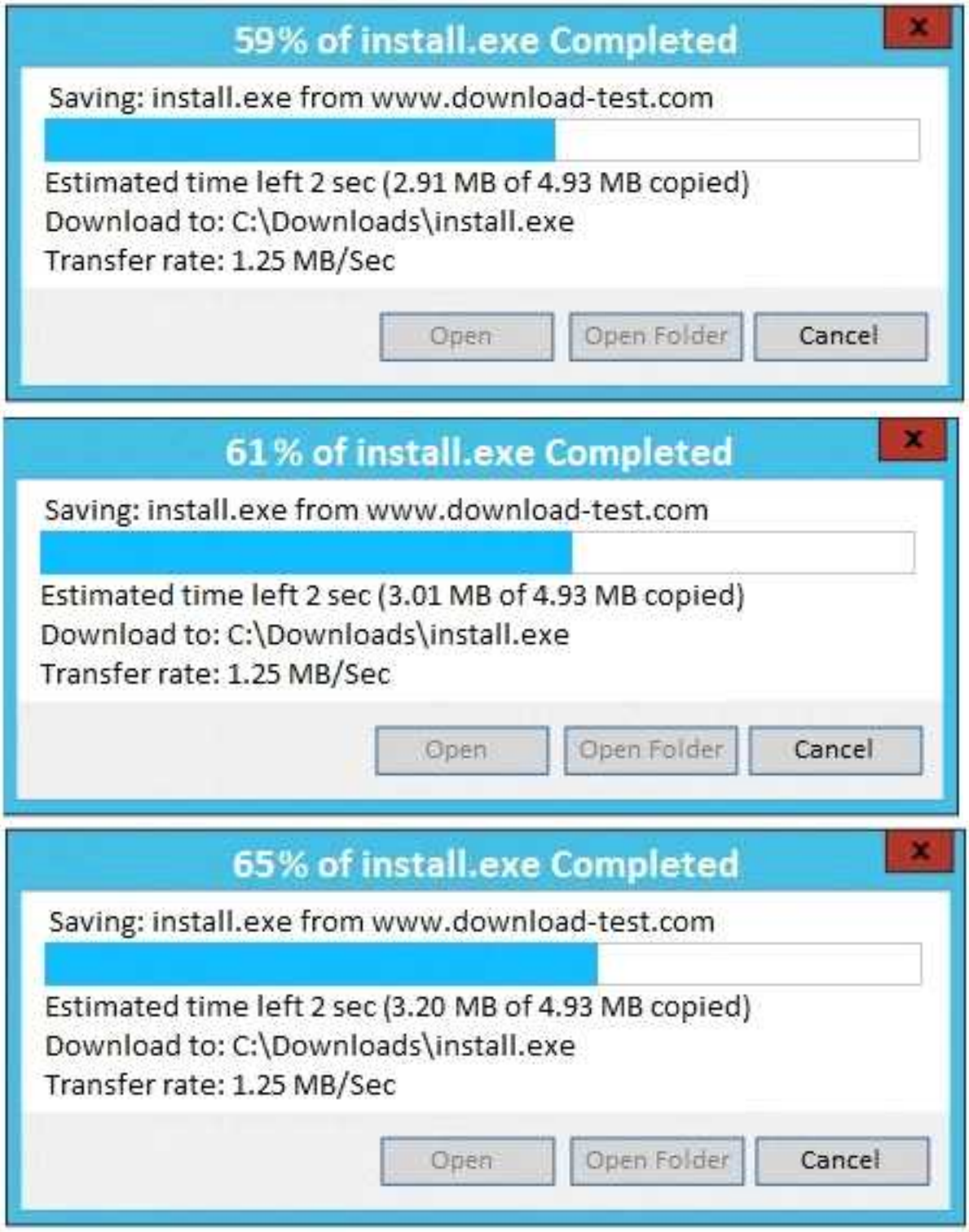
Question: 21

An administrator wants to install a patch to an application.
INSTRUCTIONS
Given the scenario, download, verify, and install the patch in the most secure manner.
The last install that is completed will be the final submission.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Command Prompt Window
C:\Downloads>


Download - Test
www.download-test.com/files
Download Center
Home > Download Center > Application Patch
The links in this section correspond to separate files available in this download. Download the files most appropriate for you.
File Name
Mirror
Download Files Below
install.exe
Mirror1
Download
install.exe
Mirror 2
Download
install.exe
Mirror 3
Download
install.exe
Mirror 4
Download
install.exe
Mirror 5
Download
install.exe
Mirror 6
Download
HASH: 1759adb5g34700aae19bc4578fc19cc2

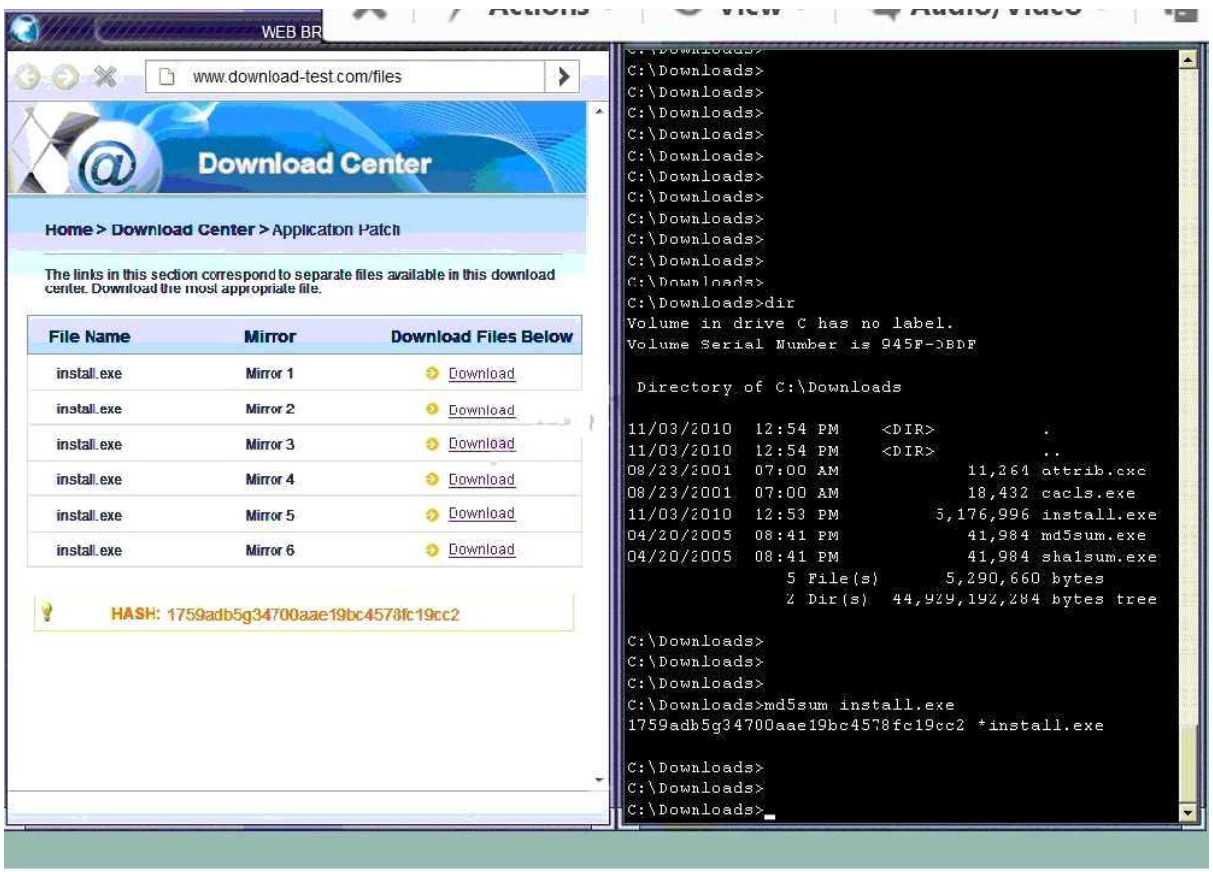

Security Alert
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name of the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No
58% of install.exe Completed
Saving: install.exe from www.download-test.com
Estimated time left 2 sec (2.86 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec
Open
Open Folder
Cancel



A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:

Since we need to do this in the most secure manner possible, they should not be used.Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



Finally, type in install.exe to install it and make sure there are no signature verification errors.

B. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown.

Since we need to do this in the most secure manner possible, they should not be used.Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.
Finally, type in install.exe to install it and make sure there are no signature verification errors.

Answer: A

Question: 22

DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	
Collection of organizations in the same industry vertical developing services based on a common application stack	
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	
Marketing organization that outsources email delivery to An online provider	
Organization that has migrated their highly customized external websites into the cloud	

Answer:

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS | Community cloud with PaaS | Community cloud with SaaS | Hybrid cloud

Private cloud with IaaS | Private cloud with PaaS | Private cloud with SaaS | Public cloud with IaaS

Public cloud with PaaS | Public cloud with SaaS

Question: 23

DRAG DROP
A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.

Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos	oAuth
OTP	SAML

Answer:

Answer: B

Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	oAuth
Authentication to cloud-based corporate portals will feature single sign-on	SAML
Any infrastructure portal will require time-based authentication	OTP
Customers will have delegated access to multiple digital services	Kerberos

Question: 24

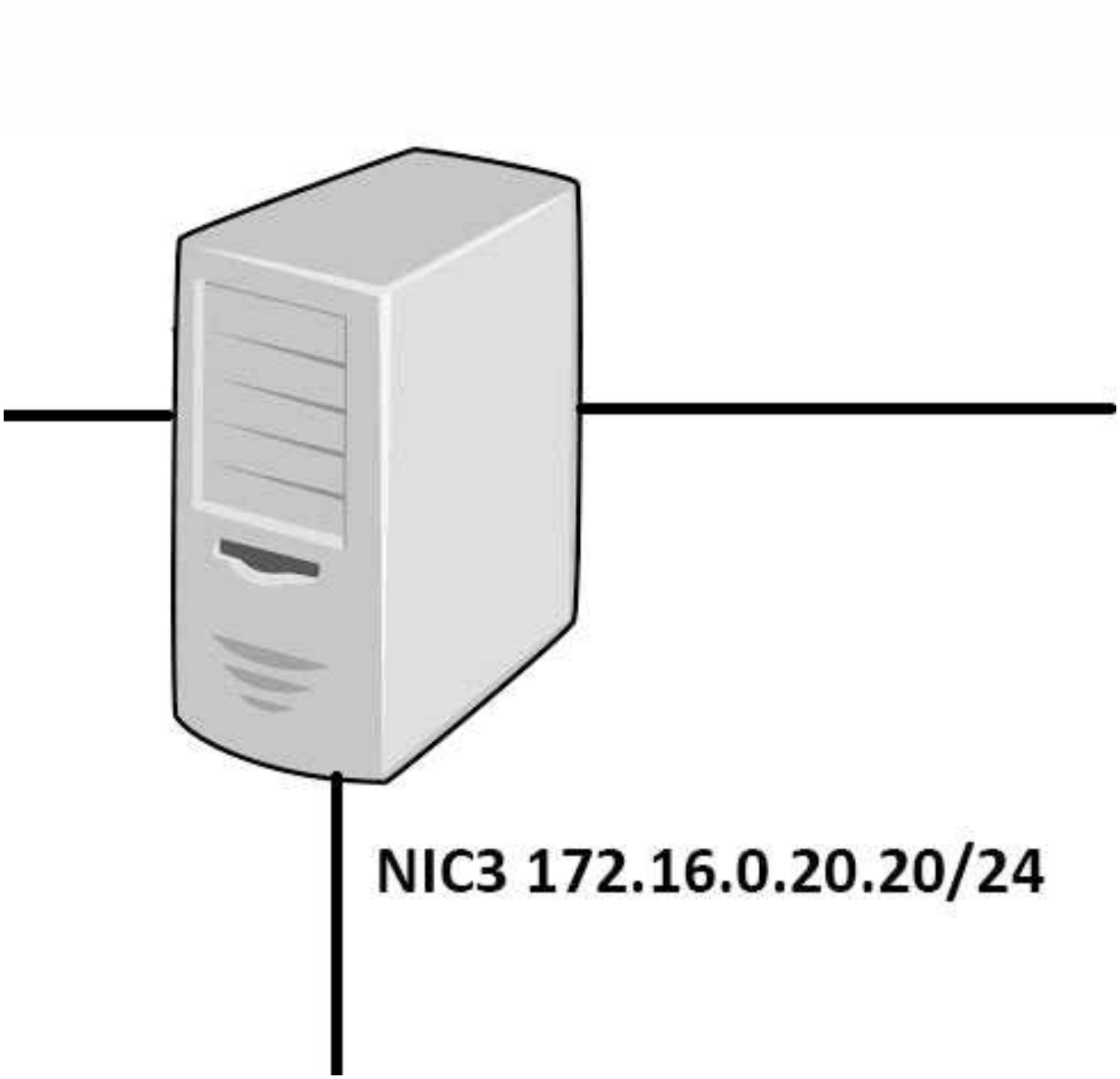
An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:
1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location
The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

A. Develop a security exemption, as it does not meet the security policies
B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
C. Require the solution owner to accept the identified risks and consequences
D. Review the entire procurement process to determine the lessons learned

Answer: C

Question: 25

DRAG DROP
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.


NIC3 172.16.0.20.20/24

The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should ot initiate outbound connections on NIC2

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389	Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Deny IP from ANY to ANY	Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

Answer:

The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network — Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1 — Permit UDP from 192.168.1.20 to 172.30.10.3

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network — Permit IP from 172.30.10.3 to 192.168.1.20

The DB server should ot initiate outbound connections on NIC2 — Deny IP from 10.0.10.20 to ANY

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434		
Deny TCP from 10.0.10.20/24 to ANY	Deny IP from ANY to ANY	Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434		

Question: 26

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:
The data is for internal consumption only and shall not be distributed to outside individuals
The systems administrator should not have access to the data processed by the server
The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)
A. SELinux
B. DLP
C. HIDS
D. Host-based firewall
E. Measured boot
F. Data encryption
G. Watermarking

Answer: C,E,F

Question: 27

An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

A. Secure storage policies
B. Browser security updates
C. Input validation
D. Web application firewall
E. Secure coding standards
F. Database activity monitoring

Answer: C,F

Question: 28

A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

A. ISA
B. BIA
C. SLA

D. RA

Answer: C

Question: 29

Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
 Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
 IPv4 Address................ : 172.30.0.28
 Subnet Mask................. : 255.255.0.0
 Default Gateway............. : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

A. Allow 172.30.0.28:80 -> ANY
B. Allow 172.30.0.28:80 -> 172.30.0.0/16
C. Allow 172.30.0.28:80 -> 172.30.0.28:443
D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

Question: 30

A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues
B. Posing as a copier service technician and indicating the equipment had “phoned home” to alert the technician for a service call
C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed
D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

Answer: A

Thank You for trying CAS-003 PDF Demo

To Buy our CAS-003 Premium Full Version visit link below

https://www.certkillers.net/Exam/CAS-003

Start Your CAS-003 Preparation

“”

Download and Pass Exam CAS-003 Easily with CertKillers.net questions.