



Vendor: CompTIA

Exam Code: CAS-001

Exam Name: CompTIA Advanced Security Practitioner

Version: DEMO

Updated 6 Lab Simulator Questions

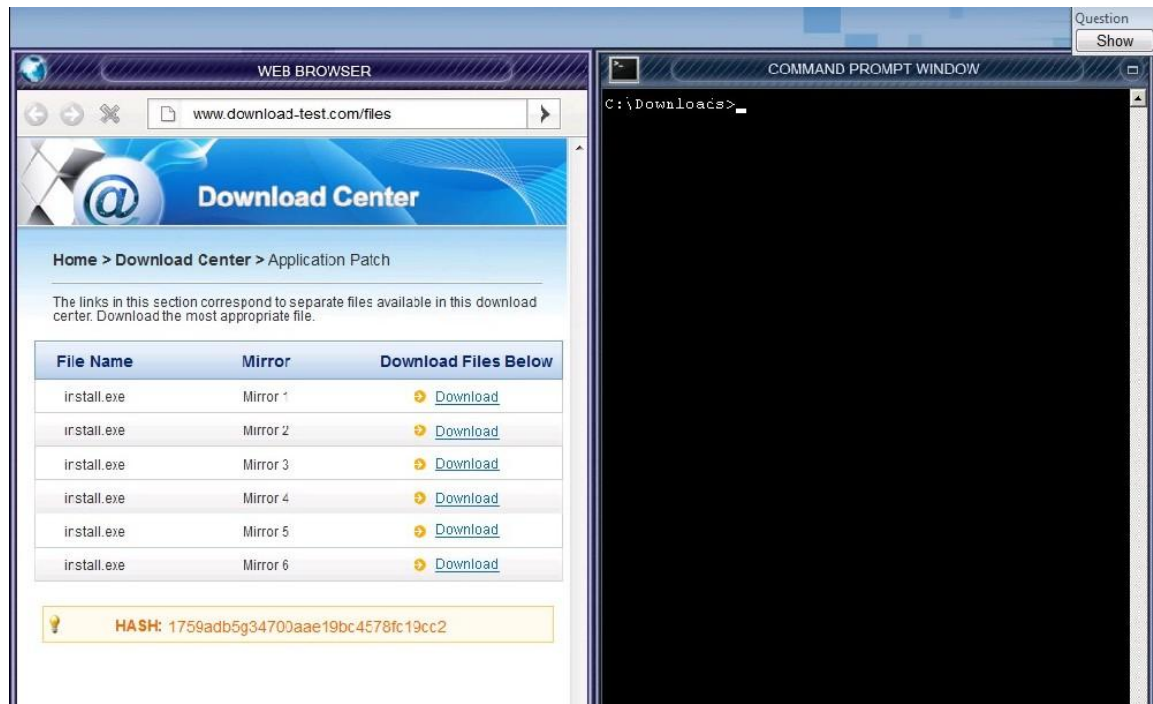
QUESTION 1

Lab Simulation

An administrator wants to install a patch to an application.

Given the scenario, download, verify and install the patch in the most secure manner.

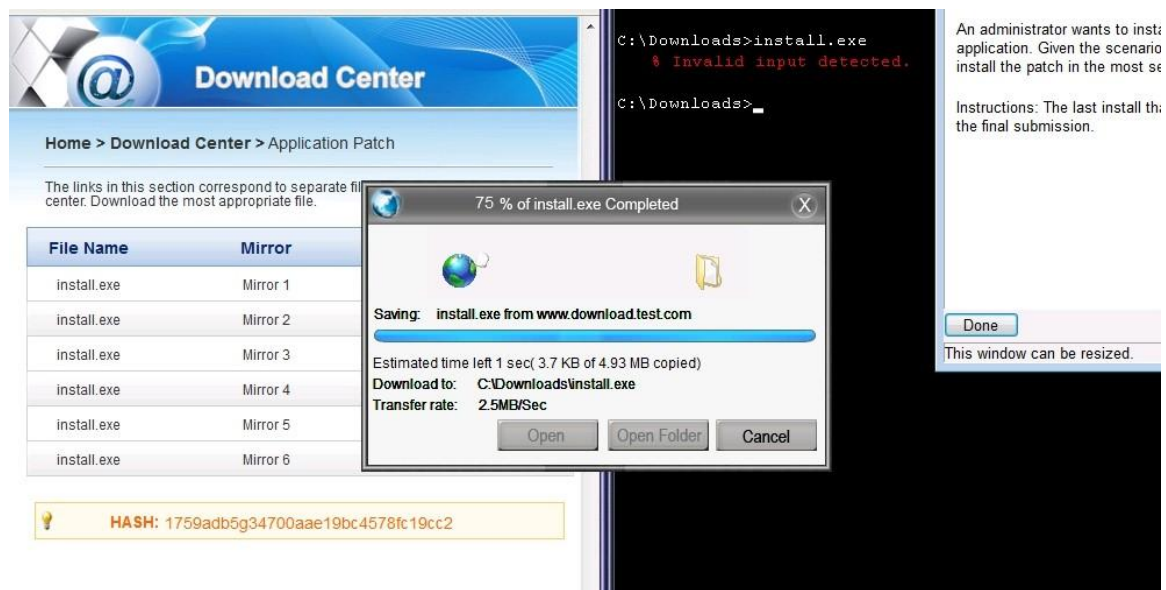
Instructions The last install that is completed will be the final submission

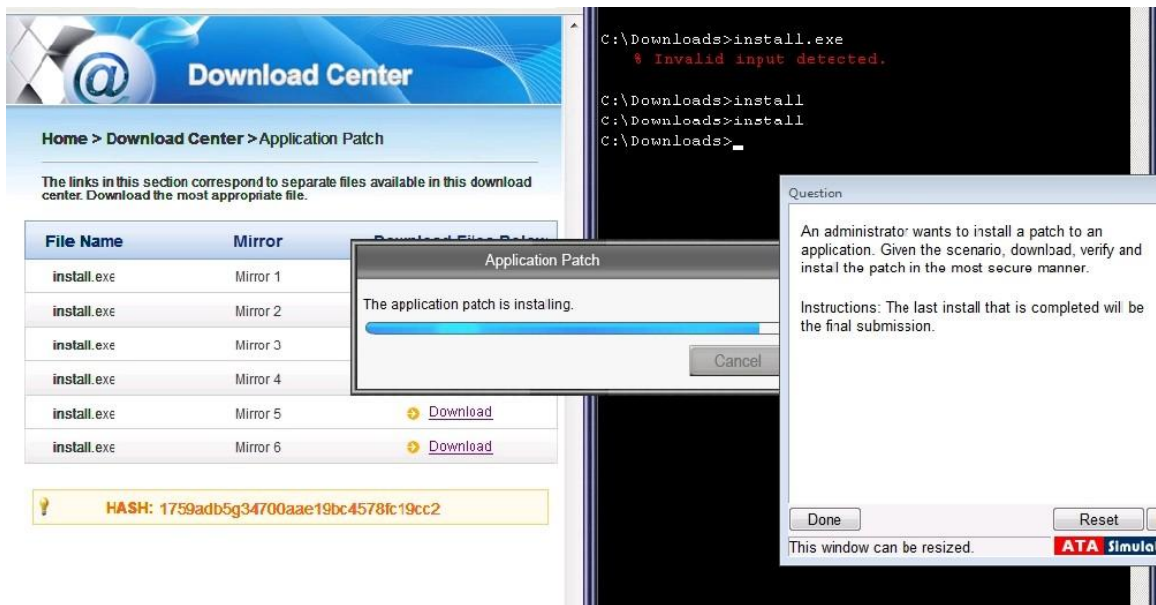
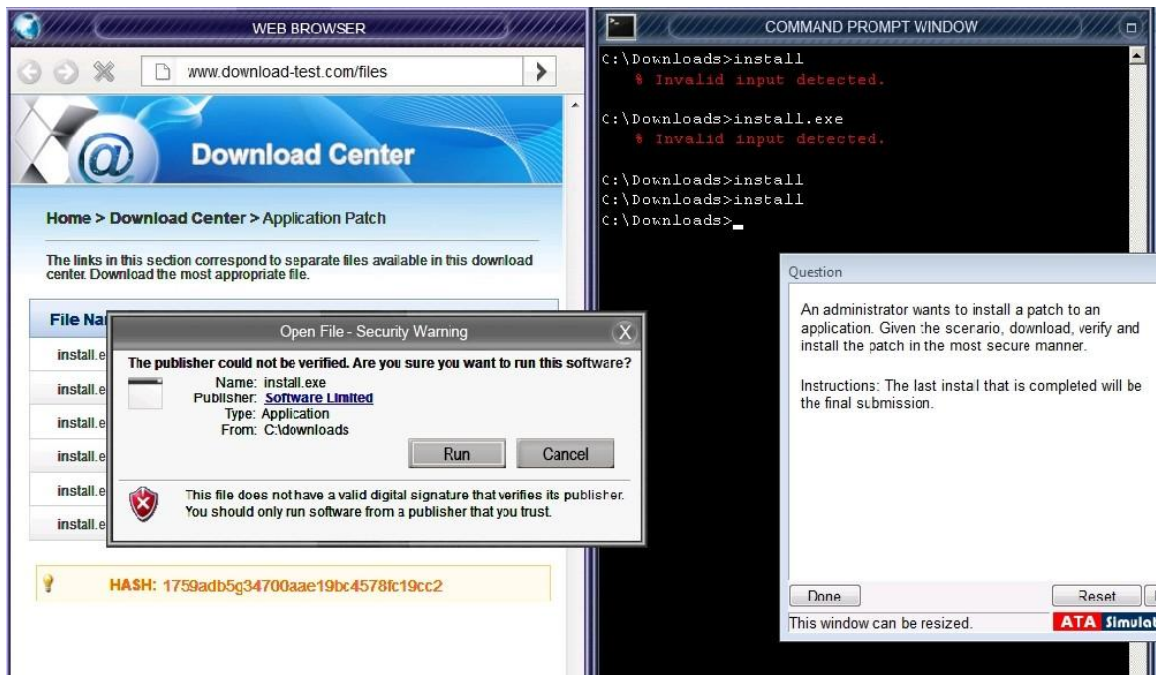


Answer:

You need to check the hash value of download software with md5 utility.

Check the below images for more details:





QUESTION 2

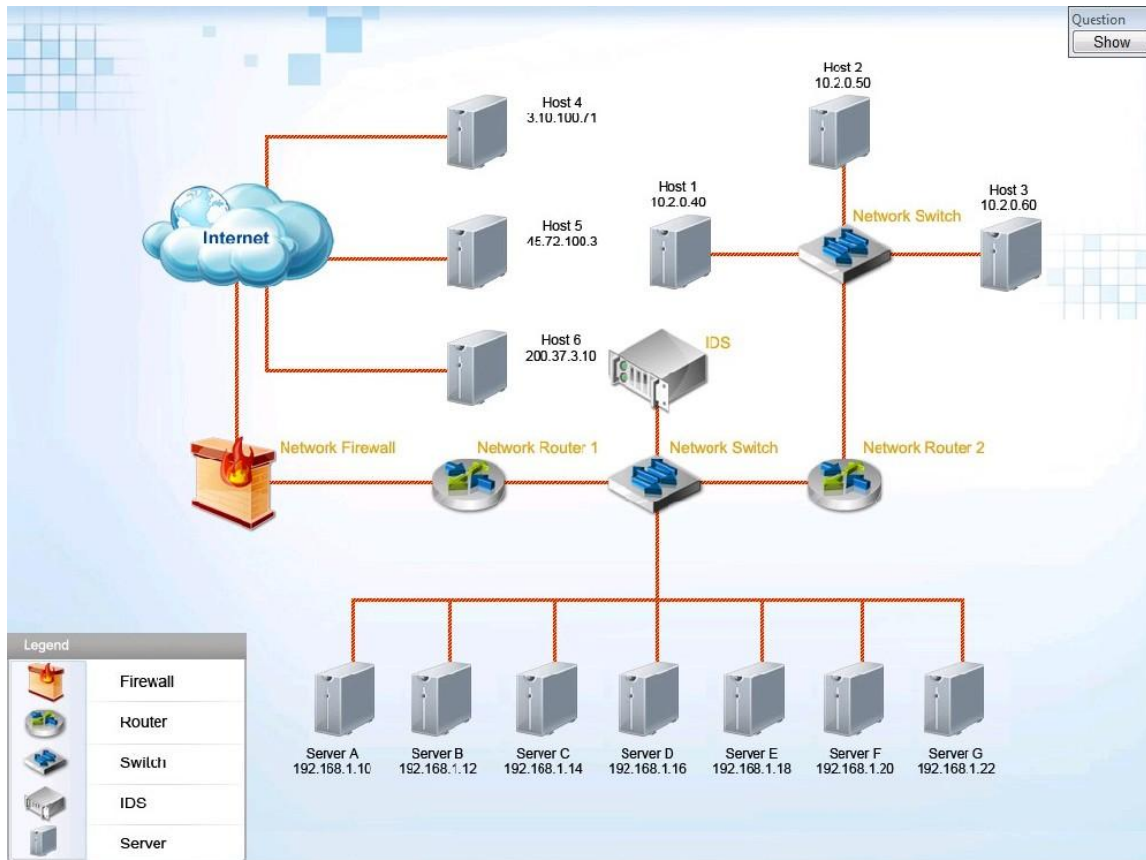
Lab Simulation

The IDS has detected abnormal behavior on this network Click on the network devices to view device information Based on this information, the following tasks need to be completed:

1. Select the server that is a victim of a SQL injection attack.
2. Select the source of the buffer overflow attack.

3. Modify the access control list (ACL) on the router(s) to ONLY block the buffer overflow attack.

Instructions: Simulations can be reset at any time to the initial state: however, all selections will be deleted.



Answer: You can see the answer from our Full Version

QUESTION 2

A company has been purchased by another agency and the new security architect has identified new security goals for the organization. The current location has video surveillance throughout the building and entryways. The following requirements must be met:

1. Ability to log entry of all employees in and out of specific areas
2. Access control into and out of all sensitive areas
3. Two-factor authentication

Which of the following would MOST likely be implemented to meet the above requirements and provide a secure solution? (Select TWO).

- A. Proximity readers
- B. Visitor logs
- C. Biometric readers
- D. Motion detection sensors
- E. Mantrap

Answer: AC

QUESTION 3

During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40% of the desktops do not meet requirements. Which of the following is the cause of the noncompliance?

- A. The devices are being modified and settings are being overridden in production.
- B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
- C. The desktop applications were configured with the default username and password.
- D. 40% of the devices have been compromised.

Answer: A

QUESTION 4

Which of the following does SAML use to prevent government auditors or law enforcement from identifying specific entities as having already connected to a service provider through an SSO operation?

- A. Transient identifiers
- B. Directory services
- C. Restful interfaces
- D. Security bindings

Answer: A

QUESTION 5

In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

- A. Provide free email software for personal devices.
- B. Encrypt data in transit for remote access.
- C. Require smart card authentication for all devices
- D. Implement NAC to limit insecure devices access.
- E. Enable time of day restrictions for personal devices.

Answer: BD

QUESTION 6

Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for

the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies.

Which of the following solutions is BEST suited for this scenario?

- A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
- B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
- C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.
- D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Answer: C

QUESTION 7

Warehouse users are reporting performance issues at the end of each month when trying to access cloud applications to complete their end of the month financial reports.

They have no problem accessing those applications at the beginning of the month.

Network information:

DMZ network - 192.168.5.0/24
VPN network - 192.168.1.0/24
Datacenter - 192.168.2.0/24
User network - 192.168.3.0/24
HR network - 192.168.4.0/24
Warehouse network - 192.168.6.0/24
Finance network - 192.168.7.0/24

Traffic shaper configuration:

VLAN Bandwidth limit (Mbps)
VPN50
User175
HR220
Finance230
Warehouse75
Guest50

External firewall allows all networks to access the Internet.

Internal Firewall Rules:

ActionSourceDestination
Permit192.168.1.0/24192.168.2.0/24
Permit192.168.1.0/24192.168.3.0/24
Permit192.168.1.0/24192.168.5.0/24
Permit192.168.2.0/24192.168.1.0/24
Permit192.168.3.0/24192.168.1.0/24
Permit192.168.5.0/24192.168.1.0/24
Permit192.168.4.0/24192.168.7.0/24
Permit192.168.7.0/24192.168.4.0/24
Permit192.168.7.0/24any
Deny192.168.4.0/24any

Deny192.168.1.0/24192.168.4.0/24
Denyanyany

Which of the following restrictions is the MOST likely cause?

- A. Bandwidth limit on the traffic shaper for the finance department
- B. Proxy server preventing the warehouse from accessing cloud applications
- C. Deny statements in the firewall for the warehouse network
- D. Bandwidth limit on the traffic shaper for the warehouse department

Answer: D

QUESTION 8

A university Chief Information Security Officer is analyzing various solutions for a new project involving the upgrade of the network infrastructure within the campus. The campus has several dorms (two-four person rooms) and administrative buildings. The network is currently setup to provide only two network ports in each dorm room and ten network ports per classroom. Only administrative buildings provide 2.4 GHz wireless coverage.

The following three goals must be met after the new implementation:

1. Provide all users (including students in their dorms) connections to the Internet.
2. Provide IT department with the ability to make changes to the network environment to improve performance.
3. Provide high speed connections wherever possible all throughout campus including sporting event areas.

Which of the following risk responses would MOST likely be used to reduce the risk of network outages and financial expenditures while still meeting each of the goals stated above?

- A. Avoid any risk of network outages by providing additional wired connections to each user and increasing the number of data ports throughout the campus.
- B. Transfer the risk of network outages by hiring a third party to survey, implement and manage a 5.0 GHz wireless network.
- C. Accept the risk of possible network outages and implement a WLAN solution to provide complete 5.0 GHz coverage in each building that can be managed centrally on campus.
- D. Mitigate the risk of network outages by implementing SOHO WiFi coverage throughout the dorms and upgrading only the administrative buildings to 5.0 GHz coverage using a one for one AP replacement.

Answer: C

QUESTION 9

A security auditor is conducting an audit of a corporation where 95% of the users travel or work from non-corporate locations a majority of the time. While the employees are away from the corporate offices, they retain full access to the corporate network and use of corporate laptops. The auditor knows that the corporation processes PII and other sensitive data with applications requiring local caches of any data being manipulated.

Which of the following security controls should the auditor check for and recommend to be implemented if missing from the laptops?

- A. Trusted operating systems

- B. Full disk encryption
- C. Host-based firewalls
- D. Command shell restrictions

Answer: B

QUESTION 10

Part of the procedure for decommissioning a database server is to wipe all local disks, as well as SAN LUNs allocated to the server, even though the SAN itself is not being decommissioned. Which of the following is the reason for wiping the SAN LUNs?

- A. LUN masking will prevent the next server from accessing the LUNs.
- B. The data may be replicated to other sites that are not as secure.
- C. Data remnants remain on the LUN that could be read by other servers.
- D. The data is not encrypted during transport.

Answer: C

QUESTION 11

Which of the following BEST describes the implications of placing an IDS device inside or outside of the corporate firewall?

- A. Placing the IDS device inside the firewall will allow it to monitor potential internal attacks but may increase the load on the system.
- B. Placing the IDS device outside the firewall will allow it to monitor potential remote attacks while still allowing the firewall to block the attack.
- C. Placing the IDS device inside the firewall will allow it to monitor potential remote attacks but may increase the load on the system.
- D. Placing the IDS device outside the firewall will allow it to monitor potential remote attacks but the firewall will not be able to block the attacks.

Answer: B

QUESTION 12

At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning.

Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

- A. Add guests with more memory to increase capacity of the infrastructure.
- B. A backup is running on the thin clients at 9am every morning.
- C. Install more memory in the thin clients to handle the increased load while booting.
- D. Booting all the lab desktops at the same time is creating excessive I/O.
- E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
- F. Install faster SSD drives in the storage system used in the infrastructure.
- G. The lab desktops are saturating the network while booting.
- H. The lab desktops are using more memory than is available to the host systems.

Answer: DF

QUESTION 13

A security administrator is shown the following log excerpt from a Unix system:

```
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from
198.51.100.23 port 37914 ssh2
2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from
198.51.100.23 port 37915 ssh2
2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from
198.51.100.23 port 37916 ssh2
2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from
198.51.100.23 port 37918 ssh2
2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from
198.51.100.23 port 37920 ssh2
2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from
198.51.100.23 port 37924 ssh2
```

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

- A. An authorized administrator has logged into the root account remotely.
- B. The administrator should disable remote root logins.
- C. Isolate the system immediately and begin forensic analysis on the host.
- D. A remote attacker has compromised the root account using a buffer overflow in sshd.
- E. A remote attacker has guessed the root password using a dictionary attack.
- F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
- G. A remote attacker has compromised the private key of the root account.
- H. Change the root password immediately to a password not found in a dictionary.

Answer: CE

QUESTION 14

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch.

Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

- A. Code review
- B. Sandbox
- C. Local proxy
- D. Fuzzer
- E. Web vulnerability scanner

Answer: CD

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14