Vendor: CompTIA

Exam Code:SY0-501

Exam Name: CompTIA Security+ Certification Exam

Version: Demo

QUESTION 1

DRAG DROP

An attack has occurred against a company.

INSTRUCTIONS

You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker\\'s tablet and reviewing the output. (Answer Area 1)

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server. (Answer area 2) All objects will be used, but not all placeholders may be

filled. Objects may only be used once. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
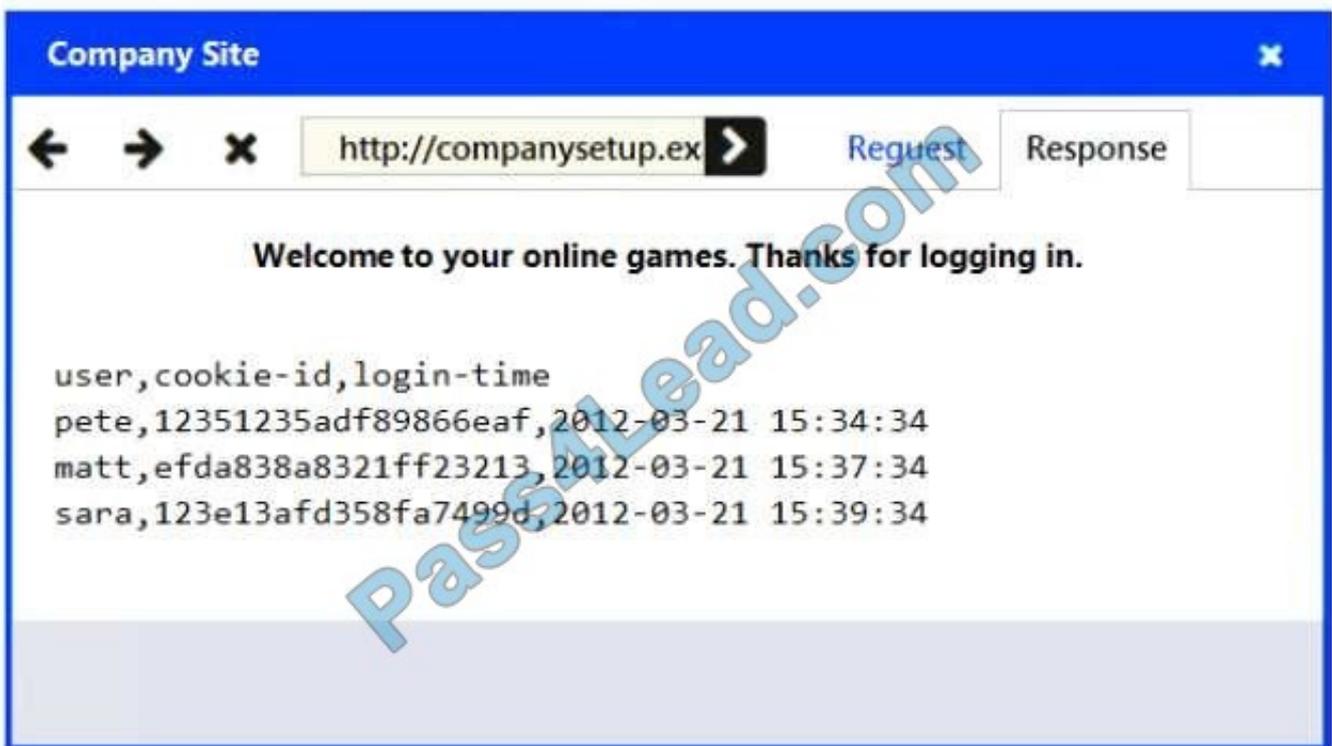
Company Site

http://companysetup.ex ›   Request   Response

Welcome to your online games. Thanks for logging in.

```
user,cookie-id,login-time
pete,12351235adf89866eaf,2012-03-21 15:34:34
matt,efda838a8321ff23213,2012-03-21 15:37:34
sara,123e13afd358fa7499d,2012-03-21 15:39:34
```
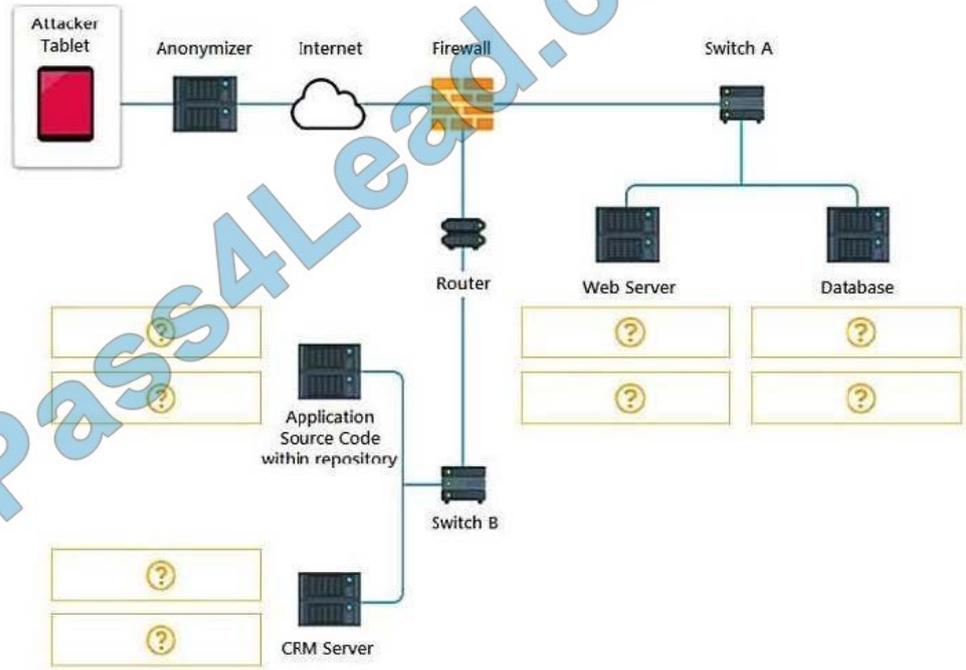
Select and Place:

Answer Area 1

SQL Injection

Cross Site Scripting

XML Injection

Session Hijacking

Type of attack

[?]

Answer Area 2

Input Validation

Code Review

WAF

URL Filtering

Record level access control

Attacker Tablet

Anonymizer   Internet   Firewall   Switch A

Router

Web Server   Database

[?]

[?]

[?]   [?]

[?]   [?]

Application Source Code within repository

Switch B

[?]

[?]

CRM Server

Correct Answer:

Answer Area 1

SQL Injection

XML Injection

Session Hijacking

Type of attack

Cross Site Scripting

Answer Area 2

Attacker Tablet — Anonymizer — Internet — Firewall — Switch A

Router

Web Server — Database

WAF — Input Validation

URL Filtering — ?

Application Source Code within repository

Switch B

Record level access control — ?

CRM Server
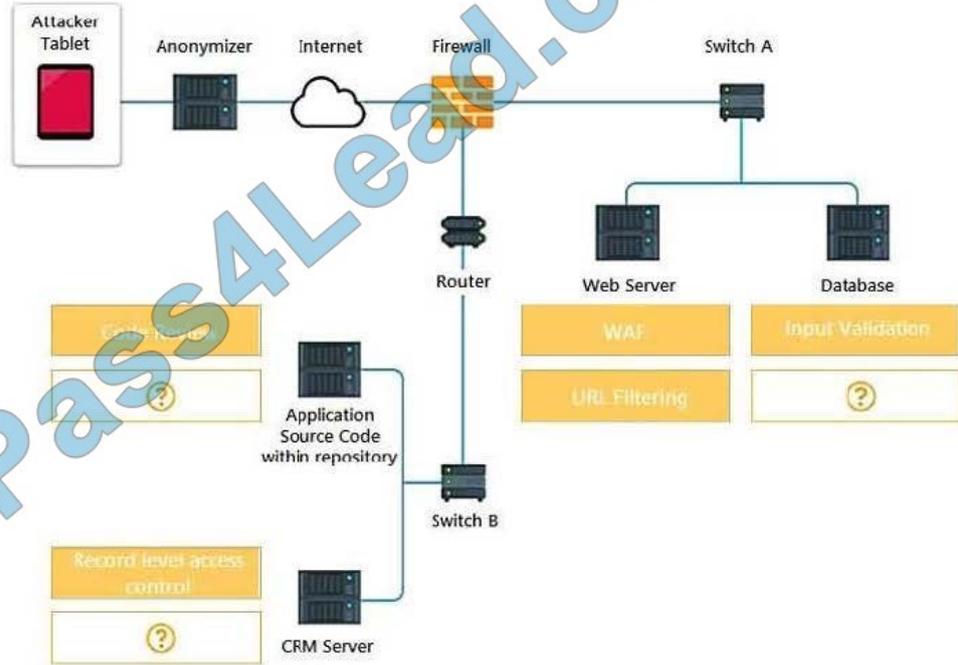
QUESTION 2

A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized. Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication

B. SSO

C. Biometrics

D. PKI

E. Federation

Correct Answer: B

QUESTION 3

A security analyst receives the following output:

Time	Action	Host	File Name	User
12/15/2017	Policy: Endpoint USB Transfer - Blocked	Host1	Q3-Financials.PDF	User1

Which of the following MOST likely occurred to produce this output?

A. The host-based firewall prevented an attack from a Trojan horse

B. USB-OTG prevented a file from being uploaded to a mobile device

C. The host DLP prevented a file from being moved off a computer

D. The firewall prevented an incoming malware-infected file

Correct Answer: C

QUESTION 4

A preventive control differs from a compensating control in that a preventive control is:

A. put in place to mitigate a weakness in a user control.

B. deployed to supplement an existing control that is EOL.

C. relied on to address gaps in the existing control structure.

D. designed to specifically mitigate a risk.

Correct Answer: C

QUESTION 5

Which of the following encryption algorithms require one encryption key? (Choose two.)

A. MD5

B. 3DES

C. BCRYPT

D. RC4

E. DSA

Correct Answer: BD

QUESTION 6

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

A. 53

B. 110

C. 143

D. 443

Correct Answer: A

QUESTION 7

The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

A. In-transit

B. In-use

C. Embedded

D. At-rest

Correct Answer: B

QUESTION 8

Which of the following authentication concepts is a gait analysis MOST closely associated?

A. Somewhere you are

B. Something you are

C. Something you do

D. Something you know

Correct Answer: C

QUESTION 9

An auditor requiring an organization to perform real-time validation of SSL certificates. Which of the following should the organization implement?

A. OCSP

B. CRL

C. CSR

D. KDC

Correct Answer: A

QUESTION 10

During a security audit of a company\\'s network, unsecure protocols were found to be in use. A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2

B. TLS1.2

C. SSL1.3

D. SNMPv3

Correct Answer: A

Product and Software: This article applies to all Aruba controllers and ArubaOS versions. The program Secure Shell (SSH) is a secure replacement for Telnet and the Berkeley r-utilities (rlogin, rsh, rcp, and rdist). SSH provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another. SSH provides strong host-to-host and user authentication as well as secure encrypted communications over an insecure internet.

SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, which is functionally similar to FTP, but is SSH2 encrypted.

SSH2 key authentication is a feature that Aruba Networks currently does not support and you need to use X509 certificates for authentication. SSH2 private keys can be converted to X509 cert format. Use the same private key to generate a certificate request and have the certificate signed by a valid CA. After the certificate is signed by the CA, it can be uploaded to the controller as \\'Public Cert\\' and used for SSH authentication.

QUESTION 11

Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap

B. Secure cabinet

C. Faraday cage

D. Safe

Correct Answer: C

QUESTION 12

A security analyst is performing a BIA.

The analyst notes that In a disaster, failover systems must be up and running within 30 minutes.

The failover systems must use backup data that Is no older than one hour Which of the following should the analyst include In the business continuity plan?

A. A maximum MTTR of 30 minutes

B. A maximum MTBF of 30 minutes

C. A maximum RTO of 60 minutes

D. A maximum RPO of 60 minutes

E. An SLA guarantee of 60 minutes

Correct Answer: E

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.