- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in June/2020)**

Visit Braindump2go and Download Full Version SY0-501 Exam Dumps

QUESTION 968
Which of the following reduces data integrity risk from an authorized user mistakenly entering the wrong data format or type on a web form?

A. Proper input handling
B. Strong encryption
C. Least privilege
D. Backups

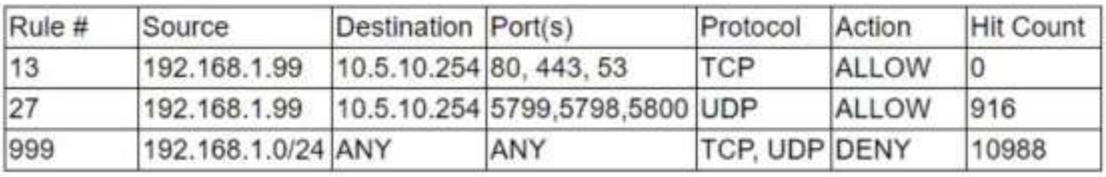
Answer: A

QUESTION 969
A security administrator is enhancing the security controls in an organization with respect to the allowed devices policy. The administrator wrote a . reg file with the code below:
HKEY_LOCAL_MACHINE\System\Current control set\Services\USBSTOR
"Start = dword :00000004
Which of the following BEST represents what the administrator is doing?

A. Changing the name of the USB port
B. Requiring USB device encryption
C. Upgrading the system to USB 3.0
D. Blocking the use of USB devices

Answer: D

QUESTION 970
After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:



Rule #	Source	Destination	Port(s)	Protocol	Action	Hit Count
13	192.168.1.99	10.5.10.254	80, 443, 53	TCP	ALLOW	0
27	192.168.1.99	10.5.10.254	5799,5798,5800	UDP	ALLOW	916
999	192.168.1.0/24	ANY	ANY	TCP, UDP	DENY	10988

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled.
B. The VLAN is not trunked properly.
C. There is a policy violation for DNS lookups.

D. The firewall policy is misconfigured.

Answer: D

QUESTION 971
A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the Internet?

A. VLAN
B. Air gap
C. NAT
D. Firewall

Answer: A

QUESTION 972
A security analyst is responsible for assessing the security posture of a new high-stakes application that is currently in the production environment but has not yet been made available to system users. Which of the following would provide the security analyst with the MOST comprehensive assessment of the application's ability to withstand unauthorized access attempts?

A. Dynamic analysis
B. Vulnerability scanning
C. Static code scanning
D. Stress testing

Answer: B

QUESTION 973
A technician is required to configure updates on a quest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots
B. Revert to known state
C. Rollback to known configuration
D. Shadow copy

Answer: A

QUESTION 974
A small contracting company's IT infrastructure enables the processing of various levels of sensitive data for which not all employees have access. However, the employees share physical office space. Which of the following controls would help reduce the risk of accidental spillage of sensitive, data?

A. Install screen filters.
B. Install cable locks for computers.
C. Use an IDS within the employees' offices
D. Segment the network into VLANs.
E. Implement a DLP solution.

Answer: E

QUESTION 975
Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicates an error.
B. The vendor has not published security patches recently.
C. The object has been removed from the Active Directory.
D. Logs show a performance degradation of the component

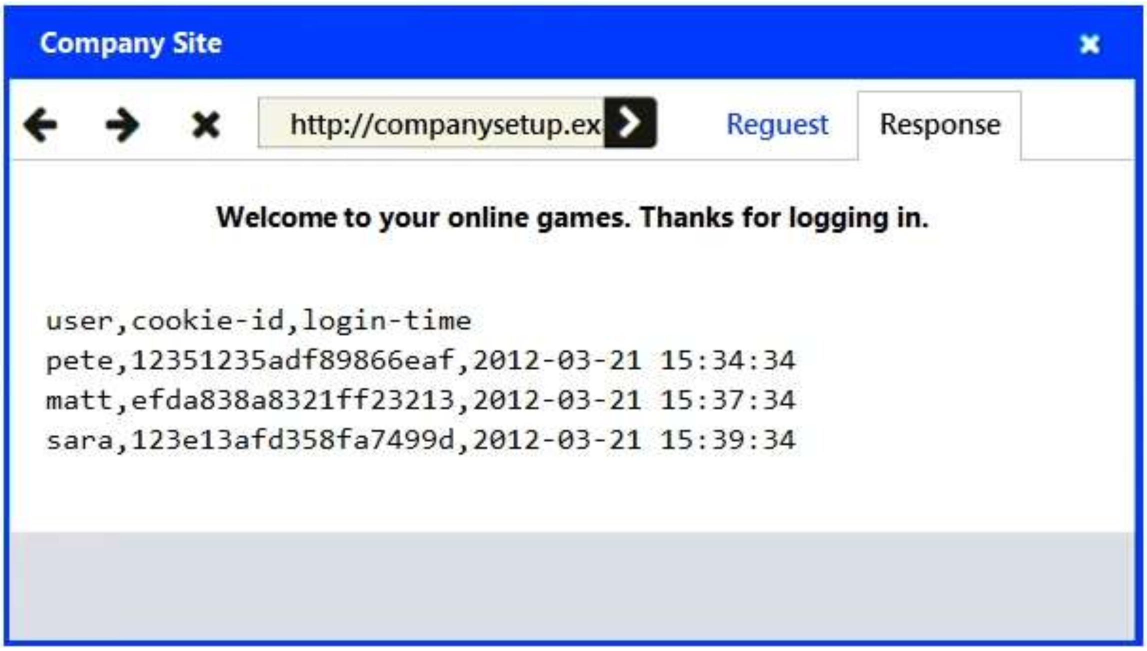
Answer: C

QUESTION 976
A forensic analyst needs to collect physical evidence that may be used in legal proceedings. Which of the following should be used to ensure the evidence remains admissible in court?

A. Bit-level image
B. Chain of custody
C. Log capture
D. Incident response plan

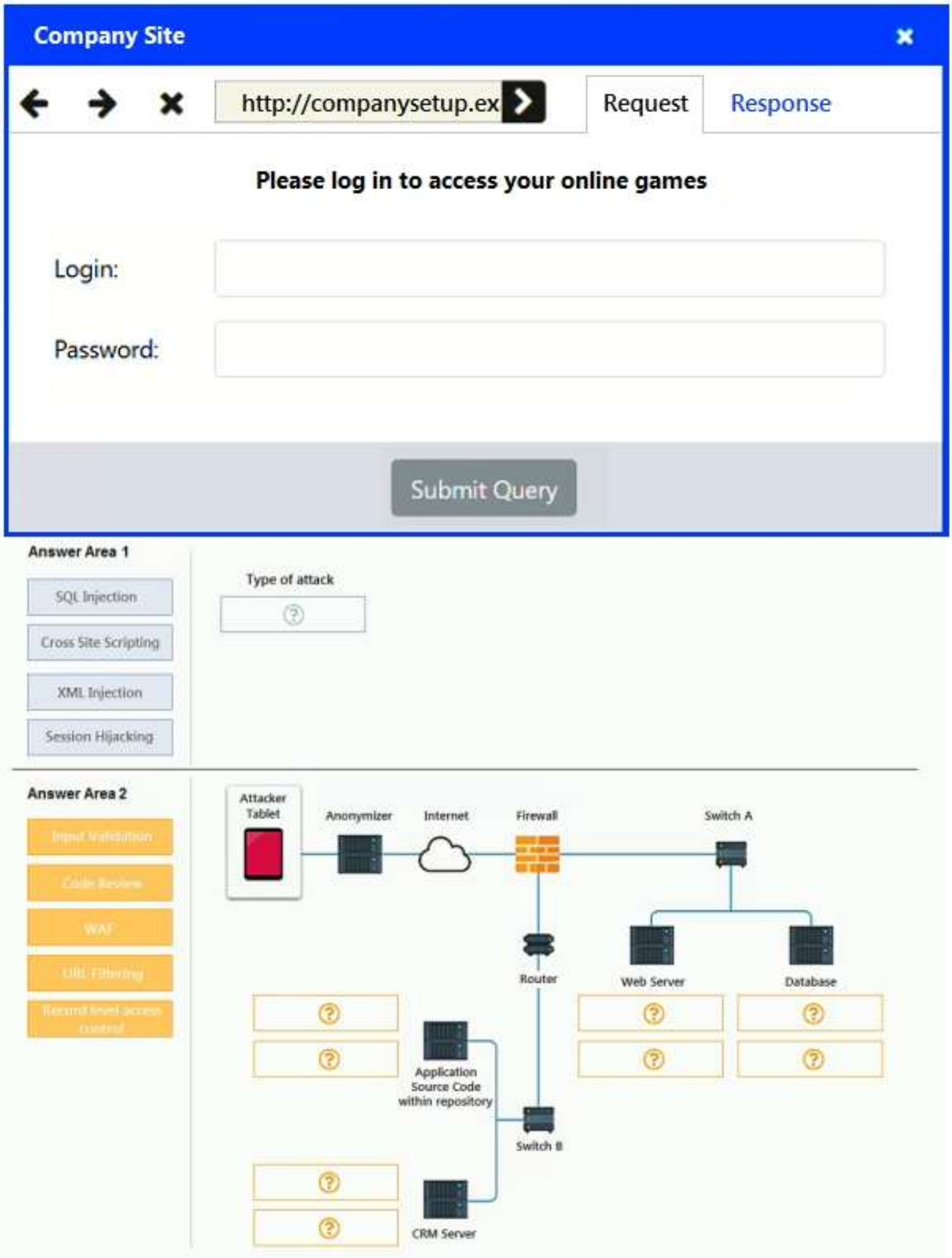
Answer: B

QUESTION 977
Drag and Drop Question
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.



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
```



Company Site

http://companysetup.ex

Request Response

Please log in to access your online games

Login:

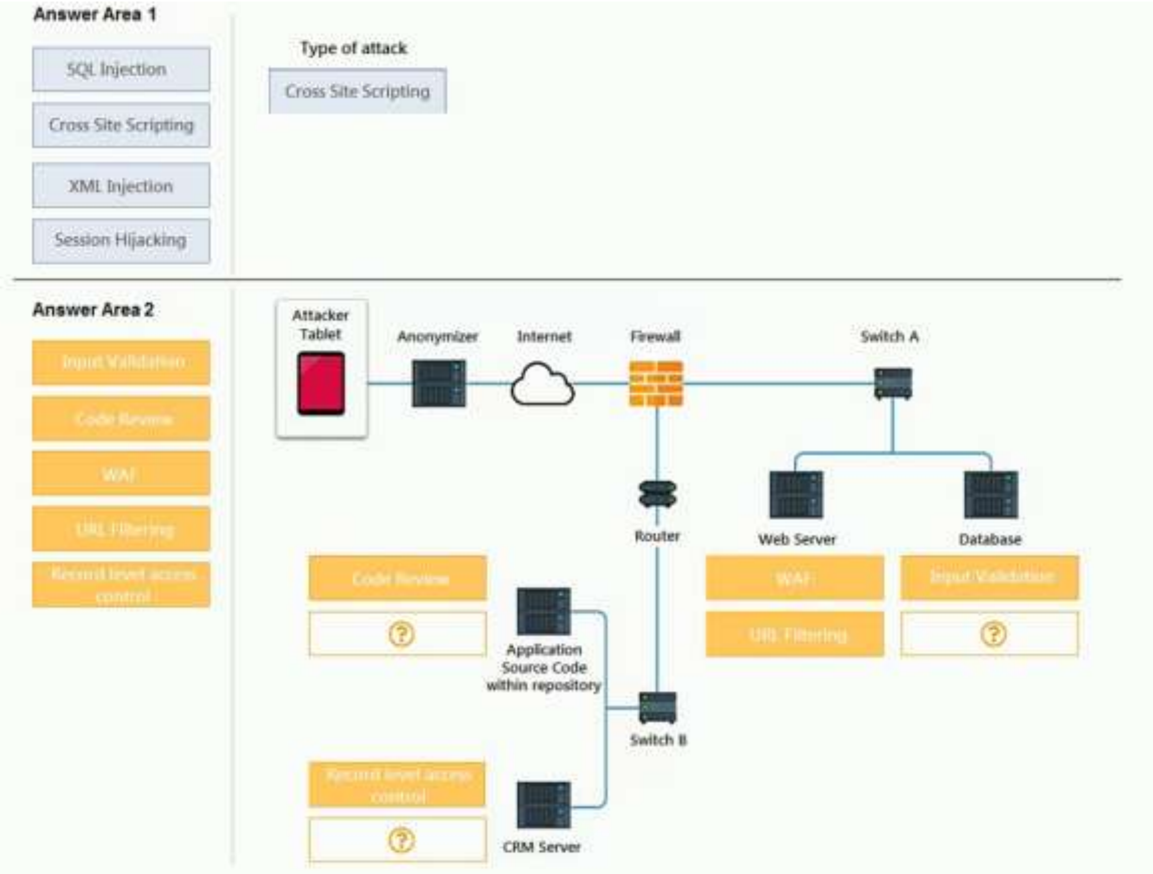
Password:

Submit Query

Answer Area 1

Answer Area 2

Answer:



QUESTION 978
A security administrator is implementing a SIEM and needs to ensure events can be compared against each other based on when the events occurred and were collected.
Which of the following does the administrator need to implement to ensure this can be accomplished?

A. TOTP
B. TKIP
C. NTP
D. HOTP

Answer: A

QUESTION 979
The Chief Information Security Officer (CISO) at a large company tasks a security administrator to provide additional validation for website customers. Which of the following should the security administrator implement?

A. HTTP
B. DNSSEC
C. 802.1x
D. Captive portal

Answer: D