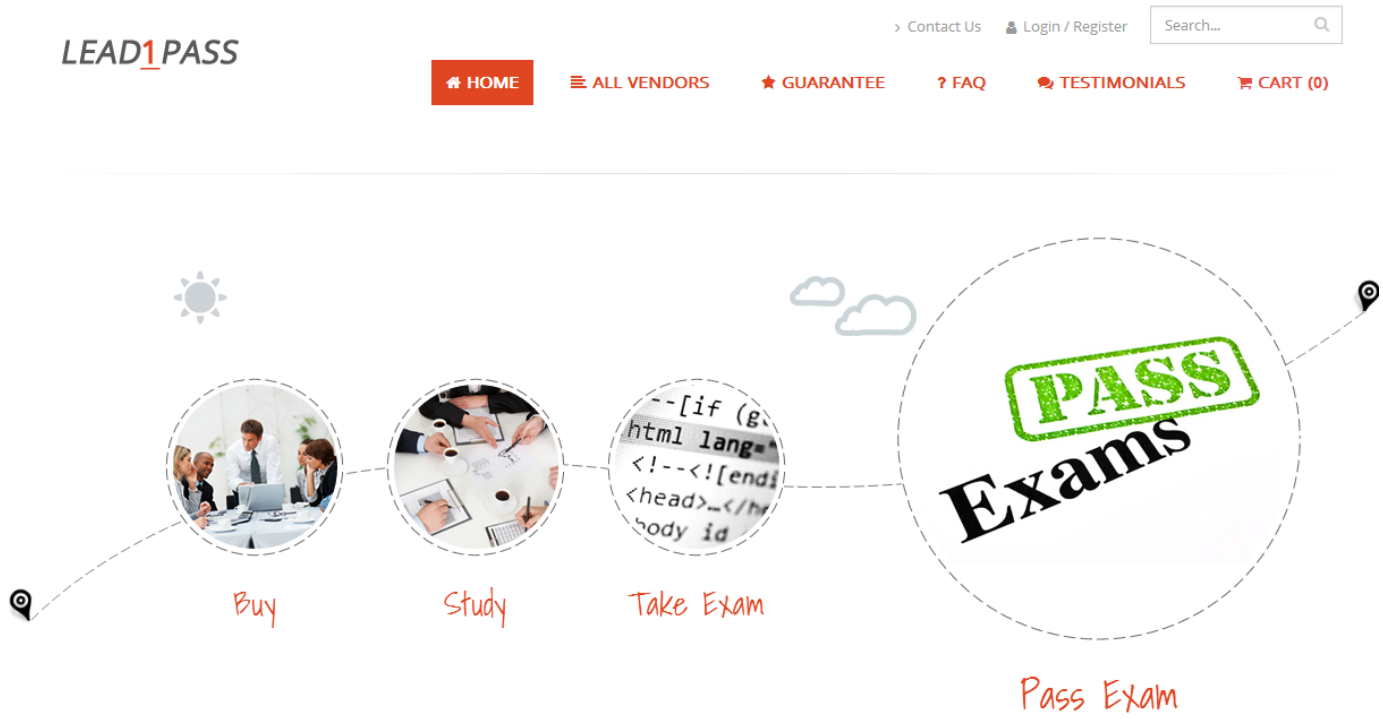
Lead1Pass



Try **PDF Demo** before you buy

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

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.

http://www.lead1pass.com/

Latest Exam Guide & Learning Materials

Exam : **SY0-501**

Title : CompTIA Security+ Certification Exam

Vendor : CompTIA

Version : DEMO

NO.1 An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?
A. BYOD model
B. DAC model
C. VDI environment
D. CYOD model
Answer: D

NO.2 After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?
A. NTLM service
B. RADIUS server
C. NTP server
D. LDAP service
Answer: C

NO.3 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: D

NO.4 A company moved into a new building next to a sugar mil. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?
A. Man-made
B. Foundational
C. Environmental
D. Natural
Answer: B

NO.5 An Organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.

The application team receive a report with the following results:

Host	Environment	Baseline deviation ID (criticality)
NYAccountingDev	Development	
NYAccountingStg	Staging	
NYAccountingProd	Production	2633 (low), 3124 (high)

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate If the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?

A. Process a risk acceptance for 2633 and 3124.

B. Process a risk acceptance for 2633 and remediate 3124.

C. Remediate 2633 and 3124 immediately.

D. Shut down NYAccountingProd and Investigate the reason for the different scan results.

Answer: B

NO.6 The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Prevent data exposure queries.

B. Limit the use of third-party libraries.

C. Submit the application to QA before releasing it.

D. Obfuscate the source code.

Answer: D

NO.7 A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. Netstat

B. Nmap

C. tcpdump

D. Protocol analyzer

Answer: B

NO.8 A security analyst is reviewing the logs from a NGFWs automated correlation engine and sees the following:

Match time	Object name	Source address	Summary
2019-07-23 10:14:33	Possible Beacon Detection	10.202.10.89	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:14:52	Possible Beacon Detection	10.202.88.88	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:19:12	Potential C2 Communication Detected	10.202.55.3	Host repeatedly visited malware domains (100).
2019-07-23 10:21:21	Compromised Asset	10.202.100.12	Host is compromised based on a sequence of recent threat log activity.
2019-07-23 10:30:37	Possible Beacon Detection	10.202.123.99	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:32:03	Possible Beacon Detection	10.202.44.107	Host visited known malware URL (15).

Which of the following should the analyst perform fiRST?

A. Isolate the compromised host from the network.

B. Clear the logs and see If the same events reoccur.

C. Set up a packet capture to analyze the unknown TCP and UDP traffic.

D. Refresh the URL filtering database to ensure accuracy.

E. Set up an alert to receive an email notification for all events.

Answer: A

NO.9 A business sector is highly competitive and safeguarding trade secrets and critical information is paramount On a seasonal basis an organization employs temporary hires and contractor personnel to accomplish its mission objectives The temporary and contract personnel require access to network resources only when on the clock Which of the following account management practices are the BEST ways to manage these accounts'? (Select TWO)

A. Employ an account expiration strategy

B. Employ time-of-day restrictions

C. Employ a password lockout policy

D. Employ a random key generator strategy

E. Employ password complexity

Answer: A,B

NO.10 Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the windows/Currentversion/Run registry key?

A. Escalation of privilege

B. Active reconnaissance

C. Pivoting

D. Persistence

Answer: A

NO.11 An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.

The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on

vacation.
Which of the following BEST describes what is happening?
A. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.
B. Some users are meeting password complexity requirements but not password length requirements.
C. The password history enforcement is insufficient, and old passwords are still valid across many different systems.
D. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems.
Answer: A
Section: (none)
Explanation

NO.12 A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking equipment and media are functioning as expected, which leads the technician to certain PKI components.
Which of the following should the technician use to validate this assumption? (Choose two.)
A. CRL
B. PFX
C. OCSP
D. SCEP
E. PEM
F. CER
Answer: A,C

NO.13 A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator. Which of the following protocols should be configured on the RADIUS server? (Select TWO).
A. NTLM
B. MSCHAP
C. PAP
D. PEAP
E. SAML
Answer: B,D

NO.14 Using an ROT13 cipher to protocol confidential information for unauthorized access is known as:
A. diffusion
B. Non repudiation
C. Obfuscation
D. Steganography

Answer: C

NO.15 A technician is evaluating a security appliance solution. The company needs a system that continues to pass traffic if the system crashes. Which of the following appliance feature would BEST meet the company's needs?
A. Fall Secure
B. Fall open
C. Fall Safe
D. Fall closed.
Answer: B

NO.16 An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements, and must also be able to log in to the headquarters location remotely. Which of the following BEST represent how the remote employees should have been set up initially? (Select TWO).
A. Individual accounts
B. User-based access control
C. Location-based policies
D. Group-based access control
E. Shared accounts
F. Mapped drives
Answer: A,D

NO.17 An employee on the Internet-facing part of a company's website submits a 20-character phrase in a small textbox on a web form. The website returns a message back to the browser stating Error: Table 'advprofile' entry into column 'lname' has exceeded number of allowed characters. Error saving database information.
Of which of the following is this an example?
A. Buffer overflow
B. Improperly configured account
C. Resource exhaustion
D. Improper error handling
Answer: D

NO.18 A security administration a hardening a VPN connection. Recently, company pre-shared keys were hijacked during an MITM attack and reused to breach the VPN connection. Which of the following should the security administrator do to BEST address this issue?
A. Implement PFS
B. Implement IPSec
C. Implement PIG
D. Implement TLS

Answer: C

NO.19 An organization wants to control user accounts and privileged access to database servers. The organization wants to create an audit trail of account requests and approval. but also wants to facilitate operational efficiency when account and access changes are needed. The organization has the following account management practices:
Which of the following should the security consultant configure in the MDM policies for the tables? (Select TWO.)
A. Remote wipe
B. Geofencing
C. Cable locks
D. GPS tagging
E. Carrier unlocking
F. Screen locks
Answer: A,B

NO.20 Given the output:

Date/time	Computer name	User ID	Website
3-15-18 2:00	Officedesktop	CompanyUser	www.comptia.org
3-15-18 2:13	Officedesktop	CompanyUser	www.companysite.com
3-15-18 2:22	Officedesktop	CompanyUser	www.localbank.org
3-15-18 2:46	Officedesktop	CompanyUser	www.myschool.edu

Which of the following account management practices should the security engineer use to mitigate the identified risk?
A. Eliminate password reuse.
B. Implement two-factor authentication.
C. Implement least privilege.
D. Eliminate shared accounts.
Answer: D

NO.21 Which of the following is the main difference between symmetric end asymmetric cryptographic algorithms?
A. Random vs pseudo-random key generation
B. The use of PKI in symmetric algorithms
C. HSM-based key generation
D. Only one Key used in symmetric algorithms
Answer: D

NO.22 A coffee company has hired an IT consultant to set up a Wifi network that will provide Internet access to customers who visit the company's chain of cafes. The coffee company has provided no requirements other than that customers should be granted access after registering via a web form and accepting the terms of service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?

A. WPS
B. Open Wifi
C. WPA with PSK
D. Captive portal
Answer: D
A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-fi or wired network before they are granted broader access to network resources.

NO.23 Passive reconnaissance during a penetration test consists of:
A. open-source intelligence gathering
B. probing the target network in a methodical manner
C. non-intrusive vulnerability scanning
D. social engineering to obtain target information
Answer: A

NO.24 A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0C-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?
A. MAC flooding
B. ARP poisoning
C. DNS hijacking
D. URL redirection
Answer: B
ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses.

NO.25 An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?
A. Sanitize all of the data.
B. Shred the hard drive.
C. Wipe the hard drive.
D. Degauss the hard drive.

Answer: B

NO.26 A user attempts to send an email to an external domain and quickly receives a bounce-back message. The user then contacts the help desk stating the message is important and needs to be delivered immediately. While digging through the email logs, a systems administrator finds the email and bounce-back details:
Your email has been rejected because it appears to contain SSN information. Sending SSN information via email to external recipients violates company policy.
Which of the following technologies successfully stopped the email from being sent?
A. UTM
B. DLP
C. DEP
D. WAF
Answer: B

NO.27 A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Select TWO).
A. WDS
B. Captive portal
C. RADIUS federation
D. 802.1X
E. WPS
F. WPA2
Answer: D,F

NO.28 A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?
A. UEfi
B. Hardware root of trust
C. ARP poisoning
D. TPM
E. Supply chain
F. Crypto-malware
Answer: E

NO.29 A security engineer needs to obtain a recurring log of changes to system files. The engineer is most concerned with detecting unauthorized changes to system dat a. Which of the following tools can be used to fulfill the requirements that were established by the engineer?
A. FDE
B. file integrity monitor

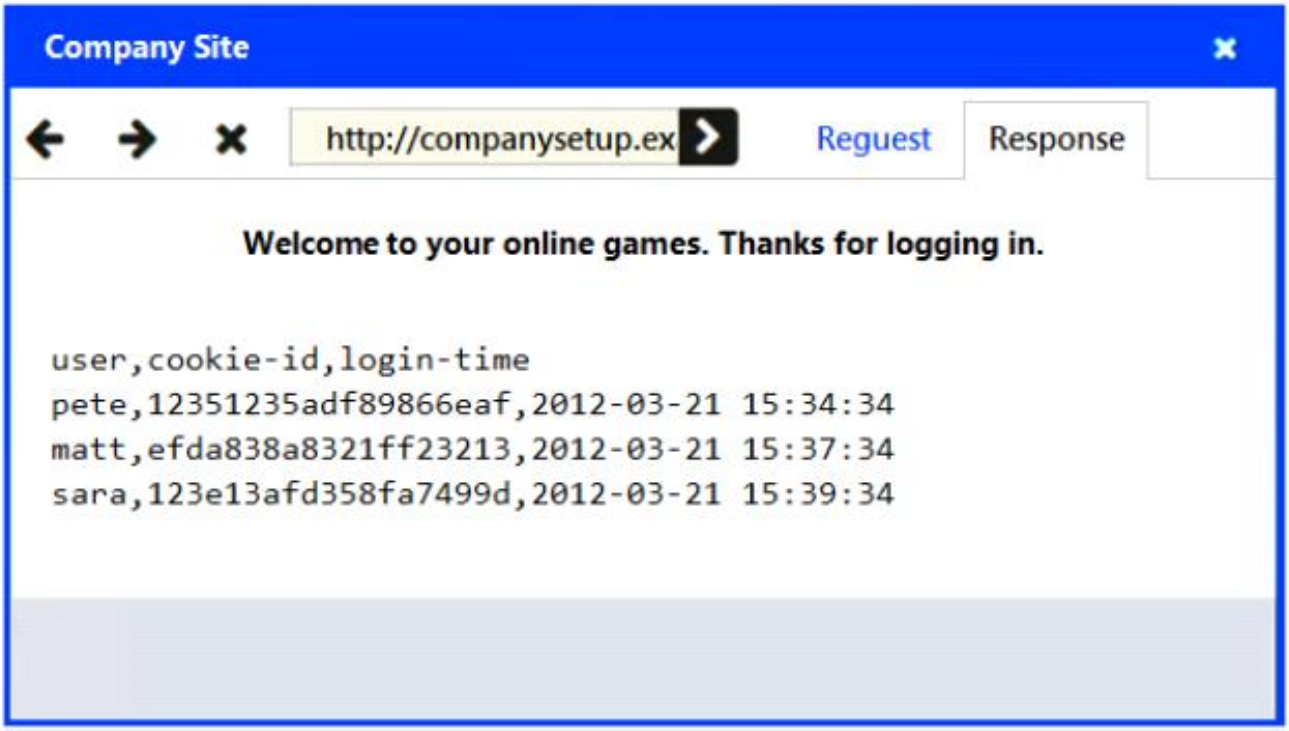
C. TPM
D. Trusted operating system
E. UEfi
Answer: B

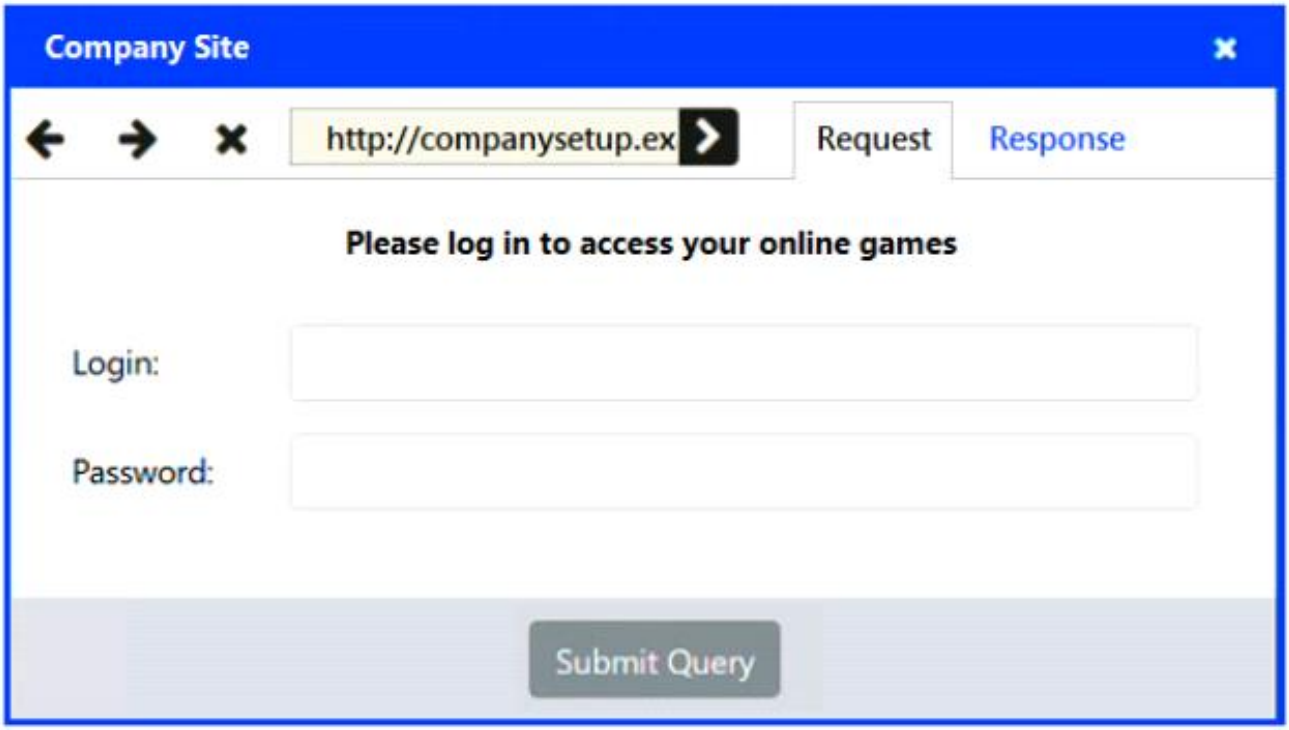
NO.30 A company recently experienced a network security breach and wants to apply two-factor authentication to secure its network. Which of the following should the company use? (Select TWO)
A. fingerprint scanner and voice recognition
B. Smart card and PIN
C. Proximity card and CAC
D. User ID and password
E. Cognitive password and OTP
Answer: C,E

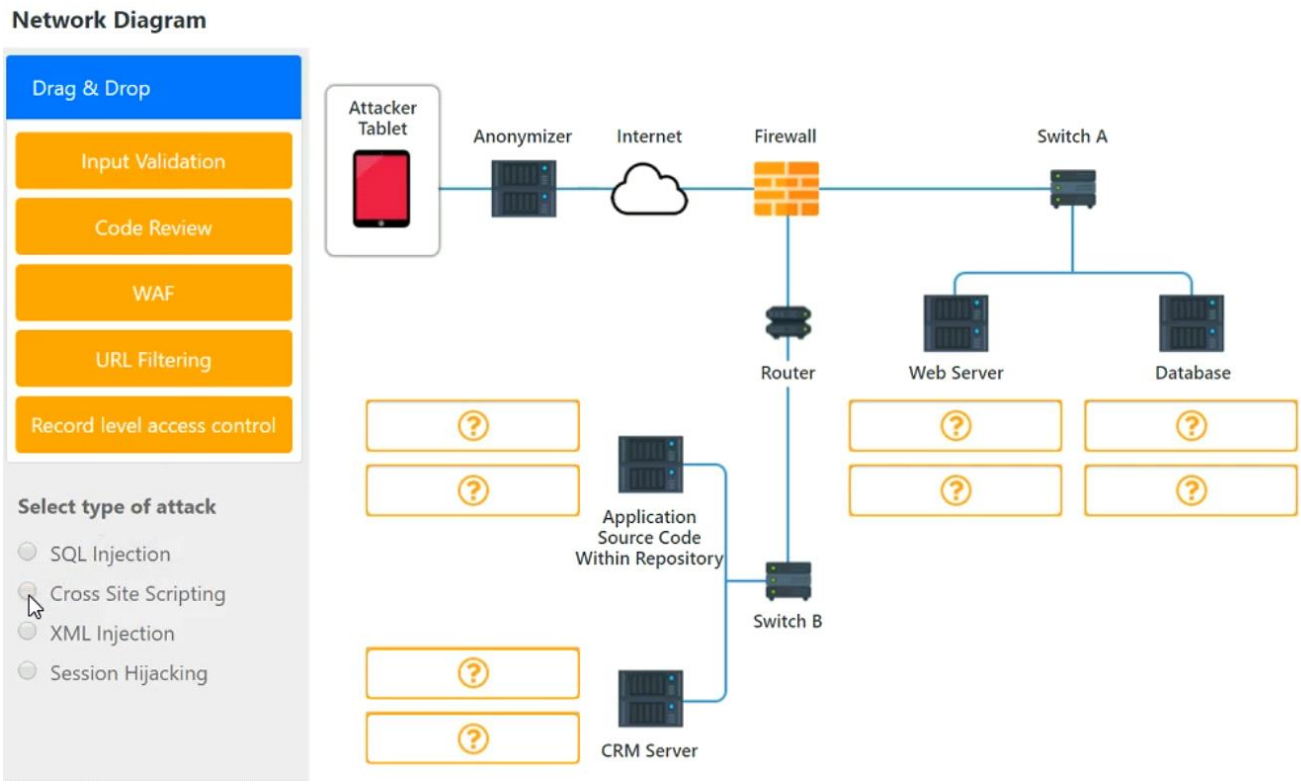
NO.31 Which of the following has the potential to create a DoS attack on a system?
A. A surveillance camera that has been replaced and is not plugged in
B. A disabled user account that has not been deleted
C. A server room Wifi thermostat with default credentials
D. A wireless access point with WPA2 connected to the network
Answer: C

NO.32 A security analyst wants to obfuscate some code and decides to use ROT13. Which of the following is an example of the text "HELLO WORLD" in ROT13?
A. QYEBJ BYYRU
B. KHOOR ZRUOG
C. URYYB JBEYQ
D. DLROWOLLEH
Answer: C

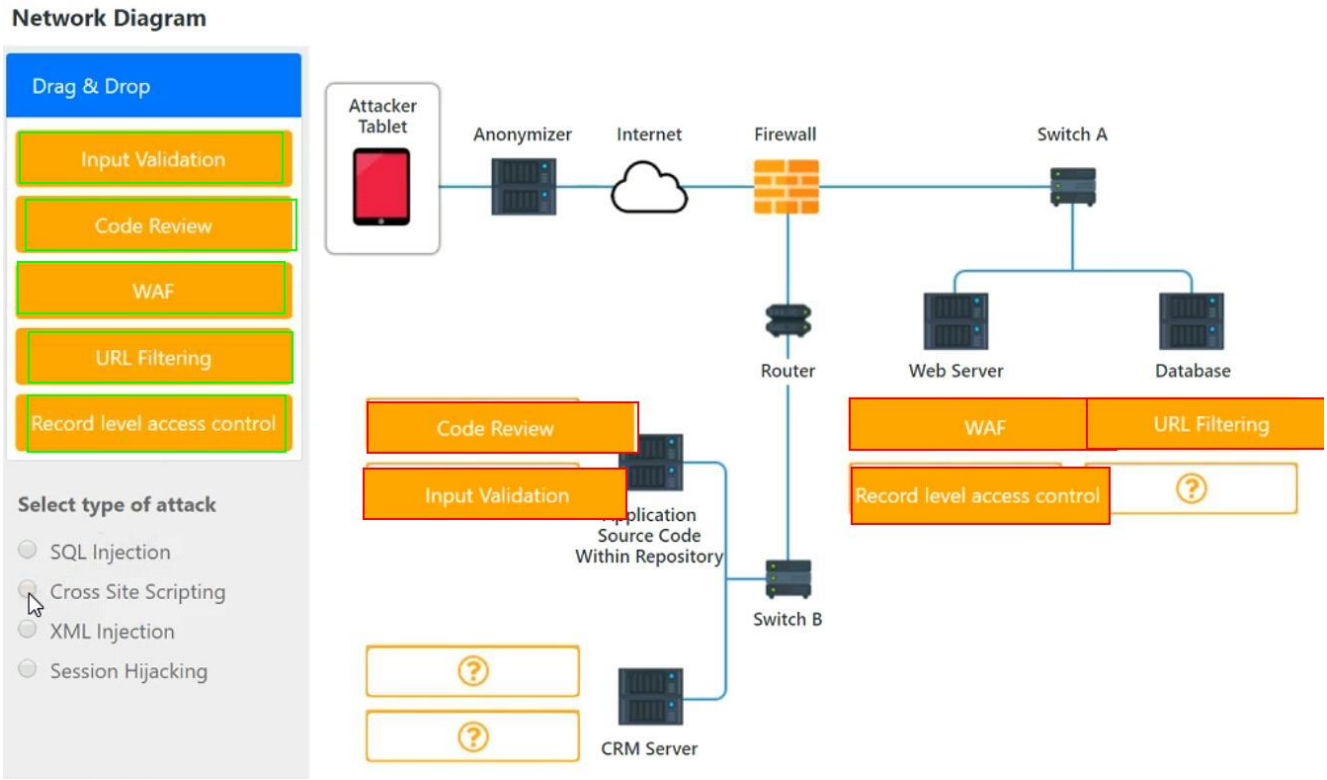
NO.33 An attack has occurred against a company.
INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1) Identify which compensating controls should be implemented 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
Reguest
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


Company Site
http://companysetup.ex
Request
Response
Please log in to access your online games
Login:
Password:
Submit Query



Answer:



NO.34 A Chief Security Officer (CSO) has implemented a policy to prevent the reuse of hard drives due to the risk of information spillage to unauthorized users. Which of the following would be the MOST practical process to decommission the workstations?

A. Remove all the hard drives and dispose of them in the trash.

B. Remove all the hard drives and degauss them.

C. Remove all the hard drives and shred the disks.
D. Remove all the hard drives and purge them.
Answer: C

NO.35 An employee of a large payroll company has a machine that recently started locking up randomly with greatly increased processor consumption Which of the following is the fiRST action an analyst should lake to investigate this potential loC?
A. Take a full disk image of the filesystem to analyze files for possible malicious activity.
B. Capture a memory dump of the system for further evaluation of malicious processes
C. Reimage the machine from a known-good image and get it back to the employee
D. Actively monitor traffic from the system to see if there is some form of command and control
Answer: A

NO.36 Which of the following involves the use of targeted and highly crafted custom attacks against a population of users who may have access to a particular service or program?
A. Phishing
B. Hoaxing
C. Spear phishing
D. Vishing
Answer: C

NO.37 A healthcare company is revamping its IT strategy in light of recent regulations. The company is concerned about compliance and wants to use a pay-per-use model. Which of the following is the BEST solution?
A. On-premises hosting
B. Community cloud
C. Public SaaS
D. Hosted infrastructure
Answer: C

NO.38 The Chief Security Officer (CSO) for an online retailer received a report from a penetration test that was performed against the company's servers. After reviewing the report, the CSO decided not to implement the recommended changes due to cost; instead, the CSO increased insurance coverage for data breaches. Which of the following describes how the CSO managed the risk?
A. Ignorance
B. Avoidance
C. Acceptance
D. Transference
Answer: D

NO.39 The network information for a workstation is as follows:

IP address/subnet mask	Default gateway	DNS server
172.16.17.200/24	172.16.17.254	172.16.17.254

When the workstation's user attempts to access www.example.com. the URL that actually opens is www.notexample.com. The user successfully connects to several other legitimate URLs. Which of the following have MOST likely occurred? (Select TWO).

A. ARP poisoning

B. IP spoofing

C. Domain hijacking

D. DNS poisoning

E. Buffer overflow

Answer: C,D

NO.40 A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identity mission-critical applications and systems.

B. Identity the impact on safety of the property.

C. Identify redundant and high-availability systems.

D. Identify the single point of failure in the system.

Answer: A