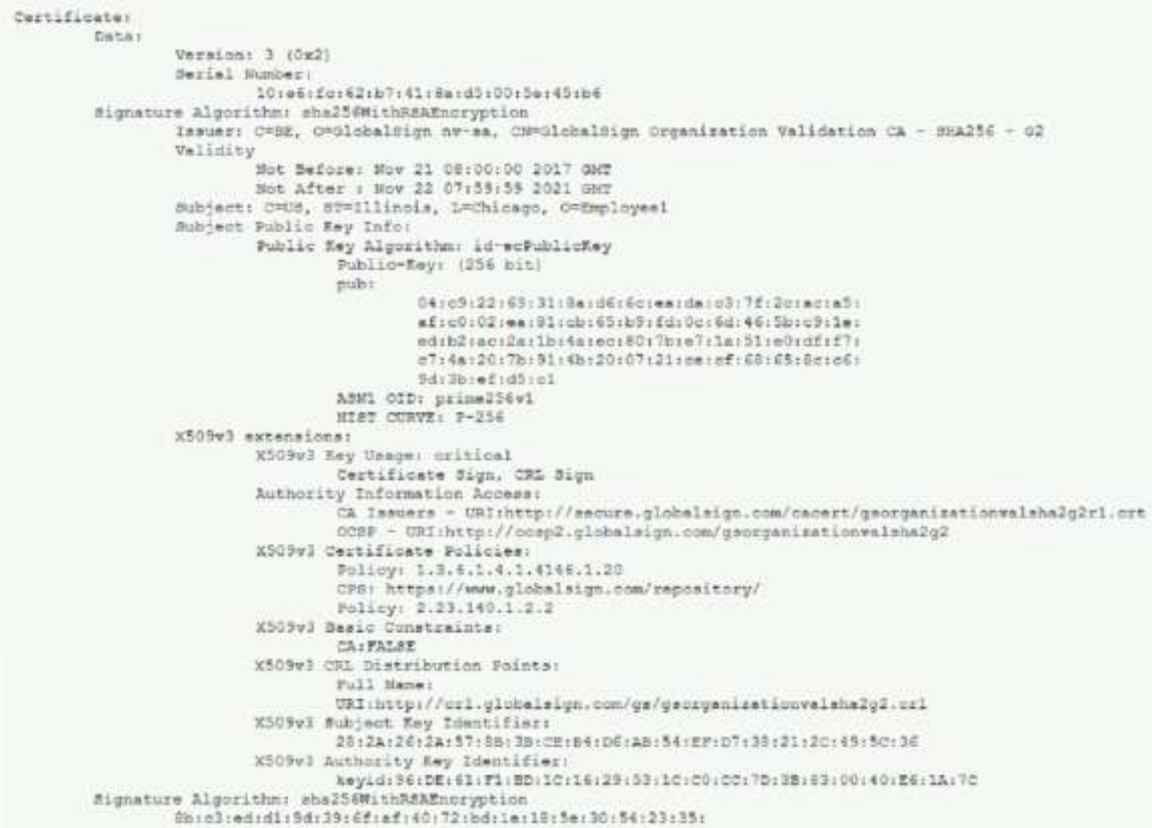
QUESTION 606

A remote user reports the inability to authenticate to the VPN concentrator.
During troubleshooting, a security administrate captures an attempted authentication and discovers the following being presented by the user's VPN client:



```
Certificate:
        Data:
                Version: 3 (0x2)
                Serial Number:
                        10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
        Signature Algorithm: sha256WithRSAEncryption
                Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
                Validity
                        Not Before: Nov 21 08:00:00 2017 GMT
                        Not After : Nov 22 07:59:59 2021 GMT
                Subject: C=US, ST=Illinois, L=Chicago, O=Employee1
                Subject Public Key Info:
                        Public Key Algorithm: id-ecPublicKey
                                Public-Key: (256 bit)
                                pub:
                                        04:c9:22:65:31:8a:d6:6c:ea:da:c3:7f:2c:ac:a5:
                                        af:c0:02:ea:91:cb:65:b9:fd:0c:6d:46:5b:c9:1e:
                                        ed:b2:ac:2a:1b:4a:ec:80:7b:e7:1a:51:e0:df:f7:
                                        e7:4a:20:7b:91:4b:20:07:21:ce:cf:68:65:8c:c6:
                                        9d:3b:ef:d5:c1
                                ASN1 OID: prime256v1
                                NIST CURVE: P-256
                X509v3 extensions:
                        X509v3 Key Usage: critical
                                Certificate Sign, CRL Sign
                        Authority Information Access:
                                CA Issuers - URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
                                OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2
                        X509v3 Certificate Policies:
                                Policy: 1.3.6.1.4.1.4146.1.20
                                CPS: https://www.globalsign.com/repository/
                                Policy: 2.23.140.1.2.2
                        X509v3 Basic Constraints:
                                CA:FALSE
                        X509v3 CRL Distribution Points:
                                Full Name:
                                URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl
                        X509v3 Subject Key Identifier:
                                28:2A:26:2A:57:8B:3B:CE:B4:D6:AB:54:EF:D7:38:21:2C:49:5C:36
                        X509v3 Authority Key Identifier:
                                keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:83:00:40:E6:1A:7C
        Signature Algorithm: sha256WithRSAEncryption
                8b:c3:ed:d1:9d:39:6f:af:40:72:bd:1e:18:5e:30:54:23:35:
```

Which of the following BEST describes the reason the user is unable to connect to the VPN service?

A. The user's certificate is not signed by the VPN service provider
B. The user's certificate has been compromised and should be revoked.
C. The user's certificate was not created for VPN use
D. The user's certificate was created using insecure encryption algorithms

Answer: B

QUESTION 607

A DevOps team wants to move production data into the QA environment for testing.

This data contains credit card numbers and expiration dates that are not tied to any individuals.
The security analyst wants to reduce risk.
Which of the following will lower the risk before moving the data?

A. Redacting all but the last four numbers of the cards
B. Hashing the card numbers
C. Scrambling card and expiration data
D. Encrypting card and expiration numbers

Answer: B

QUESTION 608
Following the most recent patch deployment, a security engineer receives reports that the ERP application is no longer accessible.
The security engineer reviews the situation and determines a critical security patch that was applied to the ERP server is the cause.
The patch is subsequently backed out.
Which of the following security controls would be BEST to implement to mitigate the threat caused by the missing patch?

A. Anti-malware
B. Patch testing
C. HIPS
D. Vulnerability scanner

Answer: B

QUESTION 609
A Chief Information Security Officer (CISO) is running a test to evaluate the security of the corporate network and attached devices.
Which of the following components should be executed by an outside vendor?

A. Penetration tests
B. Vulnerability assessment
C. Tabletop exercises
D. Blue-team operations

Answer: A

QUESTION 610
A security manager is determining the best DLP solution for an enterprise.
A list of requirements was created to use during the source selection.
The security manager wants to confirm a solution exists for the requirements that have been defined.
Which of the following should the security manager use?

A. NDA
B. RFP
C. RFQ
D. MSA
E. RFI

Answer: E

QUESTION 611
Designing a system in which only information that is essential for a particular job task is allowed to be viewed can be accomplished successfully by using:

A. mandatory vacations.
B. job rotations
C. role-based access control
D. discretionary access
E. separation of duties

Answer: C

QUESTION 612
The information security manager of an e-commerce company receives an alert over the weekend that all the servers in a datacenter have gone offline.
Upon discussing this situation with the facilities manager, the information security manager learns there was planned electrical maintenance.
The information security manager is upset at not being part of the maintenance planning, as this could have resulted in a loss of:

A. data confidentiality.
B. data security.
C. PCI compliance
D. business availability.

Answer: D

QUESTION 613
A company contracts a security consultant to perform a remote white-box penetration test.
The company wants the consultant to focus on Internet-facing services without negatively impacting production services.
Which of the following is the consultant MOST likely to use to identify the company's attack surface? (Select TWO)

A. Web crawler
B. WHOIS registry
C. DNS records
D. Company's firewall ACL
E. Internal routing tables
F. Directory service queries

Answer: BE

QUESTION 614
A company is concerned about disgruntled employees transferring its intellectual property data through covert channels.
Which of the following tools would allow employees to write data into ICMP echo response packets?

A. Thor
B. Jack the Ripper
C. Burp Suite
D. Loki

Answer: D

QUESTION 615
A security engineer is making certain URLs from an internal application available on the Internet.
The development team requires the following
- The URLs are accessible only from internal IP addresses

- Certain countries are restricted
- TLS is implemented.
- System users transparently access internal application services in a round robin to maximize performance

Which of the following should the security engineer deploy7

A. DNS to direct traffic and a WAF with only the specific external URLs configured
B. A load balancer with GeolP restrictions and least-load-sensing traffic distribution
C. An application-aware firewall with geofencing and certificate services using DNS for traffic direction
D. A load balancer with IP ACL restrictions and a commercially available PKI certificate

Answer: B

QUESTION 616
A company enlists a trusted agent to implement a way to authenticate email senders positively.
Which of the following is the BEST method for the company to prove Vie authenticity of the message?

A. issue PIN-enabled hardware tokens
B. Create a CA win all users
C. Configure the server to encrypt all messages in transit
D. include a hash in the body of the message

Answer: A

QUESTION 617
A company recently migrated to a SaaS-based email solution.
The solution is configured as follows.
- Passwords are synced to the cloud to allow for SSO
- Cloud-based antivirus is enabled
- Cloud-based anti-spam is enabled
- Subscription-based blacklist is enabled

Although the above controls are enabled, the company's security administrator is unable to detect an account compromise caused by phishing attacks in a timely fashion because email logs are not immediately available to review.
Which of the following would allow the company to gam additional visibility and reduce additional costs? (Select TWO)

A. Migrate the email antivirus and anti-spam on-premises
B. Implement a third-party CASB solution.
C. Disable the current SSO model and enable federation
D. Feed the attacker IPs from the company IDS into the email blacklist
E. Install a virtual SIEM within the email cloud provider
F. Add email servers to NOC monitoring

Answer: BE