For devsecops engineer :

1. What is a VPN and what is the purpose of it

A Virtual Private Network is a technology used to create secure and encrypted connection over the internet. It helps us to provide privacy and security to users worldwide.

PURPOSE :  
A. It **encrypts** all data that it sends over the internet, preventing unauthorized parties from connecting and accessing out info.  
B. It helps us **to bypass geographical barriers** by masking IP addresses to a different location, enables access to region locked content and services.

C. **Optimize** Online activities, by hiding our IP and online activities from ISPs, ads, 3rd party apps etc.

D. It **Enhances Security** by hiding out IP address and routing traffic via different tunnels, preventing hacking, snooping etc.

2. What is a firewall and explain firewall stateful concept

A FW is a software/device that monitors and controls incoming and outgoing traffic based on predefined user rules.   
Purpose : Establish a barrier between trusted internal network and untrusted outer internet.

STATEFUL Concept : It is the capability of a firewall to monitor active connections’ state and make decisions based on it (traffic). Here FW maintains a state table of the state of established connections.

1. What is the difference between a vulnerability scan and a penetration test ?

**Vulnerability Scan =**

GOAL – Identify and access Vulnerability in a system or network.  
 METHOD – Automated tools scanning network, systems or apps, relying on DB of known Vulnerabilities

Performed – Regularly

**Penetration Testing =**

GOAL – Simulating real world attacks to identify Vulnerability  
 METHOD – Using automated tools combo with manual techniques to track Vulnerabilities and attempt to exploit them to gain hacks.

Performed – Periodically

1. Explain the difference between asymmetric and symmetric encryption

|  |  |  |
| --- | --- | --- |
| TYPE | SYMMETRIC | ASYMMETRIC |
| Key sharing | Securely distribution | Simple with public/private keys. |
| Key Type | 1 Shared key | Public key (encrypting), private key (decrypting) |
| Performance | Faster | Slow |
| Security | Less – key distribution | High – Pub/Private key pair |
| Use Case & eg | Large data volume encrypton eg: AES, DES | Secure communications, digital signs eg :RSA |

1. What is referred to as a Man-in-the-Middle Attack ?

Here, attacker intercepts and alters communication between 2 servers.

WORKING-

1. ATTACKER intercepts comms between 2 parties by being in between the sender and receiver.
2. Attacking techniques like ARP spoofing, DNS spoofing etc are used.
3. Attacker eavesdrop on the conversation, alter messages or even plant viruses for receiver.
4. Explain the principle of least privilege

It states that users, individuals or processes should be granted only minimum necessary permission (GRANULAR) to perform their tasks and functions.

1. Why do you think it is essential to prioritize SCA first in DevSecOps Cycle?

It is needed because :

1. By integrating security assessments earlier, issues and Vulnerabilities can be accesses earlier.
2. Identifying issues earlier saves time in long run making the whole process efficient.
3. Improves cost management.
4. Reduces overall risk of getting Vulnerabilities in PROD.
5. How do you implement security in a CI/CD pipeline?
6. Static Code Analysis = we can use SonarQube like tools to analyze source code for security Vulnerabilities.
7. SCA tools can run automatically as a part of our build process.
8. Integrate dependency scanning in our pipeline by utilizing tools like OWASP or Snyk to identify Vulnerabilities.
9. Utilize secret management tools like Hashicorp’s vault, AWS Secrets Manager etc into the build process.
10. What are some common security tools used in DevSecOps?

|  |  |
| --- | --- |
| Static App security test tools | SonarQube, Fortify |
| Dynamic App security test tools | ZAP, Burp Suite |
| Software Analysis tools | Snuk, Dependency Check |
| Containers | Docker Security |
| Secret Management | Azure Key Vault, AWS Secret Manager |

11. How do you ensure that secrets are protected within your DevSecOps pipeline?

1. We must avoid HARDCODED Secrets.

2. Use Seceret management tools – Hashicorp Vault, AWS Secetet Manager, GCP Key store etc.

3. Encrypt secerets in transit using protocols like HTTPS, TLS etc

4. Rotate secrets weekly, regularly etc as per need.

10. Case study :

a. CSPM have triggered an alert, we have a customer with a cloud database exposed to the internet, you have a meeting with him tomorrow.

i. What do you ask him ? Do he need to change his cloud database configuration ? Why ?

1. Ask why the alert was triggered including all specifics, nature of exposure, and any risks associated with it.

2. Inquire about current configuration – Access controls, authentications etc.

3. Discuss best practices and ask about risk and impact of exposed database – unauth accesses, data exposure etc

4. [Yes, he need to change configuration] - Recommend **configuration changes** necessary to secure DN like – restricting net access to trusted networks only, implementing strong and granular authentication and access rrespectively.

5. Implementing continuous monitoring to ensure security of DB.

b. A developer pushed a code with vulnerabilities on Azure DevOps repository. Suez have a devsecops tool to detect vulnerabilities.

i. What is the best way to communicate vulnerabilities information with him ?

1. Reaching out to developer asap.

2. Clearly communicating the details of vulnerabilities , its types, severity levels, impacts etc.

3. Providing full explanation on specified context.

4. Offer guidance on how to remediate vulnerabilities.

5. Encouraging collab between different teams – security team, testing team, developers etc.

6. Offer resources and docs needed for the completion of security practice.

7. Consider vulnerabilities detected as a learning opportunity so that it can be stopped before happening again.