CYBER SECURITY

CIE-04

SECTION 01

1) WHY IS WAF (WIRELESS APPLICATION FIREWALL) SECURITY IMPORTANT? GIVE ITS TYPES AND FEATURES.

1. WAFs are important for a growing number of organizations that offer products or services online—this includes mobile app developers, social media providers, and digital bankers.
2. A WAF can help you protect sensitive data, such as customer records and payment card data, and prevent leakage.
3. WAF can help you meet compliance requirements such as PCI DSS (the Payment Card Industry Data Security Standard), which applies to any organization handling cardholder data and requires the installation of a firewall.
4. A WAF is thus an essential component of an organization's security model.
5. It is important to have a WAF, but it is recommended you combine it with other security measures, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and traditional firewalls, to achieve a defense-in-depth security model.

TYPES OF WEB APPLICATIONS FIREWALLS

- **Network-based WAF**—usually hardware-based, it is installed locally to minimize latency. However, this is the most expensive type of WAF and necessitates storing and maintaining physical equipment.
- **Host-based WAF**—can be fully integrated into the software of an application. This option is cheaper than network-based WAFs and is more customizable, but it consumes extensive local server resources, is complex to implement, and can be expensive to maintain. The machine used to run a host-based WAF often needs to be hardened and customized, which can take time and be costly.
- **Cloud-based WAF**—an affordable, easily implemented solution, which typically does not require an upfront investment, with users paying a monthly or annual security-as-a-service subscription. A cloud-based WAF can be regularly updated at no extra cost, and without any effort on the part of the user.

FEATURES OF WAF ARE:

- Attack database Signature
- AI powered traffic pattern
- DDOS
- Customisation
- Corelation engines

- Content delivery networks
- Application profiling

B) EXPLAIN IAM BEST PRACTICES

- IAM stands for Identity Access Management. ○ IAM allows you to manage users and their level of access to the aws console.
- It is used to set users, permissions and roles. It allows you to grant access to the different parts of the aws platform.
- AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. ○ With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
- Without IAM, Organizations with multiple users must either create multiple user accounts, each with its own billing and subscriptions to AWS products or share an account with a single security credential. Without IAM, you also don't have control about the tasks that the users can do.
- IAM enables the organization to create multiple users, each with its own security credentials, controlled and billed to a single aws account. IAM allows the user to do only what they need to do as a part of the user's job.

IAM BEST PRACTICES

1. Adopt a Zero Trust Approach to Security
2. Identify and Protect High-Value Data
3. Enforce a Strong Password Policy
4. Use Multi-Factor Authentication (MFA)
5. Automate Workflows
6. Adopt The Principle of Least Privilege
7. Enforce Just-in-Time Access Where Appropriate
8. Leverage Both Role-Based Access Control and Attribute-Based Access Control Policies
9. Regularly Audit Access to Resources
10. Centralize Log Collection

SECTION -02

INSTALLATION OF BURP SUITE:

- **Step 1:** Visit the official Burp Suite website using any web browser.
- **Step 2:** Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.
- **Step 3:** Click on Go straight to downloads.
- **Step 4:** select Burp suite community edition and select windows (64-bit) and then click on download.

Step 5: Now check for the executable file in downloads in your system and run it.

Step 7: Loading of Installation Wizard will appear which will take a few seconds.

Step 8: click on Next.

Step 9: choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.

Step10: click on Next Button.

Step 11: installation process will start and will hardly take a minute to complete the installation.

Step 12: Click on Finish

Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop

Run the software, Click on I Accept.

Step 15: Choose click Next.

- **Step 16:** click on Use Burp Defaults.
- Step 17: Project will start loading.
- Step 18: Finally new project window will appear.

Certificate import to browser

- Step 1: - Double click on the burp suite app & click on the next then click on the Start burp
- Step 2: - Now burp suite will be open & select the proxy and turn on the Intercept then click on the open browser option
- Step 4: - Search the http://Burpsuite then click on the CA certificate
- Step 5: - Then CA certificate will be downloaded
- Step 6: - Open the fire fox then go to settings

- Step 7: - Then click on the manage more settings
- Step 8: - Search the proxy then click on the proxy settings
- Step 9: - Choose the manual proxy configuration & enter the HTTP proxy and Port then click on ok option EX: - 127.0.0.1 & 8080
- Step 10: - Search the certificate then click on the view certificates
- Step 11: - Select the port swigger CA certificate & Import the certificate then Click on the ok option
- Step 12: - Open the fire fox then search the any website name\
- Step 13: - Now we can't reach the website, So
- Step 14: - Open the burp suite & click on the forward option then click on drop
- Step 15: - Now we can reach the website

Create a cloud account in AWS & Access the IAM user service & create two user accounts & one group and add 2 created users to the group and setup two factor authentication to any one user.

Step 1: - Open the chrome browser & search the AWS then click on the amazon web services-AWS official site ¬
Step 2: - Then click on create a free account ¬
Step 3: - Enter your email address & AWS account name then click on verify email address ¬
Step 4: - Enter verification code then click on verify ¬
Step 5: - Enter Root user password & confirm the password then click on Continue ¬
Step 6: - Full fill the contact information then click on continue ¬
Step 7: - Full fill the billing information then click on verify and continue
Step 8: - Enter one time password (OTP) then click on make payment ¬
Step 9: - Enter your phone number & captcha then click on send SMS ¬
Step 10: - Then enter the verification code ¬
Step 11: - Then click on complete sign up ¬
Step 12: - Click on Go to AWS management console ¬
Step 13: - Click on sign in to the console
Step 14: - Select the IAM user & enter your email address then click on Next ¬
Step 15: - Enter the captcha then click on submit ¬

Step 16: - Enter your password then click on sign in option ¬
Step 17: - Then click on IAM ¬
Step 18: - Click on user
Step 19: - Then click on Add user ¬
Step 20: - Enter user name then if you want add multiple user Choose Add another user for each additional user & type their user names Select the password – AWS MCA. then Select the customer password & Enter the password. Then click on Next: permission ¬
Step 21: - Click on create group ¬
Step 22: - Enter the group name & Give a policies then click on create group ¬
Step 23: - Then group will be created Cyber Security
Step 24: - Search the users then click on users ¬
Step 25: - Then click on Add MFA ¬
Step 26: - Then click on Activate MFA ¬
Step 27: - Enter the user name then click on continue ¬
Step 28:-Then download the google authentication app in your phone ¬
Step 29:-Then scan the QR code to add your AWS account to the Authenticator app ¬
Step 30: - Enter the numeric code from the authentication into AWS console. Then wait for a new code to appear in the authenticator. Enter the second code. Then click on "Assign MFA" 14.

Demonstrate the creation of S3 bucket service in AWS & store some files in S3 bucket. ¬

Step 1: - After login, go to products in AWS & select the storage option then click on the Amazon simple storage service(S3) ¬
Step 2: - Click on Get started with amazon S3 ¬
Step 3: - Then click on create bucket ¬ Step 4: - Enter the bucket name then scroll down Cyber
Step 5: - Click on create bucket ¬
Step 6: - Then bucket will be created ¬
Step 7: - Select the bucket then click on the upload option ¬
Step 8: - Click on the Add files then click on the upload
Step 9:- Then file will be uploading to S3 bucket.