F5-ASM/WAF

Duration: 40 Hours (5 Days)

Overview

The F5-ASM/WAF course is designed to provide learners with comprehensive knowledge and skills to manage and secure web applications using the F5 Application Security Manager (ASM), which is a robust Web Application Firewall (WAF). The course covers a broad range of topics from understanding the flow of application traffic, setting up the BIG-IP system, and utilizing F5's advanced security features to protect against web-based threats.Participants will gain insights into the OWASP Top 10 security risks and how to mitigate them, learn to deploy security policies, tune these policies for optimal performance, and understand the importance of Signature-based defenses. With a focus on building a Positive security model, Securing cookies, and Handling parameters, the course also dives into the Integration with vulnerability scanners, the use of Layered policies, and Defenses against brute force attacks and DoS.By the end of the F5 WAF training, learners will be equipped with practical skills in web application firewall training, allowing them to secure applications effectively. This course is beneficial for security professionals seeking to enhance their expertise in F5 security solutions and for organizations aiming to safeguard their web applications against evolving cyber threats.

Audience Profile

The F5-ASM/WAF course is designed for IT professionals focusing on web application security and traffic management.

- Network Security Engineers
- System Administrators managing web application infrastructures
- Security Architects designing secure network environments
- Application Developers seeking to understand security deployment
- IT Security Consultants providing advice on application security
- Network Administrators responsible for F5 BIG-IP ASM/WAF devices
- Cybersecurity Analysts analyzing and securing web applications
- IT Professionals preparing for F5 certification exams
- DevOps Engineers integrating security into continuous deployment
- Webmasters responsible for maintaining the security of websites
- Compliance Officers ensuring adherence to web application security standards
- Technical Support Engineers supporting F5 security products
- Cloud Security Specialists working with cloud-based web applications

Course Syllabus

Table of Content

- Application Traffic Flow.
- Initial setup of BIG-IP
- Basic traffic processing components on F5
- HTTP header and explanation of OWASP Top 10
- Security Model
- Ways to deploy initial security policy on ASM.

- Tuning of your policy
- Attack Signatures
- Approach towards building a positive security policy.
- Securing Cookies and other headers.
- Reporting and Logging Functionalities on ASM.
- Static and Dynamic Parameter Handling
- Comparing Security Policies
- ASM deployment types
- Use of Templates for policy creation.
- Process of Automatic Policy building.
- Integration of ASM with Vulnerability Scanners
- Use of Layered policies.
- Enforce login and protection of application from Brute Force
- Details of Session tracking and Web Scraping.
- Protecting your application against DOS.