F5-TRG-BIG-AWF-SU1
Setting up F5 Advanced WAF

Overview

Do you need to secure your applications quickly from today's threats such as those from automated agents, bots, and common vulnerabilities? Are you limited by time, resources, and knowledge of your web applications? Do you need protection against CVEs without thinking too deeply about them?

In this 1 day course, participants identify and mitigate common web application vulnerabilities on the client and application sides of the threat spectrum. Participants use F5 Advanced WAF to quickly configure advanced protection against common Layer 7 vulnerabilities (OWASP Top Ten) and bot defense.

This course is intended for users who wish to rapidly deploy a basic web application security policy with minimal configuration.

Course Length

1 days

Topics covered in this course Include

- Differentiating between client-side and application-side web vulnerabilities
- Categorizing Attack Techniques
- Use the Guided Configuration to deploy a Web Application Security Policy
- Defining the key parts of a Web Application Security Policy
- Understanding request logging options
- Identifying HTTP headers and methods
- Defining attack signatures, attack signature staging, and violations
- Overview of the OWASP Top Ten
- Review learning suggestions and basic policy tuning
- Deploy Threat Campaign

- Mitigate Credentials Stuffing
- Secure a URL from client-side fraud using DataSafe encryption and obfuscation
- Use the automated L7 Behavioral Denial of Service feature to detect and mitigate DoS attacks

Audience

This course is intended for security and network administrators who will be responsible for the deployment of F5 Advanced Web Application Firewall to secure web applications from common vulnerabilities and denial of service.

Prerequisites

There are no F5-technology-specific prerequisites for this course. However, completing the following before attending would be very helpful for students with limited BIG-IP administration and configuration experience:

- Administering BIG-IP instructor-led course

-or-

- F5 Certified BIG-IP Administrator

The following free web-based training courses, although optional, will be very helpful for any student with limited BIG-IP administration and configuration experience. These courses are available at F5 University:

- Getting Started with BIG-IP
- Getting Started with BIG-IP Application Security Manager (ASM)

The following general network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course:

- OSI model encapsulation
- Routing and switching
- Ethernet and ARP

- TCP/IP concepts
- IP addressing and subnetting
- NAT and private IP addressing
- Default gateway
- Network firewalls
- LAN vs. WAN

Course Outline

Chapter 1: Setting Up the BIG-IP System

- Introducing the BIG-IP System
- Initially Setting Up the BIG-IP System
- Archiving the BIG-IP System Configuration
- Leveraging F5 Support Resources and Tools

Chapter 2: Threat Overview and Guided Configuration

- Today's Threat Landscape
- Differentiating Benign and Malicious Clients
- Categorizing Attack Techniques
- Defining the Layer 7 Web Application Firewall
- Defining Traffic Processing Objects
- Introducing F5 Advanced WAF
- Using Guided Configuration for Web Application Security

Chapter 3: Exploring HTTP Traffic

- Exploring Web Application HTTP Request Processing
- Overview of Application-Side Vulnerabilities
- Defining Attack Signatures
- Defining Violations

Chapter 4: Securing HTTP Traffic

- Defining Learning
- Defining Attack Signature Staging
- Defining Attack Signature Enforcement

Chapter 5: Mitigating Credentials Stuffing

- Defining Credentials Stuffing Attacks
- Credential Stuffing Mitigation Workflow

Chapter 6: Form Encryption Using BIG-IP DataSafe

- What Elements of Application Delivery are Targeted?
- Exploiting the Document Object Model
- Protecting Applications Using DataSafe
- Configuring a DataSafe Profile

Chapter 7: Deploying Threat Campaigns

- Defining Threat Campaigns
- Live Update for Threat Campaigns

Chapter 8: Using L7 Behavioral Analysis to Mitigate DoS

- Defining Behavioral Denial of Service Mitigation
- Defining the DoS Protection Profile