Configuring F5 Advanced WAF (previously licensed as ASM)

Duration: 4 days

Description

In this 4 day course, students are provided with a functional understanding of how to deploy, tune, and operate F5 Advanced Web Application Firewall to protect their web applications from HTTP-based attacks.

The course includes lecture, hands-on labs, and discussion about different F5 Advanced Web Application Firewall tools for detecting and mitigating threats from multiple attack vectors such web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero day exploits.

Participants

This course is intended for SecOps personnel responsible for the deployment, tuning, and day-to-day maintenance of F5 Adv. WAF.

Participants will obtain a functional level of expertise with F5 Advanced WAF, including comprehensive security policy and profile configuration, client assessment, and appropriate mitigation types.

• Experience with LTM is not required.
• Prior WAF knowledge is not required.
• This course is on the list of approved study resources for the F5 ASM 303 certification exam.

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 (https://university.f5.com):

? Getting Started with BIG-IP web-based training
? Getting Started with BIG-IP Application Security Manager (ASM) web-based training

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

Objectives

Topics covered:

• Resource provisioning for F5 Advanced Web Application Firewall
• Traffic processing with BIG-IP Local Traffic Manager (LTM)
• Web application concepts
• Mitigating the OWASP Top 10 and other vulnerabilities
• Security policy deployment
• Security policy tuning
• Deploying Attack Signatures and Threat Campaigns
• Positive security building
• Securing cookies and other headers
• Reporting and logging
• Advanced parameter handling
• Using Automatic Policy Builder
• Integrating with web vulnerability scanners
• Login enforcement for flow control
• Brute force and credential stuffing mitigation
• Session tracking for client reconnaissance
• Using Parent and Child policies
• Layer 7 DoS protection - Transaction Per Second-based DoS protection - Layer 7 Behavioral DoS Protection
• Configuring Advanced Bot Defense - Web Scraping and other Microservice Protection - Working with Bot Signatures
• Using DataSafe to Secure the client side of the Document Object Model

Programme

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: Traffic Processing with BIG-IP

? Identifying BIG-IP Traffic Processing Objects

? Understanding Profiles
? Overview of Local Traffic Policies
? Visualizing the HTTP Request Flow

Chapter 3: Web Application Concepts

? Overview of Web Application Request Processing
? Web Application Firewall: Layer 7 Protection
? Layer 7 Security Checks
? Overview of Web Communication Elements
? Overview of the HTTP Request Structure
? Examining HTTP Responses
? How F5 Advanced WAF Parses File Types, URLs, and Parameters
? Using the Fiddler HTTP Proxy

Chapter 4: Web Application Vulnerabilities

? A Taxonomy of Attacks: The Threat Landscape
? Common Exploits Against Web Applications

Chapter 5: Security Policy Deployment

? Defining Learning
? Comparing Positive and Negative Security Models
? The Deployment Workflow
? Assigning Policy to Virtual Server
? Deployment Workflow: Using Advanced Settings
? Configure Server Technologies
? Defining Attack Signatures
? Viewing Requests
? Security Checks Offered by Rapid Deployment
? Defining Attack Signatures

Chapter 6: Policy Tuning and Violations

? Post-Deployment Traffic Processing
? How Violations are Categorized
? Violation Rating: A Threat Scale
? Defining Staging and Enforcement
? Defining Enforcement Mode
? Defining the Enforcement Readiness Period
? Reviewing the Definition of Learning
? Defining Learning Suggestions
? Choosing Automatic or Manual Learning
? Defining the Learn, Alarm and Block Settings
? Interpreting the Enforcement Readiness Summary
? Configuring the Blocking Response Page

Chapter 7: Attack Signatures and Threat Campaigns

? Defining Attack Signatures
? Attack Signature Basics
? Creating User-Defined Attack Signatures
? Defining Simple and Advanced Edit Modes
? Defining Attack Signature Sets
? Defining Attack Signature Pools
? Understanding Attack Signatures and Staging
? Updating Attack Signatures
? Defining Threat Campaigns
? Deploying Threat Campaigns

Chapter 8: Positive Security Policy Building

? Defining and Learning Security Policy Components
? Defining the Wildcard
? Defining the Entity Lifecycle
? Choosing the Learning Scheme
? How to Learn: Never (Wildcard Only)
? How to Learn: Always
? How to Learn: Selective
? Reviewing the Enforcement Readiness Period: Entities
? Viewing Learning Suggestions and Staging Status
? Defining the Learning Score
? Defining Trusted and Untrusted IP Addresses
? How to Learn: Compact

Chapter 9: Securing Cookies and Other Headers

? The Purpose of F5 Advanced WAF Cookies
? Defining Allowed and Enforced Cookies
? Securing HTTP headers

Chapter 10: Visual Reporting and Logging

? Viewing Application Security Summary Data
? Reporting: Build Your Own View
? Reporting: Chart based on filters
? Brute Force and Web Scraping Statistics
? Viewing Resource Reports
? PCI Compliance: PCI-DSS 3.0
? Analyzing Requests
? Local Logging Facilities and Destinations
? Viewing Logs in the Configuration Utility
? Defining the Logging Profile
? Configuring Response Logging

Chapter 11: Lab Project 1

Chapter 12: Advanced Parameter Handling

? Defining Parameter Types
? Defining Static Parameters
? Defining Dynamic Parameters
? Defining Parameter Levels
? Other Parameter Considerations

Chapter 13: Automatic Policy Building

? Overview of Automatic Policy Building
? Defining Templates Which Automate Learning
? Defining Policy Loosening
? Defining Policy Tightening
? Defining Learning Speed: Traffic Sampling
? Defining Track Site Changes

Chapter 14: Web Application Vulnerability Scanner Integration

? Integrating Scanner Output
? Importing Vulnerabilities
? Resolving Vulnerabilities
? Using the Generic XML Scanner XSD file

Chapter 15: Deploying Layered Policies

? Defining a Parent Policy
? Defining Inheritance
? Parent Policy Deployment Use Cases

Chapter 16: Login Enforcement and Brute Force Mitigation

? Defining Login Pages for Flow Control
? Configuring Automatic Detection of Login Pages
? Defining Brute Force Attacks
? Brute Force Protection Configuration
? Source-Based Brute Force Mitigations
? Defining Credential Stuffing
? Mitigating Credential Stuffing

Chapter 17: Reconnaissance with Session Tracking

? Defining Session Tracking
? Configuring Actions Upon Violation Detection

Chapter 18: Layer 7 DoS Mitigation

? Defining Denial of Service Attacks
? Defining the DoS Protection Profile
? Overview of TPS-based DoS Protection
? Creating a DoS Logging Profile
? Applying TPS Mitigations

? Defining Behavioral and Stress-Based Detection

Chapter 19: Advanced Bot Defense

? Classifying Clients with the Bot Defense Profile
? Defining Bot Signatures
? Defining F5 Fingerprinting
? Defining Bot Defense Profile Templates
? Defining Microservices protection

Chapter 20: Form Encryption using DataSafe

? Targeting Elements of Application Delivery
? Exploiting the Document Object Model
? Protecting Applications Using DataSafe
? The Order of Operations for URL Classification

Chapter 21: Review and Final Labs

? Final Lab Project (Option 1) – Production Scenario
? Final Lab Project (Option 2) – Managing Traffic with Layer 7 Local Traffic Policies