F5 Networks

F5ASM12: F5 Networks Configuring BIG-IP ASM: Application Security Manager

Lean how to use the features and functionality of BIG-IP Application Security Manager (ASM) in this 4-day course.

$4,620.00

- 4 Days

Upcoming Dates

Course Description

The BIG-IP Application Security Manager course gives participants a functional understanding of how to deploy, tune, and operate BIG-IP Application Security Manager (ASM) to protect their web applications from HTTP-based attacks.

The course includes lecture, hands-on labs, and discussion about different ASM components 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.

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: Traffic Processing with BIG-IP

- Identifying BIG-IP Traffic Processing Objects
- Understanding Network Packet Flow
- Understanding Profiles
- Overview of Local Traffic Policies and ASM

Chapter 3: Web Application Concepts

- Overview of Web Application Request Processing
- Web Application are vulnerable even with SSL
- Layer 7 Protection with Web Application Firewalls
- Examining HTTP and Web Application Components
- Overview of Web Communication Elements
- Parsing URLs
- Overview of the HTTP Request Structure
- HTTP Methods ASM Accepts by Default
- Comparing POST with GET
- Risks Within Other Methods
- HTTP Request Components: Headers

- Examining HTTP Responses
- User Input Forms: Free Text Input
- How ASM Parses File Types, URLs, and Parameters
- Using the Fiddler HTTP Proxy Tool

Chapter 4: Common Web Application Vulnerabilities

- Common Exploits Against Web Applications

Chapter 5: Security Policy Deployment

- Comparing Positive and Negative Security Models
- Approaching Deployment: Positive or Negative Security?
- The Deployment Wizard: How will Policy Builder Be Used?
- The Deployment Wizard Workflow
- Reviewing Requests
- Security Checks Offered by Rapid Deployment
- Response Checks Using Data Guard

Chapter 6: Policy Tuning and Violations

- Post-Configuration Traffic Processing
- Defining False Positives
- How Violations are Categorized
- Violation Rating: A Threat Scale
- Enforcement Settings & Staging: Global Policy Control
- Defining Signature Staging
- Defining the Enforcement Readiness Period
- Defining Learning
- Violations and Learning Suggestions
- Defining Learning Suggestions
- Choosing a Learning Mode: Automatic or Manual
- Defining the Learn, Alarm and Block settings
- Interpreting the Enforcement Readiness Summary
- Configuring the Blocking Response Page

Chapter 7: Attack Signatures

- Defining Attack Signatures
- Creating User-Defined Attack Signatures
- Defining Attack Signature Sets
- Defining Attack Signature Pools
- Updating Attack Signatures
- Understanding Attack Signatures and Staging

Chapter 8: Positive Security Policy Building

- Defining Security Policy Components
- Choosing the Learning Scheme
- How To Learn: Add All Entities
- Staging and Entities: The Entity Lifecycle
- How to Learn: Never (Wildcard Only)
- How to Learn: Selective
- Learning Differentiation: Real Threats or False Positives

Chapter 9: Cookies and Other Headers

- ASM Cookies: What to Enforce
- Understanding Allowed and Enforced Cookies

- Configuring Security Processing on HTTP headers

Chapter 10: Reporting and Logging

- Reporting: Build Your Own View
- Brute Force and Web Scraping Statistics
- PCI Compliance: PCI-DSS 3.0
- Viewing DoS Reports
- Generating a Security Events Report
- Local Logging Facilities and Destinations
- Viewing Current Log Files via Configuration Utility
- Logging Profile: Build What You Need

Chapter 11: User Roles and Policy Modification

- Defining User Roles
- Allowed Object References across Partitions
- Partitions Facilitate Administrative Agility
- Comparing Security Policies
- Merging Security Policies
- Editing and Exporting Security Policies
- Restoring with Policy History
- Examples of ASM Deployment Types
- ConfigSync and ASM Security Data
- ASMQKVIEW: Provide to F5 Support for Troubleshooting

Chapter 12: Lab Project 1

Chapter 13: Advanced Parameter Handling

- Defining Parameter Types
- Defining Static Parameters
- Defining Dynamic Parameters
- Defining Dynamic Parameter Extraction Properties
- Defining Parameter Levels
- Other Parameter Considerations

Chapter 14: Application-Ready Templates

- Templates: Pre-Configured Baseline Security

Chapter 15: Automatic Policy Building

- Overview of Automatic Policy Building
- Choosing a Policy Type
- Defining Trusted and Untrusted IP Addresses
- Defining the Learning Score

Chapter 16: Web Application Vulnerability Scanners

- Integrating ASM with Vulnerability Scanners
- Will Scan be Used for a New or Existing Policy?
- Importing vulnerabilities
- Resolving Vulnerabilities
- Using the Generic XML Scanner XSD file

Chapter 17: Login Enforcement & Session Tracking

- Defining a Login URL
- Defining Session Tracking

- Configuring Violation Detection Actions
- Session Hijacking Mitigation
- Fingerprinting Overview

Chapter 18: Brute Force and Web Scraping Mitigation

- Defining Anomalies
- Mitigating Brute Force Attacks via Login Page
- Defining Session-Based Brute Force Protection
- Defining Dynamic Brute Force Protection
- Defining the Prevention Policy
- Mitigating Web Scraping
- Defining Geolocation Enforcement
- Configuring IP Address Exceptions

Chapter 19: Layer 7 DoS mitigation

- Defining Denial of Service Attacks
- Defining DoS Profile General Settings
- Defining TPS-based DoS Protection
- Defining Operation Mode
- Defining Mitigation Methods
- Defining Stress-Based Detection
- Defining Proactive Bot Defense
- Using Bot Signatures

Chapter 20: ASM and iRules

- Identifying iRule Components
- Defining ASM iRule Commands
- Triggering iRules with Events
- Defining ASM iRule Events
- Using ASM iRule Event Modes

Chapter 21: XML and Web Services

- Defining XML
- Defining Web Services
- Using Web Services Security
- Defining the XML Profile
- XML Attack Signatures

Chapter 22: Web 2.0 Support: JSON Profiles

- Defining Asynchronous JavaScript and XML
- Defining JavaScript Object Notation (JSON)
- Configuring a JSON profile

Chapter 23: Review and Final Labs

Chapter 24: Additional Training and Certification

- Getting Started Series Web-Based Training
- F5 Instructor Led Training Curriculum
- F5 Professional Certification Program

Appendix A (Helpful Hints)

Appendix B (Rapid Deployment Methodology)

Appendix C (Additional Topics)

Appendix D (L1 and L2 Support Checklist)

Audience

This course is intended for security and network administrators who will be responsible for the installation, deployment, tuning, and day-to-day maintenance of the Application Security Manager.

Prerequisites

There are no required F5 technology-specific prerequisites for this course.

However, completing one the following before attending would be very helpful for students unfamiliar with BIG-IP:

- Administering BIG-IP instructor-led course
- F5 Certified BIG-IP Administrator

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

What You Will Learn

After completing this course, students will learn:

- Setting up the BIG-IP system
- Traffic processing with BIG-IP Local Traffic Manager (LTM)
- Web application concepts
- Web application vulnerabilities
- Security policy deployment
- Security policy tuning
- Attack signatures
- Positive security building
- Securing cookies and other headers
- Reporting and logging
- User roles
- Policy modification, merging, and exporting
- Advanced parameter handling
- Using application templates
- Using Automatic Policy Builder
- Integrating with web vulnerability scanners
- Login enforcement and session tracking
- Web scraping detection and mitigation
- Layer 7 DoS protection

- ASM and iRules
- XML and web services support
- AJAX and JSON support