ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

F5 Networks Configuring BIG-IP ASM v13: Application Security Manager

Course Summary

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 exploits.

Topics

- Setting up BIG-IP System
- Traffic Processing with BIG-IP
- Web Application Concepts
- Common Web Application Vulnerabilities
- Security Policy Deployment
- Policy Tuning and Violations
- Attack Signatures
- Positive Security Policy Building
- Cookies and Other Headers
- Reporting and Logging
- Lab Project
- User Roles and Policy Modification
- Advanced Parameter Handling
- Application-Ready Templates
- Automatic Policy Building
- Web Application Vulnerability Scanners
- Login Enforcement & Session Tracking
- Brute force and Web Scraping Mitigation
- Layered Policies
- Layer 7 DoS Mitigation
- ASM and iRules
- Content Profiles
- Review and Final Labs
- Additional Training and Certification

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

Administering BIG-IP; basic familiarity with HTTP, HTML and XML; basic web application and security concepts.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ProTech "Charting the Course ...

protechtraining.com

... to Your Success!"

F5 Networks Configuring BIG-IP ASM v13: Application Security Manager

Course Outline

I. Setting up BIG-IP System
- A. Introducing the BIG-IP System
- B. Initially Setting Up the BIG-IP System
- C. Archiving the BIG-IP Configuration
- D. F5 Support Resources and Tools

II. Traffic Processing with BIG-IP
- A. Identifying BIG-IP Traffic Processing Objects
- B. Understanding Network Packet Flow
- C. Understanding Profiles
- D. Overview of Local Traffic Policies and ASM
- E. HTTP Request Flow

III. Web Application Concepts
- A. Overview of Web Application Request Processing
- B. Web Application are vulnerable even with SSL
- C. Layer 7 Protection with Web Application Firewalls
- D. Overview of Web Communication Elements
- E. Parsing URLs
- F. Overview of the HTTP Request Structure
- G. Comparing POST with GET
- H. Risks within other methods
- I. Methods Enforcement for URLs
- J. HTTP Response Codes
- K. Examining HTTP Responses
- L. HTTP User Input Form Free Text Input
- M. User Input Forms Free Text input
- N. How ASM Parses File Types, URLs and Parameters
- O. Using the Fiddler HTTP Proxy

IV. Common Web Application Vulnerabilities
- A. Common Exploits Against Web Applications

V. Security Policy Deployment
- A. Comparing Positive and Negative Security
- B. Deployment Combining Positive and Negative Security
- C. The Deployment Workflow
- D. Policy Type How will the Policy be applied
- E. Policy Templates: Determines the level of protection
- F. Policy Template: Automatic or Manual Policy Building
- G. Deployment Workflow: Advanced Settings
- H. Viewing Requests
- I. Security Checks offered by Rapid Deployment
- J. Response Checks using Data Guard

VI. Policy Tuning and Violations
- A. Post-Deployment Traffic Processing
- B. Defining Violations
- C. Defining False Positives
- D. How violations are categorized
- E. Violation Ratings: A Threat Scale
- F. Defining Staging and Enforcement
- G. Defining Enforcement Mode
- H. Defining the Enforcement Readiness Period
- I. Defining Learning
- J. Defining Learning Suggestions
- K. Choosing Automatic or Manual Learning
- L. Defining the Learn, Alarm and Block Settings
- M. Interpreting the Enforcement Readiness Summary
- N. Configuring the Blocking Response Page

VII. Attack Signatures
- A. Defining Attack Signatures
- B. Creating User-Defined Attack Signatures
- C. Defining Attack Signature Sets
- D. Defining Attack Signature Pools
- E. Updating Attack Signatures
- F. Understanding Attack Signatures and Staging

VIII. Positive Security Policy Building
- A. Defining Security Policy Components
- B. Defining the Wildcard
- C. The Entity Staging Lifecycle
- D. Choosing the Learning Scheme
- E. How to Learn: Never (Wildcard only)
- F. How to Learn: Always
- G. How to Learn: Selective
- H. Reviewing the Enforcement Readiness Period Entities
- I. Violations Without Learning Suggestions
- J. Defining the Learning Score
- K. Defining Trusted and untrusted IP Address
- L. How to learn Compact

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

F5 Networks Configuring BIG-IP ASM v13: Application Security Manager

Course Outline (cont'd)

IX. Cookies and Other Headers
- A. ASM Cookies: What to Enforce
- B. Defining Allowed and Enforced Cookies
- C. Configuring Security Processing on HTTP Headers

X. Reporting and Logging
- A. Reporting : Build Your Own View
- B. Reporting: Chart based on filters
- C. Brute Force and Web Scraping Statistics
- D. Viewing ASM Reports
- E. PCI Compliance: PCI-DSS 3.0
- F. Viewing Log files and Local Graphics
- G. Logging Profiles: Build What you Need

XI. Lab Project

XII. User Roles and Policy Modification
- A. Defining User Roles
- B. Defining ASM User Roles
- C. Defining Partitions
- D. Configuring User Partition Access
- E. Comparing Security Policies with Policy Diff
- F. Merging Security Policies
- G. Editing and Exporting Security Policies
- H. Restoring with Policy History
- I. Examples of ASM Deployment Types
- J. ConfigSync and ASM Security Data
- K. ASMQKVIEW: Provide to F5 Support of Troubleshooting

XIII. Advanced Parameter Handling
- A. Defining Parameters Types
- B. Defining Static Parameters
- C. Defining Dynamic Parameters
- D. Defining Dynamic Parameter Extraction Properties
- E. Defining Parameter Levels
- F. Other Parameter Considerations

XIV. Application-Ready Templates
- A. Application Templates: Pre-Configured Baseline Security

XV. Automatic Policy Building
- A. Overview of Automatic Policy Building
- B. Defining Templates Which Automate Learning
- C. Defining Policy Loosening
- D. Defining Policy Tightening
- E. Defining Learning Speed Traffic Sampling
- F. Defining Track Site Changes

XVI. Web Application Vulnerability Scanners
- A. Integrating Scanner Output Into ASM
- B. Will Scan be Used for a New or Existing Policy?
- C. Importing Vulnerabilities•Resolving Vulnerabilities
- D. Using the Generic XML Scanner XSD file

XVII. Login Enforcement & Session Tracking
- A. Defining a Login URL
- B. Login Enforcement: Time and Logout Conditions
- C. Defining Session Tracking
- D. Configuring Actions Upon Violation Detection
- E. Session Hijacking Mitigation
- F. Why Fingerprint A Client

XVIII. Brute force and Web Scraping Mitigation
- A. Defining Anomalies
- B. Mitigating Brute Force Attacks via Login Page
- C. Defining Session-Based Brute Force Protection
- D. Defining Dynamic Brute Force Protection
- E. Defining the Prevention Policy
- F. Defining Web Scraping
- G. Defining Geolocation Enforcement
- H. Configuring IP Address Exceptions

IXX. Layer Policies
- A. Defining a Parent Policy
- B. Defining Inheritance
- C. Parent Policy Deployment Use Cases

XX. Layer 7 DoS Mitigation
- A. Defining Denial of Service Attacks
- B. Defining DoS Profile General Settings
- C. Defining Proactive Bot Defense
- D. Using Bot Signatures
- E. Defining TPS-based DoS Protection
- F. Defining Operation Mode
- G. Defining Mitigation Methods
- H. Defining Behavioral and Stress-Based Detection
- I. Defining Behavioral DoS

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

F5 Networks Configuring BIG-IP ASM v13: Application Security Manager

Course Outline (cont'd)

XXI. ASM and iRules

A. Common Uses for iRules
B. Identifying iRule Components
C. Triggering iRules with Events
D. Defining ASM iRule Events
E. Defining ASM iRule Commands
F. Using ASM iRule Event Modes

XXII. Content Profiles

A. Defining Asynchronous JavaScript and XML
B. Defining JavaScript Object Notation (JSON)
C. Defining Content Profiles
D. The Order of Operations for URL Classification

XXIII. Review and Final Labs

A. Course Review Questions
B. Answers to Review Questions

XXIIII. Additional Training and Certification

G. Getting Started Series Web-Based Training
H. F5 Instructor Led Training Curriculum
I. F5 Professional Certification Program

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically