F5 Networks Configuring BIG-IP Advanced WAF v14: Web Application Firewall (formerly ASM)

Duration: *4 Day(s)*

Course Overview

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.

Review this course online at https://www.alta3.com/courses/F5AWAFC14x

Objectives

- Deploy F5 Advanced Web Application Firewall to protect web applications.
- Recognize and mitigate multiple attack vectors such as web scraping and zero day exploits.
- Implement security policies and understand traffic processing within BIG-IP systems.
- Utilize iRules and advanced tools for comprehensive web threat defense.

Who Should Attend

- Security Administrators
- Network Administrators
- Web Application Developers
- IT Security Consultants

Prerequisites

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

Course Outline

Setting Up the BIG-IP System

1. Introducing the BIG-IP System
2. Initially Setting Up the BIG-IP System
3. Archiving the BIG-IP System Configuration
4. Leveraging F5 Support Resources and Tools

Traffic Processing with BIG-IP

5. Identifying BIG-IP Traffic Processing Objects
6. Overview of Network Packet Flow

7. Understanding Profiles
8. Overview of Local Traffic Policies
9. Visualizing the HTTP Request Flow

Web Application Concepts

10. Overview of Web Application Request Processing
11. Web Application Firewall: Layer 7 Protection
12. F5 Advanced WAF Layer 7 Security Checks
13. Overview of Web Communication Elements
14. Overview of the HTTP Request Structure
15. Examining HTTP Responses
16. How F5 Advanced WAF Parses File Types, URLs, and Parameters
17. Using the Fiddler HTTP Proxy

Common Web Application Vulnerabilities

18. A Taxonomy of Attacks: The Threat Landscape
19. What Elements of Application Delivery are Targeted?
20. Common Exploits Against Web Applications

Security Policy Deployment

21. Defining Learning
22. Comparing Positive and Negative Security Models
23. The Deployment Workflow
24. Policy Type: How Will the Policy Be Applied
25. Policy Template: Determines the Level of Protection
26. Policy Templates: Automatic or Manual Policy Building
27. Assigning Policy to Virtual Server
28. Deployment Workflow: Using Advanced Settings
29. Selecting the Enforcement Mode
30. The Importance of Application Language
31. Configure Server Technologies
32. Verify Attack Signature Staging
33. Viewing Requests
34. Security Checks Offered by Rapid Deployment
35. Defining Attack Signatures
36. Using Data Guard to Check Responses

Policy Tuning and Violations

37. Post-Deployment Traffic Processing
38. Defining Violations
39. Defining False Positives

Attack Signatures

Positive Security Policy Building

Cookies and Other Headers

Reporting and Logging

Lab Project 1

Advanced Parameter Handling

Policy Diff and Administration

Automatic Policy Building

Web Application Vulnerability Scanner Integration

Layered Policies

Login Enforcement, Brute Force Mitigation, and Session Tracking

Web Scraping Mitigation and Geolocation Enforcement

Layer 7 DoS Mitigation and Advanced Bot Protection

49. Defining Proactive Bot Defense
50. Defining Behavioral and Stress-Based Detection
51. Defining Behavioral DoS Mitigation

F5 Advanced WAF and iRules

52. Common Uses for iRules
53. Identifying iRule Components
54. Triggering iRules with Events
55. Defining F5 Advanced WAF iRule Events
56. Defining F5 Advanced WAF iRule Commands
57. Using F5 Advanced WAF iRule Event Modes

Using Content Profiles

58. Defining Asynchronous JavaScript and XML
59. Defining JavaScript Object Notation (JSON)
60. Defining Content Profiles
61. The Order of Operations for URL Classification

Review and Final Labs