F5 Networks Configuring BIG-IP Advanced WAF: 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/F5AWAFC

Objectives

- Deploy and configure the F5 Advanced Web Application Firewall
- Identify and mitigate web-based attack vectors
- Implement security policy tuning and traffic monitoring
- Use advanced tools for proactive threat detection and management

Who Should Attend

- Security Administrators
- Network Administrators
- IT Security Managers
- Cybersecurity Analysts

Prerequisites

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

Course Outline

Lesson 1: 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

Lesson 2: 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

Lesson 3: 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

Lesson 4: 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

Lesson 5: 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

Lesson 6: Policy Tuning and Violations

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

40. How Violations are Categorized
41. Violation Rating: A Threat Scale
42. Defining Staging and Enforcement
43. Defining Enforcement Mode
44. Defining the Enforcement Readiness Period
45. Reviewing the Definition of Learning
46. Defining Learning Suggestions
47. Choosing Automatic or Manual Learning
48. Defining the Learn, Alarm and Block Settings
49. Interpreting the Enforcement Readiness Summary
50. Configuring the Blocking Response Page

Lesson 7: Attack Signatures & Threat Campaigns

51. Defining Attack Signatures
52. Attack Signature Basics
53. Creating User-Defined Attack Signatures
54. Defining Simple and Advanced Edit Modes
55. Defining Attack Signature Sets
56. Defining Attack Signature Pools
57. Understanding Attack Signatures and Staging
58. Updating Attack Signatures
59. Defining Threat Campaigns
60. Deploying Threat Campaigns

Lesson 8: Positive Security Policy Building

61. Defining and Learning Security Policy Components
62. Defining the Wildcard
63. Defining the Entity Lifecycle
64. Choosing the Learning Scheme
65. How to Learn: Never (Wildcard Only)
66. How to Learn: Always
67. How to Learn: Selective
68. Reviewing the Enforcement Readiness Period: Entities
69. Viewing Learning Suggestions and Staging Status
70. Violations Without Learning Suggestions
71. Defining the Learning Score
72. Defining Trusted and Untrusted IP Addresses
73. How to Learn: Compact

Lesson 9: Cookies and Other Headers

74. F5 Advanced WAF Cookies: What to Enforce
75. Defining Allowed and Enforced Cookies

76. Configuring Security Processing on HTTP headers

Lesson 10: Reporting and Logging

77. Overview: Big Picture Data
78. Reporting: Build Your Own View
79. Reporting: Chart based on filters
80. Brute Force and Web Scraping Statistics
81. Viewing F5 Advanced WAF Resource Reports
82. PCI Compliance: PCI-DSS 3.0
83. The Attack Expert System
84. Viewing Traffic Learning Graphs
85. Local Logging Facilities and Destinations
86. How to Enable Local Logging of Security Events
87. Viewing Logs in the Configuration Utility
88. Exporting Requests
89. Logging Profiles: Build What You Need
90. Configuring Response Logging

Lesson 11: Lab Project 1

Lesson 12: Advanced Parameter Handling

1. Defining Parameter Types
2. Defining Static Parameters
3. Defining Dynamic Parameters
4. Defining Dynamic Parameter Extraction Properties
5. Defining Parameter Levels
6. Other Parameter Considerations

Lesson 13: Automatic Policy Building

7. Overview of Automatic Policy Building
8. Defining Templates Which Automate Learning
9. Defining Policy Loosening
10. Defining Policy Tightening
11. Defining Learning Speed: Traffic Sampling
12. Defining Track Site Changes

Lesson 14: Web Application Vulnerability Scanner Integration

13. Integrating Scanner Output
14. Importing Vulnerabilities
15. Resolving Vulnerabilities
16. Using the Generic XML Scanner XSD file

Lesson 15: Deploying Layered Policies

17. Defining a Parent Policy
18. Defining Inheritance
19. Parent Policy Deployment Use Cases

Lesson 16: Login Enforcement and Brute Force Mitigation

20. Defining Login Pages
21. Configuring Automatic Detection of Login Pages
22. Defining Session Tracking
23. What Are Brute Force Attacks?
24. Brute Force Protection Configuration
25. Defining Source-Based Protection
26. Source-Based Brute Force Mitigations
27. Defining Credentials Stuffing
28. Mitigating Credentials Stuffing

Lesson 17: Reconnaissance with Session Tracking

29. Defining Session Tracking
30. Configuring Actions Upon Violation Detection

Lesson 18: Layer 7 DoS Mitigation

31. Defining Denial of Service Attacks
32. Defining the DoS Protection Profile
33. Overview of TPS-based DoS Protection
34. Create a DoS Logging Profile
35. Applying TPS Mitigations
36. Defining Behavioral and Stress-Based Detection

Lesson 19: Advanced Bot Protection

37. Classifying Client with the Bot Defense Profile
38. Defining Bot Signatures
39. Defining Proactive Bot Defense
40. Defining Behavioral and Stress-Based Detection
41. Defining Behavioral DoS Mitigation

Lesson 20: Form Encryption using DataSafe

42. Targeting Elements of Application Delivery
43. Exploiting the Document Object Model
44. Protecting Applications Using DataSafe

45. The Order of Operations for URL Classification

Lesson 21: Review and Final Labs