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

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

Attack Signatures

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

Positive Security Policy Building

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

Cookies and Other Headers

72. F5 Advanced WAF Cookies: What to Enforce
73. Defining Allowed and Enforced Cookies
74. Configuring Security Processing on HTTP headers

Reporting and Logging

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

Lab Project 1

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

Policy Diff and Administration

7. Comparing Security Policies with Policy Diff
8. Merging Security Policies
9. Restoring with Policy History
10. Examples of F5 Advanced WAF Deployment Types
11. ConfigSync and F5 Advanced WAF Security Data
12. ASMQKVIEW: Provide to F5 Support for Troubleshooting

Automatic Policy Building

13. Overview of Automatic Policy Building
14. Defining Templates Which Automate Learning
15. Defining Policy Loosening
16. Defining Policy Tightening
17. Defining Learning Speed: Traffic Sampling
18. Defining Track Site Changes

Web Application Vulnerability Scanner Integration

19. Integrating Scanner Output into F5 Advanced WAF
20. Will Scan be Used for a New or Existing Policy?
21. Importing Vulnerabilities
22. Resolving Vulnerabilities
23. Using the Generic XML Scanner XSD file

Layered Policies

24. Defining a Parent Policy
25. Defining Inheritance
26. Parent Policy Deployment Use Cases

Login Enforcement, Brute Force Mitigation, and Session Tracking

27. Defining Login Pages
28. Configuring Automatic Detection of Login Pages
29. Defining Session Tracking
30. What Are Brute Force Attacks?
31. Brute Force Protection Configuration
32. Defining Source-Based Protection
33. Source-Based Brute Force Mitigations
34. Defining Session Tracking
35. Configuring Actions Upon Violation Detection
36. Session Hijacking Mitigation Using Device ID

Web Scraping Mitigation and Geolocation Enforcement

37. Defining Web Scraping
38. Mitigating Web Scraping
39. Defining Geolocation Enforcement
40. Configuring IP Address Exceptions

Layer 7 DoS Mitigation and Advanced Bot Protection

41. Defining Denial of Service Attacks
42. The General Flow of DoS Protection
43. Defining the DoS Profile
44. Overview of TPS-based DoS Protection
45. Applying TPS mitigations
46. Create a DoS Logging Profile
47. Defining DoS Profile General Settings
48. Defining Bot Signatures

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