Training: F5

Configuring BIG-IP Advanced WAF: Web Application Firewall

TRAINING GOALS:

Learn to deploy and operate F5 Advanced WAF to protect web applications from the most critical security risks as described in the OWASP Top 10 list, from bots and other automated agents, and from Denial of Service (DoS) attacks operating at the HTTP layer of the web application delivery ecosystem. Through a combination of lecture, hands-on labs, and discussion, secure applications from the majority of common attacks by the end of the first day. Take technical deep dives into mitigating web scraping, account aggregation, account creation, ad fraud, CAPTCHA defeat, card cracking, carding, cashing out, credential stuffing, and other unwanted automated application abuse as described in the OWASP automated threats list.

Observe various vulnerability mitigations in real time by playing the role of an attacker in lab exercises. Gain context for securing applications, including analysis of HTTP and the elements of both modern and traditional web applications such as file types, parameters, URLs, and login pages. Learn to recognize client and server-side technologies such as JSON and AJAX, and learn to address vulnerabilities that might be present in common application development tools such as PHP, AngularJS, and others.

Review recommended practices for reporting, security event logging, and integration with third-party web application vulnerability scanners in detail. Follow prescribed step-by-step directions for activities initially, and gradually gain proficiency so that, by the end of class, little or no instruction is needed to complete simple to more complex configurations.

Audience

This course is intended for SecOps personnel responsible for the deployment, tuning, and day-to-day maintenance of F5 Adv. WAF. Participants will obtain a functional level of expertise with F5 Advanced WAF, including comprehensive security policy and profile configuration, client assessment, and appropriate mitigation types. Experience with LTM and prior WAF knowledge are not required.

CONSPECT:

- Chapter 1: Introducing the BIG-IP System

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Initially Setting Up the BIG-IP System
- Archiving the BIG-IP Configuration
- Leveraging F5 Support Resources and Tools

- Chapter 2: Traffic Processing with BIG-IP
  - Identifying BIG-IP Traffic Processing Objects
  - Understanding Profiles
  - Overview of Local Traffic Policies
  - Visualizing the HTTP Request Flow
- Chapter 3: Overview of Web Application Processing
  - Web Application Firewall: Layer 7 Protection
  - Layer 7 Security Checks
  - Overview of Web Communication Elements
  - Overview of the HTTP Request Structure
  - Examining HTTP Responses
  - How F5 Advanced WAF Parses File Types, URLs, and Parameters
  - Using the Fiddler HTTP Proxy
- Chapter 4: Overview of Web Application Vulnerabilities
  - A Taxonomy of Attacks: The Threat Landscape
  - Common Exploits Against Web Applications
- Chapter 5: Security Policy Deployments: Concepts and Terminology
  - Defining Learning
  - Comparing Positive and Negative Security Models
  - The Deployment Workflow
  - Assigning Policy to Virtual Server
  - Deployment Workflow: Using Advanced Settings
  - Configure Server Technologies
  - Defining Attack Signatures
  - Viewing Requests
  - Security Checks Offered by Rapid Deployment
- Chapter 6: Policy Tuning and Violations
  - Post-Deployment Traffic Processing
  - How Violations are Categorized
  - Violation Rating: A Threat Scale
  - Defining Staging and Enforcement
  - Defining Enforcement Mode
  - Defining the Enforcement Readiness Period

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Reviewing the Definition of Learning
- Defining Learning Suggestions
- Choosing Automatic or Manual Learning
- Defining the Learn, Alarm and Block Settings
- Interpreting the Enforcement Readiness Summary
- Configuring the Blocking Response Page

- Chapter 7: Using Attack Signatures and Threat Campaigns
  - Defining Attack Signatures
  - Attack Signature Basics
  - Creating User-Defined Attack Signatures
  - Defining Simple and Advanced Edit Modes
  - Defining Attack Signature Sets
  - Defining Attack Signature Pools
  - Understanding Attack Signatures and Staging
  - Updating Attack Signatures
  - Defining Threat Campaigns
  - Deploying Threat Campaigns
- Chapter 8: Positive Security Policy Building
  - Defining and Learning Security Policy Components
  - Defining the Wildcard
  - Defining the Entity Lifecycle
  - Choosing the Learning Scheme
  - How to Learn: Never (Wildcard Only)
  - How to Learn: Always
  - How to Learn: Selective
  - Reviewing the Enforcement Readiness Period: Entities
  - Viewing Learning Suggestions and Staging Status
  - Defining the Learning Score
  - Defining Trusted and Untrusted IP Addresses
  - How to Learn: Compact
- Chapter 9: Securing Cookies and other Header Topics
  - The Purpose of F5 Advanced WAF Cookies
  - Defining Allowed and Enforced Cookies
  - Securing HTTP headers
- Chapter 10: Visual Reporting and Logging
  - Viewing Application Security Summary Data

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Reporting: Build Your Own View
- Reporting: Chart based on filters
- Brute Force and Web Scraping Statistics
- Viewing Resource Reports
- PCI Compliance: PCI-DSS 3.0
- Analyzing Requests
- Local Logging Facilities and Destinations
- Viewing Logs in the Configuration Utility
- Defining the Logging Profile
- Configuring Response Logging

- Chapter 11: Lab Project 1
- Chapter 12: Advanced Parameter Handling
  - Defining Parameter Types
  - Defining Static Parameters
  - Defining Dynamic Parameters
  - Defining Parameter Levels
  - Other Parameter Considerations
- Chapter 13: Automatic Policy Building
  - Defining Templates Which Automate Learning
  - Defining Policy Loosening
  - Defining Policy Tightening
  - Defining Learning Speed: Traffic Sampling
  - Defining Track Site Changes
- Chapter 14: Integrating with Web Application Vulnerability Scanners
  - Integrating Scanner Output
  - Importing Vulnerabilities
  - Resolving Vulnerabilities
  - Using the Generic XML Scanner XSD file
- Chapter 15: Deploying Layered Policies
  - Defining a Parent Policy
  - Defining Inheritance
  - Parent Policy Deployment Use Cases
- Chapter 16: Login Enforcement and Brute Force Mitigation
  - Defining Login Pages for Flow Control
  - Configuring Automatic Detection of Login Pages
  - Defining Brute Force Attacks

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

    - Brute Force Protection Configuration
    - Source-Based Brute Force Mitigations
    - Defining Credential Stuffing
    - Mitigating Credential Stuffing
- Chapter 17: Reconnaissance with Session Tracking
    - Defining Session Tracking
    - Configuring Actions Upon Violation Detection
- Chapter 18: Layer 7 Denial of Service Mitigation
    - Defining Denial of Service Attacks
    - Defining the DoS Protection Profile
    - Overview of TPS-based DoS Protection
    - Creating a DoS Logging Profile
    - Applying TPS Mitigations
    - Defining Behavioral and Stress-Based Detection
- Chapter 19: Advanced Bot Defense
    - Classifying Clients with the Bot Defense Profile
    - Defining Bot Signatures
    - Defining F5 Fingerprinting
    - Defining Bot Defense Profile Templates
    - Defining Microservices protection
- Chapter 20: Final Projects

REQUIREMENTS:

The following free Self-Directed Training (SDT) courses, although optional, are helpful for any student with limited BIG-IP administration and configuration experience:

- Getting Started with BIG-IP
- Getting Started with Local Traffic Manager (LTM)
- Getting Started with F5 Advanced WAF

General network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course, including OSI model encapsulation, routing and switching, Ethernet and ARP, TCP/IP concepts, IP addressing and subnetting, NAT and private IP addressing, NAT and private IP addressing, default gateway, network firewalls, and LAN vs. WAN.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by F5 (course completion).

This course helps prepare participants for the F5 Certified Technology Specialist, BIG-IP ASM (F5-CTS, BIG-IP ASM) certification. Candidates must first hold the F5 Certified Administrator, BIG-IP credential and then pass the BIG-IP ASM Specialist exam (303).

More information: https://education.f5.com/learning-path/view/16

This course helps prepare participants for the F5 Certified Solution Expert, Security (F5-CSE, SEC) certification. Before taking the Security Solutions exam (401), candidates must hold all of the following credentials: F5 Certified Administrator, BIG-IP (F5-CA, BIG-IP); F5 Certified Technology Specialist, BIG-IP LTM (F5-CTS, BIG-IP LTM); F5 Certified Technology Specialist, BIG-IP ASM (F5-CTS, BIG-IP ASM); and F5 Certified Technology Specialist, BIG-IP APM (F5-CTS, BIG-IP APM).

More information: https://education.f5.com/learning-path/view/20

TRAINER:

Certified F5 Networks Trainer.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310