Setting up F5 Advanced WAF

Chapter 1: Setting Up the BIG-IP System

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

Chapter 2: Threat Overview and Guided Configuration

- Today's Threat Landscape
- Differentiating Benign and Malicious Clients
- Categorizing Attack Techniques
- Defining the Layer 7 Web Application Firewall
- Defining Traffic Processing Objects
- Introducing F5 Advanced WAF
- Using Guided Configuration for Web Application Security

Chapter 3: Exploring HTTP Traffic

- Exploring Web Application HTTP Request Processing
- Overview of Application-Side Vulnerabilities
- Defining Attack Signatures
- Defining Violations

Chapter 4: Securing HTTP Traffic

- Defining Learning
- Defining Attack Signature Staging
- Defining Attack Signature Enforcement

Chapter 5: Mitigating Credentials Stuffing

- Defining Credentials Stuffing Attacks
- Credential Stuffing Mitigation Workflow

Chapter 6: Form Encryption Using BIG-IP DataSafe

- What Elements of Application Delivery are Targeted?

- Exploiting the Document Object Model
- Protecting Applications Using DataSafe
- Configuring a DataSafe Profile

Chapter 7: Deploying Threat Campaigns

- Defining Threat Campaigns
- Live Update for Threat Campaigns

Chapter 8: Using L7 Behavioral Analysis to Mitigate DoS

- Defining Behavioral Denial of Service Mitigation
- Defining the DoS Protection Profile