BIG-IP Application Security Manager v11.2 Table of Contents

Preface P-1
F5 Networks P-1
F5 Product Suite Overview P-1
Hardware P-4
Virtual Editions P-8
F5 Services P-9
F5 Resources and Tools P-11

Module 1: Installation & Initial Access 1-1
BIG-IP ASM Overview 1-1
ASM Feature Set Summary 1-2
ASM Protection Summary 1-3
BIG-IP ASM Hardware Platforms 1-3
BIG-IP ASM Deployment Types 1-6
BIG-IP ASM Standalone 1-6
BIG-IP ASM in-line with BIG-IP LTM 1-6
Multiple BIG-IP ASM devices behind a BIG-IP LTM 1-6
BIG-IP ASM module on BIG-IP LTM 1-6
BIG-IP ASM Device Group 1-7
BIG-IP ASM Virtual Edition (VE) 1-7
Licensing and the Setup Utility 1-8
Configuration Process 1-8
Management Port Serial Console 1-9
License Administration 1-10
License Activation via the Configuration Utility 1-11
Web Configuration Utility 1-13
Command Line Access 1-14
Provisioning 1-15
Installation and Setup Labs 1-17
Lab – Installation and Setup 1-17
Lab – System Licensing 1-19
Lab – Setup Utility 1-21
Lab – Configuration Backup 1-23

Module 2: Web Application Concepts 2-1
Anatomy of a Web Application 2-1
Secure Socket Layer 2-4

Hardened Servers 2-4
Network Firewalls 2-4
Web Application Firewalls 2-6

HTTP & HTML Web Page Components 2-7
Overview of Web Communication 2-7
Parsing URLs 2-8
HTTP Requests 2-8
GET Method 2-9
POST Method 2-9
HEAD Method 2-10
Uniform Resource Identifier 2-10
Query Strings 2-10
HTTP Version 2-11
HTTP Headers 2-11
HTTP Responses 2-14
HTTP Response Status Codes 2-14
HTML Concepts Overview 2-15
User Input Forms 2-15
Using Fiddler 2-17
Lab – Fiddler 2-20

Module 3: Web Application Vulnerabilities 3-1
Web Application Vulnerabilities Overview 3-1
Open Web Application Security Project Top 10 (2010) 3-1
Injection attacks 3-2
Cross Site Scripting 3-2
Broken Authentication and Session Management 3-5
Insecure Direct Object references 3-6
Hidden Field Manipulation 3-6
Cross Site Request Forgery 3-7
Security Misconfiguration 3-8
Insecure Cryptographic Storage 3-9
Failure to Restrict URL Access 3-9
Insufficient Transport Layer Protection 3-10
Unvalidated Redirects and Forwards 3-11
Parameter tampering 3-12
Cookie Poisoning 3-12
Denial of Service and Distributed Denial of Service 3-13
Brute Force 3-14

Risk Mitigation and ASM 3-15
Lab – HTTP Vulnerabilities 3-16

Module 4: ASM Configuration 4-1
Nodes 4-1
Pool Member 4-1
Pools 4-1
Pool Configuration 4-2
Virtual Servers 4-2
Network Packet Flow 4-3
HTTP Classes 4-4
HTTP Traffic Classifiers 4-4
HTTP Classes: Actions 4-4
HTTP Class Profile Configuration 4-4
SSL Termination/Initiation 4-6
Virtual Server Configuration 4-7
HTTP Request Flow 4-8
Lab – Pool, HTTP Profile, and Virtual Server Configuration 4-9

Module 5: Security Policy Overview 5-1
Positive Security Model 5-1
Negative Security Model 5-2
Basic Security Policy Creation and Initial Configuration 5-2
Security Policy Name 5-2
Defining an Application Language 5-2
Application-Ready Security Policy 5-3
Dynamic Session ID in URL 5-3
Staging-Tightening Period 5-3
Case Sensitive Security Policy 5-3
Maximum HTTP Header Length 5-3
Maximum Cookie Header Length 5-3
Allowed Response Status Codes 5-3
Trigger ASM iRule Events 5-4
Trust XFF Header 5-4
Security Policy Components 5-5
File Types 5-5
URLs 5-6
Parameters 5-6
Methods 5-7
Headers 5-7

Cookie Processing in ASM 5-7
Wildcard Entities 5-9
Violations and Traffic Learning 5-10
Tightening 5-11
Staging 5-11
Requests 5-12
Security Policy Blocking 5-14
Learn, Alarm, and Block Flags 5-14
Blocking Response Page 5-15
Lab – Security Policy Configuration 5-16
Attack Signatures 5-19
Attack Signature Pool 5-20
Attack Signature Sets 5-20
User-defined Attack Signatures 5-21
Lab – User-defined Attack Signatures 5-24

Module 6: Deployment Wizard 6-1
Deployment Wizard 6-1
Rapid Deployment Scenarios 6-1
Data Guard 6-3
Rapid Deployment Methodology 6-4
Lab – Rapid Deployment 6-5
Lab – Data Guard 6-9
Lab – Attack Signatures 6-11
Application-Ready Security Policy 6-13
Rapid Deployment Configuration 6-15
Lab – Application-Ready Security Policy Lab 6-17

Module 7: Vulnerability Assessment Tools 7-1
Creating a new baseline policy 7-1
Adding a vulnerability assessment to an existing policy 7-1
Resolving vulnerabilities 7-2
WhiteHat Sentinel 7-2
IBM Rational AppScan 7-3
Cenzic Hailstorm 7-3
QualysGuard 7-5
Lab – Option 1: WhiteHat Sentinel 7-6
Lab – Option 2: Qualys 7-8
Lab – Option 3: AppScan 7-10
Lab – Option 4: Cenzic 7-12

Module 8: Application Visibility & Reporting 8-1
AVR Prerequisites 8-1
Analytics profile 8-1
Lab – Analytics Profile Setup 8-2
Dashboard 8-3
Reporting Overview 8-3
Charts 8-4
PCI Compliance Reports 8-5
Lab – PCI Compliance Reporting 8-6
Logs 8-7
Viewing Log Files 8-7
Logging Profiles 8-9
Event Correlation 8-10
Response Logging 8-10
Lab – Logging messages locally and remotely 8-11
Lab – Response logging 8-13

Module 9: Administering ASM 9-1
Defining partitions 9-1
User Management and Roles 9-1
Lab – Partitions and User Roles 9-4
Modifying Security Policies 9-7
Lab – Security Policy Modification 9-8
ASM Synchronization 9-10
Device Groups 9-10
qkview 9-11

Module 10: Lab Project 10-1

Module 11: Traffic Learning 11-1
Learning Concepts Overview 11-1
Learning Process Resources 11-2
Length Learning 11-3
Pattern Learning 11-4
Meta-Character Learning 11-4
RFC Violations 11-5
Access Violations 11-6
Length Violations 11-8
Input Violations 11-9
Cookie Violations 11-11
Lab – Traffic Learning 11-17

Table of Contents

Module 12: Parameters 12-1
Parameter Overview 12-1
Parameter Types 12-2
Sensitive Parameters 12-2
User Input Parameter Value Types 12-3
Static Parameter Value Types 12-4
Dynamic Parameter Value Types 12-4
Extractions 12-5
XML Value Types 12-6
JSON Value Types 12-6
Parameter Character Sets 12-6
Parameter Levels 12-7
Global Parameters 12-7
URL Parameters 12-8
Flow Parameters 12-8
Parameter Logic 12-8
Lab – Protecting Dynamic Parameters 12-10
Lab – Protecting Static Parameters 12-13

Module 13: Real Traffic Policy Builder 13-1
Real Traffic Policy Builder Configuration 13-1
Real Traffic Policy Builder Configuration Example 13-2
Real Traffic Policy Builder Policy Types 13-6
Automatic Policy Building Stages 13-7
Real Traffic Policy Builder Rules 13-7
Trusted and Untrusted IPs 13-8
Lab – Automatic Security Policy Builder 13-10
Lab – Automatic Security Policy Builder (option2) 13-13

Module 14: Advanced Topics 14-1
iRules 14-1
iRule Syntax 14-2
ASM iRule Events 14-2
ASM iRule Commands 14-3
TcL Commands 14-4
iRule Configuration 14-6
Lab – iRule creation and configuration 14-7
Sessions and Logins 14-10
Lab – Login URL Creation 14-12
Lab – Session Awareness and Tracking 14-15

Lab – Username Session Tracking 14-18
Anomaly Detection 14-21
Denial of Service Attacks 14-21
Brute Force Attacks 14-22
Lab – Session-based Brute Force 14-24
IP Enforcer 14-26
Web Scraping 14-26
Lab – Web Scraping 14-28
Anti_Virus Protection 14-30
Cross-site Request Forgery Protection 14-31
Lab – Cookie Enforcement 14-32
Geolocation Enforcement 14-37
Lab –Geolocation Enforcement 14-38
IP Address Exceptions 14-40
Lab –IP Address Exception 14-41

Module 15: XML and Web Services 15-1
XML Concepts 15-1
Web Services Concepts 15-2
XML Profile 15-2
Schema and WSDL Validation 15-3
XML Attack Signatures 15-3
Web Services Security 15-7
Defense Configuration 15-5
Associating and XML Profile with an URL 15-8
Associating and XML Profile with a parameter 15-8
Lab – XML and Web Services 15-9

Module 16: AJAX and JSON concepts 16-1
AJAX Overview 16-1
JSON Overview 16-2
ASM Support of AJAX/JSON 16-3
JSON Profile 16-4
Associating a JSON Profile with a URL 16-4
Associating a JSON Profile with a Parameter 16-4
Lab – JSON Parsing 16-5

Table of Contents

Module 17: Protocol Security Module 17-1

FTP Overview 17-2

FTP Security Profile Configuration 17-4

SMTP Protection 17-5

SMTP Security Profile Configuration 17-6

HTTP Security 17-8

HTTP Security Profile Configuration 17-9

PSM Statistics 17-13

Lab – Protocol Security Module 17-18

Module 18: IP Address Intelligence 18-1

iprepd daemon 18-1

Licensing 18-1

Requirements 18-2

Post-license troubleshooting 18-3

ASM Settings 18-4

IP Address Whitelist 18-5

IP Address Intelligence categories 18-6

IP Address Intelligence learning 18-8

Module 19: Analytics Review & Final Project 19-1

Lab – Analytics Review 19-1

Review Questions 19-2

Lab – Configuration Lab Project 2 19-4

Appendix A (Installation Guidelines) A-1

Appendix B (New Features for 11.2) B-1

Appendix C Additional Topics C-1

Traffic Capturing Using HTTPWatch C-1

Lab – Using HttpWatch C-4

Regular Expressions C-6

Writing Rules for User-Defined Attack Signatures C-16

Appendix D (Helpful hints) D-1

Appendix E (Protecting a production environment) E-1

PowerPoint Presentation Printout