F5 Big-IP Application Security Manager v11

Code: ACBE–F5-ASM

Days: 4

Course Description:

This four-day course gives networking professionals a functional understanding of the BIG-IP® LTM v11 system as it is commonly used, as well as an in-depth understanding of advanced features. The course covers installation, configuration, and management of BIG-IP LTM systems. This hands-on course includes lectures, labs, and discussions.

Course Summarize:

Module 1: Installation & Initial Access

- BIG IP ASM Overview
- ASM Feature Set Summary
- ASM Protection Summary

BIG-IP ASM Deployment Types

- BIG-IP ASM Standalone
- BIG-IP ASM in-line with BIG-IP LTM
- Multiple BIG-IP ASM devices behind a BIG-IP LTM
- BIG-IP ASM module on BIG-IP LTM
- BIG-IP ASM Device Group
- BIG-IP ASM Virtual Edition

Licensing and the Setup Utility

- Configuration Process
- Accessing the Web Configuration Utility
- Command Line Access
- Provisioning

Installation and Setup Labs

- Lab – Installation and Setup
- Lab – System Licensing
- Lab – Setup Utility
- Lab – Configuration Backup

Module 2: Web Application Concepts

- Anatomy of a Web Application
- Secure Socket Layer
- Server Hardening
- Network Firewalls and Application Security
- Web Application Firewalls

HTTP & HTML Web Page Componets

- HTTP Concepts Overview
- HTTP Request Components
- HTTP Methods
- Uniform Resource Identifier
- HTTP Version
- HTTP Headers
- HTTP Responses
- Response Status Codes
- HTML Concepts Overview
- HTTP Header Overview
- Public vs Private
- No-Cache and No Store
- HTML Concepts Overview
- Expiration Indicators
- Content Duration
- Header Types
- User Input Forms
- Using Fiddler2
- Lab – Fiddler2

Module 3: Web Application Vulnerabilities

- Web Application Vulnerabilities Overview
- Injection attacks
- Cross Site Scripting
- Broken Authentication and Sessions Management
- Insecure Direct Object References
- Forceful Browsing
- Cross Site Request Forgery

- Hidden Field Manipulation
- Cookie Poisoning
- Unvalidated Redirects and Forwards
- Risk Mitigation and ASM
- Lab – HTTP Vulnarabilities

Module 4: ASM Application Configuration

- Pool Members and Pools
- Nodes
- Virtual Servers
- Network Packet Flow
- HTTP Classes
- Application Security Class
- HTTP Class Filters
- Virtual Server Configuration
- SSL Termination/Initiation
- HTTP Request Flow
- Lab – Web Application Configuration

Module 5: Security Policy Overview

- Positive Security Model
- Negative Security Model
- Security Policy Properties
- Security Policy Configuration
- Security Policy Components
- File Types
- URLs
- Parameters
- Wildcard Entities
- Violations and Traffic Learning
- Tightening
- Staging
- Methods
- Headers
- Cookie Processing in ASM
- Requests

- Traffic Learning
- Policy Blocking
- Lab – Security Policy
- Attack Signatures
- Attack Signature Pools and Sets
- Lab – Attack Signatures

Module 6: Security Policy Building Tool

- Deployment Wizard
- Rapid Deployment Scenarios
- Data Guard
- Rapid Deployment Methodology
- Lab – Rapid Deployment
- Lab – Data Guard
- Lab – Attack Signatures
- WhiteHat Sentinel

Module 7: Application-Ready Security Policy

- Overview
- Lab – Application – Ready Security Policy Lab

Module 8: Configuration Lab Project 1

Module 9: Reporting

- Dashboard
- Reporting Overview
- Charts
- PCI Compliance Reports
- Lab – Reporting
- Logs
- Logging Profiles
- Lab – Logging messages locally and remotely

Module 10: Administering ASM

- ASM User Management
- Lab – Partitions and User Roles

- Modifying Security Policies
- Lab – Modifying Security Policy
- ASM Synchronization
- Device Groups
- Qkview

Module 11: Traffic Learning

- Learning Concepts Overview
- Learning Process Resources
- Length Learning
- Pattern Learning
- Meta-Character Learning
- Violations
- Lab – Traffic Learning

Module 12: Parameters

- Parameters Overview
- Parameters Types
- User Input Parameter Value Types
- Static Parameter Value Types
- Dynamic Parameter Value Types
- ExtractionsXML Value Types
- JSON Value Types
- Parameter Character Sets
- Parameter Levels
- Global Parameters
- URL Parameters
- Flow Parameters
- Parameter Logic
- Lab – Protecting Dynamic Parameters
- Lab – Protecting Static Parameters

Module 13: Security Policy Builder

- Policy Builder Introduction
- Policy Builder Configuration
- Policy Builder Policy Types
- Policy Builder Rules

- Lab – Security Policy Builder

Module 14: Advanced Topics

- iRules
- iRule Syntax
- ASM iRule Events
- ASM iRule Commands
- TcL Commands
- iRule Configuration
- Lab – iRule creation and configuration
- Login Pages
- Lab – Login Page Protection
- Anomaly Detection
- Denial of Service Attacks
- Brute Force Attacks
- IP Enforcer
- Web Scraping
- Lab – Web Scraping
- Anti-Virus Protection
- Configurable ICAP servers
- Cross-Site Request Forgery Protection

Module 15: XML and Web Services

- XML Concepts
- XML Profile
- Web Services Protection
- Validation Enforcement Configuration
- Securing XML content
- XML Attack Signatures
- Web Services Security
- Defense Configuration
- Defense Formatting Settings
- Associating and XML Profile with an URL
- Lab – XML and Web Services

Module 16: AJAX and JSON Concepts

- AJAX Overview
- JSON Overview
- ASM Support of AJAX/JSON
- JSON Profile
- Associating a JSON Profile with a URL
- Associating a JSON Profile with a Parameter
- Lab – JSON Parsing

Module 17: Protocol Security Manager

- Protocol Security Manager Overview
- FTP Protection
- Active Mode
- Passive Mode
- FTP Security Profile Configuration
- SMTP Protection
- SMTP Security Profile Configuration
- HTTP Security Profile Overview
- HTTP Security Profile Configuration
- Protocol Security Manager Statistics
- Configuring Protocol Security Manager
- Lab – Protocol Security Manager FTP

Module 18: Configuration Lab Project 2

- Review Questions
- Configuration Lab Project 2

Appendix A - Pre-Installation checklist

- Configuration Worksheet

Appendix B-New Features for ASM v11

Appendix C-Additional Topics

- Traffic Capturing using HTTPWatch
- Lab – HTTP Watch Lab
- Regular Expressions
- Writing Rules for User-Defined Attack