Imperva Application Security - WAF Gateway

Overview

In this 4 day hands-on course, students will learn:

- _Configure SecureSphere for an on premises Web Application Firewall including ThreatRadar subscription services
- _Evaluate the configuration of the Web Application Firewall to verify assets are protected
- _Implement security controls using Policies and Followed Actions
- _Configure Web Profiling and Active Blocking
- _Analyze Violations and Alerts
- _Perform best practice tuning tasks
- _Integrate external web scanner data with SecureSphere and manage identified vulnerabilities. Configure SecureSphere Web Gateway to work in a Reverse Proxy deployment mode

Course Length

4 days

Who Should Attend

This course is intended for security administrators, security analysts, security engineers, and Web application developers who are responsible for securing and monitoring Web applications with SecureSphere.

Prerequisites

Before taking this course, you should have the following skills:

- _General understanding of application layer security concepts, application layer Web, and/or database protocols.
- _Basic understanding of HTML and HTTP o URLs, Parameters, headers, methods, HTTP server response codes, etc.
- _Experience implementing or managing data center security or database applications.

Lesson Objectives

Lesson 1: Lab Environment and SecureSphere Web UI

- _Review the SecureSphere Architecture
- _Become familiar with the presentation of the training materials.
- _Learn to use the Imperva training portal to find supplemental course materials.
- _Become familiar with the lab environment, topology, and user accounts.
- _Become familiar with the SecureSphere Web UI's major components and navigating the Web UI.

Lesson 2: Initial Web UI Configuration

- _Set password strength requirements.
- _Enable users to enter comments when making changes to security policies.
- _Create SecureSphere user accounts and roles.
- _Configure Active Directory authentication.
- _Update ADC content.

Lesson 3: Sites Tree Configuration

- _Create a Site.
- _Create a Server Group.
- _Create a Service and default Application.
- _Discover and secure previously unknown servers on the network.
- _Add discovered servers to a Site.

Lesson 4: HTTP Service Configuration

- _Configure Forwarded Connections (Load Balanced Traffic)
- _Install Protected Web Servers' SSL Keys
- _Configure Data Masking
- _Configure Web Error Pages

Lesson 5: HTTP Application Configuration

- _Create and Configure Web Applications as needed.
- _Direct HTTP client traffic to the appropriate Web Application.
- _Adjust initial learning thresholds so that SecureSphere more accurately profile web traffic.

Lesson 6: Actions

- _Define, compare, and contrast Action Interfaces, Action Sets, and Followed Actions.
- _Explain placeholders, and where to find complete details regarding them.
- _Create Email, FTP, Syslog, etc., Action Interfaces as needed.
- _Create Email, FTP, Syslog, etc., Action Sets as needed.
- _Use Followed Actions to implement Action Sets on system administration jobs.

Lesson 7: Security Policies

- _Given different types of Web attacks, configure appropriate polices to defend Web applications.
- _Implement Followed Actions in Security Policies.
- _Configure and apply:
  - Signature policies to defend Web applications from attacks with easily recognizable signatures.
  - Protocol policies to defend Web applications from protocol attacks.
  - Correlation policies to protect against multi-front Web attacks.
  - Custom Web policies to protect specific application weaknesses.
- _Explain the factors that determine when to use modify a built-in policy, and when to create a copy of a built-in policy and modify it instead.

Lesson 8: Web Application Profiling

- _Describe the components of the Web Application Profile.
- _Explain how the Web Application Profile learns and protects web applications.
- _Define and explain how application activity is mapped to the profile application mapping.
- _Identify common web application components used in the learning process.
- _Define and explain how web application user tracking operates.
- _Explain how to select Web Profile Policy rules for the protected web application.

Lesson 9: ThreatRadar

- _Identify and configure appropriate ThreatRadar feeds to help secure web applications.
- _Identify when to use and how to configure TR Reputation Services.
- _Identify when to use and how to configure ThreatRadar Bot Protection.
- _Identify when to use and how to configure Intelligence (Community Defense)

Lesson 10: Alerts and Violations

- _Use the Monitoring Dashboard to view a summary of current Violations and Alerts.
- _Perform detailed analysis of Alerts and Violations to identify false positives, attacks, and tuning opportunities.
- _Use the "Add as Exception" and "add to profile" buttons to tune policies and profiles.
- _Manage the workflow of Security Monitoring by using SecureSphere's Alert Flags.

Lesson 11: Reporting

- _Describe the features of SecureSphere's Report Settings.
- _Describe how to work with report Keywords.
- _Create reports of various types, including System Events, Configuration, and Alertsreports.
- _Schedule Reports and the Reports Archivejob.
- _Create security-focused reports, such as Daily or Weekly Top 10Alert reports.

Lesson 12: Web Application Security Tuning

- _Use Reports to identify where to tune SecureSphere.
- _Use the Profile Optimization Wizard to help tune Profiles.
- _Explain the impact and trade-offs of various Profile tuning options.
- _Examine multiple ways to tune Security Policies.

Lesson 13: Active Blocking

- _Configure SecureSphere to enforce the tuned configuration.
- _Move SecureSphere from Simulation to Active Blocking mode.
- _Verify the non-default error page is working.
- _Identify and manage Followed Action Block events.
- _Configure additional Web Error Page Groups as needed.

Lesson 14: Reverse Proxy

- _Select the appropriate reverse proxy mode based on deployment requirements for URL rewriting, cookie signing, SSL termination, and/or response rewriting.
- _Configure Reverse Proxy mode settings.
- _Configure and apply SSL Cipher Suites to inbound and outbound proxy rules.
- _Create and configure default and custom web error pages for use in security policies.
- _Configure URL rewrite and redirection rules.
- _Configure SecureSphere to work with SSL Client Certificates.

Lesson 15: End of Class Capstone Exercise

The Capstone Exercise challenges students to perform a series of tasks designed to help students reinforce learning by recalling and applying the concepts and skills presented during the class. Tasks include:

- _Configure a Site Hierarchy to protect a Web Application.
- _Mask sensitive data, such as credit card numbers, so they are not exposed.
- _Configure SecureSphere's Web Application profiles and map web traffic to appropriate Web Applications.
- _Configure SecureSphere to properly support and inspect traffic that is load balanced or proxied before reaching the protected web servers.
- _Automate and archive regular SecureSphere system backups.
- _Configure SecureSphere to protect web servers against data leakage.
- _Configure SecureSphere to share information with external monitoring servers, such as a syslog server.
- _Perform Security Tuning to optimize SecureSphere's configuration.
- _Create a variety of reports.
- _Find and protect unexpected / rogue servers on the network