Citrix ADC 12.x Advanced Concepts – Secure Web Applications CNS-318

Course Summary

Description

Citrix Web App Firewall protects web apps and sites from known and unknown attacks. This three-day course will teach you how to address application services security requirements with Web App Firewall. After studying Citrix Web App Firewall, you'll learn about many different types of web attacks and vulnerabilities, such as SQL injection and cookie tampering, and how to protect against them. The course also covers policies, profiles and expressions; monitoring, management and reporting; and troubleshooting techniques. Highlighted features include the Adaptive Learning Engine and Secure Insight. This advanced course is designed for IT professionals with previous Citrix Networking experience.

Objectives

After taking this course, students will be able to:

- Identify common web attacks and vulnerabilities
- Understand PERL compatible regular expressions
- Understand how to operate the adaptive learning engine
- Configure Citrix Web App Firewall to protect web applications
- Utilize Citrix ADC Secure Insight to monitor, manage, and report on Application Services security
- Troubleshoot Citrix Web App Firewall

Topics

- Citrix Web App Firewall Overview
- Citrix Web App Firewall Profiles and Policies
- Implementing Citrix Web App Firewall Protections
- Additional Citrix Web App Firewall Protections
- Monitoring and Troubleshooting Citrix Web App Firewall
- Security and Filtering
- Authentication with Security Assertion Markup Language (SAML)
- Authentication with OAuth, OpenID, and nFactor

Audience

This course is designed for students with previous Citrix Networking experience, this course is best suited for individuals who will be deploying and/or managing Citrix Web App Firewall in Citrix Networking environments.

Prerequisites

Before taking this course, Citrix recommends students prepare for this course by taking CNS-220 Citrix ADC 12.x Essentials and Traffic Management (PT10730), or CNS-222 Citrix ADC 12.x Essentials and Citrix Gateway (PT10395).

Duration

Three days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Citrix ADC 12.x Advanced Concepts – Secure Web Applications CNS-318

Course Outline

I. Citrix Web App Firewall Overview

A. The Business Problem
B. Industry Standards
C. Protection Methodologies
D. Introducing Citrix Web App Firewall

II. Citrix Web App Firewall Profiles and Policies

A. Citrix Web App Firewall Policies
B. Citrix Web App Firewall Profiles
C. Citrix Web App Firewall Learning
D. Citrix Web App Firewall Engine Settings

III. Implementing Citrix Web App Firewall Protections

A. Security Checks and Data Flow • Rules and Adaptive Learning
B. Signatures and Comment Stripping
C. Top-Level Protections

IV. Additional Citrix Web App Firewall Protections

A. Cookie Consistency
B. Advanced Form Protection Checks
C. URL Protections
D. Protecting Sensitive Data

V. Monitoring and Troubleshooting Citrix Web App Firewall

A. Web App Firewall and Web Applications
B. Logging and Reporting
C. Customizing Errors
D. Troubleshooting

VI. Security and Filtering

A. Application level Quality of Experience (AppQoE)
B. IP Reputation
C. Rate Limiting
D. HTTP Callout

VII. Authentication with Security Assertion Markup Language (SAML)

A. What is SAML?
B. Configuring SAML on Citrix ADC

VIII. Authentication with OAuth, OpenID, and nFactor

A. OAuth and OpenID
B. Configuring OAuth on Citrix ADC
C. Multi-Factor Authentication with nFactor
D. Configuring nFactor

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically