FortiWeb

COURSE DETAILS

Course Code: FortiWeb
Current Version: 6.0
Delivery Type: Instructor-led
Duration: 3 days

PREREQUISITES

- Knowledge of OSI layers and the HTTP protocol
- Basic knowledge of HTML, JavaScript, and server-side dynamic page languages, such as PHP
- Basic experience using FortiGate port forwarding

COURSE CONTENT

In this three-day class, you will learn how to deploy, configure, and troubleshoot Fortinet's web application firewall: FortiWeb.

Instructors will explain key concepts of web application security, and lead lab exercises in which you will explore protection and performance features. In the lab, you will experience traffic and attack simulations that use real web applications. You will work with those simulations to learn how to distribute load from virtual servers to real servers, while enforcing logical parameters, inspecting flow, and securing HTTP session cookies.

COURSE OBJECTIVES

After completing this course, you should be able to:

- Understand application-layer threats
- Fight defacement and DoS
- Prevent zero-day attacks without disrupting live traffic
- Make apps retroactively compliant with OWASP Top 10 for 2013 and PCI DSS 3.0
- Discover vulnerabilities in your servers and hosted web apps for tailored, efficient protection
- Configure FortiGate together with FortiWeb, for stronger HTTP and XML application security
- Prevent accidental scan circumvention, while allowing FTP and SSH
- Configure blocking and reporting for an external FortiADC or FortiGate, and FortiAnalyzer
- Choose the right operating mode
- Balance load among a pool of servers
- Enforce SSL/TLS, authentication, and sophisticated access control for "naked" apps
- Train FortiWeb to defend your specific apps
- Blacklist suspected hackers, DDoS participants, and content scrapers
- Troubleshoot traffic flow, including flow for FTP/SSH
- Diagnose false positives and customize signatures
- Optimize performance

FortiWeb

COURSE OUTLINE

1. Introduction
2. Basic Setup
3. Integrating Front-End SNAT and Load Balancers
4. DoS and Defacement
5. Signatures, Sanitization, and Auto-Learning
6. SSL/TLS
7. Authentication and Access Control
8. PCI DSS 3.0 Compliance
9. Caching and Compression
10. HTTP Routing, Rewriting, and Redirects
11. Troubleshooting

WHO SHOULD ATTEND

Networking and security professionals involved in the administration and support of FortiWeb.