+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 22/01/2024

Sign up

Fortinet FortiWeb training (NSE6)

3 days (21 hours)

Presentation

Unprotected Web applications are a gateway for hackers and attacks. FortiWeb's multi-layered, correlated approach protects your web applications against a wide range of vulnerabilities, including those in the OWASP Top 10. When combined with FortiGuard Labs' web application security service, you're protected against application vulnerabilities, bots and malicious URLs. Our two heuristic detection engines secure your applications against advanced threats such as SQL injection, cross-site scripting, buffer overflow, cookie poisoning, malicious sources and denial-of-service attacks.

In this three-day training course, you will learn how to deploy, configure and troubleshoot Fortinet's Web application firewall: FortiWeb. You will work on simulated attacks using real web applications. Based on traffic simulations, you'll learn how to load-balance virtual servers on real servers, while applying logical parameters, inspecting the flow and securing HTTP session cookies. As always, we'll be teaching you the latest version of the tool, FortiWeb 7.4.

Objectives

- Understanding the threats to application layers
- Combating defacing and denial-of-service attacks
- Prevent 0-day attacks without disrupting direct traffic
- Make applications retroactively compatible with
- OWASP Top 10 2013 and PCI DSS 3.0
- Discover the vulnerabilities of your servers and hosted Web applications for personalized, effective protection.
- Configuring FortiGate with FortiWeb for enhanced security of HTTP and XML applications
- Prevent accidental bypassing of scans, while enabling FTP and SSH protocols
- Setting up blocking and reporting for an external FortiADC or FortiGate, and for FortiAnalyze
- Choose the right operating mode

- Load balancing within a server pool
- Securing "naked" applications: SSL/TLS protocols, authentication and sophisticated access control.
- Shape FortiWeb to protect your specific applications.
- Create a blacklist of suspects: hackers, DDoS attackers and content scrapers.
- Troubleshoot traffic flow problems (including FTP/SSH).
- Diagnose false positives and customize signatures
- Optimizing performance

Target audience

To all those who regularly administer Filtering Policies deployed on Fortigates via FortiManager.

Prerequisites

- Knowledge of OSI layers and HTTP protocol
- Basic knowledge of HTML and JavaScript, as well as a dynamic server-side page language (e.g. PHP)
- Basic knowledge of FortiGate port forwarding

FortiWeb training program

1. Introduction 2. Basic configuration 3. External SIEM integration 4. Load balancer and SNAT integration 5. Defacement and denial-of-service attacks 6. Signatures, sanitization and self-learning 7. SSL and TLS 8. Authentication and access control 9. PCI DSS 3.0 compliance 10. Caching and compression 11. Rewriting & redirects 12. Troubleshooting 13. Diagnostics

Certification

This course prepares you for the FortiWeb 7 specialist exam, and is also part of the preparatory course for the NSE 6 certification exam.

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or internal security difficulties within the company (intra-company or virtual classroom) that might be encountered.

problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.