Securing Cisco Networks with Open Source Snort

Durée: 4 Jours Réf de cours: SSFSNORT Version: 4.0 Méthodes d'apprentissage: Classe à distance

Résumé:

The Securing Cisco Networks with Open Source Snort course shows you how to deploy a network intrusion detection system based on Snort. Through a combination of expert instruction and hands-on practice, you will learn how to install, configure, operate, and manage a Snort system, rules writing with an overview of basic options, advanced rules writing, how to configure PulledPork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules, and more.

This course is worth 20 Continuing Education (CE) Credits

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

This course is designed for technical professionals who need to know how to deploy an open source intrusion detection system (IDS) based on Snort.

Objectifs pédagogiques:

- **After completing this course, you should be able to:**
- Describe Snort technology and identify the resources available for maintaining a Snort deployment
- Install and configure a Snort deployment
- Configure the command-line options for starting a Snort as a sniffer, a logger, and an intrusion detector, and create a script to start Snort automatically
- Identify and configure available Snort intrusion detection outputs
- Describe rule sources, updates, and utilities for managing rules and updates
- Detail the components of the snort.lua file and determine how to configure it for your deployment
- Configure Snort for inline operation using the inline-only features
- Configure rules for Snort using basic rule syntax
- Describe how traffic flows through Snort and how to optimize rules for better performance
- Configure advanced-rule options for Snort rules
- Configure OpenAppID features and functionality
- Tune Snort for efficient operation and profile system performance

Pré-requis:

Attendees should meet the following prerequisites:

- Technical understanding of TCP/IP networking and network architecture
- Proficiency with Linux and UNIX text editing tools (vi editor is suggested but not required)

Test et certification

Recommended as preparation for exams:

- There are no exams currently aligned to this course

Contenu:

Snort Technology Introduction

- Snort Basics
- Snort Resources

Snort Installation

- Installation Prerequisites
- Performing the Snort Installation

Snort Operation Introduction

- Running Snort from the Command Line
- Configuring Snort to Start Automatically

Snort Intrusion Detection Output

- Configuring Snort Intrusion Detection Output

Rule Management

- Snort Rulesets
- PulledPork Installation and Configuration

Snort Configuration

- Examining the snort.lua File
- Inspector Configuration

Inline Operation and Configuration

- Configuring Inline Operation
- Configuring Inline-Specific Features

Snort Rule Syntax and Usage

- Basic Rule Syntax
- Common Rule Options

Snort Rule Traffic Processing Flow

- Examining Snort Traffic Flow

Advanced Rule Options

- PCRE Rule Options
- Hash Rules
- Byte Rule Options
- Implementing Flowbits
- File Detention

OpenAppID Detection Configuration

- Exploring the Open AppID Preprocessor
- Examining AppID Events and Statistics
- Detector Basics

Snort Tuning

- Viewing Performance Statistics
- Configuring Snort Rule Filters
- Implementing BPFs in Snort
- Performance Profiling

Labs

- Discovery Lab 1: Connecting to the Lab Environment
- Discovery Lab 2: Snort Installation
- Discovery Lab 3: Snort Operation
- Discovery Lab 4: Snort Intrusion Detection Output
- Discovery Lab 5: PulledPork Installation
- Discovery Lab 6: Configuring Variables
- Discovery Lab 7: Reviewing Inspector Configurations
- Discovery Lab 8: Inline Operation
- Discovery Lab 9: Basic Rule Syntax and Usage
- Discovery Lab 10: Advanced Rule Options
- Discovery Lab 11: OpenAppID Configuration
- Discovery Lab 12: Tuning Snort

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement