SSFSNORT (SECURING CISCO NETWORKS WITH OPEN SOURCE SNORT) 3.0

Objetivo

After taking this course, you should be able to: â□¢ Define the use and placement IDS/IPS components; â□¢ Identify Snort features and requirements; â□¢ Compile and install Snort; â□¢ Define and use different modes of Snort; â□¢ Install and utilize Snort supporting software.

PÃºblico Alvo

This course is designed for technical professionals who need to know how to deploy and manage a Cisco Firepower NGFW/NGIPS in their network environment.

PrÃ©-Requisitos

To fully benefit from this course, you should have the following knowledge and skills: â□¢ Technical understanding of TCP/IP networking and network architecture; â□¢ Basic familiarity with firewall and IPS concepts. For reference, this is the recommended Cisco course that may help you meet these prerequisites: Implementing and Administering Cisco Solutions (CCNA).

Carga HorÃiria

32 horas (4 dias).

ConteÃºdo ProgramÃitico

Course Introduction
Course Outline
Course Goals & Objectives

Detecting Intrusions with Snort 3.0
History of Snort
IDS
IPS
IDS vs. IPS
Examining Attack Vectors
Application vs. Service Recognition

Sniffing the Network
Protocol Analyzers
Configuring Global Preferences

Capture and Display Filters
Capturing Packets
Decrypting Secure Sockets Layer (SSL) Encrypted Packets

Architecting Nextgen Detection
Snort 3.0 Design
Modular Design Support
Plug Holes with Plugins
Process Packets
Detect Interesting Traffic with Rules
Output Data

Choosing a Snort Platform
Provisioning and Placing Snort
Installing Snort on Linux

Operating Snort 3.0
Topic 1: Start Snort
Monitor the System for Intrusion Attempts
Define Traffic to Monitor
Log Intrusion Attempts
Actions to Take When Snort Detects an Intrusion Attempt
License Snort and Subscriptions

Examining Snort 3.0 Configuration
Introducing Key Features
Configure Sensors
Lua Configuration Wizard

Managing Snort
Pulled Pork
Barnyard2
Elasticsearch, Logstash, and Kibana (ELK)

Analyzing Rule Syntax and Usage
Anatomy of Snort Rules
Understand Rule Headers
Apply Rule Options
Shared Object Rules
Optimize Rules
Analyze Statistics

Use Distributed Snort 3.0
Design a Distributed Snort System
Sensor Placement
Sensor Hardware Requirements
Necessary Software
Snort Configuration

Monitor with Snort

Examining Lua
Introduction to Lua
Get Started with Lua

Lab outline
Lab 1: Capture and Analyze Packets
Lab 2: Initiate the Snort Installation
Lab 3: Complete an Installation of Snort
Lab 4: Configure and Run Snort
Lab 5: Tweak the Installation
Lab 6: Rapid Deployment with Lua
Lab 7: Integrate Snort Optimizers
Lab 8: Analyze Rule Syntax
Lab 9: Hello World Lua Style