SSFRULES

Securing Cisco Networks with Snort Rule Writing Best Practices

Securing Cisco® Networks with Snort Rule Writing Best Practices (SSFRULES) ist ein Kurs, der von Cisco Learning Services High-Touch Delivery angeboten wird. Es handelt sich um einen praxisorientierten Kurs, der Benutzer von Open-Source-Snort- oder Sourcefire-FireSIGHT1-Systemen in die Snort-Regelsprache und die Best Practices für die Regelerstellung einführt. Sie werden sich ausschließlich auf die Snort-Regelsprache und das Schreiben von Regeln konzentrieren. Angefangen von der Regelsyntax und -struktur bis hin zur fortgeschrittenen Verwendung von Regeloptionen werden Sie Exploit-Paketaufzeichnungen analysieren und die erlernten Theorien zur Regelerstellung anwenden, indem Sie Funktionen der Regelsprache implementieren, um Alarme für den angreifenden Netzwerkverkehr auszulösen. Dieser Kurs bietet auch Anleitungen und Laborübungen zur Erkennung bestimmter Arten von Angriffen, wie z. B. Pufferüberläufe, unter Verwendung verschiedener Techniken zur Regelerstellung. Sie werden Ihre Fähigkeiten beim Schreiben von Regeln mit zwei Herausforderungen testen: eine theoretische Herausforderung, die Ihre Kenntnisse der Regelsyntax und -verwendung prüft, und eine praktische Herausforderung, bei der Sie ein ausnutzendes Ereignis analysieren und untersuchen, so dass Sie Ihre Installationen gegen Angriffe verteidigen können Dieser Kurs kombiniert Vorlesungsmaterial und praktische Übungen, um sicherzustellen, dass Sie in der Lage sind, Open-Source-Regeln erfolgreich zu verstehen und umzusetzen.

Kursinhalt

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernoberfläche integriert.

Zielgruppe

This course is designed for technical professionals who need to know how to write rules and understand open source Snort language. The primary audience for this course includes:

- Security Administrators
- Security Consultants
- Network Administrators
- System Engineers
- Technical Support Personnel
- Channel Partners and Resellers

Voraussetzungen

- Technisches Verständnis von TCP/IP-Netzen und Netzarchitektur
- Kenntnisse in der Verwendung und Bedienung von Cisco SourcefireR Systems oder Open Source Snort
- Kenntnisse im Umgang mit Befehlszeilen-Tools zur Textbearbeitung, z. B. dem vi-Editor
- Grundlegende Erfahrung im Schreiben von Regeln wird empfohlen

Bearbeitungszeit

ca. 18 Stunden

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**CSFR**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referentengeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.	
6 Monate Freischaltung	**€ 1.000,-**

Training		Preise zzgl. MwSt.
Termine in Deutschland	**3 Tage**	**€ 3.595,-**
Online Training	**3 Tage**	**€ 3.595,-**

Termin/Kursort — Kurssprache Englisch

13.05.-15.05.24 Online — 22.07.-24.07.24 Online

03.06.-05.06.24 Online

SSFRULES

Security

Stand 12.04.2024

ExperTeach

Inhaltsverzeichnis

SSFRULES – Securing Cisco Networks with Snort Rule Writing Best Practices

Course Outline

Module 1: Introduction to Snort Rule Development
Module 2: Snort Rule Syntax and Usage
Module 3: Traffic Flow Through Snort Rules
Module 4: Advanced Rule Options
Module 5: OpenAppID Detection
Module 6 Tuning Snort

Lab Outline

Lab 1: Connecting to the Lab Environment
Lab 2: Introducing Snort Rule Development
Lab 3: Basic Rule Syntax and Usage
Lab 4: Advanced Rule Options
Lab 5: OpenAppID
Lab 6: Tuning Snort

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de