SSFIPS (SECURING CISCO NETWORKS WITH SOURCEFIRE INTRUSION PREVENTION SYSTEM)

Objetivo

Securing Cisco Networks With Sourcefire Intrusion Prevention System (SSFIPS) que proporciona aos alunos os conhecimentos necessários para instalar, configurar, gerenciar e realizar atividades de suporte ao produto. É curso desenvolvido para capacitação operacional do produto, com utilização intensiva de laboratórios. Esse é um curso oficial desenvolvido pela Cisco Learning High-Touch Delivery. O aluno vai aprender a utilizar e configurar NGIPS Cisco SourceFire, incluindo o controle de aplicações, as características de firewall, roteamento e comutação (switching). Também irá aprender a proceder ajustes no sistema para uma melhor performance e uma maior conhecimento da rede, através da obtenção das vantagens pelas ferramentas de análise, incluindo tipos de arquivos e detecção de “malwares” (network-based malware detection). Este curso combinado com a leitura dos materiais fornecidos e com as atividades práticas em laboratórios, garantem que implementação e gerenciamento com sucesso de uma solução Cisco SourceFire. Este curso ele é preparatório para a realização do exame Securing Cisco Networks with Sourcefire (500-285). O curso possuí duas modalidades de oferta, uma com carga horária de quatro dias (32 horas) sendo presencial (Instructor-Led Classroom) e outra com cinco dias (40 horas) virtual (Instructor-Led Virtual). Após completar este treinamento o aluno estará apto à: • Descrever uma solução com Cisco NGIPS Sourcefire; • Navegar pela interface de configuração (GUI) pelas características administrativas, incluindo as funcionalidades relacionadas a relatórios (reports) e informações sobre as ameaças identificadas; • Descrever como implantar e gerenciar uma solução Cisco Sourcefire e seus produtos; • Descrever o papel da tecnologia FireSIGHT em uma solução Cisco SourceFire; • Descrever, criar e implantar a utilização de objetos nas políticas de controle de acesso; • Descrever as características avançadas de configuração de políticas de controle e de administração; • Analisar eventos; • Escrever e configurar regras básicas.

Público Alvo

O público primário inclui os indivíduos os profissionais que demandam conhecimentos para instalar, operar, prestar suporte e otimizar uma solução Cisco NGIPS SourceFire.

Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno possua conhecimentos fundamentais no protocolo TCP/IP e de sistemas para detecção de intrusão (IDS) e prevenção (IPS).

Carga Horária

32 horas (4 dias).

Conteúdo Programático

Course Introduction
• Overview
• Course Goal and Objectives
• Course Flow
• Additional References
• Your Training Curriculum

Module 1: Cisco SourceFire System Overview and Classroom setup
.
• Overview of the SourceFire System
• Discuss SourceFire System NGIPS and NGFW functionality
• Review the class infrastructure
• Preparação da infrastructure

Module 2: Device Management

• Describe device management features and settings
• Discuss interface configuration and deployment modes
• Understand how to create and configure the following:
• Passive interfaces
• Inline interfaces
• Virtual switches
• Virtual routers
• Hybrid interfaces
• Policy-based NAT
• Gateway VPN

Module 3: Object Management

• Understand how to create objects
• Learn how to add and edit Network, Port, VLAN tag and Application Filter Object
• Discuss variable sets and how to create
• Understand Security Zone objects and Geolocation
Module 4: Access Control Policy

• Understand how to create an Access Control policy
• Describe how to assign zones and networks to the policy
• Discuss policy actions
• Discuss application control and how to apply it to the Access Policy
• Describe how tom implement File and IPS policy in an access control rule
• Discuss how to apply user constraints
• Describe URL filtering in the Access Control Policy

Module 5: Network-based Malware Detection

- Describe the file and network-based malware detection and malware blocking features
- Review how this technology functions behind-the-scenes
- Describe file dispositions and how they relate to malware detection and blocking
- Discuss file and network-based malware policy
- Describe how to use file and network-based malware policies in access control policy rules

Module 6: FireSIGHT Technology

- Describe the role FireSIGHT technologies play in the SourceFire System
- Configuring host and user discovery
- Discuss discovery and discovery events
- Demonstrate how to access discovery information
- Discuss connection data and view connection events
- Describe user discovery

Module 7: Correlation Policies

- Describe Correlation Rules and Policies
- Demonstrate White Lists
- Discuss Network Profiling

Module 8: IPS Policy Basics

- Describe the concept of policy layers
- Demonstrate how to leverage policy layers in the user interface
- Describe the Advanced Policy flattened view
- Provide an overview of the IPS policy management interface
- Describe the elements of a policy

Module 9: Advanced IPS Policy Configurations

- Describe advanced policy configuration
- Discuss details of preprocessor technology and SourceFire System configuration options

Module 10: User Account Management

- Understand Internal and External user account management
- Describe user roles
- Describe custom user roles
- Discuss Privilege Escalation
- Configure Internal user accounts
- Configure external LDAP account objects
- Configure external RADIUS account objects

Module 11: User Account Management

- Learn how Snort analyses network packets
- Familiarize yourself with the Analysis Workflow and the actions to consider for all alerts
- Understand how to tune IPS alerts
- Discuss the analyst´s role in security incident response
- Understand how the Context Explorer can aid in event analysis

Module 12: Reporting

- Learn how to generate reports
- Demonstrate how to create and customize report templates

Appendix

Module 13: Basic Rule Syntax and Usage

- Understand rule structure
- Understand rule syntax
- Discuss some basic rule options and their usage
- Configure and create Snort Rules

Module 14: Case Studies in Rule Writing and Packet Analysis

- Understand the role that research plays in analysis
- Present various scenarios and describes how each is addressed with rule
- Discuss rule writing techniques

Laboratórios

- Lab 1: Verifying the license
- Lab 2: Testing the Environment by Running Attacks PCAPS (Tests)
- Lab 3: View Events
- Lab 4: Layer 2 and 3 Simulation (Optional)
- Lab 5: Configuring the Inline Interface
- Lab 6: Creating objects
- Lab 7: Creating Access Control Policy (Port Inspection)
- Lab 8: Creating Access Control Policy (Application Awareness)
- Lab 9: URL Filtering
- Lab 10: Including an IPS Policy in Access Control Rules
- Lab 11: Creating File Policy
- Lab 12: Tuning The Network Discovery Policy
- Lab 13: Viewing FireSIGHT Data
- Lab 14: User Discovery
- Lab 15: Creating a Correlation Policy Based on Connection Data
- Lab 16: White Lists
- Lab 17: Working with Connection Data and Traffic Profiles
- Lab 18: Creating an Intrusion Policy
- Lab 19: Including FireSIGHT Recommendations in an Intrusion Policy

- Lab 20: Tunning Your HTTP_Inspect Prepocessor
- Lab 21: Applying and Testing Your Policy and Variable Set
- Lab 22: Creating User Accounts and Configuring the User Interface Timeout Value
- Lab 23: Testing Exempt and Non-exempt Users
- Lab 24: Permission Escalation
- Lab 25: Working with External Accounts
- Lab 26: Analysis Lab
- Lab 27: Tuning Events
- Lab 28: Context Explorer
- Lab 29: Comparing Trends with Reports
- Lab 30: Writing Custom Rules (Appendix)
- Lab 31: Research and Packet Analysis (Appendix)
- Lab 32: Revisiting Kaminsky DNS Vulnerability