IPS (IMPLEMENTING CISCO INTRUSION PREVENTION SYSTEM) 7.0

Objetivo

O treinamento proporciona ao profissional os conhecimentos necessários para implantação e suporte em uma solução IPS da Cisco (Appliances e Módulos de Serviços para ASA, roteadores e Switch 6500). O Currículo capacita para a instalação e a configuração básica do IPS e a utilização da interface gráfica de configuração "IDM" (Intrusion Device Management), na configuração e manutenção da base de assinaturas existente, bem como criar novas assinaturas, de acordo com os requerimentos de uma política de segurança; Serão apresentadas os componentes das assinaturas por tipos ("engines") e seus respectivos parâmetros. O aluno será apresentado aos recursos "Monitoring Center for Security" e ao "Cisco Threat Response", que são diretamente responsáveis pelo gerenciamento e maximização da eficiência de um dispositivo IPS. O aluno aprenderá conceitos sobre o módulo NM-CIDS utilizados em roteadores de acessoe do módulo IDSM-2 em um switch Cisco Catalyst 6500. Serão também abordadas durante este curso as técnicas para capturar tráfego de rede para análise e prevenção de ataques. Por fim, o aluno aprenderá como fazer a manutenção e a atualização do sistema operacional e das assinaturas de um equipamento IPS. Durante todo o curso o aluno utilizará a CLI e o IDM para efetuar as configurações do produto. Após o treinamento, o aluno será capaz de: Descrever os Sensores Cisco IPS e suas características; Utilizar o Cisco IPS Device Manager (IDM) para configurar assinaturas; Criar e implantar assinaturas personalizadas na prevenção de intrusão; Criar filtros para reduzir os possíveis falsos positivos; Realizar configurações de proteção, como por exemplo, TCP Reset e Deny Attacker Inline, dentre outros; Configurar um Sensor Cisco IPS para realizar bloqueios em dispositivos Cisco (roteadores e ASA/PIX); Executar operações de manutenção, como atualizações de assinaturas; Configurar e monitorar sensores de detecção de anomalias (Passive OS Fingerprinting e Virtual Sensors); Realizar procedimentos de manutenção e gerência.

Público Alvo

Engenheiros de Sistemas que tenham segurança como foco, Analistas de Segurança, Operadores de Segurança, Consultores de Segurança e Analistas de Suporte

Pré-Requisitos

Para total aproveitamento neste treinamento é altamente recomendado que o aluno possua certificações Cisco CCNA Security, ICND1 e IINS.

Carga Horária

40 horas (5 dias).

TELECON
Rua Funchal nº 129 – 1º Andar – CEP: 04551-060 – Vila Olímpia – São Paulo – SP
Tel.: (11) 2113-4888 – Fax.: (11) 2113-4887 – www.telecon.com.br

Conteúdo Programático

Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices
Evaluating Intrusion Prevention and Intrusion Detection Systems
Choosing Cisco IPS Software, Hardware, and Supporting Applications
Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-Evasive Countermeasures
Choosing a Network IPS and IDS Deployment Architecture

Installing and Maintaining Cisco IPS Sensors
Integrating the Cisco IPS Sensor into a Network
Performing the Cisco IPS Sensor Initial Setup
Managing Cisco IPS Devices

Applying Cisco IPS Security Policies
Configuring Basic Traffic Analysis
Implementing Cisco IPS Signatures and Responses
Configuring Cisco IPS Signature Engines and the Signature Database
Deploying Anomaly-Based Operation

Adapting Traffic Analysis and Response to the Environment
Customizing Traffic Analysis
Managing False Positives and False Negatives
Improving Alarm and Response Quality

Managing and Analyzing Events
Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
Managing and Investigating Events Using Cisco IPS Manager Express
Using Cisco IME Reporting and Notifications
Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
Using the Cisco IntelliShield Database and Services

Deploying Virtualization, High Availability, and High Performance Solutions
Using Cisco IPS Virtual Sensors
Deploying Cisco IPS for High Availability and High Performance

Configuring and Maintaining Specific Cisco IPS Hardware
Configuring and Maintaining the Cisco ASA AIP SSM and AIP SSC Modules
Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
Configuring and Maintaining the Cisco IDSM-2 Module

Lab:
Lab 2-1: Performing the Cisco IPS Sensor Initial Setup
Lab 2-2: Managing a Cisco IPS Sensor
Lab 3-1: Configuring and Modifying Basic Cisco IPS Signatures and Responses
Lab 3-2: Configuring Cisco IPS Anomaly-Based Operation
Lab 4-1: Configuring Custom Cisco IPS Signatures
Lab 4-2: Managing False Positives and False Negatives
Lab 4-3: Improving Alarm and Response Quality

Lab 5-1: Using the Cisco IME
Lab 5-2: Using Cisco IPS and Security Intelligence Web Resources
Lab 6-1: Configuring Policy Virtualization