SETC Training Corporate Logo

Formation sécurité informatique: Inspection des réseaux avec SNORT (SNORTFR, 4 jours)

Description

Le cours Formation sécurité informatique : Inspection des réseaux avec SNORT est une exploration complète de SNORT, de l'installation et de la configuration au développement de règles complexes pour l'extraction de données malveillantes et la détection d'intrusions dans les réseaux. La formation commence par un aperçu des fondements théoriques de l'analyse des données réseau avec SNORT. Elle est suivie d'une étude détaillée du travail avec les préprocesseurs SNORT pour analyser le trafic et détecter les attaques malveillantes. La formation aborde également l'utilisation de filtres et d'événements et l'écriture de règles SNORT pour la détection de charges utiles, la détection de charges non utiles et le traitement post-détection. La formation se termine par une discussion sur les meilleures pratiques et les défis liés à l'écriture de règles et à l'utilisation du préprocesseur AppId pour les détecteurs d'applications créés par les utilisateurs. Wow ! Il s'agit d'un cours de sécurité informatique très complet.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Concepts et utilisation de Snort

- Comprendre le SNORT et ses usages
- Modes d'exploration : Sniffer, Logger et Système de détection d'intrusion dans le réseau
- À propos de Packet Acquisition
- Lecture des fichiers pcap : Mode d'emploi pratique
- Lecture de la sortie de base
- Exploration de la prise en charge du protocole de tunneling
- À propos de la prise de contrôle
- À propos de l'option Configurer la valeur du signal

Configuration de Snort

- Aperçu de la configuration
- Configuration Deep Dive
- Utilisation d'include pour les IP et les ports
- Utilisation des modificateurs et des limites des variables
- Configuration du profilage des performances
- Utilisation des modules de sortie
- Utilisation des tables d'attribution des hôtes
- Comprendre le rôle des préprocesseurs

Travailler avec des préprocesseurs Partie I : Données de bas niveau

- Présentation du préprocesseur Frag3
- Format Frag3 et configuration de base
- Configuration avancée de Frag3
- Utilisation des préprocesseurs Stream et Session
- Configuration de la session
- Configuration des flux
- Plus sur Stream : TCP. UDP, ICMP et IP

Utilisation des préprocesseurs - Partie II : protocoles d'application

- Aperçu des capacités au niveau des applications
- Inspecter HTTP

Inspection du SMTP
Inspection de POP et IMAP
Inspection du FTP
Inspection de SSH
Inspection du DNS
Contrôle du SSL
Inspection de SIP (VOIP)

Utilisation des préprocesseurs - Partie II : Détection d'intrusion

Utilisation de sfPortscan pour détecter une attaque
Configuration des alertes sfPortscan
Réglage de sfPortscan
Utilisation du normalisateur
Utilisation du préprocesseur de réputation
Ajout de règles à la réputation à l'aide d'expressions régulières
Utilisation du préprocesseur de données sensibles

Utilisation des événements et des filtres

Aperçu des événements et des filtres
Exploration des filtres de taux
Exploration des filtres d'événements
Utilisation de la suppression d'événements
Travailler avec la journalisation des événements
À propos de la recherche d'événements

Rédaction de règles : Concepts et utilisation

La structure d'une règle
À propos des actions de règles
Spécifier les protocoles et les adresses IP
Spécifier les numéros de port et la direction
Exploration des expressions régulières du PCRE : Syntaxe et utilisation
Exploration des techniques : Saut d'octet, test d'octet et extraction d'octet
À propos des règles dynamiques
Utilisation des options de règles

Options des règles de détection des charges utiles

Rédaction des règles de détection des charges utiles
Règles de rédaction pour le trafic général
Rédaction de règles pour le trafic HTTP
Rédaction de règles pour le trafic HTTPs
Rédaction de règles pour les intentions malveillantes
Rédaction de règles pour SIP

Options des règles de détection des charges non payantes

Rédaction de règles de détection de non-charge
Rédaction de règles pour les options TOS, TTL et IP
Rédaction de règles pour la fragmentation et le flux des paquets
Rédaction de règles pour le protocole IP
Rédaction de règles pour la communication TCP : SEQ, ACK et autres
Rédaction de règles pour ICMP
Rédaction de règles pour RPC

Options des règles de post-détection

Aperçu des options de règles de post-détection
Journalisation et gestion des sessions
Combinaison de paquets avec étiquette

Mise en œuvre de règles conditionnelles qui répondent à des événements
Remplacer dynamiquement le contenu des paquets
Mise en œuvre des événements conditionnels
Rédaction de bonnes règles
Défis théoriques et pratiques de la rédaction de règles
Correspondance des contenus
Saisir la vulnérabilité, pas l'exploitation
Saisir les bizarreries du protocole dans la règle
Optimisation des règles
Test des valeurs numériques
Utilisation du préprocesseur AppId
Exigences de dépendance
Configuration du préprocesseur
Options de règles
Événements relatifs aux règles d'application
Statistiques d'utilisation des applications
Installation du paquet de détecteurs ouverts (ODP)
Détecteurs d'applications créés par l'utilisateur