CONDOR ACADEMY
Etablissement Privé de Formation Professionnelle
Agréé par l'Etat

Formation Sur : LES TECHNOLOGIES IPS / IDS (SNORT)

04 JOURS « 24 HEURES » | DU 09 AU 12 MAI 2022 | CONDOR ACADEMY

Détection et prévention d'intrusions : SNORT IDS/IPS

De nos jours le réseau d'entreprise s'étende de plus, et le nombre de donnée critique sur les SI augmente. Ce qui implique aussi une augmentation du nombre d'attaque.
Tout responsable de réseau se doit d'assurer la sécurité des données et, en cas de problèmes, d'agir en conséquence. Snort est l'un des outils les plus performants de lutte contre l'intrusion et sa maîtrise constitue un pilier fondamental de toute politique de sécurité.
Sécurité réseau avec Snort et les IDS vous donne les clés d'une stratégie de sécurité et du déploiement d'outils adaptés. Il qui permet de surveiller le trafic réseau, d'être tenu en garde contre les attaques et de veiller aux intrusions.
Cette Formation explique comment déployer Snort et les IDS / IPS, à savoir les systèmes de détection d'intrusion.

PUBLICS CONCERNÉ

- Administrateurs de sécurité / de réseaux
- Ingénieurs système
- Personnel de support technique utilisant des IDS et IPS.

FORMATEUR

Assuré par Mr **AMIR DJENNA**, Consultant Expert en Cyber Sécurité, Enseignant chercheur à l'université.

OBJECTIFS PÉDAGOGIQUES :

- Permettre à un administrateur de réseau/sécurité de découvrir Snort, l'installer, le configurer, et le déployer sur un environnement de production et de pouvoir en retirer les informations pertinentes.
- Mettre l'accent sur les aspects théoriques et pratiques en proposant à chaque stagiaire de manipuler sa propre sonde.
- Mettre l'accent sur les tendances récentes en matière de mise en place et d'implémentation des IDS/IPS de nouvelle génération sera également abordée.

METHODE PEDAGOGIQUE :

Plusieurs méthodes d'apprentissage et outils didactiques permettant de mesurer le progrès et l'intégration des concepts par les participants sont utilisés tout au long de la formation.
Exposé, Démonstration, Étude de cas, Simulation, Exercices ….

Programme

JOUR 01

I. Détecter les intrusions avec Snort 3.0

- Histoire de Snort
- IDS
- IPS
- IDS Vs IPS
- Examen des vecteurs d'attaque
- Reconnaissance des applications et des services

II. Renifler le réseau

- Analyseurs de protocoles
- Configuration des préférences globales
- Filtres de capture et d'affichage
- Capture de paquets
- Décryptage des paquets cryptés SSL (Secure Sockets Layer)

JOUR 02

I. Architecture de la détection de nouvelle génération

- Conception Snort 3.0
- Prise en charge de la conception modulaire
- Bouchez les trous avec les plugins
- Traiter les paquets
- Détecter le trafic intéressant avec des règles
- Des données de sortie

II. Choisir une plateforme Snort

- Approvisionnement et place
- Installer Snort sur Linux

JOUR 03

I. Fonctionnement de Snort 3.0

- Sujet 1 : Démarrer Snort
- Surveiller le système pour les tentatives d'intrusion
- Définir le trafic à surveiller
- Tentatives d'intrusion dans le journal
- Actions à entreprendre lorsque Snort détecte une tentative d'intrusion
- snort de licence et abonnements

II. Examen de la configuration de Snort 3.0

- Présentation des fonctionnalités clés
- Configurer les capteurs
- Assistant de configuration Lua

III. Gérer le reniflement

- Porc effiloché
- Barnyard2
- Elasticsearch, Logstash et Kibana (ELK)

JOUR 04

I. Analyse de la syntaxe et de l'utilisation des règles

- Anatomie des règles de Snort
- Comprendre les entêtes de règle
- Appliquer les options de règle
- Règles d'objet partagé
- Optimiser les règles
- Analyser les statistiques

II. Utiliser Snort distribué 3.0

- Concevoir un système Snort distribué
- Emplacement du capteur
- Configuration matérielle requise pour le capteur
- Logiciel nécessaire
- Configuration de reniflement
- Surveiller avec Snort

III. Examiner Lua

- Introduction à Lua
- Se familiariser avec Lua

CONDOR ACADEMY

Portfolio + CD de support de cours sera remis à la fin de la formation aux apprenants comprenant les slides sur la théorie, les exercices et travaux pratiques et les corrigés de ces derniers.
Une évaluation à chaud sera proposée aux apprenants à la fin du cours.

Une attestation de formation sera remise aux apprenants ayant suivi la formation avec assiduité.

CONTACTEZ-NOUS !

Nos équipes sont à votre disposition pour élaborer votre projet de formation

Site web :
www.condoracademy.dz

Contact :
+213 (0) 560 70 86 90
+213 (0) 560 97 54 27

Adresse email:
academy.condor@condor.dz