Formation Securing Cisco Networks with Snort Rule Writing Best Practices

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Sécuriser les réseaux Cisco avec les meilleures pratiques d'écriture de règles Snort est un cours intensif en laboratoire qui présente aux utilisateurs des systèmes open source Snort ou Sourcegire FIRESIGHT le langage des règles Snort et les meilleures pratiques d'écriture de règles. Les utilisateurs se concentrent exclusivement sur le langage et l'écriture des règles de Snort. En partant de la syntaxe et de la structure des règles jusqu'à l'utilisation avancée des options de règle, vous analyserez les captures de paquets d'exploitation et mettrez en pratique les théories d'écriture de règles apprises - implémentant des fonctionnalités de langage de règles pour déclencher des alertes sur le trafic réseau incriminé. des exercices sur la façon de détecter certains types d'attaques, tels que les débordements de tampon, en utilisant diverses techniques d'écriture de règles. Vous testerez vos compétences en rédaction de règles dans deux défis : un défi théorique qui teste la connaissance de la syntaxe et de l'utilisation des règles, et un défi pratique dans lequel nous vous présentons un exploit à analyser et à rechercher afin que vous puissiez défendre vos installations contre l'attaque. Ce cours combine des supports magistraux et des travaux pratiques tout au long du cours pour vous assurer que vous êtes en mesure de comprendre et de mettre en oeuvre avec succès les règles open source.

Référence	SSFRULES
Durée	3 jours (21h)
Tarif	2 700 €HT
Repas	60 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (ENG)

du 29 au 31 mai 2024

du 4 au 6 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Décrire la structure des règles, la syntaxe des règles, les options des règles et leur utilisation.
| Configurer et créer des règles Snort
| Décrire le processus d'optimisation des règles pour créer des règles efficaces
| Décrire les préprocesseurs et la manière dont les données sont présentées au moteur de règles
| Créer et implémenter des expressions régulières fonctionnelles dans les règles Snort
| Concevoir et appliquer des règles à l'aide des options de règle byte_jump/test/extract
| Identifier les concepts derrière la modélisation de protocole pour écrire des règles plus performantes

Public

| les professionnels de la sécurité qui ont besoin de savoir écrire des règles et comprendre le langage open source Snort

Prérequis

| Compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau - ICND1 Recommandé
| Connaissance pratique de l'utilisation et du fonctionnement de Cisco Sourcefire Systems ou de Snort open source
| Connaissance pratique des outils d'édition de texte en ligne de commande, tels que l'éditeur vi
| Une expérience de base en rédaction de règles est suggérée

Programme de la formation

Module 1 : Bienvenue sur le réseau virtuel Cisco et Sourcefire
Module 2 : Syntaxe et utilisation des règles de base
Module 3 : Optimisation des règles
Module 4 : Utilisation des expressions régulières compatibles Perl (PCRE) dans les règles
Module 5 : Utilisation des options de règle Byte_Jump/Test/Extract Module 6 : Concepts de modélisation de protocole et utilisation de Flowbits dans l'écriture de règles
Module 7 : Études de cas sur la rédaction de règles et l'analyse de paquets
Module 8 : Surveillance des performances des règles
Module 9 : Laboratoires, exercices et défis pratiques d'écriture de règles Laboratoires
| Lab 1 : Familiarisation avec l'infrastructure
| Lab 2 : Écrire des règles personnalisées
| Lab 3 : Règles de suppression
| Lab 4 : Remplacer du contenu
| Lab 5 : Scénario de règle SSH
| Lab 6 : Optimisation des règles
| Lab 7 : Utilisation de PCREtest pour tester les options Regex
| Lab 8 : Utiliser PCREtest pour tester des expressions régulières personnalisées
| Lab 9 : Écrire des règles contenant PCRE
| Lab 10 : Exploiter la confiance de SADMIND
| Lab 11 : Utilisation de l'opération ET au niveau du bit dans l'option de règle Byte_Test Lab 12 : Détection de la traversée de répertoires ZenWorks à l'aide de Byte_Extract
| Lab 13 : Écrire une règle Flowbit
| Lab 14 : Défi Flowbits supplémentaires
| Lab 15 : Renforcez votre règle de force brute avec Flowbits
| Lab 16 : Recherche et analyse de paquets
| Lab 17 : Revisiter la vulnérabilité de Kaminsky
| Lab 18 : Configuration du profilage des règles
| Lab 19 : Test des performances des règles
| Lab 20 : Configurer le profilage des règles pour afficher les performances du PCRE Lab 21 : Empêcher l'accès des utilisateurs à un site restreint
| Lab 22 : Injection SQL
| Lab 23 : L'attaque SQL revisitée

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.