Hacking et sécurité : utilisation de WireShark

Lien : https://innov-systems.com/formation/hacking-et-securite-utilisation-de-wireshark

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC47

CATÉGORIE
Test d'Intrusions, Techniques de Hacking, Contre Mesures et Audit

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Acquérir une bonne maitrise de Wireshark pour une analyse en profondeur de tout ce qui transite sur le réseau et la détection des principales sources de dysfonctionnement des réseaux
- Savoir diagnostiquer un problème réseau

POUR QUI ?

- Administrateurs réseaux
- Professionnels de la sécurité informatique

Innov Systems

Programme détaillé

1 / Rappels des fondamentaux

- Méthodes de communications (unicast, multicast, broadcast)
- Les topologies et le contrôle d'accès
- Modèle de l'OSI
- Format d'une trame Ethernet
- Tailles et signification (Runt, Giant…) et le protocole ARP
- Protocole de couche 2 (802.3, 802.1p, 802.1q, 802.1ad)
- Multicast de couche 2
- Format d'un paquet IP
- Les adresses particulières (loopback, APIPA,…)
- Les adresses de multicast (adresses connues et fonctionnalités), méthode de diffusion
- Protocole ICMP (rôle et analyse des réponses)

2 / Débuter avec WireShark

- Principes et fonctions de base
- Installation et maintenance

3 / Fonctionnalités Wireshark

- Définition de paramètres généraux et personnels
- Définition de valeurs de temps et d'interprétation de résultats
- Création et application de filtres d'affichage
- Suivi des flux et réassemblage de données
- Personnalisation du profil Wireshark
- Utilisation du système expert de Wireshark
- Sniffing réseau en lignes de commandes

Innov Systems

4 / Analyse des menaces de sécurité sur les LAN

- Analyse de trafic en clair
- Analyse d'attaques de sniffing
- Analyse des techniques de reconnaissance réseau
- Détection des tentatives de craquage de mots de passe
- Autres attaques
- Outils complémentaires de Wireshark
- Filtres d'affichages importants

5 / Analyse des flux applicatifs

- DNS
- DHCP
- HTTP
- FTP

6 / Analyse des communications email

- Forensic d'email
- Analyse d'attaques sur les communications email
- Filtres importants

7 / Inspection du trafic malware

- Préparation de Wireshark
- Analyse de trafic malveillant
- Botnets IRC

8 / Analyse des performances réseau

- Création d'un profile spécifique au dépannage réseau
- Optimisation avant analyse

Innov Systems

- Problèmes liés à TCP/IP

9 / Présentation des outils en lignes de commande

- wireshark.exe
- tshark.exe
- dumpcap.exe
- capinfos.exe
- editcap.exe
- mergecap.exe
- text2cap.exe
- rawshark.exe

10 / Les tâches de dépannage avec Wireshark

- Résolution de problèmes Ethernet et Wi-Fi
- Focus sur les ralentissements réseaux et délais
- Identification de problèmes par l'utilisation du système Expert de Wireshark
- Identification d'erreurs d'application
- Optimisation de la détection d'un problème
- Désinfection d'un fichier de traces

11 / Utilisation de Graphs pour détecter les problèmes

- Maîtrise basique et avancée des fonctions de Graph IO
- Graphs pour les problèmes de débit
- Graphs pour les problèmes de ralentissement
- Graphs sur les autres problèmes réseau

Inov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca
30 Août au 03 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés