Alliance Du Numérique
Groupement IT // Business et Solutions en commun

Durée : 2 jours soit 14 h
Horaires : à définir avec le client
Date : à définir avec le client

Tarif : 980 € HT/personne
Tarif membre ADN : nous consulter

Objectifs :
-Mettre en place des captures pertinentes
- Personnaliser l'environnement Wireshark
- Mettre en œuvre les filtres et colonnes permettant une analyse efficace des principaux protocoles
- Utiliser de façon simple les statistiques et graphes.

Pré-requis :
Connaissances de base sur les réseaux et TCP/IP

Moyens pédagogiques :
Poste de travail, un environnement réseau et des fichiers de captures pour la mise en pratique des notions abordées. Support de cours fourni au format pdf.

Méthodes pédagogiques :
Alternance d'exposés ou de présentations, de travaux pratiques/dirigés.

Moyens techniques :
Formation en téléprésentiel, à distance.
Ordinateur équipé d'une caméra et d'un microphone avec une connexion internet stable.

Modalités d'évaluation des acquis :
Les compétences acquises sont vérifiées au travers de mises en situation et/ou de quiz réalisés par le stagiaire.
L'évaluation de la formation se fait à chaud par un questionnaire de satisfaction ainsi que des échanges directs entre le formateur et le stagiaire.

PROGRAMME DE FORMATION

Wireshark 3.x – Les fondamentaux

Public concerné :
Toute personne adulte ayant besoin d'analyser les réseaux TCP/IP en suivant les échanges protocolaires (DNS, DHCP, http,...) afin d'en comprendre le fonctionnement. Cette analyse portera essentiellement sur Ethernet en mode filaire, IP, TCP et UDP ainsi que les protocoles majeurs utilisés en TCP/IP.

Programme de la formation :

-L'interface de Wireshark.
-Comment capturer un flux réseau
- Avec un Hub
- Avec un switch
- Avec un TAP
- A partir d'un firewall

-Comment créer et utiliser des filtres de capture pour ne garder que les trames intéressantes.
-Comment gérer les préférences et les options de capture.
-Comment colorer les trames pour mieux identifier les flux.
-Comment créer et utiliser les filtres d'affichage pour se concentrer sur les flux pertinents.
-Comment utiliser et formater les différents horodatages disponibles.
-Comment créer de nouvelles colonnes avec des informations contenues dans les trames.
-Comment utiliser les profils pour changer rapidement les réglages mis en œuvre selon le cas à traiter (analyse TCP, DNS, http, recherche de problèmes de performance)
-Sauvegarde et impression des captures
-Exemples concrets d'analyse de flux
- Analyse du niveau 2 en Ethernet switché
- Analyse des flux ICMP, ARP, IP, UDP, TCP
- Analyse des flux applicatifs (DNS, DHCP, http, FTP)

-Comment exploiter les principales statistiques et les principaux graphiques à des fins de diagnostic.
-Présentation succincte des outils en ligne de commande
- wireshark.exe
- tshark.exe
- dumpcap.exe

Organisme de formation :
Alliance Du Numérique – 49 rue Léonard Jarraud - 16000 ANGOULEME

Accessibilité : Accueil des personnes en situation de handicap. Nous contacter pour étudier un éventuel aménagement à formation@alliancedunumerique.fr

49, rue Léonard Jarraud
16000 ANGOULEME
0 806 110 142 Service gratuit + prix appel
contact@alliancedunumerique.fr
www.alliancedunumerique.fr
Siret : 834022535 00019
N°TVA INTRA : FR 50834022535

11 octobre 2022