+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 23/04/2024

S'inscrire

Formation Wireshark

3 jours (21 heures)

Présentation

Notre formation Wireshark vous plongera dans le monde captivant de l'analyse réseau et vous dotera des connaissances et compétences essentielles pour maîtriser cette technologie de pointe.

Ce programme de formation couvre un large éventail de sujets, allant de l'introduction à Wireshark jusqu'aux aspects avancés tels que l'analyse de paquets, la détection d'anomalies réseau et la résolution de problèmes de performance.

Vous serez initié aux concepts fondamentaux de l'analyse réseau et vous explorerez les différentes applications dans divers secteurs industriels, de la cybersécurité à la gestion de réseaux d'entreprise.

Grâce à notre formation, vous apprendrez à utiliser les fonctionnalités avancées de Wireshark pour capturer, filtrer et analyser le trafic réseau de manière efficace.

Vous découvrirez également comment interpréter les données capturées pour identifier les problèmes de performance, les failles de sécurité et les comportements suspects sur le réseau.

Comme d'habitude, nous utiliserons la dernière version stable et les dernières ressources de Wireshark.

Objectifs

- Comprendre le rôle du Forensic réseau et ses applications
- Maîtriser l'utilisation des filtres de capture et d'affichage personnalisés
- Détecter et analyser le trafic en clair pour identifier les vulnérabilités
- Réaliser une forensic d'email avec Wireshark
- Configurer Wireshark pour le dépannage et l'analyse des performances réseau

Public visé

- Administrateurs réseau
- Ingénieurs en sécurité informatique
- Analystes de la performance réseau

Prérequis

- Une connaissance de base en réseau et en protocoles TCP/IP est recommandée
- Des notions préalables sur les outils d'analyse réseau seraient également bénéfiques

PROGRAMME DE NOTRE FORMATION WIRESHARK

INTRODUCTION AU FORENSIC RÉSEAU

- Comprendre le rôle du Forensic réseau et ses applications
- Découvrir les principes et les fonctions de base de Wireshark
- Installer Wireshark et se familiariser avec l'interface utilisateur
- Configurer les options de base pour la capture des paquets
- Apprendre à naviguer dans les différentes fenêtres de Wireshark

PARAMÉTRAGE AVANCÉ DE WIRESHARK

- Créer et utiliser des filtres de capture et d'affichage personnalisés
- Gérer et configurer des profils d'analyse pour différents cas d'utilisation
- Maîtriser les commandes de capture réseau en ligne de commande avec Tshark
- Comprendre l'importance des couleurs dans l'analyse de paquets
- Sauvegarder et partager des configurations pour une utilisation collaborative

ANALYSE DES MENACES DE SÉCURITÉ SUR LES LAN

- Détecter et analyser le trafic en clair pour identifier les vulnérabilités
- Reconnaître les attaques de sniffing et les techniques de reconnaissance réseau
- Identifier les tentatives de craquage de mots de passe et autres types d'attaques
- Utiliser les outils complémentaires de Wireshark pour une analyse plus approfondie
- Concevoir des filtres d'affichage pour isoler et examiner des menaces spécifiques

ANALYSE DES COMMUNICATIONS EMAIL

- Réaliser une forensic d'email avec Wireshark
- Analyser les attaques ciblant les communications email
- Comprendre le protocole SMTP et autres protocoles d'email
- Utiliser des filtres pour isoler le trafic email

- Étudier des exemples de phishing et de spam

INSPECTION DU TRAFIC MALWARE

- Préparer l'environnement Wireshark pour l'inspection du trafic malveillant
- Identifier les caractéristiques du trafic de Botnets IRC
- Utiliser des filtres avancés pour détecter la communication avec les serveurs de commande et contrôle
- Réassembler les flux de données pour extraire des malwares
- Analyser les paquets pour détecter les anomalies et les signaux d'activités malveillantes

ANALYSE DES PERFORMANCES RÉSEAU

- Configurer Wireshark pour le dépannage et l'analyse des performances réseau
- Comprendre et analyser les problèmes de connexion TCP/IP
- Utiliser les statistiques et graphiques pour identifier les goulots d'étranglement
- Exécuter des diagnostics sur les performances des applications réseau
- Optimiser le réseau en identifiant les paquets perdus, les retransmissions et les latences

RAPPELS DES FONDAMENTAUX RÉSEAUX

- Réviser les concepts clés des communications réseau, les topologies et le modèle OSI
- Examiner le format des trames Ethernet et le protocole ARP
- Comprendre les différentes couches du modèle OSI et leur interaction
- Apprendre à interpréter les informations de protocoles de couche 2 et 3
- Aborder les protocoles de routage et de contrôle des flux

UTILISATION DE L'INTERFACE DE WIRESHARK

- Explorer en détail les fonctionnalités de la barre d'outils et de la barre d'état
- Appliquer et personnaliser des filtres pour améliorer l'analyse des paquets
- Examiner le contenu des paquets en détail
- Utiliser les fonctions de suivis de flux pour analyser des conversations spécifiques
- Gérer les annotations et les marqueurs pour faciliter l'analyse ultérieure

TÂCHES D'ANALYSE ET DÉPANNAGE AVEC WIRESHARK

- Capturer et analyser le trafic réseau pour identifier les problèmes de sécurité et de performance
- Réassembler des fichiers et écouter des communications VoIP
- Identifier et résoudre les problèmes de latence et de performance TCP
- Détecter les erreurs applicatives et problèmes de congestion
- Utiliser des techniques avancées pour l'analyse de sécurité, y compris l'identification de trafic suspect et de reconnaissance réseau

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.