400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

HACKING ET SÉCURITÉ CODE2UTF('8211',0) UTILISATION DE WIRESHARK

CODE STAGE : S0006

OBJECTIFS

Savoir positionner WireShark dans le domaine de la sécurité informatique
Scode2utf('8217',0)approprier les paramétrages avancés de WireShark
Savoir exploiter et interpréter les analyses de paquets obtenues avec WireShark

DURÉE

4 jours

PUBLIC

Administrateurs réseaux
Professionnels de la sécurité informatique

PRÉ-REQUIS

Notions de sécurité informatique
Expériences dans lcode2utf('8217',0)administration des réseaux (LAN et WAN)

PROGRAMME

INTRODUCTION
Définition du Forensic
Les types de Forensics
Forensic réseau
Wireshark, principes et fonctions de base

PARAMÉTRAGE AVANCÉ DE WIRESHARK
Filtres de capture et filtres dcode2utf('8217',0)affichage
Création de profiles
Techniques essentielles
Sniffing réseau en lignes de commandes

ANALYSE DES MENACES DE SÉCURITÉ SUR LES LAN
Analyse de trafic en clair
Analyse dcode2utf('8217',0)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 dcode2utf('8217',0)affichages importants

ANALYSE DES COMMUNICATIONS EMAIL
Forensic dcode2utf('8217',0)email
Analyse dcode2utf('8217',0)attaques sur les communications email
Filtres importants

INSPECTION DU TRAFIC MALWARE
Préparation de Wireshark
Analyse de trafic malveillant
Botnets IRC

ANALYSE DES PERFORMANCES RÉSEAU
Création dcode2utf('8217',0)un profile spécifique au dépannage réseau
Optimisation avant analyse
Problèmes liés à TCP/IP