

Formation Sécurité d'un accès à Internet

Durée :	3 jours
Public :	Tous
Pré-requis :	Connaissances de Windows, Linux, Mac
Objectifs :	Comprendre les enjeux de la sécurité d'un accès Internet
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	RéS444-F
Note de satisfaction des participants:	Pas de données disponibles

Introduction

Protocoles en jeu
Délimitation du périmètre à sécuriser
Définition des menaces, motivations

La menace externe

Parcours automatiques du réseau et scans
Déni de service
Intrusions
Perte d'information

Atelier pratique : détection et protection contre différents types d'attaque : SYN Flood, UDP flood, ICMP flood.

La menace interne

Vulnérabilité des postes clients
Sécurité et cloisonnement
Gestion des accès au réseau

Atelier pratique : surveillance d'un réseau interne, analyse des vulnérabilités d'un client

Protection

Réduction de la surface d'attaque
Définition du pare-feu
Filtrage entrant
Filtrage sortant

Atelier pratique : limitation des services sur un système linux, Windows

Mise en œuvre

Problématiques des attaques de masse et de l'exploitation du réseau

Limiter les risques d'intrusion sur Windows

Principes de configuration pour UNIX, Linux et Mac OS pour l'accès à Internet

Atelier pratique : mise en place d'un pare-feu, observations