Implémenter la sécurité des réseaux

En suivant cette formation, vous allez acquérir les compétences nécessaires pour implémenter les principales solutions de sécurité afin d'assurer une protection avancée contre les attaques de cyber sécurité. Vous développerez vos connaissances dans la mise en oeuvre et l'exploitation des technologies de sécurité de base: sécurité des réseaux, sécurité dans le cloud, sécurité du contenu, protection et détection des points d'extrémité, accès sécurisé aux réseaux.

Pré-requis : *CCNA ou notions équivalentes, connaissances en réseau et système.*

Modalité :
- Distanciel en classe virtuelle
- E-learning : à venir
- Présentiel

Communauté: community.reconvert.net

Durée totale : 28 H (4 jours)

PLAN DETAILLE

Introduction à la sécurité réseau

Concepts fondamentaux de la sécurité réseau
CIA : confidentialité, intégrité, disponibilité
Types de menaces et attaques :
+ malware
+ attaques DDoS
+ phishing, etc.
Vulnérabilités communes:
+ erreurs de configuration
+ failles logicielles, etc.
Principes de défense en profondeur

Sécurité des périphériques réseau

Gestion et surveillance des périphériques (SNMP, syslog)
Privilèges et commandes CLI basées sur les rôles
Mise en oeuvre de:
+ l'authentification
+ l'autorisation
+ la comptabilité (AAA)(RADIUS, TACACS+)

Filtrage de trafic et pare-feu

Configurer listes de contrôle d'accès
Configurer les pare-feu basés sur les zones (ZBF)
Types de pare-feu: stateless, stateful

Sécurité de la couche 2

Attaques de la couche 2:
+ attaques ARP
+ attaques de diffusion
Mitigation des attaques de la couche 2 (VLAN, STP)

Systèmes de prévention des intrusions (IPS)

Principes de fonctionnement des IPS
Types d'IPS (NIPS, HIPS)
Configuration et gestion des IPS

Cryptographie

Concepts de base:
+ chiffrement
+ hachage
+ signatures numériques
Algorithmes de chiffrement symétrique et asymétrique
Infrastructure à clé publique (PKI)

Sécurité des points d'extrémité

Vulnérabilités des points d'extrémité
Protection des points d'ex-trémité:
+ antivirus
+ anti-malware
+ fire-walls logiciels
Gestion des correctifs et des MAJ

Implémenter la sécurité des réseaux

En suivant cette formation, vous allez acquérir les compétences nécessaires pour implémenter les principales solutions de sécurité afin d'assurer une protection avancée contre les attaques de cyber sécurité. Vous développerez vos connaissances dans la mise en oeuvre et l'exploitation des technologies de sécurité de base: sécurité des réseaux, sécurité dans le cloud, sécurité du contenu, protection et détection des points d'extrémité, accès sécurisé aux réseaux.

Pré-requis : *CCNA ou notions équivalentes, connaissances en réseau et système.*

Modalité :
- Distanciel en classe virtuelle
- E-learning : à venir
- Présentiel

Communauté: community.reconvert.net

Durée totale : 28 H (4 jours)

PLAN DETAILLE

VPN

Protocoles VPN (IPsec, SSL/TLS)
Configurer un VPN IPsec site-à-site
Utiliser des VPN pour l'accès à distance

Cisco ASA

Présentation du Cisco ASA
Configurer le pare-feu ASA via CLI et ASDM
Fonctionnalités avancées du Cisco ASA

Tests de sécurité

Méthodes de test de sécurité:
+ tests d'intrusion
+ analyse des vulnérabilités
Outils de test de sécurité:
+ nmap
+ Wires-hark
Analyse des résultats des tests