Formation Cybersécurité Avancé : Hacking et Sécurité Réseaux

Durée :	5 jours
Public :	Administrateurs Réseaux expérimentés
Pré-requis :	Très bonnes connaissances des réseaux
Objectifs :	Découvrir la sécurité Réseau - Comprendre les failles et menaces - Protéger ses infrastructures
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	RéS100230-F
Note de satisfaction des participants:	Pas de données disponibles

Maîtriser les fondamentaux de la Cybersécurité

Problèmes de sécurité sur l'Internet
Origine des failles, risques et menaces
Fondamentaux sur la gestion des risques
Organigramme typique d'une attaque
Logiciels malveillants (état de l'art)
Risques liés aux Malware
Antivirus (fonctionnement et limites)
Attaques logiques
Analyse d'une APT (Advanced Persistent Threat)
Authentification et gestion de mots de passe
Menaces sur les applications Web (OWASP...)

Identifier les attaques réseaux

Sécurité des réseaux LAN (Ethernet, VLAN...)
Attaques réseau classiques : usurpation, man-in-the-middle, déni de service...
Techniques de reconnaissances et de prise d'empreinte à distance
Attaques par déni de service : taxonomie, moyens de protection

Atelier pratique : exploitation ARP, prise d’empreinte via nmap

Mettre en place des pare-feux et architectures de sécurité

Problématique des architectures de sécurité
Exemples d'architectures sécurisées : DMZ, cloisonnements, VLANs multiples
Pare-feux réseaux (filtres de paquets, relais applicatifs, stateful inspection)
Acteurs majeurs du marché des pare-feux réseaux, comparaison entre produits commerciaux et produits non commerciaux

Critères de choix d'un pare-feu réseau
Exemple de configuration d'un pare-feu réseau
Évolution des pare-feux

Atelier pratique : mise en place d’un pare-feu basique et de routage de ports avec iptables

Maîtriser les protocoles de sécurité réseau

Contextes IPv4 et IPv6 : nature des faiblesses de chacun des protocoles
Handshake, record, alert et change
Faiblesses inhérentes aux protocoles : telnet vs ssh v1 / v2, encapsulation, tunnelling
TLS/SSL : rôle et fonctionnement, historique des failles, appréhension de l’impact
Le problème du repli (fallback)
Réseaux privés virtuels (VPN) : typologie des réseaux VPN, architectures et protocoles PPTP et L2TP, solutions techniques, état de l'art.
IPsec : principe de fonctionnement, mise en œuvre, architecture, modes de fonctionnement

Atelier pratique : analyse de trafic SSL, mise en place d’une session IPSec, franchissement de firewall via un tunnel ssh.

Détecter et gérer des événements de sécurité

Détection/prévention d'intrusion (IDS/IPS) : principes, architectures, mise en œuvre
Gestion des événements de sécurité (SIEM) : principes, architectures, mise en œuvre
Monitoring des logs : principes, architecture, mise en œuvre, que chercher et comment réagir ?

Atelier pratique : positionnement d’IDS, port mirroring, mise en place de suricata

Réaliser des audits de sécurité techniques

Social engineering (techniques)
Sécurité par mots de passe (cassage, politiques de mot de passe)
Audits de sécurité (état de l'art des catégories, démonstrations d'outils)
Audit organisationnel
Audit de configuration
Recherche de vulnérabilités par Metasploit et Nessus ou OpenVAS

Atelier pratique: Mise en situation d'une gestion de crise en simulation d'une attaque cybersécurité

Appréhender la sécurité des réseaux Wi-Fi (802.11)

Problématiques de sécurité : historique et état actuel
Principes de sécurisation (802.11i, 802.1X, EAP)
Architectures hot-spot, résidentielle, entreprise
Problématique du repli

Atelier : découverte de mot de passe avec aircrack-ng, usurpation de portail captif.

Atelier final : Mise en situation.

Dans le cadre du déploiement d’une appli web via un accès wifi dédié, diagnostiquer les faiblesses à chaque étape de l’établissement de la connexion jusqu’à l’application, et émettre les

recommandations appropriées.

Synthèse et conclusion