

01/ Généralités sur la sécurité

Les besoins fondamentaux de sécurité
La cybercriminalité
L'environnement juridique
Les organismes à connaître

02/ Vulnérabilités et attaques

Vulnérabilités : Exemple d'outils : Scapy, Taof, Sulley, GDB, Metasploit
Au niveau du réseau
Buffer overflow
Format Strings
Off-by-One
Race Condition
Use-After-Free
Trouver des vulnérabilités avec le fuzzing
Réseau : Exemple d'outils : Dsniff, SSLStrip, Evilgrade, Wireshark, Scapy, Cuckoo, Aircrack-ng
Sniffing
ARP Spoofing, DNS Poisoning (attaque Kaminsky)
Man-in-the-middle
VLAN Hopping, CAM Flooding
Déni de service, DDoS, DrDos
Malwares
Sécurité du Wifi (faiblesses WEP, WPA)
Tests d'intrusion : Exemple d'outils : Google Hacking, Exiftool, Maltego, TheHarvester, AMAP, NMAP, OpenVAS, Metasploit
Reconnaissance
Cartographie e du réseau
Scan de vulnérabilités
Exploitation des vulnérabilités
Post-exploitation
Au niveau Web : OWASP Top 10
Focus SQL Injection
Focus XSS
Focus CSRF
Focus Principales failles PHP

03/ Solutions techniques

Exemple d'outils : OpenSSL, EMET, Snort, Medusa, JohnTheRipper, iptables, Check Point firewalls
Défense en profondeur
Modèle de sécurité des systèmes d'exploitation récents
Mesures de sécurité avancées : DEP, ASLR, Stack Canaries, UEFI, UAC et tokens
Sécurité de l'accès au réseau (802.1X, Radius, VLANs)
Cloisonnement réseau avec les firewalls : DMZs, Stateless, Stateful
Mise en oeuvre de Proxys
Sondes de détection et de prévention d'intrusion
Authentification et gestion des identités
Cryptographie et VPNs (IPSEC, SSL, MPLS)
Supervision et SIEM

04/ Travaux pratiques réalisés

(50%)

REF. VS-015

PUBLIC

Responsables de la sécurité des systèmes d'information, administrateurs de réseaux, responsables informatiques et toute personne souhaitant connaître et résoudre les problèmes de sécurité informatique en entreprise.

OBJECTIFS

L'apprentissage des tests d'intrusion. Les échanges au travers de réseaux publics ou privés.

PRÉREQUIS

Bonnes connaissances de TCP/IP.

MOYENS PÉDAGOGIQUES

1 ordinateur et 1 support de cours par personne + 1 vidéoprojecteur. Évaluation par écrit en fin de cours et attestation de stage délivrée en fin de formation.