

SECURITE RESEAU

OBJECTIFS

Comprendre et détecter les attaques sur un S.I.

Définir l'impact et la portée d'une vulnérabilité

Réaliser un test de pénétration

Corriger les vulnérabilités

Sécuriser un réseau, et intégrer des outils de sécurité adéquats

PARTICIPANTS

Ingénieurs, Techniciens, Administrateurs systèmes et réseaux.

PRE-REQUIS

Connaissance de la suite des protocoles TCP/IP.

METHODE PEDAGOGIQUE

Théorie : 60%

Pratique : 40%

MOYENS PEDAGOGIQUES ET TECHNIQUES :

Salle informatique équipée pour 8 participants et son formateur.

Supports de cours inclus.

Sécurité et hacking

PROGRAMME

- ✓ **Introduction : Rappel TCP/IP**
- ✓ **Prise d'informations**
 - Présentation des techniques de prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants / Informations publiques / Enumération des systèmes / Enumération des services / Enumération Netbios / Fingerprinting applicatif / Enumération des règles réseau
- ✓ **Vulnérabilités clients**
 - Intrusion à distance des postes clients par exploitation des vulnérabilités sur les navigateurs Web, clients de messagerie... : Les troyens / Auto exécution de troyens
- ✓ **Vulnérabilités applicatives**
 - Intrusion à distance d'un système Windows et Linux par l'exploitation des services de type applicatif, avec la plateforme Metasploit / Escape shell / Buffer overflow
 - Etude de méthodologies d'attaques avancées en local et prise de contrôle du statut administrateur
 - Utilisation et intégration d'exploit à Metasploit
- ✓ **Vulnérabilités réseaux**
 - Attaques des règles de Firewalling, interception/analyse des transmissions réseaux cryptées / Sniffing réseau / Spoofing réseau / Bypassing de firewall / Idle Host Scanning / Détournement de connexions / Attaques des protocoles sécurisés / Déni de service
- ✓ **Vulnérabilités Web**
 - Attaque des scripts Web dynamiques (PHP, Perl ...), et des bases de données associées (MySQL, Oracle) / Cartographie du site / Failles PHP (include, fopen ...) / Attaques CGI (Escape shell...) / Injections SQL / XSS
- ✓ **Failles de type système**
 - Backdooring et prise de possession d'un système suite à une intrusion et maintien des accès / Brute force d'authentification / Espionnage du système / Backdoor Kernel
- ✓ **Sécurité générique**
 - Outils génériques de surveillance et de sécurisation du système/ réseau. / Cryptographie / Sécurité système / Firewall / VPN / IDS

