Plan formation

sécurité Avancé 5 jours

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 lesnavigateurs Web, clients de messagerie...

- Les troyens
- Auto exécution de troyens

Vulnérabilités réseaux

Attaques des règles de Firewalling,interception/analyse des transmissionsréseaux cryptées

- Sniffing réseau
- Spoofing réseau / Bypassing de firewall
- Idle Host Scanning
- Détournement de connexions
- Attaques des protocoles sécurisés
- Dénis 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

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

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