PROGRAMME DÉTAILLÉ

Code : 7619

LINUX PERFECTIONNEMENT AU HACK ETHIQUE ET DEONTOLOGIQUE

Introduction

- La notion de pentesting.
- Les limites à la sécurité offensive

Présentation des distributions de pentesting

- Les livesCD, LiveUSB persistents, et les linux embedded
- Présentation de la distribution et des outils du stage

Présentation des machines virtuelles du stage

- Présentation de VirtualBox.
- Présentation du contexte réseau des VMs.

Effectuer une cartographie complète d'une cible

Utilisation des outils de cartographie

- Utilisation des outils de type nmap.
- Utilisation de l'outil internet
- La messagerie et la collecte d'information.
- Attaque d'un poste client et contournement des défenses.

La problématique de l'accès physique

- Exemple d’une machine windows accédée illicitement.
- Exemple d’une machine linux accédée illicitement.

Ingénierie sociale et prise d'information

- Présentation des supports utilisés.
- Présentation des outils utilisés (SE).
- Quelques exemples de failles exploités.
- Une méthode très vaste

Trouver des failles de sécurité

Les failles système

- Les comptes utilisateurs et les comptes techniques
- Les droits sur les fichiers
- La mémoire

Les failles liées au réseau

- La gestion des flux réseaux et des services
- La supervision, la sécurité n’est jamais acquise

Les failles applicatives

- Attaque des failles de type Web sur les serveurs
- Attaque sur les programmes du poste client

Exploiter les failles de sécurité

- Avec la plateforme metasploit
  - msfpayload & meterpreter
  - search & use & exploit
- Au moyen des exploits publiés
  - searchsploit
  - utilisation des cve, exploitdb etc
- Directement sur les programmes
  - Les buffer overflows

- Le cracking de code

La sécurité des applications en DMZ

De l'accès à la machine jusqu'à l'obtention des droits administrateurs (root) .

- Le sniffing (ex. avec connexion ssh)
- Le spoofing réseau, tunneling & bypassing de firewall
- Le vol de session TCP / HotSpot / macchanger
- Attaque de type MITM avec ettercap / certificat ssl
- Attaques des protocoles sécurisés, dénis de service
- Architecture n-tiers et isolation des flux, limites

Les techniques de maintien des accès

- L'installation d'un rootkit
- Le remplacement de binaires essentiels setuid
- Backdoor kernel
- Les modules kernels
- Contremesures au maintien dans le système