HACKING & SÉCURITÉ: NIVEAU AVANCÉ

Mieux se défendre par la pratique des attaques

Code : CYBERHSA

Durée : 5 jours

Réduction pour particuliers et demandeurs d'emploi

OBJECTIFS :

- Appliquer les méthodes de prise d'informations
- Mettre en place des attaques distantes et locales
- Exécuter une attaque système et applicative (buffer overflow)
- Pratique d'attaques WEB
- Application des connaissances sur un TP final

PUBLIC :

Consultant en sécurité / RSSI / Techniciens / Administrateurs réseaux / Ingénieurs / Développeurs

PRE-REQUIS :

Avoir suivi la formation CYBERHSF

Bonne maîtrise des protocoles réseaux

Connaissance sur les applications WEB

Des bases en cryptographie

LES PLUS :

- Support de cours
- 70% de mise en pratique
- 1 PC par personne

PROGRAMME

JOUR 1

Informations et Réseaux:
- Objectifs et définitions
- Prise d'informations publiques
- Le scan de ports
- L'énumération (prise d'empreinte des services)

JOUR 2

Attaques réseaux
- Spoofing et sniffing réseau

Attaques système
- Exploitation de vulnérabilités
- Création de malware avec Metasploit
- Scanner de vulnérabilités
- Maintien d'accès dans une machine

CONTACTEZ-NOUS :

formation@cybernethique.com

07-54-37-19-17

JOUR 3

Vulnérabilités Web
- Analyse de site
- Les vulnérabilités WEB
- Les injections SQL
- Cross-site Scripting
- Open Redirect
- Comment se protéger

JOUR 4

Scanner Vulnérabilités Web
- L'outil Burp Suite
- Le Fuzzing avec l'outil Wfuzz

Attaques applicatives
- Définition du Buffer Overflow
- Cas pratique sous Linux

JOUR 5

CTF (Capture the Flag)

-Mise en pratique du cours sur une machine virtuelle (TP final)