



3. Fondamentaux de la cybersécurité en 5 jours avec Labs

OBJECTIFS DE LA FORMATION

L'objectif de cette formation est de :

- Comprendre les tendances des menaces actuelles sur l'Internet et leur impact sur la sécurité de l'organisation.
- Vouiserer la terminologie standard de la cybersécurité et les exigences de conformité
- Examiner des exemples d'Exploit et bénéficierez d'une expérience pratique des mesures d'atténuation vue professionnel (marketing, scientifique, managérial, culturel, design) que personnel
- Travaillerez avec des virus vivants, comme les botnets, les vers et les chevaux de Troie.



La durée de la formation est de 5 jours avec Labs.

CONTENU DE LA FORMATION

Jour 1

Les différents points qui seront traités sont les suivants :

1. Le champ de bataille cybernétique ;
2. Structure de l'Internet TCP/IPs ;
3. Évaluation de la vulnérabilité et outils ;
4. Sensibilisation à la cybersécurité.

Lab 1 : récupération technique d'un mot de passe avec l'ingénierie sociale

Jour 1

Les différents points qui seront traités sont les suivants :

1. Cyber-attaques : Footprinting et scannage ;
2. Cyberattaques : Effraction.

- **Lab 2 : énumération des services sur une cible**
- **Lab 3 : scans des ports et des vulnérabilités**
- **Lab 4 : Attaque par Brute force des mots de passe**
- **Lab 5 : Maintien l'accès permanent sur une cible MS windows**
- **Lab 6 : Prise de contrôle d'une cible à distance**

3. Fondamentaux de la cybersécurité en 5 jours avec Labs

Jour 3

Les différents points qui seront traités sont les suivants :

1. Cyberattaques : Porte dérobée et cheval de Troie (Backdoor and Trojans) ;
2. Évaluation et gestion des risques cybernétiques ;
3. Gestion des politiques de sécurité.

- **Lab 7 : création d'un malware et attaque d'une cible**

Jour 4

Les différents points qui seront traités sont les suivants :

1. Sécurisation des serveurs et des hôtes ;
2. Sécurisation des communications ;
3. Authentification et solutions de chiffrement.

- Lab 8 : durcissement des contrôles techniques avec les référentiels internationaux
- Lab 9 : attaques sur les hashes des mots de passe
- Lab 10 : chiffrement des fichiers et des disques

Jour 5

Les différents points qui seront traités sont les suivants :

1. Pare-feu et dispositifs de pointe ;
2. Analyse criminalistique ;
3. Reprise et continuité d'activité ;
4. Cyber-révolution.

- **Lab 11 : mise en place d'un IDS**

CYBERSECURITE

3. Fondamentaux de la cybersécurité en 5 jours avec Labs (Suite et fin)

FORMAT

La formation se passe sous forme de présentation Powerpoint, d'interactions entre les participants et le formateur et d'ateliers pratiques entre les participants.

INTERVENANT**Hafedh BEN HAMIDA**

• Tunisien résident en France, ingénieur certifié CISSP®, Expert Senior en sécurité des systèmes d'information. Avec plus de 17 ans d'expérience en conseil stratégique, tactique et opérationnel en sécurité pour des grands groupes internationaux et de nombreuses PME/PMI, M.BEN HAMIDA est aujourd'hui l'un des formateurs africains les plus reconnus

Pour avoir plus de détails sur les contenus de la formation veuillez cliquer ici : [Plan de formation 5 jours avec Labs](#)