

Réf : ET_SEC_ETHA

Ethical Hacking

Prise d'empreintes et failles applicatives

Objectif

Cette e-formation s'adresse aux informaticiens, aux RSSI ou aux DSI qui souhaitent appréhender les concepts et les technologies liés à la sécurité des systèmes d'information. Elle vous permettra de comprendre la notion de prise d'empreintes et de failles applicatives.

Public

Informaticiens, RSSI, DSI

Durée estimée

pour le suivi des modules indispensables

3h24

Contenu pédagogique

► Les modules indispensables

Ethical Hacking - La prise d'empreintes (2e version)



Vidéo

Ce module vous propose la consultation d'une vidéo d'une durée de 1h39.

- **Définitions et étapes d'une attaque informatique**
 - Définitions
 - Les étapes d'une attaque
- **Les outils pour la recherche d'informations**
 - Kali Linux
 - Google dorks
 - Theharvester
 - Maltego
 - Shodan
- **Prise d'empreintes informatique**
 - Nmap
 - Netdiscover
 - DNSEnum
- **Conclusion**
 - Conclusion

Ethical Hacking - Les failles applicatives (2e version)



Vidéo

Ce module vous propose la consultation d'une vidéo d'une durée de 1h48.

- **Introduction**
 - Définitions et types de failles
 - Stack overflow et Heap overflow
- **Le microprocesseur et les mémoires**
 - Le fonctionnement des microprocesseurs
 - Les registres
 - Les mémoires
- **Les bases du langage Assembleur**
 - Le langage Assembleur
 - La pile (registres ESP, EBP et EIP)
- **Buffer overflow**
 - Ability Server et Immunity Debugger
 - Fuzzing
 - Address Space Layout Randomization (ASLR)
 - Trouver des shellcodes
- **Outrepasser la protection SEH**
 - Principe et écrasement SEH
 - Exploitation
- **Conclusion**
 - Conclusion

► Le module en complément

Sécurité informatique - Ethical Hacking : Apprendre l'attaque pour mieux se défendre (6e édition)



Livre

Ce module vous propose la consultation d'un support de cours numérique.

- Introduction et définitions
- Éléments d'ingénierie sociale
- Black Market
- Prise d'empreinte ou Information Gathering
- Les failles système
- Les failles réseau
- La sécurité des communications sans fil
- Les failles web
- Les failles applicatives
- Forensic
- Malwares : étude des codes malveillants
- Les appareils mobiles : failles et investigations
- Les failles matérielles
- La sécurité des box
- Hacking du véhicule connecté
- Risques juridiques et solutions