

## Objectif

Le cours CEH forme et certifie les stagiaires à la discipline d'un "pirate éthique" dans un environnement basé sur la sécurité, d'une perspective entièrement neutre car non liée à des fabricants.

Ce cours très dense, donné sur 5 jours, vous plongera dans un environnement interactif dans lequel vous découvrirez comment scanner, tester et pirater votre propre système. L'environnement intensif de laboratoire et d'exercices pratiques vous donnera des connaissances pointues et une expérience réelle des principaux systèmes de sécurité actuels. Vous serez amené à comprendre comment fonctionne la défense périmétrique avant de scanner et d'attaquer votre propre réseau. Vous apprendrez ensuite comment les intrus acquièrent des privilèges et quelles actions peuvent être mises en œuvre pour sécuriser un système. En suivant ce cours, vous apprendrez également à détecter les intrusions, mettre en place une politique de création, comprendre ce qu'est l'ingénierie sociale, la gestion des incidents et l'interprétation des logs.

Le but du cours CEH est d'aider les organisations à prendre des mesures pro-actives contre les attaques malicieuses en attaquant soi-même son système, tout en restant dans des limites strictement légales.

## Participant

Cette formation est particulièrement recommandée aux personnes en charge de la sécurité, auditeurs, professionnels de la sécurité, administrateurs réseaux et à toute personne concernée par l'intégrité de l'infrastructure du réseau. Elle permet à des professionnels confirmés de comprendre et savoir reconnaître les faiblesses et vulnérabilités d'un système donné et utilise les mêmes connaissances et outils qu'un pirate non éthique.

## Remarque

Le support de cours est en anglais. L'examen CEH est le 312-50.

## Programme

- 1. Introduction au Ethical Hacking**
- 2. lois sur le Hacking**
- 3. Footprinting**
- 4. Hacking via Google**
- 5. Scanning**
- 6. Enumération**
- 7. Hacking de système**
- 8. Chevaux de Troie & Backdoors**
- 9. Virus & Vers**
- 10. Sniffers**
- 11. Ingénierie sociale**
- 12. Phishing**
- 13. Hacking de comptes de messagerie**
- 14. Attaques par Déni de Service**
- 15. Hijacking de sessions**
- 16. Hacking de serveurs Web**
- 17. Vulnérabilités d'application Web**
- 18. Techniques de Cracking de mot de passe Web**
- 19. Injection SQL**
- 20. Hacking de réseaux sans fil**
- 21. Sécurité physique**
- 22. Hacking de Linux**
- 23. Evading IDS, Firewalls and Detecting Honey Pots**
- 24. Débordement de tampons**
- 25. Cryptographie**
- 26. Tests d'intrusion**
- 27. Covert Hacking**
- 28. Ecriture de codes de virus**
- 29. Assembly Language Tutorial**
- 30. Exploit Writing**
- 31. Smashing the Stack for Fun and Profit**
- 32. Windows Based Buffer Overflow Exploit Writing**

- 33. Reverse Engineering**
- 34. Hacking de MAC OS X**
- 35. Hacking de Routeurs, Modems & Firewalls**
- 36. Hacking de téléphones portables,PDA & autres appareils mobiles**
- 37. Hacking de Bluetooth**
- 38. Hacking de VOIP**
- 39. Hacking de RFID**
- 40. Spamming**
- 41. Hacking de périphériques USB**
- 42. Hacking de serveurs de base de données**
- 43. Cyber Warfare Hacking, AlQaida & Terrorisme**
- 44. Techniques de filtrage de contenus Internet**
- 45. Espace privé sur Internet**
- 46. Sécuriser des PC portables**
- 47. Technologies d'espionnage**
- 48. Corporate Espionage- Hacking Using Insiders**
- 49. Créer des stratégies de sécurité**
- 50. Piratage de Software & Warez**
- 51. Hacker et tricher les jeux en ligne**
- 52. Hacking RSS and Atom**
- 53. Hacking de navigateurs Web (Firefox, IE)**
- 54. Technologies de serveurs Proxy**
- 55. Prévention de perte de données**
- 56. Hacking Global Positioning System (GPS)**
- 57. Computer Forensics and Incident Handling**
- 58. Fraudes sur les cartes de crédit**
- 59. Comment dérober des mots de Passe**
- 60. Les technologies de Pare-Feux**
- 61. Menaces et Contre-mesures**
- 62. Études de cas**