



Hacking Éthique : Le Cours Complet

[Continuer vers Lecture 4](#)

★★★★★ Modifier votre note

87 of 87 items complete [Réinitialiser la progression](#)

[Aperçu](#)[Contenu du cours](#)[Q&R](#)[Marque-pages](#)[Annonces](#)[Options ▼](#)[Section en cours](#)[Toutes les sections](#)[Toutes les ressources](#)

Section : 1

1 / 1

Introduction

4. Pourquoi il est intéressant d'apprendre la sécurité informatique

5:07



<https://bountyfactory.io/fr/index.html>

<https://www.akaoma.com/formation/ceh-certified-ethical-hacker>

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

<https://sysdream.com/formation-securite-informatique/securite-offensive-ethical-hacking/certified-ethical-hacker-v9/>

Section : 2

3 / 3

Démarrer en Sécurité Informatique

5. Découvrez si vous avez été piraté en piégeant dès maintenant vos systèmes !

8:02



<http://whatstheirip.com/>

<https://grabify.link/>

8. Les Concepts de Sécurité (Défense en profondeur, modèle Zéro confiance)

6:49



[Défense en profondeur https://fr.wikipedia.org/wiki/D%C3%A9fense_en_profondeur](https://fr.wikipedia.org/wiki/D%C3%A9fense_en_profondeur)

9. Rappels sur le Lois

8:39



[Lois-Hacking.docx](#)

Section : 3

8 / 8

Le Hacking éthique : fondamentaux et préparation du Lab

10. Télécharger & Installer VirtualBox

2:38



<https://www.virtualbox.org/wiki/Downloads>

11. Installation Facile de Kali Linux en tant que machine virtuelle

8:18



[Résolution de soucis \(voir les sujets déjà créés\) : https://forums.kali.org/](https://forums.kali.org/)

[Forum Kali Français https://www.kali-linux.fr/forum/index.php](https://www.kali-linux.fr/forum/index.php)

[Résolution de soucis BIS : https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/announcements?ids=890830](https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/announcements?ids=890830)

[Ce que doit contenir votre fichier /etc/apt/sources.list après installation](#)

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

▶

12. Installation Alternative de Kali Linux en tant que machine virtuelle

13:51

✓

🔗 Résolution de soucis (voir les sujets déjà créés) :

🔗 Forum Kali Français <https://www.kali-linux.fr/forum/index.php>

🔗 Résolution de soucis BIS : <https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/announcements?ids=890830>

🔗 Ce que doit contenir votre fichier `/etc/apt/sources.list` après installation

▶

13. En cas de soucis avec les Additions Invité (Virtualbox)

3:14

✓

📄 Problèmes-courants-Kali-Linux.docx

🔗 En cas de souci, voici le forum de Kali en français <https://www.kali-linux.fr/forum/index.php>

🔗 Si écran noir au démarrage : activer la virtualisation dans le bios

🔗 Résolution de soucis avec les additions invités : <https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/questions/2503390>

▶

14. Premiers pas avec Kali Linux

19:20

✓

🔗 Apprendre (Kali) Linux : <https://openclassrooms.com/courses/reprenez-le-controle-a-l-aide-de-linux>

🔗 Si pas de ping : désactiver pare-feu et tester autre mode de connexion (pont ou NAT)

🔗 Les commandes de base

🔗 Commandes pour pentesting (en anglais)

▶

15. Initiation à la programmation C et Python sous Kali

15:51

✓

📄 fichiers_sources.zip

▶

16. Téléchargement et installation de Metasploitable

6:30

✓

🔗 <https://sourceforge.net/projects/metasploitable/>

🔗 Si pas de ping : désactiver le pare-feu et/ou changer mode de connexion dans virtualbox

▶

17. Télécharger et Installer (gratuitement) une machine virtuelle Windows 7

5:32

✓

📄 Reactiver-win-7-apres-expiration-licence.docx

🔗 <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

🔗 N'oubliez pas de désactiver le pare-feu Windows de la machine virtuelle et de mettre le mode de connexion par pont dans Virtualbox

La Reconnaissance

▶

20. Le Google Hacking : explications et contre-mesures

9:17

✓

🔗 <http://exif.regex.info/exif.cgi>

🔗 <http://robots-txt.com/>

▶

21. Le Google Hacking partie 2 (introduction à Shodan et à la recherche Facebook)

10:14

✓

🔗 https://www.google.fr/advanced_search

🔗 <https://www.exploit-db.com/>

🔗 <https://www.shodan.io/>

🔗 <https://tineye.com/>

▶

23. Pratique avec DNS (nslookup et dig)

2:58

✓

🔗 Autre site pour récupérer des informations sur un site (DNS en particulier)

▶

25. Récupérer des informations sur les sites web (whois, adresses IP...etc)

9:49

✓

- 🔗 <https://www.iplocation.net/>
- 🔗 <https://archive.org/>
- 🔗 Introduction aux réseaux informatiques
- 🔗 Introduction à TCP/IP

▶ 26. Collecter et utiliser des données avec Maltego

10:46



- 🔗 <https://www.paterva.com/web7/>

Section : 5

4 / 4

Le Scanning Réseau & Web

▶ 30. Découvrir des services avec NMap

12:56



- 🔗 <https://nmap.org/>

▶ 31. Se protéger du Scanning réseau (pare-feu Linux)

9:13



📄 parefeu.sh

- 🔗 <https://doc.ubuntu-fr.org/ufw>

▶ 32. Découvrir des vulnérabilités Web avec Nikto et les corriger

5:52



- 🔗 <https://cirt.net/Nikto2>

▶ 33. Découvrir des vulnérabilités Web avec OWASP Zed Attack PROxy (ZAP)

9:25



- 🔗 https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Section : 6

4 / 4

Gagner l'accès

▶ 36. Les Bases de Metasploit (architecture et fonctionnalités)

8:39



- 🔗 <https://www.metasploit.com/>

▶ 37. Metasploit en pratique (exploitation d'une vulnérabilité dans Metasploitable)

9:16



- 🔗 Si "msfudpate" ne fonctionne pas : apt update; apt install metasploit-framework

▶ 38. Le Cracking de mots de passe (et pourquoi Michel1 n'est pas un bon mot de passe)

11:12



- 🔗 <http://www.openwall.com/john/>

▶ 39. Prise de contrôle à distance de la machine virtuelle Windows 7 (exploitation)

10:35



- 🔗 <http://www.oldversion.fr/windows/acrobat-reader-9-0>

Section : 7

1 / 1

Le Social Engineering (l'ingénierie sociale)

▶ 46. Le ClickJacking (Déournement de clics) et comment s'en protéger

5:07



- 🔗 https://fr.wikipedia.org/wiki/D%C3%A9tournement_de_clic

Section : 8

7 / 7

Les failles WEB

▶ 50. Mise en place de notre site vulnérable sur mesure

5:51



30. Mise en place de notre site vulnérable sur mesure

5.51

Informations sur les dossiers partagés (Virtualbox)

🔗 Si "échec de connexion" voir : <https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/questions/2522238>

🔗 <https://www.udemy.com/hacking-ethique-le-cours-complet/learn/v4/questions/2431066>

🔗 Si vous n'arrivez pas à accéder à 127.0.0.1

 sitevulnerable.zip

51. Le Top 10 OWASP : les 10 vulnérabilités web les plus populaires

10:42

🔗 [https://www.owasp.org/images/7/72/OWASP_Top_10-2017_\(en\).pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf)

53. Présentation de BeEF (Browser Exploitation Framework)

8:48

id & mot de passe : beef:beef

▶ 55. Démonstration de la faille CSRF, et comment s'en prémunir

12:26

 [attaque.html](#)

 contre-mesure-CSRF.txt

► 57. Scannons notre site vulnérable ! et autres conseils de sécurité des serveurs web

12:08

 .htaccess.txt

▶ 58. Utilisation de Damn Vulnerable Web Application et autres contre-mesures

7:36

<http://www.dvwa.co.uk/>

59. Utilisation basique de BurpSuite

🔗 <https://portswigger.net/burp/>

Section : 9

1 / 1

Les failles réseau

▶ 64. Introduction à la Sécurité Wi-Fi (notions de WEP, WPA(2), WPS)

10:19

 weplab.zip

 [fichiers-pcap.zip](#)

Section : 10

1 / 1

Les Programmes Malveillants (Malwares)

► 70. La méthode certaine pour savoir si un programme est malveillant ou non

10:06

<https://malwr.com/>

 <https://virustotal.com/>

Section : 11

2 / 2

Cryptographie

▶ 72. Introduction à PGP

11:20

https://fr.wikipedia.org/wiki/Pretty_Good_Privacy

▶ 74. Introduction à la Stéganographie

8:15

🔗 <http://steghide.sourceforge.net/>

Conclusion & Perspectives



77. Session bonus : Pour aller plus loin (offre réservée aux membres de ce cours)



<https://www.leblogduhacker.fr/les-guides/>



Avez-vous déjà pensé à créer votre propre cours Udey ?

Partagez vos connaissances sur la plus grande plate-forme d'enseignement en ligne au monde.

[En savoir plus](#)

Udey for Business

Devenir formateur

Applis mobiles

À propos d'Udey

Carrières

Blog

Sujets

Assistance

Affilié

Français ^



Droits d'auteur © 2018 Udey, Inc.

[Conditions](#)

[Politique de confidentialité et politique en matière de cookies](#)

[Propriété intellectuelle](#)