

Atelier d'initiation au hacking

Guillaume Pilot

Club de Hacking de l'Université Laval

Octobre 2015

Installation de Kali2

[Page de téléchargement de l'ISO](#)

[Instruction pour préparer une clé bootable](#)

[Guide d'installation](#)

Deux possibilités :

- ▶ Machine virtuelle (Virtualbox)
- ▶ Dualboot

Kali Linux 2 est basé sur Debian, l'installation est similaire.

Une fois l'installation terminé, créez-vous un utilisateur non root !

Site d'entraînement

CTF (Capture The Flag) :

- ▶ [Ringzer0](#)
- ▶ [Newbiecontest](#)
- ▶ [root-me](#)
- ▶ [Hack This Site](#)

Tutoriels informatique :

- ▶ [codecademy](#)
- ▶ [Open Class Rooms](#)
- ▶ [Zeste de Savoir](#)

Livres à lire

- ▶ [Les bases du hacking](#)
- ▶ [Hacking : The Art of Exploitation, 2nd Edition](#)
- ▶ [Metasploit: The Penetration Tester's Guide](#)
- ▶ [Practical Malware Analysis](#)
- ▶ [Gray Hat Hacking The Ethical Hacker's Handbook](#)

Installation Metasploitable

[Lien vers le téléchargement](#)

Metasploitable est une machine virtuelle Linux volontairement vulnérable.

Installer la VM avec Virtualbox

Réseau par pont

Accès au site web de la machine

Découverte de Metasploitable

- ▶ [Documentation](#)
- ▶ Scan des ports de la machine avec nmap
- ▶ DVWA

Découverte de Kali 2

- ▶ Interface graphique gnome3 par défaut
- ▶ Iceweasel
- ▶ Metasploit/Armitage
- ▶ [Burpsuite](#)
- ▶ [Matelgo](#)
- ▶ [Beef XSS](#)

Compétition de hacking au Québec

- ▶ [Hackfest](#)
- ▶ [Northsec](#)
- ▶ [lhack](#)

Prochain atelier

Thème : La reconnaissance

Date : Fin novembre si c'est prêt ! (sinon au début de la session prochaine)

Contenu :

- ▶ Principe théorique
- ▶ HTTrack
- ▶ Opérateur Google (GHDB)
- ▶ The Harvester
- ▶ whois/dig/nslookup
- ▶ Maltego

Idée de projet pour le lab :

- ▶ Écoute radio (antenne DBVT)
- ▶ Malware analysis sur mobile (Android/Mac)
- ▶ Raspberry pi hacking
- ▶ Botnet expérimental