

Présentation sur les bases du hacking



Plan de la présentation

Partie I

- ☐ Définition de Hacking
- ☐ Phases d'un test d'intrusion
 - ☐ Reconnaissance
 - ☐ Scan
 - ☐ Exploitation
 - ☐ PostExploitation
- ☐ Kali linux

Partie II

- ☐ Démonstration Kali Linux
 - ☐ The Harvester
 - ☐ Whois
 - ☐ Host
 - ☐ Nmap
 - ☐ Nessus
 - ☐ Metasploit
 - ☐ John the Ripper
 - ☐ Armitage
 - ☐ Nikto
 - ☐ Burp
 - ☐ Netcat

Partie III

- ☐ Livres à lire
- ☐ La pratique est l'essentiel
 - ☐ CTF
 - ☐ Club de Hacking de l'UL
- ☐ Communautés
 - ☐ QuébecSec (HackFest)
 - ☐ OWASP
 - ☐ CFI-UL
- ☐ Compétitions
- ☐ Certification
- ☐ Bug Bounty
- ☐ Idée de projet pour le Club de Hacking

Partie I

Hacker désigne un virtuose pouvant intervenir dans différents domaines comme :

- ✓ la programmation,
- ✓ l'architecture matérielle d'un ordinateur,
- ✓ l'administration système,
- ✓ l'administration réseau,
- ✓ la sécurité informatique,
- ✓ tout autre domaine de l'informatique



Les premiers « hackers »
apparaissent dans les
universités

Les chapeaux blancs ou white hat



Un white hat est un hacker éthique ou un expert en sécurité informatique qui réalise des tests d'intrusion et d'autres méthodes de tests afin d'assurer la sécurité des systèmes d'information d'une organisation.

Par définition, les white hats avertissent les auteurs lors de la découverte de vulnérabilités.

Les chapeaux noirs ou black hat

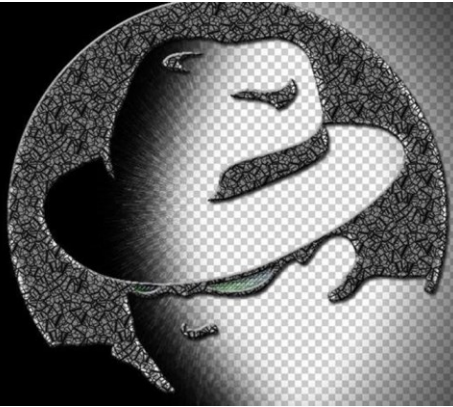


Un black hat est, en argot informatique, un hacker mal intentionné, par opposition aux white hats, qui sont les hackers aux bonnes intentions.



Ces termes auraient pour origine les films de western, où le héros ou le shérif porte un chapeau blanc tandis que le bandit porte un chapeau noir.

Les chapeaux gris ou grey hat



Un grey hat, dans la communauté de la sécurité de l'information, et généralement de l'informatique, est un hacker ou un groupe de hackers qui agit parfois avec éthique, et parfois non.

Ce terme est employé pour désigner ceux qui se situent entre hackers white hat et hackers black hat.

**KNOWS HOW TO
OPEN CMD**



**TELLS EVERYONE
HE IS A HACKER**

Script kiddie

Script kiddie est un terme péjoratif d'origine anglaise désignant les néophytes qui, dépourvus des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes en utilisant des scripts ou des programmes mis au point par d'autres.

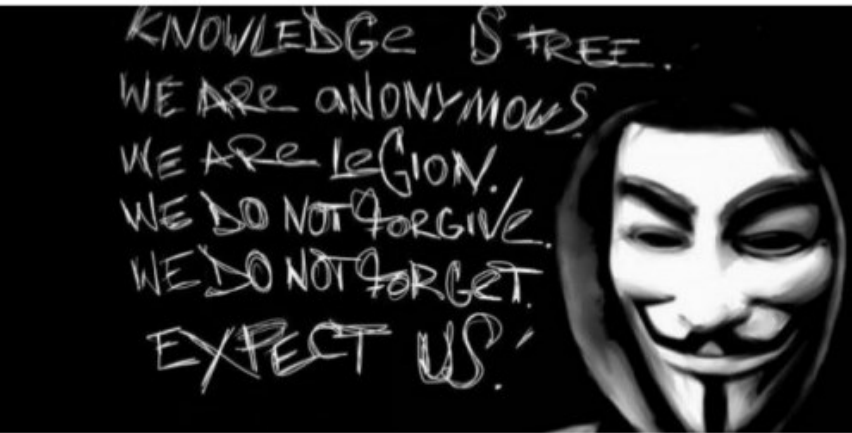
Les chapeaux bleus ou blue hat



Un blue hat est un consultant en sécurité informatique qui est chargé de vérifier l'absence de bogues et de corriger d'éventuels « exploits » avant le lancement d'un système d'exploitation sur le marché.

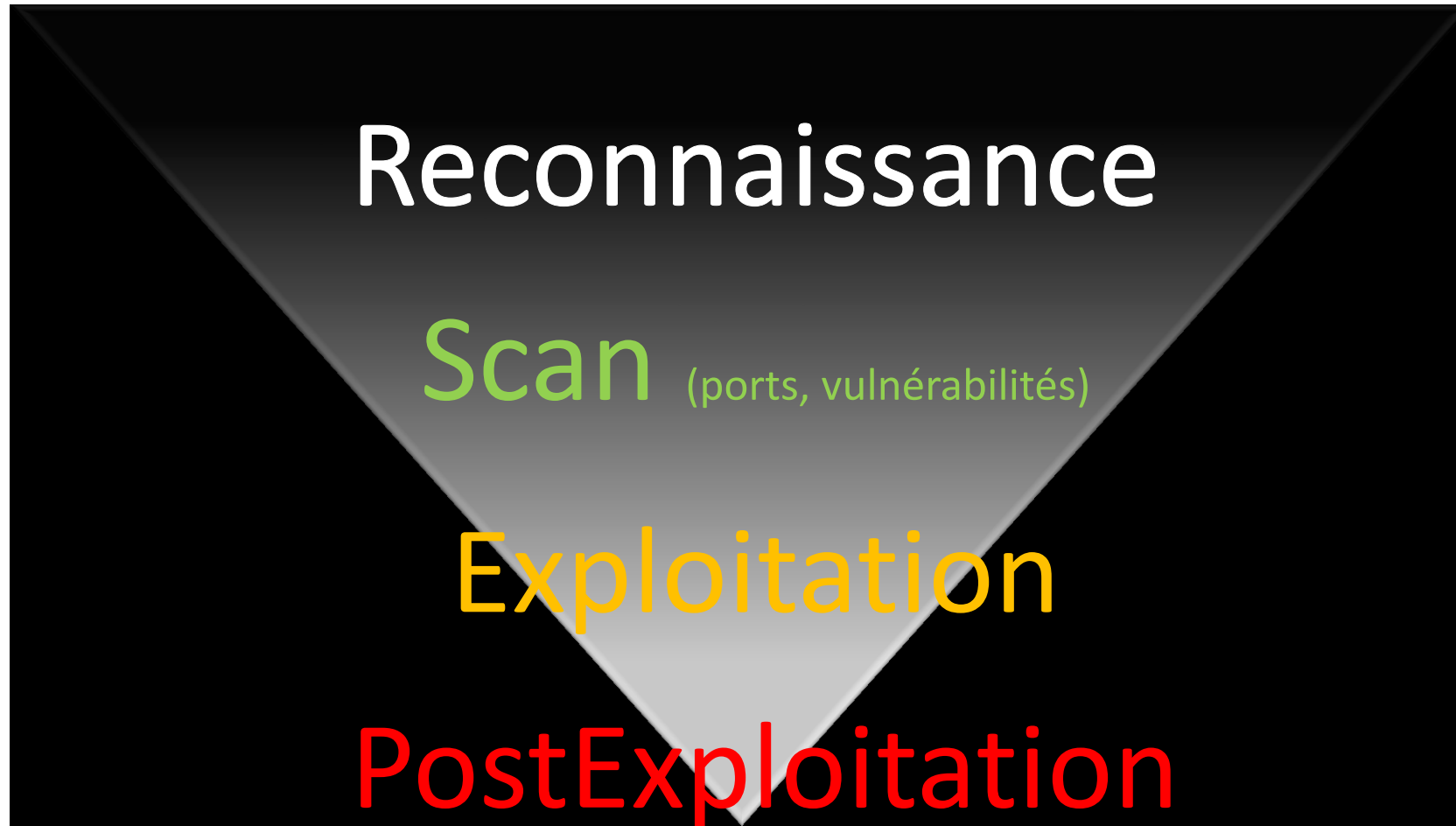
Le terme est notamment employé par Microsoft.

Les hacktivistes (cyberactivistes)



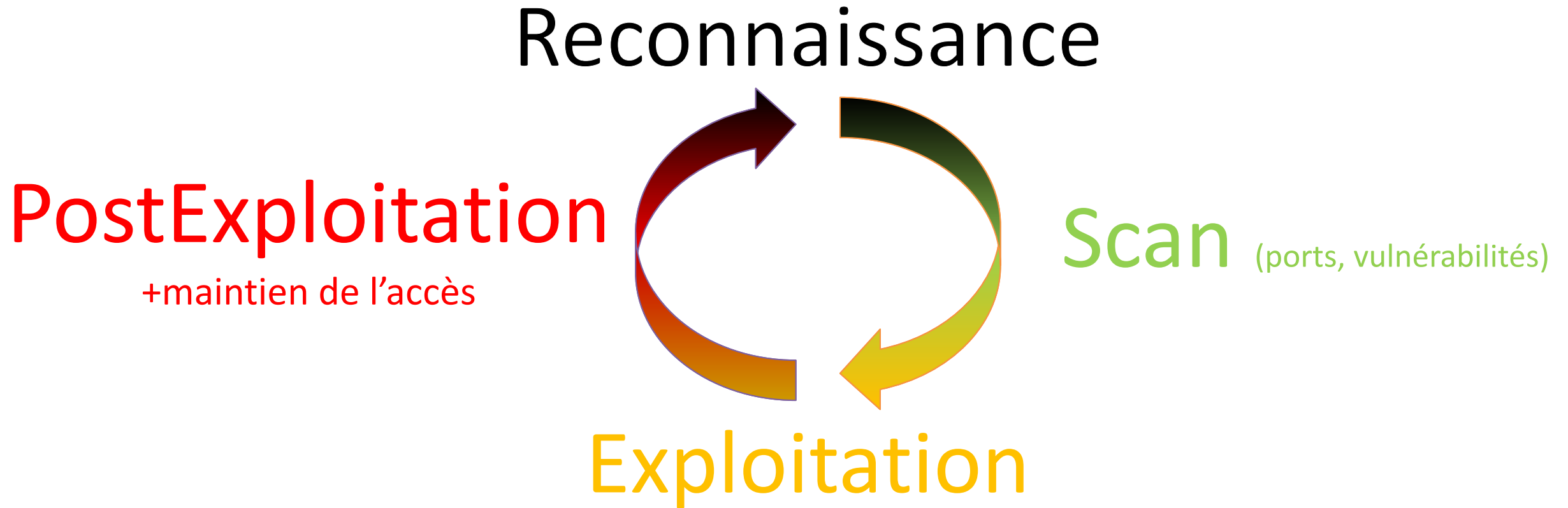
Le cyberactivisme est une forme de militantisme utilisant les compétences du piratage informatique dans le but de favoriser des changements politiques ou sociétaux. L'hacktiviste infiltre des réseaux informatiques à des fins militantes et organise des opérations coup de poing technologiques : piratages, détournements de serveurs, remplacements de pages d'accueil par des tracts (altérations), vols et diffusions de données confidentielles, etc.

Phases d'un test d'intrusion



+maintien de l'accès

Phases d'un test d'intrusion



Reconnaissance

```

**
**      |  |  |  |  _  _  _  ^  ^  _  _  _  _  |  |  _  _  _  _
**      |  _  |  '  \  /  _  \  /  /  /  \  '  |  '  \  \  /  /  _  \  _  |  _  /  _  \  '  |
**      |  _  |  |  |  |  _  /  /  _  /  (  |  |  _  \  \  /  _  \  _  \  |  |  _  /  _  |
**      \  _  |  _  |  _  |  \  _  |  \  /  /  \  ,  |  _  |  _  \  \  _  |  |  _  /  \  _  |
**

```


```
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
```

```
Domain name:      hacking.fsg.ulaval.ca
Domain status:    unavailable
Error code:       01113
Error message:    The segment of the domain name that is on the left
of the .ca extension must be used for a Canadian province or territory. (e
.g. xyx.on.ca or xyz.bc.ca). A segment is the group of characters between
the dots in the domain name. Use one of the following for the segment on t
he left of the .ca extension: ab, bc, mb, nb, nl, ns, nt, nu, on, pe, qc,
sk, yk. Contact CIRA for more information.
```



```
[-] Searching in Linkedin..  
      Searching 100 results..  
Users from Linkedin:  
=====
```

```
% WHOIS look-up made at 2018-02-07 18:30:05 (GMT)
%
% Use of CIRA's WHOIS service is governed by the Terms of Use in its Legal
% Notice, available at http://www.cira.ca/legal-notice/?lang=en
%
% (c) 2018 Canadian Internet Registration Authority, (http://www.cira.ca/)
```


Scan

Nessus 

Scans Settings

 epapavely 

FOLDERS

- My Scans
- CLDQ
- ClubHacking
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

Metasploitable

[Back to ClubHacking](#)

Configure Audit Trail Launch Export

Hosts 1 Vulnerabilities 22 Notes 1 History 1


Filter Search Hosts 1 Host

<input type="checkbox"/>	Host	Vulnerabilities
<input type="checkbox"/>	10.10.20.103	<div><div>2</div><div>1</div><div>41</div></div>

Scan Details

Name: Metasploitable
Status: Aborted
Policy: Web Application Tests
Scanner: Local Scanner
Start: 11/28/17 at 9:45 PM
End: Today at 11:23 AM
Elapsed: 2 months


Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

0

Club de Hacking



Département d'informatique et de génie logiciel

Pavel Yermalovich
clubhacking@fsg.ulaval.ca

Exploitation

Armitage View Hosts Attacks Workspaces Help

ms06_066_nwwks
ms06_070_wkssvc
ms07_029_msdns_zor
ms08_067_netapi
ms09_050_smb2_neg
ms10_061_spoolss
netidentity_xtierrpcpi
psexec
smb_relay
timbuktu_plughntcom

10.0.2.3 10.0.2.9 10.0.2.10 10.0.2.1 10.0.2.7

NT AUTHORITY\SYSTEM @ INFERNO

Console X Scan X exploit X

```
TARGET => 0
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Connecting to the target (10.0.2.9:445)...
[*] Sending the exploit packet (880 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (752128 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.10:40361 -> 10.0.2.9:7391) at 2013-01-21 20:53:28 -0500
meterpreter >
```

PostExploitation

 Command Prompt - nc -lvp 2222

```
C:\>nc -lvp 2222
listening on [any] 2222 ...
192.168.7.133: inverse host lookup failed: h_errno 11004:
connect to [192.168.7.131] from (UNKNOWN) [192.168.7.133]

hello from BT
hello back from Windows Machine
```

 **root@bt: ~**

File Edit View Terminal Help

```
root@bt:~# nc 192.168.7.131 2222
hello from BT
hello back from Windows Machine
```

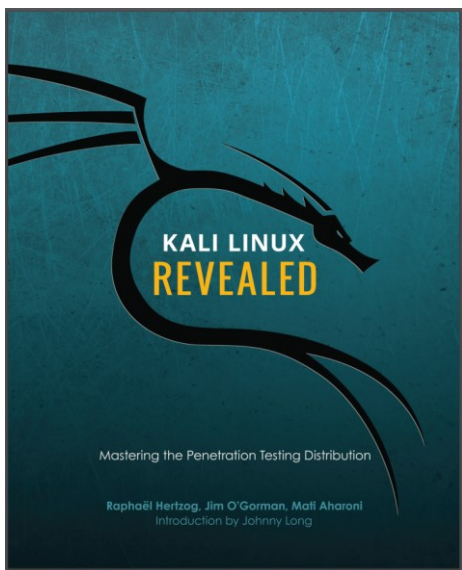
MISE EN GARDE

- La ligne est très mince entre ce qui est permis et ce qui ne l'est pas ;
- Il y a actuellement un flou juridique ;
- Plusieurs cause controversées aux États-Unis ;
(<https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/>)
- Manque de jurisprudence au Canada ;
- Pas utiliser à des fins malveillantes ;
- Chacun est responsable de ses actions.

[Kali Linux](#) is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.

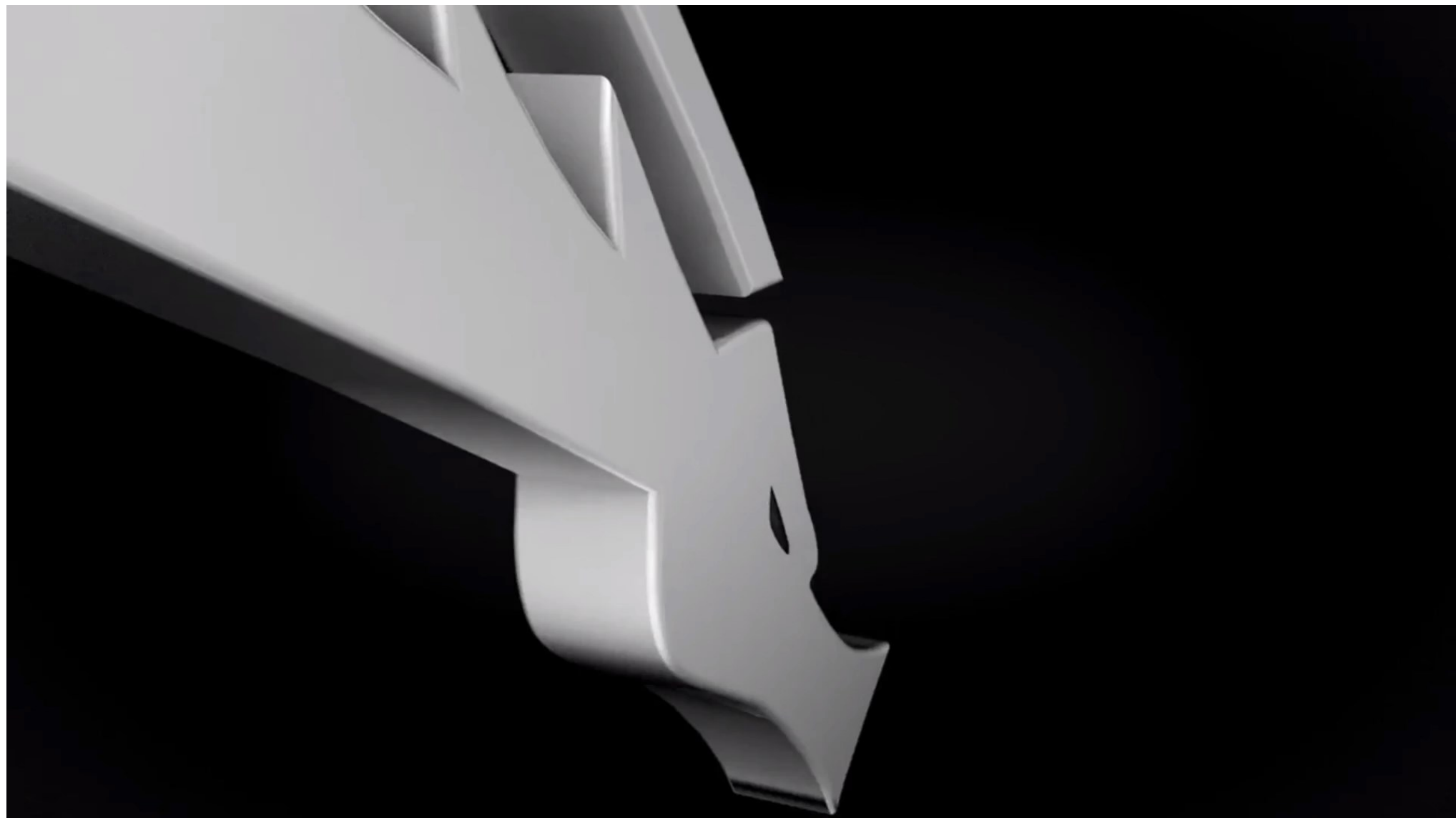
Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

Kali Linux is developed, funded and maintained by [Offensive Security](#), a leading information security training company.

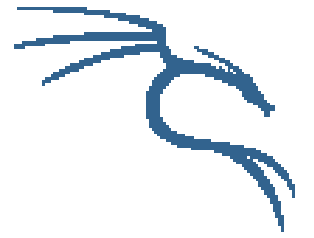


kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

[Kali Linux Revealed](#)
[Mastering the](#)
[Penetration Testing](#)
[Distribution](#)



Installation de Kali linux



[Page de téléchargement de l'ISO](#)

[Instruction pour préparer une clé bootable](#)

[Guide d'installation](#)

Deux possibilités :

- ✓ Machine virtuelle ([Virtualbox](#) et [VMware Workstation Player](#))
- ✓ Dualboot

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

**Une fois l'installation terminée, créez-vous un utilisateur non root.*

Partie II

The Harvester

```
theharvester
```

```
-d <domaine>
```

```
-l <limiter le nombre de resultats>
```

```
-b <repertoire publique Google, Bing,  
LinkedIn, ... , all>
```

```
theharvester -d ulaval.ca -l 10 -b linkedin
```

```
theharvester -d microsoft -l 20 -b all
```

Whois

```
whois <domain>
```

```
whois ulaval.ca
```

```
whois hacking.fsg.ulaval.ca
```


Host

```
host <adresse IP>
```

```
host 8.8.8.8
```

```
host -a 132.203.242.68
```

Nmap

```
nmap -s{T|U|S|UV|X|N|C} -p- -Pn -T{0-5} <IP>
```

TCP

```
nmap -sT -p- -Pn 192.168.0.1-254
```

UDP

```
nmap -sU -p- -Pn 192.168.0.1-254
```

SYN/ACK (default)

```
nmap -sS -p- -Pn 192.168.0.1-254
```

Nessus

Nessus

Scans

Settings

epapavely

FOLDERS

My Scans

CLDQ

ClubHacking

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

Metasploitable

Configure

Audit Trail

Launch

Export

Hosts

Vulnerabilities

Notes

History

Filter

Search Hosts

1 Host

Host

Vulnerabilities

10.10.20.103

2

1

41

Scan Details

Name:

Metasploitable

Status:

Aborted

Policy:

Web Application Tests

Scanner:

Local Scanner

Start:

11/28/17 at 9:45 PM

End:

Today at 11:23 AM

Elapsed:

2 months

Vulnerabilities

Critical

High


Medium

Low

Info

0

Club de Hacking



Département d'informatique et de génie logiciel

Pavel Yermalovich
clubhacking@fsg.ulaval.ca

Metasploit

- | | |
|-------------------------------|---|
| 1. Démarrez | <code>msfconsole</code> |
| 2. Exécutez | <code>search <#CVE></code> |
| 3. Sélectionnez l'exploit | <code>use <nom_exploit_chemain></code> |
| 4. Trouvez les charges disp. | <code>show payloads</code> |
| 5. Sélectionnez une charge | <code>set payload <chemin_de_la_charge></code> |
| 6. Affichez les options disp. | <code>show options</code> |
| 7. Fixez les options | <code>set <nom_option> <valeur_option></code> |
| 8. Lancez exploit | <code>exploit</code> |

Armitage

Armitage View Hosts Attacks Workspaces Help

- ms06_066_nwwks
- ms06_070_wkssvc
- ms07_029_msdns_zor
- ms08_067_netapi
- ms09_050_smb2_neg
- ms10_061_spoolss
- netidentity_xtierrpcpi
- psexec
- smb_relay
- timbuktu_plughntcom

10.0.2.3 10.0.2.9 10.0.2.10 10.0.2.1 10.0.2.7

NT AUTHORITY\SYSTEM @ INFERNO

Console X Scan X exploit X

```
TARGET => 0
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Connecting to the target (10.0.2.9:445)...
[*] Sending the exploit packet (880 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (752128 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.10:40361 -> 10.0.2.9:7391) at 2013-01-21 20:53:28 -0500
meterpreter >
```


John the Ripper

Retrouver un mot de passe
john <l'adresse de fichier avec hash>

Dictionnaires de Kali Linux /usr/share/dict/words
john --wordlist=/usr/share/dict/words <l'adresse de fichier avec hash>

John the Ripper

```
echo fakeusername:6c1e8ebbd0deb2f174665f9f39aa69f3 >  
/home/pass.txt
```

```
9334cf859035e2f0318320ceb88c7e6d  
1a1dc91c907325c69271ddf0c944bc72
```

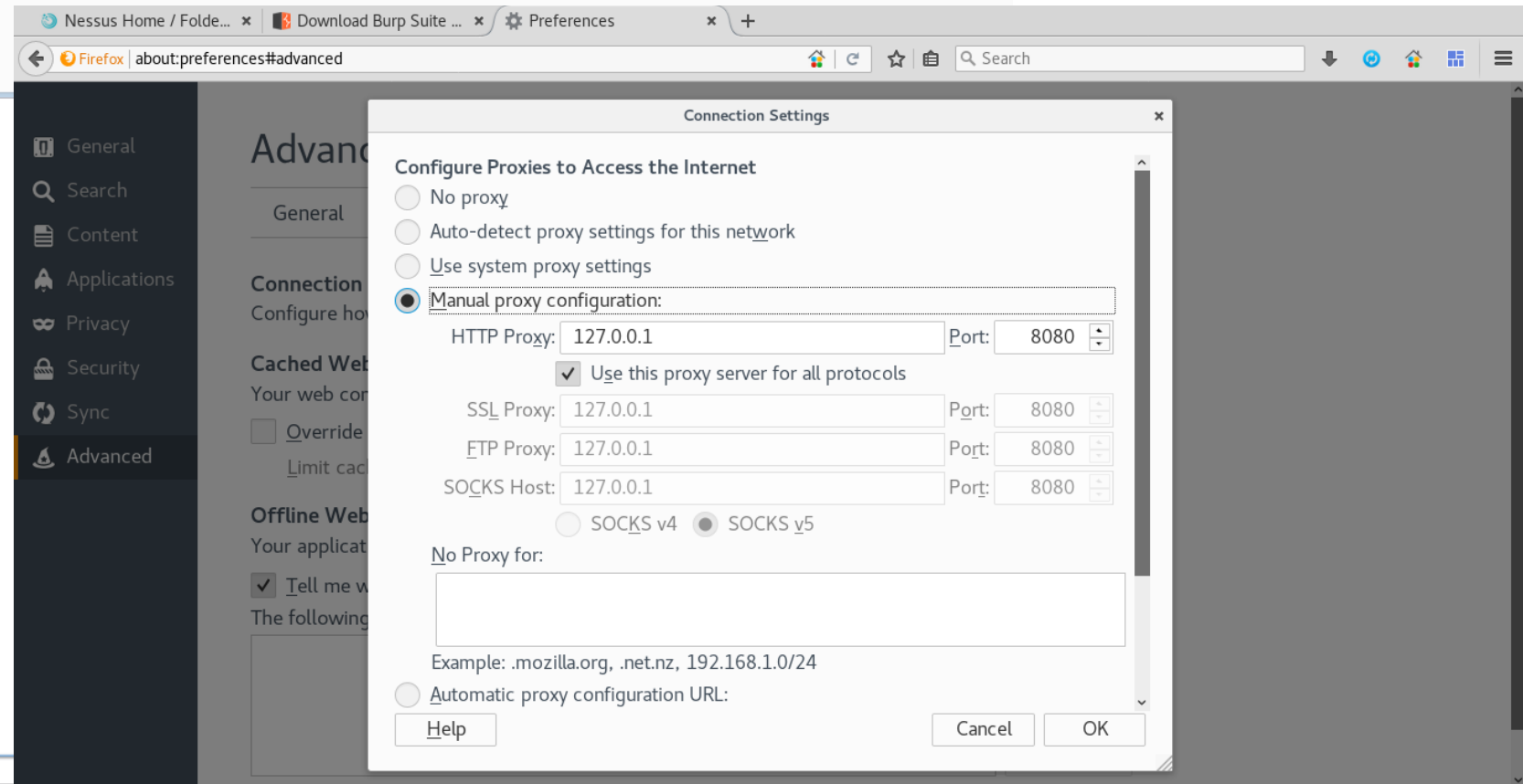
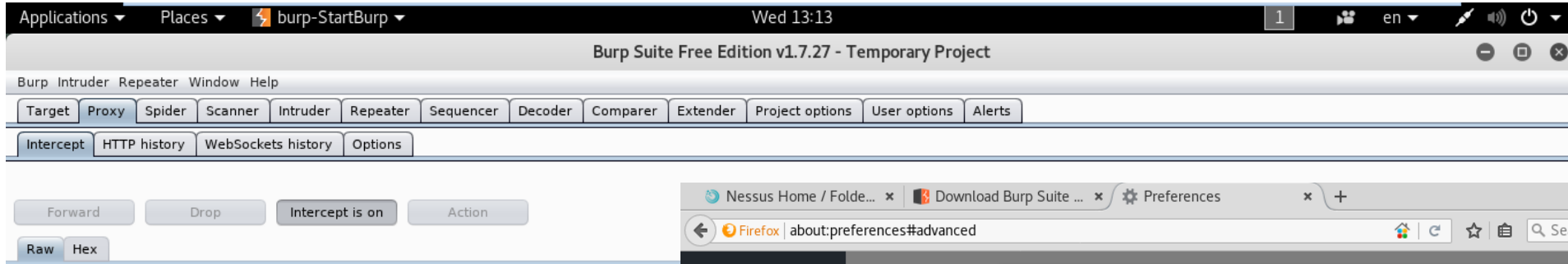
```
john --format=raw-md5 /home/pass.txt --show
```

Nikto

```
nikto -h <target ip / domen> -p <ports 1-1000 or 80,443>  
-o <file name>
```

```
nikto -h 127.0.0.1 -o /home/rapport.txt
```

Burp



Netcat

Command Prompt - nc -lvp 2222

```
C:\>nc -lvp 2222
listening on [any] 2222 ...
192.168.7.133: inverse host lookup failed: h_errno 11004:
connect to [192.168.7.131] from (UNKNOWN) [192.168.7.133]

hello from BT
hello back from Windows Machine
```

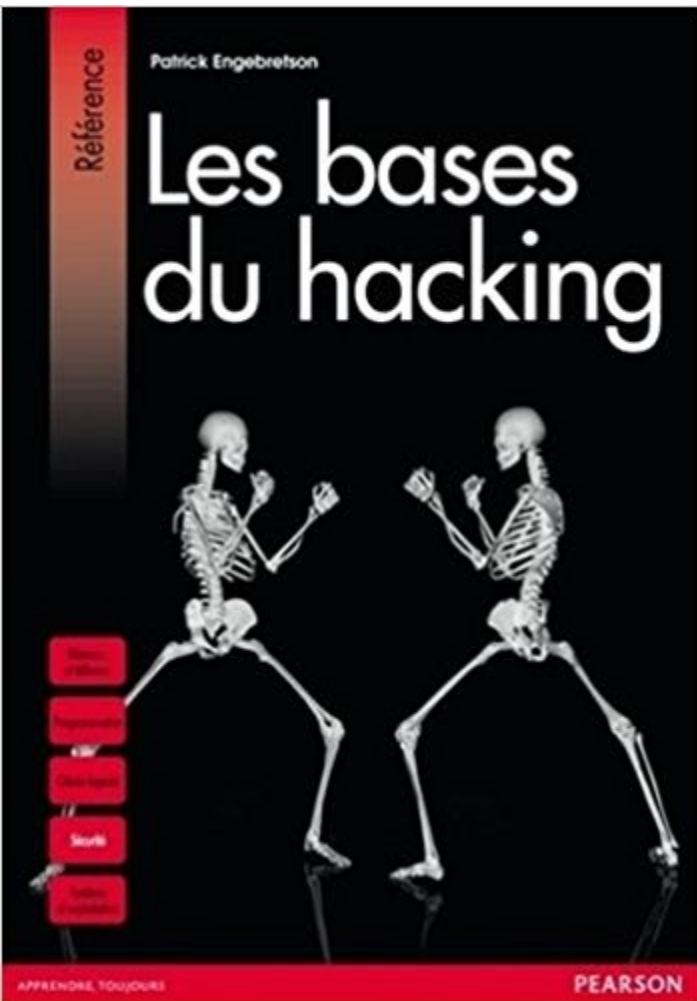
root@bt: ~

File Edit View Terminal Help

```
root@bt:~# nc 192.168.7.131 2222
hello from BT
hello back from Windows Machine
```

Partie III

Livres à lire



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

La pratique est l'essentiel

CTF (Capture The Flag) :

- [Ringzer0](#)
- [Newbiecontest](#)
- [root-me](#)
- [Hack This Site](#)
- [CTFTime.org](#)
- [xss-game](#)

Tutoriels informatique :

- ✓ [Codecademy](#)
- ✓ [Open Class Rooms](#)
- ✓ [Zeste de Savoir](#)



Environnement de pratique

- ✓ LAMP Linux (Linux + apache + mysql + php)
(<http://sourceforge.net/projects/lampsecurity/>)
- ✓ WebGoat
(https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)
- ✓ Buggy Web Application
(<http://www.itsecgames.com/>)
- ✓ Damn Vulnerable Web Application
(<http://www.dvwa.co.uk/>)
- ✓ Mutillidae II
(<https://sourceforge.net/projects/mutillidae/>)

Bâtir son coffre à outils

Avoir des outils à portée de main

Système d'exploitation

- Kali
- Security Onion
- Etc.

Navigateurs Internet, extensions et automatisation

- Firefox
- Chrome
- Internet Explorer
- Wappalyzer
- Selenium
- PhantomJS
- PythonWebKit
- Etc.

Proxy

- ZAP
- BURP
- Fiddler
- Etc.

Outils de scan générique

- Acunetix
- IBM App scan
- Nessus
- Arachni
- W3af
- Skipfish
- Etc.

Bâtir son coffre à outils

Avoir des outils à portée de main (suite)

Outils spécialisés

- SQLMap
- John the Ripper
- Plusieurs projets sur GitHub
- Etc.

Environnements de développement

- Java
- .Net
- NodeJS
- Perl
- Python
- PHP
- Etc.

Analyse de code

- Visual Code Grepper
- FXCop (ASP .NET)
- FindBugs (Java)
- HpFortify
- IBM AppScan Source Edition
- Checkmarx
- Esprima (JavaScript)
- Etc.

Outils de défense

- Snort (IDS)
- ModSecurity (WAF)
- Etc.

Bâtir son coffre à outils

Avoir un réseau d'apprentissage

Certification

- SANS
- Offensive Security
- CERT
- Etc.

Agences réglementaires et gouvernementales

- NIST
- IETF (RFC)
- ANSSI
- DITC
- ASD
- Etc.

Formation en ligne

- WWWSchool
- MSDN
- Mozilla Developer Network
- HTML5 Security Cheatsheet
- Etc.

Méthodologies et cadres de tests d'intrusions

- Pentest-standard.org
- OSSTMM v3
- NIST SP 800-115
- Etc.

Bâtir son coffre à outils

Se tenir informé

Listes de vulnérabilités

- CERT
- Security Focus
- Secunia
- CVEDetails
- Etc.

Compagnies

- Microsoft
- Symantec
- McAfee
- IBM
- Trustwave
- Sucuri
- Checkmarx
- WhiteHat Security
- Etc.

Blogues et sites informationnel

- Schneier on security,
- Krebs on security
- The Hacker News
- Google Project Zero
- Seclist.Org
- Etc.

Local PLT-3778



Loto HF

Loto HF

This is an introductory web challenge from Hackfest 2015.

Copy to clipboard : 10.10.20.101

Blog BitDucks

Blog BitDucks

Blog BitDucks is a vulnerable blog. Try to exploit some known web flaws!

Copy to clipboard : 10.10.20.102

Metasploitable 2

Metasploitable 2

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities

Copy to clipboard : 10.10.20.103

Scanning

Scanning

The Scanning challenge is a host used to practice Nmap scans.

Copy to clipboard : 10.10.20.104

Vulnerable Mail Server

Vulnerable Mail Server

The MailServer challenge is a host for practicing SMTP based attacks. You can use any payloads from tools such as SET.

Copy to clipboard : 10.10.20.105

Windows XP SP2

Windows XP SP2

A vulnerable Windows machine. Find vulnerabilities using Nessus and exploit them with Metasploit!

Copy to clipboard : 10.10.20.106

Telnet Encrypt

Telnet Encrypt

FreeBSD 8.1 vulnerable machine. Find vulnerabilities using Nessus and exploit them with Metasploit!

Copy to clipboard : 10.10.20.112

Solaris 10

Solaris 10

Time to exploit an actual Unix OS. Find vulnerabilities using Nessus and exploit them with Metasploit!

Copy to clipboard : 10.10.20.121

DirtyCow

DirtyCow

Do you know how to use DirtyCow? Hack your way in.

Copy to clipboard : 10.10.20.118

RPISEC

RPISEC

A binary exploitation training ground. More details here :

<https://github.com/RPISEC/MBE>

Copy to clipboard : 10.10.20.119

Androidx86

Androidx86

Do you know how to exploit an Android device? Hack your way in.

Copy to clipboard : 10.10.20.122



Les étapes d'un incident de sécurité dans une perspective juridique
February 22, 2018
From 18:30 to 20:00

Jeudi le 22 Février vous êtes invités à une conférence sur les incidents de sécurité dans une perspective juridique avec Jean-François De Rico spécialiste en droit des technologies de l'information.

Pizzas fournies!

[Eventbrite - QuebecSec 2018](#)

[Slack - Discussion en ligne](#)

Open Web Application Security Project



Les sujets principalement abordés sont :

- Analyse et conception d'applications sécurisées
- Techniques et méthodes de développement sécurisé
- Évaluation et validation de la sécurité des applications (tests d'intrusion, recherche de vulnérabilités)
- Sécurité d'architectures et technologies de développement logiciel

29 novembre 2017 - Journée de 6 conférences sur la sécurité applicative à L'Université Laval

LA SÉCURITÉ APPLICATIVE
Pour mieux bâtir

29 novembre 2017
En partenariat avec ISACA section de Québec



La confiance régit. Ensemble, nous y veillons.

Afin de mettre en avant plan la sécurité applicative à Québec, vos leaders bénévoles d'OWASP Québec se sont joint à d'autres conférenciers spécialistes pour cet événement. "ISACA Québec" en partenariat avec le "Bureau de sécurité de l'information de l'Université Laval" ont organisé cette fantastique journée sur la **sécurité applicative**.

Merci aux organisateurs! Nous étions "sold out" avec 165 inscriptions!



Patrick Leclerc



[Slack - Discussion en ligne](#)



Le CFI (Compétitions et Formations Informatiques) est la première délégation représentant les étudiants du domaine informatique de l'Université Laval dans les nombreuses compétitions informatiques de l'Amérique du Nord.

Cette délégation a pour but de former ses membres dans divers sujets dont la sécurité informatique et le développement de jeux vidéo, en encourageant l'apprentissage par l'expérience pratique.

Pour ce faire, le CFI organise de nombreux ateliers d'une à trois heures et encourage la participation à plusieurs événements comme le NorthSec, Hackfest et les CS Games.

<https://www.facebook.com/groups/281680249003676>

[Slack - Discussion en ligne](#)

Compétition de hacking au Québec



Certifications

- ✓ Offensive Security Web Expert
<https://www.offensive-security.com/information-securitycertifications/oswe-offensive-security-web-expert/>
- ✓ Sans GIAC Web Application Penetration Tester (GWAPT)
<https://www.giac.org/certification/webapplication-penetration-tester-gwapt>
- ✓ Cert Secure Coding Professional Certificates
<https://www.cert.org/go/secure-coding/>

Offensive Security Certified Professional



The **Offensive Security Certified Professional (OSCP)** is the companion certification for our [Penetration Testing with Kali Linux training course](#) and is the world's first completely hands-on offensive information security certification. The OSCP challenges the students to prove they have a clear and practical **understanding of the penetration testing process and life-cycle** through an arduous twenty-four **(24) hour certification exam**.

Piratage éthique



La chasse aux primes « Bug bounty »

La plupart des grandes organisations ont des programmes de récompenses :

- Google
- eBay
- Facebook
- Twitter
- etc.

Participer à des « Bug bounty » est généralement utile pour décrocher un emploi en piratage éthique.

Liste de « Bug bounty »

<https://bugcrowd.com/list-of-bug-bounty-programs>

https://hackerone.com/directory?query=ibb:yes&sort=published_at:descending&page=1

Nos projets

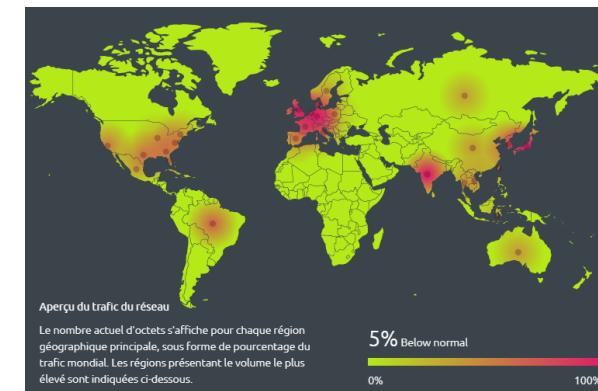
- Analyse / Visualisation de logs - attaque web

ELK (elasticsearch, logstash, kibana)



<https://www.elastic.co/assets/b165ed181426afe843/kibana-3-overview.png>

- Visualisation des attaques en temps réel



<https://www.akamai.com/fr/fr/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp>

Partie I

- ✓ Définition de Hacking
- ✓ Phases d'un test d'intrusion
 - ✓ Reconnaissance
 - ✓ Scan
 - ✓ Exploitation
 - ✓ PostExploitation
- ✓ Kali linux

Partie II

- ✓ Démonstration Kali Linux
 - ✓ The Harvester
 - ✓ Whois
 - ✓ Host
 - ✓ Nmap
 - ✓ Nessus
 - ✓ Metasploit
 - ✓ John the Ripper
 - ✓ Armitage
 - ✓ Nikto
 - ✓ Burp
 - ✓ Netcat

Partie III

- ✓ Livres à lire
- ✓ La pratique est l'essentiel
 - ✓ CTF
 - ✓ Club de Hacking de l'UL
- ✓ Communautés
 - ✓ QuébecSec (HackFest)
 - ✓ OWASP
 - ✓ CFI-UL
- ✓ Compétitions
- ✓ Certification
- ✓ Bug Bounty
- ✓ Idée de projet pour le Club de Hacking

<http://www.techtechnik.com/wp-content/uploads/2014/11/hacking.jpg>
https://shkolazhizni.ru/img/content/i119/119310_or.jpg
https://s00.yaplakal.com/pics/pics_original/1/6/9/2437961.jpg
<http://middleeasternet.com/middleeasternet/wp-content/uploads/2017/10/ctf-1000x550.jpg>
<http://static.funinformatique.com/2015/06/comment-pirater-un-compte-facebook-1.jpg>
<https://upload.wikimedia.org/wikipedia/commons/thumb/7/7a/HACKERS.jpg/220px-HACKERS.jpg>
<https://vanw0rjht5-flywheel.netdna-ssl.com/wp-content/uploads/2014/02/black-hat-white-hat-seo.jpg>
<https://cdn.searchenginejournal.com/wp-content/uploads/2017/10/black-hat-seo.png>
<https://img.wonderhowto.com/img/15/86/63579996191966/0/study-for-white-hat-hacker-associate-certification-cwa.w1456.jpg>
<https://img.wonderhowto.com/img/54/84/63568919074278/0/what-truly-means-be-gray-hat.1280x600.jpg>
<http://toussurlesh4ck3r.esy.es/img/bluehat.png>
<https://image.slidesharecdn.com/cyberactivismeterrorismeanonymousfr-160127093709/95/cyberactivisme-ou-hacktivisme-1-638.jpg?cb=1453890080>
https://www.youtube.com/watch?v=qLealoHdH_0
<https://quebecsec.ca/>
https://www.owasp.org/index.php/Quebec_City
<https://www.officialhacker.com/wp-content/uploads/2016/08/BugBountyProgram.png>
<https://www.offensive-security.com/wp-content/uploads/2012/01/oscp-certs.png>
<https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/>
<https://www.tenable.com/products/nessus/nessus-professional>
<https://cyberoperations.files.wordpress.com/2013/01/screenshot-armitage1.png>
<http://blog.hakzone.info/posts-and-articles/windows/just-another-netcat-tutorial/>