



## WARMUP CHALLENGES

### 1 - Read The Rules

solution :

Read the source code of the rule page and u will get your flag.

### 2 – Believe Your Eyes

solution :

do a strings on the rar file.

```
masscan@masscan-Inspiron-3521:~/ctf/virsecon-warmup$ strings believe_your_eyes.rar | grep LLS
LLS{if_ten_million_fireflies}
masscan@masscan-Inspiron-3521:~/ctf/virsecon-warmup$
```

### 3 – Yarn

solution :

again do a strings on the downloaded file.

```
masscan@masscan-Inspiron-3521:~/ctf/virsecon-warmup$ strings yarn | grep LLS
yLLS{it_was_just_a_ball_of_strings}j
masscan@masscan-Inspiron-3521:~/ctf/virsecon-warmup$
```

#### 4 – Puppo

solution :

download the png file. And read metadata using exiftool.

```
Chromaticity Colorant      : Unknown (0)
Chromaticity Channel 1    : 0.64 0.33
Chromaticity Channel 2    : 0.3 0.60001
Chromaticity Channel 3    : 0.14999 0.06
Comment                   : b'TExTe2RvZ2dvX3NheXNfc3VjaF9iYXNlNjRfdmVyeV93b3d9'
Image Width               : 537
Image Height              : 529
Encoding Process          : Baseline DCT, Huffman coding

masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ echo TExTe2RvZ2dvX3NheXNfc3VjaF9iYXNlNjRfdmVyeV93b3d9 | base64 -d
LLS{doggo_says_such_base64_very_wow}masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$
```

#### 5 – DotCom Scavenger Hunt

solution :

Download the zip file and unzip it. And grep for flag.

```
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ cd nothinginthebox.com/
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup/nothinginthebox.com$ ls
css  img  index.html  js  PAY.html  robots.txt
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup/nothinginthebox.com$ grep -lri LLS
PAY.html
js/jquery-1.3.1.min.js
img/layout/light-burst.jpg
img/layout/dark-burst.jpg
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup/nothinginthebox.com$ grep -lri LLS{
js/jquery-1.3.1.min.js
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup/nothinginthebox.com$ cat js/jquery-1.3.1.min.js | grep -i LLS
```

```
[last|even|odd)(?:\((\d*)\))?(?=[^-]|$)/,PSEUDO:/:((?:[\w\u00c
ssName", "for": "htmlFor"}, attrHandle: {href: function(S) {return S
V=W[U]; if(V) {var X=V.previousSibling; while(X&&X.nodeType!==1) {
ilter(T,W,true)}}, ">": function(X,T,Y) {if(typeof T==="string"&&
r V=W.parentNode; /*LLS{just find it with grep}*/X[U]=V.nodeName
tring"?W.parentNode:W.parentNode===T}} if(typeof T==="string") {
=T=X?T:T.toUpperCase(); S=0} S("parentNode",T,U,V,W,X)}, "~": func
.toUpperCase(); S=0} S("previousSibling",T,U,V,W,X)}, find: {ID: f
: return S2[S1].[]}} NAME: function(S,T,U) {if(typeof T.getElemen
```

#### 6 – Ssh, quiet!

Solution :

after connectiong ssh quitting suddenly.

used below command

```
ssh user@jh2i.com -p 50035 {cat,flag.txt}
```

## 7 – Pack'd

solution :

download the file and do a strings on it and u can see that the binary is packed with upx packer.  
Decompress that will give flag

```
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ strings packd | grep LLS
arycLLS{V
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ strings packd | grep upx
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ upx -d packd
          Ultimate Packer for eXecutables
          Copyright (C) 1996 - 2017
UPX 3.94      Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

      File size      Ratio      Format      Name
      -----
      657616 <-    323172    49.14%    linux/i386    packd

Unpacked 1 file.
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ stri
strings strip
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$ strings packd | grep LLS
LLS{packing_an_executable_can_hide_some_data}
masscan@masscan-Inspiron-3521:~/ctf/virseccon-warmup$
```

## 8 – Capture The Flag

solution :

that was a smal video given.

Use Video to JPG converter and analyse frames u will get flags.

<https://ezgif.com/video-to-jpg>