Engineering Week Cyber Challenge

Back in 2012, there was an internet phenomenon known as Cicada 3301. It was a worldwide puzzle/mystery that remains unsolved to this day. Cicada 3301 has been described as “the most baffling and enigmatic mystery on the Internet”. On three occasions, Cicada 3301 has posted spectacular puzzles on the internet and dark web, with the stated intent of "recruiting intelligent individuals".

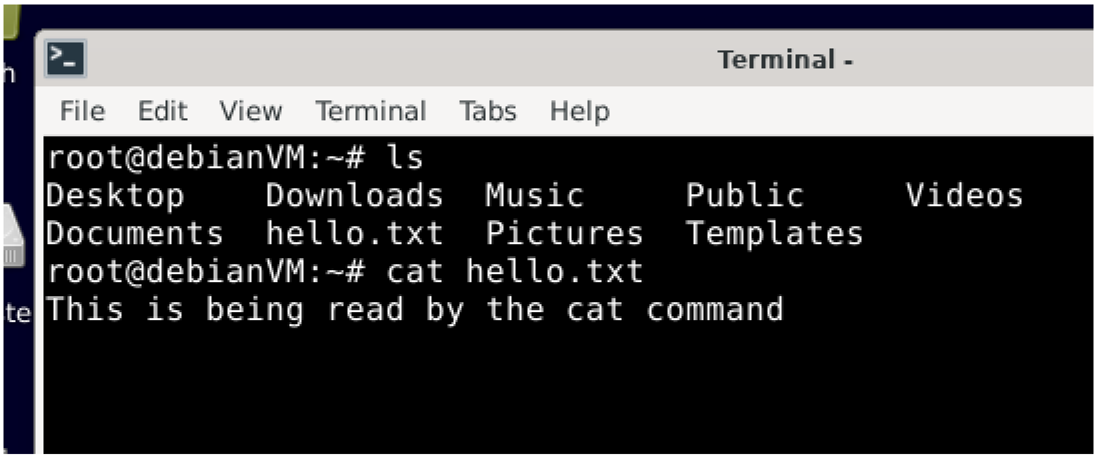
There has been much speculation and theories about Cicada 3301, including that they are recruitment tools for the NSA, MI6, Illuminati, a cult, or a hacker group. Many first thought Cicada 3301 was an Alternate Reality Game, but still very few known where this rabbit hole leads to. Those who do have disappeared from the internet.

The Invitation

This image was discovered Jan 5th, 2012 on a 4chan /x/ paranormal message board post. This is generally referred to as the invitation to the “game” or whatever Cicada 3301 should be considered. Attached to the lab is an archive of the original images you will need.

Embedded in this message, specifically in the image itself, is a hidden code. Some codes require cracking, this one just requires mild curiosity; let's see what's inside.

The Cat Command

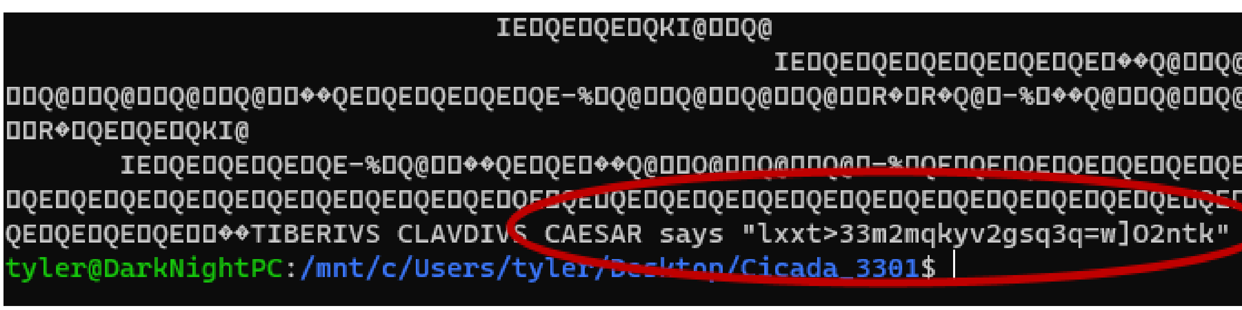


The cat command is just a command to display/output the contents of a file. In the above example, we list the files with the `ls` command, then run `cat hello.txt`. The file "hello.txt" contains the text: "This is being read by the cat command"

So if a text file can output that, what happens when we put other types of files through the cat command?

Let's try and do that with the original puzzle picture:

> cat cicada-3301-invitation.jpg

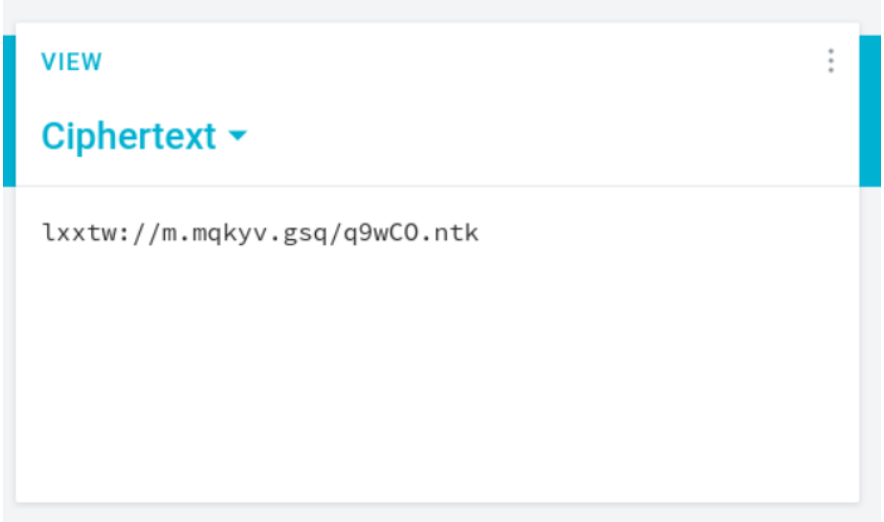


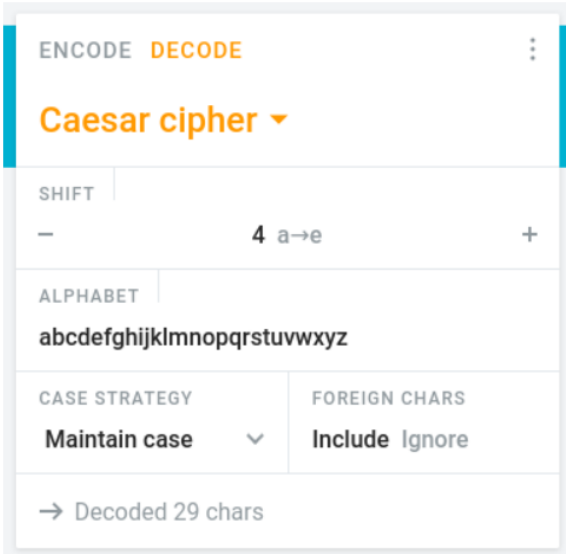
Clearly, JPEG image files are not meant to be read by human eyes but wait… there is something recognizable at the end there.

CAESAR says “lxxtw://m.mqkyv.gsq/q9wCO.ntk”

The word Caesar is a strong indicator that this is most likely a Caesar cipher: https://en.wikipedia.org/wiki/Caesar_cipher. run this through a Caesar cipher decoder:

https://cryptii.com/pipes/caesar-cipher





After some detective work, since this looks like an Imgur URL, it should look similar to this: https://i.imgur.com/XXXX.jpg, which brings us to our next picture

The Decoy

The decoy message we get presented with is more important than you first realize. It mentions two very important words in the cryptography world: **out** and **guess.**

A popular tool from the late 90s for hiding secret messages in images is known as **OutGuess**. We will install it to your machine to find the hidden message in the picture.

Open a terminal and type:

> sudo apt update
> sudo apt install outguess

```
All packages are up to date.
root@debianVM:~# sudo apt install outguess
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  outguess
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 88.1 kB of archives.
After this operation, 267 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 outguess amd64 1:0.2.2-5
[88.1 kB]
Fetched 88.1 kB in 0s (2,251 kB/s)
Selecting previously unselected package outguess.
(Reading database ... 96393 files and directories currently installed.)
Preparing to unpack .../outguess_1%3a0.2.2-5_amd64.deb ...
Unpacking outguess (1:0.2.2-5) ...
Setting up outguess (1:0.2.2-5) ...
Processing triggers for man-db (2.9.4-2) ...
root@debianVM:~#
```

You can make sure everything worked correctly because now you should be able to use the `outguess` command.

```
root@debianVM:~# outguess
OutGuess 0.2.1 Universal Stego (C) 1999-2018 Niels Provos and others

outguess [options] [<input file> [<output file>]]
        -[sS] <n>    iteration start, capital letter for 2nd dataset
        -[iI] <n>    iteration limit
        -[kK] <key>  key
        -[dD] <name> filename of dataset
        -[eE]        use error correcting encoding
        -p <param>   parameter passed to destination data handler
        -r           retrieve message from data
        -x <n>       number of key derivations to be tried
        -m           mark pixels that have been modified
        -t           collect statistic information
        -F[+-]       turns statistical steganalysis foiling on/off.
                     The default is on.
root@debianVM:~#
```

In order to read the hidden message in our picture, you will need to pass the picture into OutGuess as an option/parameter. For example:

> outguess -r cicada-3301-invitation.jpg output.txt

outguess: The outguess command itself
-r: Retrieve message from data
cicada-3301-invitation.jpg: Original image to get code out of
output.txt: Output of the hidden message

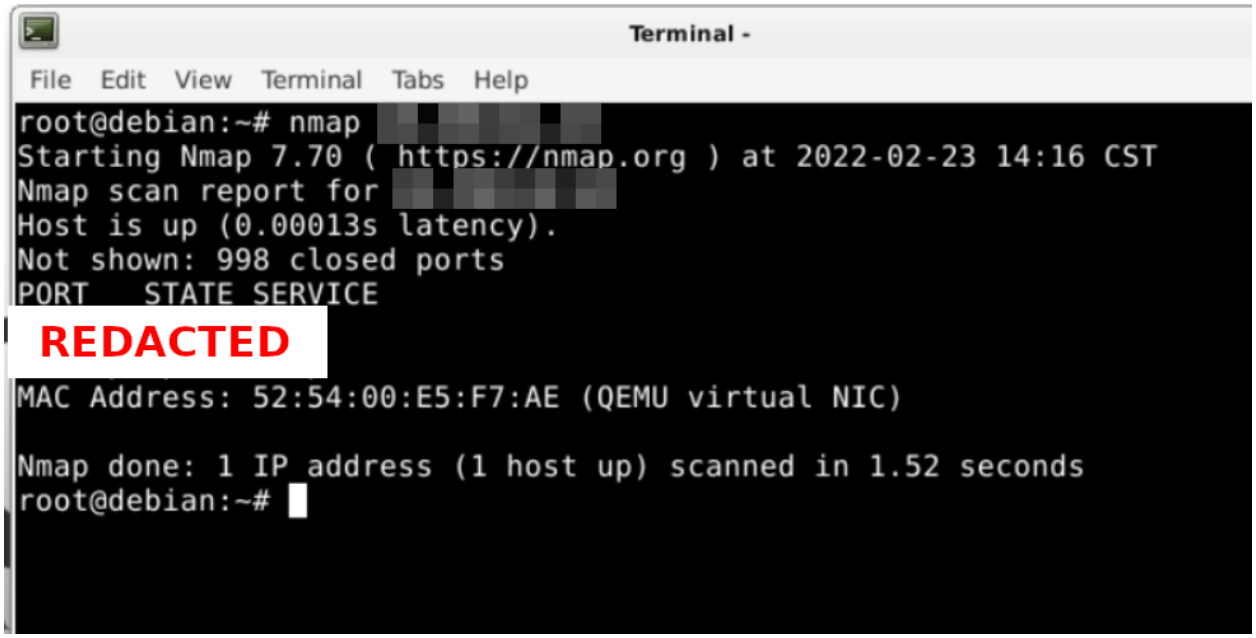
To see the results, just cat output.txt. The results should contain a top secret IP address that will help solve the next portion of this challenge

Reconnaissance Mission

Now that you have retrieved the top secret IP address, it's time to see what information can be obtained with it. To do this, you will utilize a tool called "nmap".

Syntax to use the nmap:

```
nmap SECRET_IP_ADDRESS
```



The output of the nmap scan should provide the information needed to access the leaderboard portal. If you don't recognize the ports/services, feel free to search them on the Internet for more information.

The Final Test

Now that you've accessed the portal, you should be presented with a password field and an image similar to the one below:

Using the knowledge and skills you have gained throughout this exercise, use this image to find the password and add your name to the leaderboard. Good luck and have fun!