Category 1: General Skills

- **Question: Chrono**

Flag is found in /etc/crontab, a file which keeps track of tasks that are run periodically on a linux server.

- **Question: money-ware**

Google the bitcoin address to find the name of the malware that has been installed.

- **Question: Permissions**

cd to the root folder, use ls to find the challenges folder, then cd and cat the file to obtain the flag.

- **Question: repetitions**

Use the base64 command in the webshell repeatedly to decode the flag.

- **Question: useless**

After connecting to the ssh server, use the command man useless to obtain the flag

- **Question: Special**

After connecting to the ssh server, used the command Clear & find to get name of the flag file and then use cat to obtain the flag

- **Question: Specialer**

After connecting to the ssh server, use echo */* to see all the files and applied echo "$(<example.txt)" command to each file to reveal the flag from one of the files.

Category 2: Web exploitation

- **Question: findme**

This challenge has the flag base64 encoded in the URLs of a couple of web requests that are redirected. The base64 URLs are decoded to get the flag

- **Question: RegEx**

I typed picoCTF! In the input bar and got the flag

Category 3: Reverse Engineering

- **Question: Ready Gladiator 0**

Ran the command `nc saturn.picoctf.net 59190` initially to run the game and then i chose red as my warrior and got the flag

- **Question: Reverse**

Used wget command to download the ret file. Then I used binwalk to extract it and used strings ret | grep picoCTF to get the flag

- Question: SafeOpener2

Used cat command to see the contents of the file and found the file amidst of the java code
Alternative solution: Use java decompiler

Category 3: Forensics

- **Question: hideme**

First we use wget on the flg.png link to download the flag. Then we run the command strings flag.png and observe that there is a a PNG file embedded in a ZIP file inside another PNG file. Using binwalk, we extract this file. sz allows us to get a file out of the webshell onto our local machine to view the image.

- **Question: PcapPoisoning**

Used wget command with the file link to download the file. Then used the strings trace.pcap | grep picoCTF command to get the flag

Category 4: Binary Exploitation

- **Question: Babygame 01**

Use Ghidra to reverse engineer a binary file. The game allows you to move off the top-left corner of the screen, which writes outside of the map array and changes the win variable from 0 to the ASCII value of the user's character. Using the hidden 'p' command we can then immediately solve the game.

Category 5: Cryptography

- **Question: HideToSee**

I used wget on the link to download the atbash.jpg, tried to run the strings command on it. After that i use steghide extract -sf atbash.jpg on the file and the prompt asked for a passphrase. There was no passphrase, i just pressed enter and it saved it to an ‘encrypted.txt”. So I used the command cat encrypted.txt to get a cipher text. Deciphered it with atbash deciphering tool to get the flag.

- Question: ReadMyCert

Opened the CSR file using notepad editor and deciphered it using base64 decoder, thus finding the flag.

- **Question: Rotation**

Used caesar cipher to decipher the flag