Spring 2025 Cyber Security Fundamentals

CRN 20332

Aysel Panahova

What I Learned in Chapter 1 and Chapter 2

In Chapter, I learned that our world really depends on computers because the world is evolving. As technology is growing, computers are becoming an integral part of our daily life, and we rely on them for everything from banking to communication. Therefore, people can misuse it and increase hacking situations. In order to counter these issues and improve the overall security, it is important for the world to have professional IT specialists who can manage the system effectively.

In the Chapter 2, I gained an understanding of the shell which is a powerful tool used by IT professionals to interact with computers. Unlike the GUI (Graphical User Interface) which relies on icons and buttons to navigate, the shell uses text commands to perform needed tasks. Therefore, we can say that the shell is faster and more efficient for controlling a computer, however it requires knowledge of the commands to create, access, and modify the files.

More than theoretical side, I learned about the commands that I have not used before. For example, “cat”, “touch”, “nano” commands.

1. CAT is basically a short version of concatenation, and it is commonly used to display contents of a file. For example, “cat aysel.txt” will print the file’s content to the terminal.
2. TOUCH command is used to create an empty file. For instance, if I write “touch cybersecurity.txt” this command will create an empty file named cybersecurity.txt.

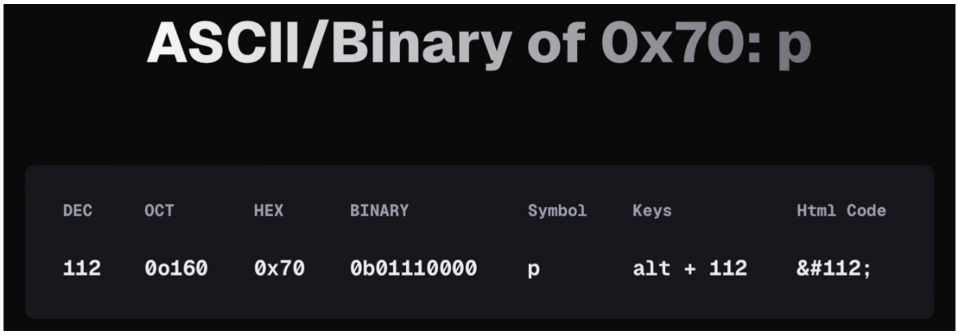
3. NANO command is a simple text editor that is used in the terminal. It is used to create, edit, save files from CLI.

QUIZ 1

Task 1 – Let’s Warm Up

This task is a simple task where we just need to convert a hexadecimal to ASCII which is a system that assigns numbers to letters, numbers, and symbols to help computers understand and store text. To convert 0x70 which is mentioned in description we can use Webshell in picoCTF.

However, there is another way to convert it, which is just searching on Google some websites to convert hexadecimals to ASCII letter. When I searched convert 0x70 to ASCII the first website showed all the details.



ASCII/Binary of 0x70: p

DEC	OCT	HEX	BINARY	Symbol	Keys	Html Code
112	0o160	0x70	0b01110000	p	alt + 112	&#112;

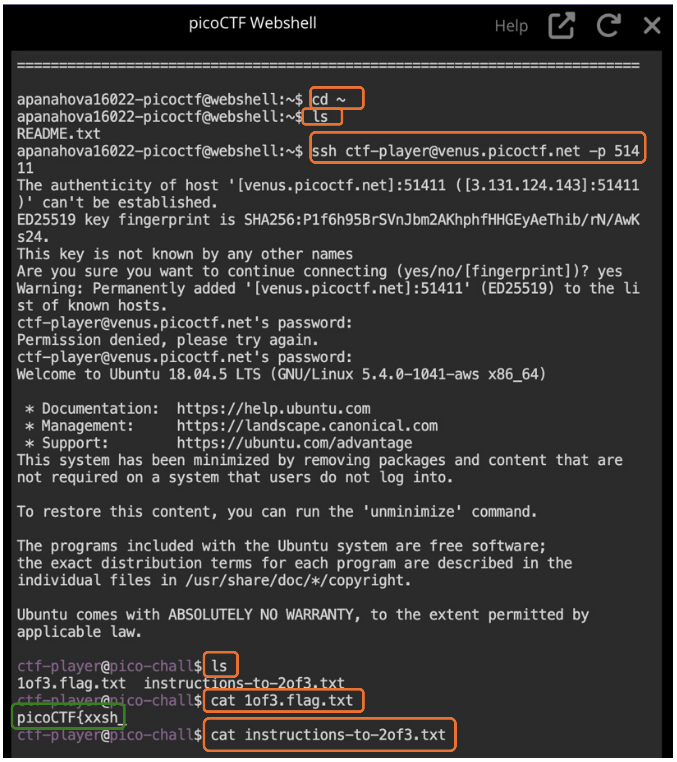
In quiz’s description we must find a letter because the question says “If I told you a **word**”. As we see, the answer is “p”

Task 2 – Magikarp Ground Mission

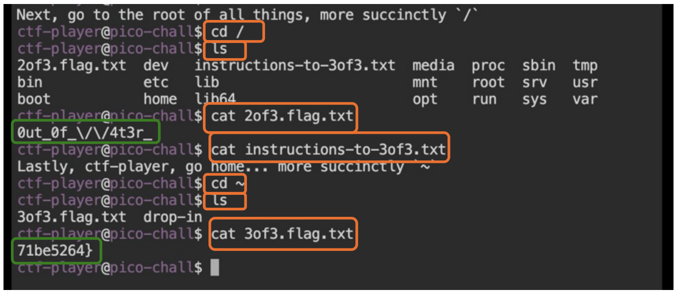
Here, we open webshell again to input several commands. First command will be "cd ~". It is used for changing the working directory (the folder that you are currently in) to user's home directory (your personal starting folder where your files are usually kept). It is used because we need to go back to starting point. ~ symbol is a shorthand for the home directory. The next command is "ls" which basically mean list. It lists the files and directories in the current working directory.

Then we press "Launch Instance" which is located on the right part of the description to see SSH. We must copy and paste this to webshell because it lets you connect to another computer called "venus.picoctf.net" (which was included in ssh ctf-player**@venus.picoctf.net** -p 51536) using a port 51411 which plays a door role. Why does it matter? It is needed because the user needs to access the server (computer) to proceed with challenge. The webshell will ask "Are you sure you want to continue connecting (yes/no/[fingerprint])? You type yes. Then it will require a password. The password is written in the description. You just need to copy and paste the password to the shell.

The next step is typing ls to list the file and then write "cat 1of3.flag.txt". The purpose of this command is to display the content of the file 1of3.flag.txt because the user needs to read the first part of the flag. We should copy and paste the result into the answer section, but this is not the final answer since we need to find all three parts of the flag. After this step we need to write "cat instructions-to-2of3.txt" which gives instructions to go to the root (main) folder (cd / moves to the main folder). Then we write "ls" command to show the files in the main folder to find the next clue. After this command, we continue the previous steps until we finish third part of the flag. After completing all these steps, we type "cd ~" to return to our home folder and then use ls to show files in the home folder to find the last clue. In the end to open the last part of the flag we must type “cat 3of3.flag.txt”.



```
==========================================================================

apanahova16022-picoctf@webshell:~$ cd ~
apanahova16022-picoctf@webshell:~$ ls
README.txt
apanahova16022-picoctf@webshell:~$ ssh ctf-player@venus.picoctf.net -p 514
11
The authenticity of host '[venus.picoctf.net]:51411 ([3.131.124.143]:51411
)' can't be established.
ED25519 key fingerprint is SHA256:P1f6h95BrSVnJbm2AKhphfHHGEyAeThib/rN/AwK
s24.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[venus.picoctf.net]:51411' (ED25519) to the li
st of known hosts.
ctf-player@venus.picoctf.net's password:
Permission denied, please try again.
ctf-player@venus.picoctf.net's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@pico-chall$ ls
1of3.flag.txt  instructions-to-2of3.txt
ctf-player@pico-chall$ cat 1of3.flag.txt
picoCTF{xxsh_
ctf-player@pico-chall$ cat instructions-to-2of3.txt
```



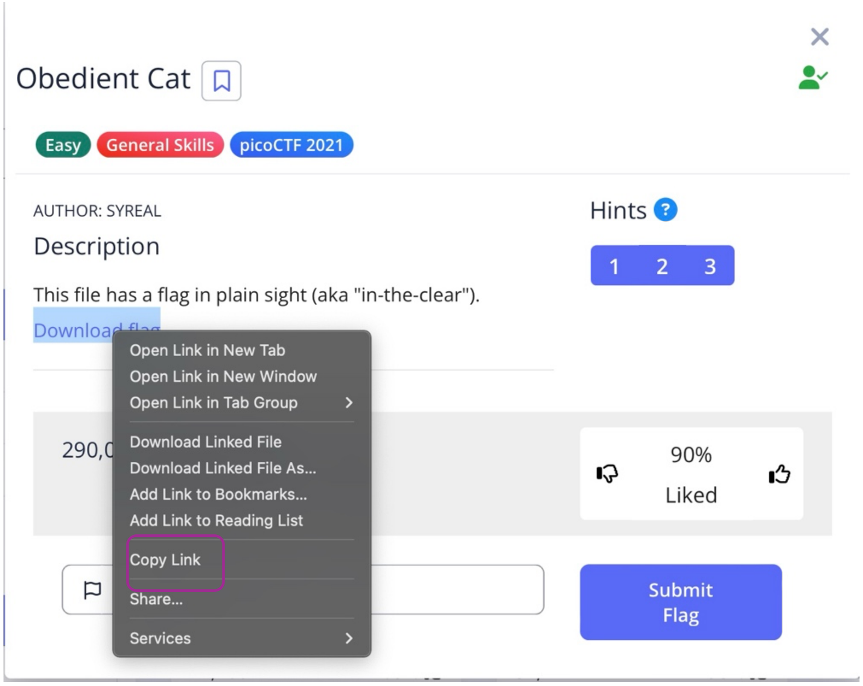
```
Next, go to the root of all things, more succinctly `/`
ctf-player@pico-chall$ cd /
ctf-player@pico-chall$ ls
2of3.flag.txt  dev   instructions-to-3of3.txt  media  proc  sbin  tmp
bin            etc   lib                       mnt    root  srv   usr
boot           home  lib64                     opt    run   sys   var
ctf-player@pico-chall$ cat 2of3.flag.txt
0ut_0f_\/\/4t3r_
ctf-player@pico-chall$ cat instructions-to-3of3.txt
Lastly, ctf-player, go home... more succinctly `~`
ctf-player@pico-chall$ cd ~
ctf-player@pico-chall$ ls
3of3.flag.txt  drop-in
ctf-player@pico-chall$ cat 3of3.flag.txt
71be5264}
ctf-player@pico-chall$ █
```

The commands are highlighted with orange color.

The parts of the flag are highlighted with green color.

Task 3 – OBEDIENT CAT

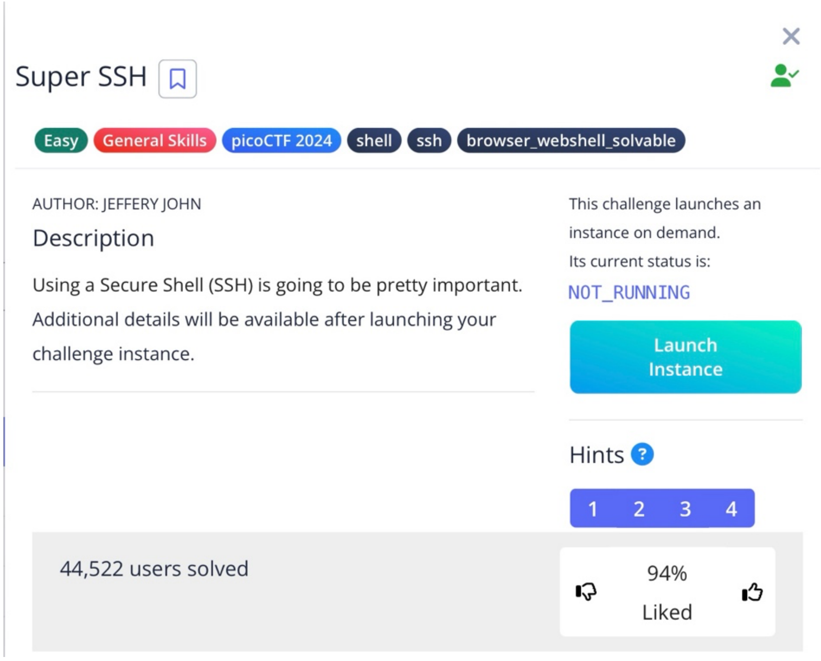
In this quiz we need to download the file that is shown in a description in a webshell not in our computer. Therefore, firstly we need to copy the address (link) of the file by right clicking on file.



After copying the link, we just need to type "wget" command and paste the link after the command so that it downloads on shell not in our computer. Then, we write "ls" to list all files in the folder. After this step we just need to write "cat flag" which opens and shows the content of the flag.

Task 4 – SECURE SSH

To solve this problem first we need to click on “LAUNCH INSTANCE” to see all the details of the description.



Super SSH

AUTHOR: JEFFERY JOHN

Description

Using a Secure Shell (SSH) is going to be pretty important. Additional details will be available after launching your challenge instance.

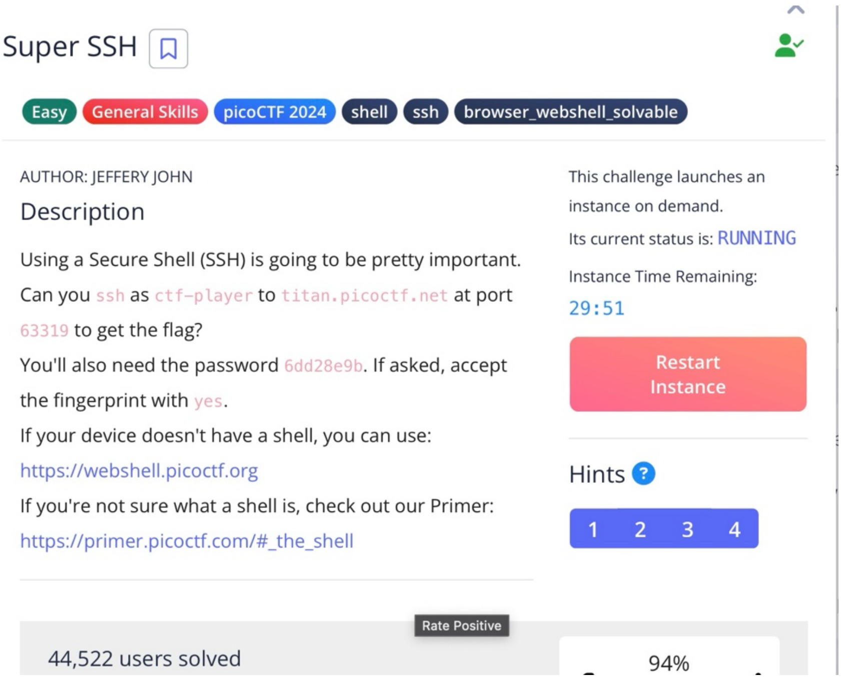
This challenge launches an instance on demand.

Its current status is:

NOT_RUNNING

44,522 users solved

94% Liked



Super SSH

AUTHOR: JEFFERY JOHN

Description

Using a Secure Shell (SSH) is going to be pretty important.
Can you `ssh` as `ctf-player` to `titan.picoctf.net` at port `63319` to get the flag?
You'll also need the password `6dd28e9b`. If asked, accept the fingerprint with `yes`.
If your device doesn't have a shell, you can use:
https://webshell.picoctf.org
If you're not sure what a shell is, check out our Primer:
https://primer.picoctf.com/#_the_shell

This challenge launches an instance on demand.

Its current status is: RUNNING

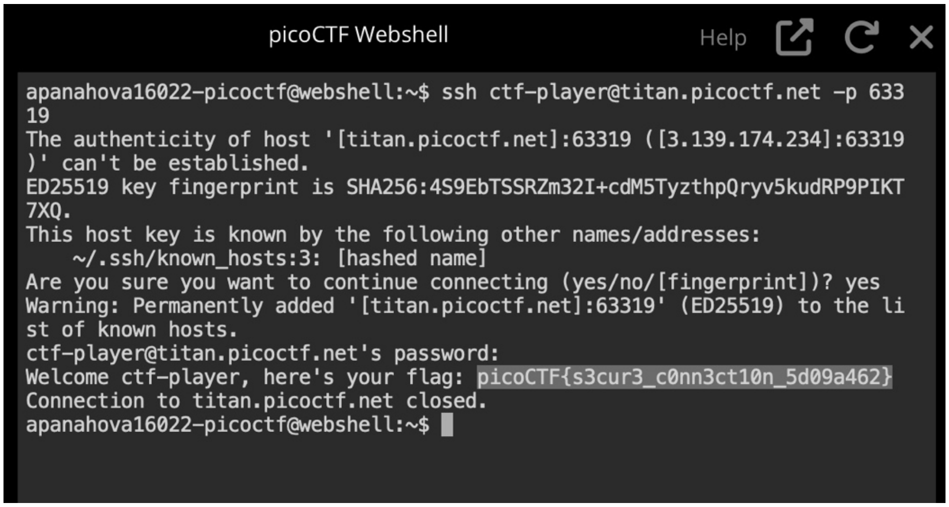
Instance Time Remaining:

29:51

44,522 users solved

94%

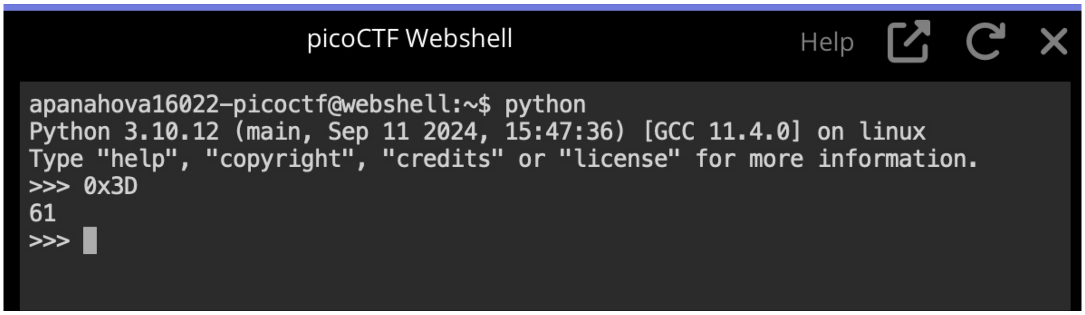
Fisrt we need to combine all details to get the flag (ssh ctf-player@titan.picoctf.net -p 63319). After this step the shell will ask to accept the fingerprint with yes and then require a password which is written in a description. (6dd28e9b). After pressing return, the flag will be displayed.



```
apanahova16022-picoctf@webshell:~$ ssh ctf-player@titan.picoctf.net -p 633
19
The authenticity of host '[titan.picoctf.net]:63319 ([3.139.174.234]:63319
)' can't be established.
ED25519 key fingerprint is SHA256:4S9EbTSSRZm32I+cdM5TyzthpQryv5kudRP9PIKT
7XQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[titan.picoctf.net]:63319' (ED25519) to the li
st of known hosts.
ctf-player@titan.picoctf.net's password:
Welcome ctf-player, here's your flag: picoCTF{s3cur3_c0nn3ct10n_5d09a462}
Connection to titan.picoctf.net closed.
apanahova16022-picoctf@webshell:~$
```

Task 5 – WARMED UP

In the final problem we can used webshell to convert hexadecimal (16) to decimal (10). First, I typed "python" command to webshell because this language is faster, more efficient and more compatible for webshells. After this step I just copied and pasted the hexadecimal to the webshell, and it returned the result.



```
apanahova16022-picoctf@webshell:~$ python
Python 3.10.12 (main, Sep 11 2024, 15:47:36) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x3D
61
>>>
```