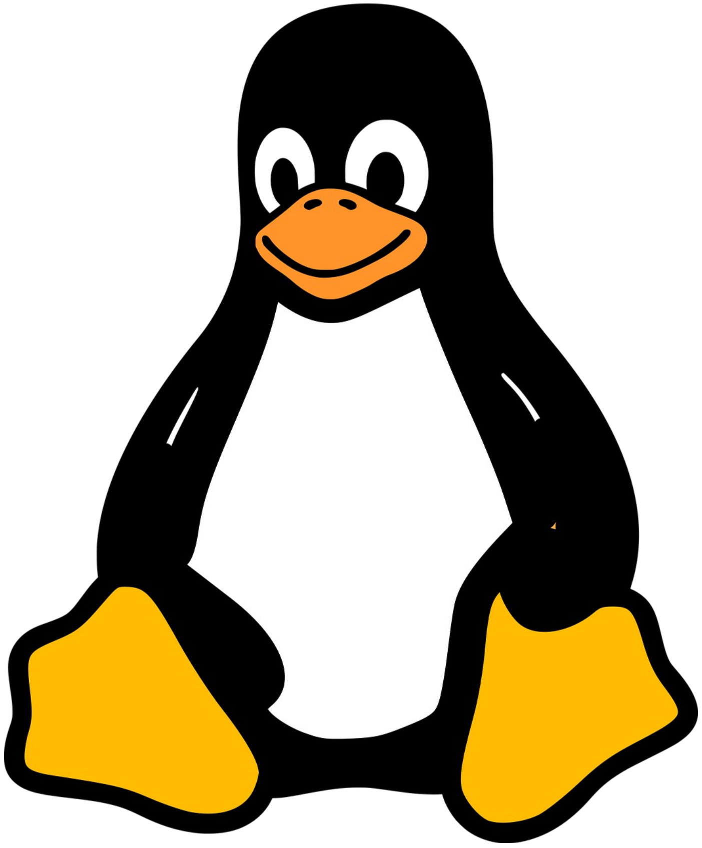
HackerFrogs Afterschool
OverTheWire Bandit: Part 2

Class:
Linux OS Operations

Workshop Number:
AS-LIN-02

Document Version:
1.9

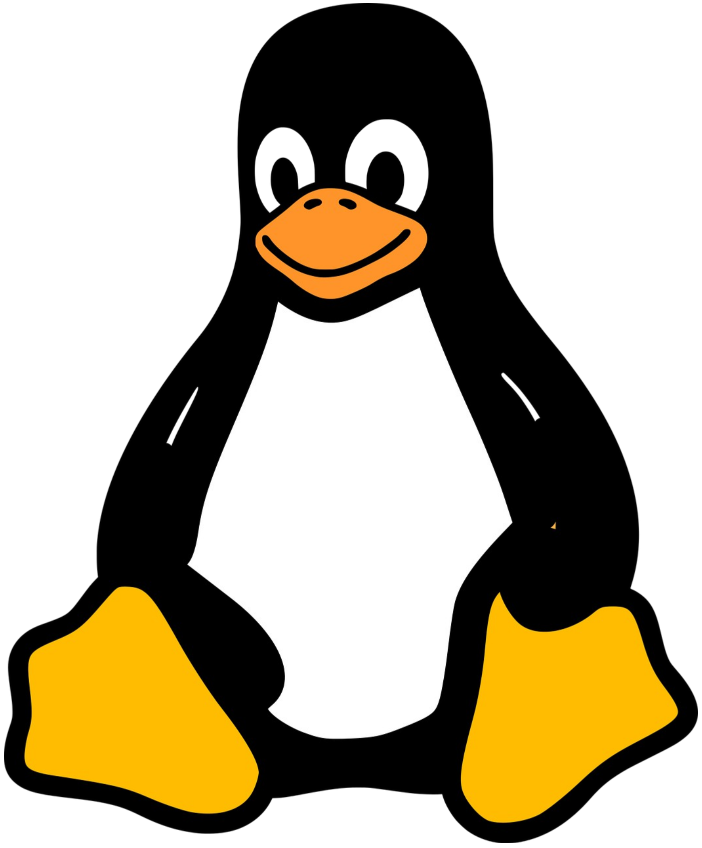
Special Requirements:
Completion of AS-LIN-01



What We Learned In The Previous Workshop

This is the second intro Linux OS operations workshop.

In the previous workshop we learned about the following Linux commands:

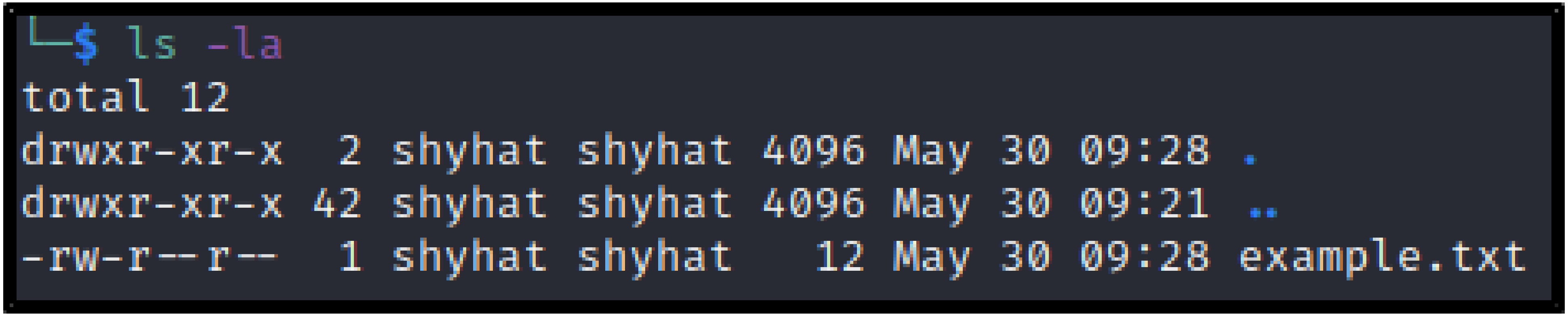


Ls Command

The Ls command lists the files and directories in the current directory.

It can be used with the `-l` argument to output in a list format, and with the `-a` argument to include hidden files and directories in the output. These two arguments can be combined to produce both ouputs, e.g., `-la`

Ls Command



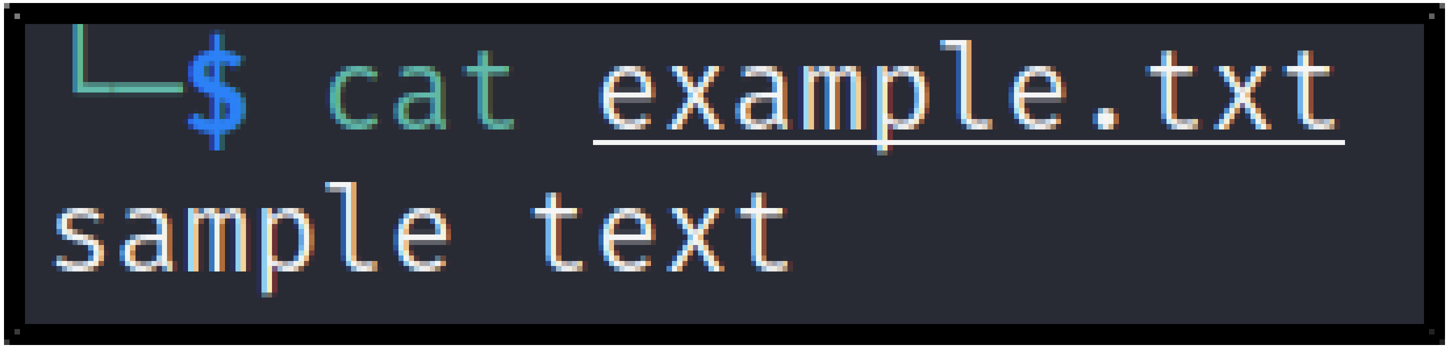
```
└─$ ls -la
total 12
drwxr-xr-x  2 shyhat shyhat 4096 May 30 09:28 .
drwxr-xr-x 42 shyhat shyhat 4096 May 30 09:21 ..
-rw-r--r--  1 shyhat shyhat   12 May 30 09:28 example.txt
```

Cat Command

The Cat command lists the contents of a file. The name of the file to be read must be supplied as an argument to the command.

E.g., `cat example.txt`

Cat Command



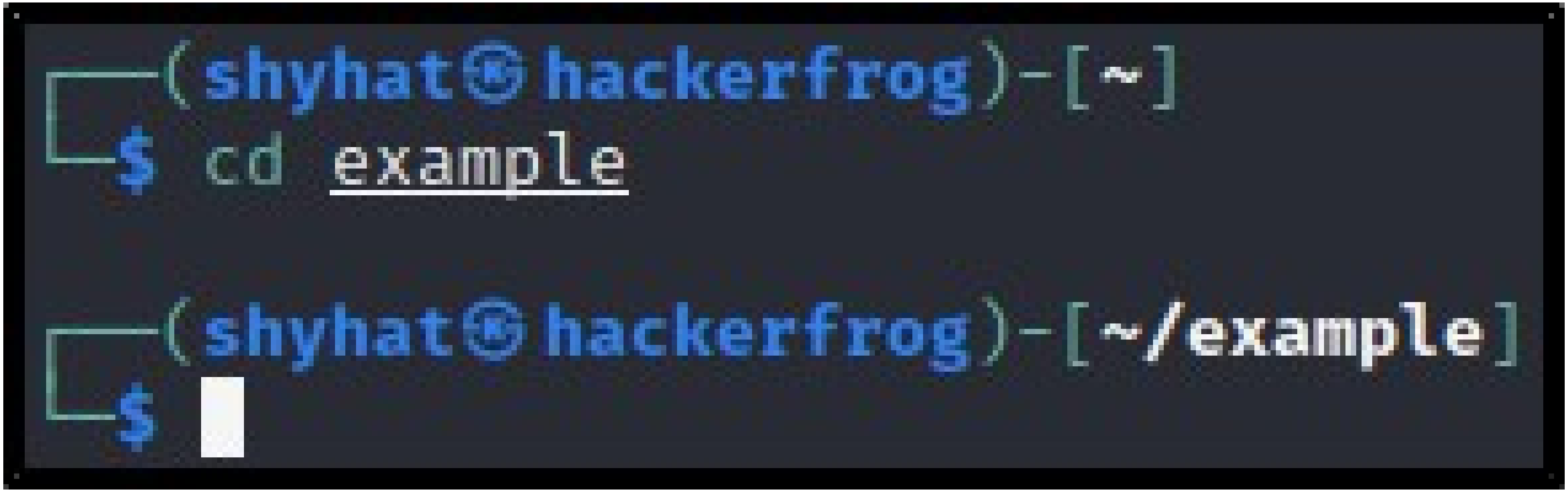
```
└─$ cat example.txt
sample text
```

Cd Command

The Cd command changes the current directory to the one specified. The new directory must be supplied as an argument to the command.

E.g., `cd downloads`

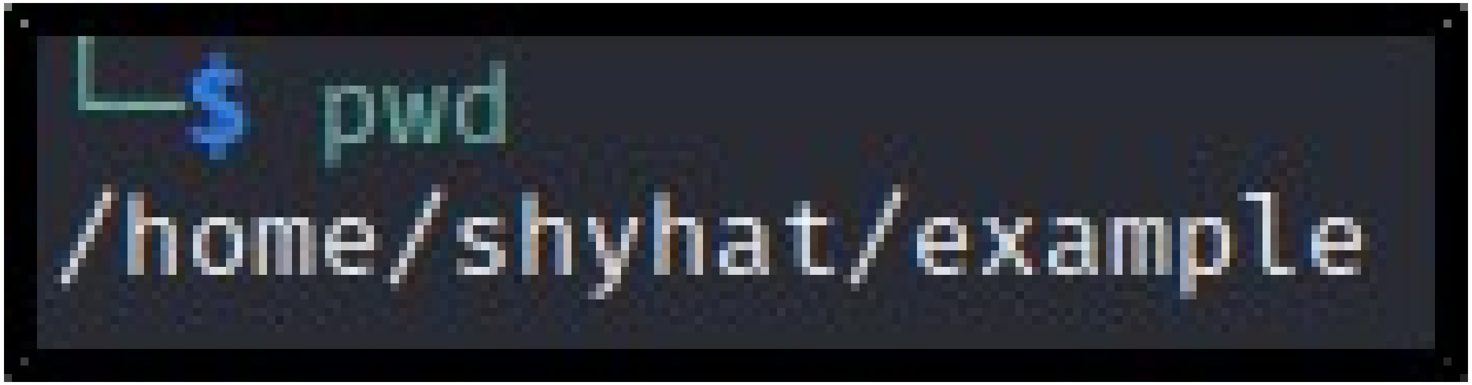
Cd Command



```
┌──(shyhat㉿hackerfrog)-[~]
└─$ cd example

┌──(shyhat㉿hackerfrog)-[~/example]
└─$ 
```

Pwd Command



```
└─$ pwd
/home/shyhat/example
```

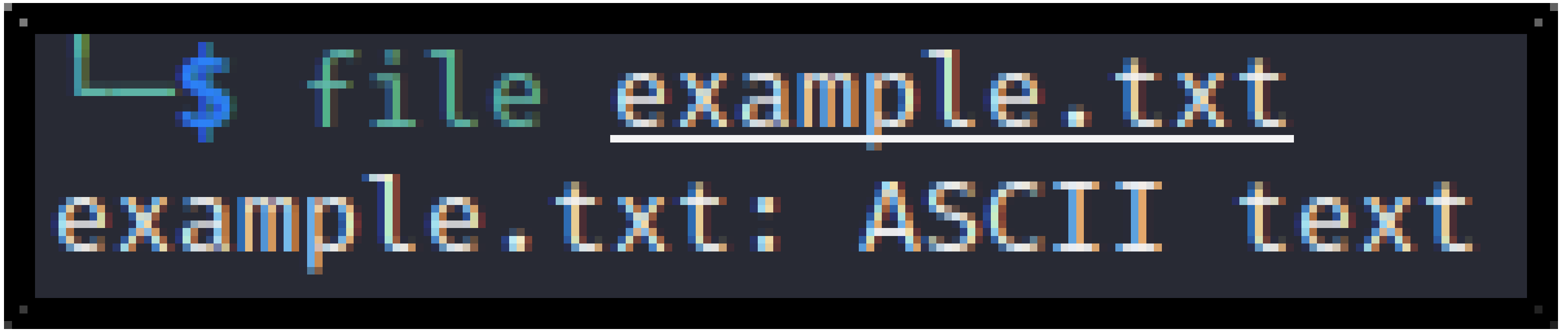
The Pwd command will output the name of the current directory (a.k.a. the present working directory).

File Command

The File command identifies the type of contents for a specified file. The file name must be supplied as an argument to the File command.

E.g., `file picture.jpg`

File Command



```
└─$ file example.txt
example.txt: ASCII text
```

Let's Continue Where We Left Off!

Login to the PicoCTF website, then let's start the following challenge:

https://play.picoctf.org/practice/challenge/320?category=5&page=1&search=find

Mkdir Command

When solving challenges in the webshell, it's useful to create new directories and work within them to keep the rest of the filesystem organized. To do so, we'll use the **mkdir** command

Mkdir Command

The **mkdir** command is used to create new directories in the current directory. The syntax for the command is as follows:

```
mkdir <new_directory_name>
```

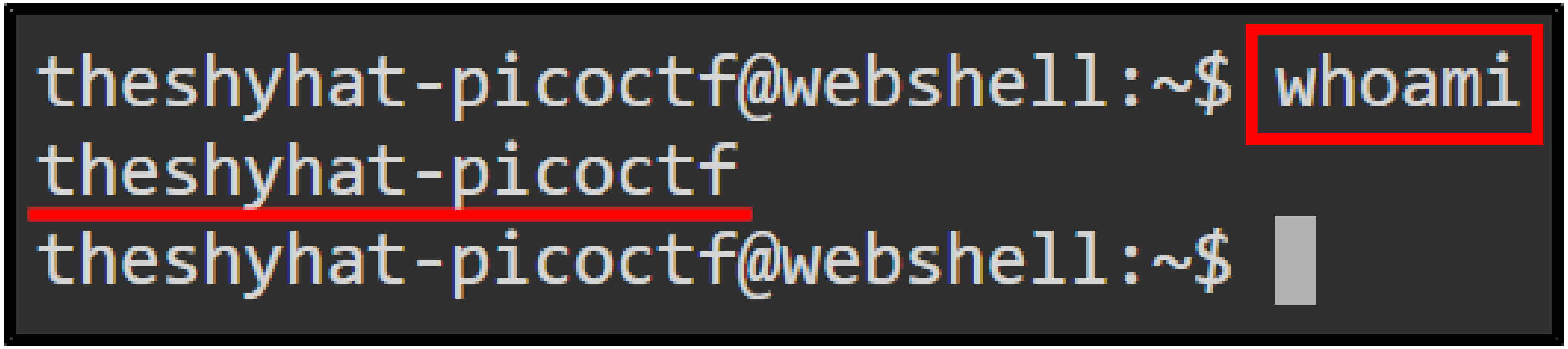
For example

```
mkdir firstfind
```

Whoami Command

The **whoami** command is used to return the name of the user account currently being used

Whoami Command



```
theshyhat-picoctf@webshell:~$ whoami
theshyhat-picoctf
theshyhat-picoctf@webshell:~$
```

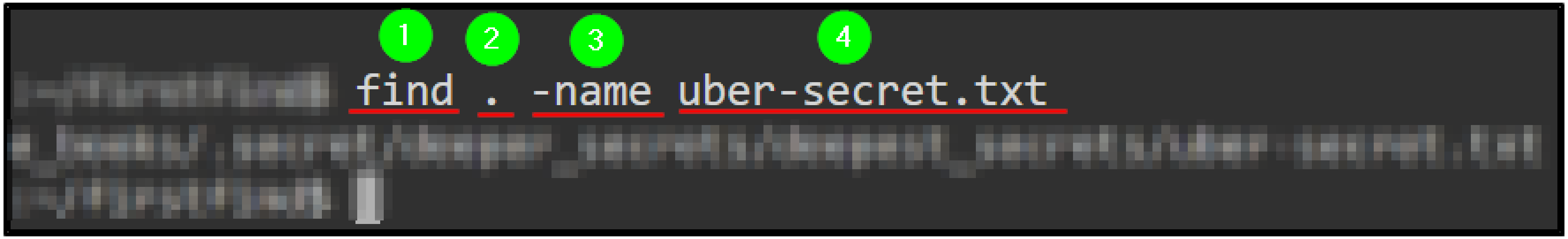
Here the **whoami** command is used, and the name of the account is **theshyhat-picoctf**

Find Command

The Find command allows a search of files and / or directories in the file system, and matches files in the output according to the criteria provided by the command arguments.

The argument `-name` searches by the name of the file

Find Command



```
[redacted] find . -name uber-secret.txt
[redacted]
[redacted]
```

1 – The command itself

2 – The location to be searched

3 – Searching by file / directory name

4 – The name of the file to find

Rm Command

To keep our PicoCTF webshell home directory clean, and because we're only allowed a certain amount of disk space, we should delete our challenge directories after we're done solving the challenge. We can do so with the **rm** command.

Rm Command

The syntax for the **rm** command is as follows:

```
rm <filename>
```

But deleting directories requires the use of the **-r** flag:

```
rm -r firstfind
```

First Grep Challenge

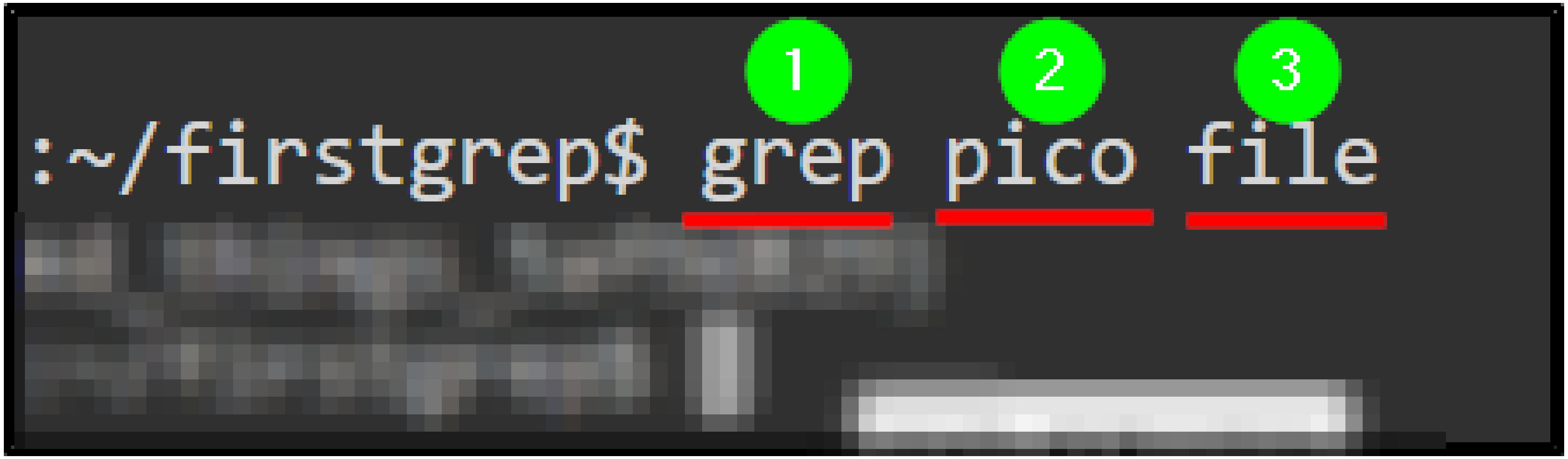
Let's solve another PicoCTF challenge to learn more Linux skills:

https://play.picoctf.org/practice/challenge/85?category=5&page=1&search=grep

Grep Command

The Grep command searches within the contents of files for specified strings. It is very commonly used to pick out specific words or phrases.

Grep Command



```
:~/firstgrep$ grep pico file
[redacted]
```

1 – The command itself

2 – The pattern to search for in the file / directory

3 – The file to be searched

Big Zip Challenge

Let's solve another PicoCTF challenge to learn more Linux skills:

https://play.picoctf.org/practice/challenge/322?category=5&page=1&search=zip

Running Grep Recursively

Grep can also be used to search inside of all files in a directory and all directories in those directories (recursion). We just need to use the **-r** flag:

```
grep -r pico .
```

This looks in the current directory and all directories underneath for the pattern “pico”

Magikarp Ground Mission Challenge

Let's wrap up by solving a challenge that will test our filesystem navigation skills (ls and cd commands):

https://play.picoctf.org/practice/challenge/189?category=5&page=1&search=magi

The Home Directory

Each user on a Linux system has a space where they can store their personal files. It's located at:

```
/home/<username>
```

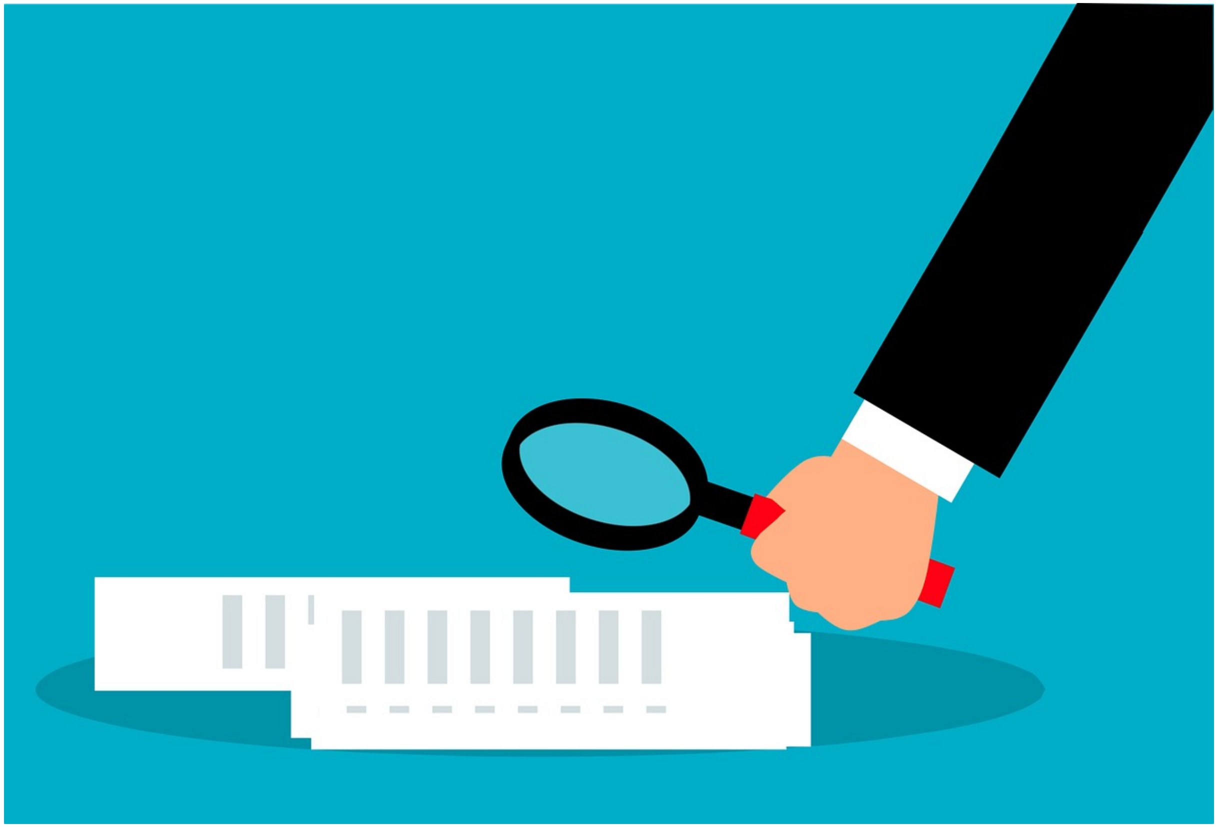
For example:

```
/home/theshyhat
```

The Top-Level Directory

The top level directory of a Linux system is the / directory, where we can find all the other directories and files in the system. It can also be called the root directory, which can be confusing, since there's another directory called the root directory...

Summary



Let's review the Linux commands we learned in today's workshop:

Find Command

The Find command is used to search for files on the system. It can used with many different arguments and flags to refine the search parameters.

Whoami Command

The **whoami** command is used to return the name of the user account currently being used

Rm Command

The rm command is used to delete files or directories, but deleting directories requires the use of the **-r** flag:

```
rm -r firstfind
```

Grep Command

The Grep command searches within the contents of files for specified strings. It is very commonly used to pick out specific words or phrases.

What's Next?

In the next HackerFrogs Afterschool Linux OS workshop, keep learning more about the Linux OS using the picoCTF platform.

Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

Until Next Time, HackerFrogs!