

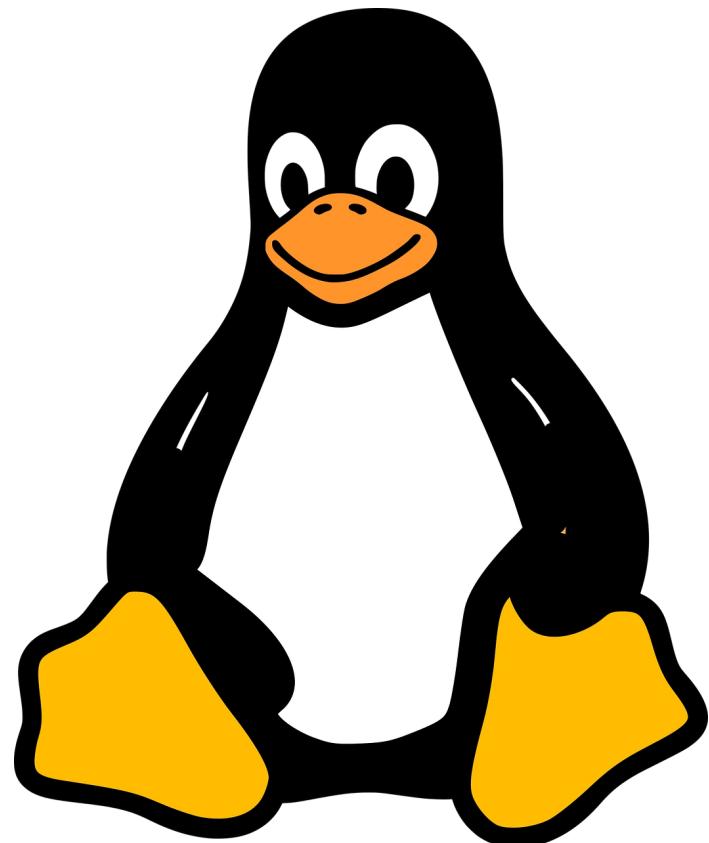
HackerFrogs Afterschool OverTheWire Bandit: Part 2

Class:
Linux OS Operations

Workshop Number:
AS-LIN-02

Document Version:
1.0

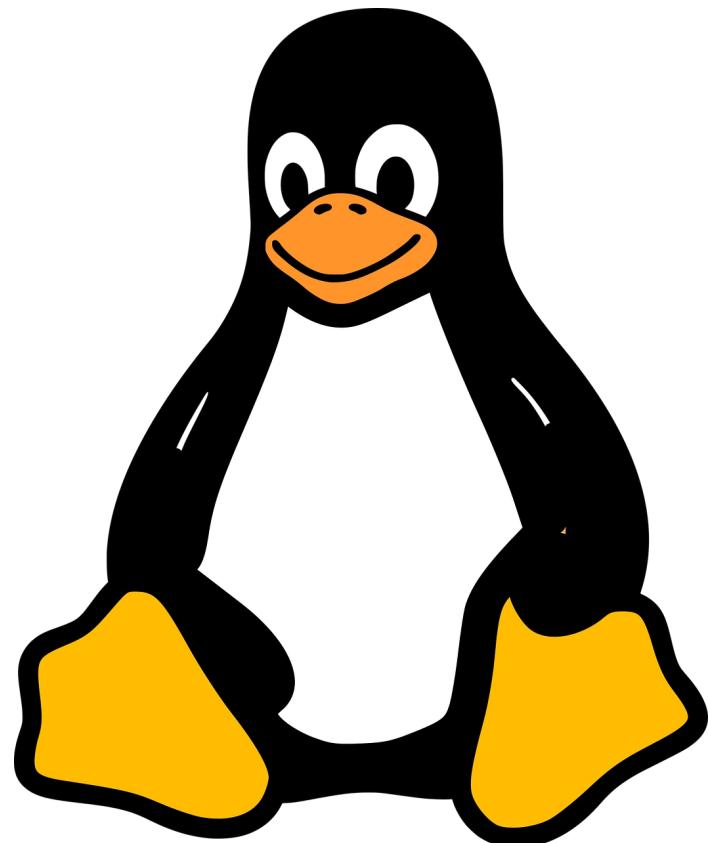
Special Requirements:
Completion of AS-LIN-01



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 outputs, 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

```
L$ cat example.txt
sample text
```

Echo Command

```
echo b0 bandit0 >> banditpass.txt
```

The Echo command creates output based on whatever argument is supplied to it. It is very useful for creating output for redirection.

Output Redirection

```
echo b0    bandit0 >> banditpass.txt
```

Output redirection is the process of redirecting the output of a command, either into a file, or into another command.

Output Redirection

```
echo b0    bandit0 >> banditpass.txt
```

Here the double greater-than (`>>`) symbols redirect output into a file, but if that file already exists, it will instead append to that file.

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]
$ █
```

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
```

Find Command

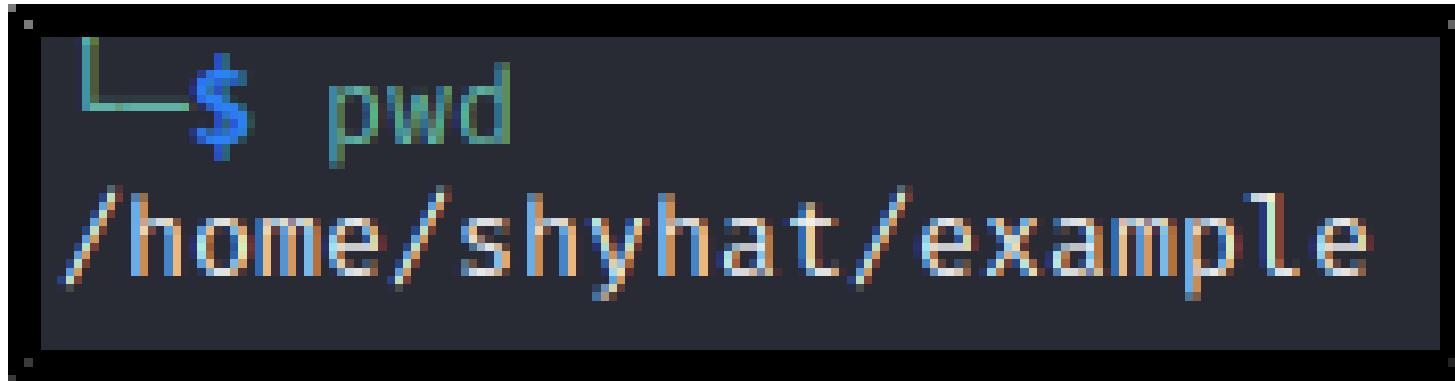
The Find command allows a search of files and / or directories in the file system, and matches files in the output according to the criteria provided by the command arguments.

The argument `-type` searches by file or directories and the argument `-size` searches for files of a particular size.

Find Command

```
$ find -type f  
./example.txt
```

Pwd Command

A screenshot of a terminal window with a black background and white text. It shows a command-line interface where the user has typed '\$ pwd' and the system has responded with the path '/home/shyhat/example'. The prompt '\$' is in green, and the rest of the text is in white.

```
$ pwd  
/home/shyhat/example
```

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

Let's Continue Where We Left Off!

Open your command line interface (CLI) terminal, then navigate to the following URL in a web browser:

<https://overthewire.org/wargames/bandit/bandit7.html>

Find Command

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



Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – The type of data to be returned, file / directory
- 4 – **The file / directory user ownership**
- 5 – The file / directory group ownership
- 6 – **The file / directory size**
- 7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

1 – The command itself

2 – The location to be searched

3 – The type of data to be returned, file / directory

4 – **The file / directory user ownership**

5 – The file / directory group ownership

6 – **The file / directory size**

7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

1 – The command itself

2 – The location to be searched

3 – The type of data to be returned, file / directory

4 – The file / directory user ownership

5 – The file / directory group ownership

6 – The file / directory size

7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – **The type of data to be returned, file / directory**
- 4 – **The file / directory user ownership**
- 5 – The file / directory group ownership
- 6 – **The file / directory size**
- 7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – The type of data to be returned, file / directory
- 4 – The file / directory user ownership**
- 5 – The file / directory group ownership
- 6 – The file / directory size**
- 7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – The type of data to be returned, file / directory
- 4 – **The file / directory user ownership**
- 5 – **The file / directory group ownership**
- 6 – **The file / directory size**
- 7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – The type of data to be returned, file / directory
- 4 – **The file / directory user ownership**
- 5 – The file / directory group ownership
- 6 – **The file / directory size**
- 7 – Omit error messages from output

Find Command

```
find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
1 2 3 4 5 6 7
```

- 1 – The command itself
- 2 – **The location to be searched**
- 3 – The type of data to be returned, file / directory
- 4 – **The file / directory user ownership**
- 5 – The file / directory group ownership
- 6 – **The file / directory size**
- 7 – **Omit error messages from output**

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



1 – The command itself

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

3 – The file to be searched

Grep Command



1 – The command itself

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

3 – The file to be searched

Grep Command



1 – The command itself

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

3 – The file to be searched

Grep Command



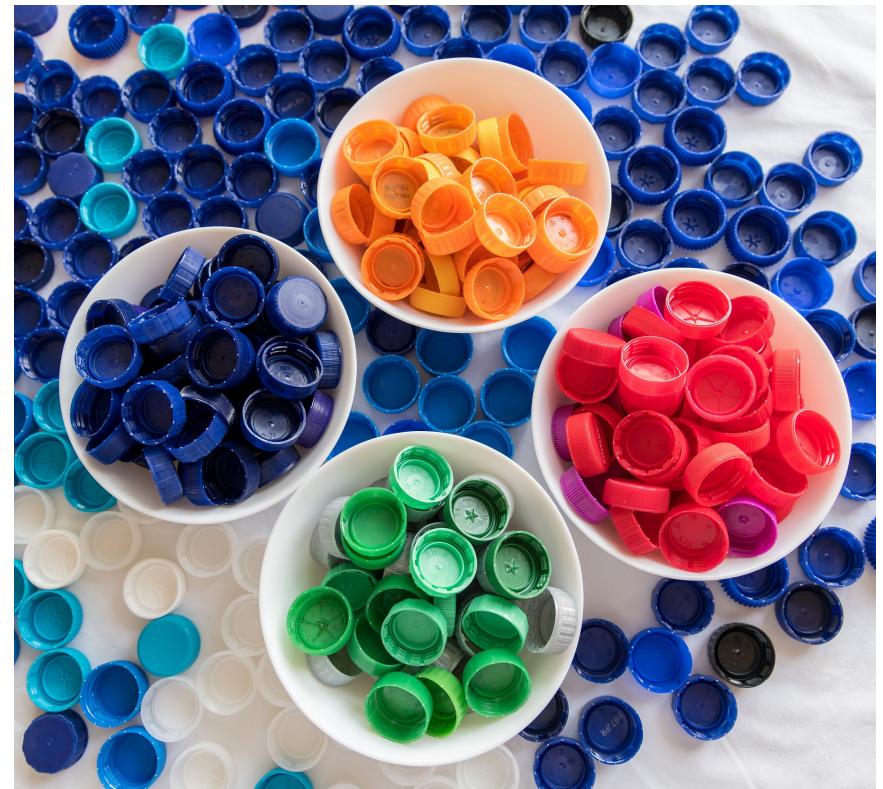
1 – The command itself

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

3 – The file to be searched

Sort Command

The Sort command takes all of the lines contained within a given file and returns them in alphabetical / numerical order.



Sort Command



1 – The command itself

2 – The input to be sorted

Sort Command



1 – The command itself

2 – The input to be sorted

Sort Command



1 – The command itself

2 – The input to be sorted

Uniq Command

The Uniq command takes all of the lines in a file and removes any lines with identical contents to the one above it. This command is very useful for removing consecutive blank lines in a given file



Uniq Command



1 – The command itself

2 – The count flag

3 – The file to be processed

Uniq Command



1 – The command itself

2 – The count flag

3 – The file to be processed

Uniq Command



1 – The command itself

2 – The count flag

3 – The file to be processed

Uniq Command



1 – The command itself

2 – The count flag

3 – The file to be processed

Command Piping

```
sort data.txt | uniq -c
```

In Linux, command piping is the process of passing the output of one command into the input of a second command.

Command Piping

```
sort data.txt | uniq -c
```

This is a very useful feature, because it allows commands to be chained together to achieve a lot of flexible output.

Command Piping



- 1 – The first command
- 2 – **The first command's input**
- 3 – The pipe
- 4 – **The second command**
- 5 – The second command's switch

Command Piping



- 1 – The first command
- 2 – The first command's input
- 3 – The pipe
- 4 – The second command
- 5 – The second command's switch

Command Piping



- 1 – The first command
- 2 – The first command's input**
- 3 – The pipe
- 4 – The second command**
- 5 – The second command's switch

Command Piping



- 1 – The first command
- 2 – **The first command's input**
- 3 – **The pipe**
- 4 – **The second command**
- 5 – The second command's switch

Command Piping



- 1 – The first command
- 2 – **The first command's input**
- 3 – The pipe
- 4 – The second command**
- 5 – The second command's switch

Command Piping



- 1 – The first command
- 2 – **The first command's input**
- 3 – The pipe
- 4 – **The second command**
- 5 – **The second command's switch**

Binary Data and Text Strings

The contents of most computer files can be roughly divided into two types:

Binary Data – Which is intended to be read by software

Text Strings – Which is intended to be read by humans

Binary Data and Text Strings

The contents of most computer files can be roughly divided into two types:

Binary Data – Which is intended to be read by software

Text Strings – Which is intended to be read by humans

Binary Data and Text Strings

The contents of most computer files can be roughly divided into two types:

Binary Data – Which is intended to be read by software

Text Strings – Which is intended to be read by humans

Binary Data and Text Strings

Files containing binary data will output gibberish when read from the CLI console.

Strings Command

The Strings command is used to return human-readable text from files. It is often used to find text inside of files that also contain both text and binary data.



Strings Command



- 1 – The command itself
- 2 – The file to extract strings from

Strings Command



1 – The command itself

2 – The file to extract strings from

Strings Command



1 – The command itself

2 – The file to extract strings from

Base64 Command

The Base64 command encodes / decodes data according to the Base64 codec. It is often used to convert data for transmission across computer networks.

0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	I	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 Command

The characters used in Base 64 encoding are shown here. Note that all Base 64 encoded strings must consist of a number of characters that is divisible by 4.

0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	I	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 Command

```
└$ echo -n password | base64  
cGFzc3dvcmQ=
```

In cases where an encoded string is not divisible by 4, the encoding process will “pad out” the string with equal symbols until the string is divisible by 4.

Base64 Command



1 – The command itself

2 – The decode switch

3 – The file to be operated upon

Base64 Command



1 – The command itself

2 – The decode switch

3 – The file to be operated upon

Base64 Command



1 – The command itself

2 – The decode switch

3 – The file to be operated upon

Base64 Command

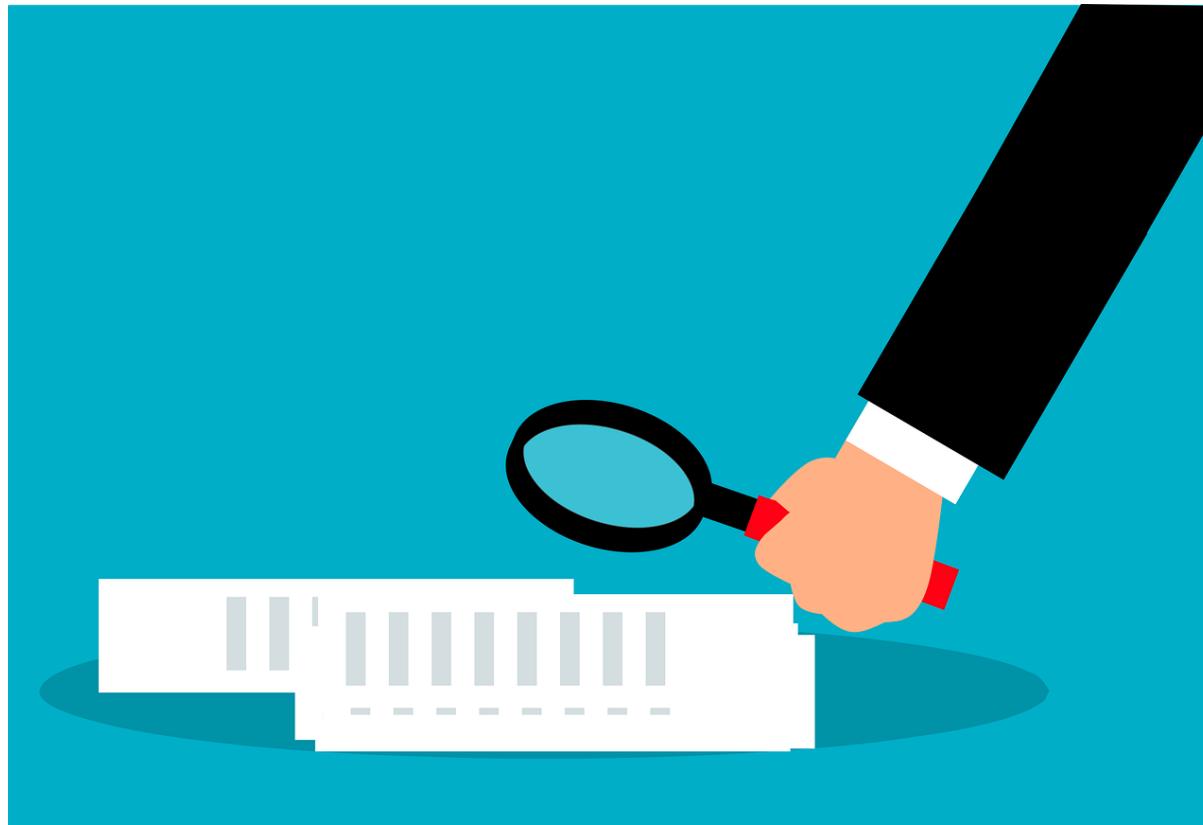


1 – The command itself

2 – The decode switch

3 – The file to be operated upon

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 be used with many different arguments and flags to refine the search parameters.



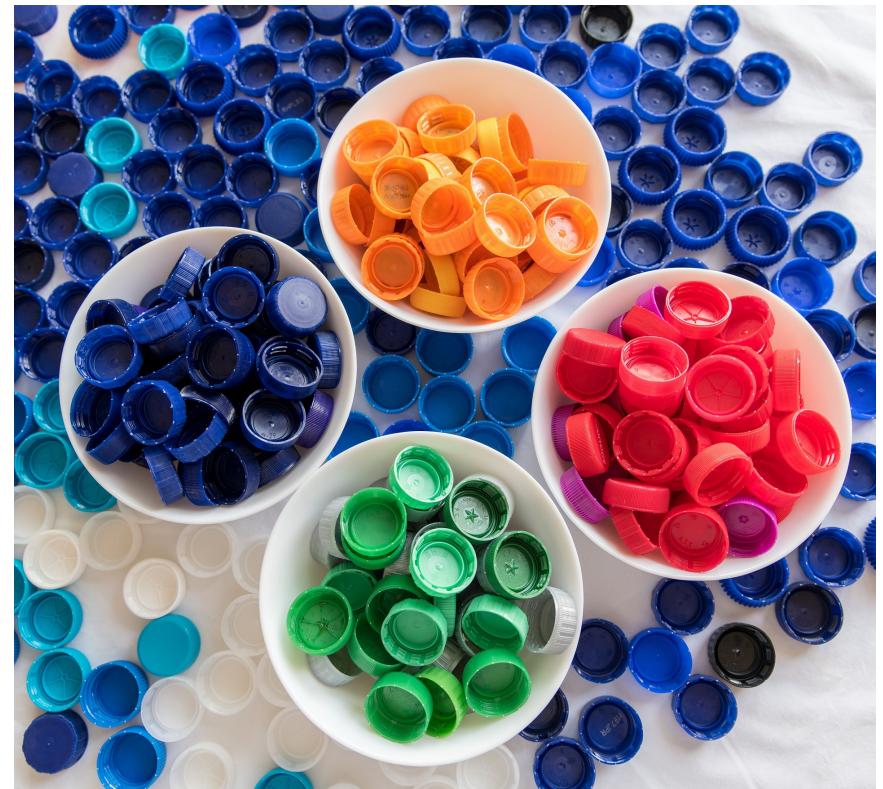
Grep Command

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



Sort Command

The Sort command takes all of the lines contained within a given file and returns them in alphabetical / numerical order.



Uniq Command

The Uniq command takes all of the lines in a file and removes any lines with identical contents to the one above it. This command is very useful for removing consecutive blank lines in a given file



Command Piping

Command piping is the process of passing the output of one command into the input of a second command (via use of the Linux pipe | character)



Strings Command

The Strings command is used to return human-readable text from files. It is often used to find text inside of files that also contain both text and binary data.



Base64 Command

The Base64 command encodes / decodes data according to the Base64 codec format. It is often used to convert data for transmission across computer networks.

0 A	16 Q	32 g	48 w
1 B	17 R	33 h	49 x
2 C	18 S	34 I	50 y
3 D	19 T	35 j	51 z
4 E	20 U	36 k	52 0
5 F	21 V	37 l	53 1
6 G	22 W	38 m	54 2
7 H	23 X	39 n	55 3
8 I	24 Y	40 o	56 4
9 J	25 Z	41 p	57 5
10 K	26 a	42 q	58 6
11 L	27 b	43 r	59 7
12 M	28 c	44 s	60 8
13 N	29 d	45 t	61 9
14 O	30 e	46 u	62 +
15 P	31 f	47 v	63 /

What's Next?

In the next HackerFrogs Afterschool Linux OS workshop, we'll switch gears and improve our Linux understanding with the TryHackMe education 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!

