<https://os.cybbh.io/public/os/latest/003_linux_essentials/bash_fg.html>

1.1 Linux basic commands

pwd

which pwd

which bash

hostname

uname -a

hostname -I

whoami

who

who --ips

who -b #last system boot

who -r #current run level

who -a or --all #print all run levels

ip addr help

ip addr show #common ones: add, remove, show

ip -4 addr

ip neigh #big brother of ARP

arp

ip route

ip route list 10.10.0.0/24

netstat #networking tool, monitoring tool (incoming/outgoing)

netstat -at

netstat -l

#grep in netstat

netstat -ap | grep journal

netstat -s

netstat -st #sorted by protocol

netstat -tp #service by tcp

#alternative to netstat “ss”

ss -a #view all tcp connection

ss -l #listening ports only

iptables -L #need root permission

sudo -l #list of files associated with sudo

1.2 Arguments

cd /

ls -lisa

\*ls -shilat #h-human readable, t-time sorted

1.4 Variables and Command Substitution

a=200

echo $a #reference using $ the variable a

unset $a

unset a #clear the variable

1.5 Redirection

#3 types of streams: std input **0**- default, std output **1**- success, std error **2**- fail

directories=$(ls /)

echo $directories

echo $directories 1> thisisanewfile

cd $HOME

ls

echo $directories 1> thisisanewfile

ls -shilat

cat thisisanewfile

\*ls doesntexist 2> errorfile

cat errorfile

cmd &> errorfile

cat errorfile

#redirect BOTH std output and std error

cmd >> errorfile 2>&1

ls -Rlisa /etc | grep syslog

↳ls -Rlisa /etc **2> /dev/null** | grep syslog **#handles error from previous**

#for loop

objects=$(ls -d /etc/\*)

echo $objects

for item in $objects; do echo $item; done

#do loop

for object in $objects;

do if [-d $object];

then echo “$object is a directory”;

else echo “$object is a file”;

fi;

done

#while loop

while [ 1 -eq 1 ]; do echo "To Infinity and Beyond!"; done

3 Linux Filesystem

cd /bin

ls -ld $PWD/\*

cd /etc

ls -shilat

less passwd

whoami

id

uid=1001(garviel) gid =1001(garviel) groups=1001(gariel),1007(lodge),1009(chapter)

cat /etc/passwd | grep garviel

cat /etc/group | grep garviel

cat /etc/group

ls -shila /bin/dd

↳25 76K -rwxr-xr-x 1 root root 75K Jan 18 2018 /bin/dd

d for directory: if it has d it can remove files within directory unless \*sticky bit\*

sudo su

find / -perm /4000 2> /dev/null -exec ls -la {} \;

↳this indicates parameters are done

\*READ up on 3.5.2 Special Permissions : SUID and SGID

4. String Manipulation

AWK

ls -l /etc

ls -l /etc | awk -F “ ” ‘{print$3”,”$4”,”$9}’ > $HOME\files.csv

cat /etc/passwd | grep root | sed s/root/bacon/g

#find the hash

echo bad\_magic\_number | openssl aes-256-cbc -salt -a -out secrets.txt.enc

openssl aes-256-cbc -a -salt -in secrets.txt -out secrets.txt.enc

#reverse

openssl aes-256-cbc -d -in secrets.txt.enc -out notsecrret.txt

What command lists the contents of directories in Linux/Unix systems?

ls

For the ls command, what arguments, or switch options, will allow you to print human-readable file sizes in a long-list format?

ls -lh

What character will pipe the standard output from

echo "I’m a plumber"

to another command, as standard input?

|

What argument/switch option, when used with man, will search the short descriptions and man-page-names for a keyword that you provide?

man -k

What is the absolute path to the root directory?

/

What is the absolute path to the default location for configuration files?

/etc

What is the directory that contains executable programs (binaries) which are needed in single user mode, to bring the system up or to repair it?

/bin

What is the absolute path to the directory which contains non-essential binaries that are accessible by standard users as well as root?

/usr/bin

An absolute path to a directory which contains binaries only accessible by the root user, or users in the root group.

/usr/sbin

What is the absolute path for the binary cat man-page?

Search the man pages for the keyword *digest*. Then, use one of the binaries listed to hash the string OneWayBestWay using the largest *sha* hash available.

Identify all members of the Lodge group. List their names in alphabetical order with a comma in between each name.

Flag Format: *name,name,name*

cat /etc/group | grep ‘lodge’

Linux Basics Regular Expressions3

10

File: home/garviel/numbers

Use regular expressions to match valid IP addresses. The flag is the number of addresses.

**cat /home/garviel/numbers | grep -Eo "^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$" | wc -l**

**18**

Linux Basics Regular Expressions4

10

File: home/garviel/numbers

Use regular expressions to match patterns that look similar to a MAC Address. Flag is a count of the number of matches.

**cat /home/garviel/numbers | grep -E '^..\-..\-..\-..\-..\-..$' | wc -l**

**4877**

Linux Basics Reformat1

File: home/garviel/numbers

Use awk to print lines:

>= 420 AND <=1337

The flag is a SHA512 hash of the output.

**cat numbers | awk 'NR >= 420 && NR <=1337 {print$1}' | sha512sum**

**Linux Basics Bash Logic2**

**10**

**The flag resides in $HOME/paths... you just need to determine which flag it is. The flag sits next to a string matching the name of a $PATH/binary on your system.**

**Hint: The correct binary is not echo**

Linux Basics Users and Groups4

10

Identify the algorithm, the amount of salted characters added, and the length of the hashed password in the file that stores passwords.

Flag format: algorithm,#characters,#length

**sha512,8,86**

\*Review Questions:

Execute the file owned by the guardsmen group in /media/Bibliotheca, as the owning user.

The flag is the code name provided after a successful access attempt.

File: home/garviel/connections

Use awk to create a separate CSV (comma separated value) file that contains columns 1-6.

The flag is an MD5 hash of the new file

Hint: Look at #fields on line 6 in the file to understand column layout.

Hint: This is a Zeek (formally known as Bro) connection log file in TSV format. Click This Link to learn about its formatting.

**- cat connections | awk**

**' {print $1, $2, $3, $4,**

**$5, $6}' OFS="," con-**

**nections > outfile**

**- chmod 777 outfile**

**- md5sum outfile**

The flag resides in $HOME/paths... you just need to determine which flag it is. The flag sits next to a string matching the name of a $PATH/binary on your system.

**cat paths | awk ‘NR==FNR{a[$1,$1];next}**

PLEASE - PHYSICAL LAYER 1

DO - DATA LINK LAYER 2

NOT- NETWORK LAYER 3

THROW- TRANSPORT LAYER 4

SAUSAGE- SESSION LAYER 5

PIZZA- PRESENTATION LAYER 6

AWAY- APPLICATION LAYER 7