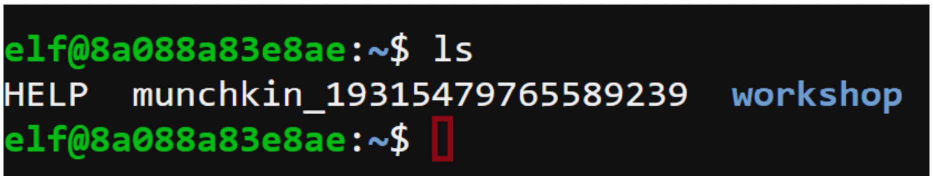
Linux Primer
SANS Holiday Hack 2020

IS 401/501
8/16/2023

Group Members:
Patrick Doolin, Casen Woody, Isaac Vaillancourt, Josh Catterall,
Isaac Falero, Aaron Thammavongsa

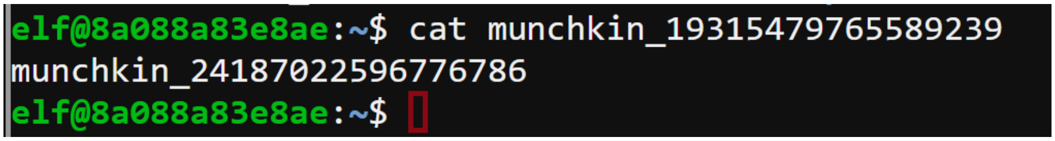
1. **Perform a directory listing of your home directory to find a munchkin and retrieve a lollipop!**



```
elf@8a088a83e8ae:~$ ls
HELP  munchkin_19315479765589239  workshop
elf@8a088a83e8ae:~$
```

Command: ls
Explanation: This command lists the contents of the directory.

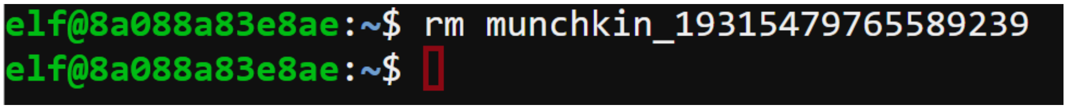
2. **Now find the munchkin inside the munchkin.**



```
elf@8a088a83e8ae:~$ cat munchkin_19315479765589239
munchkin_24187022596776786
elf@8a088a83e8ae:~$
```

Command: cat munchkin_19315479765589239
Explanation: The “cat” command shows the contents within a file. We were able to look inside the munchkin file and find the munchkin.

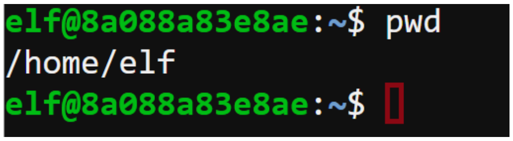
3. **Great, now remove the munchkin in your home directory.**



```
elf@8a088a83e8ae:~$ rm munchkin_19315479765589239
elf@8a088a83e8ae:~$
```

Command: rm munchkin_19315479765589239
Explanation: The “rm” command removes the designated file from its current directory.

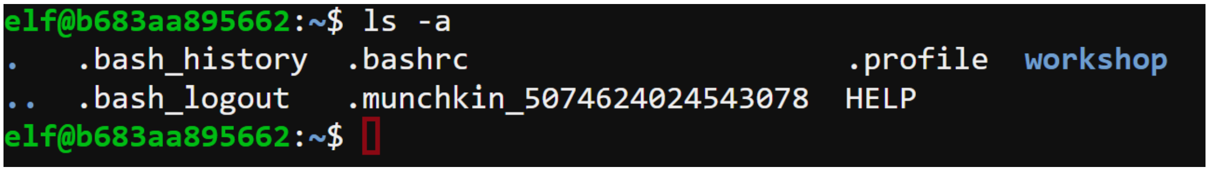
4. **Print the present working directory using a command.**



```
elf@8a088a83e8ae:~$ pwd
/home/elf
elf@8a088a83e8ae:~$
```

Command: pwd
Explanation: This command will print the full path of the current working directory.

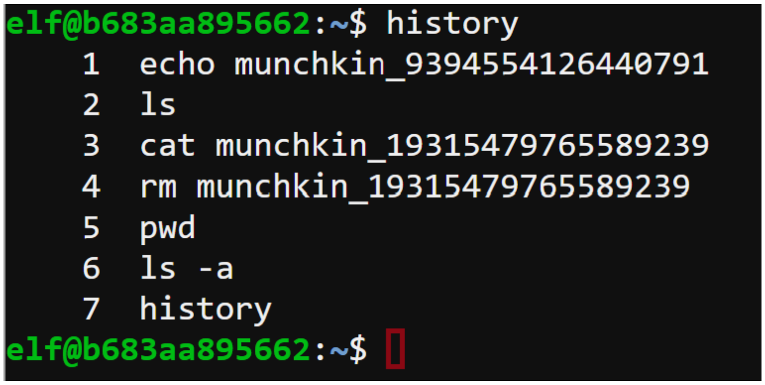
5. **Good job but it looks like another munchkin hid itself in your home directory. Find the hidden munchkin!**



```
elf@b683aa895662:~$ ls -a
.    .bash_history  .bashrc                      .profile  workshop
..   .bash_logout   .munchkin_5074624024543078   HELP
elf@b683aa895662:~$
```

Command: ls -a
Explanation: The “ls” command with the “-a” flag shows all files and directories, including the hidden ones.

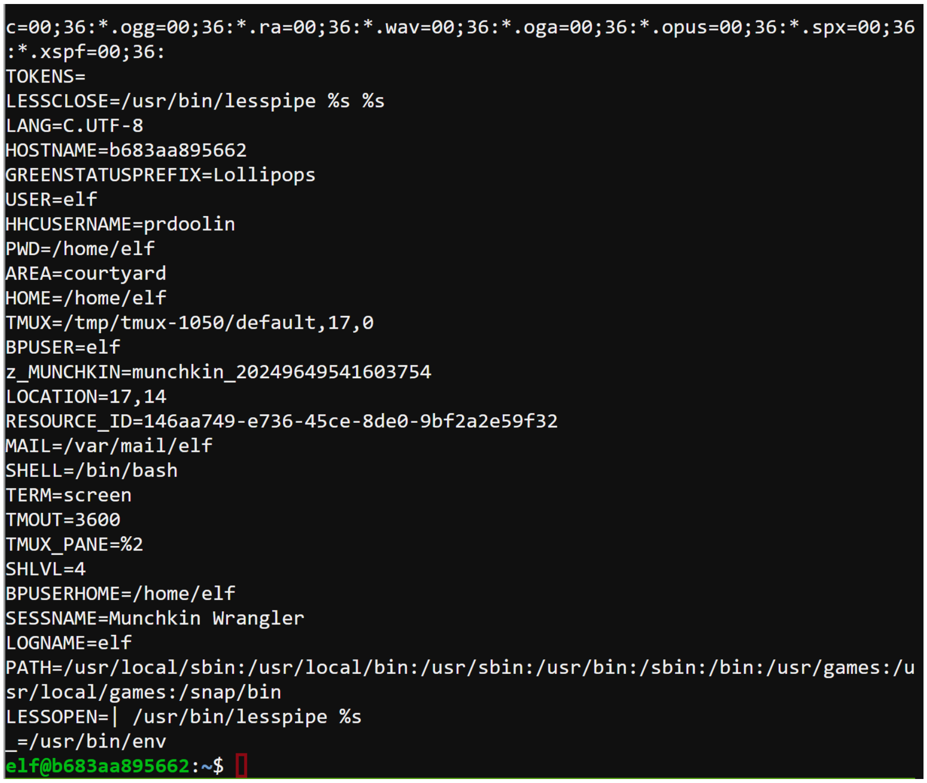
6. **Excellent, now find the munchkin in your command history.**



```
elf@b683aa895662:~$ history
    1  echo munchkin_9394554126440791
    2  ls
    3  cat munchkin_19315479765589239
    4  rm munchkin_19315479765589239
    5  pwd
    6  ls -a
    7  history
elf@b683aa895662:~$ 
```

Command: history
Explanation: This command lists all the commands used within the current terminal session.

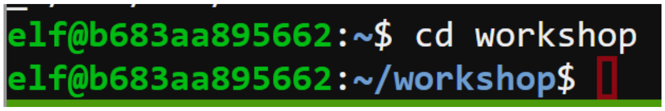
7. **Find the munchkin in your environment variables.**



```
c=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36
:*.xspf=00;36:
TOKENS=
LESSCLOSE=/usr/bin/lesspipe %s %s
LANG=C.UTF-8
HOSTNAME=b683aa895662
GREENSTATUSPREFIX=Lollipops
USER=elf
HHCUSERNAME=prdoolin
PWD=/home/elf
AREA=courtyard
HOME=/home/elf
TMUX=/tmp/tmux-1050/default,17,0
BPUSER=elf
z_MUNCHKIN=munchkin_20249649541603754
LOCATION=17,14
RESOURCE_ID=146aa749-e736-45ce-8de0-9bf2a2e59f32
MAIL=/var/mail/elf
SHELL=/bin/bash
TERM=screen
TMOUT=3600
TMUX_PANE=%2
SHLVL=4
BPUSERHOME=/home/elf
SESSNAME=Munchkin Wrangler
LOGNAME=elf
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/u
sr/local/games:/snap/bin
LESSOPEN=| /usr/bin/lesspipe %s
_=/usr/bin/env
elf@b683aa895662:~$ 
```

Command: env
Explanation: This command displays a list of the current environment.

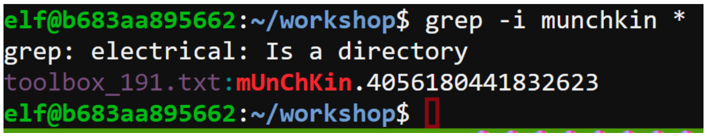
8. **Next, head into the workshop.**



```
elf@b683aa895662:~$ cd workshop
elf@b683aa895662:~/workshop$
```

Command: cd workshop
Explanation: This command changes the current directory to the directory that you designate.

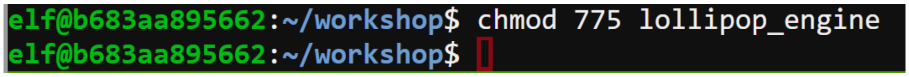
9. **A munchkin is hiding in one of the workshop toolboxes. Use "grep" while ignoring case to find which toolbox the munchkin is in.**



```
elf@b683aa895662:~/workshop$ grep -i munchkin *
grep: electrical: Is a directory
toolbox_191.txt:mUnChKin.4056180441832623
elf@b683aa895662:~/workshop$
```

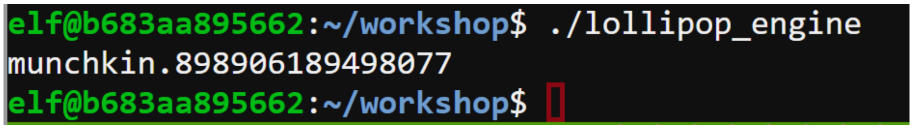
Command: grep -i munchkin *
Explanation: The “grep” command searches the directory for each occurrence of the specified string. The “-i” flag tells the command to ignore the case.

10. **A munchkin is blocking the lollipop_engine from starting. Run the lollipop_engine binary to retrieve this munchkin.**



```
elf@b683aa895662:~/workshop$ chmod 775 lollipop_engine
elf@b683aa895662:~/workshop$
```

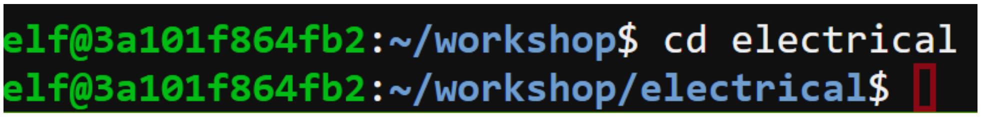
Command: chmod +x lollipop_engine
Explanation: The “chmod” command with the “+x” flag adds the execute permission to the specified file.



```
elf@b683aa895662:~/workshop$ ./lollipop_engine
munchkin.898906189498077
elf@b683aa895662:~/workshop$
```

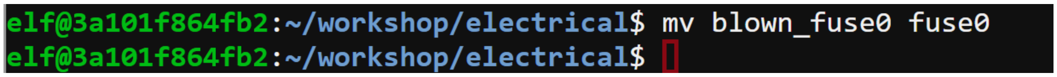
Command: ./lollipop_engine
Explanation: This command executes the specified binary file that is located in the current directory.

11. **Munchkins have blown the fuses in /home/elf/workshop/electrical. cd into electrical and rename blown_fuse0 to fuse0.**



```
elf@3a101f864fb2:~/workshop$ cd electrical
elf@3a101f864fb2:~/workshop/electrical$
```

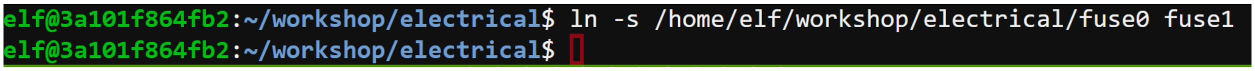
Command: cd electrical
Explanation: This command changes your current directory to the directory that you designate.



```
elf@3a101f864fb2:~/workshop/electrical$ mv blown_fuse0 fuse0
elf@3a101f864fb2:~/workshop/electrical$
```

Command: mv blown_fuse0 fuse0
Explanation: The “mv” command renames a specified file to a new designated name.

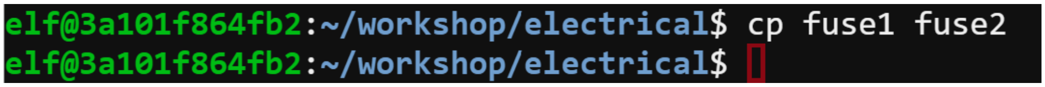
12. Now, make a symbolic link (symlink) named fuse1 that points to fuse0



```
elf@3a101f864fb2:~/workshop/electrical$ ln -s /home/elf/workshop/electrical/fuse0 fuse1
elf@3a101f864fb2:~/workshop/electrical$
```

Command: ln -s /home/elf/workshop/electrical/fuse0 fuse1
Explanation: This command creates new files with the names you specify and links it to the designated file.

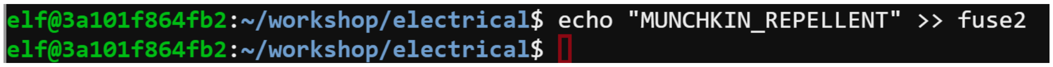
13. Make a copy of fuse1 named fuse2.



```
elf@3a101f864fb2:~/workshop/electrical$ cp fuse1 fuse2
elf@3a101f864fb2:~/workshop/electrical$
```

Command: cp fuse1 fuse2
Explanation: This command creates a copy of the selected file and renames it to the specified name.

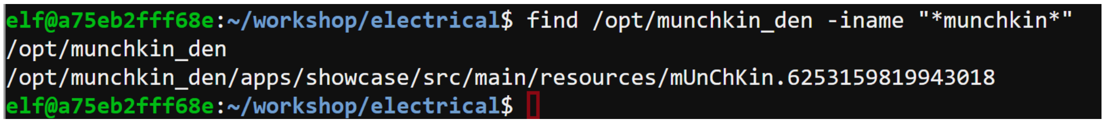
14. We need to make sure munchkins don't come back. Add the characters "MUNCHKIN_REPELLENT" into the file fuse2.



```
elf@3a101f864fb2:~/workshop/electrical$ echo "MUNCHKIN_REPELLENT" >> fuse2
elf@3a101f864fb2:~/workshop/electrical$
```

Command: echo "MUNCHKIN_REPELLENT" >> fuse2
Explanation: This command appends a string to the end of a specified file.

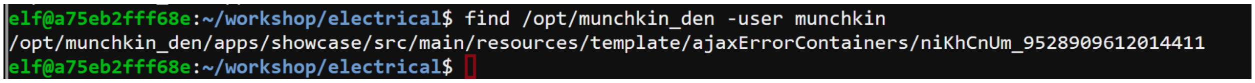
15. Find the munchkin somewhere in /opt/munchkin_den.



```
elf@a75eb2fff68e:~/workshop/electrical$ find /opt/munchkin_den -iname "*munchkin*"
/opt/munchkin_den
/opt/munchkin_den/apps/showcase/src/main/resources/mUnChKin.6253159819943018
elf@a75eb2fff68e:~/workshop/electrical$
```

Command: find /opt/munchkin_den -iname ‘*munchkin*’
Explanation: This command finds the files that have the specified string in their name within the selected directory.

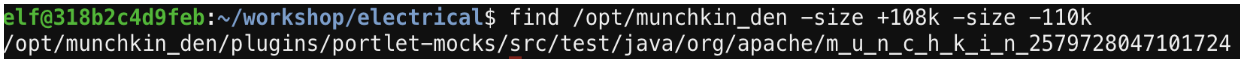
16. Find the file somewhere in /opt/munchkin_den that is owned by the user munchkin.



```
elf@a75eb2fff68e:~/workshop/electrical$ find /opt/munchkin_den -user munchkin
/opt/munchkin_den/apps/showcase/src/main/resources/template/ajaxErrorContainers/niKhCnUm_9528909612014411
elf@a75eb2fff68e:~/workshop/electrical$
```

Command: find /opt/munchkin_den -user munchkin
Explanation: This command looks for a specified user in a selected directory.

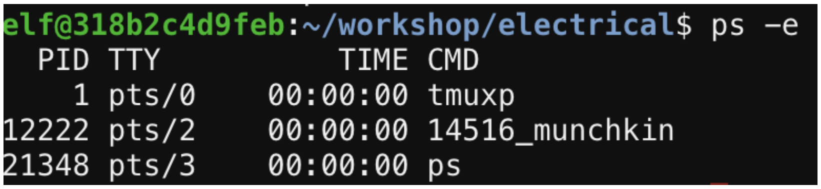
17. **Find the file created by munchkins that is greater than 108 kilobytes and less than 110 kilobytes located somewhere in /opt/munchkin_den.**



```
elf@318b2c4d9feb:~/workshop/electrical$ find /opt/munchkin_den -size +108k -size -110k
/opt/munchkin_den/plugins/portlet-mocks/src/test/java/org/apache/m_u_n_c_h_k_i_n_2579728047101724
```

Command: find /opt/munchkin_den -size +108k -size -110k
Explanation: This command searches for a file between the specified sizes within a selected directory.

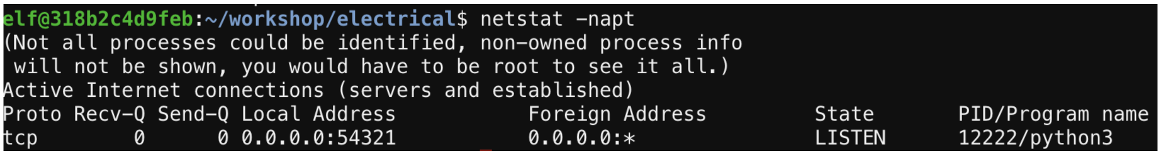
18. **List running processes to find another munchkin.**



```
elf@318b2c4d9feb:~/workshop/electrical$ ps -e
  PID TTY          TIME CMD
    1 pts/0    00:00:00 tmuxp
12222 pts/2    00:00:00 14516_munchkin
21348 pts/3    00:00:00 ps
```

Command: ps -e
Explanation: This command displays all running processes.

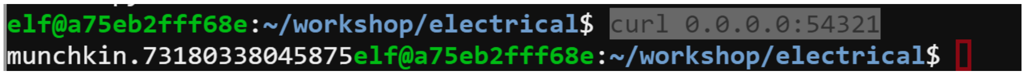
19. **The 14516_munchkin process is listening on a tcp port. Use a command to have the only listening port display to the screen.**



```
elf@318b2c4d9feb:~/workshop/electrical$ netstat -napt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:54321           0.0.0.0:*               LISTEN      12222/python3
```

Command: netstat -napt
Explanation: This command prints out network information. The '-napt' flag displays all of the active TCP ports and the TCP and UDP ports on which the computer is listening.

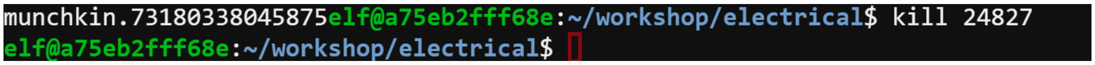
20. **Find the file created by munchkins that is greater than 108 kilobytes and less than 110 kilobytes located somewhere in /opt/munchkin_den. The service listening on port 54321 is an HTTP server. Interact with this server to retrieve the last munchkin.**



```
elf@a75eb2fff68e:~/workshop/electrical$ curl 0.0.0.0:54321
munchkin.73180338045875elf@a75eb2fff68e:~/workshop/electrical$ 
```

Command: curl 0.0.0.0:54321
Explanation: This command enables data transfer over network protocols.

21. **Your final task is to stop the 14516_munchkin process to collect the remaining lollipops.**



```
munchkin.73180338045875elf@a75eb2fff68e:~/workshop/electrical$ kill 24827
elf@a75eb2fff68e:~/workshop/electrical$ 
```

Command: kill 24827

Explanation: This command followed by a PID stops the specified process.

Division of labor:

All of the members of our group completed the lab individually as we all worked on it on our own computers. We made sure each person in the group was on the same step before we advanced any further. We all helped each other with the various steps of the lab and then finished it on our own at home since we did not complete the whole lab in class. Patrick and Isaac Vaillancourt completed the documentation.