Finishing for Linux!

Day6_FinalLinux.md

Recalling

Last Class TOPICS

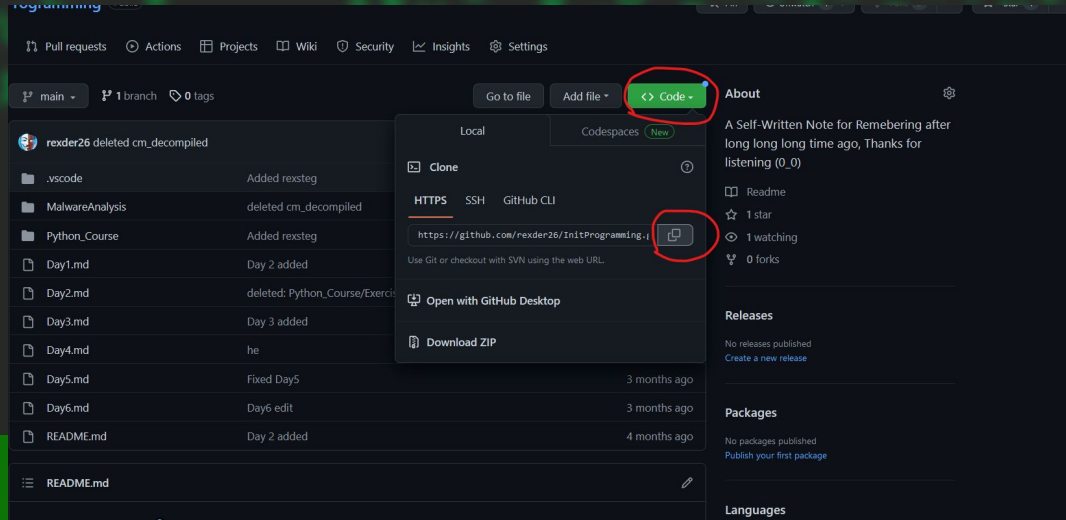
Topics

- Script Installation
- Help on linux
- Linux Services
- Symbolic linking
- alias
- tmux
- Wget
- find

Script installation

- Some hacking tools are developed by some peoples and those peoples make it open-source, that means we can get those scripts/programs from github.
- So we can download and use it. For this purpose git have a feature called ‘clone’
- Syntax
  - `git clone <link_of_the_script_from_github>`

```
┌──(rexder㉿HunterMachine)-[~]
└─$ git clone https://github.com/rexder26/InitProgramming.git
Cloning into 'InitProgramming'...
remote: Enumerating objects: 73, done.
remote: Counting objects: 100% (73/73), done.
remote: Compressing objects: 100% (52/52), done.
remote: Total 73 (delta 26), reused 59 (delta 15), pack-reused 0
Receiving objects: 100% (73/73), 1.52 MiB | 235.00 KiB/s, done.
Resolving deltas: 100% (26/26), done.
```



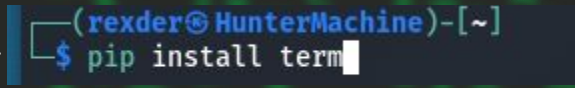
Script modules

- Scripts are made with scripting languages(programming) like

  { python,bash,go,ruby,...}

- So when we use these programming languages to do tasks their is something called modules/libraries these are needed to run the script as the dependencies.
- Example:

1. Python: to install python modules we use -> pip install <modulename>
   i. For requirements file -> `pip install -r requirements.txt`
2. Go: to install go modules -> go install <modulename>
3. Ruby: to install ruby modules -> gem install <modulename>



Python installation

- If pip is not found there will be an error

```
Command 'pip' not found, but can be installed with:
sudo apt install python3-pip
```

- It will install

```
┌──(rexder㉿HunterMachine)-[~]
└─$ pip install term
Defaulting to user installation because normal site-packages is not writeable
Collecting term
  Downloading term-2.4-py2.py3-none-any.whl (7.4 kB)
Installing collected packages: term
Successfully installed term-2.4
```

- If the package is already installed:

```
┌──(rexder㉿HunterMachine)-[~]
└─$ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: adblockparser==0.7 in /usr/lib/python3/dist-pack
ges (from -r requirements.txt (line 1)) (0.7)
Requirement already satisfied: AdvancedHTTPServer==2.2.0 in /usr/lib/python3/di
t-packages (from -r requirements.txt (line 2)) (2.2.0)
```

Go package installation

- Go scripts are scripts made with go-lang(go programming language).
- There are 2 installation methods.
  a. Old version
  b. New version
- Old version
  a. `go get github.com:capotej/groupcache-db-experiment.git`
- New version
  a. Downloading the package `go install github.com/lc/gau/v2/cmd/gau@latest`
  b. Moving the file to /usr/bin(the default download place is `/home/rexder/go/bin`

```
sudo mv filename /usr/bin
```

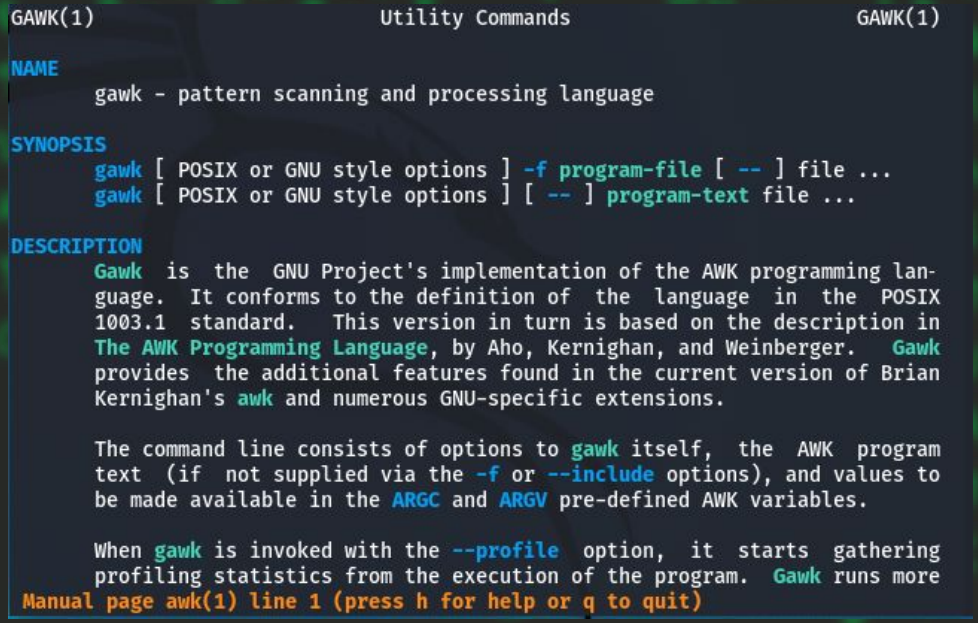
If you need help on linux about commands

You can use

- man (manual)
  - This will give you the whole manual and instruction of a tool or command.
    - `man <yourcommand>`

```
┌──(rexder㉿HunterMachine)-[~]
└─$ man awk
```

Keys: arrow keys for navigation | q for quit



Cont...

- Help
  - Some Commands have help option.
    - `<yourcommand> -h`
    - `<yourcommand> -help`
    - `<yourcommand> - -help`

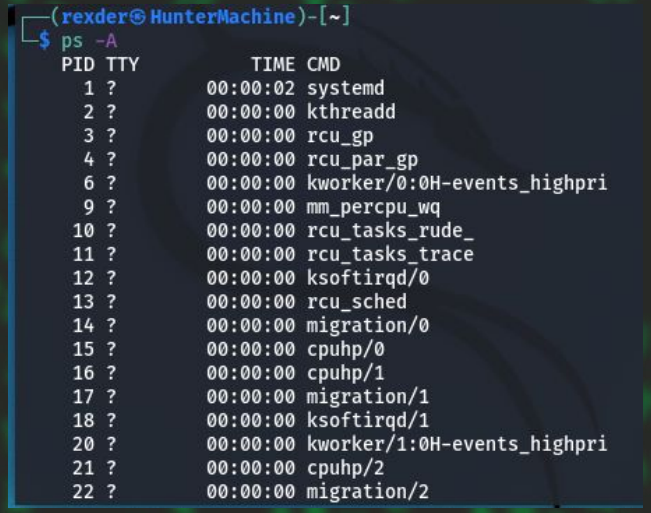
```
┌──(rexder㉿HunterMachine)-[~]
└─$ awk -help
Usage: awk [POSIX or GNU style options] -f progfile [--] file ...
Usage: awk [POSIX or GNU style options] [--] 'program' file ...
POSIX options:          GNU long options: (standard)
        -f progfile             --file=progfile
        -F fs                   --field-separator=fs
        -v var=val              --assign=var=val
Short options:          GNU long options: (extensions)
        -b                      --characters-as-bytes
        -c                      --traditional
        -C                      --copyright
        -d[file]                --dump-variables[=file]
        -D[file]                --debug[=file]
        -e 'program-text'       --source='program-text'
        -E file                 --exec=file
        -g                      --gen-pot
        -h                      --help
        -i includefile          --include=includefile
        -l library              --load=library
        -L[fatal|invalid|no-ext]        --lint[=fatal|invalid|no-ext]
        -M                      --bignum
        -N                      --use-lc-numeric
```

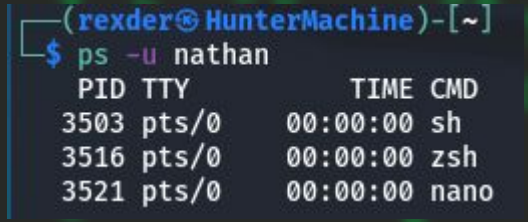
Break time

1. Download and run the python script from this github
    a. https://github.com/aboul3la/Sublist3r
2. Download and test this go project
    a. https://github.com/lc/gau
3. What is the tr command on linux?
4. What is the option for the ping command that can “use <size> as number of data bytes to be sent”

Linux Processes & Services

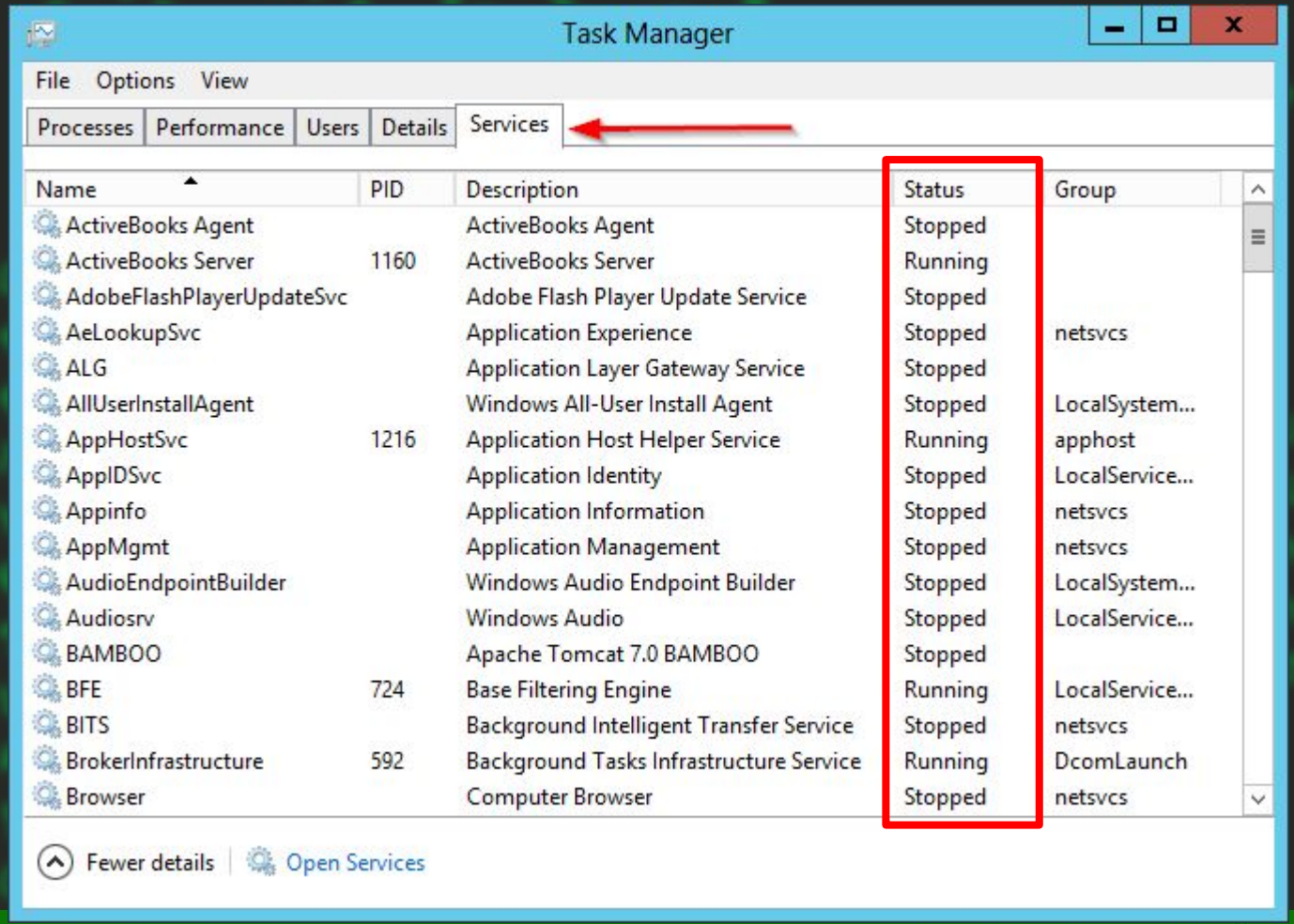
- Terms
  - Processes: Running instances of programs.
    - When you execute a program like opening a text editor, running a command, or starting a web browser, Linux loads that program into memory and starts it as a process.
  - Services: Background programs that start automatically or manually, often for system tasks (also known as daemons).
    - A Service that runs to gather any change on the system or to count time runs on Background.
- To get the processes running:
  - `ps [options]`
- More commands
  - ps -> for process running on my shell
  - ps -A -> view all running process
  - ps -u username -> view users process





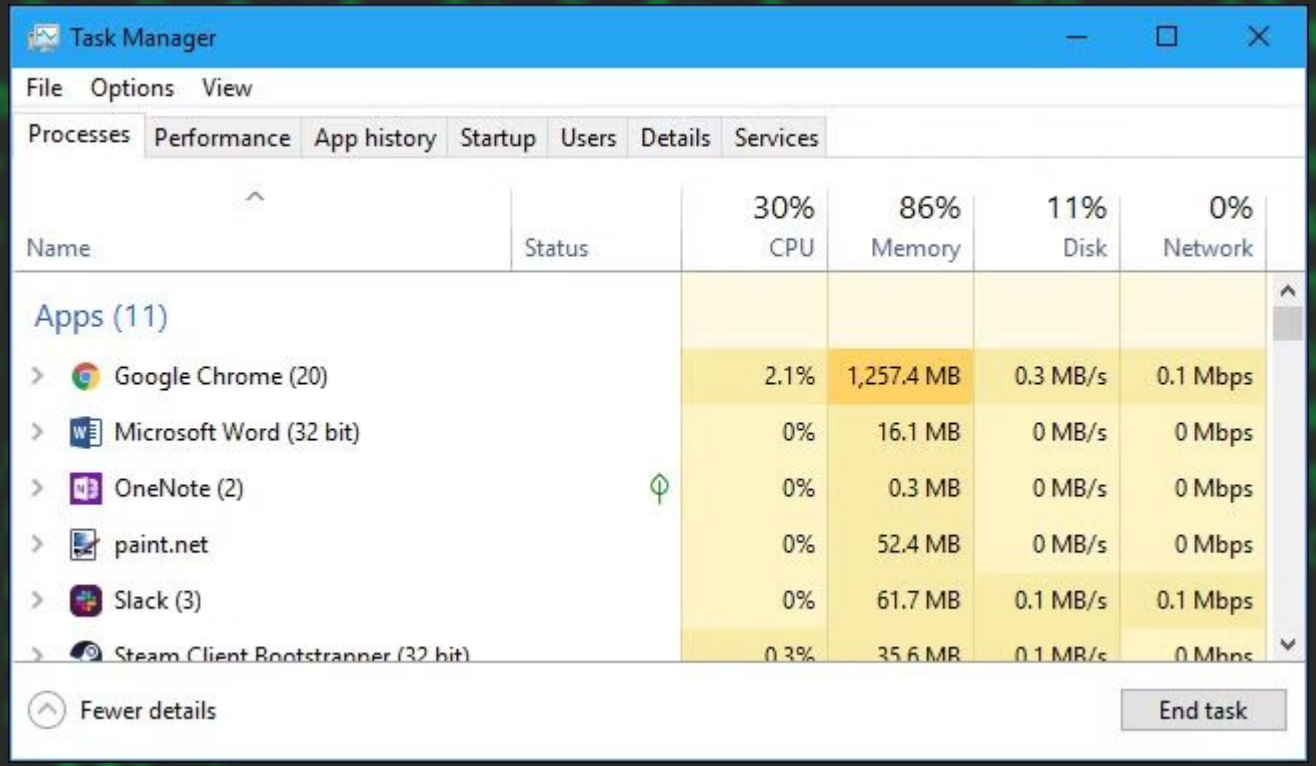
Service

These are windows services.



Processes.

Processes on Windows.



Managing Processes.

```
~ > $ kill -l
HUP INT QUIT ILL TRAP ABRT BUS FPE KILL USR1 SEGV USR2 PIPE ALRM TERM STKFLT
CHLD CONT STOP TSTP TTIN TTOU URG XCPU XFSZ VTALRM PROF WINCH POLL PWR SYS
```

- To stop process
  - kill [options] [PID]
  - killall [programname]
- More on kill
  - kill -19 PID -> to stop the process
  - kill -18 PID -> to resume the process we stopped
  - kill -9 PID -> to Stop a process immediately
  - … there are 31 options.
- PID: Process ID
- PPID: Parent Process ID

```
┌──(rexder㉿HunterMachine)-[~]
└─$ kill -9 3841
```

```
~ > $ killall picom
~ > $
```

Let’s test it!

You love it?

- This is a time Taking an not realtime.
- For Real Time we have the tool called 'top' installed on linux by default.
- But to make this fun we will use 'htop', it is colorful and more enhanced!

```
top - 08:49:20 up  4:22,  1 user,  load average: 0.05, 0.08, 0.07
Tasks: 194 total,   1 running, 192 sleeping,   1 stopped,   0 zombie
%Cpu(s):  3.5 us,  0.7 sy,  0.0 ni, 95.7 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :  10024.9 total,   8008.5 free,   1082.1 used,    934.3 buff/cache
MiB Swap:    976.0 total,    976.0 free,      0.0 used.   8687.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1478 rexder    20   0 5085600 392876 129728 S  12.3   3.8   0:46.71 gnome-s+
   1204 rexder    20   0 1157208  75424  46784 S   2.3   0.7   0:10.71 Xorg
   2035 rexder    20   0  433572  71808  39176 S   0.7   0.7   0:04.10 gnome-t+
   1548 rexder    20   0  167184   6964   6264 S   0.3   0.1   0:00.11 at-spi2+
   1620 rexder    20   0 1152360  53784  21700 S   0.3   0.5   0:01.16 gsd-med+
   4169 rexder    20   0   10092   3652   3168 R   0.3   0.0   0:00.01 top
      1 root      20   0  164052  10576   7872 S   0.0   0.1   0:02.02 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par+
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.05 ksoftir+
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.39 rcu_sch+
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.18 migrati+
```

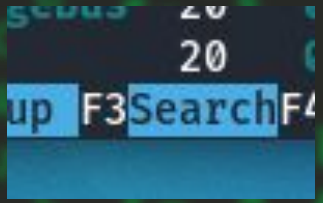
- top -

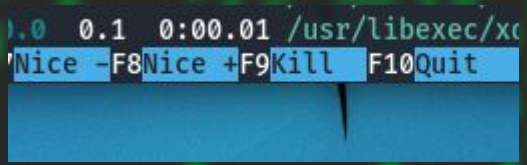
```
  0[|                                    5.3%] Tasks: 107, 252 thr, 84 kthr; 1 runnin
  1[|                                    3.9%] Load average: 0.23 0.19 0.13
  2[|                                    6.7%] Uptime: 04:31:35
  3[|                                    4.6%]
Mem[|||||||||                      1.08G/9.79G]
Swp[                                     0K/976M]

  Main   I/O
    PID USER       PRI  NI  VIRT   RES   SHR S CPU%▽MEM%   TIME+  Command
   1478 rexder      20   0 5104M  390M  128M S 15.2  3.9  1:02.97 /usr/bin/gnom
   1504 rexder      20   0 5104M  390M  128M S  3.3  3.9  0:08.43 /usr/bin/gnom
   1506 rexder      20   0 5104M  390M  128M S  3.3  3.9  0:08.82 /usr/bin/gnom
   1507 rexder      20   0 5104M  390M  128M S  3.3  3.9  0:08.78 /usr/bin/gnom
   1204 rexder      20   0 1133M 78456 48372 S  2.6  0.8  0:15.39 /usr/lib/xorg
   1505 rexder      20   0 5104M  390M  128M S  2.6  3.9  0:08.53 /usr/bin/gnom
   1250 rexder      20   0 1133M 78456 48372 S  0.7  0.8  0:01.83 /usr/lib/xorg
   1386 rexder      20   0  213M  2984  2524 S  0.7  0.0  0:25.18 /usr/bin/VBox
   2035 rexder      20   0  423M 72932 40276 S  0.7  0.7  0:06.62 /usr/libexec/
   5637 rexder      20   0  8196  4476  3428 R  0.7  0.0  0:00.05 htop
      1 root        20   0 16428  9660  7384 S  0.0  0.1  0:02.25 /lib/systemd/
    260 root        20   0 71448 25912 24448 S  0.0  0.3  0:00.60 /lib/systemd/
    280 root        20   0 22676  5840  4072 S  0.0  0.1  0:00.17 /lib/systemd/
F1Help  F2Setup F3Search F4Filter F5Tree  F6SortBy F7Nice -F8Nice +F9Kill  F10Quit
```

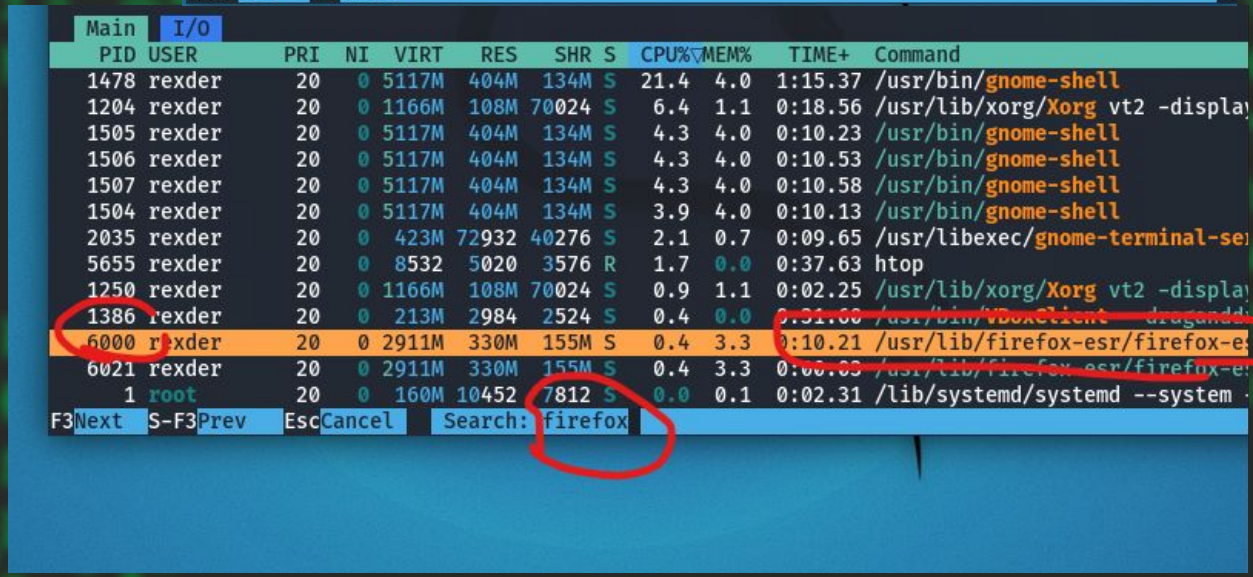
- htop -

To kill on htop

1. Search for the process
2. Choose SGNKILL(9) and kill it!

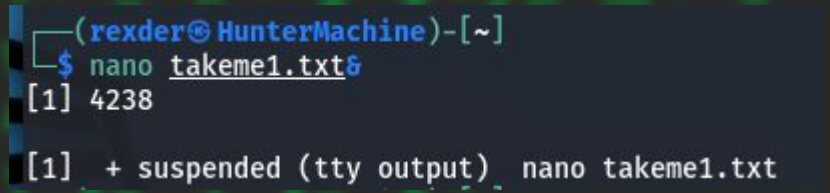




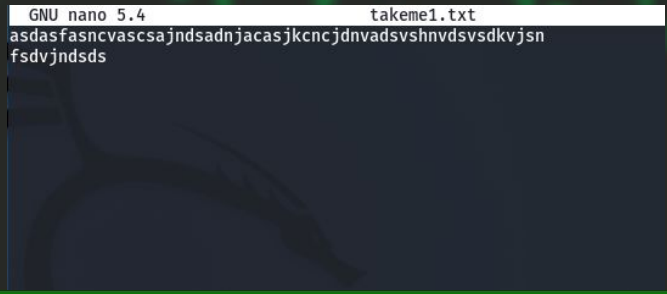


Foreground / background

- Thus far, we have run commands at the prompt and waited for them to complete. We call this running in the "**foreground**."
- Use the "**&**" operator, to run programs in the "**background**" or press ^Z



- To get the background process back to foreground
  - Fg



To stop a process going inside your shell just press ^C

Managing Services.

```
~ > $ sudo systemctl start apache2
~ > $
```

- Services Can be Started and Stopped.
- We will See different hacking Services for the future classes.
- To manage Services We can use tools called `systemctl` or `service`
- Syntax
  - sudo systemctl start <ServiceName> - Start the service
    - sudo systemctl stop <ServiceName> - Stop the service
    - sudo systemctl status <ServiceName> - to check status of the service
    - sudo systemctl enable <ServiceName> - to Make it start service when the Computer boots.
    - sudo systemctl disable <ServiceName> - to Make it stop the service from running when the Computer boots.
  - sudo service <ServiceName> start
    - sudo service <ServiceName> stop

Do you remember the redirecting thing on linux or the > sign?

Null device

- /dev/null - Redirects output to nowhere.
- If you want to ignore output, you can send it to the null device, `/dev/null`.
- The null device is a special file that throws away whatever is fed to it.
- You may hear people refer to it as the bit bucket.
- If you do not want to see errors on your screen and you do not want to save them to a file, you can redirect them to `/dev/null`
- On shell output there are 2 things.
  - STDERR = 2
  - STDOUT = 1
- To redirect the errors from a command result we do
  - command 2> filename => here if you check the file you saved on it have errors only
- To redirect the error-FREE output
  - command 1>filename
- So if we redirect our commands output to /dev/null we will get error free result
  - command 2> /dev/null

COnt...

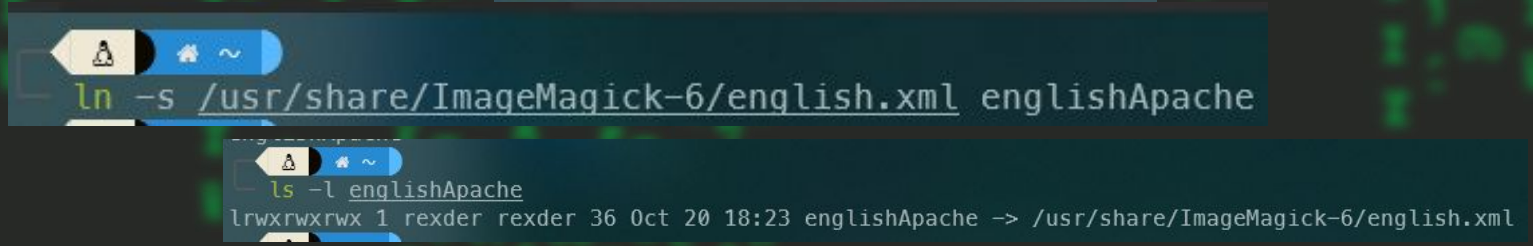
```
┌──(rexder㉿HunterMachine)-[~]
└─$ ls Hello
ls: cannot access 'Hello': No such file or directory
```

```
┌──(rexder㉿HunterMachine)-[~]
└─$ ls Hello 2> stderr.txt

┌──(rexder㉿HunterMachine)-[~]
└─$ cat stderr.txt
ls: cannot access 'Hello': No such file or directory
```

```
┌──(rexder㉿HunterMachine)-[~]
└─$ ls Hello 1> stdout.txt
ls: cannot access 'Hello': No such file or directory

┌──(rexder㉿HunterMachine)-[~]
└─$ cat stdout.txt
```

Symbolic linking

- Symbolic linking is same as Windows shortcut.
- Symbolic linking is a process of creating a linked shortcut form of file to some pre-existed file or folder.
- For example: you can create program is some file and to create a shortcut format of that file you will use symbolic linkin.
- Also if a file path is too long we can create a symbolic linking.
- Symbolic linked files shows ‘l’ in listing of ls command. Also there will be a ‘->’ to show the linked file.
- Syntax: `ln -s source_filePATH myfilename`



alias

- Used to give a name to some bunch of commands.
- Example: if i wanted to name ls -la ‘rex so any time i want to get output of ls -la i just type rex
  - alias rex=’ls -la’
- But this doesn’t work after you closed the terminal
- If you want to make it work…
  - You will add it to your shell config file
- Example for bash and fish, zsh…

```
┌──(rexder㉿HunterMachine)-[~]
└─$ alias rex='ls -la --color'

┌──(rexder㉿HunterMachine)-[~]
└─$ rex
total 176
drwxr-xr-x 19 rexder rexder  4096 Dec 23 10:31 .
drwxr-xr-x  6 root   root    4096 Dec 21 12:39 ..
-rw-------  1 rexder rexder    23 Dec 23 08:23 .bash_history
-rw-r--r--  1 rexder rexder   220 Dec  6 02:48 .bash_logout
-rw-r--r--  1 rexder rexder  5349 Dec  6 02:48 .bashrc
-rw-r--r--  1 rexder rexder  3526 Dec  6 02:48 .bashrc.original
drwx------ 22 rexder rexder  4096 Dec 23 05:16 .cache
drwx------ 21 rexder rexder  4096 Dec 23 08:58 .config
-rw-r--r--  1 rexder rexder   224 Dec 19 12:30 Day4_MoreLinux.md
drwxr-xr-x  2 rexder rexder  4096 Dec 16 02:32 Desktop
drwxr-xr-x  2 rexder rexder  4096 Dec 16 07:32 Documents
drwxr-xr-x  2 rexder rexder  4096 Dec 16 05:00 Downloads
-rw-r--r--  1 rexder rexder 11759 Dec  6 02:48 .face
lrwxrwxrwx  1 rexder rexder     5 Dec  6 02:48 .face.icon -> .face
-rw-r--r--  1 rexder rexder   278 Dec 16 02:42 .gtkrc-2.0
```

```
GNU nano 7.2                                    .bashrc

# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36

# some more ls aliases
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'
```

```
GNU nano 7.2                                    .zshrc
#lolcat .
#tmux
cowsay "Hello Nati, Welcome Back" | lolcat
#figlet HackTime
alias hackerone="cd ~/Projects/Pentests/H1"
alias ethio="cd ~/Projects/Pentests/Local"
alias tools="cd ~/tools"
```

```
GNU nano 7.2                          .config/fish/config.fish
if status is-interactive
    # Commands to run in interactive sessions can go here
tmux
cowsay "Hello Nati, Welcome Back" | lolcat
#figlet HackTime
alias hack="cd ~/Projects/Pentests/"
alias tools="cd ~/tools"
end
```

- Bash = ~/.bashrc
- Zsh = ~/.zshrc
- Fish = ~/.config/fish/config.fish

```
~/GTSTv1 > $ bounty
/m/P/B/Global > $
```

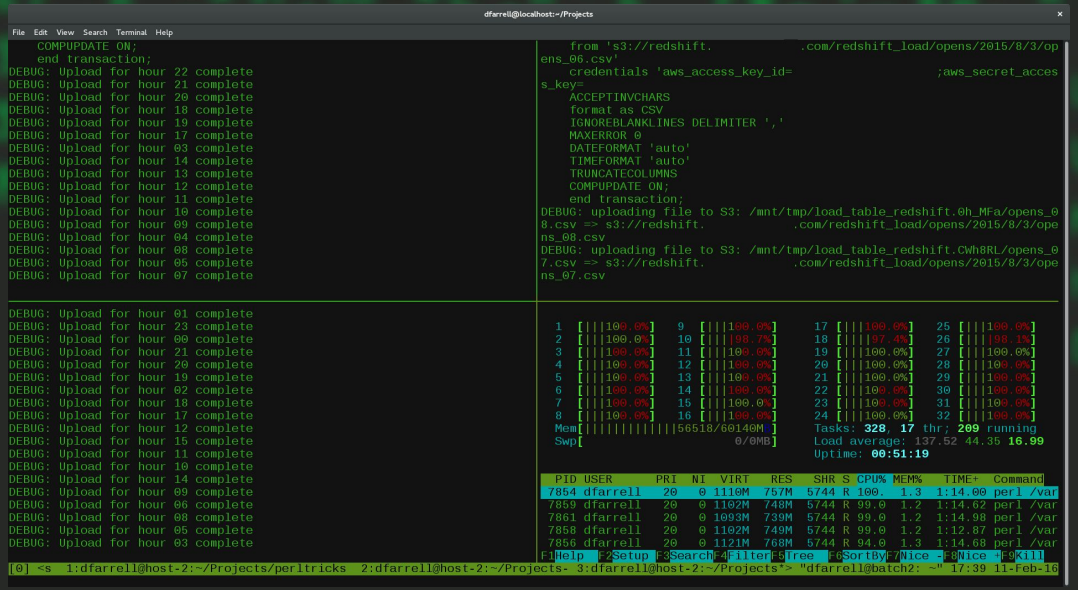
GTST - GeezTech Security Tester®

by Nathan Hailu

Whats Up, Hacker!

Tmux - Terminal Multiplexer

- Tmux is used to classify our terminal work.
- You can install it using apt. On kali it is built-in Then to start it just type ‘tmux’
- To Create config file type
  - nano .tmux.conf
  - Type this
    - unbind C-b
    - unbind l
    - set -g prefix C-a
    - unbind %
    - bind e split-window -h
    - bind o split-window -v
    - set -g base-index 1
    - setw -g pane-base-index 1
  - Save it | exit tmux and open again



Cont...

- To split horizontally
  - ^A then o
- To split vertically
  - ^A then e
- To exit
  - ^A then x or
  - just type ‘exit’

- To create tab
  - ^A then c
- To rename the tab
  - ^A then ,(comma)
- To switch tabs
  - ^A then <numbers>
  - TO switch partitions
    - ^A then <arrow>
- … for more you can google but be aware of our super key is ^A

Let’s test it!

Wget

- Is a tool used to download files from websites/servers
- Syntax
  - wget [options] [link]
- wget https://tldp.org/LDP/intro-linux/intro-linux.pdf

```
┌──(rexder㉿HunterMachine)-[~]
└─$ wget https://tldp.org/LDP/intro-linux/intro-linux.pdf
--2022-12-23 12:32:40--  https://tldp.org/LDP/intro-linux/intro-linux.pdf
Resolving tldp.org (tldp.org)... 152.19.134.152, 152.19.134.151
Connecting to tldp.org (tldp.org)|152.19.134.152|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1600364 (1.5M) [application/pdf]
Saving to: ‘intro-linux.pdf’

intro-linux.pdf             100%[=========================================>]   1.53M  17.4KB/s

2022-12-23 12:34:11 (18.3 KB/s) - ‘intro-linux.pdf’ saved [1600364/1600364]
```

find

- ON terminal if you want to search for files/folders/musics/videos, we can use find command.
- It is very essential tool
- Syntax:
  - find [search path] [options] [search word]

- More commands
  - find / -name “linux”
  - find /home -perm 777
  - find -type f | find -type d
  - find / -type f -perm /4000

Lets see

Break time

1. open firefox on your computer
2. What is the PID
3. Kill firefox
4. Login as gtst
5. Open nano with filename help.txt
6. Make it background process
7. Log back to your own user account
8. List the process of user gtst
9. Try tmux and configure it

Linux is OVER!

LINUX IS FUN! Isn't it?

Next Class we will Start our "Python programming for hackers" class

1) DO the github push
2) Please, study the commands again and again until you are god on it
    a) Hacker with poor linux skill is skid, so bedenb temaru