

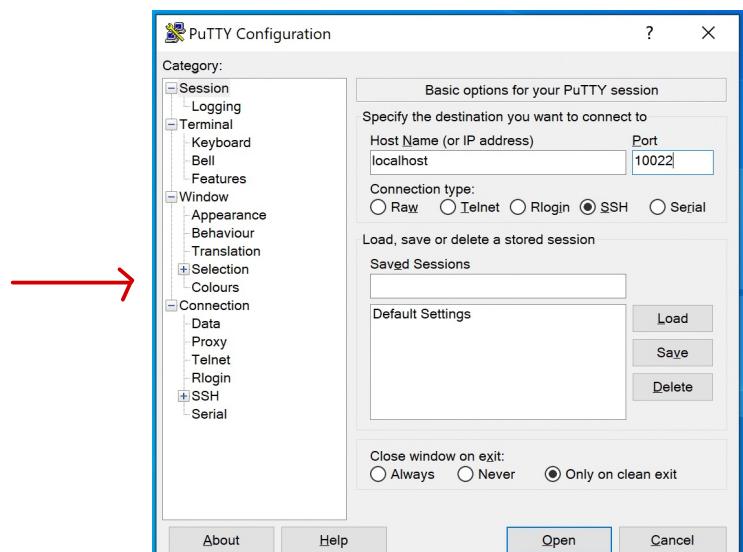
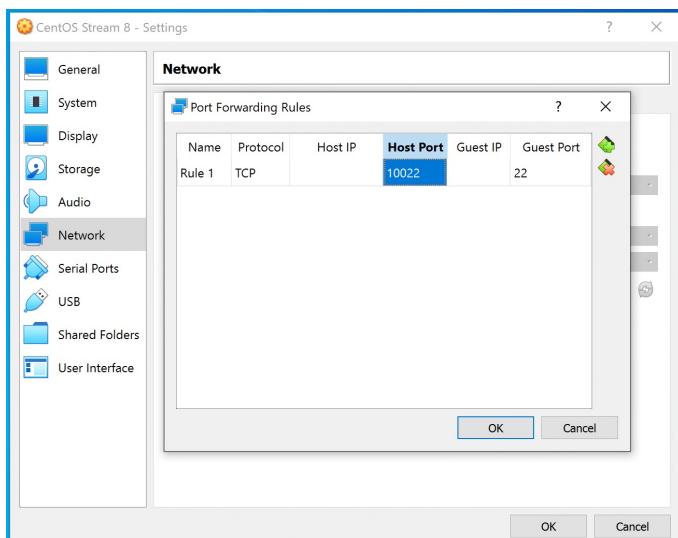
IT SECURITY

VEER SINGH

WEEK 1

9 Feb 2021

- Virtual Box → Linux
 - Putty → Full installer
 - CentOS Stream 8.ova
- To make the virtual machine:
① Oracle VM VirtualBox
② Import
③ Choose the downloaded CentOS Stream 8.ova file
④ Don't change any settings
- Username → root
 - password → INBMA0634L
- Putty to connect remotely with SSH:
① Enable network in VM
② Machine → Settings → Network
③ Advanced → Port Forwarding → "Add" {Protocol = TCP}
④ Guest Port → 22
⑤ Host Port → 10022
⑥ OK → OK
⑦ Virtual Machine → Start → Headless start
⑧ In Putty → Host name → localhost
→ Port → 10022
⑨ Open → login using same root credentials



→ Continue with "Week1 Commands.txt"

WEEK 2

16 Feb 2021

- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with "Week2 Commands .txt"

Linux File Structure

.n	Name	Size	Modify time
~bin		7	May 18 2020
/boot		4096	Feb 7 08:39
/dev		2960	Apr 12 04:41
/etc		8192	Apr 12 04:41
/home		6	May 18 2020
~lib		7	May 18 2020
~lib64		9	May 18 2020
/media		6	May 18 2020
/mnt		6	May 18 2020
/opt		6	May 18 2020
/proc		0	Apr 12 04:41
/root		194	Apr 12 04:48
/run		660	Apr 12 04:41
~sbin		8	May 18 2020
/srv		6	May 18 2020
/sys		0	Apr 12 04:41
/tmp		85	Apr 12 04:42
/usr		144	Feb 7 08:27
/var		278	Feb 7 08:39

- ① /bin → Contains essential user binaries
- ② /boot → files needed to boot the system
- ③ /dev → device files, there are not actually files but are represented as files like SATA drive
- ④ /etc → Configuration files that can be edited in a text editor.
- ⑤ /home → Contains a home folder for each user.
Contains user data files and user specific configuration files. Other users can't modify other users files.
- ⑥ /lib → Contains libraries needed by essential binaries in /bin and /sbin
- ⑦ /lib64 → 64 bit library files
- ⑧ /media → Directories for removable media like USB drives are mounted here
- ⑨ /mnt → temporary mount points
- ⑩ /opt → optional packages for optional software

- ⑪ /proc → Special files which contain kernel and process files
- ⑫ /root → home directory of the root user
- ⑬ /run → gives applications a standard place to store transient files like sockets and process IDs
- ⑭ /sbin → System administration binaries
- ⑮ /srv → Contains data for services provided by the system
- ⑯ /sys → Data about the system and its components like attached hardware
- ⑰ /tmp → Temporary files stored by applications which are then deleted
- ⑱ /usr → User binaries and read only data, applications and files of a user
- ⑲ /var → Variable data files, writable counterpart to /usr like log files

```
[root@localhost /]# ls -ld  
dr-xr-xr-x. 17 root root 224 Feb 7 08:27 .  
[root@localhost /]#
```

- first 3 alpha d → permissions for root user
- middle 3 alpha d → permissions for users who are member of root group
- last 3 alpha d → permissions for others

WEEK 3

23 Feb 2021

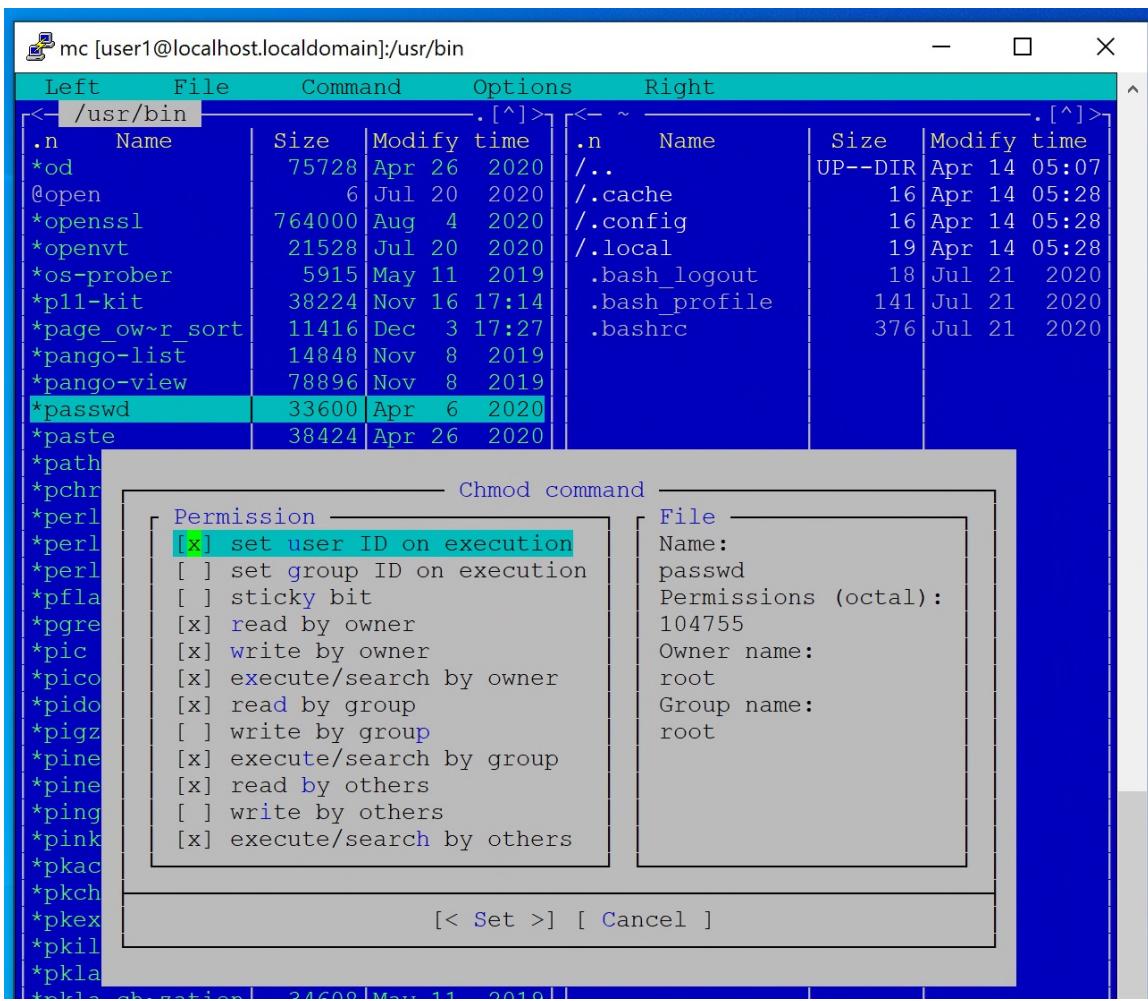
- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with "Week3 Commands .txt"

WEEK 4

2 March 2021

- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with "Week3 Commands .txt"

→ Permission vector in MC GUI



WEEK 5

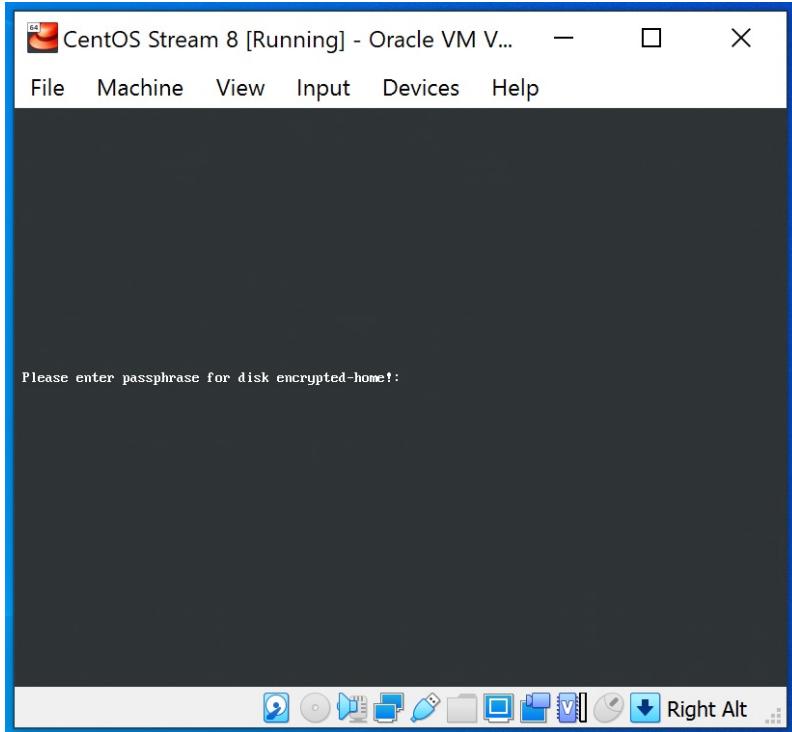
8 March 2021

- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with "Week 5 Commands .txt"

→ Edits made to the crypttab file

```
root@localhost:~  
crypttab      [---] 0 L:[ 1+ 1 2/ 2] *(35  
encrypted-home<>/dev/sda4<---->none<-->luks
```

→ VM asks for password



→ Edits made to the fstab file

BEFORE

```
root@localhost:~  
fstab      [---] 0 L:[ 1+14 15/ 15] *(615 / 615b) <EOF> [*] [X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
#  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93cbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults  
UUID=fbad58d-15f1-470b-a592-2a27be1fc0 /home xfs defaults  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults
```

AFTER

```
root@localhost:~  
fstab      [---] 41 L:[ 1+12 13/ 15] *(468 / 616b) 0032 0x020 [*] [X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
#  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93cbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults  
UUID=0dc3cf8e-e83c-434d-8649-e7a98cbc432d /home ext2 defaults  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults
```

→ Edits made to the fstab file

BEFORE

```
root@localhost:~  
fstab [----] 0 L:[ 1+14 15/ 15 ] *(616 / 616b) <EOF> [*][X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults  
UUID=0dc3cfc8e-e83c-434d-8e49-e7a98cbc432d /home ext2 defaults  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults  
  
1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

AFTER

```
root@localhost:~  
fstab [-M--] 69 L:[ 1+12 13/ 15 ] *(496 / 615b) 0032 0x020 [*][X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults  
UUID=ae5e2a96-b54c-4a90-a56d-1bc3c7bd1ee3 /home ext2 defaults  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults  
  
1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

→ Edits made to the crypttab file

```
root@localhost:~  
crypttab [-M--] 8 L:[ 1+ 0 1/ 2 ]  
enc-home<----->/dev/sda4<----->/key<-->luks
```

→ Additions made to the fstab file

Before

```
root@localhost:~  
fstab [----] 11 L:[ 1+ 2 3/ 15 ] *(14 / 615b) 0098 0x062 [*][X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults 0 0  
UUID=ae5e2a96-b54c-4a90-a56d-1bc3c7bd1ee3 /home xfs defaults 0 0  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults 0 0  
  
1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

After

```
root@localhost:~  
fstab [-M--] 93 L:[ 1+14 15/ 16 ] *(708 / 710b) 0032 0x020 [*][X]  
  
# /etc/fstab  
# Created by anaconda on Sun Feb 7 13:26:14 2021  
  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
  
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults 0 0  
UUID=ae5e2a96-b54c-4a90-a56d-1bc3c7bd1ee3 /home xfs defaults 0 0  
UUID=55aff839-efa7-4a73-88ce-2d5d809881ed none swap defaults 0 0  
UUID=0f50bcac-88bc-4f94-91f9-fce7fb5661b3 /keys ext2 defaults 0 0  
  
1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

→ Additions made to the fstab file

```
root@localhost:~ [-M--] 89 L:[ 1+14 15/ 16] *(711 / 724b) 0032 0x020 [*] [X] ^

#
# /etc/fstab
# Created by anaconda on Sun Feb 7 13:26:14 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults 0 0
UUID=ae5e2a96-b54c-4a90-a56d-1bc3c7bd1ee3 /home xfs defaults,nofail 0 0
UUID=55afff839-efa7-4a73-88ce-2d5d809881ed none swap defaults 0 0
UUID=0f50bca1-88bc-4f94-91f9-fce7fb5661b3 /keys ext2 defaults,nofail 0 0.

1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

WEEK 6

15 March 2021

→ No class, holiday

WEEK 7

22 March 2021

- make a new install
- configure network for ssh
- Continue with "Week 7 Commands .txt"

→ Changes to the fstab file

```
root@localhost:~ [-M--] 89 L:[ 1+14 15/ 16] *(711 / 724b) 0032 0x020 [*] [X] ^

#
# /etc/fstab
# Created by anaconda on Sun Feb 7 13:26:14 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=93dcbd06-65d9-4036-b9f3-1bf7829ea5a8 / xfs defaults 0 0
UUID=40b5f46d-7564-4a91-a5fa-38a70f1f9fff /home xfs defaults,nofail 0 0
UUID=55afff839-efa7-4a73-88ce-2d5d809881ed none swap defaults 0 0
UUID=f8f738dd-ace8-4918-9ad3-b3fle3f2a50a /keys ext2 defaults,nofail,ro 0 0
~
```

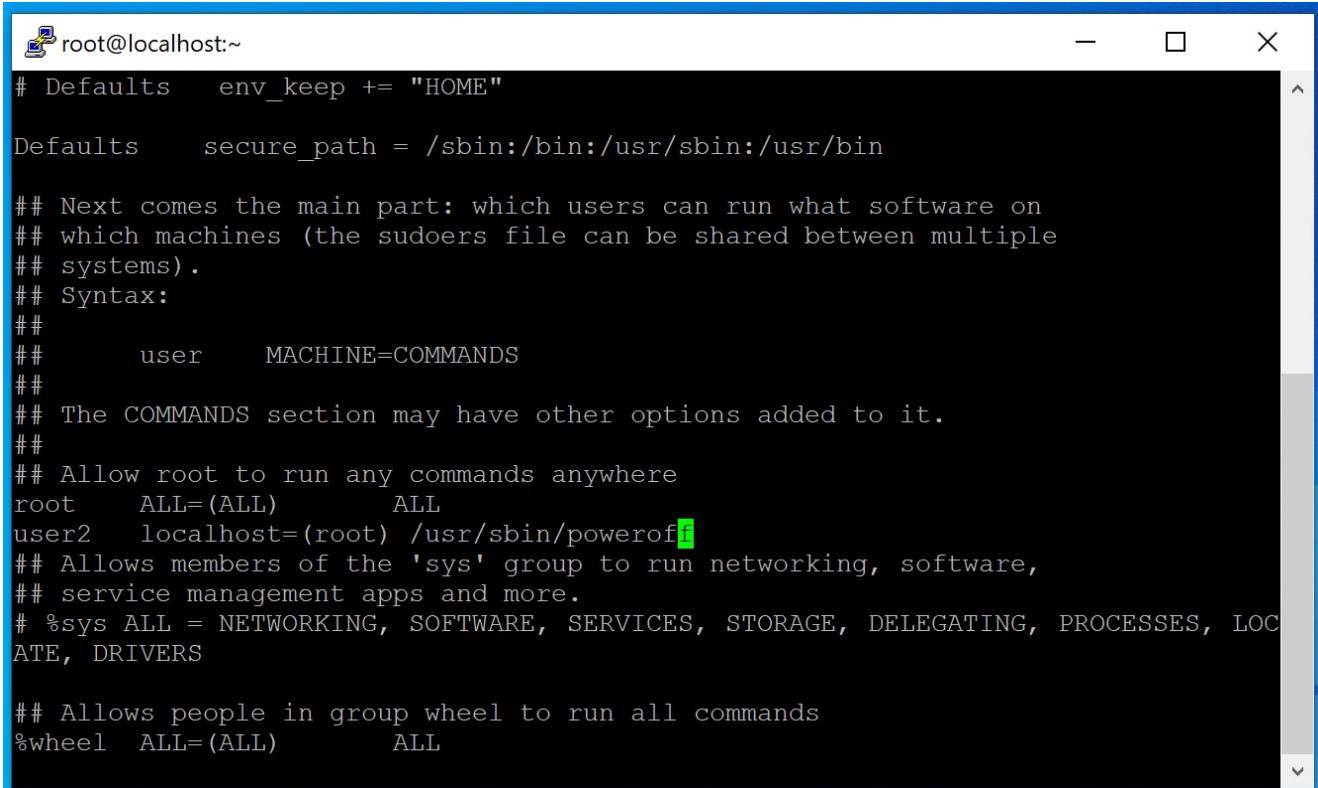
→ Additions to the crypttab file

root@localhost:~

```
home /dev/sda2 /keys/home.key luks
```

~

→ Changes to visudo



```
# Defaults env_keep += "HOME"

Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##       user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)      ALL
user2   localhost=(root) /usr/sbin/poweroff
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS

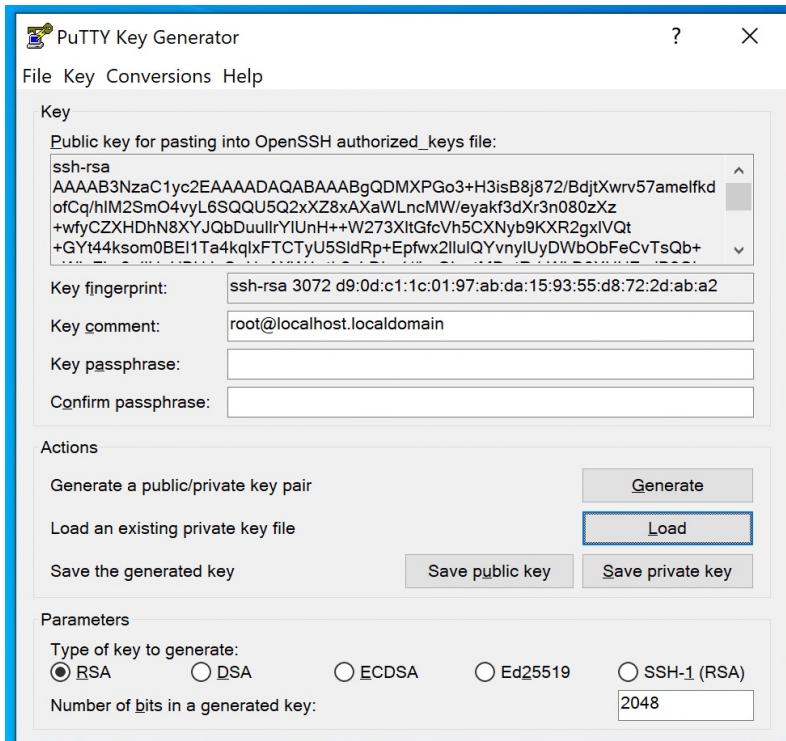
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)      ALL
```

WEEK 8

29 March 2021

- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with " Week 8 Commands .txt "

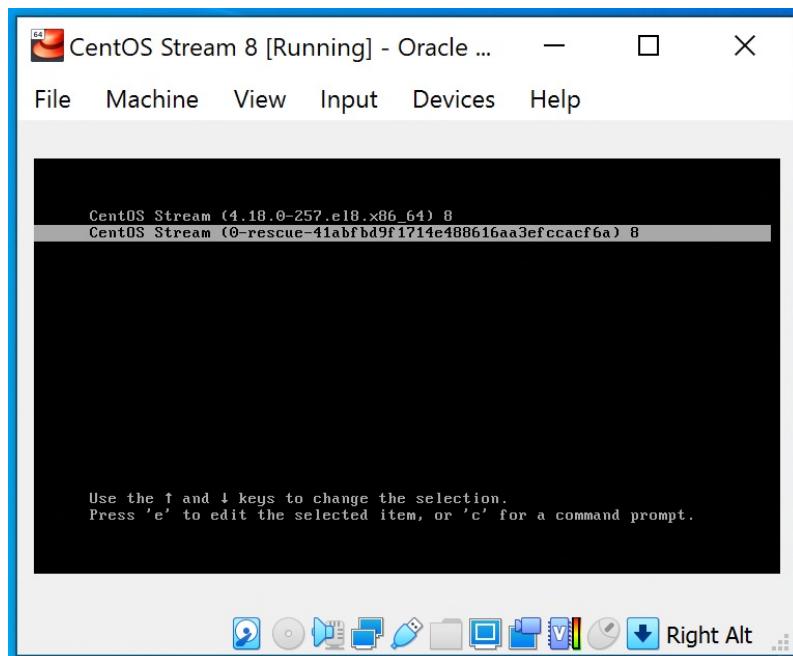
→ Putty gen



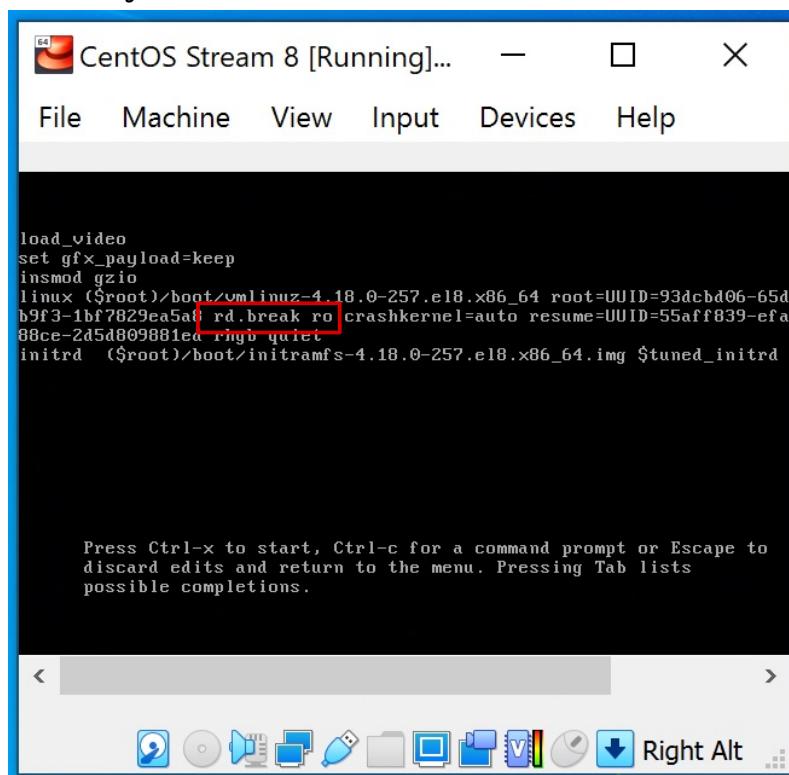
→ private Key



→ Options on boot up



→ Changes made to the file



→ We are able to access the machine

```
[ 18.344954] [drm:vmw_host_log [vmwgfx]] >ERROR= Failed to send host log message.  
Generating "/run/initramfs/rdsosreport.txt"  
  
Entering emergency mode. Exit the shell to continue.  
Type "journalctl" to view system logs.  
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot  
after mounting them and attach it to a bug report.  
  
switch_root:/# ls -la  
total 12  
drwxr-xr-x 13 root root 0 Apr 18 11:36 .  
drwxr-xr-x 13 root root 0 Apr 18 11:36 ..  
-rw-r--r-- 1 root root 0 Apr 18 11:36 console_lock  
lrwxrwxrwx 1 root root 7 Aug 11 2020 bin --> usr/bin  
drwxr-xr-x 14 root root 2580 Apr 18 11:36 dev  
-rw-r--r-- 1 root root 589 Apr 18 11:36 dracut-state.sh  
-rw-r--r-- 1 root root 2 Aug 11 2020 early_cpio  
drwxr-xr-x 10 root root 0 Apr 18 11:36 etc  
lrwxrwxrwx 1 root root 23 Aug 11 2020 init --> usr/lib/systemd/systemd  
drwxr-xr-x 3 root root 0 Aug 11 2020 kernel  
lrwxrwxrwx 1 root root 7 Aug 11 2020 lib --> usr/lib  
lrwxrwxrwx 1 root root 9 Aug 11 2020 lib64 --> usr/lib64  
drwxr-xr-x 82 root root 0 Apr 18 11:37 proc  
drwxr-xr-x 2 root root 0 Aug 11 2020 root  
drwxr-xr-x 14 root root 300 Apr 18 11:36 run  
lrwxrwxrwx 1 root root 8 Aug 11 2020 sbin --> usr/sbin  
-rwxr--r-- 1 root root 3126 Oct 8 2018 shutdown  
drwxr-xr-x 13 root root 0 Apr 18 11:36 sys  
drwxr-xr-x 17 root root 224 Feb 7 13:27 sysroot  
drwxr-xr-x 4 root root 0 Apr 18 11:36 tmp  
drwxr-xr-x 0 root root 0 Aug 11 2020 usr  
drwxr-xr-x 5 root root 0 Apr 18 11:36 var  
switch_root:/# _
```

WEEK 9

Spring break Holiday

WEEK 10

12 April 2021

- make a new install
- configure network for ssh
- headless start
- Connect with Putty
- Continue with "Week 5 Commands .txt"