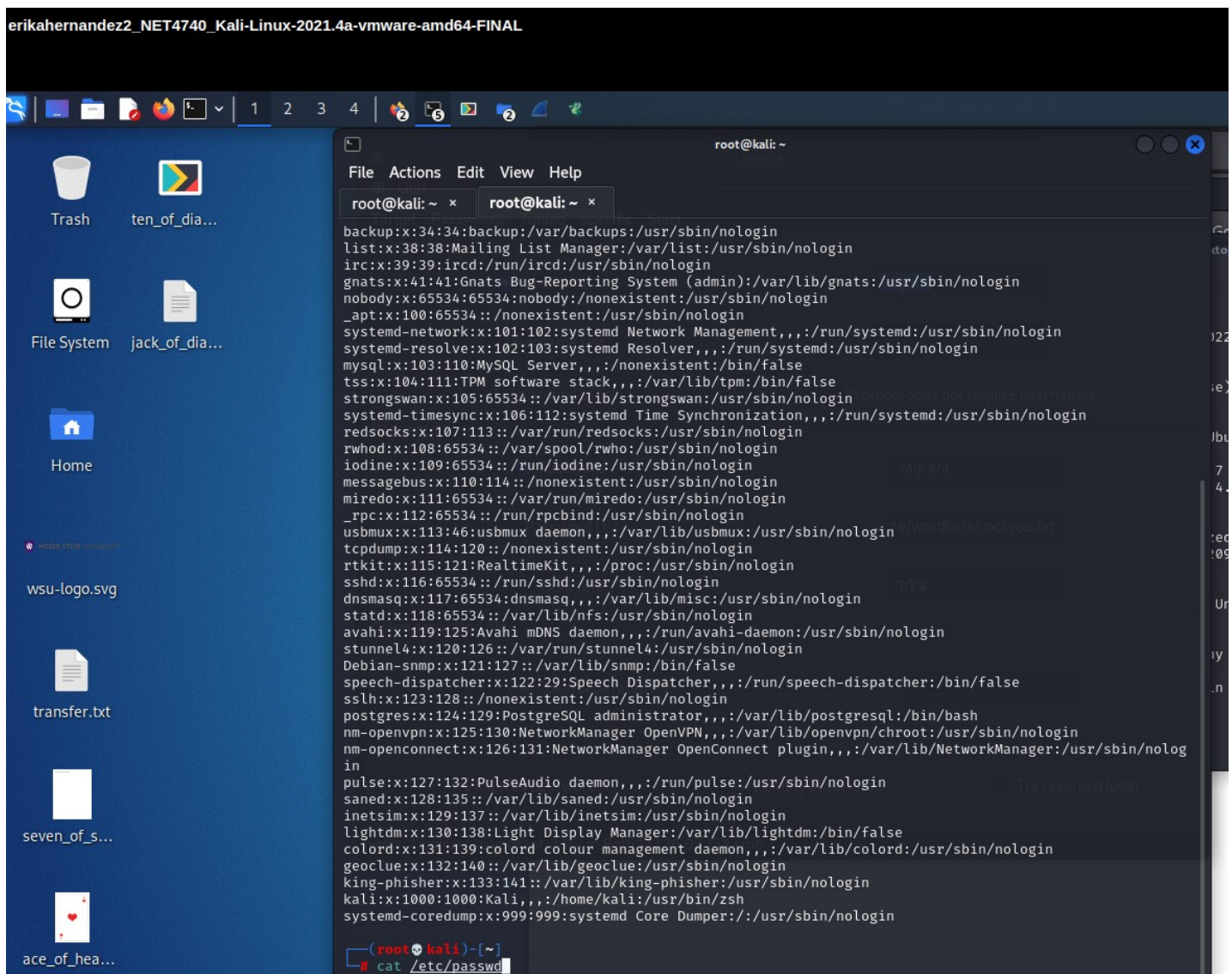


# Erika Hernandez

## Final Exam

## NET 4740

### Question 1 – List of users from each machine



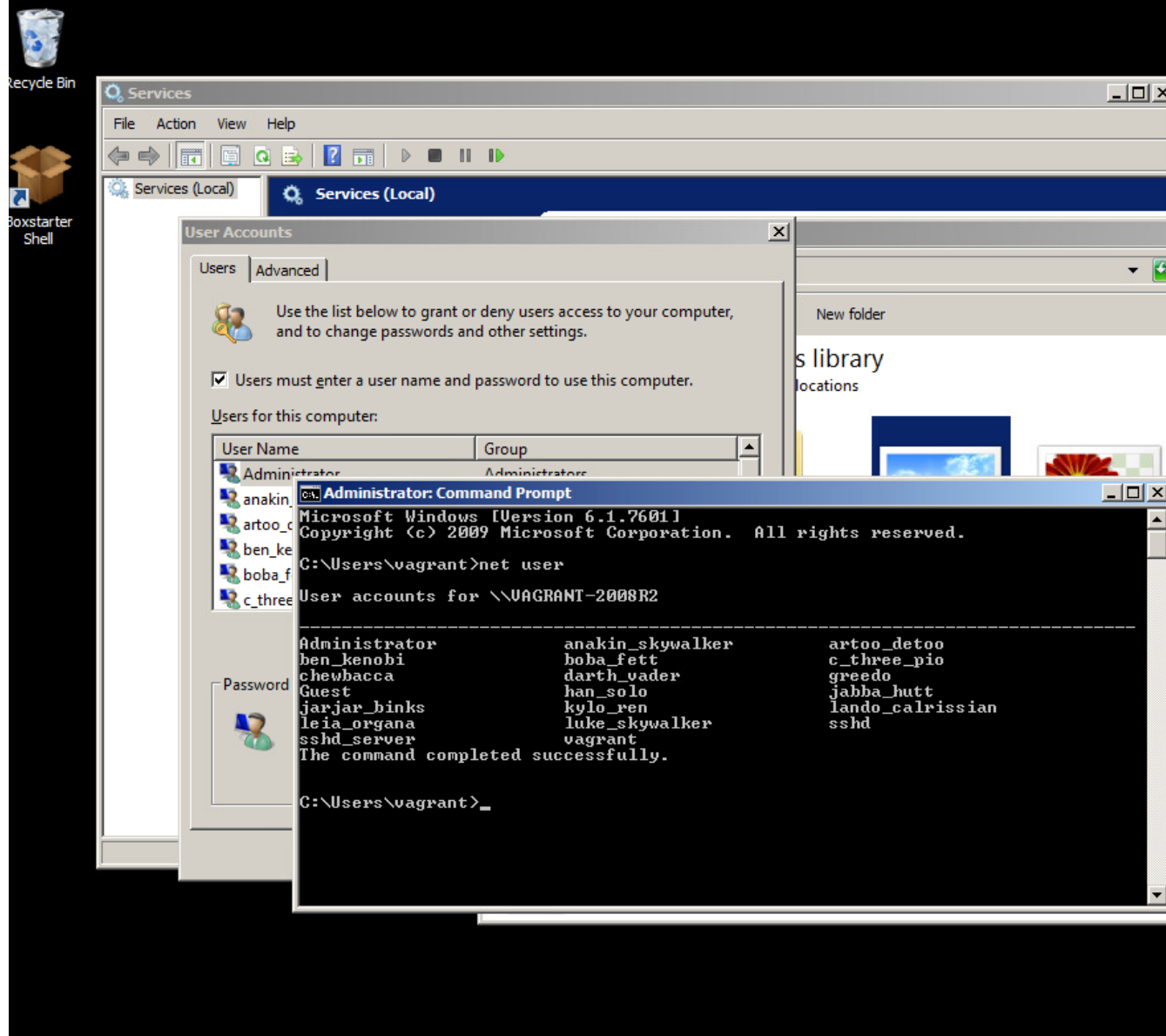
The screenshot shows a Kali Linux desktop environment. On the left is a sidebar with icons for Trash, ten\_of\_dia..., File System, jack\_of\_dia..., Home, wsu-logo.svg, transfer.txt, seven\_of\_s..., and ace\_of\_hea... The main window is a terminal titled 'root@kali: ~'. It displays the output of the command 'cat /etc/passwd', listing system users and regular users. The output is as follows:

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin  
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin  
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin  
mysql:x:103:110:MySQL Server,,:/nonexistent:/bin/false  
tss:x:104:111:TPM software stack,,:/var/lib/tpm:/bin/false  
strongswan:x:105:65534::/var/lib/strongswan:/usr/sbin/nologin  
systemd-timesync:x:106:112:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin  
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin  
rwho:x:108:65534::/var/spool/rwho:/usr/sbin/nologin  
iodine:x:109:65534::/run/iodine:/usr/sbin/nologin  
messagebus:x:110:114::/nonexistent:/usr/sbin/nologin  
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin  
_rpc:x:112:65534::/run/rpcbind:/usr/sbin/nologin  
usbmux:x:113:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin  
tcpdump:x:114:120::/nonexistent:/usr/sbin/nologin  
rtkit:x:115:121:RealtimeKit,,:/proc:/usr/sbin/nologin  
sshd:x:116:65534::/run/sshd:/usr/sbin/nologin  
dnsmasq:x:117:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin  
statd:x:118:65534::/var/lib/nfs:/usr/sbin/nologin  
avahi:x:119:125:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin  
stunnel4:x:120:126::/var/run/stunnel4:/usr/sbin/nologin  
Debian-snmpp:x:121:127::/var/lib/snmpp:/bin/false  
speech-dispatcher:x:122:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false  
sshd:x:123:128::/nonexistent:/usr/sbin/nologin  
postgres:x:124:129:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash  
nm-openvpn:x:125:130:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin  
nm-openconnect:x:126:131:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin  
pulse:x:127:132:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin  
saned:x:128:135::/var/lib/saned:/usr/sbin/nologin  
inetsim:x:129:137::/var/lib/inetsim:/usr/sbin/nologin  
lightdm:x:130:138:Light Display Manager:/var/lib/lightdm:/bin/false  
colord:x:131:139:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin  
geoclue:x:132:140::/var/lib/geoclue:/usr/sbin/nologin  
king-phisher:x:133:141::/var/lib/king-phisher:/usr/sbin/nologin  
kali:x:1000:1000:Kali,,:/home/kali:/usr/bin/zsh  
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
```

At the bottom of the terminal, the prompt '(root@kali)-[~]' is shown, followed by the command 'cat /etc/passwd' being entered.

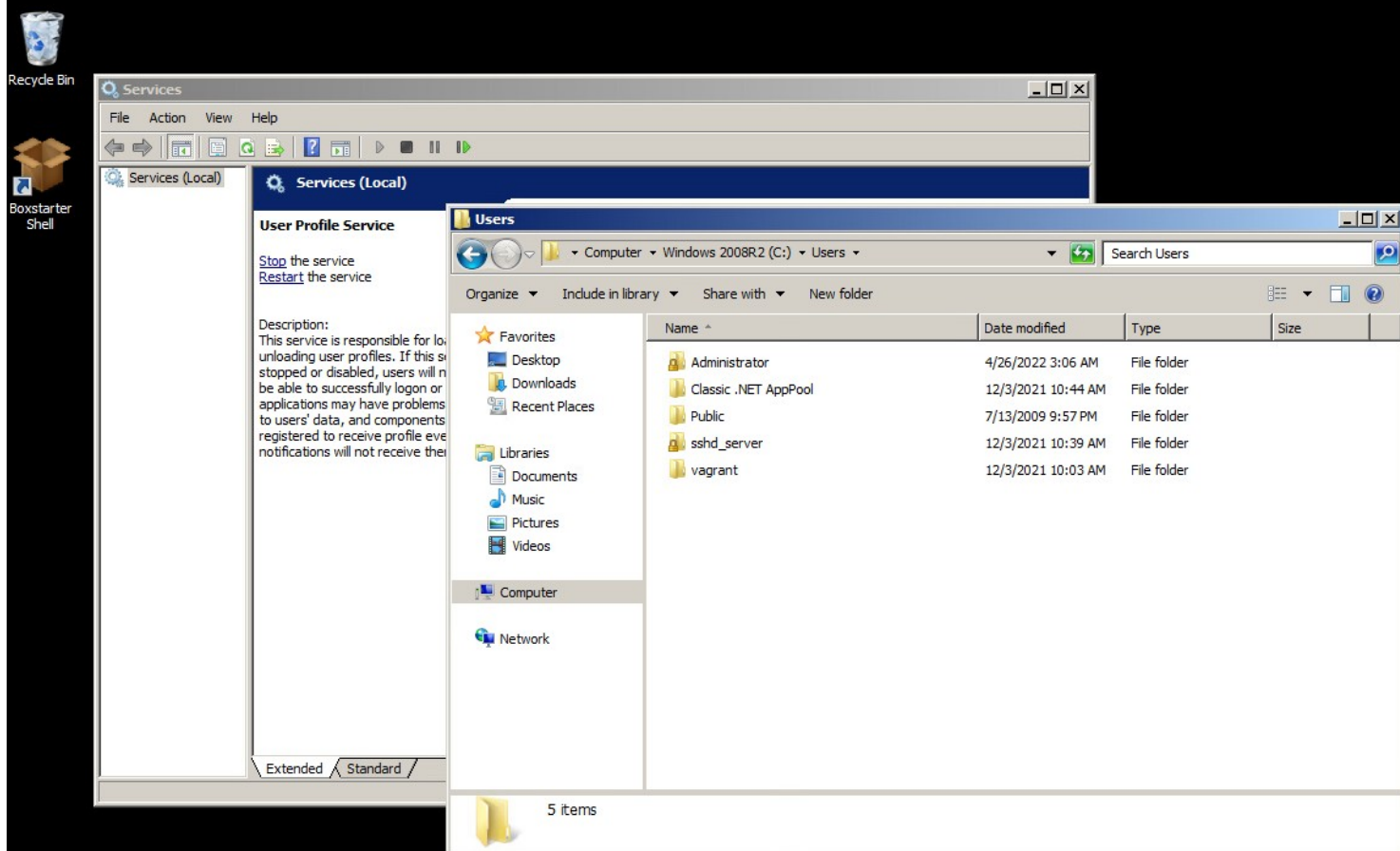
*Kali Linux users with root users*

erikahernandez2\_NET4740\_metasploitable3-win2k8-FINAL



Windows 2008- List of users for the window machine

erikahernandez2\_NET4740\_metasploitable3-win2k8-FINAL



Windows - Second method to finding users- wanted to double check on users

```

root@kali: ~ x root@ubuntu: ~ x
File Actions Edit View Help
-n or --myname=<name> client name
-U or --user=<name> user name
-s or --configfile=<path> pathname of smb.conf file
-l or --long Display full information
-V or --version Print samba version information
-P or --machine-pass Authenticate as machine account
-e or --encrypt Encrypt SMB transport (UNIX extended servers only)
-k or --kerberos Use kerberos (active directory) authentication
-C or --comment=<comment> descriptive comment (for add only)
-c or --container=<container> LDAP container, defaults to cn=Users (for add in ADS only)
vagrant@ubuntu:~$ sudo -u#-1 /bin/bash
root@ubuntu:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d
root@ubuntu:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

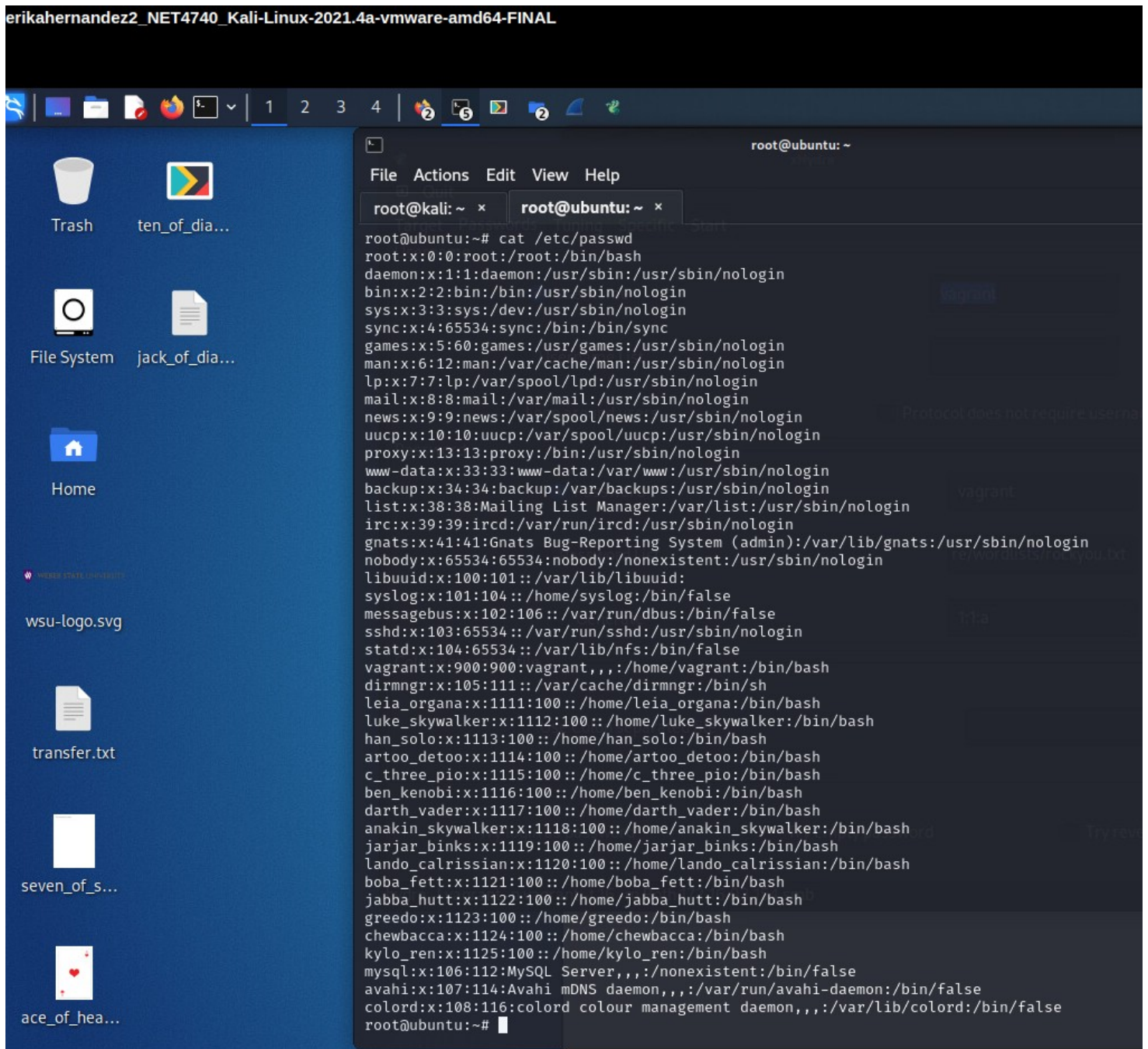
```

Ubuntu Users - I couldn't get into root user in the Ubuntu machine so I ssh into it. using the vagrant@172.16.93.154



## Question 2 – admin users

erikahernandez2\_NET4740\_Kali-Linux-2021.4a-vmware-amd64-FINAL



```
root@kali: ~ x root@ubuntu: ~ x
root@ubuntu:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
root@ubuntu:~#
```

Ubuntu as root- Here are the list of users using the root on the kali machine

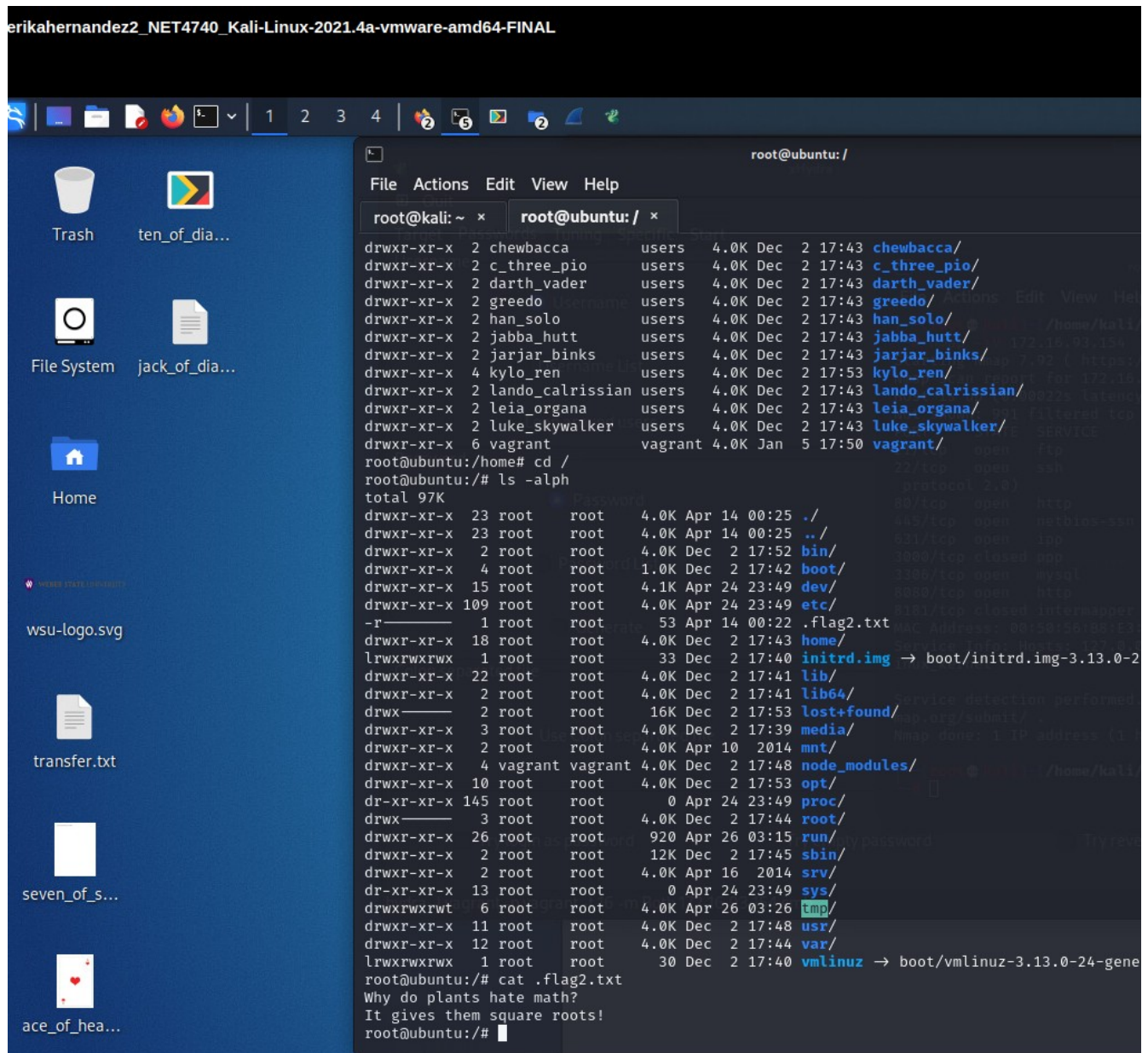
```

luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jar_jar_binks:x:1119:100::/home/jar_jar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
vagrant@ubuntu:~$ ls -al
total 57284
drwxr-xr-x  6 vagrant vagrant    4096 Jan  5 17:50 .
drwxr-xr-x 18 root    root      4096 Dec  2 17:43 ..
-rw-----  1 vagrant vagrant    812 Apr 14 02:09 .bash_history
-rw-r--r--  1 vagrant vagrant    220 Dec  2 17:42 .bash_logout
-rw-r--r--  1 vagrant vagrant   3637 Dec  2 17:42 .bashrc
drwxr-xr-x  3 root    root      4096 Dec  2 17:43 .bundle
drwx-----  2 vagrant vagrant   4096 Dec  2 17:42 .cache
drwx-----  2 root    root      4096 Dec  2 17:45 .gnupg
-rw-r--r--  1 vagrant vagrant 58617856 Dec  2 17:43 linux.iso
drwxr-xr-x 55 vagrant vagrant   4096 Dec  2 17:48 .npm
-rw-r--r--  1 vagrant vagrant    675 Dec  2 17:42 .profile
vagrant@ubuntu:~$ sudo /etc/sudoers.d/
sudo: /etc/sudoers.d/: command not found
vagrant@ubuntu:~$ sudo /etc/sudoers
sudo: /etc/sudoers: command not found
vagrant@ubuntu:~$ cd /root
-bash: cd: /root: Permission denied
vagrant@ubuntu:~$

```

Ubuntu access denied- Here is showing that it wont let me use root on the machine – using the sudoers.d command

### Question 3 – Flags 1 and 2 – Two flags for each machine



```
erikahernandez2_NET4740_Kali-Linux-2021.4a-vmware-amd64-FINAL

root@kali: ~ * root@ubuntu: / *
File Actions Edit View Help
root@kali: ~ * root@ubuntu: / *
drwxr-xr-x 2 chewbacca users 4.0K Dec 2 17:43 chewbacca/
drwxr-xr-x 2 c_three_pio users 4.0K Dec 2 17:43 c_three_pio/
drwxr-xr-x 2 darth_vader users 4.0K Dec 2 17:43 darth_vader/
drwxr-xr-x 2 greedo users 4.0K Dec 2 17:43 greedo/
drwxr-xr-x 2 han_solo users 4.0K Dec 2 17:43 han_solo/
drwxr-xr-x 2 jabba_hutt users 4.0K Dec 2 17:43 jabba_hutt/
drwxr-xr-x 2 jarjar_binks users 4.0K Dec 2 17:43 jarjar_binks/
drwxr-xr-x 4 kylo_ren users 4.0K Dec 2 17:53 kylo_ren/
drwxr-xr-x 2 lando_calrissian users 4.0K Dec 2 17:43 lando_calrissian/
drwxr-xr-x 2 leia_organa users 4.0K Dec 2 17:43 leia_organa/
drwxr-xr-x 2 luke_skywalker users 4.0K Dec 2 17:43 luke_skywalker/
drwxr-xr-x 6 vagrant vagrant 4.0K Jan 5 17:50 vagrant/
root@ubuntu:/home# cd /
root@ubuntu:/# ls -lph
total 97K
drwxr-xr-x 23 root root 4.0K Apr 14 00:25 ./
drwxr-xr-x 23 root root 4.0K Apr 14 00:25 ../
drwxr-xr-x 2 root root 4.0K Dec 2 17:52 bin/
drwxr-xr-x 4 root root 1.0K Dec 2 17:42 boot/
drwxr-xr-x 15 root root 4.1K Apr 24 23:49 dev/
drwxr-xr-x 109 root root 4.0K Apr 24 23:49 etc/
-r----- 1 root root 53 Apr 14 00:22 .flag2.txt
drwxr-xr-x 18 root root 4.0K Dec 2 17:43 home/
lrwxrwxrwx 1 root root 33 Dec 2 17:40 initrd.img -> boot/initrd.img-3.13.0-2
drwxr-xr-x 22 root root 4.0K Dec 2 17:41 lib/
drwxr-xr-x 2 root root 4.0K Dec 2 17:41 lib64/
drwx----- 2 root root 16K Dec 2 17:53 lost+found/
drwxr-xr-x 3 root root 4.0K Dec 2 17:39 media/
drwxr-xr-x 2 root root 4.0K Apr 10 2014 mnt/
drwxr-xr-x 4 vagrant vagrant 4.0K Dec 2 17:48 node_modules/
drwxr-xr-x 10 root root 4.0K Dec 2 17:53 opt/
dr-xr-xr-x 145 root root 0 Apr 24 23:49 proc/
drwx----- 3 root root 4.0K Dec 2 17:44 root/
drwxr-xr-x 26 root root 920 Apr 26 03:15 run/
drwxr-xr-x 2 root root 12K Dec 2 17:45/sbin/
drwxr-xr-x 2 root root 4.0K Apr 16 2014/srv/
dr-xr-xr-x 13 root root 0 Apr 24 23:49/sys/
drwxrwxrwt 6 root root 4.0K Apr 26 03:26/tmp/
drwxr-xr-x 11 root root 4.0K Dec 2 17:48/usr/
drwxr-xr-x 12 root root 4.0K Dec 2 17:44/var/
lrwxrwxrwx 1 root root 30 Dec 2 17:40 vmlinuz -> boot/vmlinuz-3.13.0-24-gene
root@ubuntu:/# cat .flag2.txt
Why do plants hate math?
It gives them square roots!
root@ubuntu:/#
```

Flag2.txt- The flag wouldn't open on the Ubuntu machine so i ssh it and send it over to the Kali machine. There i was able to open it and read the content of the file.



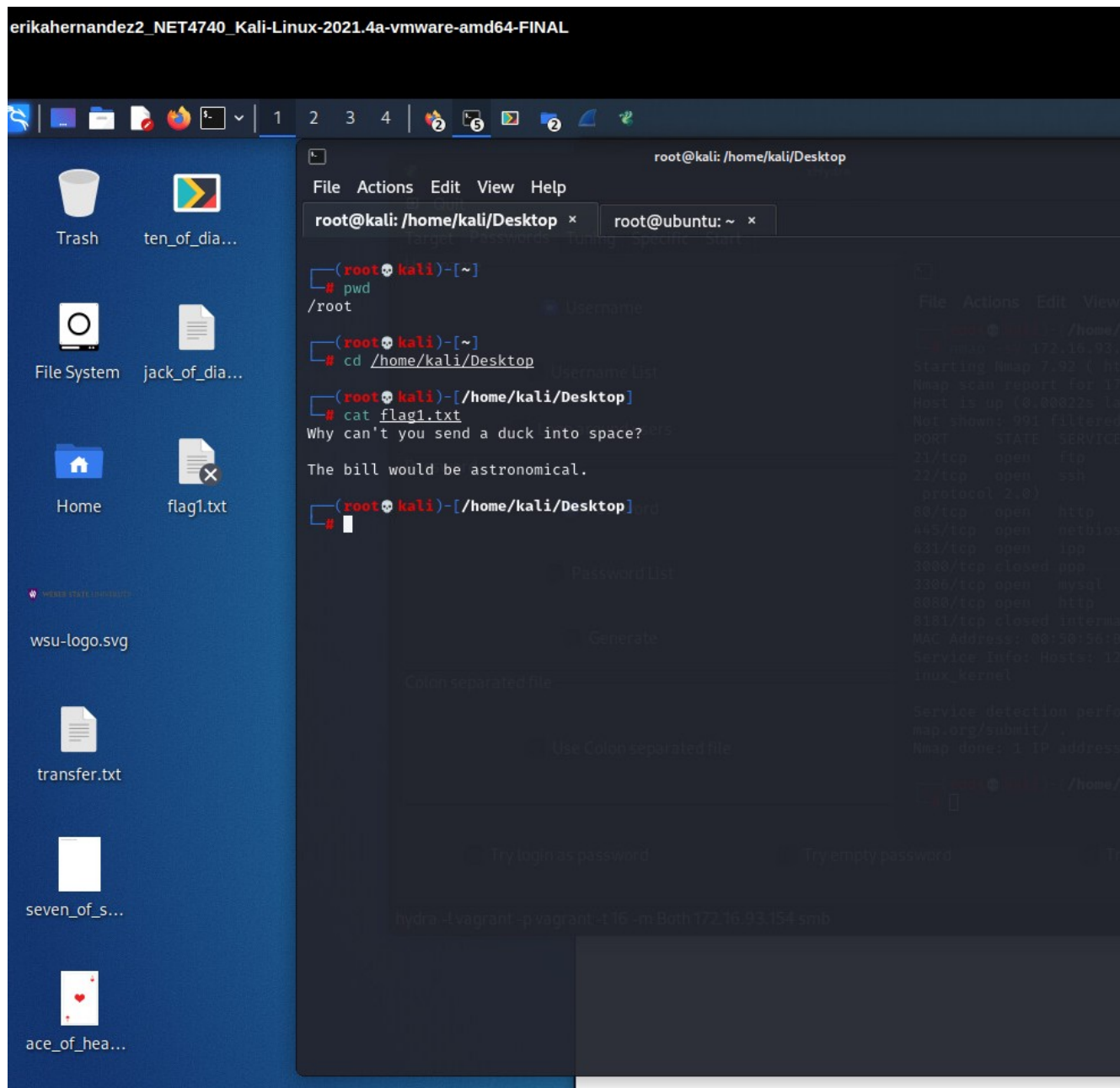
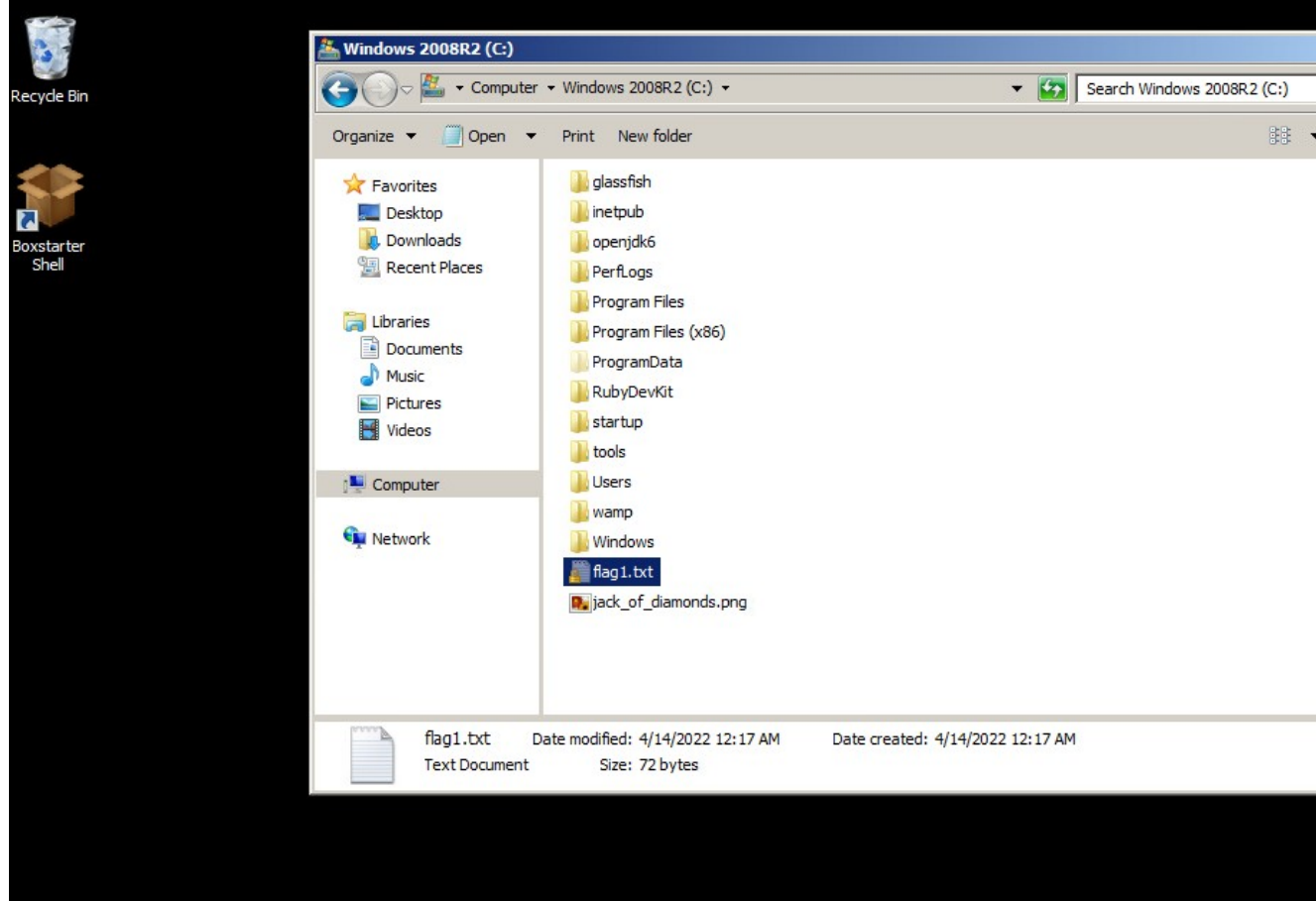


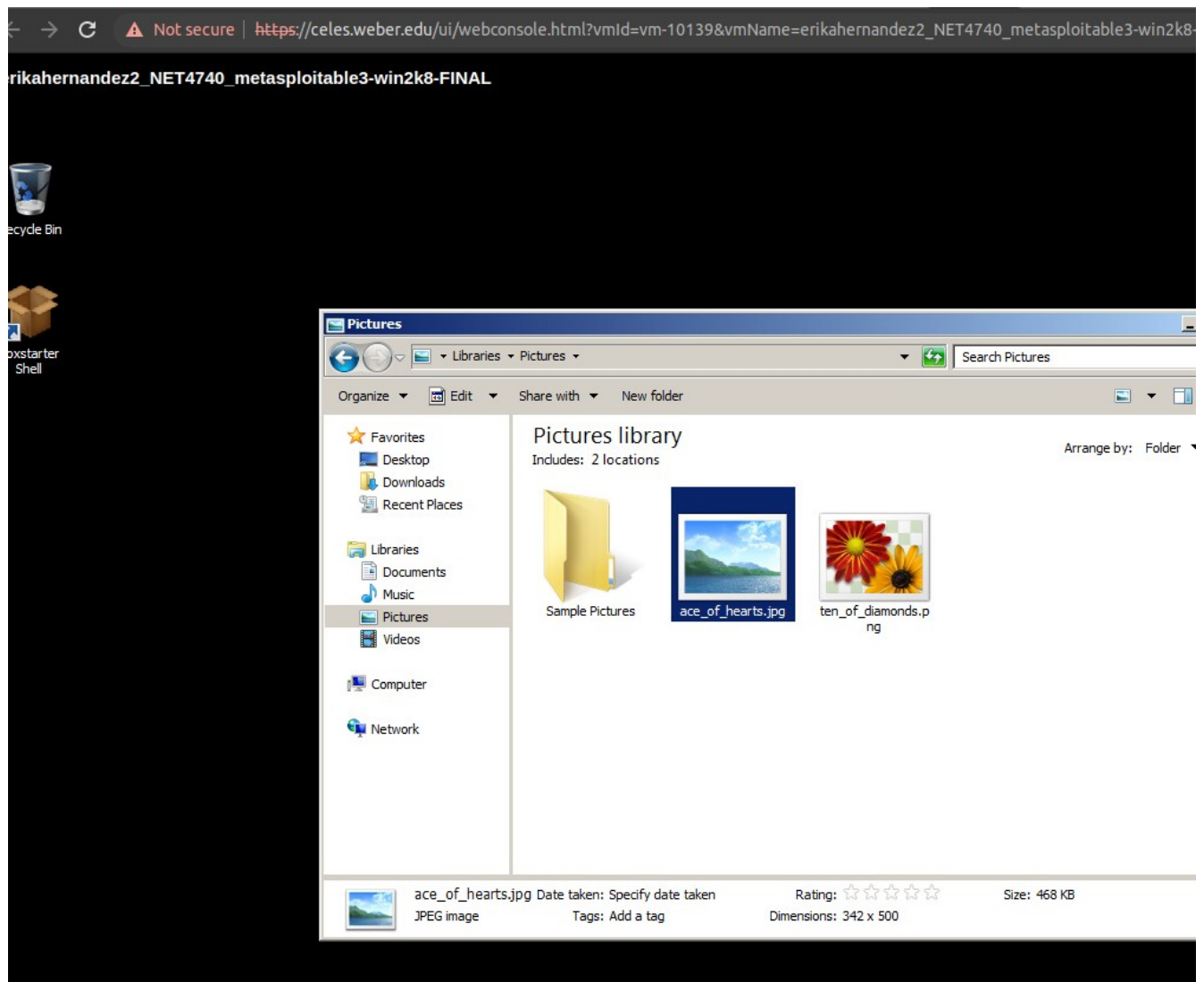
Figure 1: flag1.txt - This was the flag I got from the windows machine



erikahernandez2\_NET4740\_metasploitable3-win2k8-FINAL

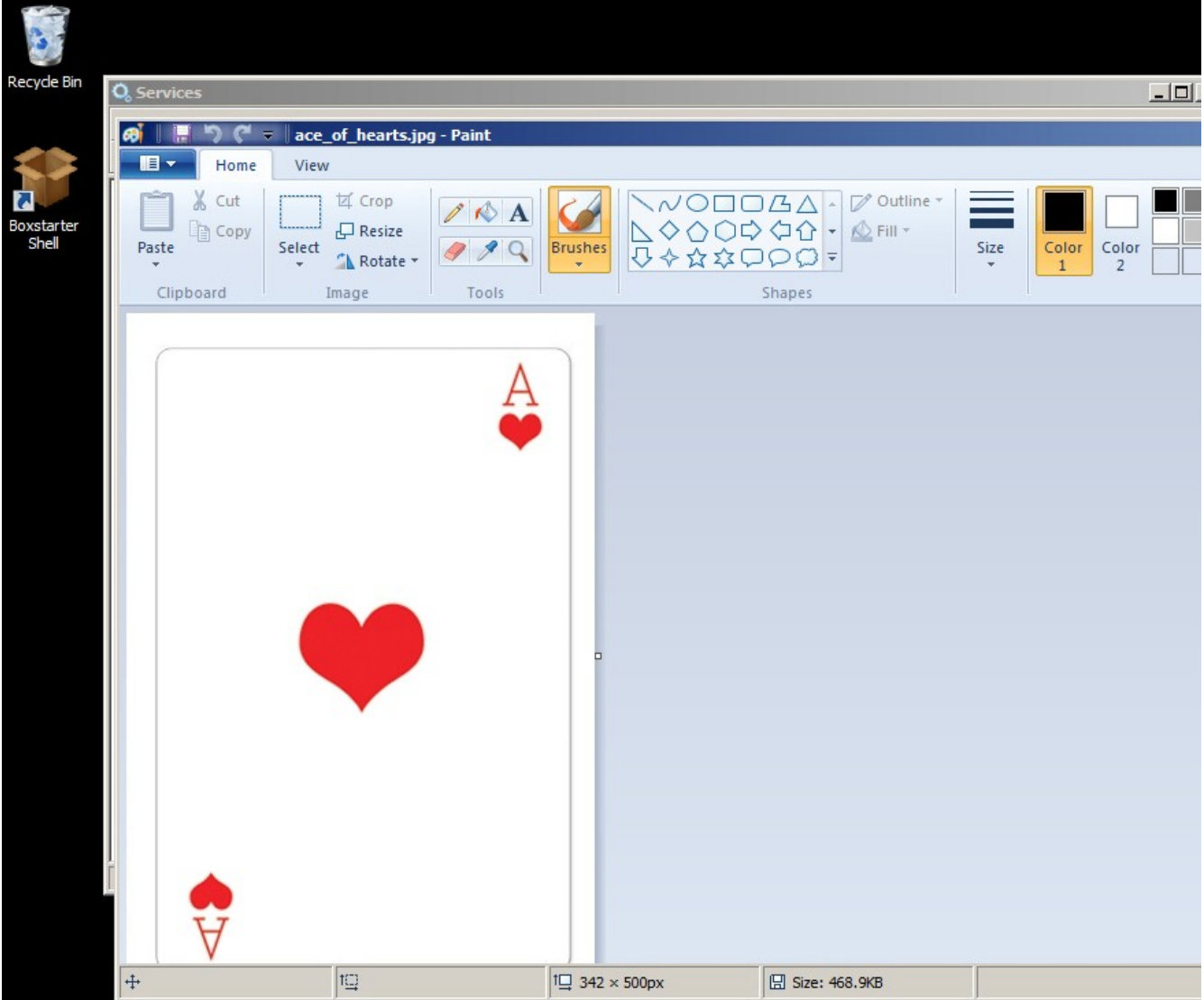


*flag1- this was in the Windows C:\ but it was a hidden file- I had to figure out how to unhide since this was a Windows 2008 machine*



*I thought these were flags- but they weren't. they looked like them to me so i just took screen shots*

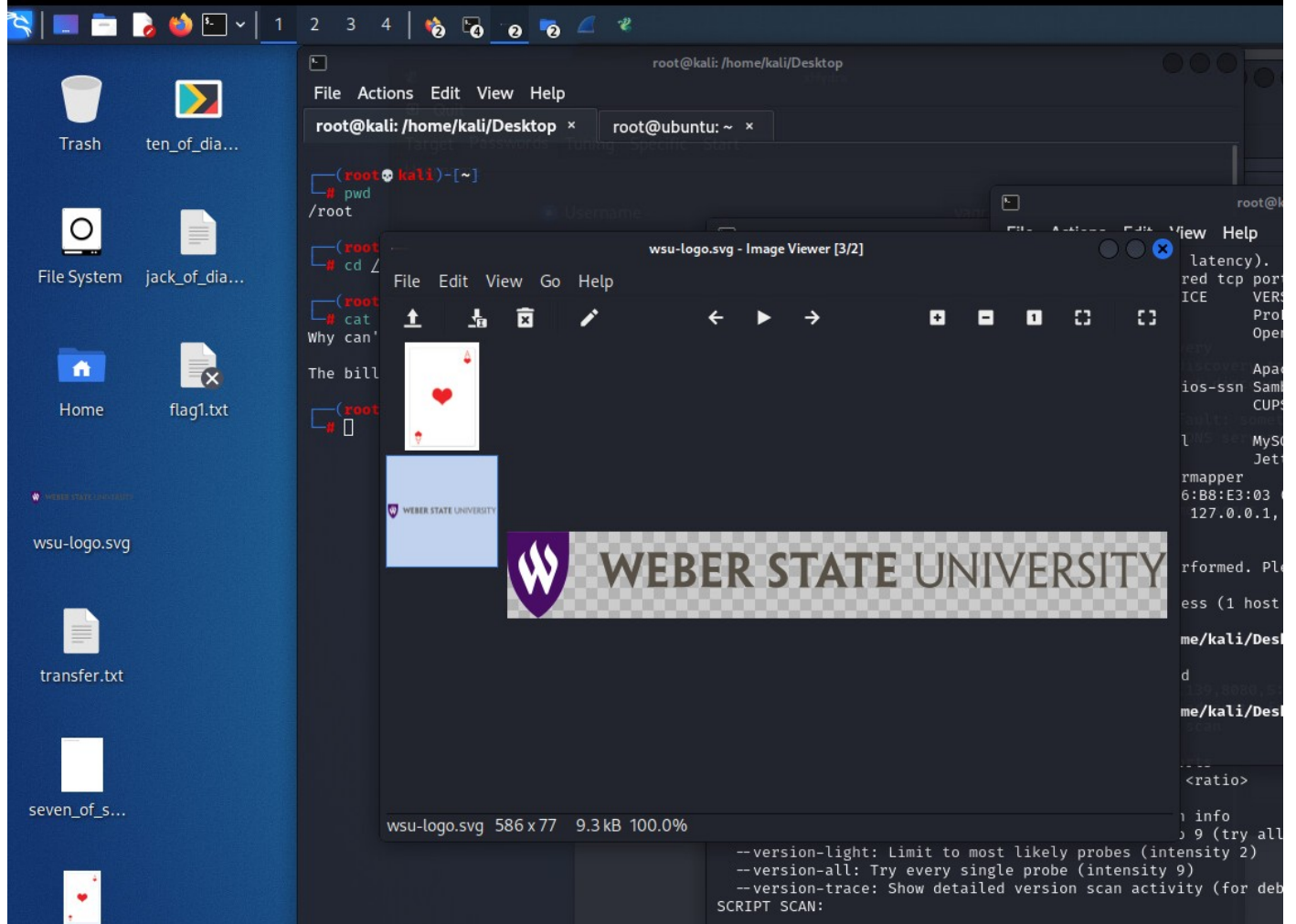
erikahernandez2\_NET4740\_metasploitable3-win2k8-FINAL



*Possible Flag? I thought was something – but was nothing.*

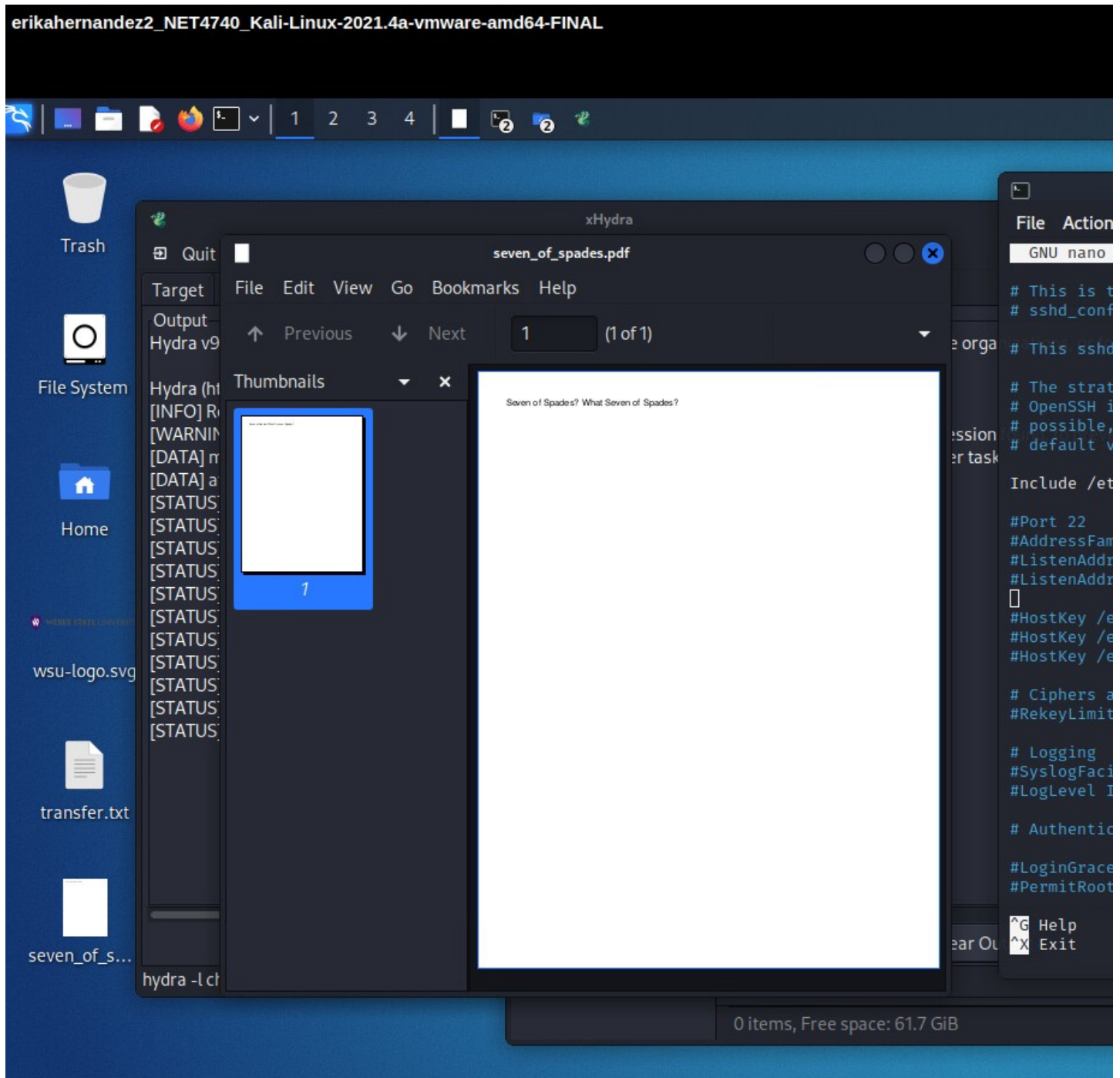
## Question 4 – Image on the desktop

erikahernandez2\_NET4740\_Kali-Linux-2021.4a-vmware-amd64-FINAL





## Question 5 – Image that was on the desktop without using the GUI



*The txt file that was on the Kali machine*

The screenshot shows a Kali Linux desktop environment. The desktop background is dark blue. On the left side, there is a sidebar with icons for Trash, ten\_of\_dia..., File System, jack\_of\_dia..., Home, flag1.txt, wsu-logo.svg, and transfer.txt. The top of the desktop has a taskbar with icons for various applications, including a terminal, a file manager, and a web browser. A terminal window is open in the center, showing the following commands and output:

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
root@kali: /home/kali/Desktop x root@ubuntu: ~ x
(root@kali)-[~]
# pwd
/root
(root@kali)-[~]
# cd /home/kali/Desktop
(root@kali)-[/home/kali/Desktop]
# cat flag1.txt
Why can't you send a duck into space?

The bill would be astronomical.

(root@kali)-[/home/kali/Desktop]
# cat transfer.txt
They're developing an air freshener that's mind-controlled.

It makes scents if you think about it.

(root@kali)-[/home/kali/Desktop]
#
```