

**Lab #8: Encryption**  
**CSC432-A**  
**Franklin Nuth**  
**19 March 2019**

## **Abstract**

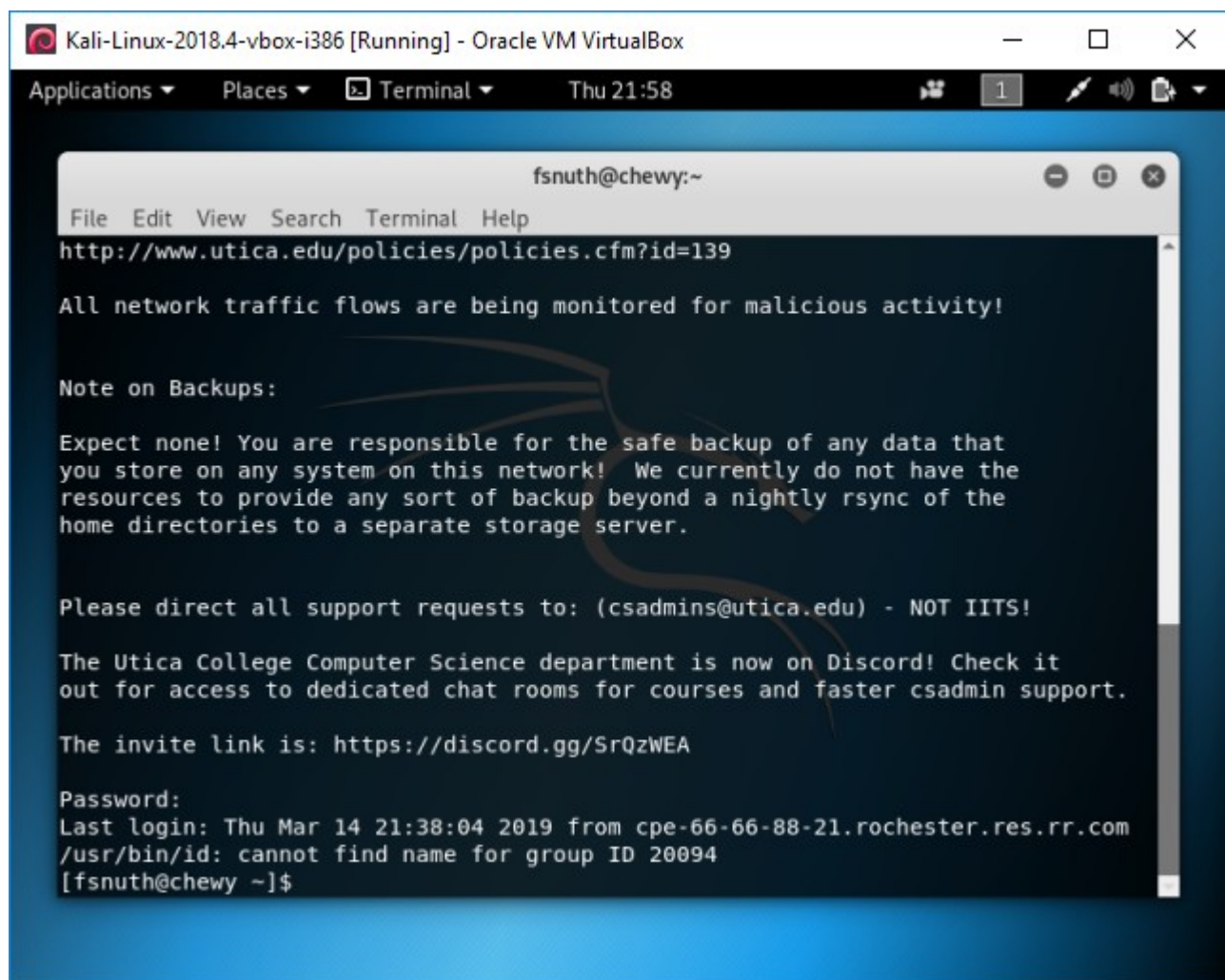
In this lab, I will be manipulating the firewall and network settings of my virtual Kali so that I can access my private network from anywhere at any time. I will be testing my ability to log in through Chewy normally and test if the SSH is working. I will also be using SSH to proxy my web traffic, which will allow me to listen in on traffic from specific ports. Then I will configure a file in my .ssh directory so that I can access Chewy without typing my username and the domain name, as well as generating an SSH key so I will have easier access to it. I will finish off by learning how to encrypt single files on my Kali Linux, as well as encrypting multiple files in a folder with GPG.

## **Introduction**

I can access my Chewy account and my virtual network from anywhere in the world if I want to. With any computer, I can go to my router and web server for reconfiguring them to my needs. Not only that, I can access my Kali from ProxMox, and not through the command window because I made sure to be secure even with SSH port forwarding. The purpose of this lab will be to automate my access through Chewy and my network by eliminating the need for many certificates along the way. Doing this lab will give me faster access to my network and eliminates the need to remember any password for going to my network.

## **Processes & Screenshots**

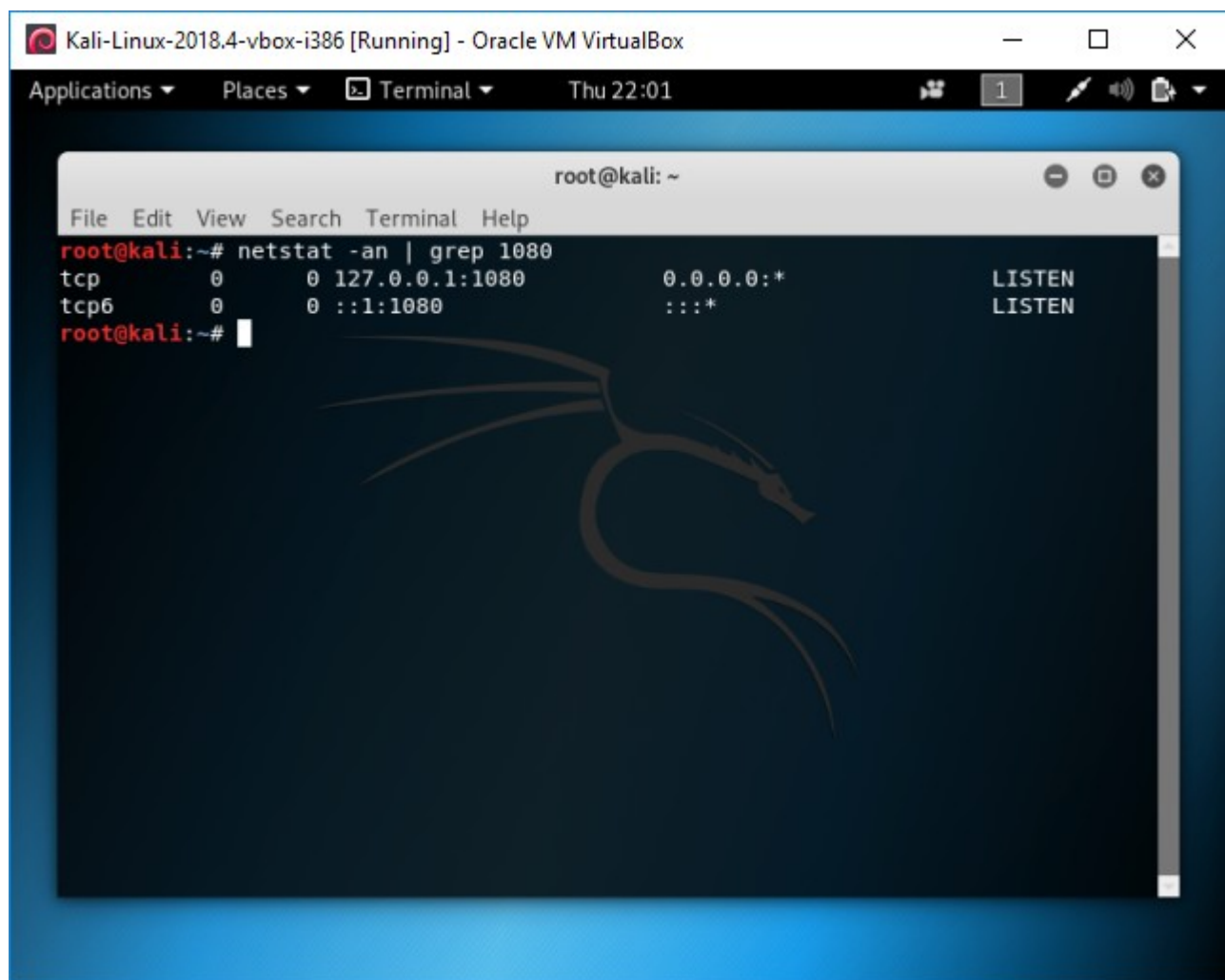
To start the lab, I need to see if I can access my Chewy account through any command window. I did this by opening a terminal on my personal Kali, and logged into my Chewy account with “ssh [fsnuth@chewy.cs.utica.edu](mailto:fsnuth@chewy.cs.utica.edu)”. This syntax will log into the account with the username “fsnuth” on Chewy, with the domain name “cs.utica.edu”.



```
fsnuth@chewy:~  
File Edit View Search Terminal Help  
http://www.utica.edu/policies/policies.cfm?id=139  
All network traffic flows are being monitored for malicious activity!  
  
Note on Backups:  
Expect none! You are responsible for the safe backup of any data that  
you store on any system on this network! We currently do not have the  
resources to provide any sort of backup beyond a nightly rsync of the  
home directories to a separate storage server.  
  
Please direct all support requests to: (csadmins@utica.edu) - NOT IITS!  
The Utica College Computer Science department is now on Discord! Check it  
out for access to dedicated chat rooms for courses and faster csadmin support.  
The invite link is: https://discord.gg/SrQzWEA  
  
Password:  
Last login: Thu Mar 14 21:38:04 2019 from cpe-66-66-88-21.rochester.res.rr.com  
/usr/bin/id: cannot find name for group ID 20094  
[fsnuth@chewy ~]$
```

*(Logging into my Chewy from my own Kali. I did this from my own Kali to see if I can truly access my network through SSH, and not just from college desktops or the Kali on my network.)*

I exited the Chewy account and back into my Kali. After that, I typed “ssh -D 1080 [fsnuth@chewy.cs.utica.edu](mailto:fsnuth@chewy.cs.utica.edu)”. This will allow the local system to listen in on port 1080 traffic, which we will manipulate later with Firefox. I then typed “netstat -an | grep 1080” to see if any traffic is being picked up from that port.



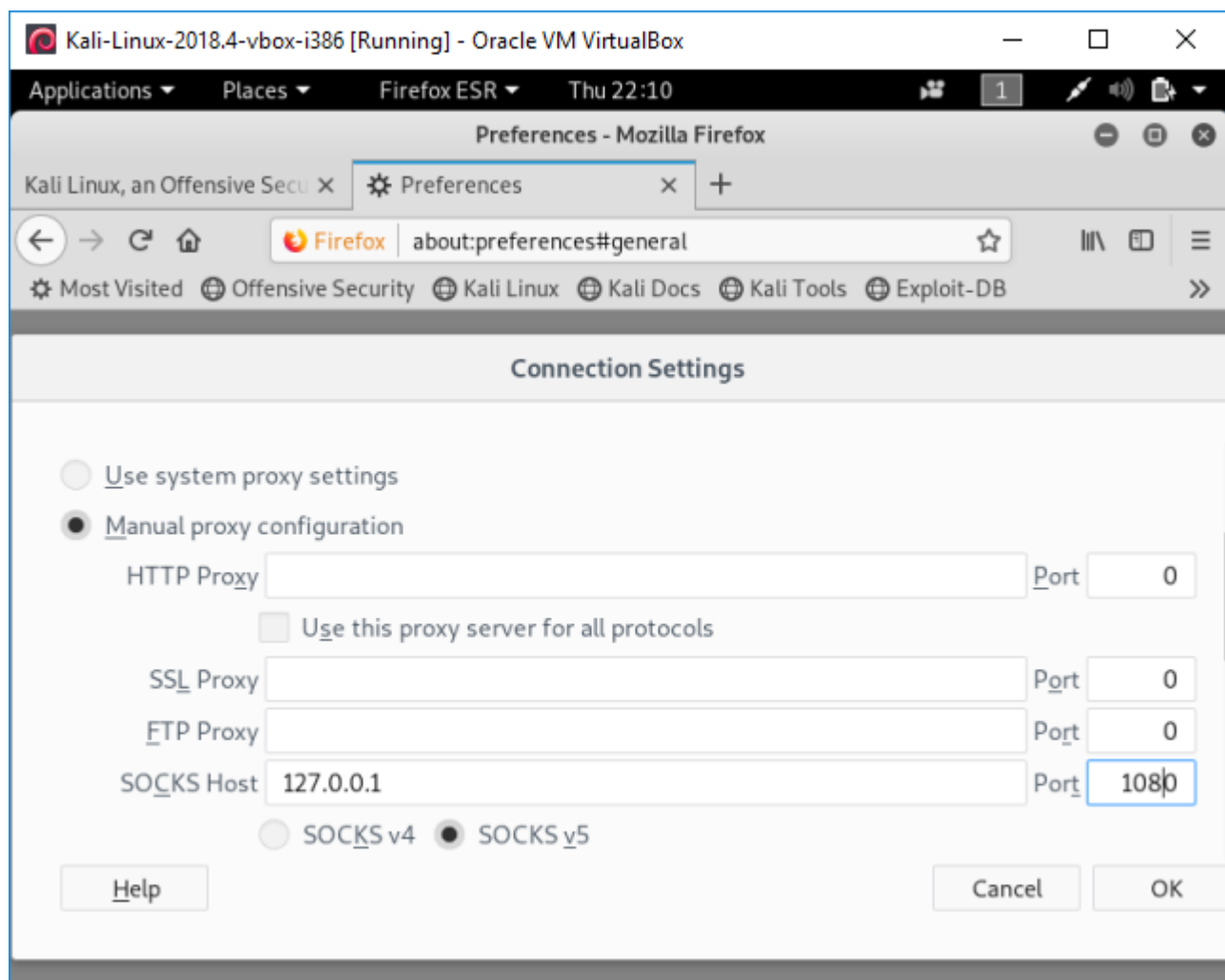
The screenshot shows a Kali Linux terminal window titled "root@kali: ~". The terminal output for the command `netstat -an | grep 1080` is as follows:

Protocol	State	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0	127.0.0.1:1080	0.0.0.0:*	LISTEN
tcp6	0	0	0	:::1:1080	:::*	LISTEN

The terminal also features a large, stylized dragon logo in the background.

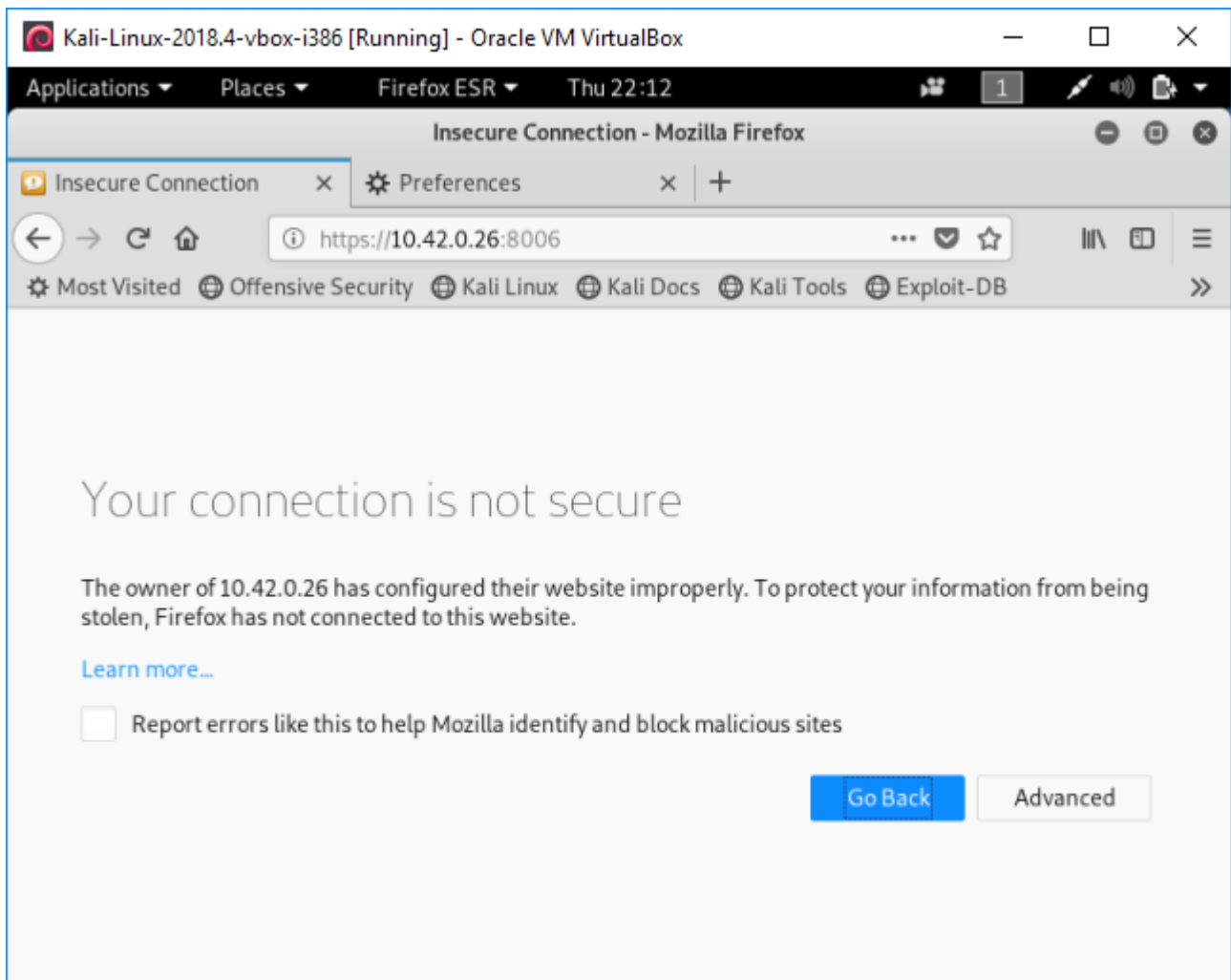
*(The result of typing “netstat -an | grep 1080”. The most interesting thing to note here is that 1080 port traffic is being listened to on 127.0.0.1, which is most likely the IP of my Chewy account.)*

After confirming that my local system is listening for port 1080 traffic, I then move on to feed it web traffic through Kali’s Firefox browser. The lab says to use IceWeasel, but that browser is not in my Kali, and the network settings menus are similar to the point where I have no reason to worry.

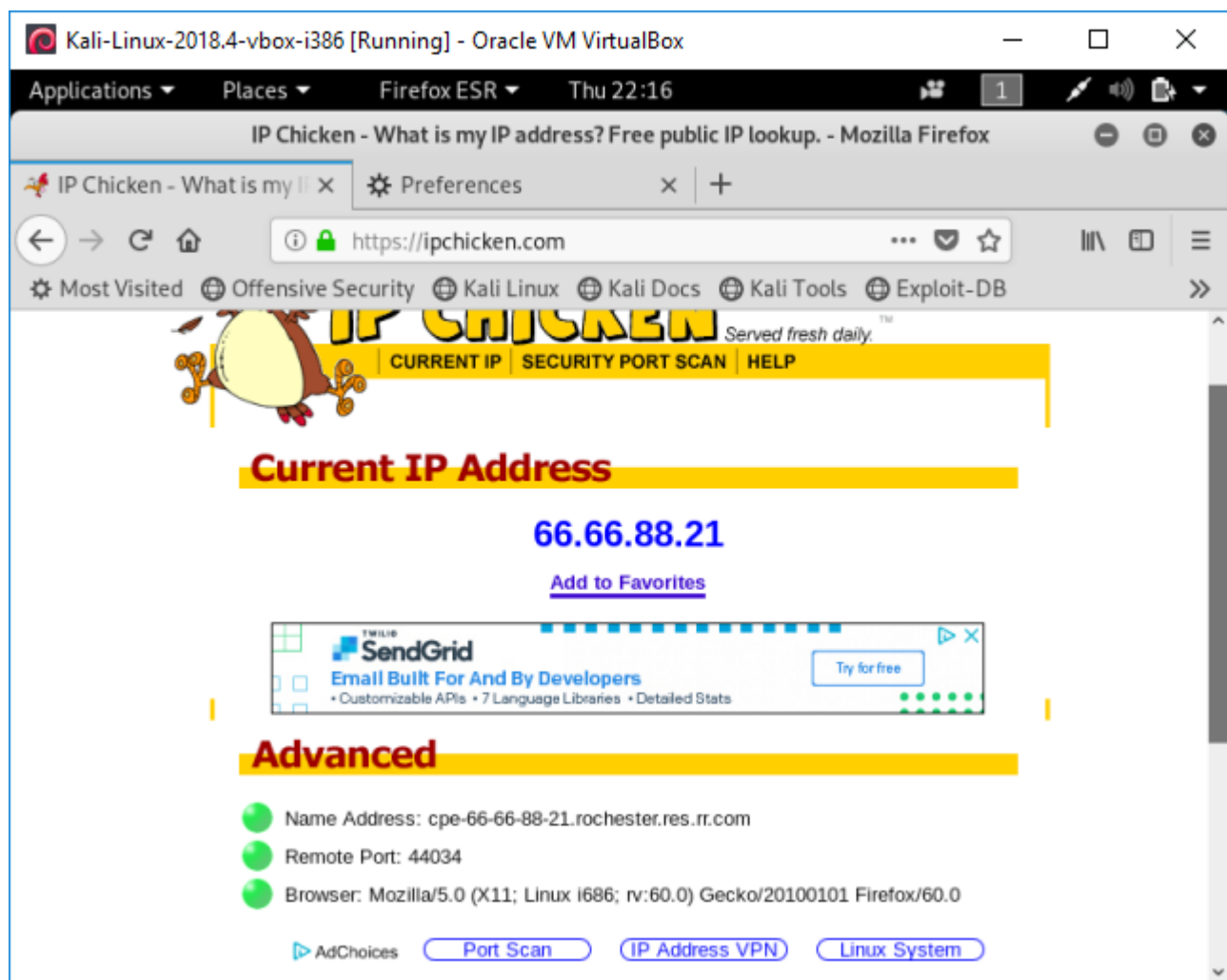


*(Configuring a manual proxy on my Kali's Firefox network settings. I notice that the IP used for the SOCKS Host and the Port is the same information we found when listening with netstat.)*

I typed "<https://10.42.0.26:8006>" into the Firefox browser, the private address for the VLE web portal. I have been denied, but the lab says this is part of the lab, so I moved on to the next step of immediately checking my IP address first with my manual settings, and the settings that DHCP gives me.



*(Trying to get in the VLE web portal. This error message is significant in that it points to the owner not configuring the website properly rather than connection error.)*

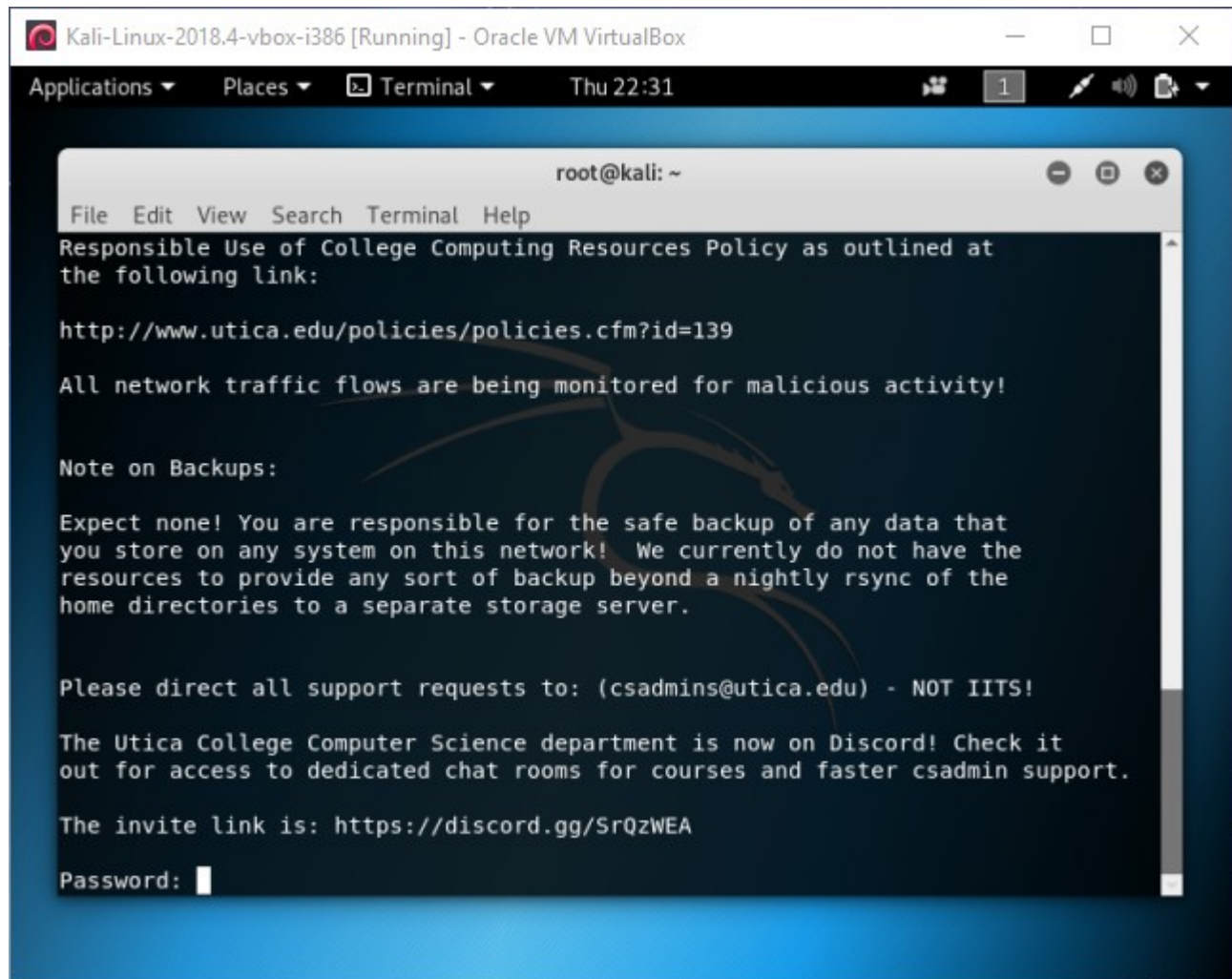


*(My IP address after changing my network settings from manual to automatic, which was previously 4.26.24.234. I noticed that the IP address changed when I change the network settings. I think this sudden switching of IP address could be used for changing the flow of web traffic.)*

After this, I created a config file in the .ssh directory of my Kali, and configured it with the following code:

```
Host chewy
ForwardAgent yes
HostName chewy.cs.utica.edu
Port 22
User fsnuth
```

After putting the above code into the config file, I attempted to SSH back into Chewy to see if I have to typed “[fsnuth@chewy.cs.utica.edu](mailto:fsnuth@chewy.cs.utica.edu)”. It turns out I don’t have to, reducing the things I have to typed to “ssh chewy”.

A screenshot of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The window title is "Kali-Linux-2018.4-vbox-i386 [Running] - Oracle VM VirtualBox". The terminal shows a root prompt "root@kali: ~" and a menu with "File Edit View Search Terminal Help". The main text in the terminal is a message from the Utica College Computer Science department, stating that network traffic is monitored for malicious activity and providing a link to the Responsible Use of College Computing Resources Policy. It also mentions that backups are not provided and directs support requests to csadmins@utica.edu. The message ends with a password prompt "Password: " and a cursor.

```
root@kali: ~
File Edit View Search Terminal Help
Responsible Use of College Computing Resources Policy as outlined at
the following link:

http://www.utica.edu/policies/policies.cfm?id=139

All network traffic flows are being monitored for malicious activity!

Note on Backups:

Expect none! You are responsible for the safe backup of any data that
you store on any system on this network! We currently do not have the
resources to provide any sort of backup beyond a nightly rsync of the
home directories to a separate storage server.

Please direct all support requests to: (csadmins@utica.edu) - NOT IITS!

The Utica College Computer Science department is now on Discord! Check it
out for access to dedicated chat rooms for courses and faster csadmin support.

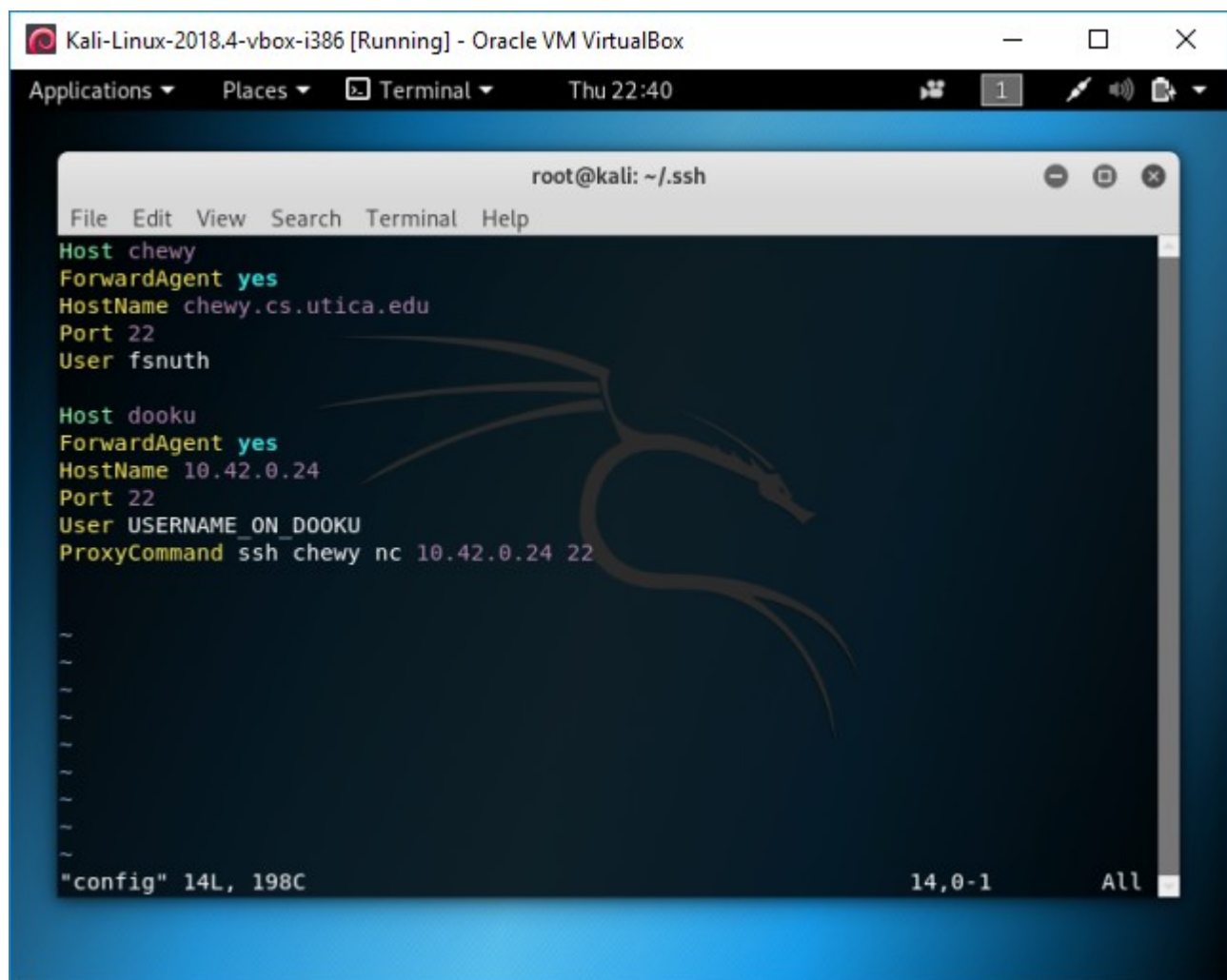
The invite link is: https://discord.gg/SrQzWEA

Password: 
```

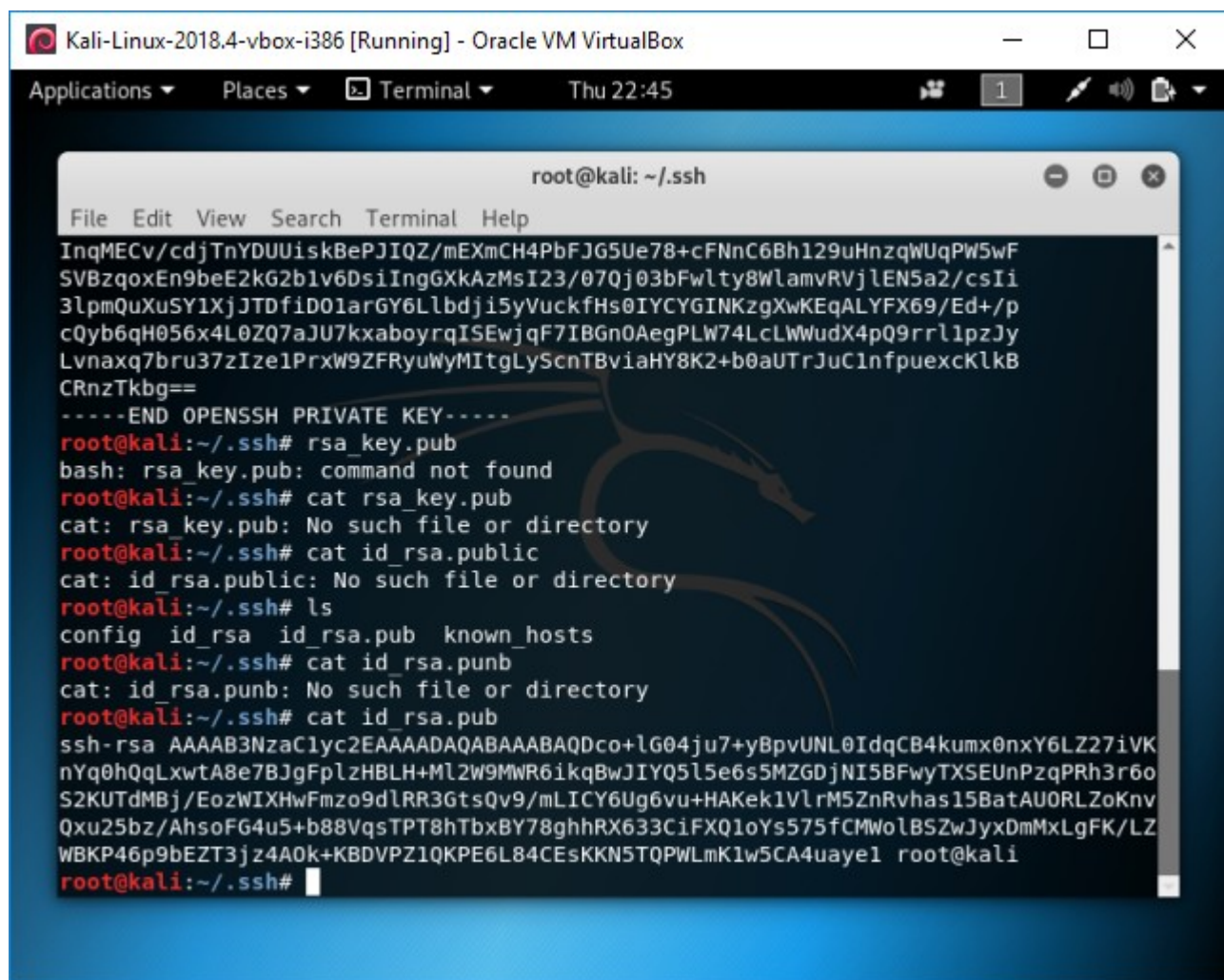
*(SSH'ing into my Chewy after editing the config file.)*

I also edited the file afterwards to configure my SSH config file for the host named dooku.





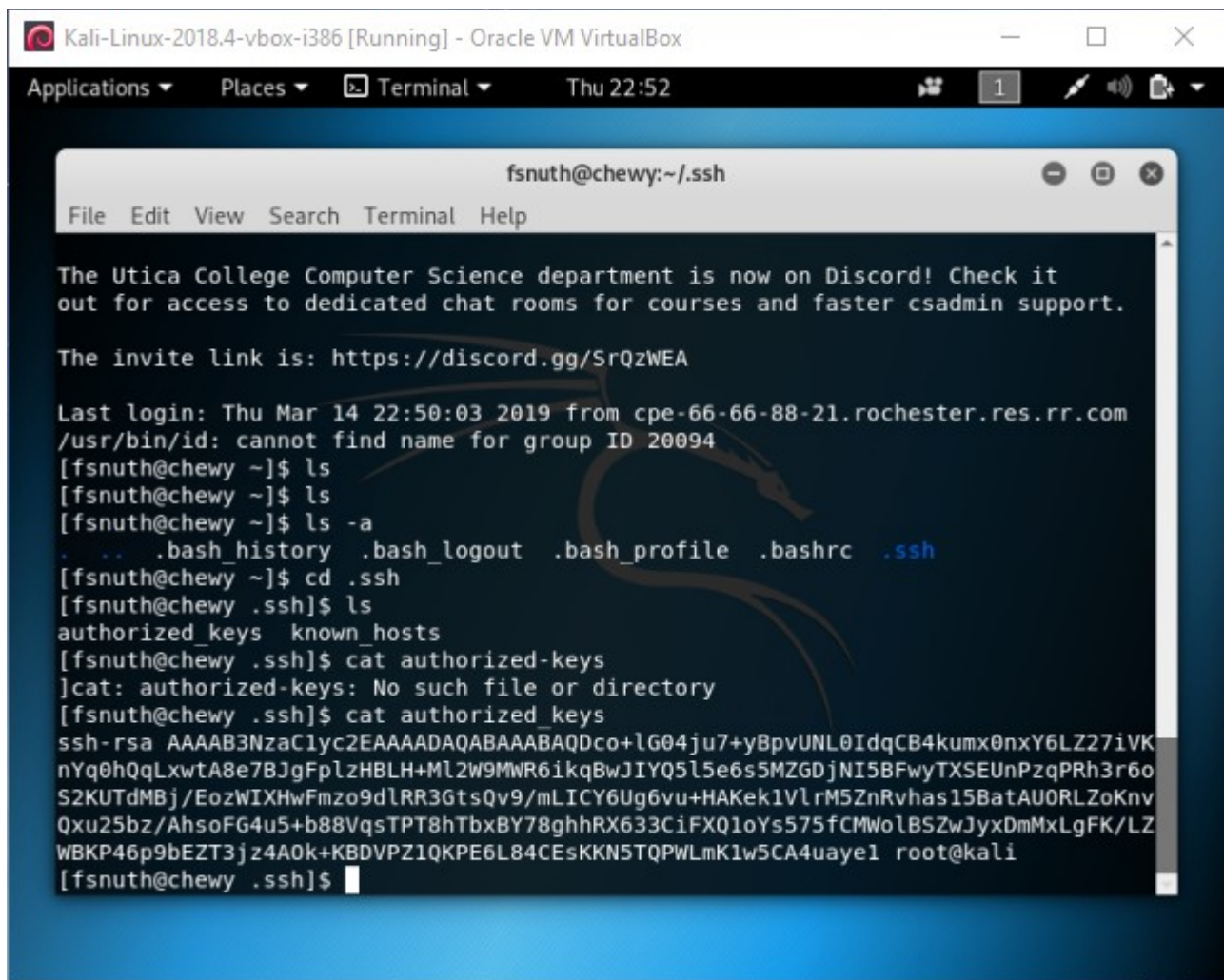
*(Configuring the SSH file for the host named dooku.)*

A screenshot of a Kali Linux virtual machine window titled "Kali-Linux-2018.4-vbox-i386 [Running] - Oracle VM VirtualBox". The window shows a terminal application with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar "root@kali: ~/.ssh". The terminal output shows the generation of an SSH key pair, followed by attempts to view the key files. The public key is displayed in a long single line. The terminal ends with the prompt "root@kali: ~/.ssh#".

```
root@kali: ~/.ssh
File Edit View Search Terminal Help
InqMECv/cdjTnYDUUiskBePJIQZ/mEXmCH4PbFJG5Ue78+cFNnC6Bh129uHnzqWUqPW5wF
SVBzqoxEn9beE2kG2blv6DsiIngGXkAzMsI23/07Qj03bFwltY8WlamvRVjlEN5a2/csIi
3lpmQuXuSY1XjJTDfiD01arGY6LLbdji5yVuckfHs0IYCYGINKzgXwKEqALYFX69/Ed+/p
cQyb6qH056x4L0ZQ7aJU7kxaboyrqISEwjQF7IBGn0AegPLW74LcLWWudX4pQ9rrl1pzJy
Lvnaqx7bru37zIze1PrxW9ZFRyuWyMITgLyScnTBviaHY8K2+b0aUTrJuClnfpuexcKlkB
CRnzTkbg==
-----END OPENSSH PRIVATE KEY-----
root@kali: ~/.ssh# rsa_key.pub
bash: rsa_key.pub: command not found
root@kali: ~/.ssh# cat rsa_key.pub
cat: rsa_key.pub: No such file or directory
root@kali: ~/.ssh# cat id_rsa.public
cat: id_rsa.public: No such file or directory
root@kali: ~/.ssh# ls
config id_rsa id_rsa.pub known_hosts
root@kali: ~/.ssh# cat id_rsa.punb
cat: id_rsa.punb: No such file or directory
root@kali: ~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDco+lG04ju7+yBpvUNL0IdqCB4kumx0nxY6LZ27iVK
nYq0hQqLxwtA8e7BJgFplzHBLH+Ml2W9MWR6ikqBwJIYQ5l5e6s5MZGDjNI5BFwyTXSEUnPzqPRh3r6o
S2KUTdMBj/EozWIXHwFmzo9dlRR3GtsQv9/mLICY6Ug6vu+HAKek1VlrM5ZnRvhas15BatAU0RLZoKnv
Qxu25bz/AhsoFG4u5+b88VqsTPT8hTbxBY78ghhRX633CiFXQ1oYs575fCMwolBSZwJyxDmMxLgFK/LZ
WBKP46p9bEZT3jz4A0k+KBDVPZ1QKPE6L84CEsKKN5TQPWLmK1w5CA4uaye1 root@kali
root@kali: ~/.ssh#
```

*(Generating the SSH keys with “ssh-keygen”).*

I went to my Chewy and configured the files in my .ssh directory. I checked the file “authorized\_keys”, which will show me the public and private keys that I generated earlier.



The screenshot shows a Kali Linux virtual machine window titled 'Kali-Linux-2018.4-vbox-i386 [Running] - Oracle VM VirtualBox'. The terminal window is titled 'fsnuth@chewy:~/ssh' and contains the following text:

```
File Edit View Search Terminal Help

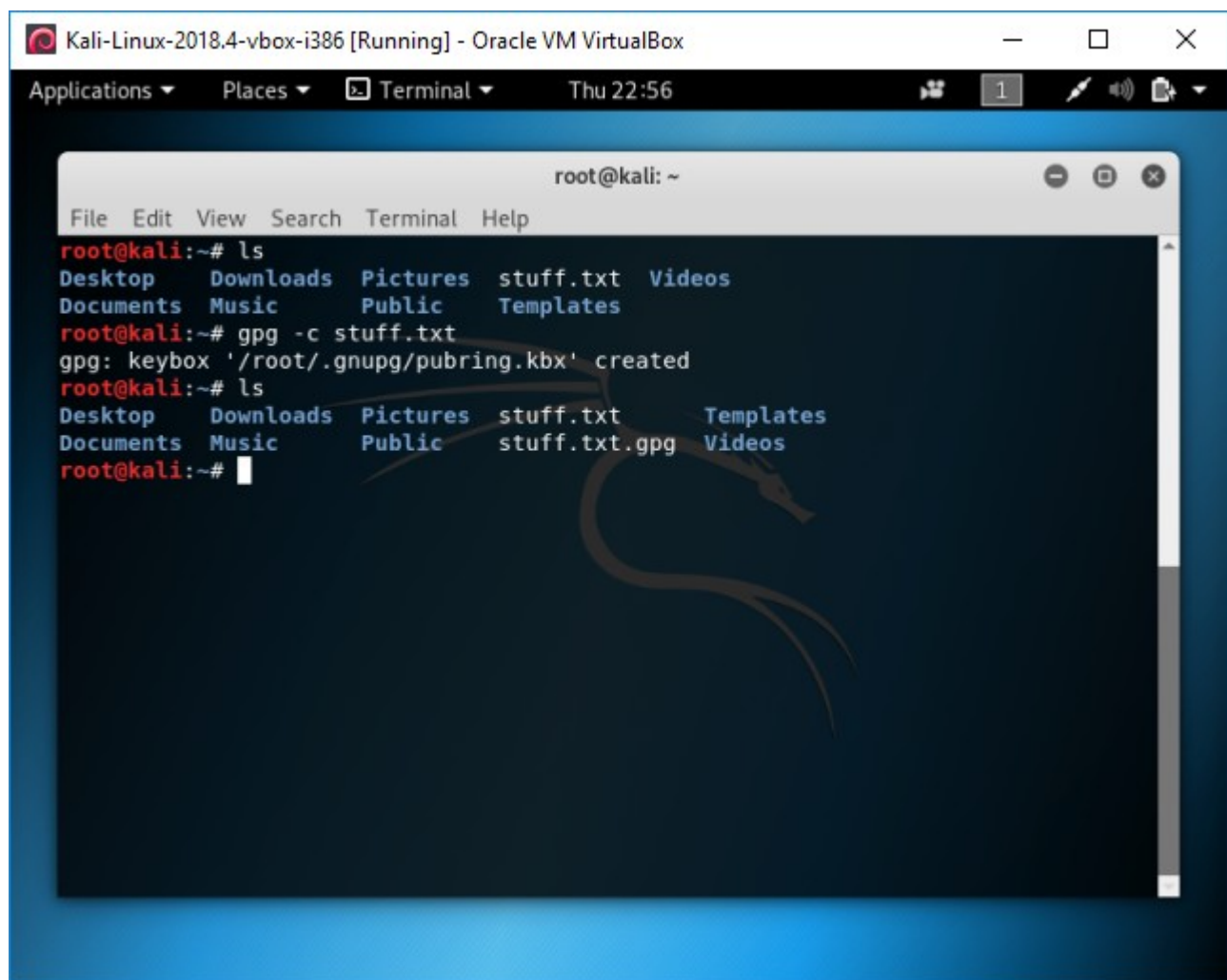
The Utica College Computer Science department is now on Discord! Check it
out for access to dedicated chat rooms for courses and faster csadmin support.

The invite link is: https://discord.gg/SrQzWEA

Last login: Thu Mar 14 22:50:03 2019 from cpe-66-66-88-21.rochester.res.rr.com
/usr/bin/id: cannot find name for group ID 20094
[fsnuth@chewy ~]$ ls
[fsnuth@chewy ~]$ ls
[fsnuth@chewy ~]$ ls -a
. . . .bash_history .bash_logout .bash_profile .bashrc .ssh
[fsnuth@chewy ~]$ cd .ssh
[fsnuth@chewy .ssh]$ ls
authorized_keys known_hosts
[fsnuth@chewy .ssh]$ cat authorized_keys
]cat: authorized-keys: No such file or directory
[fsnuth@chewy .ssh]$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDco+lG04ju7+yBpvUNL0IdqCB4kumx0nxY6LZ27iVK
nYq0hQqLxwtA8e7BJgFplzHBLH+Ml2W9MWR6ikqBwJIYQ5l5e6s5MZGDjNI5BFwyTXSEUnPzqPRh3r6o
S2KUTdMBj/EozWIXHwFmzo9dlRR3GtsQv9/mLICY6Ug6vu+HAKek1VlrM5ZnRvhas15BatAUORLZoKnv
Qxu25bz/AhsoFG4u5+b88VqsTPT8hTbxBY78ghhRX633CiFXQ1oYs575fCMWolBSZwJyxDmMxLgFK/LZ
WBKP46p9bEZT3jz4A0k+KBDVPZ1QKPE6L84CEsKKN5TQPWLmK1w5CA4uaye1 root@kali
[fsnuth@chewy .ssh]$
```

*(Checking the RSA encrypted key in the “authorized\_keys” file on Chewy’s .ssh directory.)*

Finally, I will attempt to use the GNU Privacy Guard to encrypt my files in Kali Linux. First, will encrypt single text files with “gpg -c <filename>” and encrypted multiplied files by putting them in a zip folder and encrypting said zip folder with the same syntax. If I ever need to decrypt any file or zip folder, I just need the password and I am set to decrypt with GPG.

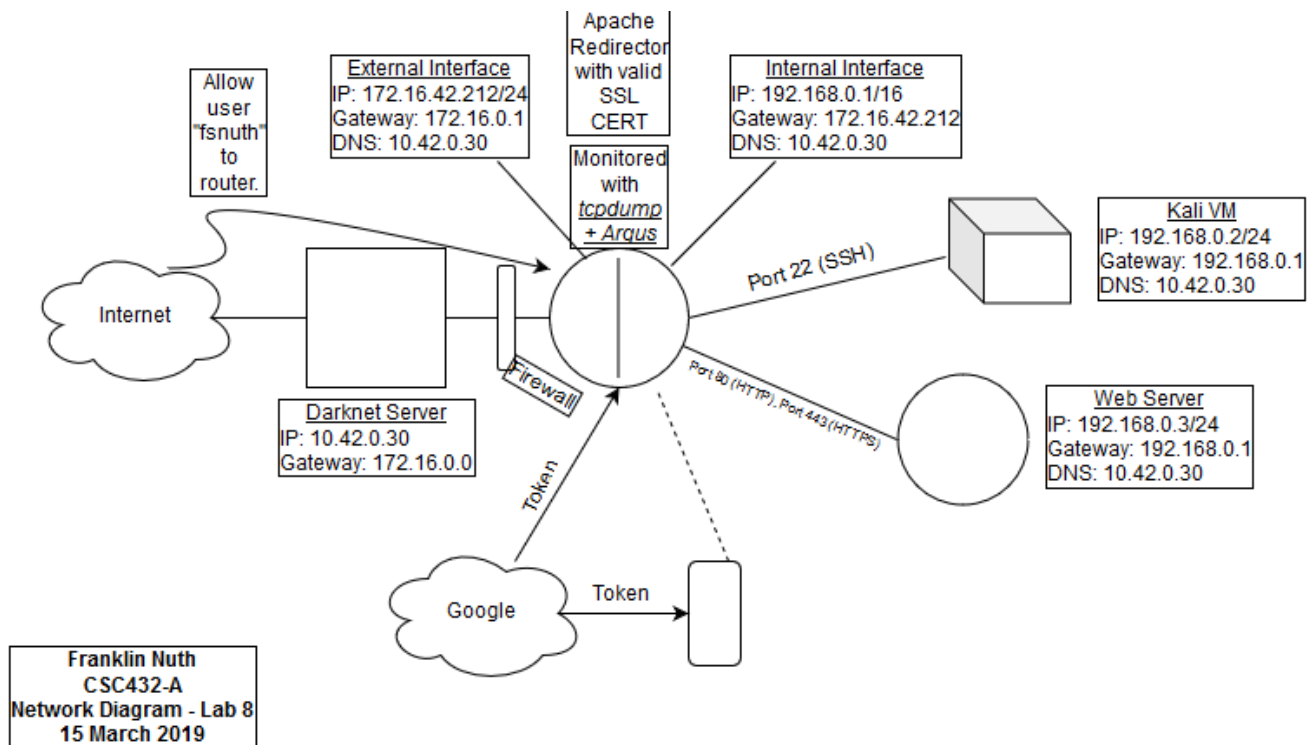
A screenshot of a Kali Linux virtual machine window titled "Kali-Linux-2018.4-vbox-i386 [Running] - Oracle VM VirtualBox". The window shows a terminal application with the following commands and output:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls  
Desktop Downloads Pictures stuff.txt Videos  
Documents Music Public Templates  
root@kali:~# gpg -c stuff.txt  
gpg: keybox '/root/.gnupg/pubring.kbx' created  
root@kali:~# ls  
Desktop Downloads Pictures stuff.txt Templates  
Documents Music Public stuff.txt.gpg Videos  
root@kali:~#
```

*(Encrypting a single file with GPG. I have a normal file called “stuff.txt” and an encrypted file with the same name and a .gpg file extension.)*

```
Zuhairs-MacBook-Pro:Desktop zuhairhallak$ gpg --decrypt franklinEncryptedFile.txt.gpg  
gpg: AES256 encrypted data  
gpg: encrypted with 1 passphrase  
"I am a pointless line of text XD."  
Zuhairs-MacBook-Pro:Desktop zuhairhallak$
```

*(The result of my partner, Zuahir, receiving my encrypted text file and decrypting it with the passphrase I emailed him.)*



*(My network diagram after doing Lab 8. With my Kali, I can easily access the router since it recognizes me by my SSH public and private keys.)*

## Issues & Resolutions

Surprisingly, I did not run into any issues upon doing this lab.

## Conclusion

In this lab, I have manipulated the firewall and network settings of my Kali so I can access my network from any computer with SSH. I have tested out how my IP address works under manual and automatic settings, as well as listening in on certain IP addresses. With SSH key generation, I can use public and private keys so that I only need to enter my password once to access my router. This lab taught me that accessing my router does not always have to be a hassle, and that there are ways to circumvent that. I might also have a bit of fun encrypted my files with GPG in the near future.



## References

Bayden, Asmali. 18 November 2018. *How To Zip, Unzip Files In Linux?* Retrieved from: <http://www.easybib.com/reference/guide/apa/website>

Hoelting, Joel. Hoelting Joel. 2016 October 10. *Video: CLC #1 - GPG Simple File/Folder Encryption*. [Video File]. Retrieved from: <https://www.youtube.com/watch?v=C0l3Oekix2M>