

Lab 4-Encryption

Dawn M Inman

CSC-432 Computer and Network Security

Professor Nick Merante

April 10, 2020

Abstract

This lab sets up easy access through SSH/PuTTY on the Kali2020 virtual machine on the Students desktop, to the chewy and darknet servers. Proxmox was used only in the access it gives to use the QEMU interface to access both CentOS7 (names router) and the students VLE. The CentOS7 routers of chewy and darknet were accessed using PuTTY and SSH via the students Kali2020 which is installed on VMWare virtualization software. The ip address proxy inside of Firefox was altered manually. Encryption was explored with the GNU Privacy Guard software that is on Kali2020 both as a standalone product to encrypt a file as well as sending the product to an email address. Encryption keys and how to obtain them with the GPG program are explored as well. Overall, this was a very successful lab with much accomplishment.

Keywords: CentOS 7, NAT, Kali 2020, Proxmox, QEMU, PuTTY, GPG, IP Proxy.

Lab 4-Encryption

Using SSH and encryption are two ways to keep connections and files secure from malicious users. Preparing the virtual lab to use these tools is necessary to be able to connect to other servers via SSH and send encrypted files for added security. In order to make sure all things are working properly with SSH and shortcuts that can be made for ease of use, many steps need to be taken.

This lab uses the chewy server, darknet server, and one virtual machine set up on the home computer. The virtual routers being used, chewy and darknet, are CentOS 7 routers which work with SSH on port 22 and the virtual computer being run has a Kali 2020 running on VMWare.

CentOS 7 is so named because it stands for Community ENTERprise Operating System. It is based on the Linux kernel, free and has been available since 2004. Red Hat Enterprise Linux is the origination of CentOS 7 so it is a compatible option when requiring Linux software. It is very popular with almost 30% of Linux web servers using it in 2011 and has been one of the most popular in hosting history. (CentOS Blog, 2020)

NAT stands for Network Address Translation. It allows an internal network (private network) to have one internet gateway. This gateway is the CentOS 7 router. The machines on the internal network can have different IP addresses inside the network but when going outside of the router it will appear as if there is only one IP address being used. (Bischoff, 2019)

Kali 2020 is a newer Kali release. It is in the line of Kali environments that have been created for Penetration Testing. The superuser account is no longer being used as the new standard is an unprivileged user that uses kali, kali for user and password, respectively. It has a single installer image, makes NetHunter rootless, improvements to theme and Kali undercover

features and new tools like cloud-enum, emailharvester, phpggc, sherlock and splinter. (g0tmilk, 2020)

Proxmox is also being used by the systems but it is not used extensively in this lab.

Proxmox VE hypervisor is based on GNU/Linux (Debian) and is open source. It has a central web-based management that does not require more installation. (Cheng, 2014) Version 5.4 is built specifically on Debian 9.8 with a “specially modified Linux Kernel 4.15”. (Proxmox, 2019) Proxmox is capable of two types of virtualization: OpenVZ and KVM. OpenVZ needs a patched Linux kernel so Linux guests are the only operating system type that can be created. In OpenVZ, the guests are called containers because they share the same architecture and kernel as the host operating system. (Cheng, 2014) KVM (Kernel-based Virtual Machine) is a modified Linux kernel built with the KVM module so that it can give hardware-assisted virtualization.

Virtualization is performed by a software-based emulator (QEMU) which simulates the virtualized environment while KVM only exposes the /dev/kvm interface. (Cheng, 2014) “This converts Linux into a Type 1 (bare-metal) hypervisor.” (What is KVM?, 2020) Then QEMU or the software-based emulator will create the virtual machines on top of KVM. (What is KVM? 2020) Proxmox VE is relatively simple to start working with but can be very in depth as Simon M.C. Cheng has authored a book called Proxmox High Availability which goes into more detail when setting up a high availability virtual cluster. (Cheng, 2014)

PuTTY is an SSH client for Windows, Mac and Linux. It has a terminal window for access to the server used in this lab, the GNU/Linux server named chewy. (How to use PuTTY on Windows, 2020) SSH is a software package and means Secure Shell. It secures system administration and file transfers even though the networks are insecure. Tatu Ylonen is the

inventor of SSH and OpenSSH which is an open source SSH program is based off of his free versions. (SSH(Secure Shell), 2020)

GPG stands for GNU Privacy Guard and is a hybrid-encryption software program that uses a mix of symmetric-key (both the same) and public-key (public and private keys needed for asymmetric key pairs used during a session). (Wikipedia, 2020) It has extensive applications as well as provides support for SSH. It is free software and was a software used by Snowden to uncover NSA secrets. (GNU Privacy Guard, 2020)

Objective

This lab's purpose is to get the Kali2020VM ready for extensive SSH use. Connections were made to Proxmox VLE, the chewy server, the darknet server and encrypting messages and sending them to email addresses was addressed. There are many steps in lab 4 processes and the Results and Analysis will try to explain all of them.

The computer that is being used is a 2011 HP Pavillion dv7, i7 quad core processor and 16GB RAM with Windows10Pro operating system. Google Chrome is the internet browser being used for connecting to Proxmox. Kali2020VM is on the students' personal laptop inside of VMWare. The Kali2020VM then runs Fire Fox internet browser, PuTTY as the SSH connection and GPG for the encryption software.

Results and Analysis¹

The first few tasks of this lab were simple and began with just logging into the chewy server with putty from a Kali VM machine. The student chose to use Kali 2020 which is a VM on a personal laptop inside of VMWare. This is accomplished through PuTTY using an SSH connection. The student's credentials were types in: dminman@chewy.cs.utica.edu using port 22. After logging in, the student has access to the chewy server.

```

dminman@chewy.cs.utica.edu's password:
Access denied
dminman@chewy.cs.utica.edu's password:
Last failed login: Thu Apr  9 16:26:03 EDT 2020 from c-68-36-43-228.hsd1.mi.comcast.net on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Apr  7 18:03:20 2020 from c-68-36-43-228.hsd1.mi.comcast.net
dminman pts/7      c-68-36-43-228.h Thu Apr  9 16:26   still logged in
dminman pts/2      c-68-36-43-228.h Tue Apr  7 18:03 - 20:42 (02:39)
dminman pts/1      c-68-36-43-228.h Tue Apr  7 17:54 - 18:03 (00:08)

wtmp begins Tue Oct 29 09:42:18 2019
dminman pts/7      c-68-36-43-228.h Thu Apr  9 16:26   still logged in
dminman pts/2      c-68-36-43-228.h Tue Apr  7 18:03 - 20:42 (02:39)
dminman pts/1      c-68-36-43-228.h Tue Apr  7 17:54 - 18:03 (00:08)

wtmp begins Tue Oct 29 09:42:18 2019
[dminman@chewy ~]$

```

Next the terminal on the Kali 2020 VM was opened and this was typed into the command line:

```
ssh -D 1080 dminman@chewy.cs.utica.edu
```

```

dminman@chewy:~
File Actions Edit View 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
dminman@chewy.cs.utica.edu's password:
Last login: Thu Apr  9 16:26:15 2020 from c-68-36-43-228.hsd1.mi.comcast.net
dminman pts/8      c-68-36-43-228.h Thu Apr  9 16:42   still logged in
dminman pts/7      c-68-36-43-228.h Thu Apr  9 16:26   still logged in
dminman pts/2      c-68-36-43-228.h Tue Apr  7 18:03 - 20:42 (02:39)

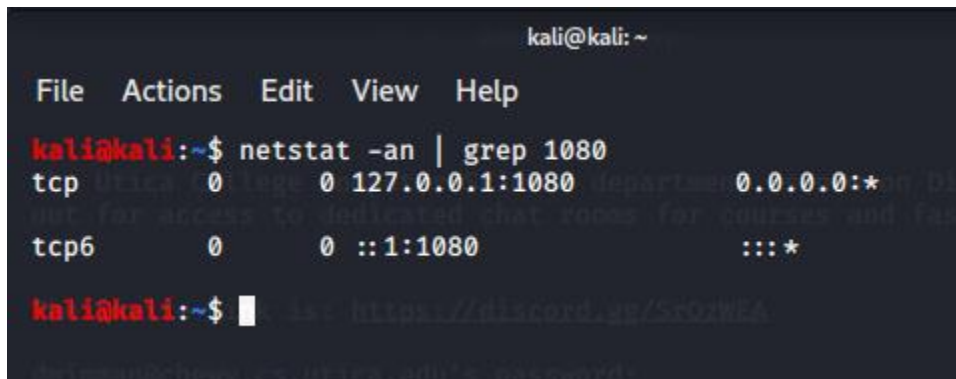
wtmp begins Tue Oct 29 09:42:18 2019
dminman pts/8      c-68-36-43-228.h Thu Apr  9 16:42   still logged in
dminman pts/7      c-68-36-43-228.h Thu Apr  9 16:26   still logged in
dminman pts/2      c-68-36-43-228.h Tue Apr  7 18:03 - 20:42 (02:39)

wtmp begins Tue Oct 29 09:42:18 2019
[dminman@chewy ~]$

```

Another terminal was opened and this was typed in:

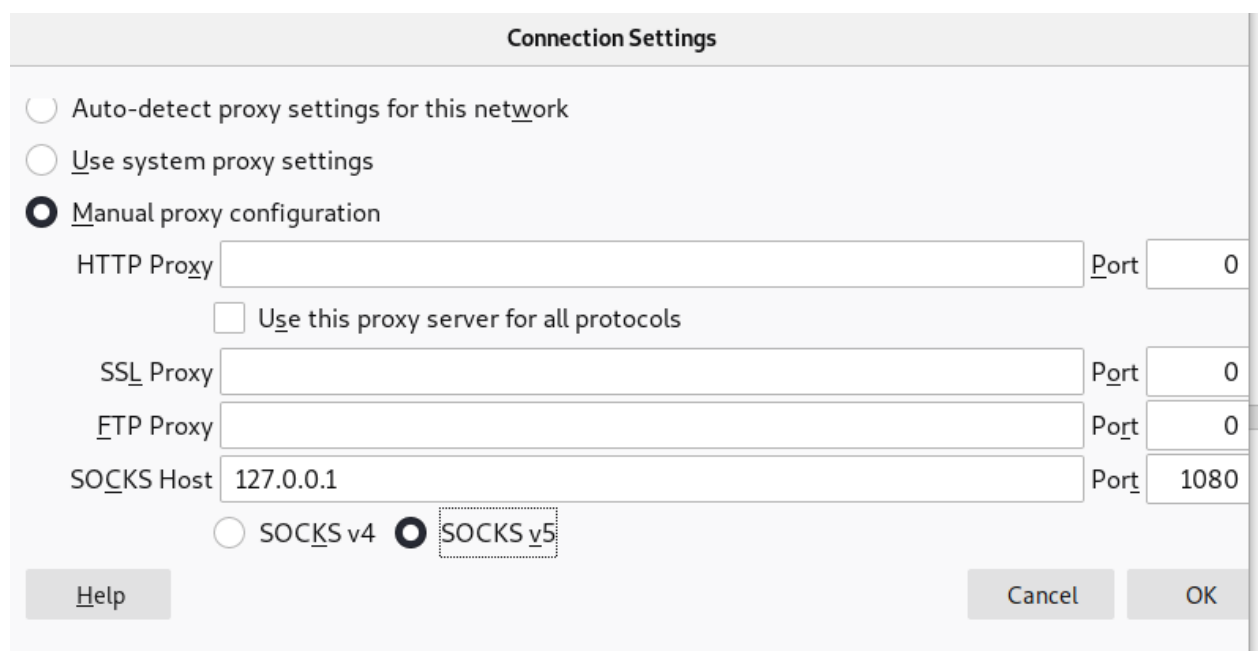
```
netstat -an | grep 1080
```



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ netstat -an | grep 1080  
tcp        0      0 127.0.0.1:1080 0.0.0.0:*  
tcp6       0      0 :::1:1080      :::*  
kali@kali:~$
```

This shows that the system is listening for traffic on port 1080. The next step is to send web traffic to it through the web browser.

Firefox is opened and the sequence of preferences, advanced, network, settings is followed. Manual Proxy server configuration is selected. All areas need to be clear except for the SOCKS host which is manually set to 127.0.0.1, port 80.



Connection Settings

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy Port

☐ Use this proxy server for all protocols

SSL Proxy Port

FTP Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

Help Cancel OK

Typing `https://10.42.0.26:8006` into the web browser goes straight to the VLE portal.

atris - Proxmox Virtual Environment - Mozilla Firefox

Kali Linux, an Offensive x Preferences x atris - Proxmox Virti x IP Chicken - What is x +

https://10.42.0.26:8006/#v1:0:18:4:.....

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

PROXMOX Virtual Environment 5.4-6 Search You are logged in as 'dminman@utica.edu'

Server View

Datacenter

atris

- 301006 (CSC432-dminman-Router)
- 301007 (CSC432-dminman-Kali)
- 301008 (CSC432-dminman-Web)

Datacenter

Search

Search:

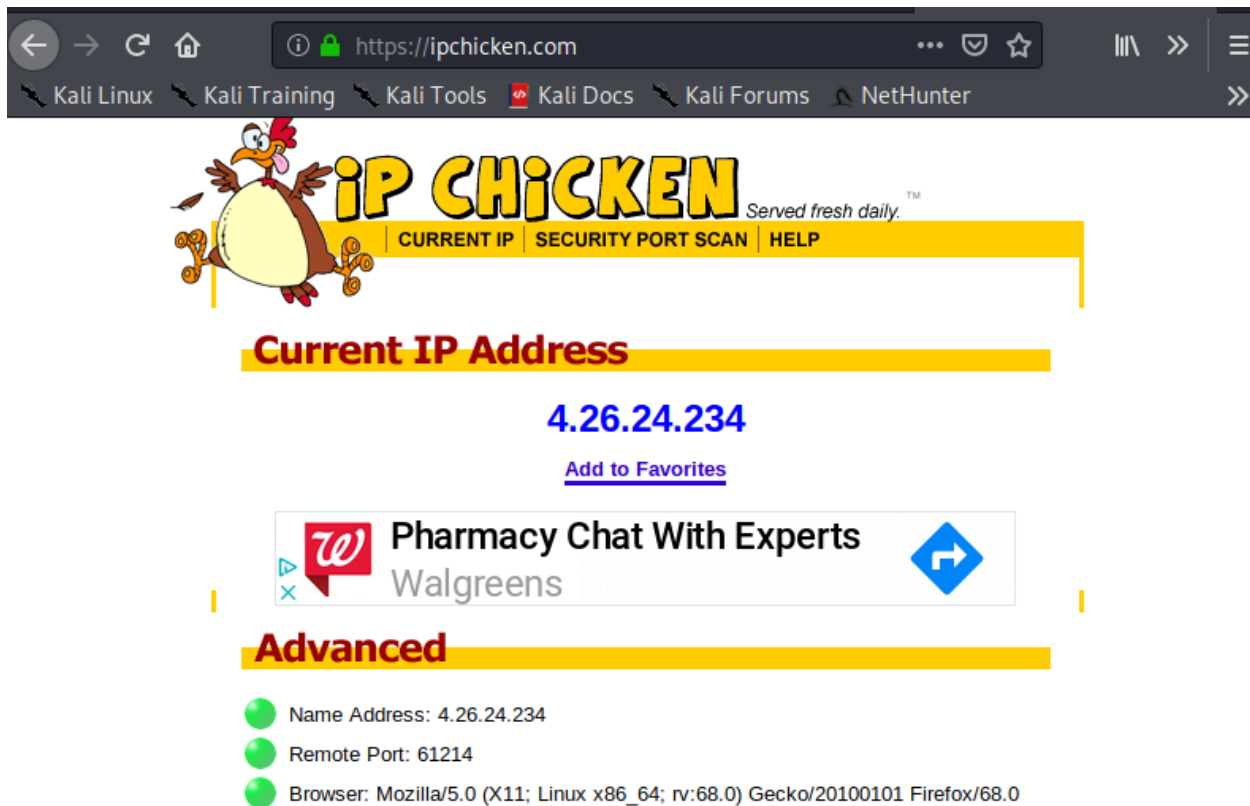
Users

Type ↑	Description	Disk usage %
node	atris	
qemu	301006 (CSC432-dminman-...	
qemu	301007 (CSC432-dminman-...	
qemu	301008 (CSC432-dminman-...	

Tasks Cluster log

Start Time ↓	End Time	Node	User name	De	Status
--------------	----------	------	-----------	----	--------

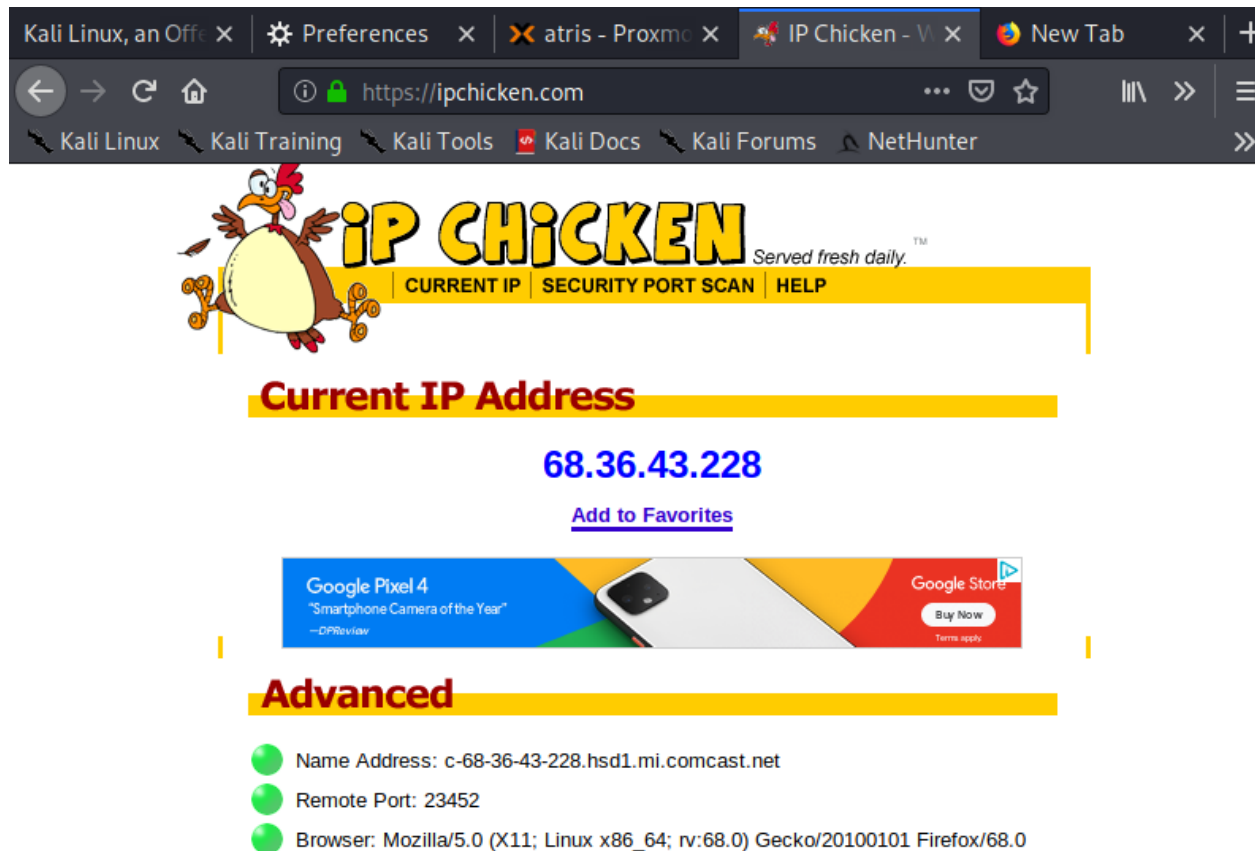
Next the web browser is addressed to <http://ipchicken.com>. The ip address shows as 4.26.24.234.



The screenshot shows a web browser window with the address bar displaying <https://ipchicken.com>. The browser's tab bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, and NetHunter. The website header features a cartoon chicken logo and the text "iP CHICKEN" with the tagline "Served fresh daily.™". Navigation links for "CURRENT IP", "SECURITY PORT SCAN", and "HELP" are visible. The main content area displays "Current IP Address" in a yellow box, followed by the IP address "4.26.24.234" in blue text and a link to "Add to Favorites". Below this is a Walgreens advertisement for "Pharmacy Chat With Experts". The "Advanced" section, highlighted in yellow, lists the following details:

- Name Address: 4.26.24.234
- Remote Port: 61214
- Browser: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

The proxy setting is reset again to automatic. Then <http://ipchicken.com> is accessed again. This changes the ip address to 68.36.43.228.



This feature of automatic changing of a proxy server address could be used during general internet use to remain anonymous during time spent online. It could also be used in a pen testing capacity so that any interaction between the target and oneself is always changing so the address doesn't get blocked by an IPS (Intrusion Detection System) or an alert administrator on the system one is trying to penetrate.

Next an SSH config file is created to customize the environment. This is done by creating a file called config in the .ssh directory. It will allow for aliases and easier access to internal systems through proxy access. This was created in the file using vim at `~/ssh/config` on the Kali 2020VM.

```
kali@kali: ~
File Actions Edit View Help
Host chewy
ForwardAgent yes
HostName chewy.cs.utica.edu
Port 22
User dminman
```

The file is tested by typing in: `ssh chewy`

```
kali@kali: ~
File Actions Edit View Help

By logging into this system you are indicating that you agree to the
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!
Last login: Thu Apr  9 16:26:15 2015 from c-68-36-43-225.had1.mi.comcast.net

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.

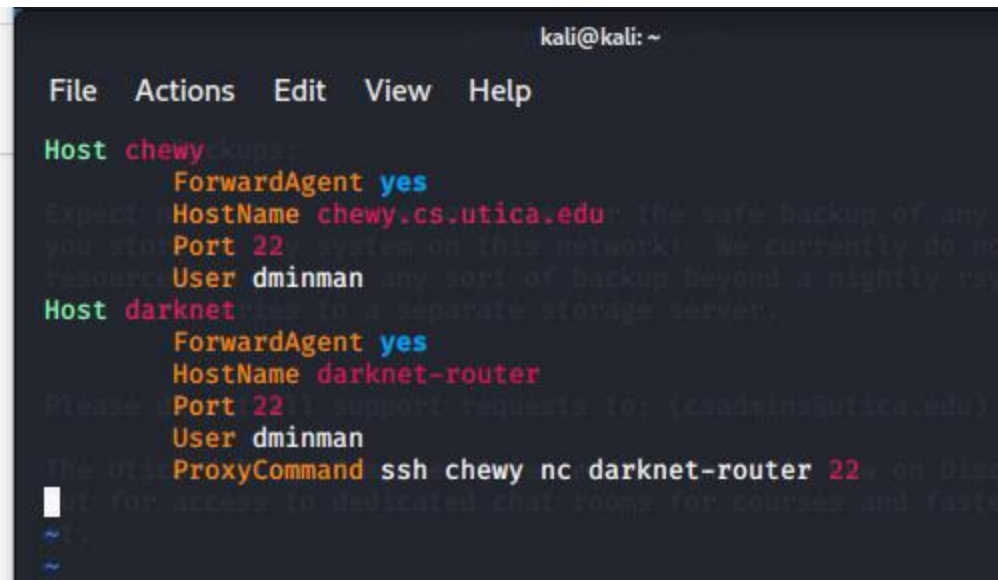
Please direct all support requests to: (csadmins@utica.edu) - NOT IITS!

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

dminman@chewy.cs.utica.edu's password: 
```

This allowed direct access to go to the chewy server without typing in all of the information or address into the terminal.



```
kali@kali: ~  
File Actions Edit View Help  
Host chewy  
    ForwardAgent yes  
    Expect HostName chewy.cs.utica.edu  
    Port 22  
    User dminman  
Host darknet  
    ForwardAgent yes  
    HostName darknet-router  
    Port 22  
    User dminman  
    ProxyCommand ssh chewy nc darknet-router 22
```

The darknet server can be set up in a similar fashion. The darknet server information was added to the `~/.ssh.config` file so that a connection can be created directly to the darknet server. Note that the Host is not indented but all the other information for that specific host uses indents. This is to show what lines belong to what Host. Using this file bypasses the firewalls between the two servers creating a direct ssh connection to darknet, although passwords for each server must be used.

```
File  Actions  Edit  View  Help

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 suppo
rt.

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

dminman@chewy.cs.utica.edu's password:
The authenticity of host 'darknet-router (<no hostip for proxy command>)' c
an't be established.
ECDSA key fingerprint is SHA256:TbxIgoOR06il3TLZMAIg4YdvbhTKU6PpWK1woxG+pAE
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'darknet-router' (ECDSA) to the list of known ho
sts.
dminman@darknet-router's password:
Last login: Fri Apr  3 20:23:47 2020 from chewy.cs.utica.edu
[dminman@darknet-ssh ~]$
```

SSH keys are addressed next. To avoid having to input passwords multiple times, a public/private key pair can be set up. In the Kali 2020VM, a terminal was opened and input:

```
ssh-keygen
```

Following the prompts, the passcode (can be different from the previous passwords) was input and an identification key was saved. The public key was also saved. There is now a key fingerprint and a randomart image.

```

File  Actions  Edit  View  Help
kali@kali:~$ vim ~/.ssh/config
kali@kali:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa.
Your public key has been saved in /home/kali/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:7hvPtD6hKRbWckHIj/ga4vwWiN8MybDvfEp4HDquBMU kali@kali
The key's randomart image is:
+---[RSA 3072]-----+
|
|   . .
|  .  .
| E . +
|
| minmin@owen.cs.utoronto.ca's password:
| o .auth.S.icity of host 'darknet-router (<no hostip for proxy command>)' c
| oO.o.e=.o .blishe.
| B+X. + +oo..ngerprint is SHA256:TbxIgoOR06il3TlZMAIg4YdvbhTKU6PpWK1woxG+pAE
| oBo*o o.o= ..
| oo*++ . .oo=.you want to continue connecting (yes/no/[fingerprint])? yes
+----[SHA256]-----+
kali@kali:~$

```

Cat the files to look at the contents.


```

KJkPv5xLZ6Wo4eZUnSYPVFrioTBdNhV86k0GHRh/WuEEbyEcG1msceiMhXIJfZx0RnVDV5
faupnuNotu1esK78ubqasDjX2FE4YETnkOHudBbmWJ273xq9KD8SqS93IV9rLi5m8pJSq
XS507UBEyIZEFhwNG8I0RnCBBpz9xKGjeSELXgIans74rtTRgyX+mbZAHpDnyahBNHRJRv
lKNKaoAtrQWUNHx40EtNQALZ9HBVfDTAvmHIc7Grb1TiDPDcwM96KHZBZUHH297eI1g1m/
mwv7z0ghUs2DBvJCpYW8KX5+CY5V6g4AAjgdEPnFJo2UHs7VAxDpQXvFujMhCU9GlnBHLB
GKyNZNGQbgve272hLzKM2WwoAHwhHbxHUUddlsoHOZLZgREDgCCWiu4IHnJWheYcRYTWi3
0v8+WJ6/j72rvbJYB0IkGlrLgkgfTzTsZzV9sU8FKEluRjr2digrUSAPjr7zrueq6FivWw
v8zcmjtm/MOTc4+9NZlt1bu0LXpapSNJLWHM3DWlflfnnLIbavIQxI1bKTrPC/Vi/MY14P
7ks7XE+jlpQN+lQ8wO6xEmliuAwU5KttJ/3rQDyIZJa9/mF2bwRKtA1njWibm+hsry8QYy
gFD8LmDiqFM7/Y8fyxgn/17WAbW6ebRs69uqs2yTRNe7xhLqQkQWp1oyfIME1Ekbu6+8Nf
Pp0CA1ZqeQLjqvIoWiOf+auDVqFySLfL9NnPidZWuWymN+RienFC8xsHRiaIfLwLfCe+S
vyCKXaQbnIaiFfNQfu8o6to4WgefCVY+MeT8pSFSDILiWykx/Ef2fWwaeen0+T7HL1l+o8
yHBpKyioAonnF6rWXZCyNTMgJpH3J6jdc9zBppKxVcAMTSQ+buSAdiMJiefKKe39VUda8V
cMXiJGftFLbXX5JNNSK107k11+ps6/Xoj8pt92hUkhcUnSwukUEjDzyZs+8We3XJWgdoK
eFPHiU8ge5H5XIGwsX4WhJmPNYAMY3/JHK0Zj2Ydc83E5bS9ckTPcxDKksE+EYnoJnWe7Y
z/sgQA=
-----END OPENSSH PRIVATE KEY-----
kali@kali:~$ cat /home/kali/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQCPZH+RZ+n//4vDPhzqFMTnOmV1xUMHLnuieS
dgrHWYpv+6+vFtZEn42tPYtbCRdny5+pzDtwFW2r71jLAoymOtQkBZIQ/i5yYuCum8SQdKXQHsz
H01jyTKGaNTJfYCYZbmLq9CWfNqELpA6hS8NbbWjhZ+UB9tbGQZOIOUX7RaUJm5/30yEb8FycSU
b5WpkUXjmBahMcMA8WbKTzfandUsxLW5f4d0EHCTyUIZLfSJCJ/o9y7LiTczgHd1hnazafwVDGL
xtWGM7maNi/JrqOCl1tvobFakCXwHz/ZzUNv6xaUL0ZzzytAuT+w9gZDo501QxEmXfI5tOnDbgO
fi91egY1di397yrnz4pDSqzZyE4sahGPqbr2ZwF0PR98vUfXyuffnzgD00lhSjog6V/K9IFBmGN
30N7Fo+xfesEQ9pXNhLAqinfZVhEuKTVYQ+MGcFtqn6+aDD5EP1B505hwVIJXuxfQME4rhBJ84
ORYusqdkXBqAl6V91Thy0GUUa8= kali@kali
kali@kali:~$

```

Next the public key needs to be pushed to chewy so that instead of needing a password, the key is used to authenticate.

```
Ssh-copy-id -I ~/.ssh/id_rsa.pub chewy
```

The password for chewy will need to be entered, and then the passcode. Then Kali2020 VM is logged into chewy. Verify the public key with the following commands. When using ssh chewy, if everything is correctly done, the passcode will be asked for instead of the password.

```
ssh chewy
```

```
cd ~/.ssh
```

```
cat authorized_keys
```

This is where the public keys are contained. The student wanted to change the passcode, so went back into the authorized keys, deleted them and started over. This allowed the student to successfully change the passcode.

```
The Utica College Computer Science department is now on Discord! Check it
out for access to dedicated chat rooms for courses and faster csadmin suppo
rt.
The invite link is: https://discord.gg/SrQzWEA

Enter passphrase for key '/home/kali/.ssh/id_rsa':
Last login: Thu Apr  9 19:54:43 2020 from c-68-36-43-228.hsd1.mi.comcast.ne
t
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:59 still logged in
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:54 - 19:55 (00:01)
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:38 - 19:38 (00:00)

wtmp begins Tue Oct 29 09:42:18 2019
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:59 still logged in
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:54 - 19:55 (00:01)
dminman pts/1 c-68-36-43-228.h Thu Apr  9 19:38 - 19:38 (00:00)

wtmp begins Tue Oct 29 09:42:18 2019
[dminman@chewy ~]$
```

Next, the same process was done for the darknet server. First, log out of chewy back into the local Kali2020VM. Then type into the command line to copy the public SSH key to darknet:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub darknet
```

The passcode will need to be entered a couple times, then the Utica password. After logging back in using the command

```
ssh darknet
```

The passphrase was entered in twice and went straight to the darknet server.


```
Enter passphrase for key '/home/kali/.ssh/id_rsa':  
Enter passphrase for key '/home/kali/.ssh/id_rsa':  
Last login: Thu Apr 9 19:30:22 2020 from chewy.cs.utica.edu  
[dminman@darknet-ssh ~]$
```

The final portion of this lab is about file encryption and shows how to encrypt and decrypt files. A file is made on the Kali2020VM of quotes inside the home directory. ~/quotes

The file is encrypted with the gpg utility by typing this into the command line. The -c mean that gpg will encrypt with a symmetric cipher using a passphrase. The default is AES-128 but can be changed with the --cipher-algo option. Also, -c can be combined with other options like -sign or -encrypt.

Gpg -c ~/quotes

A password will need to be entered and verified, then the new file is created using a .gpg extension.

To decrypt the file type in the command line

gpg quotes.gpg

```
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  quotes.gpg  Templates  Videos
kali@kali:~$ gpg quotes.gpg gpg: CAST5 encrypted data
gpg: WARNING: no command supplied. Trying to guess what you mean ...
usage: gpg [options] [filename]
kali@kali:~$ gpg quotes.gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
kali@kali:~$ ls
Desktop  Downloads  Pictures  quotes  Templates
Documents Music     Public   quotes.gpg  Videos
kali@kali:~$ cat quotes
Quotes using the names of my cats.

Marshmallows don't burn, they carmelize.
Do you know the Muffin man?
Dream as if you will live forever, eat Cupcakes like you will die today.
I love the smell of Pastels, that breathes life into my soul.
kali@kali:~$
```

Figure 1 quotes decryption

On linuxhint.com there are instructions on how to encrypt and decrypt files using gpg. These instructions include how to generate public and private key pairs, so a walk through was done and the results are as follows: (Azad, 2019)

The file quotes.gpg was removed via `rm quotes.gpg`

Update gpg by using `apt-get install`.

```
sudo apt-get install gpg -y
```

A key pair is generated.

```
sudo su
```

```
gpg --full-gen-key
```

It asks what type of key, option 1 is chosen which is RSA.

Next it asks the size. 3072 is suggested so that is used by typing it in.

Then the length of time is chosen, 6 weeks.

Confirm the choice, then a user id is needed to identify the key, dminman with the email address dminman@utica.edu and the comment of lab 4. Confirm with o for okay, then a passphrase is chosen to protect the new key. The passphrase needs to be at least 8 characters with one digit and possibly one special character. That was what was used and it worked perfectly.

```
pub  rsa3072 2020-04-09 [SC] [expires: 2020-05-21]
     21CE9D72C8800A64FBD784FDFCC9FEE454FF7171
uid                               dminman (lab 4) <dminman@utica.edu>
sub  rsa3072 2020-04-09 [E] [expires: 2020-05-21]
root@kali:/home/kali#
```

This can be used to encrypt and decrypt files. This will be tested on a new file.

```
mkdir gpg
```

```
cd gpg/
```

```
vi encrypted.txt
```

At this point, the file is created and text is entered to have something to encrypt. The file is saved and exited.

```
cat encrypted.txt
```

The file is encrypted by specifying the user email in generated key pair by the following:

```
gpg -r dminman@utica.edu -e encrypted.txt
```

```
ls -la
```



```
root@kali:/home/kali/gpg# rm encrypted.txt
root@kali:/home/kali/gpg# ls
encrypted.txt.gpg
root@kali:/home/kali/gpg# gpg -d encrypted.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID 9C4346DE595E6B13, created 2020-04-09
      "dminman (lab 4) <dminman@utica.edu>"
This file is going to be encrypted for use during lab 4.
Everything I need to encrypt this file and decrypt it will
be explained in the lab. If everything goes well, this file will be here
for a while to run tests on.
root@kali:/home/kali/gpg#
```

Each email that is sent to a different user needs to have a new encryption process for a new key. If the email is a persons' own email address, adding the email to the list of trusted users is possible but not necessary. This can be accomplished most easily in the gpg gui interface per the instructions at <https://gpgtools.tenderapp.com/kb/how-to/add-more-email-addresses-user-ids-to-your-existing-key>.

Conclusion.

This lab was successful at setting up the SSH settings and PuTTY to be able to SSH straight to the darknet server without having to log into the chewy server first. It also was successful at showing how the SSH process works and how messages can be encrypted and sent to someone's email. Not many problems presented themselves but one of them was when the darknet server information was added to the .ssh file. At first the information did not work. When the student looked at other files done a similar way online, the Host was not indented but the rest of the information was, and once that was done it fixed all the issues. Overall the student enjoyed the lab and hopes to make use of the knowledge during the class project and at a future internship and career. Excellent lab.

References

- Abrams, Lawrence. (November 29, 2019). *Kali Linux adds 'undercover' mode to impersonate Windows 10*. BleepingComputer. Retrieved from <https://www.bleepingcomputer.com/news/security/kali-linux-adds-undercover-mode-to-impersonate-windows-10/>
- Add more email addresses (user ID's) to your existing key. (October 18, 2019). GPGTools Support. Retrieved from <https://gpgtools.tenderapp.com/kb/how-to/add-more-email-addresses-user-ids-to-your-existing-key>
- Azad, Usama. (2019). How to encrypt/decrypt files using gpg. Retrieved from https://linuxhint.com/encrypt_decrypt_files_gpg/
- Centos Blog (2020). *What is Centos?* Retrieved from <https://www.centosblog.com/what-is-centos/>
- Cheng, Simon M.C. (October 27, 2014). *Basic concept of ProxMox Virtual Environment*. Packt. Retrieved from <https://hub.packtpub.com/basic-concepts-proxmox-virtual-environment/>
- Ellingwood, Justin. (August 20, 2015). *How to forward ports through a Linux gateway with iptables*. Retrieved from <https://www.digitalocean.com/community/tutorials/how-to-forward-ports-through-a-linux-gateway-with-iptables>
- Elwood. (November 26, 2019). *Kali Linux 2019.4 release*. Kali Linux News. Retrieved from <https://www.kali.org/news/kali-linux-2019-4-release/>
- g0tmi1k. (January 28, 2020). Kali Linux 2020.1 release. Retrieved from <https://www.kali.org/releases/kali-linux-2020-1-release/>
- GNU Privacy Guard. (2020). Gnupg.org. Retrieved from <https://gnupg.org/>

GNU Privacy Guard. (February 17, 2020). Definition from Wikipedia. Retrieved from
https://en.wikipedia.org/wiki/GNU_Privacy_Guard

Kenlon, Seth. (June 24, 2019). Secure your Linux network with firewall-cmd. Retrieved from
<https://www.redhat.com/sysadmin/secure-linux-network-firewall-cmd>

Proxmox. (April 11, 2019). Proxmox.com Retrieved from
<https://www.proxmox.com/en/news/press-releases/proxmox-ve-5-4>

RobertRSeattle. (March 13, 2017). *Start ssh automatically on boot*. AskUbuntu. Retrieved from
<https://askubuntu.com/questions/892447/start-ssh-automatically-on-boot>

Singh, Shiv. (August 22, 2016). How to SSH on a port other than 22. Retrieved from
<https://askubuntu.com/questions/264046/how-to-ssh-on-a-port-other-than-22>

SSH(Secure Shell). (2020). SSH.com. Retrieved from <https://www.ssh.com/ssh>

Vance, Nathan. (February 2, 2017). Understanding Firewall in multi-zoned configurations.
Retrieved from <https://www.linuxjournal.com/content/understanding-firewall-multi-zone-configurations>

RobertRSeattle. (March 13, 2017). *Start ssh automatically on boot*. AskUbuntu. Retrieved from
<https://askubuntu.com/questions/892447/start-ssh-automatically-on-boot>

Lab Network Topology

Kali2020VM--VMWare ethernet adapter--Student HP----(internal –router—external)

192.168.22.136 192.168.22.1 10.0.0.17 10.0.0.1 192.168.104.161

/

/

WWW

|

Gateway 10.42.0.1

|

chewy 10.42.0.31/16

|

darknet 172.16.0.3/16

|

External 172.16.242.32

router

Internal 192.168.11.1

/

\

Kali VM 192.168.11.10

WebServerVM 192.168.11.15