# Cyber Security Report

CMP5329 – Coursework Log format

Jaspreet Singh
Student ID: 19150299

# Lab 1: Encrypting and Decrypting with OpenSSL

This lab use various mechanisms can be the cryptography and cryptographically secure hash functions, the digital signatures, certificates and PKI (Public Key Infrastructure), specifically, OpenSSL will be used.

The SSL and TLS are important certificates that keep internet connection secure and safeguard any sensitive data that is being sent between two systems.

Cryptography is the process of converting between readable text, and an unreadable form, is used to protect confidentiality of information other than protect it during the transmission,

Cryptographic techniques involve different methods, made specific by the use of keys.

- Algorithms that use a shared key are known as symmetric algorithms.
- Algorithms that use public and private key pairs are known as asymmetric algorithms.

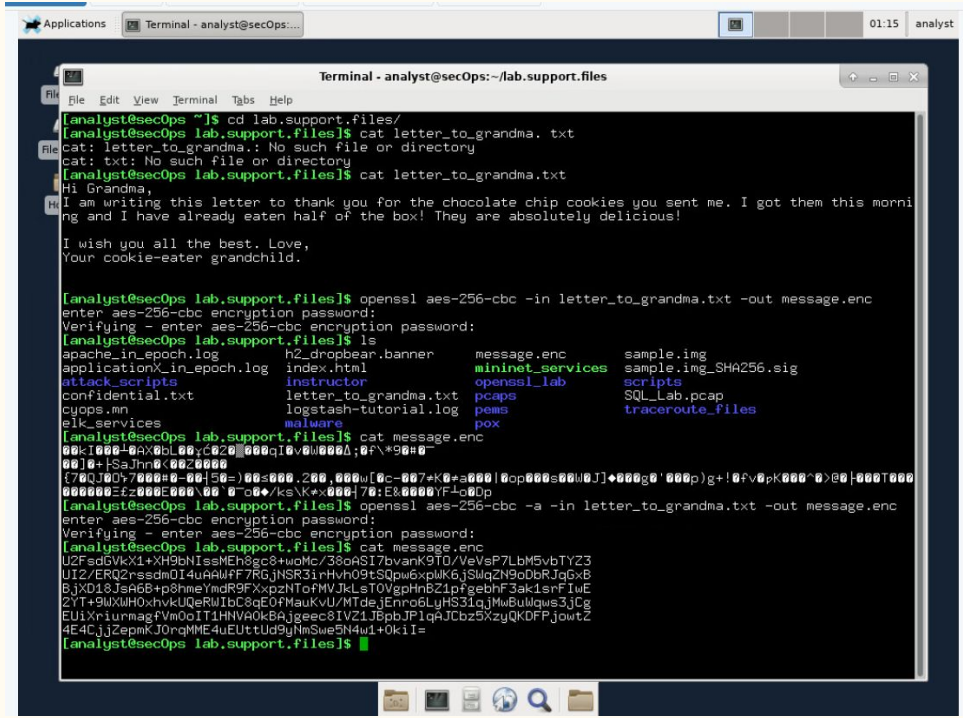
One of the biggest disadvantages is that you have to share the secret key somehow, however if an attacker finds out what the secret key is. Then files that were encrypted with that secret key are now compromised.

# Lab 1: Encrypting and Decrypting with OpenSSL

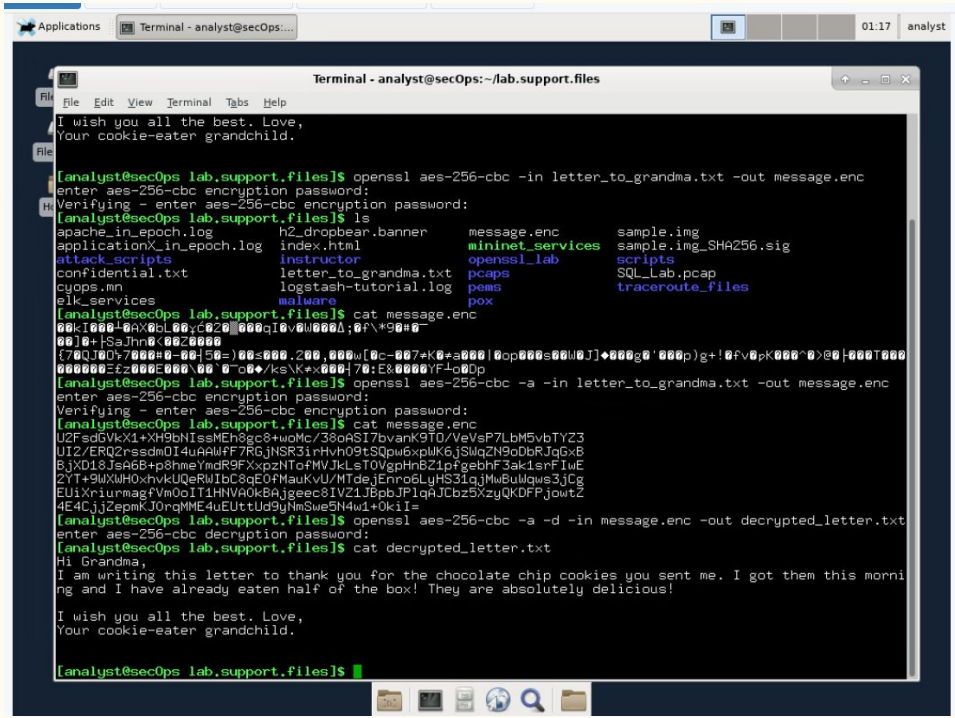
Open the directory with the txt file containing the message to encrypt with AES-256 command with the “cyberops” password and then the file won't appear readable but in fact encrypted.

Now the file is encoded by running the OpenSSL command again, but this time by adding the -a option to tell the system to encode the file as base64.

After this step the message is displayed again with the cat command.



# Lab 1: Encrypting and Decrypting with OpenSSL




The message will now be decrypted and will ask for the same password used during the encryption process.

Now when the message is displayed it will be readable as same as it was before the encryption.

The Base64 could be easily missed causing confusion and errors.

Is important to select a strong password.

# 2. Lab 3: Access Control

Access Control refers to the control over access to system resources after a user's account credentials have been authenticated and access to the system has been granted to it.

For example, a particular user, or group of users, might only be permitted access to certain files after logging into a system, while at the same time being denied access to some other resources.

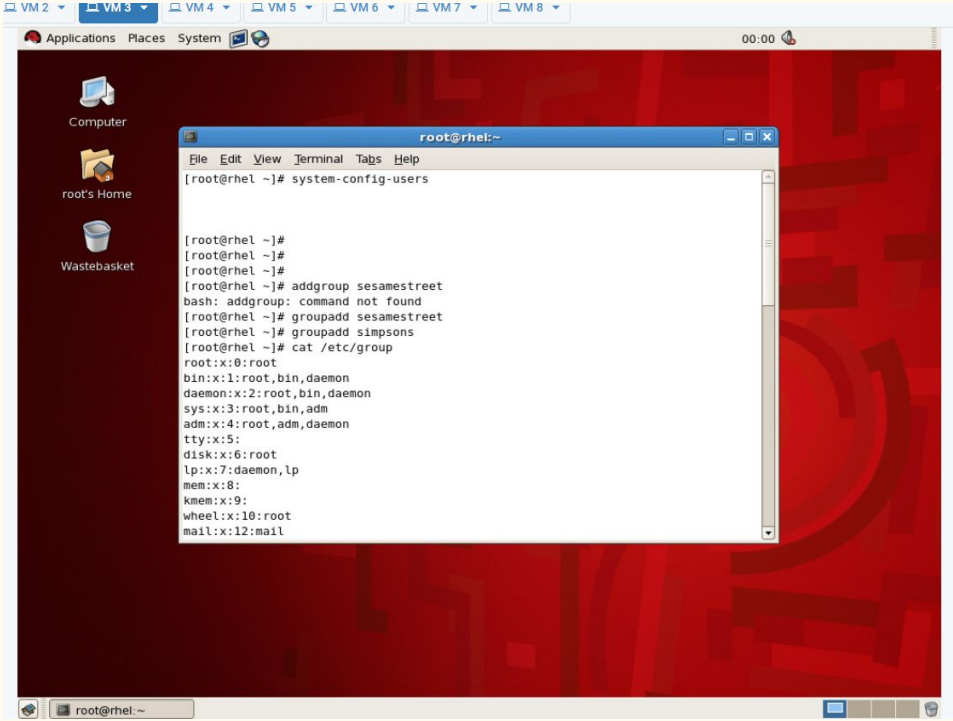
There are various types of access control:

- Discretionary Access Control ( DAC)
- Mandatory Access Control (MAC)
- Role-based Access Control (RBAC)
- Rule-based Access Control

# 2. Lab 3: Access Control

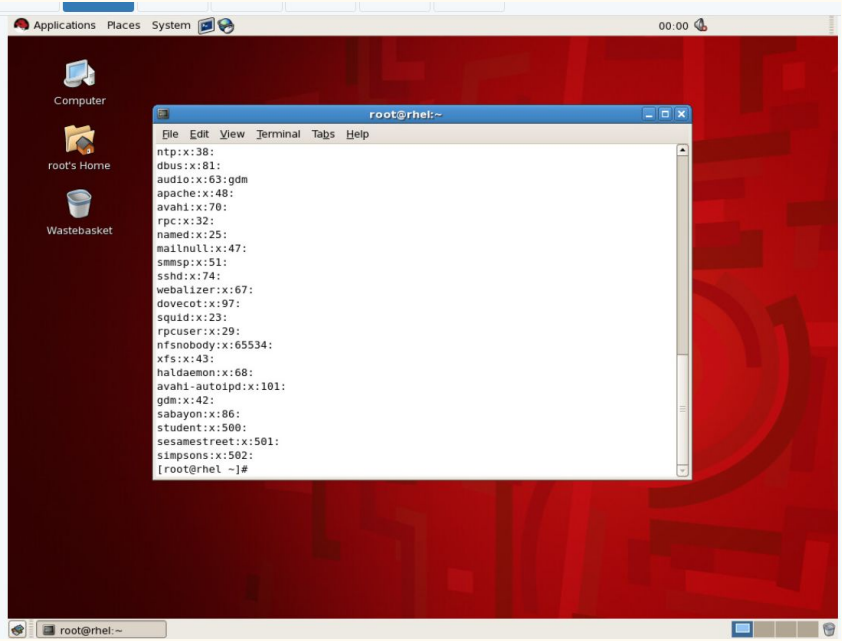
Open Red Hat Linux virtual machine login and open the terminal to reach the user manager windows that can be used to see all the groups and users present in the system.

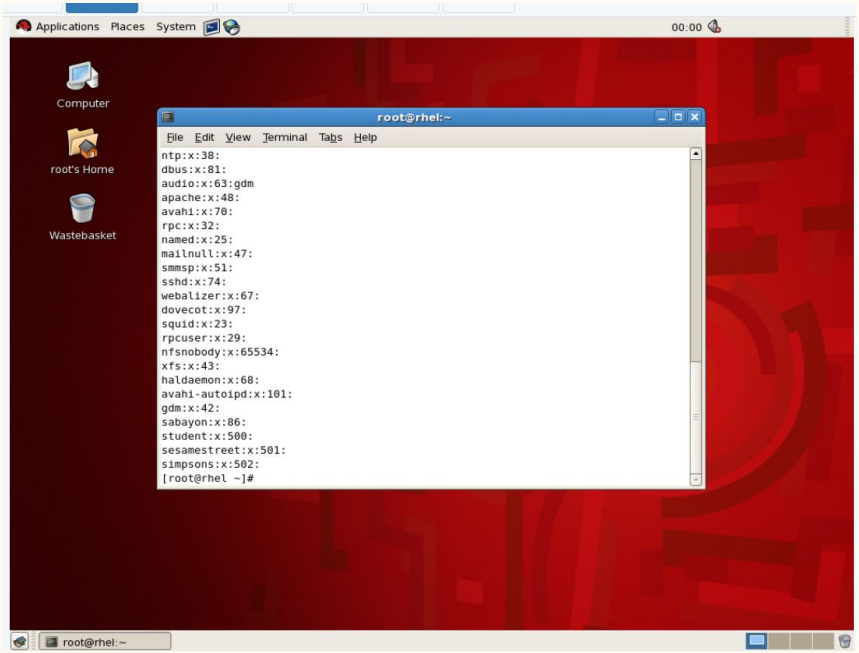
Once closed we can move to start adding new groups with the addgroup command and then display them with another command.



# 2. Lab 3: Access Control

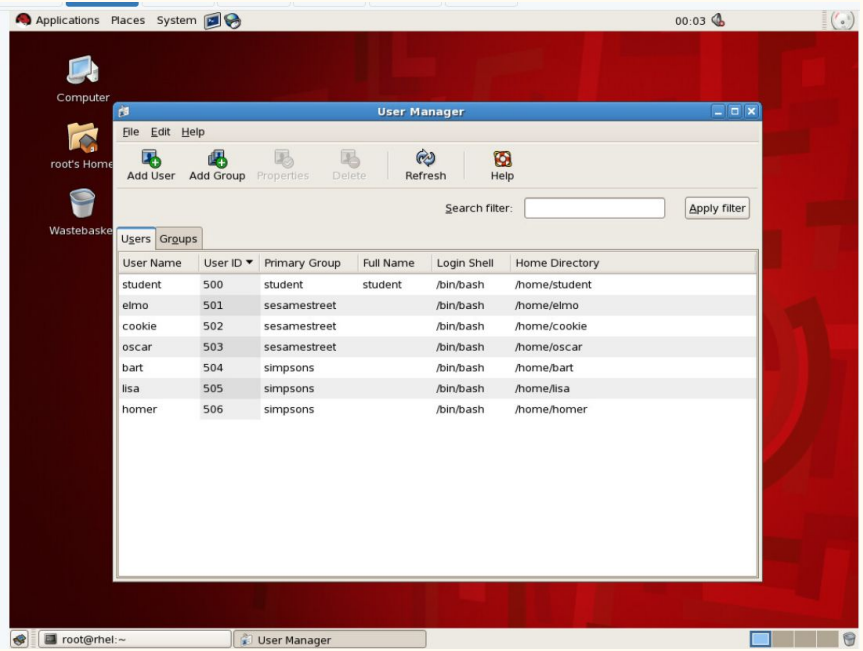
Time to add the users with the useradd command to each group.

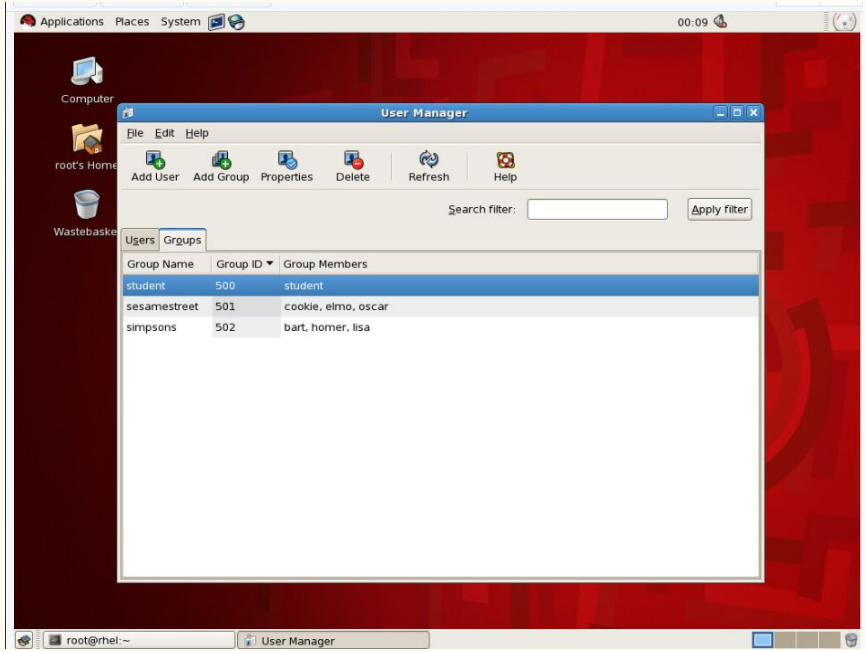


# 2. Lab 3: Access Control

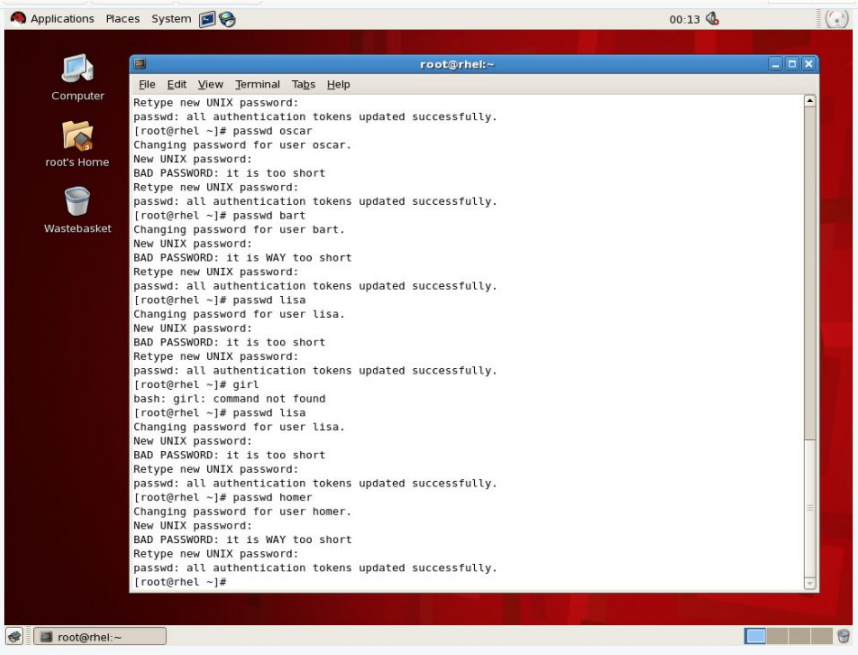
After adding the various users the user manager is used to control if all the groups and users have been correctly inserted.

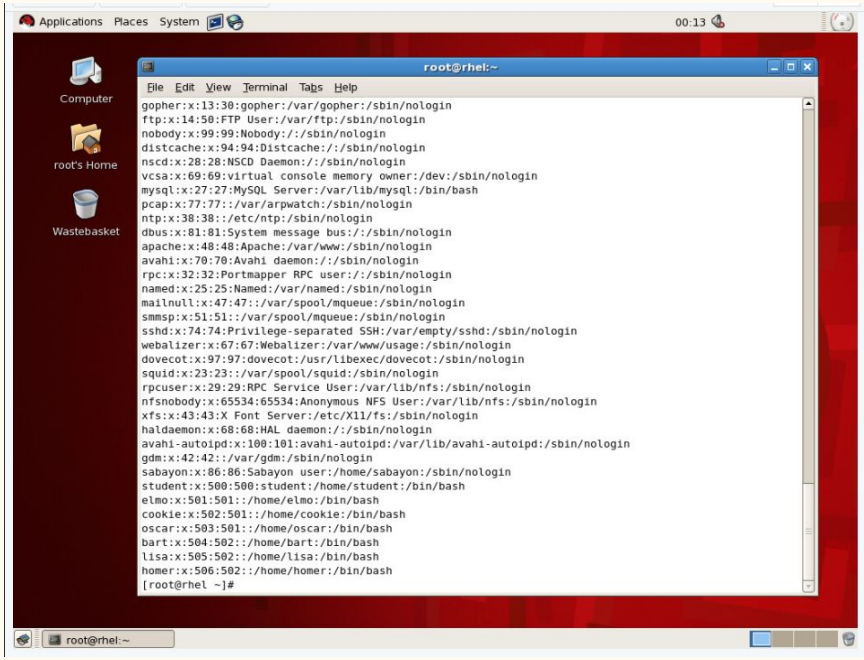


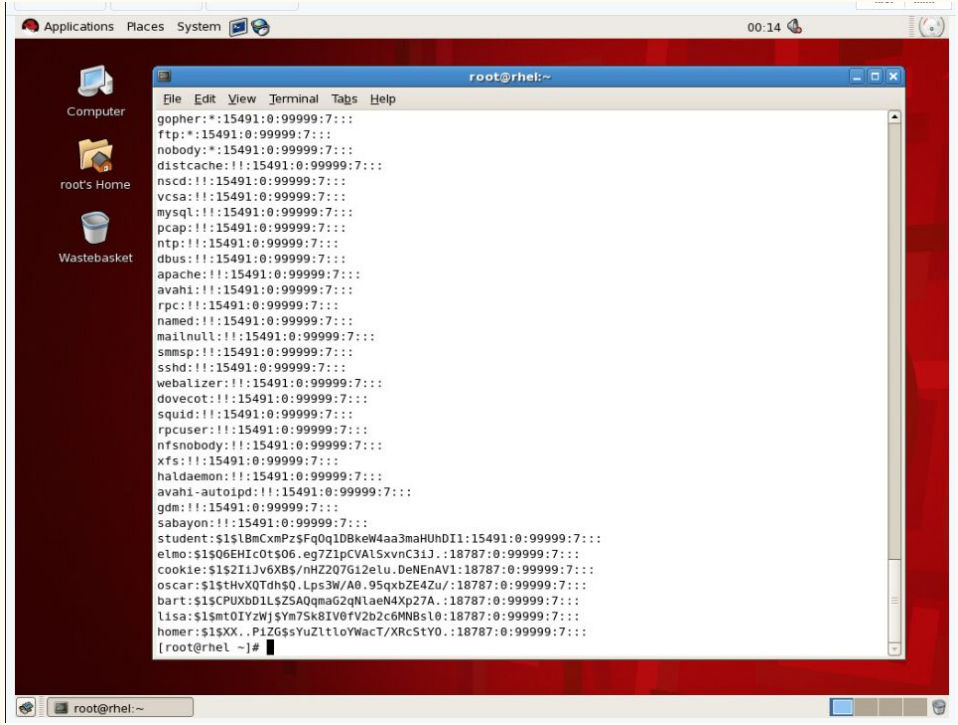
# 2. Lab 3: Access Control

All the passwords for the various users are created with the passwd command and it shows the users in the passwd file where we can see their directory too.



# 2. Lab 3: Access Control

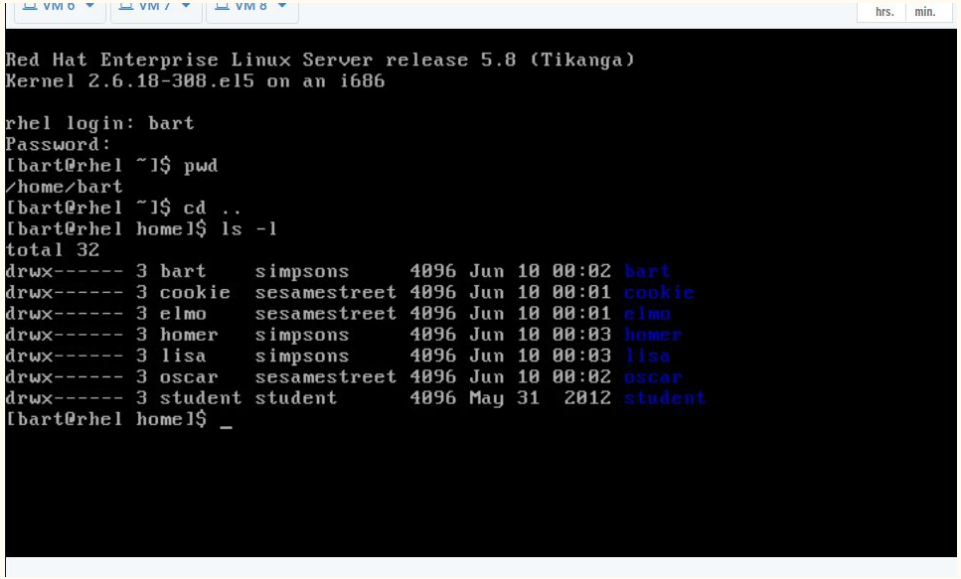



Now with the command cat /etc/shadow we can create the shadow file disponible to the root with all the details of the users created before.

# 2. Lab 3: Access Control

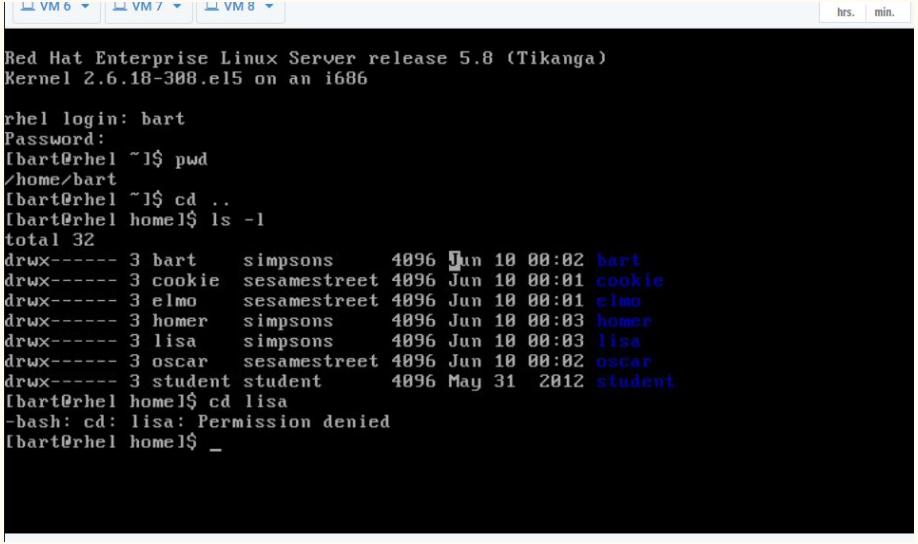
Now we can login in the accounts and experiment with their permissions but first the system should be restated with the init 6 command.

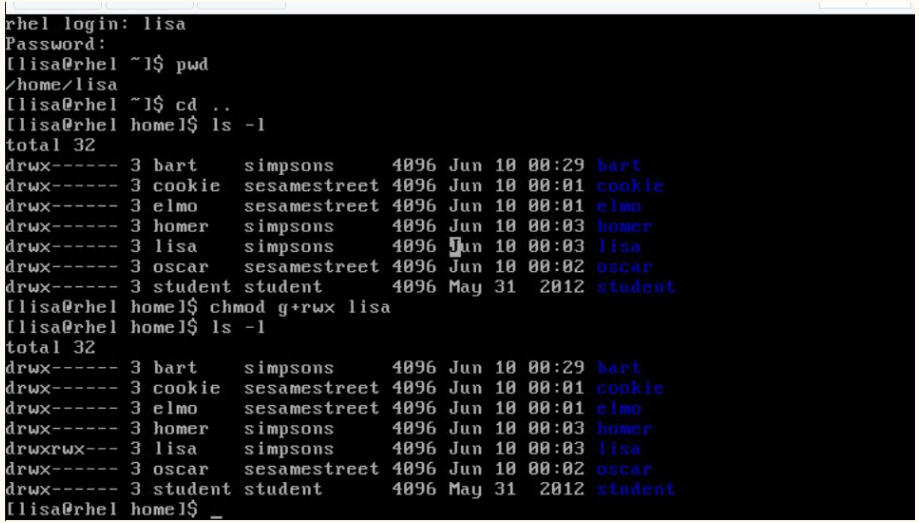
After logging in with the “bart” account we can go to it’s directory using the command pwd and then go back with the cd .. command and then display the list of the various directories present with the permissions on front for each user’s directory.



# 2. Lab 3: Access Control

When using the command cd to enter into another user's directory from the bart user the terminal shows that it doesn't have the permissions to do so and it shows permission denied.
Once logged in with the lisa account the chmod command is used to add special permissions to the lisa's group and it is now possible to see the permissions of the lisa's directory is now changed.



# 2. Lab 3: Access Control

Now if the bart account in the same group as lisa try to access the directory it will show it without the permission denied message.

If another group's account, in this case elmo, tries to access Lisa's directory, the system will still show the permission denied message.

```
Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel 2.6.18-308.el5 on an i686

rhel login: bart
Password:
Last login: Thu Jun 10 00:27:00 on tty1
[bart@rhel ~]$ cd ..
[bart@rhel home]$ cd lisa
[bart@rhel lisa]$ whoami && pwd
bart
/home/lisa
[bart@rhel lisa]$ exit_
```

```
Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel 2.6.18-308.el5 on an i686

rhel login: elmo
Password:
[elmo@rhel ~]$ pwd
/home/elmo
[elmo@rhel ~]$ cd ..
[elmo@rhel home]$ ls -l
total 32
drwx------ 3 bart    simpsons     4096 Jun 10 00:29 bart
drwx------ 3 cookie  sesamestreet 4096 Jun 10 00:01 cookie
drwx------ 3 elmo    sesamestreet 4096 Jun 10 00:01 elmo
drwx------ 3 homer   simpsons     4096 Jun 10 00:03 homer
drwxrwx--- 3 lisa    simpsons     4096 Jun 10 00:33 lisa
drwx------ 3 oscar   sesamestreet 4096 Jun 10 00:02 oscar
drwx------ 3 student student      4096 May 31  2012 student
[elmo@rhel home]$ cd lisa
-bash: cd: lisa: Permission denied
[elmo@rhel home]$ exit_
```

# 2. Lab 3: Access Control

By using the command chmod 707 Lisa's directory is now available for the other accounts as well.
For this lab is required attention to the various access control permissions using the absolute and symbolic symbols.
Passwords can’t be weak as if someone can access the root permission of the system could easily manipulate all the access of all the users and a possible malicious hacker could easily lock the users out of the system altogether.

```
Password:
Last login: Thu Jun 10 00:30:02 on tty1
[lisa@rhel ~]$ pwd
/home/lisa
[lisa@rhel ~]$ cd ..
[lisa@rhel home]$ ls -l
total 32
drwx------ 3 bart    simpsons     4096 Jun 10 00:29 bart
drwx------ 3 cookie  sesamestreet 4096 Jun 10 00:01 cookie
drwx------ 3 elmo    sesamestreet 4096 Jun 10 00:49 elmo
drwx------ 3 homer   simpsons     4096 Jun 10 00:03 homer
drwxrwx--- 3 lisa    simpsons     4096 Jun 10 00:33 lisa
drwx------ 3 oscar   sesamestreet 4096 Jun 10 00:02 oscar
drwx------ 3 student student      4096 May 31  2012 student
[lisa@rhel home]$ chmod 707 lisa
[lisa@rhel home]$ ls -l
total 32
drwx------ 3 bart    simpsons     4096 Jun 10 00:29 bart
drwx------ 3 cookie  sesamestreet 4096 Jun 10 00:01 cookie
drwx------ 3 elmo    sesamestreet 4096 Jun 10 00:49 elmo
drwx------ 3 homer   simpsons     4096 Jun 10 00:03 homer
drwx---rwx 3 lisa    simpsons     4096 Jun 10 00:33 lisa
drwx------ 3 oscar   sesamestreet 4096 Jun 10 00:02 oscar
drwx------ 3 student student      4096 May 31  2012 student
[lisa@rhel home]$ exit_
```

```
Red Hat Enterprise Linux Server release 5.8 (Tikanga)
Kernel 2.6.18-308.el5 on an i686

rhel login: elmo
Password:
Last login: Thu Jun 10 00:48:07 on tty1
[elmo@rhel ~]$ cd ..
[elmo@rhel home]$ cd lisa
[elmo@rhel lisa]$ whoami && pwd
elmo
/home/lisa
[elmo@rhel lisa]$ exit_
```

# 3. Lab 4: Reconnaissance with NMAP

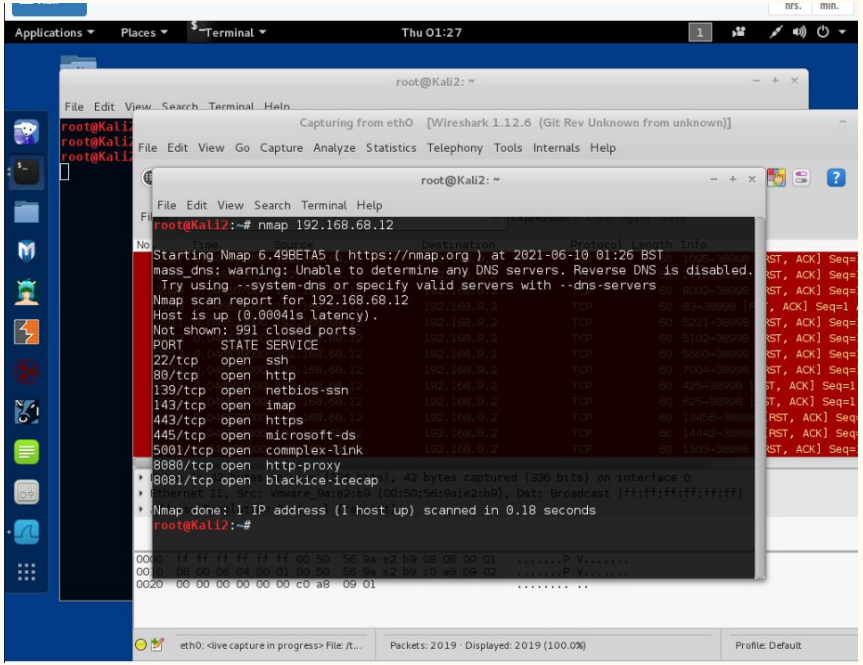
Network security is a very important subject that has to be highly maintained safe from possible malicious attacks or possible data breaches that could imply an important risk for the holder of the data, an example are the details of millions of accounts of a bank.

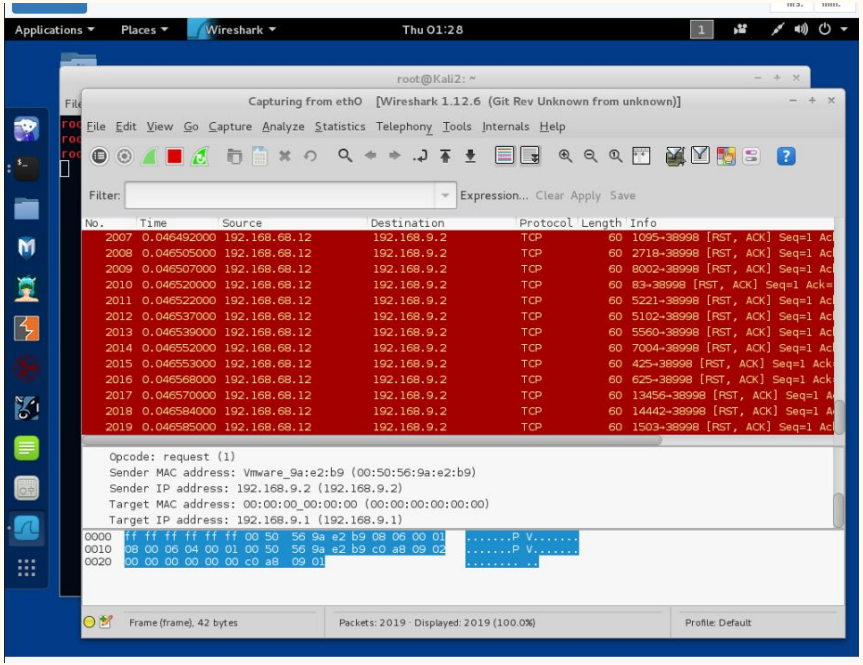
In this lab (Lab 1: Reconnaissance with Nmap & Amap) will be used the NMAP and AMAP commands to map a network to determine the status of the various ports and the possible breaches in the security of the network itself.

These commands are perfectly fine to use on an owned network but on the other hand they can easily be interpreted as a malicious attack by the admin of a company’s network and the subject performing them can be prosecuted legally.

# 3. Lab 4: Reconnaissance with NMAP

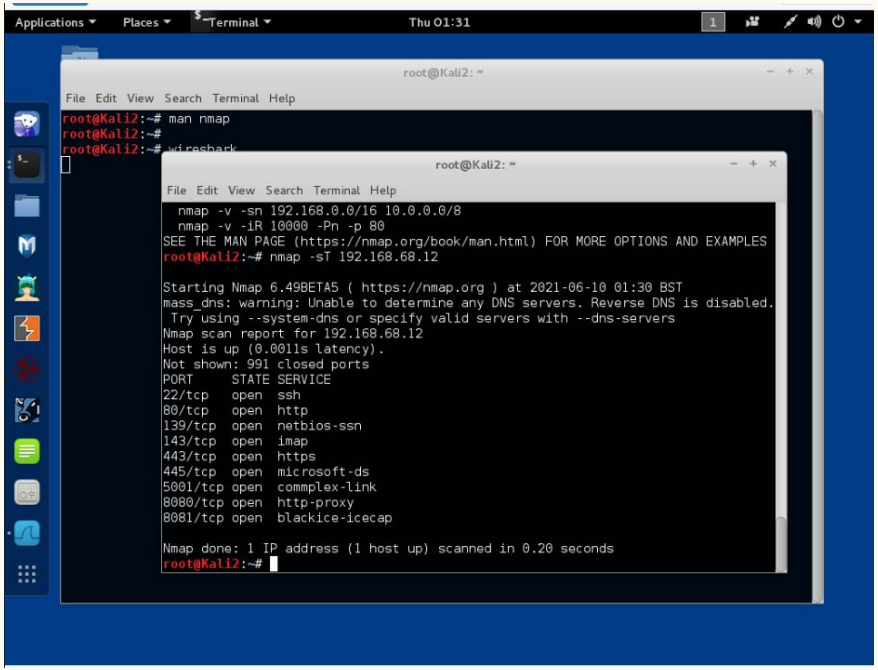
The possible commands of nmap are displayed with the man nmap command. After seeing the various commands it is time to map the network with the IP using the command nmap and see the most used 1000 ports and the details of the requests using wireshark.

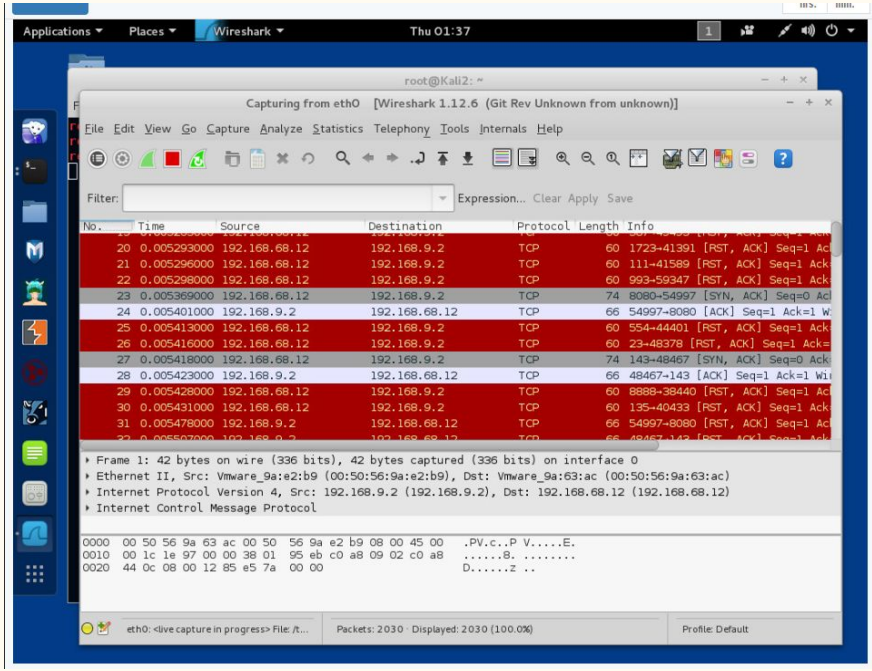


# 3. Lab 4: Reconnaissance with NMAP

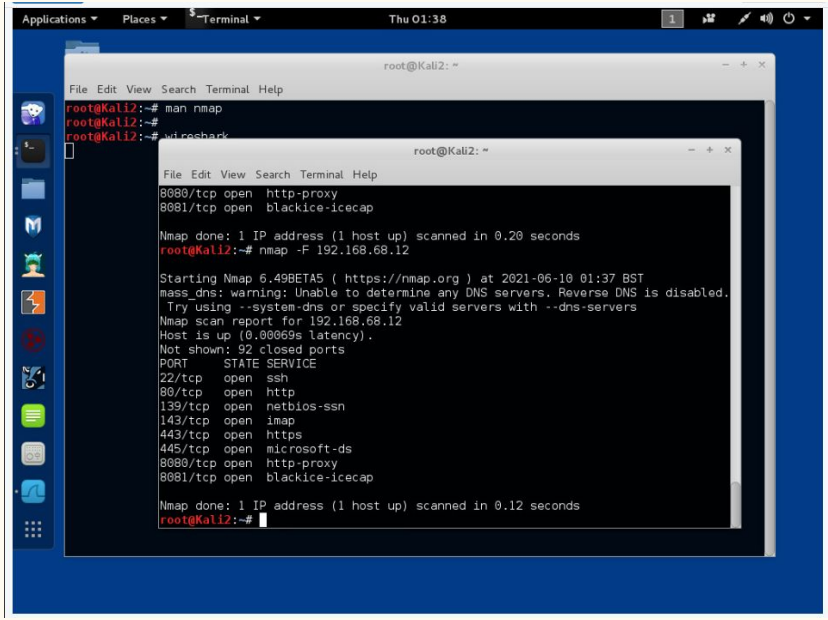
Now with the command nmap -sT a TCP connection scan will be done and some port will reply.

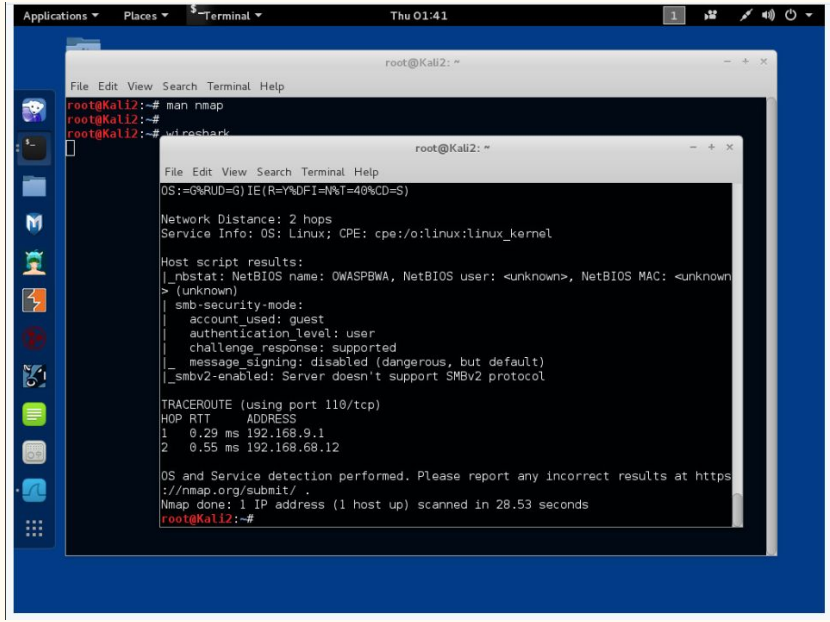


# 3. Lab 4: Reconnaissance with NMAP

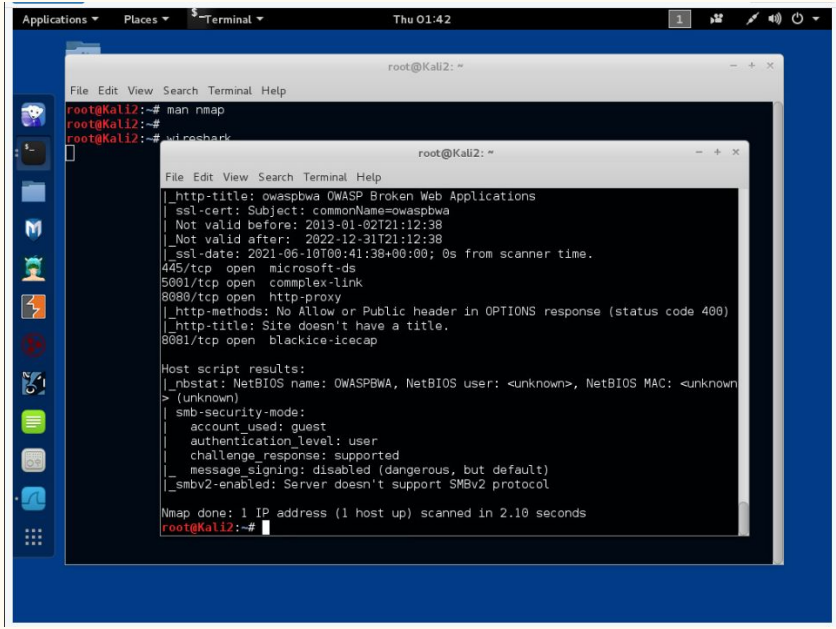
Now with nmap -F command the scan will be quicker and only the first 100 ports will be scanned. Following this scan the nmap -A scan is used and the received information increased greatly with the OS detection, version detection, script scanning and traceroute.

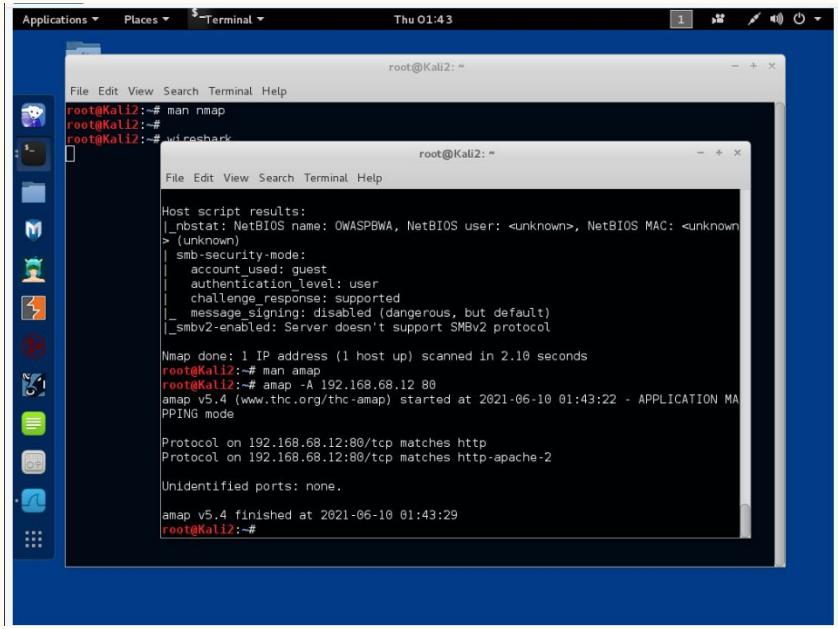


# 3. Lab 4: Reconnaissance with NMAP

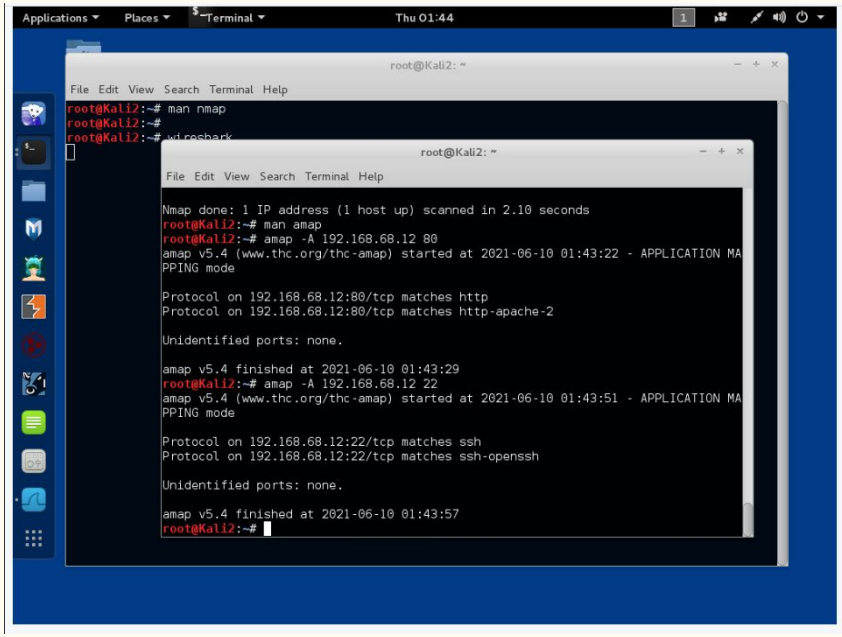
The scan with nmap with the -sC command that helps get potential vulnerabilities in the ports.
With the amap command it is possible to see if something is running on a certain port and with the man command it is possible to get the it's cheatsheet.

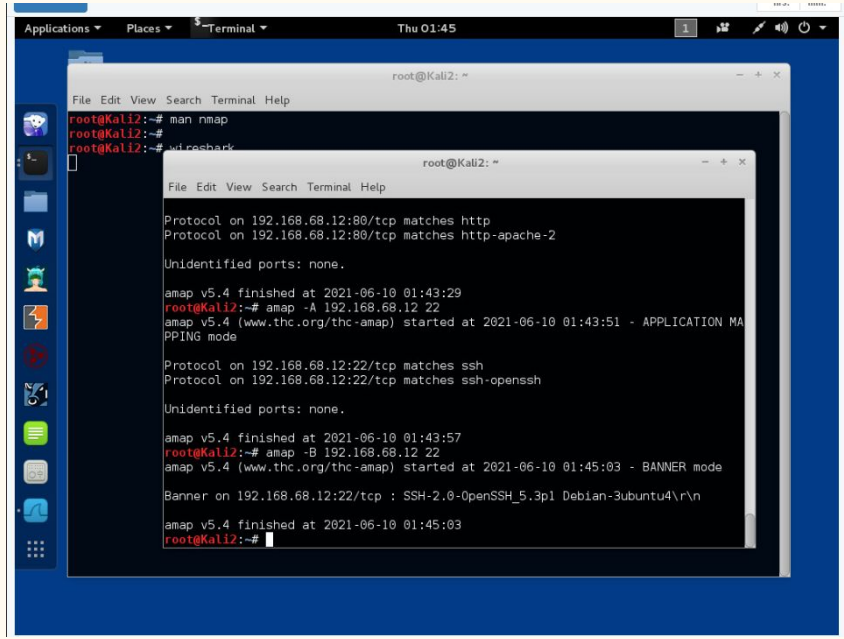


# 3. Lab 4: Reconnaissance with NMAP

Finally we can get more information about any disponible port such as the version of the protocol or of the SHH used. (Use of Anap -A/-B command)



# 3. Lab 4: Reconnaissance with NMAP

Nmap gives you the ability to explore any devices connected to a network, finding information like  which applications are listening on open ports and the operating system a device is running. This information lets a hacker design an attack that perfectly suits the target environment.

These commands should be used wisely as if a hacker wants to remain anonymous it could easily use a VPN and utilize the amap -F command to be less visible as the requests sent are just a fraction compared to the other commands.

Hackers can also use these scanning commands to find a bunch of services running on open ports, this can be a huge benefit, if one of them is vulnerable to possible breaches.

# 4. Lab 5: Password cracking with John the Ripper

Cybersecurity Compliance involves meeting various controls that are enacted by a regulatory authority, law, or industry to protect the confidentiality, integrity, and availability of data stored. Most cybersecurity compliance requirements require a risk and vulnerability assessment. These determinate what's your organization's most critical security flaws, as well as how efficient are the controls that are already in place.

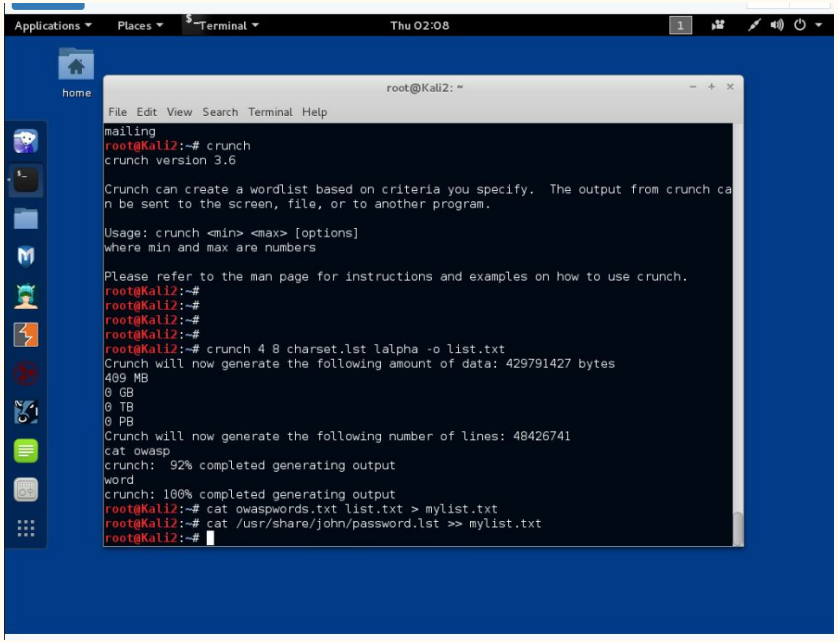
Cybersecurity isn't just about software and hardware. Having policies and procedures in place to reduce risk is also important for both safety and compliance. That's why companies have mandatory cybersecurity training for their employees and they conduct various risk and vulnerability assessments.

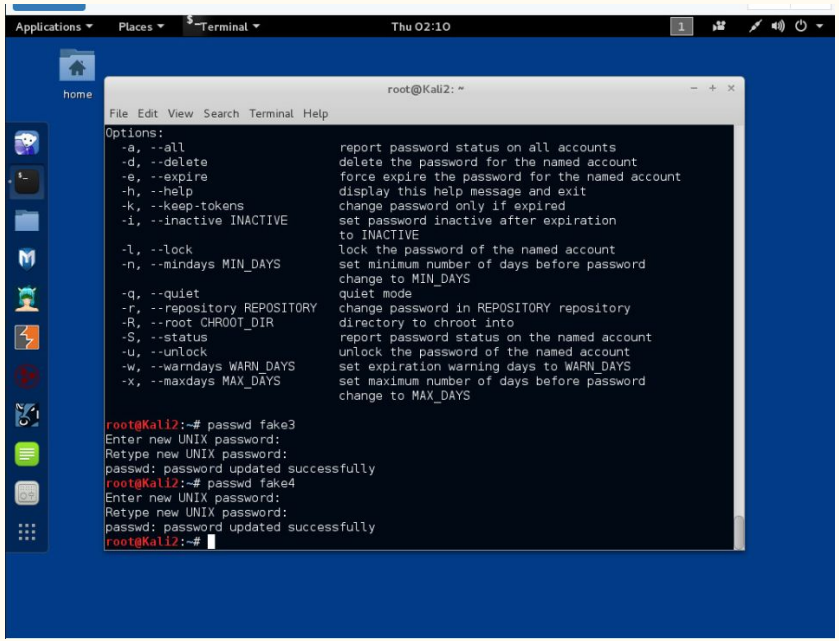
The most famous ways to crack passwords of a system are by using:

- John the Ripper
- Hashcat

# 4. Lab 5: Password cracking with John the Ripper

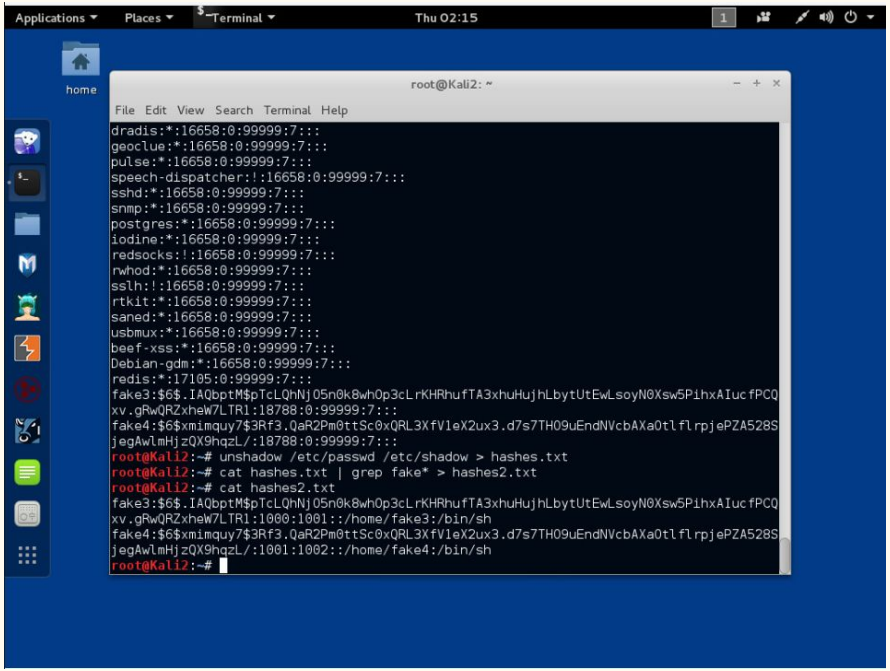
The cewl command is used to copy contents of the attacked virtual machine to a text file then the crunch command is used to create the passwords. Finally these files are united with the other list created by john the ripper. Then using the adduser and passwd command we create the fake account's details.

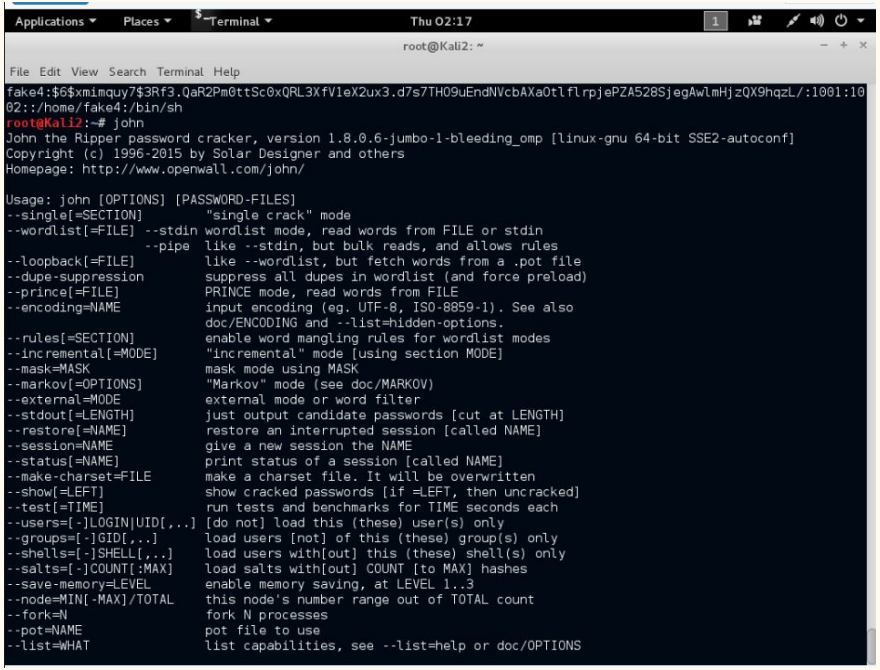


# 4. Lab 5: Password cracking with John the Ripper

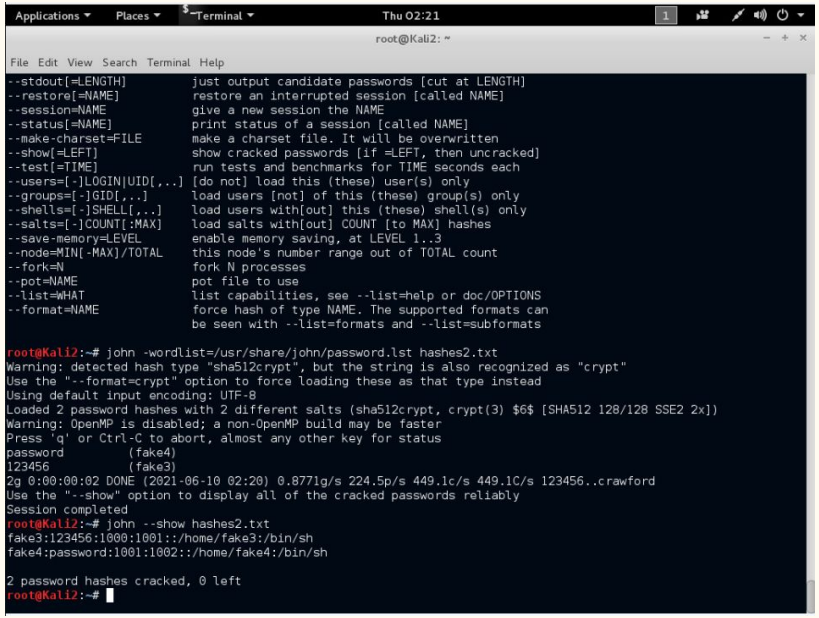
Now the updated files of the new user's details are united in the hash.txt file then it's narrowed down to the 2 fake accounts and shown in the terminal. Then we open john the ripper to see the possible options.

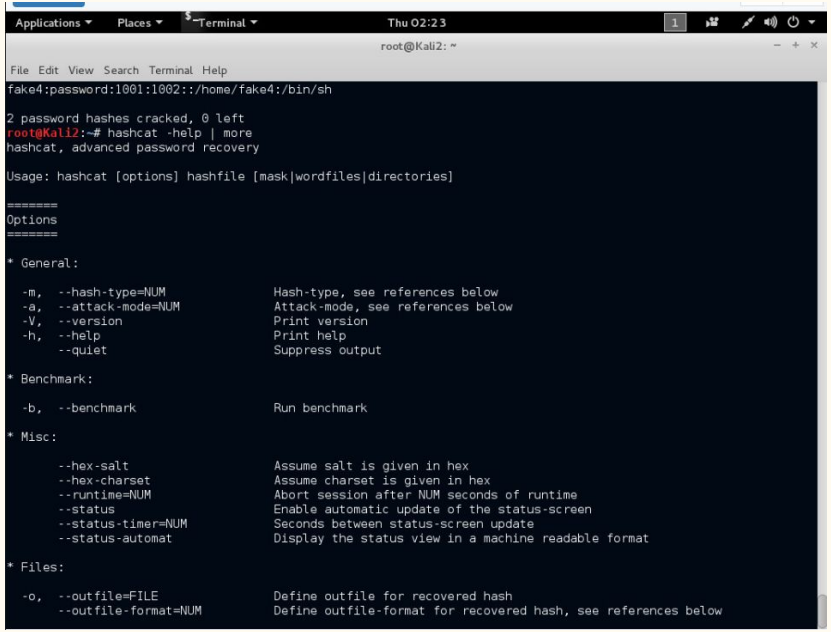


# 4. Lab 5: Password cracking with John the Ripper

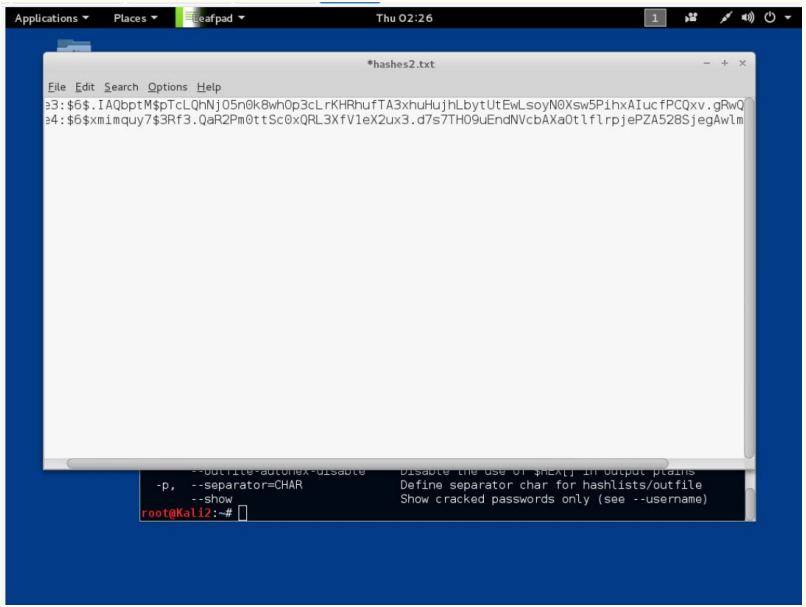
Using john the ripper to crack the passwords in the hashes2.txt file and then showing them in the terminal. Now is the time to use hashcat and crack them in another way but first let's see the possible commands available.

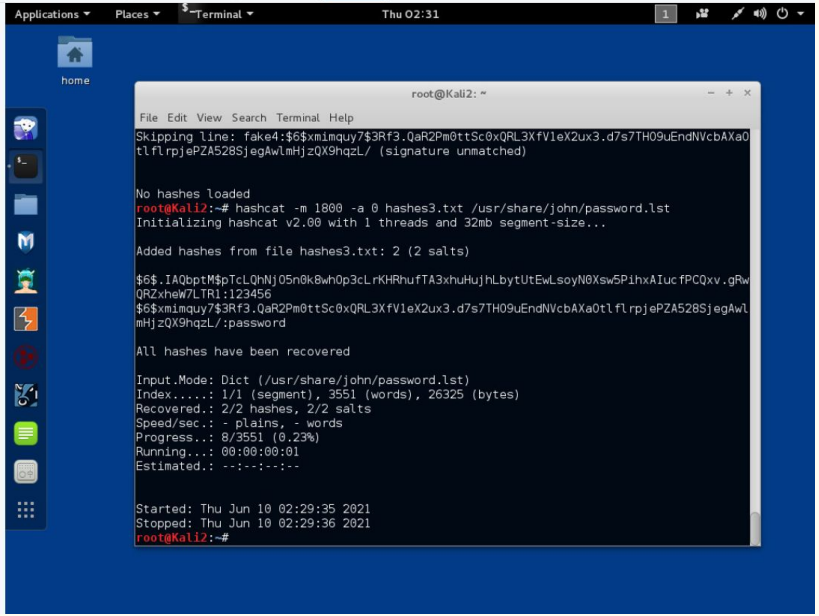


# 4. Lab 5: Password cracking with John the Ripper

To use the hashcat, the file hashes3 is created with only the hash password and then the cracking command is used with the list of john the ripper and then the message is displayed showing the passwords.



# 4. Lab 5: Password cracking with John the Ripper

For this lab it is fundamental to understand that these commands are just for educational purposes and can easily an infringement of the law.

John the Ripper operates in a different way from hashcat as it’s more of a brute force attack to crack the passwords while hashcat is used to confront hashes till it finds the right password.

JtR can be more direct as it does not require to have the hash files of the passwords; they can still be recovered with a precise attack to the user.

Unfortunately most of the passwords are still easy combinations of words and not many users use a password that fully comply with the advised entropy.

# References:


- https://moodle.bcu.ac.uk/course/view.php?id=79458
- https://netlab.catcemea.org.uk/home.cgi
- https://www.reddit.com/
- https://help.yahoo.com/kb/SLN35642.html


The End