Cyber Security Report

CMP5329 – Coursework Log format

Jaspreet Singh

Student ID: 19150299

1. *Lab 1: Encrypting and Decrypting with OpenSSL*

In this lab, i`ve used OpenSSL to encrypt and decrypt text messages by the application of various applied information security mechanisms.

These mechanisms can be the cryptography and cryptographically secure hash functions, the digital signatures, certificates and PKI (Public Key Infrastructure).

The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) that is just an updated, and more secure version of the first, are important certificates that keep internet connection secure and safeguard any sensitive data that is being sent between two systems. The two systems can be a server and a client (for example, an online store and the user's browser) or server to server (for example, an application with personal identifiable information).

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, processing and storage but it can also be used to encrypt stationary data and maintain confidentiality and Integrity of the information.

The conversion consists of a sequence of actions that change the appearance of the message during transmission but do not alter the content. Cryptographic techniques can ensure confidentiality and protect messages against unauthorized users. Here comes the digital signatures, which assure the message integrity and the public key infrastructure (PKI) that is needed to do various operations on digital certificates and manage public-key encryption. It`s purpose is to facilitate the secure transfer of different network activities such as internet banking, online stores and emails.

Cryptographic techniques involve different methods, made specific by the use of keys. There are two types:

- Algorithms that use a shared key are known as symmetric algorithms and require both parties to use the same secret key.
- Algorithms that use public and private key pairs are known as asymmetric algorithms, these use one key for encryption and a different key for decryption. One of these must be kept secret but the other can be public.

The encryption and decryption algorithms used can be public but the shared secret and private key must remain secret. 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.

Now here's the Lab 9.1.1.6 - Encrypting and Decrypting Data Using OpenSSL.

First i've opened the directory with the txt file containing the message to encrypt, once opened the file is time to encrypt it with the AES-256 command with the “cyberops” password and then when the file is opened again it won't show appear readable but in fact encrypted.

Did the contents of the message.enc file display correctly? What does it look like? Explain.

- No. The file is unreadable as just symbols are now displayed. The symbols are shown because OpenSSL has generated a binary file after the encryption command.

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. (Fig.1)

Is message.enc displayed correctly now? Explain.

- Yes. Even if the is encrypted, it is now displayed correctly because it has been converted from binary to text and encoded with Base64.

Can you think of a benefit of having message.enc Base64-encoded?

- Yes. The encrypted message can now be copied and pasted somewhere else.

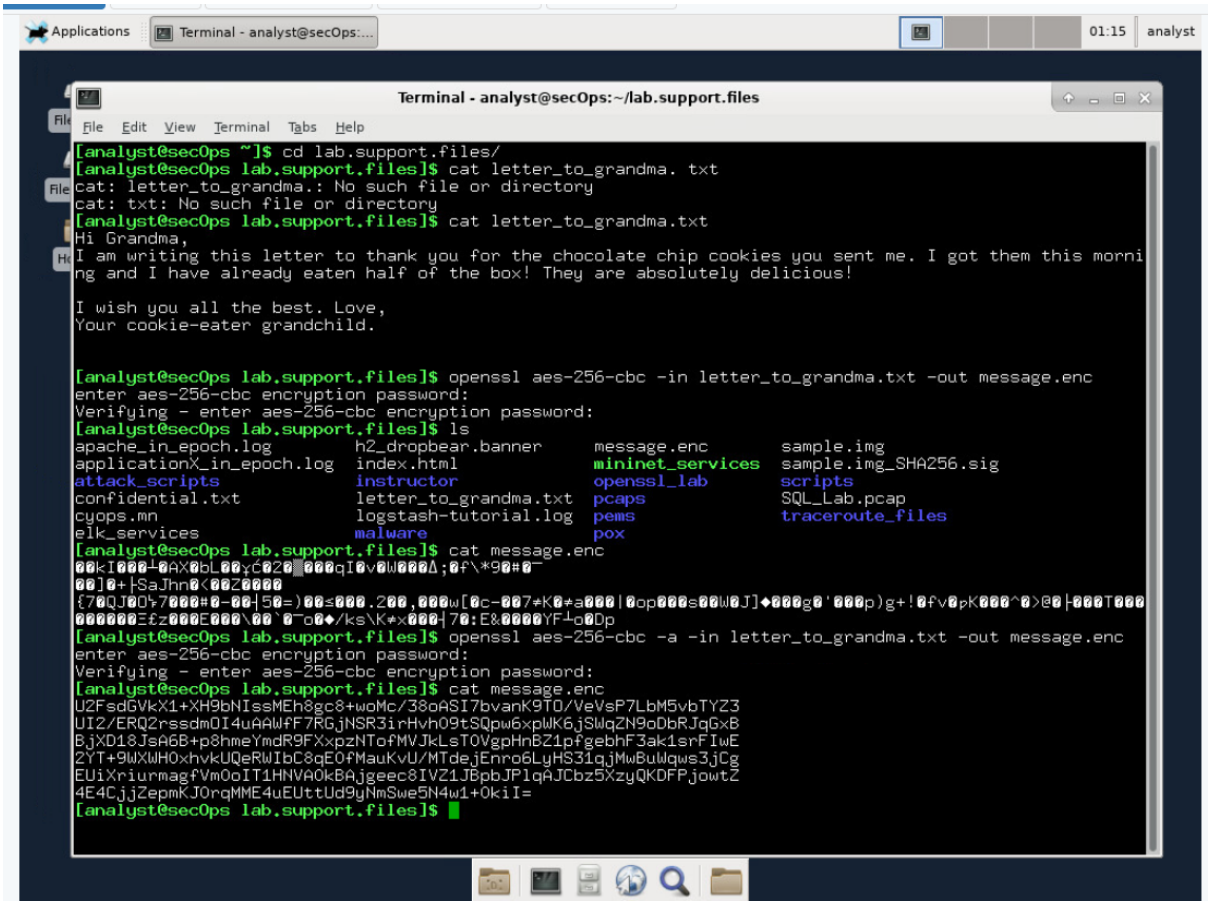

Fig.1 (Part 1: Encrypting Messages with OpenSSL)

Now we can move to the second part of the lab where the message will now be decrypted and will ask for the same password used during the encryption process.(“cyberops”) Now when the message is displayed it will be readable as same as it was before the encryption. (Fig.2)

Was the letter decrypted correctly?

- Yes

The command used to decrypt also contains -a option. Can you explain?

- Because message.enc was Base64 encoded after the encryption process took place, message.enc must be decoded in Base64 before OpenSSL can decrypt it.

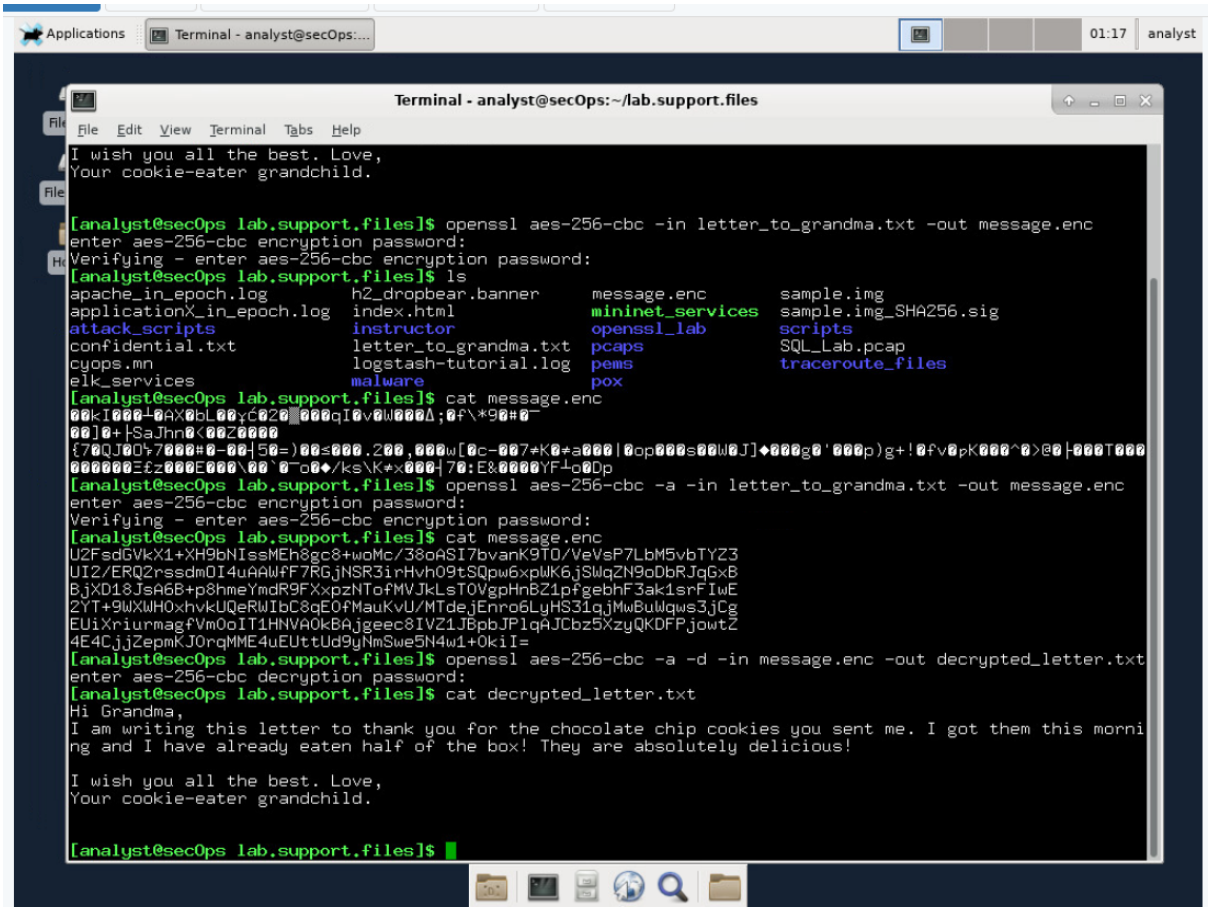

Fig.2 (Part 2: Decrypting Messages with OpenSSL)

For this lab is required attention to the various encoding mechanisms, especially with the Base64 that could be easily missed causing confusion and errors. As for major security, it is advised to select a stronger password for the encoding/decoding process.

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), used in operating systems,here subjects are able to choose permissions for the resources they control.
- Mandatory Access Control (MAC), here the subjects cannot grant access to other subjects to their resources, labels are used on the data and the security clearance is used to tell who can access what.
- Role-based Access Control(RBAC), here roles are created for each group, typically used in companies.
- Rule-based Access Control, here the access is granted by some rules, a good example is the firewall.

The various types of permissions (read,write,execute) that can be assigned in the system by using specific codes, some of these will be used in this lab. (Lab 17: Authentication, Authorization and Access Control)

First I've opened the Red Hat Linux virtual machine and then after the login in the account it is time to open the terminal to open 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. (Fig.3/4)

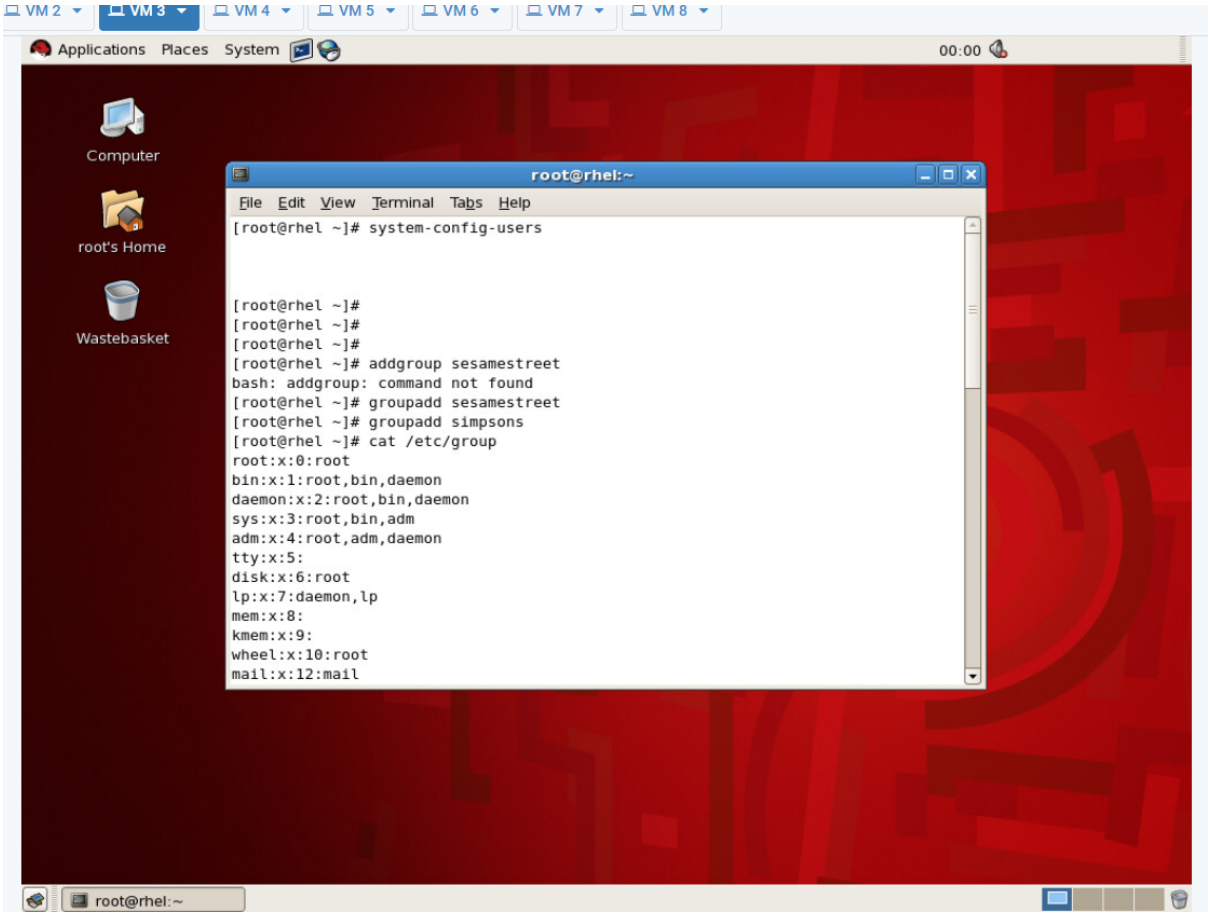

Fig.3 (Adding groups and displaying them pt.1)

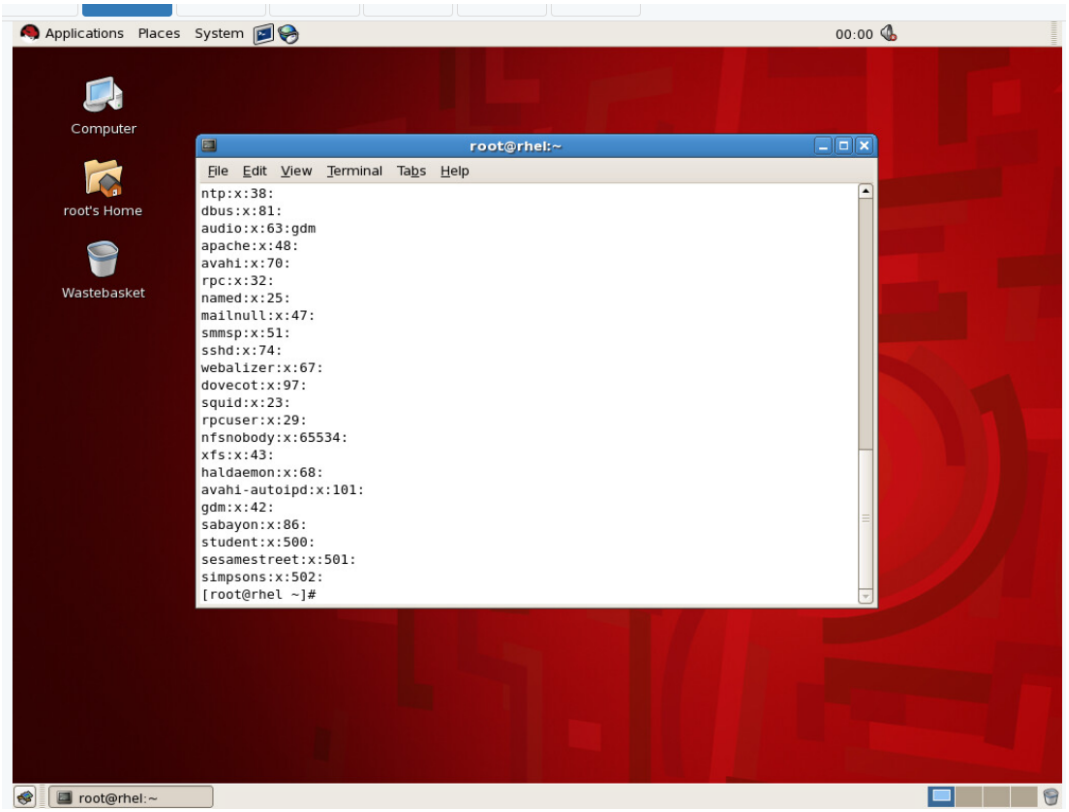

Fig.4 (Adding groups and displaying them pt.2)

Now is time to add the users with the useradd command. (Fig.5)

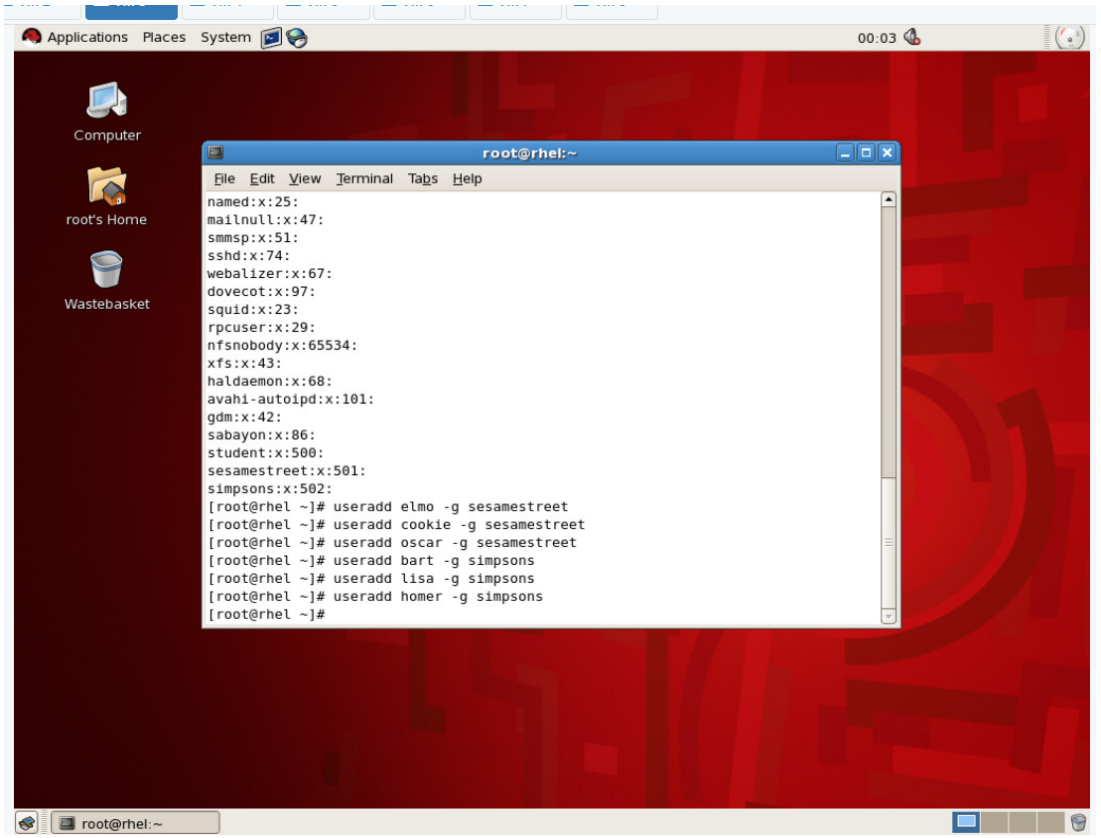

Fig.5 (Adding users command)

After adding the various users the user manager is used to control if all the groups and users have been correctly inserted. (Fig.6/7)

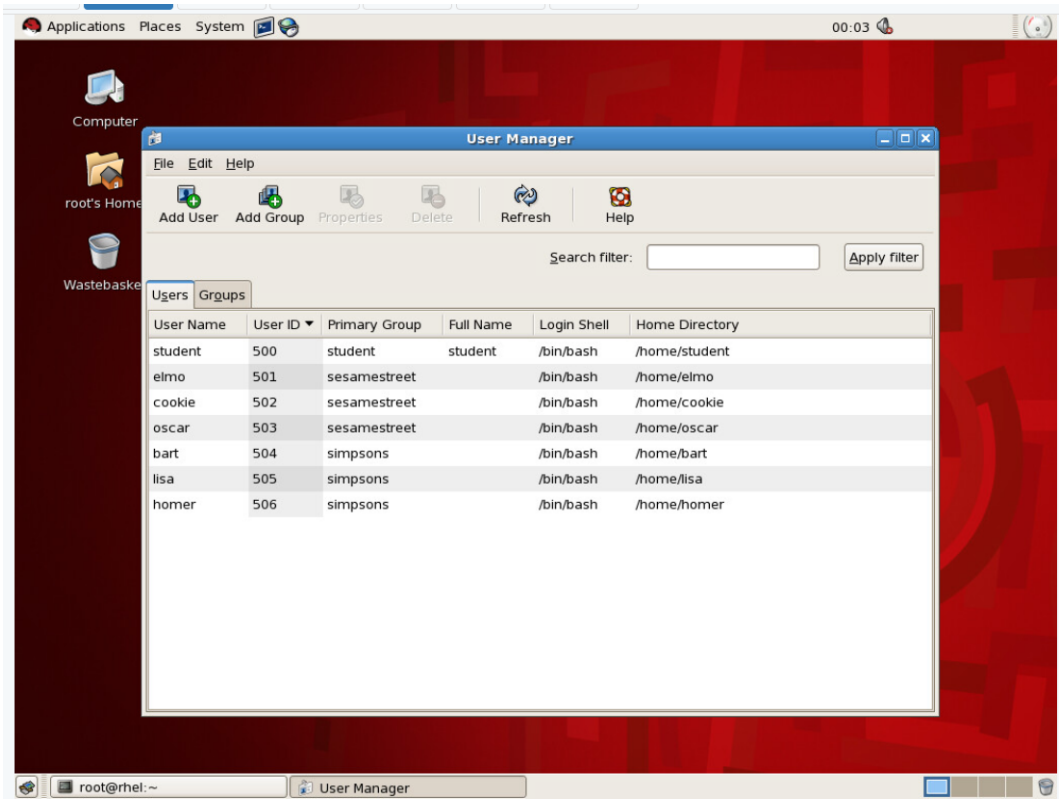

Fig.6 (Checking if users and groups have been created and inserted correctly pt.1)

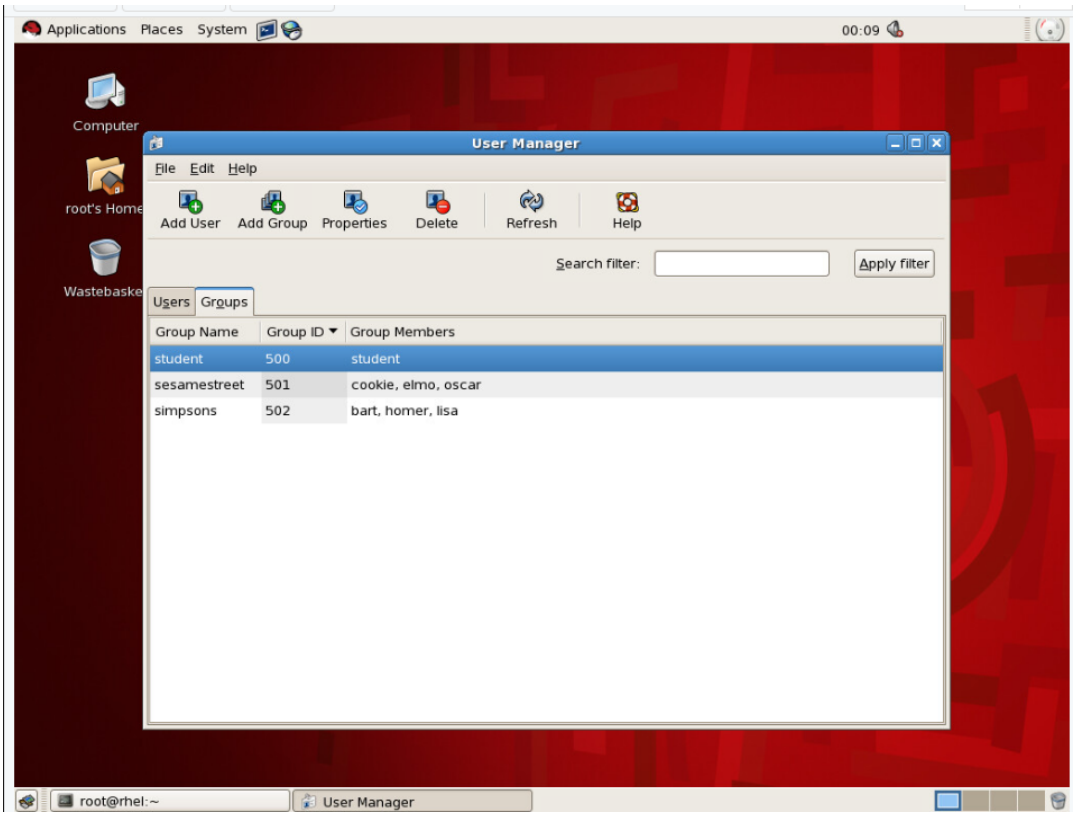

Fig.7 (Checking if users and groups have been created and inserted correctly pt.2)

Now 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. (Fig.8/9)

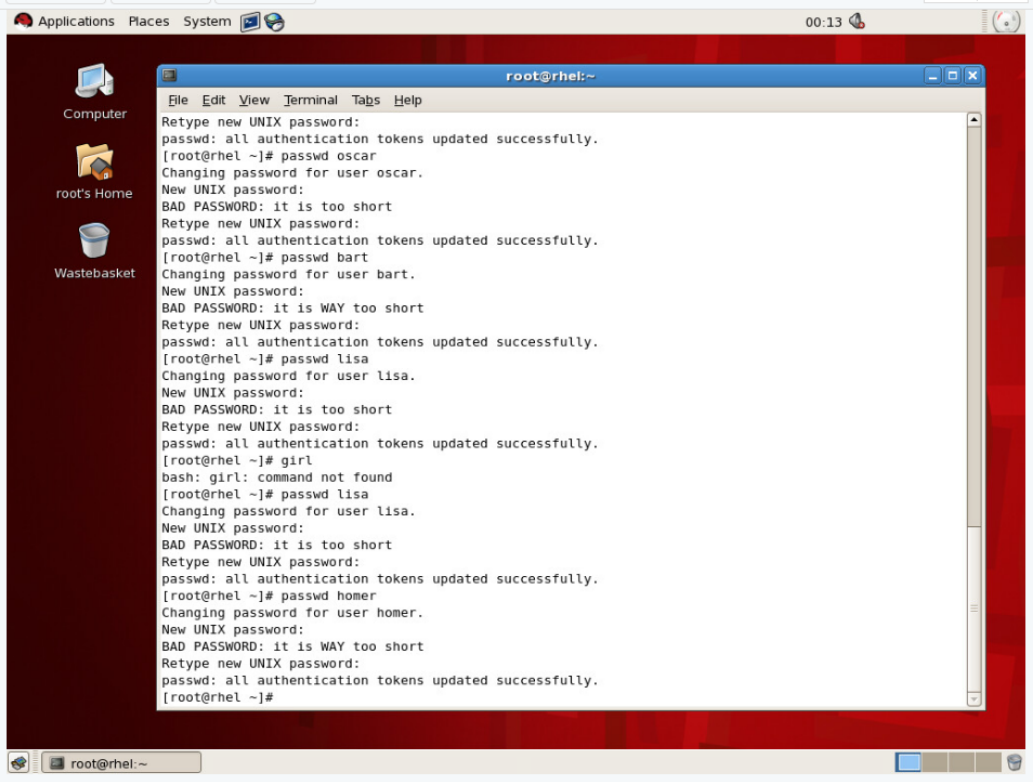

Fig.8 (Creating passwords for all the users)

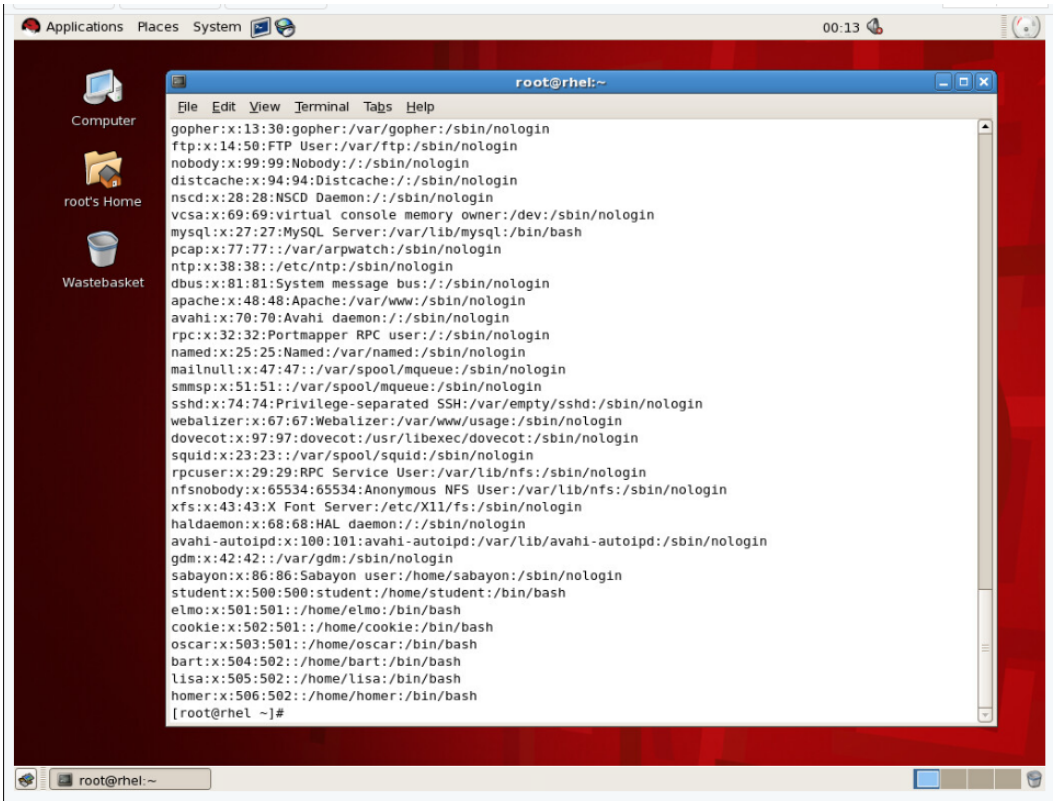

Fig.9 (Show users in the passwd file)

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. (Fig.10)

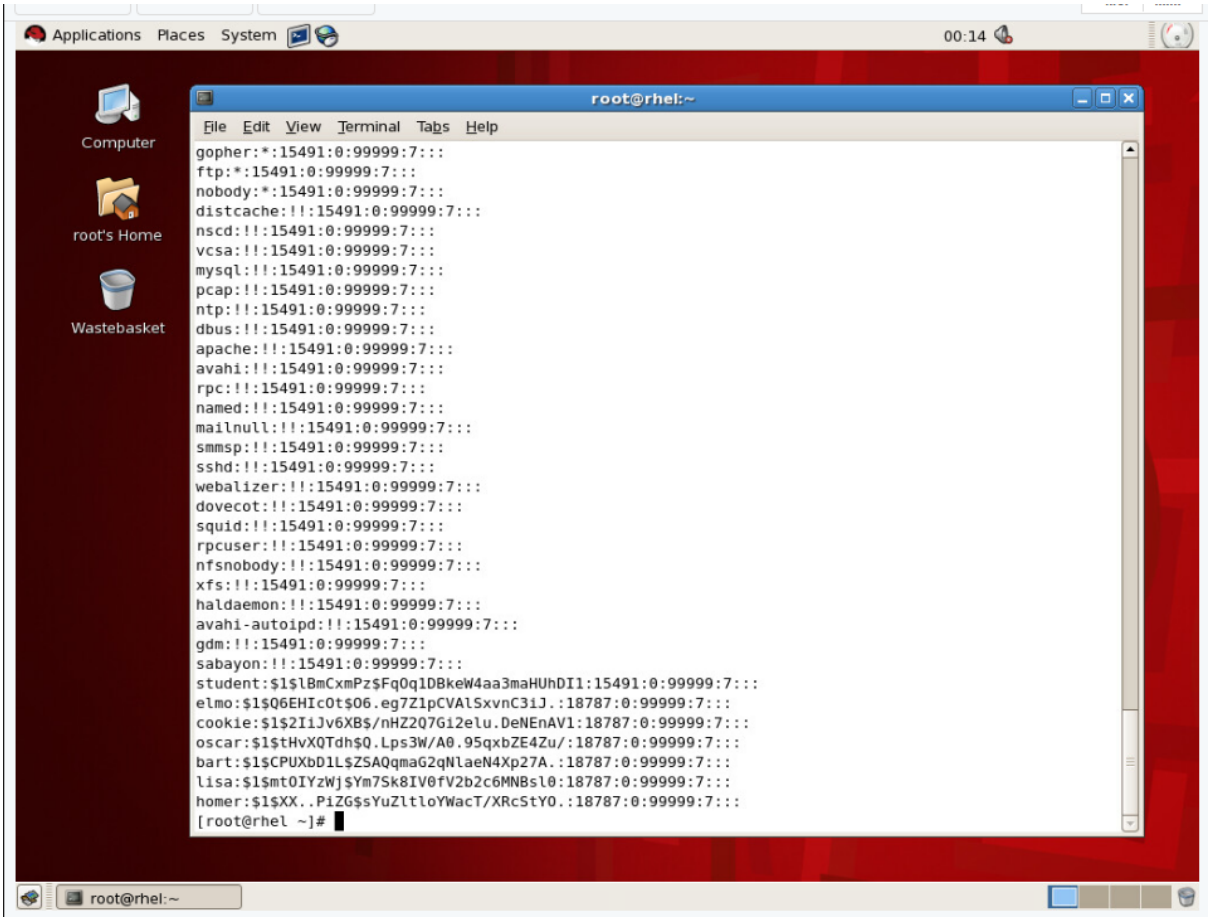

Fig.10 (Creating the shadow file for the root group)

2.3 Discussion Questions

1. groupadd namegroup
2. passwd username
3. useradd username
4. The /etc/shadow file stores contain the password hash information for the user account.

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. (Fig. 11)

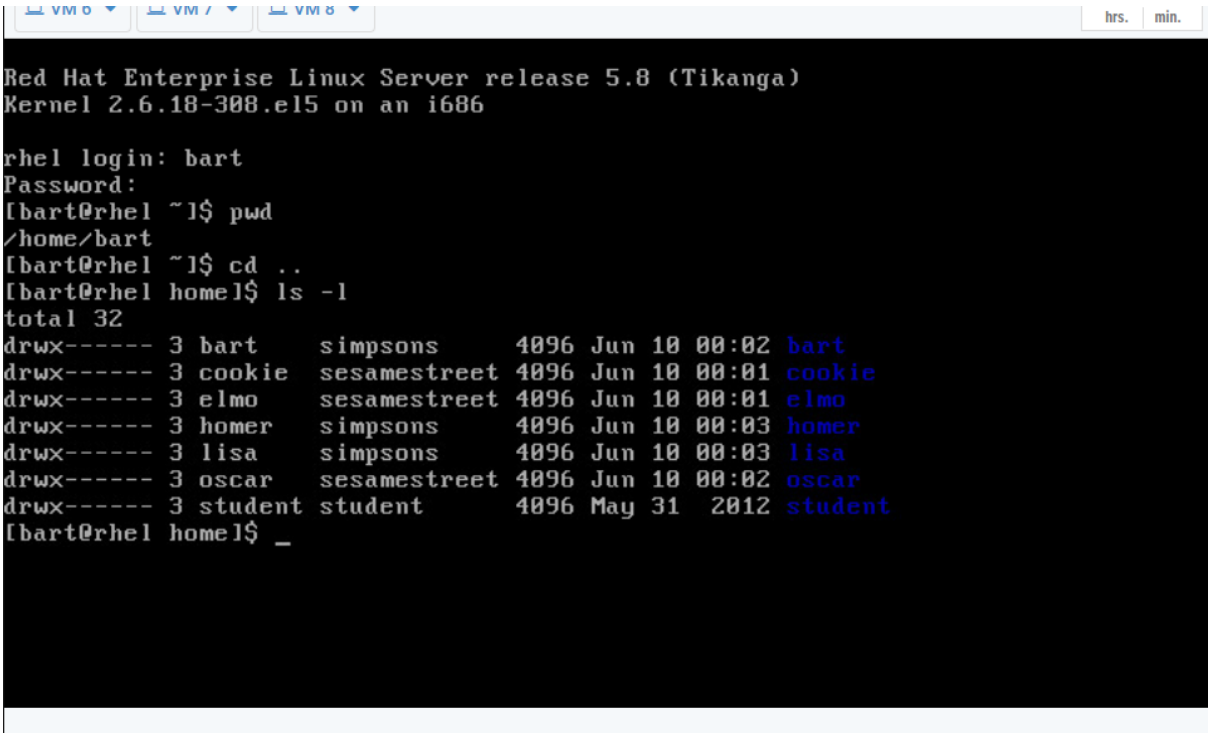

Fig.11 (Logging in the bart account and see permissions for each directory)

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. (Fig. 12)

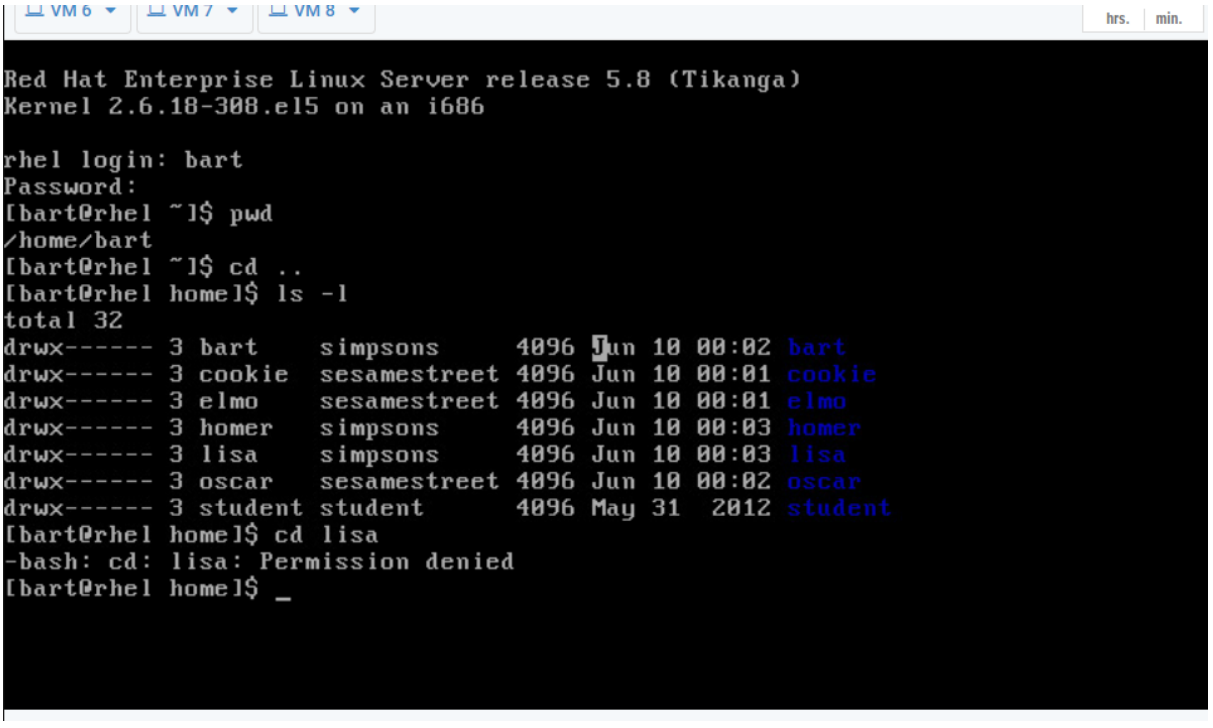

Fig.12 (Permission denied after trying to access another account's directory)

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. (Fig.13)

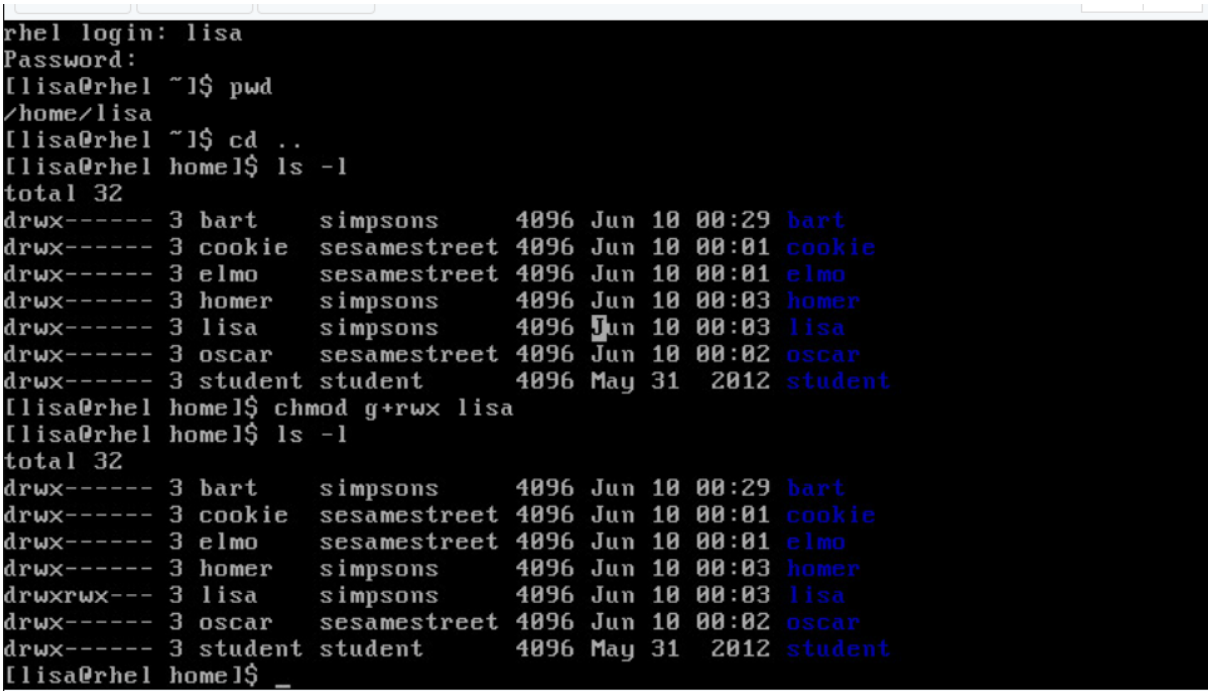

Fig.13 (Change lisa's directory permissions.)

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. (Fig.14

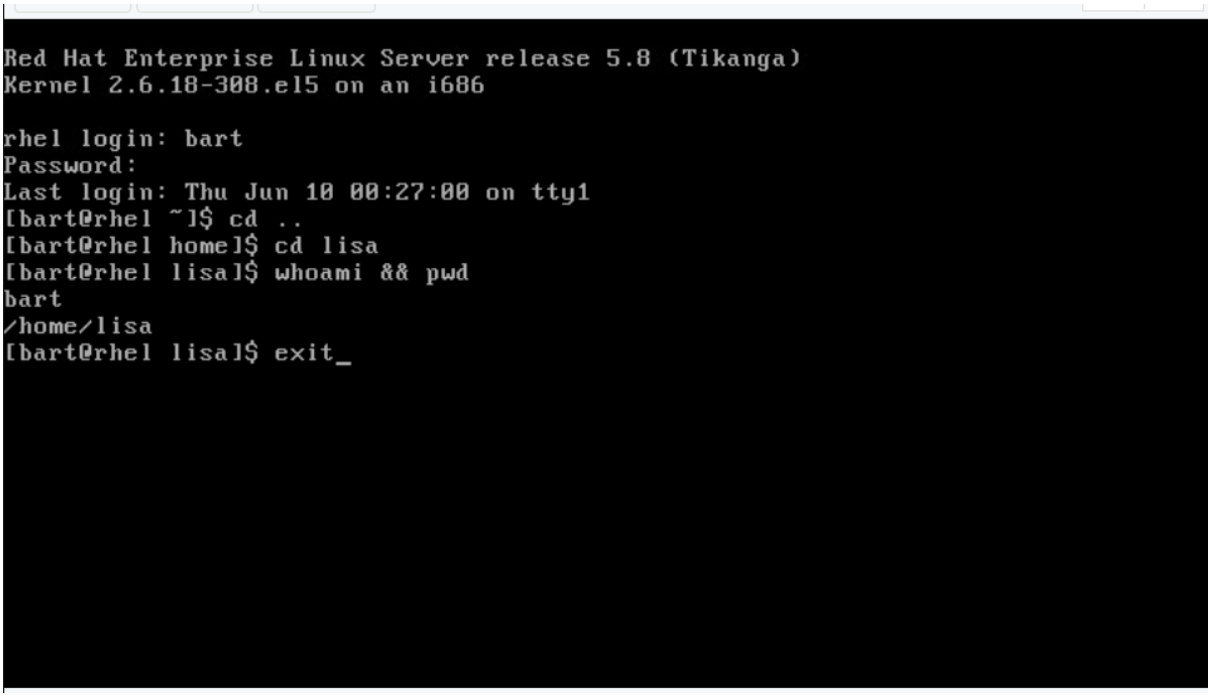

Fig.14 (Bart can now access lisa's directory with more permissions)

3.3 Discussion Questions

1. chmod g+rw lisa
2. chmod o+rwx lisa
3. chmod g-r lisa
4. chmod o-rx lisa

If another group's account, in this case elmo, tries to access Lisa's directory, the system will still show the permission denied message. (Fig.15)

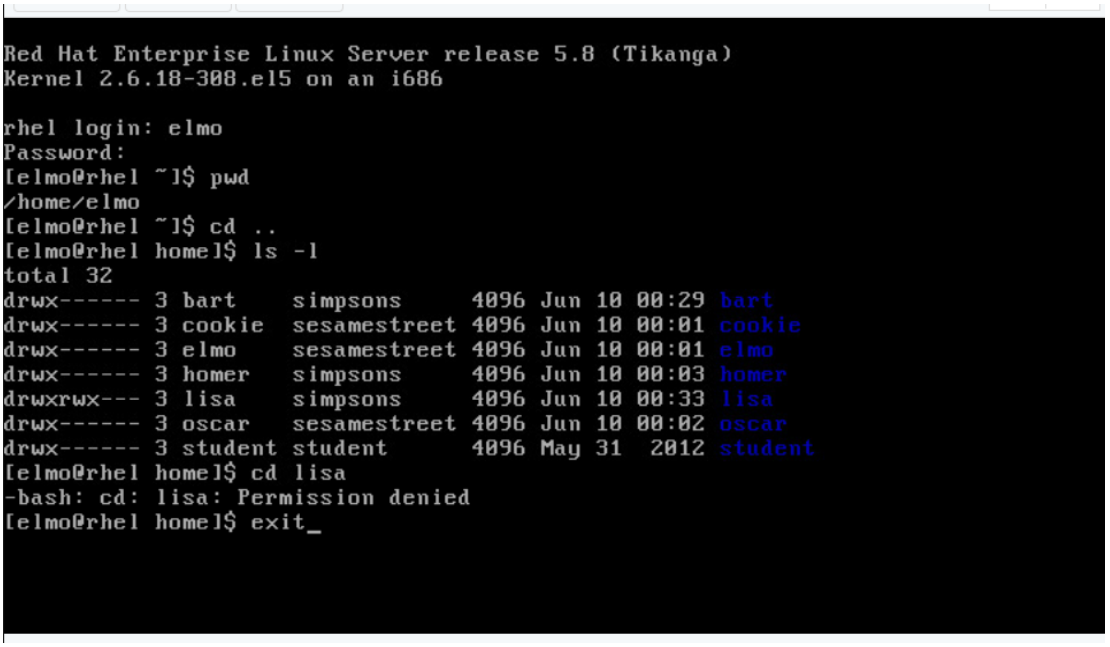

Fig.15 (Elmo cannot access lisa's directory)

Now by using the command chmod 707 Lisa's directory is now available for the other accounts as well and Elmo can now access it. (Fig.16/17)

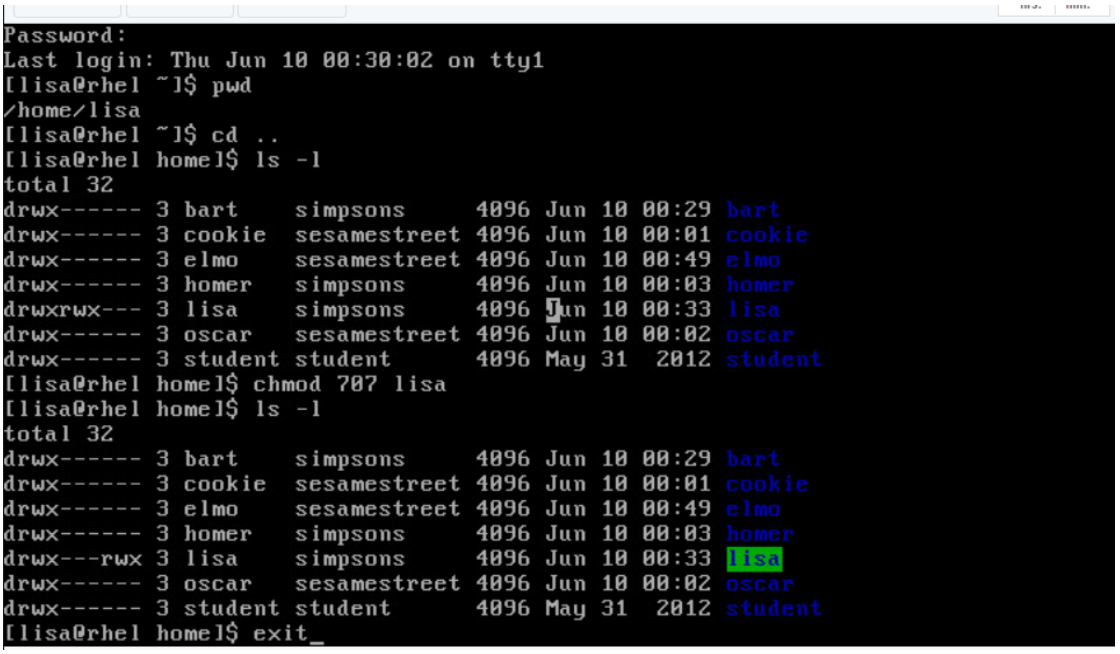

Fig.16 (Lisa's directory permission change)

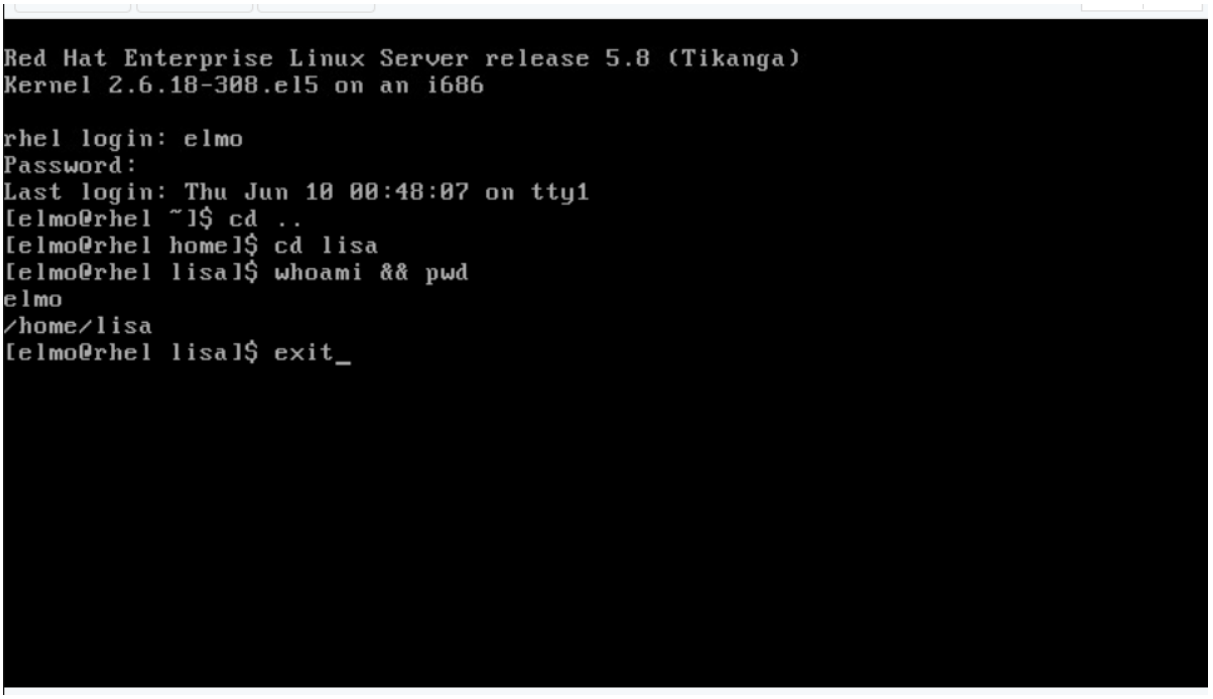

Fig.17 (Elmo can access lisa's directory)

4.3 Discussion Questions

1. 666
2. 444
3. 555
4. 777

For this lab is required attention to the various access control permissions using the absolute and symbolic symbols. As in the previous lab the passwords for the various users can't be weak as the system will advise to change in something else. Finally 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.

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.

After the login in the kali linux machine 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 192.168.68.12 and see the most used 1000 ports and the details of the requests using wireshark. (Fig.18/19)

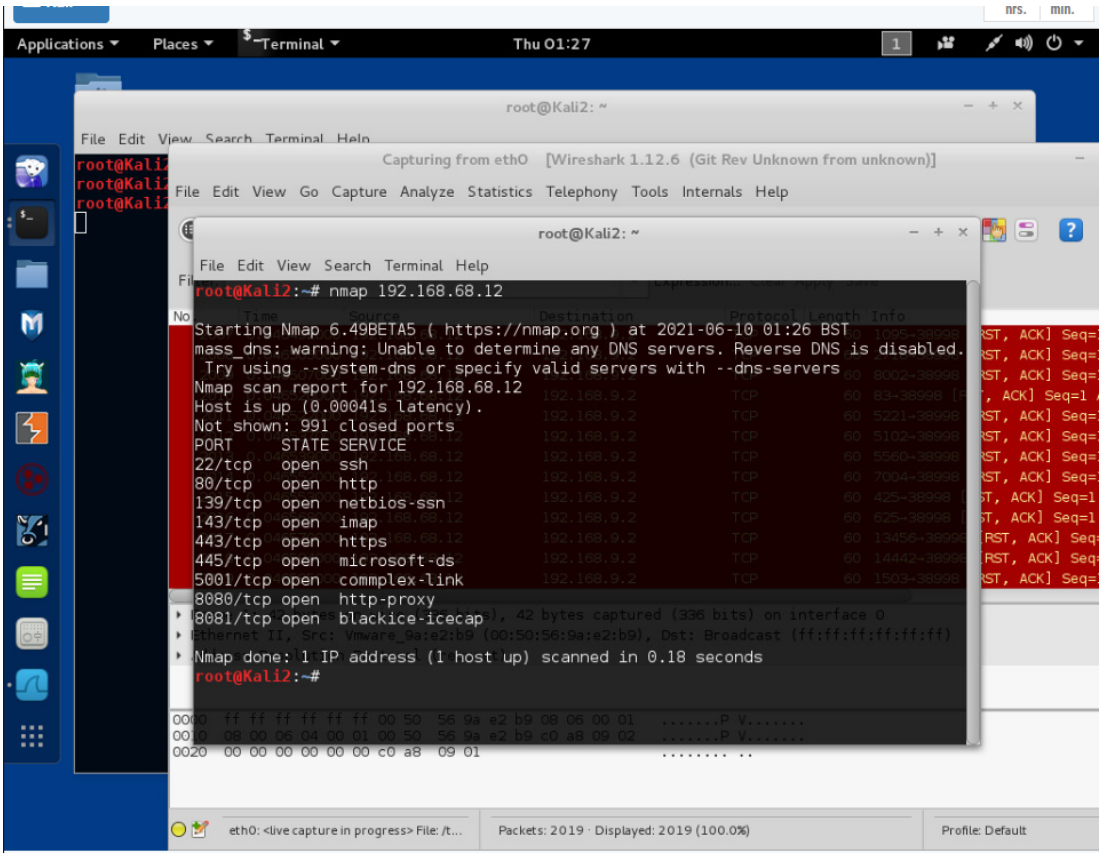

Fig.18 (Nmap ip command and main open ports displayed)

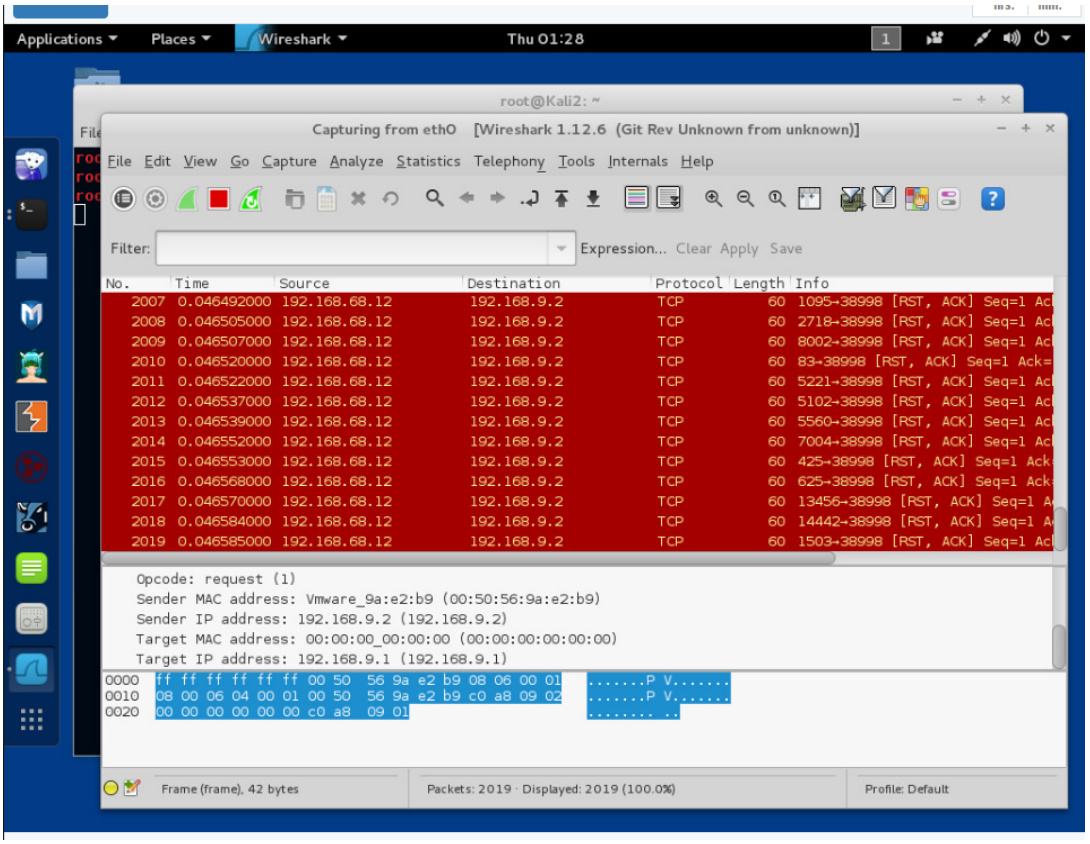

Fig.19 (Wireshark ports request details)

Now with the command nmap -sT a TCP connection scan will be done and some port will reply. (Fig.20/21)

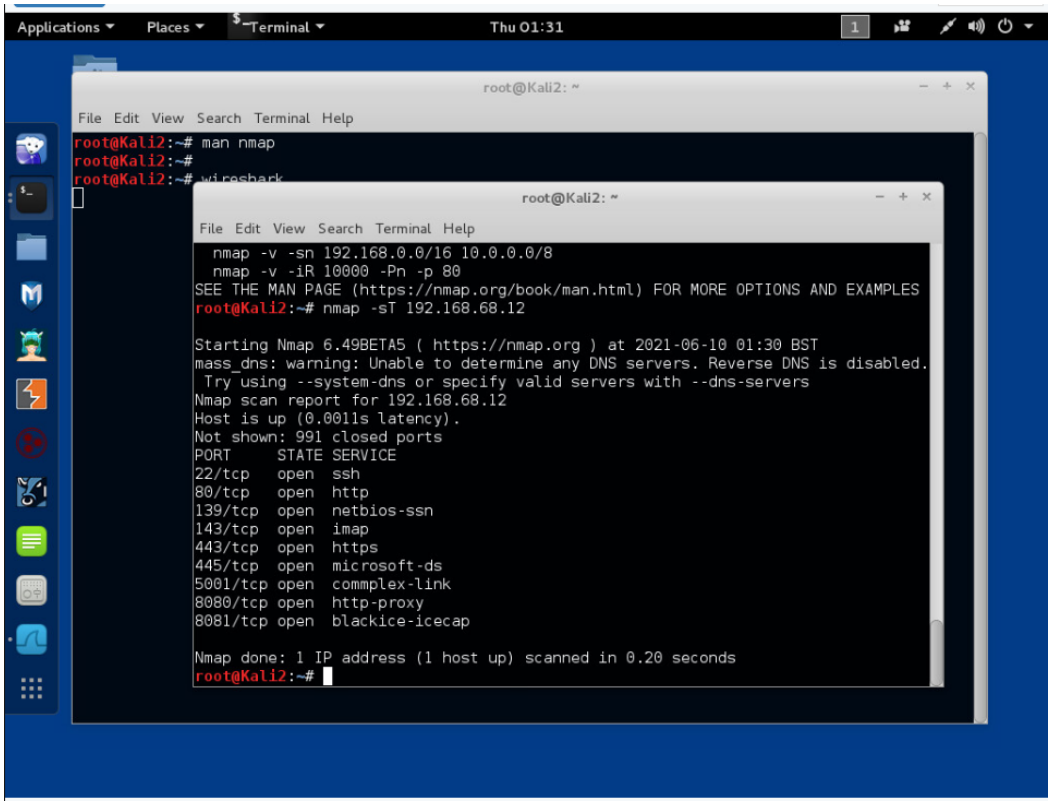

Fig.20 (Nmap scan with TCP connection)

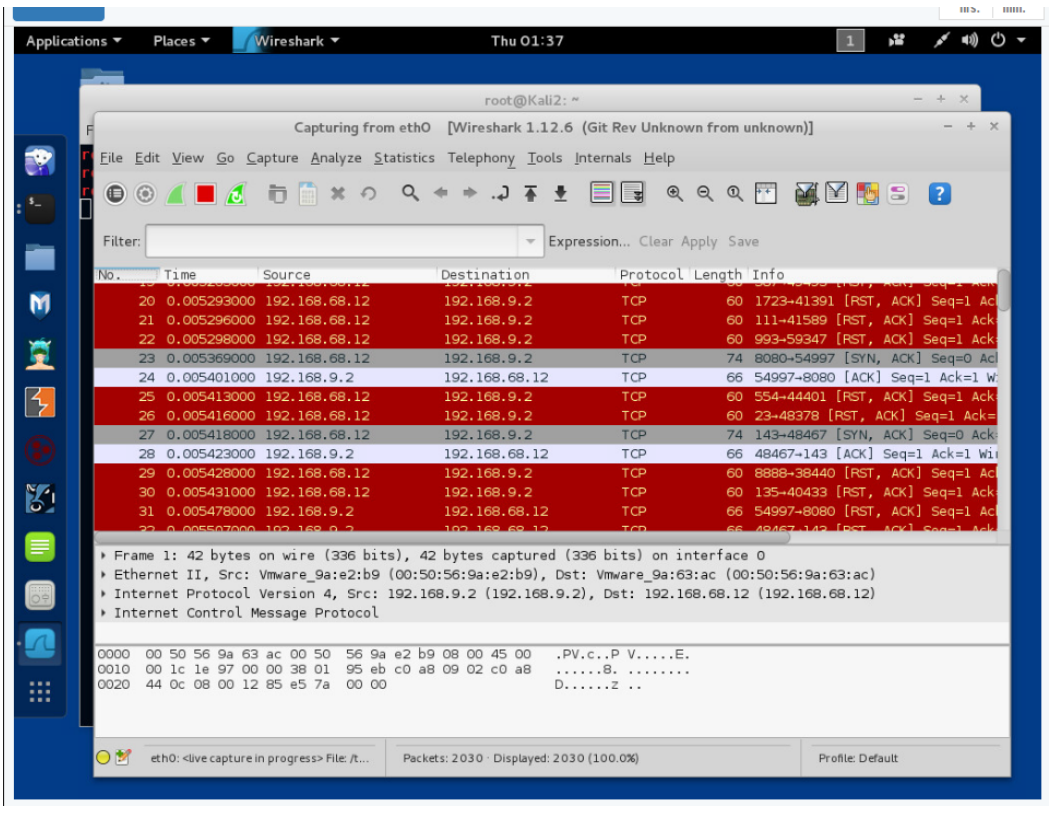

Fig.21 (Wireshark ports request details with TCP connection)

Now with nmap -F command the scan will be quicker and only the first 100 ports will be scanned. (Fig.22)

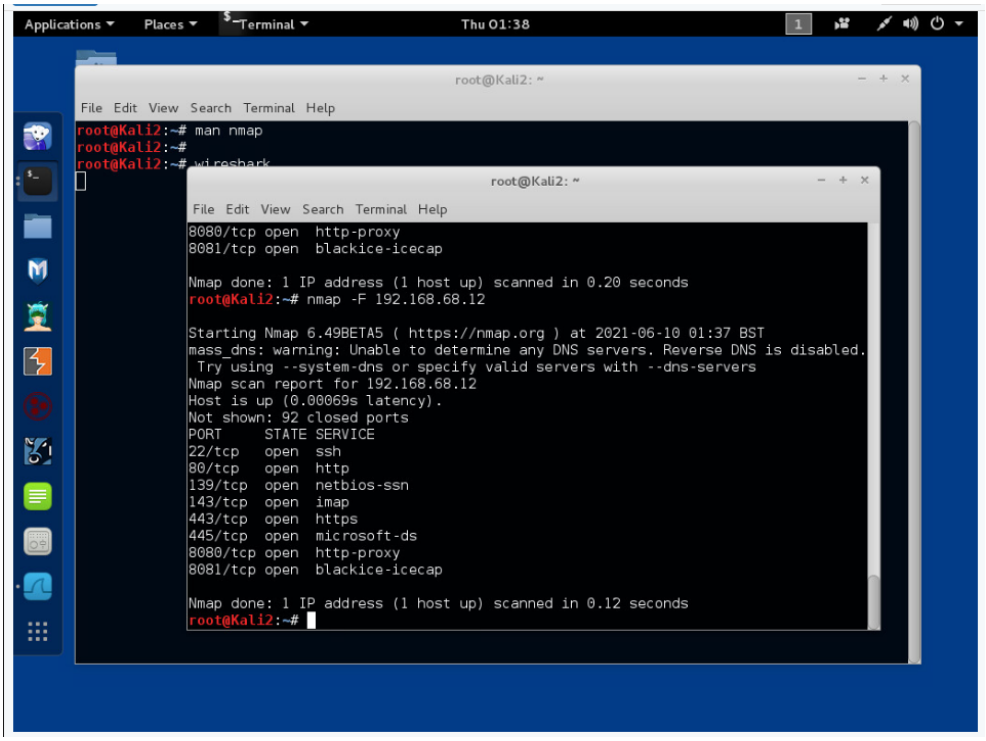

Fig.22 (Nmap scan with -F to reduce number of ports scanned)

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. (Fig.23)

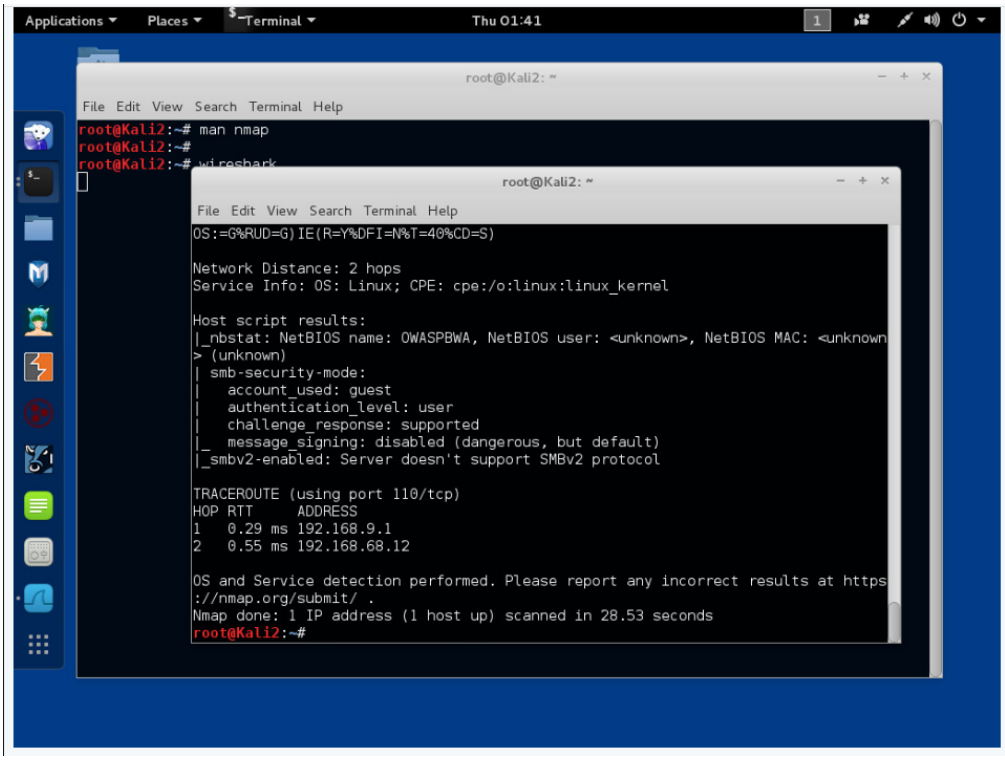

Fig.23 (Nmap scan with -A to get more informations)

Another scan with nmap is with the -sC command that helps get potential vulnerabilities in the various ports. (Fig.24)

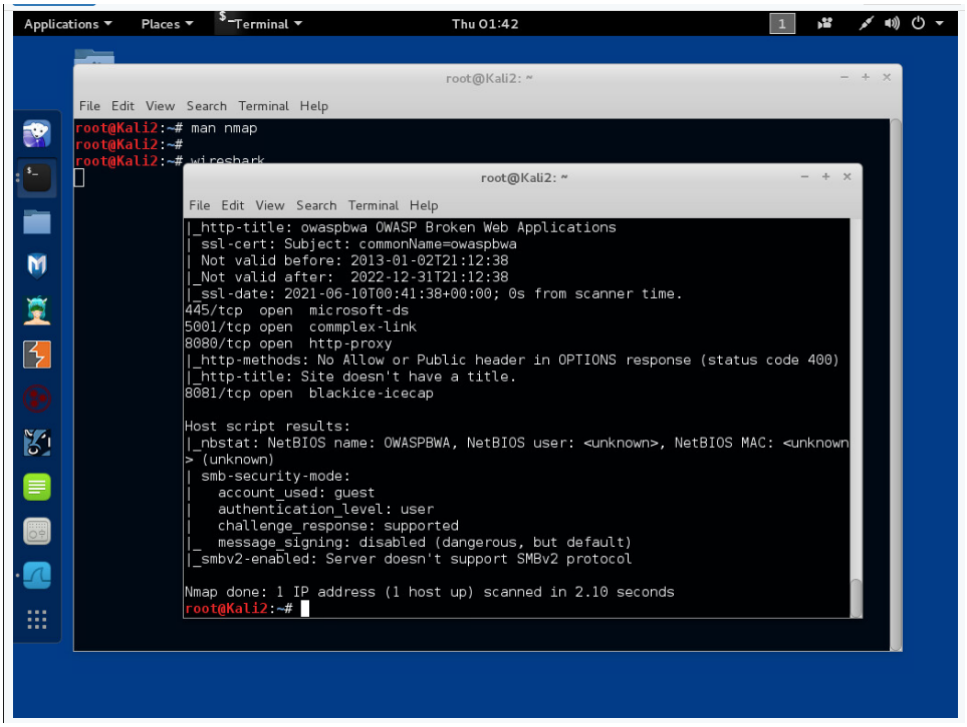

Fig.24 (Nmap scan with -sC to get possible vulnerabilities)

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. (Fig.25)

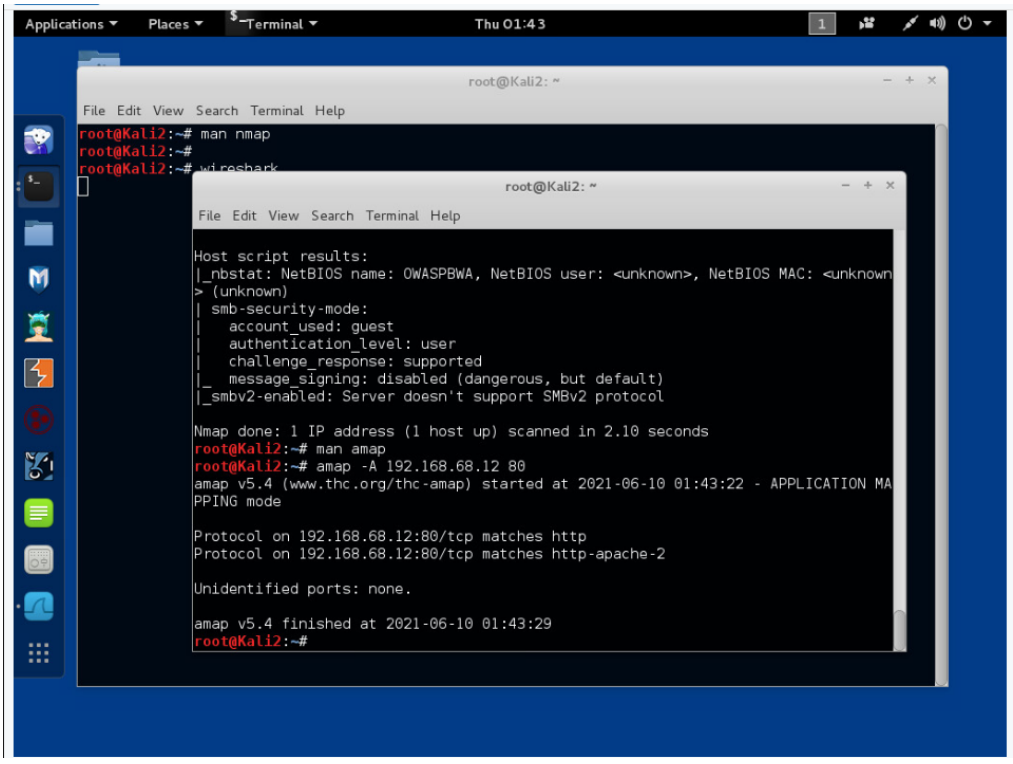

Fig.25 (Amap help command)

Finally we can get more information about any disponible port such as the version of the protocol or of the SHH used. (Fig. 26/27)

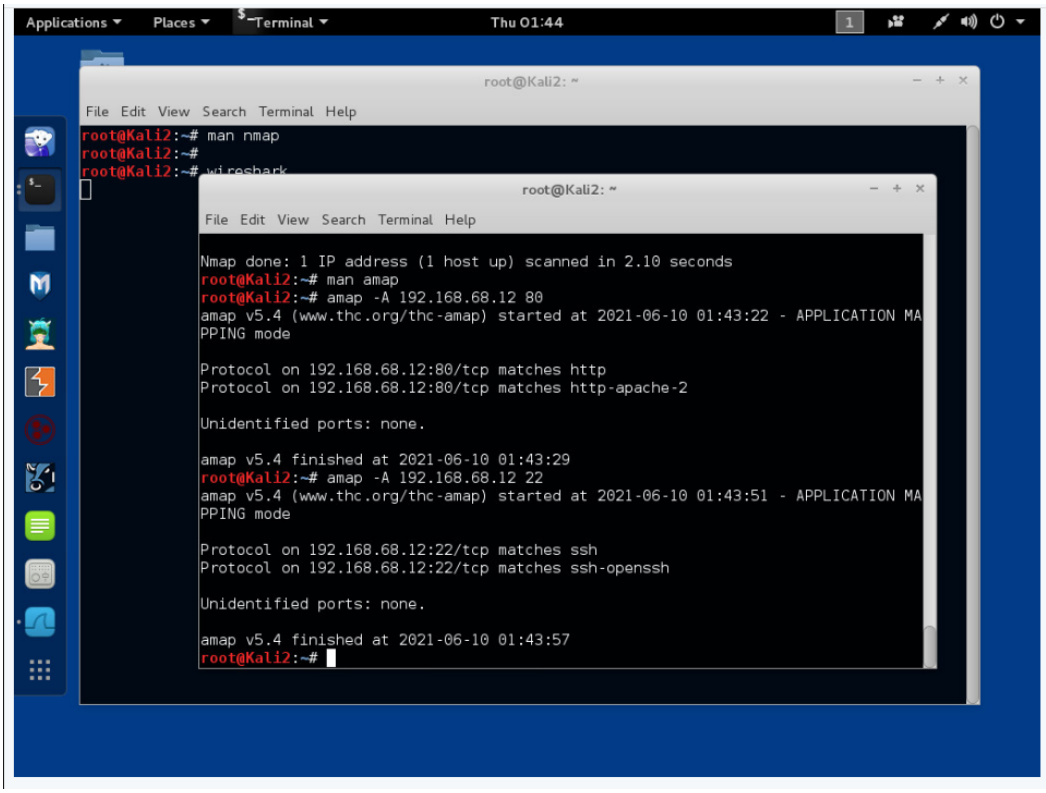

Fig.26 (Amap -A command)

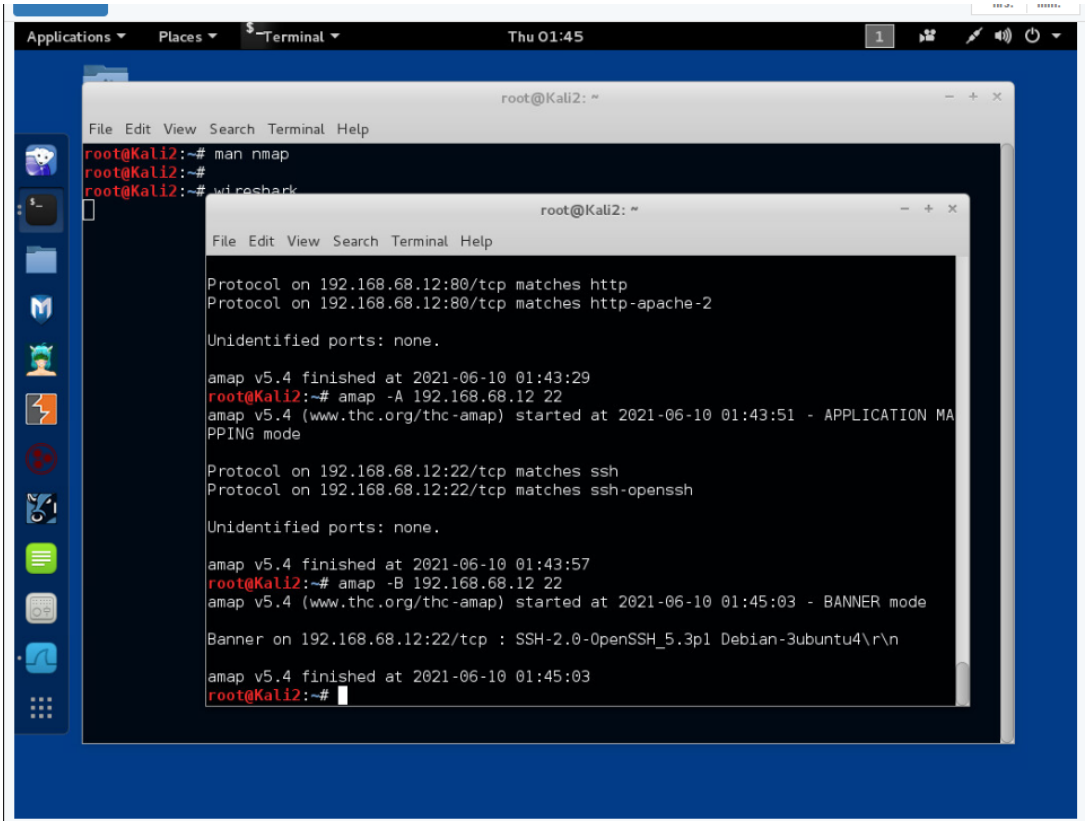

Fig.27 (Amap -B command)

When it comes to attacking devices on a network, you can't hit what you can't see. 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 so it can be used by malicious users to pry on a network to possibly attack and get data from.
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 (1000 with the normal nmap to the 100 with the -F).
Another possible method of attack could be using the high volume of requests to the system so if a malicious user sent multiple enormour requests as a DDOS the system could fail to operate fluently as it’s supposed to.
Hackers can also use these scanning commands to find a bunch of services running on open ports can be a huge benefit, especially if one of them has a version that is out of date and 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.

To begin working towards compliance, it’s important to check what rules or laws you need to comply with. Most cybersecurity compliance requirements require a risk and vulnerability assessment. These are critical in determining what your organization’s most critical security flaws are, as well as how efficient are the controls that are already in place.

Some of the most important technical controls to be implemented based on your risk assessment are the firewall, a monitoring software, having an antivirus, use multi factor identification,regular backups and encrypting passwords.

The financial sector is one of the most strictly regulated as banks and financial institutions work closely with customers’ private information, social security data, and financial records. Banks are also the most attacked sector, as most of the time the perpetrators are financially driven to find or create a breach in a bank's networks.

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 and Hashcat. The first uses a dictionary method so it takes text string samples from a word list using common dictionary words to crack passwords. The second guesses the password, by hashing it, and then compares the resulting hash to the one it's trying to crack. If the hashes are the same then the password is cracked.

In this lab (Lab 5: Password Cracking with John the Ripper and Hashcat) I've created a list of passwords and users that will be cracked with John the Ripper and Hashcat.

First 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 some passwords with restrictions.

Finally these files are later united in a file with the other list created by john the ripper.Then using the adduser and passwd command we create the fake account's details. (Fig. 28/29)

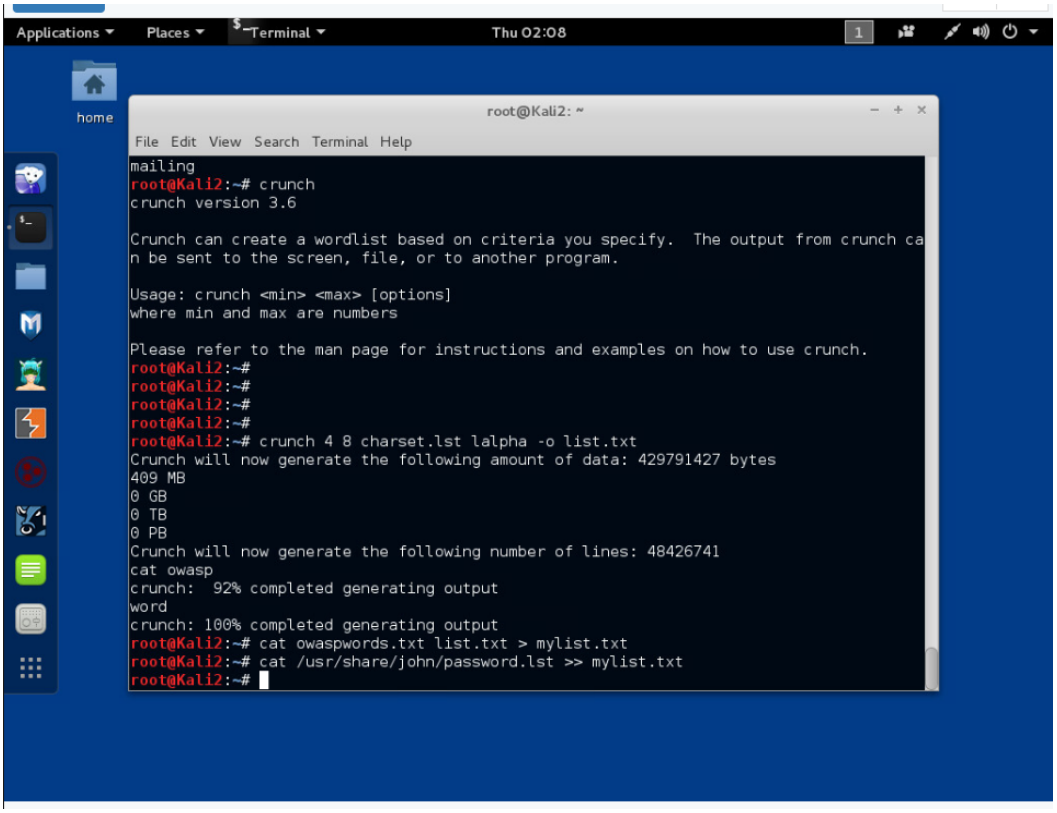

Fig.28 (Crunch and combining lists)

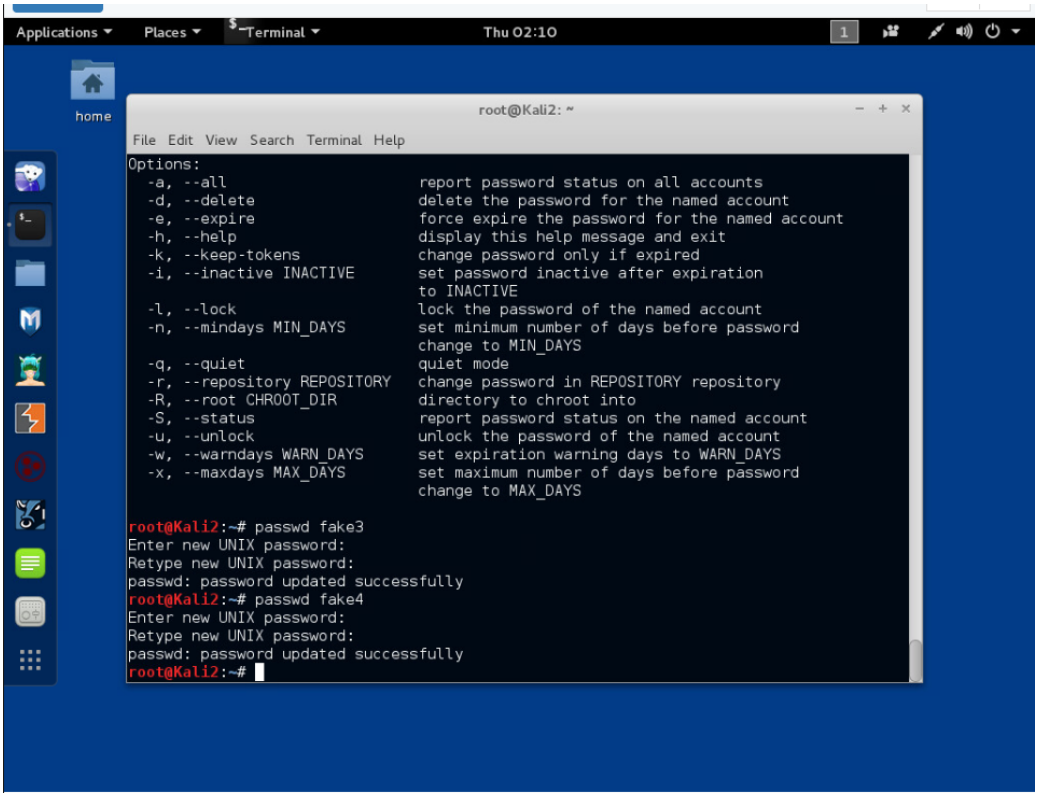

Fig.29 (Creating fake accounts with passwords)

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. (Fig. 30/31)

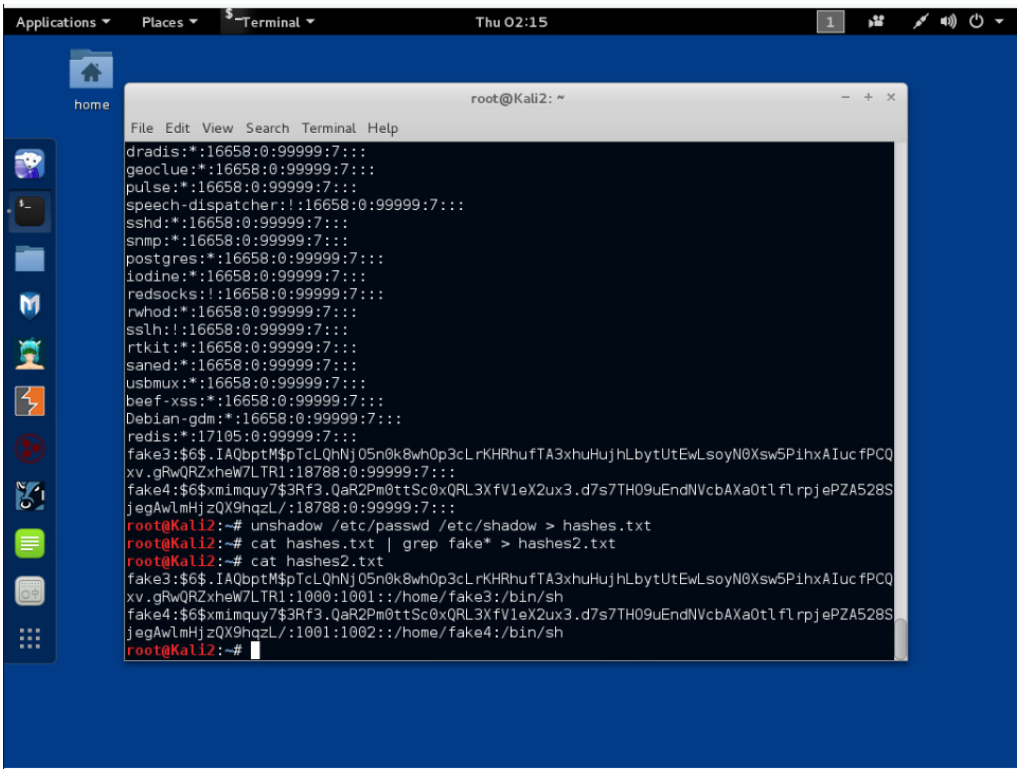

Fig.30 (Take information, narrow it down and display)

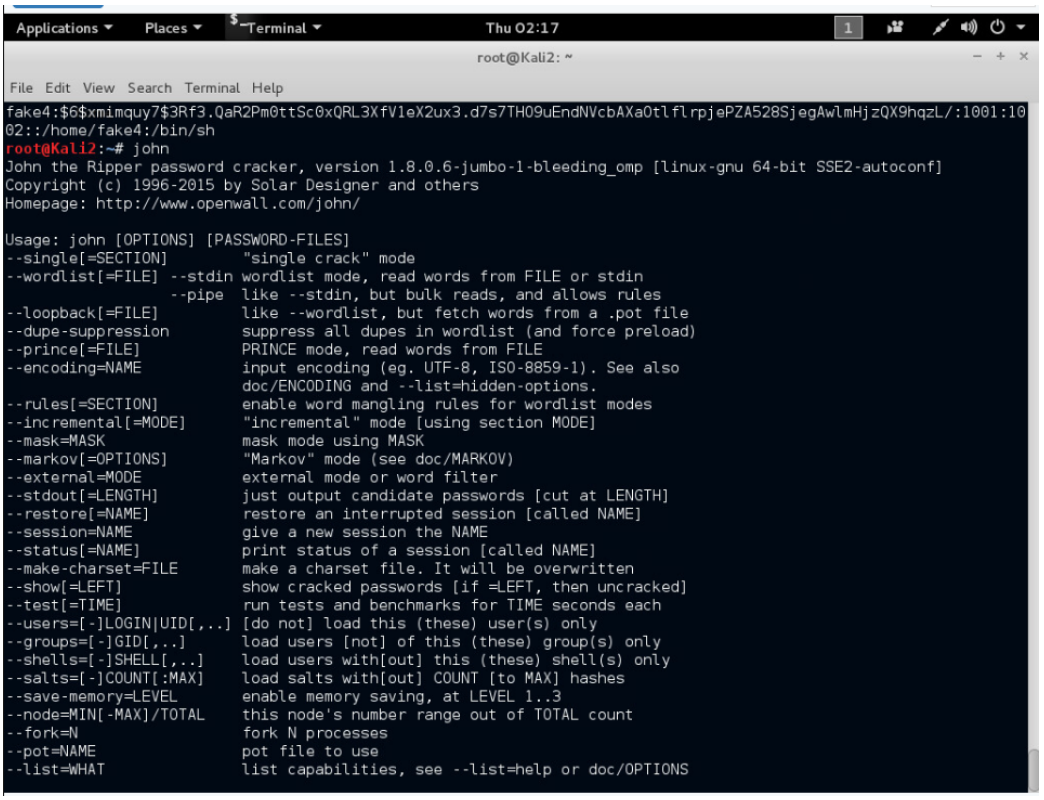

Fig.31 (John the ripper options)

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. (Fig. 32/33)

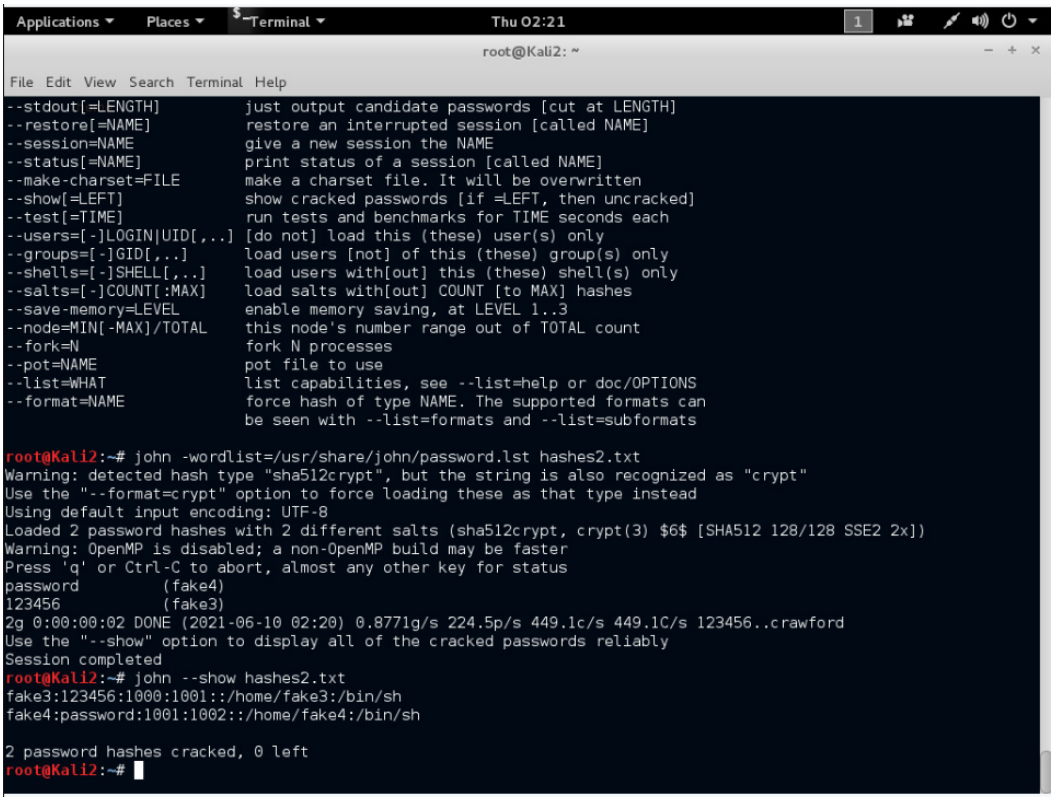

Fig.32 (John the ripper cracked passwords and display)

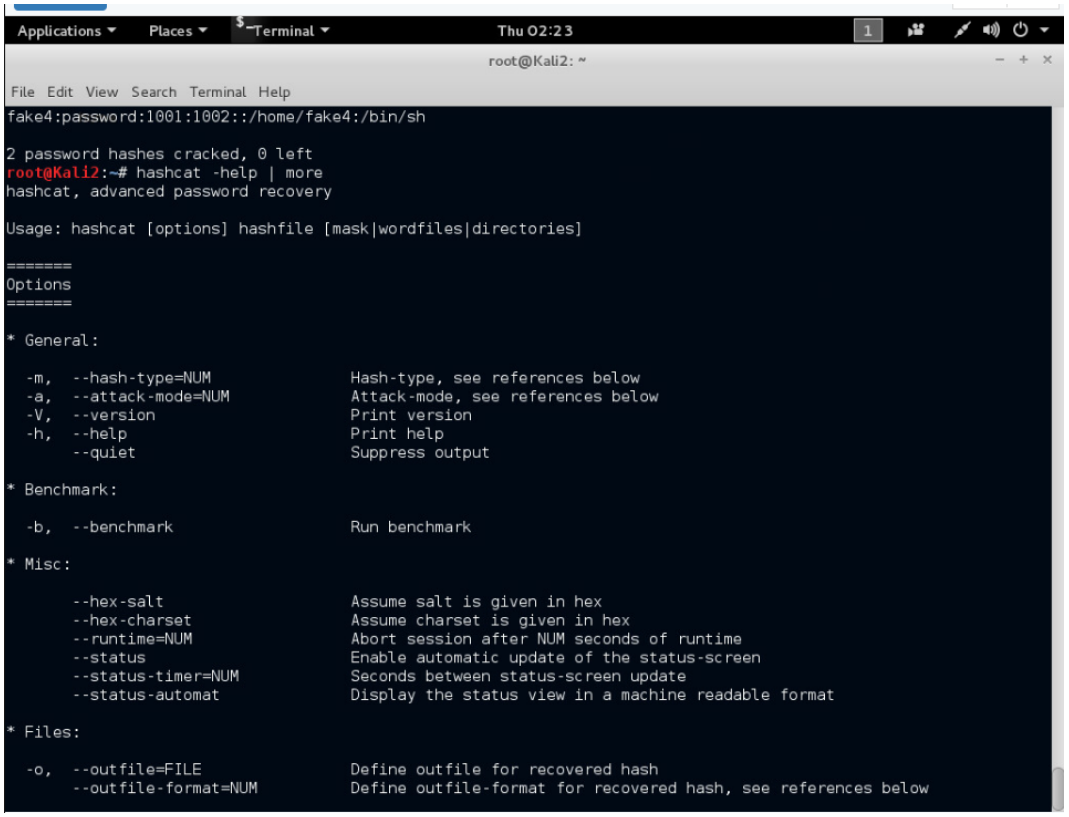

Fig.33 (hashcat help command)

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. (Fig. 34/35)

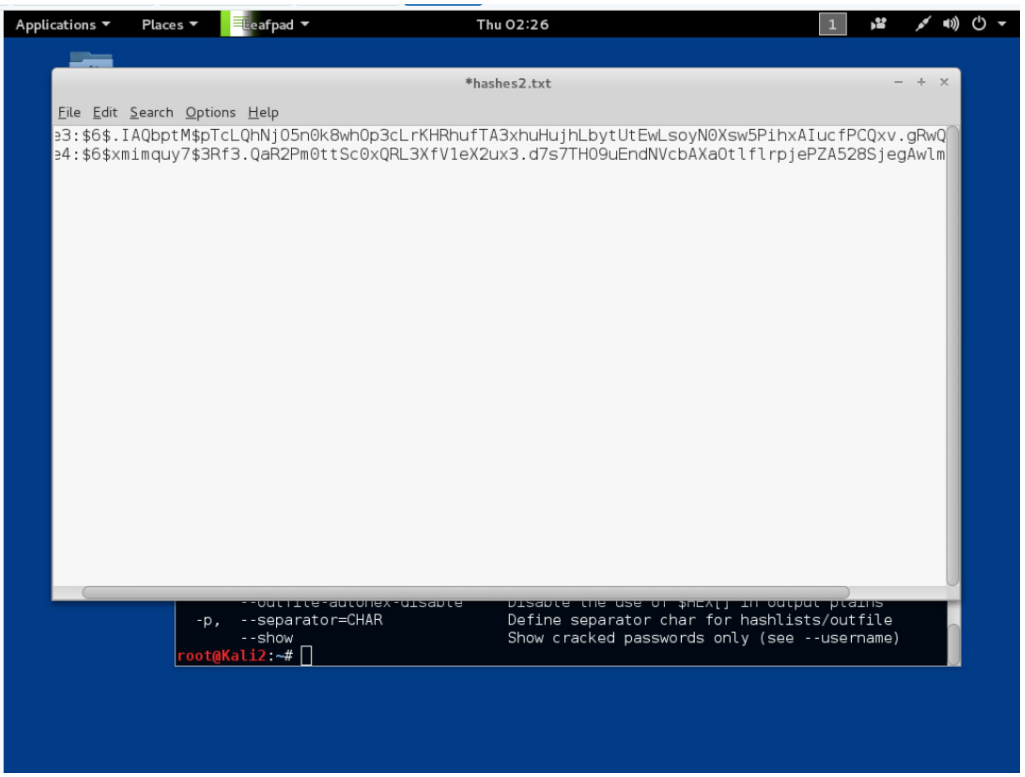

Fig.34 (hash of the passwords in the file)

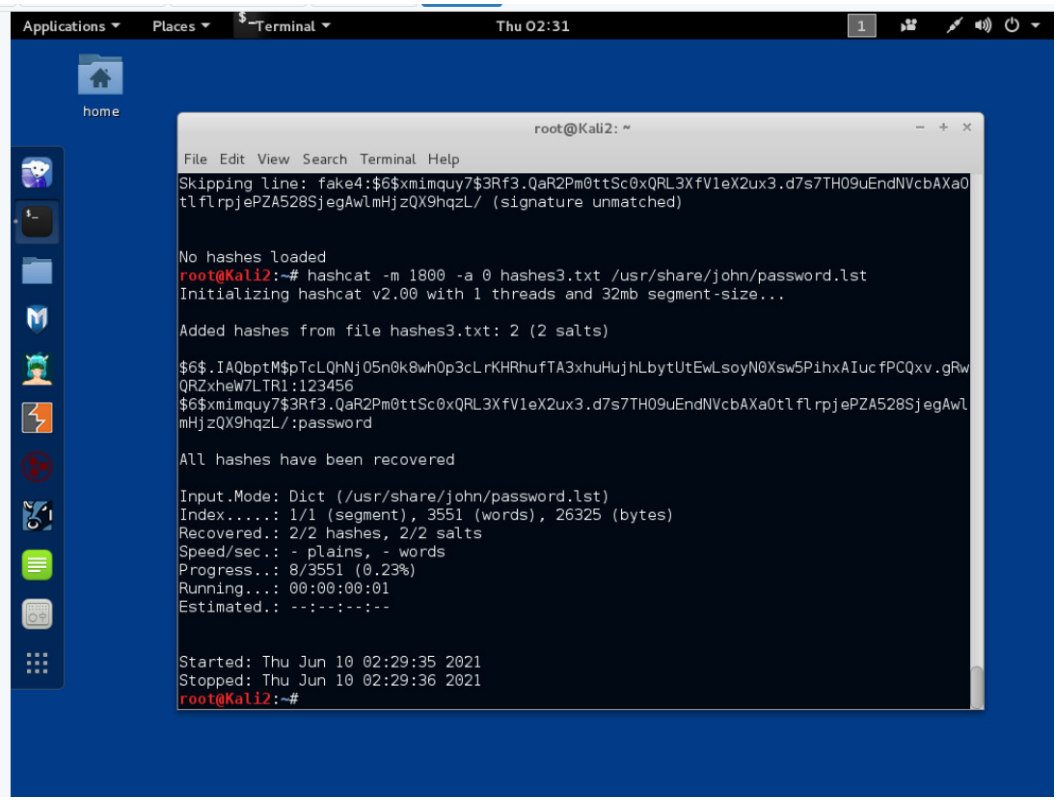

Fig.35 (hashed passwords)

For this lab it is fundamental to understand that these commands are just for educational purposes and can easily be 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.
While these two methods can certainly crack passwords they could require a very long time to do so if the lists used does not contain words that the users could've used in it's 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