6G7Z1009 Introduction to Computer Forensics and Security week 10 – Lab 2

This lab aims to understand how Kerberos works in our labs.

I. **Review questions (write down your answers) based on the lecture notes and further readings:**

1.1 What problems do Kerberos address?

1.2 What are the major working steps of Kerberos?

II. **Preparation:**

- **Just turn on the machine to linux environment and do not login**
- **Press "CTR+ALT+F1" and go to the first virtual terminal (If you need more virtual terminals, you can easily use "CTR+ALT+F2/oR F3 or/F4/or F5 or F6". If you want to go to the graphical interface, press "CTR+ALT+F7")**
- **Type your user name and login**

2.1 Task 1: To use klist and show Kerberos ticket

- **Type command "man klist" to understand the meaning and usage of klist**
- **Type the command "mount –t nfs4" and record the result you have just seen (notice the sec=krb5 option, which means a Kerberos service ticket is needed to access the NFS server). To record your result, you could use "mount –t nfs4 > filename"**
- **Type the command "ls /home/users" and to observe the contents on that directory.**
- **Type the command "klist" and record the result you have observed (using "klist > myklist") and find out your TGT and TGS**

2.2 Task 2: To use kdestroy to demonstrate before and after you use Kerberos authentication method.

- **Type "man kdestroy" to understand the meaning and usage of kdestroy**
- **Type "kdestroy"**
- **Type "klist" and record the result (to record your result, you may use redirection symbol: klist > filenamex)**

- **Type “mkdir –m 700 /tmp/yourname” (this will create a directory, please refer to linux guidance the usage of mkdir or you can use “man mkdir” to understand it)**
- **Type “HOME=/tmp/yourname”. This will change your home directory from /home/users/yourname to /tmp/yourname**
- **Type “env” and check whether /tmp/yourname is your home directory**
- **Type “cd ” and record the result**
- **Type “ls /home/users/ ” and record the result**
- **Type “sudo killall –USR1 automount” (you can use “man automount” for details.)**
- **Wait for a couple a seconds, and then type “ls /home/users/” and ls /home/users/yourname”, record the result and explain it**

2.3 Task 3: To use kinit to show recover tickets (the process of Kerberos)

- **Type “man kinit” to understand the meaning and usage of kinit**
- **Type “kinit” and record the result**
- **Type “klist” and record the result**
- **Type “ls /home/users/yourname”, record the result and explain it.**

2.4 Task 4: to use Wireshark (a network monitor tool) to observe packets when a user log into the other machine (please try to log in to your neighbor machine)

- **Two of you pair together.**
- **Machine 1 stays virtual terminal (not a graphic interface).**
- **Machine 2 can go to the graphic interface by pressing “ALT+F7/F8” and then open a terminal.**
    - **Type /sbin/ifconfig and find Ethernet interface name that has a public IP address, for example, eth1.**
    - **Type command “wireshark” and select eth1 and start capture network packets**
- **Machine 1 now can try to log in to machine 2 by using ssh yourusername@machine 2**
- **After your login, you can stop Wireshark, look at the packets and explain it**

Important:

2.5 Task 5, please make sure you log out from all your virtual terminal by typing the commands “logout” or “exit” or using “CTR+D”