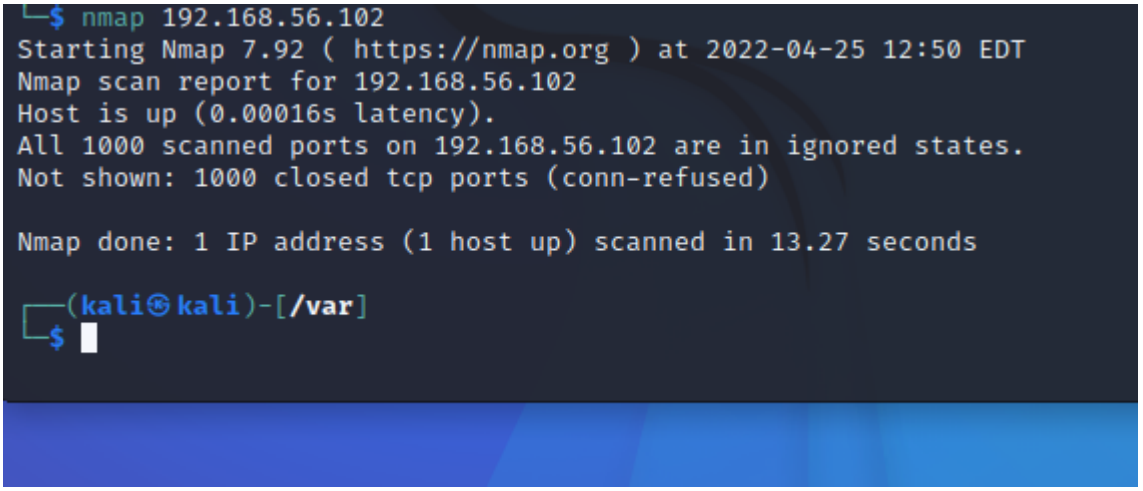
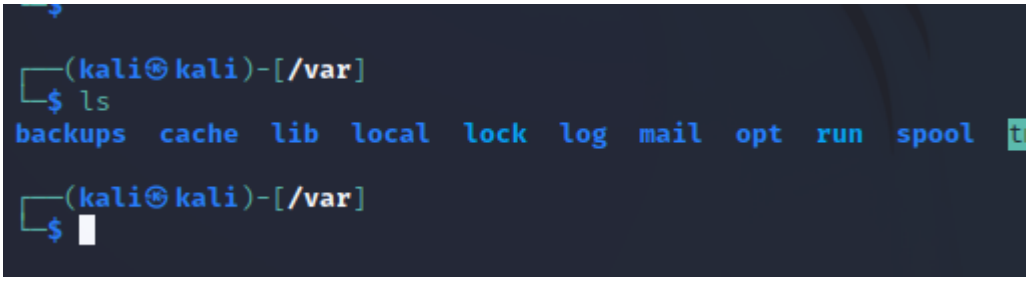
Mert Furkan Ergüden 170709015 – Computer Networks and Security Lab Report

I used the nmap method in this lab. I tried to look at the traffic status in the console by typing " nmap ipadres". Because I didn't do this step in lab class last week. This field is missing. I have attached the relevant pictures to the report.



This week, I will examine the logs inside my linux machine. In the Linux operating system, logs are available in the var/log address.



When we enter the log folder, we can see all the logs of the computer here.

```
┌──(kali㉿kali)-[/var]
└─$ cd log

┌──(kali㉿kali)-[/var/log]
└─$ ls
alternatives.log    daemon.log.2.gz  lightdm                macchanger.log.1.gz  stunnel4
alternatives.log.1  debug            macchanger.log.2.gz    syslog               
apache2             debug.1          messages               syslog.1             
apt                 debug.2.gz       messages.1             syslog.2.gz          
auth.log            dpkg.log         messages.2.gz          sysstat              
auth.log.1          dpkg.log.1       mysql                  user.log             
auth.log.2.gz       faillog          nginx                  user.log.1           
boot.log            fontconfig.log   openvpn                user.log.2.gz        
boot.log.1          inetsim          postgresql             wtmp                 
boot.log.2          installer        private                Xorg.0.log           
boot.log.3          journal          README                 Xorg.0.log.old       
btmp                kern.log         runit                  Xorg.1.log           
btmp.1              kern.log.1       samba                  
daemon.log          kern.log.2.gz    speech-dispatcher      
daemon.log.1        lastlog

┌──(kali㉿kali)-[/var/log]
└─$
```


Then we can see all login logs by typing "cat auth.log" command.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[/var/log]
└─$ cat auth.log
Apr 25 12:46:36 kali lightdm: pam_unix(lightdm-greeter:session): session ope
ed for user lightdm(uid=130) by (uid=0)
Apr 25 12:46:36 kali systemd-logind[463]: New session c1 of user lightdm.
Apr 25 12:46:36 kali systemd: pam_unix(systemd-user:session): session opened
for user lightdm(uid=130) by (uid=0)
Apr 25 12:46:47 kali lightdm: gkr-pam: unable to locate daemon control file
Apr 25 12:46:47 kali lightdm: gkr-pam: stashed password to try later in open
session
Apr 25 12:46:47 kali lightdm: pam_unix(lightdm-greeter:session): session clo
ed for user lightdm
Apr 25 12:46:47 kali lightdm: pam_unix(lightdm:session): session opened for
ser kali(uid=1000) by (uid=0)
Apr 25 12:46:47 kali systemd-logind[463]: Removed session c1.
Apr 25 12:46:47 kali systemd-logind[463]: New session 2 of user kali.
Apr 25 12:46:47 kali systemd: pam_unix(systemd-user:session): session opened
for user kali(uid=1000) by (uid=0)
Apr 25 12:46:47 kali lightdm: gkr-pam: gnome-keyring-daemon started properly
and unlocked keyring
Apr 25 12:46:53 kali polkitd(authority=local): Registered Authentication Age
t for unix-session:2 (system bus name :1.41 [/usr/lib/policykit-1-gnome/polk
t-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/Authentic
tionAgent, locale en_US.UTF-8)
Apr 25 12:55:01 kali CRON[3264]: pam_unix(cron:session): session opened for
ser root(uid=0) by (uid=0)
Apr 25 12:55:01 kali CRON[3264]: pam_unix(cron:session): session closed for
```

As a result, I was only able to look at the logs. I can not read some of the logs.