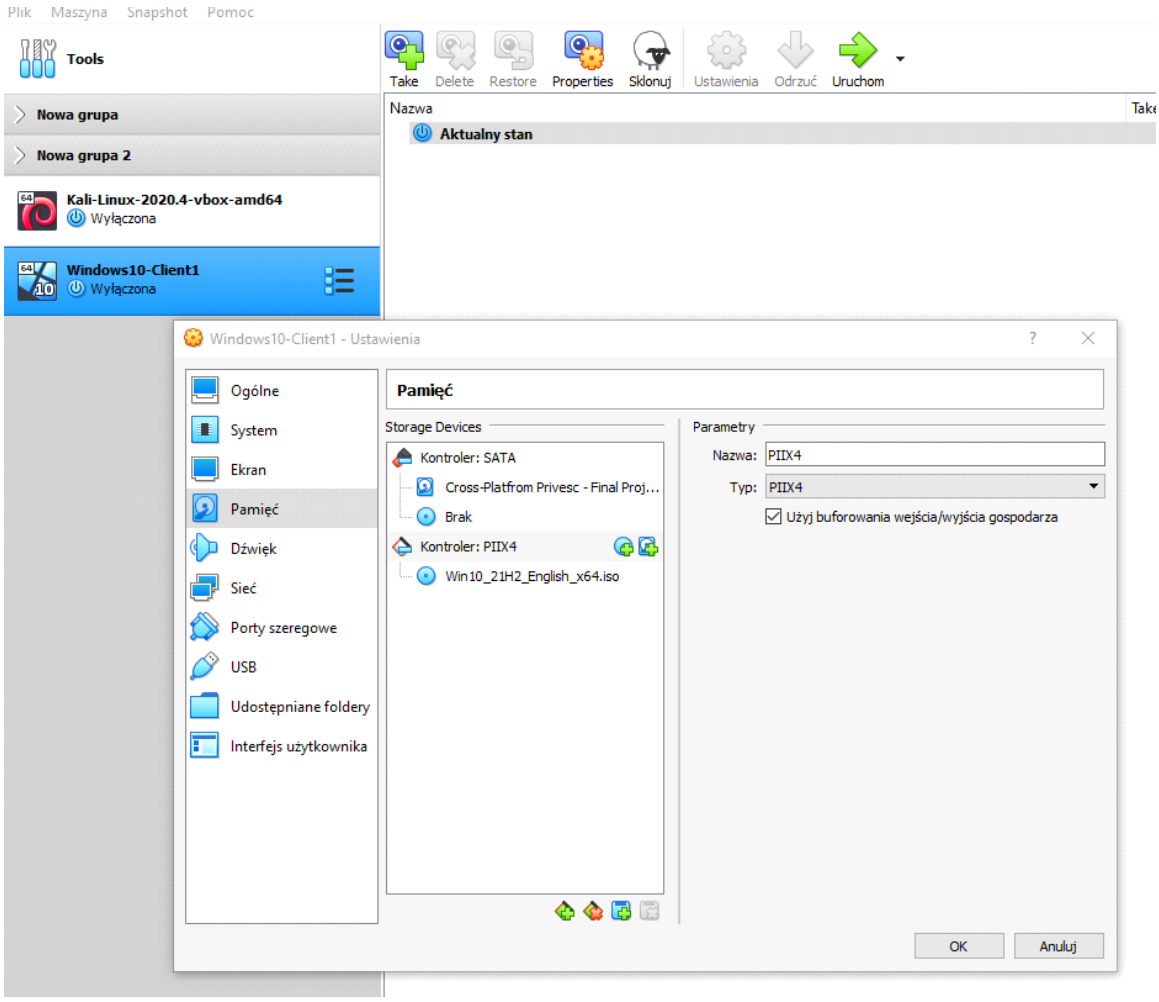
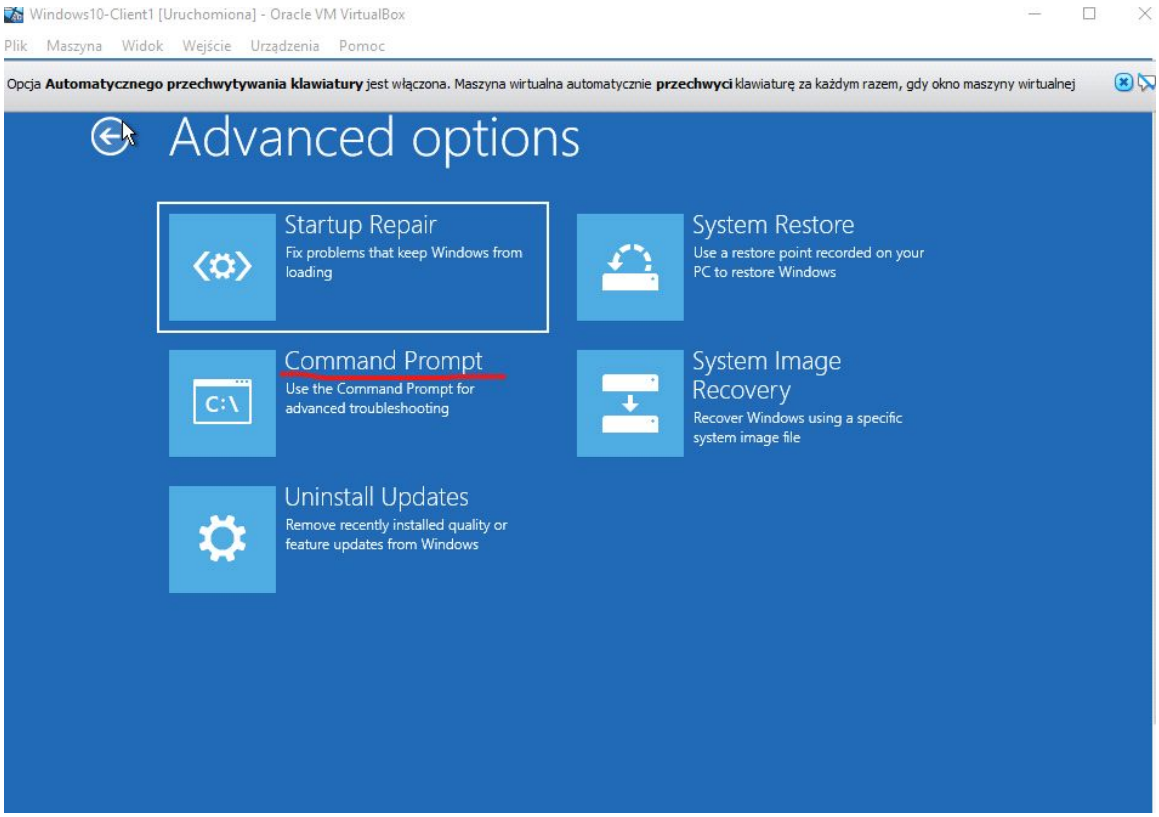
Cross Platform Privilege Escalation - Final Project

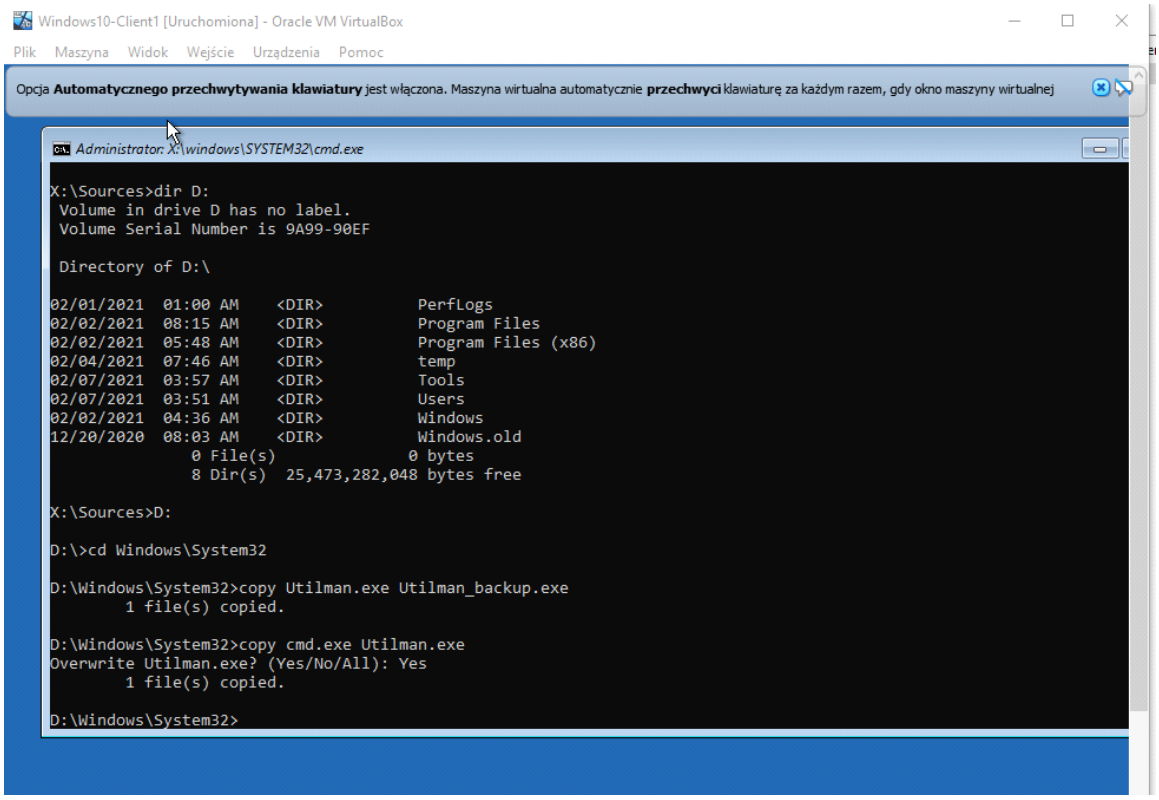
Firts we mounting Windows10



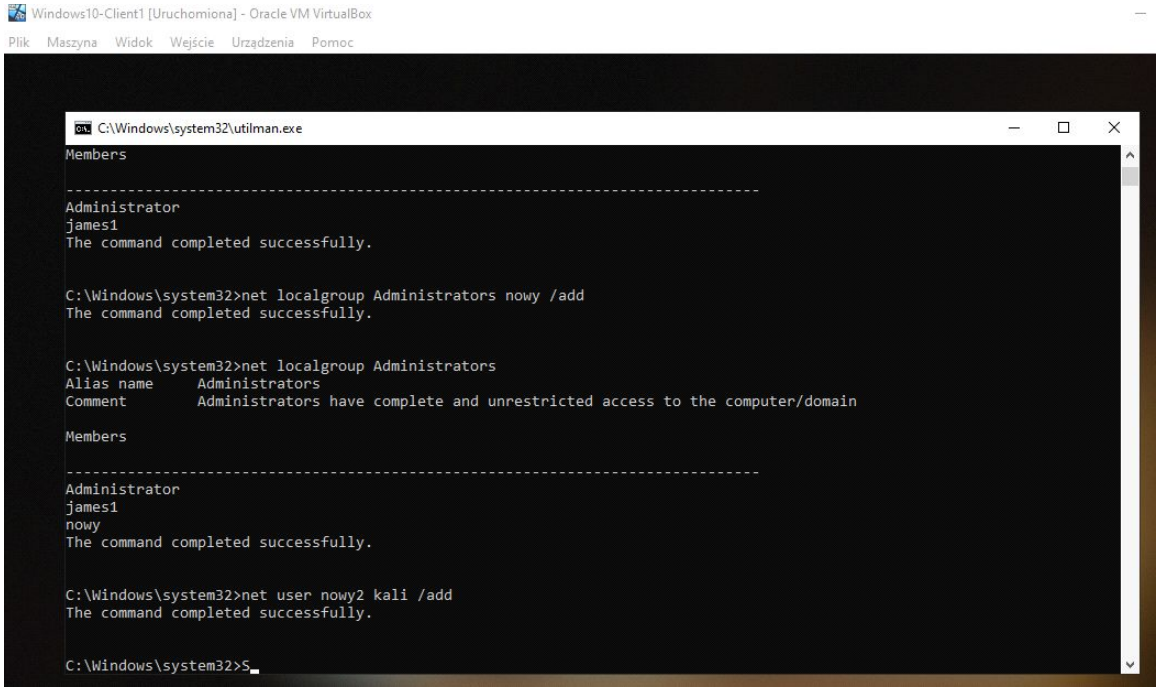
We launching it and choosing CMD option



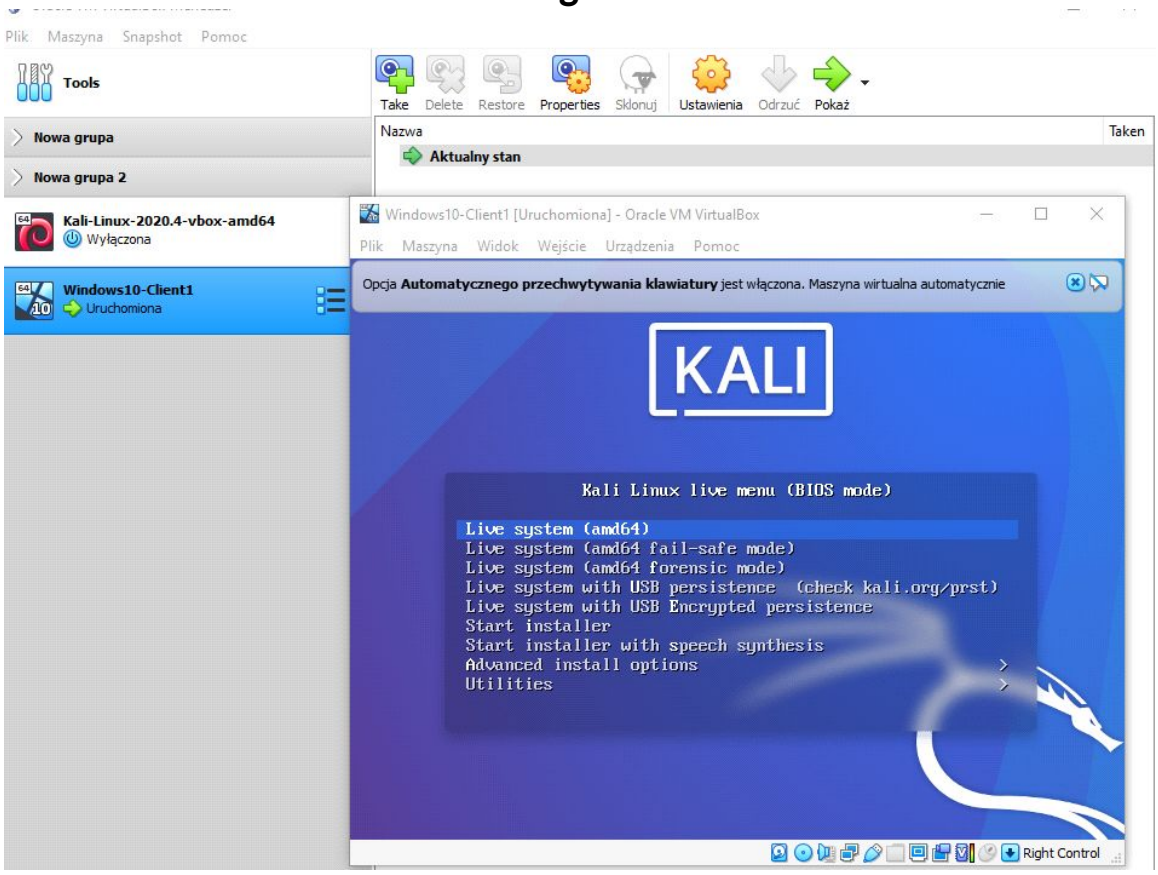
Some Files manipulations over here ;)



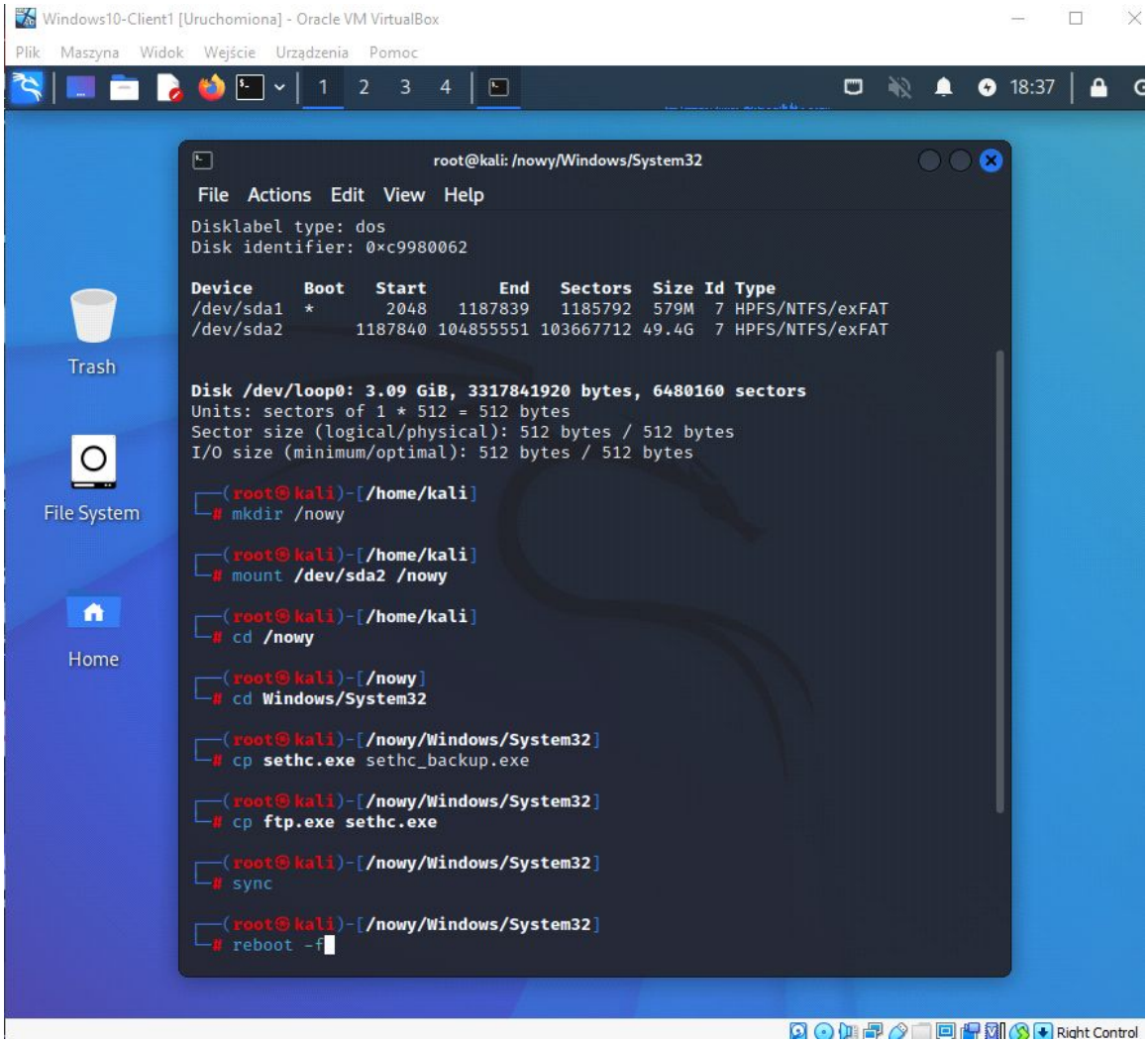
Creating 2 users



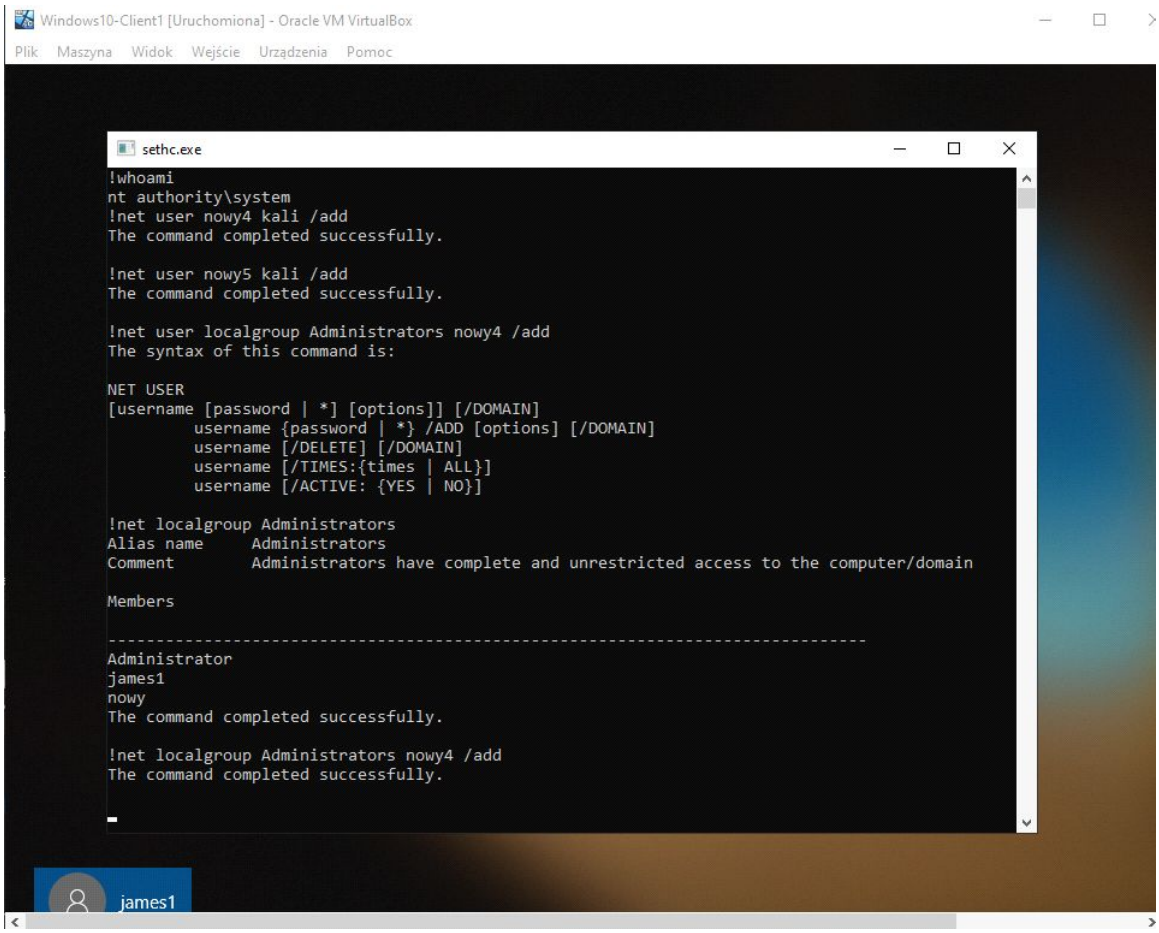
And Using Kali linux:



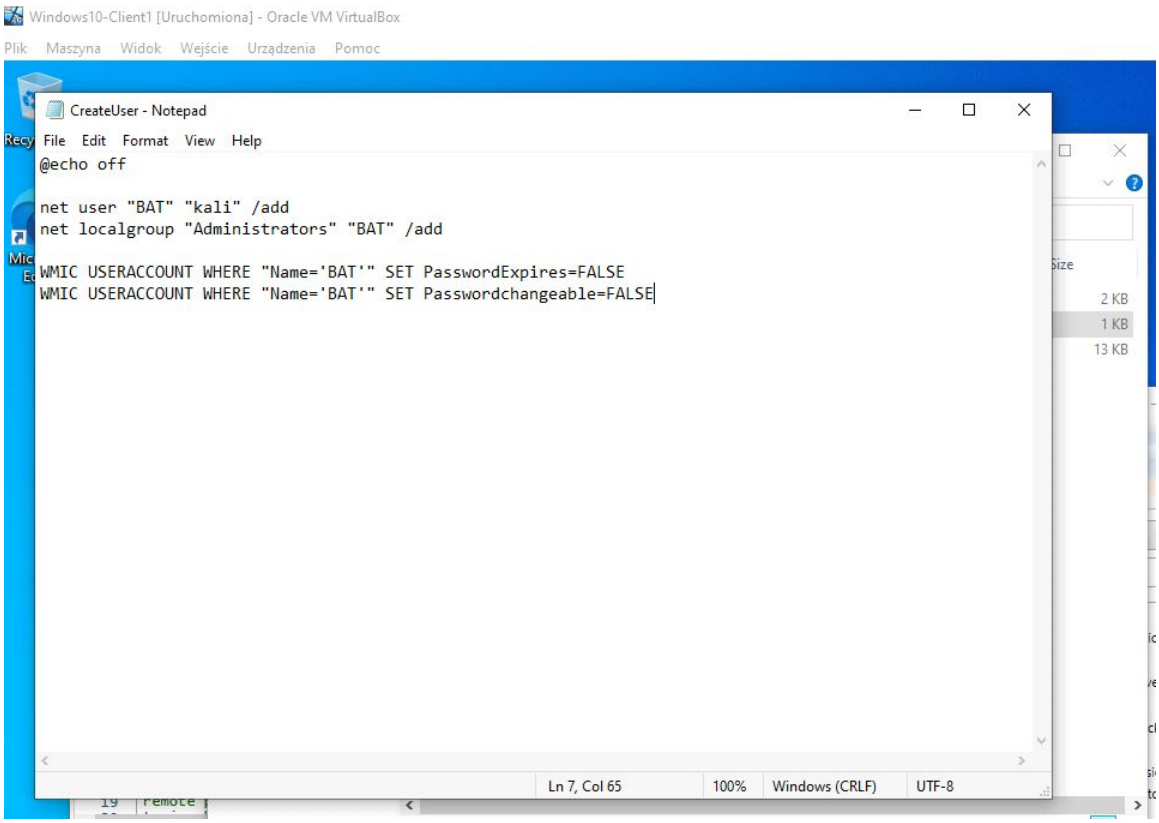
This time we switching ftp.exe with sethc.exe



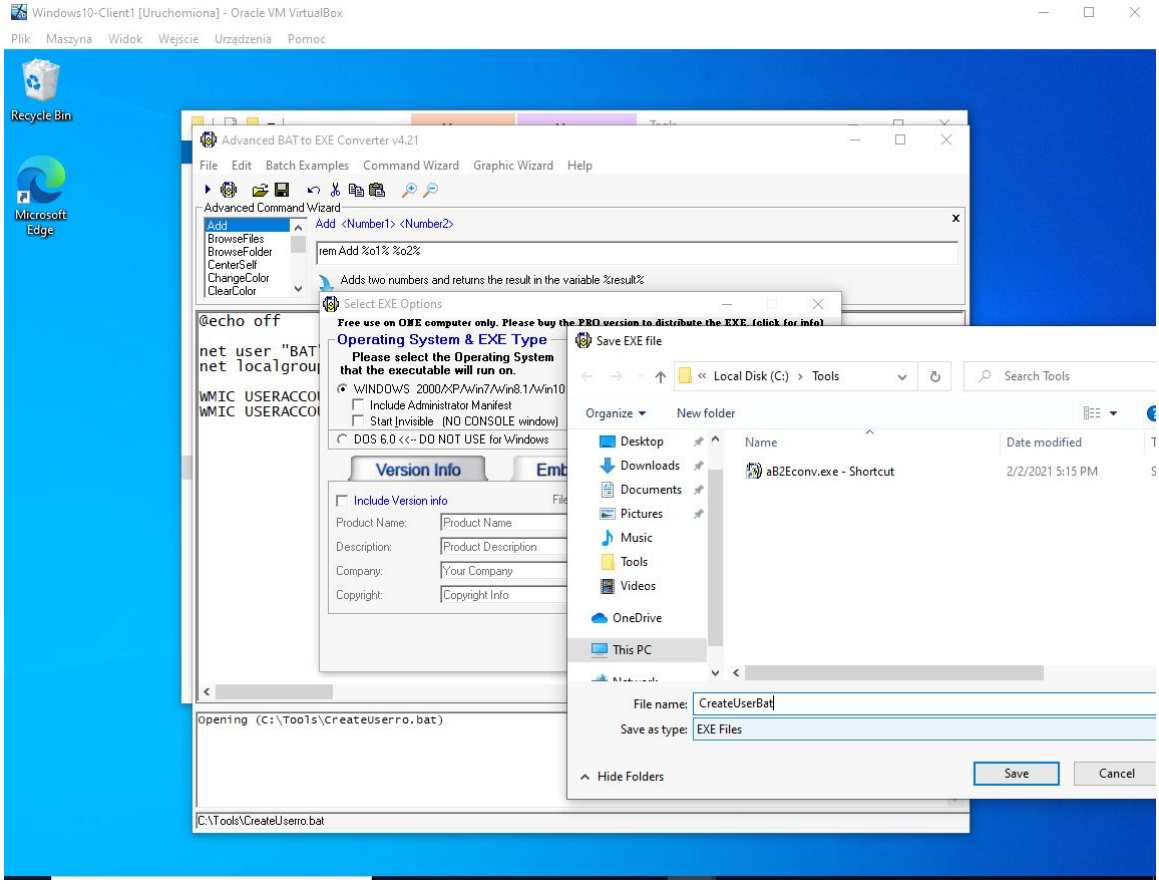
And it's working nicely ;)



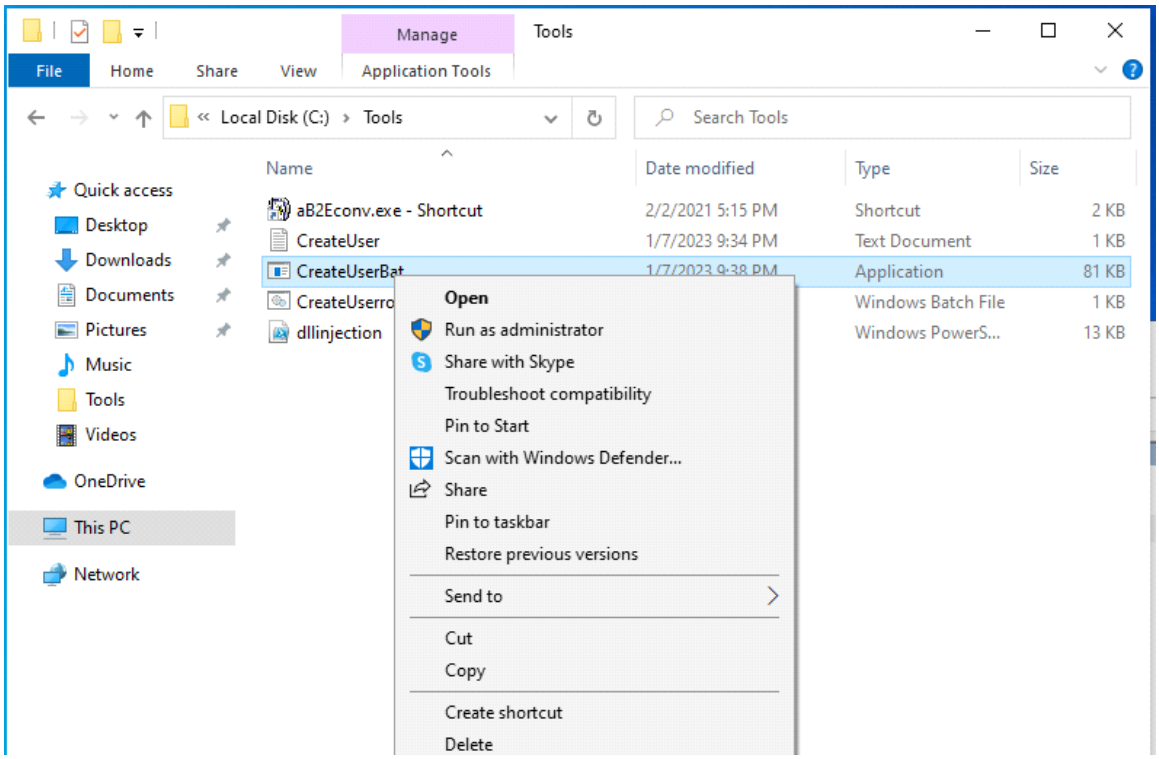
I created .bat file to create new user



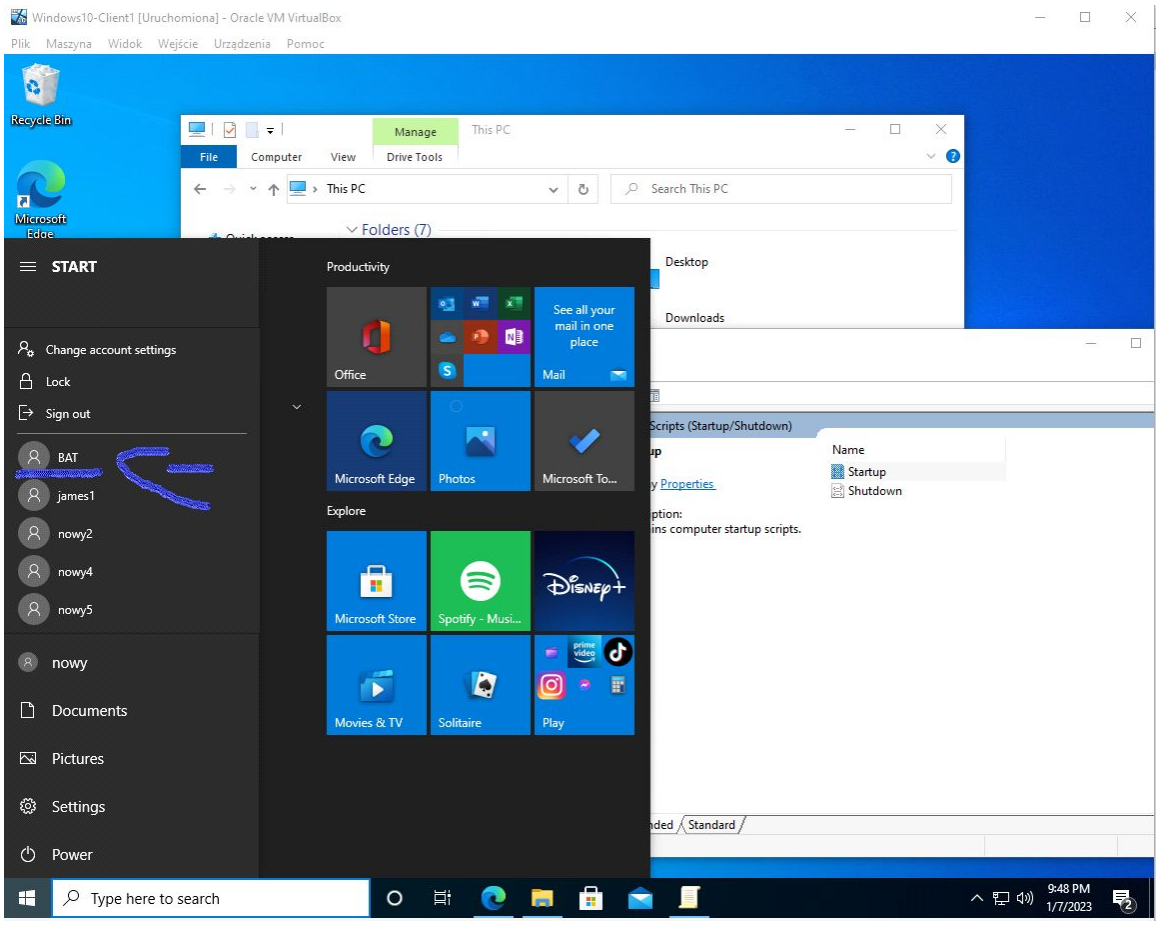
I created .exe using tools on the system



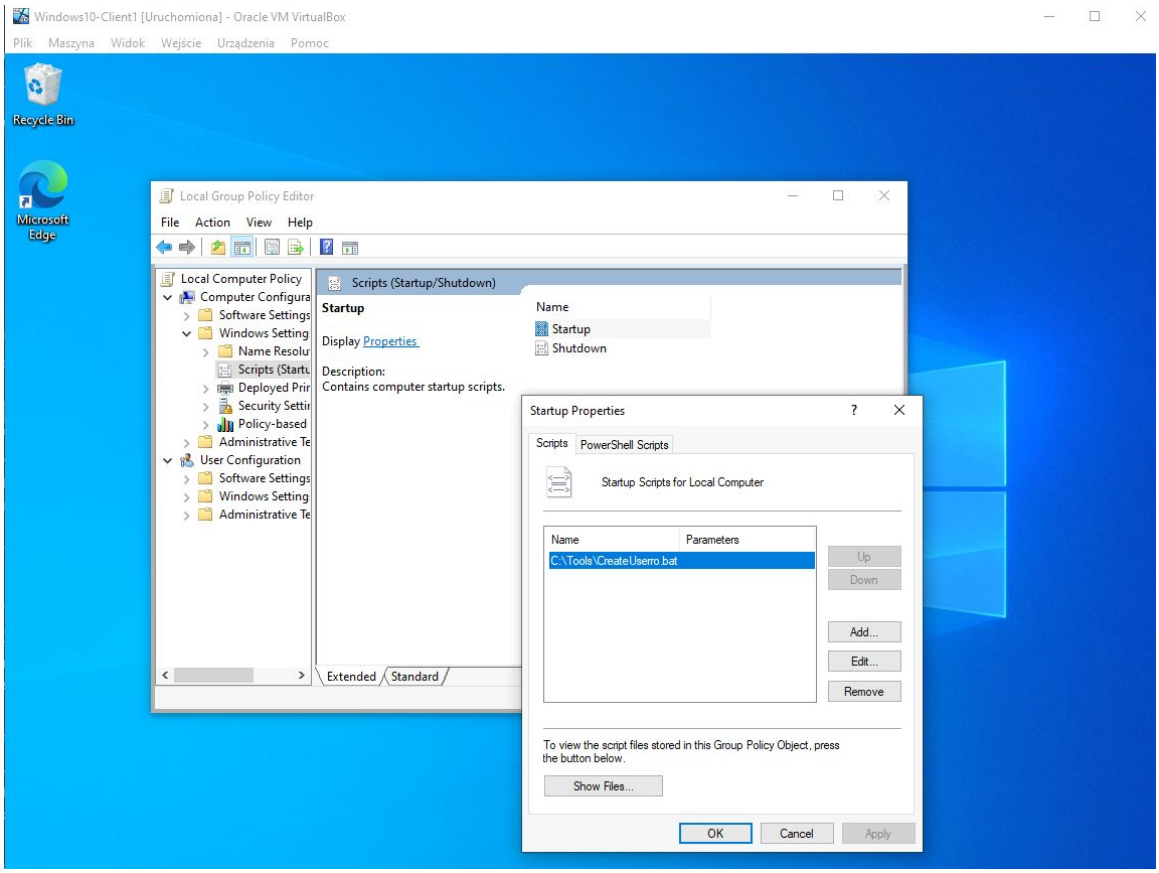
Executing progrogram



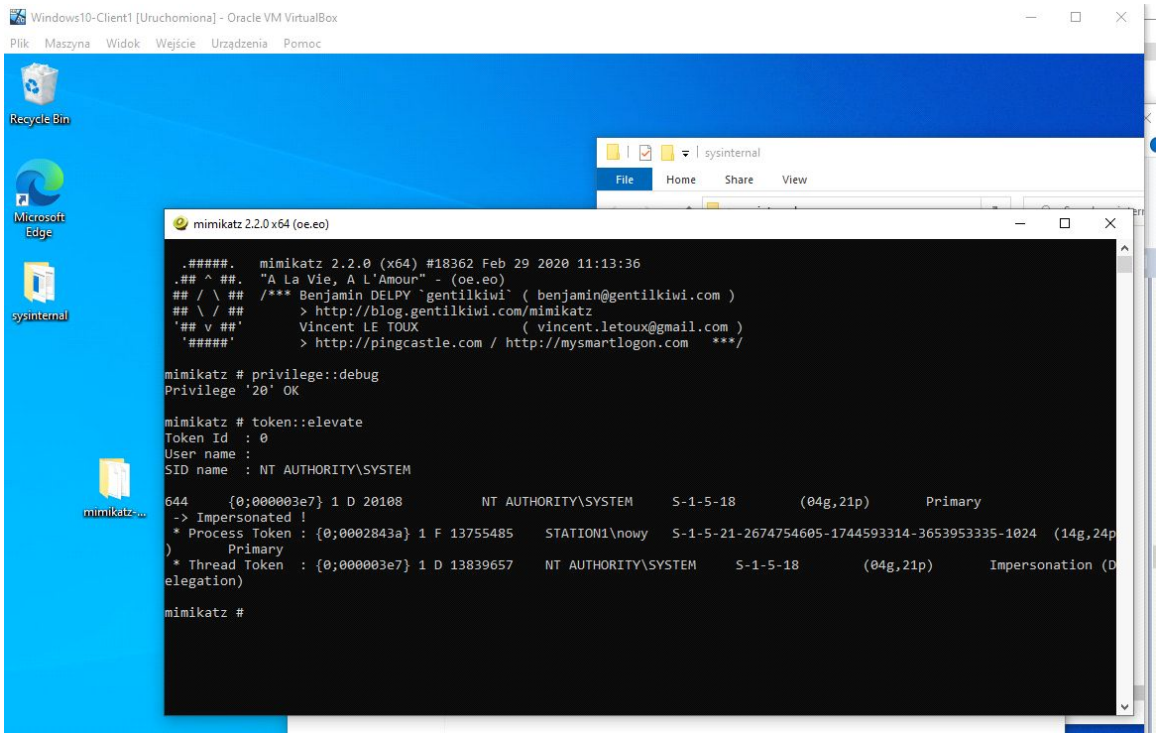
We can see that it worked !



We could also add this to GPO

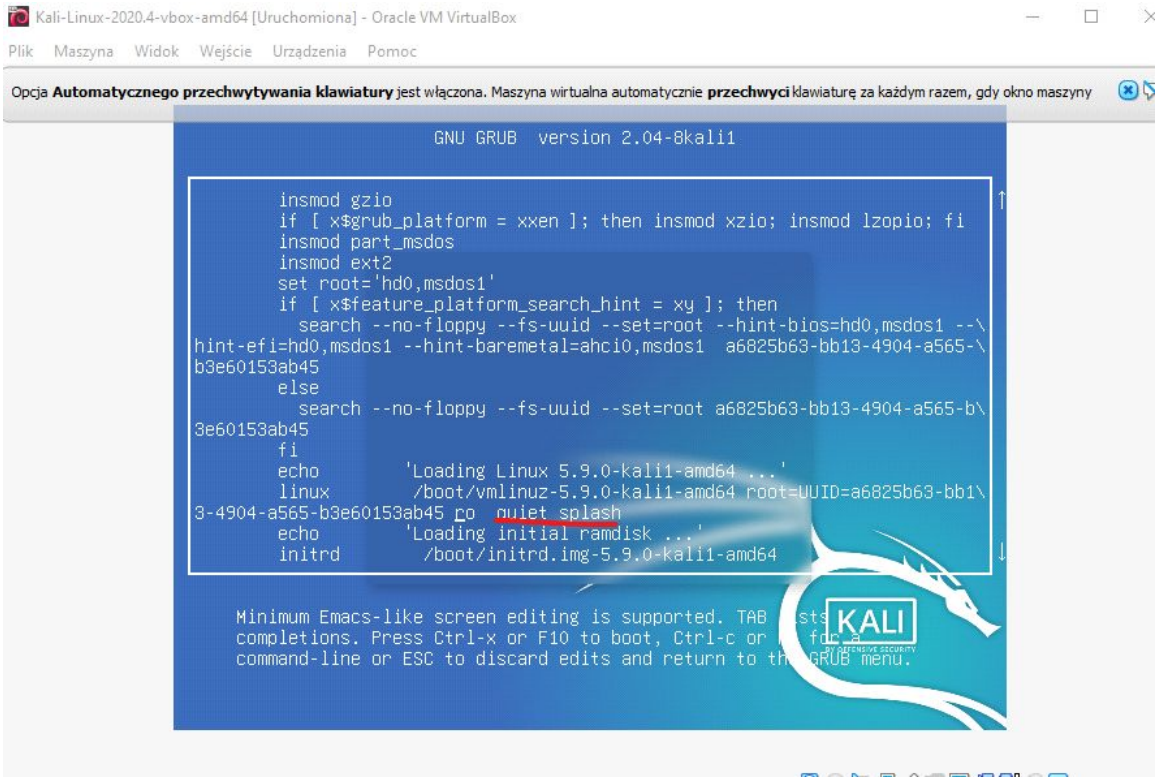


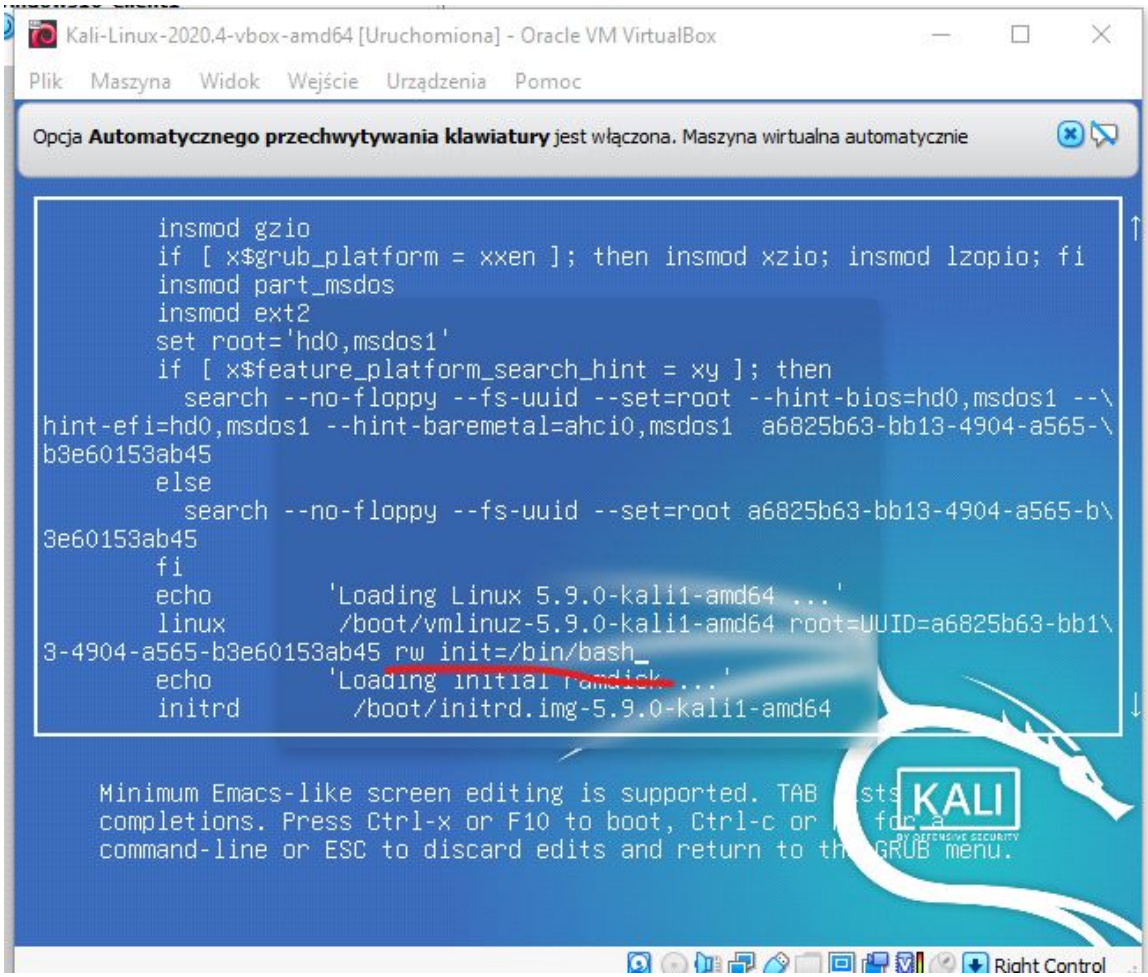
To gain NT-Authority we can use mimikatz



PART 2

We can gain acces to the machine via manipulating GRUB Bootloader





and now adding user ;)

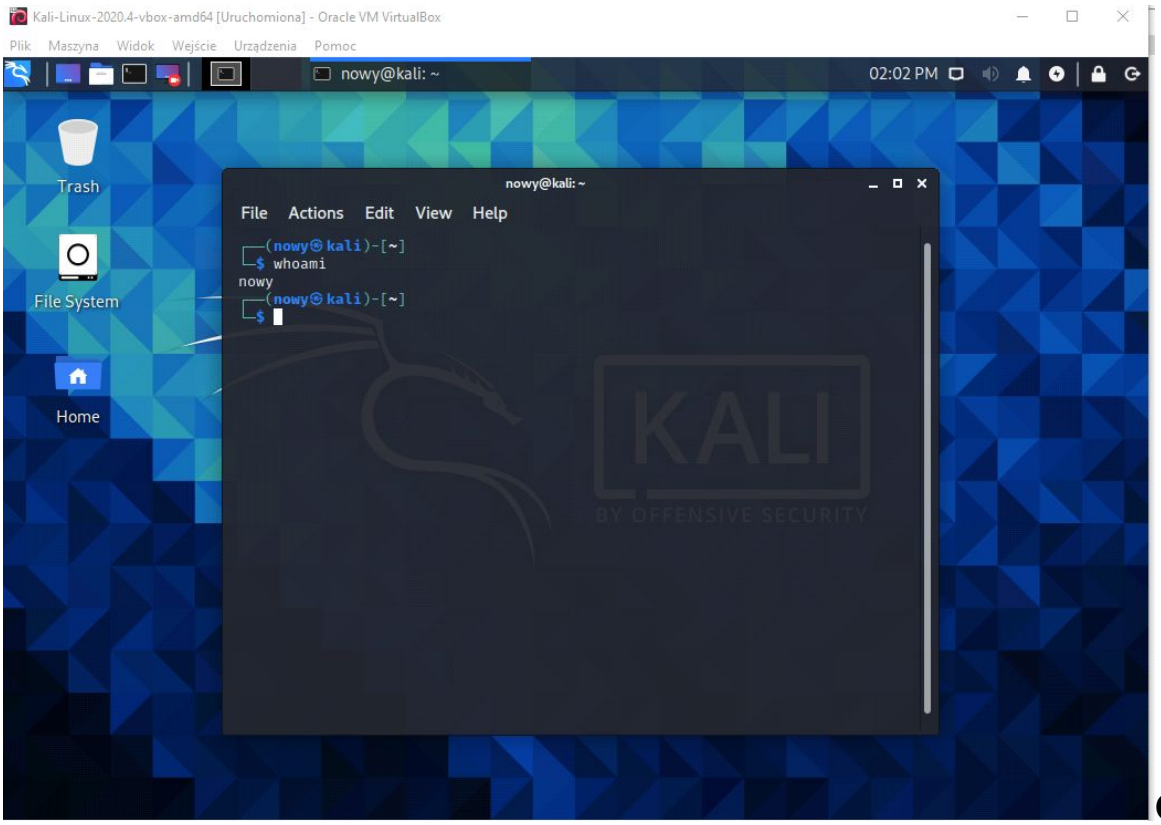
Kali-Linux-2020.4-vbox-amd64 [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

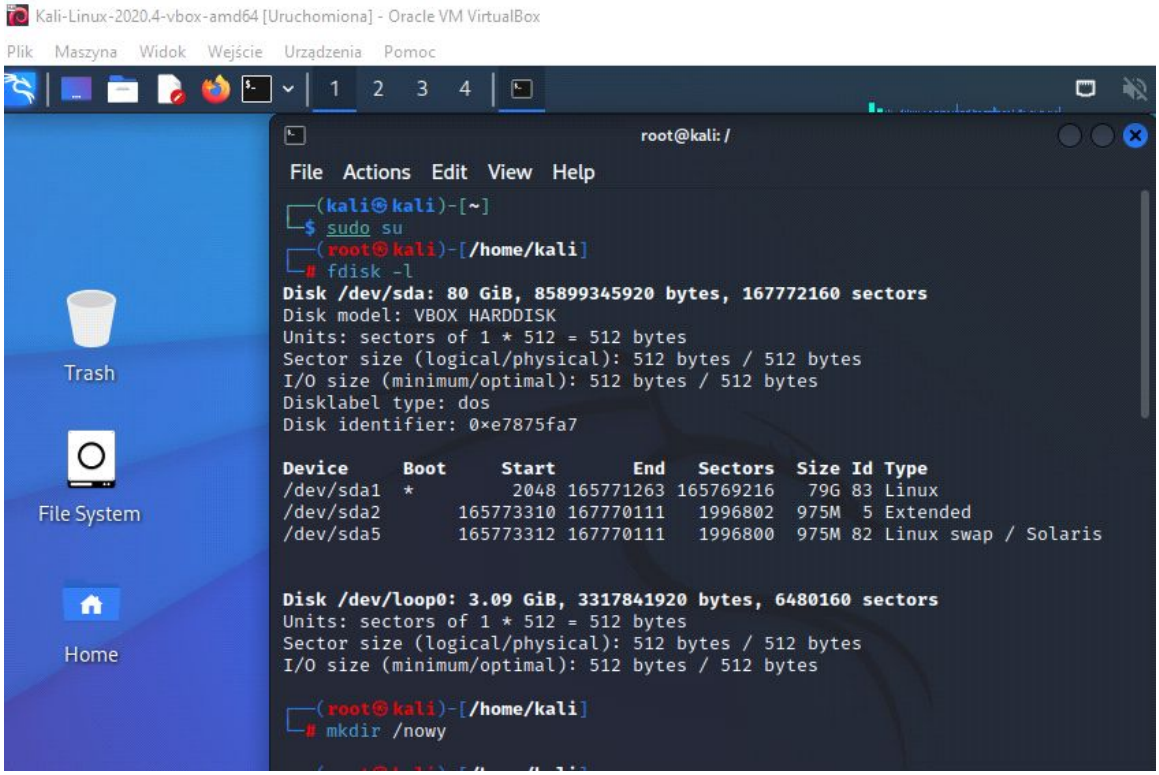
Opcja **Automatycznego przechwytywania klawiatury** jest włączona. Maszyna wirtualna automatycznie **przechwyci** klawiaturę za każdym

```
/dev/sda1: clean, 307841/5185536 files, 2852557/20721152 blocks
done.
[    2.391121] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
[    2.452408] usb 1-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
[    2.452926] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
[    2.453406] usb 1-1: Product: USB Tablet
[    2.453867] usb 1-1: Manufacturer: VirtualBox
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# adduser nowy
Adding user `nowy' ...
Adding new group `nowy' (1001) ...
Adding new user `nowy' (1001) with group `nowy' ...
Creating home directory `/home/nowy' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nowy
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root@(none):/# adduser nowy sudo
Adding user `nowy' to group `sudo' ...
Adding user nowy to group sudo
Done.
root@(none):/# _
```

Right Control



Or using KALI Live



Kali-Linux-2020.4-vbox-amd64 [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

1 2 3 4

Trash

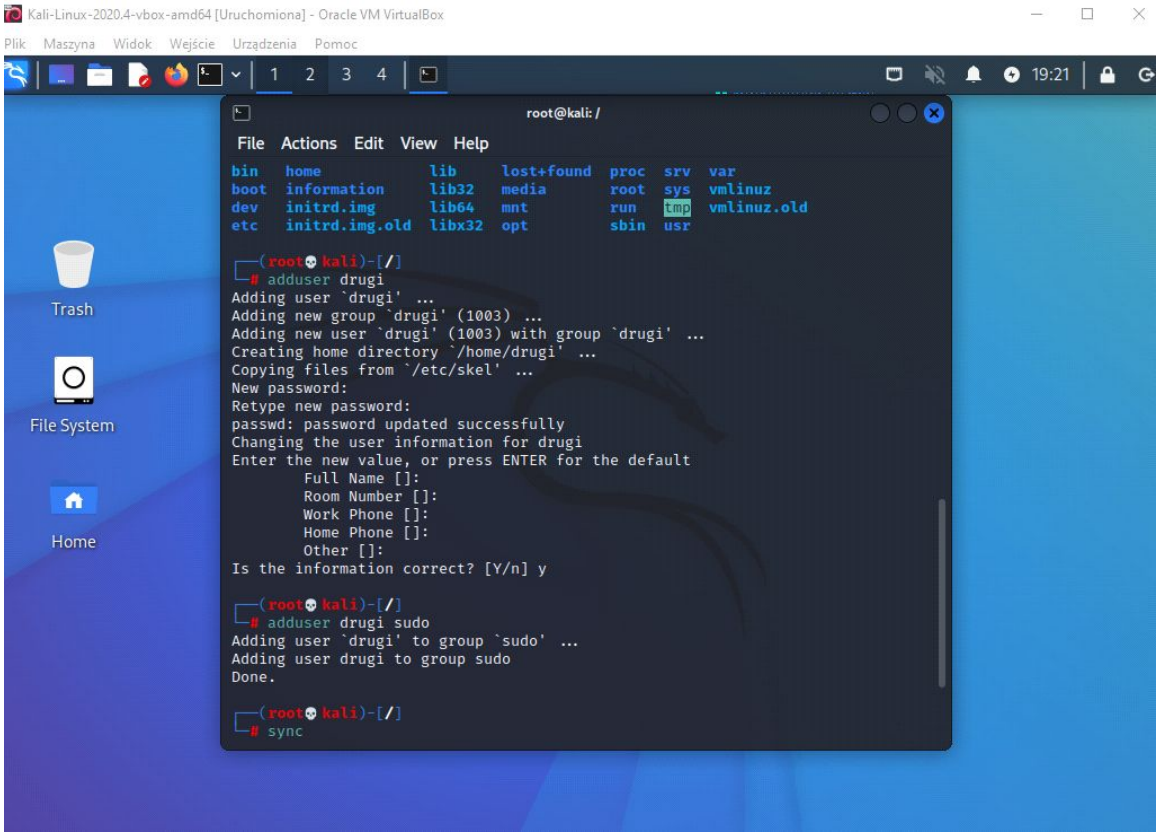
File System

Home

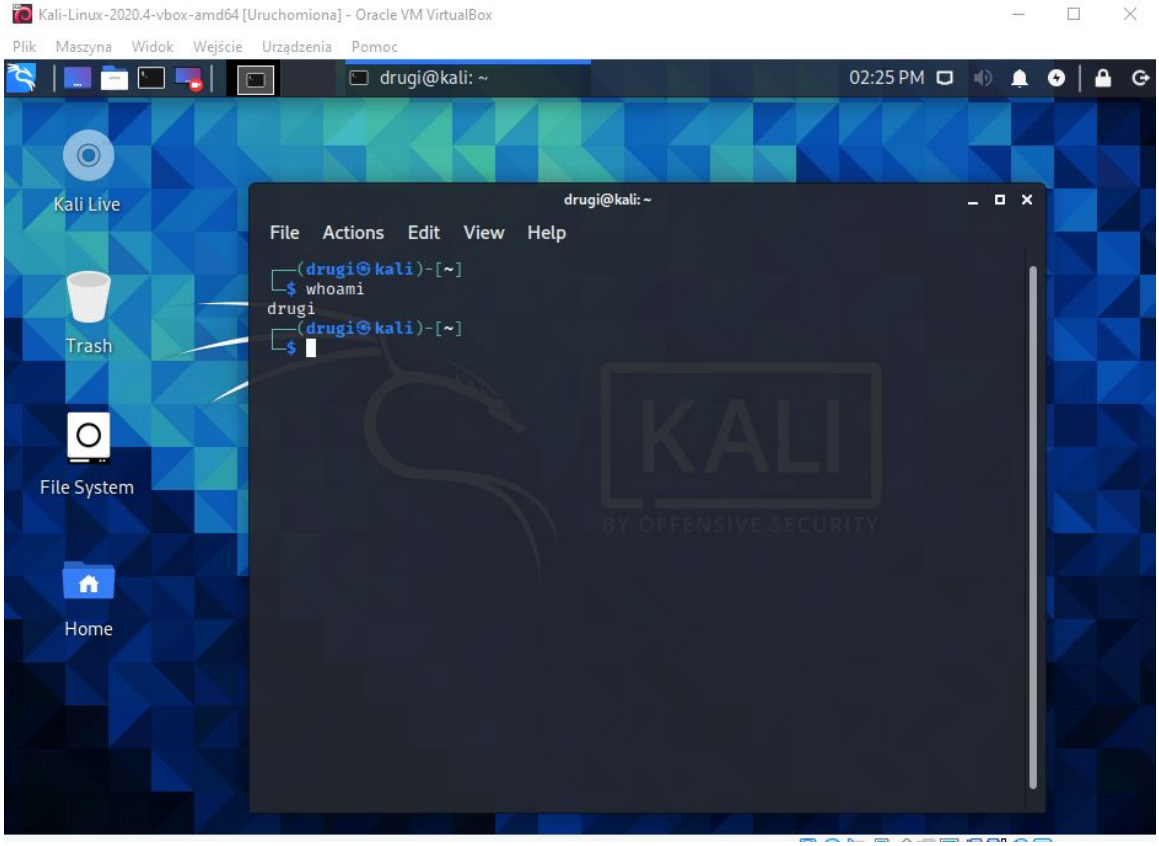
root@kali: /

File Actions Edit View Help

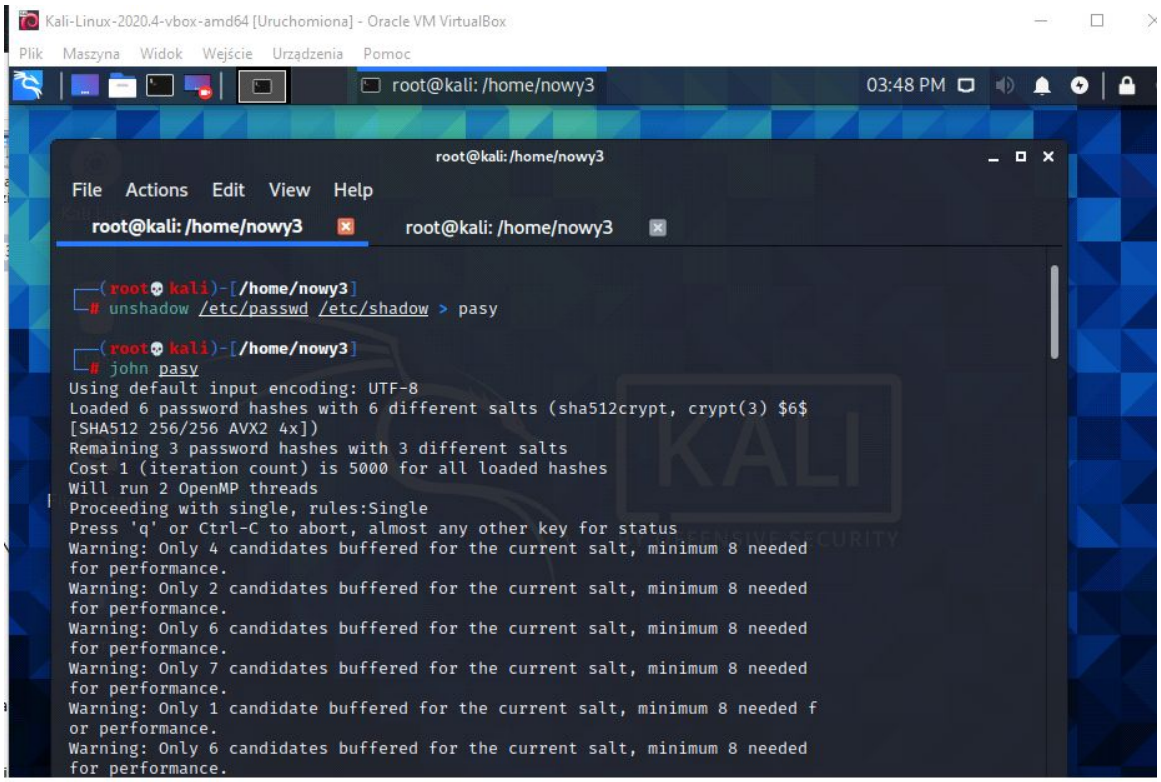
```
└─# mount /dev/sda2 /nowy
mount: /nowy: wrong fs type, bad option, bad superblock on /dev/sda2, missing
 codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.

┌──(root㉿kali)-[/home/kali]
└─# mount /dev/sda5 /nowy
mount: /nowy: unknown filesystem type 'swap'.
       dmesg(1) may have more information after failed mount system call.

┌──(root㉿kali)-[/home/kali]
└─# mount /dev/sda1 /nowy

┌──(root㉿kali)-[/home/kali]
└─# chroot /nowy
┌──(root💀kali)-[/]
└─# pwd
/

┌──(root💀kali)-[/]
└─# ls
bin   home            lib     lost+found  proc  srv  var
boot  information     lib32   media       root  sys  vmlinuz
dev   initrd.img      lib64   mnt         run   tmp  vmlinuz.old
etc   initrd.img.old  libx32  opt         sbin  usr

┌──(root💀kali)-[/]
└─# adduser drugi
Adding user `drugi' ...
Adding new group `drugi' (1003) ...
Adding new user `drugi' (1003) with group `drugi' ...
Creating home directory `/home/drugi' ...
```



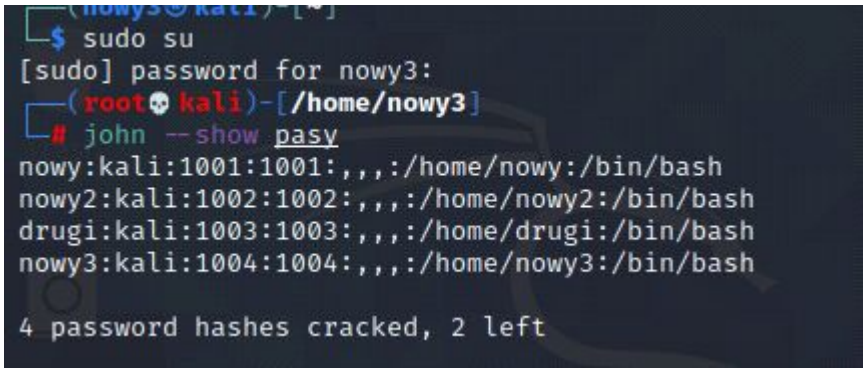
As we can see it's working ;)



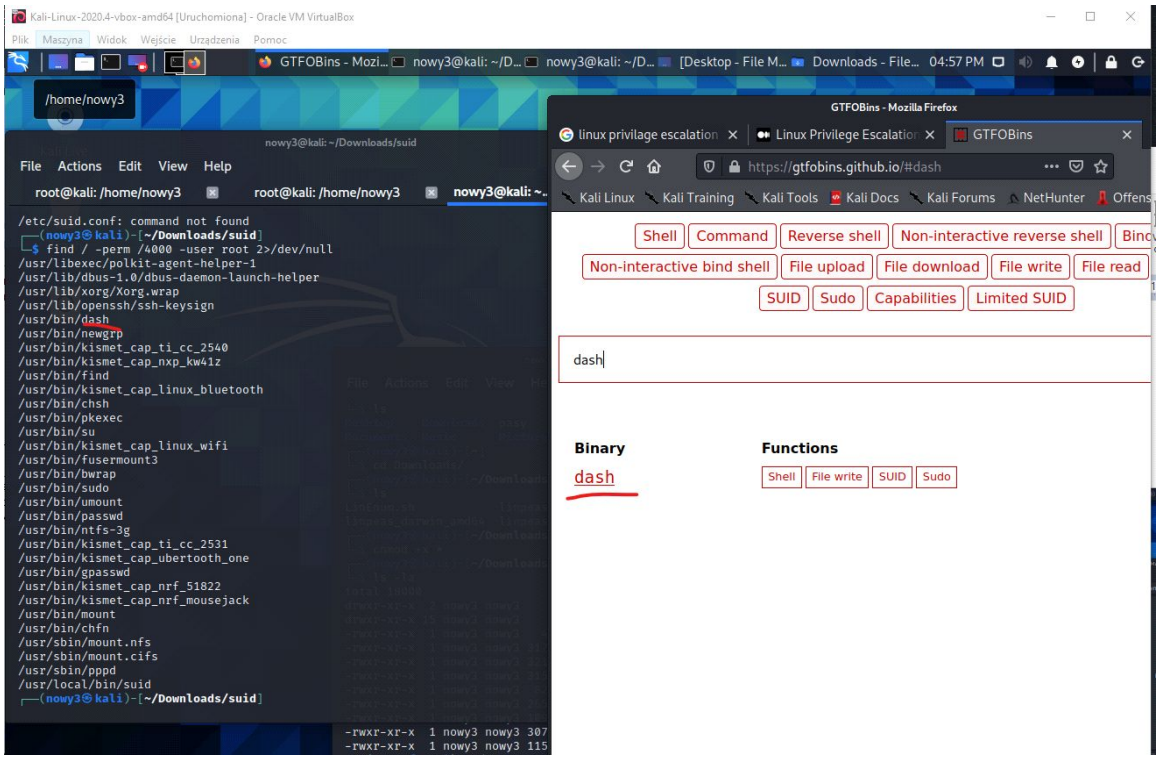
Trying to crack passwords:



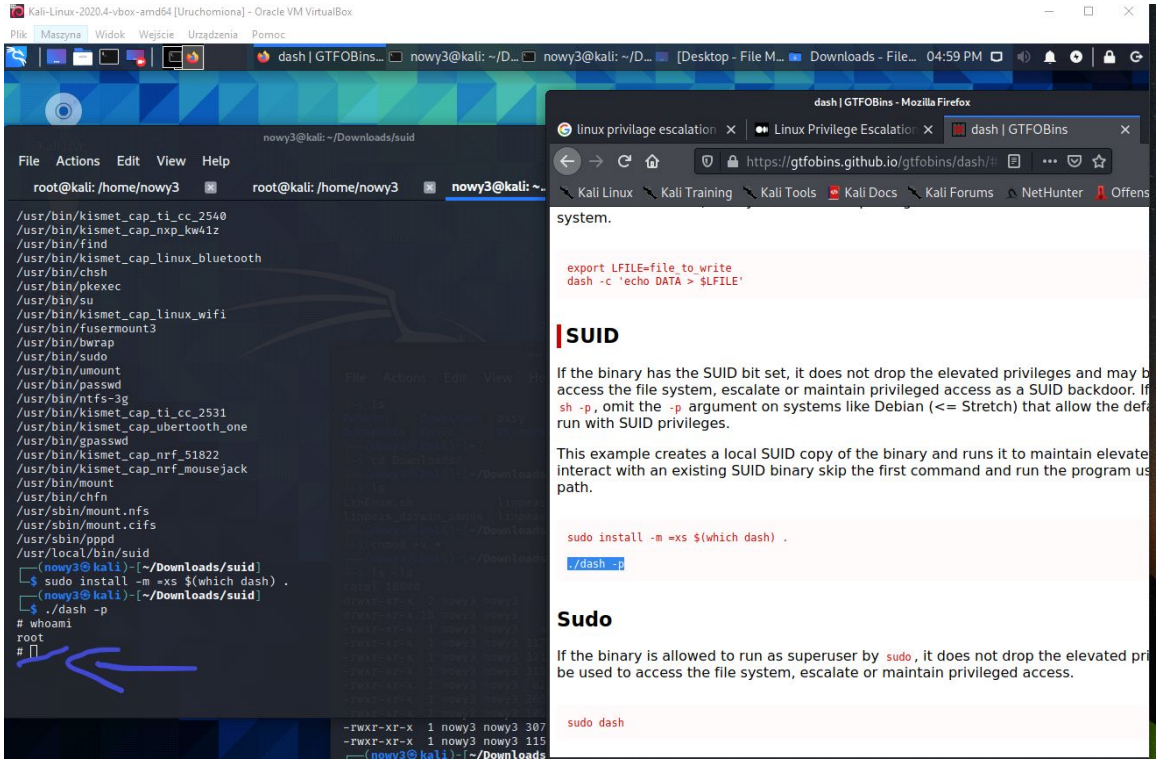
But seems that it cracked only passwords that I've created Silly me ;p



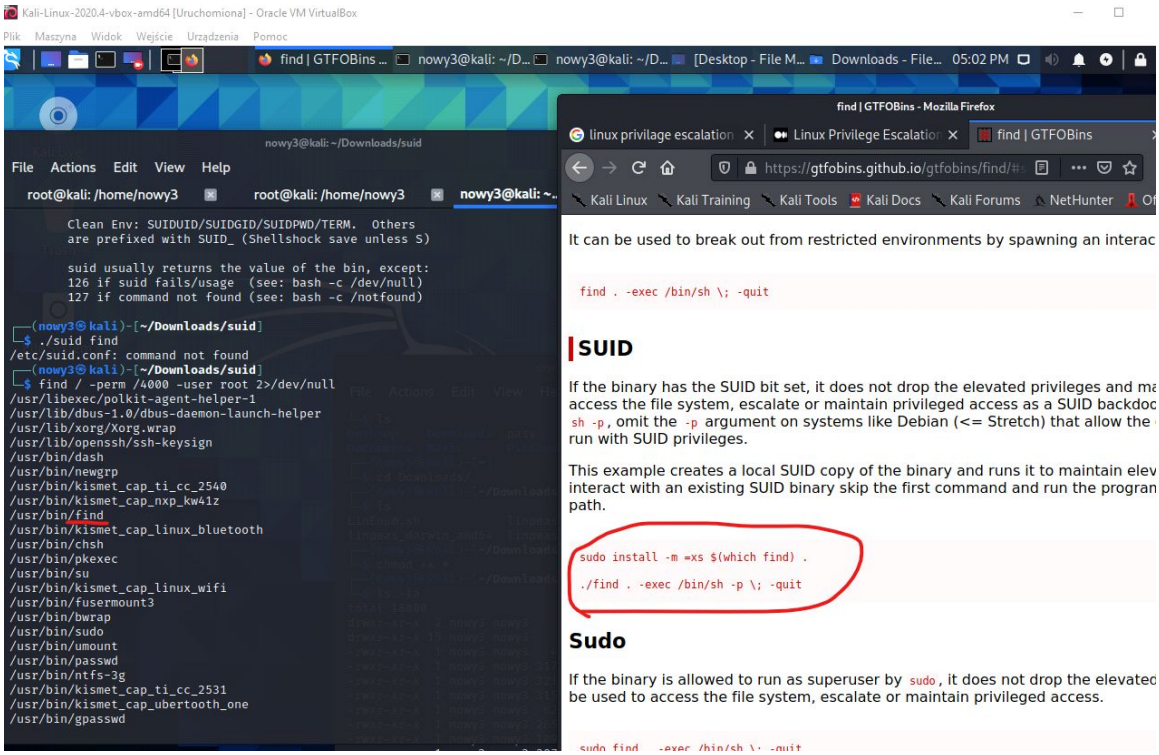
Let's use another tools like SUID



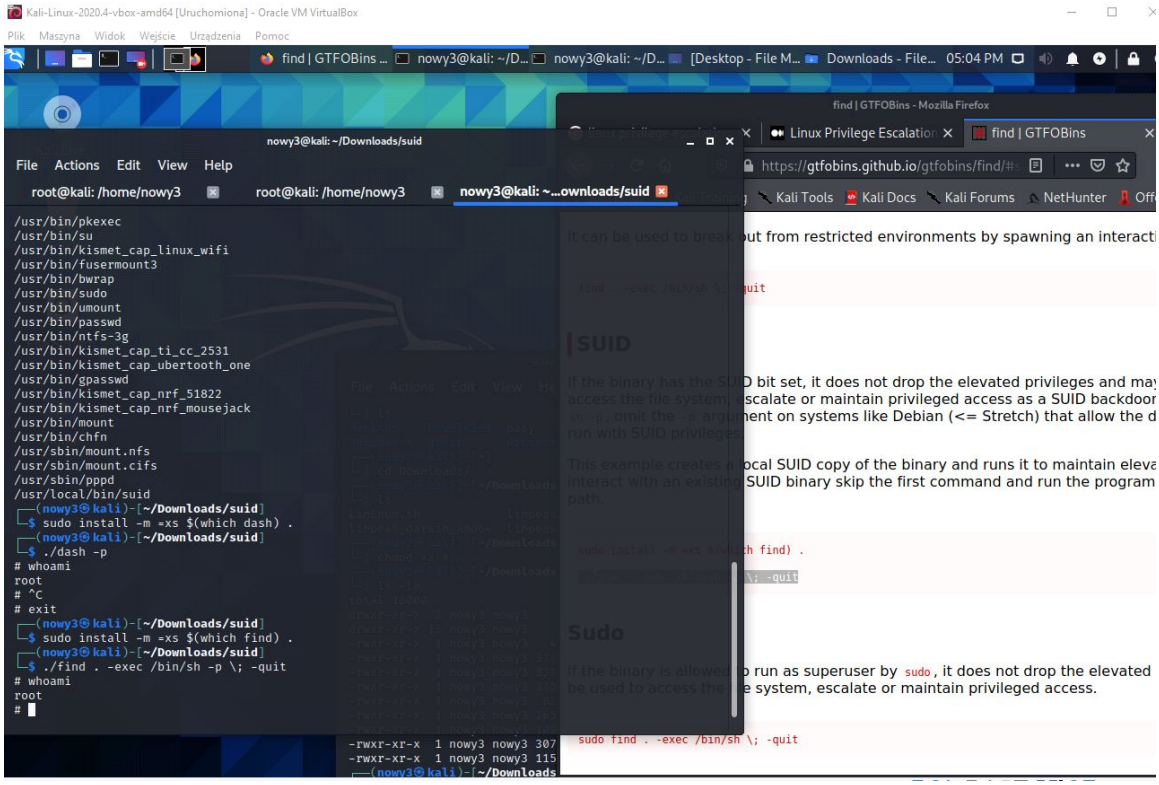
lets use it :)



And try with another one

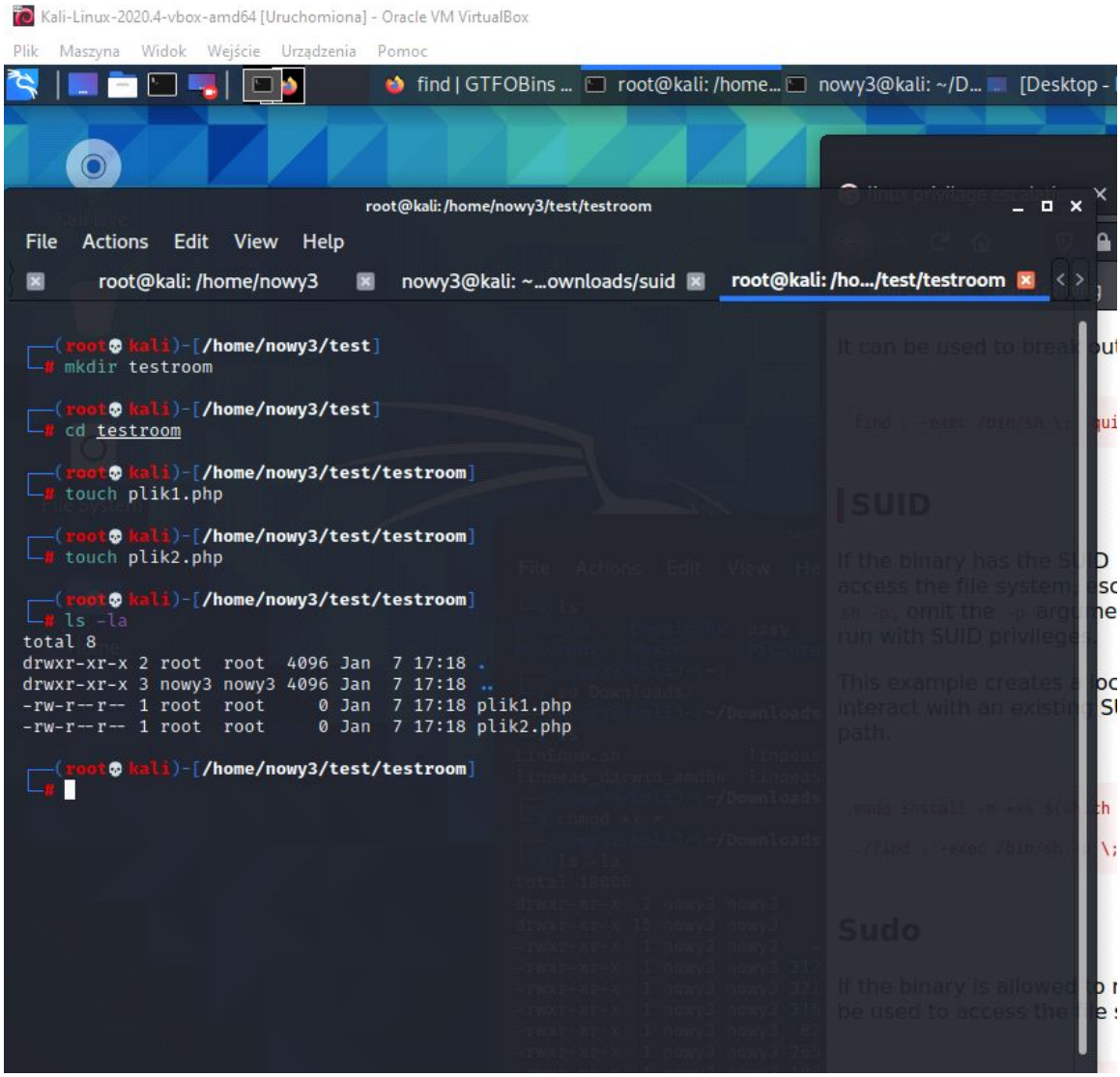


Working too

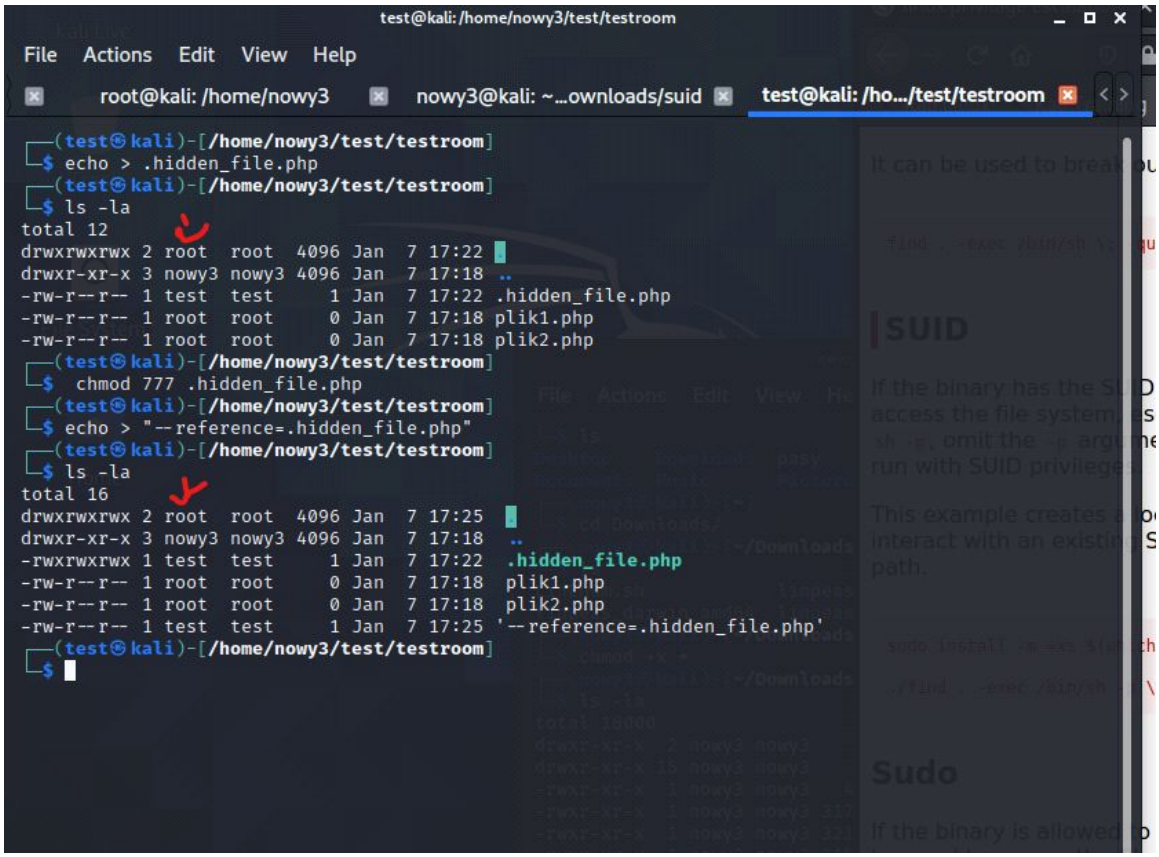


And the Secon way to escalate :

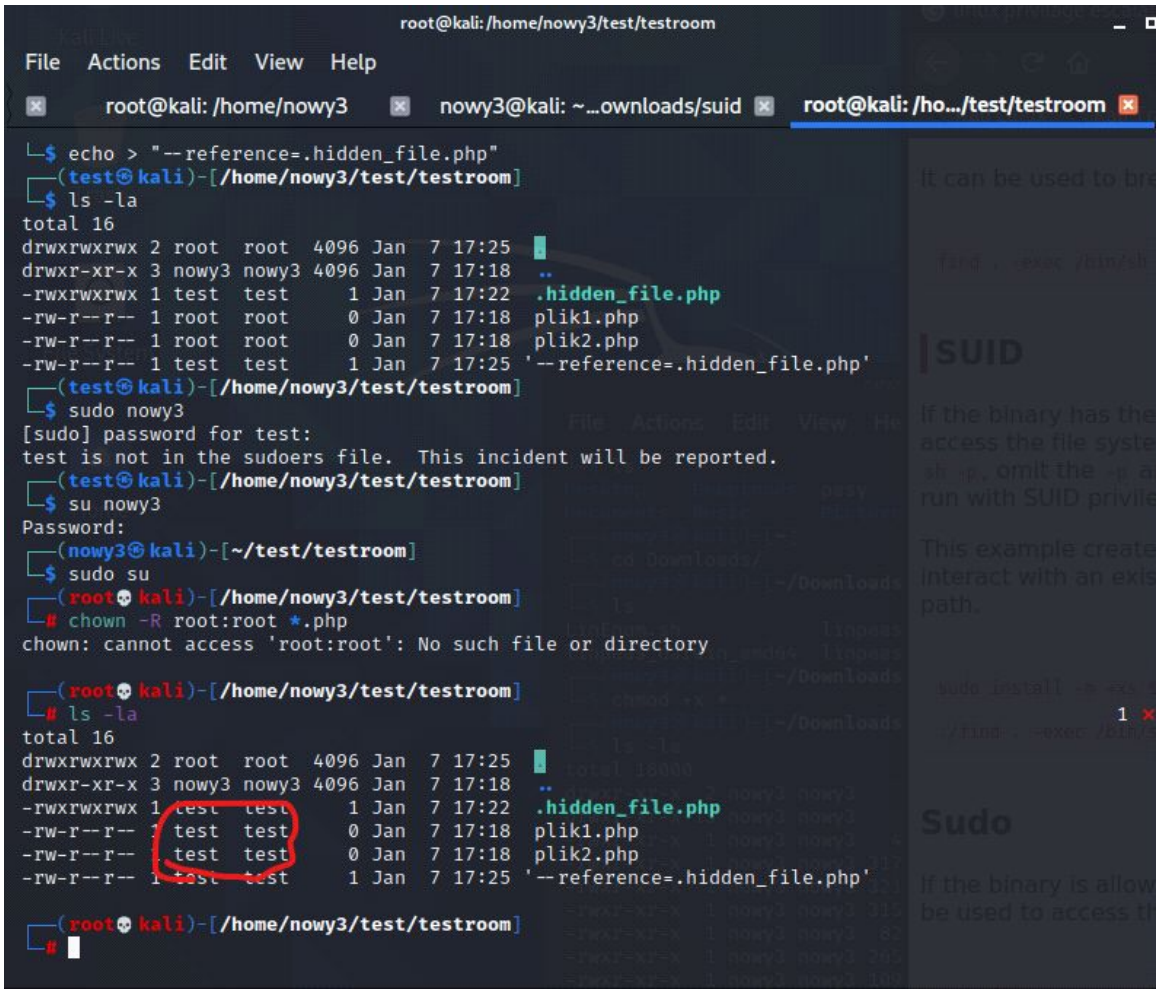
We creating 2 files as root:



and 2 files as a normal user



One magic command and all of root's files belongs to user ;)



Thank You very much, hope that You enjoyed my work.