

# Cybersecurity Tools with Python

## What does it do?

Implementation of three tools in Python using the Scapy library: Port scanner, Sniffer and DOS simulator. The tools run specifically in unix-based systems, all tests were done using virtual machines with VirtualBox NAT network environments.

## How to Use?

### Dependencies

- Scapy Library
  - Run:

```
$ python -m pip install scapy
```

- Tkinter Library
  - Run:

```
$ python -m pip install tk
```

### Tests Scenarios

- Virtualized Environment using VirtualBox
  - NAT Network
    - IP - 10.0.2.0/24
    - xubuntu\_1 - IP 10.0.2.5 / Interface enp0s9 (Attacker)
    - xubuntu\_2 - IP 10.0.2.4 / Interface enp0s9
    - xubuntu\_2 - Apache Server in the 80 port

The image shows two terminal windows from an Oracle VM VirtualBox. The left window, titled 'xubuntu\_1 [Ejecutando] - Oracle VM VirtualBox', shows the output of the 'ifconfig' command for the 'alexcsb@security-PC' user. It displays details for the 'enp0s9' interface (ethernet) and the 'lo' loopback interface. The right window, titled 'xubuntu\_2 [Ejecutando] - Oracle VM VirtualBox', shows the output of the 'netstat -antu' command for the same user, displaying active internet connections (servers and established) with columns for Protocol, Recv-Q, Send-Q, Local Address, Foreign Address, and State.

- Give execution permission to all directories
  - Within the **src** directory, run:

```
$ sudo chmod -R 777 ./dos
$ sudo chmod -R 777 ./port_scan
$ sudo chmod -R 777 ./sniffing
```

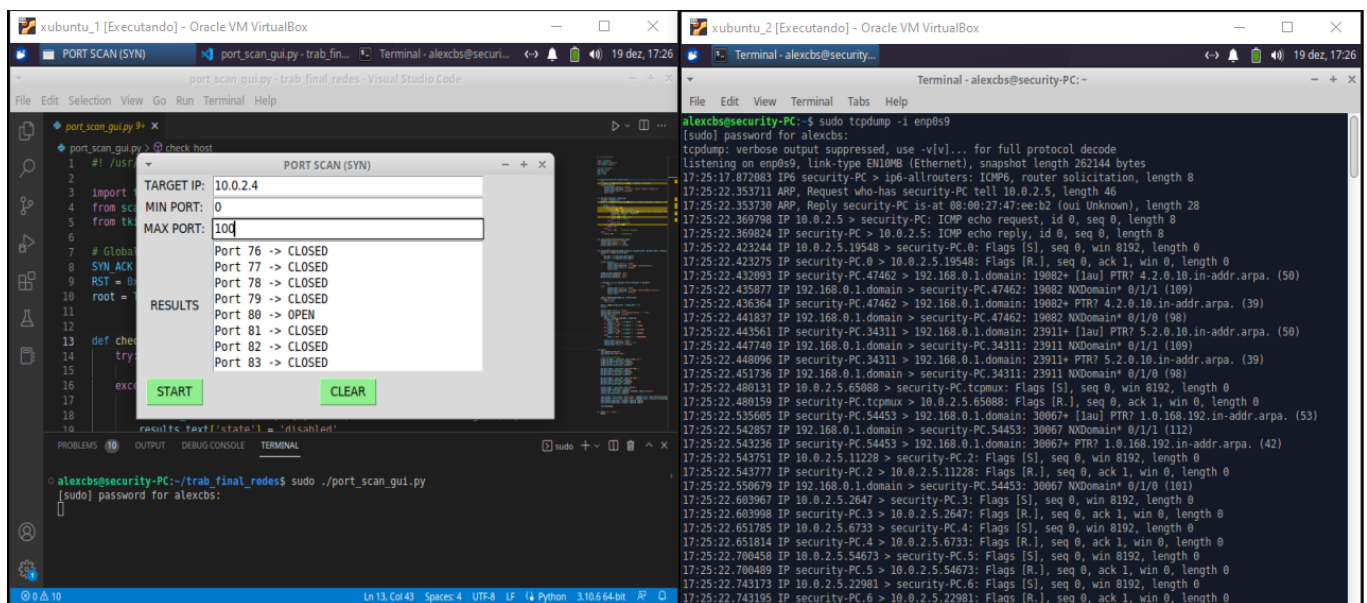
- DOS
  - Within the **src/dos** directory, run:

```
$ sudo ./dos.py
```

The image shows two terminal windows from an Oracle VM VirtualBox. The left window, titled 'xubuntu\_1 [Ejecutando] - Oracle VM VirtualBox', shows the execution of the 'dos.py' script in the 'src/dos' directory. The script prompts for a target IP address (10.0.2.4) and DOS intensity (1, 2, or 3), then successfully starts the DOS attack. The right window, titled 'xubuntu\_2 [Ejecutando] - Oracle VM VirtualBox', shows the output of the 'sudo tcpdump -i enp0s9' command, displaying a verbose output of network traffic captured on the 'enp0s9' interface, including HTTP requests and responses.

- Port Scanner
  - Within the **src/port\_scan** directory, run:

```
$ sudo ./port_scan.py
```



- Sniffing
  - Within the **src/sniffing** directory, run:

```
$ sudo ./sniffing.py
```

