



PUESTA EN PRODUCCIÓN SEGURA

Unidad 1. Actividad 3



2 DE NOVIEMBRE DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Ejercicio 1.	2
-------------------	---

Ejercicio 1.

Escriba y ejecute el comando anterior, compruebe que esta incluida la librería nmap de Python. Una vez instalada escriba el programa anterior de escaneos de puertos.

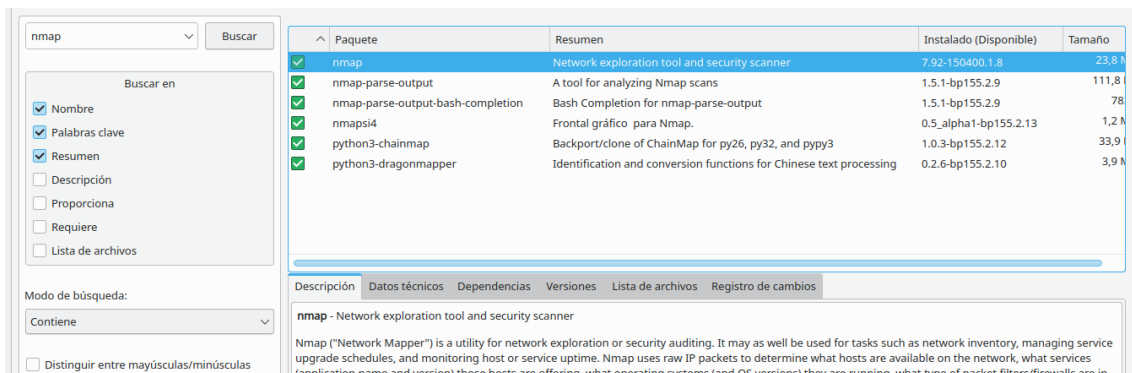
Instalamos la librería de nmap

```
pps@localhost:~> sudo pip3 install Python-nmap
Collecting Python-nmap
  Downloading python-nmap-0.7.1.tar.gz (44 kB)
    |████████████████████| 44 kB 1.0 MB/s
Installing collected packages: Python-nmap
  Running setup.py install for Python-nmap ... done
Successfully installed Python-nmap-0.7.1
pps@localhost:~>
```

Comprobamos que esta instalado:

```
pps@localhost:~> python3
Python 3.6.15 (default, Sep 23 2021, 15:41:43) [GCC] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import nmap
>>> nmap.__version__
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'nmap.__version__' is not defined
>>> nmap.__version__
'0.7.1'
>>>
```

Ahora lo instalamos tambien desde yast:



The screenshot shows the YaST package manager interface. On the left, there is a search bar with 'nmap' entered and a 'Buscar' button. Below it, search criteria are listed: 'Nombre' (checked), 'Palabras clave' (checked), 'Resumen' (checked), 'Descripción' (unchecked), 'Proporciona' (unchecked), 'Requiere' (unchecked), and 'Lista de archivos' (unchecked). The 'Modo de búsqueda' is set to 'Contiene'. At the bottom left, there is a checkbox for 'Distinguir entre mayúsculas/minúsculas' which is unchecked.

The main window displays a list of packages. The 'nmap' package is highlighted in blue. The table below shows the details of the installed packages:

Paquete	Resumen	Instalado (Disponible)	Tamaño
✓ nmap	Network exploration tool and security scanner	7.92-150400.1.8	23.8 MB
✓ nmap-parse-output	A tool for analyzing Nmap scans	1.5.1-bp155.2.9	111,8 KB
✓ nmap-parse-output-bash-completion	Bash Completion for nmap-parse-output	1.5.1-bp155.2.9	78 KB
✓ nmapsi4	Frontal gráfico para Nmap.	0.5_alpha1-bp155.2.13	1,2 MB
✓ python3-chainmap	Backport/clone of ChainMap for py26, py32, and pypy3	1.0.3-bp155.2.12	33,9 KB
✓ python3-dragonmapper	Identification and conversion functions for Chinese text processing	0.2.6-bp155.2.10	3,9 KB

Below the table, there are tabs for 'Descripción', 'Datos técnicos', 'Dependencias', 'Versiones', 'Lista de archivos', and 'Registro de cambios'. The 'Descripción' tab is selected, showing the following text:

nmap - Network exploration tool and security scanner

Nmap ("Network Mapper") is a utility for network exploration or security auditing. It may as well be used for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in

El código usado en el script es:

```
GNU nano 7.2 actividad5_1.py
import nmap

Port_ini = 70
Port_fin = 90
Ip_des = "192.168.22.100"
escaneo = nmap.PortScanner()

for j in range(Port_ini, Port_fin + 1):
    resultado = escaneo.scan(Ip_des, str(j))
    resultado = resultado['scan'][Ip_des]['tcp'][j]['state']
    print(f'El puerto número {j} se encuentra {resultado}')
```

Una vez ejecutado vemos que hace el escaneo de puertos y el 80 es el único abierto:

```
pps@localhost:~> python3 actividad5_1.py
El puerto número 70 se encuentra closed
El puerto número 71 se encuentra closed
El puerto número 72 se encuentra closed
El puerto número 73 se encuentra closed
El puerto número 74 se encuentra closed
El puerto número 75 se encuentra closed
El puerto número 76 se encuentra closed
El puerto número 77 se encuentra closed
El puerto número 78 se encuentra closed
El puerto número 79 se encuentra closed
El puerto número 80 se encuentra open
El puerto número 81 se encuentra closed
El puerto número 82 se encuentra closed
El puerto número 83 se encuentra closed
El puerto número 84 se encuentra closed
El puerto número 85 se encuentra closed
El puerto número 86 se encuentra closed
El puerto número 87 se encuentra closed
El puerto número 88 se encuentra closed
El puerto número 89 se encuentra closed
El puerto número 90 se encuentra closed
pps@localhost:~> █
```