AUDITORÍA DE SEGURIDAD INFORMÁTICA CON SOFTWARE LIBRE

NAJASH 0.2.1

Pedro Matías Cacivio
INSTEL & Seguridad

Motodo de Trabajo

OWASP

The Open Web Application Security Project

OSSTMM

Open Source Security Testing Methodology Manual

www.osstmm.org

ISSAF

InterSyS Software Administrativo Financiero

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Applications Places System | Terminal | root@dvd: ... | ettercap | Passwords | Terminal | Terminal | root@dvd: ~ | 10:34:06

- Kali Linux
  - Top 10 Security Tools
  - Information Gathering
    - DNS Analysis
    - IDS/IPS Identification
    - Live Host Identification
    - Network Scanners
    - OS Fingerprinting
    - OSINT Analysis
    - Route Analysis
    - Service Fingerprinting
    - SMB Analysis
    - SMTP Analysis
    - SNMP Analysis
    - SSL Analysis
    - Telephony Analysis
    - Traffic Analysis
    - VoIP Analysis
    - VPN Analysis
  - Vulnerability Analysis
  - Web Applications
  - Password Attacks
  - Wireless Attacks
  - Exploitation Tools
  - Sniffing/Spoofing
  - Maintaining Access
  - Reverse Engineering
  - Stress Testing
  - Hardware Hacking
  - Forensics
  - Reporting Tools
  - System Services
- Accessories
- Games
- Graphics
- Internet
- Office
- Programming
- Sound & Video
- System Tools

168 GB Volume

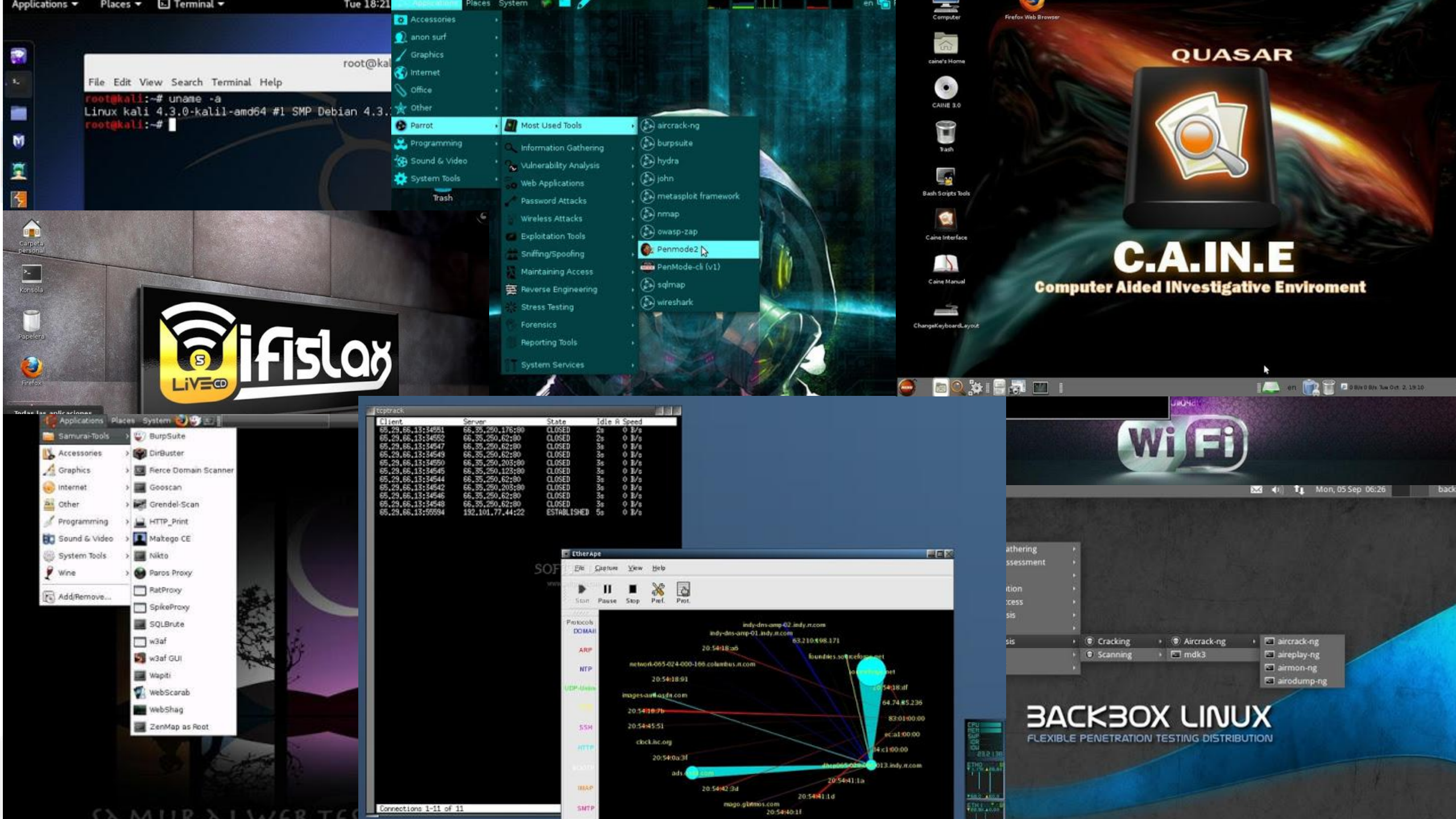
```
Terminal
File  Edit  View  Search  Terminal  Help

      (  (               )             (             )
      )\))(   '    (   ( /(            )\     (   ( /(
     ((_)()\ )   ))\  )\()) (   `  )  ((_) (  )\  )\())
     _(())\_)() /((_)((_)\  )\  /(/(     _   )\((_)(_))/
     \ \((_)/ /(_))  | |(_)((_)((_)_\ | | ((_)(_)| |_
      \ \/\/ / / -_) | '_ \(_-<| '_ \)| |/ _ \| ||  _|
       \_/\_/  \___| |_.__//__/| .__/ |_|\___/|_| \__|
                                |_|

              --=[WebSploit FrameWork
+---**---==[Version :2.0.3
+---**---==[Codename :CyberTron
+---**---==[Available Modules : 16
              --=[Update Date : [r2.0.3-116 9.10.2012]
```

```
root@dvd: ~/Desk
File  Edit  View  Search  Te
root@dvd:~/Desktop# var
        You will be
No update available
Script is installed

`YMM'   `MM'
  VMA    ,V
   VMA  ,V
    VMMP     ,M
     MM      AB
     MM     A'
   .JMML..AMA.
==================
=       Welcome to
=       Use this to
=       Feel free t
=       Official th
=       Check out t
=       You are run
==================
Message of the day

 [+] Cleaning iptab
[-] Cleaned.

 [+] Activating IP
```

```
File
%%   %   %%%%%%%%    %%%%%%%%%%%%
%%   %%  %%%%%%    %%%%%%%%%%%%%
%%   %%%%%%%%%%    %%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%   %%%   %%%%%%%%%%%%%%%%%%%%
%%%%     %%    %%%%%%%%%%%  %%%%%%%
%%%%  %%  %%  %       %%       %%    %
%%%%  %%  %%  %  %%% %%%%  %%%%  %%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%
%%%%%%%%%%%% %%%%     %%%%%    %%  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Save your shells from AV! Upgrade to
exe templates with Metasploit Pro --

       =[ metasploit v4.6.2-20130703
+ -- --=[ 1135 exploits - 715 auxili
+ -- --=[ 309 payloads - 30 encoders

msf >
```

```
Terminal  Help
ge: https://www.trustedsec.com        [---]

 Social-Engineer Toolkit (SET). The one
 of your social-engineering needs.

    Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

         Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

```
or credentials.

ts in the list)
nly... (press 'q' to exit)
```


Applications Places Terminal
root@kali
File Edit View Search Terminal Help
root@kali:~# uname -a
Linux kali 4.3.0-kali1-amd64 #1 SMP Debian 4.3.
root@kali:~#
Accessories
anon surf
Graphics
Internet
Office
Other
Parrot
Programming
Sound & Video
System Tools
Trash
Most Used Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
metasploit framework
nmap
owasp-zap
Penmode2
PenMode-cli (v1)
sqlmap
wireshark
Carpeta personal
Konsola
Papelera
Firefox
ifislax
LiVECD
QUASAR
C.A.IN.E
Computer Aided INvestigative Enviroment
Computer
Firefox Web Browser
caine's Home
CAINE 3.0
Trash
Bash Scripts Tools
Caine Interface
Caine Manual
ChangeKeyboardLayout
Applications Places System
Samurai-Tools
Accessories
Graphics
Internet
Other
Programming
Sound & Video
System Tools
Wine
Add/Remove...
BurpSuite
DirBuster
Fierce Domain Scanner
Gooscan
Grendel-Scan
HTTP_Print
Maltego CE
Nikto
Paros Proxy
RatProxy
SpikeProxy
SQLBrute
w3af
w3af GUI
Wapiti
WebScarab
WebSlag
ZenMap as Root
tcptrack
Client Server State Idle A Speed
Connections 1-11 of 11
EtherApe
File Capture View Help
Start Pause Stop Pref. Prot.
Protocols
DOMAIN
ARP
NTP
SSH
HTTP
IMAP
SMTP
WiFi
Mon, 05 Sep 06:26
Cracking
Scanning
Aircrack-ng
mdk3
aircrack-ng
aireplay-ng
airmon-ng
airodump-ng
BACKBOX LINUX
FLEXIBLE PENETRATION TESTING DISTRIBUTION

serpiente@debian: ~

```
*****************************************************
*            BIENVENIDO A NAJASH 0.2.1              *
*               INSTEL & SEGURIDAD                  *
*                 (=SERPIENTE=)                     *
*                                                   *
*****************************************************

0 - Interacción con nmap
1 - Técnicas de Ataques de Escaneo de Red
2 - Vulnerabilidades WEB de un sitio (demora tiempo)
3 - Keylogger
4 - Auditoria WIFI
5 - Registros de IP y Hosts  Víctimas
6 - Menú  de Información TCP/UDP y SOCKETS
7 - Herramientas de Seguridad Forense
8 - Recuperar Contraseñas en base a su hash usando HASHCAT
9 - EXIT
Ingresa tu Opcion:
```

```
-----------------------------------
-       VARIANTES MÁS USADAS EN NMAP    -
-            (=SERPIENTE=)              -
- ----------------------------------

INGRESA UNA OPCIÓN QUE QUIERAS REALIZAR

- 0- Salir del Menú Nmap

- 1- Determina los Servicios en Puertos TCP y Sistema Operativo

- 2- Chequea las Máquinas Vivas de una red Determinando su MAC e IP

- 3- Intenta Distintas Formas de Escaneo TCP SYN, ACK o UDP

- 4- Escaneo ICMP del tipo ECHO, Marca de Fecha, Máscara de red y Sistema Operativo

- 5- Escaneo Análisis TCP SYN/CONNECT() en Puertos TCP y UDP además de sus Versiones

- 6- Detección de Servicios por sondeo TCP Null, FIN, y Xmas

- 7- Realiza un Sondeo de Manera Agresiva en los Puertos que se Especifiquen

- 8- Realiza un Sondeo de listas o rangos de Host o IP que Determines en un Archivo

- 9- Sirve para Escanear Usando Maquinas ZOMBIES no Dejando Rastros

- 10- Sondeo para Expertos, Permite Especificar tus Parámetros flags TCP
Ingrese el Sondeo que Quiera Realizar:
```

```
*****************************************
*  BIENVENIDOS AL MENÚ DE HERRAMIENTAS   *
*            ESCANER DE RED              *
*          ANGRYIP y NBTSCAN             *
*****************************************

0 - Salir del Panel ScanRed
1 - Ejecutar AngryIP en Forma Gráfica
2 - Escanear un Equipo con NBTSCAN
3 - Escanea un Bloque /24
4 - Escanea un Rango por Ejemplo: 192.168.0.1-200
5 - Escanea Lista de IP Generada Previamente por Ejemplo: /t00ls/list
 Ingresa tu Opción:
```

```
*****************************************
*      TEST DE VULNERABILIDADES WEB     *
*                                       *
*****************************************

0 - Salir del Panel Vulnerabilidades Web
1 - Auditoria WordPress
2 - Auditoria http y https NIKTO
3 - Auditoria XSS (Cross Site Scripter) NO ANDA
4 - Auditoria Sitio con MySQL por Ejemplo: http://sitio.com/page.php?id=6
5 - Archery - Vulnerability Assessment and Management Tool

 Ingresa tu Opción:
```

CHACO
Gobierno de todos

```
*****************************************
*                KEYLOGGER              *
*                                       *
*****************************************

0 - Salir del Panel KEYLOGGER
1 - Activando Keylogger
2 - Lectura de Log
3 - Suspender Keylogger
4 - Borrar los Logueos 'logkeys.log'

 Ingresa tu Opción:
```

```
*****************************************
*  TEST DE VULNERABILIDADES WIFI (WIFITE)  *
*                                       *
*****************************************

0 - Saliendo del Panel Vulnerabilidades Wifi
1 - Ejecutar WIFITE en Forma Convencional
2 - Auditoria WEP
3 - Auditoria WPA y WPA2
4 - Auditoria WPS

 Ingresa tu Opción:
```

ECOM · POLICÍA DEL CHACO División Cibercrimen · POLICÍA DEL CHACO · Ministerio de Seguridad y Justicia Chaco Gobierno de todos · Subsecretaría de Niñez, Adolescencia y Familia Chaco Gobierno de todos

```
*****************************************
*    REGISTROS SOBRE IP Y HOSTS VICTIMAS     *
*                                            *
*****************************************

0 - Salir del Panel Registros
1 - Usando el Comando 'whois'
2 - Interactuando con 'dig'
3 - Dominios en DNS
4 - Consultar si una IP Pública, Consultó a un DNS
5 - NSLOOKUP
6 - Reverse DNS


 Ingresa tu Opción:
```

```
*****************************************
*   MENU  DE INFORMACIÓN TCP/UDP y SOCKETS   *
*                                           *
*****************************************

0 - Saliendo del Panel Registros
1 - Mostrar Todos los Sockects en Escucha
2 - Mostrar Conexiones Específicas Establecidas
3 - Conexiones de Paquetes TCP IPv4
4 - Mostrar todas las conexiones, por un puerto Específico. Ejemplo: https o 443
5 - Mostrar el Número y el Tipo de Conexiones Activas
6 - Resumen del Estado de los SOCKETS
7 - Listar de Puertos en Escucha y PID de los Programas

 Ingresa tu Opción:
```

```
*********************************************
*          MENU DE SEGURIDAD FORENSE        *
*                                           *
*********************************************

0 - Saliendo del Panel Forense
1 - Obtener HASH MD5 SHA256 y SHA512 los Archivos Deben estar en la Carpeta /t00ls/Hash1
2 - Obtener Metadatos de Archivos, estos deben estar en t00ls/MetaData
3 - Borrar Metadatos de Archivos, estos deben estar en t00ls/MetaDataBorrar
4 - Clonar una Imagen Binaria Desde una Fuente a un Destino Calculando su Hash SHA512
5 - Análisis de Redes Wifi con KISMET
6 - Captura TCP en la Conexión Activa
7 - Captura TCP en un Puerto y Dispositivo de Red


 Ingresa tu Opción:
```

```
*****************************************
*   MENU  DE INFORMACIÓN TCP/UDP y SOCKETS   *
*                                           *
*****************************************

0 - Saliendo del Panel Registros
1 - Mostrar Todos los Sockects en Escucha
2 - Mostrar Conexiones Específicas Establecidas
3 - Conexiones de Paquetes TCP IPv4
4 - Mostrar todas las conexiones, por un puerto Específico. Ejemplo: https o 443
5 - Mostrar el Número y el Tipo de Conexiones Activas
6 - Resumen del Estado de los SOCKETS
7 - Listar de Puertos en Escucha y PID de los Programas

 Ingresa tu Opción:
```