

PYTHON DOCUMENTATION: PORT SCANNER

Server for scanning IP address

Command `sudo python3 scanner.py`

```

M O U N T A I N C Y B E R S E C   P R O J E C T S
BASIC IP PORT SCANNER
made with python
-----
Target Scanning: 192.168.0.1
Time started: 2024-11-20 11:26:13.921882
-----
Port 5000 is open
Port 7000 is open
Port 51277 is open
Port 53271 is open
Port 57621 is open

PORT SCANNER % sudo lsof -i :portNumber

PORT SCANNER % sudo lsof -i :7000
COMMAND PID      USER    FD  TYPE   DEVICE  SIZE/OFF  NODE NAME
ControlCe 683      8u     IPv4  0xcb13d6a40bc4834a  0t0  TCP *:afs3-fileserver (LISTEN)
ControlCe 683      9u     IPv6  0xbd0e4f3aa8a26b2e  0t0  TCP *:afs3-fileserver (LISTEN)

PORT SCANNER % sudo lsof -i :57621
Password:
COMMAND PID      USER    FD  TYPE   DEVICE  SIZE/OFF  NODE NAME
Spotify 1129      75u     IPv4  0xd97b23418b8056b3  0t0  TCP *:57621 (LISTEN)
Spotify 1129      35u     IPv4  0xd8af5d18bb5ca940  0t0  UDP *:57621

PORT SCANNER % sudo lsof -i :53271
COMMAND PID      USER    FD  TYPE   DEVICE  SIZE/OFF  NODE NAME
Spotify 1129      i1u     IPv4  0x6a6a42aec1bade70  0t0  TCP *:53271 (LISTEN)

PORT SCANNER % sudo lsof -i :51277
COMMAND PID      USER    FD  TYPE   DEVICE  SIZE/OFF  NODE NAME
rapporstd 652      8u     IPv4  0x679c0da5795dff4d  0t0  TCP *:51277 (LISTEN)
rapporstd 652      9u     IPv6  0xa89c2f07900e0233  0t0  TCP *:51277 (LISTEN)
rapporstd 652      0u     IPv6  0x222d897083c6372a  0t0  TCP *:51277 (LISTEN)
51277->[fe8::]:53074 (ESTABLISHED)

```

After running this port scan on my local network, I came across 5 open ports. After researching these ports on Google, I ran the command `sudo lsof -i :port#`

- Port 5000
 - Apple Airplay Receiver
 - Can be disabled at *system settings > General > Airplay & Handoff*
 - Using PID 683
- Port 7000
 - Used for UPnP for local network with Airplay
 - Using PID 683
- Port 51277
 - Rapportd which is part of Mac OS
 - Using PID 652
- Ports 53271 & 57621
 - Spotify app & background processes
 - Using PID 1129