HOWTO — kali_server & mcp_server (Quick Guide)

This short HOWTO shows how to install and run two files: - **kali_server.py** — Flask API exposing Kali tools. - **mcp_server.py** — MCP client connecting to that API.

1️⃣ Requirements

- Kali Linux or Linux host with: `nmap`, `gobuster`, `dirb`, `nikto`, `sqlmap`, `metasploit-framework`, `hydra`, `john`, `wpscan`, `enum4linux`.
- Python 3.8+, `pip`, and network access between both components.

2️⃣ Setup

```
python3 -m venv .venv
source .venv/bin/activate
pip install flask requests
```

Set environment variables:

```
export API_PORT=5000
export WPSCAN_API_TOKEN="your_token_here"
```

3️⃣ Run the API Server (kali_server.py)

```
python kali_server.py --port 5000 --debug
```

Check:

```
curl http://localhost:5000/health
```

4️⃣ Run the MCP Client (mcp_server.py)

```
python mcp_server.py --server http://<KALI_IP>:5000
```

It registers tools like nmap_scan, gobuster_scan, hydra_attack, etc.

5️⃣ Example Usage

```
curl -X POST -H 'Content-Type: application/json'
  -d '{"command":"whoami"}'
  http://localhost:5000/api/command
```

6️⃣ Security

- Never expose server publicly.
- Add token-based auth and HTTPS.
- Run as non-root user or inside a container.

7️⃣ Common Issues

- **ImportError mcp.server.fastmcp** → install or fix path.
- **Missing tools in /health** → install them.
- **wpscan error** → add token or install tool.

Use responsibly — only on authorized systems.