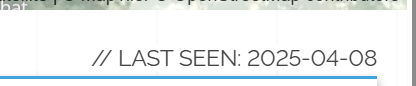
**1. Reconnaissance**

**📘 Passive Reconnaissance (Shodan.io**

* **Target IP**: 124.41.196.171
* **Tool Used**: [Shodan.io](https://www.shodan.io)
* **Objective**: Understand how public-facing IPs expose services.
* **Findings**:

**General Information**

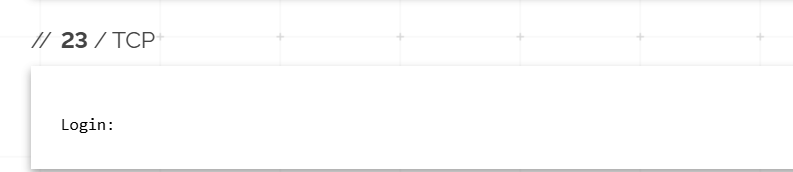
* **Location**: Kathmandu, Nepal​
* **ISP**: WorldLink Communications Pvt Ltd​
* **ASN**: AS17501​
* **Last Seen**: April 8, 2025​



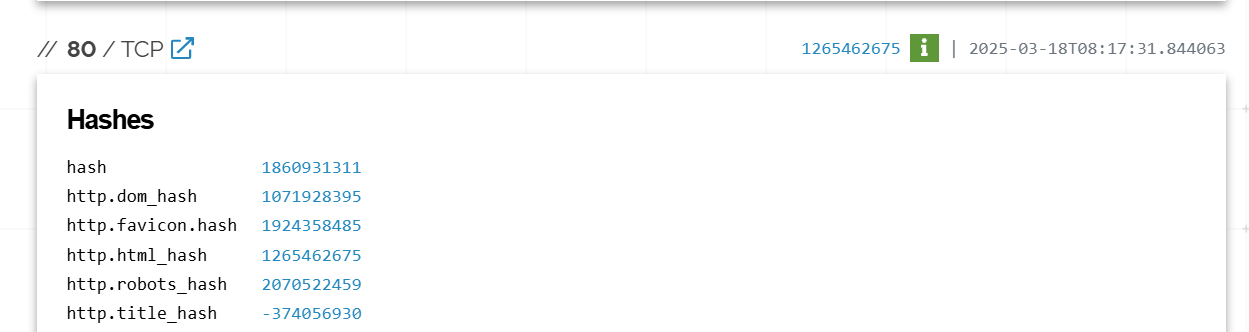
**🔓 Open Ports and Services**

The device has several open ports, indicating accessible services:​

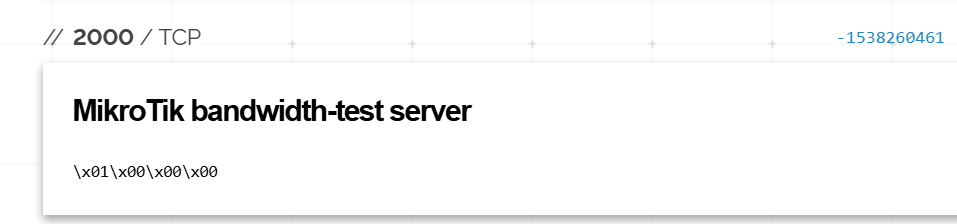
* **Port 23 (Telnet)**: This port is open, which could allow remote login access.​



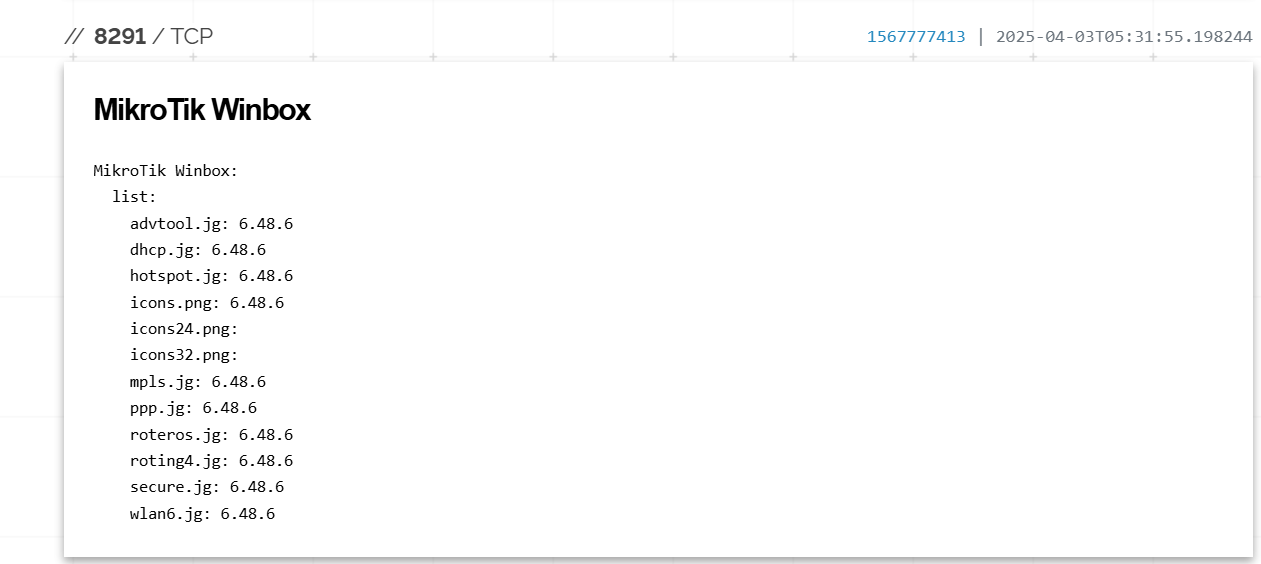
* **Port 80 (HTTP)**: Hosts a web interface identified as a MikroTik RouterOS configuration page.​



* **Port 2000**: Associated with the MikroTik bandwidth-test server.​



* **Port 8291**: Used by MikroTik's Winbox utility for router management.​



**🛠️ Device and Software Details**

* **Device Type**: MikroTik Router​
* **Operating System**: RouterOS version 6.48.6​
* **Web Interface Title**: RouterOS router configuration page

### 📶 2. Ping

* Checked if the host is alive



**⚠️ Security Considerations**

The presence of open ports, especially Telnet (port 23), can epose security risks if not properly secured. It's advisable to ensure that:​

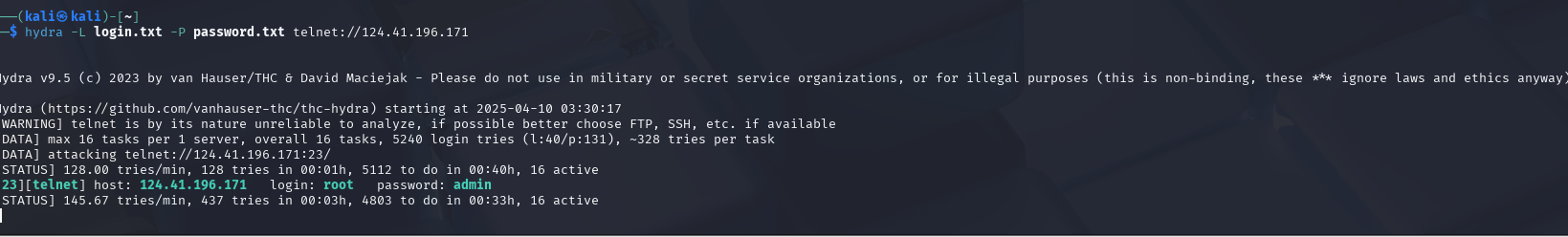
* Default credentials are changed.​
* Unnecessary services are disabled.​
* The router's firmware is up to date to patch known vulnerabilities.​

**💥 4. Exploitation Attempts (Shodan IP)**

**⚒️ Hydra (Educational Use Only)**

### Brute Force

hydra -l login.txt -P password.txt telnet://124.41.196.171

****

**Got login: root and password: admin**

**I try to login but it say incorrect login or password**

**✅ Conclusion**

I initially explored IP 124.41.196.171 using **Shodan** and performed **ping, and hydra** for learning purposes.