**IoT Device Exposure Analysis using Shodan**

**Introduction**

This project aims to identify and analyze vulnerable Internet of Things (IoT) devices that are exposed to the public internet using the Shodan search engine. IoT devices such as webcams, routers, and smart home systems are often connected with weak configurations or outdated firmware, making them susceptible to cyberattacks. By performing this analysis, we gain insights into common exposures, open ports, and service banners, and provide recommendations to improve IoT security.

**Tools Used**

1. **Shodan.io** – A search engine for internet-connected devices.
2. **Web Browser** – For running Shodan queries and viewing results.
3. **Document Editor (MS Word/Google Docs)** – For preparing this project report.
4. **Optional Tools:** Excel/Power BI for visualizing data trends.

**Shodan Queries and Analysis**

**🔹 Device 1: Exposed Webcam and KNX Smart Device**

1.Shodan query- port:554

2.Findings-

* **IP Address & Hostname:** 124.123.42.176 (actcorp.in)
* **Location:** Hyderabad, India
* **Organization:** ACT HYD
* **ISP:** Atria Convergence Technologies Ltd.
* **ASN:** AS55577
* **Open Ports Found:**
  + **554/TCP:** Responded with RTSP/1.0 401 Unauthorized, indicating a Real-Time Streaming Protocol service is active.
  + **3671/UDP:** Detected a KNX Gateway device with detailed KNXnet/IP services, MAC address, and supported protocols.
  + **9090/TCP:** Web service running GoAhead HTTP server, showing an HTTP 200 OK response for an IP-COM login page.
* **Device Details (from KNX gateway):**
  + Friendly Name: SpaceLogic KNX IP Interface
  + MAC Address: 00:24:60:02:1D:6B
  + Supported KNX services: Core, Device Management, Tunneling, Object Server, Remote Configuration.

3.Analysis-

 **Port 554** confirms a video streaming service is active, likely a webcam or CCTV system using RTSP.

 **Port 3671** reveals a KNX home/building automation device is exposed, which could allow attackers to manipulate smart home systems if unsecured.

 **Port 9090** shows a web login interface (IP-COM), possibly for a network device, which could be vulnerable if default credentials are used.

 The combination of these ports suggests the device owner may not realize their smart building systems and cameras are publicly exposed online, creating significant security risks.

4.Mitigation

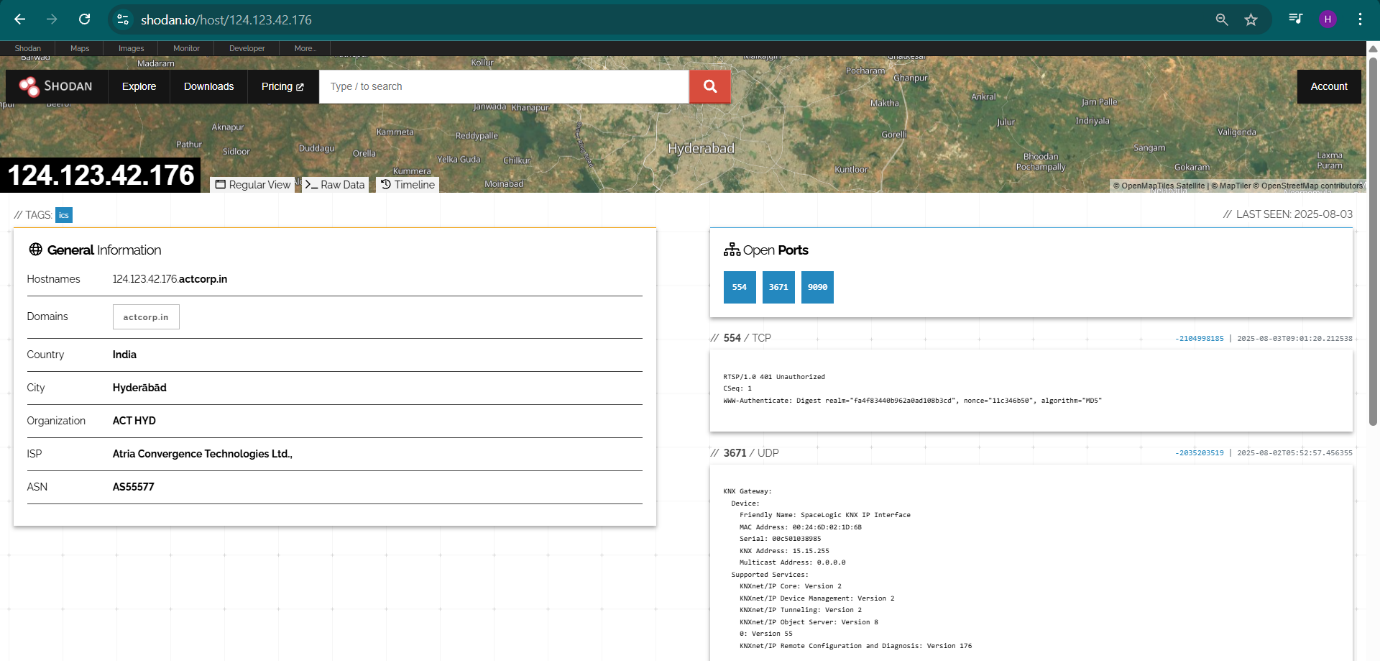
 Immediately restrict internet exposure by placing devices behind a firewall or NAT.

 Disable unnecessary port forwarding for ports 554, 3671, and 9090.

 Enforce strong, unique passwords on all device interfaces (webcams, KNX gateways, routers).

 Regularly update firmware to patch known vulnerabilities.

 Limit device management interfaces to trusted IP ranges using access control lists (ACLs).





**🔹 Device 2: Exposed Web Server**

1.Shodan query- port:80

2.Findings-

**IP Address:** 118.233.128.136

**Hostname:** 118-233-128-136.dynamic.kbronnet.com.tw

**Country:** Taiwan

**City:** Pingtung

**Organization/ISP:** kbro CO. Ltd.

**ASN:** AS38841

**Open Port:** 80 (HTTP)

**Web Technologies Detected:** RequireJS (JavaScript framework)

**Service Banner on Port 80:** HTTP/1.1 200 OK with empty title, standard HTTP security headers (X- Frame-Options: SAMEORIGIN, X-XSS-Protection: 1; mode=block).

3.Analysis-

The device exposes an HTTP service on port 80 to the public internet, which could be:

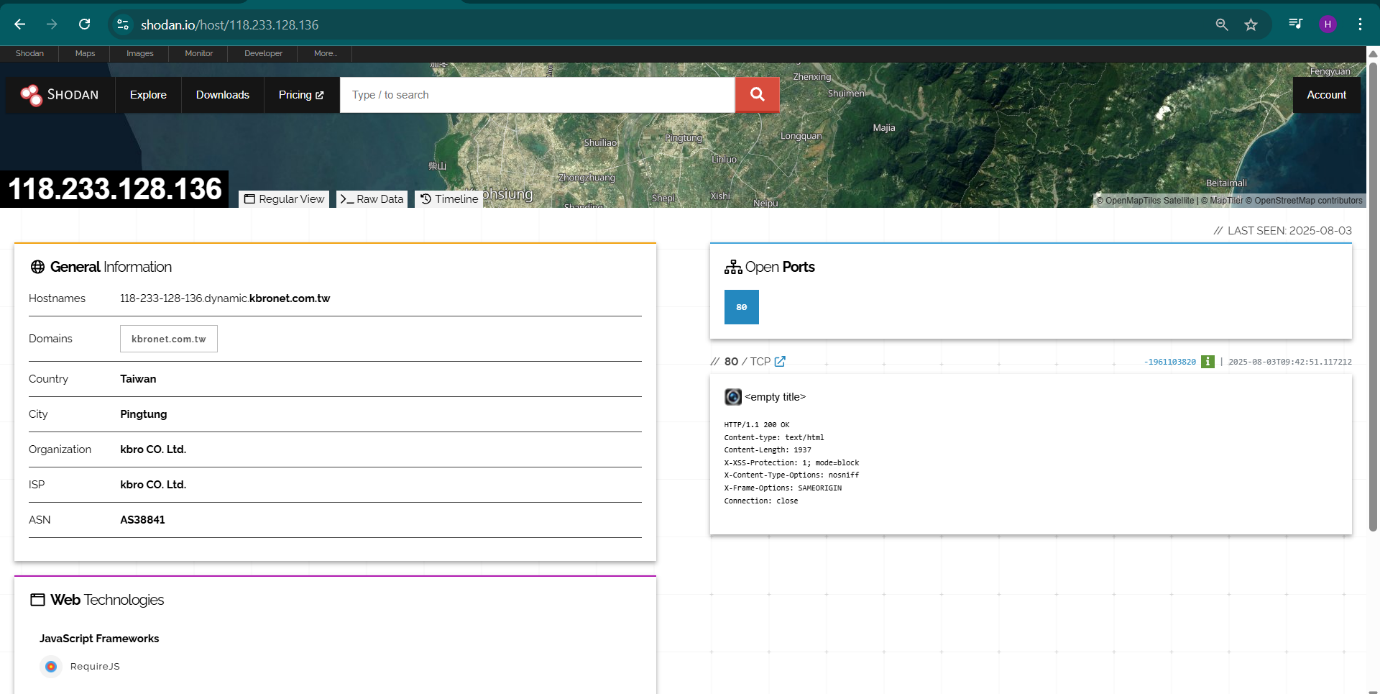
* A web management interface for a router, modem, or other network device.
* An entry point potentially vulnerable to web-based attacks (e.g., brute-force login, outdated firmware exploits).
* The lack of a meaningful page title suggests it could be a misconfigured or abandoned web interface.

Exposing such interfaces to the internet without proper authentication or updates can let attackers:

* Bypass weak/default passwords.
* Exploit known vulnerabilities in the device’s firmware.
* Use the device as a foothold into the internal network.

4.Mitigation

* Restrict HTTP access on port 80 using firewall rules or by allowing only trusted IP ranges (e.g., administrator’s home/office).
* Replace HTTP with HTTPS if remote access is necessary.
* Disable remote web access entirely if not required.
* Update device firmware to patch any known vulnerabilities.
* Enforce strong, unique passwords for the device.



**Conclusion**

This project highlights how Shodan can be used to discover vulnerable IoT devices and understand the risks associated with exposing such devices to the public internet. The findings emphasize the importance of securing IoT devices through proper configurations, updates, and network protections.