CHRIST UNIVERSITY
BENGALURU, INDIA
Declared as Deemed to be University under Section 3 of UGC Act 1956

# CSHO331CSP24 – ETHICAL HACKING

# ASSIGNMENT 20: CHECK INTERNET EXPOSURE VIA SHODAN

**B. Tech - Computer Science and Engineering**
**(Artificial Intelligence and Machin**


**NAME: KURAGAYALA RACHEL**
**REGISTER NO: 2462106**
**CLASS: 3 BTCSAIML A**

**SCHOOL OF ENGINEERING AND TECHNOLOGY,**
**CHRIST (Deemed to be University),**
**Kumbalgodu, Bengaluru-560 074**


August 2025

# Assignment 20: Check Internet Exposure via Shodan

**Objective:**
The goal of this assignment is to simulate an attacker's perspective by using Shodan.io to analyse a public IP address, identify exposed services, and suggest measures to secure the system.

**Methodology:**
- Checked my own public IP on Shodan which returned **no results**.
- Used a different public IP (193.248.195.54) found using Shodan search filters (webcams).
- I gathered banner information, HTTP headers, and service data.
- Analysed the type of services exposed and assessed security risks.
- Documented results in this report, masking the real IP for privacy.

**Findings from Shodan:**

**General Information**
- IP Address: (masked: 193.248.xxx.54)
- City: Beauvais, France
- ISP / Org: Orange S.A.
- Hostname: 193-248-195-xx.ftth.fr.orangecustomers.net
- Domain: orangecustomers.net
- ASN: AS3215

**Service Details**

**Port 88 – Sunny Web Box**
- HTTP Response: 200 OK
- Server Header: Sunny Web Box
- Last Modified: Sat, 12 Jul 2025
- Security Issue: Uses plain HTTP (not encrypted), and may be running outdated firmware.

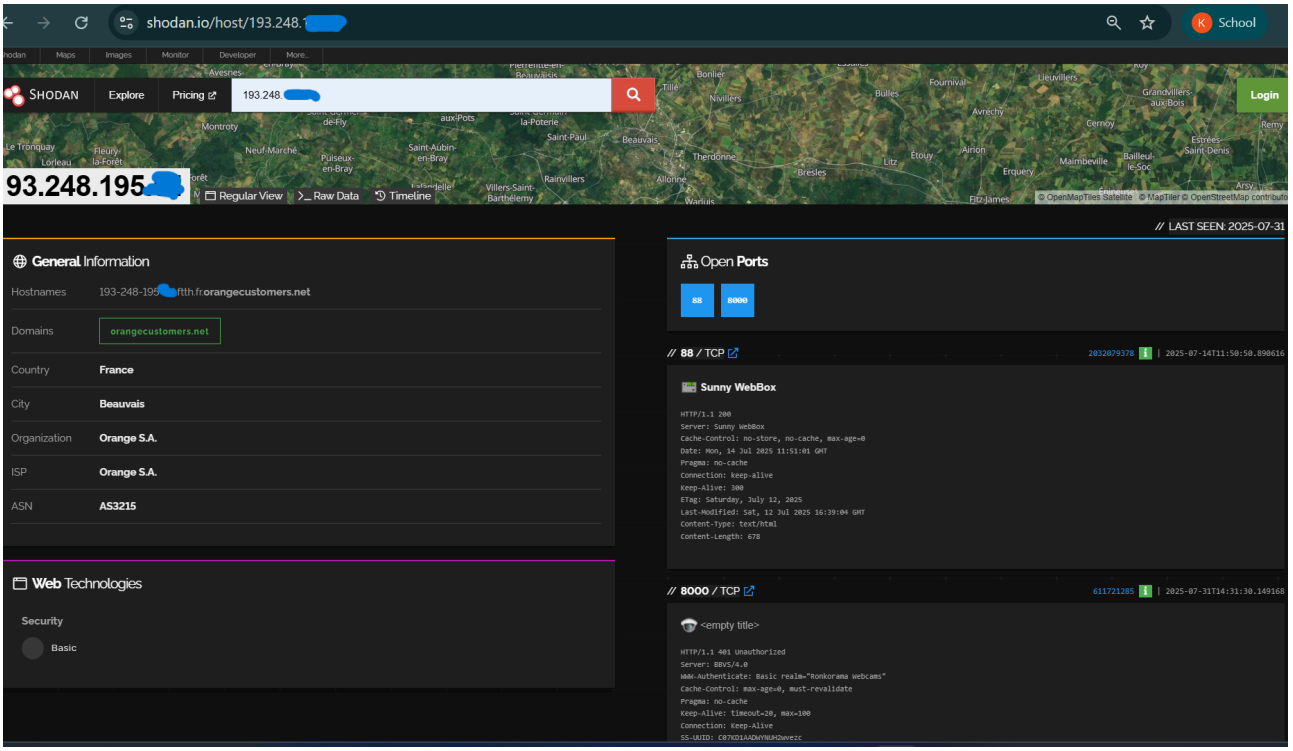
**Port 8000 – Webcam Service**
- HTTP Response: 401 Unauthorized
- Auth Required: Basic HTTP Authentication
- Realm: "Ronkorama Webcams"
- Server Header: BBVS/4.0
- Security Issue: Uses HTTP without encryption, exposing credentials to interception.

**Security Analysis:**
- Unencrypted Traffic: Both services run over HTTP, not HTTPS making them vulnerable to data interception.

• Weak Authentication: Webcam uses Basic Auth that is risky if default credentials are used.
• Exposed IoT Devices: Systems like Sunny Web Box are known to have past vulnerabilities.
• Public Accessibility: Services are accessible globally (no IP filtering or access restrictions).

**Screenshot:**
(IP is masked.)

The screenshot displays the Shodan search result for the selected public IP address. It shows banner information for open ports (88 and 8000), including service names, server headers, and response codes. This visual evidence supports the findings by confirming the existence of exposed services such as the Sunny Web Box and a webcam feed.




**Code / Tools Used:**
• Shodan Web Interface: https://shodan.io
• Screenshot Tool: Snipping Tool (Windows)
• No custom code or scripts were used for this assignment.

**Conclusion:**

This assignment shows how attackers can use Shodan to find exposed devices like webcams and solar inverters online. The analysed system lacked encryption and proper access control, highlighting the need for HTTPS, stronger authentication, and regular updates.