**Cyber Security – Assessment # 2**

**Part 1: Conceptual**

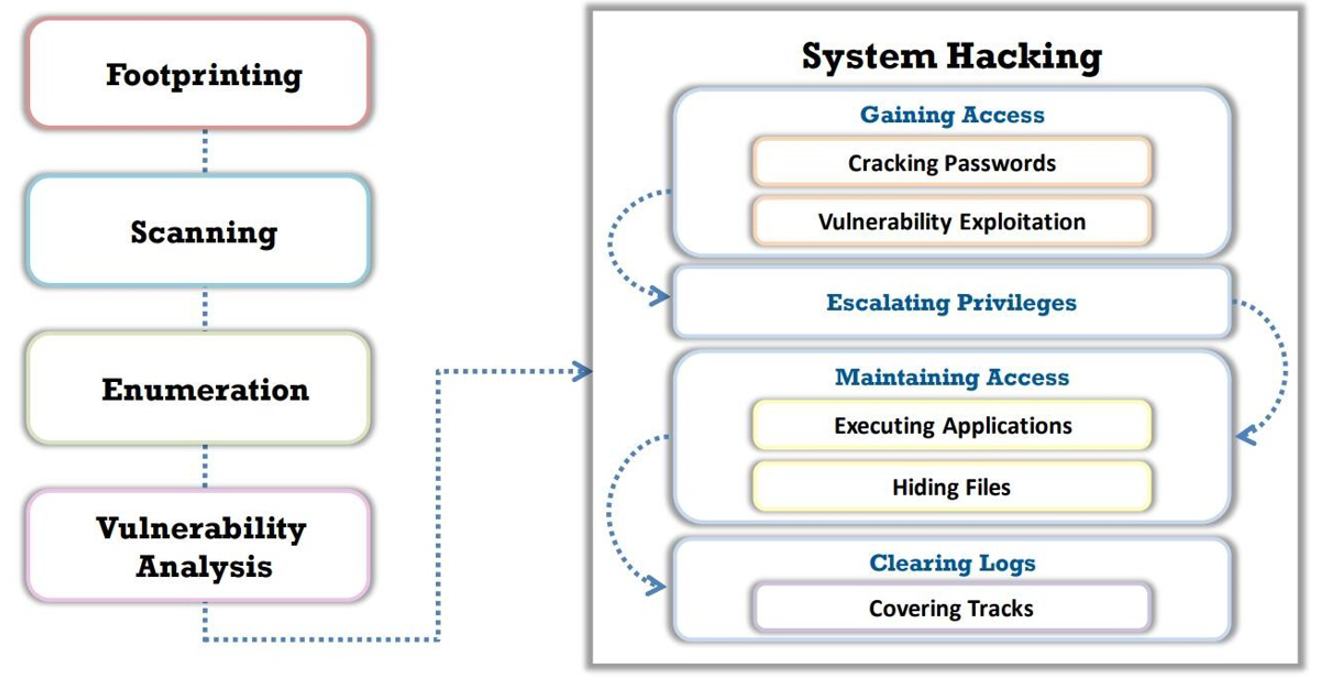
**Q1**.- Define following terminologies: -

a. Confidentiality

b. Integrity

c. Authentication

**Q2.** Briefly explain following CEH methodology flow diagram: -



**Part 2: Lab**

**Q3.** Open-Source Intelligence (OSINT) refers to the process of collecting, analyzing, and utilizing publicly available information to generate actionable intelligence. This data can come from a wide range of sources, such as websites, social media platforms, news articles, public records, forums, and even multimedia content. OSINT is widely used in cybersecurity, law enforcement, journalism, and business intelligence to uncover hidden insights without accessing classified or private data. By leveraging tools and techniques to gather and verify information, OSINT helps organizations and individuals make informed decisions, identify threats, and track trends—often at low cost and with minimal risk. Using OSINT, gather information about "**Tesla**”: -

* Company Name
* Key Services / Products
* Scope of Services
* Website
  + Fully Qualified Domain Name (FQDN)
  + Hosting Country / Company
  + Age
  + IP Address
  + Geo Location of Web Server (longitude/latitude)
  + Technologies
  + Load Balancer / Web Application Firewall (WAF), if any
* Data center Devices:-
  + Datacom (routers, switches)
  + Next Generation Firewall (NGFW) vendor
  + Network Time Protocol (NTP) Server
  + Apache Server
  + Web Application Firewall (WAF),if any
  + Load Balancer, if any
* Content Delivery Network (if any)
* Sub-domains [ identify 2 x tools other than Subdomain finder & Asset finder]

**Q4.** Using Shodan, search for following IOT devices: -

* Webcams:
  + Yawcams
  + WebcamXP
  + Android IP Webcam Server
  + Security DVRs
* Printers & Copiers
  + HP Printers
  + Xeros Copiers / Printers
  + Epson Printers
  + Canon Printers
* Home Devices
  + Yamaha Stereos
  + Apple AirPlay Receivers
  + Chromecasts / Smart TVs
  + OctoPrint 3D Printer Controllers
* FTP Servers with Anonymous Login

**Part 1: Conceptual**

1. **Answers:**

Confidentiality: Ensuring that data is accessible only to authorized individuals and protected from unauthorized access.

Integrity: Maintaining the accuracy and reliability of data by preventing unauthorized modifications or corruption.

Authentication: The process of verifying the identity of users, devices, or systems before granting access.

1. **Answers:**

This diagram represents the System Hacking Process in ethical hacking. It consists of four initial phases before hacking into a system:

1. Foot printing (Reconnaissance) – Gathering publicly available information about the target.
2. Scanning – Identifying vulnerabilities and open ports in the system.
3. Enumeration – Extracting system details like usernames, network shares, and running services.
4. Vulnerability Analysis – Analyzing discovered vulnerabilities for possible exploitation.

Once vulnerabilities are identified, the System Hacking Phase begins:

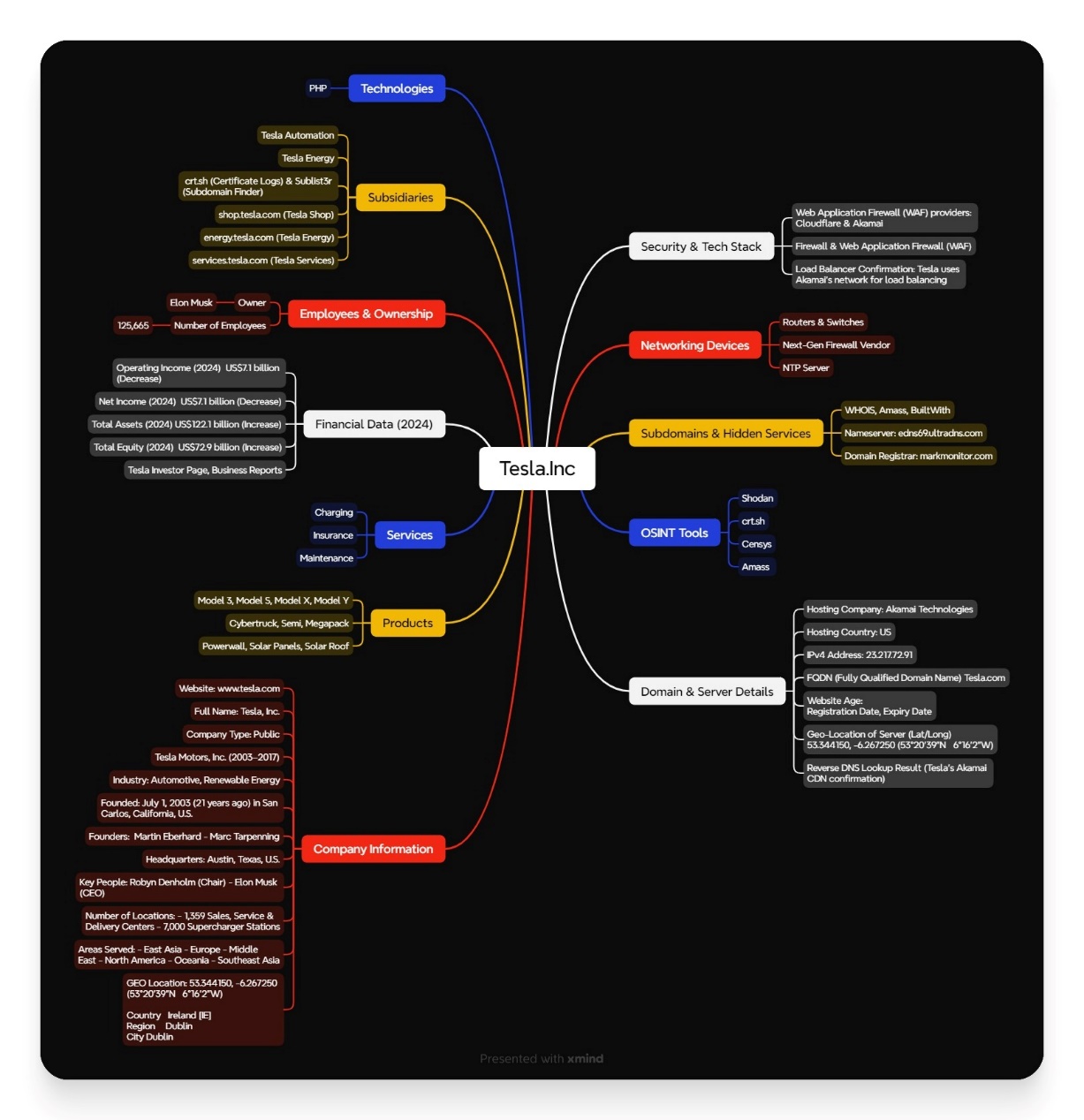
1. Gaining Access – Breaking into the system by cracking passwords or exploiting vulnerabilities.
2. Escalating Privileges – Gaining higher-level (admin/root) access for full control.
3. Maintaining Access – Installing backdoors, executing malicious applications, and hiding files.
4. Clearing Logs – Removing evidence of hacking activities to avoid detection.

Conclusion

This diagram outlines the ethical hacking attack lifecycle, which is used in penetration testing to identify and fix security weaknesses in a system.

**Part 2: Lab**

**Mind Map:**

****

**Table of Contents**

* Introduction
* Tesla OSINT Investigation
* IoT Devices Research Using Shodan
* Tools & Techniques Used

**Introduction**

1. What is OSINT?

Open-Source Intelligence (OSINT) is the practice of collecting and analyzing publicly available data from various sources to extract useful information. OSINT is widely used in:

* Cybersecurity (threat intelligence, security audits)
* Law Enforcement (tracking criminals, investigations)
* Journalism (fact-checking, uncovering hidden info)
* Business Intelligence (competitor analysis, risk management)

What This Report Covers?

Detailed investigation of Tesla, Inc. using OSINT techniques

IoT device research using Shodan

Tools used & verification methods

* **Tesla OSINT Investigation:**

|  |  |  |
| --- | --- | --- |
| Category | Details | Tools / Data Sources |
| Company Name | Tesla, Inc. | WHOIS Lookup, Tesla Website |
| Key Services / Products | - Electric Vehicles: Model S, Model 3, Model X, Model Y, Cybertruck, Roadster - Energy Solutions: Solar Panels, Powerwall, Megapack - Software Services: FSD, Tesla Insurance, Supercharger Network | Tesla Website, Tech News |
| Scope of Services | - EV Manufacturing & Sales - Battery & Energy Solutions - AI & Autopilot Technology - EV Charging Infrastructure - Software & AI-based Services | Business Reports, Investor Page |
| Website (FQDN) | www.tesla.com | nslookup, whois |
| Hosting Provider & Country | Provider: Akamai (CDN) Country: USA | nslookup, ipinfo.io, shodan.io |
| Website Age | Registered On: 1992-11-04  Expires On: 2026-11-03  Last Updated: 2024-10-02 | WHOIS Lookup (whois tesla.com) |
| IP Address | 23.195.108.48 (Akamai CDN) | nslookup tesla.com |
| Geo-Location of Server | Lat/Long: 37.7510, -97.8220 (Approx.) Server Location: USA (Virginia / California) | ipinfo.io/23.195.108.48 |
| Technologies Used | - Web Server: AkamaiGHost  - Programming: JavaScript, ReactJS  - Security: Cloudflare WAF, Akamai WAF - Analytics: Google Analytics, Adobe Analytics | builtwith.com, wappalyzer.com |
| Load Balancer / WAF | Load Balancer: Akamai  WAF: Cloudflare / Akamai | wafw00f -a tesla.com |
| Data Center Devices | - Routers & Switches: Cisco / Juniper  - Next-Gen Firewall: Palo Alto Networks, Fortinet - NTP Server: Cisco / Juniper  - Web Server: AkamaiGHost (Not Apache) | shodan.io, censys.io |
| Content Delivery Network (CDN) | Akamai CDN | nslookup www.tesla.com |
| Sub-Domain Enumeration Tools | Tool 1: amass (Kali Linux) Tool 2: crt.sh (Certificate Transparency Logs) | amass enum -d tesla.com, crt.sh/?q=tesla.com |
| Example Subdomains | shop.tesla.com, energy.tesla.com, services.tesla.com | crt.sh, amass |

* **IoT Devices Research Using Shodan.io:**

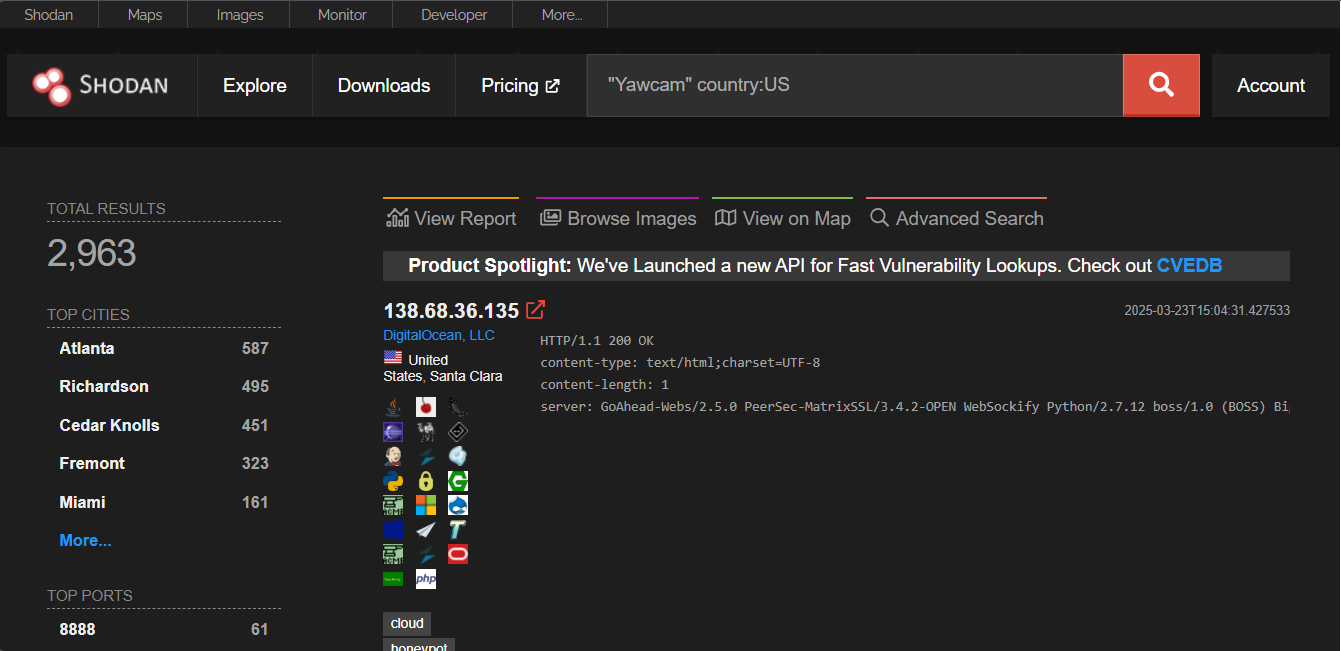
|  |  |  |
| --- | --- | --- |
| Device Type | Search Query (Shodan.io) | Expected Results |
| Yawcams (Webcams) | "Yawcam" country:US | Exposed webcam IPs |
| WebcamXP | "WebcamXP" country:US | Live camera feeds |
| Android IP Webcam | "Android Webcam" country:US | Exposed mobile cameras |
| Security DVRs | "DVR" port:554 country:US | Open security cameras |
| HP Printers | "HP Printer" port:9100 | Open HP printers on the internet |
| Xerox Printers | "Xerox Printer" port:9100 | Exposed Xerox printers |
| Epson Printers | "Epson Printer" | Open Epson devices |
| Canon Printers | "Canon Printer | Vulnerable Canon printers |
| Yamaha Stereos | "Yamaha" port:80 | Open Yamaha devices |
| Apple AirPlay Receivers | "AirPlay" port:7000 | Exposed Apple AirPlay devices |
| Chromecasts / Smart TVs | "Chromecast" port:8008 | Publicly accessible Chromecast devices |
| OctoPrint 3D Printers | "OctoPrint" | Open 3D printer controllers |
| FTP Servers | "220 Anonymous FTP" port:21 | FTP servers allowing anonymous login |

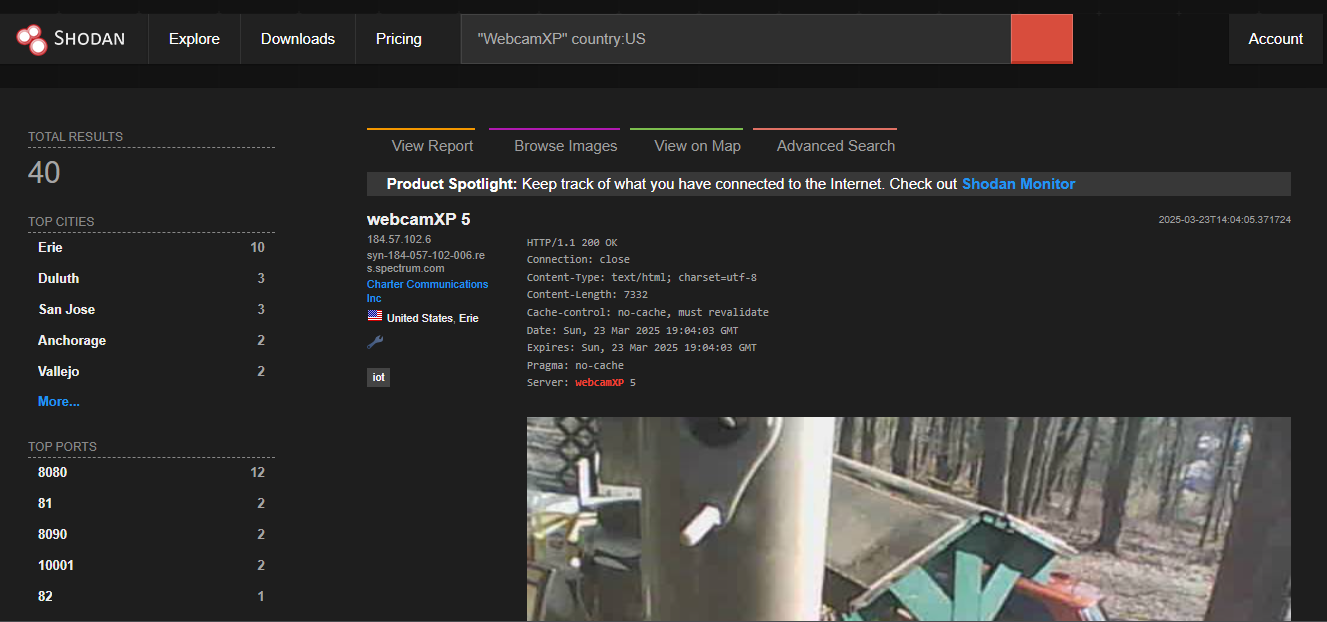
* **Tools & Techniques Used:**

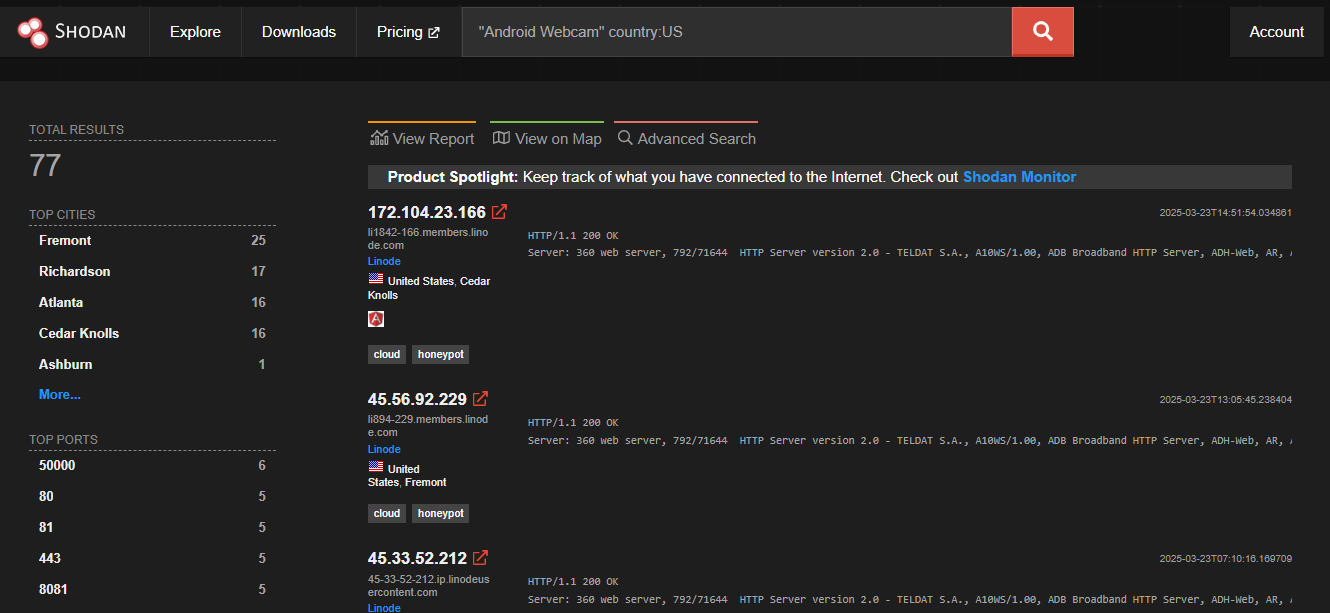
|  |  |
| --- | --- |
| Tool Name | Purpose |
| WHOIS Lookup | Domain registration details (Tesla.com) |
| Nslookup | IP address and hosting details |
| ipinfo.io | Geo-location of Tesla's IP address |
| BuiltWith / Wappalyzer | Identify website technologies |
| WAFW00F | Detect Web Application Firewall (WAF) |
| Amass (Kali Linux) | Subdomain enumeration |
| crt.sh | Certificate-based subdomain discovery |
| Shodan.io | Find exposed IoT devices |
| Censys.io | Find network devices like firewalls, routers |

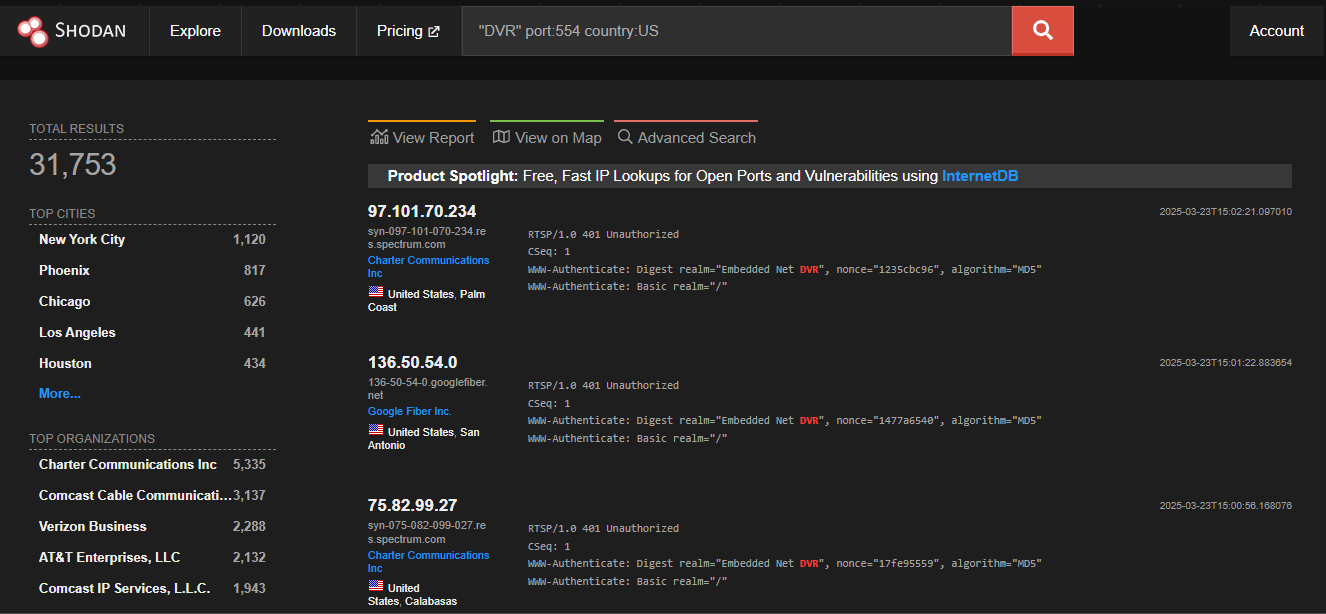
**Screenshot’s Shodan.io**

**Webcams:**

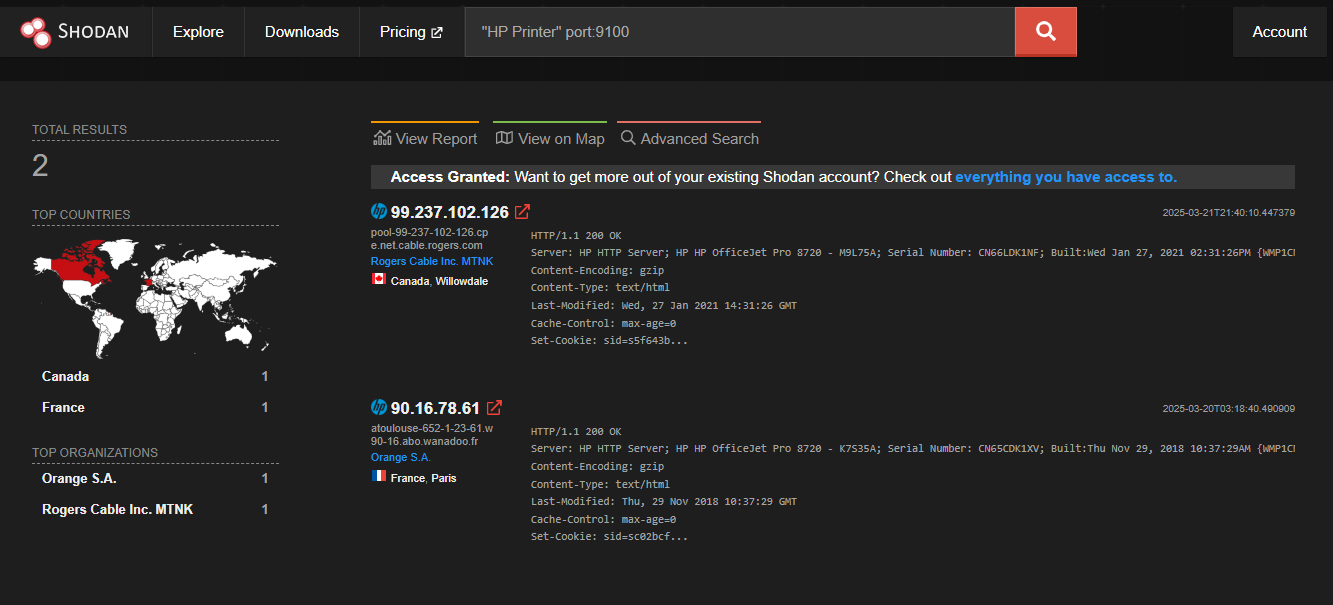


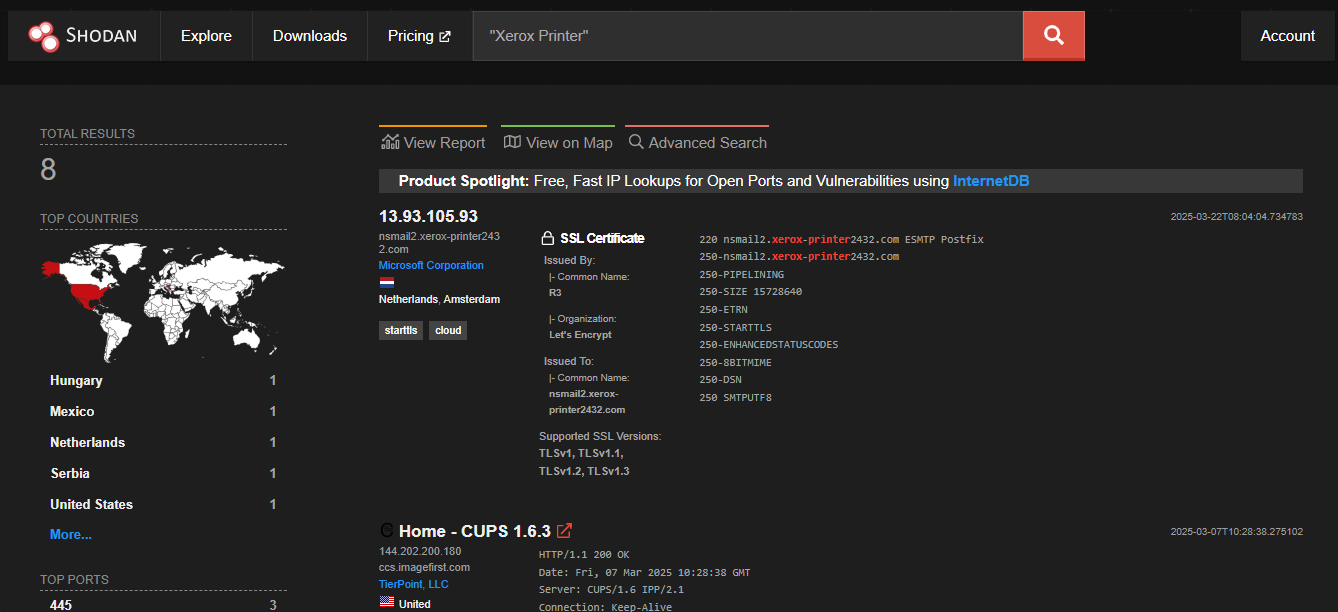


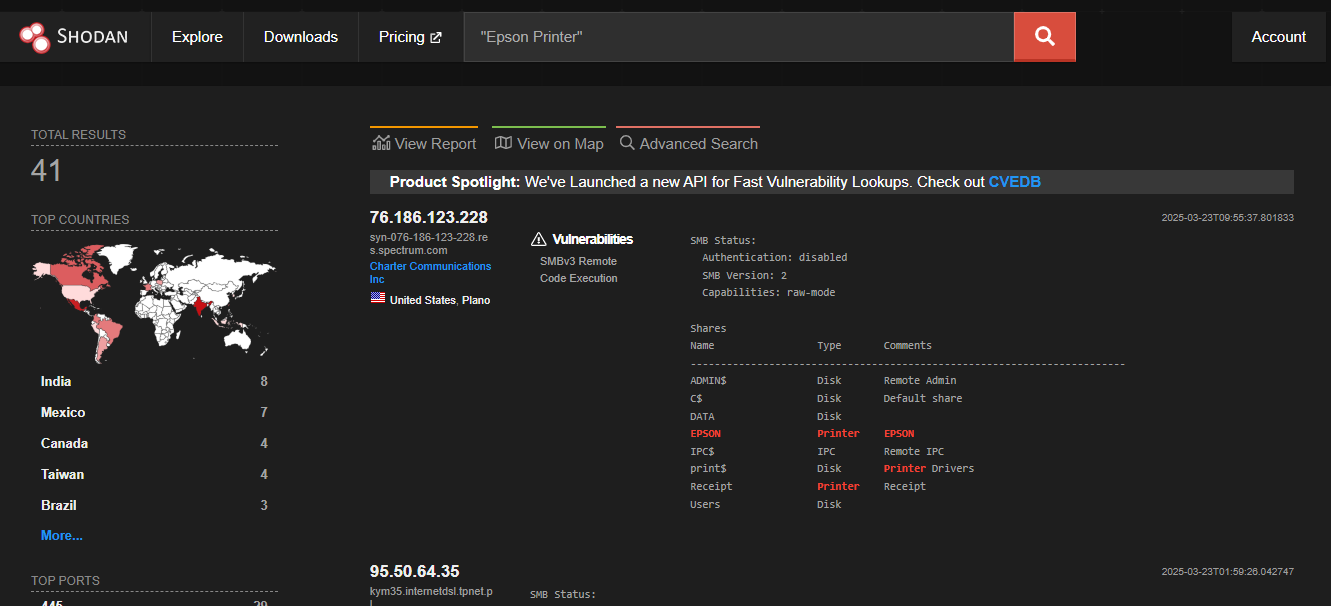


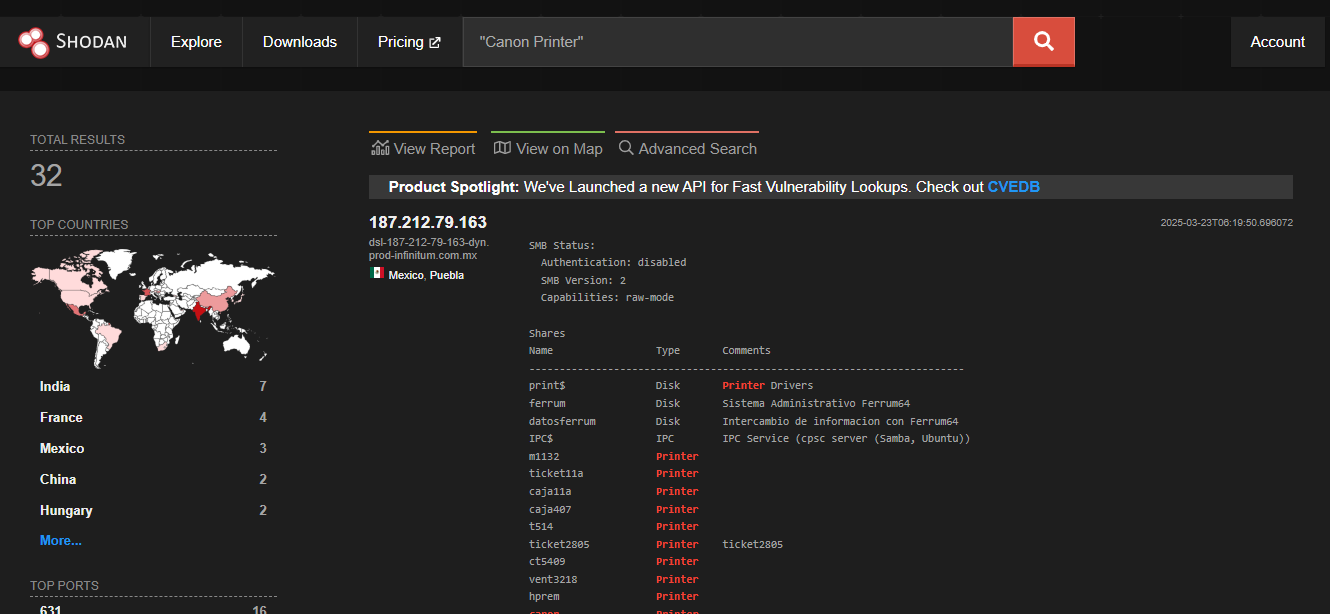


**Printers & Copiers:**

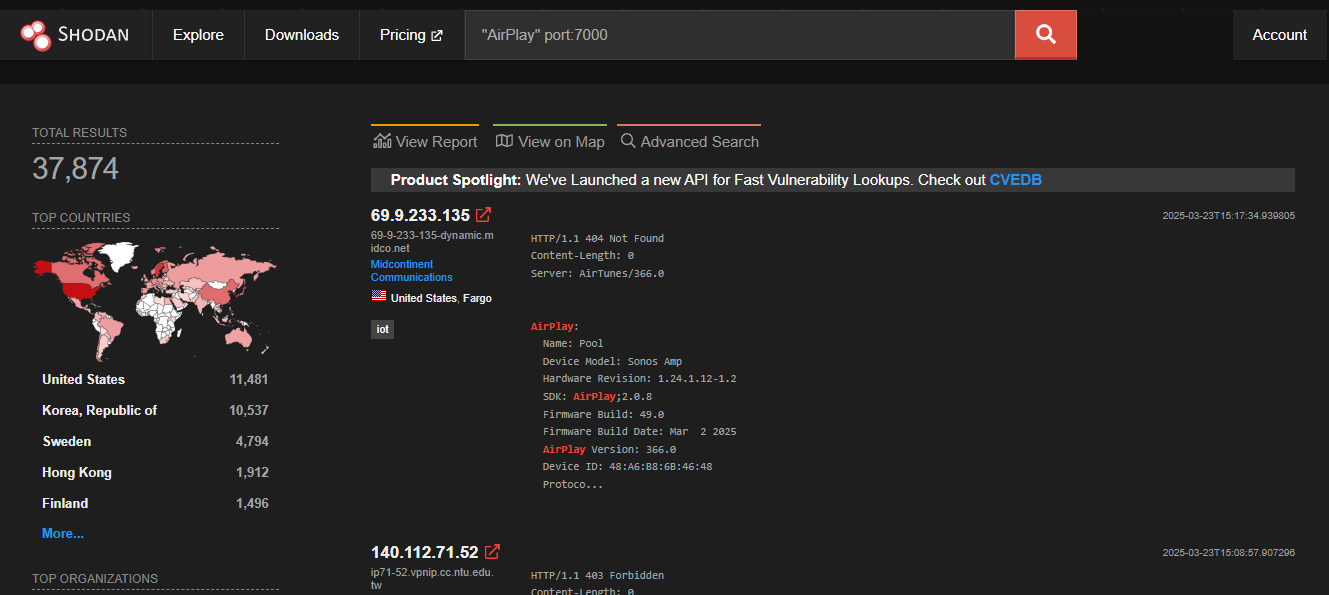


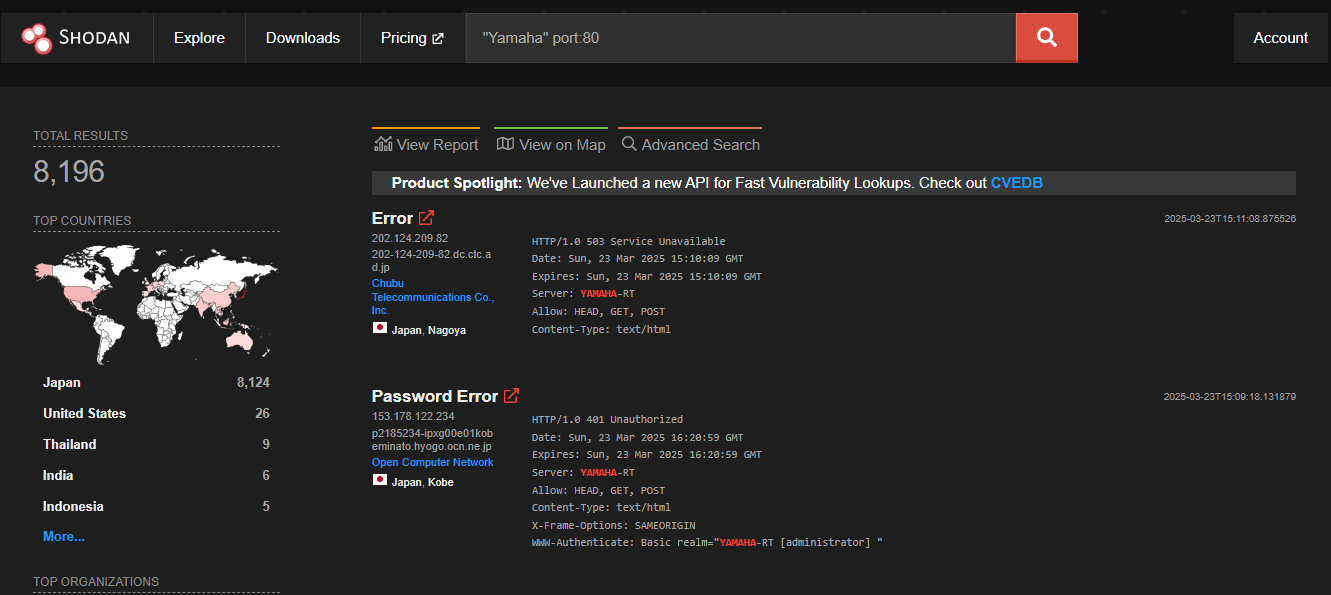


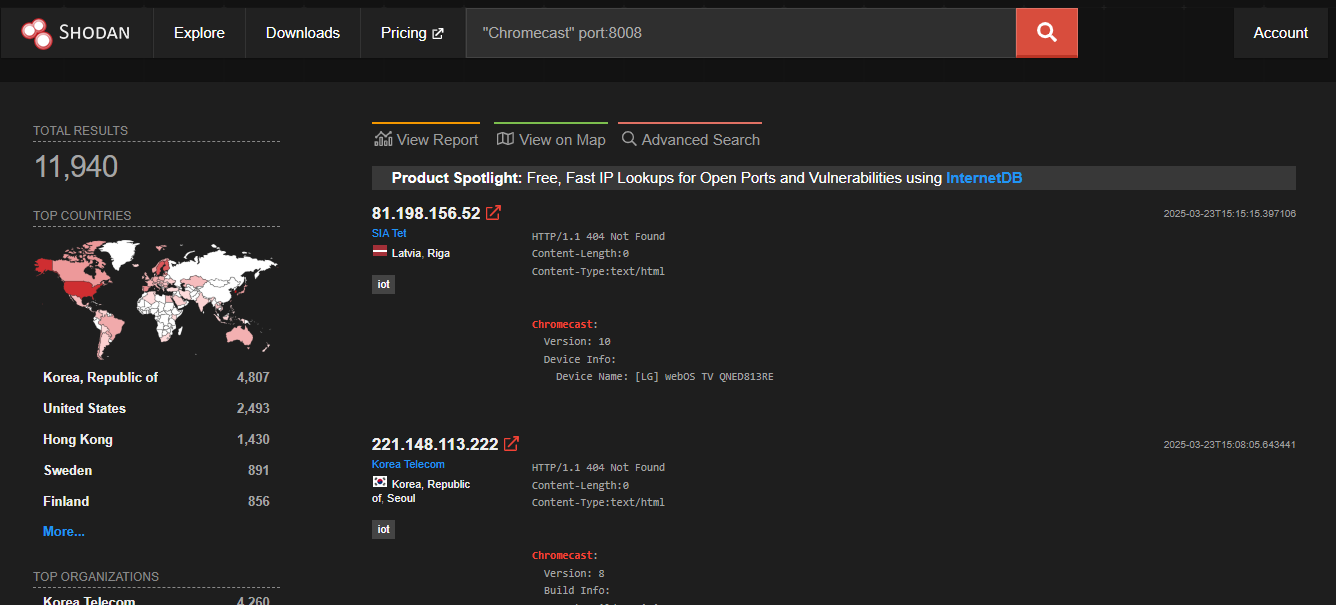


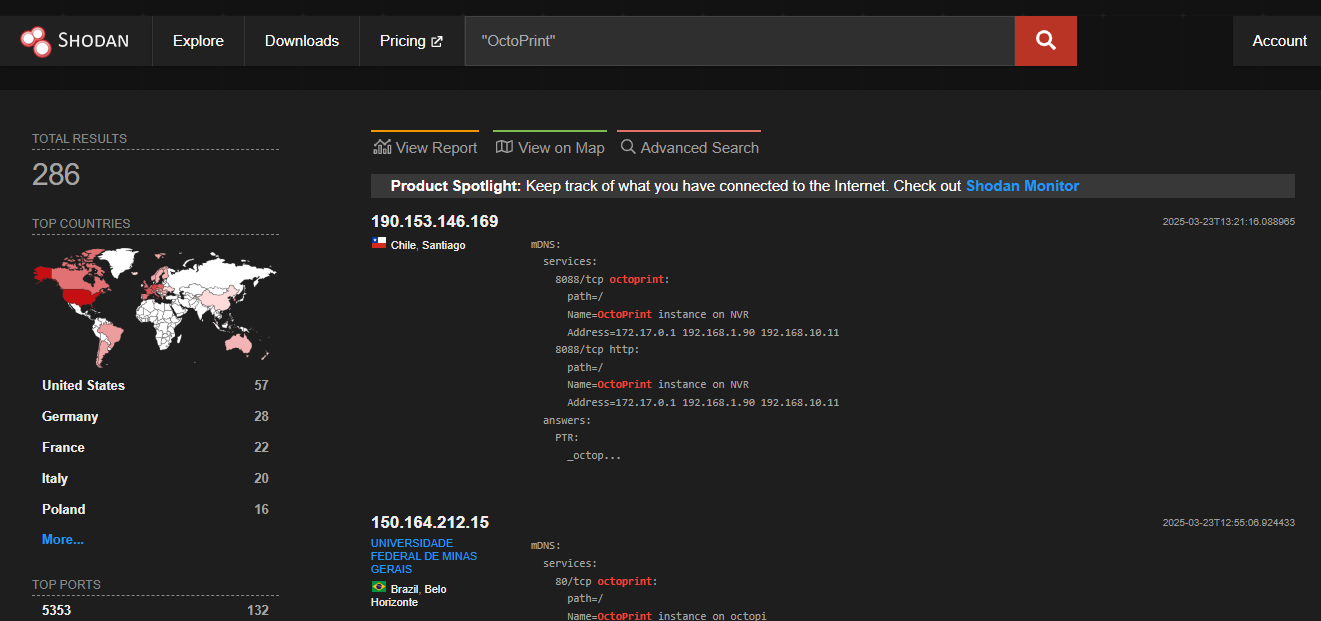


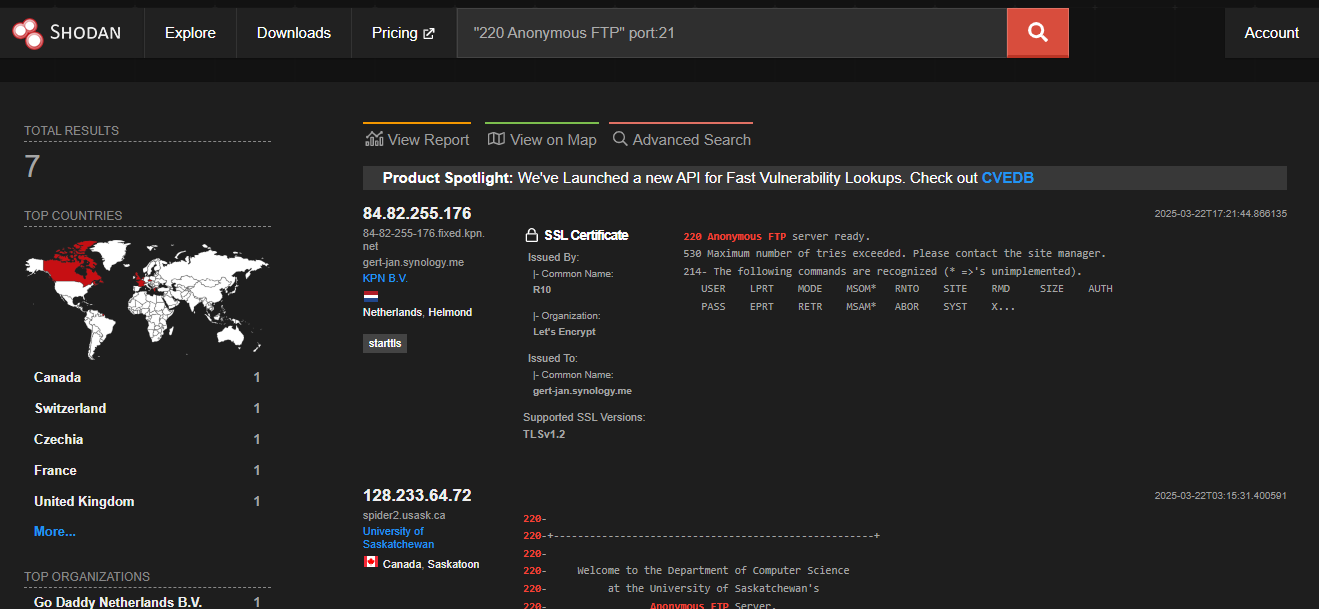
**Home Devices:**











**Conclusion:**

This OSINT investigation successfully gathered detailed information about Tesla, Inc. and identified exposed IoT devices using Shodan. Key findings include:

1. **Tesla's Digital Footprint:**
   * Tesla's website (www.tesla.com) is hosted on Akamai CDN, protected by Cloudflare and Akamai WAFs, and uses technologies like JavaScript and ReactJS.
   * Subdomains like shop.tesla.com and energy.tesla.com were identified using tools like amass and crt.sh.
2. **Exposed IoT Devices:**
   * Shodan queries revealed exposed webcams (Yawcams, WebcamXP), printers (HP, Xerox, Epson), and smart devices (Chromecasts, Yamaha Stereos).
   * FTP servers allowing anonymous logins were also discovered, posing significant security risks.

This report highlights the importance of securing public-facing assets and IoT devices to prevent unauthorized access and cyberattacks.