

# LAB 2: Passive Reconnaissance

Destiny Hale

9/18/25

**Question 1: Login to Shodan (<https://www.shodan.io/>) using your Gmail account or any other account you have created with the portal. Search Web Camera or Web Cam in the search bar, and you will be shown a report where a number of accessible web cameras are listed.**

**• Task 1: Find a device where there is at least one open port and the domain name (URL) is displayed. If you find multiple such devices, just choose one arbitrarily. Take a screenshot highlighting the domain name and the open ports. Attach the screenshot in your submission. 4 points**

The screenshot shows the Shodan search results for IP address 98.220.73.139. The interface includes a search bar at the top with the text 'SHODAN Explore Downloads Pricing Search' and a search icon. Below the search bar, the IP address '98.220.73.139' is displayed. The main content area is divided into two columns. The left column, titled 'General Information', lists various details: Hostnames (c-98-220-73-139.hsd1.il.comcast.net), Domains (comcast.net, highlighted with a green box), Country (United States), City (Indianapolis), Organization (Comcast Cable Communications, LLC), ISP (Comcast Cable Communications, LLC), and ASN (AS7922). The right column, titled 'Open Ports', shows a list of open ports: 81 and 554, which are highlighted with a purple circle. Below the open ports section, there is a section for 'Hikvision IP Camera 4.1.50' with a camera icon and a '<empty title>' label. The HTTP response details for this camera are shown below: HTTP/1.1 200 OK, Date: Wed, 17 Sep 2025 18:38:47 GMT, Server: IWeb5, X-Frame-Options: SAMEORIGIN, ETag: '8-d42-1e8', Content-Length: 489, Content-Type: text/html, Connection: keep-alive, Keep-Alive: timeout=60, max=99. The top right corner of the screenshot shows 'Account' and 'LAST SEEN: 2025-09-17'.

**• Task 2: Using WHOIS (<https://who.is/>) or Netcraft (<https://sitereport.netcraft.com/>), find the IP address of the domain name you found in Task 1. Take a screenshot highlighting the IP address and attach it in your submission. Go through the complete report you retrieved from WHOIS or Netcraft. Do some research online about the vulnerabilities or weakness the device has. Briefly describe all the security weaknesses or vulnerabilities you found. 6 points**

## WHOIS Domain Lookup

Look up registration details, contacts, and nameservers for any domain name

### comcast.net

WHOIS Information

IP Address: 96.99.227.0

### Camera vulnerabilities:

Several vulnerabilities were found in these cameras, including buffer overflow, remote command injection, privilege escalation, and authentication bypass.

**Question 2: Login to Shodan again, but this time search for port:502. Select a device that meets the following criteria:**

- 1. There is at least some information in the device identification field.**
- 2. There is at least one CVE listed in the Vulnerabilities section.**

**• Task 1: Capture some screenshots showing the device id, open ports, and the CVE lists. Attach the screenshots in your submission. 5 points**

**SHODAN** Explore Downloads Pricing Search Account

13.245.7.136 Regular View Raw Data Timeline

// TAGS: cloud // LAST SEEN: 2025-08-23

### General Information

Hostnames: ec2-13-245-7-136-af-south-1.compute.amazonaws.com

Domains: **amazonaws.com**

Cloud Provider: Amazon

Cloud Region: af-south-1

Cloud Service: EC2

Country: South Africa

City: Cape Town

Organization: Amazon Data Services South Africa

### Open Ports

502 2058 4321 4455 4782 7474 12206 12286 12301 32400 51106

// 502 / TCP 2040958958 | 2025-08-23T04:58:26.966483

#### TRENDnet IP Camera

NSA325

```
HTTP/1.1 200 OK
Date: Sat, 23 Aug 2025 04:58:26 GMT
Server: boltServer
X-Powered-By: Express
content-length: 918
content-type: text/html
Set-Cookie: csrfToken=kdV25LSuUWncp5XQLKP
```

// 2058 / TCP 117081007 | 2025-08-23T03:14:50.800478

## Vulnerabilities

All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**2021 (1)**

**CVE-2021-32052** **6.1** In Django 2.2 before 2.2.22, 3.1 before 3.1.10, and 3.2 before 3.2.2 (with Python 3.9.5+), URLValidator does not prohibit newlines and tabs (unless the URLField form field is used). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because HttpResponse prohibits newlines in HTTP headers.

**2020 (1)**

**CVE-2020-29396** **9.9** A sandboxing issue in OdoO Community 11.0 through 13.0 and OdoO Enterprise 11.0 through 13.0, when running with Python 3.6 or later, allows remote authenticated users to execute arbitrary code, leading to privilege escalation.

**2009 (2)**

**CVE-2009-3720** **5.0** The updatePosition function in lib/xmlltok\_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

**CVE-2009-2940** **7.5** The pygresql module 3.8.1 and 4.0 for Python does not properly support the PQescapeStringConn function, which might allow remote attackers to leverage opening issues involving multibyte character

• **Task 2: Do some research about the device you chose and describe the device type and found vulnerabilities in a paragraph. Try to keep the paragraph limited into 5-10**

**sentences. 5 points**

The device listed here is an IP camera made by the manufacturer Trendnet. IP cameras are devices that send and receive video footage over an IP network (Bay Alarm Bulletin, n.d.). These devices are usually connected to a network video recorder (NVR) through wifi to transmit footage. There are three networks you can connect these devices to: wireless, wired, and cellular. A few features of Trendnet IP cameras include PoE support, HD resolution, and night vision (Trendnet, n.d.). A few vulnerabilities this camera has are input validation, privilege escalation, denial of service, and SQL injection.

- **Task 3: Select a CVE from the CVE list shown in the Vulnerabilities section and search for that CVE in <https://cve.mitre.org/>. Identify the attack/vulnerability described in the CVE.**

According to the CVE (2021), CVE-2009-3720 is a denial-of-service attack. The vulnerability was found within the update position function in Expat 2.0.1. This allowed attackers to cause a DoS via an XML document and UTF-8 sequences, which later triggered a buffer overflow.

**Go to <https://attack.mitre.org/matrices/enterprise/network/> and find the attack from the matrix. If the attack is not listed there, try to search in other attack matrices given in the MITRE ATT&CK website. Once you find the attack listed as a technique, try to find out one relevant detection and one mitigation methods. Take screenshots showing the detection id and the mitigation id. Attach your screenshots in your submission and briefly summarize the selected detection and mitigation methods.**

## Detection

ID	Data Source
DS0015	Application Log

This detection involves monitoring application logging, messaging, and other forms of transmission that may result in a denial-of-service attack (Mitre Att&ck, 2025).

# Mitigations

ID	Mitigation
M0815	Watchdog Timers

This mitigation includes system reboots and is performed when a timeout condition occurs (Mitre Att&ck, 2025).

Sources:

CVE-2009-3720 | CVE | June 6, 2021

<https://www.cve.org/CVERecord?id=CVE-2009-3720>

Denial of Service | Mitre Att&ck | April 15, 2025

<https://attack.mitre.org/techniques/T0814/>

Networking and Surveillance | TRENDnet | n.d.

<https://www.trendnet.com/products/surveillance>

What Are IP Cameras and How Do They Work? | Bay Alarm Bulletin | n.d.

<https://www.bayalarm.com/blog/what-are-ip-cameras-and-how-do-they-work/>