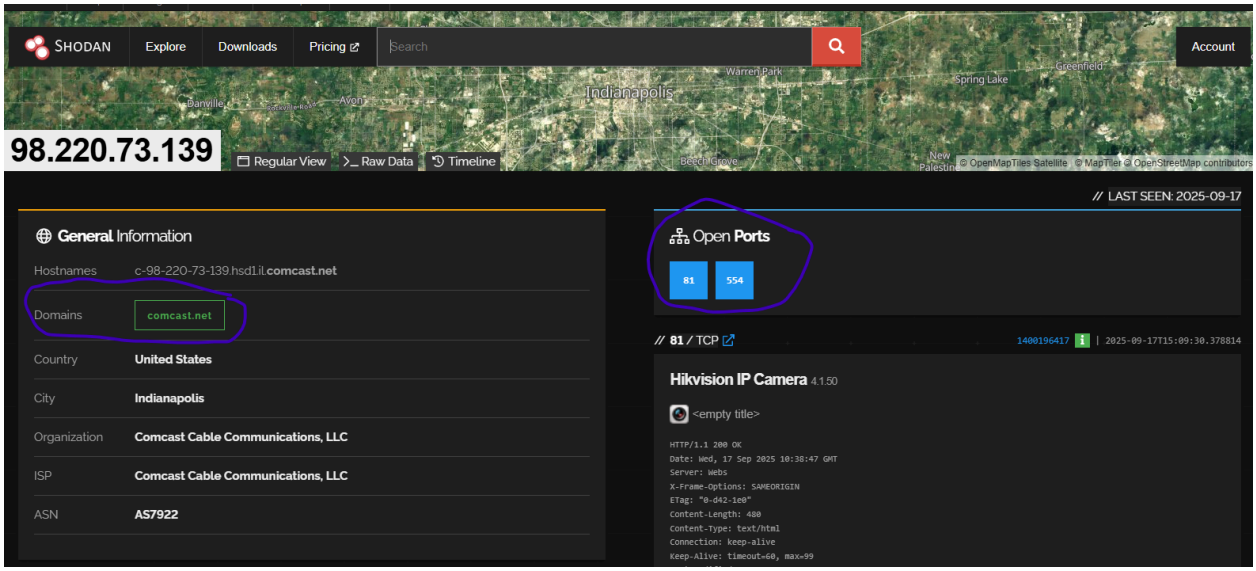
LAB 2: Passive Reconnaissance

Destiny Hale

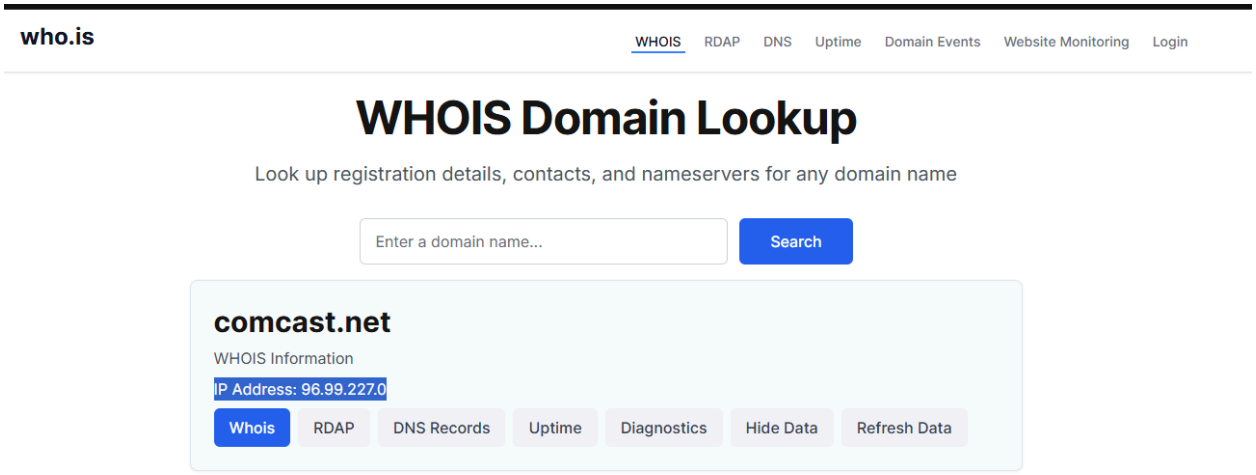
9/18/25

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



• 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



Camera vulnerabilities:

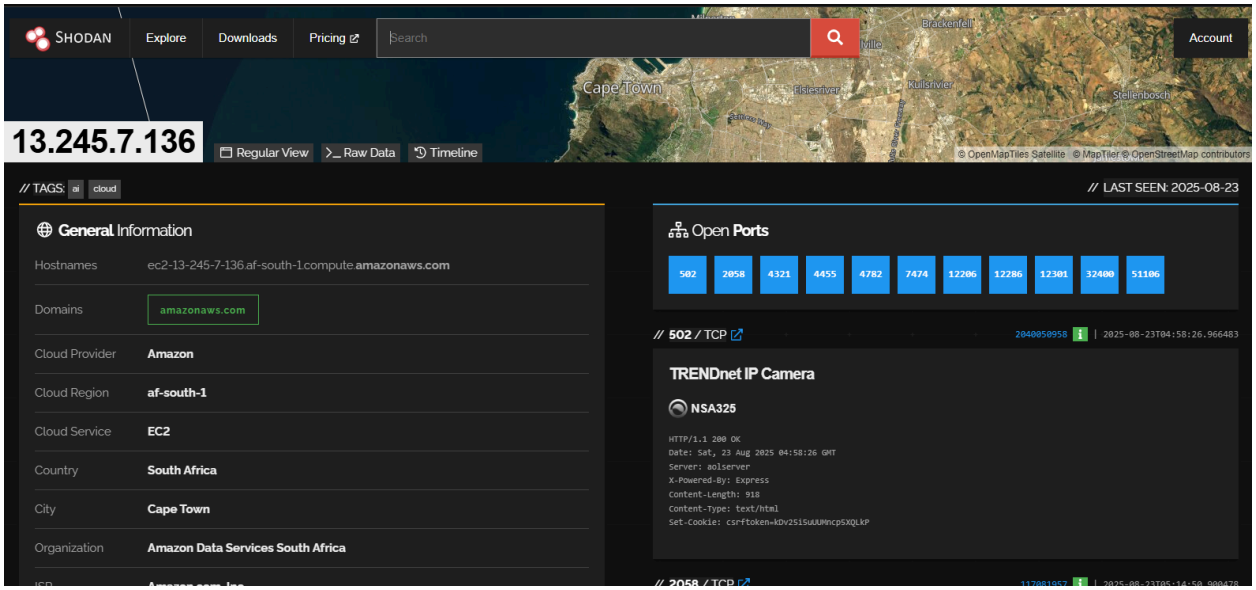
Several vulnerabilities were found in these cameras, including buffer overflow, remote command injection, privilege escalation, and authentication bypass.

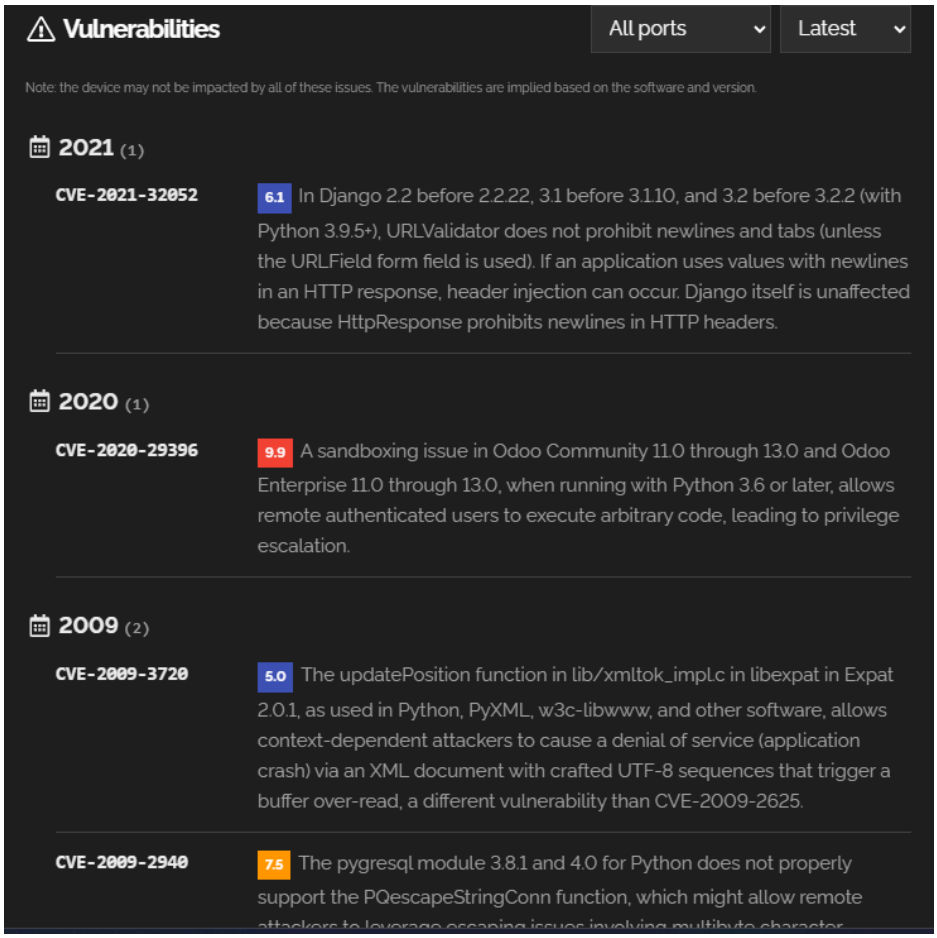
Question 2: Login to Shodan again, but this time search for port:502. Select a device that meets the following criteria:

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





• 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

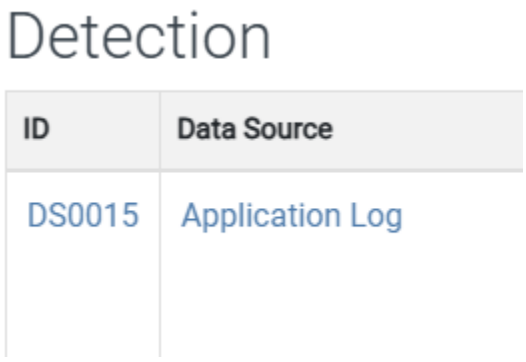
sentences. 5 points

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.



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/