7/22/2025

IOT Security Lab

Internet exposed IOT

M Sameer Malik

https://www.linkedin.com/in/sameer-malik-18b52634b/

Disclaimer:

This lab is shared **strictly for educational purposes** and to promote ethical cybersecurity practices. I **do not endorse or encourage** the misuse of any techniques or tools demonstrated here. Readers are **solely responsible** for ensuring their actions comply with all applicable laws and regulations.

Hack responsibly. Hack legally. Hack ethically.

Table of Contents

IOT SECURITY LAB

OBJECTIVES:

- Realize the importance IOT Security.
- Awareness regarding ever-increasing insecure IOT devices.
- *Exploring Internet-Exposed Camera Systems using Shodan zoomeye and OSINT*

Shodan:

As with any cybersecurity operation, the initial step is always reconnaissance. The primary objective during this phase is to identify a target and gather as much open-source information as possible. In this lab, the focus is on identifying internet-exposed devices using search engines such as Shodan.io.

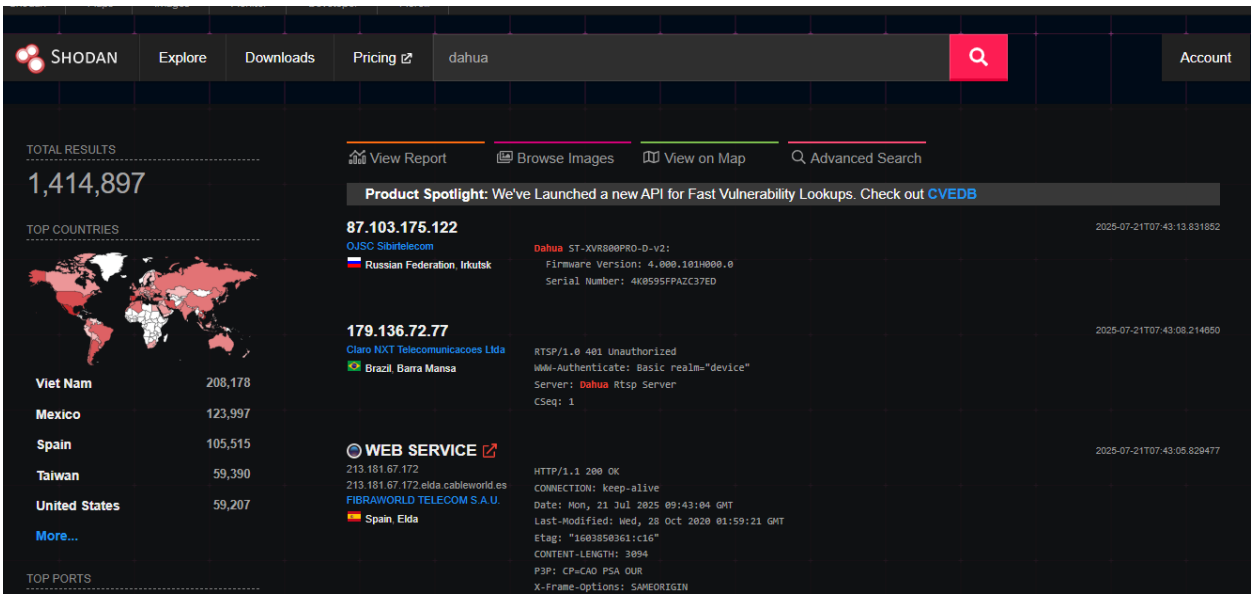
Shodan is a powerful search engine that indexes publicly accessible devices connected to the internet, including IP cameras, routers, and other IoT systems.

To maximize the effectiveness of the search, it is essential to use filters and well-structured queries, which help narrow down results based on criteria such as device type, location, port numbers, and banners.

The Shodan interface is relatively user-friendly and supports advanced query syntax, enabling users to refine their search efficiently.

In this lab, the target devices are Dahua IP cameras, and the search is refined further using country and city-level filters to simulate a geographically scoped reconnaissance effort.

However, it is important to note that Shodan's free version imposes limitations on the number of viewable results, which can restrict the depth of exploration. For broader access, alternative tools such as ZoomEye may be considered.



Zoomeye:

Given the limitations of Shodan's free tier, an effective alternative is ZoomEye.org. ZoomEye is generally more accessible to free users and offers broader visibility into internet-exposed devices.

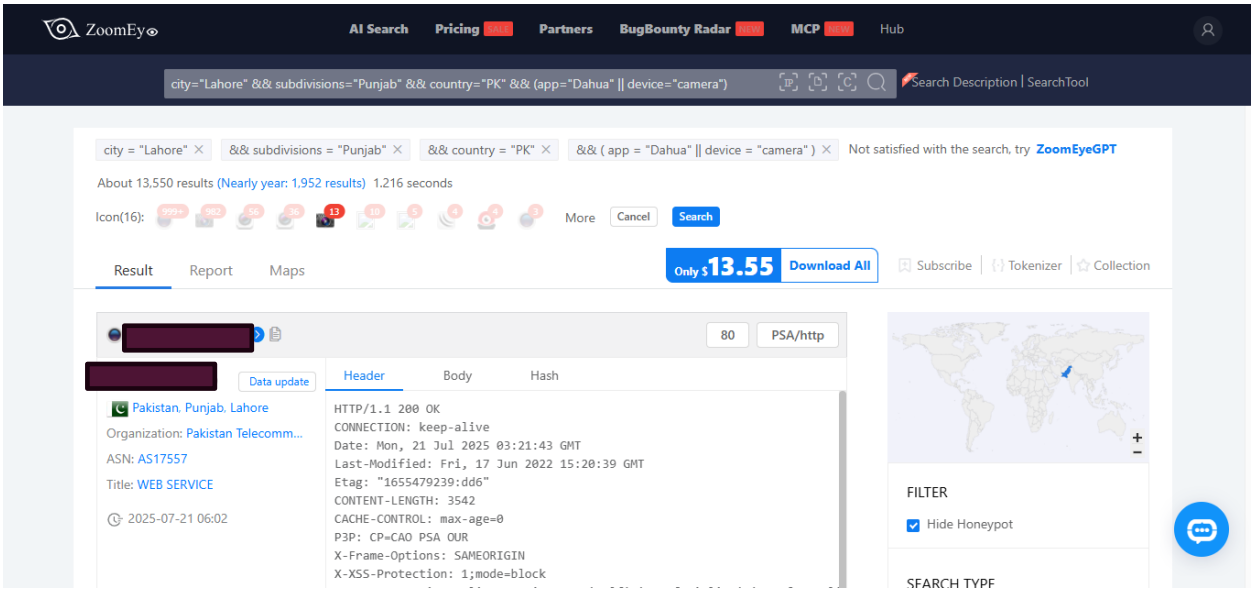
It is also considered more lenient in terms of the number of results available without a subscription, making it a valuable tool for reconnaissance, particularly in educational and research contexts.

Although ZoomEye's query syntax can be more complex compared to Shodan, it compensates for this with the inclusion of **ZoomGPT**, an integrated AI assistant that helps users construct precise search queries using natural language input.

This feature greatly simplifies the process for those unfamiliar with advanced query structures and enhances the efficiency of reconnaissance.

In this lab, ZoomEye is used to identify the IP address of a targeted Dahua device, replicating the reconnaissance process under real-world conditions. Additionally, ZoomEye provides a unique advantage by identifying known honeypots—decoy systems deployed to attract and analyze malicious activity.

These honeypots can be filtered out of search results to ensure that only legitimate exposed devices are being analyzed during the lab.



Nmap:

After identifying a viable target, the next logical step is to conduct active reconnaissance to gather more detailed information about the system.

In this phase of the lab, I performed a **network scan using Nmap** on the extracted IP address. Nmap (Network Mapper) is a powerful and widely-used open-source tool designed for network discovery and security auditing.

To perform a more comprehensive analysis, I used the following flags during the scan:

1. **-A (Aggressive Scan)**
   This option enables a suite of advanced scanning features, including OS detection, version detection, script scanning, and traceroute.

   It is particularly useful during initial assessment to get a complete picture of the target's exposed services and potential vulnerabilities.

2. **-T4 (Timing Template)**
   The -T flag controls the timing and speed of the scan. While -T5 is the fastest, it is also the noisiest and most detectable. In red team or stealth-based operations, it is recommended to use slower timing options such as -T2 to avoid triggering intrusion detection systems (IDS).

   However, for lab environments where speed is prioritized over stealth, -T4 offers a balanced option that speeds up the scan without sacrificing much accuracy.

This active reconnaissance helps to enumerate open ports, detect running services, and identify potential vulnerabilities that could later be explored in a controlled, ethical manner.

Command: nmap -A <ip> -T4

Analysis:

After reviewing the detailed Nmap scan results, I identified that **port 80** was open and hosting an HTTP service. This finding aligned with the earlier reconnaissance conducted through ZoomEye.

In addition to port 80, several other ports were detected as open, each potentially offering an entry point depending on the services running behind them.

If these services are misconfigured, outdated, or unpatched, they could pose significant security risks — a critical insight when evaluating the security posture of internet-exposed IoT devices.

Whois:

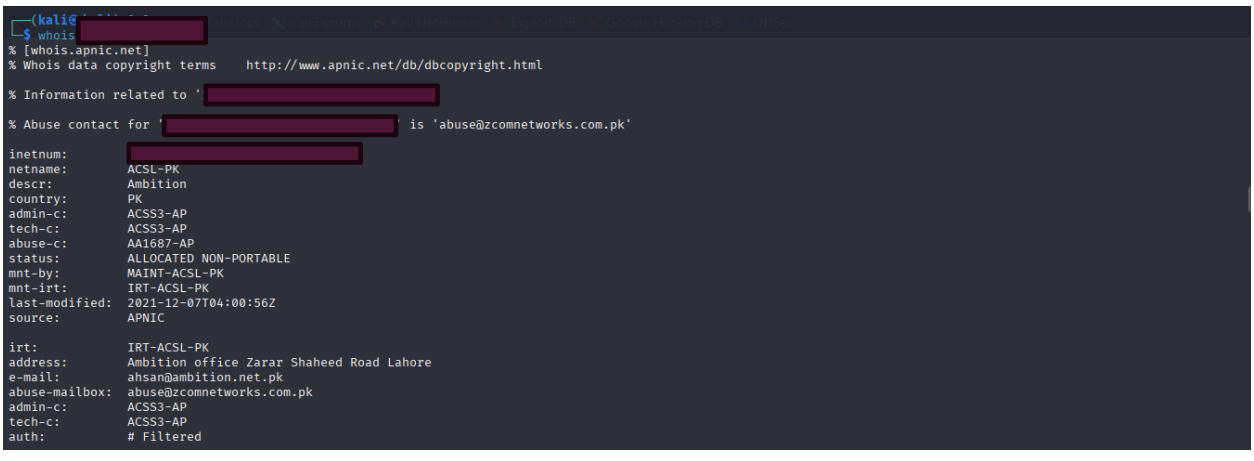
To gain deeper contextual information about the target, I conducted a **WHOIS lookup** on the IP address.

The whois utility provides registration and ownership details associated with the IP, such as the Internet Service Provider (ISP), country, contact information, and autonomous system (AS) number.

This information is useful not only for identifying the hosting environment but also for understanding the broader infrastructure and organizational ties.

WHOIS data can also help validate whether the device is genuinely deployed by an individual, a company, or is part of a larger network segment, aiding in risk classification and further scoping of the target.

Command: whois <ip>



Exploiting Default Credentials:

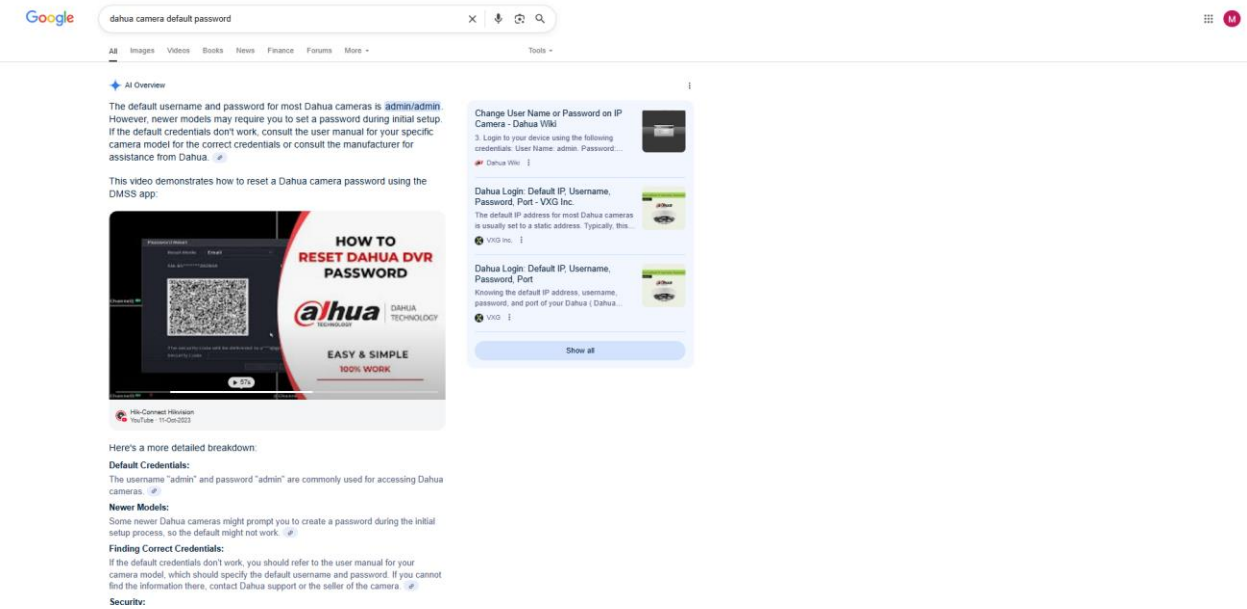
One of the most common and critical vulnerabilities found across a wide range of IoT devices is the continued use of **default credentials**. Many devices, including IP cameras, are shipped with manufacturer-set usernames and passwords that users often neglect to change. This creates a significant security risk, as these credentials are publicly documented and widely known within the cybersecurity community.

To explore this vulnerability, I conducted open-source research using Google to search for the **default credentials used by Dahua cameras**. While the top search results did provide some information, further investigation revealed that several of those sources were outdated. To ensure accuracy, I extended my research to forums, vendor documentation, and distributor guides.

Through this process, I discovered that a **commonly used default credential set** for Dahua devices is:

- **Username:** admin
- **Password:** admin123

These credentials are frequently left unchanged in real-world deployments, especially when devices are set up in bulk or by non-technical personnel. Identifying this information highlights the importance of credential hygiene and demonstrates how attackers can easily gain unauthorized access if proper security practices are not enforced.



Password Database:

Another valuable resource for identifying default credentials is **PasswordDatabase.com**.

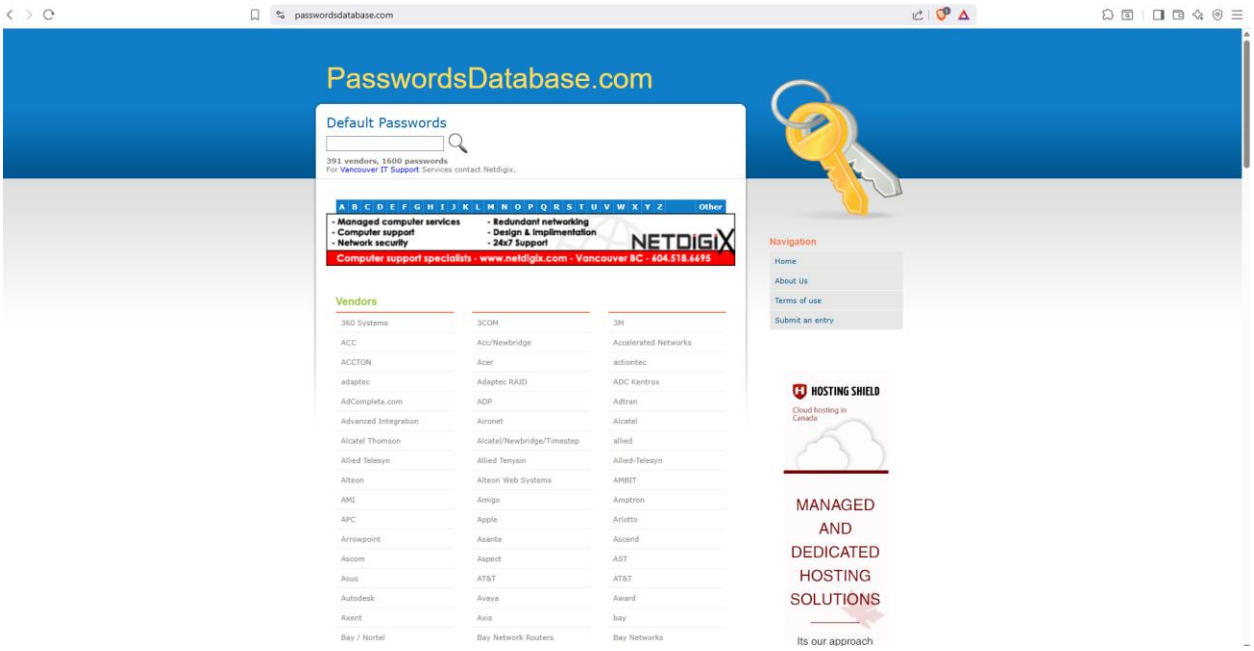
This website maintains an extensive collection of default usernames and passwords for a wide range of vendors, including IoT devices, networking equipment, and industrial systems.

It is frequently referenced by security professionals and penetration testers during the reconnaissance phase.

The database is searchable by vendor, product type, or keyword, making it an efficient tool for quickly locating known default login information.

Utilizing such resources highlights how easily attackers can discover weak credentials if devices are not properly secured or reconfigured after deployment.

However one should never rely on single tool for these types of operations, always confirm your finding from 2 or more sources!



Gaining Access:

After identifying the default credentials for the targeted Dahua camera, I attempted to authenticate using the commonly known combination of

username: admin and **password: admin123**.

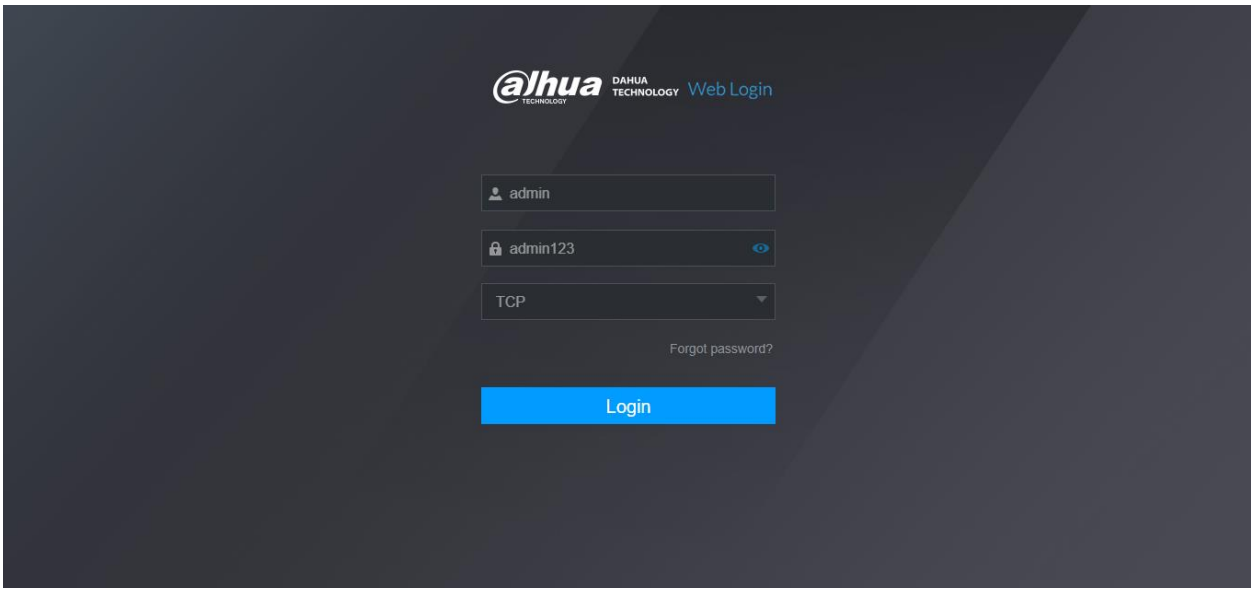
Upon testing, it was confirmed that the device had not been reconfigured and still used the factory-default login credentials.

This indicates a significant **misconfiguration or more accurately, administrative negligence** — as leaving default credentials unchanged poses a major security risk.

Unauthorized access could allow an attacker to view live camera feeds, change settings, or pivot into the internal network, depending on the device's configuration and placement.

This finding reinforces the importance of enforcing secure credential policies, especially in internet-exposed IoT environments.

To access the below given login page I entered the ip of the camera in my browser and after some time of loading this page showed up.

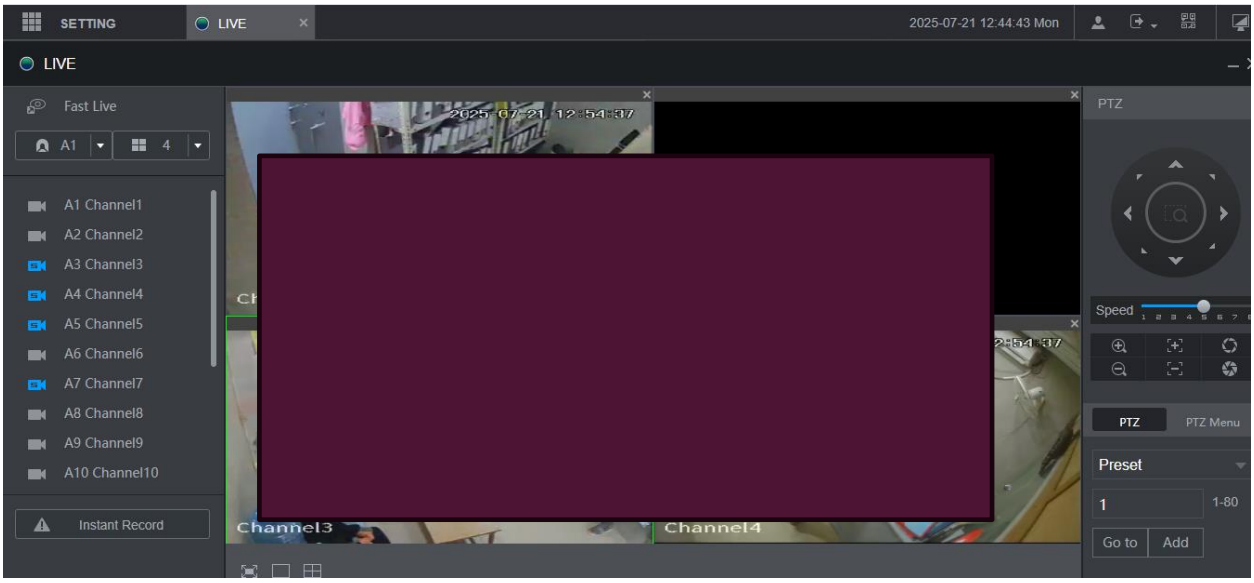


LIVE Feed:

Ultimately, I was able to **gain full access to the device**, confirming that it was vulnerable due to the use of default credentials.

This demonstrates how effortlessly a threat actor could compromise an IoT device that has been improperly configured or neglected during deployment.

The process required no advanced exploitation techniques, just open-source intelligence and basic enumeration. This highlights the **real-world risk posed by default credentials** and emphasizes the urgent need for secure provisioning, proper access control, and routine device audits in IoT environments.



Mitigations:

Based on the vulnerabilities and misconfigurations observed during this lab, the following mitigation strategies are recommended to enhance the security of internet-exposed IoT devices, particularly IP cameras like those from Dahua:

1. **Change Default Credentials Immediately**
   One of the most critical steps is to ensure that all factory-default usernames and passwords are changed during the initial setup. Strong, unique passwords should be enforced for all administrative interfaces.

2. **Restrict Public Exposure**
   Devices should not be directly exposed to the internet unless absolutely necessary. Where exposure is required, access should be restricted via IP allowlists, VPN tunnels, or reverse proxies with authentication layers.

3. **Disable Unused Services and Ports**
   Unused services and open ports should be disabled to reduce the attack surface. For example, if remote access via HTTP is not needed, port 80 should be closed or limited to internal network access.

4. **Regular Firmware Updates and Patching**
   IoT devices often contain known vulnerabilities that are addressed in firmware updates. Regularly applying firmware patches from the official vendor is essential to protect against known exploits.

5. **Implement Network Segmentation**
   IoT devices should be isolated from critical internal systems using VLANs or firewalled subnets. This limits lateral movement in case a device is compromised.

6. **Enable Logging and Monitoring**
   Where supported, logging and audit trails should be enabled on the devices. Centralized monitoring can help detect unauthorized access attempts or abnormal behavior in real time.

7. **Use Strong Encryption and HTTPS**
   Administrative interfaces should always be accessed over HTTPS, and data transmitted between devices should be encrypted to prevent interception and tampering.

8. **Disable Universal Plug and Play (UPnP)**
   UPnP can expose internal services to the internet without user knowledge. Disabling UPnP on routers and IoT devices helps prevent unintended exposure.

9. **Conduct Regular Security Audits**
   Periodic assessments of all connected devices should be performed to identify misconfigurations, outdated firmware, and weak authentication mechanisms.

Conclusion:

This lab effectively demonstrated how internet-exposed IoT devices—specifically Dahua IP cameras—can be identified, profiled, and potentially compromised using publicly available tools and open-source intelligence.

Beginning with passive reconnaissance through platforms like Shodan and ZoomEye, I was able to locate misconfigured devices based on service banners and metadata.

Active scanning using Nmap revealed open services, with port 80 exposing a web interface. Through basic credential research and validation, I confirmed that the device still used its factory-default login credentials, resulting in full unauthorized access.

This process underscores a major and recurring issue in the IoT ecosystem: **negligent device configuration**.

Many manufacturers and end users fail to change default credentials, leaving devices highly vulnerable to exploitation with minimal effort.

This is not a theoretical risk—it is an easily reproducible and realistic threat vector that has been widely abused by threat actors, including in large-scale botnet campaigns.

The findings from this lab highlight the importance of:

- Implementing proper credential hygiene.
- Regularly auditing internet-facing devices.
- Disabling unnecessary services and ports.
- Using segmentation and firewall rules to limit exposure.

In conclusion, securing IoT devices is not solely a technical challenge—it is also a matter of awareness and responsibility. As this lab has shown, even basic reconnaissance can lead to full compromise if proper security practices are not in place.