Report Overview

This report summarizes the findings from the Google Dork search site:shodan.io "default password", which was used to identify exposed devices and services that may still be using factory default passwords. Default passwords are often widely known and can be exploited by attackers to gain unauthorized access to sensitive systems.

1. Objectives

- **Primary Goal:** To identify and document any systems exposed on the internet with default credentials.
- **Secondary Goal:** To assess the security posture of discovered devices and recommend steps to secure them.

2. Tools Used

- **Google Dork Search:** `site:shodan.io "default password"`
- **Shodan.io:** A search engine for internet-connected devices, used to locate devices and services that may have exposed default credentials.

3. Findings

IP Address Found:

- **IP Address:** 12.38.208.94
- **Location:** United States, Sunnyvale
- **Service Identified:** HTTP (nginx web server)

Detailed HTTP Response:

- **Status Code:** 200 OK (indicating the server is up and running)
- **Server Information:** nginx (a widely used web server software)
- **Response Headers:**
  - **X-Frame-Options:** DENY (indicating protection from clickjacking attacks)
  - **X-Content-Type-Options:** nosniff (preventing the browser from trying to guess the content type)
- **Content Type:** `text/html`
- **Transfer Encoding:** chunked (used to send the body in chunks)

Server Response:

Upon querying the server, the response returned an HTML page with an incomplete structure (indicated by the header `c50`), suggesting that the server is potentially hosting a web page or login interface.

12.38.208.94

- NEW HORIZON COMMUNICATIONS CO
- United States, Sunnyvale

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 06 Aug 2025 13:44:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: DENY
X-Content-Type-Options: nosniff

c50
<!DOCTYPE html>
<html><head>
<meta charset="utf-8"/>
<link rel="shortcut icon" type="ima...
```

4. Conclusion

The search query `site:shodan.io "default password"` led to the identification of an exposed device running a web server (nginx) at IP address `12.38.208.94`. While the server responded with a basic HTML page and headers, the exact contents of the page are unclear without further inspection. The potential for default passwords or misconfigurations makes this a high-risk target for attackers.