

Project Documentation SecOverview

Samuel Giger

February 17, 2025

Abstract

This document describes the installation and usage of my hobby project SecOverview to enable you to create a simple assessment of your infrastructure.

Do not scan assets without the permission of the owner. Use this app at your own risk.

For feedback or input on optimizations, don't hesitate to contact me via the contact form on the page: samuelgiger.com

Contents

1	Overview	4
2	Installation	5
3	News/RSS	6
4	YARA Scans	7
5	NMAP Scan	8
6	IP Check	9
7	DNS Operation	10
8	Ransomware Data	11

1 Overview

This document describes the installation and handling of the hobby project github.com/gigersam/SecOverview. This project is intended to help small infrastructures gain better insight and an overview of possible leaks or assets that are accessible. Therefore, the project aims to help analyze certain aspects of it.

In this version, the following actions are implemented:

- RSS Feeds
- Ransomware Victims (Source: [Ransomware.live](https://ransomware.live))
- NMAP Scans
- DNS Query
- IP/ASN Check (Source: bgpview.io)
- YARA Rules Check

The NMAP scans also save the discovered assets in a database for later viewing. These scans should provide an overview of the assets in the infrastructure.

2 Installation

The current version has been tested on a basic Debian 12 (Bookworm). The application uses Python, Django, Gunicorn, and NGINX. This version only supports SQLite as a database. For Debian 12, an install script is available.

Script: SecOverview Install Script

Download the script via a browser or use the following command:

```
wget https://github.com/gigersam/SecOverview/blob/main/install.sh
```

After downloading the script, add execution rights to the file with the following command:

```
sudo chmod +x install.sh
```

Then execute the file as an administrator with the command:

```
sudo ./install.sh
```

After installation, an output with the admin password will be displayed.

The script also creates a service for the Django application named "secoverview.service".

To access the application, use a browser and navigate to the server at:

```
http://YOUR-IP/
```

After that, a login screen will be displayed, where you will be able to log in with the admin credentials.

3 News/RSS

On the "News/RSS" page, all the latest news from the added RSS feeds will be displayed:

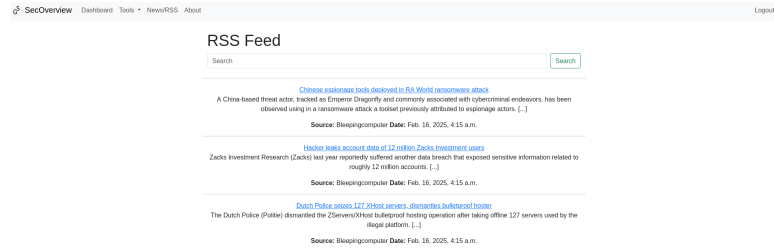


Figure 1: RSS News Overview

To add a new RSS feed, you will be required to access the admin panel. Therefore, navigate to the page *http://YOUR-IP/admin*. Under RSSAPP - Feed Sources - Add Feed Source, you can add more sources. For example, add BleepingComputer's RSS feed to the database:

URL: *https://www.bleepingcomputer.com/feed/*
NAME: *BleepingComputer*

After visiting the "News/RSS" page tab, you will be able to see the latest news. This way, you can add more news feeds.

4 YARA Scans

To use the YARA scanner, you will be required to add some YARA rules. In this example, the YARA rules from abuse.ch will be used. These rules need to be placed in the folder `/home/secoverview/secoverview/secoverview/media/yararules/`. This example shows how to add the rules if there is direct access to the server.

All the following commands need to be run as an administrator!

First, get the YARA rules from abuse.ch:

```
wget https://yaraify.abuse.ch/yarahub/yaraify-rules.zip
```

After downloading, the rules need to be unzipped using the unzip command:

```
unzip yaraify-rules.zip -d /home/secoverview/secoverview/secoverview/media/yararules/
```

If the files are successfully unzipped, the service "secoverview.service" needs to be restarted:

```
systemctl restart secoverview.service
```

After adding the YARA rules, there is an option under Tools - YARA Scan to upload a file and scan it. After the scan, the result will be displayed under the document selection.

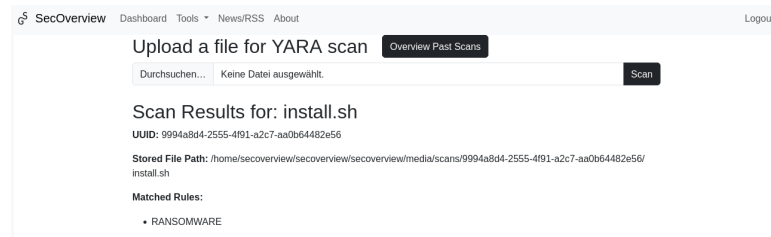


Figure 2: YARA Scan Result

5 NMAP Scan

With the help of the NMAP integration, the application is able to scan the network for assets. These assets are stored in a database along with the scan results. Under Tools - NMAP - Scans - Create Scan, a scan can be created. The following inputs are valid:

IP/Subnet: *192.168.1.1 or 192.168.1.0/24*

Scan Parameters: *All NMAP parameters, e.g., "-sV -n -R -p 1-1024"*

After running the scan, the scan results will be available under NMAP Overview - Scans - View.

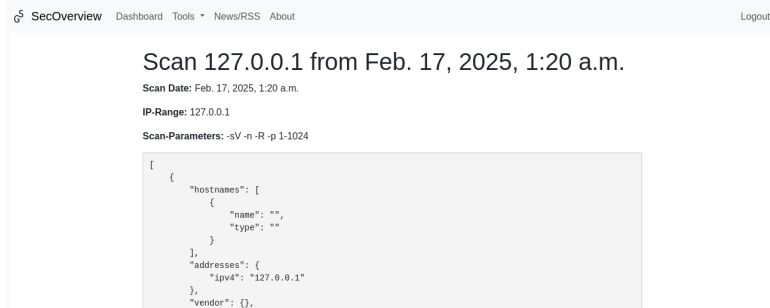


Figure 3: NMAP Scan

In the overview under Tools - NMAP, past scans and assets are visible.

6 IP Check

With the help of the IP Check, the ASN (BGP) data can be viewed. The IP Check app can be found under Tools - IP Check. Therefore, the data is fetched from bgpview.io and displayed:

SecOverview

DashboardToolsNews/RSSAbout

Logout

IP Check bgpview.io

IP:
8.8.8.8

Check

IP: 8.8.8.8

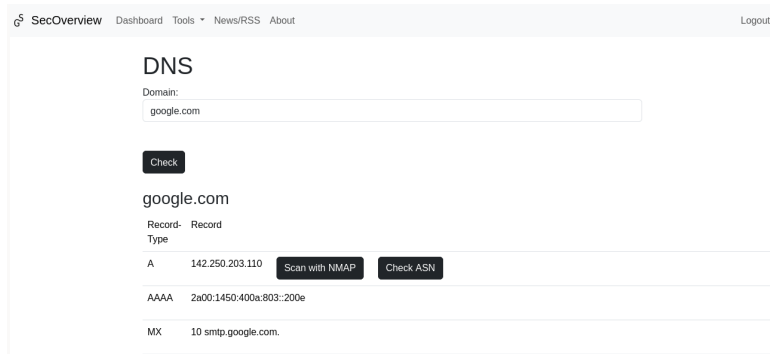
PTR Record: dns.google

Prefix	Name	Description	ASN	ASN-Name	ASN-Description	ASN-Country
8.8.8.0/24	GOGL	Google LLC	15169	GOOGLE	Google LLC	US
8.0.0.0/12	NET8	American Registry for Internet Numbers	3356	LEVEL3	Level 3 Parent, LLC	US
8.0.0.0/9	NET8	American Registry for Internet Numbers	3356	LEVEL3	Level 3 Parent, LLC	US

Figure 4: IP Check Result

7 DNS Operation

With the help of the DNS Operation, a DNS record can be queried and later analyzed or its values checked with other apps. The DNS Operation app can be found under Tools - DNS Operations. After a query, the following is returned:



The screenshot shows the 'DNS' section of the SecOverview application. At the top, there is a navigation bar with 'SecOverview', 'Dashboard', 'Tools', 'News/RSS', 'About', and a 'Logout' link. Below the navigation bar, the 'DNS' title is followed by a 'Domain:' label and a text input field containing 'google.com'. A 'Check' button is positioned below the input field. The results for 'google.com' are displayed below. A table shows DNS records with columns 'Record Type' and 'Record'. The first row shows an 'A' record with the value '142.250.203.110'. To the right of this value are two buttons: 'Scan with NMAP' and 'Check ASN'. The second row shows an 'AAAA' record with the value '2a00:1450:400a:803::200e'. The third row shows an 'MX' record with the value '10 smtp.google.com.'.

Record Type	Record
A	142.250.203.110
AAAA	2a00:1450:400a:803::200e
MX	10 smtp.google.com.

Figure 5: DNS Operation Result

8 Ransomware Data

The app Ransomware Data fetches the victims and ransomware groups from ransomware.live. To fetch the data, go to Tools - Ransomware Data and use the button ****Update Victims and Groups****. After updating the data, it is searchable in the Overview views.

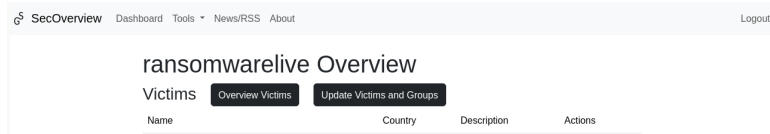


Figure 6: Ransomware Data Overview