Active mode using Nmap

With Dash framework

The goal of the active mode is to run a scan on the network to get informations such as IP addresses, open ports, running services and their versions, etc… All the informations can be visualised on a local web dashboard, made with Dash framework.

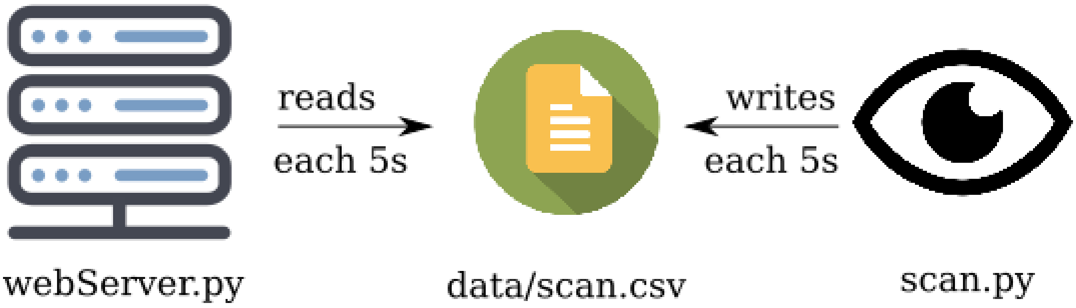
I. Presentation

The main idea is that we have two processes, (or maybe later two threads) that use a CSV file to read and write, periodically.

The first process, **scan.py** periodically runs a NMAP scan and writes the resulting informations in **data/scan.csv**. Some parameters can be adjusted, such as the network IP, the subnet mask, the period duration and the output file.

Once the CSV file has been written, it contains the following informations:

- IP - The IP of the scanned host
- Hostname - The hostname of the scanned host
- Protocol - The protocol (TCP/UDP) used
- Port - The opened ports on the scanned host
- Service - The services running on the ports
- Version - The versions of the services



From now, we assume the CSV file is filled with some informations. Those informations are read by the **webServer.py** process, and presented on a local web server, running on port 8050.

II. Pre-requisites

Download the Dash framwork for Python:

```
$ pip intall dash
$ pip install dash-html-components
$ pip install dash-core-components
$ pip install dash-table-experiment
$ pip install pandas
```

III. How to run it ?

Download or update your Git local repository, from here. Then simply run webServer.py and scan.py. All should be done automatically.

```
$ python webServer.py
$ python scan.py
```

To test the ability of the web server to refresh automatically, you can start services such as SSH and check if this is detected on the web interface.

```
$ service ssh start
```

IV. Future improvements

- Make the dashboard user friendly
- Add a view to group informations (by IP, by service, etc…)
- Analyse services version to check if the version is vulnerable
- …