SNARE Documentation

Release v0.3

mushmush

Jun 12, 2021

Contents:

CHAPTER 1

SNARE

Super Next generation Advanced Reactive honEypot

SNARE is a web application honeypot and is the successor of Glastopf, which has many of the same features as Glastopf as well as ability to convert existing Web pages into attack surfaces with TANNER. Every event sent from SNARE to TANNER is evaluated, and TANNER decides how SNARE should respond to the client. This allows the honeypot to produce dynamic responses which improves its camouflage. SNARE when fingerprinted by attackers shows that it is a Nginx Web application server.

1.1 Basic Concepts

- Surface first. Focus on the attack surface generation. Clone with `Cloner`.
- Sensors and masters. Lightweight collectors (SNARE) and central decision maker (tanner).

1.2 Getting started

You need Python3. We tested primarily with >=3.4

This was tested with a recent Ubuntu based Linux.

Steps to setup:

1. Get SNARE: `git clone https://github.com/mushorg/snare.git` and `cd snare`
2. [Optional] Make virtual environment: `python3 -m venv venv`
3. [Optional] Activate virtual environment: `. venv/bin/activate`

Note: Do not use sudo with below commands if you're running snare in virtual environment.

4. Install requirements: `sudo pip3 install -r requirements.txt`
5. Setup snare: `sudo python3 setup.py install`

6. Clone a page: `sudo clone --target http://example.com --path <path to base dir>`
7. Run SNARE: `sudo snare --port 8080 --page-dir example.com --path <path to base dir>` (See *Snare command line parameters* description for more info)
8. Test: Visit http://localhost:8080/index.html
9. (Optionally) Have your own tanner service running.

[Note : Cloner clones the whole website, to restrict to a desired depth of cloning add `--max-depth` parameter]

You obviously want to bind to 0.0.0.0 and port 80 when running in *production*.

Docker build instructions

1. Change current directory to `snare` project directory
2. `docker-compose build`
3. `docker-compose up`

More information about running `docker-compose` can be found here.

CHAPTER 2

Snare command line parameters

snare [**–page-dir** *folder*] [**–list-pages**] [**–host-ip**] [**–index-page** *filename*] [**–port** *port*] [**–interface** *ip_addr*] [**–debug**] [**–tanner** *tanner_ip**] [**–skip-check-version**] [**–slurp-enabled**] [**–slurp-host** *host_ip*] [**–slurp-auth**] [**–config** *filename*] [**–auto-update**] [**–update-timeout** *timeout*]

2.1 Description

- **page–dir** – name of the folder to be served
- **list–pages** – list available pages
- **host–ip** – host ip to bind to, default: localhost
- **index–page** – file name of the index page, default: index.html
- **port** – port to listen on, default: 8080
- **interface** – interface to bind to
- **debug** – run web server in debug mode, default: False
- **tanner** – ip of the tanner service, default: tanner.mushmush.org
- **skip–check-version** – skip check for update
- **slurp–enabled** – enable nsq logging
- **slurp–host** – nsq logging host, default: slurp.mushmush.org
- **slurp–auth** – nsq logging auth, default: slurp
- **config** – snare config file, default: snare.cfg
- **auto–update** – auto update SNARE if new version available, default: True
- **update–timeout** – update SNARE every timeout (possible labels are: **D** – day, **H** – hours, **M** – minutes), default: 24H
- **server–header** – set server header, default: nginx

CHAPTER 3

Cloner

Cloner clones the website that we require to be served by snare.

3.1 Cloner command line parameters

clone [**–target** *website_url*] [**–max-depth** *clone_depth*] [**–log_path** *LOG_PATH*] [**–css-validate** *CSS_VALIDATE*] [**–path** *PATH*]

3.2 Description

- **target** – url of website to be cloned
- **max–depth** – maximum depth of the web-pages desired to be cloned (optional), default: full depth of the site
- **log_path** – path of the log file (optional)
- **css-validate** – set wheather css validation is required (optional)
- **path** – path to save the page to be cloned (optional)

CHAPTER 4

Indices and tables

- genindex
- modindex
- search