snare Documentation

Release 0.2

viswak

Jul 30, 2018

Contents

Contents:

CHAPTER 1

SNARE

Super Next generation Advanced Reactive honEypot

1.1 Basic concept

- Surface first: Focus on the attack surface generation.
- Sensors and masters. Lightweight collector (SNARE) and central decision maker/emulator (TANNER).

1.2 Getting started

You need Python3. We tested primarily with >=3.4 This was tested with a recent Ubuntu based Linux.

- Get SNARE: `git clone https://github.com/mushorg/snare.git`
- Install requirements: `pip3 install -r requirements.txt`
- Clone a page: `sudo python3 clone.py --target http://example.com`
- Run SNARE: `sudo python3 snare.py --port 8080 --page-dir example.com` (See *Snare command line parameters* description for more info)
- Test: Visit `http://localhost:8080/index.html`
- (Optionally) Have your own tanner service running.

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

CHAPTER 2

Snare command line parameters

snare.py [**–page-dir** *folder*] [**–list-pages**] [**–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
- **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.py [**–target** *website_url*] [**–max-depth** *clone_depth*]

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

CHAPTER 4

Indices and tables

- genindex
- modindex
- search