EyeWitness 1.0 Cheatsheet (ingenieriainformatica.uniovi.es)

Tool used to capture screenshots from a list of URLs

https://www.fortynorthsecurity.com

```
################################################################################
#                                EyeWitness                                    #
################################################################################
#           FortyNorth Security - https://www.fortynorthsecurity.com           #
################################################################################

Starting Web Requests (2 Hosts)
Attempting to screenshot http://enol.si.uniovi.es
Attempting to screenshot http://zeus.etsimo.uniovi.es
[*] WebDriverError when connecting to http://enol.si.uniovi.es
Finished in 11.40915322303772 seconds

[*] Done! Report written in the /home/operario/2020-10-29_181423 folder!
Would you like to open the report now? [Y/n]
```

GENERAL USAGE

```
EyeWitness.py [--web] [-f Filename] [-x Filename.xml] [--single Single URL] [--no-dns] [--timeout Timeout] [--jitter # of Seconds] [--delay # of Seconds] [--threads # of Threads] [--max-retries Max retries on a timeout] [-d Directory Name] [--results Hosts Per Page] [--no-prompt] [--user-agent User Agent] [--difference Difference Threshold]  [--proxy-ip 127.0.0.1] [--proxy-port 8080] [--proxy-type socks5] [--show-selenium] [--resolve] [--add-http-ports ADD_HTTP_PORTS] [--add-https-ports ADD_HTTPS_PORTS][--only-ports ONLY_PORTS] [--prepend-https] [--selenium-log-path SELENIUM_LOG_PATH]  [--resume ew.db] [--ocr]
```

NOTES

For virustotal subdomains support you can setting your API KEY in the config.json file.

OPTIONS

Input Options

-f Filename: Line-separated file containing URLs to capture

--no-dns: Skip DNS resolution when connecting to websites

--single Single URL: Single URL/Host to capture

-x Filename.xml: Nmap XML or .Nessus file

Input Options

--web: HTTP Screenshot using Selenium

Timing Options

--delay # of Seconds: Delay between the opening of the navigator and taking the screenshot

--jitter # of Seconds: Randomize URLs and add a random delay between requests

--max-retries Max retries on a timeout: Max retries on timeouts

--threads # of Threads: Number of threads to use while using file based input

--timeout Timeout: Maximum number of sec. to wait while requesting a web page (Default: 7)

Report Output Options

-d Directory Name: Directory name for report output

--no-prompt: Don't prompt to open the report

--results Hosts Per Page: Number of Hosts per page of report

Web Options

--add-http-ports ADD_HTTP_PORTS: Comma-separated additional port(s) to assume are http (e.g. '8018,8028')

--add-https-ports ADD_HTTPS_PORTS: Comma-separated additional port(s) to assume are https (e.g. '8018,8028')

--difference Difference Threshold: Difference threshold when determining if user agent requests are close "enough" (Default: 50)

--only-ports ONLY_PORTS: Comma-separated list of exclusive ports to use (e.g. '80,8080')

--prepend-https: Prepend http:// and https:// to URLs without either

--proxy-ip 127.0.0.1: IP of web proxy to go through

--proxy-port 8080: Port of web proxy to go through

--proxy-type socks5: Proxy type (socks5/http)

--resolve: Resolve IP/Hostname for targets

--selenium-log-path SELENIUM_LOG_PATH: Selenium geckodriver log path

--show-selenium: Show display for selenium

--user-agent User Agent: User Agent to use for all requests

Resume Options

--resume ew.db: Path to db file if you want to resume

RDP Options

--ocr: Use OCR to determine RDP usernames

by José Manuel Redondo López