a2svREADME.md at master · hahwula2sv · GitH...

Saved to Dropbox • Aug 28, 2017, 8:26 AM



hahwul / a2sv

Code

Issues 3

Pull requests 2

Pulse



README md





1. A2SV?

Auto Scanning to SSL Vulnerability. HeartBleed, CCS Injection, SSLv3 POODLE, FREAK... etc

A. Support Vulnerability

[CVE-2007-1858] Anonymous Cipher [CVE-2012-4929] CRIME(SPDY) [CVE-2014-0160] CCS Injection [CVE-2014-0224] HeartBleed [CVE-2014-3566] SSLv3 POODLE

[PLAN] SSL ACCF
[PLAN] SSL Information Analysis

2. How to Install?

[CVE-2015-0204] FREAK Attack

[CVE-2015-4000] LOGJAM Attack

[CVE-2016-0800] SSLv2 DROWN

A. Download(clone) & Unpack A2SV

B. Dev Plan

git clone https://github.com/hahwul/a2sv.git cd a2sv

B. Install Python Package / OpenSSL

pip install argparse pip install netaddr

apt-get install openssl
C. Run A2SV

python a2sv.py -h

3. How to Use?

usage: a2sv [-h] [-t TARGET] [-tf TARGETFI]

```
optional arguments:
    -h, --help
                           show this help mes
    -t TARGET, --target TARGET
                           Target URL and IP
                            > e.g -t 127.0.0.
    -tf TARGETFILE, --targetfile TARGETFILE
                           Target file(list) |
                            > e.g -tf ./targe
    -p PORT, --port PORT
                           Custom Port / Defai
                            > e.g -p 8080
    -m MODULE, --module MODULE
                           Check SSL Vuln wit
                            [anonymous]: Anony
                            [crime]: Crime(SPD
                            [heart]: HeartBlee
                            [ccs]: CCS Injection
                            [poodle]: SSLv3 PO
                            [freak]: OpenSSL FI
                            [logjam]: OpenSSL :
                            [drown]: SSLv2 DRO
    -d DISPLAY, --display DISPLAY
                           Display output
                            [Y,y] Show output
                            [N,n] Hide output
    -u, --update
                           Update A2SV (GIT)
    -v, --version
                           Show Version
[Scan SSL Vulnerability]
  python a2sv.py -t 127.0.0.1
  python a2sv.py -t 127.0.0.1 -m heartbleed
  python a2sv.py -t 127.0.0.1 -d n
  python a2sv.py -t 127.0.0.1 -p 8111
```

python a2sv.py -tf target_list.txt

[Update A2SV]

python a2sv.py --update

4. Support

Submit New Issue(github)

Contact hahwul@gmail.com

5. Screen shot



```
[A2SV REPORT]
  P0RT]: 443
  SCAN TIME]: 2017-05-23 23:49:11.532711
 ulnerability
                  CVE
                                  CVSS v2 Base Score
                                                               State
Anonymous Cipher CVE–2007–1858 AV:N/AC:H/Au:N/C:P/I:N/A:N Not Vulnerable.
CRIME(SDPY)
                  CVE-2012-4929 AV: N/AC: H/Au: N/C: P/I: N/A: N Not Vulnerable.
HeartBleed
                  CVE-2014-0160 AV: N/AC: L/Au: N/C: P/I: N/A: N Not Vulnerable.
CCS Injection
                  CVE-2014-0224 AV: N/AC: M/Au: N/C: P/I: P/A: P Not Vulnerable.
SSLv3 P00DLE
                  CVE-2014-3566 AV: N/AC: M/Au: N/C: P/I: N/A: N Vulnerable!
                  CVE-2015-0204 AV: N/AC: M/Au: N/C: N/I: P/A: N Not Vulnerable.
OpenSSL FREAK
                  CVE-2015-4000 AV: N/AC: M/Au: N/C: N/I: P/A: N Not Vulnerable.
OpenSSL LOGJAM
                  CVE-2016-0800 AV: N/AC: M/Au: N/C: P/I: N/A: N Exception
SSLv2 DROWN
```

6. Code Reference Site

```
poodle:
https://github.com/supersam654/Poodle-Checker
heartbleed:
https://github.com/sensepost/heartbleed-poc
ccs injection:
https://github.com/Tripwire/OpenSSL-CCS-Inject-Test
freak:
https://gist.github.com/martinseener/d50473
228719a9554e6a
```



Desktop version