Onion Scan

Information Security Inc.

iSEC
information security inc.

Contents

- What is OnionScan?
- What is scanned for?
- Installing OnionScan
- Running OnionScan
- QuickStart
- References

What is OnionScan?

- OnionScan is a free and open source tool for investigating the Dark Web
- OnionScan goals => to help operators of hidden services find and fix operational security issues with their services
- OnionScan goals => to help researchers and investigators monitor and track Dark Web sites

What is scanned for?

- Web sites => Apache mod_status Leak, Open Directories, EXIF Tags, Server Fingerprint, Analytics IDs, PGP Identities
- SSH => OnionScan collected information about SSH endpoints including software versions and the SSH public key fingerprint
- FTP & SMTP => OnionScan collected information from other non-web servers, most notably software banners. These banners are often misconfigured to reveal information about the target server - including OS version, and sometimes hostnames and IP addresses

What is scanned for?

- Cryptocurrency Clients => OnionScan scans for common cryptocurrency clients including Bitcoin and Litecoin
- Protocol Detection => OnionScan also detects for the presence of many other protocols including IRC, XMPP, VNC & Ricochet

Installing OnionScan

- Getting Dependencies

```
go get github.com/HouzuoGuo/tiedot
go get golang.org/x/crypto/openpgp
go get golang.org/x/net/proxy
go get golang.org/x/net/html
go get github.com/rwcarlsen/goexif/exif
go get github.com/rwcarlsen/goexif/tiff
```

Installing OnionScan

- tor needs to be installed and running

```
           :~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
   Active: active (exited) since Wed 2018-02-14 10:34:10 JST; 37min ago
  Process: 7273 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 7273 (code=exited, status=0/SUCCESS)

Feb 14 10:34:10 kali2017 systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
Feb 14 10:34:10 kali2017 systemd[1]: Started Anonymizing overlay network for TCP (multi-instance-master).
```

Installing OnionScan

- Compile from git cloned source

```
go get github.com/s-rah/onionscan
go install github.com/s-rah/onionscan
```

Running OnionScan

- Compile from git cloned source

```
            :~/go/bin# pwd
/root/go/bin
            :~/go/bin# ./onionscan
Usage of ./onionscan:
    onionscan [flags] hiddenservice | onionscan [flags] --list list | onionscan --mode analysis
  -batch int
        number of onions to scan concurrently (default 10)
  -cookie string
        if provided, onionscan will use this cookie
  -crawlconfigdir string
        A directory where crawl configurations are stored
  -dbdir string
        The directory where the crawl database will be stored (default "./onionscandb")
  -depth int
        depth of directory scan recursion (default: 100) (default 100)
  -fingerprint
        true disables some deeper scans e.g. directory probing with the aim of just getting a fingerprint of the service. (default true)
  -jsonReport
        print out a json report providing a detailed report of the scan.
  -jsonSimpleReport
        print out a simple report as json, false by default
  -list string
        If provided OnionScan will attempt to read from the given list, rather than the provided hidden service
  -mode string
        one of scan or analysis. In analysis mode, webport must be set. (default "scan")
  -reportFile string
        the file destination path for report file - if given, the prefix of the file will be the scanned onion service. If not given, the report will be wr
itten to stdout
  -scans string
        a comma-separated list of scans to run e.g. web,tls,... (default: run all)
  -simpleReport
        print out a simple report detailing what is wrong and how to fix it, true by default (default true)
  -timeout int
        read timeout for connecting to onion services (default 120)
  -torProxyAddress string
        the address of the tor proxy to use (default "127.0.0.1:9050")
  -verbose
        print out a verbose log output of the scan
  -webport int
        if given, onionscan will expose a webserver on localhost:[port] to enabled searching of the database (default 8080)
```

QuickStart

```
           :~/go/bin# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
           :~/go/bin# service tor start
           :~/go/bin#
           :~/go/bin#
           :~/go/bin#
           :~/go/bin# netstat -anepl | less
           :~/go/bin# ./onionscan --verbose kpvz7kpmcmne52qf.onion
2018/02/13 20:15:29 Starting Scan of kpvz7kpmcmne52qf.onion
2018/02/13 20:15:29 This might take a few minutes..

2018/02/13 20:15:29 INFO: Checking kpvz7kpmcmne52qf.onion http(80)
2018/02/13 20:15:52 INFO: Found potential service on http(80)
2018/02/13 20:15:52 INFO: Starting to Scan Page: http://kpvz7kpmcmne52qf.onion/
2018/02/13 20:15:59 INFO: Grabbed 217 byte document
2018/02/13 20:15:59 INFO: Scanning URI: http://kpvz7kpmcmne52qf.onion/server-status
2018/02/13 20:16:02 INFO: Grabbed 162 byte document
2018/02/13 20:16:02 INFO: Scanning URI: http://kpvz7kpmcmne52qf.onion/private_key
2018/02/13 20:16:03 INFO: Grabbed 162 byte document
2018/02/13 20:16:03 INFO: Scanning Depth: 0
2018/02/13 20:16:03 INFO: Scanning URI: http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page
2018/02/13 20:16:06 INFO: Grabbed 28896 byte document
```

QuickStart

- Web scan

```
           ':~/go/bin# service tor start
           ':~/go/bin# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
   Active: active (exited) since Wed 2018-02-14 10:34:10 JST; 2s ago
  Process: 7273 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 7273 (code=exited, status=0/SUCCESS)

Feb 14 10:34:10 kali2017 systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
Feb 14 10:34:10 kali2017 systemd[1]: Started Anonymizing overlay network for TCP (multi-instance-master).
           :~/go/bin# pwd
/root/go/bin
           :~/go/bin# ./onionscan --verbose --scans web  kpvz7kpmcmne52qf.onion
2018/02/14 10:34:17 Starting Scan of kpvz7kpmcmne52qf.onion
2018/02/14 10:34:17 This might take a few minutes..

2018/02/14 10:34:17 INFO: Checking kpvz7kpmcmne52qf.onion http(80)



--------------- OnionScan Report ---------------
Generating Report for: kpvz7kpmcmne52qf.onion

No risks were found.
```

QuickStart

- OnionScan database

```
            :~/go/bin# pwd
/root/go/bin
            :~/go/bin# stat onionscandb/
  File: onionscandb/
  Size: 4096            Blocks: 8          IO Block: 4096   directory
Device: 801h/2049d      Inode: 6243356     Links: 4
Access: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2018-02-13 20:15:29.459695420 +0900
Modify: 2018-02-13 20:14:44.948259472 +0900
Change: 2018-02-13 20:14:44.948259472 +0900
 Birth: -
```

QuickStart

- OnionScan database

```
             :~/go/bin# cd onionscandb/
             :~/go/bin/onionscandb# pwd
/root/go/bin/onionscandb
             :~/go/bin/onionscandb# ls -ahl
total 24K
drwx------ 4 root root 4.0K Feb 13 20:14 .
drwxr-xr-x 3 root root 4.0K Feb 13 20:14 ..
drwx------ 3 root root 4.0K Feb 13 20:14 crawls
-rw-r--r-- 1 root root  121 Feb 13 20:14 data-config.json
-rw------- 1 root root    1 Feb 13 20:14 number_of_partitions
drwx------ 6 root root 4.0K Feb 13 20:14 relationships
```

QuickStart

- OnionScan database

```
            :~/go/bin/onionscandb/crawls# pwd
/root/go/bin/onionscandb/crawls
            :~/go/bin/onionscandb/crawls# ls -alh
total 65M
drwx------ 3 root root 4.0K Feb 13 20:14 .
drwx------ 4 root root 4.0K Feb 13 20:14 ..
-rw------- 1 root root  32M Feb 14 10:54 dat_0
-rw------- 1 root root  32M Feb 14 10:54 id_0
drwx------ 2 root root 4.0K Feb 13 20:14 URL
            :~/go/bin/onionscandb/crawls# strings dat_0 | less
{"Page":{"Status":200,"Headers":{"Connection":["keep-alive"],"Content-Type":["text/html; charset=UTF-8"],"Date":["Tue, 13 Feb 2018 11:15
:59 GMT"],"Server":["nginx"]},"Title":"Hello!","Forms":null,"Images":null,"Anchors":[{"Target":"http://kpvz7kpmcmne52qf.onion/wiki/index
.php/Main_Page","Title":"","Class":"","Text":"Hidden Wiki"}],"Links":null,"Scripts":null,"Snapshot":"\u003chead\u003e\n\u003cmeta http-e
quiv=\"Content-Type\" content=\"text/html; charset=utf8\" /\u003e\n\u003ctitle\u003eHello!\u003c/title\u003e\n\u003c/head\u003e\n\n\u003
cbody\u003e\n\u003cp\u003eLooking for the Uncensored \u003ca href=\"/wiki/index.php/Main_Page\"\u003eHidden Wiki\u003c/a\u003e?\u003c/p\
u003e\n\u003c/body\u003e\n\u003c/html\u003e\n","Raw":null,"Hash":""},"Timestamp":"2018-02-13T20:15:59.385434377+09:00","URL":"http://kpv
z7kpmcmne52qf.onion/"}

{"Page":{"Status":404,"Headers":{"Connection":["keep-alive"],"Content-Type":["text/html"],"Date":["Tue, 13 Feb 2018 11:16:01 GMT"],"Serv
er":["nginx"]},"Title":"404 Not Found","Forms":null,"Images":null,"Anchors":null,"Links":null,"Scripts":null,"Snapshot":"\u003chtml\u003
e\r\n\u003chead\u003e\u003ctitle\u003e404 Not Found\u003c/title\u003e\u003c/head\u003e\r\n\u003cbody bgcolor=\"white\"\u003e\r\n\u003cce
nter\u003e\u003ch1\u003e404 Not Found\u003c/h1\u003e\u003c/center\u003e\r\n\u003chr\u003e\u003ccenter\u003enginx\u003c/center\u003e\r\n\
u003c/body\u003e\r\n\u003c/html\u003e\r\n","Raw":null,"Hash":""},"Timestamp":"2018-02-13T20:16:02.42568607+09:00","URL":"http://kpvz7kpm
cmne52qf.onion/server-status"}
```

References

- GitHub
https://github.com/s-rah/onionscan

- OnionScan Doc (Whats scanned)
https://github.com/s-rah/onionscan/blob/master/doc/what-is-scanned-for.md

- OnionScan Doc
https://github.com/s-rah/onionscan/blob/master/doc/