

Masscan Basics

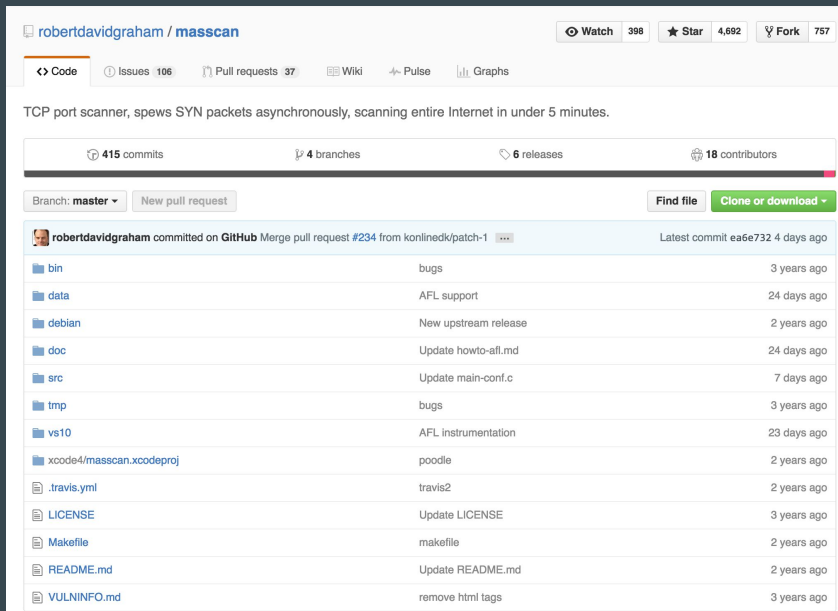
...

How to Get C&Ds Without Download 4Chan Porn

What Is It

<http://blog.erratasec.com/>

<https://github.com/robertdavidgraham/masscan>



The screenshot shows the GitHub repository page for `robertdavidgraham / masscan`. At the top, it displays repository statistics: 398 Watchers, 4,692 Stars, and 757 Forks. Below this, navigation tabs include Code, Issues (106), Pull requests (37), Wiki, Pulse, and Graphs. A description states: "TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes." Repository statistics show 415 commits, 4 branches, 6 releases, and 18 contributors. The main content area shows a list of files and folders with their last commit dates:

File/Folder	Last Commit
bin	bugs 3 years ago
data	AFL support 24 days ago
debian	New upstream release 2 years ago
doc	Update howto-afl.md 24 days ago
src	Update main-conf.c 7 days ago
tmp	bugs 3 years ago
vs10	AFL instrumentation 23 days ago
xcode4/masscan.xcodeproj	poodle 2 years ago
.travis.yml	travis2 2 years ago
LICENSE	Update LICENSE 3 years ago
Makefile	makefile 2 years ago
README.md	Update README.md 2 years ago
VULNINFO.md	remove html tags 3 years ago

“TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.”

Why That Thing

When you want to scan a whole bunch of things for just one thing

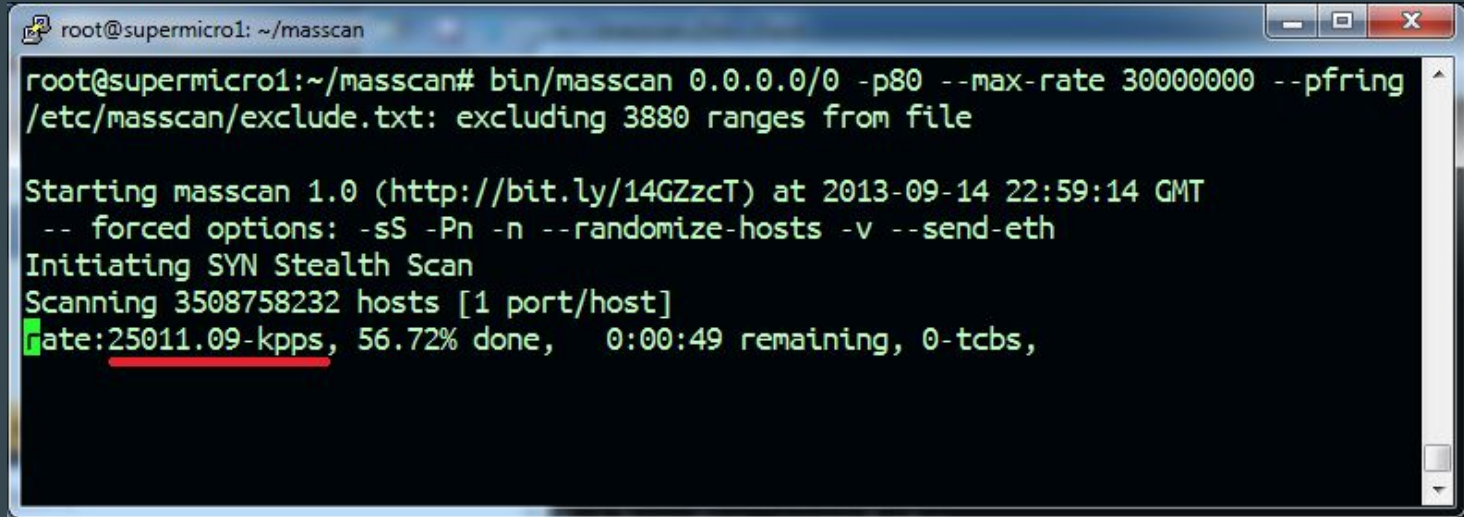
No really, it's nmap but for just one port

But for the entire internet



The Interwebz You Say?

In 5 minutes you say? Not really. Speeds are dependant on local network, operating system, number of visible sunspots

A terminal window titled 'root@supermicro1: ~/masscan' with standard window controls. The terminal shows the execution of the 'bin/masscan' command with various options. The output includes the exclusion of 3880 ranges from a file, the start time of the scan, the scan type (SYN Stealth Scan), the number of hosts being scanned, and the current progress (56.72% done) and estimated time remaining (0:00:49).

```
root@supermicro1: ~/masscan
root@supermicro1:~/masscan# bin/masscan 0.0.0.0/0 -p80 --max-rate 30000000 --pfring
/etc/masscan/exclude.txt: excluding 3880 ranges from file

Starting masscan 1.0 (http://bit.ly/14GZzcT) at 2013-09-14 22:59:14 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 3508758232 hosts [1 port/host]
Rate: 25011.09-kpps, 56.72% done, 0:00:49 remaining, 0-tcps,
```

How I Do This Thing?

```
$ sudo apt-get install git gcc make libpcap-dev
```

```
$ git clone https://github.com/robertdavidgraham/masscan
```

```
$ cd masscan
```

```
$ make
```

How I Do This Thing...And Use It

```
$ ./masscan -help
```

usage:

```
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000    ## scan some web ports on 10.x.x.x at 10kpps
```

```
masscan --nmap    ## list those options that are compatible with nmap
```

```
masscan -p80 10.0.0.0/8 --banners -oB <filename>    ## save results of scan in binary format to  
<filename>
```

```
masscan --open --banners --readscan <filename> -oX <savefile>    ## read binary scan results in  
<filename> and save them as xml in <savefile>
```

Just the Tips and Tricks

OMG Use:

```
--rate    ##    Limits the rate at which you spew SYN packets
```

```
--excludefile  ##  Put internet/ip blocks that you never ever want to scan
```

```
-oG  ##  like nmap, write that shit to a file for later
```

Demo