## Bro stuff

Justin Azoff

Aug 4, 2015

# try.bro.org on github

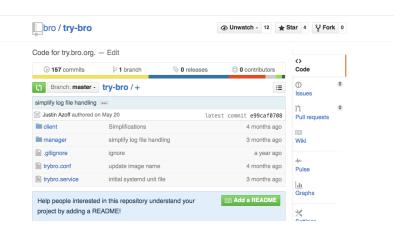


Figure: try.bro on github

# Bro Dockerfiles on github

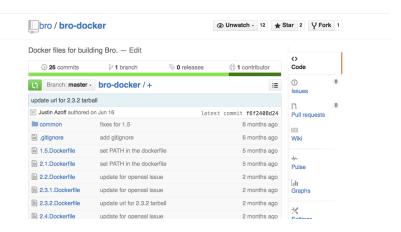


Figure: try.bro on github

## try.bro.org CORS

- CORS is enabled on API endpoints.
- http: //www.ncsa.illinois.edu/People/jazoff/bro.html

#### **BHR**

New implemenation of a BlackHole Router with bro integration.

```
▶ https://github.com/JustinAzoff/bhr-site
  https://github.com/JustinAzoff/bhr-bro
Use:
@load ./bhr-bro
redef BHR::block_types += {
    Scan::Port_Scan,
    Scan::Address_Scan,
};
```

### Fuzz

► Let's fuzz bro!

#### Fuzz

- Let's fuzz bro!
- ▶ Basic approach yields 1.8 executions/second too slow
- ► Tabled for a while.

#### Fuzz take 2

New features to the rescue:

```
afl-fuzz persistent mode http://lcamtuf.blogspot.com/2015/06/new-in-afl-persistent-mode.html \\
```

Hack up bro and try again:

```
src/Net.cc | 12 ++++++----
src/main.cc | 25 ++++++++++++++---
2 files changed, 29 insertions(+), 8 deletions(-)
```

#### Fuzz take 2

New features to the rescue:

afl-fuzz persistent mode http://lcamtuf.blogspot.com/2015/06/new-in-afl-persistent-mode.html

Hack up bro and try again:

```
src/Net.cc | 12 ++++++----
src/main.cc | 25 ++++++++++++++---
2 files changed, 29 insertions(+), 8 deletions(-)
```

Result: 1000+ executions/second.

#### Fuzz take 2

```
New features to the rescue:
afl-fuzz persistent mode
http://lcamtuf.blogspot.com/2015/06/new-in-afl-persistent-
mode.html
Hack up bro and try again:
src/Net.cc | 12 ++++++----
2 files changed, 29 insertions(+), 8 deletions(-)
Result: 1000+ executions/second.
But no crashes :(
```

#### TODO: Fuzz take 3

Need to build a test bro binary that bypasses libpcap and basic tcp reassembly to feed data directly into analyzers.

#### Fuzz Detour

Maybe I should try something simpler like bro-cut.

#### Fuzz Detour

Maybe I should try something simpler like bro-cut.

```
american fuzzy lop 1.83b (buqqy_bro-cut)
     process timina -
                                                                                                                                           --- overall results -
                     run time : 0 days. 0 hrs. 19 min. 9 sec
                                                                                                                                          | cvcles done : 1
        last new path: 0 days, 0 hrs, 0 min, 22 sec | total paths: 100
    last unia crash : 0 days, 0 hrs, 0 min, 20 sec
                                                                                                                                            | uniq crashes : 2
      last uniq hang: 0 days, 0 hrs, 8 min, 51 sec
                                                                                                                                                      uniq hangs: 13
    cycle progress -
      now processing: 98* (98.00%)
                                                                                                             map density: 138 (0.21%)
    paths timed out : 0 (0.00%) | count coverage : 4.69 bits/tuple
- stage progress ----
                                                                                            ---- findinas in depth -----
     now trving : havoc
                                                                                             | favored paths : 8 (8.00%)
    stage execs: 29.9k/30.0k (99.50%) | new edges on: 8 (8.00%)
    total execs: 1.21M
                                                         | total crashes : 2 (2 unique)
                                                                                                | total hangs : 10.2k (13 unique)
      exec speed: 1290/sec

→ fuzzing strategy yields 

→ path geometry

→ path 
        bit flips : 11/27.2k, 0/27.2k, 0/27.2k
                                                                                                                                          levels: 5
      byte flips: 0/3405, 0/3331, 1/3279
                                                                                                                                         | pendina: 74
    arithmetics: 10/187k, 0/41.3k, 0/142
                                                                                                                                     pend fav: 0
      known ints: 0/17.5k, 0/92.9k, 0/144k
     dictionary: 0/0, 0/0, 13/22.5k
                                                                                                                                          | imported : n/a
                  havoc: 53/578k, 0/0
                                                                                                                                            variable : 0
                    trim: 50.12%/1871, 1.39%
                                                                                                                                                                              Гcpu: 50%7
```

Figure: bro-cut fuzz crashes

## bro-cut bugs

### Failed conversion of out of range or invalid timestamps

### File header contains a missing or null separator

```
#separator
#fields a
hi

#separator \x00
#fields a
hi
```

### bro-cut bugs -=2

```
american fuzzy lop 1.83b (bro-cut)
process timing -
                                                 --- overall results ---
       run time : 0 days, 13 hrs, 39 min, 44 sec
                                                 | cycles done : 210
 last new path : 0 days, 12 hrs, 52 min, 34 sec
                                                 | total paths : 160
last uniq crash : none seen yet
                                                 I unia crashes: 0
 last unia hana : 0 davs. 0 hrs. 31 min. 47 sec
                                                    unia hanas : 9
⊢ cycle progress ----- map coverage -----
now processing : 1* (0.62%)
                                      map density: 141 (0.22%)
paths timed out : 0 (0.00%)
                                  | count coverage : 6.05 bits/tuple
+ findings in depth -----
 now trying : splice 11
                                  | favored paths : 9 (5.62%)
 stage execs : 210/500 (42.00%)
                                  new edges on: 9 (5.62%)
 total execs: 75.7M
                                  1 total crashes : 0 (0 unique)
                                     total hangs: 123 (9 unique)
  exec speed: 1543/sec

→ fuzzing strategy yields -----

                                               --- path aeometry
bit flips : 2/117k, 0/117k, 0/117k
                                                    levels: 9
byte flips : 0/14.7k, 0/14.7k, 0/14.6k
                                                pending: 0
| arithmetics : 0/821k, 0/221k, 0/770
                                                pend fav: 0
 known ints: 0/74.5k, 0/408k, 0/642k
                                                I own finds: 42
dictionary: 0/0, 0/0, 0/246k
                                                  imported : n/a
      havoc: 37/26.0M, 2/46.9M
                                                   variable: 0
       trim: 42.30%/18.4k, 0.00%
```

Figure: bro-cut fuzz success