Bro stuff

Justin Azoff

Aug 4, 2015
Figure: try.bro on github
Bro Dockerfiles on github

Figure: try.bro on github
CORS is enabled on API endpoints.

http://www.ncsa.illinois.edu/People/jazoff/bro.html
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,
};
Let’s fuzz bro!
Fuzz

- Let’s fuzz bro!
- Basic approach yields 1.8 executions/second - too slow
- Tabled for a while.
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(-)
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 +++++++++++-
src/main.cc | 25 ++++++++++++++++++++++++--
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.

Figure: bro-cut fuzz crashes
Failed conversion of out of range or invalid timestamps

#fields ts
#types  time
77777777777777777

File header contains a missing or null separator

#separator
#fields a
hi

#separator \x00
#fields a
hi
bro-cut bugs == 2

**Figure**: bro-cut fuzz success