The Bro Package Manager and You

Seth Hall
Chief Evangelist
Corelight, Inc
About Me

• Incident Responder
• Detection-Response Architect
• Core Bro developer
• Co-founder & Chief Evangelist

Bro at all of them!
Funded by
mozilla
aux/plugins?

NOTE: We no longer maintain any Bro plugins here. Most of the plugins that used to be available here have been moved over to use the Bro Package Manager instead. See https://github.com/bro/packages for a list of Bro packages currently available.
NOTE: We no longer maintain any Bro plugins here. Most plugins that used to be available here have been moved to the Bro Package Manager instead. See https://github.com/bro/bro/package for a list of Bro packages currently available.
Simple to install

$ sudo pip install bro-pkg

More complete docs...
Configure and Integrate

• If Bro isn’t in your path…

  • $ export PATH=/opt/bro/bin/:$PATH
  
  • $ mkdir ~/.bro-pkg
  
  • $ bro-pkg autoconfig > ~/.bro-pkg/config
  
  • @load packages

• You may need to deal with some permission issues, but it’s documented! Please take a look at the docs!
Bundles for DevOps

$ bro-pkg bundle my-stuff.bundle
Move my-stuff.bundle over to another machine...

$ bro-pkg unbundle my-stuff.bundle
Bundles for DevOps

$ bro-pkg bundle my-stuff.bundle

Move my-stuff.bundle over to another machine...

$ bro-pkg unbundle my-stuff.bundle
What’s out there?

• Update the local list of global packages
  • $ bro-pkg refresh

• Get the list of packages
  • $ bro-pkg list all
What's out there?

bro/0xxon/bro-postgresql
bro/0xxon/bro-sumstats-counttable
bro/corelight/bro-drwatson
bro/corelight/bro-hardware
bro/corelight/bro-long-connections
bro/corelight/bro-shellshock
bro/corelight/bro-xor-exe-plugin
bro/corelight/top-dns
bro/dopheide/bro_notice_correlation
bro/dopheide/venom
bro/hhzzk/dns-tunnels
bro/hosom/file-extraction
bro/hosom/log-filters
bro/initconf/CVE-2017-5638_struts
bro/initconf/CVE-2017-5638_struts.git
bro/initconf/phish-analysis
bro/initconf/scan-NG
bro/initconf/smtp-url-analysis
bro/j-gras/add-json
bro/j-gras/bro-af_packet-plugin
bro/j-gras/bro-lognorm
bro/j-gras/intel-extensions
bro/joesecurity/Joe-Sandbox-Bro
bro/jonzeolla/scan-sampling
bro/jsiwek/bro-test-package
bro/jswaro/tcprs
bro/ncsa/bro-doctor
bro/ncsa/bro-interface-setup
bro/ncsa/bro-is-darknet
bro/ncsa/bro-simple-scan
bro/pgaulon/bro-notice-slack
bro/scebro/ldap-analyzer
bro/setthall/bro-brainfuck
bro/setthall/bro-myricom
bro/setthall/credit-card-exposure
bro/setthall/domain-tld
bro/setthall/ssn-exposure
bro/setthall/unknown-mime-type-discovery
bro/srozb/dns_axfr
bro/theflakes/bro-large_uploads
What’s out there?

40 Packages!

bro/0xxon/bro-postgresql
bro/0xxon/bro-sumstats-counttable
bro/corelight/bro-drwatson
bro/corelight/bro-hardware
bro/corelight/bro-long-connections
bro/corelight/bro-shellshock
bro/corelight/bro-xor-exe-plugin
bro/corelight/top-dns
bro/dopheide/bro_notice_correlation
bro/dopheide/venom
bro/hhzzk/dns-tunnels
bro/hosom/file-extraction
bro/hosom/log-filters
bro/initconf/CVE-2017-5638_struts
bro/initconf/CVE-2017-5638_struts.git
bro/initconf/phish-analysis
bro/initconf/scan-NG
bro/initconf/smtp-url-analysis
bro/j-gras/add-json
bro/j-gras/bro-af_packet-plugin
bro/j-gras/bro-lognorm
bro/j-gras/intel-extensions
bro/joesecurity/Joe-Sandbox-Bro
bro/jonzeolla/scan-sampling
bro/jsiwek/bro-test-package
bro/jswaro/tcprs
bro/ncsa/bro-doctor
bro/ncsa/bro-interface-setup
bro/ncsa/bro-is-darknet
bro/ncsa/bro-simple-scan
bro/pgaulon/bro NOTICE slack
bro/scebro/ldap-analyzer
bro/setthall/bro-brainfuck
bro/setthall/bro-myricom
bro/setthall/credit-card-exposure
bro/setthall/domain-tld
bro/setthall/ssn-exposure
bro/setthall/unknown-mime-type-discovery
bro/srozb/dns AXFR
bro/theflakes/bro-large uploads
corelight/bro-long-connections

New log: conn_long.log

$ bro-pkg install corelight/bro-long-connections
joesecurity/Joe-Sandbox-Bro

Upload files to a JOE Sandbox

$ bro-pkg install joesecurity/Joe-Sandbox-Bro
module JoeSandbox;

export {

    # Joe Sandbox api key
    const apikey: string = "YOUR_API_KEY" &redef;

    # Joe Sandbox api url
    # const apiurl: string = "http://example.net/joesandbox/index.php/api/";
    const apiurl: string = "https://jbxcloud.joesecurity.org/api/" &redef;

    # Please accept the Joe Sandbox Cloud Terms and Conditions if you are
    # using Joe Sandbox Cloud.
    # https://jbxcloud.joesecurity.org/download/termsandconditions.pdf
    const accept_tac: bool = F &redef;
}
sethhall/unknown-mime-type-discovery

New log: unknown_mime_type_discovery.log

$ bro-pkg install sethhall/unknown-mime-type-discovery
ncsa/bro-doctor

BroCtl plugin to help diagnose problems

$ bro-pkg install ncsa/bro-doctor
pgaulon/bro-notice-slack

Notice action to send notices to Slack.

$ bro-pkg install pgaulon/bro-notice-slack
Future

Rethink how configuration works

Rethinking how parts of Bro are distributed

Bro Package Manager website
(or type “bro package manager” into google)