Bro - Configuration and Tuning
EDUCAUSE 2016

Vlad Grigorescu

vladg@illinois.edu
National Center for Supercomputing Applications

1460993400.000
(Mon Apr 18 08:30:00 PDT 2016)
Finding the documentation for a given record, event, etc.

Bro scripts are parsed and documentation is auto-generated.

For current (stable and git master) documentation, see:

- https://www.bro.org/sphinx/index.html
- https://www.bro.org/sphinx-git/index.html
Documentation is split into 4 main sections

**Introduction Section**
Covers general Bro and cluster concepts, installation and a quick-start guide. Can be thought of as the "sysadmin guide."

**Using Bro Section**
Covers how to work with log files, specific IR use-cases, and how to write some basic Bro scripts. Can be thought of as the "incident responder guide."

**Reference Section**
Mostly comprised of auto-generated documentation. This is the "power user reference guide."
Development Section

Information and guides for specific development tasks (like writing a custom Bro plugin). In combination with https://www.bro.org/development/index.html, this creates the "developer guide."
Index and Search

Two features that are often ignored is the documentation index and search.

- [https://www.bro.org/sphinx/genindex.html](https://www.bro.org/sphinx/genindex.html)
  The index is your best reference for quickly finding information about a specific built-in function, event or record type.

- [https://www.bro.org/sphinx/search.html](https://www.bro.org/sphinx/search.html)
  Finally, the search is the most open-ended reference method – searching the documentation and the scripts (including comments).
Example queries

1. "What does the `trans_depth` field of the HTTP log represent?"
   Searching the documentation for `trans_depth` leads to:
   ```plaintext
   trans_depth: count & log
   Represents the pipelined depth into the connection of this request/response transaction.
   ```

2. "What events does the SSH analyzer generate?"
   Documentation ⇒ Script Reference ⇒ Protocol Analyzers. The table of contents at the top list all the protocol analyzers, including `Bro::SSH`. Clicking on that link, lists the SSH record types and the events associated with the analyzer.

3. "What’s the syntax for defining a port, again?"
   Documentation ⇒ Script Reference ⇒ Types, which has information on each built-in type.
Architecture overview
Cluster topology and how to start the Bro processes?

node.cfg Example

```bash
> cat $BRO_PREFIX/etc/node.cfg

[manager]
type=manager
host=172.19.5.89

[worker-1]
type=worker
host=172.19.5.87
interface=eth5
lb_method=myricom
lb_procs=12
pin_cpus=2,3,4,5,6,7,8,9,10,11,12,13
env_vars="LD_PRELOAD=/opt/snf/lib/libsnf.so.0"
```
> cat $BRO_PREFIX/etc/broctl.cfg

# Recipient address for all emails send out by Bro
MailTo = vladg@illinois.edu

# Location of the log directory.
LogDir = /var/opt/bro/logs

# Rotation interval in seconds for log files on manager node.
LogRotationInterval = 3600
Local Networks

networks.cfg Example

> cat $BRO_PREFIX/etc/networks.cfg

# List of local networks in CIDR notation, 
# optionally followed by a descriptive tag.

2620:0:0c80::/48 NCSA IPv6
141.142.0.0/16 NCSA IPv4
143.219.0.0/16 NCSA Super-Secret IPv4
10.142.0.0/16 NCSA internal
10.5.0.0/16 NCSA internal (Blue Waters)
172.24.0.0/13 NCSA internal
198.17.196.0/25 NCSA out of band SafetyNet
209.201.74.0/23 Access Center
How does Bro load scripts? I

<table>
<thead>
<tr>
<th>Script Load Order</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 base/init-bare.bro</td>
<td>Type definitions, records generated in C++.</td>
</tr>
<tr>
<td>2 base/init-default.bro</td>
<td>Loads base/*. Disabled with --bare-mode (-b)</td>
</tr>
<tr>
<td>3 site/local.bro</td>
<td>Local site policy. site/* will not be overwritten when upgrading or reinstalling!</td>
</tr>
<tr>
<td>4 broctl/main.bro</td>
<td>Misc. cluster settings (e.g. disable stderr.)</td>
</tr>
<tr>
<td>5 base/frameworks/cluster</td>
<td>Cluster support</td>
</tr>
<tr>
<td>6 site/local-manager.bro</td>
<td>Local site policy loaded only by specific node types. (or local-worker, etc)</td>
</tr>
<tr>
<td>7 broctl/auto.bro</td>
<td>Broctl generated settings (e.g. local-networks)</td>
</tr>
</tbody>
</table>
How does Bro load scripts? II

local.bro Examples

# FTP
@load protocols/ftp/software
@load protocols/ftp/detect
@load site/protocols/ftp/port_mismatch
redef FTP::default_capture_password = T;
redef FTP::logged_commands += {"USER"};
How do I load and configure a script?

Find a script

Bro documentation ⇒ Script Reference ⇒ Bro Script Index

Find the documentation

Options

SMTP::suspicious_origination_countries
Type: set [string]
Attributes: &redef
Default: {}

Places where it's suspicious for mail to originate from represented as all-capital, two character country codes (e.g., US). It requires libGeoIP support built in.

SMTP::suspicious_origination_networks
Type: set [subnet]
Attributes: &redef
How do I load and configure a script? II

Add it to local.bro

@load protocols/smtp/detect-suspicious-orig.bro

redef SMTP::suspicious_origination_countries = {
    "BT", # Bhutan
    "BW", # Botswana
    "CD", # Congo, The Democratic Republic of the
    "CI", # Cote d’Ivoire
    # ...
};

redef SMTP::suspicious_origination_networks = {
    208.66.194.0/24 # McColo, Inc.
};
This is a "hook" which is executed when Bro processes a notice. A hook is similar to an event.
If a hook handler modifies a parameter, it’s modified for subsequent code paths.
Notice::policy Hook short circuit

If a hook handler returns false, further handlers are not called.
Whitelist a host entirely

```cpp
hook Notice::policy(n: Notice::Info)
{
  if ( n?$id && n$id?$id_orig_h &&
       n$id$orig_h == 141.142.148.8 )
    return F;
}
```

Whitelist host + notice type

```cpp
hook Notice::policy(n: Notice::Info)
{
  if ( n$id$orig_h == 141.142.148.8 &&
       n$note == SSH::Login )
    return F;
}
```
Blacklist host + notice type

```cpp
hook Notice::policy(n: Notice::Info) {
    if ( n$id$orig_h == 141.142.148.8 &&
         n$note == SSH::Login )
        add n$actions[Notice::ACTION_BHR];
}
```
<table>
<thead>
<tr>
<th>Section</th>
<th>Documentation Links</th>
</tr>
</thead>
</table>
| Architecture, Quick Start     | Documentation ⇒ Bro Cluster Architecture  
                              | Documentation ⇒ Quick Start Guide                      |
| Config Files                  | Documentation ⇒ Cluster Configuration ⇒ Basic Cluster Configuration |
| Hooks                         | Documentation ⇒ Script Reference ⇒ Types                |
| Notice Framework              | Documentation ⇒ Frameworks ⇒ Notice Framework           |