The Bro Network Security Monitor

Abstract

Bro is an open-source network security platform that illuminates your network's activity in detail, with the stability and flexibility for production deployment at scale.

Bro reduces incoming packet streams into higher-level events and applies customizable scripts to determine the necessary course of action. This simple design allows you to configure an array of real-time alerts, execute arbitrary programs on demand, and log data for later use.

[1] https://www.bro.org/why_choose_bro.pdf

Where to Acquire

Installed in the Security511 Linux VM.

Web site is: https://www.bro.org/

Examples/Use Case

Run bro against a pcap, create bro log files in the current directory. Some of following logs files may be created, dpending on the pcap content:

- conn.log
- dns.log
- files.log
- http.log
- irc.log
- packet_filter.log
- ssl.log
- weird.log

```
$ bro -r /pcaps/virut-worm.pcap
```

Carve executables from a file:

```
$ sudo bro -r /pcaps/virut-worm.pcap /opt/bro/share/bro/file-extraction/extract.bro
$ ls -la /nsm/bro/extracted
```

Carve multiple file types: exe, txt, jpg, png, html and "other" (uses the extension .xxx):

```
$ sudo bro -r /pcaps/virut-worm.pcap /opt/bro/share/bro/file-extraction/extract-all.bro
$ ls -la /nsm/bro/extracted
```

Display x.509 issuer subjects:

```
$ bro -C -r /pcaps/normal/https/alexa-top-500.pcap
$ cat ssl.log | bro-cut issuer_subject
```

Additional Info