bro - what is in my network?

Dobrica Pavlinušić, HULK
Valentino Šefer
What is Bro?

- Flexible network security monitor with event correlation
- Traffic inspection
- Attack detection
- Log recording
- Distributed analysis
- Full programmability

- Bro decodes **protocols** on your network
- Generates nice and structured log files based on protocol, with uid for correlation
- Ground-truth about your network (it comes from packets on it, after all)
- **It doesn't depend on signatures or ports of traffic to find out what it is**
- It can be used with content hashing and lists like [https://intel.criticalstack.com/](https://intel.criticalstack.com/) to detect known bad actors.
- It can use pcap files or live traffic
- Event based, bind to them from external process (e.g. `iptables -j DROP`)
- Bro script is DSL for network analysis which IDS in implemented in (using 400+ scripts)

---

**Every powerful tool can be used for good and evil.**
If you don't care about state of your network, you might want to know what "metadata" network operators can collect about you as user.
Security onion

-ETOOMUCHWORK (or: "I don't want to do all this manually")

https://securityonion.net/

Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It’s based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

In this talk, we don't care about Snort, Suricata, only about Bro and don't care about Web UI.
Do you know your network?

We are university setting running wired and wifi network for our users.

Multiple buildings (1Gbps uplink, 1Gbps link between buildings, 2-6Gbps backbone aggregation - we can DoS our uplink from inside!)

~3100 active IP addresses

~53 smart switches

~1900 network ports

~30 vlans

~40 wifi APs

~1300 wifi users per day <10% @5GHz

~11000 user accounts
So, you need machine for bro....

Commodity Dell hardware OptiPlex 7040

i7-6700 CPU 3.40GHz (bro uses 4 cores ~2GHz)

2 port Intel 82575EB Gigabit Network

You will need 3GHz to process 1Gbps traffic with pf_ring to calculate content hashing

Same machine is used as master and logger.

Our bro config is not optimal, but does work for us and shows how useful bro is.

You should have separate bro master node and multiple workers, but we don't have that.
Network infrastructure

- Mikrotik CCR-1036-8G-2S+
- Dell PowerConnect 6024
- Dell PowerConnect 6024F
- Dell PowerConnect 5548

- TP-Link WDR4300 + Lede FFZG build
- Workstations

- Dell Optiplex 7040
  - i7 6700
  - 16GB DDR4
  - 250GB NVMe SSD
  - 2x1G Intel NIC
Dell PowerConnect 6024 port mirror

interface ethernet g2
description sw-dpc-ffzg-local

interface ethernet g22
description sw-lib

interface ethernet g19
port monitor g2
port monitor g3
port monitor g21
port monitor g22
port monitor g23
port monitor g24
port monitor vlan-tagging

simple and limiting - only one port can be destination
Mikrotik tilera, tzsp, TaZmen Sniffer Protocol, WTF?!

Mikrotik "router" == doesn't have switch chip == no port mirroring

tzsp streaming in udp packets

/tool sniffer
set filter-interface=all memory-limit=10000KiB
streaming-enabled=yes streaming-server=10.9.10.2

https://github.com/thefloweringash/tzsp2pcap

modprobe dummy
ip link set dummy0 up
/home/dpavlin/tzsp2pcap -f | /usr/bin/tcpreplay --topspeed -i dummy0 - &

terrible, terrible way to waste kernel/user-space copy just to keep bro happy and think that it's listening to simple interface
bro on Debian

package is suitable for pcap file analysis and evaluation but lacks pf_ring and broker support (due to missing pf_ring and actor-framework dependencies)

dpavlin@enesej:~$ git clone --recursive git://git.bro.org/bro
dpavlin@enesej:~/bro$ ./configure --enable-broker && make install

deploy with broctl deploy, carefully symlink all config dirs back to debian locations
start customizing bro configuration files in /etc/bro or /usr/local/bro/etc/
install broctl cron
root@enesej:~# broctl status

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Host</th>
<th>Status</th>
<th>Pid</th>
<th>Started</th>
</tr>
</thead>
<tbody>
<tr>
<td>logger</td>
<td>logger</td>
<td>enesej</td>
<td>running</td>
<td>21215</td>
<td>29 May 19:42:39</td>
</tr>
<tr>
<td>manager</td>
<td>manager</td>
<td>enesej</td>
<td>running</td>
<td>21286</td>
<td>29 May 19:42:40</td>
</tr>
<tr>
<td>proxy</td>
<td>proxy</td>
<td>enesej</td>
<td>running</td>
<td>21355</td>
<td>29 May 19:42:42</td>
</tr>
<tr>
<td>tilera</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21586</td>
<td>29 May 19:42:43</td>
</tr>
<tr>
<td>b101-1</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21593</td>
<td>29 May 19:42:43</td>
</tr>
<tr>
<td>b101-2</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21606</td>
<td>29 May 19:42:43</td>
</tr>
<tr>
<td>b101-3</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21605</td>
<td>29 May 19:42:43</td>
</tr>
<tr>
<td>b101-4</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21604</td>
<td>29 May 19:42:43</td>
</tr>
<tr>
<td>tzsp</td>
<td>worker</td>
<td>enesej</td>
<td>running</td>
<td>21599</td>
<td>29 May 19:42:43</td>
</tr>
</tbody>
</table>

root@enesej:/var/log/bro/current# ls
simple shell tools for useful counts

dpavlin@enesej:/var/log/bro/2017-06-01$ cat /srv/bro-tools/notice-count.sh
zcat notice.* | bro-cut -d note | sort | uniq -c
dpavlin@enesej:/var/log/bro/2017-06-01$ /srv/bro-tools/notice-count.sh
  291 CaptureLoss::Too_Much_Loss
  13 HTTP::SQL_Injection_Attacker
   9 HTTP::SQL_Injection_Victim
    3 PacketFilter::Dropped_Packets
  232 Scan::Address_Scan
    6 Scan::Port_Scan
    2 SSH::Interesting_Hostname_Login
  103 SSH::Password_Guessing
  4107 SSL::Invalid_Server_Cert
  1024 Traceroute::Detected
  267 Weird::Activity
root@bro:~#

less -S # chop long lines

bro-cut -d username # log files have header used by bro-cut

awk -F '\t' '{ print $12 }'

sort | uniq -c | column -t | less -S

zless, zcat # broctl rotate and compress logs every hour

https://github.com/ffzg/bro-tools
Work in progress