The Bro Network Security Monitor

Brooverview

NCSA
Outline

Philosophy and Architecture

A *framework* for network traffic analysis.
Outline

Philosophy and Architecture
   A *framework* for network traffic analysis.

History
   From research to operations.
Outline

Philosophy and Architecture
   A framework for network traffic analysis.

History
   From research to operations.

Architecture
   Components, logs, scripts, cluster.
What is Bro?
What is Bro?

Packet Capture
What is Bro?

- Packet Capture
- Traffic Inspection
What is Bro?

- Packet Capture
- Traffic Inspection
- Attack Detection
What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

Log Recording

NetFlow

syslog
What is Bro?

Packet Capture
Traffic Inspection
Attack Detection
Log Recording
Flexibility
Abstraction
Data Structures

TCPDUMP
WIRESHARK
SNORT
NetFlow
syslog
What is Bro?

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
- Flexibility
- Abstraction
- Data Structures
What is Bro?

- Packet Capture
- Traffic Inspection
- Attack Detection
- Log Recording
- Flexibility
- Abstraction
- Data Structures

- TCPDUMP
- WIRESHARK
- SNORT
- NetFlow
- syslog
- python
- NCSA
What is Bro?

Packet Capture
Traffic Inspection
Attack Detection
Log Recording
Flexibility
Abstraction
Data Structures

“Domain-specific Python”
What is Bro?

Packet Capture
Traffic Inspection
Attack Detection
Log Recording

Sum is more than the pieces

“Domain-specific Python”

Flexibility
Abstraction
Data Structures
Philosophy
Philosophy

Fundamentally different from other IDS.
Reset your idea of an IDS before starting to use Bro.
Philosophy

Fundamentally different from other IDS.
Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework*.
Primarily an IDS, but many use it for general traffic analysis.
Philosophy

Fundamentally different from other IDS.
Reset your idea of an IDS before starting to use Bro.

Real-time network analysis framework.
Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.
Can accommodate a range of detection approaches.
Philosophy

Fundamentally different from other IDS.
Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework*.
Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.
Can accommodate a range of detection approaches.

Highly stateful.
Tracks extensive application-layer network state.
Philosophy

Fundamentally different from other IDS.
Reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework*.
Primarily an IDS, but many use it for general traffic analysis.

Policy-neutral at the core.
Can accommodate a range of detection approaches.

Highly stateful.
Tracks extensive application-layer network state.

Supports forensics.
Extensively logs what it sees.
Target Audience
Target Audience

Network-savvy users.
Requires understanding of your network.
Target Audience

Network-savvy users.
Requires understanding of your network.

Unixy mindset.
Command-line based, fully customizable.
Target Audience

Network-savvy users.
Requires understanding of your network.

Unixy mindset.
Command-line based, fully customizable.

Large-scale environments.
Effective also with liberal security policies.
Bro History


Vern writes 1st line of code
Bro History


- Vern writes 1st line of code
- v0.2 1st CHANGES entry
- v0.4 HTTP analysis
- LBNL starts using Bro operationally
- Scan detector
- IP fragments
- Linux support
- v0.7a48 Consistent CHANGES
- v0.7a90 Profiling State Mgmt
- v0.8aX/0.9aX
- Signatures
- SMTP
- IPv6 support
- User manual
- v0.7a175/0.8aX
- Communication
- Persistence
- Namespaces
- Log Rotation
- 0.8a37
- GeoIP
- Conn Compressor
- v1.0 BinPAC
- IRC/RPC analyzers
- 64-bit support
- Sane version numbers
- v1.1/v1.2
- SSL/SMB
- STABLE releases BroLite
- v1.3
- v1.4
- DHCP/BitTorrent
- HTTP entities
- NetFlow
- Bro Lite Deprecated
- v1.5 BroControl
- v1.6
- Resource tuning
- Broccoli
- v1.7 DPD
- v1.8
- v1.9
- v2.0 New Scripts
- v2.1 IPv6 Input Framew.
- v2.2 (beta)
- v2.3
- v2.4
- v2.5
- v2.6
- v2.7
- v2.8
**Installations across the US**

- Universities
- Research Labs
- Supercomputer Centers
- Fortune 50 Industry

**Examples**

- Lawrence Berkeley National Lab
- Indiana University
- National Center for Supercomputing Applications
- National Center for Atmospheric Research

... and many more sites

**Fully integrated into Security Onion**

Popular security-oriented Linux distribution

**Recent User Meetings**

- Bro Workshop 2011 at NCSA
- Bro Exchange 2012 at NCAR
- Bro Exchange 2013 at NCSA

Each attended by about 50-90 operators from 30-50 organizations
Deployment

Internet \hline Internal Network
Deployment

Internet \rightarrow \text{Tap} \rightarrow \text{Bro} \rightarrow \text{Internal Network}
Deployment

Internet  Tap  Internal Network

Bro

Runs on commodity platforms.
Standard PCs & NICs.
Supports FreeBSD/Linux/OS X.
Creating Visibility with Bro
Creating Visibility with Bro

> bro -i en0
[ ... wait ...]
> cat conn.log
Creating Visibility with Bro

```plaintext
> bro -i en0
[ ... wait ...]
> cat conn.log

#fields ts id.orig_h id.orig_p id.resp_h id.resp_p proto service duration
1144876741.1198 192.150.186.169 53115 82.94.237.218 80 tcp http 16.14929
1144876612.6063 192.150.186.169 53090 198.189.255.82 80 tcp http 4.437460
1144876596.5597 192.150.186.169 53051 193.203.227.129 80 tcp http 0.372440
1144876606.7789 192.150.186.169 53082 198.189.255.73 80 tcp http 0.597711
1144876741.4693 192.150.186.169 53116 82.94.237.218 80 tcp http 16.02667
1144876745.6102 192.150.186.169 53117 66.102.7.99 80 tcp http 1.004346
1144876605.6847 192.150.186.169 53075 207.151.118.143 80 tcp http 0.029663
```
Creating Visibility with Bro

> bro -i en0
[ ... wait ...]
> cat conn.log

<table>
<thead>
<tr>
<th>#fields ts</th>
<th>id.orig_h</th>
<th>id.orig_p</th>
<th>id.resp_h</th>
<th>id.resp_p</th>
<th>proto</th>
<th>service</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1144876741.1198</td>
<td>192.150.186.169</td>
<td>53115</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.14929</td>
</tr>
<tr>
<td>1144876612.6063</td>
<td>192.150.186.169</td>
<td>53090</td>
<td>198.189.255.82</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>4.437460</td>
</tr>
<tr>
<td>1144876596.5597</td>
<td>192.150.186.169</td>
<td>53051</td>
<td>193.203.227.129</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.372440</td>
</tr>
<tr>
<td>1144876606.7789</td>
<td>192.150.186.169</td>
<td>53082</td>
<td>198.189.255.73</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.597711</td>
</tr>
<tr>
<td>1144876741.4693</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.02667</td>
</tr>
<tr>
<td>1144876745.6102</td>
<td>192.150.186.169</td>
<td>53117</td>
<td>66.102.7.99</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>1.004346</td>
</tr>
<tr>
<td>1144876605.6847</td>
<td>192.150.186.169</td>
<td>53075</td>
<td>207.151.118.143</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.029663</td>
</tr>
</tbody>
</table>

> cat http.log
Creating Visibility with Bro

```bash
> bro -i en0
[ ... wait ...]
> cat conn.log
```

<table>
<thead>
<tr>
<th>#fields ts</th>
<th>id.orig_h</th>
<th>id.orig_p</th>
<th>id.resp_h</th>
<th>id.resp_p</th>
<th>proto</th>
<th>service</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1144876741.1198</td>
<td>192.150.186.169</td>
<td>53115</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.14929</td>
</tr>
<tr>
<td>1144876612.6063</td>
<td>192.150.186.169</td>
<td>53090</td>
<td>198.189.255.82</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>4.437460</td>
</tr>
<tr>
<td>11448766596.5597</td>
<td>192.150.186.169</td>
<td>53051</td>
<td>193.203.227.129</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.372440</td>
</tr>
<tr>
<td>11448766606.7789</td>
<td>192.150.186.169</td>
<td>53082</td>
<td>198.189.255.73</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.597711</td>
</tr>
<tr>
<td>1144876741.4693</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.02667</td>
</tr>
<tr>
<td>1144876745.6102</td>
<td>192.150.186.169</td>
<td>53117</td>
<td>66.102.7.99</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>1.004346</td>
</tr>
<tr>
<td>1144876605.6847</td>
<td>192.150.186.169</td>
<td>53075</td>
<td>207.151.118.143</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.029663</td>
</tr>
</tbody>
</table>

```bash
> cat http.log
```

<table>
<thead>
<tr>
<th>#fields ts</th>
<th>id.orig_h</th>
<th>id.orig_p</th>
<th>id.resp_h</th>
<th>id.resp_p</th>
<th>proto</th>
<th>service</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1144876741.6335</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/lib/lib.css</td>
<td>200</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.1687</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/previous.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876741.2838</td>
<td>192.150.186.169</td>
<td>53115</td>
<td>docs.python.org</td>
<td>/lib/lib.html</td>
<td>200</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.3337</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/up.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.3337</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/next.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.3337</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/contents.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.3337</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/modules.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876742.3337</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>docs.python.org</td>
<td>/icons/index.png</td>
<td>304</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
<tr>
<td>1144876745.6144</td>
<td>192.150.186.169</td>
<td>53117</td>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>/</td>
<td>200</td>
<td>Mozilla/5.0</td>
<td></td>
</tr>
</tbody>
</table>
## Creating Visibility with Bro

```plaintext
> bro -i en0
[ ... wait ...]
> cat conn.log
```

<table>
<thead>
<tr>
<th>#fields</th>
<th>ts</th>
<th>id.orig_h</th>
<th>id.orig_p</th>
<th>id.resp_h</th>
<th>id.resp_p</th>
<th>proto</th>
<th>service</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1144876741.1198</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.14929</td>
</tr>
<tr>
<td></td>
<td>1144876612.6063</td>
<td>192.150.186.169</td>
<td>53090</td>
<td>198.189.255.82</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>4.437460</td>
</tr>
<tr>
<td></td>
<td>1144876656.5503</td>
<td>192.150.186.169</td>
<td>53051</td>
<td>193.203.227.129</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.372440</td>
</tr>
<tr>
<td></td>
<td>1144876606.7789</td>
<td>192.150.186.169</td>
<td>53082</td>
<td>198.189.255.73</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.597711</td>
</tr>
<tr>
<td></td>
<td>1144876741.4693</td>
<td>192.150.186.169</td>
<td>53116</td>
<td>82.94.237.218</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>16.02667</td>
</tr>
<tr>
<td></td>
<td>1144876745.6102</td>
<td>192.150.186.169</td>
<td>53117</td>
<td>66.102.7.99</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>1.004346</td>
</tr>
<tr>
<td></td>
<td>1144876605.6847</td>
<td>192.150.186.169</td>
<td>53075</td>
<td>207.151.118.143</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
<td>0.029663</td>
</tr>
</tbody>
</table>

```plaintext
[...] host          uri                     status_code | user_agent
docs.python.org    /lib/lib.css         200          | Mozilla/5.0
docs.python.org    /icons/previous.png 304          | Mozilla/5.0
docs.python.org    /lib/lib.html        200          | Mozilla/5.0
docs.python.org    /icons/up.png        304          | Mozilla/5.0
docs.python.org    /icons/next.png      304          | Mozilla/5.0
docs.python.org    /icons/contents.png  304          | Mozilla/5.0
docs.python.org    /icons/modules.png   304          | Mozilla/5.0
```

```plaintext
docs.python.org    /icons/index.png     304          | Mozilla/5.0
www.google.com      /                     200          | Mozilla/5.0
```
Architecture

Network

Packets
Architecture

- Protocol Decoding
- Event Engine
- Network

Events → Event Engine → Packets
Architecture

Network

Policy Script Interpreter

Event Engine

Analysis Logic

Protocol Decoding

Logs

Notification

Events

Packets

Network
Architecture

Network

Protocol Decoding

Analysis Logic

Policy Script Interpreter

Event Engine

Logs

Notification

Events

Packets

“User Interface”
Event Model

Web Client

1.2.3.4/4321

Request for /index.html

Status OK plus data

Web Server

5.6.7.8/80
Event Model

Request for /index.html

Status OK plus data

Stream of TCP packets

1.2.3.4/4321

Web Client

Web Server

5.6.7.8/80
Event Model

Request for `/index.html`

Web Client

1.2.3.4/4321

Stream of TCP packets

Web Server

5.6.7.8/80

Status OK plus data

connection_established(1.2.3.4/4321→5.6.7.8/80)
Event Model

- **Web Client**
  - IP: 1.2.3.4/4321

- **Web Server**
  - IP: 5.6.7.8/80

Request for /index.html

Status OK plus data

Stream of TCP packets

**Event**

- connection_established(1.2.3.4/4321⇒5.6.7.8/80)

**TCP stream reassembly for originator**

**Event**

- http_request(1.2.3.4/4321⇒5.6.7.8/80, "GET", "/index.html")
Event Model

1.2.3.4/4321

Request for /index.html

Status OK plus data

5.6.7.8/80

Stream of TCP packets

connection_established(1.2.3.4/4321⇒5.6.7.8/80)

TCP stream reassembly for originator

http_request(1.2.3.4/4321⇒5.6.7.8/80, “GET”, “/index.html”)

TCP stream reassembly for responder

http_reply(1.2.3.4/4321⇒5.6.7.8/80, 200, “OK”, data)
Event Model

Web Client

Request for /index.html

Web Server

Status OK plus data

1.2.3.4/4321

5.6.7.8/80

Stream of TCP packets

Event

collection_established(1.2.3.4/4321⇒5.6.7.8/80)

TCP stream reassembly for originator

Event

http_request(1.2.3.4/4321⇒5.6.7.8/80, “GET”, “/index.html”)

TCP stream reassembly for responder

Event

http_reply(1.2.3.4/4321⇒5.6.7.8/80, 200, “OK”, data)

Event

collection_finished(1.2.3.4/4321, 5.6.7.8/80)
Task: Report all Web requests for files called “passwd”.

Script Example: Matching URLs
Task: Report all Web requests for files called “passwd”.

```c
event http_request(c: connection,  # Connection.
                   method: string,    # HTTP method.
                   original_URI: string,  # Requested URL.
                   unescaped_URI: string, # Decoded URL.
                   version: string)  # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...);  # Alarm.
}
```
Task: Count failed connection attempts per source address.
Task: Count failed connection attempts per source address.

```plaintext
global attempts: table[addr] of count &default=0;

event connection_rejected(c: connection)
{
    local source = c$id$orig_h; # Get source address.
    local n = ++attempts[source]; # Increase counter.
    if ( n == SOME_THRESHOLD ) # Check for threshold.
        NOTICE(...); # Alarm.
}
```
Distributed Scripts
Distributed Scripts

Bro comes with >10,000 lines of script code.
Prewritten functionality that’s just loaded.
Distributed Scripts

Bro comes with >10,000 lines of script code.  
Prewritten functionality that’s just loaded.

Scripts generate alarms and logs.  
Amendable to extensive customization and extension.
Bro comes with support for ...
Bro comes with support for ...

Extract files from HTTP, SMTP, etc.

Extract/monitor SSL certificates.

Detect malware via Team Cymru's Malware Hash Registry.

Report vulnerable software versions on the network.

Detect popular web applications.

Detect SSH brute-forcing.

Notable external scripts:
- Bro module for Mandiant APT1 report
- Lucky 13 detector.
- ICSI SSL notary
Bro Ecosystem

Internet  Tap  Internal Network

Bro
Bro Ecosystem

Internet → Tap → Bro → BroControl
BroControl → User Interface
Bro → Output
Tap → Control

Internal Network → Tap → Bro → BroControl
BroControl → User Interface
Bro → Output
Tap → Control

Internet ← Tap ← Bro ← BroControl
BroControl ← User Interface
Bro ← Output
Tap ← Control

Bro Control
User Interface

Bro Ecosystem
Bro Ecosystem

- **Internet**
- **Internal Network**
- **Contributed Scripts**
- **Functionality**
- **Bro**
- **Events State**
- **Other Bros**
- **Control**
- **Output**
- **BroControl**
- **User Interface**

Tap

*Bro Ecosystem*
Bro Ecosystem

- **Internet**
- **Internal Network**
  - **Tap**
  - **Bro**
    - **Contributed Scripts**
    - **Functionality**
    - **Control**
    - **Output**
  - **BroControl**
    - **Events**
    - **User Interface**
  - **Events**
  - **State**
  - **Other Bros**
  - **Broccoli**
    - **Bro Client Communication Library**

Other Bros

Bro Control

Output

User Interface

Internal Network

Bro Ecosystem

Contributed Scripts

Functionality

Control

Output

Events

State

Internet

Tap

Other Bros

Broccoli

Bro Client Communication Library

NCSA
Bro Ecosystem

Internet → Tap → Bro → BroControl → Broccoli

Bro → Functionality to Contributed Scripts

Bro → Broccoli Python
Bro → Broccoli Ruby
Bro → Broccoli Perl

Bro → Events to State

BroControl → Control
BroControl → Output

BroControl → User Interface

Other Bros → Events

Internal Network → Tap → Bro
Bro Ecosystem

- **Internet**
  - Tap to **Bro**
  - **BroControl**
    - User Interface
    - Control
    - Output
  - **Bro**
    - Functionality
  - **Contributed Scripts**
  - **Other Bros**
    - **Broccoli Ruby**
    - **Broccoli Python**
    - Broccoli Perl
  - **Internal Network**
    - Tap to **Bro**
    - **BroControl**
    - Events
    - State
    - **Bro Control**
      - Events
      - Bro Client Communication Library

NCSA
Bro Ecosystem

Internet → Bro → Other Bros

Tap → BroControl

Control → Output

Events → State

Contributed Scripts

bro-aux  BinPAC  capstats
BTest  trace-summary

http://www.bro-ids.org/download
git://git.bro-ids.org

Broccoli

Broccoli Ruby
Broccoli Python
(Broccoli Perl)

Bro Client Communication Library
Bro Ecosystem

Bro Distribution
bro-2.1.tar.gz

Contributed Scripts
bro-aux  BinPAC  capstats
BTest  trace-summary

Functionality
Control
Output
User Interface

Events
State

Time Machine
Tap

Internal Network

Bro

BroControl

Other Bros

Broccoli

Bro Client Communication Library

Broccoli Python
Broccoli Ruby
(Broccoli Perl)

Contributed Scripts

http://www.bro-ids.org/download
git://git.bro-ids.org

NCSA
Bro Cluster Ecosystem

Internet → Tap → Internal Network

Tap

Contributed Scripts
- bro-aux
- BinPAC
- capstats
- BTest
- trace-summary

Time Machine

External Bro
- Broccoli
- Broccoli Ruby
- Broccoli Python
- (Broccoli Perl)

Broccoli Ruby

Broccoli Python

Broccoli

Bro Control

User Interface

Output

Bro Client Communication Library

1. Time Machine
2. External Bro
3. Contributed Scripts
4. Internet
5. Internal Network
6. Tap

17

Internals

Broccoli

NCSA

International Computer Science Institute
**Bro Cluster Ecosystem**

- **Internet**
- **Internal Network**
  - **Tap**
  - **Load-Balancer**
    - **Packets**
      - **Bro**
      - **Bro**
      - **Bro**
      - **Bro**
  - **Time Machine**

**Contributed Scripts**
- bro-aux
- BinPAC
- capstats
- BTest
- trace-summary

**Broccoli**
- Broccoli Ruby
- Broccoli Python
- (Broccoli Perl)

**Bro Client Communication Library**

**User Interface**
- Control
- Output

**Functionality**
- Time Machine
- Events
- capstats

**Packets**
- Events
- State
- BTest
- BinPAC
- trace-summary

**Bro Cluster Ecosystem**
- Bro-aux
- Bro-aux
- Bro-aux
- Bro-aux
Bro Cluster Ecosystem