

An Overview of Bro IDS

NEOISF
November 2009

Pete Garvin
Managing Engineer
PROTECTUS

Contents

Who & What

Architecture

Input & Output

Events

Policy

Example

Reasons To Use Bro

Relation To Snort

Who

Bro and supporting info for
this presentation comes from:

- Lawrence Berkeley National Lab
- International Computer Science Institute
- National Science Foundation
- Bro Community

www.bro-ids.org

What Bro Is

- Network Intrusion Detection System
- Unix-based
- Open source
- Network traffic analysis framework
- Research platform
- Very flexible

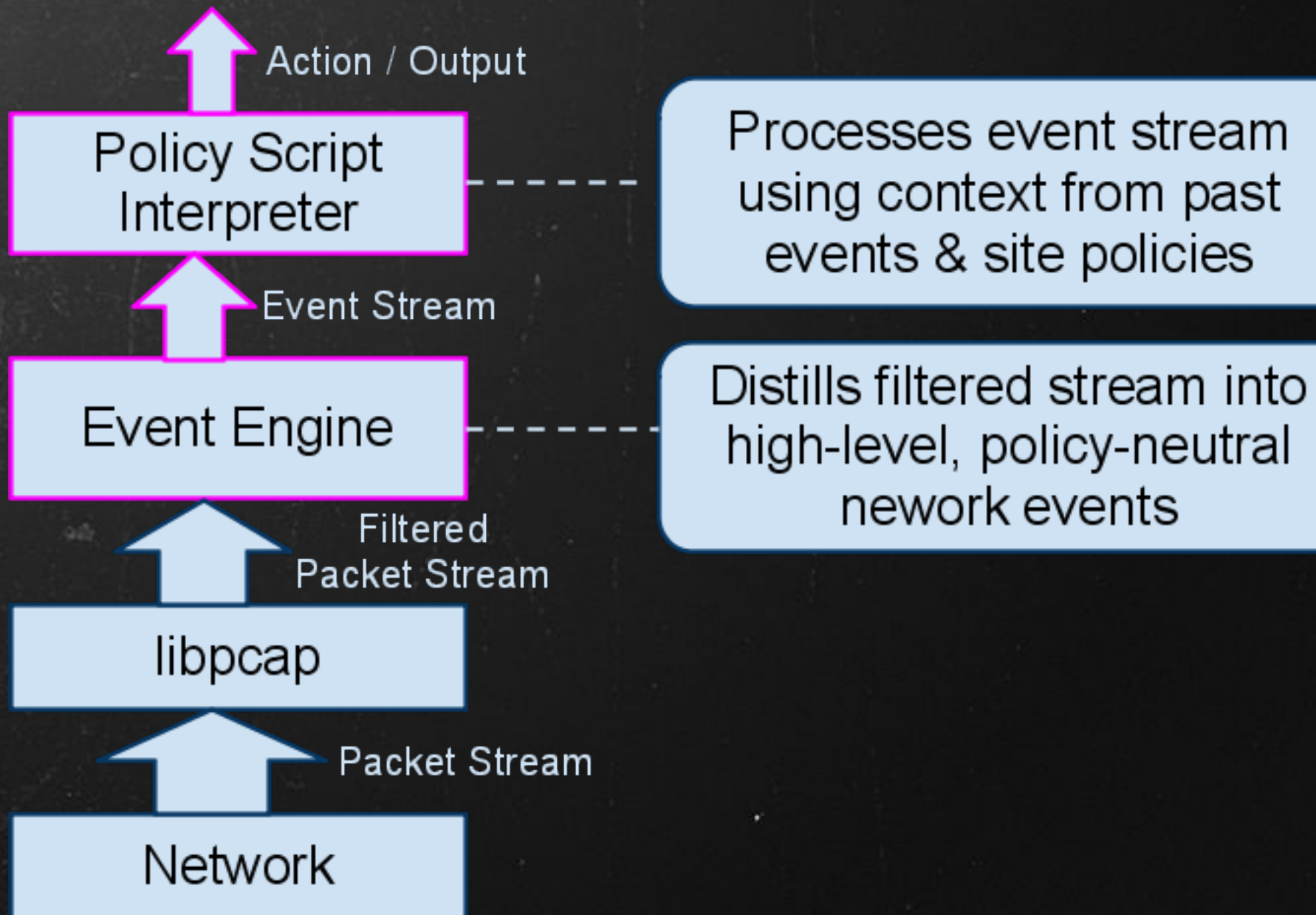
What Bro Does Well

- Multi-layer analysis
- Behavioral monitoring
- Policy enforcement
- Policy-based intrusion detection
- Logging network activity

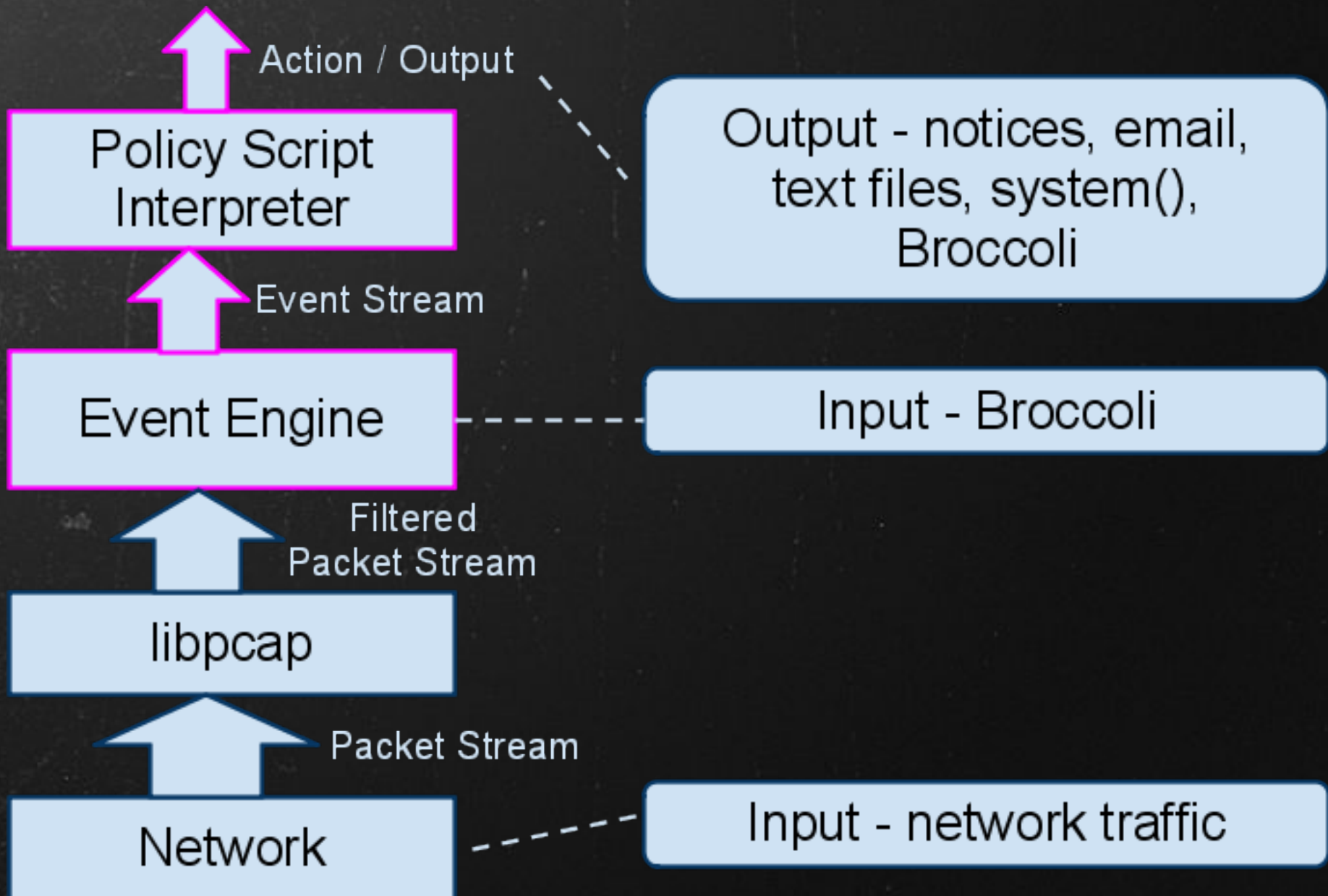
What Bro Is Not

- **Out-of-the-box solution** - although brolite policy script is a place to start
- **Signature matching** - although supports signatures
- **Anomaly detection** - although can be used for that
- **Default configuration** - although many policy scripts are provided

Bro Architecture

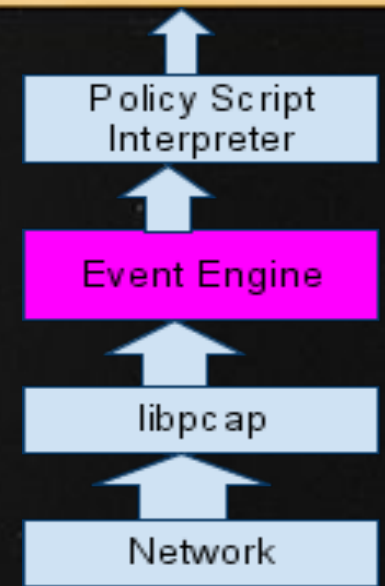


Input / Output



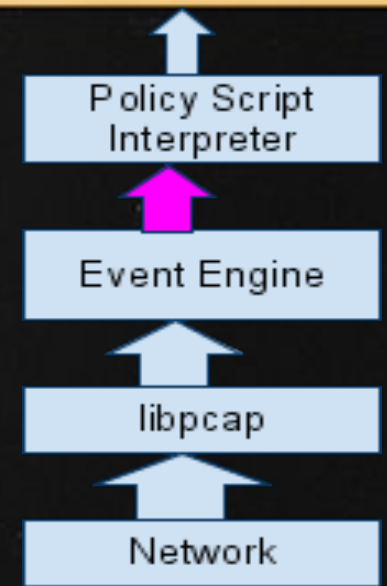
Event Engine

- Written in C++
- Policy neutral
- Analyzes traffic & generates events
- Selects protocol analyzer using port #
- Analyzer selection can be overridden
- Dynamic Protocol Detection
 - Payload used to determine protocol



Events

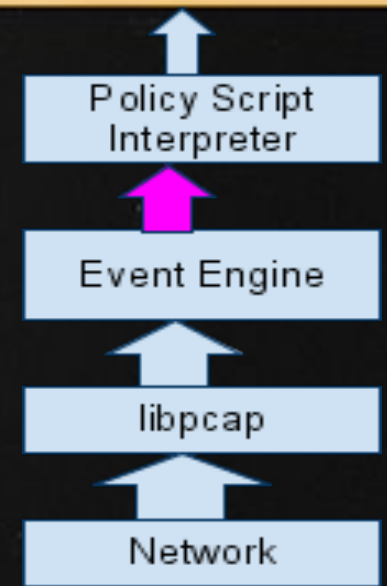
- About 320 event types
- Events generated by:
 - Event engine (mostly)
 - Timers
 - Policy scripts
- Events handled by policy scripts
- Examples:
 - `connection_established(c: connection)`
 - `connection_finished(c: connection)`



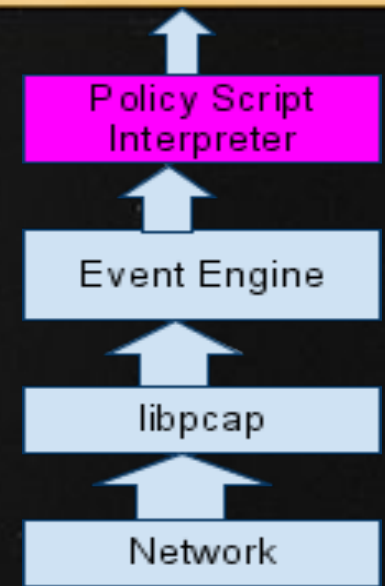
Example Events

- new_connection
- new_packet
- smtp_request
- http_header
- ssl_certificate_seen
- icmp_echo_reply
- authentication_rejected
- dns_PTR_reply
- arp_request

* Event parameters not shown

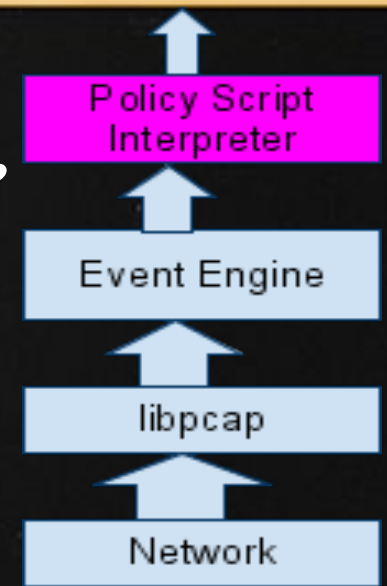


Policy Scripts



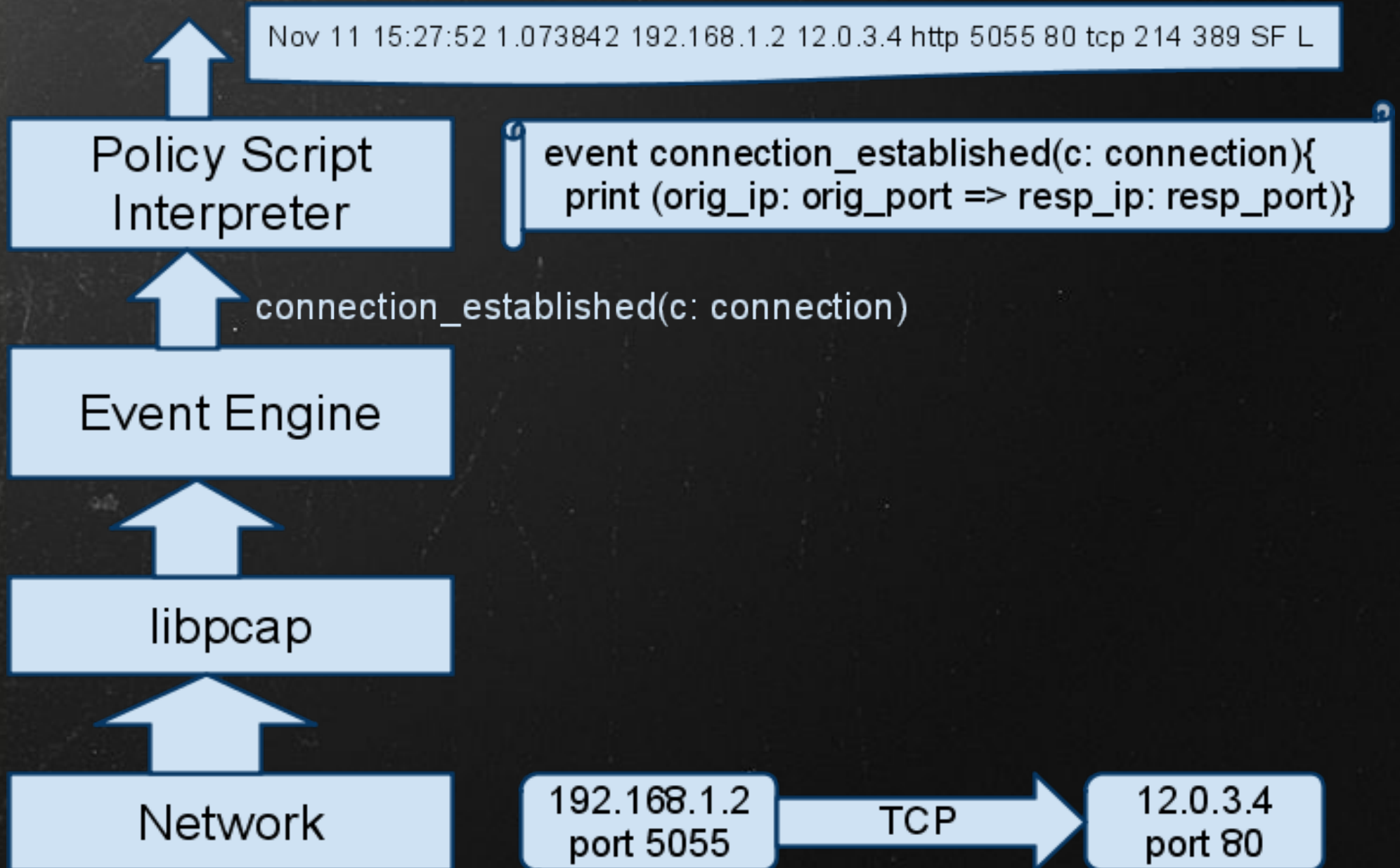
- Written in Bro's language
- Analyze network events
- Determine if events are noteworthy
- Specify what actions to take
- Specify how to report activities

Scripting Language



- Types, values & constants
- Refinement/redefinition
- Functions & event handlers
- Statements & expressions
- Built-in functions

Example

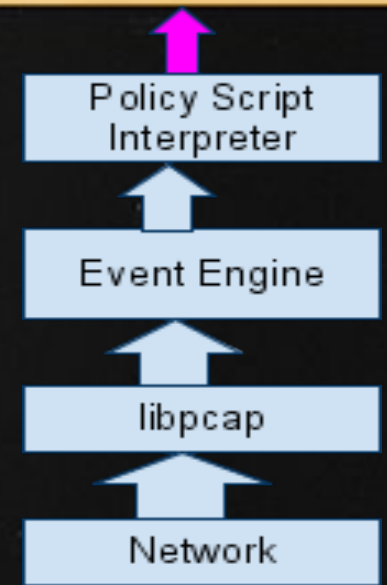


Example (cont.)

Nov 11 15:27:52	1.073842		
Time	Duration		
192.168.1.2	12.0.3.4	http	
Source	Destination	Service	
5055	80	tcp	
SrcPort	DstPort	Protocol	
214	389	SF	L
SrcBytes	DstBytes	State	Dir

Notices

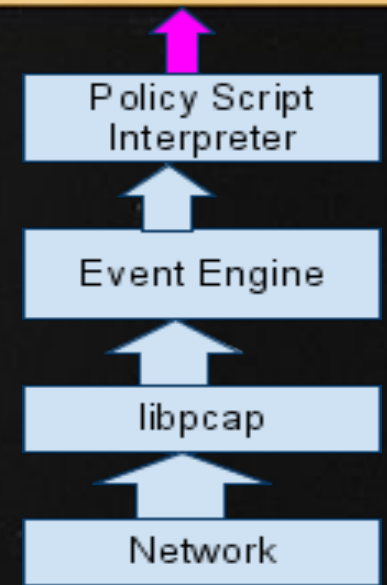
- Policy scripts create Notices
 - Something happened
 - Not necessarily bad
- Actions can be assigned to Notices
 - NOTICE_IGNORE
 - NOTICE_FILE
 - NOTICE_EMAIL
 - NOTICE_PAGE



Sample Notices

- PasswordGuessing
- PortScan
- SynFloodStart
- WeirdActivity
- ARPUnsolicitedReply
- ICMPUnpairedEchoReply
- InteractiveRSH

* Notice parameters not shown



Interesting Items

Broccoli

- Bro Client Communications Library
- Allows applications to speak to Bro

Time Machine

- Bulk-packet recorder
- Per-connection recording cutoff
- Works with Bro

And Much More.....

Reasons to Use Bro

- Verify results from another IDS
- Improve traffic forensics capabilities
- Provide policy-based checks
- As a research platform

Relation to Snort

- Includes Snort compatibility support
- snort2bro script
 - Converts Snort signatures to Bro signatures
 - Enhances signatures to take advantage of additional context

Requirements

Rough low-end estimates:

- 1 GHz CPU for 100 Mbps, <5K pkts/sec
- Unix or Linux, FreeBSD recommended
- 512 MB - 1 GB RAM
- 10 GB - 50 GB
- Superuser privileges
- 3 network interfaces
- Perl, libpcap,

Questions?

Thanks to all the people behind Bro!

www.bro-ids.org