NETSCOUT | Arbor

# The IDS Formerly Known as Bro

or “The IDS that was *supposed* to be called something other than Bro by now”

Andrew Beard, Software Architect

# What is it good for?

- Network Monitoring and operations
- Network Forensics
- Intrusion Detection
- Internet and Network Research
- Totalitarian Dictatorships

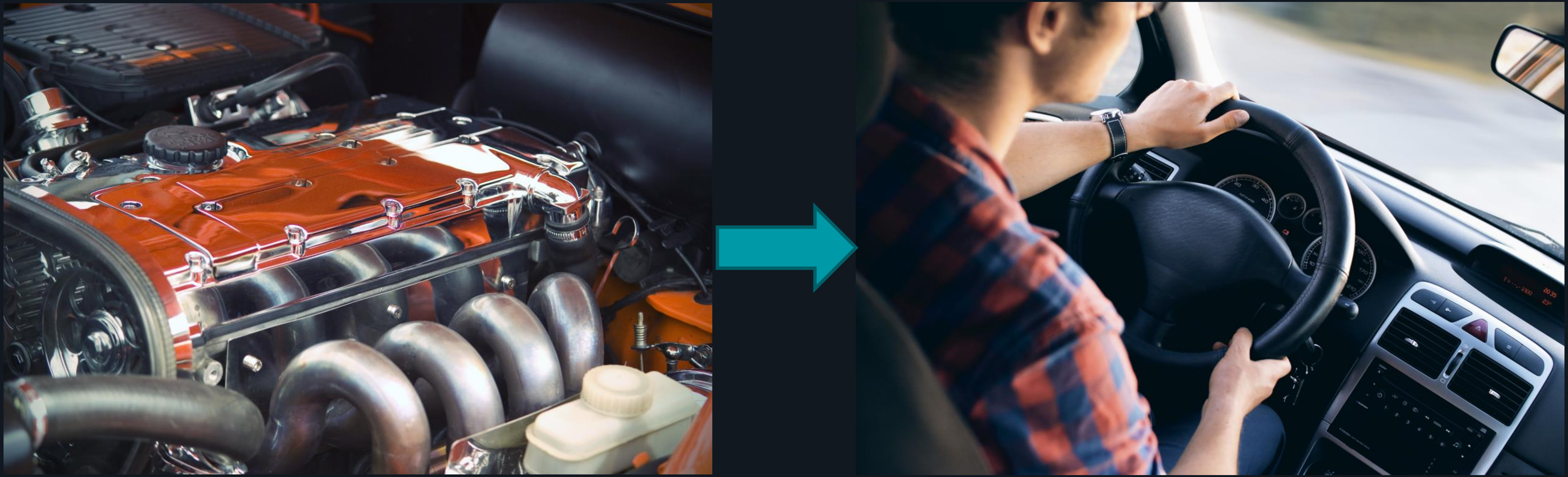
# Agenda

- A Different Approach to Learning Bro
- The Workshop VM
- Logs
- Scripts
- Events

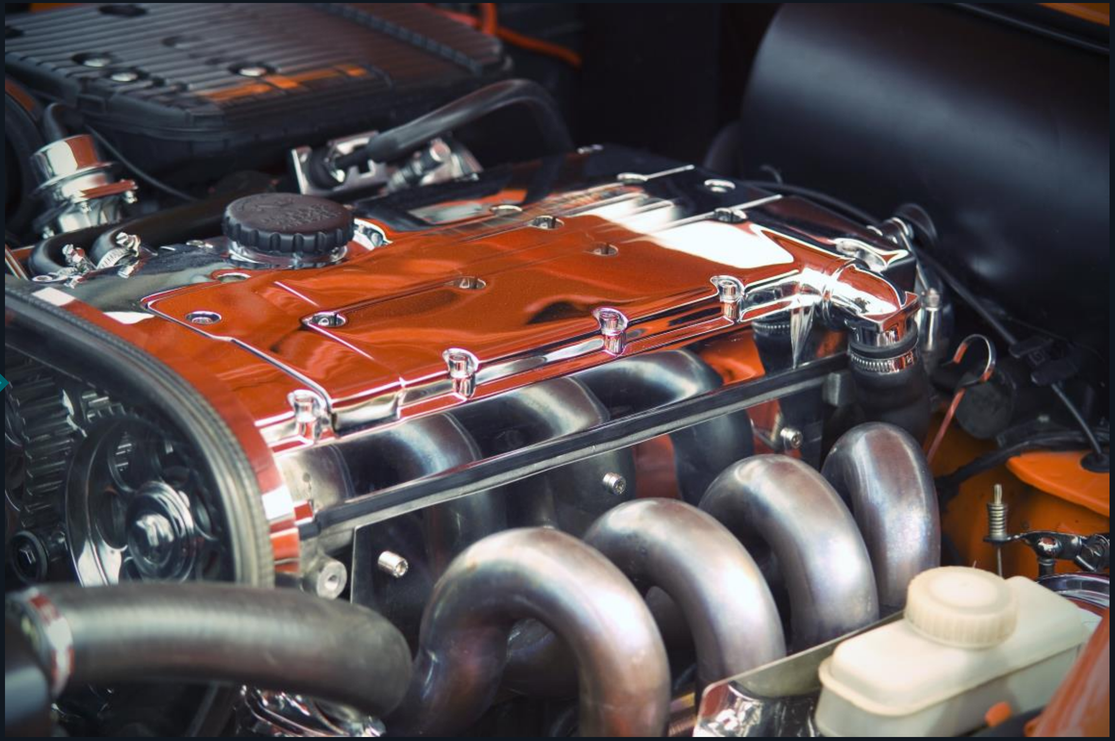
# A Different Approach to Learning Bro

Learning how to use Bro backwards

# Most Bro Training



# What We’re Going To Try



NETSCOUT | Arbor

# The Workshop VM

# The Supplied Bro VM

## Optional Subtitle is 24pt Arial Bold White, Title Case

- OVA file, useable with VMware products
- Never tried it with VirtualBox or other hypervisors
- Ubuntu 16.04 system with deb packages from the Bro Project
- $BRO_HOME is /opt/bro
- Default username: bro, password: broUser
- CLI only.  Install GUI with
  - `sudo apt-get install ubuntu-desktop`

# The Shared Lab System

## If you don’t have a VM

- Very similar to the VM
- Behind a separate WiFi network
  - SSID: BroTraining, password: 81+gone+MARS+66
- If you need an account grab a login
- Login via SSH to 10.20.10.20

BroTraining

81+gone+MARS+66

10.20.10.20

# Making sure Bro works

## Exercise 0

- Log in as your user
- There should be a broworkshop directory in your home directory
- Run ”git pull” in that directory
- From the test subdirectory run check_bro.sh
- Output should be Passed!

NETSCOUT | Arbor

# Logs

# Running Bro

- Start by processing captured network traffic files (pcaps)

```
bro -r <pcap file>
```

- Log files end up in the working directory (make sure it's writable)

# Bro connections

- conn.log is usually the most important log file
- Connections flow from origin (“orig”) to responder (“resp”)
- Can contain both IPv4 and IPv6
- Each connection gets a unique ID
- Includes TCP, UDP, and ICMP

# A bit about logs

- Default format is tab-separated values (TSV)
- Two types of IDs
  - Connection IDs start with C
  - File IDs start with F
- Bro logs are relational
- Can analyze using simple text processing commands

# What is Bro?

- Bro is a piece of software that converts captured network traffic into metadata log files

**This is a very naïve description of Bro**

# Chaining shell commands

## The pipe operator

- Output of one command is fed into the input of the next
- Can thinking of it as a filtering and aggregation pipeline
- In most cases here the first command will be reading from a Bro log file

```
sudo dmesg | less
```

# Useful command line utilities

- grep
  - Search for a string in the input
  - -v inverts the search, printing things that don’t contain the string

```
cat conn.log | grep dns
```

- bro-cut
  - Specify a subset of a bro log
  - Can reorder fields
  - -d converts timestamps to human-readable (but timestamp field must be included)

```
cat conn.log | bro-cut uid missed_bytes
```

# Useful command line utilities

- sort
  - Sort the rows of the input
  - -r for reverse, -n for numbers

```
cat conn.log | bro-cut missed_bytes uid | sort –n
```

- uniq
  - Remove *adjacent* duplicated lines
  - -c counts the number of occurrences

```
cat dns.log | bro-cut query | sort | uniq -c
```

# Exercise 1

## Using Bro logs

- What's the network's main DNS server? Which host is *not* using this DNS server?

- What IP address is hosting www.qrz.com? What about aa9pw.com? What's the difference between these two sites?

- What two external IP addresses are communicated with the *most?*

- What is the most common application protocol present in the packet capture?

# Scripts

# Bro scripts

- Text files
- Interpreted at runtime
- Convention is usually to use the .bro extension
- Included scripts are in subdirectories of $BRO_HOME/share/bro

# Running Bro part 2

## Electric Boogaloo

- Specify scripts to load on the command line

```
    bro –r <pcap file> [script file]
```

- Can specify full path

```
/opt/bro/share/bro/policy/frameworks/files/entropy-test-all-files.bro
```

- Script directory can be assumed

```
policy/frameworks/files/entropy-test-all-files.bro
```

- So can the file extension

```
policy/frameworks/files/entropy-test-all-files
```

# Scripts loading scripts

- @load directive is your friend
- Want to load multiple scripts?  Create a bro script file that contains the scripts you want with a @load directive.  That can be inserted via command line.
- Directives can also be added to /opt/bro/share/bro/site/local.bro (loaded automatically)

# Changing values

- Can redefine (“redef”) some global variables
- Frequently used for configuration

```
redef FTP::default_capture_password = T;
```

- Can be used to add to or extend some variables

```
redef FTP::guest_ids += { “anon” };
```

# What is Bro?

- Bro is a piece of software that *can* convert captured network traffic into metadata log files
- Bro is a platform for analyzing and processing network data

**This is *still* a very naïve description of Bro**

# Exercise 2

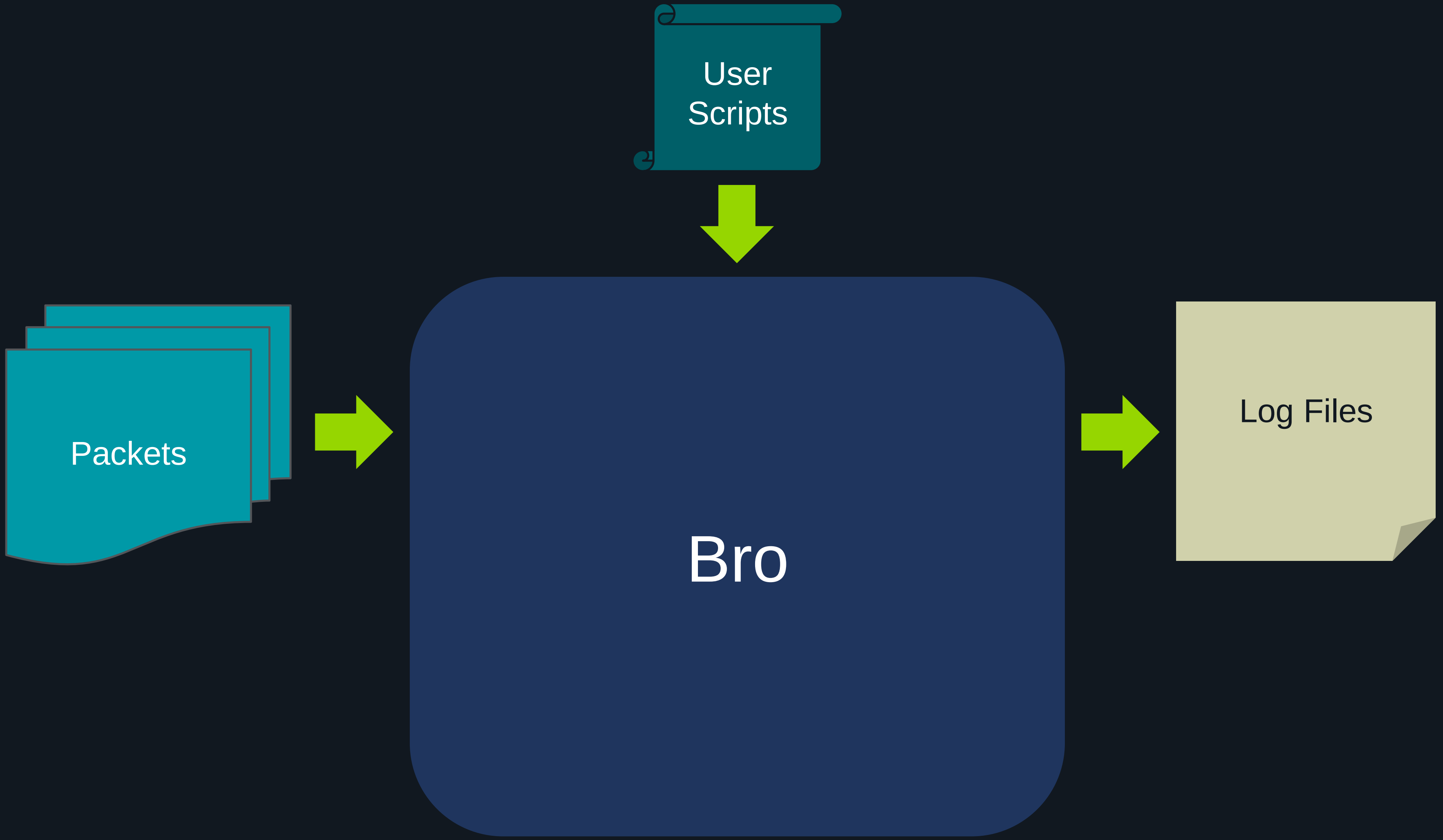
## Using Bro Scripts

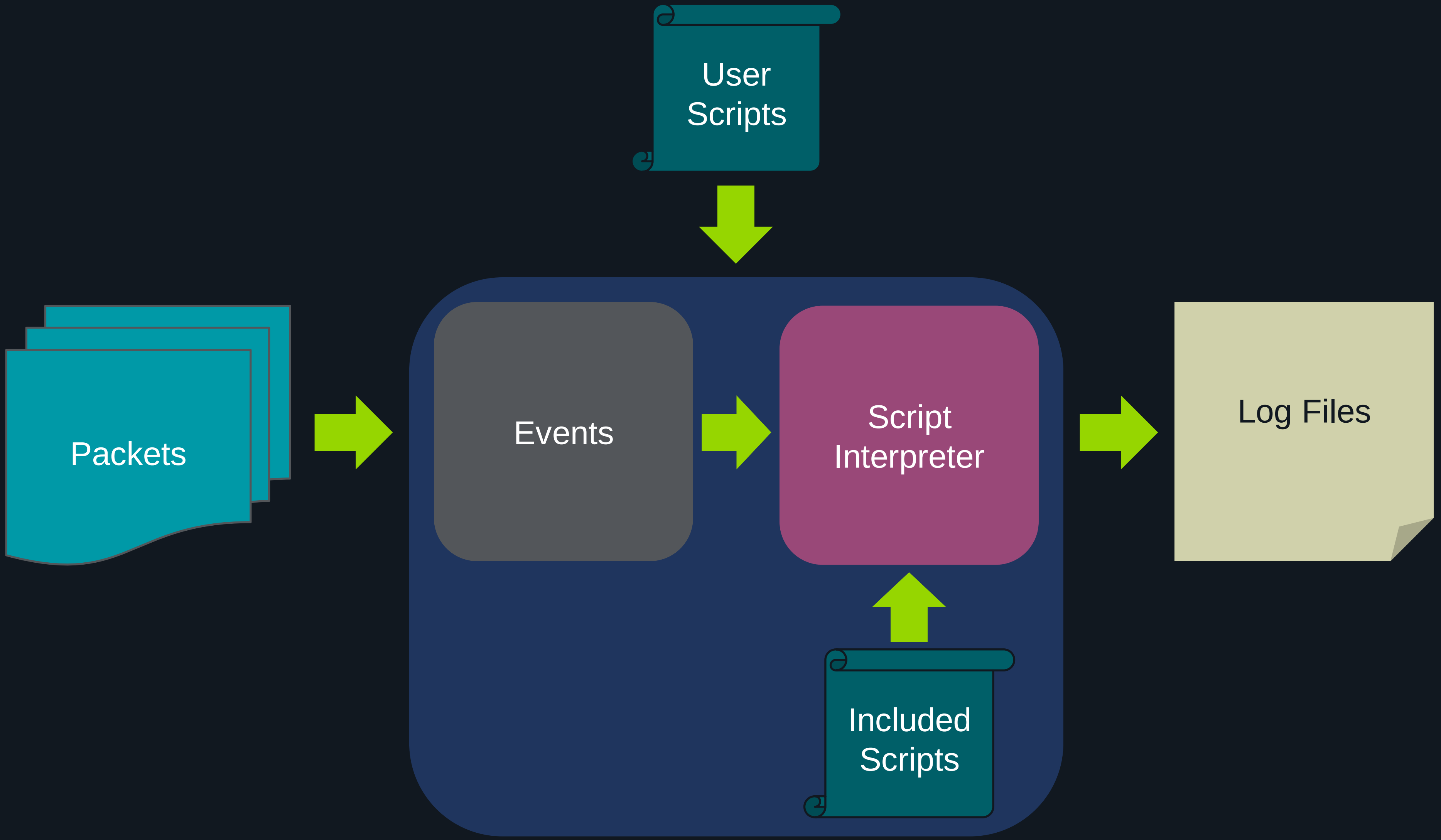
- A client downloaded a PDF file from an external server.  The file is no longer available from the remote system, but you have the content in the pcap file. Extract the file.

- Which internal IPv4 addresses correspond to local-link IPv6 addresses?

NETSCOUT | Arbor

# Events


User Scripts
Packets
Bro
Log Files


User Scripts
Packets
Events
Script Interpreter
Log Files
Included Scripts

# Dumping the event list

- There's an ~~app~~ script for that!

  `policy/misc/dump-events`

- Really useful for discovering relevant events
- Look up matching events in the Bro Script Reference
- Event arguments are also shown for debugging

# Event handlers

- Bro code that’s invoked whenever a given event happens

```
event dns_request (c: connection, msg: dns_msg, query: string,
                   qtype: count, qclass: count) {
    if ( c$id$orig_h == 192.168.1.40 ) {
        print(query);
    }
}
```

# What can Bro do?

## Log files and printouts are for chumps

- Run external applications
- Deal with binary files
- Call external REST APIs
- Interact with network devices (switches, routers, firewalls, etc)

# What is Bro?

- Bro is a piece of software that *can* convert captured network traffic into metadata log files
- Bro is a platform for analyzing and processing network data
- Bro is system for triggering actions based on events derived from network traffic

**Now we’re talking**

# Exercise 3

## Writing Bro scripts

- A script is being loaded that adds the MD5 and SHA1 hashes for all observed files to files.log.  Add SHA256 hashes as well.

- Write a Bro script to print the number of connections when finished processing a capture file.

# Things we didn’t cover

- Bro installation and configuration
- Live network interfaces
- Multi-node and clustering
- Advanced scripting
- Alerting
- The Intel Framework

# Next steps

- Bro File Analysis Exercises
- Learn to Brogram
- try.bro.org
- Bro Script Reference

NETSCOUT | Arbor

# Thanks!

Andrew Beard

@bearda24

abeard@arbor.net