Using Zeek Without Scripting

Roanoke InfoSec Exchange
June 9th, 2022

What is Zeek?

Running Zeek In A Container (Simple)

- Requires Docker only
- Pull the image

```
docker pull bearda/broworkshop
```

- Run it

```
docker run -it bearda/broworkshop
```

Running Zeek

- Bro is a command line utility (and a daemon)
- Start by processing captured network traffic files (pcaps)

```
zeek -r <pcap file>
```

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

Zeek Connections

- conn.log is usually the most important log file
- Connections flow from origin (“orig”) to responder (“resp”). Session flow, not packet flow.
- Can contain both IPv4 and IPv6
- Each connection gets a unique ID
- Includes TCP, UDP, and ICMP

A bit about the logs

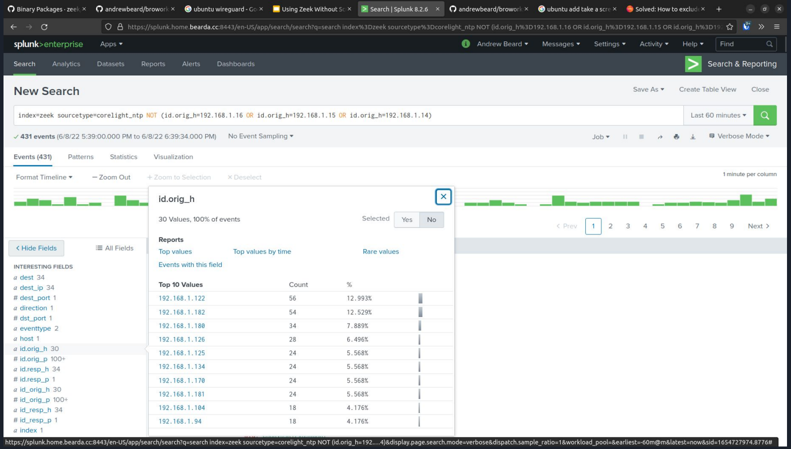
- Default format is tab-separated values (TSV)
- Two types of IDs
- Connection IDs start with C
- File IDs start with F
- Bro logs are relational
- Can analyze using simple text processing commands

Useful Command Line Processing Tools

- zeek-cut: Output one or more specified columns from a zeek log file
- uniq: Only output unique lines from a given input
- sort: Reorder input lines
- wc: Count number of lines

Log Aggregation

- Stick that Zeek data into something like Elasticsearch or Splunk
    - Elasticsearch has Zeek support built into Filebeat
    - Multiple Zeek TAs for Splunk



New Search

```
index=zeek sourcetype=corelight_ntp NOT (id.orig_h=192.168.1.16 OR id.orig_h=192.168.1.15 OR id.orig_h=192.168.1.14)
```

✓ 431 events (6/8/22 5:39:00.000 PM to 6/8/22 6:39:34.000 PM) No Event Sampling

Events (431)

INTERESTING FIELDS

a dest	34
a dest_ip	34
# dest_port	1
a direction	1
# dst_port	1
a eventtype	2
a host	1
a id.orig_h	30
# id.orig_p	100+
a id.resp_h	34
# id.resp_p	1
a id_orig_h	30
# id_orig_p	100+
a id_resp_h	34
# id_resp_p	1
a index	1

id.orig_h

30 Values, 100% of events Selected: Yes [✓ No]

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
192.168.1.122	56	12.993%
192.168.1.182	54	12.529%
192.168.1.180	34	7.889%
192.168.1.126	28	6.496%
192.168.1.125	24	5.568%
192.168.1.134	24	5.568%
192.168.1.170	24	5.568%
192.168.1.181	24	5.568%
192.168.1.104	18	4.176%
192.168.1.94	18	4.176%

Zeek Scripts

- You don’t have to write them to run them
- Look under $ZEEK_HOME/share/zeek for .zeek files
- Many will be loaded by default
- Tack the path to the script file on the end of the zeek command:

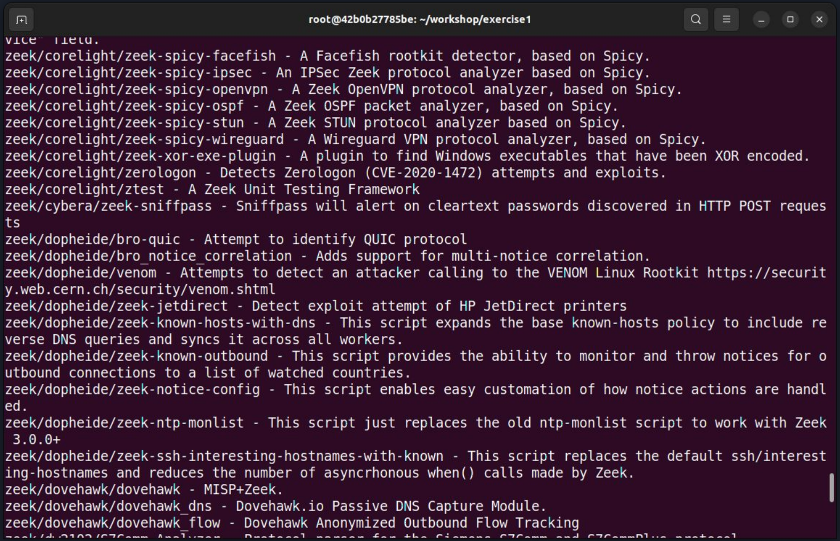
```
zeek -r <pcap file> <script file>
```

Example Zeek Scripts

- Extracting all files
- Comparing the hash of all files to Team Cymru’s malware hash registry
- Looking for known IOCs
- Detecting network tools like traceroute
- Identifying specific vulnerabilities or attacks, like Heartbleed
- Detecting bruteforce login attempts
- Adding VLAN tags to the connection logs

Even More Scripts

- Zeek Package Manager (zkg)
- `zkg list all`
- Currently 205 Zeek package available



```
vice" field.
zeek/corelight/zeek-spicy-facefish - A Facefish rootkit detector, based on Spicy.
zeek/corelight/zeek-spicy-ipsec - An IPSec Zeek protocol analyzer based on Spicy.
zeek/corelight/zeek-spicy-openvpn - A Zeek OpenVPN protocol analyzer, based on Spicy.
zeek/corelight/zeek-spicy-ospf - A Zeek OSPF packet analyzer, based on Spicy.
zeek/corelight/zeek-spicy-stun - A Zeek STUN protocol analyzer based on Spicy.
zeek/corelight/zeek-spicy-wireguard - A Wireguard VPN protocol analyzer, based on Spicy.
zeek/corelight/zeek-xor-exe-plugin - A plugin to find Windows executables that have been XOR encoded.
zeek/corelight/zerologon - Detects Zerologon (CVE-2020-1472) attempts and exploits.
zeek/corelight/ztest - A Zeek Unit Testing Framework
zeek/cybera/zeek-sniffpass - Sniffpass will alert on cleartext passwords discovered in HTTP POST reques
ts
zeek/dopheide/bro-quic - Attempt to identify QUIC protocol
zeek/dopheide/bro_notice_correlation - Adds support for multi-notice correlation.
zeek/dopheide/venom - Attempts to detect an attacker calling to the VENOM Linux Rootkit https://securit
y.web.cern.ch/security/venom.shtml
zeek/dopheide/zeek-jetdirect - Detect exploit attempt of HP JetDirect printers
zeek/dopheide/zeek-known-hosts-with-dns - This script expands the base known-hosts policy to include re
verse DNS queries and syncs it across all workers.
zeek/dopheide/zeek-known-outbound - This script provides the ability to monitor and throw notices for o
utbound connections to a list of watched countries.
zeek/dopheide/zeek-notice-config - This script enables easy customation of how notice actions are handl
ed.
zeek/dopheide/zeek-ntp-monlist - This script just replaces the old ntp-monlist script to work with Zeek
 3.0.0+
zeek/dopheide/zeek-ssh-interesting-hostnames-with-known - This script replaces the default ssh/interest
ing-hostnames and reduces the number of asyncrhonous when() calls made by Zeek.
zeek/dovehawk/dovehawk - MISP+Zeek.
zeek/dovehawk/dovehawk_dns - Dovehawk.io Passive DNS Capture Module.
zeek/dovehawk/dovehawk_flow - Dovehawk Anonymized Outbound Flow Tracking
zeek/dw2102/S7Comm-Analyzer - Protocol parser for the Siemens S7Comm and S7CommPlus protocol
```

Want to learn more?

https://github.com/andrewbeard/broworkshop