Zeek

Jonathan Cole
Dakota State University
Dec 7th, 2021

Introduction to Zeek

- Analyzes packet captures or live network traffic to provide relevant data
- Associates requests to responses for session-level logging
- Includes many built-in protocol analyzers
- Framework for extensions using scripts, integrations

About Zeek

Originally named Bro…

Written by Vern Paxson in 1995 at Lawrence Berkeley National Laboratory

Initially designed as a traffic analysis system, not an intrusion detect tool

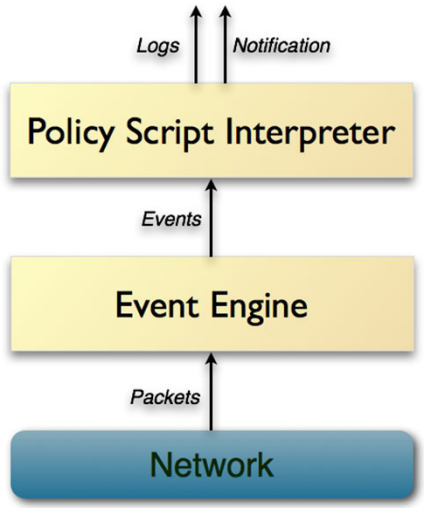
Open source, but commercial options available from Corelight

- Corelight @ Home
- Security Onion, RockNSM

Zeek Architecture

Analyzers:

- Packet
- Protocol
- File



Sample Protocol Parsers:

DHCP	HTTP	MySql	SMTP	Syslog	NTLM
DNS	IRC	RADIUS	SSH	Tunnels	RDP
FTP	Kerberos	SIP	SSL	DCE-RPC	SMB

Outputs - Network Analysis

conn.log - TCP/UDP/ICMP connections (similar to NetFlow)

dns.log - DNS activity (equivalent to passive DNS log content)

http.log - HTTP activity

rdp.log - RDP activity

smtp.log - SMTP activity

smb_mapping - connection detail and path for mapped SMB shares

Outputs - File Analysis

files.log - File analysis (hash, etc.)

x509.log - Certificate information

pe.log - Portable Executable (Windows executable) files

smb_files.log - Files reconstructed from SMB activity

Outputs - Inventory Analysis

known_devices.log - Observed system inventory

known_services.log - Observed service inventory

software.log - Observed software inventory

Output - Specialized Analysis

signatures.log - matches to signature rules

weird.log - unexpected protocol observations

intel.log - matches observed using the Zeek Intelligence Framework

notice.log - Potentially concerning traffic observations

Correlating Fields

Unique IDs

- Connections - `uid`
  - same across all fields, can link multiple logs
- File - `*_fuid`
  - not the same, deterministic for a given run

Community ID

- Provides a unique value to describe a conversation
- Similar to uid, but designed to be tool agnostics
  - Works in Arkime, Beats, Wireshark, and more

Value consists of an encoded hash with several values:

```
version+":"+base64(sha1(seed+source_address+destination_address+protocol+0x00+source_port+destination_port))
```

Extending Zeek - Frameworks

Zeek Package Manager

- 150 in packages.zeek.org

Plugins (C++)

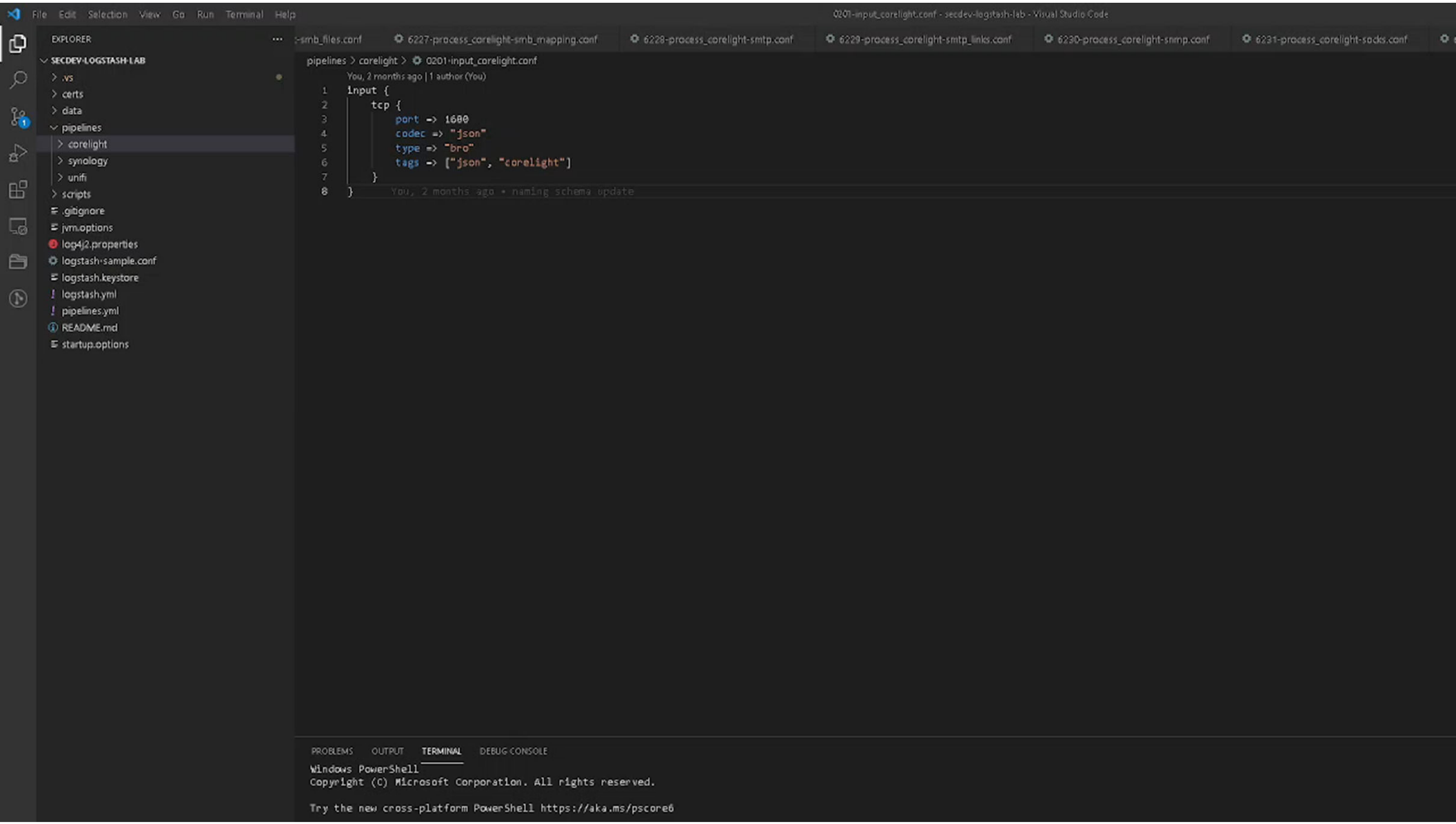
- Pac files (source files for binpac)

Signature Engine

Scripts

- Zeek Scripting Language
- Spicy - open source parser generator, abstracts binpac
  - File Analyzer or Protocol Analyzer

Demo


File Edit Selection View Go Run Terminal Help
0201-input_corelight.conf - secdev-logstash-lab - Visual Studio Code
EXPLORER
SECDEV-LOGSTASH-LAB
.vs
certs
data
pipelines
corelight
synology
unifi
scripts
.gitignore
jvm.options
log4j2.properties
logstash-sample.conf
logstash.keystore
logstash.yml
pipelines.yml
README.md
startup.options
-smb_files.conf
6227-process_corelight-smb_mapping.conf
6228-process_corelight-smtp.conf
6229-process_corelight-smtp_links.conf
6230-process_corelight-snmp.conf
6231-process_corelight-socks.conf
pipelines > corelight > 0201-input_corelight.conf
You, 2 months ago | 1 author (You)
input {
tcp {
port => 1600
codec => "json"
type => "bro"
tags => ["json", "corelight"]
}
}
You, 2 months ago • naming schema update
PROBLEMS
OUTPUT
TERMINAL
DEBUG CONSOLE
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6

Conclusion

Next steps:

- Learn Zeek Scripting - https://try.zeek.org
- Zeek Developer Wiki - https://github.com/zeek/zeek/wiki#development-guides
- Zeek Community - https://zeek.org/community/
  - Slack Channel is active