Learning Zeek's Language

Joe Abraham
NETWORK SECURITY CONSULTANT
@joeabrah www.joeabrahamtech.com

Overview

Zeek signature framework

Default scripts

- Demo

What do you want to see?

- Demo

Zeek script customization

Zeek Scripting

Zeek provides users with a domain-specific, Turing-complete *scripting language* for expressing arbitrary analysis tasks

Behavior and signature analysis

Other detection models

Modular organization allows for adding/ removing capabilities

Many inputs to choose from

Event-driven Model

Events are natively not good or bad

- Scripts tell Zeek what to do with events
- Can be alerts or other actions

The Zeek Signature Framework

Signature Framework

Gives Zeek signature analysis/rule-based functionality

Write specific criteria for events or traffic to match; alert or other action invoked after signature is tripped

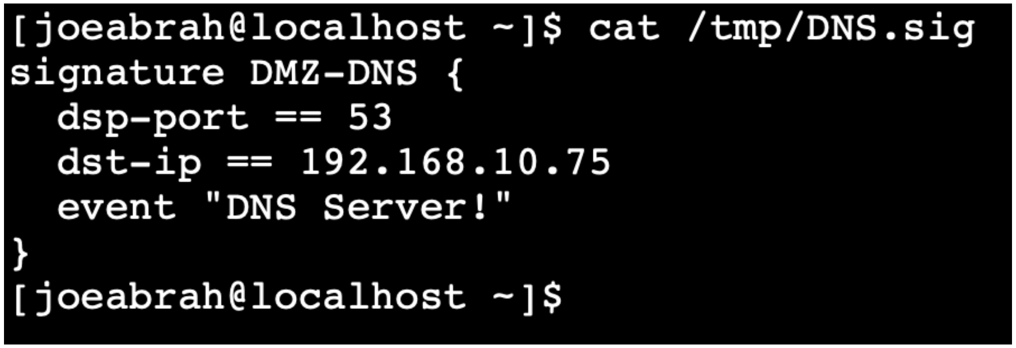
More like typical IDS with rules based on type of traffic, header information, contents of payload

Reach out on port 53

DNS server in DMZ

Can write for wrong DNS

Matched on defined parameters



```
[joeabrah@localhost ~]$ cat /tmp/DNS.sig
signature DMZ-DNS {
  dsp-port == 53
  dst-ip == 192.168.10.75
  event "DNS Server!"
}
[joeabrah@localhost ~]$
```

Signature Matching

Header Conditions

Source/Destination IP, protocols, etc.

Content Conditions

Use regex to match content

Dependency Conditions

Match other signatures or other dependencies in Zeek

Zeek Signature Actions

Event

Raises event (log, email, etc.) via script or plugin

Enable

Activate analyzers or scripts dynamically based on signature

Demo

Look at signature within CLI

Discuss contents

Run PCAP through rule

Looking at Zeek’s Scripts

Zeek Scripts

base/ Directory

policy/ Directory

Demo

Explore base/ directory

Break down sample script

What Do You Want to See?

What Information to Look For?

What are your use-cases?

Globomantics wants “network monitoring”

Capstats, misconfigurations, etc.

Network monitoring/security go together!

What Will the Tool Provide?

Turn on default scripts if you’re not sure, tune over time

What’s the normal protocol behavior? Where are my DNS and DHCP servers?

Do we need custom scripts or signatures as well?

Tuning is ongoing for all monitoring and security devices

Zeek Script Customization

Customizing Zeek’s Scripts

Operators

== != < >

Types

Boolean, time, etc.

Attributes

&log, &default, etc.

Declarations

Export, option, etc.

Statements

local, add, delete

Directives

@DIR, @LOAD, etc.

Event Handlers

Similar to functions, do not return a value but are called from a script and executed after event is detected

Logging Scripts

Customize based on needs

Change from ASCII to JSON

Custom formats

Module Recap

Summary

Zeek language

Signature framework

Zeek default scripts

What do you want to see?

Zeek script customization

Coming up: Tracking Zeek’s Discoveries