Optimizing Rules with New Features

Matt Glass

CISSP, CEH

www.linkedin.com/in/matthewglass2

Overview

Leverage new options in Snort version 3

Utilizing active response

Leveraging AppId

Processing files by type and hash

Guidelines for rule writing

Course Summary

Leveraging Snort Version 3 Features

Active Response

Active response features enable Snort to interrupt potential hostile traffic flows.

react

Drops the request and sends a custom HTML page to the source

reject

Injects TCP resets or ICMP unreachable packets

rewrite

Overwrites packet content with new values specified in the rule

AppId

Provides application identifiers to Snort rules for processing

Contains pre-defined applications and allows for custom detectors

Rules can leverage AppID to take actions based on app usage

Demo

Leveraging the active response and AppId options

Address these security goals:

- Configure react to send a block page and use a rule to send this page when external users attempt to access Metasploitable over HTTP.
- Use the same block page for internal use of Twitter.

Test your rules

Snort File Processing

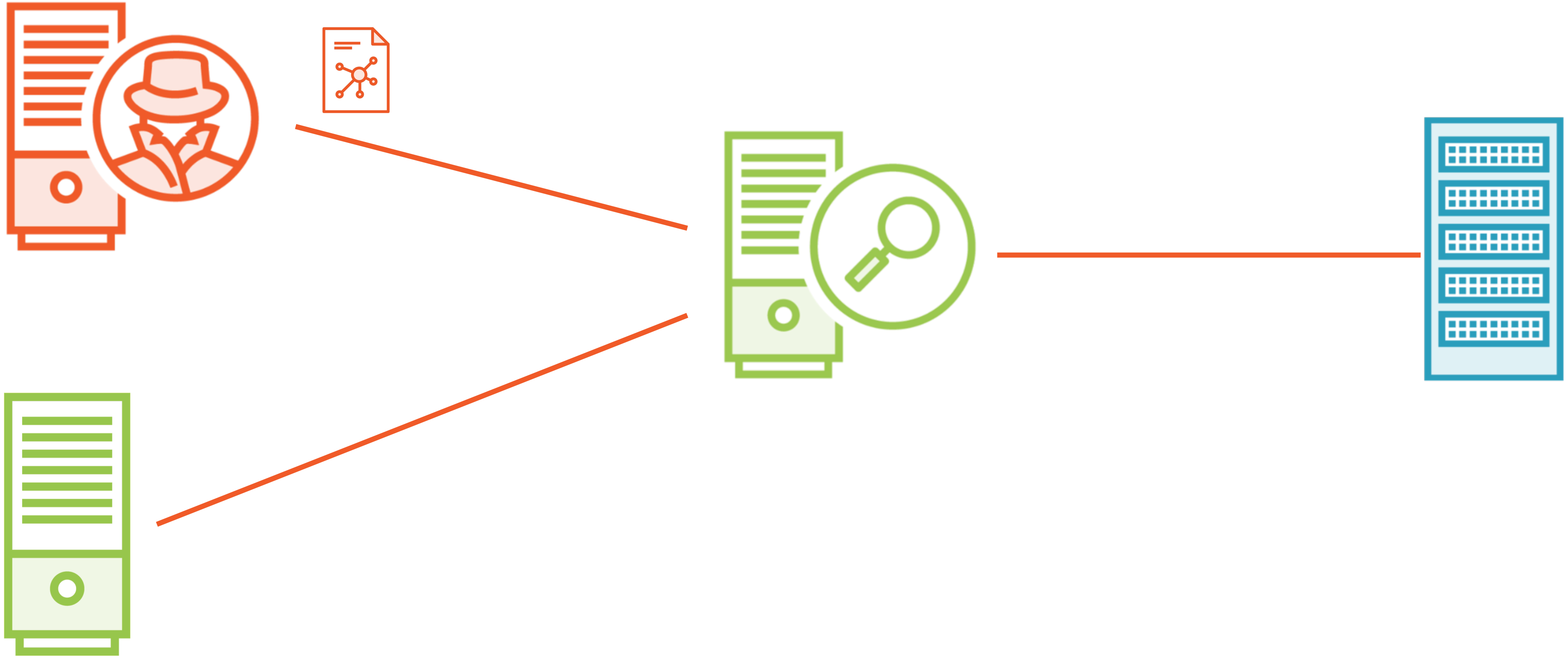
Detecting Files by Type

Snort version 3 file detection is configured in snort.lua

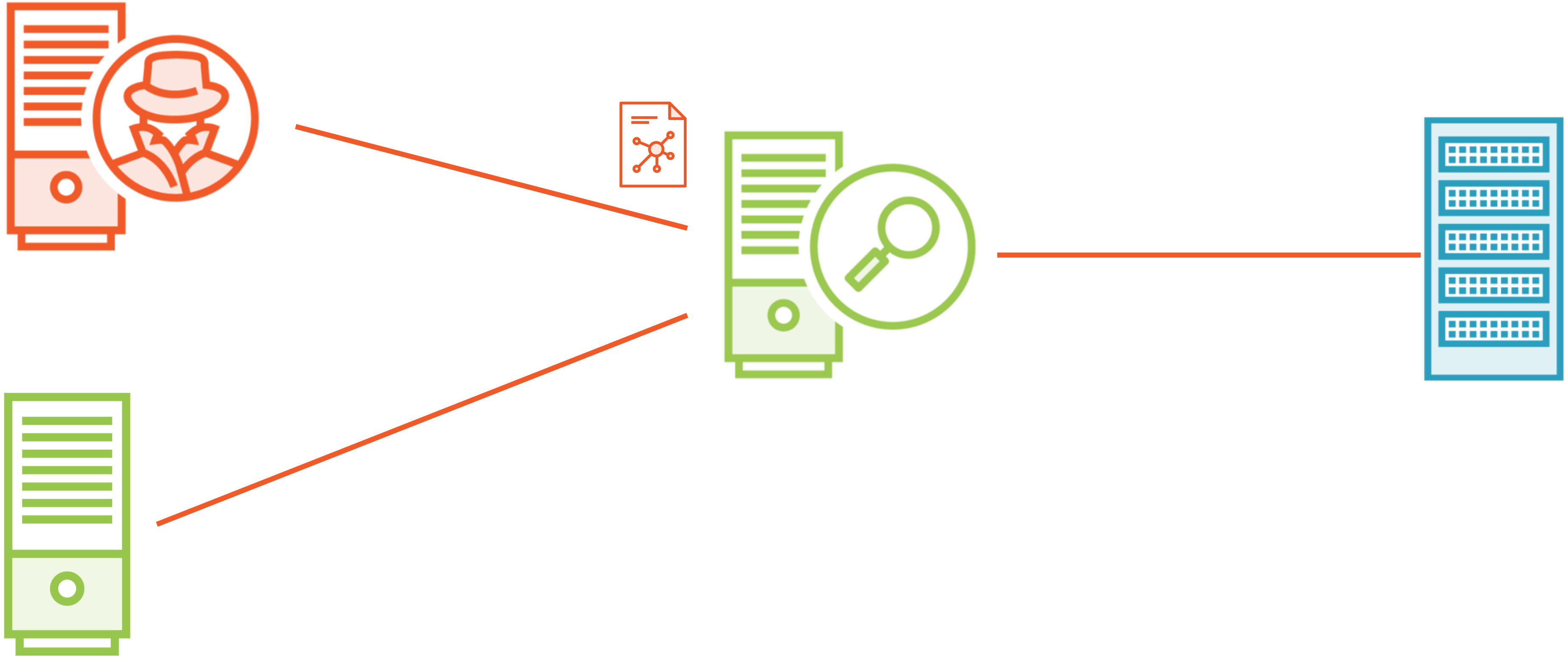
References file_magic.lua to detect file types

Custom file types can be added to detect more types

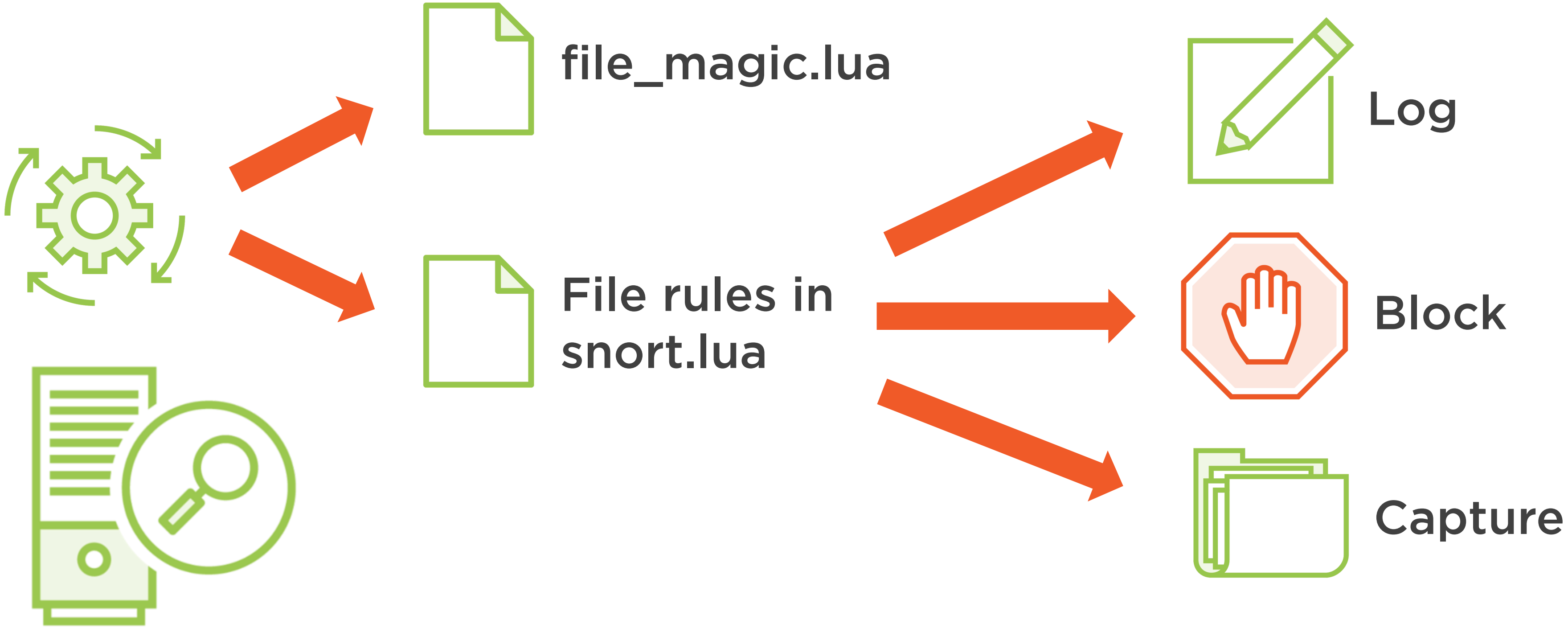
Detecting Files by Type



Detecting Files by Type



Detecting Files by Type



file_magic.lua

File rules in snort.lua

Log

Block

Capture

File processing in Snort is limited to HTTP, SMTP, IMAP, POP3, FTP, and SMB

Demo

Using Snort File Detection

- Log executable files that are transferred across Snort
- Capture transferred files for analysis and future use

Test your rules

Demo

Create a malicious file blacklist

- Use SHA values of known malicious files to create rules
- Detect and block future transmissions of the captured files

Test your rules

Wrapping Up

Writing Good Snort Rules

Good Snort rules not only catch the target traffic, they also maximize speed and efficiency while minimizing false positives.

Use content

Content matching reduces false positives

Vulnerability focus

Write based on what is vulnerable not a specific exploit of that vulnerability

Order matters

Place non-payload options before content to maximize speed and efficiency

Summary

Purpose of custom rules

Wrote your first Snort rules

Leveraged content payload detection

Used non-payload options

Enhanced rules with version 3 capabilities

Detected and blocked malicious files

Continued Learning

Continue refining and testing your custom rules

Explore each version of Snort and its capabilities

Introduce new options and test your ability to detect threats