Welcome to

8. Network Intrusion Detection

Communication and Network Security 2021

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

8-Network-Intrusion-Detection.tex in the repo security-courses

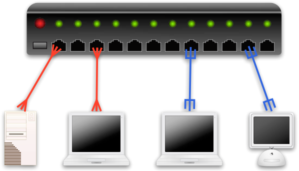
Goals for today

The Zeek Network Security Monitor

Todays goals:

- See how sniffing can be automated using two example tools Zeek and Suricata
- Use Ansible to provision services - which can easily be modified to cover multiple servers
- See some network tool configs

Plan for today



Subjects

- Intrusion Detection Systems
- NIDS vs HIDS
- Suricata Zeek
- Network Security Data Visualization
- Kibana Dashboards

Exercises

- Run Zeek and Suricata on small pcaps

Time schedule

- 17:00 - 18:15
  Introduction and basics
- 30min break
- 18:45 - 19:30
- 15min break
- 19:45 -20:30 45min

Reading Summary

ANSM chapter (7,8),9,10 - 140 pages
DETECTION MECHANISMS
Generally, detection is a function of software that parses through collected data in order to generate alert data.
This software is referred to as a detection mechanism.

Chapter 7 Detection Mechanisms, Indicators of Compromise, and Signatures
Chapter 8 Reputation-Based Detection
Chapter 9 Signature-Based Detection with Snort and Suricata
Chapter 10 The Bro Platform // Now Zeek

Zeek in the default configuration activates 10.000s of script lines out-of-the-box.
Gives great output with little effort and complements Suricata/NIDS

Reading Summary, continued

The Zeek Network Security Monitor

ANSM chapter 7: Detection Mechanisms and Indicators of Compromise, and Signatures

- Indicators of Compromise (IOC) any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner
- Background information, useful when we talk about Zeek (previously Bro) later
- Intrusion Detection Systems try to detect ... but what if we know that some domains, servers, IPs etc are signs of bad activity - even compromise
- IP reputation - some IPs are used for controlling malware command and control (C2) servers etc.
- A signature can contain one or more IOCs

Reading Summary, continued

ANSM chapter 8: Reputation-Based Detection

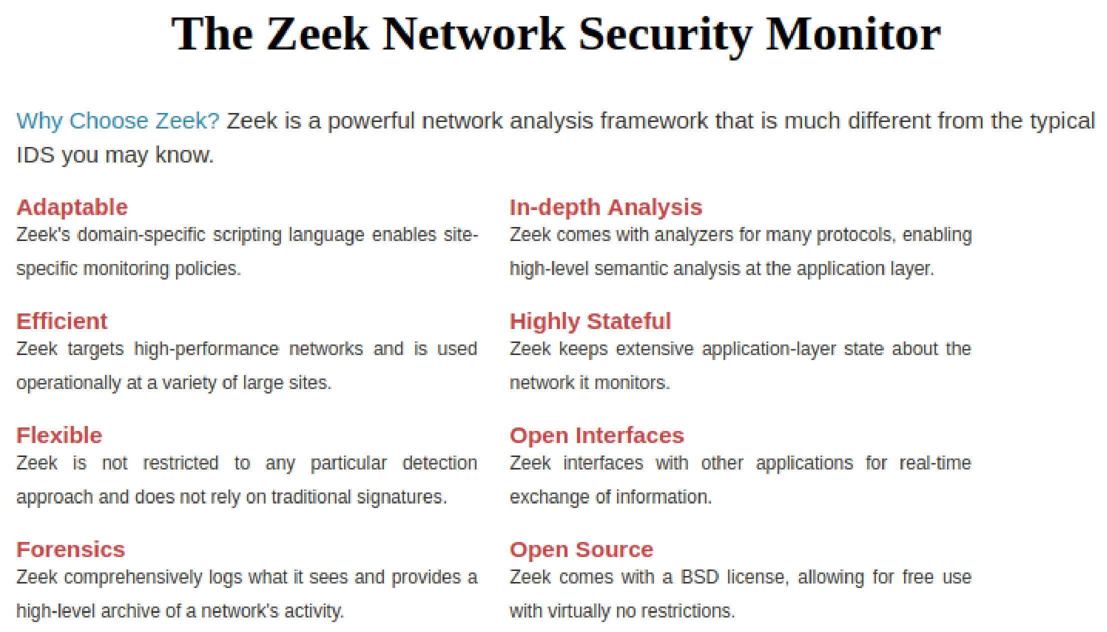
- The most basic form of intrusion detection is reputation-based detection
- Similar concept to block lists for SMTP spam relays
- I often recommend https://github.com/stamparm/maltrail as a source of lists
- Other sources are lists like RIPE NCC delegated, which IP prefixes are handed out in different countries
  https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest
  ripencc|DK|ipv4|185.129.60.0|1024|20151130|allocated|
- Mentions SiLK https://tools.netsa.cert.org/silk/
  If we end up having time today, or another day, we should look into this tool chain also!

Reading Summary, continued

ANSM chapter 9: Signature-Based Detection with Snort and Suricata

- Suricata IDS
- IDS rules are introduced
- I recommend a commercial license for the EmergingThreats ruleset

Reading Summary, continued



The Zeek Network Security Monitor

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Zeek's domain-specific scripting language enables site-specific monitoring policies.

Efficient
Zeek targets high-performance networks and is used operationally at a variety of large sites.

Flexible
Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

In-depth Analysis
Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Highly Stateful
Zeek keeps extensive application-layer state about the network it monitors.

Open Interfaces
Zeek interfaces with other applications for real-time exchange of information.

Open Source
Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

ANSM chapter 10: The Zeek (Bro) Platform

- Zeek concepts and logs - many useful ones by default!

Intrusion Detection

- networkbased intrusion detection systems (NIDS)
- host based intrusion detection systems (HIDS)

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

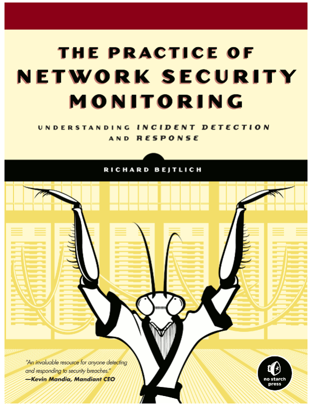
Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

Reading Summary, False Positives

- True Positive (TP). An alert that has correctly identified a specific activity. If a signature was designed to detect a certain type of malware, and an alert is generated when that malware is launched on a system, this would be a true positive, which is what we strive for with every deployed signature.Indicators of Compromise and Signatures
- False Positive (FP). An alert has incorrectly identified a specific activity. If a signature was designed to detect a specific type of malware, and an alert is generated for an instance in which that malware was not present, this would be a false positive.
- True Negative (TN). An alert has correctly not been generated when a specific activity has not occurred. If a signature was designed to detect a certain type of malware, and no alert is generated without that malware being launched, then this is a true negative, which is also desirable. This is difficult, if not impossible, to quantify in terms of NSM detection.
- False Negative (FN). An alert has incorrectly not been generated when a specific activity has occurred.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

Network Security Monitoring

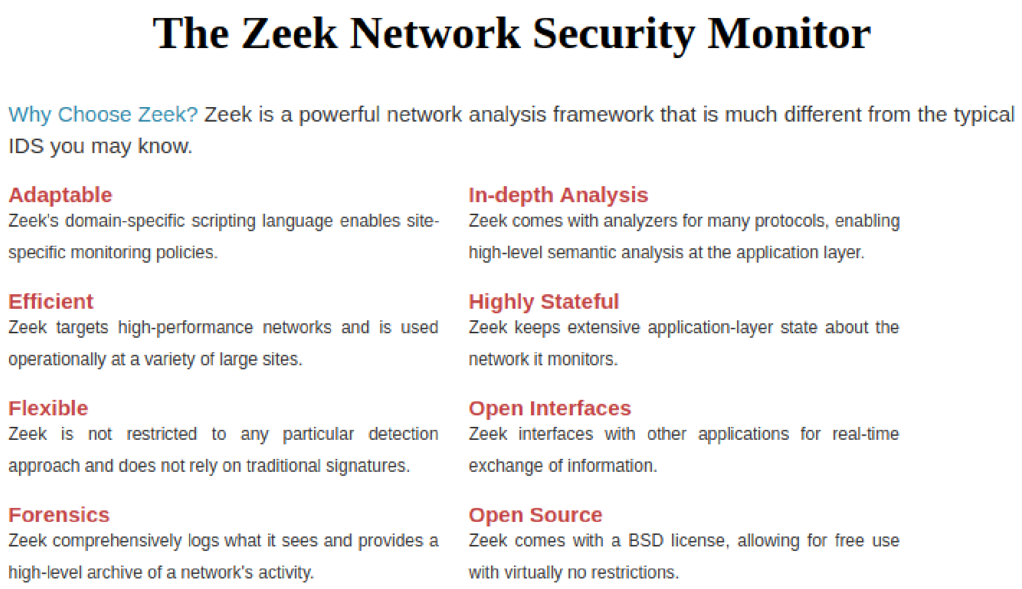

THE PRACTICE OF
NETWORK SECURITY
MONITORING
UNDERSTANDING INCIDENT DETECTION AND RESPONSE
RICHARD BEJTLICH
"An invaluable resource for anyone detecting and responding to security breaches."
—Kevin Mandia, Mandiant CEO
no starch press

Network Security Monitoring (NSM) - monitoring networks for intrusions, and reacting to those

Recommend the book *The Practice of Network Security Monitoring Understanding Incident Detection and Response* by Richard Bejtlich July 2013

Example systems are Security Onion `https://securityonion.net/` or SELKS `https://www.stamus-networks.com/open-source/`

The Zeek Network Security Monitor



The Zeek Network Security Monitor

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Zeek's domain-specific scripting language enables site-specific monitoring policies.

Efficient
Zeek targets high-performance networks and is used operationally at a variety of large sites.

Flexible
Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

In-depth Analysis
Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Highly Stateful
Zeek keeps extensive application-layer state about the network it monitors.

Open Interfaces
Zeek interfaces with other applications for real-time exchange of information.

Open Source
Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework

Zeek is the tool formerly known as Bro, changed name in 2018. `https://www.zeek.org/`

Zeek IDS is

The Zeek Network Security Monitor

While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

`https://www.Zeek.org/`

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

`http://suricata-ids.org/` `http://openinfosecfoundation.org`

We will now move to the workshop materials:
Suricata, Zeek og DNS Capture
`https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop`

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools