Welcome to

2. Find, Fix, F3EAD started

Introduction to Incident Response Elective, KEA

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/
2-Find-Fix-F3EAD-started.tex in the repo security-courses

Goals for today

- Intelligence-driven incident-response process
- F3EAD process: Find, Fix Finish, Exploit, Analyze, Disseminate

Photo by Thomas Galler on Unsplash

Plan for today

- First phases of the F3EAD cycle
- Find phase, which identifies the starting point for both intelligence and operational activities
- Fix phase, tracking down signs of adversary activity on your networks
- Start using tools – find tools for the job

Exercise theme:

- Work with a packet capture – extract data
- Choose tools, research tools

Time schedule

- 1) Going over my presentation, first part of F3EAD Find – first 45min
- 2) Nitroba packet capture analysis – 45 min
- Break 15min
- 3) Next part of F3EAD Fix – 2x45min including 4)
- 4) Looking more into tools – which tools should we have used
- At the end summary of today and questions

Reading Summary

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

Part II: Practical Application

> Once you understand the fundamentals, it is time to get down to business. Part 2 steps through the intelligence-driven incident-response process using the F3EAD process: Find, Fix Finish, Exploit, Analyze, Disseminate. These steps will ensure that you are gathering and acting on the right information in the right order to get as much as possible from the intelligence-driven incident-response processes.

- Chapter 4: Find
- Chapter 5: Fix

Chapter 4: Find

This chapter focuses on the Find phase, which identifies the starting point for both intelligence and operational activities. In the traditional F3EAD cycle, the Find phase often identifies high-value targets for special operations teams to target. In intelligence-driven incident response, the Find phase identifies relevant adversaries for incident response.

In the case of an ongoing incident, you may have identified or been given some initial indicators and need to dig for more;

Source: Source: *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

kea

Actors Versus People

> Identity is a funny thing. In many cases, when we say they or them or refer to an adversary, it's easy to assume we're referring to the people behind an attack. In some, rare cases, we are talking about the actual individuals (this is called attribution, some- thing we'll discuss more in the intelligence chapters). But in most cases when we're referring to actors, we refer to a persona based on the tactics, techniques, and pro- cesses (TTPS) used together to achieve a goal. We mentally group these together and personify them, since human beings understand stories told that way. This is an abstraction, because we usually don't know if it's one person or a large group. We call this abstraction of linked TTPs and a goal an actor, regardless of the number of people involved.

Source: Source: *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

- Compare this to the MITRE ATT&CK framework adversaries and groups
  https://attack.mitre.org/

Identification

The Identification phase is the moment where the defender identifies the presence of an attacker impacting their environment. This can occur though a variety of methods:

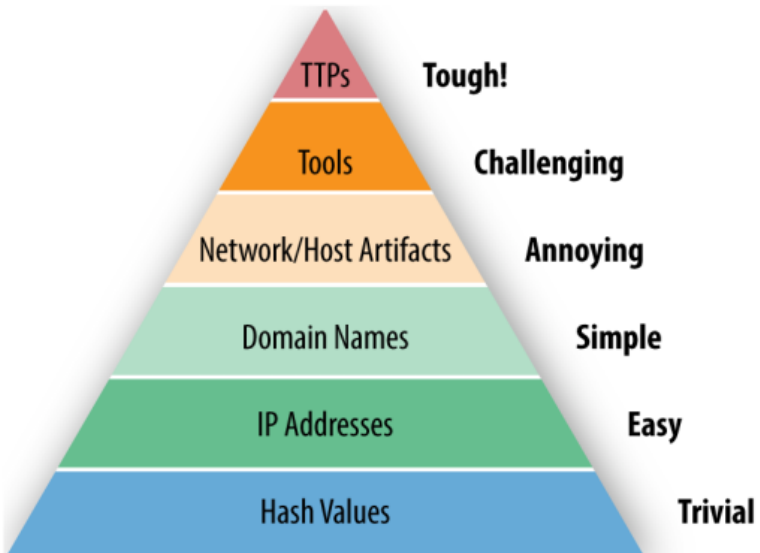
- Identifying the attacker entering the network, such as a server attack or an incoming phishing email
- Noticing command-and-control traffic from a compromised host
- Seeing the massive traffic spike when the attacker begins exfiltrating data
- Getting a visit from a special agent at your local FBI field office
- And last, but all too often, showing up in an article by Brian Krebs

Starting with Known Information

In **almost every situation**, some **information will be available** on threat actors, whether that comes from previous incidents or attack attempts within your own envi- ronment (internal information) or intelligence reports produced by researchers, ven- dors, or other third parties (external information). Ideally, a combination of both types will be available in order to provide the best overall picture of the threat.

- Usually something *happens*

David J Bianco's Pyramid of Pain



The most useful information is informa- tion that's hard for the actor to change. Incident responder David J. Bianco captured this concept, and its impact on the adversary, in his Pyramid of Pain

Indicator of Compromise Pieces

- Filesystem indicators – File hashes, filenames, strings, paths, sizes, types, signing certificates
- Memory indicators – Strings and memory structures
- Network indicators – IP addresses, host names, domain names, HTML paths, ports, SSL certificates

Each type of indicator has unique uses, is visible in different positions (whether mon- itoring a single system or a network), and depending on the format it's in, may be useful with different tools.

The Order of Volatility (OOV)

Table 1.2 *The expected life span of data*

Type of Data	Life Span
Registers, peripheral memory, caches, etc.	Nanoseconds
Main memory	Ten nanoseconds
Network state	Milliseconds
Running processes	Seconds
Disk	Minutes
Floppies, backup media, etc.	Years
CD-ROMs, printouts, etc.	Tens of years

Certainly care and planning should be used when gathering information from a running system. Isolating the computer—from other users and the network—is the first step. And given that some types of data are less prone to disruption by data collection than others, it's a good idea to cap- ture information in accordance with the data's expected life span.

Source: *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004

Data Formats

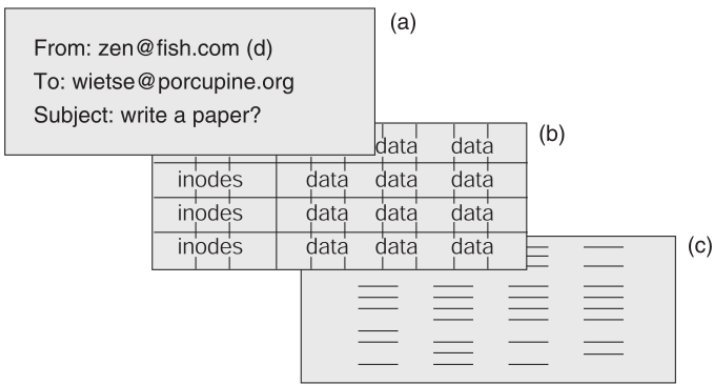
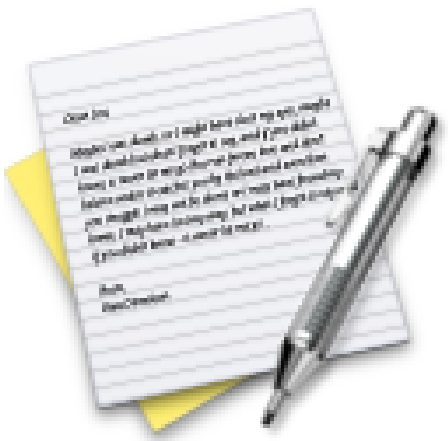


Figure 1.2 *A simplified picture of files as seen by (a) users and applications, (b) file system software in the operating system, and (c) hardware*

Source: *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004

- Data can be stored in many format, or obtained from various sources
- We should use the correct tools
- This is also why IoCs should be *expressed in a platform-independent manner*

Exercise

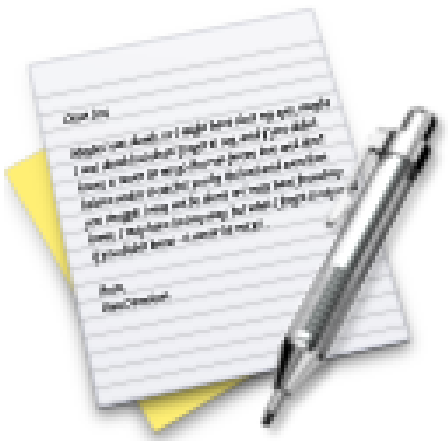


Now lets do the exercise

⚠ Nitroba Pcap 45 min

which is number **13** in the exercise PDF.

Exercise



Now lets do the exercise

Zeek on the web 10min

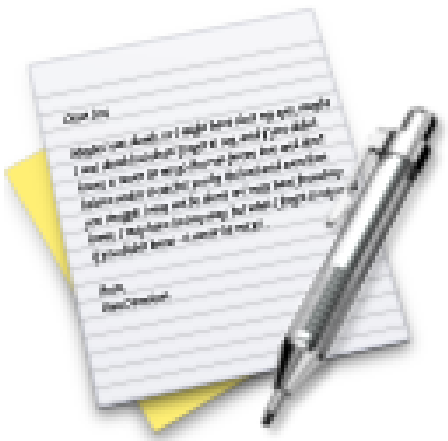
which is number **14** in the exercise PDF.

Exercise

Now lets do the exercise

Zeek decode packets 10min

which is number **15** in the exercise PDF.



Now lets do the exercise

Indicators of Compromise – zeek intel module

which is number **16** in the exercise PDF.

Chapter 5: Fix

> The process of using previously identified intelligence or threat data to identify where an adversary is, either in your environment or externally, is called a Fix. In the Fix phase of F3EAD, all the intelligence you gathered in the Find phase is put to work tracking down signs of adversary activity on your networks.

Source: Source: *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

Chapter describes three ways to *fix* the location of adversary activity:

- Using indicators of compromise,
- Adversary behavioral indicators, also known as TTPs
- Adversary goals.

Intrusion Detection – Network Intrusion Detection System (NIDS)

Network alerting involves identifying network traffic that could indicate malicious activity. Several stages of the kill chain involve network communications between the attackers and the victim machine, and it is possible to identify this activity by using intelligence. The activities we can identify by using network traffic include the follow- ing:

- Reconnaissance – network scanning, probes
- Delivery – Attachments, Links, Metadata
- Command and control – known Command and Control serves used in malware, IRC ports
- Lateral movement – unusual traffic patterns internally
- Actions on target –

Source: Source: *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

Actions on targets can be hard to identify with network data only, maybe large data transfers can be spotted, but recommend getting data from systems

System Alerting – Host Intrusion Detection System (HIDS)

The complement to network monitoring is system monitoring. In the same way that network alerting is focused on particular aspects of the kill chain, system alerting can be similarly be divided into the following areas:

- Exploitation
- Installation
- Actions over target

  System alerting is always dependent on the operating system. With rare exceptions, most tools—open source and commercial—are focused on a particular operating sys- tem. This is necessary because most security alerting takes place at the lowest levels of the operating system, requiring deep integration into process management, memory management, filesystem access, and so forth.

Source: Source: *Intelligence-Driven Incident Response* (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

- Linux buffer overflow log messages seen earlier are specific to Linux
- Windows Defender has become very advanced over the years

Zeek on Windows

kea

> As we shared at ZeekWeek 2022 in October, we're thrilled to announce emerging support for Zeek on Windows, thanks to an open-source contribution from Microsoft. Part of its **integration of Zeek into its Defender for Endpoint security platform**, this contribution provides **fully-native build support for Windows platforms** and opens up a range of future technical possibilities in this vast ecosystem. Make sure to check out Microsoft's talks on the technical aspects of this integration as well as the detection capabilities this move enables.

Source: https://zeek.org/2022/11/28/zeek-on-windows/

- Microsoft link

  https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/new-network-based-detections-and-improved-device-discovery-using/ba-p/3682111

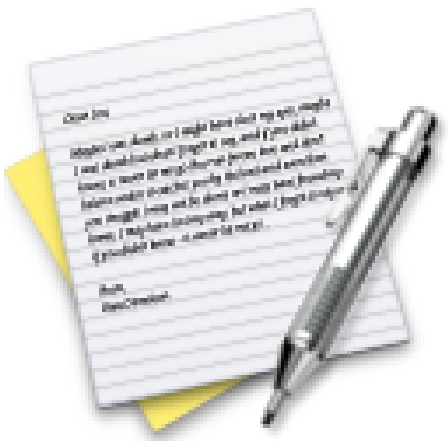
Moving to the book

We will now go through parts of the book, starting at page 87, Fixing GLASS WIZARD

Notes:

- Book still calls Zeek for Bro, name changed in 2018
- Older tools like SiLK and Argus has mostly been replaced with newer ones Elastiflow or Akvorado https://github.com/robcowart/elastiflow https://github.com/akvorado/akvorado

Exercise

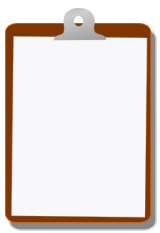


Now lets do the exercise

⚠ Log4Shell CVE-2021-44228 IoCs 30 min

which is number **17** in the exercise PDF.

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

Buy the books! Create your VMs