Welcome to

4. Structured Incident Response and IoCs

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/
4-Structured-Incident-Response-and-IoCs.tex in the repo security-courses

Goals for today

- Practical work
- How to choose between alternatives – tools and software packages
- How to get started analysing

Photo by Thomas Galler on Unsplash

Plan for today

- Book chapter 7
- Gathering data
- Why do we gather data
- How do we store this incident data
- Example case: look at the Maersk incident
- Example tools, including some Windows tools at the end!

Exercise theme:

- Installing MISP Project

Time schedule

- 1) Going over a few cases – first 45min
- 2) Choosing tools – 45 min
- Break 15min
- 3) Threat Information gathering, selecting and presenting – 45min
- 4) Buffer and Valentina Palacin book

Reading Summary

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

Now we need to **gather all of that data**, analyze it for intelligence value, and integrate it into not only detection and prevention methods, but also more strategic-level initiatives such as risk assessments, prioritization of efforts, and future security investments. To get to the point where you can do all these things, you have to engage the intelligence portion of the F3EAD cycle: Exploit, Analyze, and Disseminate.

- Chapter 7: Exploit

In the Exploit phase, we begin the process that **ensures that we learn** from the incident. We focus on the threat, and not just the enemy. Because of this, it is important that we **not only extract technical indicators** related to the particular attack, such as malware samples and command-and-control IP addresses, but **also the overarching aspects that led to the intrusion** and allowed the attackers to be, at least to some degree, successful.

Source: Source: *Intelligence-Driven Incident Response* (IDIR)

- Avoiding similar incidents is the goal

Gathering Information

Depending on how you manage your incident-response data, it is entirely possible that the most difficult part of the Exploit phase will be finding the important bits of intelligence from the investigation. When it comes to **gathering incident-response data**, we have seen it **all—from elaborate systems, to Excel spreadsheets, to Post-It notes with IP addresses stuck to a whiteboard**. There is no wrong way to gather that data, but if you want to be able to extract it so that it can be analyzed and used in the future, there are certainly some ways to make the process easier.

Source: Source: *Intelligence-Driven Incident Response* (IDIR)

Storing Threat Information

Formats listed in the book

- OpenIOC
- CyBOX, STIX, and TAXII
- Incident Object Definition and Exchange Format (IODEF) RFC 5070
- Real-time Inter-network Defense (RID)
- Vocabulary for Event Recording and Incident Sharing (VERIS)
- Common Attack Pattern Enumeration and Classification (CAPEC)
- TLP White/Green/Amber/Red (Traffic Light Protocol)

Don't worry about the names currently, remember these are often in JSON and XML

Part 1: Cases and Analyses

Learning from others is easier than doing everything wrong yourself.

Lets go and find some analysis of the Maersk NotPetya, official and not-official

- Start at *Cyber attack update JUNE 28, 2017*
  https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update
- Lets gather facts about the case – business facts and technical facts
- Since our course is incident response, lets not forget how did they recover, did they learn, could this have been avoided altogether

Part 2: Tools for Tracking Actions

A variety of tools are available to track your incident data as well as the actions that have been taken. This section covers ways to organize data, using both publicly avail- able and purpose-built tools. When you are just getting started with incident response and do not have existing systems in place to track information and actions that have been taken, it is often best to start small and grow into increased capability and functionality.

Source: Source: *Intelligence-Driven Incident Response* (IDIR)

- Evaluating tools and software packages.
- We know we are going to be handling incidents, we need multiple tools

Personal note taking apps

Figure 6-1. Using Google Sheets for a Spreadsheet of Doom

- Zim personal wiki https://zim-wiki.org/
- Obsidian https://obsidian.md/
- Spreadsheet of Doom via IDIR 118

Incident Response Apps – Threat-Intelligence Platforms

Let's discuss – what do we need? Use the book as input, consider the following:

> As you can probably tell from our coverage of standards and the numerous requirements for managing all the information that you have exploited during an investigation, capturing and analyzing all of this information is no trivial task. A **threat intelligence platform** is often used to **simplify** that process and make **gathering, storing, and searching** this information **easier**.

Source: Source: *Intelligence-Driven Incident Response* (IDIR)

- Malware Information Sharing Platform (MISP)
- Collaborative Research into Threats (CRITS)
- Your Everyday Threat Intelligence (YETI)
- FIR https://github.com/certsocietegenerale/FIR – via IDIR book page 117
  FIR is an open source ticketing system built from the ground up to support intelligence-driven incident response.

Now lets do the exercise

ⓘ Install MISP Project 45min

which is number **21** in the exercise PDF.

Part 3: Threat Information gathering, selecting and presenting

We will continue with the exercise, but also – importantly – start to consider what and how to present to management.

- What do we tell the management, what do they need?
- What should be prioritized?
- Which feeds do we need, and partners
  Example https://www.ecrimelabs.com/danish-misp-user-group https://twitter.com/danishmisp

Part 4:Buffer and Valentina Palacin book

One of the books in the Cybersecurity bundle is:

Practical Threat Intelligence and Data-Driven Threat Hunting A hands-on guide to threat hunting with the ATT&CK Framework and open source tools Valentina Palacín

- I already owned this book on paper, and consider it a great book
- Very practically oriented
- Lots of references to other tools, methods, standards
- Has exercises within

Event Tracing for Windows (ETW)

Event Tracing for Windows (ETW) is a Windows debugging and diagnostic feature that provides an "efficient kernel-level tracing facility that lets you log kernel or application-defined events to a log file."ETW allows you to trace events in production without computer or application restarts.

According to Microsoft, the Event Tracing API is broken into three components:

- Event controllers (start and stop tracing sessions and enable providers)
- Event providers
- Event consumers

Kea

Ruben Boonen developed a tool called SilkETW that tries to help with this process and allows you to download the ETW data in JSON format. This capability makes it really easy to integrate the data that's been extracted with third-party SIEMs such as Elasticsearch and Splunk. In addition, the JSON can be converted and exported into PowerShell and you can combine Yara Rules with SilkETW to enhance your research.

- https://github.com/fireeye/SilkETW (also take note of the company FireEye)
- Let's try it!

Sysinternals

The Valentina book also references the old-skool and always relevant Sysinternals tools!

If you have been keeping up with the threat hunting news lately, you may have seen that Sysmon seems to be everyone's favorite. System Monitoring (Sysmon) is part of **Mark Russinovich's Sysinternals Suite** (https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite). The reason why it gained such attention is because it turned out to be a great way to achieve endpoint visibility without impacting the system's performance.

Sysmon is a system service and device driver that monitors and logs system activity to the **Windows event log**. Sysmon configuration can be adjusted to better suit our collection needs since it **provides XML rules that can include and exclude uninteresting items**. The list of available filter options increases with each Sysmon upgrade.
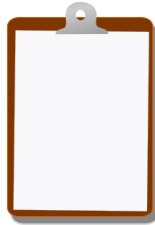
- Originally started as ntinternals back in 1996!

Now lets do the exercise

⚠ DNSSEC KeyTrap 20min

which is number **22** 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