Welcome to

# 9. Rinse and Repeat: Redo exercises, work through examples

## 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/

9-rinse-and-repeat.tex in the repo security-courses

# Goals for today


- Make sure it all *connects* – why did we ...
- Summary of the course
- Know what to expect at the exam

Photo by Thomas Galler on Unsplash

# Plan for today

- Go through exercises again – why are some with infocirle and some with triangle
- Exam subjects, questions, finishing up

Exercise theme:

- Revisit some exercises? especially if related to incident response

# Time schedule

- 1) Exercise summary – 45min
- 2) More exercises and discussion – 45 min
- Break 15min
- 3) Exam related items – 45min
- 4) Finishing up – 45min

# Part 1-2: Exercise Summary

We did a lot of exercises, hopefully they helped us gain insights

- We will now go through the table of contents, I will desribe why we did these exercises
- Part 2 will be you redoing some specific exercises – some of the important ones!

# Part 3: Exam related items

kea

You can now ask questions, or we can walk through all the subjects

Notes: Exam subjects for Introduction to Incident Response

- Exam will be up to 25 min
- Keywords listed are *ideas* for things to go through not a checklist
  Consider it example items that fit into this subject.
- You will only have 10 min to go through your presentation
- Feel free to include tools and references to tools throughout!
- Watch out if you do a demo! Better to have a video without audio, and talk over it
- After this we will do up to 15 min of questions and dialogue in the subject and the course

# Subjects 1-2

## 1. Overview of Incident Response

Why do we need Incident Response, a few threats and context
Definitions of Incident Response, Computer Forensics
Main resources we have used, IDIR book, NIST, other books

## 2. Cyber Attack Phases and IR

Main processes and methods, intrusion kill chain, incident response cycle
Overall description of how attacks happen, and how we deal with them
Mitre ATT&CK framework can be used here

# Subjects 3-4

## 3. Incident Response Life Cycle

Detailed about what happens when we have identified an incident
Go through the phases and explain as much as possible within 10minutes
Use NIST SP800-61r2 figure 3-1, IDIR or other books or references as you wish
You can also use the F3EAD process
You can even present overview and compare instead

## 4. Order of Volatility and Tools

Explain the concept of Order of Volatility (OOV) from Forensics Discovery, Farmer Venema 200
List example tools, explain how they fit with volatility
Why do we run memory tools first, and can wait with disk and storage analysis
Live Response vs cold images and files with data

## 5. Evidence and IoCs

Anything related to facts we find and use
Definitions of IoCs, examples of IoCs
Domains, DNS, Passive DNS,
File related, Hash values, IP addresses
Enrichment and metadata related to facts
Processing of facts, where do we find them
Ideas Whois, RIPE Stat, RIPE delegated list of IP prefixes etc.
Logging can also be used here

kea

## 6. Tools we have used during the course

Take your favourite tool we have used in classe, create screenshot
Walk us through the process, what it provides, how the tool helps, what is the output
Beware you CAN do demos, but if something goes wrong ... better to have a video without sound and present IMHO
Brim, tcpdump, wireshark, Packetbeat
Sysinternals
Zeek, Suricata
Volatility framework
Loki IOC and YARA scanner
MISP Project
... anything we mentioned in class or tried is OK

## 7. How to establish an Incident Response Capability

What are the steps to create this capability in an organisation
Use input from NIST document and IDIR book also provides detailed information
Also the exercise from March 30 may help
Select the parts of this which interest you the most, can be organizational, technical or a
Outline steps which you would propose to a CEO when you got hired as CISO

## 8. Vulnerability Cases

Ideas

a) Take a known vulnerability, like Log4Shell Go through how it works, what it does, what are prerequsites etc. What are some IoCs, signs of intrusion with this Focus on how this relates to Incident Response, how would an organisation react

OR

b) What preperative steps could help CMDB?, how would architecture changes reduce likelihood or prevent this from happening How can organisations learn from cases in other organisations

OR

c) Budgets and incident response Talk about steps from the incident response life cycle and how it relates to cost - usually it is MUCH more efficient to spend a little on preparation, to shorten incidents

# Part 4: Finishing up in this course

We do have another day, but lets summarize:


I would like to use some time to finish up this course.

- Was it useful?
- Do you want to work within this specific area
- Do you want to know *about* security or work *in security*