Welcome to

7. Threat Hunting and Intelligence

Introduction to Incident Response Elective, KEA

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

Slides are available as PDF, kramse@Github

7-Threat-Hunting-and-Intelligence.tex in the repo security-courses

Goals for today

- Adversary emulation
- Performing disk analysis
- See what a privilege escalation can look like

Photo by Thomas Galler on Unsplash

Plan for today

- Adversary emulation
- Privilege escalation – what is it
- Example privesc on Linux
- Finding persistence and bad files – example with Linux

Exercise theme:

- Privilege escalation with SUID
- Disk image forensics
- Cloud environments influence on incident response

Time schedule

- 1) Talk about another resource, Valentina Palacín book – first 45min
- 2) Investigate a few links from this book – 45 min
- Break 15min
- 3-4) Exercises privilege escalation and disk imaging – 2x45min

Reading Summary

Browse chapter 1 from Practical Threat Intelligence, Valentina Palacín - if you have it

Practical Threat Intelligence and Data-Driven Threat Hunting Valentina Palacín, 2021, ISBN: 978-1-83855-637-2

- Chapter 1: What Is Cyber Threat Intelligence?
- This book is very much hands on with lots of links, references, tools and names
- I will now present a bit from the book, since you don't have it

Investigate links

- We cannot go through all of it, but we can get inspired
- Since this came from real actors, campaigns, threats it is mostly what a real case would be

This will lead to the later part, doing *an investigation*

Investigate links 1: OSSEM

OSSEM: To help with the heavy work of creating data dictionaries, the Rodriguez brothers created the Open Source Security Events Metadata (OSSEM) for documenting and standardizing security event logs. The project is open source and can be accessed through the project's GitHub repository https://github.com/hunters-forge/OSSEM.

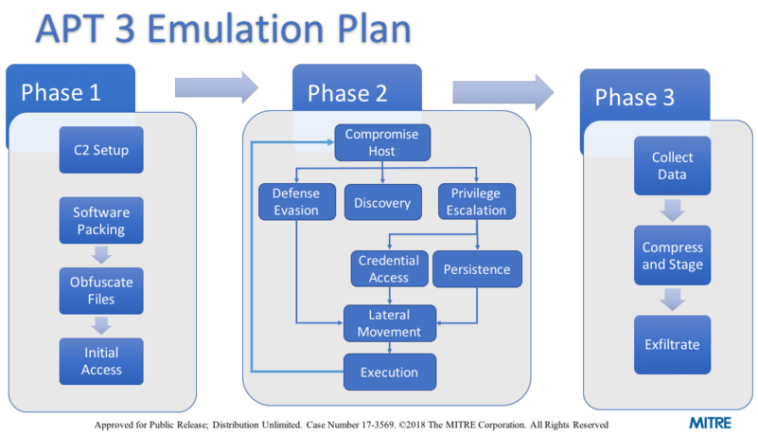
Investigate links 2: Threat Hunter Playbook

The Threat Hunter Playbook: This open source project is maintained by the Rodriguez brothers and is meant to help with the documentation project and sharing threat hunting concepts, developing certain techniques, and building the hypothesis. You can read more about it in the project's GitHub repository https://github.com/hunters-forge/ThreatHunter-Playbook

Investigate links 3: Adversary emulation

Emulating the adversary: Adversary emulation is a way for red teamers to replicate adversary behaviors in their organization's environments. In order to do that, the adversary behaviors need to be mapped and the techniques used by them need to be chained together to create an action plan. The MITRE ATT&CK™ Framework provides an example of how to create an emulation plan based on APT3
https://attack.mitre.org/resources/adversary-emulation-plans/

MITRE Adversary Emulation Plans



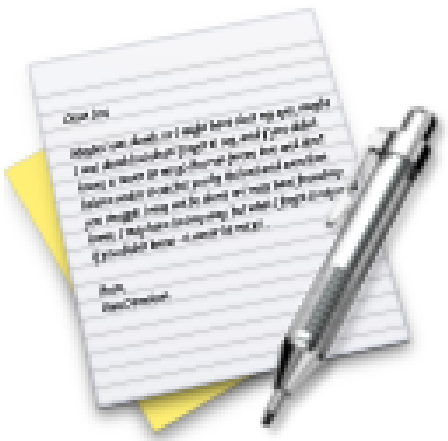
To showcase the practical use of ATT&CK for offensive operators and defenders, MITRE created Adversary Emulation Plans. These are prototype documents of what can be done with publicly available threat reports and ATT&CK.

Source: https://attack.mitre.org/resources/adversary-emulation-plans/

Investigate links 4: Mordor dataset

Mordor: For this stage of the hunt, the Rodriguez brothers created the Mordor project, which provides "pre-recorded security events generated by simulated adversarial techniques"in JSON format.
https://github.com/hunters-forge/mordor

Exercise

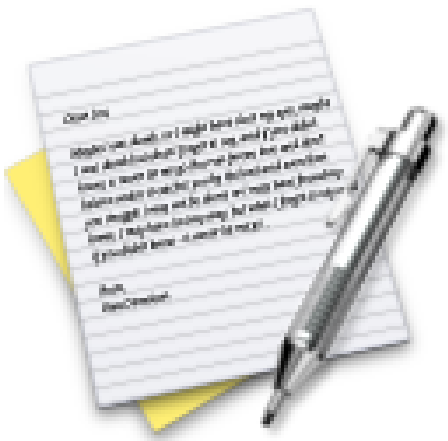


Now lets do the exercise

⚠ Privilege escalation using SUID 30min

which is number **23** in the exercise PDF.

Exercise

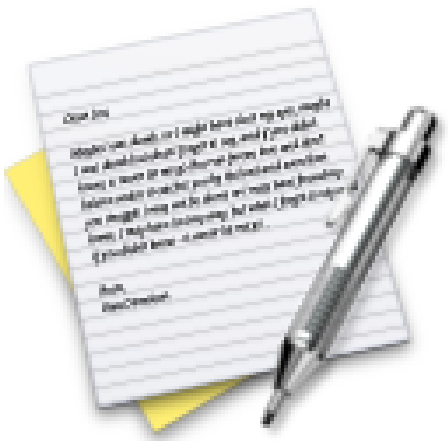


Now lets do the exercise

⚠ Disk Image Forensics – 45 min

which is number **25** in the exercise PDF.

Exercise

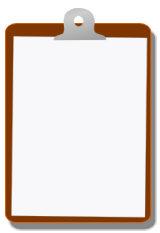


Now lets do the exercise

ℹ Cloud environments influence on incident response 20min

which is number **24** 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

Read the books! Play with tools