How to Become Friends With Your RA Team

(with the Help of an Agency)

Pass The Salt 2023 Rump session

Thibault Blaiset

Disclaimer

- This is a « last minute » lightning talk so :
  - haven’t told « the Agency » about this lightning talk and they might not fully agree with what I suggest
  - haven’t checked my employer’s « public talks policy »
  - … what follows are my own opinions, not anyone else’s

« Mandatory whoami »

- Thibault Blaiset

- Always been in infosec
  - mostly Risk Assessment (RA)
  - some incident response
  - a little bit of part-time pentesting

- So far less advanced than most of you regarding deep technical stuff

The Problem

let's imagine the Pentest team

doesn't know how to become friends with

the Risk Assessment team

The Solution

Luckily, they will HAVE to work together … because The Principal suggests them to do so

EBIOS RISK MANAGER

2 / Participants in the workshop[20]

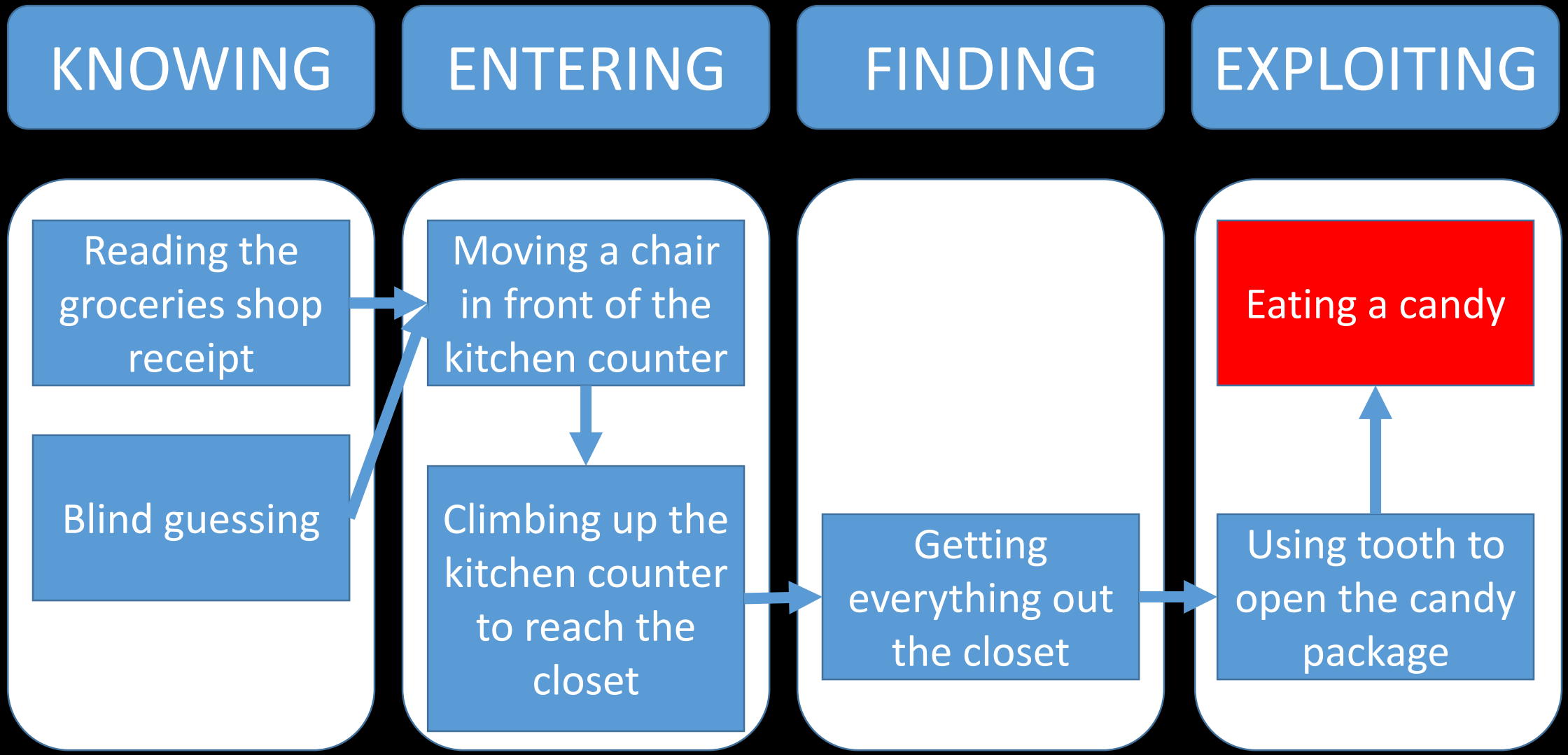
- CISO;
- IT department/Information management team;
- A specialist in cybersecurity will possibly supplement the working group, according to the team's level of knowledge and the desired level of precision.

A Quick Word on EBIOS-RM

- EBIOS-RM : risk assessment method by ANSSI
- Your RA team might be using it
- Helps Product Owners make sensible decisions about IT security risks
- Takes up to 5 workshops with PO, IT, etc.
- Today’s talk is only about the « technical one »
  - comes after defining the scope, the threat model and « Strategic scenarios »

[https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/]

Workshop 4 - Child-Candy Example (simplified)



The Key to Your New Friendship

Templating
Templating
Templating

Templating ? What do You Mean ?! It has Already Been Done !

- *Today we'll work on defining Operationnal Scenario templates*

- *[….]*

- *It looks like we are going to write a MITRE ATT&CK framework clone …*

Actually, the goal is to customise some content for the organisation's specific context

What do the RA Team Expect ? How Will all this Help Them ?

- Probably 10 to 20 scenario templates
  - some might look like the Child-Candy example
  - others may be composed of 50+ items (APT, Supply chain, etc.)

- When performing a new RA, the team will then be able to « import » the templates and tune them to the the scope of the assessment

Pros and Cons

- Cons
  - Takes time
  - Can seem painful and boring
- Pros
  - Helps your company's RA team better design the technical parts of the scenarios
  - Gives all of us an opportunity to get vulnerabilities better covered

  → Saves time for everyone

So In the End it’s Mostly Pros

Credits

- All EBIOS-RM content belongs to the ANSSI
- Pictures from « Never Have I Ever » belong to Netflix

Thank you !

Don’t hesitate to reach out to me (firstname.lastname@assurance-maladie.fr)