Opposing Force

[Attack Trees] Methodology and Application in Red Teaming Operations

hackinthebox

Keeping Knowledge Free for Over a Decade

who am i

- Matteo Beccaro | Twitter: @_bughardy_
  - Chief Technology Officer at @_opposingforce.
  - Conference speaker & trainer.
  - Messing around with networks and protocols.
  - Often flying around the globe.
- Founder & CTO at **Opposing Force**
  - The first Italian firm specialize in offensive physical security

OPPOSING FORCE

what do we do

- at **Opposing Force**
  - We dedicate big % of our time in internal RESEARCH on HARDWARE, SOFTWARE and METHODOLOGY
  - We assess the HUMAN, CYBER and PHYSICAL security of Corporations and Governments.
  - We perform ATTACK SIMULATIONS with extended scope (often no limitations at all).

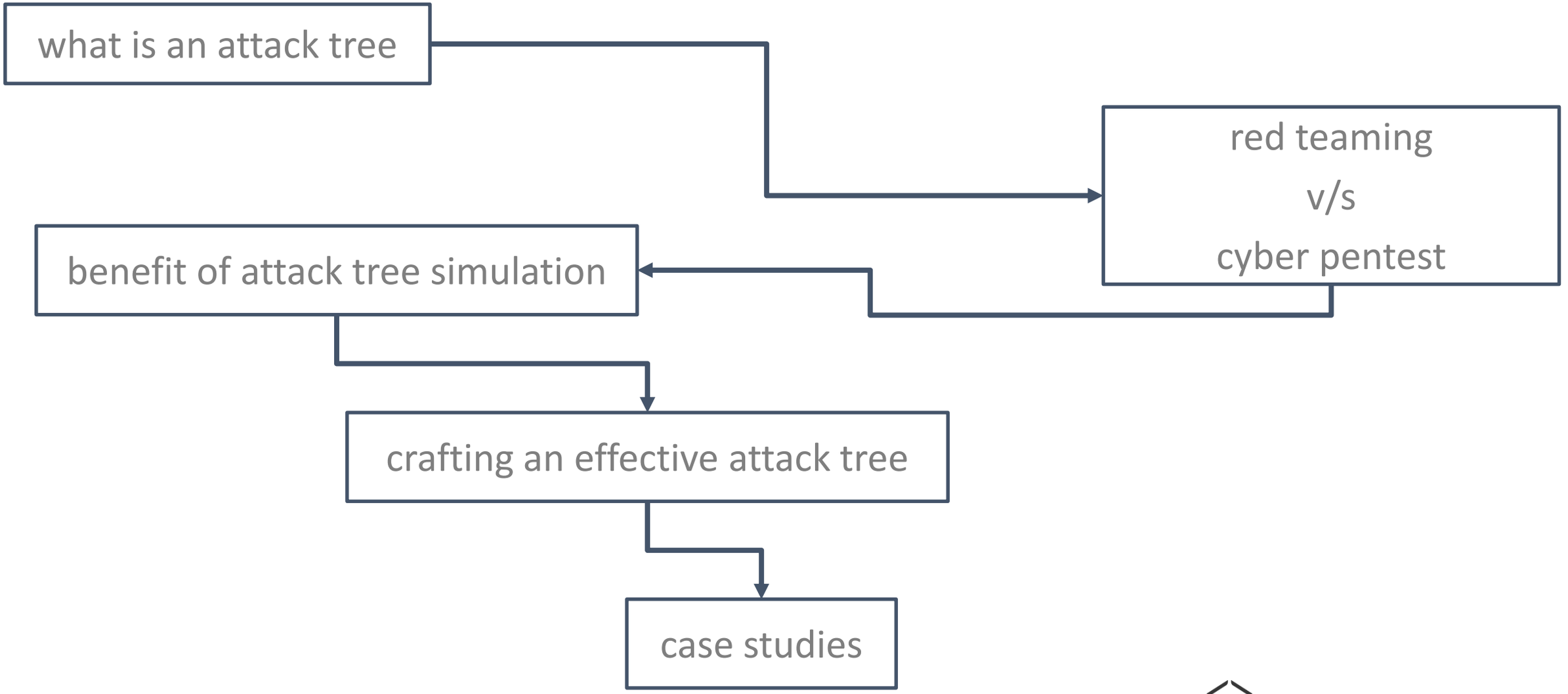
what do we do

- in **2018** we started working on ATTACK TREE theory, trying to apply it to our engagement.
  - We quickly found that it could help to speed up the information gathering and crafting of attack scenarios phases.
  - To meet our purposes we had to adapt it to the OFFENSIVE side.
  - We also need rules to quickly adapt our strategy to a fast changing scenario where information and events can be unpredictable.

what do we do

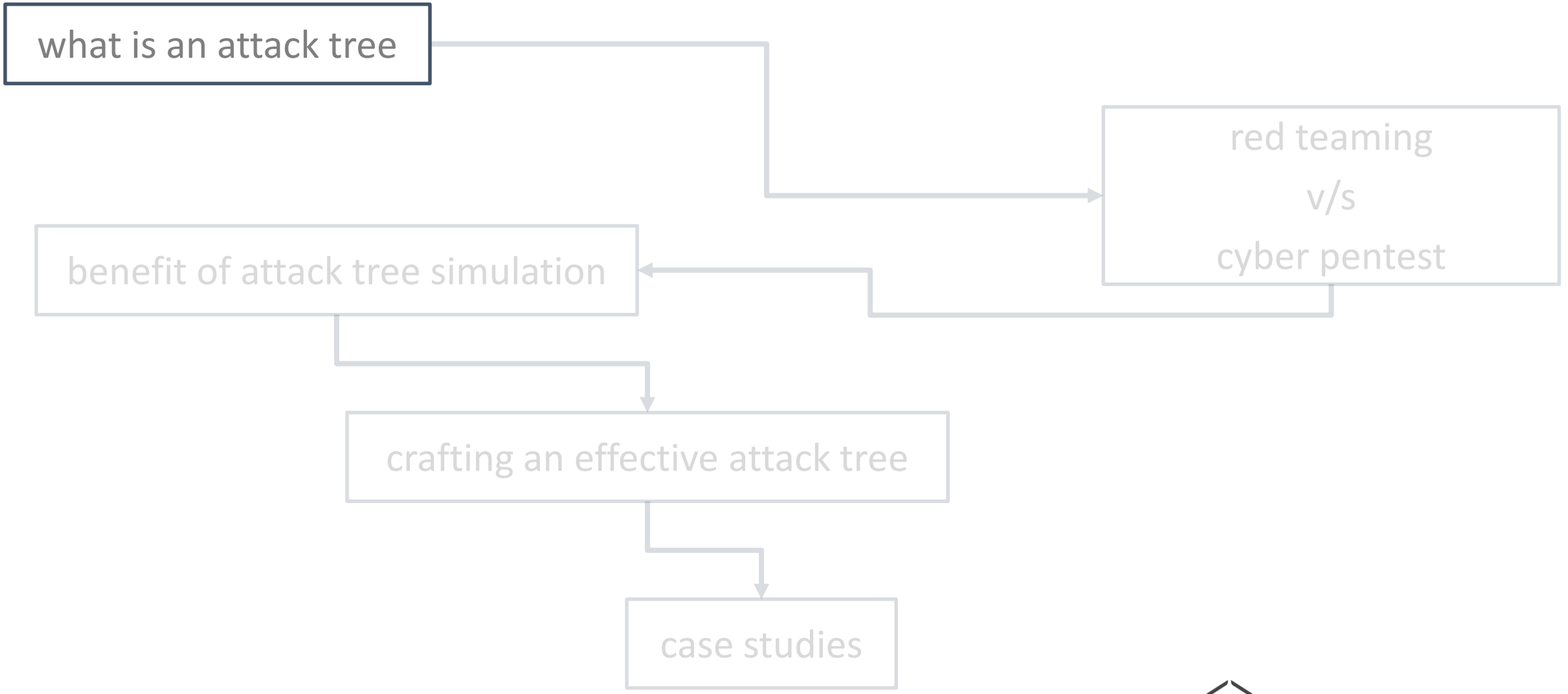
…so, what is an attack tree? how can I apply it?

agenda



OPPOSING FORCE

agenda



OPPOSING FORCE

what is an attack tree

"Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes." - Bruce Schneier

what is an attack tree

Citing again Bruce Schneier, Attack Trees are:

- A way of thinking and describing security systems and subsystems.
- A way of building an automatic database that describes the security of a system.
- A way of capturing expertise, and reusing it.
- A way of making decisions about how to improve security, or the effects of a new attack on security.

what is an attack tree

An *Attack Tree*, in its standard definition, is a formal way to perform threat and risk analysis of a defined system.

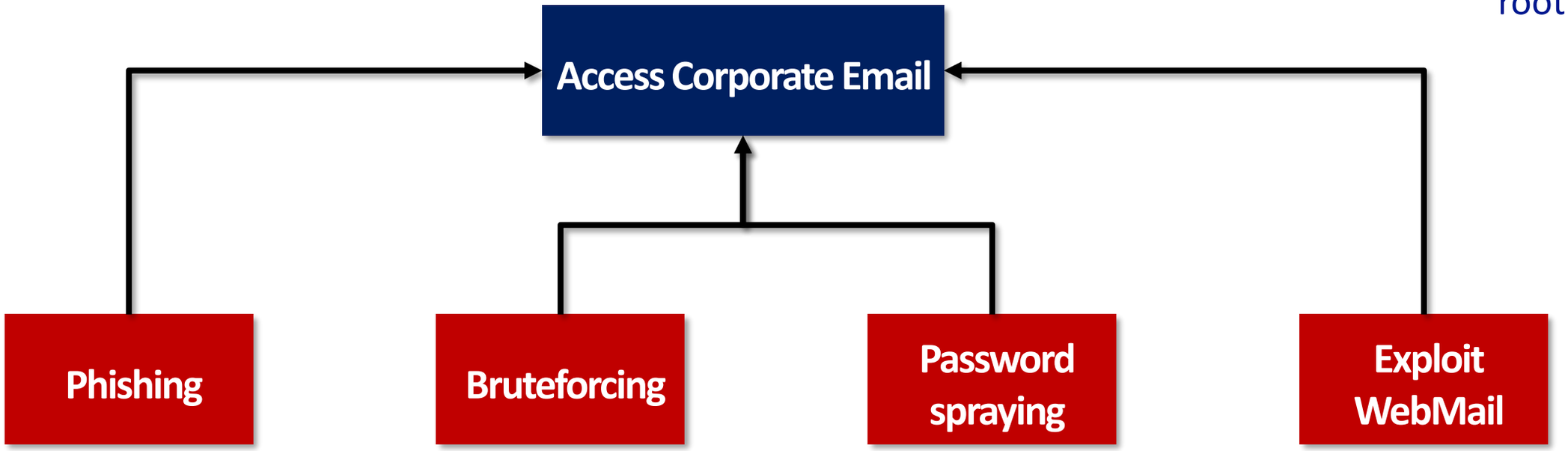
what is an attack tree

An attack tree is composed by two (2) main elements: *leaf nodes* and *root node(s).*

- A root node is the goal of the overall attack
- A leaf node is a specific attack

what is an attack tree

leaf nodes
root node

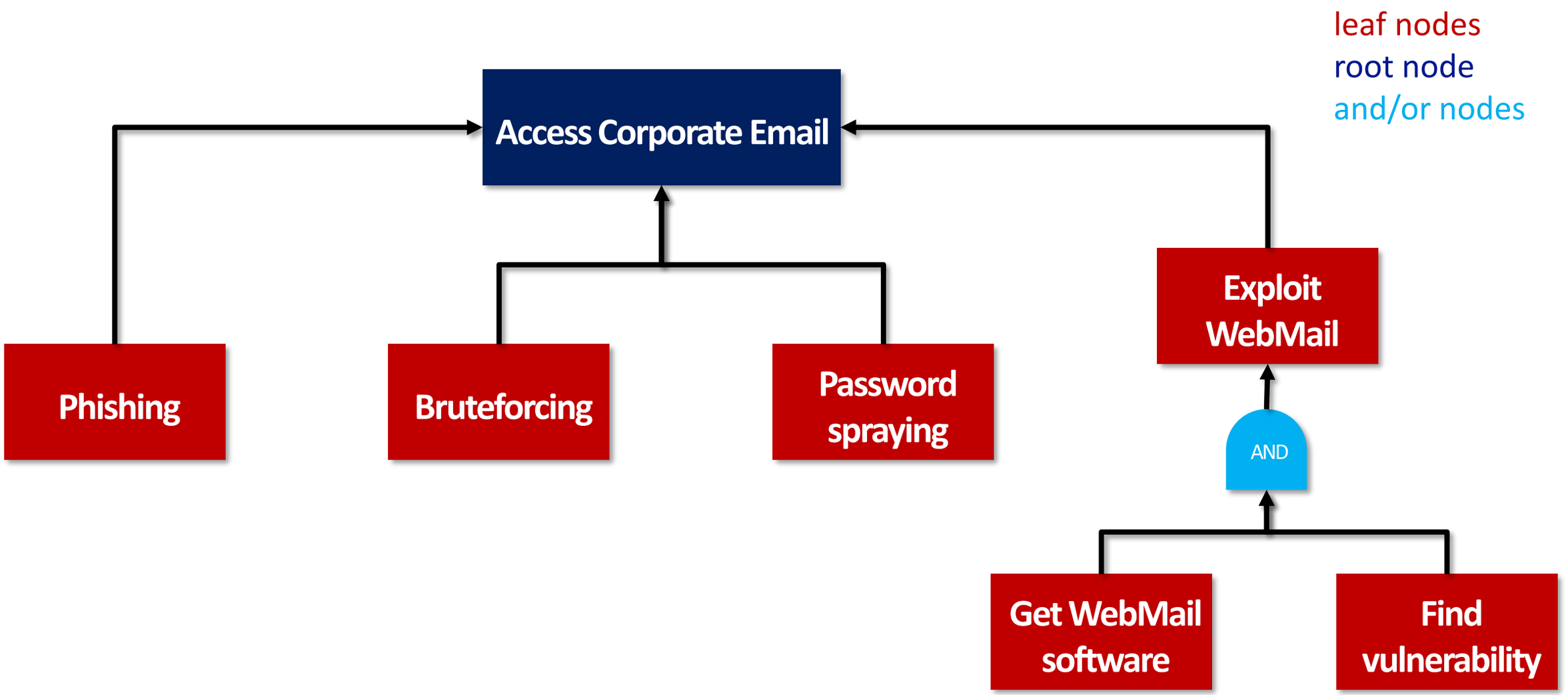


what is an attack tree

An attack tree is composed by two (2) main elements: *leaf nodes* and *root node(s).*

- A root node is the *goal* of the overall attack.
- A leaf node is a specific attack (or *subgoal*).
- And / Or node represent different way to achieve the attack:
  - An *and node* means all sub-attacks must be achieved.
  - An *or node* means at least one attack must be achieved.

what is an attack tree



what is an attack tree

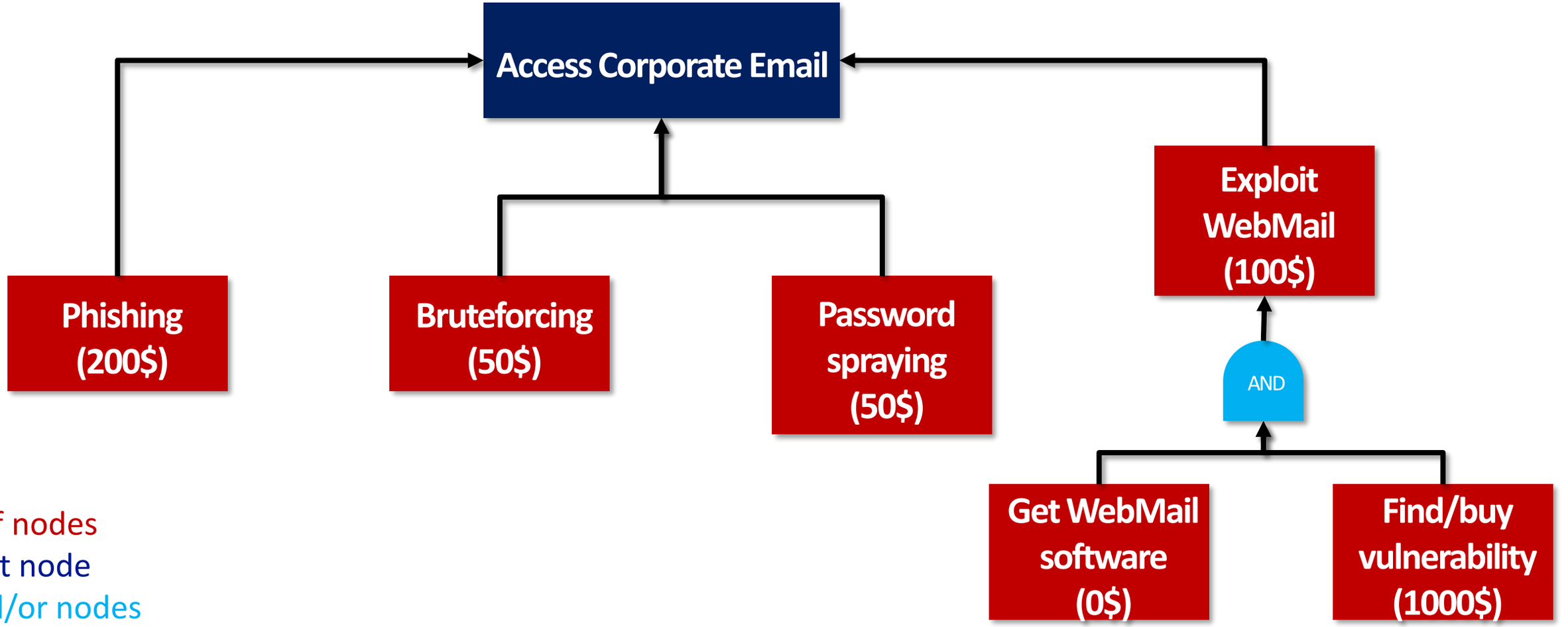
We shall define a value for each *leaf node* in order to understand the attack scenarios against the asset, *root node,* we want to defend.

This value can be:

- Boolean: doable, not doable.
- Continuous: cost, risk, etc to attack or defend.

In our example we will use the cost needed for the attack to succeed.

what is an attack tree



leaf nodes
root node
and/or nodes
X = cost

OPPOSING FORCE

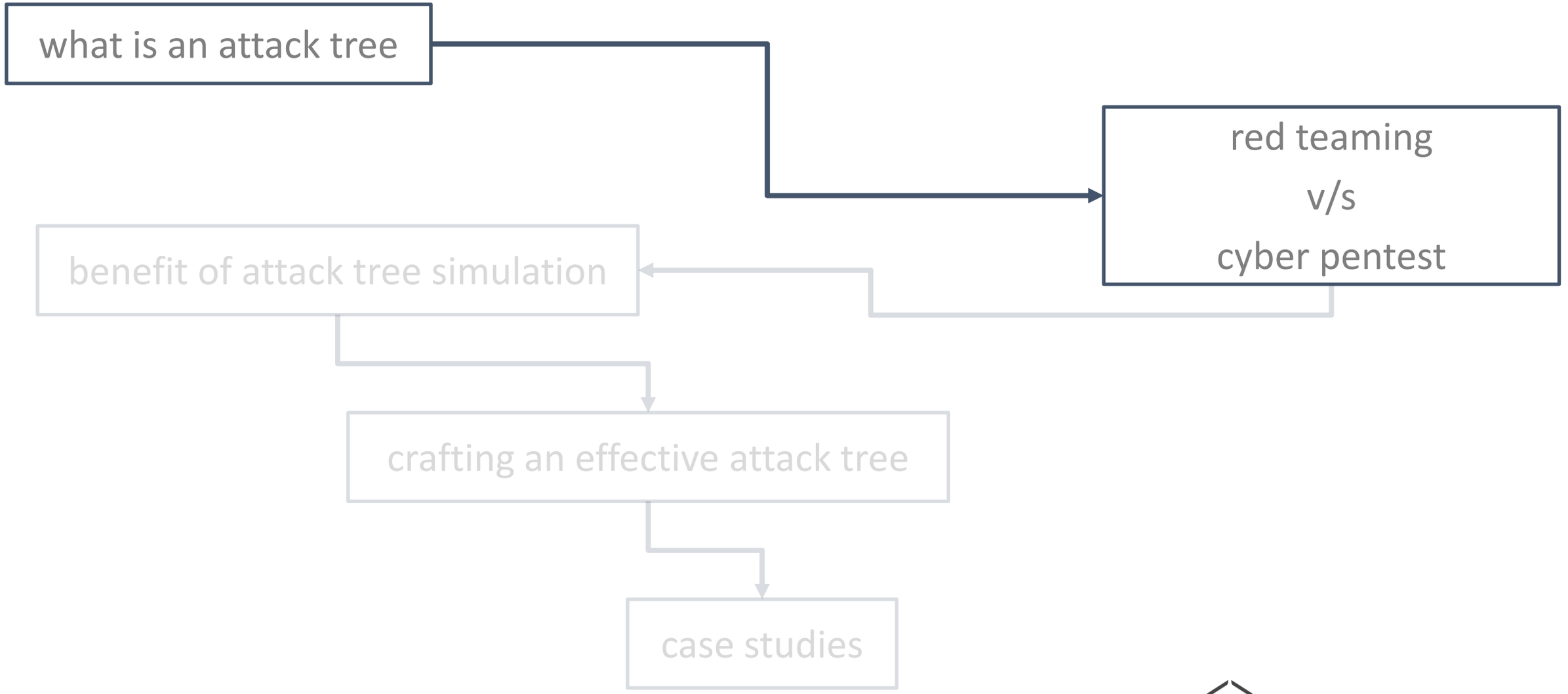
what is an attack tree

In complex scenarios we could have multiple *goals*, or assets, to protect.

More complex attack tree can be messy to represent graphically.

From a defensive point of view, the goal of an attack tree is to identify possible attacks and increase their costs/risk, or reduce their probability applying appropriate countermeasure.

agenda



OPPOSING FORCE

red teaming v/s cyber pentest

Ninjas	
Strengths	**Weaknesses**
Fast	No Armor
Stealthy	Small
Dedicated to Training	
Hand-to-Hand/Sword Combat	

Pirates	
Strengths	**Weaknesses**
Strong	Loud
Brute-Force Attack	Drunk (Some say this could be a strength too)
Great at Plundering	Can be Careless
Long-Range Combat	

https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/

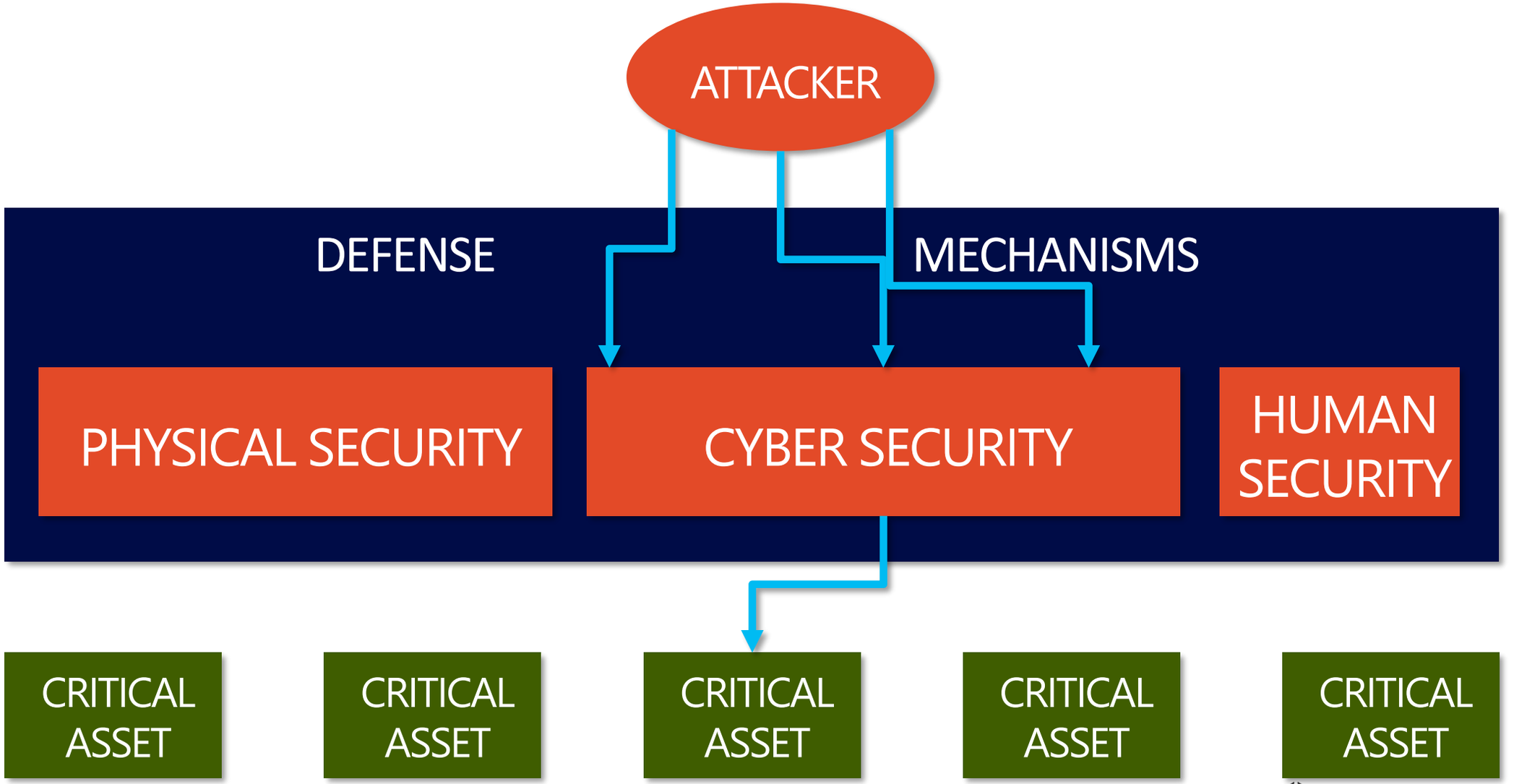
OPPOSING FORCE

red teaming v/s cyber pentest

“penetration testing is validating a configuration when you believe it to be secure.”

Daniel Miessler (https://danielmiessler.com/study/security-assessment-types)

red teaming v/s cyber pentest



OPPOSING FORCE

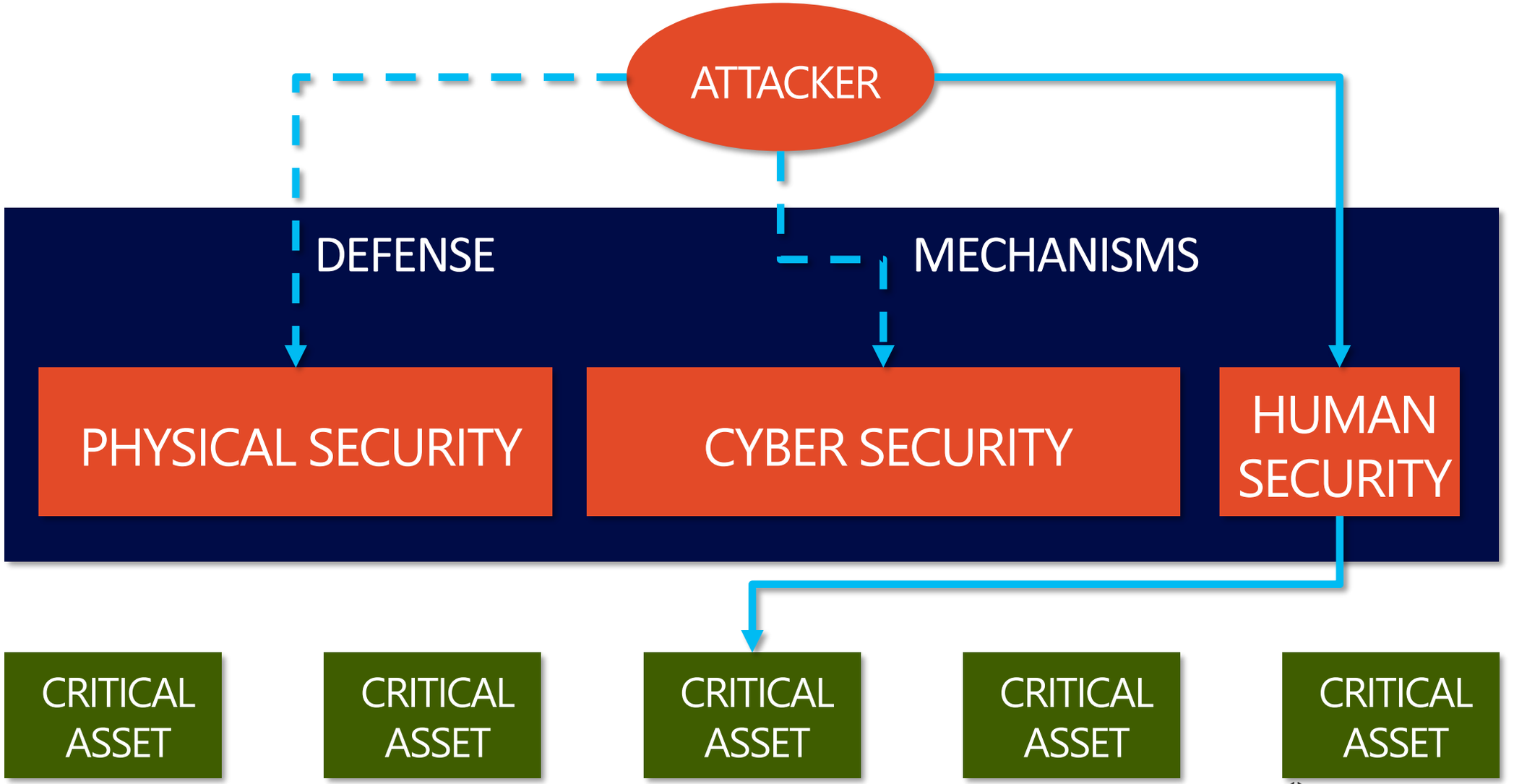
red teaming v/s cyber pentest

“red team” is: an independent group that challenges an organization to improve its effectiveness.

Daniel Miessler (https://danielmiessler.com/study/security-assessment-types)

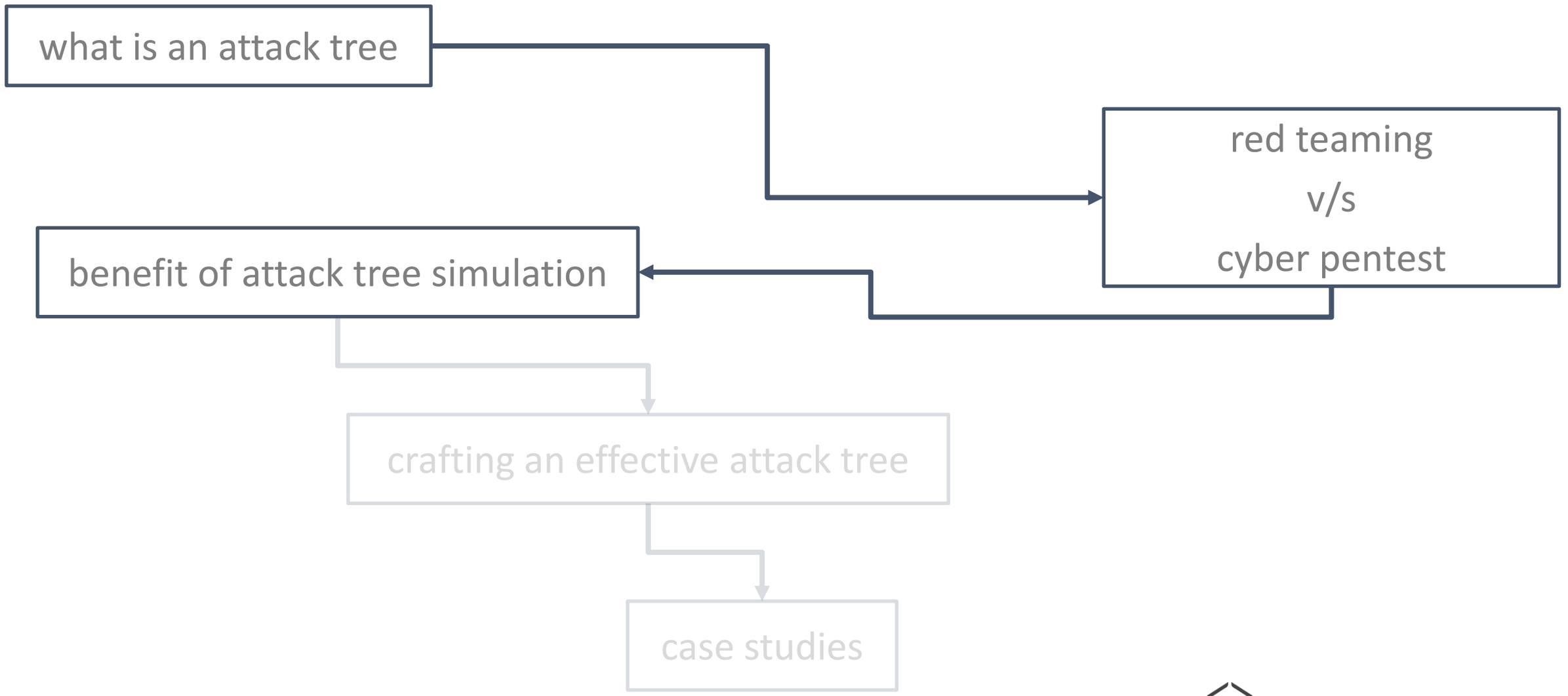
During a red teaming engagement we must identify possible threat agents and goals for a specific organization. Then execute attack scenarios that are likely caried out by such threat agents.

red teaming v/s cyber pentest



OPPOSING FORCE

agenda



OPPOSING FORCE

benefit of attack tree simulation

As we saw, in red teaming activities *we must first identify the possible attack scenarios.*

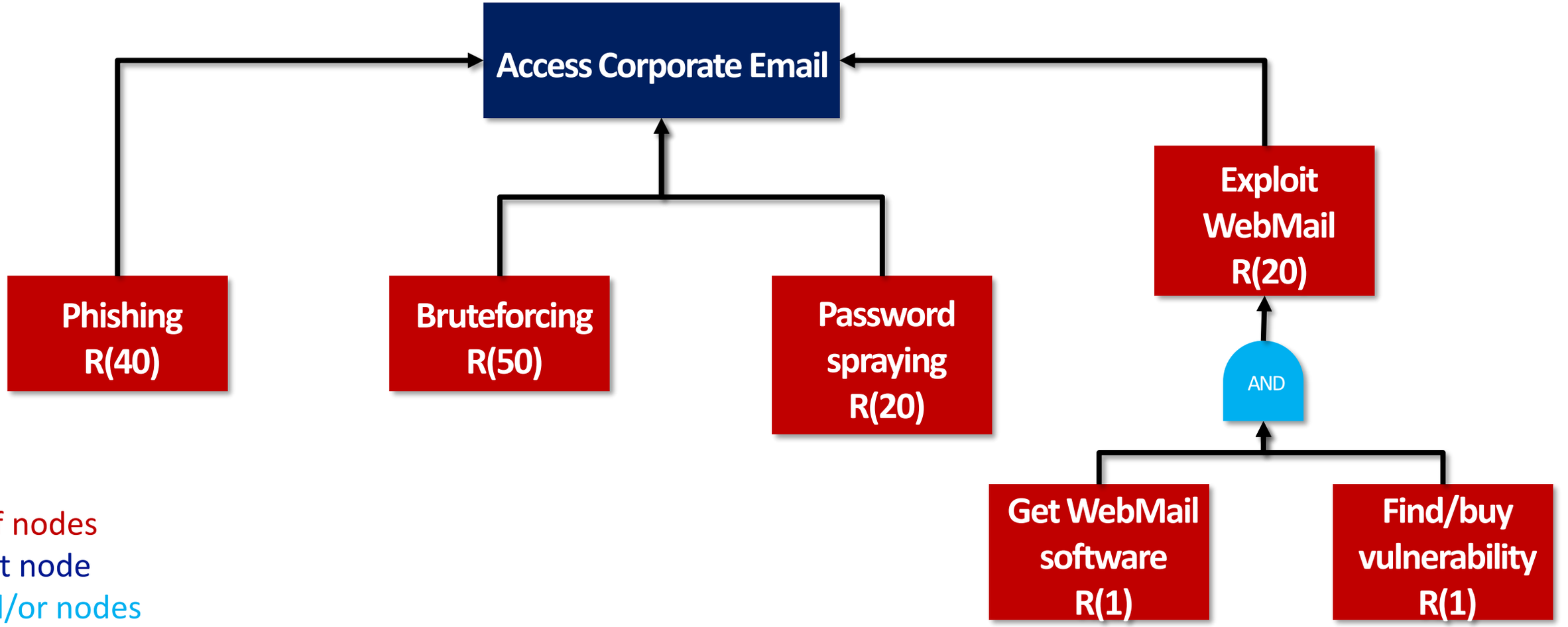
Attack trees allows us to investigate possible attack scenarios, understanding the risks and benefits, before executing them.

benefit of attack tree simulation

We use two different type of attack trees:

First one: to understand which attacks we can perform, how risky they are, what benefits we can get from a successful attack and how much we need to invest, in terms of time and money, to execute it.

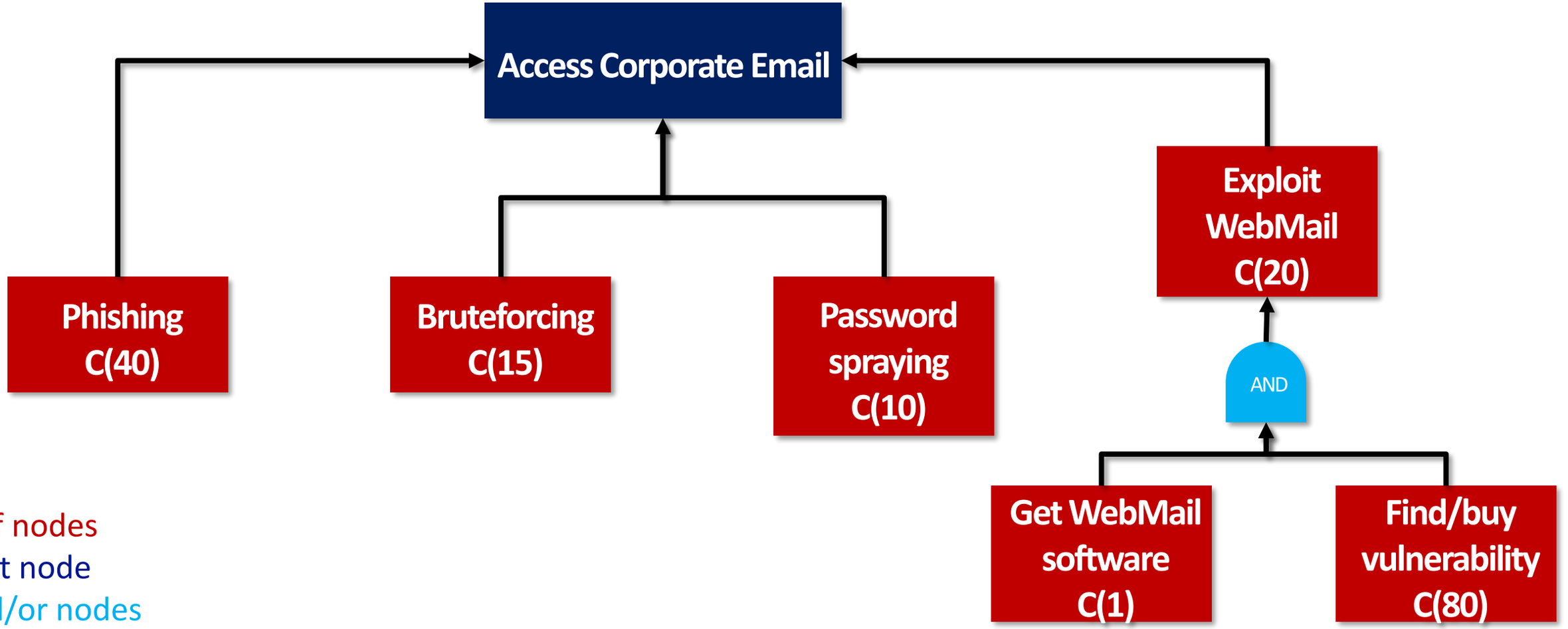
benefit of attack tree simulation



leaf nodes
root node
and/or nodes
R(X) = 1..100

OPPOSING FORCE

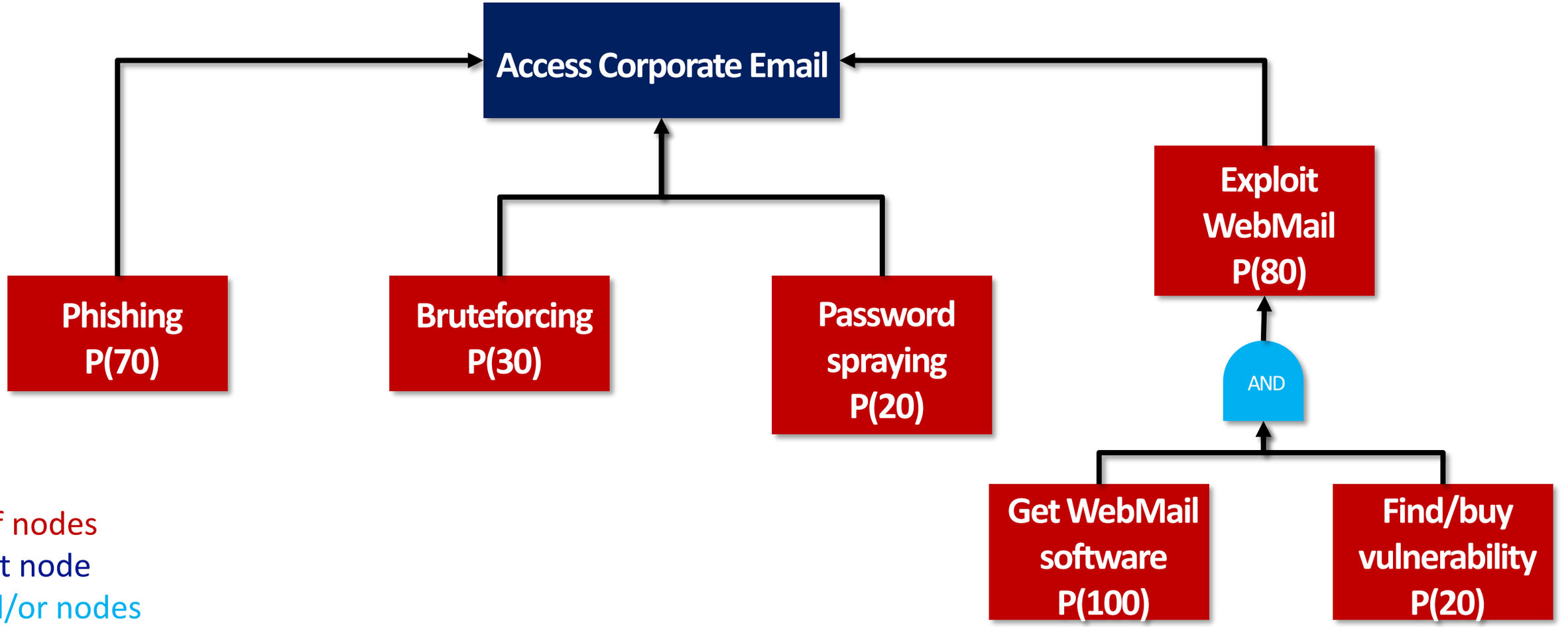
benefit of attack tree simulation



leaf nodes
root node
and/or nodes
C(X) = 1..100

OPPOSING FORCE

benefit of attack tree simulation



leaf nodes
root node
and/or nodes
P(X) = 1..100

OPPOSING FORCE

benefit of attack tree simulation

With this information we can calculate the *feasibility* of each attack.

We can use multiple formulas, for our examples we will calculate the effort using:

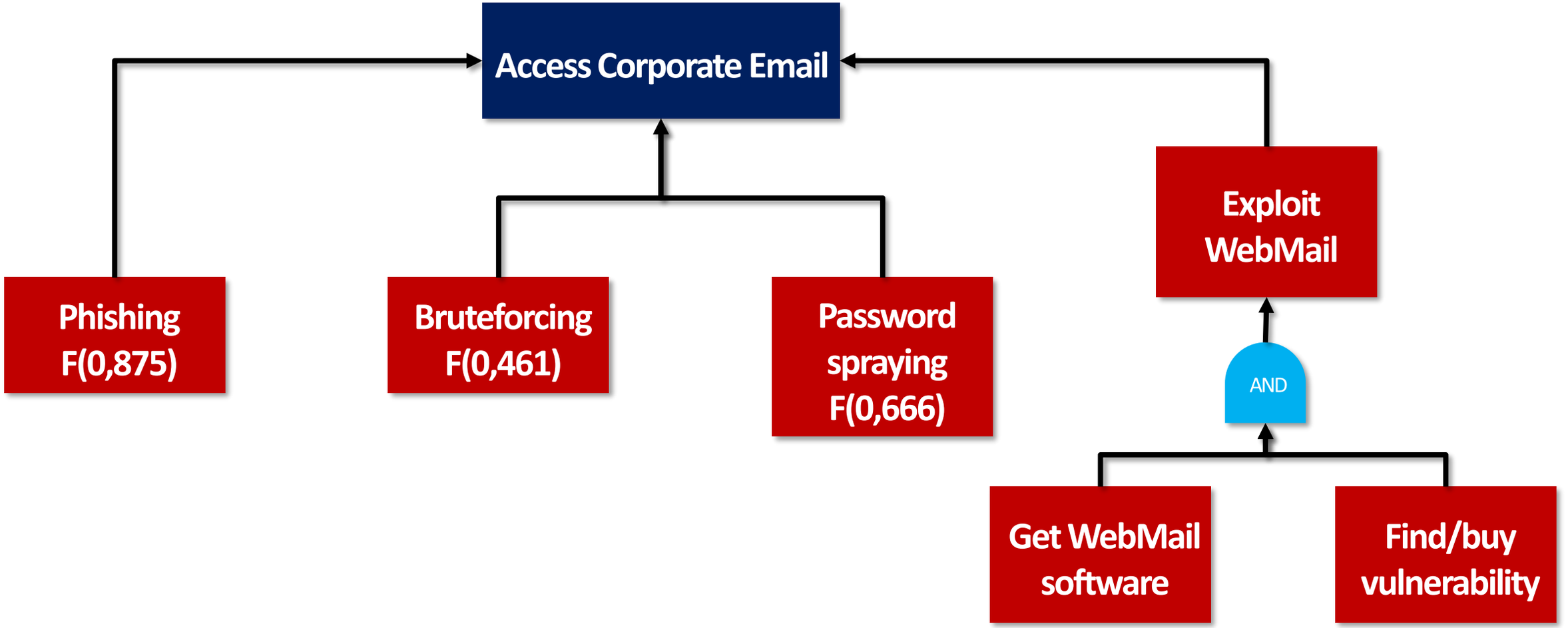
$$f = \frac{\min p}{\sum r_i + \sum c_i}$$

benefit of attack tree simulation

With this information we can analyse which attack scenarios execute, or in which order.

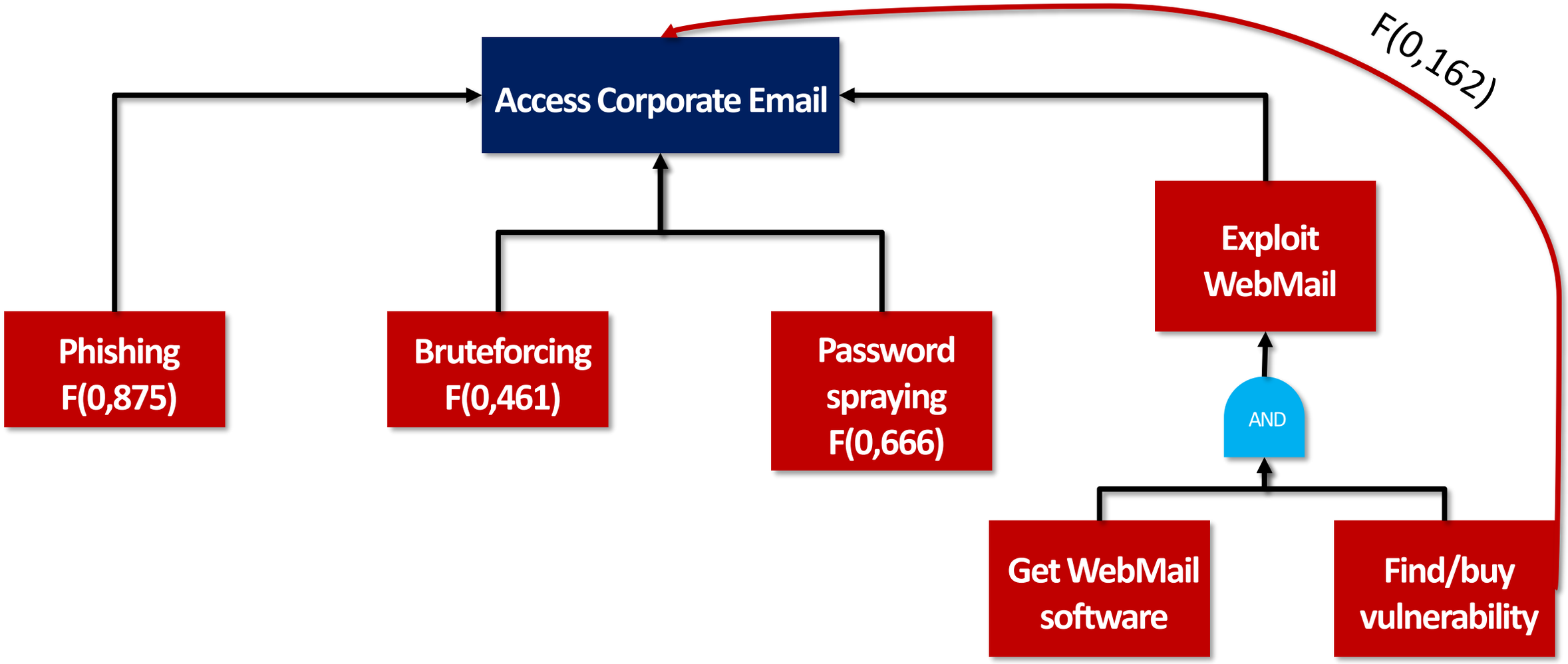
More knowledge we can gather from our target, more precise our tree will become.

benefit of attack tree simulation



OPPOSING FORCE

benefit of attack tree simulation

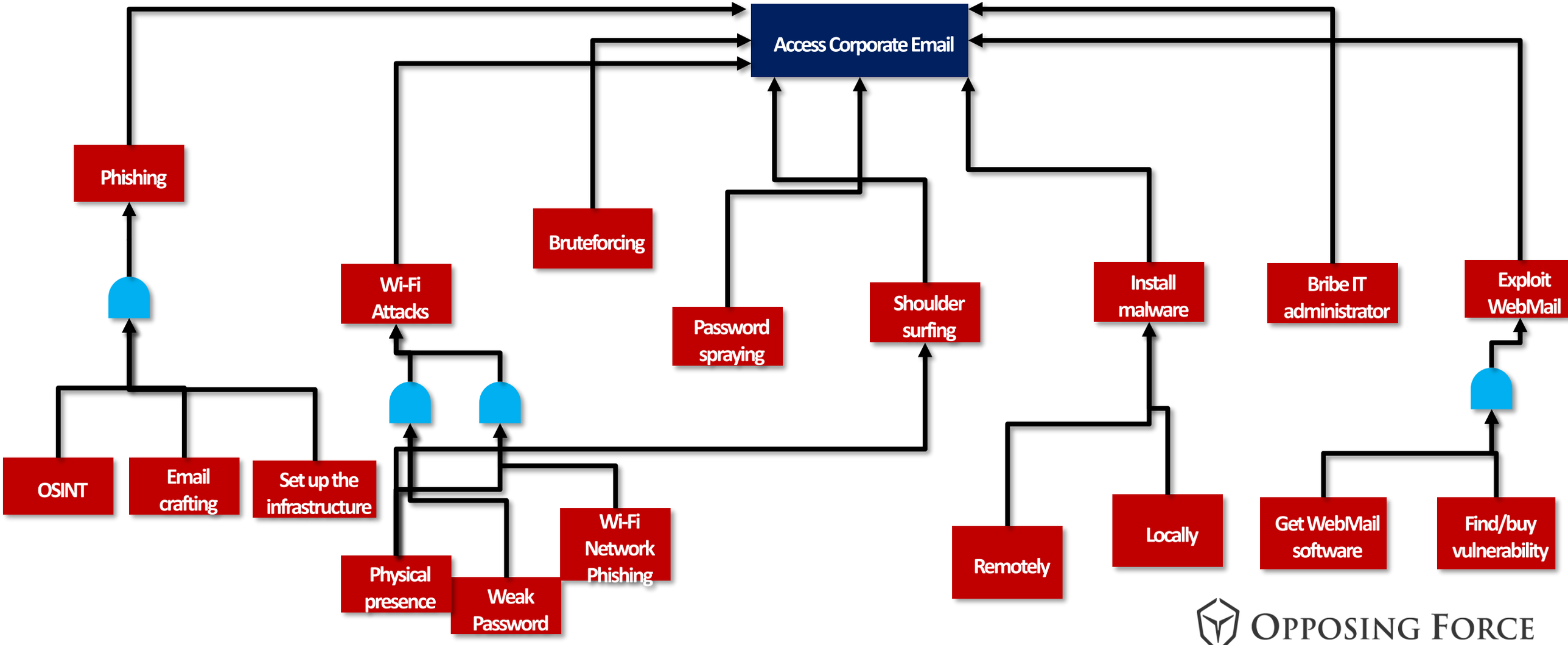


OPPOSING FORCE

benefit of attack tree simulation

Graphical representation gets messy with complex scenarios.

benefit of attack tree simulation



OPPOSING FORCE

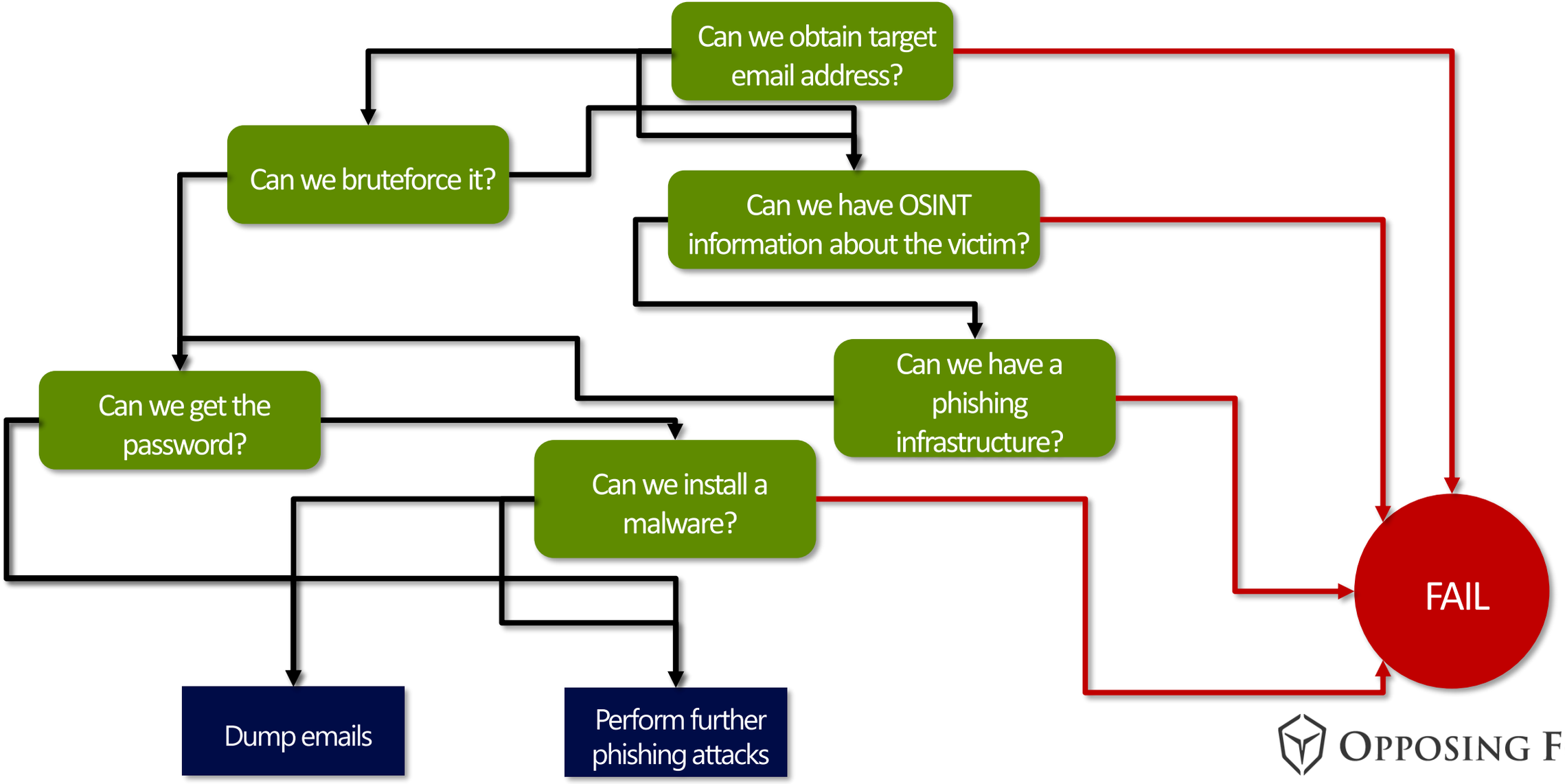
benefit of attack tree simulation

To simplify complex attack scenarios we can use a second type of tree graph instead of incrementing the complexity of a attack tree graph.

This graph is also useful before going in the field. We want to further explore the chosen path. We need to craft a *what-if graph.*

Let’s suppose we want to execute the *phishing attack*. We want to understand what issues we can encounter during the attack, and what to do in such cases.

benefit of attack tree simulation

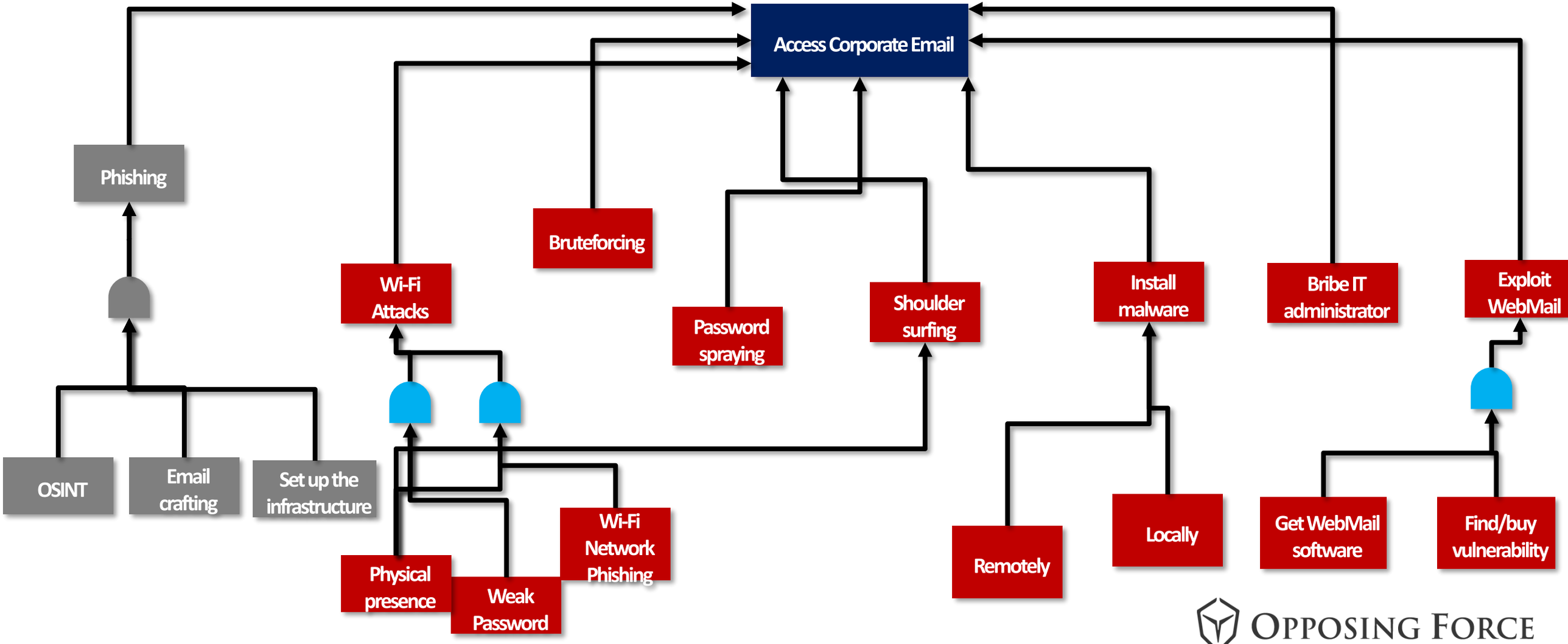


OPPOSING FORCE

benefit of attack tree simulation

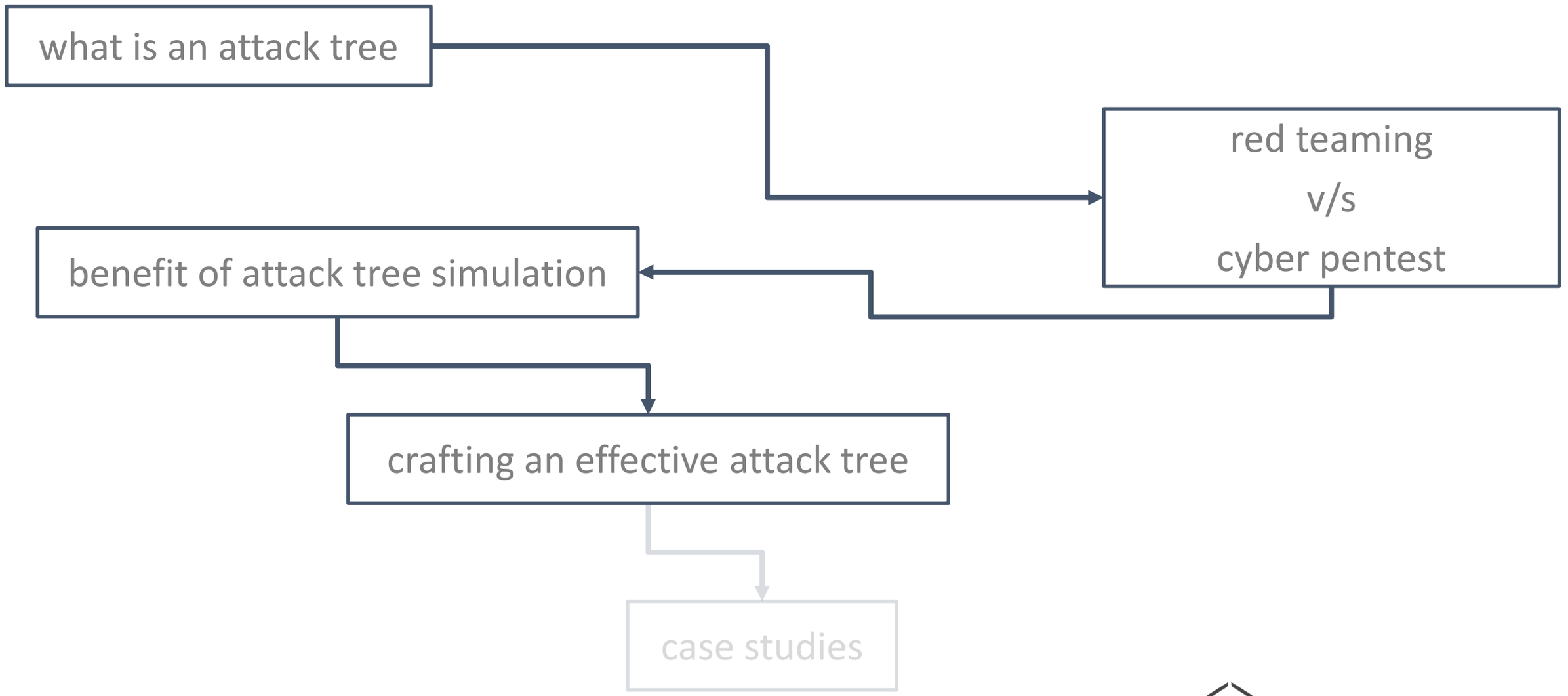
If we fail, we get back to our tree attack graph to perform a second path.

benefit of attack tree simulation



OPPOSING FORCE

agenda



OPPOSING FORCE

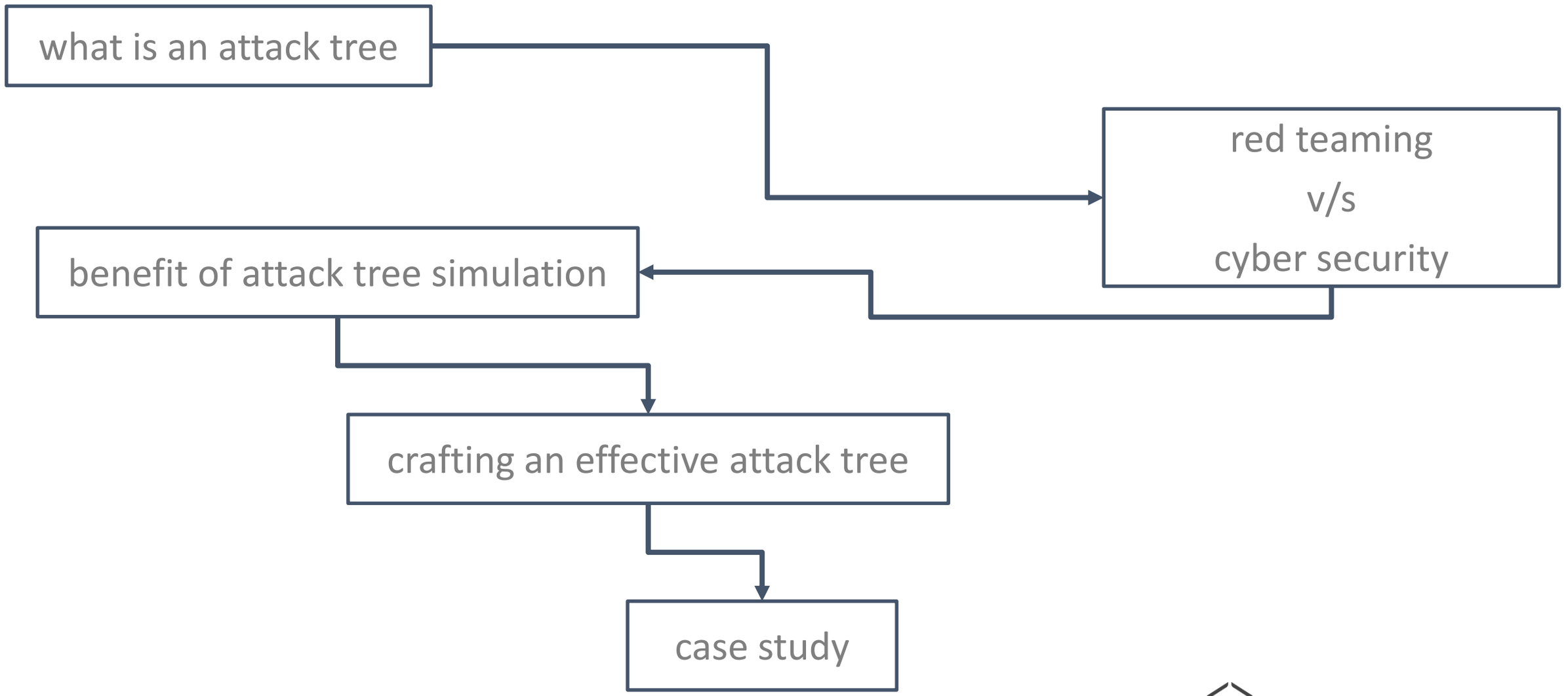
crafting an effective attack tree

How can we build an attack tree from scratch?

crafting an effective attack tree

- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenarios.
  - What if we don't get that information?

agenda



OPPOSING FORCE

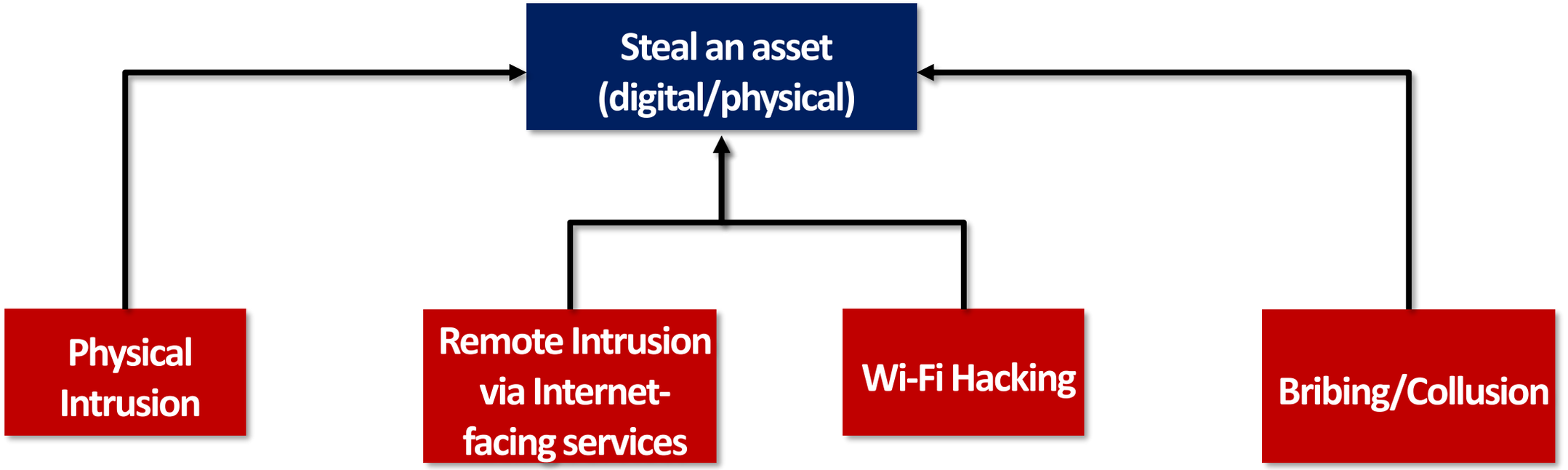
case study

- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenarios.
  - What if we don't get that information?

Steal an asset (digital/physical)

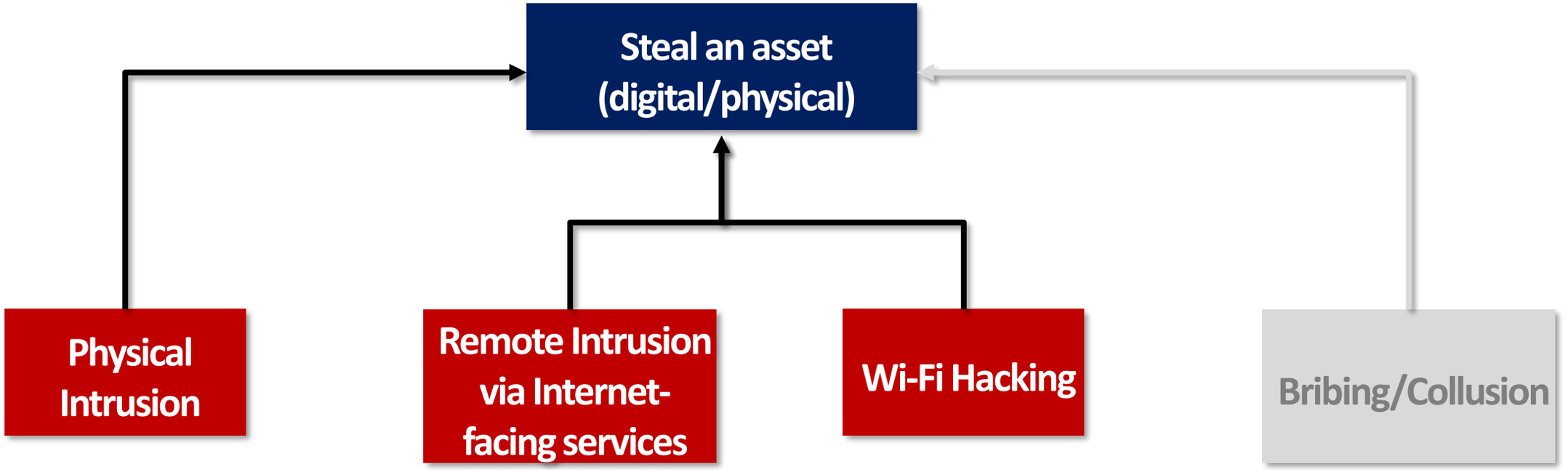
- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenarios.
  - What if we don't get that information?

case study


Steal an asset (digital/physical)
Physical Intrusion
Remote Intrusion via Internet-facing services
Wi-Fi Hacking
Bribing/Collusion

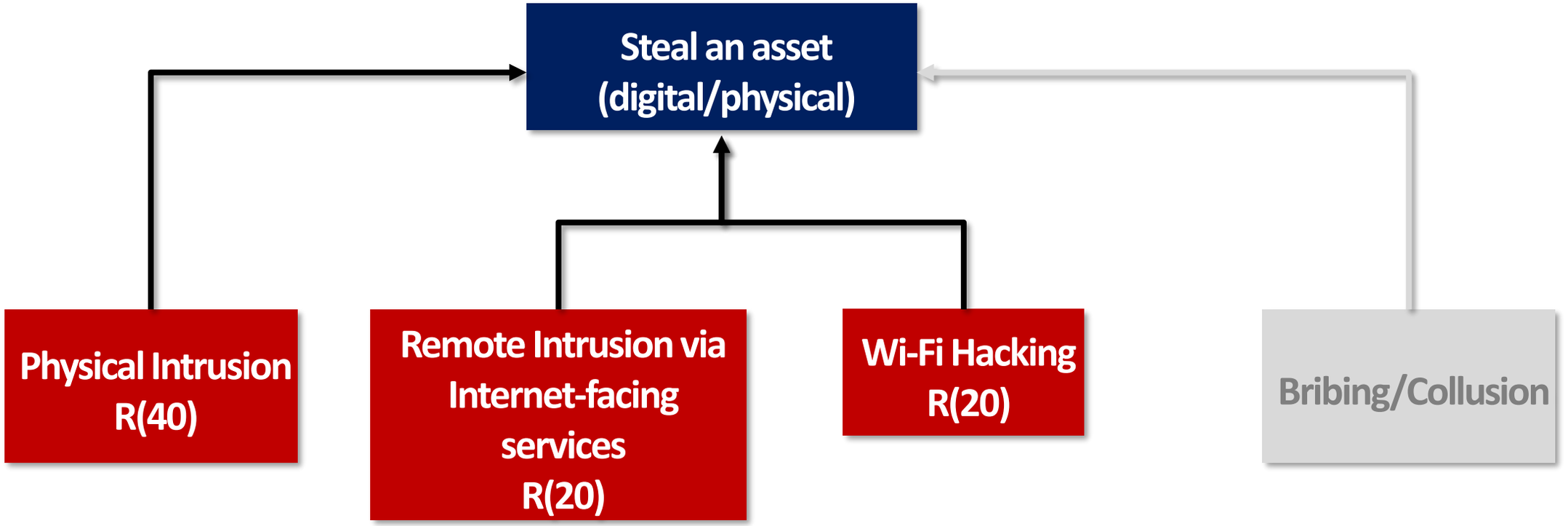
- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenarios.
  - What if we don't get that information?

case study

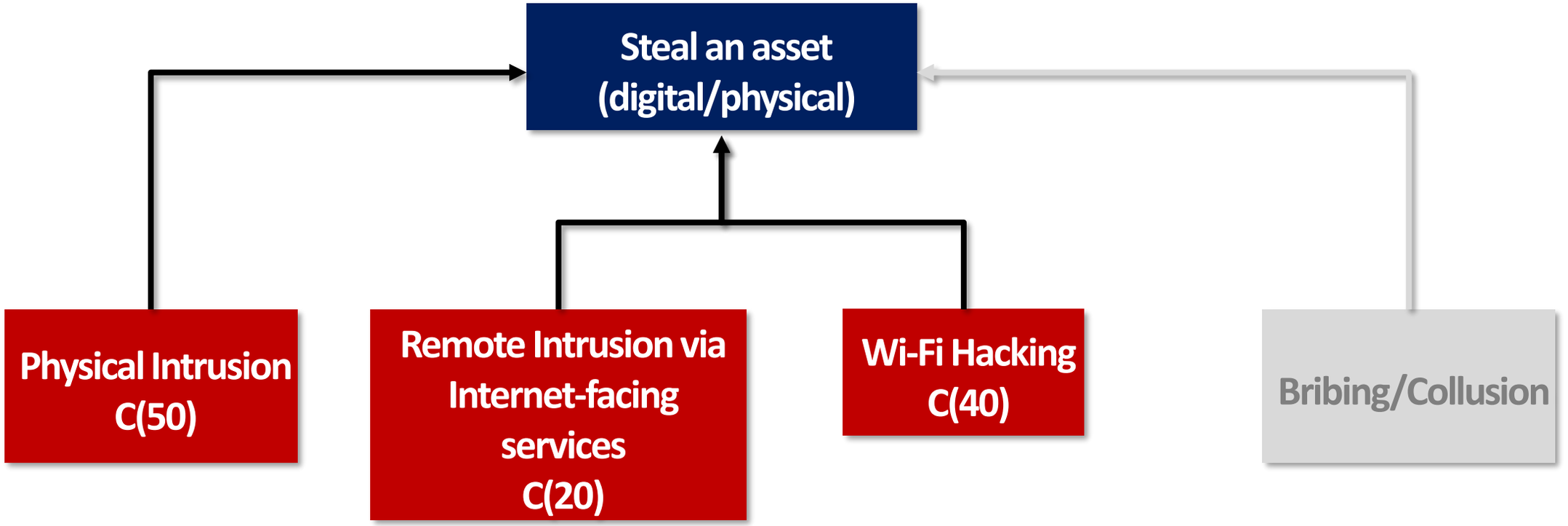

Steal an asset (digital/physical)
Physical Intrusion
Remote Intrusion via Internet-facing services
Wi-Fi Hacking
Bribing/Collusion

- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenarios.
  - What if we don't get that information?

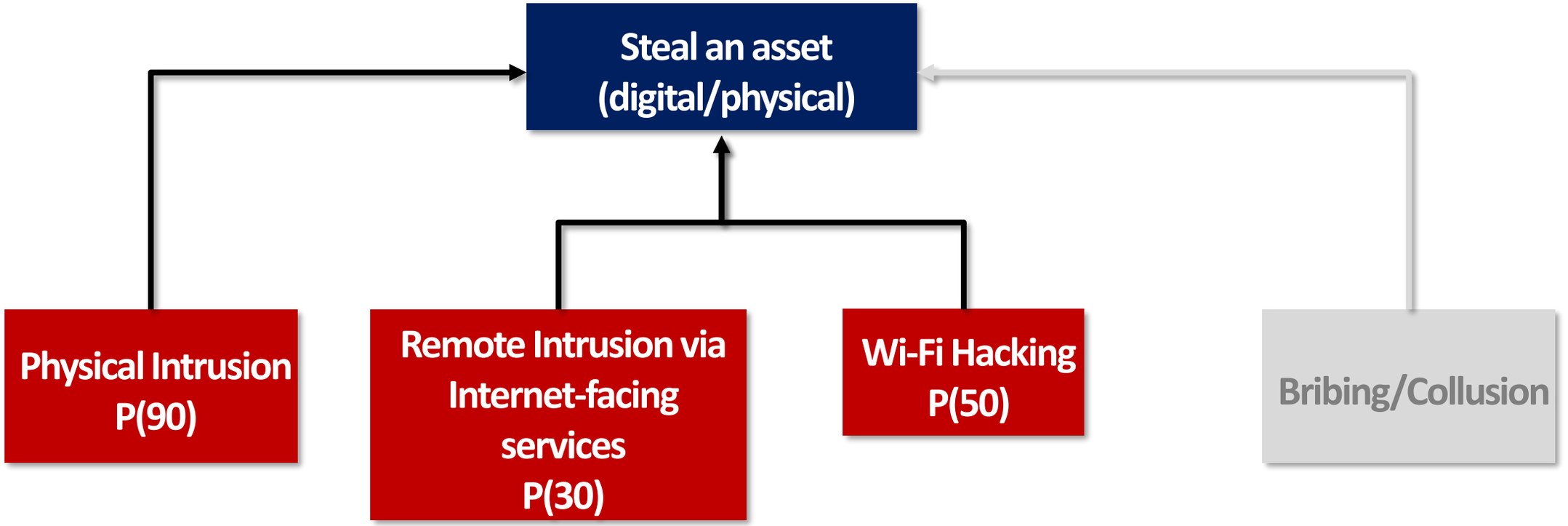
case study


Steal an asset (digital/physical)
Physical Intrusion R(40)
Remote Intrusion via Internet-facing services R(20)
Wi-Fi Hacking R(20)
Bribing/Collusion

case study

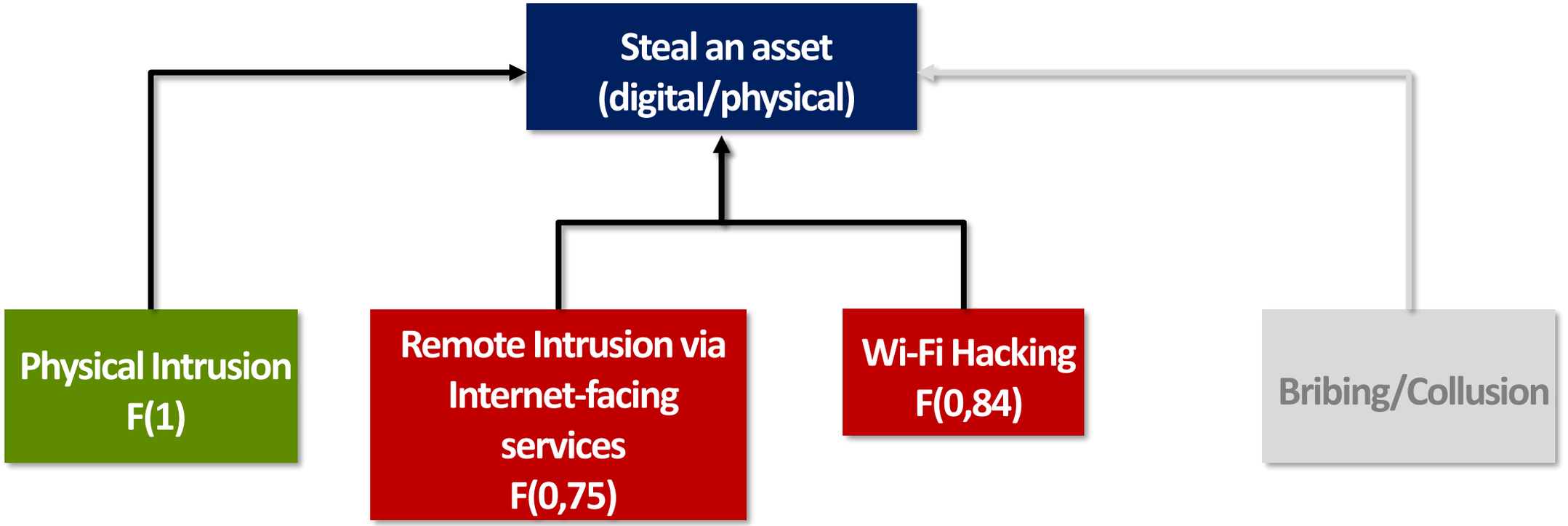

Steal an asset (digital/physical)
Physical Intrusion C(50)
Remote Intrusion via Internet-facing services C(20)
Wi-Fi Hacking C(40)
Bribing/Collusion

case study


Steal an asset (digital/physical)
Physical Intrusion P(90)
Remote Intrusion via Internet-facing services P(30)
Wi-Fi Hacking P(50)
Bribing/Collusion

$$f = \frac{\min p}{\sum r_i + \sum c_i}$$

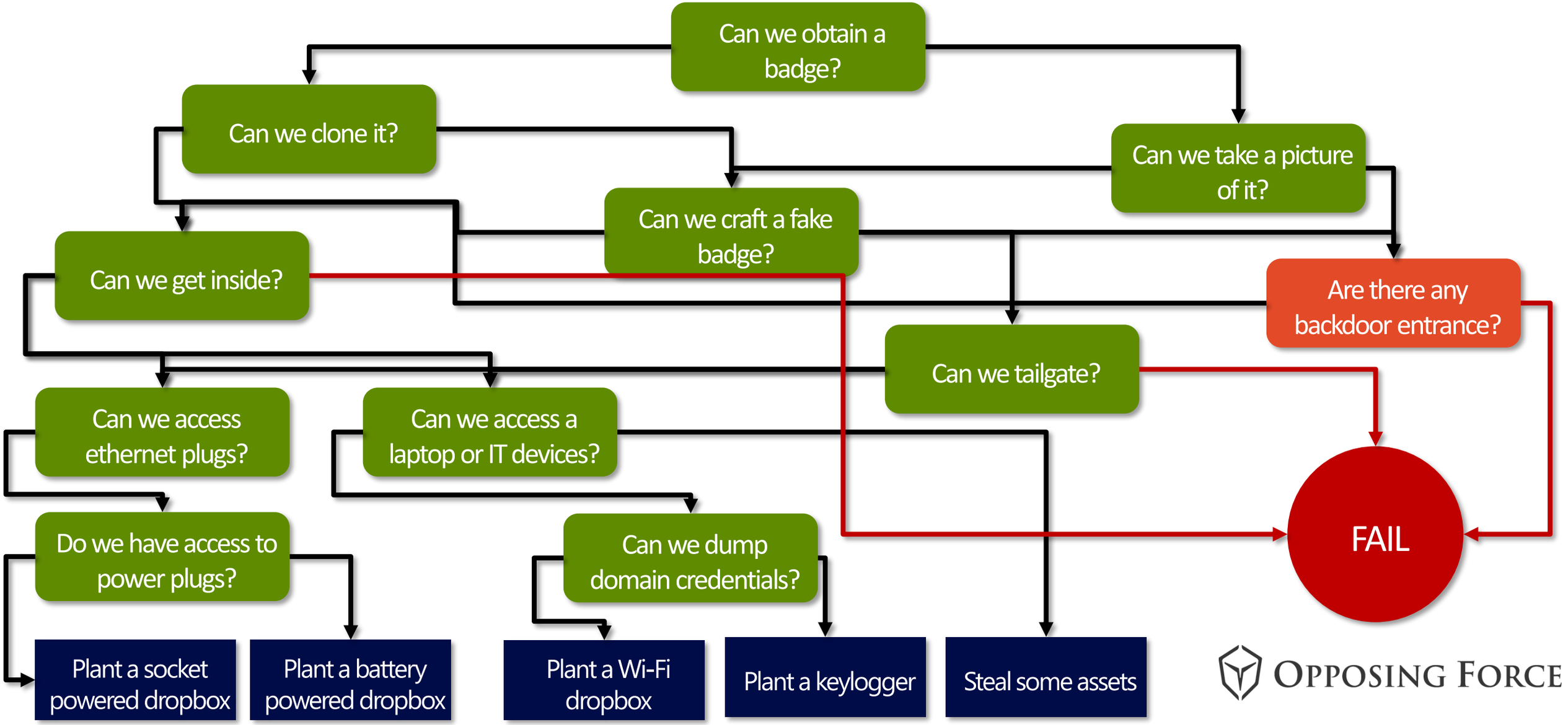
case study



OPPOSING FORCE

- Identify goal(s). If there are multiple goal, each is a separate attack tree.
- Identify possible scenarios (attacks) to execute to reach the goal.
- Identify possible and impossible scenarios.
- Evaluate the *feasibility* of each scenario
- Identify information required to execute the scenario.
  - What if we don't get that information?

case study



OPPOSING FORCE

repeat for all possible scenarios

Any question?

Don’t be shy..

Thank you

engage@opposingforce.it | www.opposingoforce.it | @_opposingforce