28 SEPTEMBER 2023

17:00 @ HEIA-FR

Development, Security and Operations

CYBERSECURITY SEMINAR

FRIBOURG

cy//ective

Penetration Testing

Cybersecurity Seminar Fribourg

Author

MANUEL CIANCI

Date

28. SEPTEMBER 2023

Agenda

ABOUT US 01

PENETRATION TESTING 02

HOW TO SECURE YOUR APPLICATIONS 03

COLLABORATION 04

SELECTED FINDINGS 05

TAKE AWAYS 06

About us

WHO WE ARE

Who am I

PROFESSIONAL

- Software Engineer
- (Cloud) Security Engineer/Consultant/Architect
- Leadership, company management

- 10.2021 - cyllective
- 09.2013 - 09.2021 - Swisscom
  - Software Engineer
  - Security Consultant / Engineer
  - Head of Security-Delivery @ Group Security

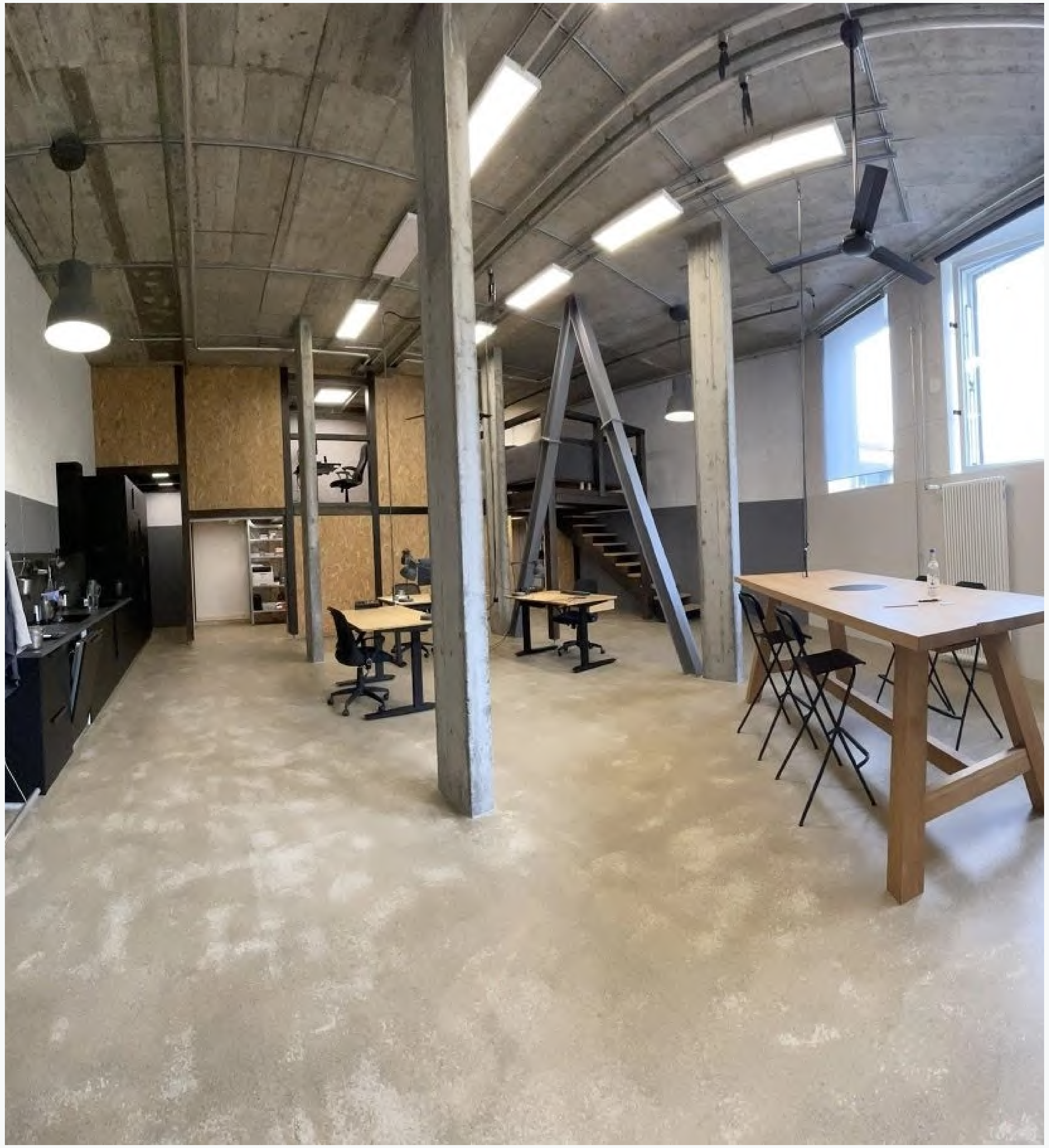
PRIVATE

- Family
- Sports enthusiast
- CTF player

WHO WE ARE

cy//ective

- Founded in Switzerland, 2013
- Privately held «Security Boutique»
- Offensive Security Services
- Highly technical expertise
- Contributing to the community



Management Team

SOPHUS SIEGENTHALER

Founder, Managing Partner,
IT-Security Engineer/Consultant

Focus: Network Security, Mac, Azure, CISOaaS, Consulting, Threat Modeling, DFIR, etc.

MANUEL CIANCI

Managing Partner,
IT-Security Architect

Focus: Cloud Security, Mobile Applications, AWS, CISOaaS, Consulting, DevSecOps, etc.

BAHNSTRASSE 44, CH-3008 BERN

cyllective Headquarters

SEEBURGSTRASSE 39, CH-6006 LUZERN

Second Office

Penetration Testing

DEFINITION

https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

Penetration Tester

fido passkeys whitepaper

fido **passkey** whitepaper

fido **implementation example**

fido **alliance standards**

fido **contact email**

What is Penetration Testing

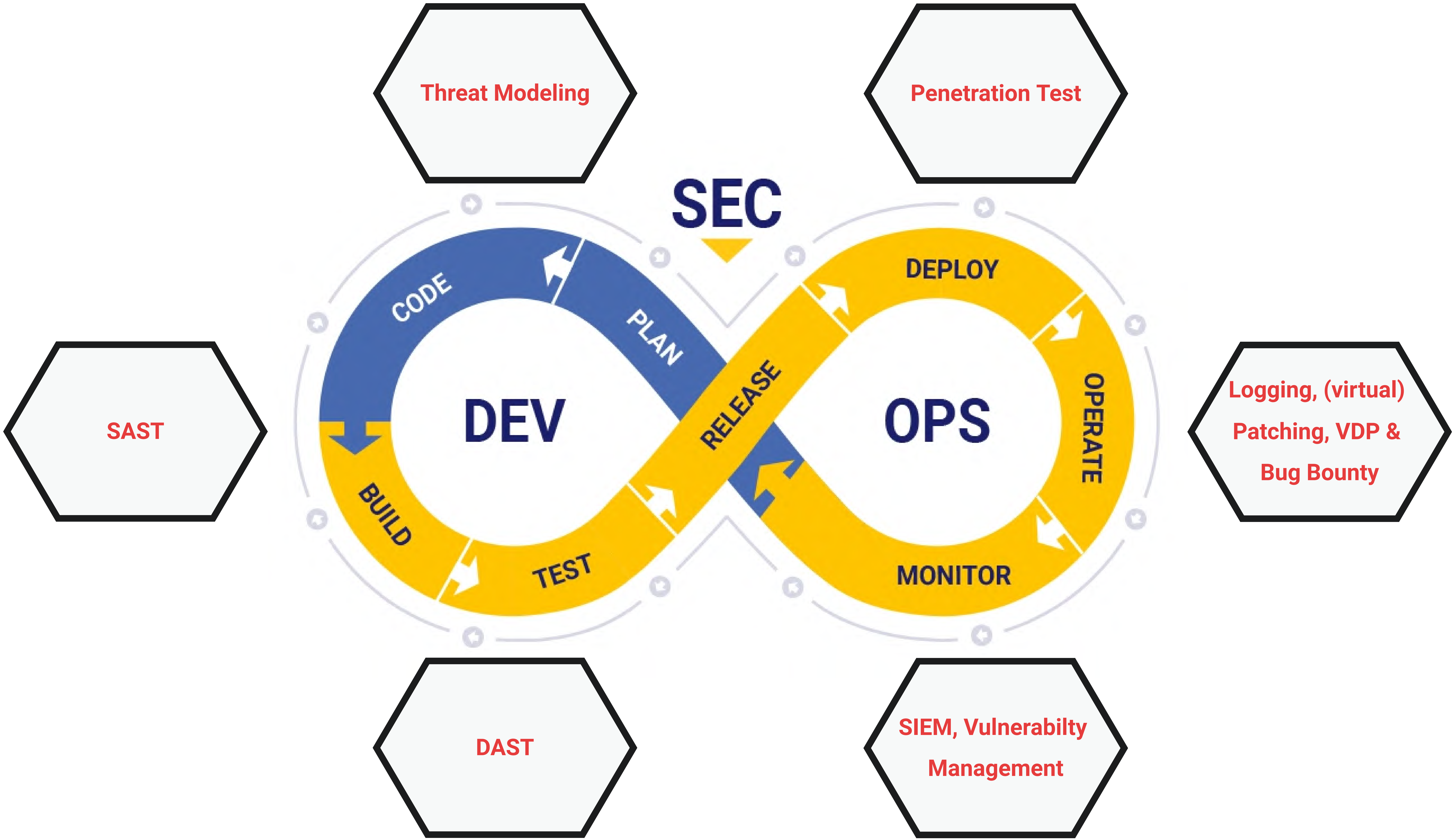
1. **Definition**:
   - A simulated cyber attack against a system, application, or network.
2. **Objective**:
   - Identify vulnerabilities before malicious actors do.
3. **Ethical Hacking**:
   - Conducted by professionals with consent.
4. **Comprehensive View**:
   - Uncovers weaknesses and deep insights across technology, processes, and people.
5. **Different Flavors / Customized Attacks**:
   - Blackbox, Greybox, Whitebox Penetration Testing
   - Red/Purple Teaming, with and without Social Engineering

Why is Penetration Testing important?

1. **Proactive Security**:
   - Identify and fix vulnerabilities before they're exploited.
2. **Regulatory Compliance**:
   - Some industries mandate regular testing.
3. **Trust & Reputation**:
   - Maintain customer and stakeholder confidence.
4. **Evolving Threat Landscape**:
   - Constantly changing cyber threats require regular assessments.
5. **Reduce Costs**:
   - Early detection can prevent costly breaches.
6. **Education**:
   - Helps IT and developers understand real-world attack scenarios.
7. **Risk Management**:
   - Provides a clear picture of current security posture and potential risks.

How to secure your applications

STAY PRACTICAL



Threat Modeling

Penetration Test

SAST

Logging, (virtual) Patching, VDP & Bug Bounty

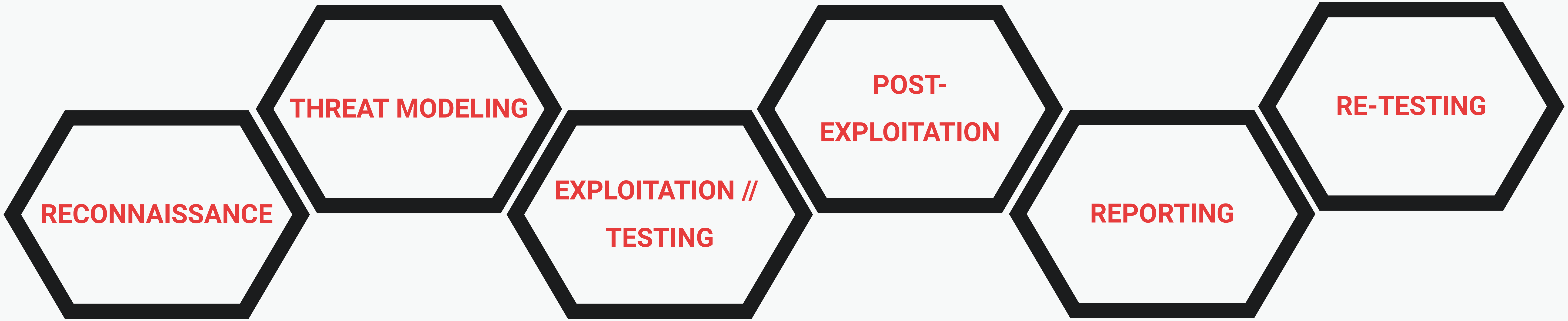
DAST

SIEM, Vulnerabilty Management

Collaboration

HOW TO GET THE MOST OUT OF A PENETRATION TEST

Phases of a Pentesting Engagement



RECONNAISSANCE

THREAT MODELING

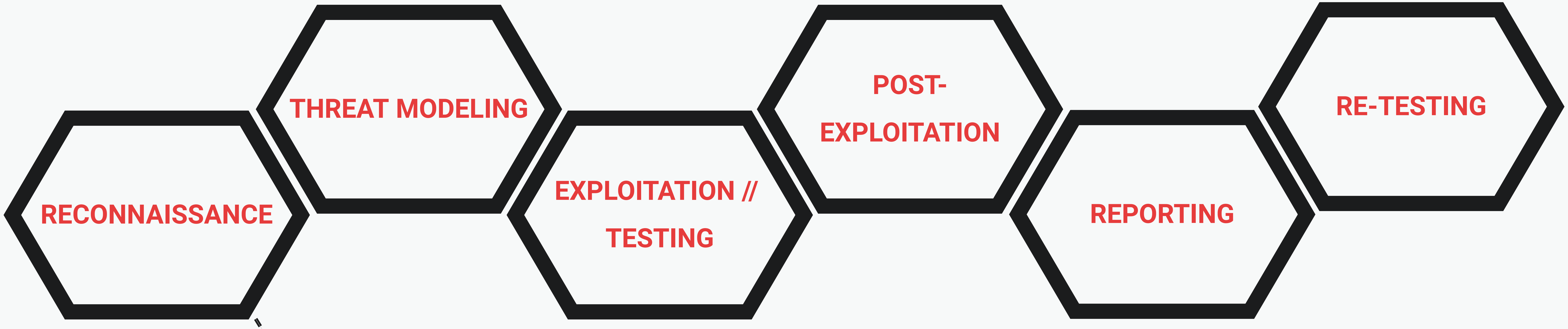
EXPLOITATION // TESTING

POST-EXPLOITATION

REPORTING

RE-TESTING

Reconnaissance



RECONNAISSANCE

THREAT MODELING

EXPLOITATION // TESTING

POST-EXPLOITATION

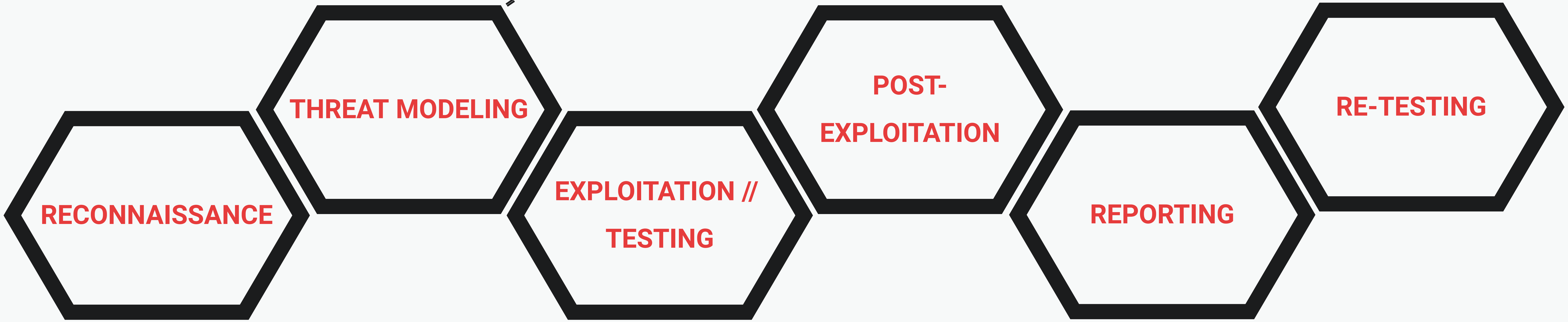
REPORTING

RE-TESTING

- Hand-over all necessary information to the pentester
    - Domains, IPs, Inventory, etc.

Threat Modeling

- You are the experts of the product
- Use Penetration Tester to enrich and verify your Threat Models!



RECONNAISSANCE

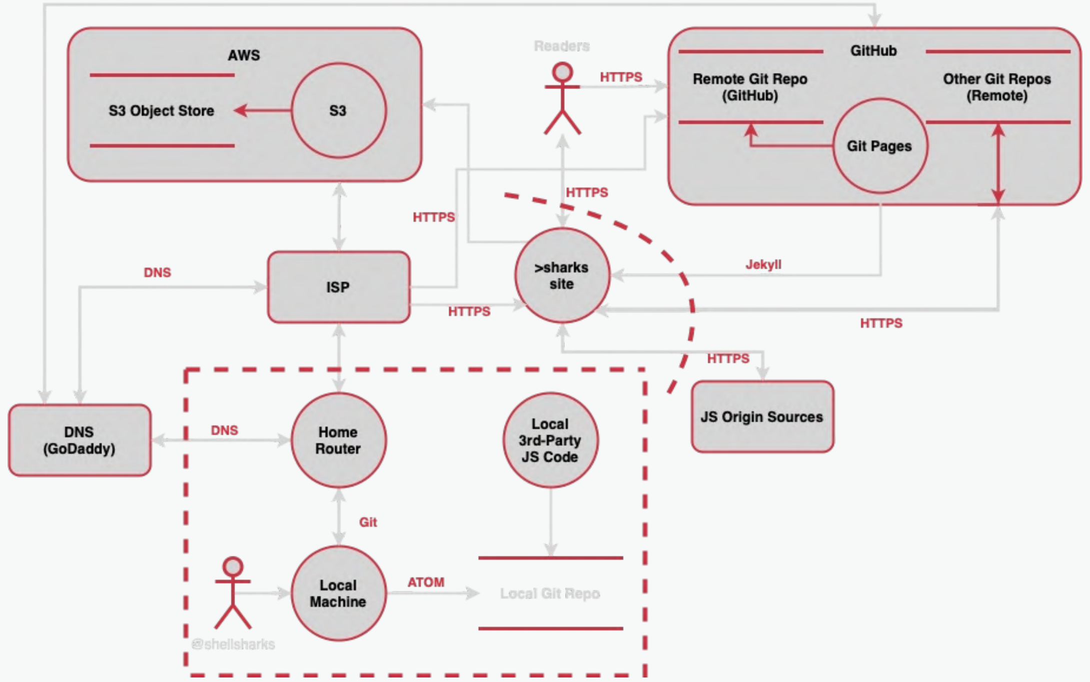
THREAT MODELING

EXPLOITATION // TESTING

POST-EXPLOITATION

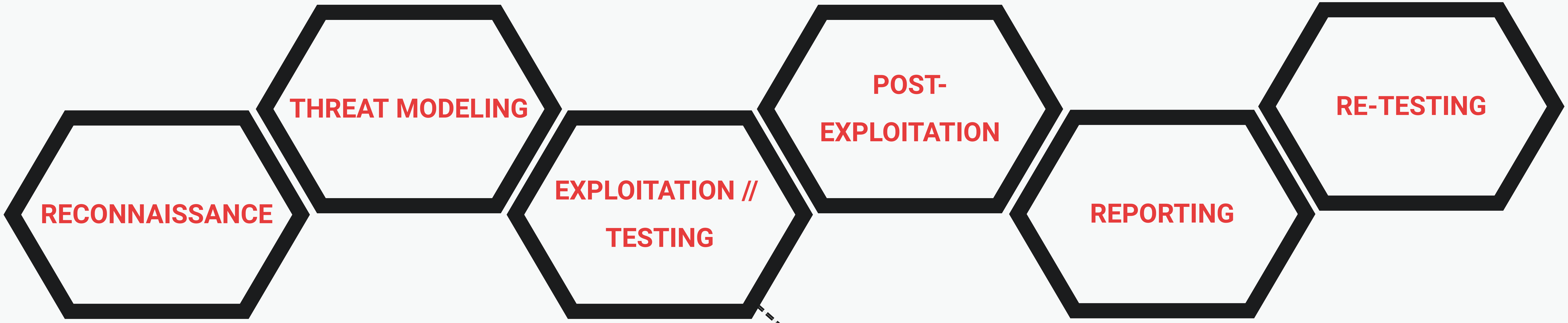
REPORTING

RE-TESTING



cy//ective

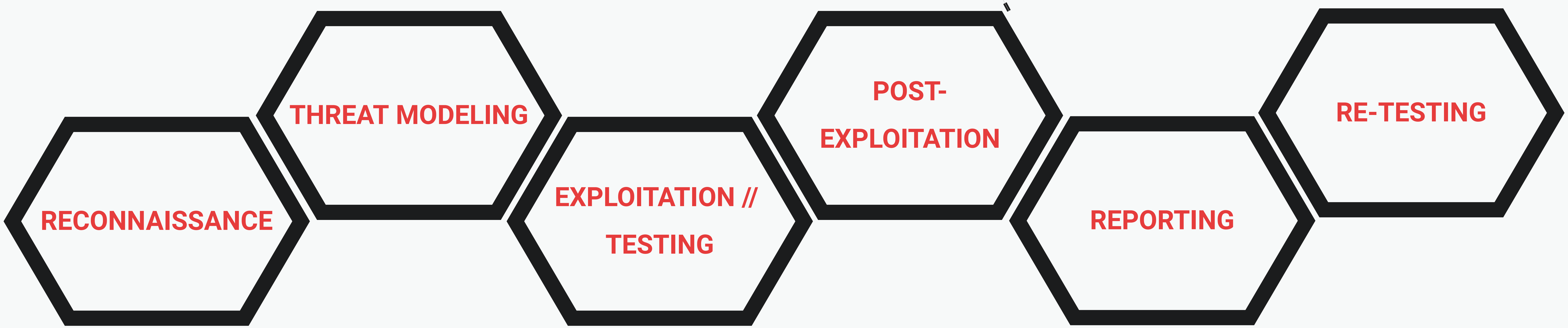
Exploitation // Testing



- No deployments during pentesting time
- Give access to internals (Source Code, Documentation, Swagger files, Test Cases, Threat Model, etc.)
- Whitebox if possible

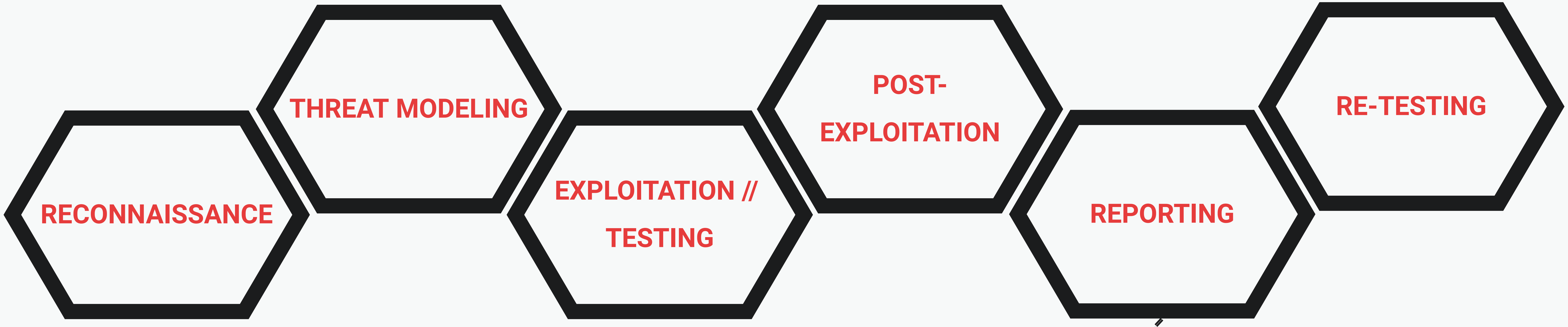
Post-Exploitation

- How far should the tester go? Where to stop?
- Relevant in Red Teaming Excercises



cy//ective

Reporting

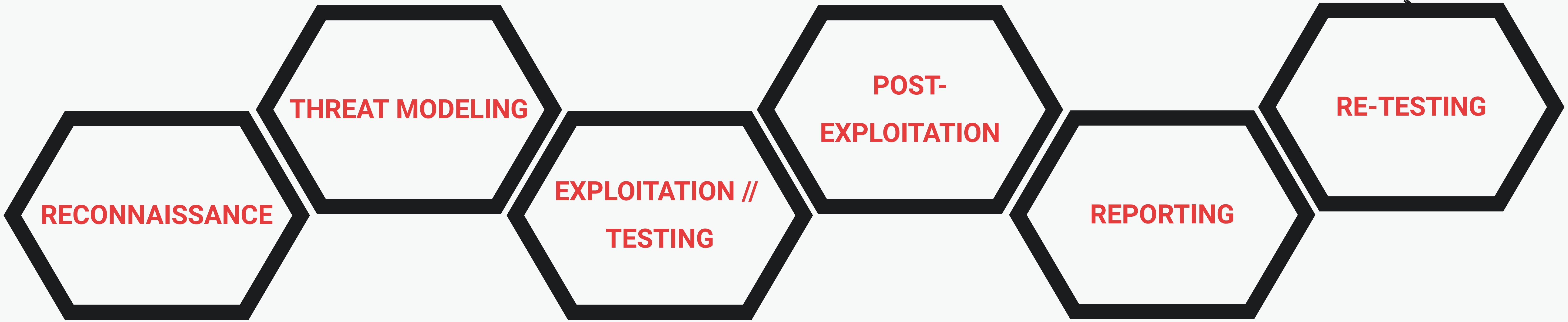


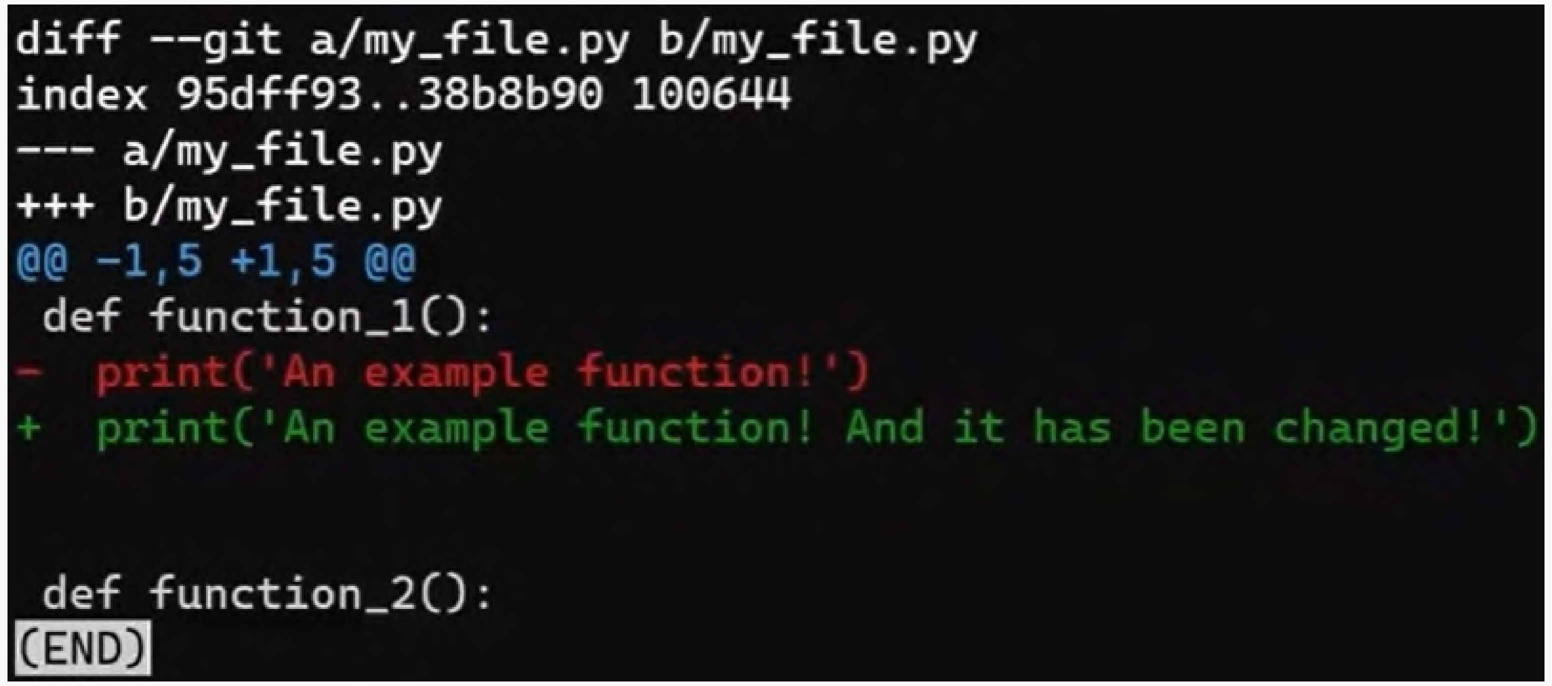
- Management Summary, rated findings, technical explanation and remediation measures to each finding
- A good report always contains a chapter with what was tested.
- Do you have internal knowledge of bugs/malpractices but you don't get the prioritization/budget to address it? Use the Penetration Test to get the attention! :)

cy//ective

Re-Testing

- Provide Changelog, Diffs of the changes





```
diff --git a/my_file.py b/my_file.py
index 95dff93..38b8b90 100644
--- a/my_file.py
+++ b/my_file.py
@@ -1,5 +1,5 @@
 def function_1():
-   print('An example function!')
+   print('An example function! And it has been changed!')


 def function_2():
(END)
```

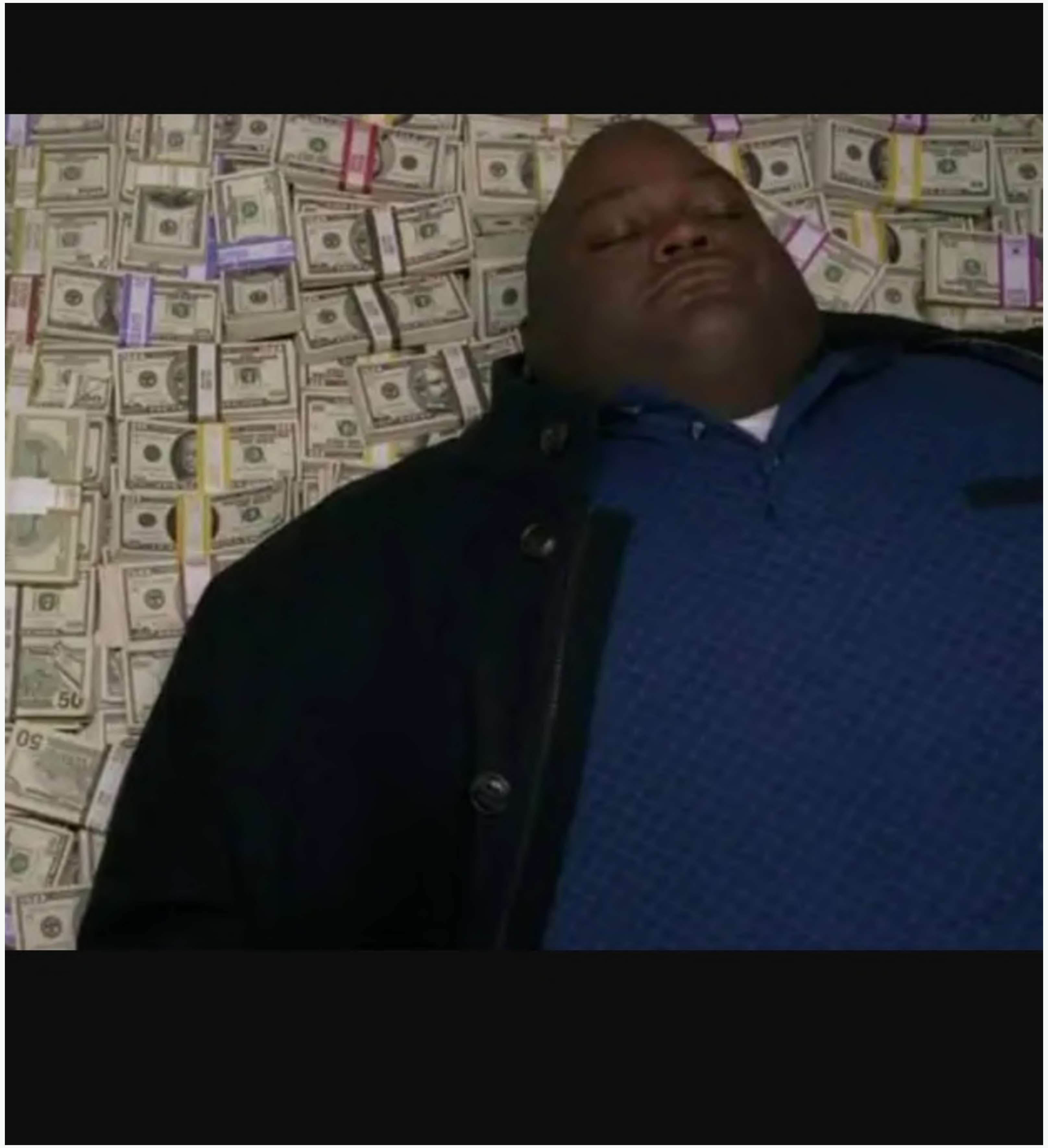
Selected findings by cyllective

(.. AND ATTEMPTS ..)

RACE CONDITION - INFINITE MONEY

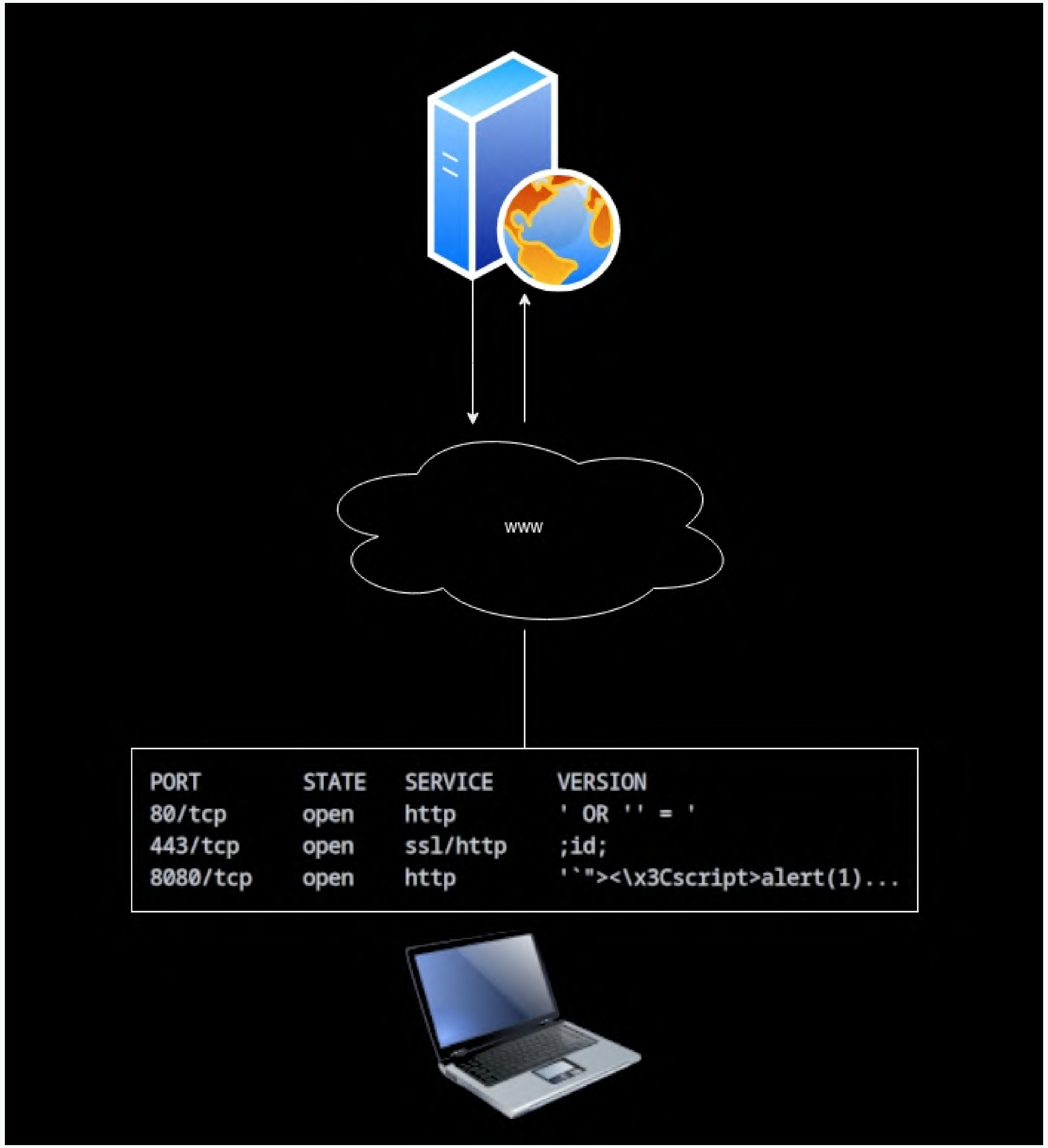
Selected findings by cyllective

- Whitebox Penetration Test - Online Shop
- Possibility to buy vouchers/giftcards
- Custom vouchers to buy "real" ones
- Race condition
- Allowed to double the custom vouchers



CODE INJECTION - SERVER SIDE PORT SCANNER

Selected findings||attempts by cyllective



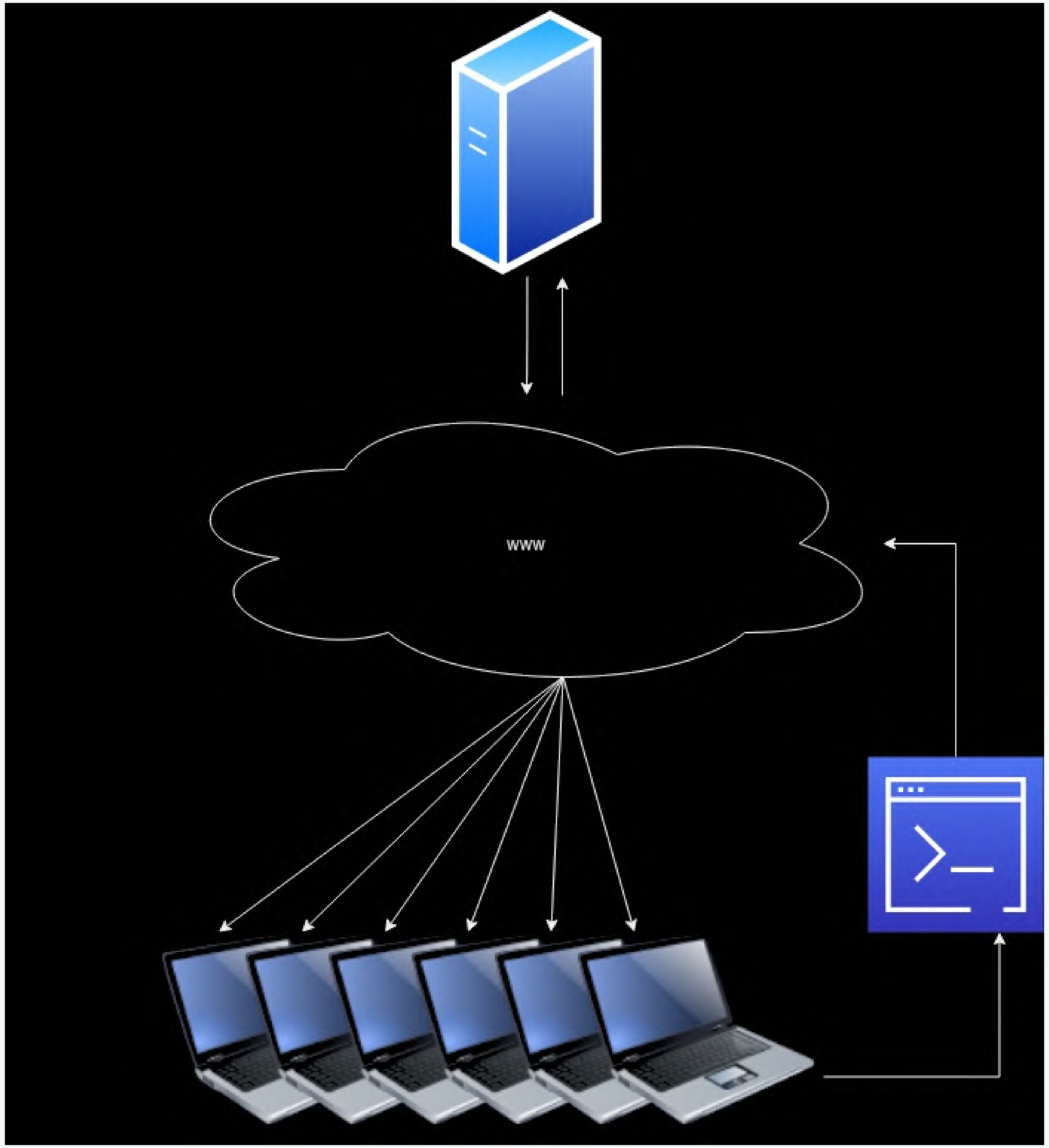
```
PORT       STATE   SERVICE    VERSION
80/tcp     open    http       ' OR '' = '
443/tcp    open    ssl/http   ;id;
8080/tcp   open    http       '`"><\x3Cscript>alert(1)...
```

- Whitebox Penetration Test - Security website
- Offers a port scan to the visitors
- Scans the visitors' exposed ports
- Displays information about open ports on the website
- Serve malicious service information via exposed ports
- Not successful :(

CONTROL ALL MANAGED DEVICES

Selected findings by cyllective

- Greybox Penetration Test of a customers' Device Management
- Configuration scripts are downloaded
- Scripts can be intercepted
- Service account credentials with admin privileges for management platform
- RCE on all managed devices



Takeaways

TOP 3

Takeaways

01

DO THREAT MODELINGS ALL THE TIME

02

COMBINATION OF SECURITY MEASURES IS KEY

03

MAKE AS MUCH USE OF PENTEST AS POSSIBLE - COLLABORATE!

Questions?

Contact

cy//ective

Email

manuel@cyllective.com

Social Media

https://www.linkedin.com/in/anciancim

https://twitter.com/cianci_m

<— Scan me if you dare to :]