Atelier Pentesting Part 1

Adrien Lasalle @2024

Requirements

Virtual Machine Software

- VirtualBox (Windows or Linux)
- Vmware Fusion (Apple)

Kali Linux Image

- Kali.org/get-kali
- 64bits Image Installer
- Apple Silicon ARM64

Disclaimer

Ethical Mind

- Report vulnerabilities
- Do not publish your results before correction

Legal

- Pentesting on your own devices
- Pentesting with authorization

$whoami

Adrien Lasalle - Pentester

- **Personal Blog** : alrikrr.github.io
- **Github** : @AlrikRr
- **LinkedIn** : adrien-lasalle

$whoami

Adrien Lasalle - Pentester

- **External Pentesting**
- **Internal / Network / Active Directory Pentesting**
- **Attack Surface Mapping**
- **Hardware Hacking**
- **Cloud Pentesting**

Pentesting from A to Z

Pentesting mission with a client from A to Z

What is Pentesting ?

Skills

- Skilled Cyber Security experts
- Simulate threat actor activities
- Up to date every day

Goals

- Finding Vulnerabilities
- Provide Remediations
- Final report for the client

Legal

- Ethical Mind
- Authorization signed
- Report all the activities

Pentesting type

White Box

- Full Information
- Full Access
- Full cooperation
- Security controls down

Grey Box

- Some minor access
- Some scope information
- Some cooperation
- Can start black

Black Box

- No Access
- No Scope information
- You are alone
- Default Security controls

Rules of Engagement

ROE includes

- Scope (Servers, Apps, Accounts, etc)
- Limits of the tests
- Starting date
- Ending date

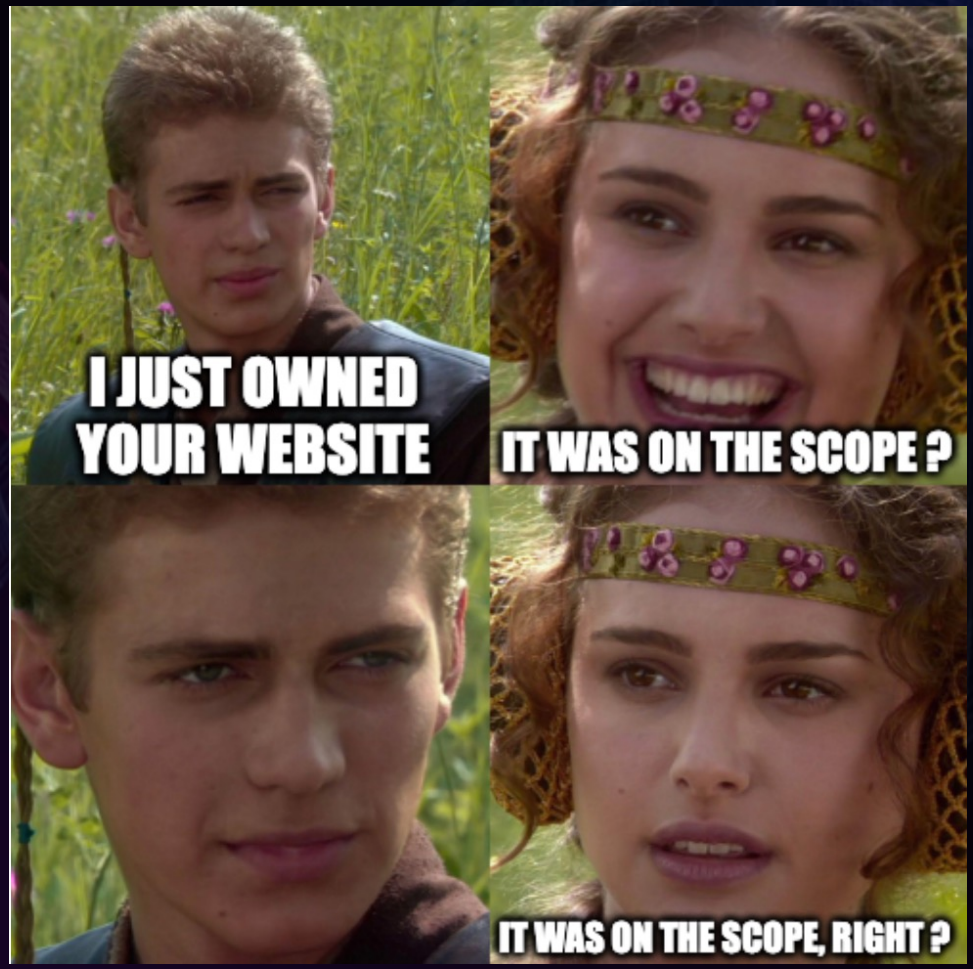
Cons ?

Time & Price

- Time limited
- Can be expensive

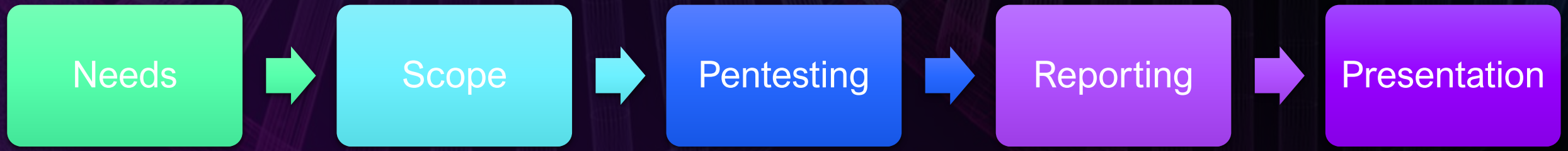
Scope Information

- Scope too small
- Scope too big
- Client needs



Schedule

Classic pentesting schedule



Pentesting Activities

Some interesting pentesting fields & Missions

Mission types

Web Pentesting

Internal Pentesting

Application Security

Mission Types

IoT Pentesting

Industrial Pentesting

Others ...

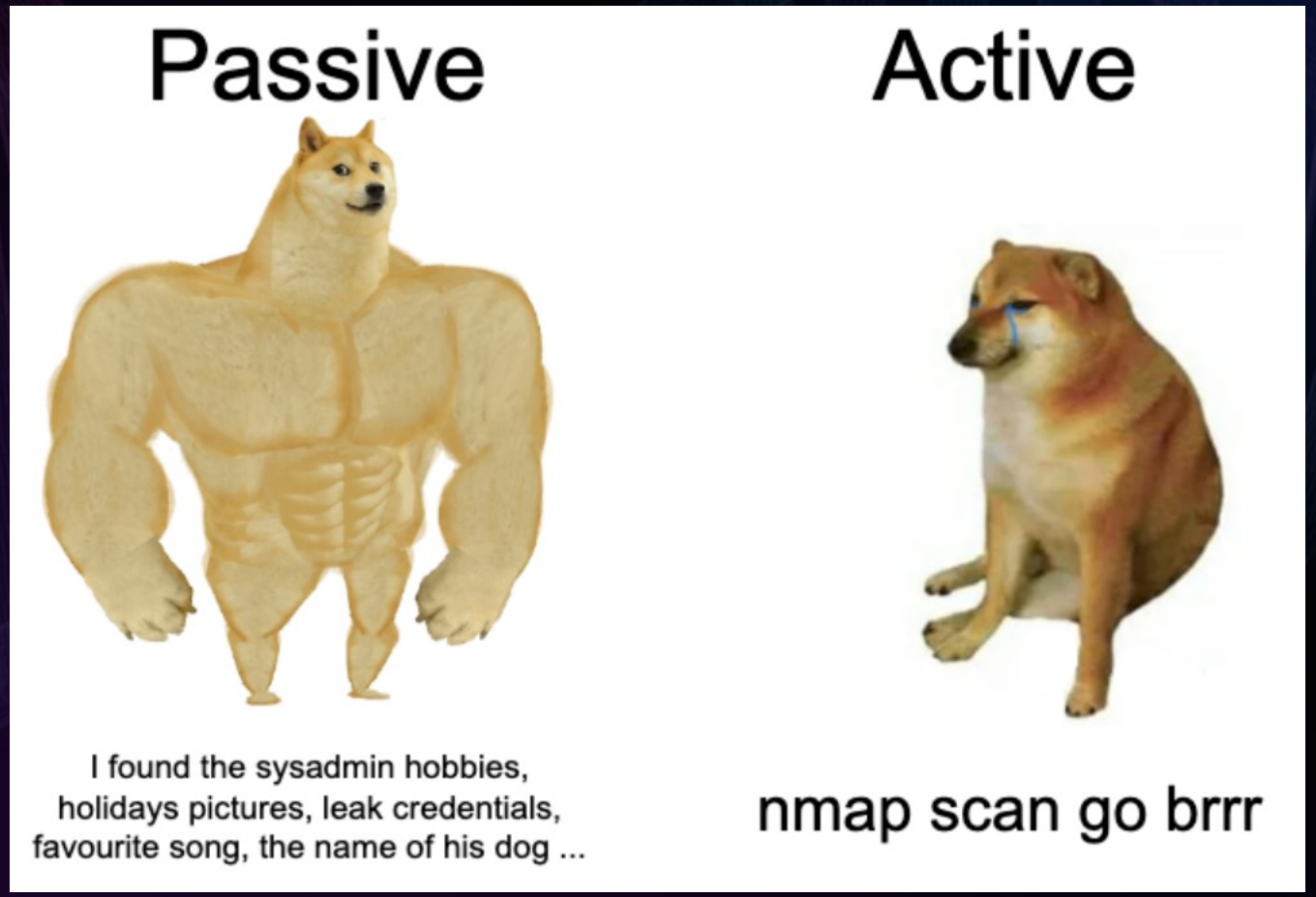
Type of Activities

Passive

- OSINT
- Internet research
- Publicly expose information
- Invisible Reconnaissance

Active

- Active Scanning
- Leave traces on server logs
- Can disturb services



Reconnaissance

Information Gathering

- Server Type
- Version number
- Security Controls

Attack Path

- Build custom attack path
- Save time for next phase

Exploitation

Is it Risky ?

- No harmful exploit
- Always keep the client informed
- Collect Screenshot and PoC
- Fully understand the exploit before use

Initial Access

- Gain Access to Application
- Gain Access to Server
- Gain Access to User or Admin account

Post Exploitation - Pivoting

Privilege Escalation

- Road to Root Access

Why stop here ?

- Other machines in the same network ?
- Other accounts ?
- Juicy Information (Passwords, API, Applications)

Red Teaming ?

Pentesting or Red Teaming ?

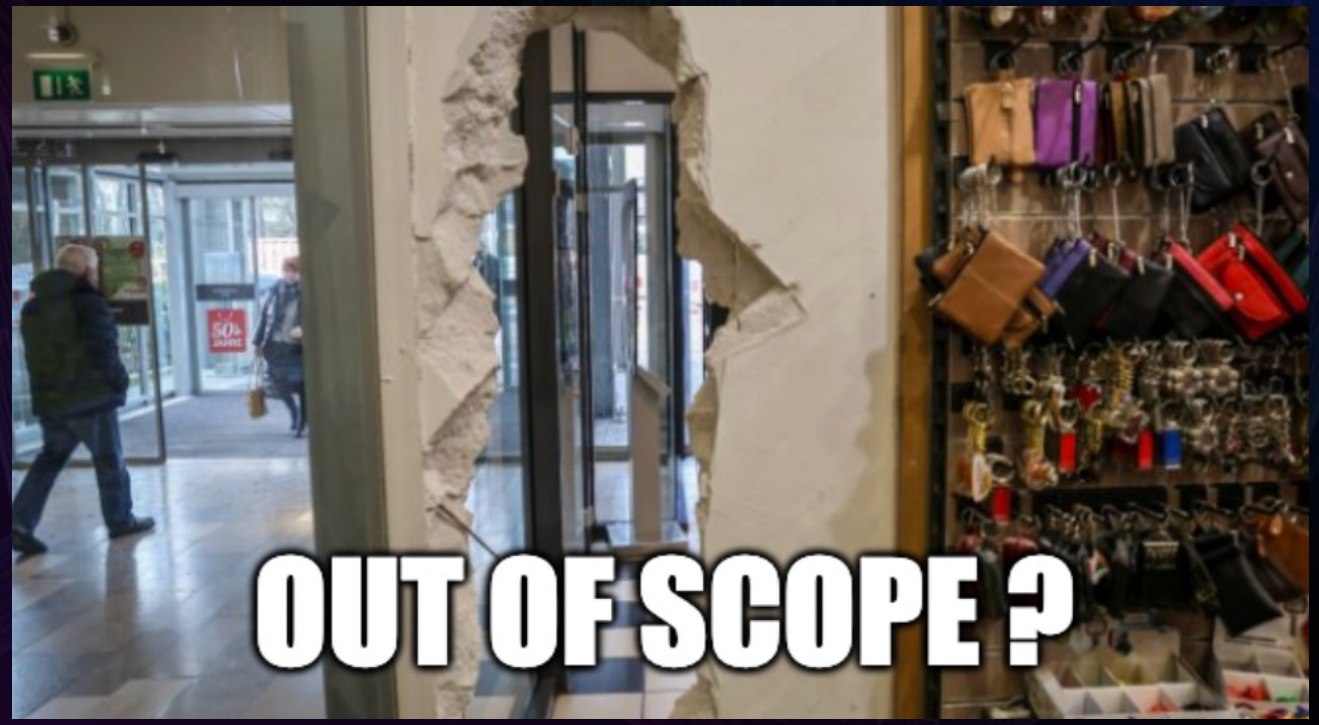
Main differences

Time & Scope

- What is the scope ? Yes.
- Longer projects can take several months
- Multi Skills Team
- Few people know about it

Activities

- Social Engineering
- Physical Pentesting (Out of jail pass needed !)
- Simulate a motivated threat actor



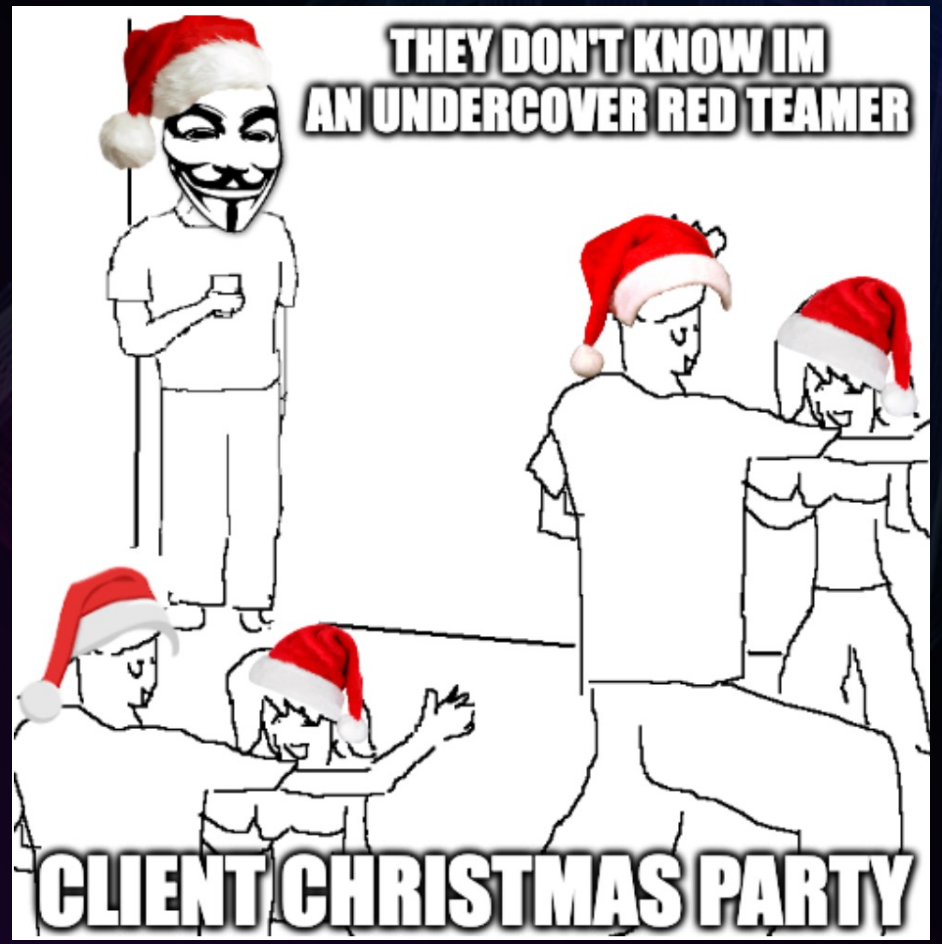
Physical Security

Pros

- On site reconnaissance
- Social Engineering
- Lockpicking
- Internal Pentesting

Cons

- Police



Report Writing

The least fun part of the job

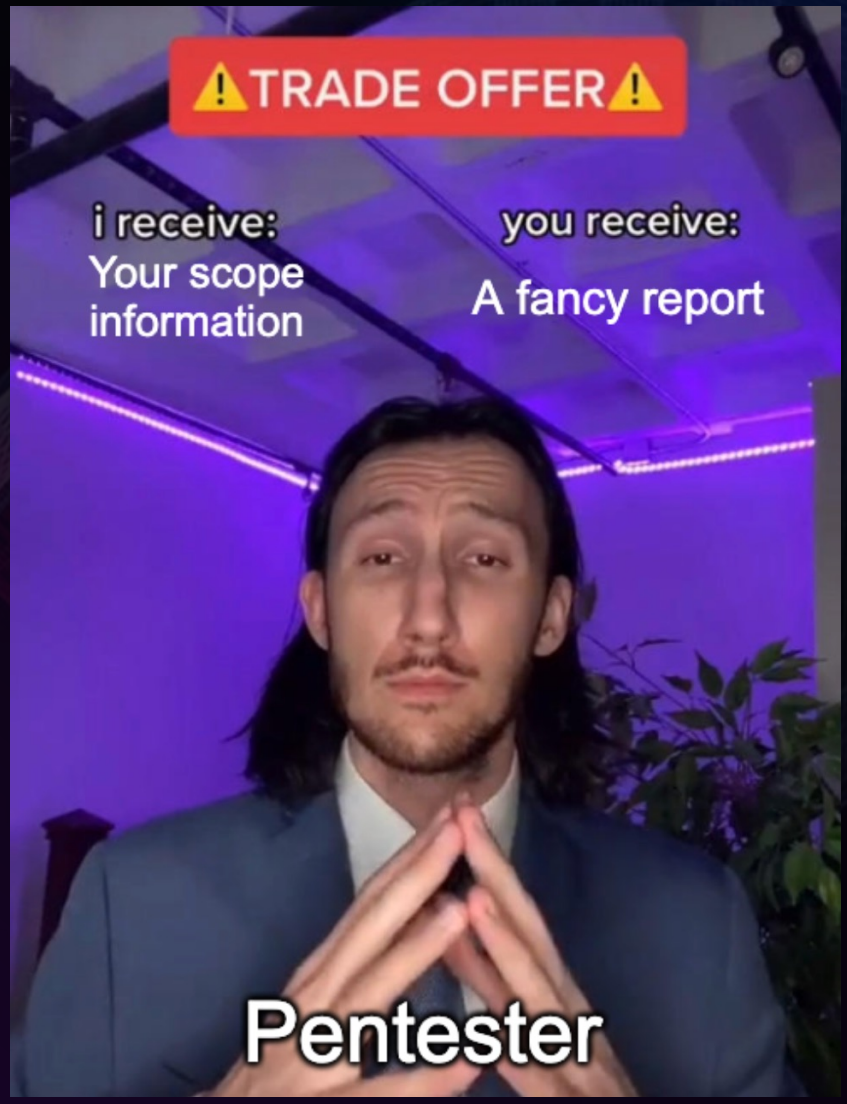
Sorting Vulnerabilities

Proof Of Concept

- Exploit screenshot
- How exploit works
- Is it critical ?

Custom Severity

- Sort Vulns
- Executive + Technical
- Custom severity depending of conditions



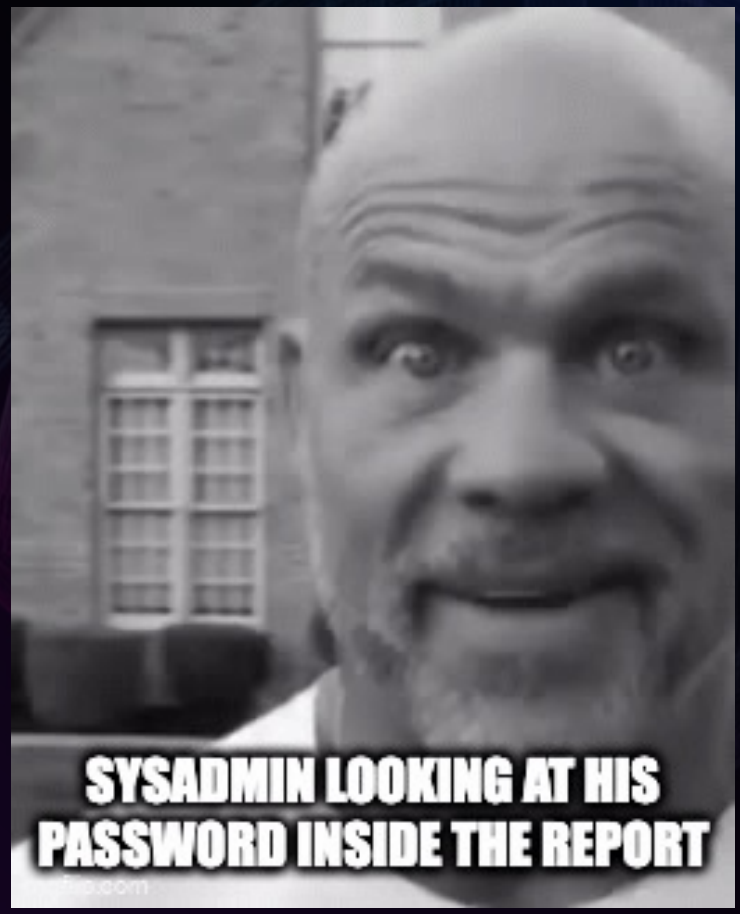
Remediations

How to patch

- What is the name of the vulnerability ?
- How can I patch it ?

Report Presentation

- Questions
- Advices



Interested ? Where to start

Total noob or beginner, where do I start?

“Free” Resources

Tryhackme.com

Root-me.org

Hackthebox.com /
vulnhub.com

Youtube Channels

@_JohnHammond

@NetworkChuck

@davidbombal

Certifications

Entry Level

- CompTIA (Security+, Network+)
- eJPT (INE)
- CEH (Eccouncil)

Advanced

- eWPT (INE)
- PNPT (TCM Security)
- OSCP (Offsec)

Atelier Pentesting Part 2

Adrien Lasalle @2024

Links

DVWA lab

- https://github.com/opsxcq/docker-vulnerable-dvwa
- Install docker (sudo apt install docker.io)

Web Basics

Using root-me challenges

- HTML
- Javascript
- Client / Server

DVWA

Web Attacks

- XSS
- SQL
- Command Injection

Thank you

https://github.com/AlrikRr/Talks