Khoa Mạng máy tính & Truyền thông
Ngành An toàn thông tin

BÁO CÁO TỔNG KẾT ĐỒ ÁN – Bảo mật Web & Ứng dụng

GVHD: Ngô Khánh Khoa

PTHELPER: AN OPEN SOURCE TOOL TO SUPPORT THE PENETRATION TESTING PROCESS

Group_C15
Khoa MMT&TT, ngành ATTT
Trường ĐH Công nghệ Thông Tin, ĐHQG Tp. HCM

Thông tin nhóm

C15

- Nguyễn Phan Hữu Khánh - 22520645
- Nguyễn Kim Khánh - 22520643
- Trần Anh Khôi - 22520701
- Lăng Thị Cẩm Nhung - 22521057

Thông tin đề tài

- Tên bài báo:
  - PTHELPER: AN OPEN SOURCE TOOL TO SUPPORT THE PENETRATION TESTING PROCESS
- Tác giả:
  - Jacobo Casado de Gracia
  - Alfonso Sánchez-Macián
- Nơi công bố:
  - Universidad Carlos III de Madrid, Madrid, Spain
- Thời gian công bố:
  - 12/01/2024

Nguồn: https://arxiv.org/abs/2406.08242

Nội dung báo cáo

Phần I: Tổng quan

Phần II: Kiến trúc

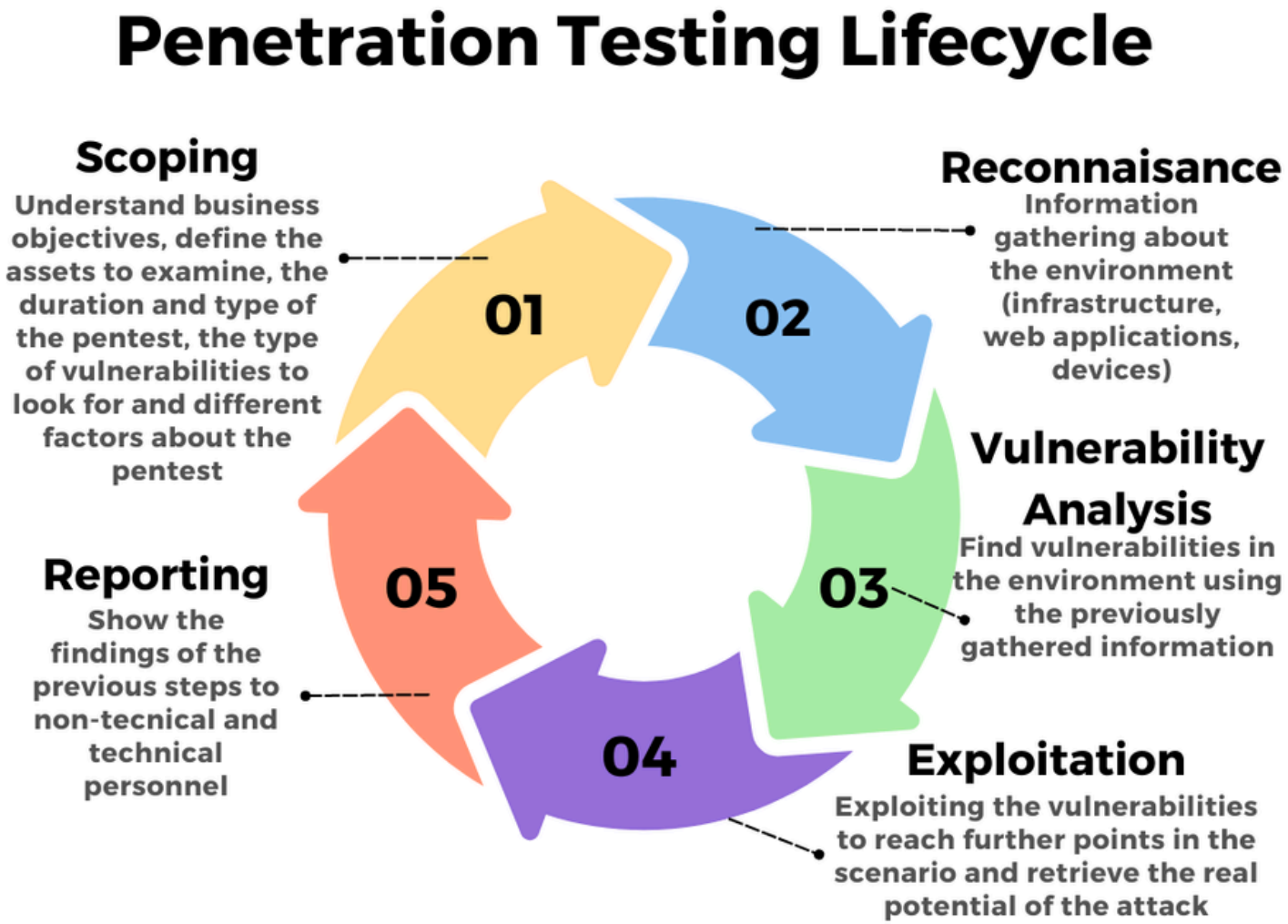
Phần III: Triển khai

Phần IV: Đánh giá & kết luận

Tổng quan

Phần I: Tổng quan

- Pentest (viết tắt của Penetration Testing) là một phương pháp được sử dụng để kiểm tra tính bảo mật của một hệ thống hoặc mạng máy tính
- Mục tiêu: tìm ra các lỗ hổng bảo mật có thể tồn tại trong hệ thống


Penetration Testing Lifecycle
Scoping
Understand business objectives, define the assets to examine, the duration and type of the pentest, the type of vulnerabilities to look for and different factors about the pentest
01
Reconnaisance
Information gathering about the environment (infrastructure, web applications, devices)
02
Vulnerability Analysis
Find vulnerabilities in the environment using the previously gathered information
03
Exploitation
Exploiting the vulnerabilities to reach further points in the scenario and retrieve the real potential of the attack
04
Reporting
Show the findings of the previous steps to non-tecnical and technical personnel
05

Pentest truyền thống

- Dữ liệu cần thiết để tạo báo cáo không đồng nhất
- Công việc ngoài chuyên môn
- Pentest là hoạt động tốn thời gian và nguồn lực
- Nguy cơ lỗ hổng bị bỏ qua

-> Cần tự động hóa Pentest

Pentest automation

- Giảm đáng kể thời gian và công sức
- Giảm thiểu nguy cơ lỗ hổng bị bỏ qua
- Có thêm thời gian để tập trung vào các công việc khác
- Giúp dễ dàng theo dõi thông tin được tạo ra trong suốt quá trình

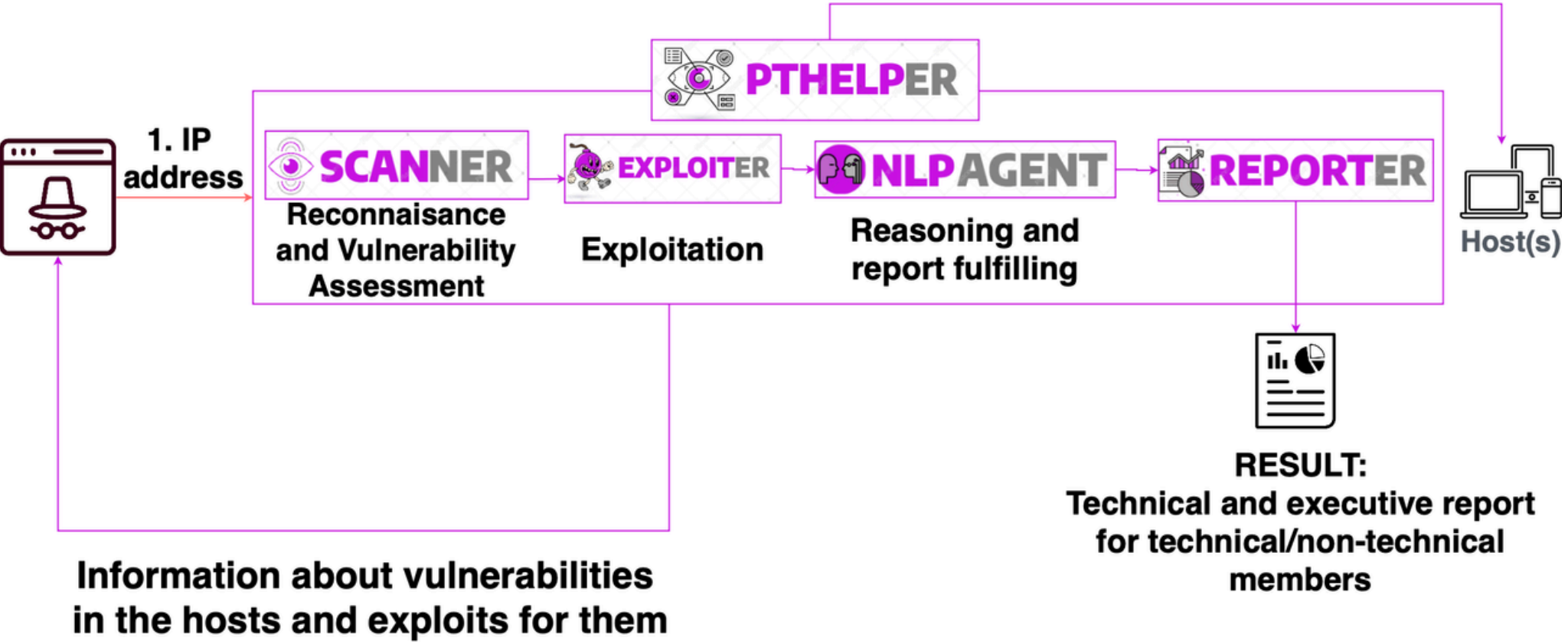
PTHelper

- Một công cụ mô đun được thiết kế cho pentester làm việc, cung cấp trợ giúp và công cụ cho từng giai đoạn quy trình

PTHELPER

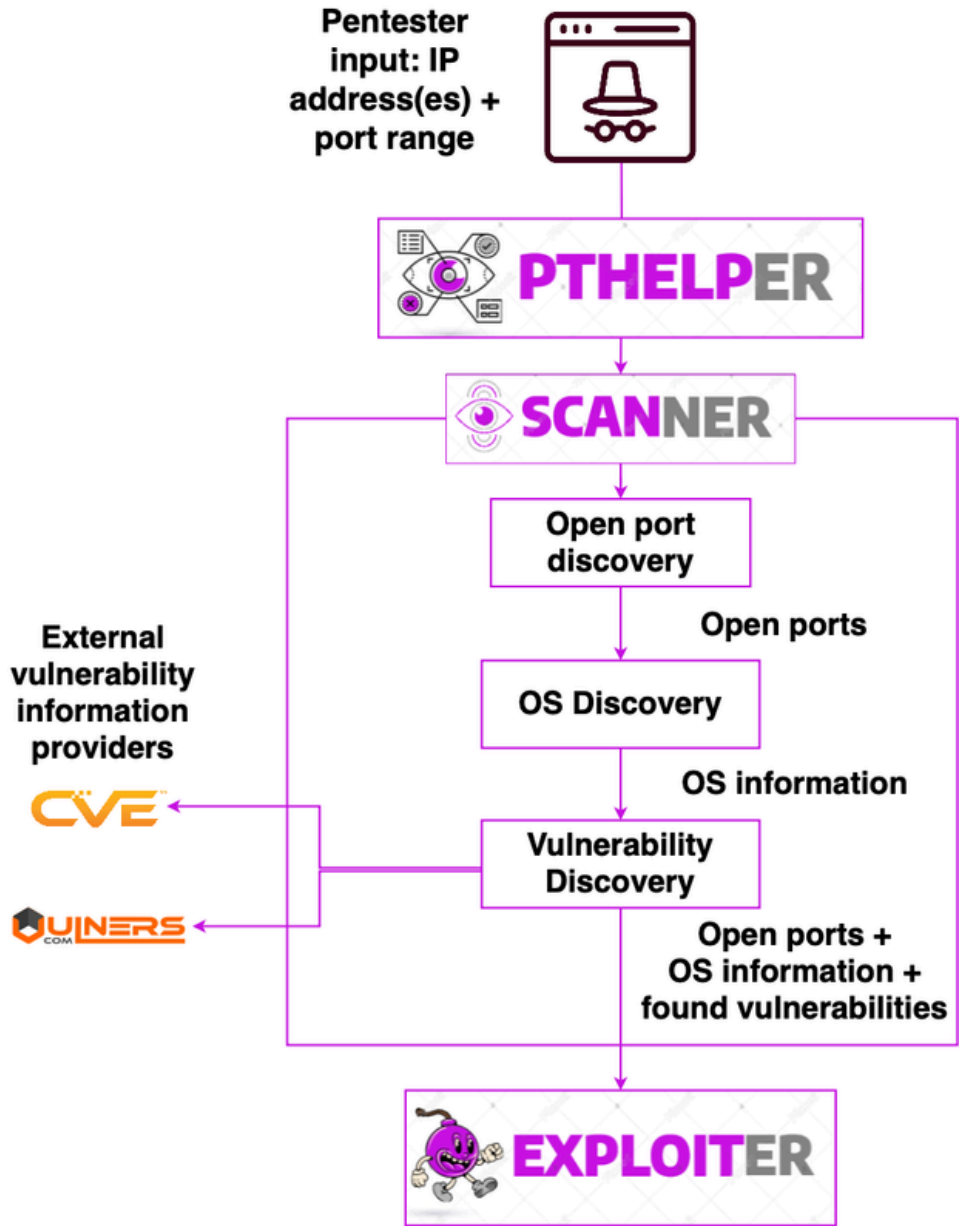
Kiến trúc

Phần II: Kiến trúc

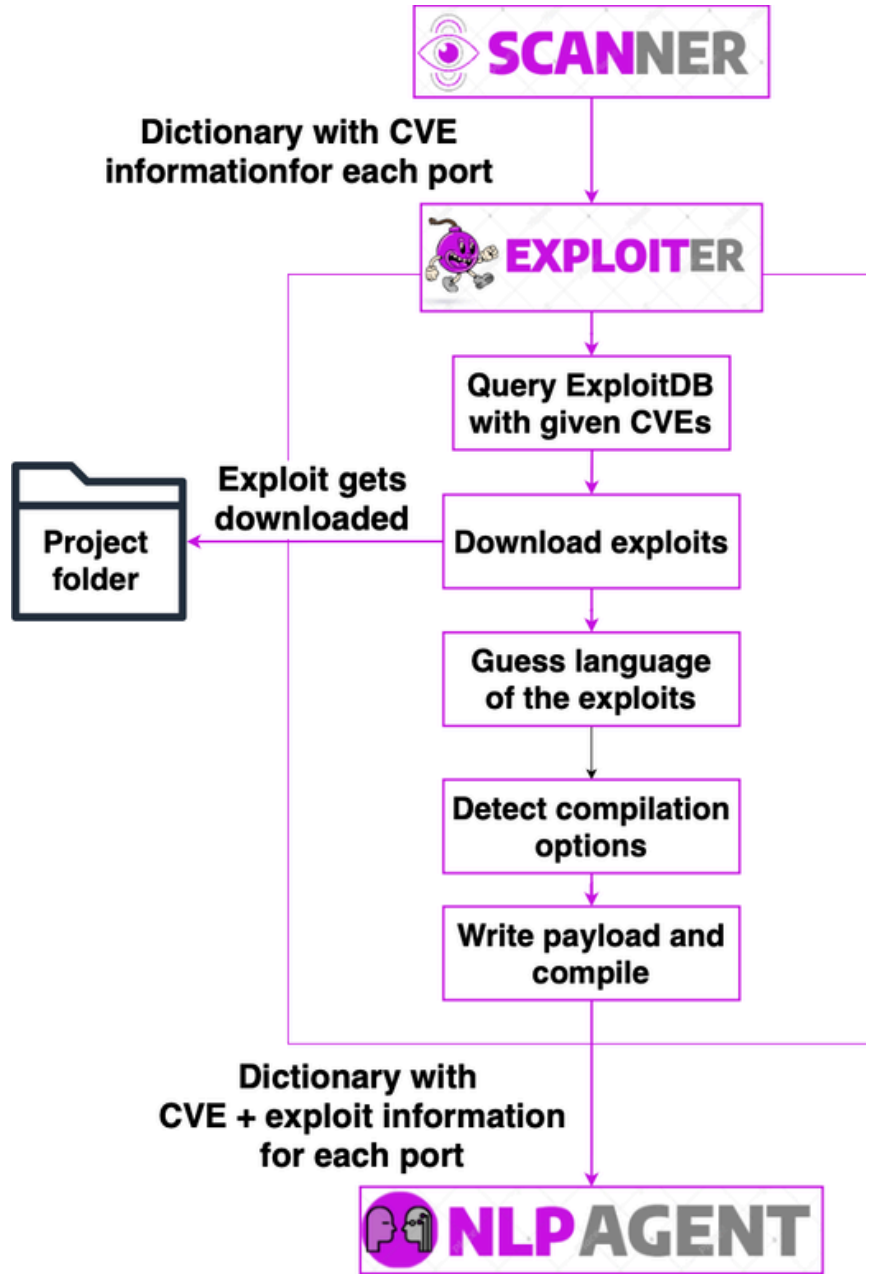


Cách PTHelper được sử dụng trong quy trình kiểm tra thâm nhập (Pentest)

1. Module Scanner



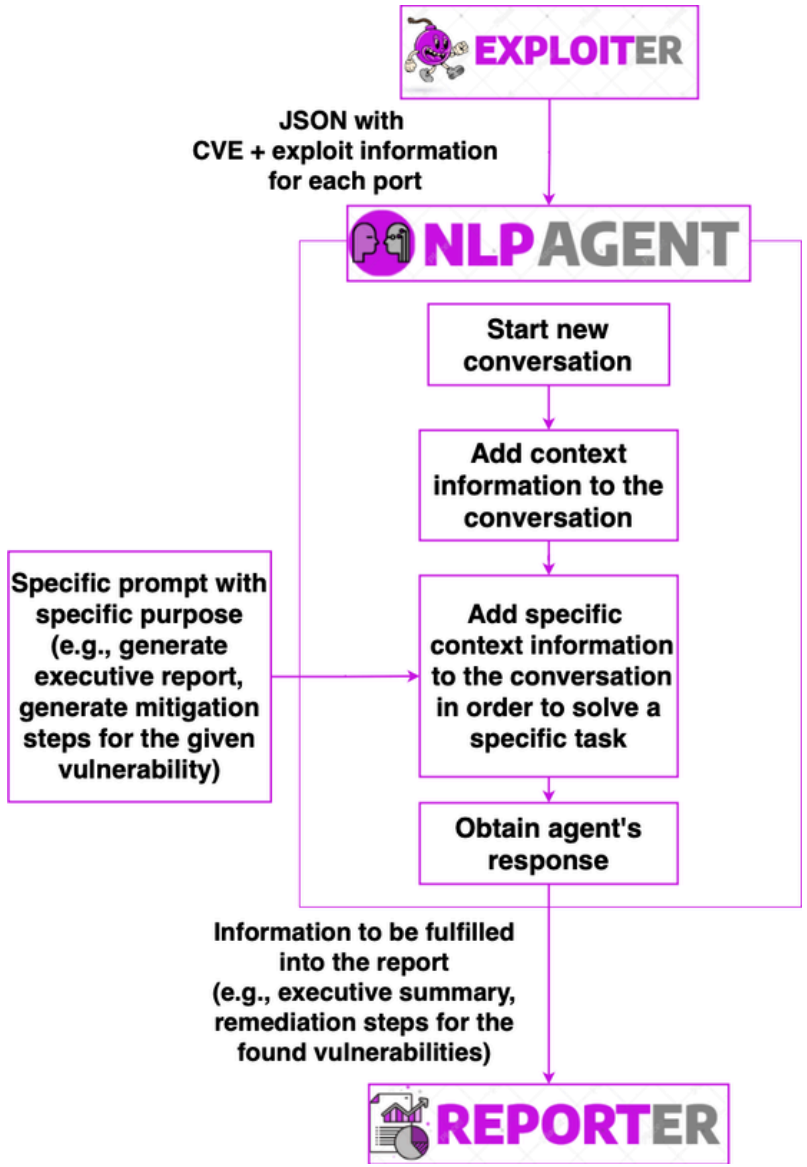
2. Module Exploiter



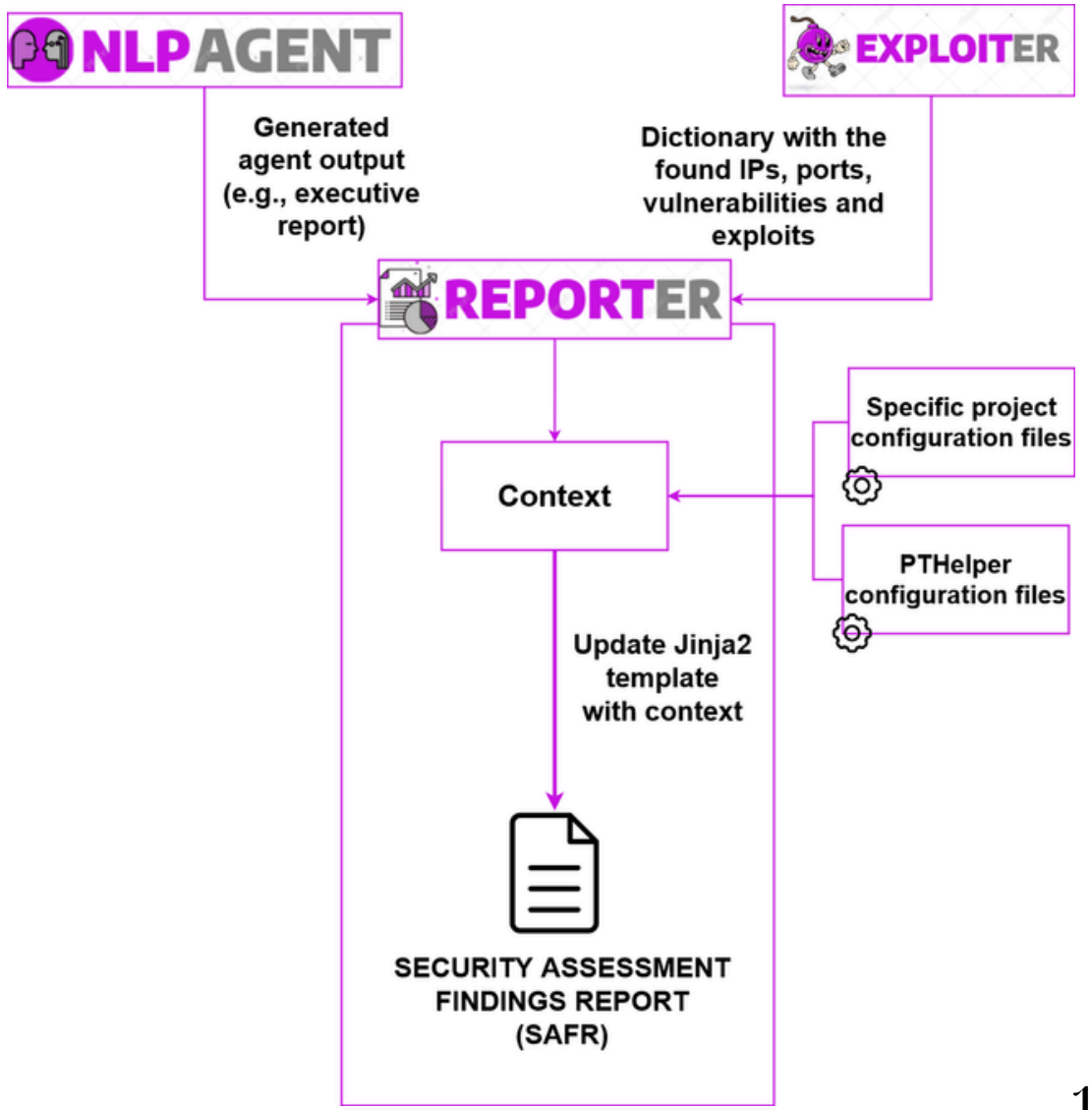
3. Module NLPagent

Cho phép:

- Tùy chỉnh phiên bản API của ChatGPT
- Nâng cấp và tích hợp các API NLP khác như Google Bard hoặc Llama 2 từ Meta
- Cấu hình Temperature quyết định mức độ sáng tạo hay tính logic trong đầu ra của NLPAgent



4. Module Reporter



Triển khai

Cài đặt

Link công cụ: PTHelper

Setup and requirements

In order to install the tool, please install the dependences first with `pip install -r requirements.txt` in the root folder of the tool. After that, execute `python3 pip install -e .` and use `pthelper` with the needed parameters. The parameters are:

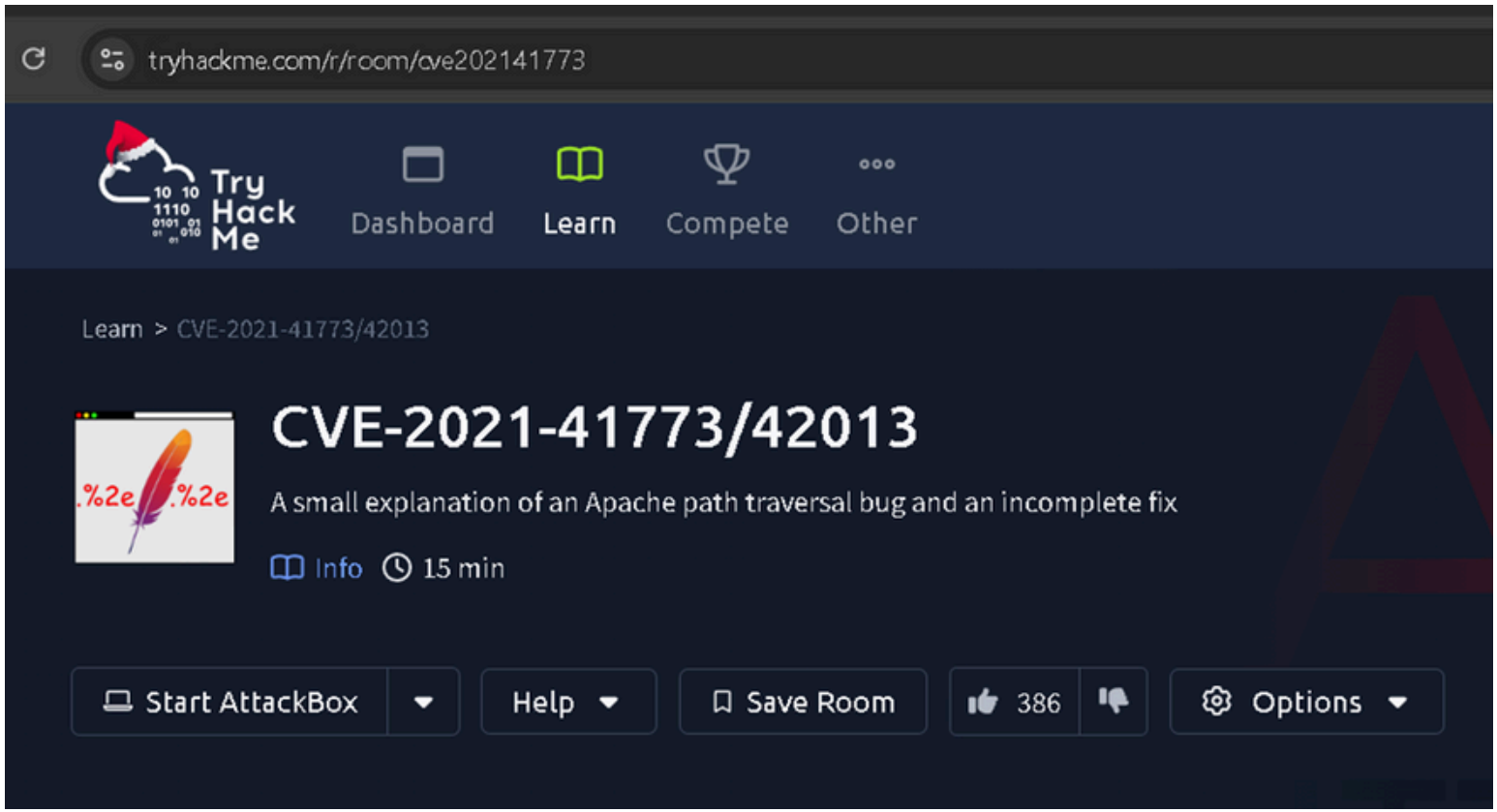
The tool also needs the `nmap` and, obviously, the `python3` binary. It is recommended to use the tool in Kali Linux, as the tool was developed and tested in this distribution. Remember to setup the correct OpenAI and NVD API key, located in the `config/pthelper_config.py` folder.

Cấu hình

Request NVD api key: NVD_api

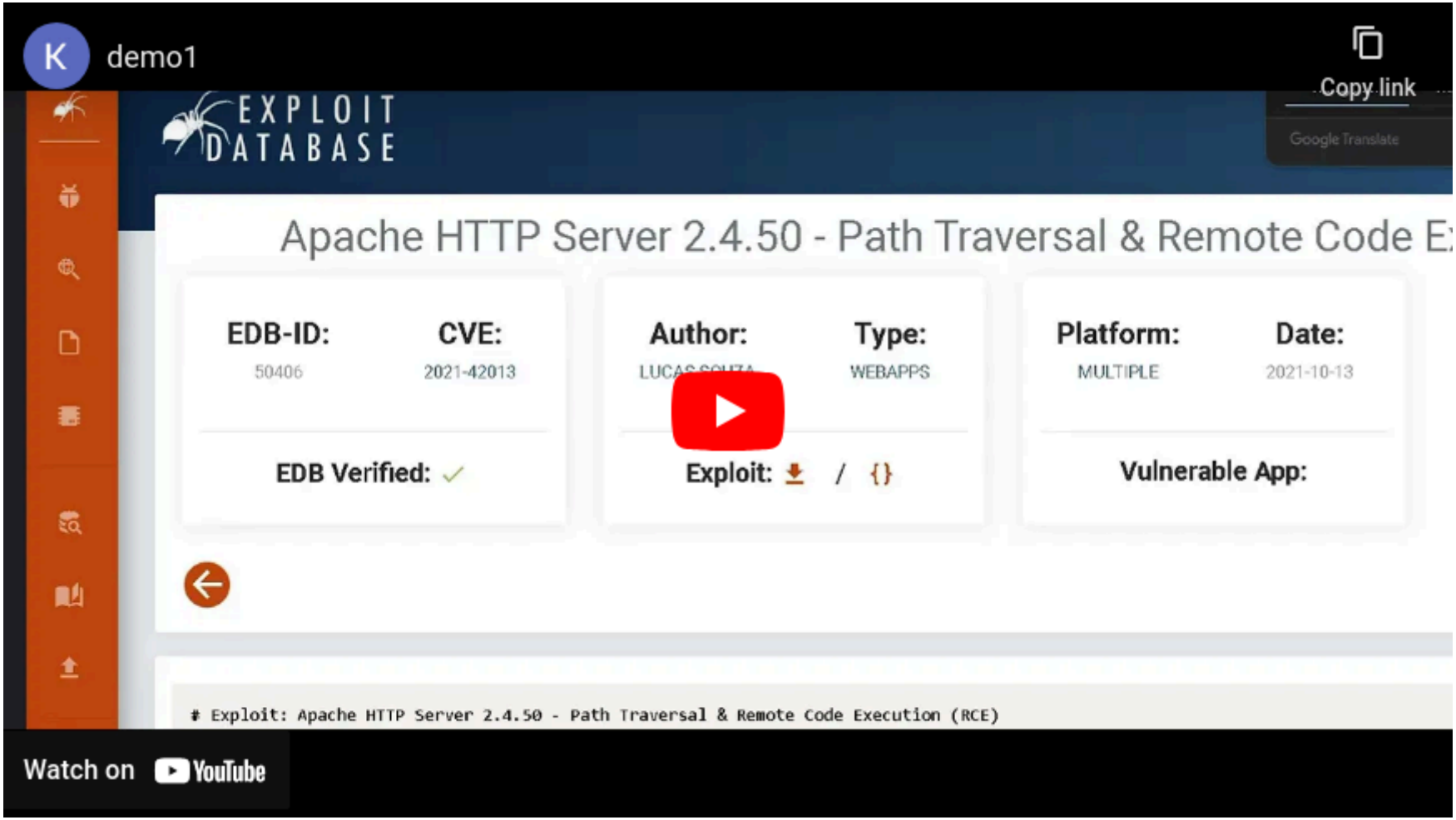
Create OpenAI api key: OpenAI_api

Kịch bản 1



TryHackMe room

Kịch bản 1


demo1
Copy link
Google Translate
EXPLOIT DATABASE
Apache HTTP Server 2.4.50 - Path Traversal & Remote Code E
EDB-ID:
50406
CVE:
2021-42013
Author:
Type:
WEBAPPS
Platform:
MULTIPLE
Date:
2021-10-13
EDB Verified:
Exploit:
/ {}
Vulnerable App:
Exploit: Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)
Watch on YouTube

Kịch bản 1

Kết quả:

- Port: 8080 (Apache 2.4.49)
- Số lượng lỗ hổng phát hiện: 35 CVE
- Thời gian chạy khoảng 16 phút

Kịch bản 1

VULNERABILITY SUMMARY & REPORT CARD

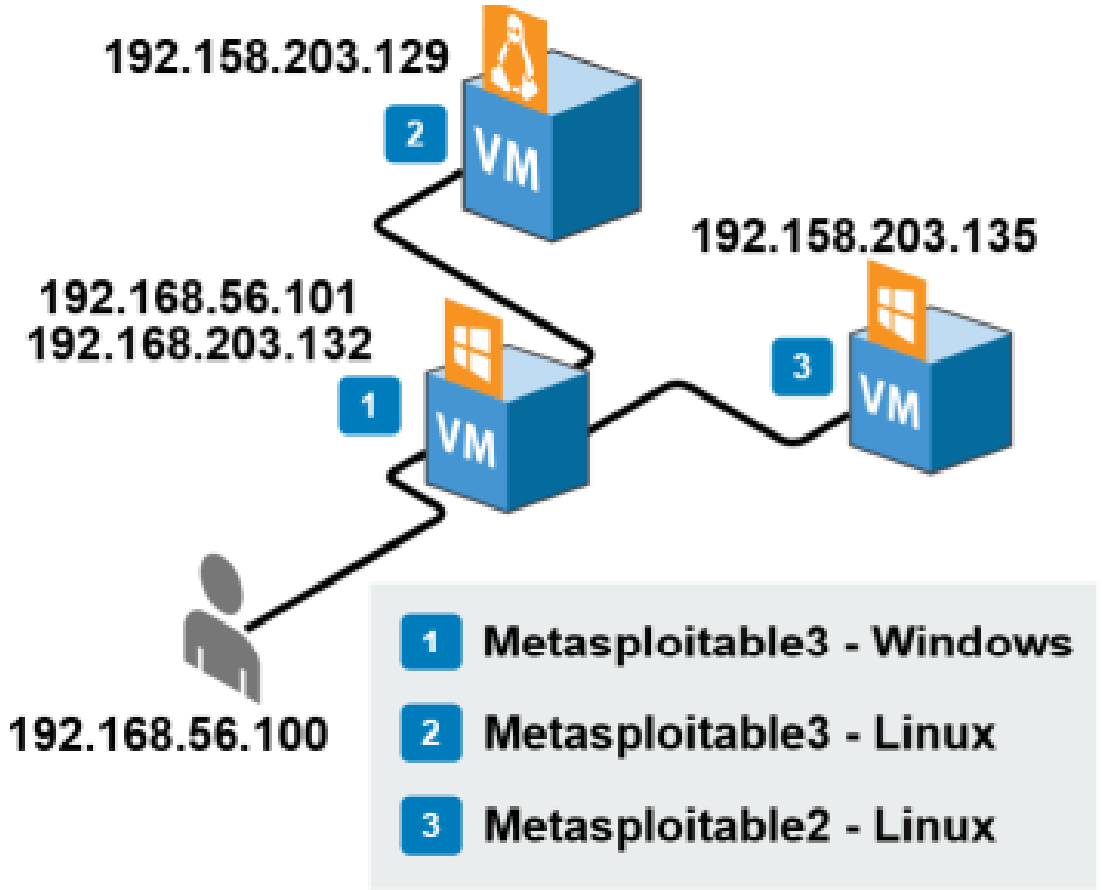
The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

11	18	6		0
Critical	High	Moderate	Low	Informational

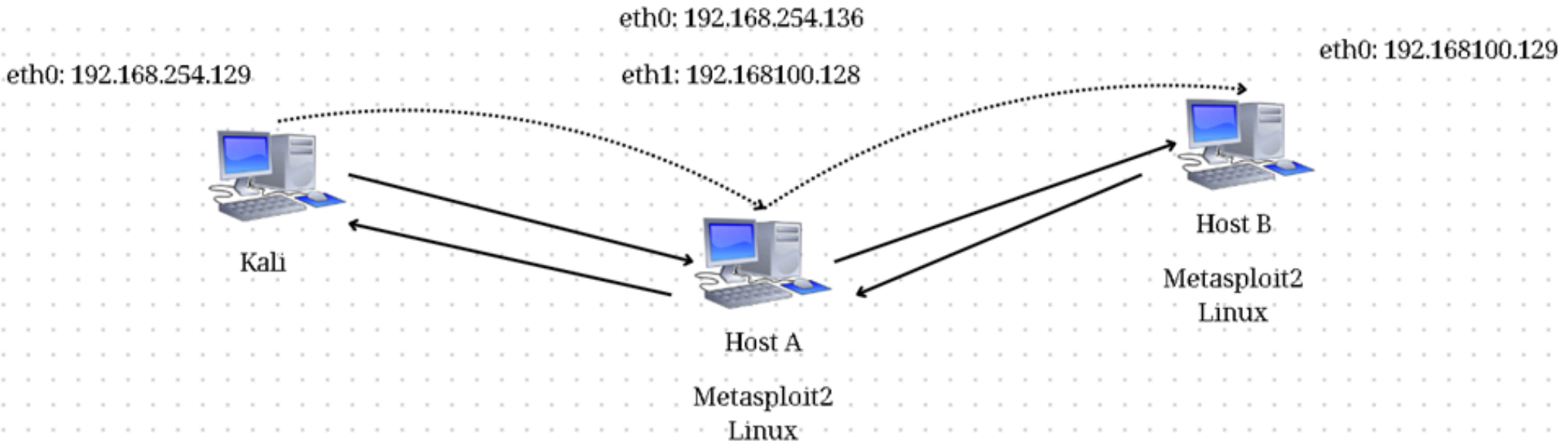
Report

Kịch bản 2



Black box infrastructure

Kịch bản 2



Black box infrastructure

Phần III: Triển khai

Kịch bản 2

Kết quả:

- Port: 22 (OpenSSH 4.7)
- Số lượng lỗ hổng phát hiện: 31 CVE
- Host A và Host B đều chạy khoảng 14 phút

Kịch bản 2

VULNERABILITY SUMMARY & REPORT CARD

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

Critical	High	Moderate	Low	Informational
2	10	19		0

Report A

Kịch bản 2

Hosts analyzed

Host	Information about the host			
	Ports	Service	Version	CVEs
127.0.0.1	22	ssh	4.7p1 Debian 8ubuntu1	CVE-2023-48795 CVE-2023-51385 CVE-2023-38408 CVE-2021-36368 CVE-2020-15778 CVE-2019-6111 CVE-2019-6110 CVE-2019-6109 CVE-2018-20685 CVE-2018-15473 CVE-2017-15906 CVE-2016-6515 CVE-2016-6210 CVE-2016-3115 CVE-2016-20012 CVE-2016-1908 CVE-2016-10708 CVE-2016-10012 CVE-2016-10011 CVE-2016-10010 CVE-2016-10009 CVE-2015-8325

Report B

Đánh giá & kết luận

Ưu điểm

- Tự động hóa quá trình kiểm thử mà quyền khai thác vẫn nằm ở pentester
- Dễ sử dụng
- Cung cấp mã khai thác và các thông tin hữu ích liên quan
- Tạo báo cáo tự động, tiết kiệm thời gian cho pentester
- Kiến trúc module giúp việc tích hợp các tính năng hoặc công cụ mới trở nên dễ dàng

Vấn đề

- Tồn tại lỗi chức năng
- Mã khai thác chưa tối ưu

Nhóm C15

Cảm ơn thầy và các bạn đã lắng nghe

Email: inseclab@uit.edu.vn
Website: https://inseclab.uit.edu.vn/
Fanpage: https://www.facebook.com/inseclab