

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

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

Phân I: Tổng quan

Phân II: Kiến trúc

Phân III: Triển khai

Phân IV: Đánh giá & kết luận



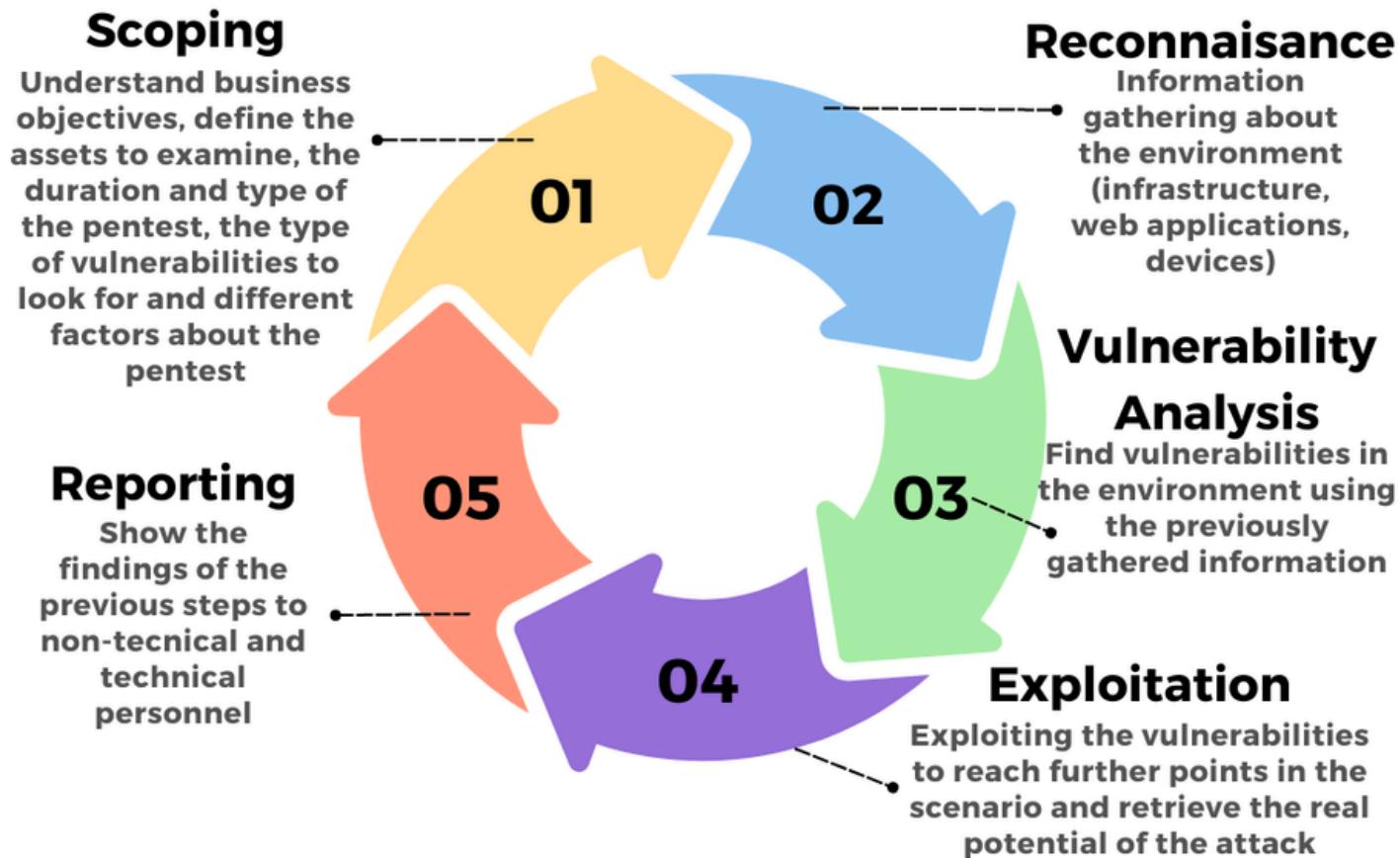
Tổng quan



- 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



Pentest truyền thông

- 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



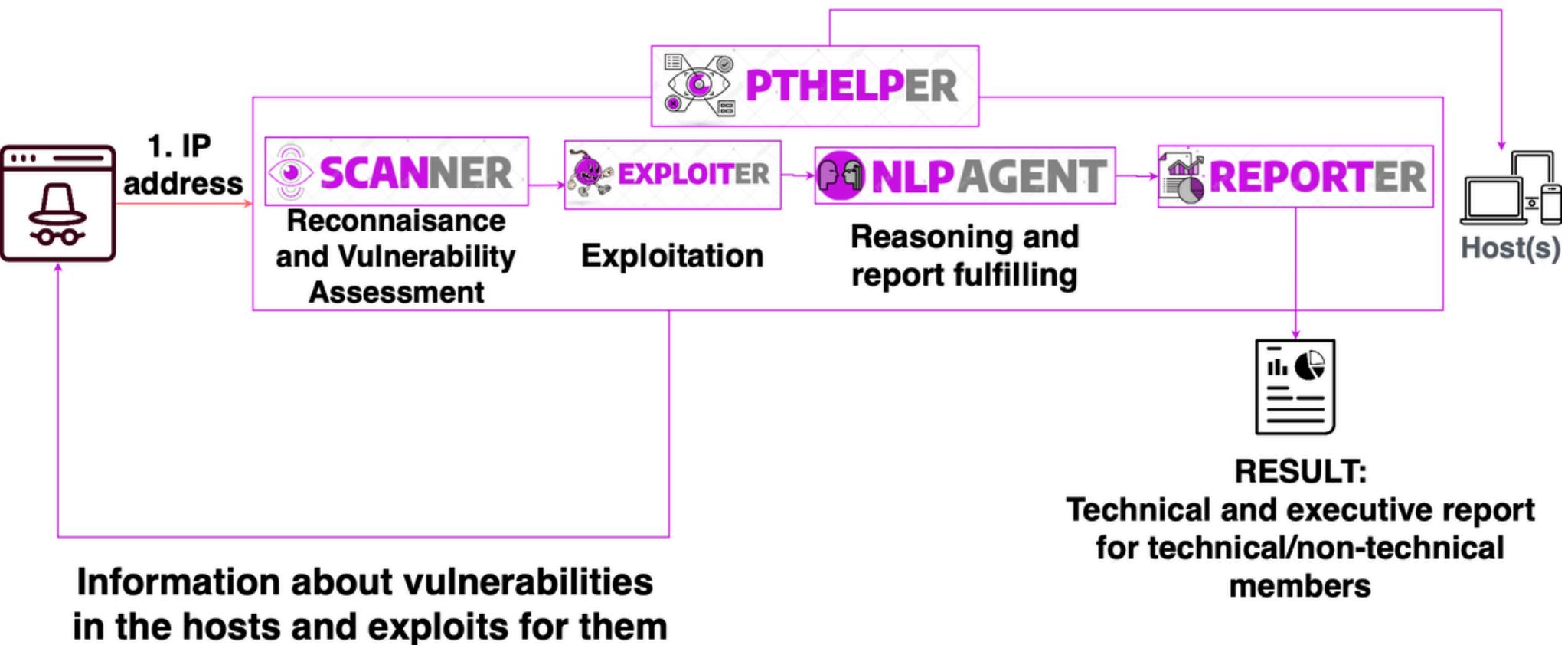


Kiến trúc

11



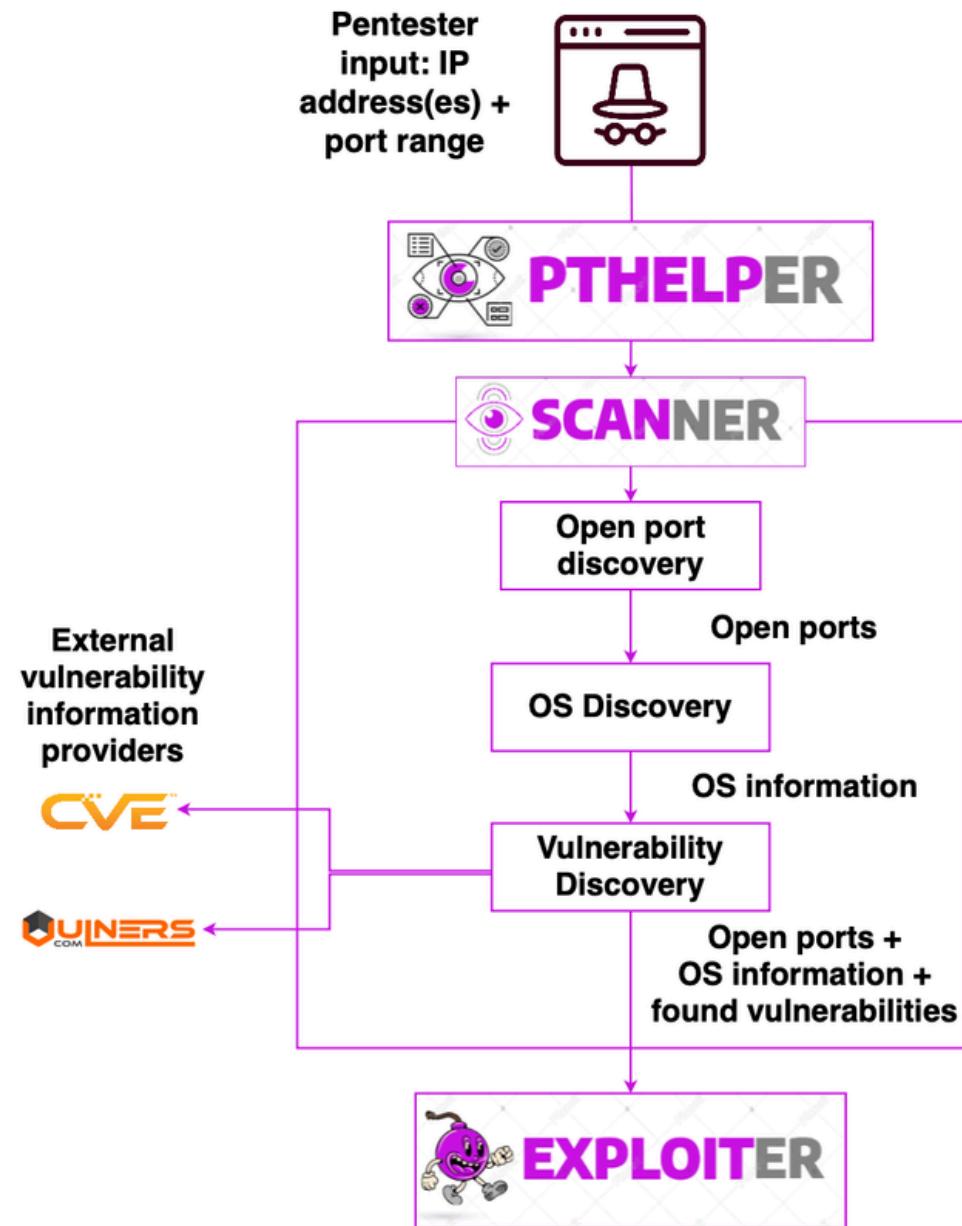
Phần II: Kiến trúc



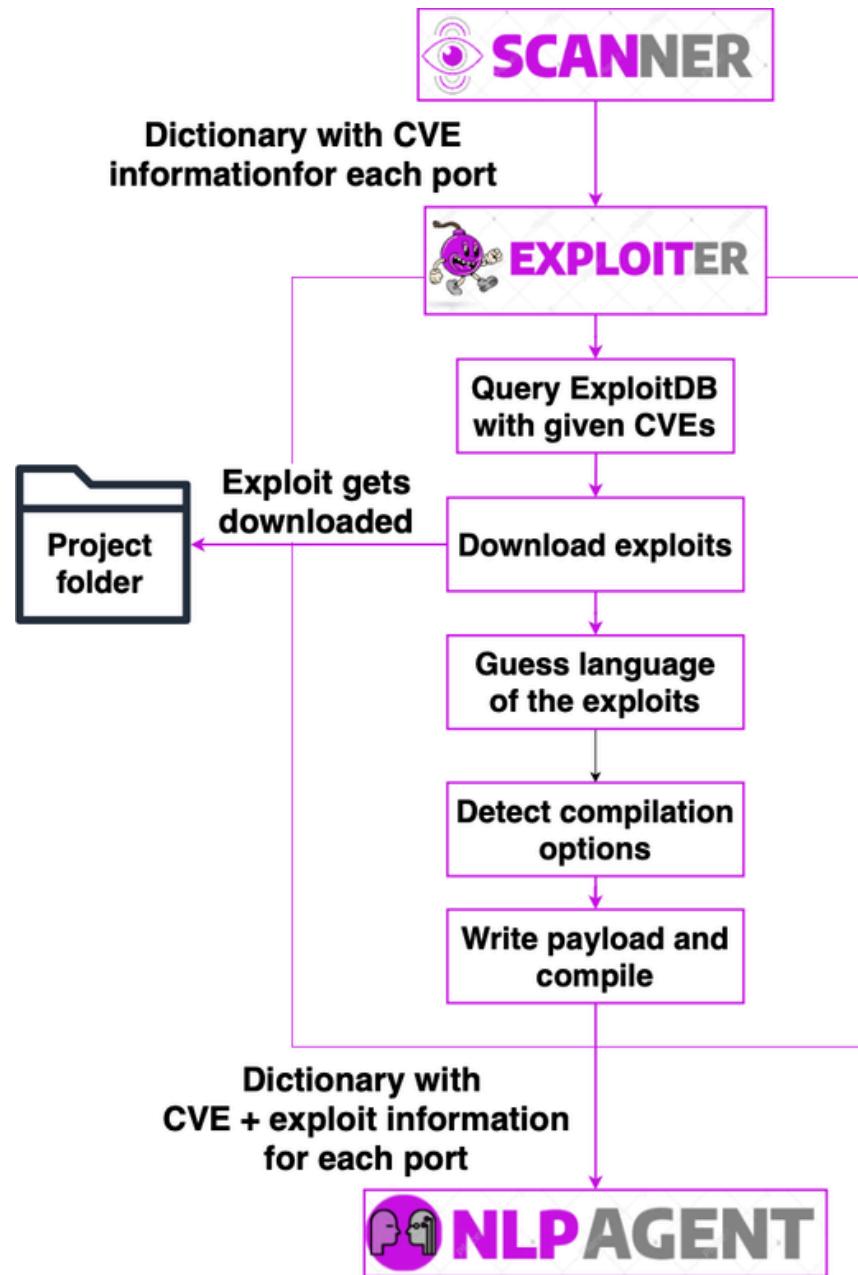
Cách PTHelper được sử dụng trong quy trình kiểm tra thâm nhập (Pentest)



1. Module Scanner



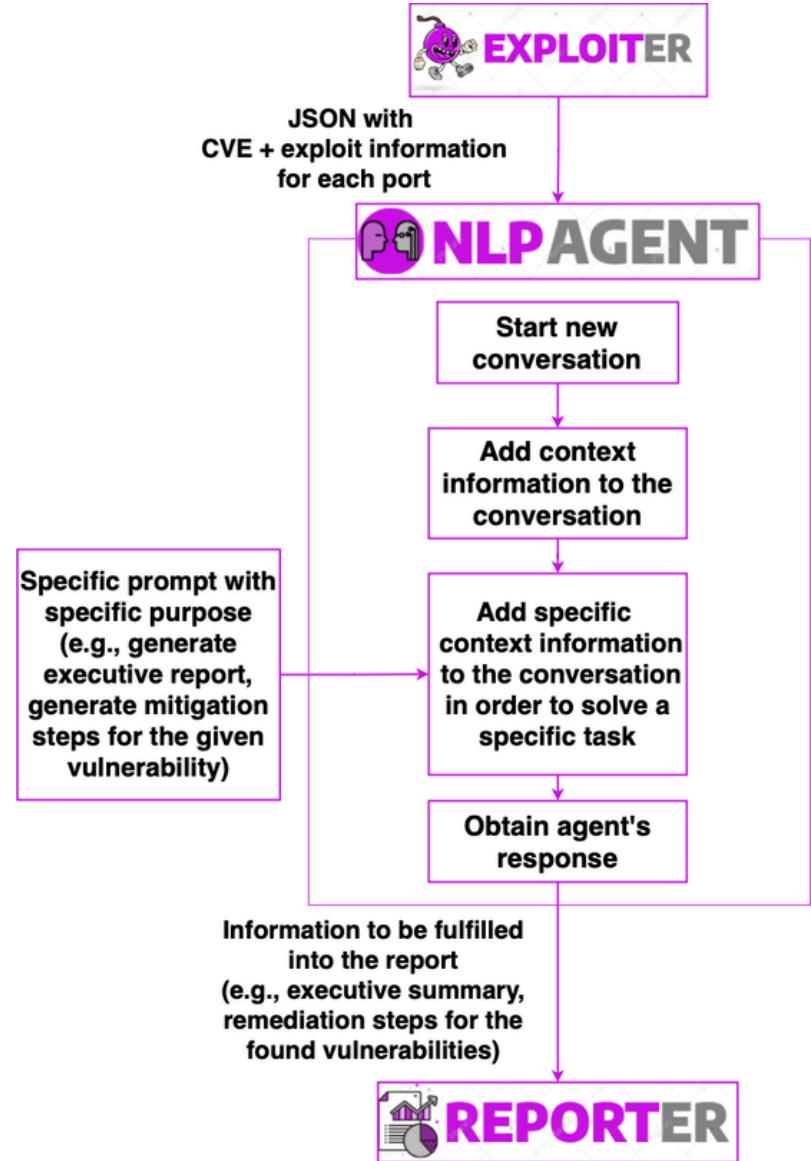
2. Module Exploiter



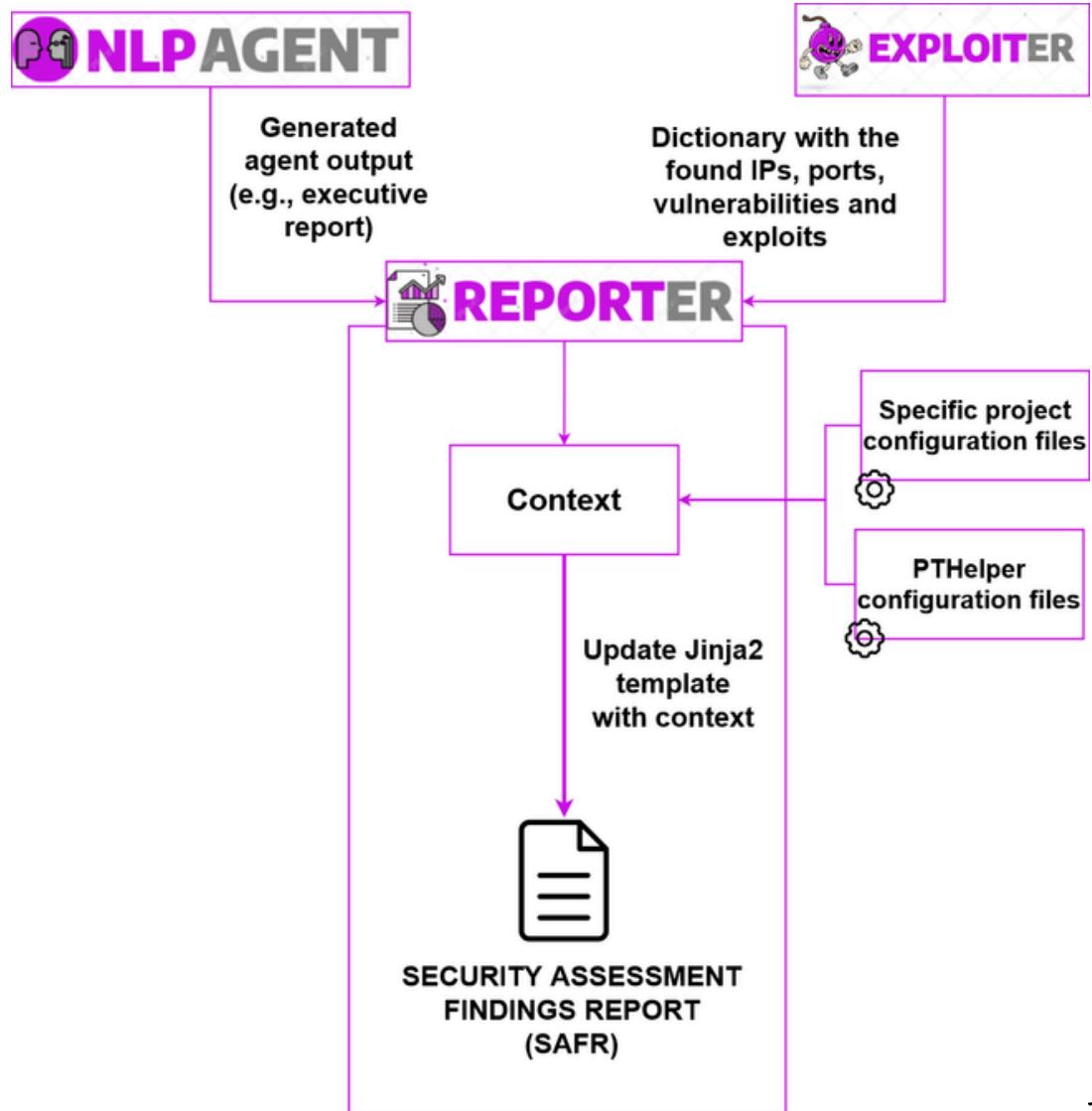
3. Module NLPAgent

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

17



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.



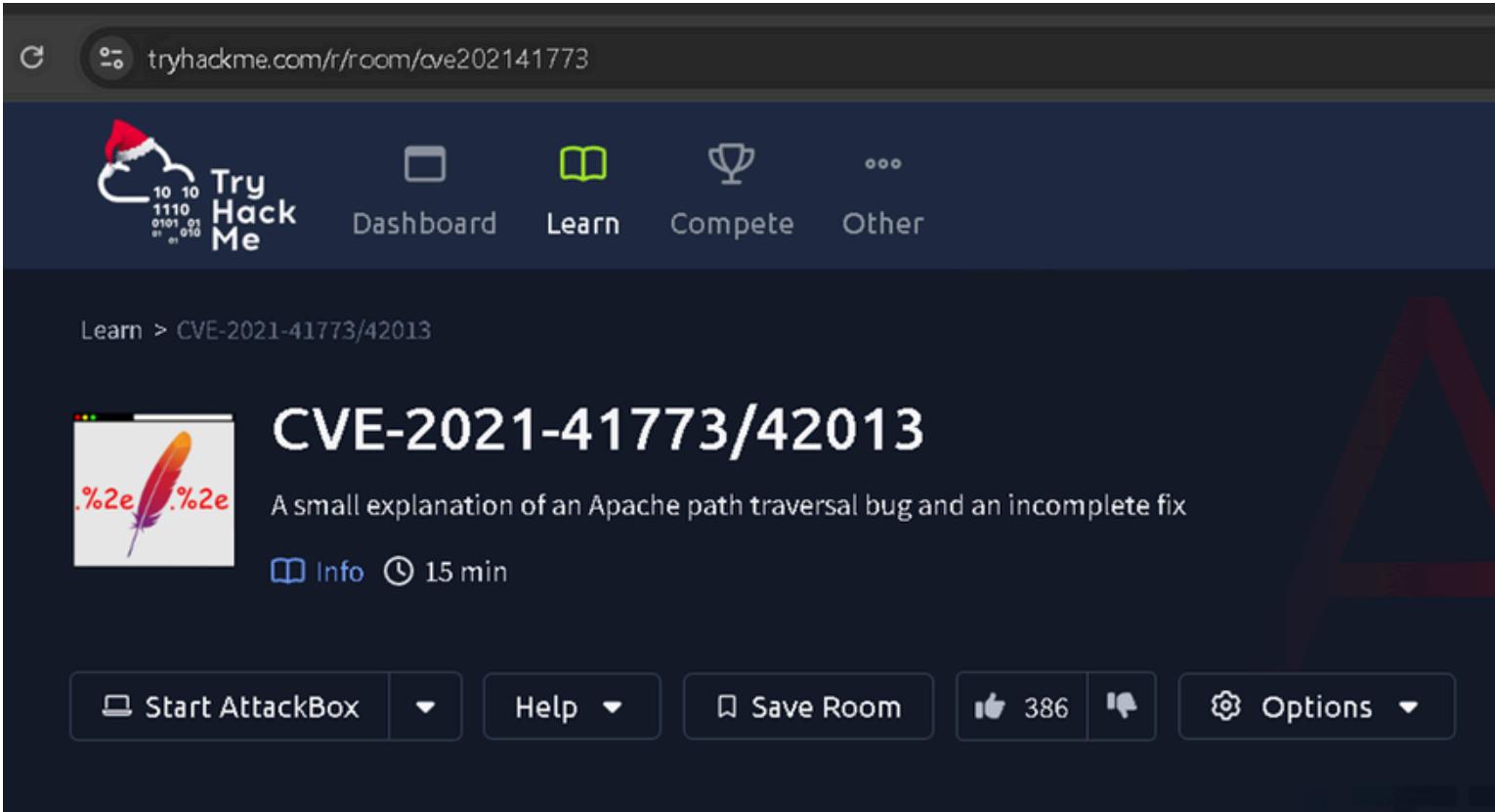
Cấu hình

Request NVD api key: NVD_api

Create OpenAI api key: OpenAI_api



Kịch bản 1

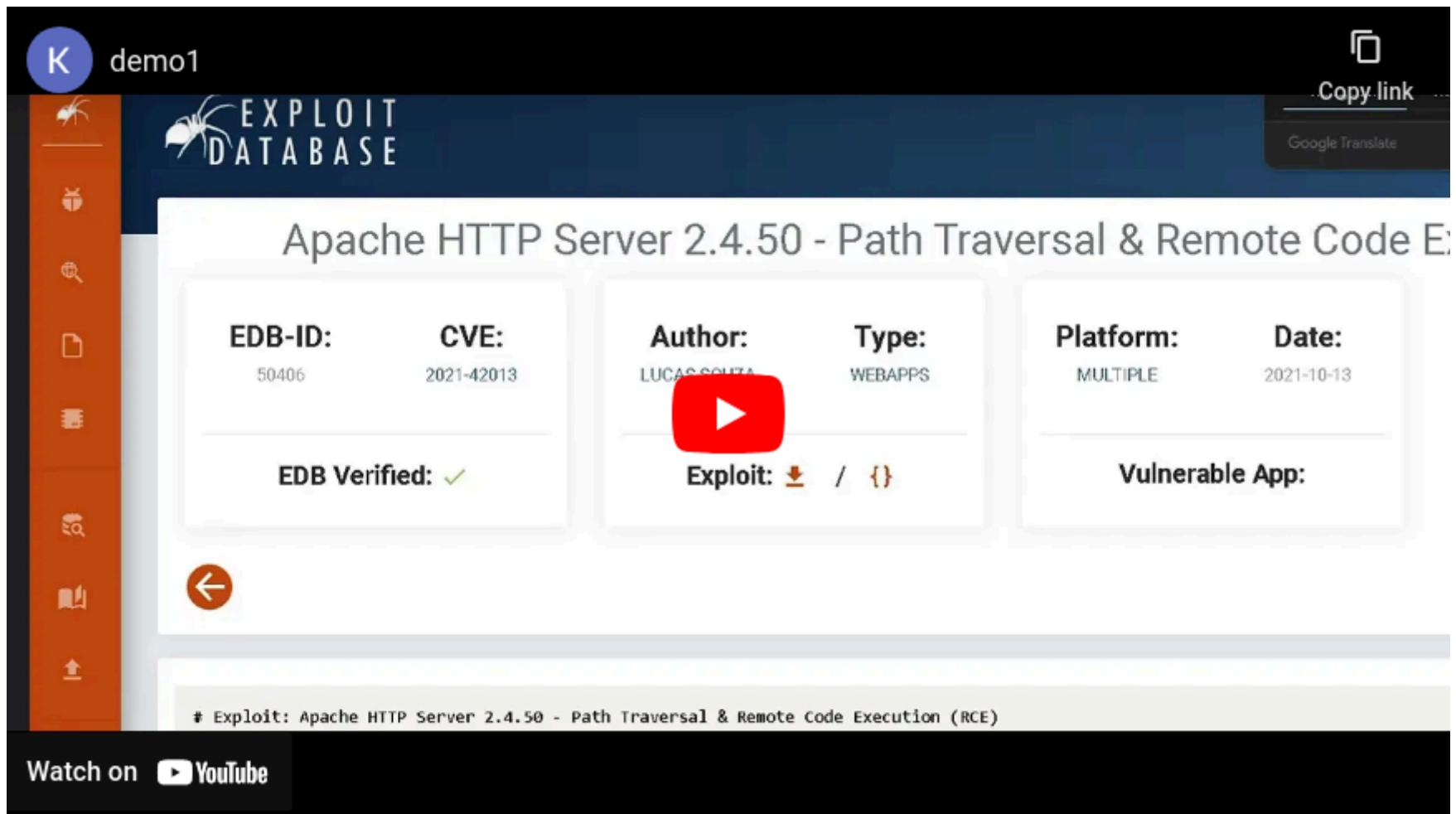
A screenshot of a web browser displaying a TryHackMe room. The URL in the address bar is "tryhackme.com/r/room/cve202141773". The page header includes the TryHackMe logo with a Santa hat, and navigation links for Dashboard, Learn, Compete, and Other. Below the header, the path "Learn > CVE-2021-41773/42013" is shown. The main content features a large title "CVE-2021-41773/42013" next to a small icon of a computer monitor with a feather quill pen. A subtitle reads "A small explanation of an Apache path traversal bug and an incomplete fix". Below this, there is an "Info" button with a book icon and a "15 min" duration indicator. At the bottom of the page are several interactive buttons: "Start AttackBox" with a dropdown arrow, "Help" with a dropdown arrow, "Save Room" with a clipboard icon, a like/dislike counter showing "386" likes and 1 dislike, and "Options" with a dropdown arrow.

TryHackMe room

20



Kịch bản 1



The screenshot shows a web interface for the Exploit Database. At the top, there's a navigation bar with a user icon (K), the name "demo1", and a search bar. To the right of the search bar are buttons for "Copy link" and "Google Translate". On the left, there's a vertical sidebar with icons for search, file, and other database functions.

The main content area displays a exploit entry for "Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution". The details are summarized in the following table:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50406	2021-42013	LUCAS SOUTA	WEBAPPS	MULTIPLE	2021-10-13

Below the table, there are links for "Exploit" (with download and exploit files), "Vulnerable App:", and a "Watch on YouTube" button.

At the bottom of the page, there's a note: "# Exploit: Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)".



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:

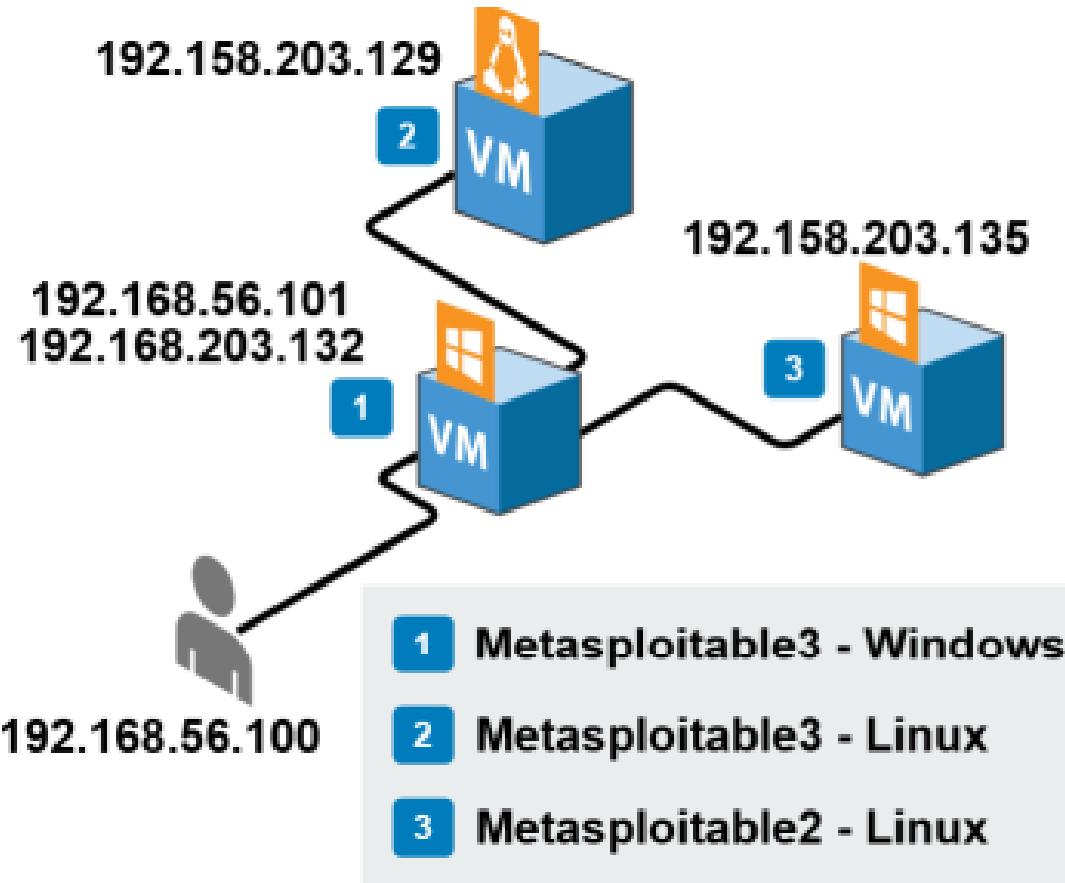
Internal Penetration Test Findings

11	18	6		0
Critical	High	Moderate	Low	Informational

Report



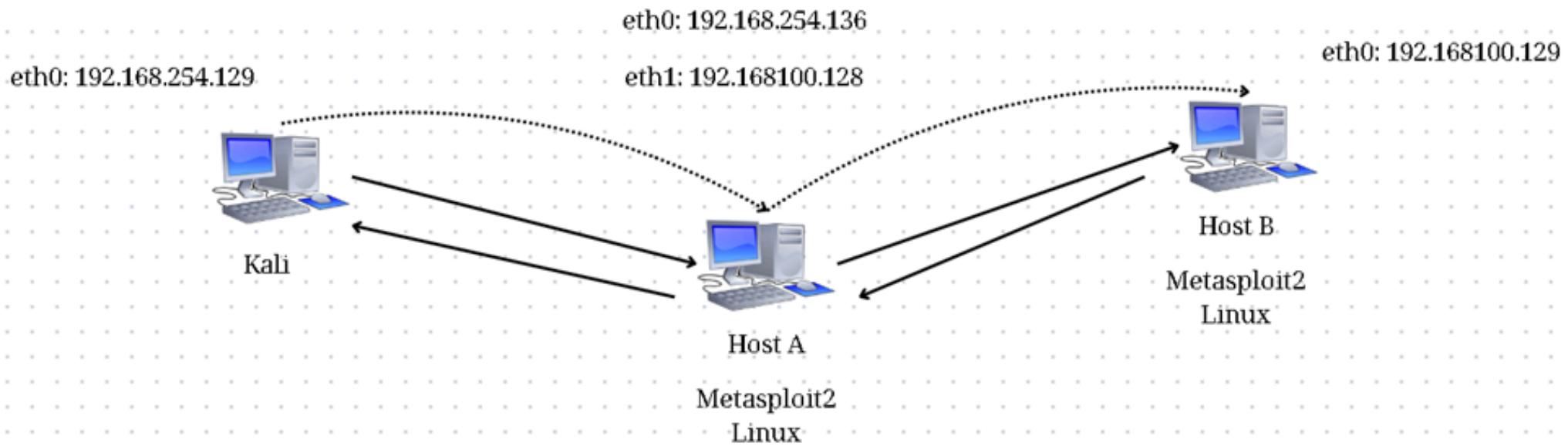
Kịch bản 2



Black box infrastructure



Kịch bản 2



Black box infrastructure

25



Phân III: Triển khai



K demo2

(venv)kali@kali: ~/PTHelper/projects/tfm/exploits

File Actions Edit View Help

(venv)kali@kali: ~/PTHelper x (venv)kali@kali: ~/PTHelper/projects/tfm/exploits

GNU nano 8.1 CVE-2018-15473_45210.py

```
#!/usr/bin/env python

# Copyright (c) 2018 Matthew Oakley
#
# Permission is hereby granted, free of charge, to any person obtaining
# a copy of this software and associated documentation files (the "Software"),
# to deal in the Software without restriction, including without limitation
# the rights to use, copy, modify, merge, publish, distribute, sublicense,
# and/or sell copies of the Software, and to permit persons to whom the
# Software is furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included
# in all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
# EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
# MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
# IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
# DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
# ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
# MISUSE OF THE SOFTWARE.
```

[Read 84 lines (converted from DOS format)

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execu
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justi

Copy link

Watch on YouTube



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

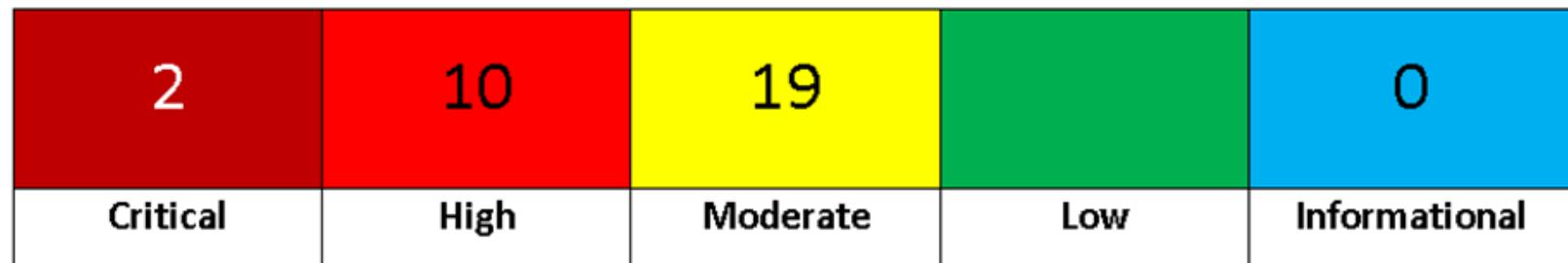


Kịch bản 2

VULNERABILITY SUMMARY & REPORT CARD

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

Internal Penetration Test Findings



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 Ubuntu1	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

29





Đánh giá & kết luận

30



Phân IV: 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



Phân IV: Đánh giá & kết luận

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>