Report Pentesting Network Security of HASS Company

Made by Mr Thai Long – Mr Quang Vinh – Mr Trung Hieu

This report is made with a request from HASS company that prohibits copying or performing similar acts without the owner's permission.

Ngày thực hiện: 07-07-2024

**I. Giới Thiệu**

**1. Mục Tiêu**

Mục tiêu của cuộc kiểm thử xâm nhập là xác định và đánh giá các lỗ hổng bảo mật trong hệ thống mạng và ứng dụng của Công ty HASS, nhằm đề xuất các biện pháp khắc phục và nâng cao mức độ bảo mật.

**2. Phạm Vi**

Cuộc kiểm thử bao gồm:

* Hệ thống mạng nội bộ.
* Các ứng dụng web và dịch vụ trực tuyến.
* Hệ điều hành Windown 10

### II. Phát Hiện Lỗ Hổng

**1. Lỗ Hổng CVE-2021-44228 (Log4Shell)**

Lỗ hổng CVE-2021-44228, còn được gọi là Log4Shell, là một lỗ hổng nghiêm trọng trong thư viện Log4j của Apache. Lỗ hổng này cho phép kẻ tấn công thực thi mã từ xa bằng cách gửi một chuỗi đặc biệt đến hệ thống.

* **Mô tả:** Kẻ tấn công có thể khai thác lỗ hổng này bằng cách gửi các chuỗi dữ liệu được chế tạo đặc biệt tới các dịch vụ và ứng dụng sử dụng Log4j.
* **Tác động:** Thực thi mã từ xa, truy cập trái phép vào hệ thống và dữ liệu.

**2. Tấn Công Lừa Đảo (Phishing Mail)**

Phát hiện các email lừa đảo được gửi tới nhân viên công ty nhằm đánh cắp thông tin đăng nhập và cài đặt phần mềm độc hại.

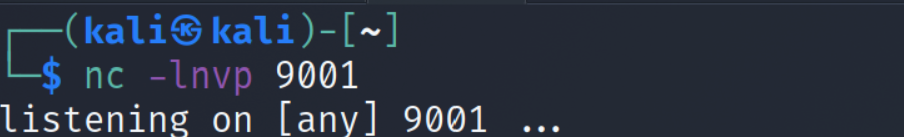
* **Mô tả:** Kẻ tấn công gửi các email chứa liên kết hoặc tệp đính kèm độc hại, giả mạo làm thông tin từ các nguồn tin cậy.
* **Tác động:** Đánh cắp thông tin nhạy cảm, cài đặt phần mềm độc hại và chiếm quyền điều khiển tài khoản người dùng.

### III. Các Bước Pentest Lỗ Hổng

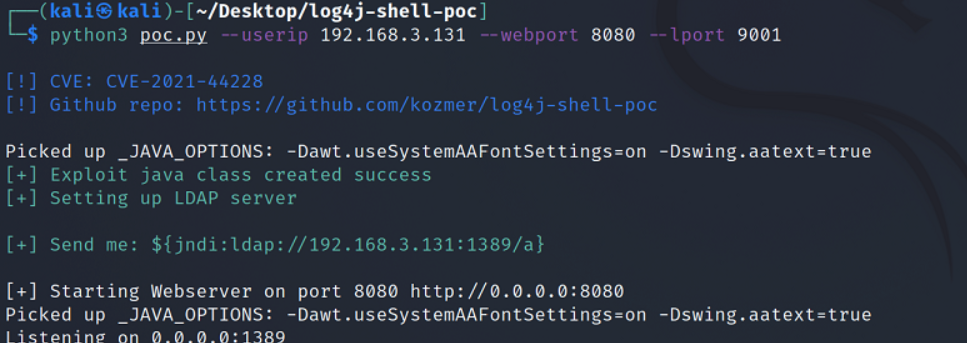
**1. Kiểm Thử Lỗ Hổng CVE-2021-44228 (Log4Shell)**

**Thu thập thông tin:** Xác định các dịch vụ và ứng dụng đang sử dụng Log4j thông qua quét hệ thống và phân tích mã nguồn.

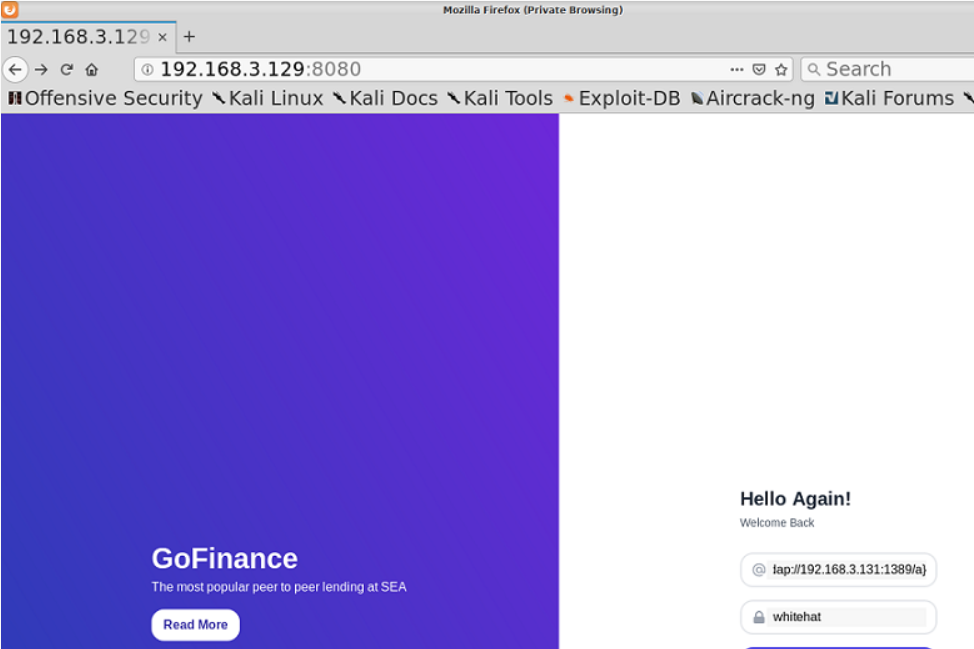
Chạy netcat để lắng nghe kết nối trên cổng 9001



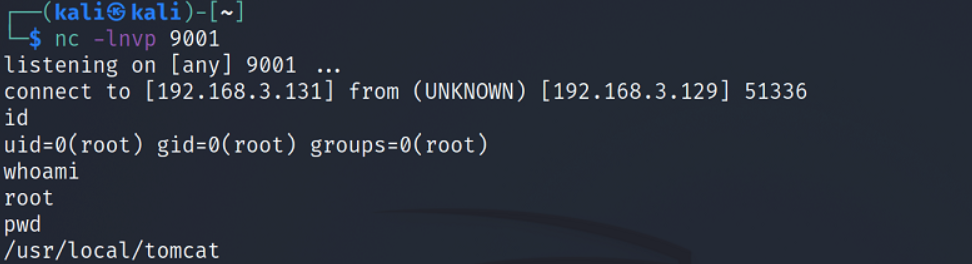
Mở một Terminal khác và chạy tệp poc.py vừa tải về ở trên. Trong đó, userip là địa chỉ ip của kali linux:



Lệnh trên sẽ tạo ra một máy chủ LDAP cục bộ độc hại. Sao chép giá trị đằng sau mục "Send me" và dán vào máy chủ web tồn tại lỗ hổng. Sau đó, click vào Login



Lúc này, payload được thực thi, và trong cửa sổ terminal, một reverse shell xuất hiện:

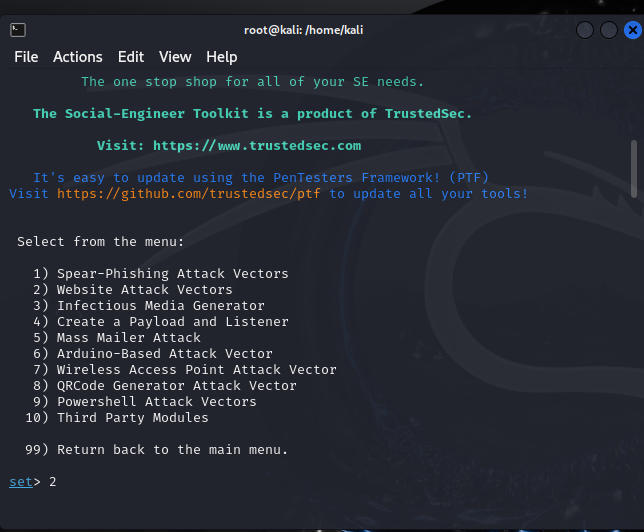


**2. Tấn Công Lừa Đảo (Phishing Mail):**

Tạo phishing mail bằng setoolkit:



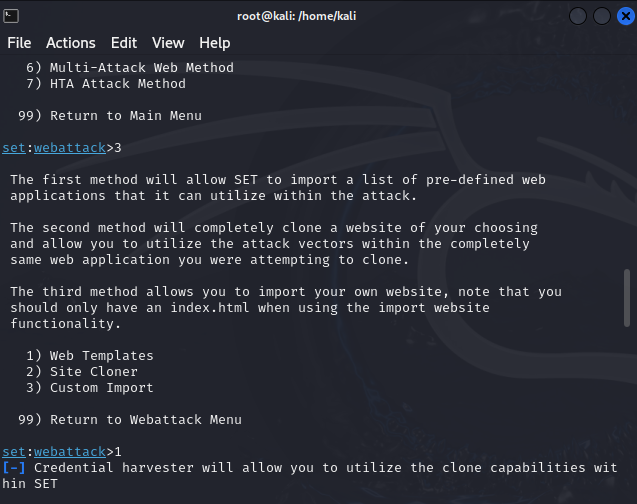
Chọn công cụ “ Website Attack Vectors” :



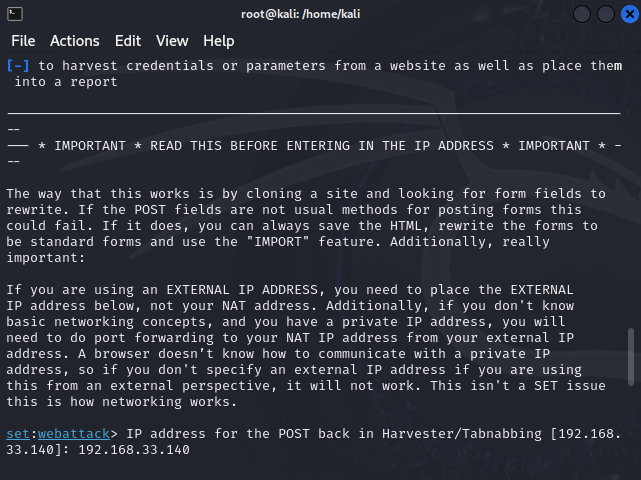
Chọn “Credential Harvester Attack Method” :



Tiếp theo chọn “ Web Templates”



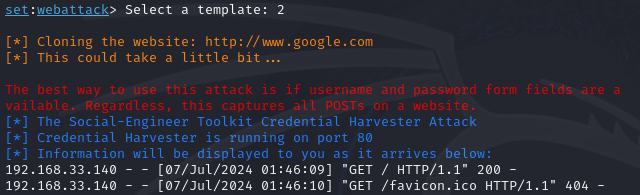
Nhập ip máy hacker để fake web interface “192.168.33.140”:



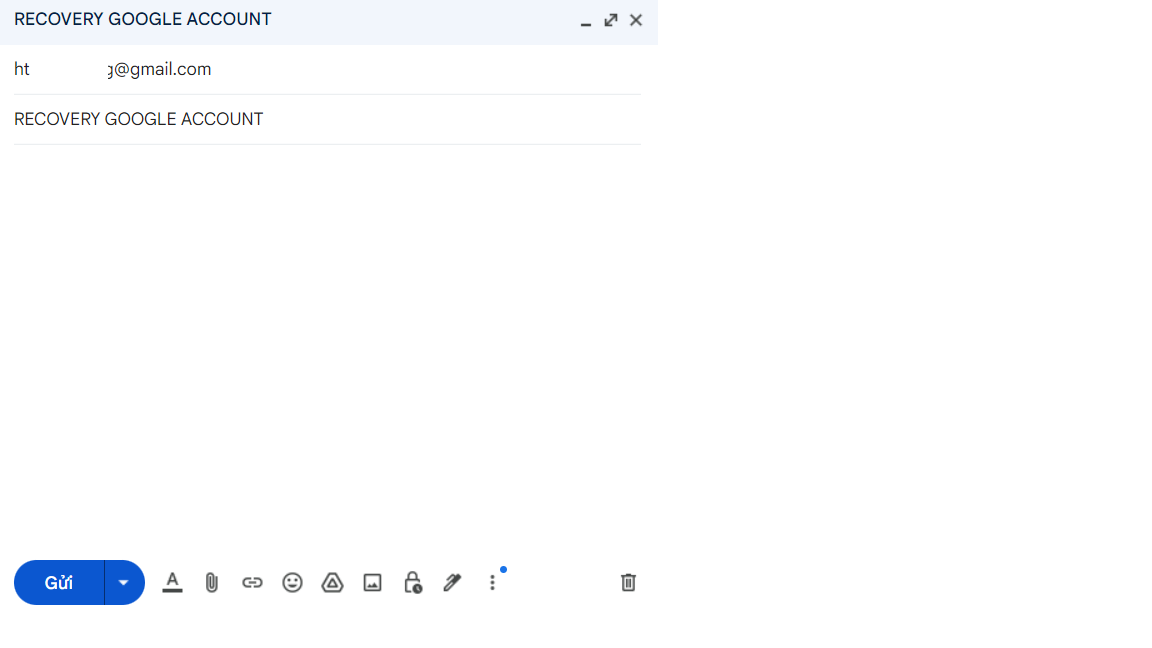
Chọn trang web có sẵn trong công cụ, ở đây là google :



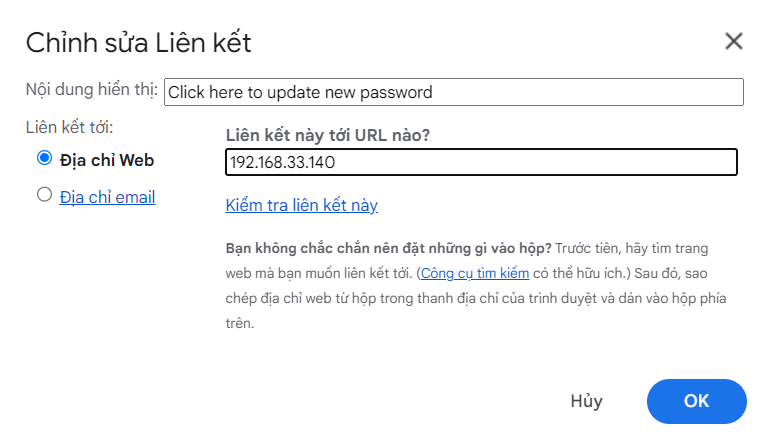
Thông báo thành công :



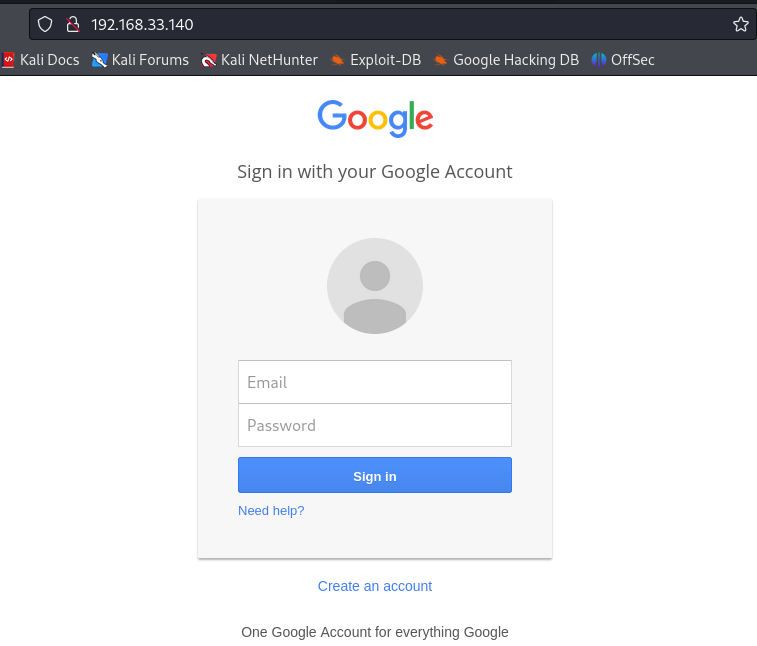
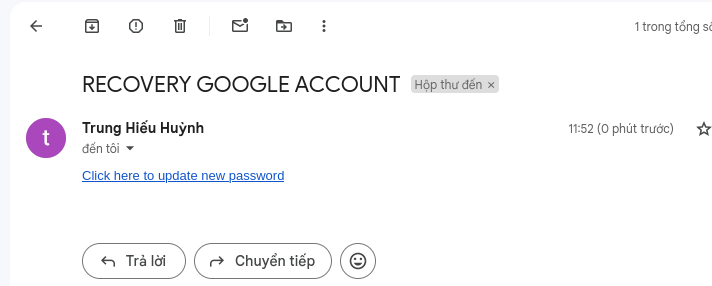
Ở trình duyệt, vào gmail gửi một fake mail đến cho victim với nội dung cập nhật mật khẩu người dung:



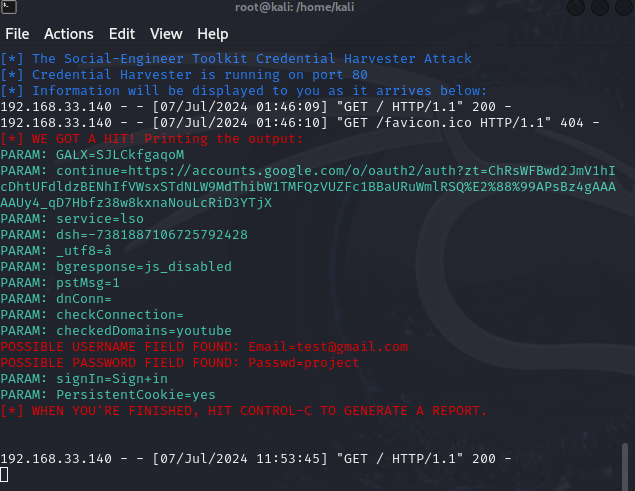
Chèn một liên kết với nội dung “ Click here to update new password”. Gõ ip máy của hacker vào đường liên kết URL:



Sau khi victim ấn vào link liên kết sẽ dẫn đến trang web giả mạo goole của hacker :



Sau khi victim điền user và passoword vào rồi. Thì máy hacker sẽ hiện lên thông báo :



Ở đây ta thấy Email: [test@gmail.com](mailto:test@gmail.com) và password là : project

**IV. Phân tích kết quả :**

Phân tích lỗ hổng:

1. **Lỗ hổng CVE-2021-44228 (Log4Shell):**

* **Phát hiện:** Dịch vụ web sử dụng Log4j phiên bản dễ bị tấn công.
* **Khai thác:** Thành công thực thi mã từ xa trên máy chủ web. Tạo truy cập trái phép vào hệ thống.

**Tấn Công Lừa Đảo (Phishing Mail):**

* **Phát hiện:** Một số lượng lớn email lừa đảo đã được mở và liên kết đã được nhấp vào bởi nhân viên.
* **Tác động:** Đánh cắp thông tin đăng nhập của nhiều nhân viên, dẫn đến nguy cơ truy cập trái phép vào hệ thống.

V. Khuyến Nghị:

**1. Biện Pháp Khắc Phục**

* **Lỗ hổng CVE-2021-44228 (Log4Shell):**
  + Nâng cấp Log4j lên phiên bản mới nhất không còn lỗ hổng.
  + Cấu hình tường lửa để chặn các yêu cầu đáng ngờ.
* **Tấn Công Lừa Đảo (Phishing Mail):**
  + Đào tạo nhân viên về nhận diện email lừa đảo.
  + Triển khai các biện pháp bảo mật email như SPF, DKIM, và DMARC.
  + Sử dụng các công cụ phát hiện và ngăn chặn tấn công lừa đảo.

**2. Đào Tạo và Nâng Cao Nhận Thức**

* Tổ chức các khóa đào tạo định kỳ về an ninh mạng cho nhân viên.
* Thường xuyên cập nhật thông tin về các mối đe dọa bảo mật mới và các biện pháp phòng ngừa.

### VI. Kết Luận

Cuộc kiểm thử xâm nhập đã phát hiện nhiều lỗ hổng bảo mật nghiêm trọng trong hệ thống của Công ty HASS, đặc biệt là lỗ hổng CVE-2021-44228 (Log4Shell) và các email lừa đảo (Phishing Mail). Việc khắc phục các lỗ hổng này và nâng cao nhận thức về an ninh mạng là vô cùng cần thiết để bảo vệ hệ thống và dữ liệu của công ty. Chúng tôi khuyến nghị Công ty HASS thực hiện các biện pháp khắc phục và duy trì kiểm tra an ninh mạng định kỳ để đảm bảo an toàn tối đa.

Đồng thực hiện :

Mr Thai Long

Mr Quang Vinh

Mr Trung Hieu

Chuyên viên it