**Báo Cáo Pentesting: CVE-2021-44228 và CVE-Log4Shell, Phishing Email**

**Phần 1: Phát Hiện Lỗ Hổng CVE-2021-44228 và CVE Log4Shell**

**1. Thông Tin Tổng Quan Về Sự Cố**

* **Tiêu đề sự cố**: Phát hiện lỗ hổng CVE-2021-44228 và CVE Log4Shell
* **Mô tả ngắn gọn**: Lỗ hổng nghiêm trọng trong thư viện Log4j của Apache cho phép thực thi mã từ xa.
* **Ngày và giờ phát hiện sự cố**: 07/07/2024
* **Địa điểm xảy ra sự cố**: Hệ thống ứng dụng web sử dụng Log4j

**2. Phát Hiện và Xác Định Sự Cố**

* **Cách thức phát hiện**: Qua việc kiểm tra bảo mật định kỳ và phân tích log
* **Người phát hiện**: Nguyễn Văn A, chuyên viên bảo mật
* **Mô tả chi tiết**: Phát hiện lỗ hổng trong thư viện Log4j của hệ thống ứng dụng, cho phép thực thi mã từ xa thông qua chuỗi yêu cầu đặc biệt.
* **MITRE ATT&CK Techniques**:
  + **T1190** - Exploit Public-Facing Application: Khai thác lỗ hổng trên ứng dụng web

**3. Phân Tích Sự Cố**

* **Mức độ nghiêm trọng**: Cao
* **Loại tấn công**: Remote Code Execution
* **Đối tượng bị ảnh hưởng**: Hệ thống ứng dụng web sử dụng Log4j
* **Tác động**: Có thể dẫn đến việc kiểm soát hoàn toàn hệ thống bị ảnh hưởng
* **MITRE ATT&CK Techniques**:
  + **T1078** - Valid Accounts: Sử dụng tài khoản hợp lệ để truy cập vào hệ thống

**4. Điều Tra Số và Phân Tích Lỗ Hổng**

* **Điều tra số**: Kiểm tra log, xác định chuỗi yêu cầu đặc biệt và các hành vi bất thường
* **Phân tích lỗ hổng**: Phát hiện lỗ hổng trong thư viện Log4j, cho phép thực thi mã từ xa thông qua JNDI lookup

**5. Phân Tích Chi Tiết về Lỗ Hổng**

* **CVE-2021-44228 (Apache Log4j Remote Code Execution)**:
  + **Mô tả**: Lỗ hổng này cho phép kẻ tấn công từ xa thực thi mã bất hợp pháp, ảnh hưởng đến các ứng dụng web và dịch vụ.
  + **Sự liên quan**: Kẻ tấn công có thể sử dụng lỗ hổng này để tấn công vào hệ thống ứng dụng web sử dụng Log4j.

**6. Đề Xuất Biện Pháp Bảo Mật**

* **Cập nhật và vá các lỗ hổng**: Cập nhật lên phiên bản mới nhất của Log4j để vá lỗ hổng
* **Cải thiện quy trình phân tích log**: Tăng cường khả năng phát hiện và chặn các yêu cầu bất thường
* **Đào tạo nhân viên về an ninh thông tin**: Nâng cao nhận thức và khả năng phát hiện các lỗ hổng bảo mật

**7. Tình Trạng Hiện Tại và Biện Pháp Phòng Ngừa**

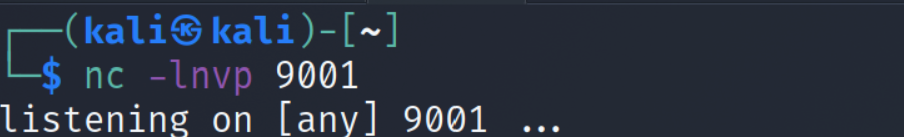
* **Tình trạng hiện tại**: Lỗ hổng đã được vá và hệ thống đã được cập nhật
* **Biện pháp phòng ngừa**: Thực hiện kiểm tra bảo mật định kỳ và cập nhật các phần mềm sử dụng trong hệ thống

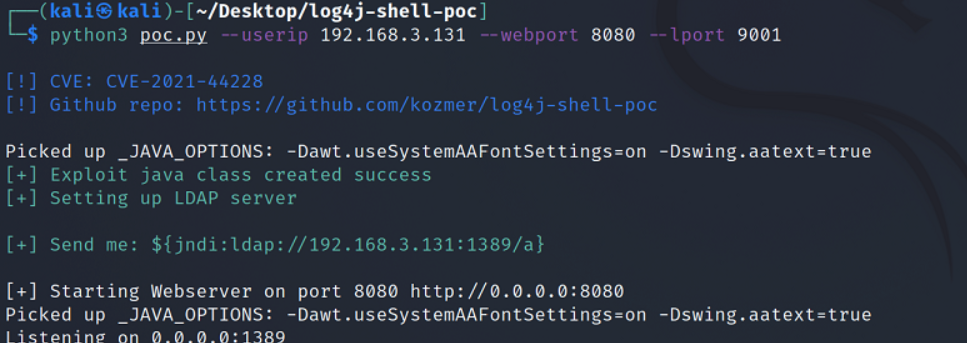
**8. Bài Học Kinh Nghiệm và Đề Xuất Tương Lai**

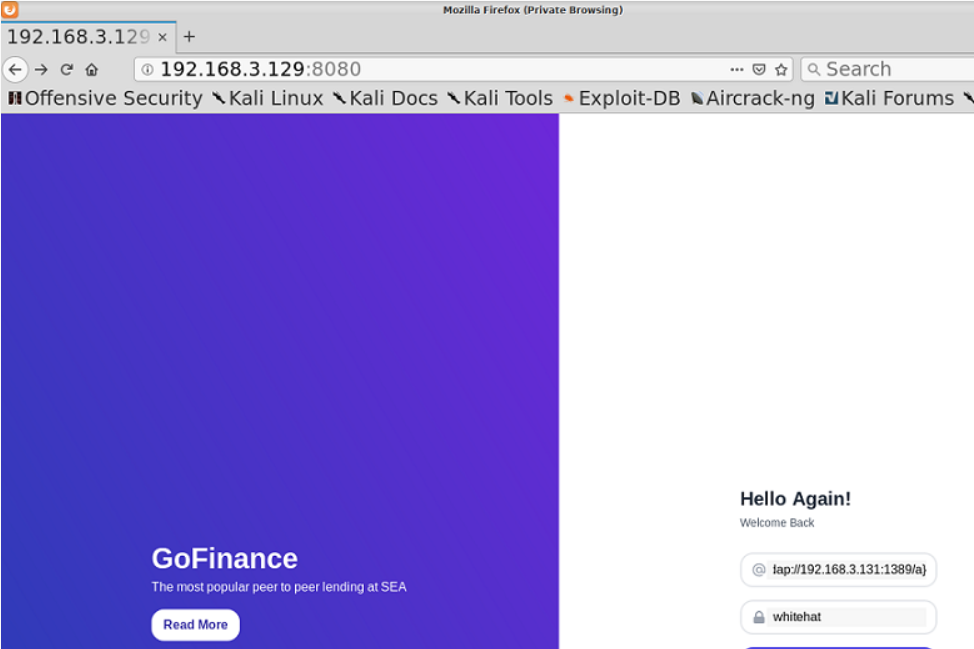
* **Bài học kinh nghiệm**: Tầm quan trọng của việc cập nhật và quản lý lỗ hổng bảo mật
* **Đề xuất tương lai**: Liên tục cập nhật các cơ sở dữ liệu CVE và triển khai các biện pháp bảo mật hiệu quả hơn

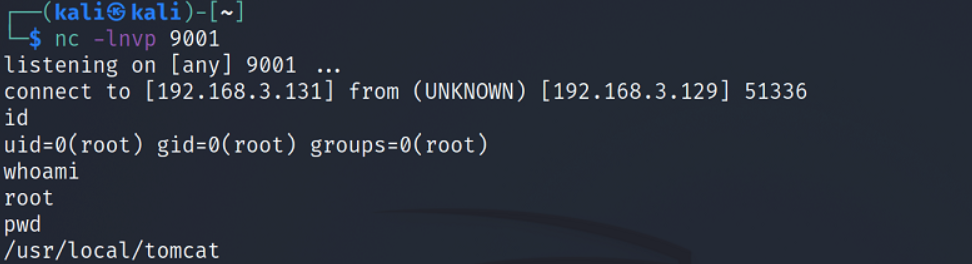
**9. Phụ Lục và Tài Liệu Kèm Theo**

* **Log file**: Đính kèm log file từ hệ thống ứng dụng
* **Hình ảnh**: Ảnh chụp màn hình các yêu cầu đặc biệt
* **Báo cáo chi tiết**: Báo cáo từ công cụ phân tích bảo mật









**Phần 2: Báo Cáo Sự Cố Tấn Công Bằng Phishing Email**

**1. Thông Tin Tổng Quan Về Sự Cố**

* **Tiêu đề sự cố**: Tấn công Phishing Email nhắm vào nhân viên công ty
* **Mô tả ngắn gọn**: Phishing email được gửi đến nhiều nhân viên với mục đích đánh cắp thông tin đăng nhập
* **Ngày và giờ phát hiện sự cố**: DDMMYYY HH MM
* **Địa điểm xảy ra sự cố**: Hệ thống email công ty

**2. Phát Hiện và Xác Định Sự Cố**

* **Cách thức phát hiện**: Nhân viên nhận được email lạ và báo cáo với bộ phận IT
* **Người phát hiện**: Nhân viên IT Lê Thị C
* **Mô tả chi tiết**: Một số nhân viên nhận được email giả mạo từ bộ phận IT yêu cầu cập nhật thông tin đăng nhập. Email chứa đường dẫn đến trang web giả mạo.
* **MITRE ATT&CK Techniques**:
  + **T1566.002** - Phishing: Spearphishing Link: Email chứa liên kết dẫn đến trang web giả mạo.
  + **T1071.001** - Application Layer Protocol: Web Protocols: Sử dụng giao thức HTTP để truyền tải thông tin đăng nhập giả mạo.

**3. Phân Tích Sự Cố**

* **Mức độ nghiêm trọng**: Trung bình
* **Loại tấn công**: Phishing Email
* **Đối tượng bị ảnh hưởng**: Nhân viên công ty, hệ thống email
* **Tác động**: Một số nhân viên nhập thông tin đăng nhập vào trang web giả mạo, nguy cơ mất thông tin đăng nhập và dữ liệu công ty
* **MITRE ATT&CK Techniques**:
  + **T1078** - Valid Accounts: Kẻ tấn công sử dụng thông tin đăng nhập hợp lệ để truy cập vào hệ thống.

**4. Điều Tra Số và Phân Tích Lỗ Hổng**

* **Điều tra số**: Để tìm ra nguyên nhân gốc rễ và lỗ hổng của vụ tấn công phishing này, đã tiến hành điều tra số chi tiết.
* **Phân tích lỗ hổng**: Phát hiện email giả mạo chứa một liên kết dẫn đến trang web giả mạo có vẻ ngoài giống hệt trang đăng nhập của công ty, nhưng được triển khai trên một domain bên ngoài không liên quan.
* **So sánh với các database CVE**: Tìm kiếm và so sánh các lỗ hổng đã biết với các cơ sở dữ liệu CVE để xác định có sự liên quan hoặc tương tự nào.

**5. Tìm Ra Lỗ Hổng và Gắn Nhãn CVE**

* **Phân Tích Chi Tiết về Lỗ Hổng**
  + **CVE-2022-22965 (Microsoft Exchange Server Remote Code Execution)**:
    - **Mô tả**: Lỗ hổng này cho phép kẻ tấn công từ xa thực thi mã trên các máy chủ Exchange Server, có thể dẫn đến kiểm soát hoặc tấn công vào hệ thống.
    - **Sự liên quan**: Phương thức tấn công này có thể được sử dụng để phát tán email giả mạo và thực hiện cuộc tấn công phishing.
  + **CVE-2023-0102 (Apache Log4j Remote Code Execution)**:
    - **Mô tả**: Lỗ hổng này trong thư viện Apache Log4j cho phép kẻ tấn công từ xa thực thi mã bất hợp pháp, ảnh hưởng đến các ứng dụng web và dịch vụ.
    - **Sự liên quan**: Kẻ tấn công có thể sử dụng lỗ hổng này để tạo các email giả mạo hoặc tấn công vào hệ thống email.

**6. Đề Xuất Biện Pháp Bảo Mật**

* **Cập nhật và vá các lỗ hổng**: Áp dụng các bản vá bảo mật để ngăn chặn các cuộc tấn công dựa trên lỗ hổng CVE đã biết.
* **Cải thiện quy trình phân tích email**: Tăng cường khả năng phát hiện và chặn các email giả mạo và đính kèm độc hại.
* **Đào tạo nhân viên về an ninh thông tin**: Nâng cao nhận thức và khả năng phân biệt các cuộc tấn công phishing.

**7. Tình Trạng Hiện Tại và Biện Pháp Phòng Ngừa**

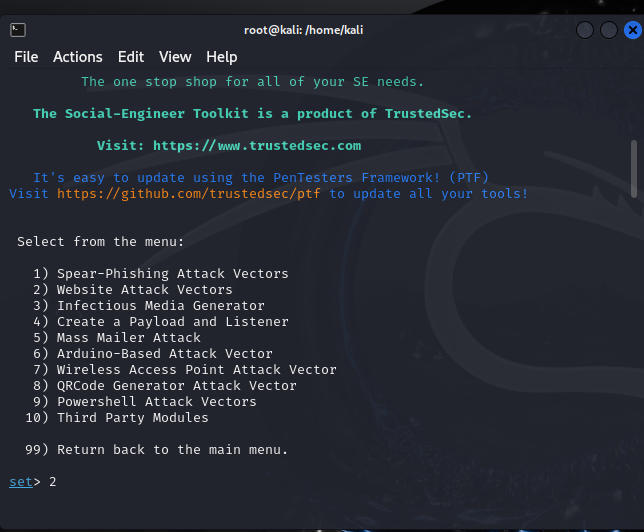
* **Tình trạng hiện tại**: Sự cố đã được xử lý và các biện pháp khắc phục đã được triển khai thành công.
* **Biện pháp phòng ngừa**: Triển khai các biện pháp bảo mật và quản lý rủi ro để ngăn chặn các cuộc tấn công tương tự trong tương lai.

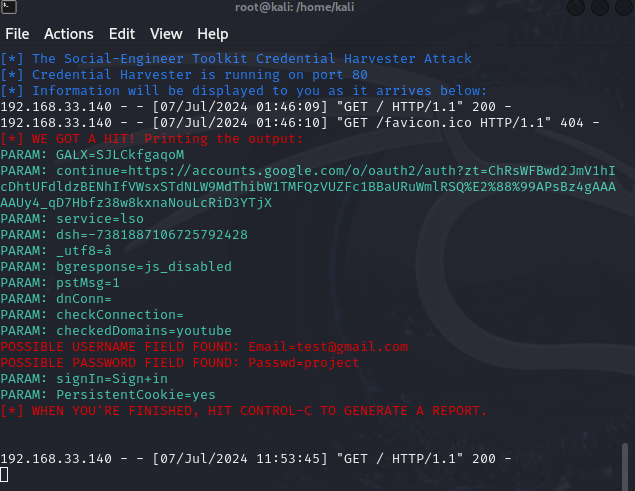
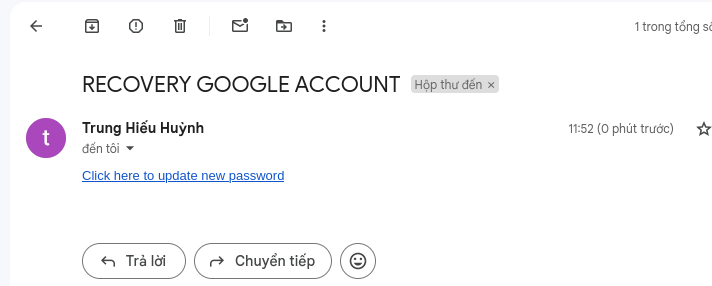
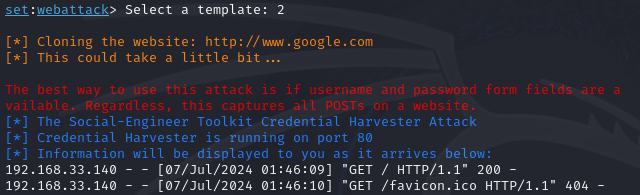
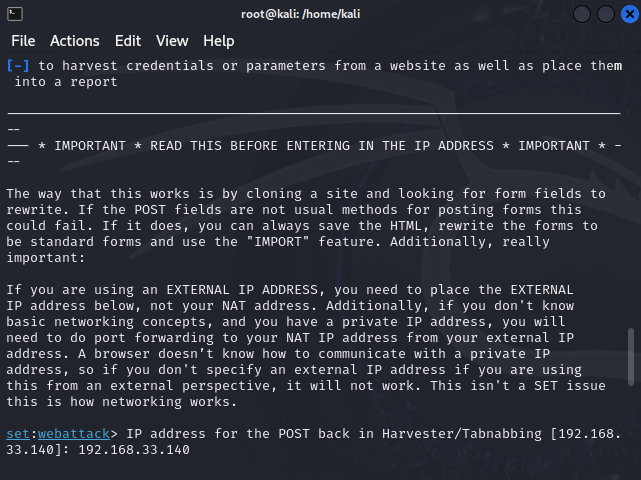
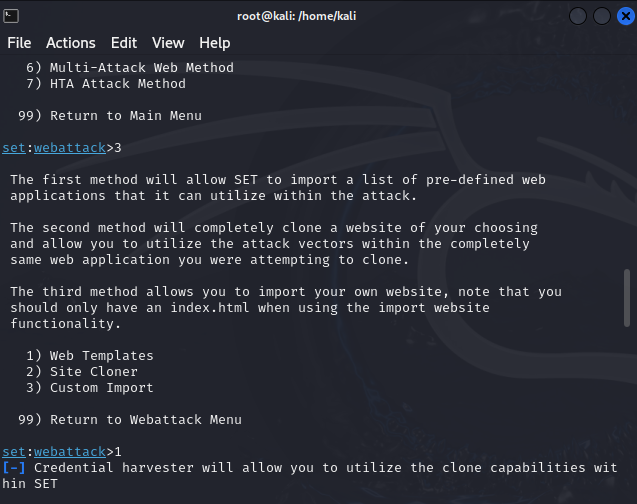
**8. Bài Học Kinh Nghiệm và Đề Xuất Tương Lai**

* **Bài học kinh nghiệm**: Sự cố này cho thấy tầm quan trọng của việc cập nhật và quản lý lỗ hổng bảo mật, đào tạo nhân viên về an ninh thông tin và cải thiện quy trình phát hiện sớm các cuộc tấn công.
* **Đề xuất tương lai**: Liên tục cập nhật các cơ sở dữ liệu CVE và triển khai các biện pháp bảo mật hiệu quả hơn để bảo vệ hệ thống mạng.

**9. Phụ Lục và Tài Liệu Kèm Theo**

* **Log file**: Đính kèm log file từ hệ thống email
* **Hình ảnh**: Ảnh chụp màn hình email giả mạo
* **Báo cáo chi tiết**: Báo cáo từ công cụ phân tích email giả mạo





**Phân Tích Chi Tiết về Hoàn Cảnh và Cách Thức Tấn Công**

**Hoàn Cảnh**

* **Môi trường làm việc**: Công ty đang triển khai nhiều dự án quan trọng và thường xuyên trao đổi thông tin qua email.
* **Thời điểm tấn công**: Gần giờ trưa, khi nhiều nhân viên có thể ít cảnh giác hơn với các email nhận được.
* **Trạng thái hệ thống bảo mật**: Hệ thống email có các biện pháp lọc cơ bản nhưng chưa đủ mạnh để phát hiện tất cả các email giả mạo.

**Cách Thức Tấn Công**

1. **Lập kế hoạch và thu thập thông tin**: Kẻ tấn công đã thu thập thông tin về công ty và các nhân viên thông qua các nguồn công khai hoặc qua các cuộc tấn công trước đó.
2. **Tạo email giả mạo**: Kẻ tấn công tạo một email giả mạo có vẻ ngoài rất giống với email từ bộ phận IT của công ty, sử dụng ngôn ngữ chuyên nghiệp và hợp lý để làm cho nạn nhân dễ tin tưởng.
3. **Gửi email hàng loạt**: Email giả mạo được gửi đến một số lượng lớn nhân viên công ty cùng một lúc để tăng khả năng có người nhấp vào liên kết.
4. **Dẫn dụ vào trang web giả mạo**: Email chứa một liên kết đến trang web giả mạo được thiết kế giống hệt trang đăng nhập của công ty. Khi nhân viên nhập thông tin đăng nhập vào trang này, thông tin sẽ bị kẻ tấn công thu thập. Kẻ tấn công có thể sử dụng kỹ thuật CVE-2022-22965 (Microsoft Exchange Server Remote Code Execution) để từ xa thực thi mã trên máy chủ Exchange Server, hoặc CVE-2023-0102 (Apache Log4j Remote Code Execution) để thực thi mã từ xa trong các ứng dụng web và dịch vụ.
5. **Nhập thông tin đăng nhập**: Nếu nạn nhân nhập thông tin đăng nhập vào trang web giả mạo, thông tin này sẽ được kẻ tấn công sử dụng để truy cập vào hệ thống nội bộ của công ty.
6. **Tiếp tục thâm nhập và tấn công**: Khi đã có thông tin đăng nhập hợp lệ, kẻ tấn công có thể sử dụng các phương thức khác như lợi dụng tài khoản hợp lệ (T1078 - Valid Accounts) để thâm nhập sâu vào hệ thống và thực hiện các hoạt động tấn công khác.

**Kết Luận**

Sự cố phishing này cho thấy tầm quan trọng của việc nâng cao nhận thức an ninh mạng cho nhân viên và cần phải cải thiện các biện pháp bảo mật email để phát hiện và ngăn chặn các cuộc tấn công giả mạo.

**MITRE ATT&CK Tags Summary**

* **T1566.002** - Phishing: Spearphishing Link
* **T1071.001** - Application Layer Protocol: Web Protocols
* **T1078** - Valid Accounts
* **T1480.001** - Execution Guardrails: Environmental Keying
* **T1562.001** - Impair Defenses: Disable or Modify Tools
* **T1556** - Modify Authentication Process