**Báo cáo tiến độ Đồ án chuyên ngành Mạng**

**Đề tài: Ứng dụng các công cụ của Security Onion nhằm phân tích và phát hiện một cuộc tấn công (Web, Database,…)**

1. **TÌM KIẾM TÀI LIỆU THAM KHẢO:**

* Dựa vào hướng dẫn của thầy em đã tìm được nhiều nguồn tài liệu tham khảo cả tiếng việt lẫn tiếng anh. Tuy nhiên đa phần các nguồn đều khá cũ, chỉ phù hợp với các phiên bản cài đặt và sử dụng từ những năm 2012 nên em tập trung tìm hiểu tài liệu từ trang chủ của Security Onion từ link sau:
* Link: <https://docs.securityonion.net/_/downloads/en/16.04/pdf/>
* Trang hướng dẫn tải và cài đặt như:
* Link: <https://docs.securityonion.net/en/16.04/vmware.html>
* Trang hướng dẫn tải cài đặt DVWA để làm mục tiêu tấn công trong mô hình:
* Link: <https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson1/index.html>
* Và một số nguồn tài liệu tham khảo khác sẽ được liệt kê chi tiết hơn trong báo cáo đồ án.

1. **TÌM HIỂU LÝ THUYẾT:**

* Tìm hiểu lý thuyết về hệ thống Security Onion: Là một hệ thống NIDS (Network intrusion detection system) giúp nhằm phân tích và phát hiện các mối nguy hại, các cuộc tấn công, xâm nhập trong mạng như: tấn công Web, Database,… hay đơn giản chỉ là thăm dò khai thác thông tin sử dụng các công cụ hỗ trợ như nmap của Kali linux.
* Tìm hiểu về các cụ được hỗ trợ trong Security Onion như:

+ Snort: Công cụ giúp phát hiện cuộc tấn công trong thời gian thực bằng cách chặn bắt và phân tích các gói tin trong môi trường mạng. Công cụ đi kèm bộ luật giúp dễ dàng trong việc phát hiện và phân loại các cuộc tấn công khác nhau. Tuy nhiên Snort không kèm giao diện nên ta cần phải có Sguil, Squert.

+ Bro: Công cụ hỗ trợ can thiệp vào luồng dữ liệu mạng và kiểm tra các gói tin truyền trên mạng.

+ Sguil: Công cụ hỗ trợ giao diện phân tích các cuộc tấn công phát hiện được từ Snort-Alert, tạo bảng thống kê theo thời gian.

+ Squert: Ứng dựng Web sẽ tổng hợp, thống kê, phân loại các cuộc tấn công từ dữ liệu của Snort thu thập được theo mô hình sơ đồ và theo thời gian.

* Tìm hiểu về lý thuyết các phương thức truyền gói tin trong mạng, các mối nguy hại, nguy cơ tấn công trong mạng.
* Tìm hiểu về một số hình thức tấn công để dùng cho quá trình demo như:

+ Thăm dò nạn nhân bằng công cụ nmap của Kali Linux

+ Tấn công Web như XSS, SQL injection, Command injection với nạn nhân sử dụng là Ứng dụng Web nhiều lỗ hổng (DVWA) được cài đặt trên Fedora

* Trên đây chỉ tổng hợp ngắn gọn về lý thuyết tìm hiểu được, các phần chi tiết hơn sẽ được trình bày trong báo cáo đồ án.

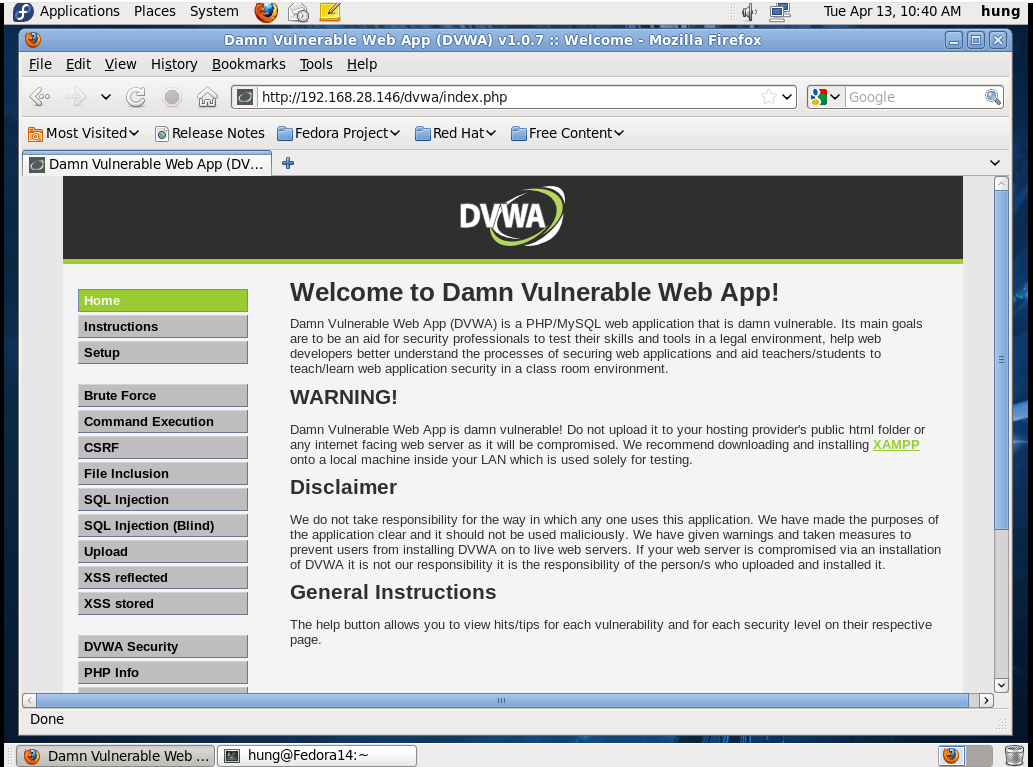
1. **CÀI ĐẶT MÔ HÌNH HỆ THỐNG DEMO:**

* Mô hình hệ thống demo hiện tại bao gồm các thành phần sau (được cài đặt trên VMWare Win10):

+ Security Onion: Đây là hệ thống mã nguồn mở Linux, cách thức tải và cài đặt cấu hình sẽ được ghitrong báo cáo.

*Hình 1: Giao diện hệ thống Security Onion sau khi cài đặt*

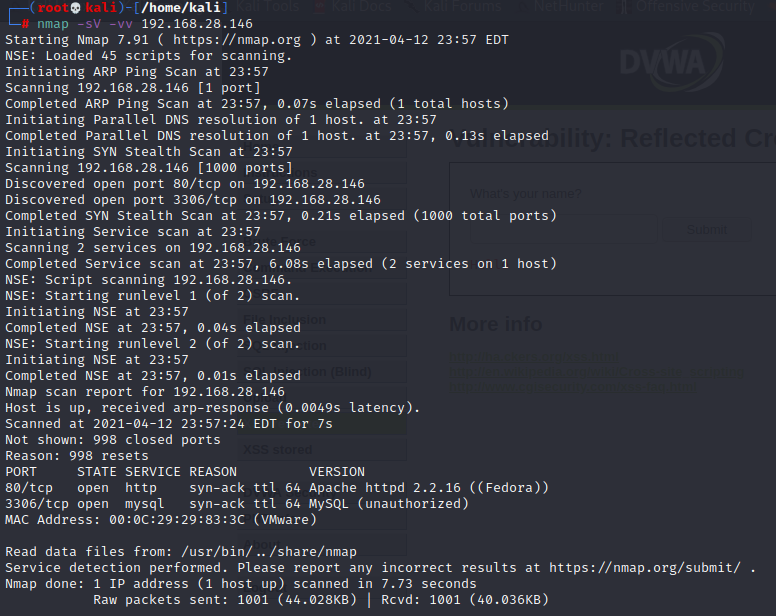
+ DVWA (nạn nhân): Đây là một ứng dụng Web chứa nhiều lỗ hổng bảo mật thích hợp cho việc nghiên cứu, thử nghiệm các cuộc tấn Web. Cách thức tải và cài đặt trên Fedora 14 sẽ được ghi trong báo cáo.



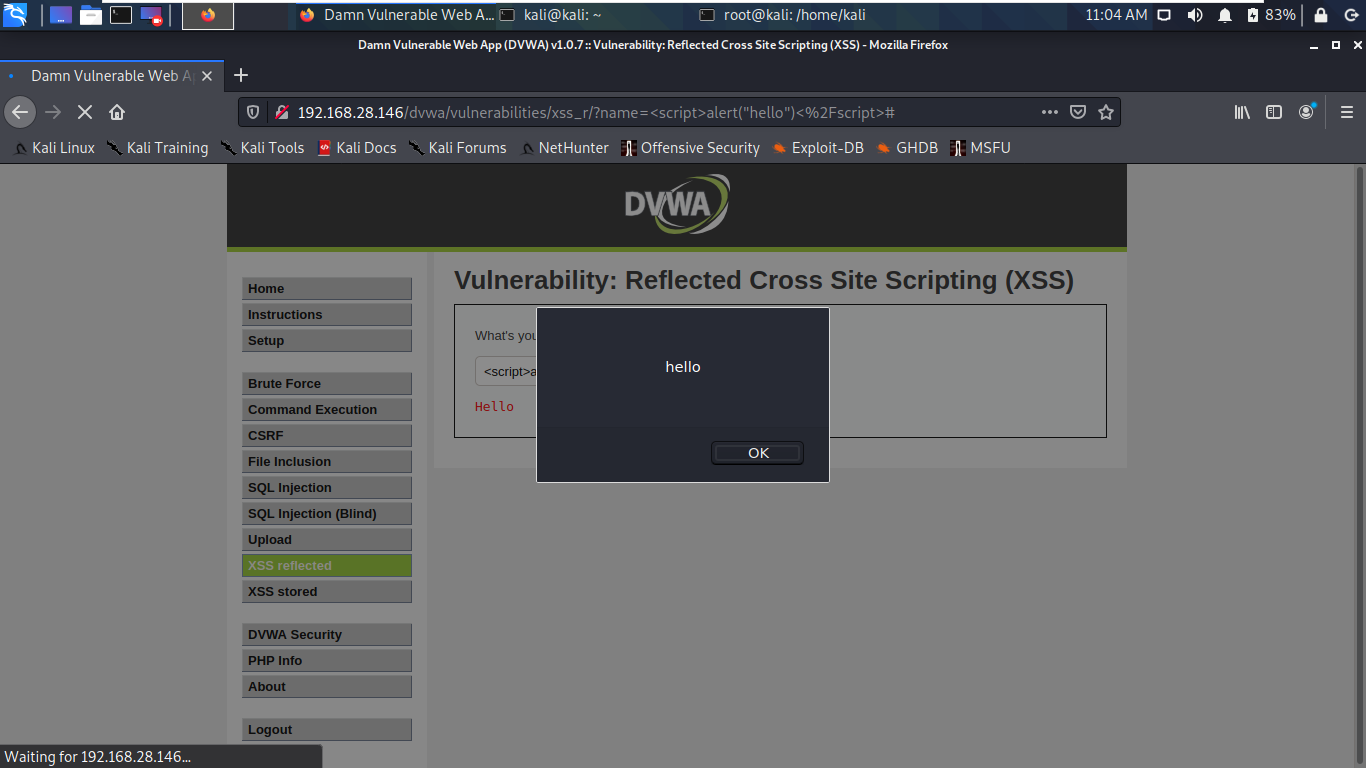
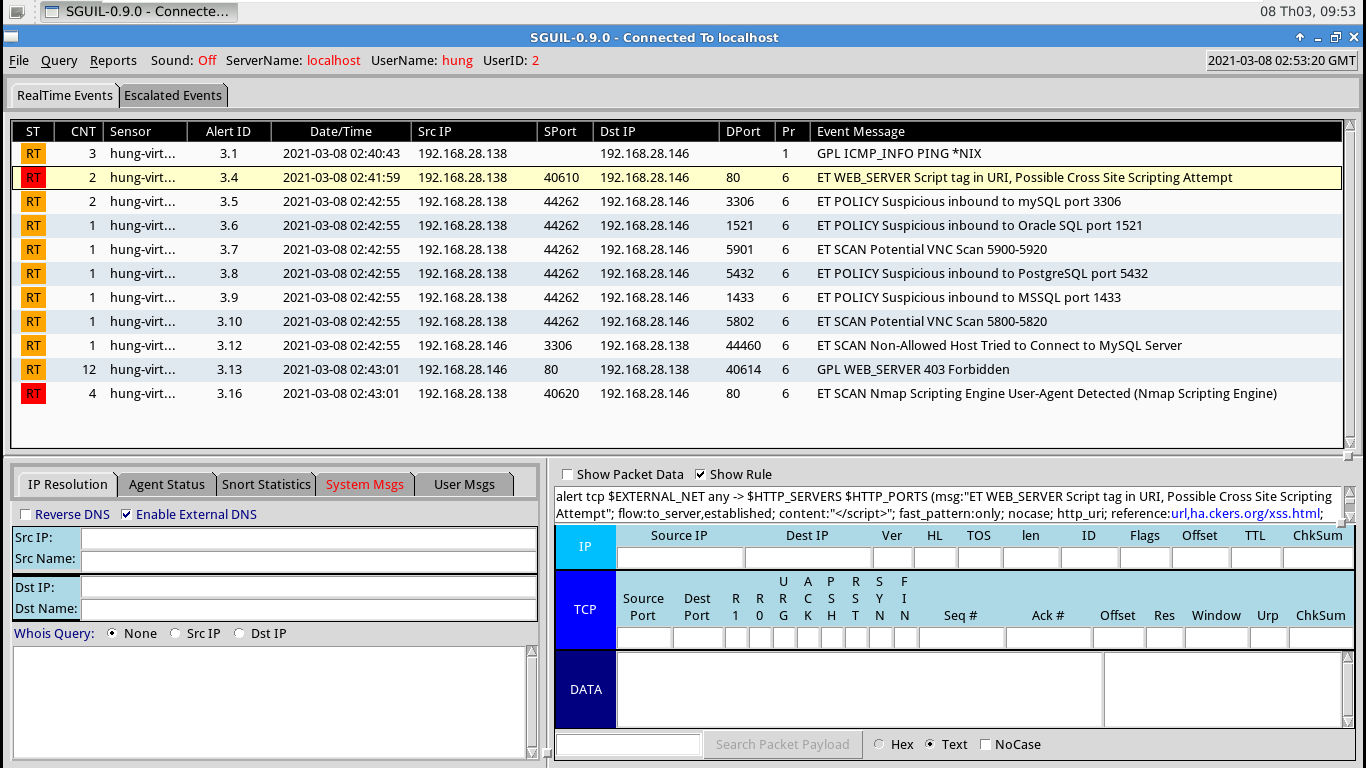
*Hình 2: Giao diện web DVWA sau khi cài đặt trên Fedora 14*

+ Kali Linux (kẻ tấn công): Hệ điều hành Linux chứa nhiều công cụ hữu ích dùng cho các hoạt động kiểm thử (pentest) hacking,… cách thức tải và cài đặt cấu hình sẽ được ghitrong báo cáo.

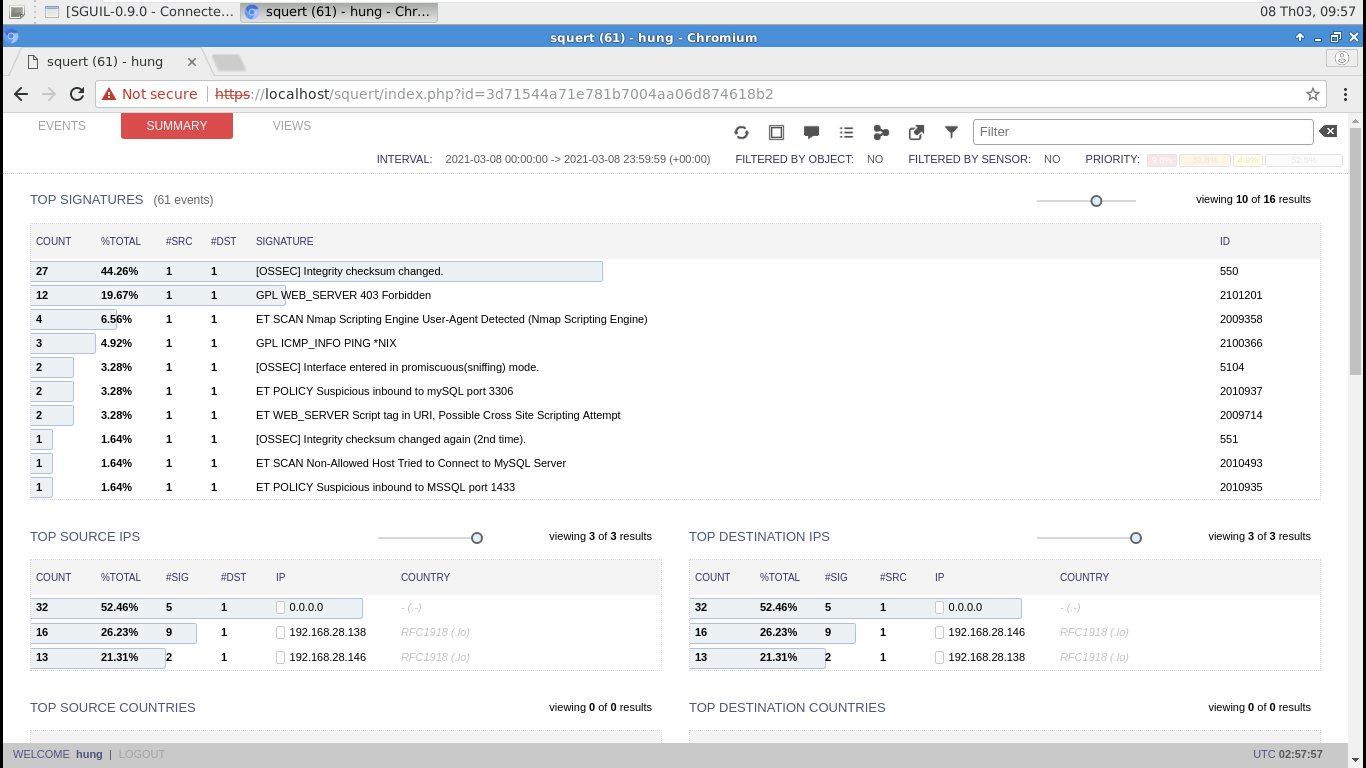
*Hình 3: Giao diện Kali Linux sau khi cài đặt*

* Từ đây ta sẽ dùng Kali Linux thăm dò nạn nhân bằng công cụ nmap sau đó tận dụng các lỗ hổng của DVWA để thực hiện 1 vài cuộc tấn công như XSS, Command injection,… Cách thức chi tiết thực hiện tấn công cũng như sơ đồ các máy trong mạng sẽ được đề cập trong báo cáo.

*Hình 4: Kali Linux thực hiện thăm dò nạn nhân bằng công cụ nmap*

*Hình 5: Kali Linux thực hiện tấn công XSS trên DVWA*

*Hình 6: Sguil sẽ liệt kê và phân loại các cuộc tấn công theo thời gian thực dựa vào dữ liệu mà cảm biến Snort thu thập được*

*Hình 7: Ứng dụng web Squert sẽ thống kê thông tin các cuộc tấn công theo tần suất*

1. **HƯỚNG HOÀN THIỆN, PHÁT TRIỂN:**

* Nghiên cứu để nắm rõ hơn về cách sử dụng các công cụ tích hợp sẵn trên Security Onion để phát khả năng của hệ thống. Nghiên cứu thêm về bộ luật của Snort từ đó có thể sửa đổi cũng như bổ sung luật để phù hợp nhu cầu sử dụng cũng như phát hiện thêm nhiều dạng tấn công khác nhau.
* Hiện tại mô hình tấn công thuộc loại lý tưởng: kẻ tấn công và nạn nhân đều thuộc cùng 1 mạng con. Vì vậy sẽ nghiên cứu thêm về mô hình từ đó triển khai thử máy nạn nhân và kẻ tấn công thuộc 2 mạng khác nhau (ví dụ kẻ tấn công thông qua môi trường internet). Nếu thành công có thể mở rộng mô hình sử dụng phần mềm GNS3 với router ảo của Cisco để định tuyến giữa các mạng.