**Install WireShark**

Trong terminal, sử dụng câu lệnh sau để cài đặt Wireshark – chương trình bắt gói mạng và phân tích gói tin, và tshark – trình CLI của Wireshark:

* **apt-get install wireshark**
* **apt-get install tshark**

A screenshot of a computer

Description automatically generated

Sau khi cài xong, sử dụng command sau để có thể mở Wireshark lên

* **wireshark**

A picture containing text, screenshot, software, computer icon

Description automatically generated

Chúng ta thử xem có capture được gói tin nào không. Thử vào bên trong **eth0** ta có thể thấy rằng có nhiều gói tin ICMP đang được bắt từ máy Kali chuyển sang máy Ubuntu. Vậy là chúng ta đã cài đặt thành công Wireshark

A screenshot of a computer

Description automatically generated

**Install InetSim**

Chúng ta sẽ bắt đầu cài Inetsim, một môi trường để chạy virus, cài đặt thông qua những command sau đây:

* apt-get install libnet-server-perl
* apt-get install libnet-dns-perl
* apt-get install libipc-shareable-perl
* apt-get install libdigest-sha-perl
* apt-get install libio-socket-ssl-perl
* apt-get install iptables-de

A screenshot of a computer program

Description automatically generated with medium confidence

Sau khi cài đặt các gói xong, ta sẽ tiếp tục cài một gói deb của Inetsim trên trang chủ của nhà phát hành. Tại đây: [www.inetsim.org/debian/binary/inetsim\_1.2.4-1\_all.deb](http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb)

Chúng ta sẽ sử dugnj câu lệnh sau đây để có thể download trực tiếp file về mà không càn phải thông qua một trình duyệt nào cả

* wget [www.inetsim.org/debian/binary/inetsim\_1.2.4-1\_all.deb](http://www.inetsim.org/debian/binary/inetsim_1.2.4-1_all.deb)

A screenshot of a computer

Description automatically generated

Vì đây là môt file .deb nên chúng ta sẽ sử dụng câu lệnh sau đây để cài đặt file deb:

* dpkg -i inetsim\_1.2.4-1\_all.deb

Sau khi cài đặt xong chúng ta thử dung câu lệnh sau để test xem đã cài đặt thành công inetsim chưa:

* inetsim –help

A screenshot of a computer program

Description automatically generated with medium confidence

Sau đó chúng ta sẽ tiến hành config file inetsim. Vào bên trong thư mục **/etc/inetsim/.** Sau đó bắt đầu chỉnh sửa phần bên trong file **inetsim.conf** bằng câu lệnh **nano hoặc vim**

A screenshot of a computer

Description automatically generated

Bên trong chúng ta sẽ tìm các thành phần sau và chỉnh lại

* service\_bind\_address your IP ADDRESS
* redirect\_enabled yes
* redirect\_exclude\_port tcp:22

A screenshot of a computer

Description automatically generated

A screenshot of a computer

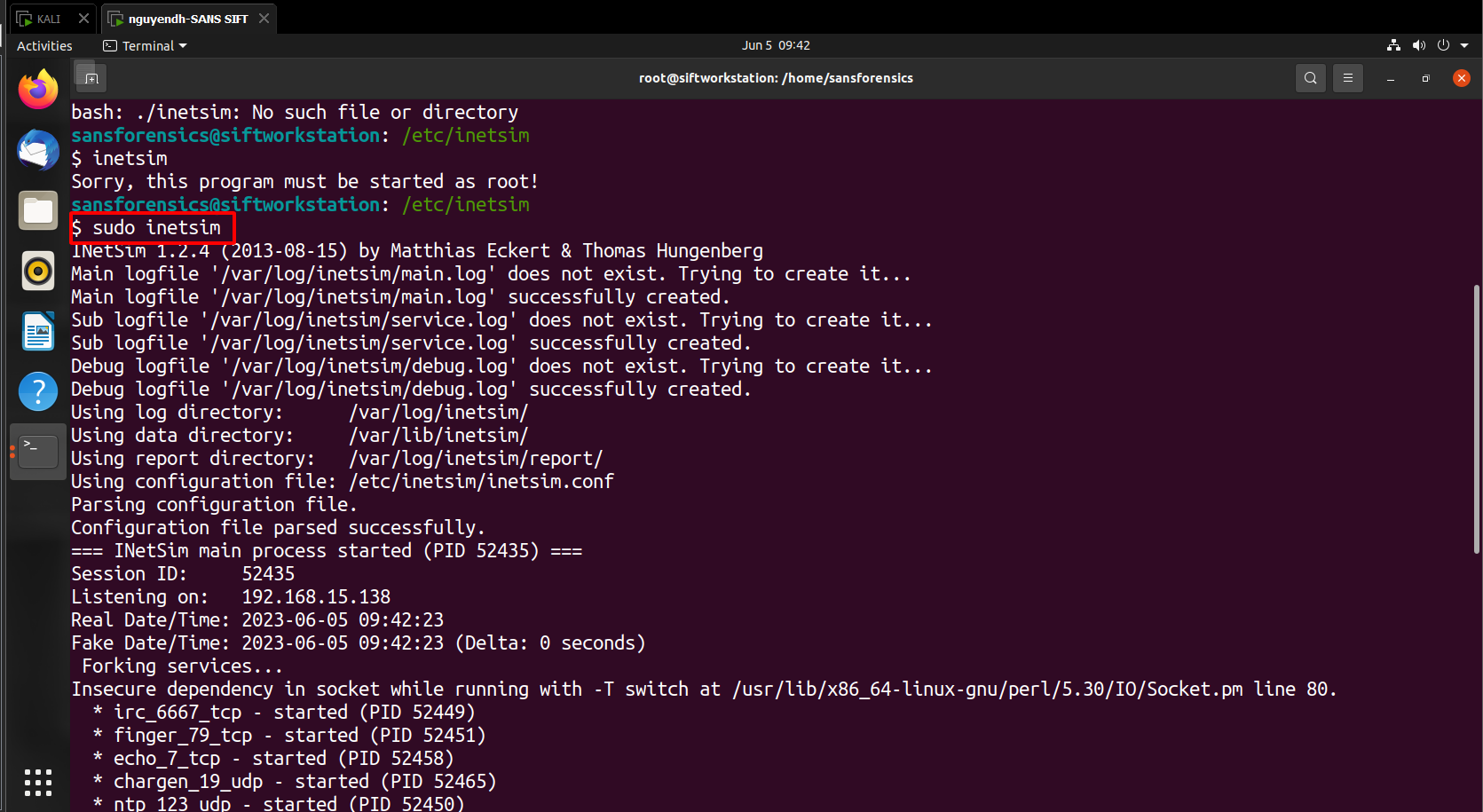
Description automatically generated

A screenshot of a computer

Description automatically generated

Sau đó lưu lại bằng tổ hợp Ctrl+X và test bằng câu lệnh sau:

* sudo inetsim



**Install Burp Suite**

Burp Suite là một công cụ kiểm thử bảo mật ứng dụng web, được sử dụng để phát hiện các lỗ hổng bảo mật trong ứng dụng web. Nó có chức năng quét và phân tích các yêu cầu HTTP và HTTPS, cung cấp khả năng tương tác với các trang web và cho phép người dùng xác định các lỗ hổng bảo mật như SQL injection, cross-site scripting (XSS), và các lỗ hổng khác. Burp Suite cũng cung cấp các tính năng khác như tự động hóa kiểm thử, proxy và interceptor cho phép người dùng can thiệp vào các yêu cầu và phản hồi của trang web.

Chúng ta sẽ bắt đầu cài burp suite với những package sau đây:

* sudo apt-get install openjdk-9-jdk
* <https://portswigger.net/burp/releases/download?product=free&version=1.7.26&type=linux>

Sau khi cài xong, chúng ta sẽ mở được burpsuit như hình dưới

A screenshot of a computer

Description automatically generated

**Install Deep Freeze**

Bây giờ chún ta sẽ bắt đầu cài đặt Deep Freeze