**Họ và Tên :** Nguyễn Tuấn Anh

**Mã sinh viên :** B17DCAT008

**Nhóm thực hành:** 2

**BÀI THỰC HÀNH MÔN AN TOÀN MẠNG NÂNG CAO Danh sách hình ảnh**

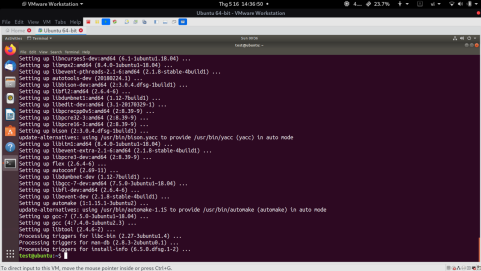
Hình 1. 1.Quá trình thực hiện lệnh autogen.sh trong thư mục honeyd................................................2 Hình 1. 2.Thực hiện chạy configure trong honeyd ..............................................................................3 Hình 1. 3.Quá trình chạy không có lỗi thiếu thư viện..........................................................................3 Hình 1. 4.Cài đặt honeyd .....................................................................................................................3 Hình 1. 5.Thông tin cấu hình ba máy ảo trong file config...................................................................3 Hình 1. 6.Kết quả mong muốn khởi chạy 3 máy ảo ............................................................................3 Hình 1. 7.Kết quả rò quét máy 1 với hệ điều hành phát hiện là windows như đã cấu hình.................3 Hình 1. 8.Kết quả thu từ quan sát từ máy chạy honeyd .......................................................................3

Hình 2. 1.Thực hiện tải mã nguồn mới nhất từ trang chủ của Snort....................................................3 Hình 2. 2.Tải mã nguồn của daq ..........................................................................................................3 Hình 2. 3.Thực hiện chạy lệnh cài đặt daq với make...........................................................................3 Hình 2. 4.Cài đặt hoàn tất snort ...........................................................................................................3 Hình 2. 5.Thực hiện chạy snort sau khi đã tạo và lưu file cấu hình.....................................................3 Hình 2. 6.Thực hiện ping và quan sát trên máy đã cài snort................................................................3 Hình 2. 7.Thực hiện quan sát file alert.................................................................................................3 Hình 2. 8.Thực hiện thay đổi cấu hình bổ xung rule cho snort............................................................3 Hình 2. 9.Thực hiện ping với giá trị gói 1000 với tham sô -s..............................................................3 Hình 2. 10.Kết quả cảnh báo thu được.................................................................................................3

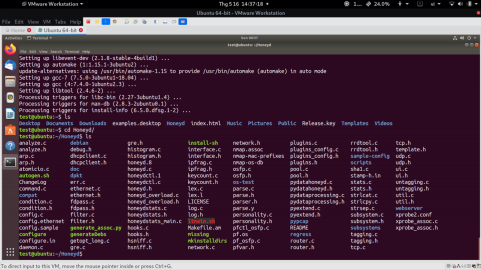
**I.Thực hành với Honeyd**

Sau khi clone mã nguồn của công cự từ github về, thực hiện quá trình cài đặt với các câu lệnh sau.

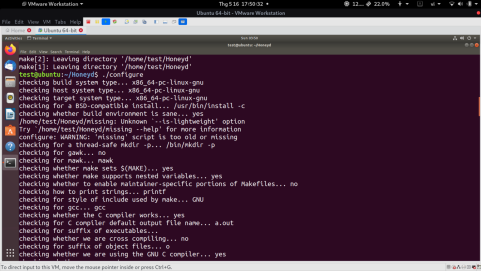
Chạy lệnh $ ./autogen.sh

**Hình 1. 1.Quá trình thực hiện lệnh autogen.sh trong thư mục honeyd**

Tiếp tục chạy lệnh ./confugure

**Hình 1. 2.Thực hiện chạy configure trong honeyd**

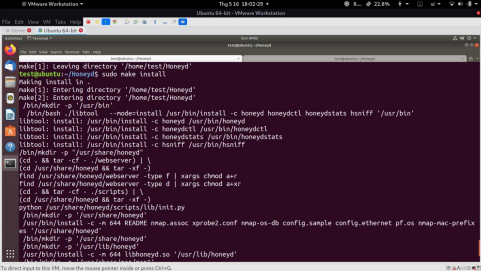
.

**Hình 1. 3.Quá trình chạy không có lỗi thiếu thư viện**

Thực hiện cài đặt sau khi đã kiểm tra các thư viện tiếp đó chạy lệnh

$ sudo make install

để cài đặt.

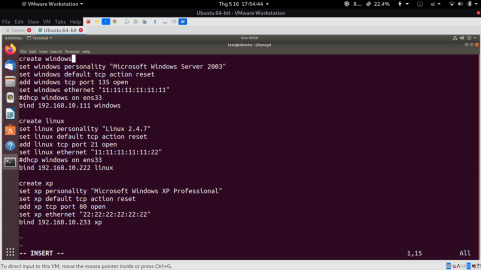
**Hình 1. 4.Cài đặt honeyd**

Tiến hành config cho file cấu hình của honeyd.

Sử dụng trình soạn thảo Vim để sửa file cấu hình.

$ vi honeyd.conf

.

**Hình 1. 5.Thông tin cấu hình ba máy ảo trong file config**

Thay đổi lại các thông tin về địa chỉ máy ảo cho phù hợp với mạng LAN

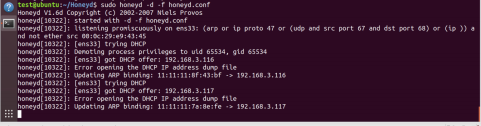
∙ Máy 1 : 192.168.3.101

∙ Máy 2 : 192.168.3.102

∙ Máy 3 : 192.168.3.103

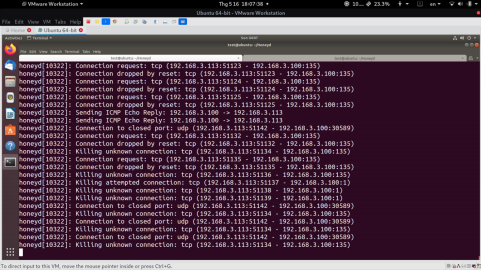
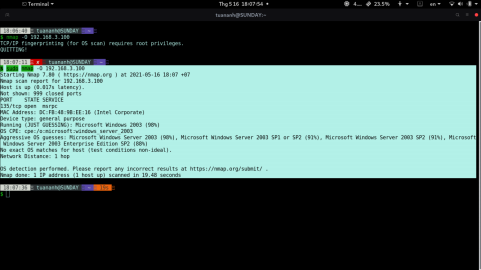
Khởi chạy honeyd bằng lệnh sau khi đã có lưu lại file cấu hình.

$ sudo honeyd -d -f honeyd.conf

**Hình 1. 6.Kết quả mong muốn khởi chạy 3 máy ảo**

.

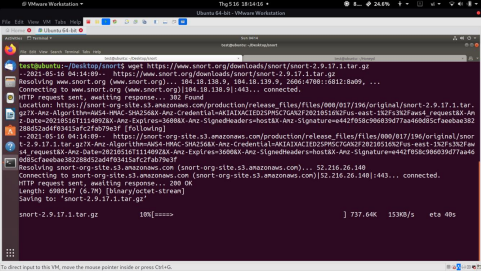
Kết quả trên máy Host đến máy ảo.

Thực hiện rò quét từ máy thật tới các máy ảo vừa tạo với honeyd. Sử dụng Nmap **Hình 1. 7.Kết quả rò quét máy 1 với hệ điều hành phát hiện là windows như đã cấu hình Hình 1. 8.Kết quả thu từ quan sát từ máy chạy honeyd**

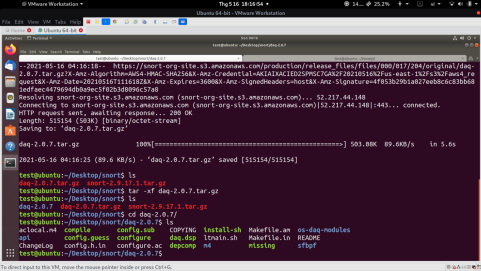
.

**II.Thực hành với Snort**

Thực hiện tải mã nguồn của snort

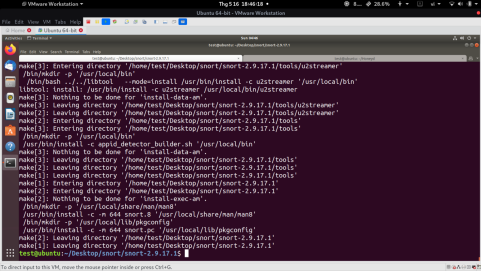
**Hình 2. 1.Thực hiện tải mã nguồn mới nhất từ trang chủ của Snort**

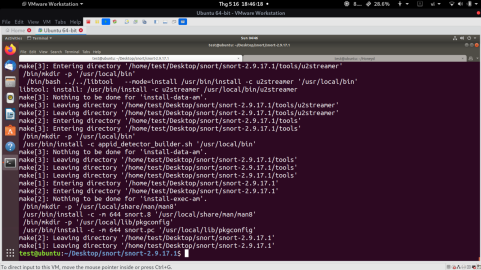
.

**Hình 2. 2.Tải mã nguồn của daq**

.

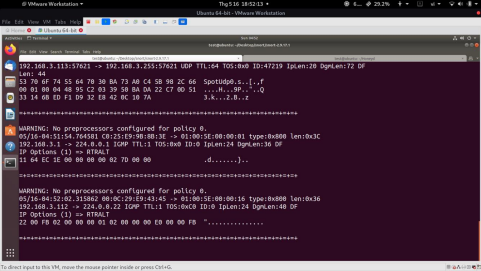
Thực hiện cài đặt daq và snort

**Hình 2. 3.Thực hiện chạy lệnh cài đặt daq với make**

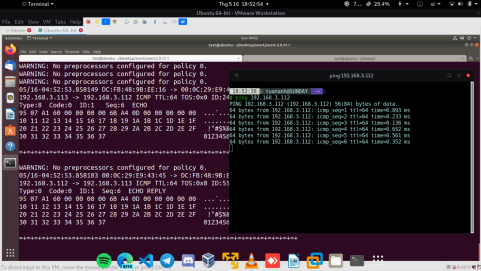
****

**Hình 2. 4.Cài đặt hoàn tất snort**

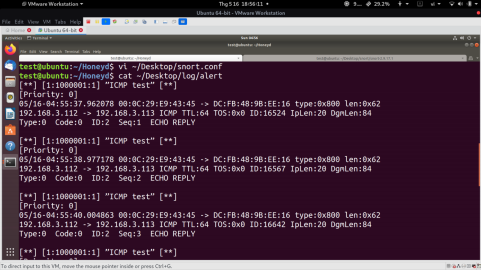
.

**Hình 2. 5.Thực hiện chạy snort sau khi đã tạo và lưu file cấu hình**

.

**Hình 2. 6.Thực hiện ping và quan sát trên máy đã cài snort**

.

**Hình 2. 7.Thực hiện quan sát file alert**

.

**Hình 2. 8.Thực hiện thay đổi cấu hình bổ xung rule cho snort**

.

**Hình 2. 9.Thực hiện ping với giá trị gói 1000 với tham sô -s**

.

**Hình 2. 10.Kết quả cảnh báo thu được**