5. QUÁ TRÌNH THỰC HIỆN

5.1. CẤU HÌNH MÁY PFSENSE 2.7.2

- CẤU HÌNH MÁY ẢO CHO PFSENSE

// Tùy chọn cho : RAM (2) và CPU (2)

// Tùy chọn cho NETWORK ADAPTER : NAT (192.168.230.140/24)

// Tùy chọn cho NETWORK ADAPTER 02 : VMNET2 (192.168.2.1/24)

- KIỂM TRA thiết lập cho WAN

// Chọn INTERFACE và chọn WAN

// WAN thì mình lấy DHCP từ VMWARE

// TẮT : “Block private networks and loopback addresses” và “Block bogon networks”

- THÊM RULE cho WAN

// FIREWALL, chọn RULES và chọn WAN

// Chọn ADD để thêm một rule mới

// Chọn PASS, chọn ANY (Protocol)

- Có thể kiểm tra bằng ping từ KALI đến IP WAN của pfsense (ping phải thành công)

- KIỂM TRA thiết lập cho LAN

// Có thể để mặc định cũng được

- CẤU HÌNH DNS Forwarders

// Chọn SERVICES, chọn DNS RESOLVER và tắt dịch vụ này

// Chọn SERVICES, chọn DNS FORWARDER và bật dịch vụ này

5.2. CÀI ĐẶT VÀ CẤU HÌNH SURICATA TRÊN PFSENSE 2.7.2

- CÀI ĐẶT dịch vụ suricata trên pfsense

// SYSTEM và chọn PACKAGE MANAGER

// Chọn AVAILABLE PACKAGES và nhập suricata (chọn INSTALL để cài đặt)

// Sau khi hoàn tất thì sẽ có mục suricata trong SERVICES

- CẤU HÌNH SURICATA cho WAN (interface)

// Chọn INTERFACE và chọn ADD

// Mục INTERFACE : chọn WAN

// Mục LOGGING : để mặc định

// Chọn mục EVE OUTPUT và tùy chọn

- CẤU HÌNH hardware checksum offloading

// Chọn SYSTEM, chọn ADVANCED và chọn NETWORKING

// Tích Hardware Checksum Offloading

// Chọn SAVE và pfsense sẽ khởi động lại

- CẤU HÌNH ETOPEN (dùng ruleset)

// Chọn GLOBAL SETTINGS và chọn ETOPEN (có thể chọn thêm SNORT)

// Chọn UPDATES và chọn update để cập nhập bộ rule của etopen

// Chọn vào INTERFACE và chọn EDIT

// Chọn WAN CATEGORIES và chọn SELECT ALL (chọn SAVE để áp dụng thiết lập)

// Chọn RESTART để khởi động lại INTERFACE (có thể đợi một lát)

- KIỂM TRA kết quả

// PING thử từ máy KALI vào IP WAN

// Phát hiện PING trong ALERTS (RULE 1:2100366)

// Chọn LOGS VIEW và xem eve.json

5.3. CÀI ĐẶT WAZUH BẰNG QUICKSTART

- KIỂM TRA MÁY ẢO

// LƯU Ý cấu hình máy ảo một tí

// RAM thì bạn để trên 8 GB

// CPU thì bạn tùy chỉnh (càng cao thì càng nhanh) (mình để 3 Cores)

// Ổ cứng ảo thì nên trên 100 GB

- CẤU HÌNH ip tĩnh cho máy wazuh

// # /etc/netplan/00-installer-config.yaml

// # tùy chỉnh theo mẫu

// # This is the network config written by 'subiquity'

// network:

// ethernets:

// ens33:

// dhcp4: false

// addresses: [192.168.230.100/24]

// routes:

// - to: default

// via: 192.168.230.1

// nameservers:

// addresses: [192.168.230.1]

// version: 2

// # áp dụng thiết lập : sudo netplan apply

// # kiểm tra ping thành công đến google.com

- CẤU HÌNH hostname

// # dùng lệnh hostnamectl : sudo hostnamectl set-hostname wazuh-server (tùy chọn tên nào cũng được)

- CẤU HÌNH sử dụng tài khoản root

// # gán hay tạo mật khẩu : sudo passwd

// # dùng root : su – (hay sudo root)

- KHỞI ĐỘNG lại máy ảo

// # dùng lệnh : sudo reboot

- CẬP NHẬP hệ thống bằng apt

// # dùng lệnh apt : sudo apt update && sudo apt full-upgrade (có thể thêm –y để bỏ qua xác nhận)

- LINK doc của wazuh cho quickstart : https://documentation.wazuh.com/current/quickstart.html

- CÀI ĐẶT wazuh bằng script

// # dùng lệnh : curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

LƯU Ý :

- Phải chạy script dưới root

- Kết thúc sẽ cấp pass cho tài khoản admin

- Truy cập dashboard và xem kết quả

5.4. CÀI ĐẶT WAZUH AGENT TRÊN PFSENSE 2.7.2

- DÙNG SSH cho pfsense 2.7.2

// Chọn SYSTEM và chọn ADVANCED

// Bật Enable Secure Shell và chọn SAVE

// Truy cập từ máy MANAGEMENT

- CÀI ĐẶT NANO để tùy chỉnh tập tin

// # cập nhập repo : pkg update

// # cài đặt nano : pkg install nano

- THIẾT LẬP FREEBSD để dùng cho repo

// # /usr/local/etc/pkg/repos/pfSense.conf

// nano /usr/local/etc/pkg/repos/pfSense.conf

// FreeBSD: { enabled: yes }

// # /usr/local/etc/pkg/repos/FreeBSD.conf

// nano /usr/local/etc/pkg/repos/FreeBSD.conf

// FreeBSD: { enabled: yes }

// # cập nhập lại : pkg update

- CÀI ĐẶT WAZUH AGENT cho pfsense

// # tìm kiếm gói wazuh-agent : pkg search wazuh (sẽ thấy các gói có liên quan đến từ khóa wazuh)

// # cài đặt bằng pkg : pkg install wazuh-agent-4.11.2

- CẤU HÌNH WAZUH-AGENT trên pfsense

// # copy file cấu hình sẵn vào wazuh : cp /etc/localtime /var/ossec/etc/

// # tùy chỉnh : /var/ossec/etc/ossec.conf

// cd /var/ossec/etc

// nano /var/ossec/etc/ossec.conf

// # thay IP bằng IP của WAZUH-SERVEr

// <address>192.168.230.100<address>

// # thay PROTOCOL bằng TCP

// <protocol>tcp</protocol>

- KHỞI CHẠY DỊCH VỤ wazuh-agent

// # bật tính năng autorun cho dịch vụ

// sysrc wazuh\_agent\_enable="YES"

// # tạo symbolick để chạy script

// ln -s /usr/local/etc/rc.d/wazuh-agent /usr/local/etc/rc.d/wazuh-agent.sh

// # khởi chạy dịch vụ

// service wazuh-agent start

- CẤU HÌNH GIÁM SÁT eve.json

// # tìm vị trí của tập tin eve.json

// truy cập logs view và chọn eve.json

// # tùy chỉnh : /var/ossec/etc/ossec.conf

// nano /var/ossec/etc/ossec.conf

// # thêm localfile cho eve.json

// <localfile>

// <log\_format>json</log\_format>

// <location>/var/log/suricata/suricata\_em039435/eve.json</location>

// </localfile>

// # khởi động lại dịch vụ wazuh-agent

// service wazuh-agent restart

5.5. KIỂM TRA KẾT QUẢ

- Trên máy KALI

// ping đến IP WAN của pfsense

// Kết quả sẽ ping thành công

A screenshot of a computer

AI-generated content may be incorrect.

- Trên máy PFSENSE

// Kiểm tra ALERTS của suricata sẽ có cảnh báo (cảnh báo cho việc ping)

// Xem cảnh báo trong eve.json trong LOG VIEWS (chọn eve.json) A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

- Trên WAZUH

// Xem các cảnh cáo trong ALERTS.LOG (/var/ossec/logs/alert.log)

// Kiểm tra THREAT HUNTING và EXPLORE trên WAZUH

A screenshot of a computer

AI-generated content may be incorrect.