

Bộ Giáo Dục Và Đào Tạo  
Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh  
**Khoa Công Nghệ Thông Tin**



**MÔN HỌC : BẢO MẬT NGƯỜI DÙNG CUỐI**

**ĐỀ TÀI: TRIỂN KHAI VÀ BẢO MẬT NGƯỜI DÙNG CUỐI**

**Giảng Viên Hướng Dẫn : ThS. Đỗ Phi Hưng**

**Thành Viên :**

1. Nguyễn Mỹ Hạnh – MSSV: 22DH110969
2. Huỳnh Huy Hoàng – MSSV: 22DH111127
3. Nguyễn Tuấn Hy – MSSV: 22DH111472

*Tp. Hồ Chí Minh, ngày .... tháng .... năm ...*

This image shows a full page of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page, providing a template for handwriting practice or general writing. There are no margins, text, or other markings on the page.

### **Lời cảm ơn**

Lời đầu tiên, chúng em xin gửi lời cảm ơn chân thành tới Trường Đại học Ngoại ngữ - Tin học Thành phố Hồ Chí Minh và sau là khoa Công nghệ Thông tin đã tạo điều kiện cho chúng em được tiếp cận với môn Bảo mật người dùng cuối và cũng như là đề tài Triển khai và bảo mật người dùng cuối. Đặc biệt nhóm em xin gửi lời cảm ơn sâu sắc tới Thầy Đỗ Phi Hưng là giảng viên hướng dẫn của nhóm em. Trong suốt thời gian qua Thầy đã dành nhiều thời gian và công sức để chỉ bảo, hỗ trợ và đánh giá nội dung của đề tài một cách khách quan và chính xác. Những ý kiến đóng góp của Thầy đã giúp nhóm em hoàn thiện hơn về sản phẩm của mình.

Nhóm em cũng xin gửi lời cảm ơn đến các bạn sinh viên khác đã giúp đỡ và chia sẻ kinh nghiệm trong quá trình làm việc nhóm để có thể ngày một hoàn thiện hơn.

Bài báo cáo đề tài môn Bảo mật người dùng cuối thực hiện trong khoảng thời gian 1 tháng. Vì lượng kiến thức của chúng em còn nhiều hạn chế nên không tránh khỏi những thiếu sót, chúng em rất mong nhận được những ý kiến đóng góp quý báu từ Thầy để tiếp thu kiến thức lĩnh vực này được hoàn chỉnh hơn, học hỏi thêm nhiều kinh nghiệm, đồng thời có điều kiện bổ sung, nâng cao trình độ để hành trang tốt hơn trong công việc sau này.

Cuối cùng, nhóm em xin được phép thay mặt các thành viên trong nhóm xin được gửi lời chúc sức khỏe và thành công đến với Thầy và các bạn sinh viên.

Trân trọng!

---

## Mục lục:

CHƯƠNG I. GIỚI THIỆU .....	6
1. Giới thiệu tổng quan: .....	6
2. Lý do chọn đề tài: .....	6
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT .....	7
1. Bảo mật người dùng cuối là gì: .....	7
2. Các mối đe dọa phổ biến đối với người dùng cuối: .....	7
a. Phishing (Lừa đảo qua email hoặc website giả mạo): .....	7
b. Malware (Phần mềm độc hại): .....	7
c. Keylogger / Spyware: .....	8
d. Social Engineering (Kỹ thuật lừa đảo tâm lý): .....	9
e. Khai thác điểm yếu phần mềm: .....	9
3. Các phương pháp bảo mật cơ bản cho người dùng cuối: .....	9
a. Bảo mật kỹ thuật: .....	9
b. Bảo mật hành vi – nhận thức người dùng: .....	9
c. Sử dụng các công cụ hỗ trợ: .....	10
4. Lợi ích của bảo mật người dùng cuối: .....	10
a. Bảo vệ thông tin cá nhân và tài sản số: .....	10
b. Ngăn chặn sự lây lan mã độc vào hệ thống tổ chức: .....	10
c. Tăng cường an ninh tổng thể cho tổ chức/doanh nghiệp: .....	10
d. Tuân thủ các quy định và tiêu chuẩn bảo mật: .....	10
e. Tăng năng suất làm việc và sự tin tưởng vào công nghệ: .....	10
f. Giảm thiểu chi phí khắc phục và rủi ro pháp lý: .....	11
g. Góp phần xây dựng văn hóa an toàn thông tin: .....	11
5. Nhược điểm của việc nếu không bảo mật người dùng cuối: .....	11
a. Phụ thuộc vào ý thức và hành vi người dùng: .....	11
b. Chi phí đầu tư ban đầu tương đối cao: .....	11
c. Dễ bị bỏ qua hoặc xem nhẹ: .....	11
d. Ảnh hưởng đến trải nghiệm người dùng: .....	11

---

e. Khó kiểm soát với thiết bị cá nhân (BYOD – Bring Your Own Device): .....	11
f. Không thể đảm bảo an toàn tuyệt đối: .....	12
6. Khái niệm về IDS/IPS: .....	12
7. Công cụ Snort là gì: .....	12
a. Tính năng chính của Snort: .....	12
b. Các chế độ hoạt động của Snort: .....	13
8. Khái niệm về quản lý người dùng cuối (System Endpoint Management): .....	13
9. Các chức năng chính của hệ thống quản lý endpoint: .....	13
10. Một số công cụ quản lý người dùng cuối phổ biến: .....	13
CHƯƠNG III: TRIỂN KHAI .....	14
1. Sơ đồ hệ thống mạng LAN: .....	14
2. Cài đặt các dịch vụ AD DS, DNS, DHCP trên Windows Server: .....	16
3. Thiết kết các rule IPS/IDS: .....	22
a. Cài đặt Pfsense: .....	22
b. Cài đặt Snort trên pfsense: .....	26
3. Các rule quản lý người dùng cuối: .....	29
4. Các case tấn công: .....	37
5. Kết luận: .....	44

---

## CHƯƠNG I. GIỚI THIỆU

### 1. Giới thiệu tổng quan:

- Trong thời đại số hóa hiện nay, người dùng cuối (end-users) trở thành mục tiêu phổ biến của các cuộc tấn công mạng như phishing, malware, ransomware, keylogger,... Bởi vì người dùng cuối thường là mắt xích yếu nhất trong hệ thống bảo mật, các hacker khai thác điểm yếu này để xâm nhập vào mạng nội bộ, đánh cắp dữ liệu, hoặc gây rủi ro an toàn thông tin.
- Bảo mật người dùng cuối (End-User Security) là tổng hợp các biện pháp kỹ thuật và hành vi nhằm đảm bảo rằng các cá nhân khi sử dụng thiết bị (máy tính, điện thoại, email, ứng dụng, mạng internet,...) không trở thành lỗ hổng an ninh. Nó bao gồm cả phần mềm, phần cứng và nhận thức người dùng.

### 2. Lý do chọn đề tài:

- Tính cấp thiết: Sự gia tăng các cuộc tấn công mạng như phishing, ransomware nhắm vào người dùng cá nhân và tổ chức cho thấy cần phải tăng cường biện pháp bảo vệ người dùng cuối.
- Yếu tố con người là mắt xích yếu: Dù hệ thống có mạnh đến đâu, nếu người dùng không có nhận thức bảo mật tốt (click link lạ, mở file đính kèm nguy hiểm,...), toàn bộ hệ thống vẫn bị xâm phạm.
- Phạm vi ảnh hưởng lớn: Không chỉ ảnh hưởng đến cá nhân, một người dùng bị tấn công có thể là cánh cổng để hacker xâm nhập vào cả doanh nghiệp.
- Ứng dụng thực tiễn cao: Kết quả nghiên cứu có thể áp dụng trực tiếp vào đào tạo nhân viên, học sinh – sinh viên, và tổ chức để nâng cao bảo mật.

### 3. Phạm vi đề tài:

- Đề tài tập trung vào các giải pháp bảo mật cho người dùng cuối, chủ yếu ở cấp độ cá nhân và doanh nghiệp nhỏ, với các nội dung:
    - + Các mối đe dọa phổ biến với người dùng cuối (malware, phishing, social engineering,...)
    - + Các biện pháp bảo mật kỹ thuật (phần mềm diệt virus, firewall cá nhân, cập nhật hệ thống,...)
    - + Biện pháp hành vi – nâng cao nhận thức người dùng (đào tạo, mô phỏng tấn công,...)
    - + Chính sách bảo mật dành cho người dùng cuối
    - + Một số công cụ hỗ trợ phổ biến (Antivirus, DLP, 2FA, EDR, VPN,...)
  - Không đi sâu vào mã hóa chuyên sâu, kiến trúc mạng lớn hoặc bảo mật hệ điều hành cấp thấp.
-

## CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

### 1. Bảo mật người dùng cuối là gì:

- Bảo mật người dùng cuối (End-User Security) là tập hợp các biện pháp kỹ thuật, chính sách và hoạt động nhằm bảo vệ người dùng cuối – tức là những người trực tiếp sử dụng thiết bị và hệ thống CNTT – khỏi các mối đe dọa về an toàn thông tin.
- Người dùng cuối thường là mắt xích cuối cùng trong chuỗi vận hành hệ thống, và cũng là mục tiêu dễ bị tấn công nhất, bởi vì:
  - + Thường thiếu kiến thức chuyên môn về bảo mật.
  - + Có thể bị thao túng bởi kỹ thuật lừa đảo tinh vi.
  - + Dễ bị khai thác qua email, phần mềm độc hại, thiết bị ngoại vi,...
- Mục tiêu của bảo mật người dùng cuối là giúp người dùng:
  - + Nhận thức được các nguy cơ an ninh.
  - + Có công cụ và kỹ năng phòng tránh các mối đe dọa.
  - + Không trở thành “cửa ngõ” để tin tặc xâm nhập vào tổ chức.

### 2. Các mối đe dọa phổ biến đối với người dùng cuối:

#### a. Phishing (Lừa đảo qua email hoặc website giả mạo):

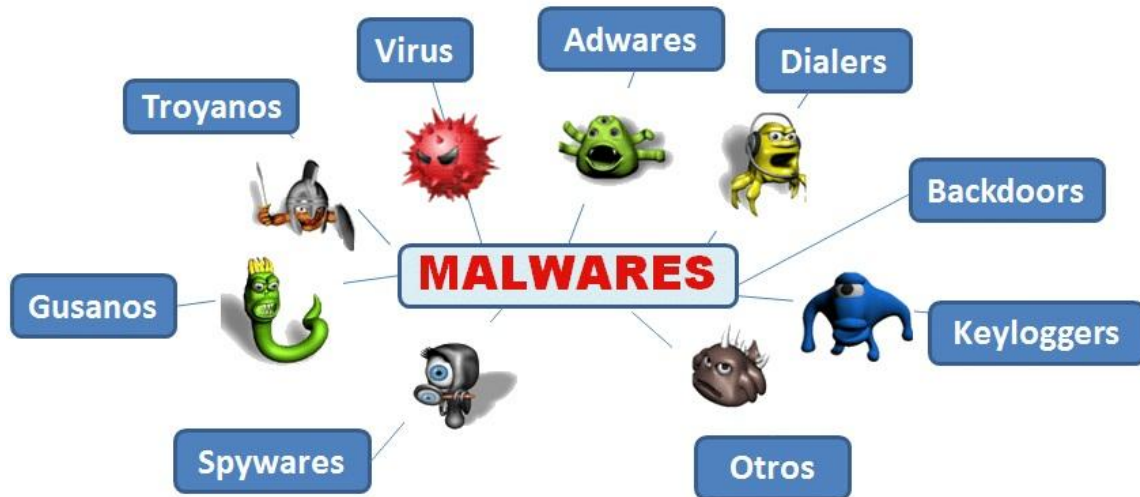
- Tin tặc giả danh ngân hàng, cơ quan chức năng, hoặc nội bộ công ty để dụ người dùng click vào đường link giả, từ đó đánh cắp thông tin đăng nhập, mã OTP hoặc tải xuống phần mềm độc hại.



Hình 1. Minh họa Phishing

#### b. Malware (Phần mềm độc hại):

- Bao gồm virus, trojan, ransomware, spyware,... có thể lây qua USB, tải phần mềm crack, hoặc file đính kèm trong email.
- **Ransomware** rất phổ biến: mã hóa toàn bộ dữ liệu người dùng và yêu cầu tiền chuộc.



Hình 2. Minh họa các Malware thường thấy

c. Keylogger / Spyware:

- Ghi lại mọi thao tác bàn phím, màn hình hoặc webcam để đánh cắp thông tin đăng nhập, thông tin cá nhân.



Hình 3. Minh họa Keylogger



d. Social Engineering (Kỹ thuật lừa đảo tâm lý):

- Hacker khai thác lòng tin, sự thiếu hiểu biết, hoặc sơ suất của người dùng để thuyết phục họ tự cung cấp mật khẩu, mã OTP, hoặc thực hiện hành vi nguy hiểm.



Hình 4. Social Engineering

e. Khai thác điểm yếu phần mềm:

- Tin tặc lợi dụng lỗ hổng trong hệ điều hành hoặc ứng dụng chưa cập nhật để tấn công thiết bị người dùng.

3. Các phương pháp bảo mật cơ bản cho người dùng cuối:

a. Bảo mật kỹ thuật:

Biện pháp	Mô tả
Phần mềm diệt virus	Cài phần mềm có bản quyền, cập nhật thường xuyên để phát hiện và ngăn chặn malware.
Tường lửa cá nhân (Firewall)	Kiểm soát lưu lượng ra/vào máy tính người dùng, ngăn truy cập trái phép.
Cập nhật hệ điều hành và phần mềm	Vá các lỗ hổng bảo mật để ngăn hacker khai thác.
Xác thực đa yếu tố (MFA / 2FA)	Thêm lớp bảo mật thứ hai khi đăng nhập, ví dụ: mã OTP, xác thực ứng dụng.
VPN	Mã hóa kết nối Internet khi làm việc từ xa, đảm bảo dữ liệu không bị nghe lén.

Bảng 1. Bảo mật kỹ thuật

b. Bảo mật hành vi – nhận thức người dùng:

Hành vi cần có	Mô tả
Không nhấp vào đường link/email lạ	Phân biệt email thật – giả, không click vào liên kết đáng ngờ.
Không sử dụng phần mềm không rõ nguồn gốc	Tránh tải phần mềm crack hoặc từ website không tin cậy.

Đặt mật khẩu mạnh và thay đổi định kỳ	Mật khẩu dài, gồm chữ hoa, thường, số, ký tự đặc biệt.
Khóa máy tính khi rời khỏi chỗ làm việc	Tránh để lộ thông tin nếu có người khác sử dụng thiết bị.
Tham gia tập huấn bảo mật	Nâng cao nhận thức qua các buổi đào tạo, mô phỏng tấn công phishing.

*Bảng 2. Bảo mật hành vi*

c. Sử dụng các công cụ hỗ trợ:

- EDR (Endpoint Detection & Response): Giám sát hành vi máy tính người dùng, phát hiện và phản ứng khi có hành vi nghi ngờ.
- DLP (Data Loss Prevention): Ngăn dữ liệu quan trọng bị rò rỉ qua email, USB,...
- Password manager: Giúp lưu trữ và tạo mật khẩu mạnh, tránh việc dùng chung mật khẩu.

4. Lợi ích của bảo mật người dùng cuối:

a. Bảo vệ thông tin cá nhân và tài sản số:

- Ngăn chặn rò rỉ thông tin như: mật khẩu, số CMND/CCCD, tài khoản ngân hàng, dữ liệu sức khỏe...
- Giảm nguy cơ mất tài sản qua các vụ tấn công như phishing hoặc đánh cắp mã OTP.

=> Ví dụ thực tế: Một người dùng bị tấn công qua email giả mạo ngân hàng, tiết lộ mã OTP, dẫn đến mất tiền trong tài khoản.

b. Ngăn chặn sự lây lan mã độc vào hệ thống tổ chức:

- Nếu một người dùng bị lây nhiễm ransomware hoặc virus, mã độc có thể lan sang máy chủ, toàn bộ mạng nội bộ.
- Bảo mật người dùng cuối giúp cô lập và ngăn chặn lây lan từ sớm.

=> Lợi ích cho doanh nghiệp: Tránh tổn thất do hệ thống ngưng trệ, mất dữ liệu khách hàng hoặc phải trả tiền chuộc.

c. Tăng cường an ninh tổng thể cho tổ chức/doanh nghiệp:

- Một hệ thống chỉ mạnh nếu từng mắt xích đều an toàn. Người dùng cuối là lớp đầu tiên và cuối cùng tiếp xúc với dữ liệu.
- Khi mỗi người dùng có ý thức bảo mật, tổ chức tránh được rủi ro từ bên trong.
- Chi phí đầu tư cho đào tạo bảo mật nhỏ hơn rất nhiều so với chi phí khắc phục sau khi bị tấn công.

d. Tuân thủ các quy định và tiêu chuẩn bảo mật:

- Bảo mật người dùng giúp tổ chức tuân thủ các chuẩn mực như: ISO 27001, GDPR, HIPAA,...
- Tránh bị phạt vi phạm hoặc mất uy tín vì để lộ thông tin người dùng.

e. Tăng năng suất làm việc và sự tin tưởng vào công nghệ:

- Khi người dùng biết cách tự bảo vệ, họ sử dụng công nghệ tự tin và hiệu quả hơn.
- Giảm thời gian gián đoạn do sự cố bảo mật (bị khóa máy, mất dữ liệu...).

f. Giảm thiểu chi phí khắc phục và rủi ro pháp lý:

- Chi phí để xử lý hậu quả một cuộc tấn công (ransomware, đánh cắp dữ liệu) thường rất lớn.
- Có thể bao gồm: mất mát dữ liệu, ngừng vận hành, mất khách hàng, bị kiện hoặc bị phạt.

=> Phòng bệnh hơn chữa bệnh: Bảo vệ từ người dùng cuối là lớp phòng ngự đầu tiên, hiệu quả và tiết kiệm nhất.

g. Góp phần xây dựng văn hóa an toàn thông tin:

- Người dùng có ý thức bảo mật sẽ lan tỏa thói quen tốt đến đồng nghiệp, gia đình, cộng đồng.
- Góp phần xây dựng một môi trường số an toàn và văn minh.

5. Nhược điểm của việc nếu không bảo mật người dùng cuối:

a. Phụ thuộc vào ý thức và hành vi người dùng:

- Dù có triển khai phần mềm hay hệ thống bảo mật hiện đại, nếu người dùng thiếu nhận thức hoặc hành xử bất cẩn, thì nguy cơ bị tấn công vẫn cao.
- Một cú nhấp chuột vào đường link độc hại cũng có thể phá hỏng toàn bộ hệ thống bảo mật.

⇒ Ví dụ: Nhân viên văn phòng mở file Excel lạ chứa macro độc hại, gây mã hóa toàn bộ dữ liệu công ty.

b. Chi phí đầu tư ban đầu tương đối cao:

- Bao gồm:
  - + Chi phí phần mềm diệt virus, EDR, DLP, quản lý thiết bị,...
  - + Chi phí đào tạo nhận thức an toàn thông tin cho người dùng.
  - + Chi phí nhân sự giám sát, hỗ trợ kỹ thuật.

Với doanh nghiệp nhỏ hoặc tổ chức giáo dục, đây có thể là gánh nặng tài chính.

c. Dễ bị bỏ qua hoặc xem nhẹ:

- Nhiều người dùng nghĩ rằng "mình không có gì để mất" hoặc "chỉ hacker mới bị tấn công", dẫn đến thái độ chủ quan.
- Bảo mật thường bị coi là việc của bộ phận IT, không phải trách nhiệm cá nhân.

⇒ Kết quả: Người dùng không cập nhật phần mềm, dùng chung mật khẩu, hoặc chia sẻ thông tin dễ dãi.

d. Ảnh hưởng đến trải nghiệm người dùng:

- Các lớp bảo mật như xác thực đa yếu tố (MFA), mã hóa USB, hạn chế quyền truy cập,... đôi khi khiến người dùng cảm thấy phiền phức, rườm rà, khó sử dụng.
- Có thể gây phản tác dụng nếu người dùng tìm cách lách hoặc tắt các công cụ bảo mật.

e. Khó kiểm soát với thiết bị cá nhân (BYOD – Bring Your Own Device):

- Khi người dùng mang laptop cá nhân, điện thoại cá nhân vào hệ thống doanh nghiệp, sẽ khó kiểm soát phần mềm, cấu hình bảo mật, hoặc hành vi truy cập của thiết bị đó.
  - Nguy cơ cao về rò rỉ dữ liệu và tấn công từ thiết bị không được quản lý.
-

f. Không thể đảm bảo an toàn tuyệt đối:

- Bảo mật người dùng cuối chỉ là một phần trong tổng thể bảo mật hệ thống. Nếu không có firewall doanh nghiệp, giám sát mạng, sao lưu dữ liệu,... thì vẫn có lỗ hổng.
- Tin tặc liên tục thay đổi phương thức tấn công nên cần cập nhật bảo mật thường xuyên.

6. Khái niệm về IDS/IPS:

Thành phần	Viết tắt	Tên đầy đủ	Giải thích
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập	IDS giám sát lưu lượng mạng và/hoặc hoạt động hệ thống để phát hiện các hành vi khả nghi, nhưng không tự động ngăn chặn. Nó chỉ cảnh báo cho quản trị viên.
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập	IPS cũng phát hiện các hành vi tấn công giống IDS, nhưng nó chủ động ngăn chặn bằng cách chặn lưu lượng, reset kết nối, hoặc sửa đổi gói tin.

*Bảng 3. Bảng khái niệm về IDS/IPS*

So sánh nhanh giữa IDS và IPS:

Tiêu chí	IDS	IPS
Chức năng chính	Phát hiện	Phát hiện + Ngăn chặn
Phản ứng	Thụ động (cảnh báo)	Chủ động (chặn hoặc phản ứng)
Vị trí triển khai	Chế độ giám sát (promiscuous)	Chế độ inline (nằm giữa traffic)
Nguy cơ ảnh hưởng hệ thống	Ít	Có thể làm chậm hoặc gián đoạn

*Bảng 4. So sánh nhanh giữa IDS và IPS*

7. Công cụ Snort là gì:

- Snort là một phần mềm mã nguồn mở do Cisco phát triển, có thể hoạt động như IDS hoặc IPS, tùy vào cách cấu hình.

a. Tính năng chính của Snort:

- Phân tích lưu lượng mạng theo thời gian thực
- Phát hiện tấn công như: buffer overflow, port scan, brute force...
- Có thể ghi log, sinh cảnh báo hoặc ngăn chặn tấn công (nếu cấu hình như IPS)
- Hỗ trợ viết rule để phát hiện hoặc chặn các mẫu tấn công cụ thể

## b. Các chế độ hoạt động của Snort:

- Sniffer mode: bắt gói tin và hiển thị ra màn hình
- Packet logger mode: bắt gói tin và ghi vào file log
- Network Intrusion Detection System (NIDS) mode: phát hiện và cảnh báo tấn công theo rule
- IPS mode (nếu kết hợp với inline): chặn lưu lượng theo rule

## 8. Khái niệm về quản lý người dùng cuối (System Endpoint Management):

- Quản lý người dùng cuối hay còn gọi là quản lý thiết bị đầu cuối (Endpoint Management) là quá trình kiểm soát, giám sát và bảo vệ các thiết bị kết nối đến hệ thống mạng của tổ chức. Các thiết bị này bao gồm máy tính cá nhân, laptop, máy tính bảng, điện thoại thông minh, máy in, thiết bị IoT và các thiết bị đầu cuối khác.
- Trong bối cảnh ngày càng nhiều người làm việc từ xa và sử dụng thiết bị cá nhân (BYOD – Bring Your Own Device), việc quản lý và bảo mật các endpoint đóng vai trò then chốt nhằm:
  - + Ngăn chặn sự xâm nhập từ bên ngoài.
  - + Đảm bảo thiết bị tuân thủ chính sách bảo mật.
  - + Tăng cường tính sẵn sàng và ổn định của hệ thống CNTT.

## 9. Các chức năng chính của hệ thống quản lý endpoint:

STT	Chức năng	Mô tả ngắn gọn
1	Giám sát thiết bị	Theo dõi trạng thái hoạt động và an ninh của thiết bị đầu cuối
2	Cấu hình thiết bị từ xa	Triển khai cài đặt, chính sách bảo mật từ xa
3	Quản lý bản vá và phần mềm	Cập nhật, cài đặt phần mềm hoặc vá lỗ hổng bảo mật tự động
4	Bảo vệ thiết bị	Tích hợp giải pháp chống virus, chống mã độc
5	Xóa dữ liệu từ xa và khóa thiết bị	Bảo vệ dữ liệu trong tình huống mất cắp hoặc đánh rơi
6	Báo cáo và cảnh báo	Tạo báo cáo tổng quan về tình trạng thiết bị và gửi cảnh báo bất thường

Bảng 5. Bảng chức năng chính của hệ thống quản lý endpoint

## 10. Một số công cụ quản lý người dùng cuối phổ biến:

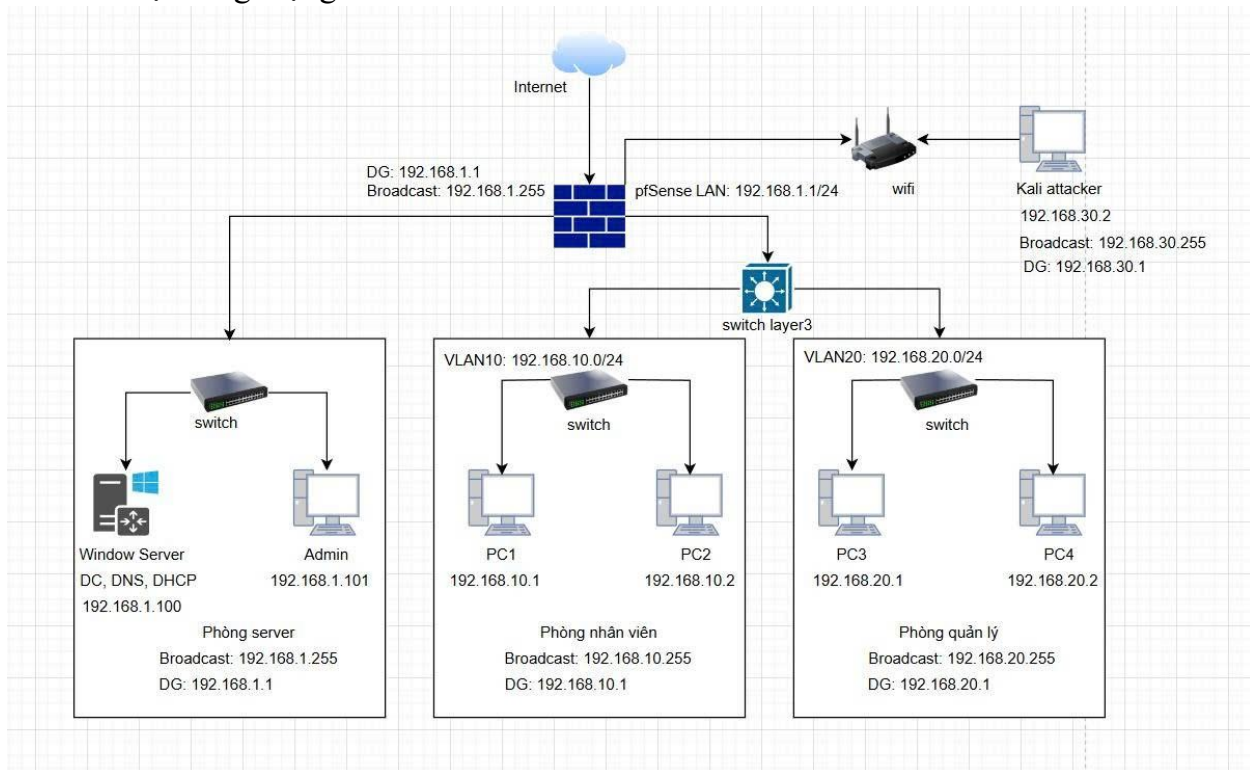
Tên công cụ	Mô tả
Microsoft Intune	Nền tảng quản lý điểm cuối tích hợp chặt chẽ với Microsoft 365; hỗ trợ Windows, Android, iOS, macOS
VMware Workspace ONE	Giải pháp quản lý thiết bị và ứng dụng đa nền tảng; bảo mật tốt, linh hoạt cho doanh nghiệp
Miradore (bản miễn phí và trả phí)	Giải pháp đơn giản để quản lý thiết bị di động và máy tính từ xa

ManageEngine Endpoint Central	Cung cấp khả năng quản lý và bảo mật toàn diện endpoint trong tổ chức
Cisco Meraki Systems Manager	Quản lý thiết bị qua đám mây; dễ triển khai, phù hợp với doanh nghiệp nhỏ và vừa

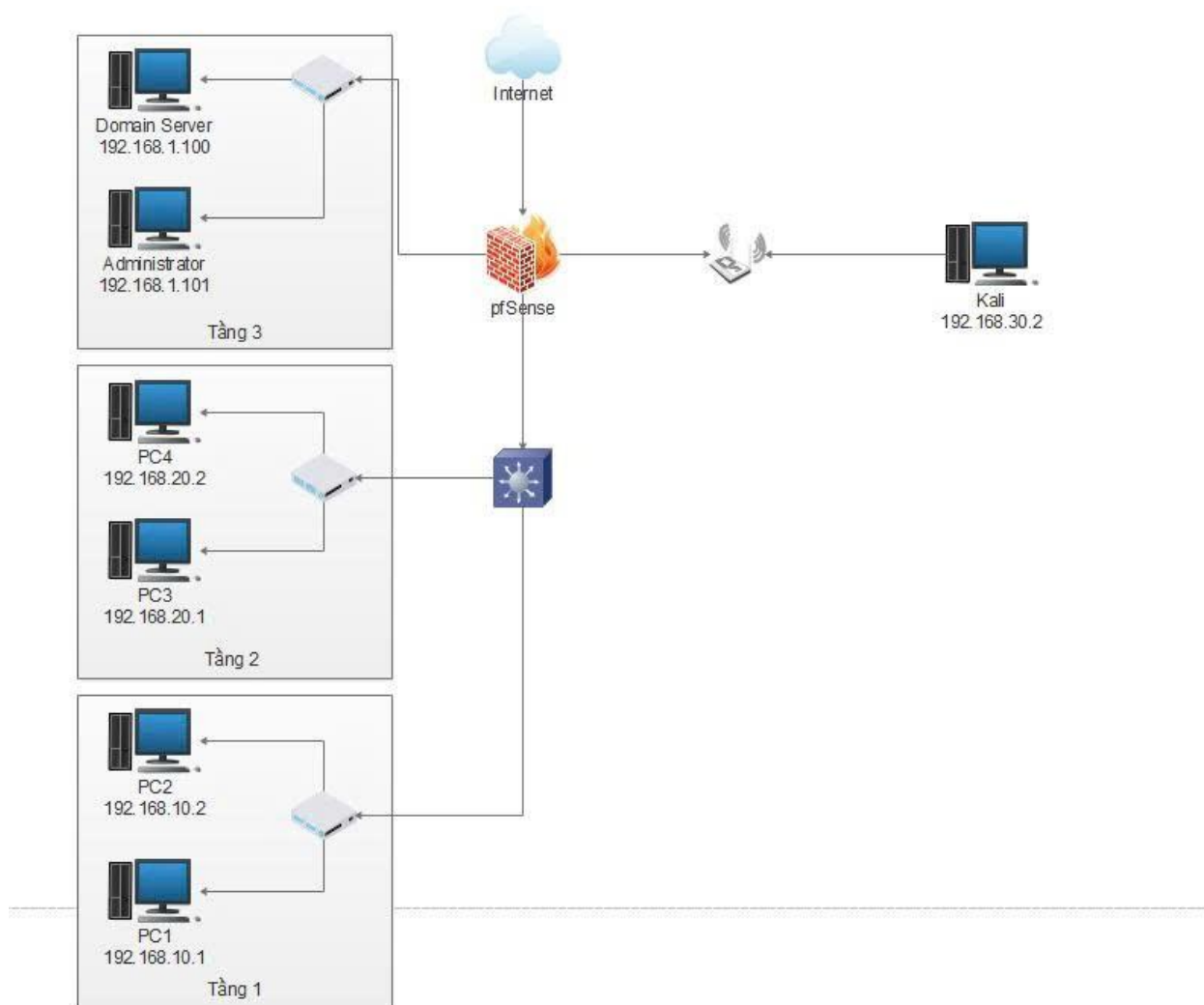
*Bảng 6. Bảng công cụ quản lý người dùng cuối phổ biến*

### CHƯƠNG III: TRIỂN KHAI

#### 1. Sơ đồ hệ thống mạng LAN:

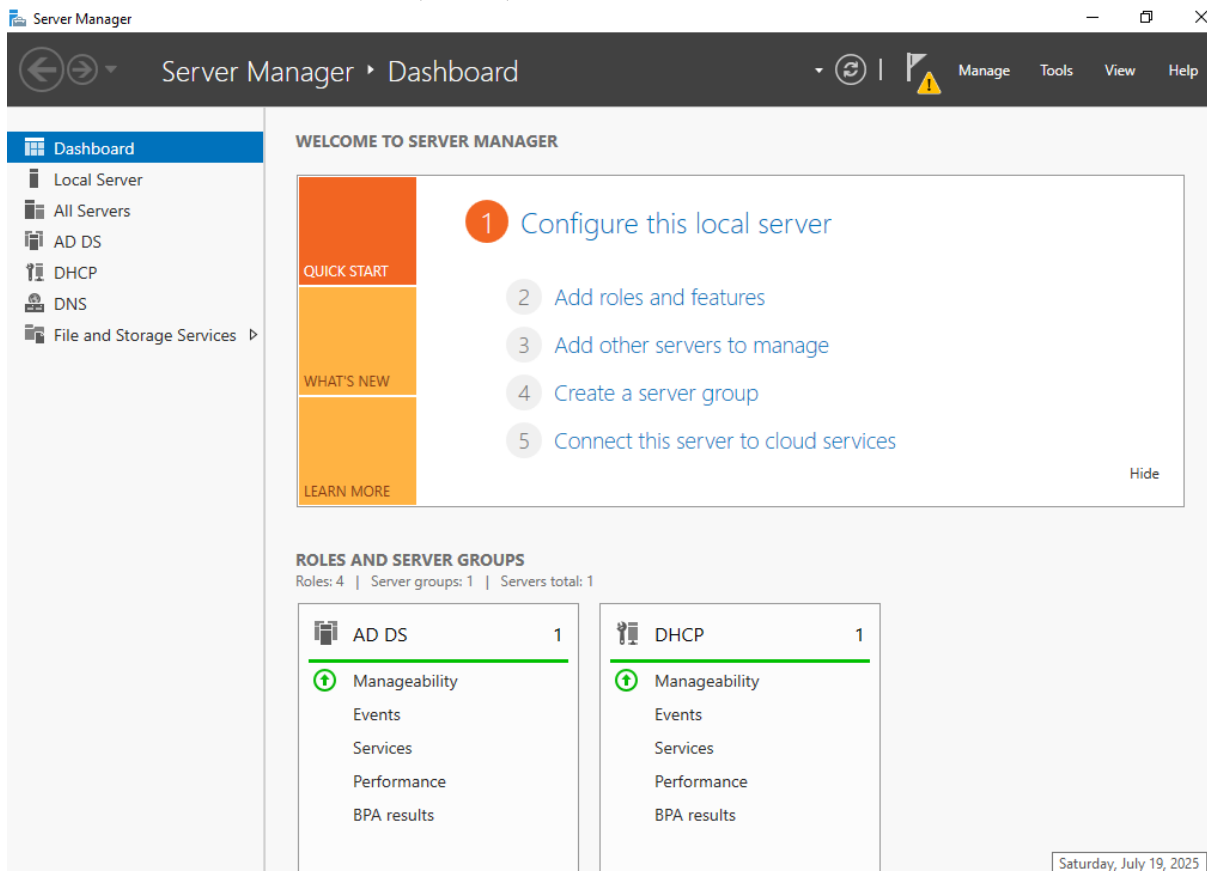


*Hình 5. Sơ đồ hệ thống mạng LAN*



Hình 6. Sơ đồ vật lý

## 2. Cài đặt các dịch vụ AD DS, DNS, DHCP trên Windows Server:

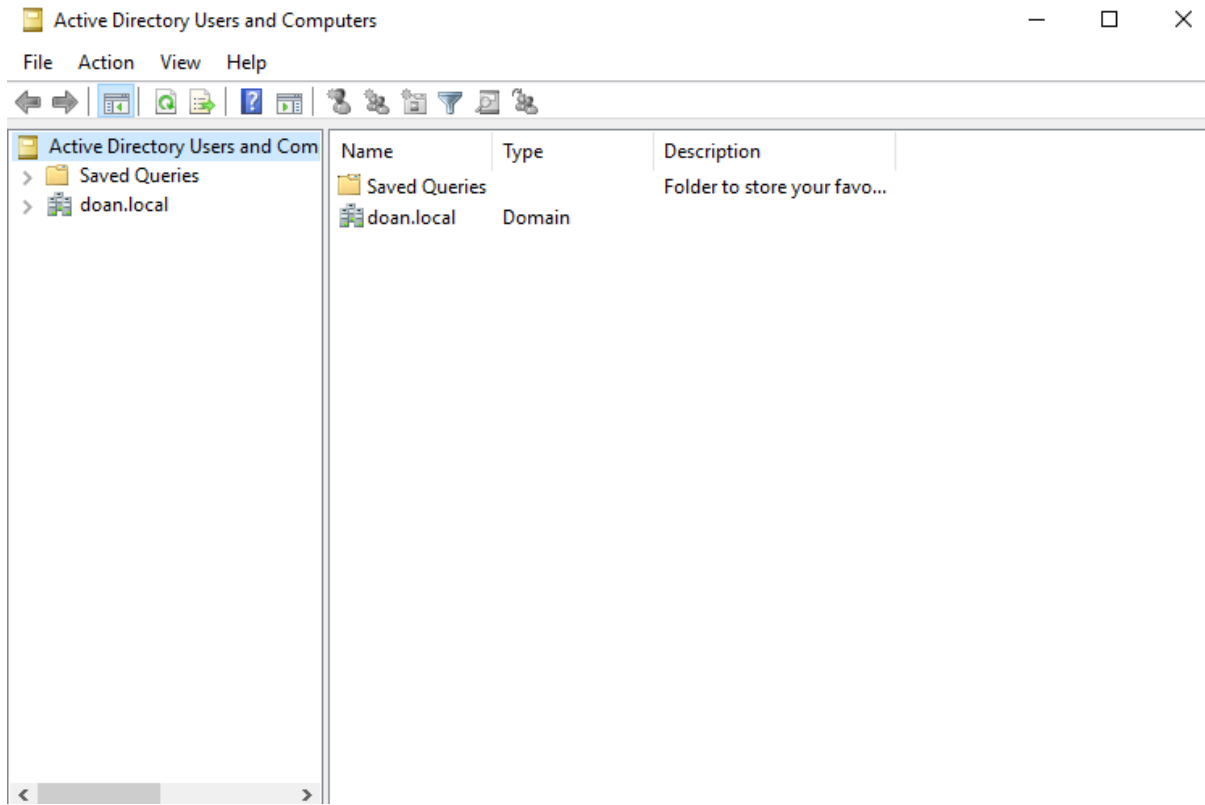


*Hình 7. Cấu hình DC thành công*

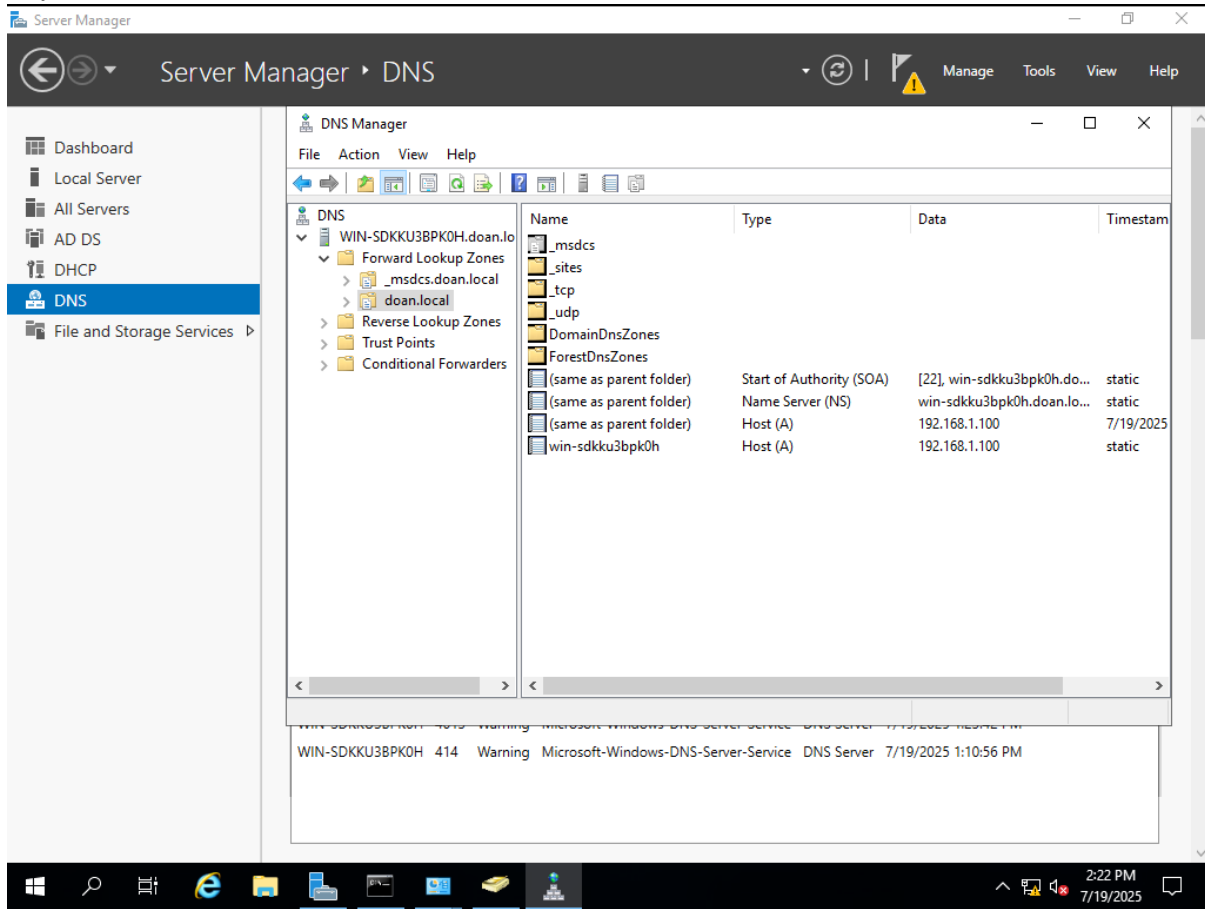
Cấu hình Windows Server thành Domain Controller + DNS thành công

Domain đã được tạo và domain controller hoạt động.





Dịch vụ DNS đã được cấu hình, Zone doan.local được thiết lập trong DNS Manager, có đầy đủ record NS, SOA và A trở về 192.168.1.100



Hình 8. Cấu hình DHCP để tạo IP tự động

Cấu hình DHCP để tạo IP tự động trên Windows Server

Tạo 1 scope mới với dải IP từ 192.168.1.10 tới 192.168.1.200

#### New Scope Wizard

##### Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

#### New Scope Wizard

##### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



##### Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

##### Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

**Router (Default Gateway): nhập 192.168.1.1**

New Scope Wizard

**Router (Default Gateway)**

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

192.168.1.1

Remove

Up

Down

&lt; Back

Next &gt;

Cancel

## DNS Servers: nhập 192.168.1.100

New Scope Wizard

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:



Add

Resolve

192.168.1.100

Remove

Up

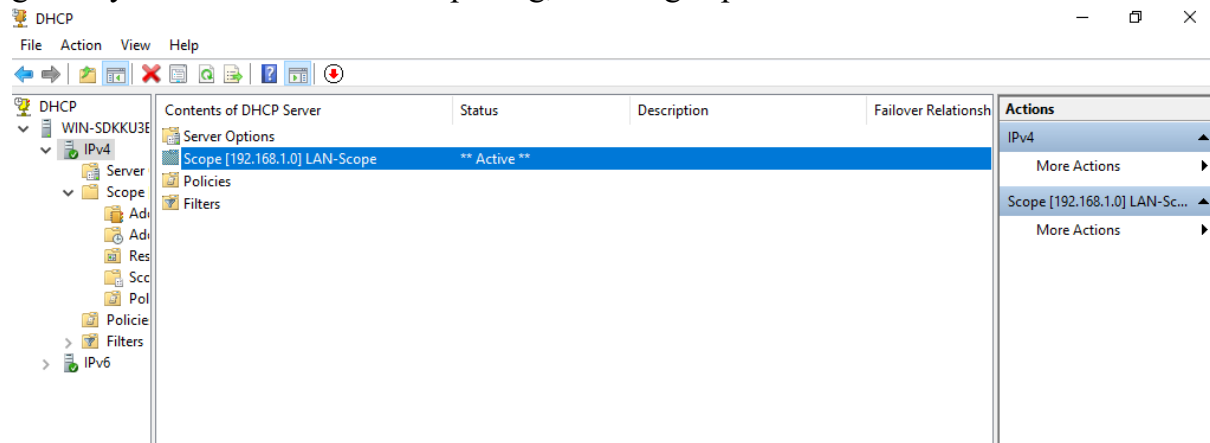
Down

< Back

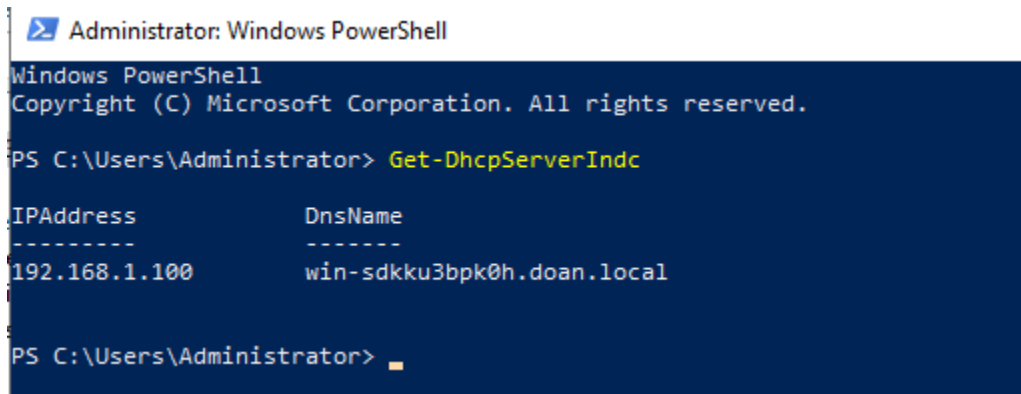
Next >

Cancel

Scope LAN-Scope đang có biểu tượng **Active** ✓ cho thấy cấu hình dải IP, subnet, gateway và DNS đều đã thiết lập đúng, sẵn sàng cấp địa chỉ cho client



**DHCP server đã được authorize thành công** trong Active Directory, IP 192.168.1.100 cùng tên FQDN, nghĩa là server đã nằm trong danh sách được phép cấp DHCP cho client



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-DhcpServerIndc

IPAddress            DnsName
-----
192.168.1.100        win-sdtku3bpk0h.doan.local

PS C:\Users\Administrator>

```

### 3. Thiết kết các rule IPS/IDS:

#### a. Cài đặt Pfsense:

#### **Bước 1: Tải pfSense ISO:**

- + Truy cập: <https://www.pfsense.org/download/>
- + Chọn phiên bản: Netgate pfSense CE (Community Edition)
- + Architecture: AMD64 (64-bit)
- + Installer: ISO Installer
- + Mirror: Chọn gần bạn nhất

#### **Bước 2: Tạo máy ảo (VMware / VirtualBox):**

- + RAM: tối thiểu 1GB (khuyến nghị 2GB)
- + CPU: 1 hoặc 2 core
- + Disk: 10GB trở lên
- + Network Adapter: Chọn 2 card mạng:
- + WAN: kết nối ra ngoài (NAT/Bridge)
- + LAN: kết nối nội bộ (Internal/Host-Only)

#### **Bước 3: Boot từ file ISO**

- + Gắn file ISO vào ổ đĩa ảo (CD/DVD)
- + Boot máy ảo và khởi động vào trình cài đặt pfSense

#### **Bước 4: Giao diện cài đặt**

- + Chọn Install pfSense
- + Bấm Enter liên tục để tiếp tục qua các màn hình

#### **Bước 5: Kiểm tra nhận diện WAN & LAN**

- + WAN và LAN sẽ hiển thị địa chỉ IP (nếu không có IP thì bạn cần cấu hình thủ công)

## Bước 6: Thiết lập IP LAN thủ công (nếu cần)

- + Chọn menu 2 > Thiết lập IP LAN tĩnh (vd: 192.168.1.1/24)
- + Cấu hình DHCP Server (có thể bật để máy con tự nhận IP)

```

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

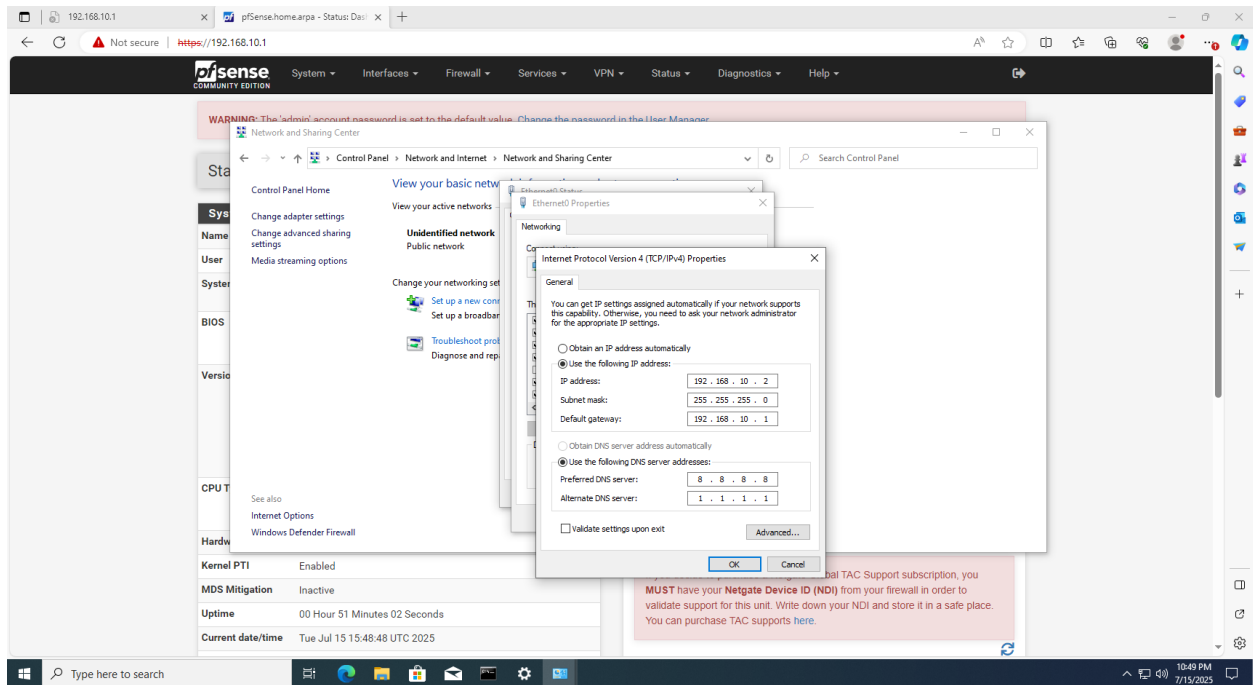
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.63/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell - pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (ssh)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Jul 15 15:01:52 ...
php-fpm(3991): /index.php: Successful login for user 'admin' from: 192.168.10.2 (
Local Database)
swap_pager: indefinite wait buffer: bufobj: 0, blkno: 241689, size: 8192
swap_pager: indefinite wait buffer: bufobj: 0, blkno: 241783, size: 12298
swap_pager: indefinite wait buffer: bufobj: 0, blkno: 287879, size: 4896
swap_pager: out of swap space
swap_pager_getswapSPACE(38): failed

```

Hình 9. Giao diện đã cài đặt thành công pfSense



Hình 10. Chỉn sửa IP của máy admin

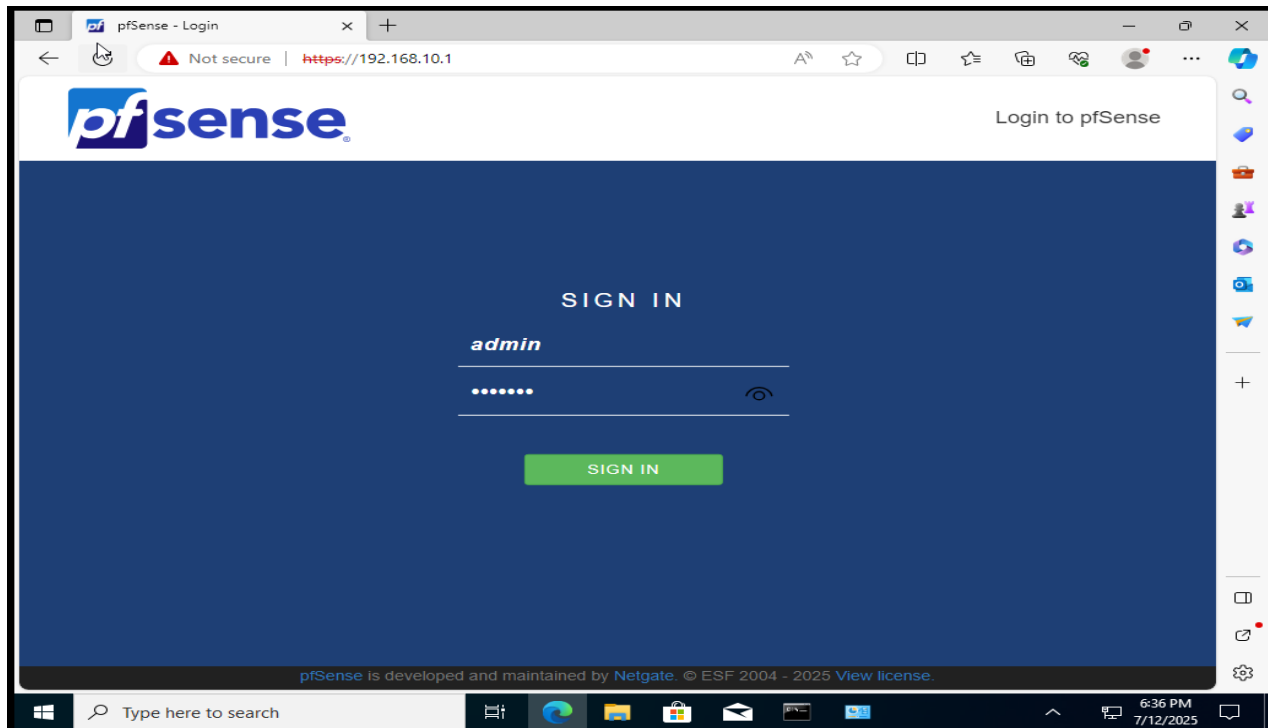
## Bước 7: Truy cập từ trình duyệt

- + Trên một máy ảo khác trong cùng mạng LAN, mở trình duyệt và truy cập: 192.168.10.1

Đăng nhập mặc định:

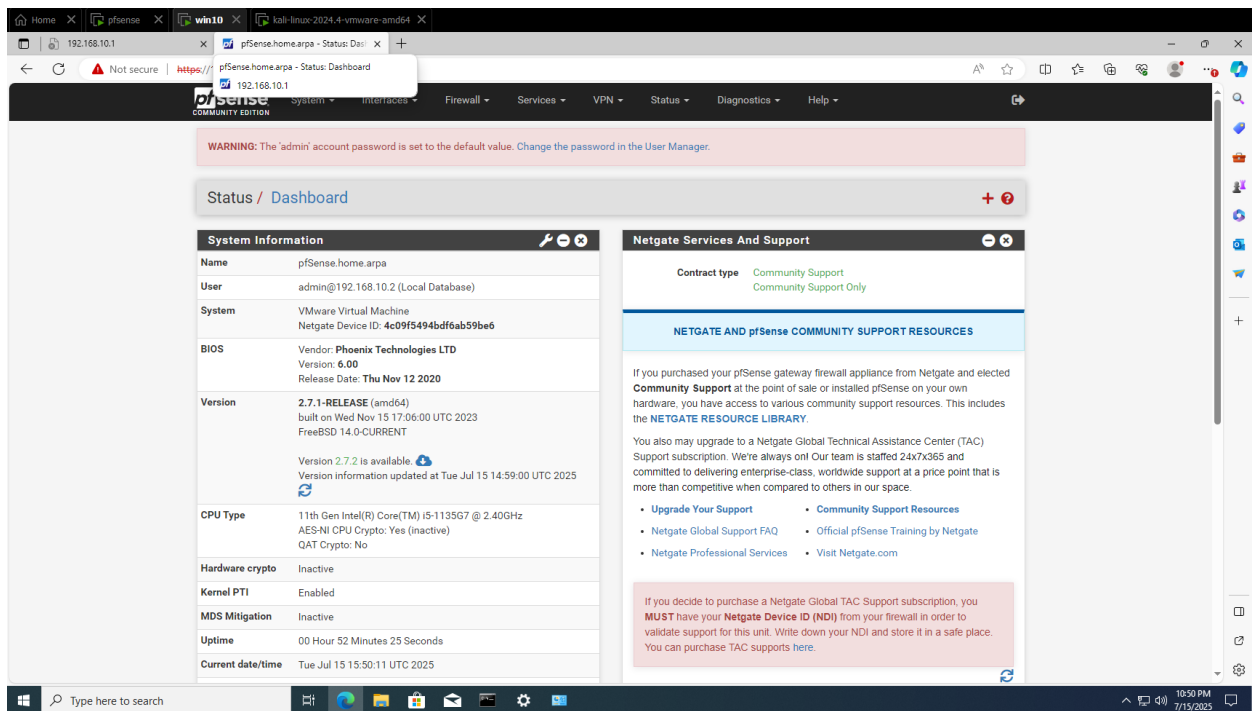
- + **Username:** admin
- + **Password:** pfsense





Hình 11. Giao diện truy cập 192.168.10.1

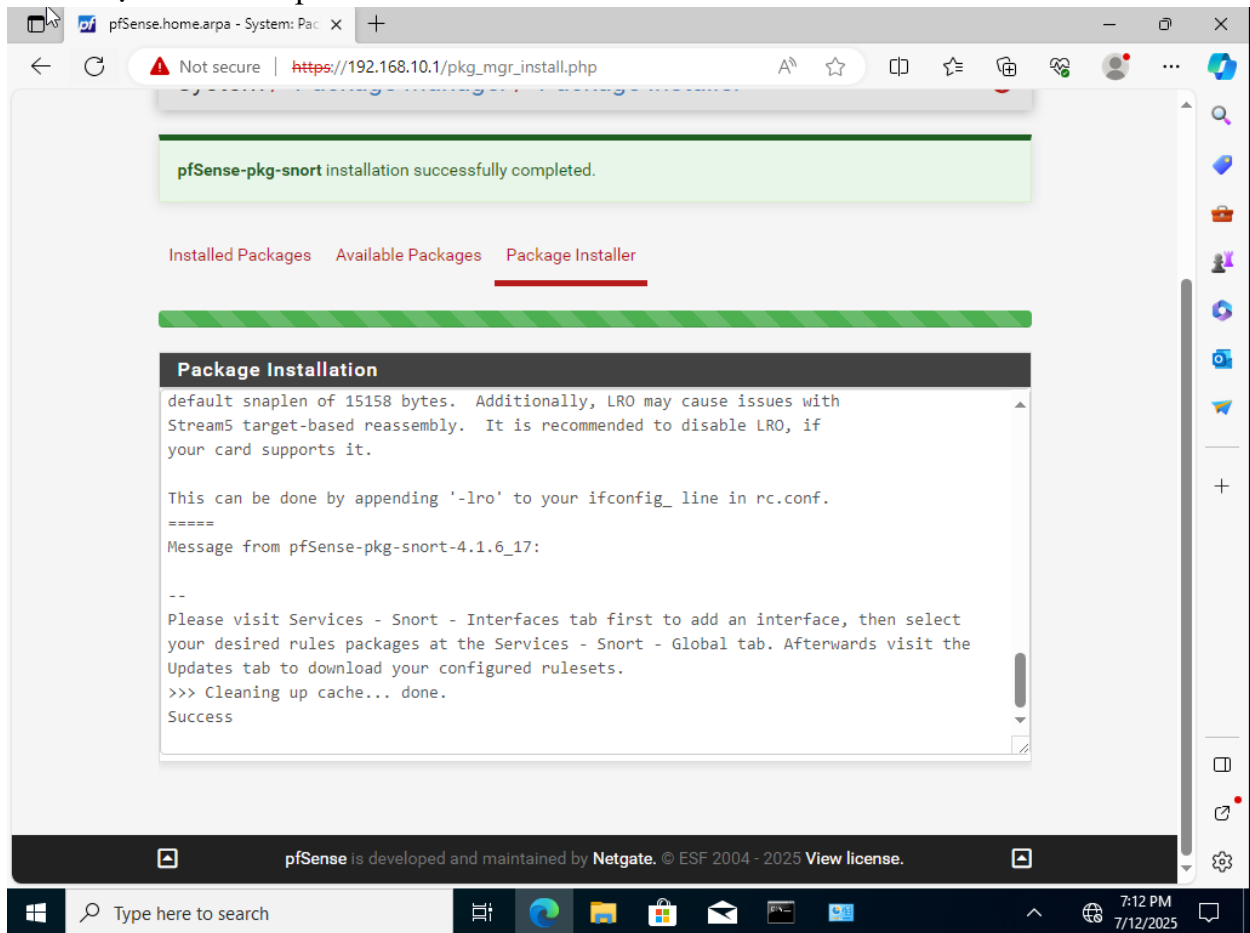
Truy cập thành công giao diện pfsense trên máy admin với địa chỉ là 192.168.10.1



Hình 12. Giao diện Dashboard của pfsense

Đăng nhập thành công sẽ chuyển sang trang giao diện của pfsense

#### b. Cài đặt Snort trên pfsense:



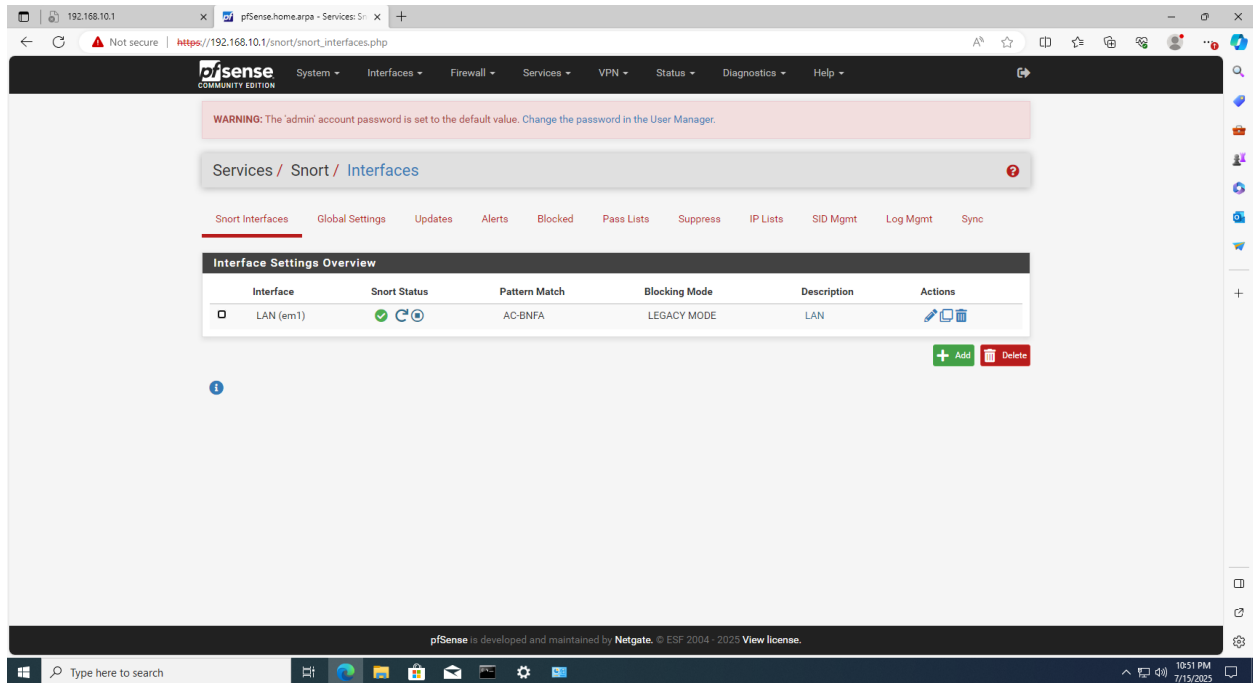
Hình 13. Cài đặt gói Snort

#### Bước 1: Mở Package Manager

- Vào System > Package Manager > Available Packages
- Tìm kiếm từ khóa: snort

#### Bước 2: Cài đặt Snort

- Nhấn nút Install bên cạnh gói Snort
- Chờ khoảng vài phút để quá trình cài đặt hoàn tất
- Cài đặt Snort thành công



Hình 14. Cấu hình Snort

### Bước 1: Vào giao diện Snort

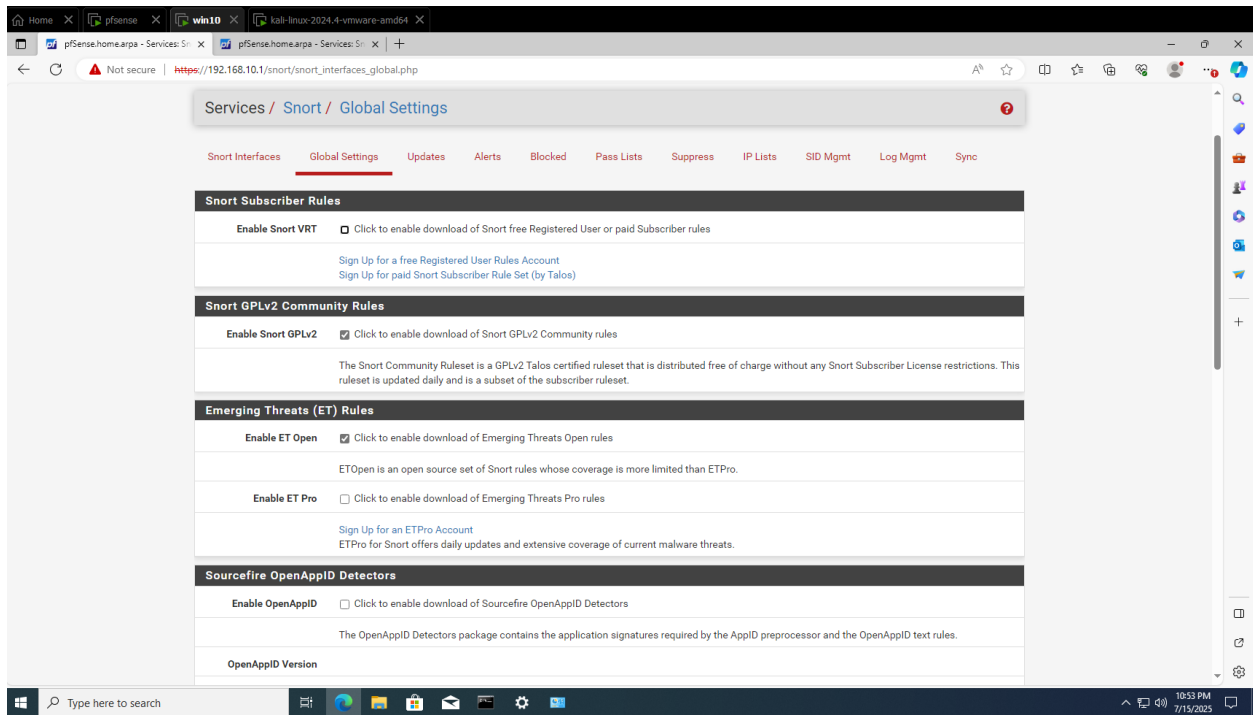
- + Vào Services > Snort

### Bước 2: Thêm interface để bảo vệ

- + Chuyển đến tab Interfaces
- + Nhấn +Add
- + Chọn interface muốn bảo vệ (ví dụ: WAN hoặc LAN)
- + Đặt tên, bật *Enable*, bật *Block Offenders* nếu muốn chặn

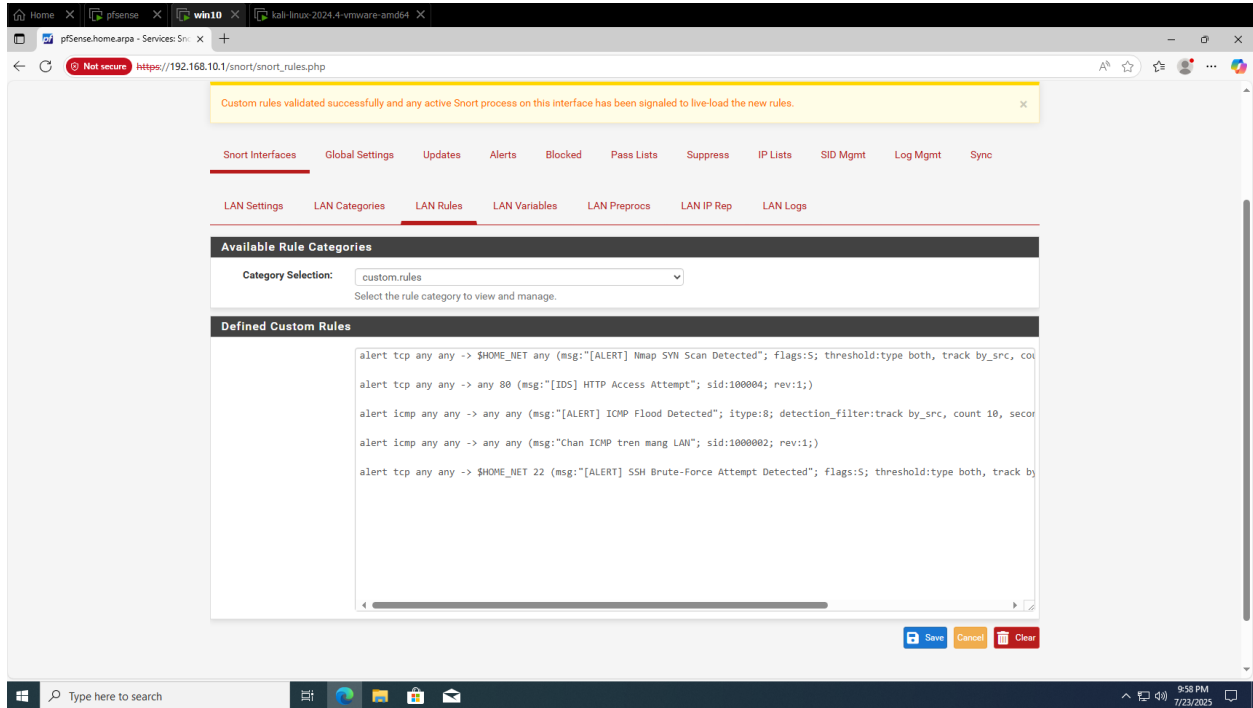
### Bước 3: Thiết lập rules

- + Trong phần interface vừa thêm > Chuyển sang tab Categories
- + Chọn các nhóm rule bạn muốn bật (nên bật các nhóm phổ biến như trojan, policy, scan, malware...)



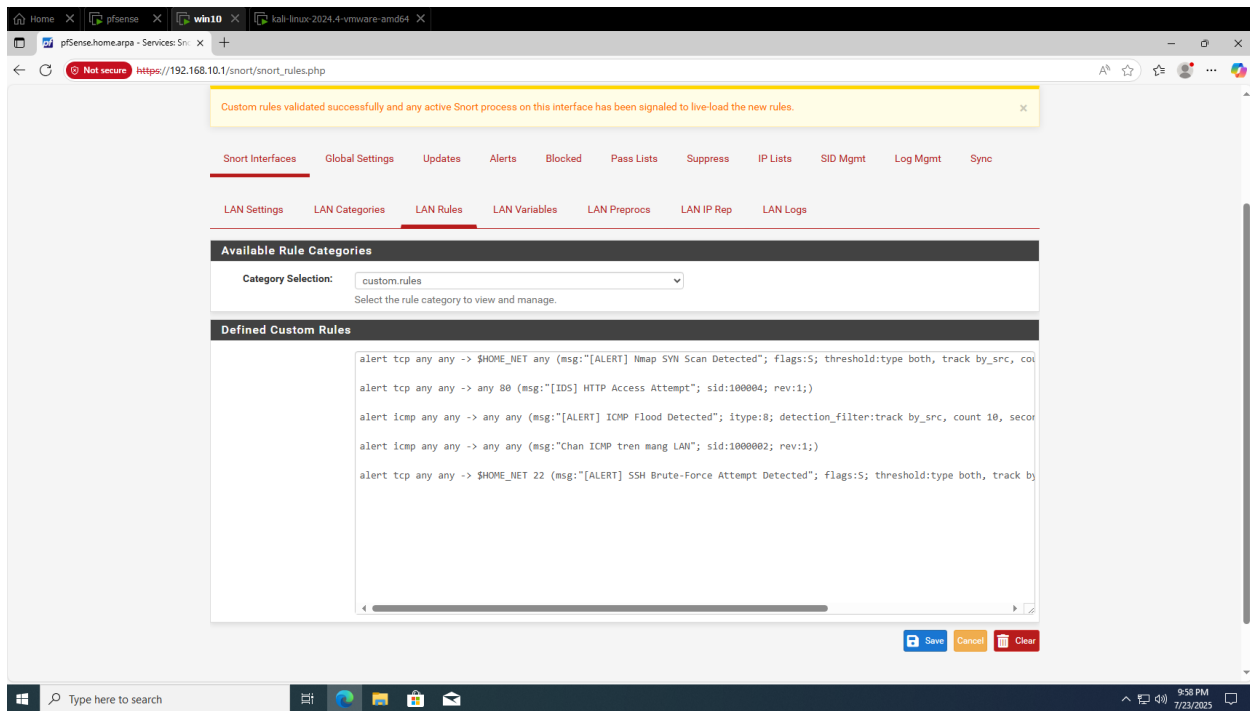
Hình 15. Tải rules

Tích chọn các rule để tải các rule về.



Hình 16. Viết rules

Sau khi tải các rule về, chuyển vào mạng LAN muốn đặt rule, chọn Custom Rules.



Hình 17. Thông báo đã apply rules thành công

Viết các rule muốn thực hiện và Save lại, sau khi Save và Apply thành công thì sẽ hiển thị thông báo như trên.

### 3. Các rule quản lý người dùng cuối:

#### 3.1. Giới thiệu về Wazuh

- Wazuh là một nền tảng mã nguồn mở dùng để giám sát bảo mật, phát hiện xâm nhập, và phân tích log tập trung. Nó cung cấp khả năng theo dõi các endpoint, cảnh báo theo thời gian thực và tích hợp dễ dàng với các công cụ như ELK Stack. Wazuh được chọn vì tính linh hoạt, khả năng mở rộng cao và miễn phí bản quyền. Ngoài ra, cộng đồng hỗ trợ mạnh mẽ cũng giúp việc triển khai và vận hành trở nên hiệu quả hơn.

#### 3.2. Cài đặt Wazuh làm công cụ giám sát

##### Bước 1: Cập nhật hệ thống và cài đặt gói curl

```
huyhoang@huyhoang-VMware-Virtual-Platform:~$ sudo apt install curl -y
[sudo] password for huyhoang:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (8.5.0-2ubuntu10.6).
The following package was automatically installed and is no longer required:
  libsigsegv2
Use 'sudo apt autoremove' to remove it.
```

**Bước 2:**

- Tải file wazuh-install.sh từ trang chủ Wazuh để cài đặt phần mềm

```
huyhoang@huyhoang-VMware-Virtual-Platform:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

- Lệnh bash wazuh-install.sh -a tự động cài đặt Wazuh với cấu hình mặc định (cài full stack Wazuh: Manager, Indexer, Elasticsearch, Dashboard, Kibana)

```
huyhoang@huyhoang-VMware-Virtual-Platform:~$ bash wazuh-install.sh -a
```

- Cài đặt thành công Wazuh all-in-one

```
20/07/2025 17:29:18 INFO: --- Wazuh dashboard ---
20/07/2025 17:29:18 INFO: Starting Wazuh dashboard installation.
20/07/2025 17:30:09 INFO: Wazuh dashboard installation finished.
20/07/2025 17:30:09 INFO: Wazuh dashboard post-install configuration finished.
20/07/2025 17:30:09 INFO: Starting service wazuh-dashboard.
20/07/2025 17:30:10 INFO: wazuh-dashboard service started.
20/07/2025 17:30:33 INFO: Initializing Wazuh dashboard web application.
20/07/2025 17:30:34 INFO: Wazuh dashboard web application initialized.
20/07/2025 17:30:34 INFO: --- Summary ---
20/07/2025 17:30:34 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: MzPD5wFRGLQsrfI6ALa930*vtgpg?pq5
20/07/2025 17:30:34 INFO: Installation finished.
huyhoang@huyhoang-VMware-Virtual-Platform:~$
```

*Hình 18. Tải thành công Wazuh*

- Kiểm tra các tài khoản Wazuh bằng lệnh:

```
huyhoang@huyhoang-VMware-Virtual-Platform:~$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
[sudo] password for huyhoang:
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: 'MzPD5wFRGLQsrfI6ALa930*vtgpg?pq5'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: 'g4af?nEMvenYYKugtwKM*LXl+iDKwHIB'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
indexer_username: 'kibanaro'
indexer_password: '2.Rs6yqPW6CPhYEaq2DeMXwib.CBc.JC'

# Filebeat user for CRUD operations on Wazuh indices
indexer_username: 'logstash'
indexer_password: 'fbJKgeyEnx6ZFj8*b1eoqqA0oBjkG?qT'

# User with READ access to all indices
indexer_username: 'readall'
```

*Hình 19. Kiểm tra tài khoản wazuh*

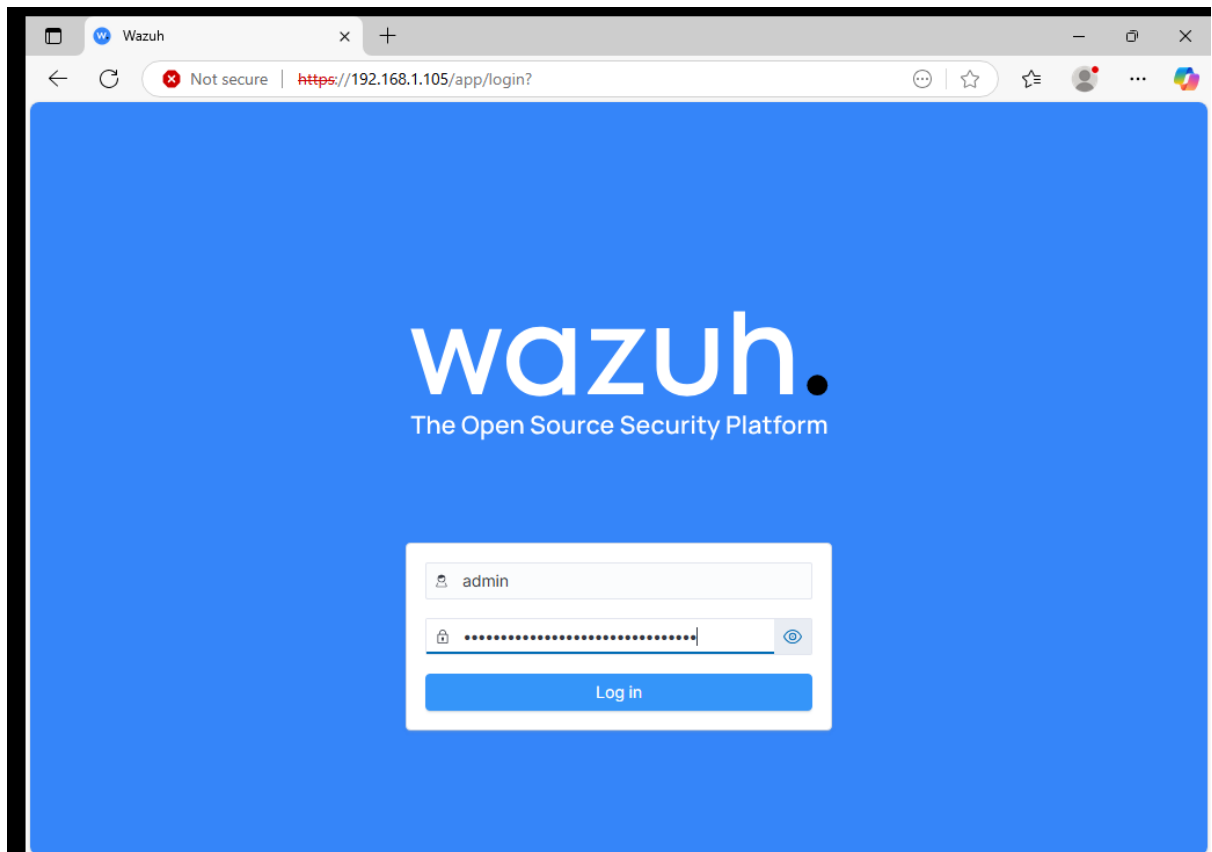
- Tắt tự động cập nhật Wazuh để tránh lỗi

```
huyhoang@huyhoang-VMware-Virtual-Platform:~$ sudo sed -i "s/^deb /#deb/" /etc/ap  
t/sources.list.d/wazuh.list  
huyhoang@huyhoang-VMware-Virtual-Platform:~$ sudo apt update  
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease  
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease  
Fetched 126 kB in 2s (55.6 kB/s)
```

Hình 20. Tắt tự động cập nhật Wazuh

### Bước 3: Truy cập Wazuh

- Trên máy khách (windows) bật trình duyệt truy cập với lệnh: *https:192.168.1.105*. Sau đó nhập tài khoản admin và mật khẩu mặc định được cấp trên sẽ hiển thị giao diện wazuh.



Hình 21. Giao diện đăng nhập Wazuh GUI

- Tiếp theo nhấn Deploy new agent để tạo agent với tên agent admin\_pc, hệ điều hành Windows, IP của ubuntu.
- Deploy new agent như sau:

LINUX

☐ RPM amd64

☐ RPM aarch64

☐ DEB amd64

☐ DEB aarch64

WINDOWS

☒ MSI 32/64 bits

macOS

☐ Intel

☐ Apple silicon

For additional systems and architectures, please check our [documentation](#).

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

192.168.1.105

☒ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

admin\_pc

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

Run the following commands to download and install the agent:

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile \$env:tmp\wazuh-agent; msixexec.exe /i \$env:tmp\wazuh-agent /q WAZUH\_MANAGER='192.168.1.105' WAZUH\_AGENT\_NAME='admin\_pc'

Hình 21,22. Cách deploy agent giám sát



- Có 1 script, copy lệnh đó rồi bật power shell với quyền admin rồi dán vào. Sau đó khởi động lại Wazuh service.

```
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

Hình 23. Khởi động lại Wazuh service thành công

#### Bước 4: Kiểm tra và đánh giá hệ thống

- Kiểm tra kết nối giữa agent và manager
  - Trên Wazuh vào agent để kiểm tra trạng thái của agent Window đã cài

Agents (1) <span>Show only outdated</span> <span>Deploy new agent</span> <span>Refresh</span> <span>Export formatted</span> <span>More</span> <span></span>									
<input type="text" value="Search"/>									WQL
<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	admin_pc	192.168.1.104	default	Microsoft Windows 10 Education 10.0.19045.2965	node01	v4.12.0	<span></span> <span></span> <span></span>	<span></span> <span></span> <span></span>

Hình 24. New agent sau khi deploy

#### Bước 5: Tạo các sự kiện bảo mật giả lập (rule) để kiểm tra giám sát

- **Rule 1: Phát hiện người dùng nhiều lần mở cmd.exe**

```
GNU nano 7.2 /var/ossec/etc/rules/local_rules.xml *
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--Rule hien co--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <!--Rule 2: Phat hien nguoi dung mo CMD tren Window -->
  <rule id="100002" level="7">
    <if_sid>67027</if_sid>
    <field name="win.system.providerName">Microsoft-Windows-Security-Auditing</field>
    <description>Phat hien nguoi dung mo CMD (cmd.exe)</description>
    <group>windows,process_creation</group>
  </rule>
</group>
```

Hình 25. Rule 1. Phat hien user mo CMD

- Test log bằng cách: Trên máy windows admin gõ lệnh cmd.exe xong vào wazuh GUI để xem log bắt được.

456 hits					
Jul 22, 2025 @ 18:51:49.349 - Jul 23, 2025 @ 18:51:49.349					
Export Formatted           645 available fields           Columns           Density           1 fields sorted           Full screen					
	timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 23, 2025 @ 18:51:46.797	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:44.049	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:42.698	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:42.696	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:42.678	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:26.877	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 23, 2025 @ 18:51:26.835	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002

Hình 26. Log của rule 1

- Phân tích chi tiết log:
  - Người dùng hoặc hệ thống trên máy **admin\_pc** đã mở CMD nhiều lần trong khoảng thời gian ngắn (có thể là script, malware, hoặc thao tác lập thủ công). Có thể đây là hành vi bất thường (tự động hóa, khai thác, thử lệnh trái phép), cần được điều tra thêm.
  - Timestamp: Thời điểm xảy ra sự kiện (ví dụ: Jul 23, 2025 @ 18:51:46.797). Mỗi dòng là một lần người dùng hoặc tiến trình mở CMD.
  - agent.name: Tên của máy/agent gửi log về – ở đây là admin\_pc, tức là các sự kiện này đều đến từ một máy tính có tên là admin\_pc.
  - rule.description: Mô tả cảnh báo – rule này phát hiện người dùng mở CMD (cmd.exe)
  - rule.level: Mức độ cảnh báo là 7 (trong thang 0–15 của Wazuh, từ mức 7 đã được coi là mức nghiêm trọng trung bình).
  - rule.id: ID của rule là 100002
- **Rule 2: Phát hiện người dùng tạo user mới trong windows**  
 Rule này giúp phát hiện hành vi tạo tài khoản người dùng mới, một dấu hiệu quan trọng để theo dõi hoạt động quản trị trái phép, leo thang đặc quyền hoặc xâm nhập hệ thống.

```
<!--Rule 3: Phát hiện tạo user mới -->
<rule id="100005" level="10">
  <if_sid>60109</if_sid>
  <field name="win.system.eventID">4720</field>
  <description>Mot user mới được tạo trên máy Windows</description>
  <group>windows,account_management,user_creation</group>
</rule>
</group>
```

Hình 27. Rule 2. Phát hiện người dùng tạo user mới

- Test log bằng cách: Vào cmd quyền admin trên máy windows admin để tạo mới user bằng lệnh:

```
C:\. Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.6093]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user newuser abc123 /add
The command completed successfully.

C:\Windows\system32>_
```

Hình 28. Tạo user trên cmd quyền admin

- Vào wazuh GUI để xem log:

	timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 24, 2025 @ 03:59:35.013	admin_pc	User account changed	8	60110
	Jul 24, 2025 @ 03:59:34.981	admin_pc	User account enabled or created	8	60109
	Jul 24, 2025 @ 03:59:34.967	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 03:59:34.967	admin_pc	Mot user mới được tạo trên máy ...	10	100005

Hình 29. Log rule 2

- Phân tích log chi tiết:
  - Máy admin\_pc đã ghi nhận có hành vi tạo mới tài khoản người dùng trên hệ thống Windows tại thời điểm cụ thể. Hành vi này có thể là:
    - Do quản trị viên tạo user mới (hợp lệ), hoặc
    - Là dấu hiệu xâm nhập nếu tài khoản được tạo trái phép để duy trì truy cập (persistent backdoor)
  - Timestamp: Thời điểm xảy ra sự kiện (ví dụ: Jul 24, 2025 @ 03:59:34.967). Mỗi dòng đại diện cho một lần hệ thống ghi nhận có user mới được tạo
  - agent.name: Tên máy/agent gửi log về – ở đây là admin\_pc, tức là sự kiện này xảy ra trên máy tính có tên admin\_pc
  - rule.description: Mô tả cảnh báo – ở đây là “Một user mới được tạo trên máy Windows”

- rule.level: Mức độ cảnh báo là 10, thuộc mức nghiêm trọng cao (Wazuh chia từ 0–15; mức 10 trở lên thường yêu cầu kiểm tra gấp)
- rule.id: ID của rule là 100005

- **Rule 3: Phát hiện người dùng thêm user vào nhóm Administrator**

Rule này phát hiện khi một user được thêm vào nhóm Administrator trên hệ thống Windows (Event ID 4732). Đây là hành vi tăng quyền (privilege escalation), có thể dẫn đến rủi ro bảo mật nghiêm trọng

```
<!--Rule 4: Phát hiện thêm user mới vào nhóm Admin -->
<rule id="100006" level="12">
  <if_sid>60154</if_sid>
  <field name="win.system.eventID">4732</field>
  <description>Warning: Mot user duoc them vao nhom Admin</description>
  <group>windows,privilege_escalation,account_management</group>
</rule>
</group>
```

Hình 30. Rule 3. Phát hiện người dùng add user vào group admin

- Test log bằng cách: Vào cmd quyền admin trên máy windows admin để thêm user mới tạo vào nhóm admin bằng lệnh:

```
Microsoft Windows [Version 10.0.19045.6093]
(c) Microsoft Corporation. All rights reserved.







C:\Windows\system32>net user newuser abc123 /add
The command completed successfully.

C:\Windows\system32>net localgroup Administrators newuser /add
The command completed successfully.

C:\Windows\system32>
```

Hình 31. Lệnh add user vào group admin

- Truy cập wazuh GUI để xem chi tiết log thu được:

	↓ timestamp	agent.name	rule.description	rule.level	rule.id
	Jul 24, 2025 @ 11:24:21.787	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 11:24:19.797	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 11:24:19.794	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 11:24:19.722	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 11:23:57.918	admin_pc	Phat hien nguoi dung mo CMD (c...	7	100002
	Jul 24, 2025 @ 11:23:57.918	admin_pc	Warning: Mot user duoc them va...	12	100006

Hình 32. Log rule 3

- Phân tích log chi tiết:

- Máy admin\_pc đã ghi nhận một hành vi thêm user vào nhóm Administrator đây là hành vi nâng cao đặc quyền (privilege escalation). Hành vi này có thể là:
  - Hợp lệ: Quản trị viên đang thêm user vào nhóm quản trị
  - Nguy hiểm: Nếu được thực hiện bí mật hoặc sau khi tạo user mới → có thể là dấu hiệu xâm nhập nhằm kiểm soát hệ thống
- timestamp: Thời điểm xảy ra sự kiện (ví dụ: Jul 24, 2025 @ 11:23:57.918). Mỗi dòng đại diện cho một lần hệ thống ghi nhận có người dùng được thêm vào nhóm Admin.
- agent.name: Tên máy/agent gửi log về – ở đây là admin\_pc, tức là sự kiện xảy ra trên máy tính tên admin\_pc.
- rule.description: Mô tả cảnh báo – ở đây là “Warning: Một user được thêm vào nhóm Admin”
- rule.level: Mức độ cảnh báo là 12, thuộc mức **ngghiêm trọng rất cao**. Mức này thể hiện hành vi có khả năng ảnh hưởng trực tiếp đến bảo mật hệ thống
- rule.id: ID của rule là 100006

4. Các case tấn công:

a. *Nmap SYN Scan – Test Rule 1*

- Kịch bản:

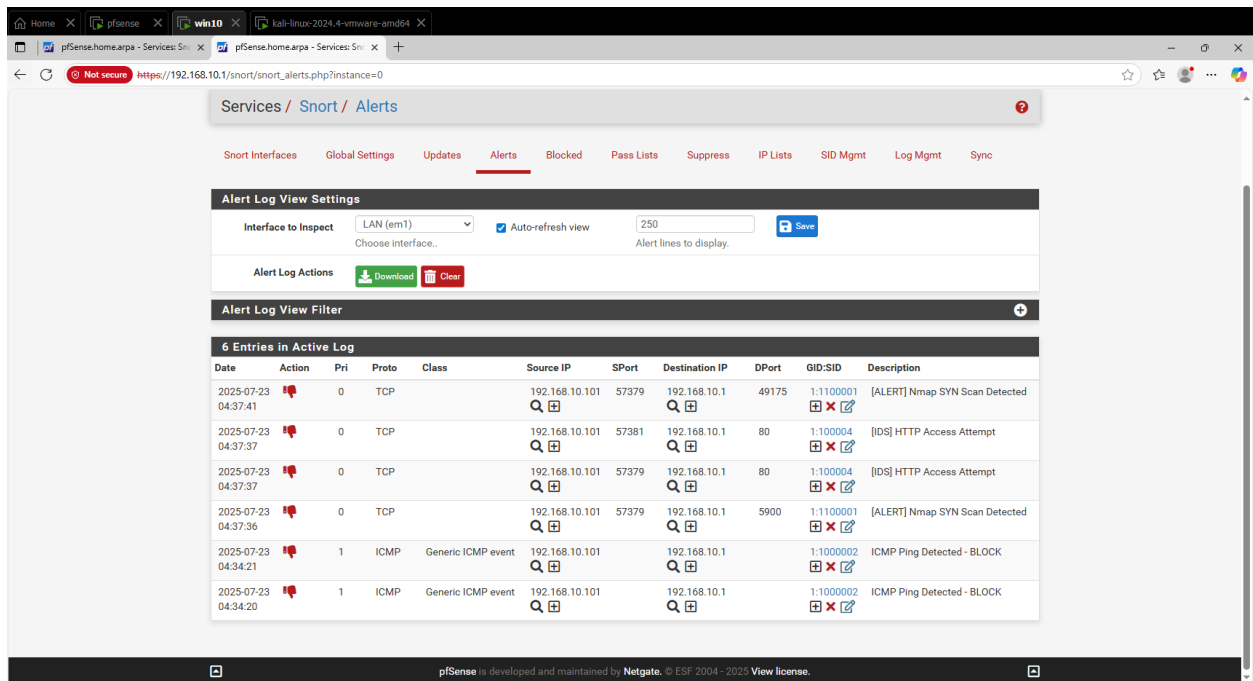
- Trong môi trường an ninh mạng, việc phát hiện sớm các hành vi do thám hệ thống là vô cùng quan trọng. Một trong những kỹ thuật thường được kẻ tấn công sử dụng là SYN Scan – một kiểu quét cổng nửa mở bằng công cụ Nmap.
  - Trong kịch bản này, chúng ta sẽ sử dụng máy Kali Linux để thực hiện lệnh *nmap -sS* nhằm mô phỏng hành vi tấn công quét cổng. Đồng thời, kiểm tra xem hệ thống IDS Snort có thể phát hiện và ghi nhận hành vi SYN Scan này hay không, thông qua rule đã được cấu hình sẵn.
  - Mục tiêu là đánh giá khả năng giám sát và cảnh báo sớm của Snort, góp phần nâng cao năng lực phòng thủ mạng nội bộ trước các nguy cơ tấn công tiềm ẩn.
-

```
(kali@kali)-[~]
$ nmap -sS 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 04:17 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0073s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Hình 32. Terminal máy Kali

Cách tấn công: Mở máy Kali và sử dụng terminal và nhập dòng lệnh: `sudo nmap -sS 192.168.1.1`

- + -sS: Gửi gói TCP SYN đến nhiều cổng
- + Rule sẽ bắt gói TCP có flag S nếu  $\geq 10$  lần trong 5 giây



Hình 33. Chuyển sang tab Alert để xem logs

Sau đó ta chuyển sang tab Alert để xem logs

**Giải thích logs:**

- + Bắt tất cả các gói TCP có flag SYN (flags:S)

- + Nếu thấy từ cùng một nguồn (by\_src)  $\geq 10$  SYN trong vòng 5 giây  
→ cảnh báo là SYN scan, đặc biệt là Nmap.

**Ý nghĩa rule:** Đây là dấu hiệu của Nmap SYN Scan (tấn công dò quét cổng) – hacker cố xác định cổng nào đang mở bằng cách gửi gói SYN rồi theo dõi phản hồi.

#### b. HTTP Access Attempt – Test Rule 2

##### - Kịch bản:

- Trong một hệ thống mạng, các truy cập HTTP không được phép – đặc biệt là từ các nguồn lạ – có thể là dấu hiệu của hành vi do thám hoặc khai thác lỗ hổng tiềm tàng.
- Để kiểm thử khả năng giám sát của hệ thống IDS Snort, kịch bản này mô phỏng một HTTP Access Attempt – tức một nỗ lực truy cập dịch vụ web qua cổng 80 – từ máy Kali Linux đến máy chủ nội bộ.

```
(kali㉿kali)-[~]
$ curl http://192.168.1.1

<html>
<head>
<title>302 Found</title>
</head>
<body bgcolor="#FFFFFF" text="#000000" link="#2020ff" vlink="#4040cc">
<h2>302 Found</h2>
<span>The requested URL is going to be https.</span>
<div style="display:none">
<span>Padding so that MSIE deigns to show this error instead of its own canned one.</span>
<span>Padding so that MSIE deigns to show this error instead of its own canned one.</span>
<span>Padding so that MSIE deigns to show this error instead of its own canned one.</span>
<span>Padding so that MSIE deigns to show this error instead of its own canned one.</span>
<span>Padding so that MSIE deigns to show this error instead of its own canned one.</span>
</div>
<hr/>
</body>
</html>
```

**Cách tấn công:** Ta mở terminal ở máy Kali và nhập: curl <http://192.168.1.1>

- Lệnh này gửi một truy vấn HTTP đơn giản, đóng vai trò như một gói tin nghi vấn, giúp kiểm tra xem Snort có thể phát hiện và cảnh báo về hành vi truy cập HTTP này hay không.
- Kịch bản này giúp xác minh độ hiệu quả của rule Snort trong việc theo dõi các kết nối web không mong muốn – một trong những kỹ thuật phát hiện xâm nhập mức ứng dụng (Application Layer Intrusion) phổ biến.

2025-07-23 04:43:30		0	TCP	192.168.10.101	51022	192.168.10.1	80	1:100004 	[IDS] HTTP Access Attempt
2025-07-23 04:43:30		0	TCP	192.168.10.101	51020	192.168.10.1	80	1:100004 	[IDS] HTTP Access Attempt

Hình 34. Load lại tab Alerts để xem logs

### Giải thích logs:

- + Vào lúc 08:43:07 ngày 2025-07-20, một kết nối TCP được phát hiện từ máy 192.168.10.101 (port ngẫu nhiên 40326) đến máy 192.168.1.1 qua port 80, đây là truy cập HTTP.

**Ý nghĩa rules:** phát hiện mọi truy cập HTTP, không phân biệt nội dung, giúp ghi nhận hoạt động web.

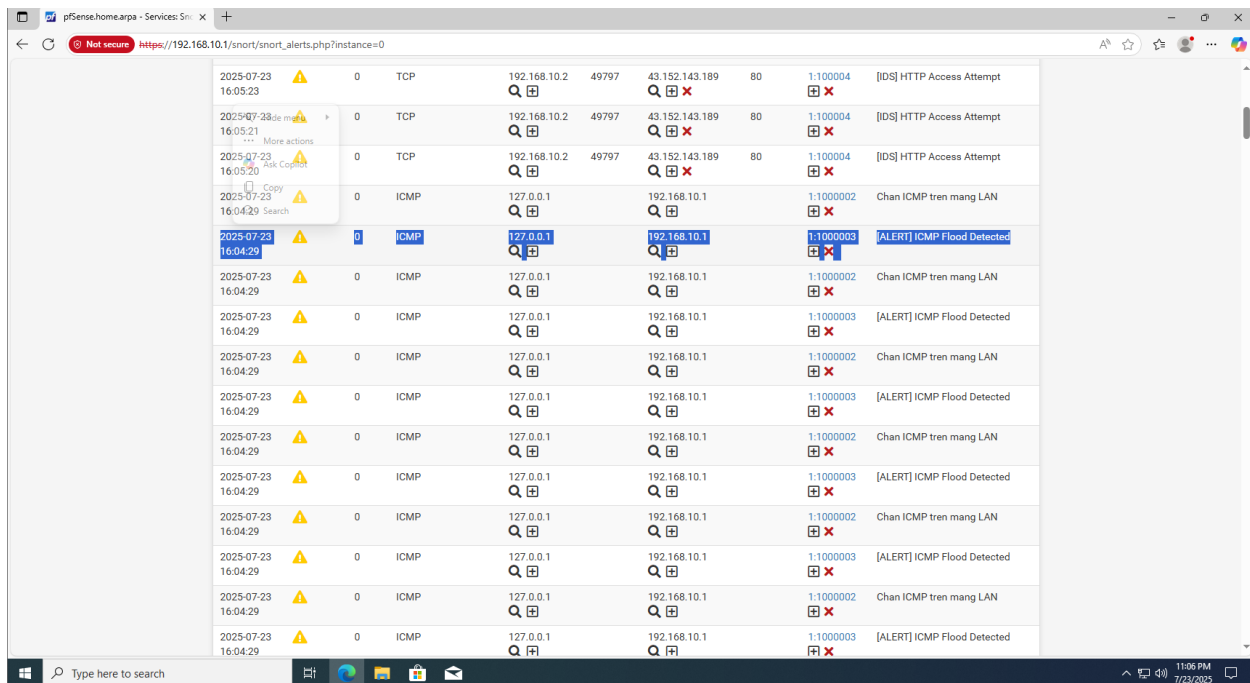
### c. ICMP Flood– Test Rule 3

- Kịch bản:
  - Trong môi trường mạng thực tế, các cuộc tấn công từ chối dịch vụ (DoS) dựa trên ICMP Flood là hình thức phổ biến nhằm làm nghẽn băng thông hoặc khiến hệ thống đích bị quá tải.
  - Kịch bản này mô phỏng một cuộc tấn công ICMP Flood từ máy Kali Linux đến hệ thống mục tiêu, nhằm kiểm thử xem hệ thống IDS Snort có thể phát hiện và cảnh báo đúng hành vi tấn công này hay không.
- Cách tấn công: Ta mở terminal ở máy Kali và nhập: `sudo hping3 -l --flood -d 192.168.10.1`

```
(kali@kali)~$ sudo hping3 -l --flood -d 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 150 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.1 hping statistic ---
365282 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- + -l: Gửi gói ICMP
- + --flood: Gửi liên tục, tạo lượng lớn gói ICMP
- + -d 150: Dung lượng dữ liệu > 100 byte
- Sau 1–3 giây, rule sẽ bị kích hoạt nếu IDS hoạt động đúng.
- Sau khi nhập xong, đợi khoảng chừng 3-4 giây và Ctrl+C để ngắt, nếu không thì sẽ bị chặn truy cập lưu lượng mạng.
- Cuộc tấn công này có thể tạo ra hàng ngàn gói ICMP mỗi giây, gây áp lực lên thiết bị đích. Rule Snort được cấu hình để phát hiện lưu lượng ICMP vượt ngưỡng trong thời gian ngắn – một dấu hiệu điển hình của ICMP Flood Attack.
- Mục tiêu của kịch bản là kiểm tra độ nhạy và hiệu quả của Snort trong việc giám sát tấn công DoS tăng mạng, góp phần tăng cường năng lực phòng thủ mạng nội bộ.





Hình 35. Load lại tab Alerts để xem logs

### Giải thích logs:

- + Gói này thuộc luồng ICMP flood, nghĩa là có nhiều gói ICMP với kích thước lớn hơn 100 bytes được gửi đi liên tục ( $\geq 10$  gói trong 1 giây) từ cùng một nguồn (detection\_filter: track by\_src, count 10, seconds 1), nên rule sid:1000001 đã được kích hoạt.
- + Đây là một hành vi báo động, có thể là tấn công ICMP flood (DoS) để làm nghẽn hệ thống hoặc gián đoạn dịch vụ.

**Ý nghĩa rules:** là biểu hiện của tấn công ICMP Flood (DoS), trong đó attacker gửi nhiều gói ping lớn liên tục để làm nghẽn mạng.

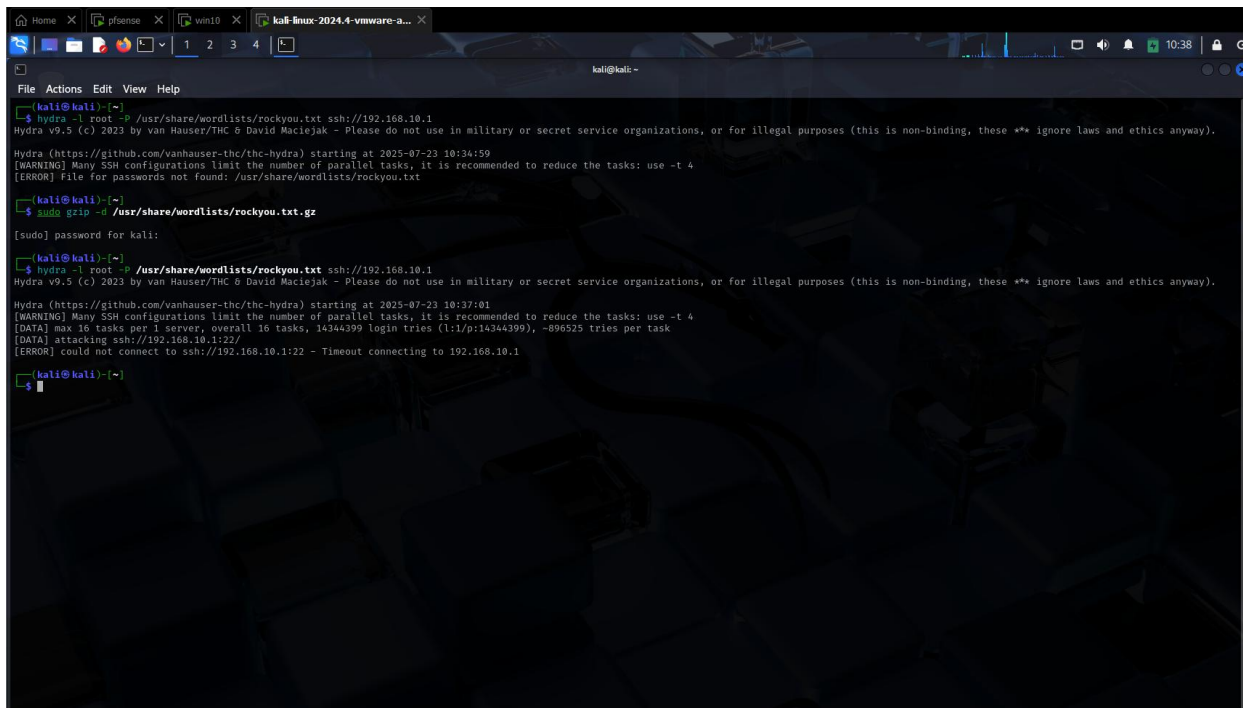
### d. Brute-force SSH – Test rule 4

#### - Kịch bản:

- Một trong những mối đe dọa phổ biến đối với hệ thống máy chủ là các cuộc tấn công Brute Force nhằm đoán mật khẩu đăng nhập, đặc biệt là qua giao thức SSH. Nếu không được giám sát chặt chẽ, những cuộc tấn công này có thể dẫn đến việc chiếm quyền điều khiển hệ thống.
- Trong kịch bản này, chúng ta sẽ sử dụng công cụ Hydra trên máy Kali Linux để mô phỏng một cuộc tấn công SSH Brute Force vào máy chủ có địa chỉ IP 192.168.10.1.
- Hành vi này sẽ tạo ra một lượng lớn kết nối SSH thất bại trong thời gian ngắn – đây chính là dấu hiệu để Snort phát hiện và cảnh báo.

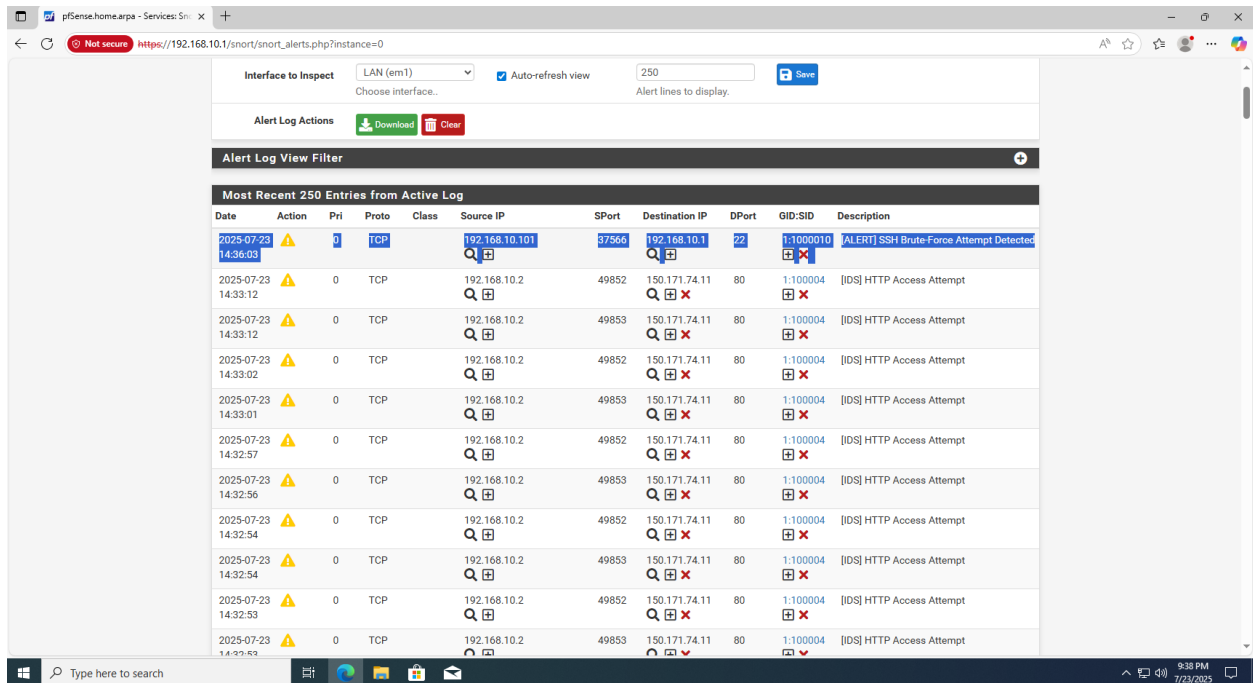
- Mục tiêu của kịch bản là kiểm tra xem rule phát hiện SSH brute force đã được cấu hình trong Snort có thể bắt được hành vi dò quét mật khẩu trái phép, từ đó cảnh báo kịp thời cho quản trị viên hệ thống hay không.

Cách tấn công: Ta mở máy Kali và nhập: `"hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.10.1"`



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.10.1  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-23 10:34:59  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt  
[kali@kali]~$ sudo gzip -r /usr/share/wordlists/rockyou.txt.gz  
[sudo] password for kali:  
[kali@kali]~$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.10.1  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-23 10:37:01  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:l/p:14344399), -896525 tries per task  
[DATA] attacking ssh://192.168.10.122/  
[ERROR] could not connect to ssh://192.168.10.122 - Timeout connecting to 192.168.10.1  
[kali@kali]~$
```

Hình 36. Terminal máy Kali



Hình 37. Mở tab Alert để xem logs

### Giải thích logs:

- Dòng log này ghi nhận một cảnh báo vào thời điểm 14 giờ 36 phút 03 giây ngày 23 tháng 7 năm 2025. Giao thức được phát hiện là TCP, với địa chỉ IP nguồn là 192.168.10.101, kết nối đến địa chỉ IP đích là 192.168.10.1 tại cổng 22 – là cổng mặc định của dịch vụ SSH. Port nguồn 37566 là port tạm thời được hệ thống Kali mở ra trong quá trình thực hiện kết nối.
- Snort đã kích hoạt rule có SID là 1000010, tức là rule phát hiện brute-force SSH do người dùng tự định nghĩa. Thông điệp “[ALERT] SSH Brute-Force Attempt Detected” là nội dung được chỉ định trong phần msg của rule, cho thấy Snort đã xác định đây là một cuộc tấn công brute-force vào SSH.
- Việc log xuất hiện như trên chứng minh rằng rule đã hoạt động chính xác: nó theo dõi số lượng gói SYN gửi đến port 22 trong một khoảng thời gian ngắn, và khi ngưỡng được vượt quá (5 gói trong vòng 60 giây), Snort đã phát hiện và ghi lại cảnh báo.

**Ý nghĩa rules:** Phát hiện hành vi brute-force vào dịch vụ SSH bằng cách theo dõi số lượng kết nối TCP (gói SYN) đến cổng 22 trong khoảng thời gian ngắn. Đây là dạng tấn công phổ biến nhằm dò tìm tài khoản/mật khẩu truy cập trái phép vào hệ thống.

### 5. Kết luận:

- Trong đề án này, hệ thống bảo mật người dùng cuối được xây dựng dựa trên hai thành phần chính: **Snort trên pfSense** để phát hiện và ngăn chặn các tấn công mạng theo thời gian thực, và **Wazuh** để giám sát hoạt động người dùng cuối như tạo user, mở CMD hay leo thang đặc quyền. Việc kết hợp IDS/IPS với giải pháp giám sát endpoint giúp nâng cao khả năng phát hiện sớm và phản ứng với các hành vi bất thường. Hệ thống hoạt động hiệu quả, có khả năng mở rộng và ứng dụng thực tế trong môi trường doanh nghiệp nhỏ đến trung bình. Qua đó, đề án thể hiện tính khả thi trong việc triển khai mô hình bảo mật chủ động và toàn diện.

### 6. Video demo

- Sau đây là các link demo ips/ids, tấn công trên kali,...  
[https://youtu.be/NKQ\\_gKmIoGY](https://youtu.be/NKQ_gKmIoGY)  
<https://youtu.be/-ARkB-R-Yck>  
<https://youtu.be/O58pBRTuy3w>