

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 : XÂY DỰNG HỆ THỐNG MẠNG BẢO MẬT ENDPOINT

Giảng Viên Hướng Dẫn: ThS. Đỗ Phi Hưng

Thành Viên:

1. Nguyễn Thị Kim Doanh – 22DH110511
2. Nguyễn Thúy Vy – 22DH114363

TP. Hồ Chí Minh, ngày 30 tháng 07 năm 2025

NHẬN XÉT CỦA GIẢNG VIÊN

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

LỜI CẢM ƠN

Đầu tiên chúng em xin gửi lời cảm ơn sâu sắc đến Trường Đại học Ngoại ngữ - Tin học TP. Hồ Chí Minh (HUFLIT) đã đưa bộ môn “Bảo Mật Người Dùng Cuối” vào chương trình giảng dạy. Đặc biệt, chúng em xin bày tỏ lòng biết ơn sâu sắc đến giảng viên bộ môn – thầy Đỗ Phi Hưng về sự hướng dẫn và hỗ trợ quý báu của thầy trong môn học. Chính thầy là người đã tận tình dạy bảo và truyền đạt những kiến thức quý báu cho chúng em trong suốt học kỳ vừa qua. Trong thời gian tham dự lớp học của thầy, chúng em đã tiếp cận với rất nhiều kiến thức bổ ích và rất cần thiết cho quá trình học tập, làm việc sau này của chúng em.

Nhờ những kiến thức sâu rộng và sự nhiệt tình của thầy trong lớp thực hành chúng em đã giúp chúng em có cơ hội thực hiện bài tập nhóm và nhiều kiến thức mới một cách hiệu quả, cũng như là thực hiện bài báo cáo cuối kỳ đạt được kết quả tốt. Tuy nhiên những kiến thức và kỹ năng về môn học này của chúng em vẫn còn nhiều hạn chế. Do đó bài báo cáo cuối kỳ của chúng em khó tránh khỏi những sai sót. Kính mong cô xem xét và góp ý giúp bài báo cáo cuối kỳ của chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn thầy! Chúng em xin chúc thầy luôn khỏe, vui vẻ và đạt được những thành công trong công tác giảng dạy.

MỤC LỤC

MỤC LỤC	3
DANH MỤC HÌNH ẢNH	5
DANH MỤC BẢNG BIỂU	7
CHƯƠNG I. GIỚI THIỆU VỀ ĐỀ TÀI.....	8
1. Mục tiêu đề tài	8
1.1. Đối tượng và phạm vi	8
1.2. Ý nghĩa	9
2. Giới thiệu các giải pháp IDS/IPS	9
2.1. Tổng quan về hệ thống mạng LAN	9
2.2. Mô hình Client – Server	11
2.3. IDS và IPS	14
2.3.1. IDS	14
2.3.2. IPS	16
2.4. Endpoint Security	18
2.5. Các hình thức tấn công mạng phổ biến	20
2.6. Các công cụ, phần mềm	21
CHƯƠNG II. XÂY DỰNG HỆ THỐNG	22
1. Thiết kế hệ thống LAN	22
1.1. Sơ đồ mạng	22
1.2. Sơ đồ demo	23
1.3. Bảng phân hoạch IP	23
1.4. Domain Controller	24
1.5. DHCP Server	24

1.6. Web Server	26
2. Triển khai IDS/IPS	26
2.1. Cài đặt Snort	26
2.2. Các rule IDS	28
2.3. Các rule IPS	28
3. Triển khai System Endpoint	28
3.1. Cài đặt Wazuh	28
3.2. Cấu hình Wazuh	30
4. Mô tả sơ đồ và bối cảnh	33
5. Kịch bản 1 (Ping ICMP)	33
6. Kịch bản 2 (Thăm dò Web Server bằng Curl)	35
7. Kịch bản 3 (Truy cập trái phép FTP)	36
CHƯƠNG III. KẾT LUẬN	38
1. Kết quả đạt được	38
2. Đánh giá	38
3. Các phương án, giải pháp bảo mật người dùng cuối	39
4. Kết luận	40
CHƯƠNG IV. TÀI LIỆU THAM KHẢO	41

DANH MỤC HÌNH ẢNH

Hình 1. Hệ thống mạng LAN	9
Hình 2. Mô hình Client - Server.....	11
Hình 3. IDS.....	14
Hình 4. IPS	16
Hình 5. Endpoint Security	18
Hình 6. DoS/DDoS.....	20
Hình 7. Brute-force Attack.....	20
Hình 8. Malware Injection	21
Hình 9. ARP Spoofing	21
Hình 10. Sơ đồ mạng.....	22
Hình 11. Sơ đồ Demo.....	23
Hình 12. Tên miền trên Serer	24
Hình 13. Thông tin máy Client nhận IP	24
Hình 14. Máy Client nhận IP từ Server.....	25
Hình 15. Truy cập Web Server trên Client.....	26
Hình 16. Cập nhật máy.....	26
Hình 17. Cài đặt Snort.....	26
Hình 18. Tải rule từ trang chủ	27
Hình 19. Giải nén file.....	27
Hình 20. Kiểm tra Snort	27
Hình 21. Một số rule IDS	28
Hình 22. Một số lệnh Iptables ngăn chặn tấn công.....	28
Hình 23. Cập nhật hệ thống.....	28
Hình 24. Tải gói Wazuh về máy	29
Hình 25. Chạy script cài đặt Wazuh.....	29
Hình 26. Thông tin đăng nhập.....	29
Hình 27. Tắt cập nhật phiên bản mới	29
Hình 28. Đăng nhập vào Wazuh	30

Hình 29. Mở file cấu hình ossec.conf	30
Hình 30. Thêm 2 file vào thư mục giám sát.....	31
Hình 31. Hệ thống ghi lại các hành vi trên thư mục giám sát.....	31
Hình 32. Tải 1 số phần mềm về máy.....	32
Hình 33. Hành vi tải phần mềm được hệ thống ghi lại	32
Hình 34. Trên máy Kali ping đến Ubuntu Server	34
Hình 35. Phát hiện Ping ICMP	34
Hình 36. Rule chặn Ping ICMP.....	34
Hình 37. Gửi gói tin thất bại	34
Hình 38. Truy xuất Web nội bộ.....	35
Hình 39. Phát hiện truy xuất Web trái phép.....	35
Hình 40. Lệnh chặn truy xuất Web	35
Hình 41. Truy xuất Web thất bại.....	36
Hình 42. Kết nối FTP đến Server.....	36
Hình 43. Phát hiện truy xuất FTP.....	36
Hình 44. Chặn kết nối FTP.....	36
Hình 45. Kết nối qua FTP thất bại	37

DANH MỤC BẢNG BIỂU

Bảng 1. So sánh Client - Server với P2P	13
Bảng 2. So sánh IDS, IPS và tường lửa	17
Bảng 3. So sánh ERD/EPP với các phần mềm Antivirus	19
Bảng 4. Phân hoạch IP	23

CHƯƠNG I. GIỚI THIỆU VỀ ĐỀ TÀI

1. Mục tiêu đề tài

Đề tài được thực hiện với mục tiêu thiết kế và triển khai một hệ thống mạng LAN hoàn chỉnh, đảm bảo tính ổn định và bảo mật cho hệ thống mạng nội bộ của doanh nghiệp hoặc tổ chức. Ngoài ra, nhóm cũng tiến hành triển khai các giải pháp an ninh mạng thông qua việc cấu hình hệ thống phát hiện và phòng chống xâm nhập (IPS/IDS) cũng như quản lý thiết bị đầu cuối nhằm giảm thiểu các nguy cơ tấn công từ bên ngoài và nội bộ. Đề tài giúp sinh viên nắm vững quy trình thiết kế, lắp đặt, cấu hình hệ thống mạng LAN, đồng thời biết cách xây dựng các chính sách bảo mật thiết thực, phục vụ cho công việc thực tế trong môi trường doanh nghiệp.

1.1. Đối tượng và phạm vi

1.1.1. Đối tượng nghiên cứu

Đối tượng nghiên cứu của đề tài là hệ thống mạng LAN nội bộ trong môi trường doanh nghiệp, gồm các thành phần như Server quản trị, các máy trạm Client, hệ thống thiết bị mạng (Switch, Router) và các thiết bị bảo mật mạng như IPS/IDS, Endpoint Security. Bên cạnh đó, đề tài cũng tập trung vào các loại hình tấn công mạng phổ biến mà doanh nghiệp có thể gặp phải, từ đó xây dựng các phương án phòng chống và xử lý sự cố phù hợp.

1.1.2. Phạm vi nghiên cứu

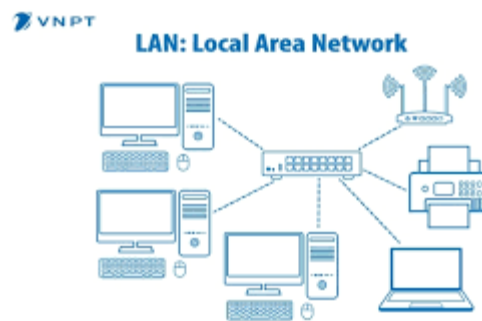
Phạm vi nghiên cứu của đề tài được giới hạn trong việc thiết kế hệ thống mạng LAN với mô hình Client-Server trên quy mô doanh nghiệp vừa và nhỏ. Đề tài thực hiện cài đặt, triển khai và kiểm thử hệ thống trong môi trường phòng lab mô phỏng, bao gồm việc cấu hình IPS/IDS với ít nhất 2 rule, thiết lập chính sách bảo vệ thiết bị đầu cuối và thực hiện 3 tình huống tấn công phổ biến để kiểm tra mức độ an toàn của hệ thống khi có và không có các giải pháp bảo vệ.

1.2. Ý nghĩa

Đề tài không chỉ giúp sinh viên củng cố và vận dụng kiến thức chuyên môn về thiết kế và quản trị mạng LAN mà còn rèn luyện kỹ năng xử lý tình huống, bảo mật mạng và phối hợp làm việc nhóm. Ngoài ra, việc mô phỏng và xử lý các tình huống tấn công thực tế sẽ trang bị cho sinh viên khả năng nhận diện và phản ứng kịp thời với các mối đe dọa trong môi trường mạng doanh nghiệp, đáp ứng tốt yêu cầu của công việc thực tế sau này.

2. Giới thiệu các giải pháp IDS/IPS

2.1. Tổng quan về hệ thống mạng LAN



Hình 1. Hệ thống mạng LAN

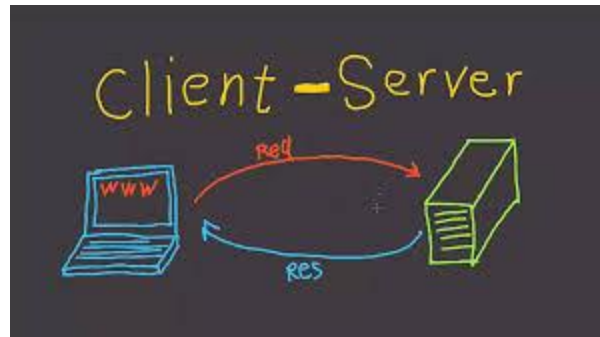
Mạng LAN (Local Area Network) là hệ thống mạng nội bộ kết nối các thiết bị như máy tính, máy in, thiết bị lưu trữ và các thiết bị mạng khác trong một phạm vi nhỏ như văn phòng, trường học hoặc tòa nhà. Mạng LAN giúp chia sẻ tài nguyên, dữ liệu và thiết bị ngoại vi một cách nhanh chóng và hiệu quả.

- Cấu trúc của hệ thống mạng LAN bao gồm các thành phần chính:
 - Switch: Kết nối các thiết bị trong mạng LAN và chuyển tiếp dữ liệu giữa chúng
 - Router: Kết nối mạng LAN với các mạng bên ngoài như Internet.
 - Server: Quản lý, cung cấp tài nguyên và dịch vụ cho các máy Client.
 - Client: Máy tính người dùng truy cập dịch vụ và dữ liệu từ Server.

Trong mạng LAN, dữ liệu được truyền qua các tầng trong mô hình OSI gồm 7 tầng: Physical, Data Link, Network, Transport, Session, Presentation và Application. Mô hình này giúp chuẩn hóa và phân chia các chức năng trong quá trình truyền dữ liệu giữa các thiết bị.

Mạng LAN đóng vai trò quan trọng trong doanh nghiệp vì giúp giảm chi phí kết nối, tăng hiệu suất làm việc nhóm và tăng khả năng quản lý hệ thống một cách tập trung.

2.2. Mô hình Client – Server



Hình 2. Mô hình Client - Server

Trong mô hình Client Server, máy khách và máy chủ giao tiếp với nhau thông qua các giao thức mạng. Giao thức là một tập hợp các quy tắc và quy chuẩn mà máy chủ và máy khách phải tuân theo để giao tiếp với nhau. Các giao thức phổ biến hiện nay bao gồm HTTPS, FTP, TCP/IP. Để lấy thông tin từ máy chủ, máy khách phải tuân theo giao thức do máy chủ cung cấp.

- Ưu điểm:

- **Khả năng kiểm soát tập trung:** Mô hình Client Server có khả năng kiểm soát tập trung. Điều này có nghĩa là tất cả các thông tin cần thiết đều được lưu trữ tại một máy chủ trung tâm. Nhờ đó, các nhà quản trị có thể dễ dàng kiểm soát mọi hoạt động của hệ thống, từ việc phân bổ tài nguyên đến xử lý sự cố.
- **Hiệu quả cao:** Máy chủ có thể xử lý các yêu cầu của nhiều máy khách cùng một lúc, giúp tăng hiệu quả sử dụng tài nguyên. Điều này là do máy chủ thường có cấu hình mạnh mẽ hơn máy khách và được kết nối với mạng 24/7.
- **Tính bảo mật:** Dữ liệu trên máy chủ có thể được bảo mật bằng các biện pháp hiện đại như tường lửa, mã hóa,... Điều này giúp bảo vệ dữ liệu của người dùng khỏi bị truy cập trái phép.
- **Khả năng mở rộng:** Mô hình Client-Server có thể được mở rộng dễ dàng bằng cách thêm các máy chủ mới. Điều này giúp đáp ứng nhu cầu ngày càng tăng của người dùng.

- **Khả năng truy cập:** Mô hình Client Server không phân biệt nền tảng hoặc vị trí. Mọi máy khách đều có thể kết nối với mạng máy tính, bất kể chúng chạy hệ điều hành gì hoặc nằm ở đâu. Điều này giúp tất cả nhân viên có thể truy cập thông tin công ty từ bất kỳ thiết bị nào, mà không cần sử dụng chế độ Terminal Mode hoặc bộ xử lý bổ sung.
- **Nhược điểm:**
 - **Tắc nghẽn lưu lượng:** Đây là nhược điểm lớn nhất của mô hình Client Server. Khi có quá nhiều máy khách yêu cầu thông tin từ cùng một máy chủ, kết nối có thể trở nên chậm hơn hoặc thậm chí bị sập. Điều này là do máy chủ phải xử lý quá nhiều yêu cầu cùng một lúc.
 - **Tính tập trung:** Đây vừa là ưu điểm vừa là nhược điểm. Tất cả dữ liệu đều được lưu trữ trên máy chủ, do đó nếu máy chủ gặp sự cố thì toàn bộ hệ thống sẽ bị ảnh hưởng. Điều này có thể dẫn đến mất dữ liệu, gián đoạn dịch vụ hoặc thậm chí là mất doanh thu.
 - **Phức tạp:** Mô hình Client-Server có cấu trúc phức tạp hơn các mô hình mạng khác, do đó khó triển khai và quản lý. Máy chủ hoạt động liên tục khi triển khai. Điều này đòi hỏi phải bảo trì hệ thống thường xuyên. Khi phát sinh vấn đề, cần phải giải quyết ngay lập tức. Do đó, cần có một nhà quản lý mạng chuyên dụng để đảm bảo máy chủ hoạt động ổn định trong suốt quá trình triển khai và sử dụng.
 - **Kém linh hoạt:** Mô hình Client-Server có thể không phù hợp với các ứng dụng yêu cầu tính linh hoạt cao, chẳng hạn như các ứng dụng di động.
 - **Chi phí:** Chi phí cao là một nhược điểm của mô hình Client Server. Điều này là do máy chủ cần phải có phần cứng và phần mềm mạnh mẽ để xử lý các yêu cầu từ máy khách. Do đó, chi phí thiết lập và duy trì máy chủ thường khá cao, có thể vượt quá khả năng chi trả của nhiều doanh nghiệp nhỏ.

Nhìn chung, mô hình Client-Server là một mô hình mạng máy tính hiệu quả và bảo mật. Tuy nhiên, cần lưu ý đến các nhược điểm của mô hình này để có thể triển khai và sử dụng mô hình một cách tốt nhất.

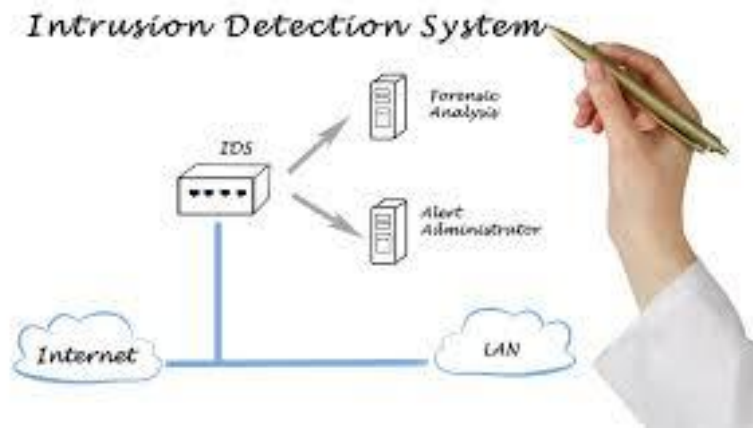
❖ So sánh giữa Client Server với Peer to Peer(P2P)

Bảng 1. So sánh Client - Server với P2P

Client – Server	Peer – to - Peer
Trong mạng client-server, máy khách và máy chủ được phân biệt rõ ràng.	Trong mạng P2P, máy khách và máy chủ là một.
Mạng client-server là mô hình mạng máy tính trong đó dữ liệu được lưu trữ tập trung trên máy chủ và được chia sẻ cho các máy khách.	Mạng ngang hàng (P2P) tập trung vào việc kết nối các máy tính với nhau.
Trong mạng client-server, máy chủ tập trung là nơi lưu trữ dữ liệu.	Trong mạng P2P, mỗi máy tính đều có dữ liệu của riêng mình.
Trong mạng client-server, máy chủ sẽ xử lý và phản hồi lại yêu cầu của máy khách.	Tất cả các node trong mạng P2P đều có thể đóng vai trò là cả máy khách và máy chủ.v
Chi phí đắt hơn	Chi phí rẻ hơn
Ổn định hơn	Không ổn định bằng
Dùng cho cả các mạng nhỏ lẫn lớn	Mạng P2P thường phù hợp cho các mạng nhỏ, với số lượng máy tính nhỏ hơn 10.

2.3. IDS và IPS

2.3.1. IDS



Hình 3. IDS

Hệ thống phát hiện xâm nhập – IDS là viết tắt của Intrusion Detection System. Đây là một phần mềm ứng dụng hoặc thiết bị được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống.

- **Hiện nay có hai loại hệ thống IDS chính:**

- **NIDS (Network Intrusion Detection System)** – Hệ thống phát hiện xâm nhập mạng, hệ thống sẽ tập hợp các gói tin để phân tích sâu bên trong nhằm xác định các mối đe dọa tiềm tàng mà không làm thay đổi cấu trúc của gói tin.
- **HIDS (Host-based Intrusion Detection System)** – Hệ thống phát hiện xâm nhập dựa trên máy chủ, được cài đặt trực tiếp trên các máy tính cần theo dõi. HIDS giám sát lưu lượng đến và đi từ thiết bị để cảnh báo người dùng về những xâm nhập trái phép.

Các hệ thống IDS hiện đại được xây dựng để thu thập lưu lượng mạng từ mọi thiết bị thông qua cả NIDS và HIDS. Vì vậy có thể cải thiện đáng kể khả năng phát hiện xâm nhập trên hệ thống.

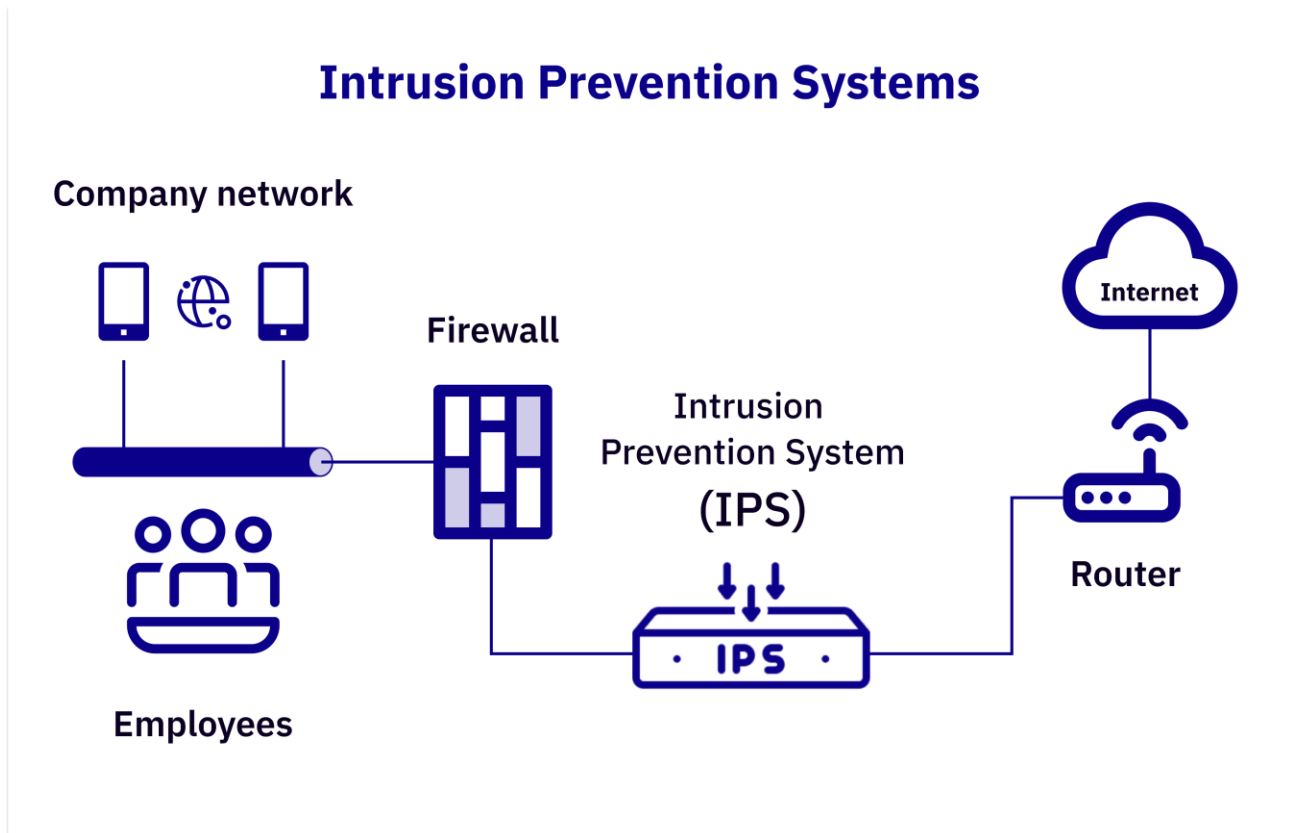
- **Ưu điểm:**

- IDS thích hợp sử dụng cho việc thu thập dữ liệu và bằng chứng của các cuộc tấn công mạng. Nhờ đó việc kiểm tra, điều tra và xử lý sự cố phát sinh dễ dàng, chính xác và kịp thời nhất.
- IDS giúp người dùng có cái toàn diện về hệ thống lưu lượng mạng. Bất cứ hoạt động khả nghi nào đều có thể được phát hiện nhanh chóng nhất.
- IDS giúp người dùng phòng ngừa, phản ứng kịp thời để có biện pháp chống lại lại các hoạt động tấn công bất ngờ có thể diễn ra trên hệ thống mạng.
- Các số liệu, thông tin IDS ghi chép, lưu trữ có thể được sử dụng để nâng cao chất lượng hệ thống bảo mật. Chúng cũng là cơ sở để đánh giá rủi ro các cuộc tấn công mạng trong tương lai.

- **Nhược điểm:**

- Người dùng cần điều chỉnh cấu hình IDS phù hợp nếu không sẽ xảy ra tình trạng báo động nhầm, báo động giả.
- Một số hệ thống IDS ngăn cản người dùng ở thiết bị khác truy cập vào hệ thống mạng.
- Khả năng phân tích lưu lượng traffic mã hóa khá thấp và chưa hiệu quả.
- Chi phí cài đặt hệ thống ISD khá cao và yêu cầu nhiều kỹ thuật phức tạp. Bạn cần cân nhắc nếu khả năng tài chính của doanh nghiệp hạn chế.

2.3.2. IPS



Hình 4. IPS

IDS là một hệ thống phân tích lưu lượng mạng để tìm các thông tin khớp với những mẫu tấn công đã biết trước. Mặt khác, IPS có khả năng phân tích các packet và ngăn chặn việc gửi packet dựa trên những loại hình tấn công mà hệ thống phát hiện được. Từ đó có thể nhanh chóng ngăn chặn tấn công vào hệ thống.

❖ So sánh IDS, IPS và tường lửa

Bảng 2. So sánh IDS, IPS và tường lửa

	IDS	IPS	Tường lửa
Mục tiêu	Tập trung vào việc phát hiện sự xâm nhập, báo cáo về những hoạt động bất thường trên hệ thống.	Ngăn chặn các mối đe dọa tiềm ẩn, các cuộc tấn công mạng trước khi gây ra hậu quả nghiêm trọng cho hệ thống.	Kiểm soát quyền truy cập mạng, ngăn chặn các cuộc tấn công từ bên ngoài hệ thống.
Chức năng	Là công cụ giám sát và phát hiện các hoạt động xâm nhập trên mạng máy tính, phát ra cảnh báo khi nhận thấy dấu hiệu đáng ngờ.	Là công cụ nhận diện, tự động ngăn chặn việc phát tán các hành vi xâm nhập.	Là công cụ theo dõi lưu lượng mạng và quyết định gói tin dữ liệu có được chuyển tiếp hay không dựa trên các quy tắc định trước.
Hoạt động	Tiến hành giám sát dữ liệu và hoạt động mạng để xác định các truy cập trái phép.	Tự động chặn kết nối, cắt ngắn chuỗi hoặc xóa các gói tin dữ liệu tiềm ẩn khả năng xâm nhập hệ thống.	Hoạt động ở cấp độ gói tin, thực hiện kiểm tra địa chỉ IP, cổng mạng và các thông tin khác trong tiêu đề gói tin trước khi chuyển tiếp gói tin này.

2.4. Endpoint Security



Hình 5. Endpoint Security

Endpoint Security (bảo mật thiết bị đầu cuối) là hệ thống toàn diện các biện pháp ngăn chặn, phát hiện và phản ứng trên mọi thiết bị kết nối mạng doanh nghiệp, từ PC, laptop, server, máy ảo (VM) đến smartphone và thiết bị IoT.

EDR (Endpoint Detection & Response) là một thành phần cốt lõi của Endpoint Security. EDR không thay thế mà tăng cường khả năng phát hiện, phân tích và phản ứng trước các cuộc tấn công phức tạp như APT, ransomware hay zero-day nhắm vào thiết bị đầu cuối.

Sự kết hợp giữa EPP (Endpoint Protection Platform) và EDR tạo nên hạt nhân công nghệ bảo mật hiện đại. Khi tích hợp với các hệ thống SIEM/SOC, giải pháp này phát triển thành XDR (Extended Detection & Response), mang lại khả năng bảo vệ rộng hơn.

❖ So sánh ERD/EPP với các phần mềm Antivirus

Bảng 3. So sánh ERD/EPP với các phần mềm Antivirus

	Phần mềm Antivirus	ERD/EPP
Phương pháp phát hiện	Dò chữ ký (signature)	Phân tích hành vi, AI/ML, threat-intel realtime
Phạm vi hiển thị (visibility)	Chỉ 1 thiết bị	Tập trung đa thiết bị + network flow
Khả năng phản ứng	Cảnh báo → chờ người dùng	Tự động cô lập thiết bị, rollback ransomware, orchestration tới firewall/SOAR
Tích hợp	Độc lập	Kết nối SIEM, IAM, Zero-Trust, ticket ITSM
Quản trị	Cập nhật thủ công/định kỳ	Console cloud, agent self-update, chính sách tùy nhóm AD/Azure AD

2.5. Các hình thức tấn công mạng phổ biến



Hình 6. DoS/DDoS

DoS/DDoS Attack: Tấn công làm tê liệt hệ thống bằng cách gửi lượng lớn gói tin giả mạo khiến tài nguyên hệ thống quá tải.



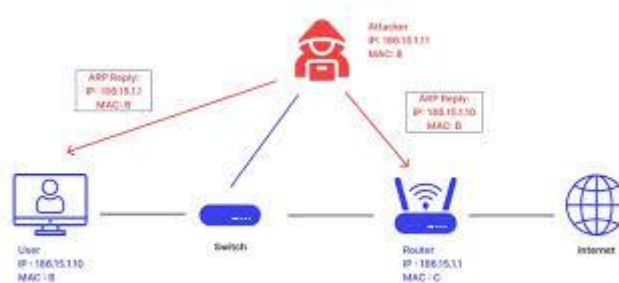
Hình 7. Brute-force Attack

Brute-force Attack: Tấn công đoán mật khẩu thông qua việc thử hàng loạt mật khẩu phổ biến cho đến khi đúng.



Hình 8. Malware Injection

Malware Injection: Cây mã độc vào hệ thống hoặc máy tính người dùng để đánh cắp dữ liệu hoặc phá hoại.



Hình 9. ARP Spoofing

ARP Spoofing: Giả mạo địa chỉ MAC để chặn và đánh cắp dữ liệu giữa thiết bị gửi và nhận.

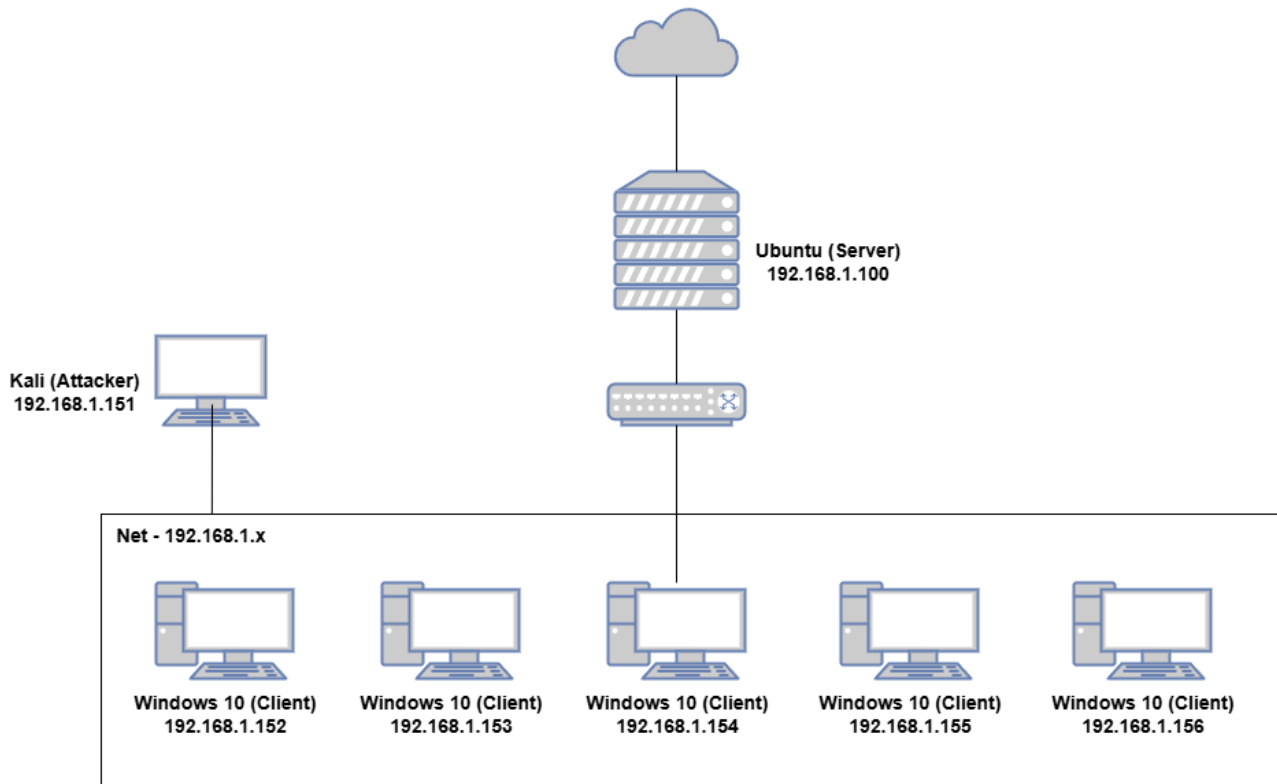
2.6. Các công cụ, phần mềm

- **Wireshark:** Phân tích, kiểm tra lưu lượng mạng, hỗ trợ debug và phát hiện bất thường.
- **Snort/Suricata:** Cài đặt IPS/IDS, thiết lập rule giám sát và ngăn chặn các mối đe dọa.
- **ESET Endpoint Security:** Bảo vệ thiết bị đầu cuối, thiết lập chính sách bảo vệ máy Client.
- **Cisco Packet Tracer/VMware/EVE-NG/GNS3:** Mô phỏng mô hình mạng, thử nghiệm cấu hình và kiểm tra kịch bản tấn công.

CHƯƠNG II. XÂY DỰNG HỆ THỐNG

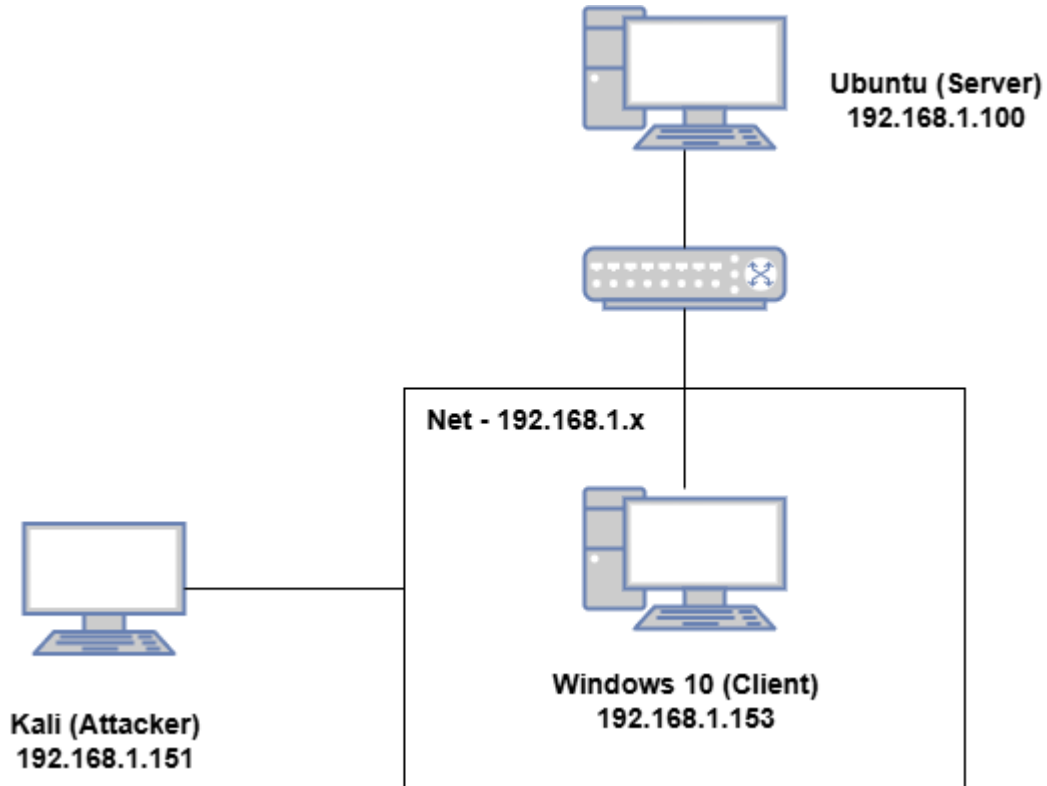
1. Thiết kế hệ thống LAN

1.1. Sơ đồ mạng



Hình 10. Sơ đồ mạng

1.2. Sơ đồ demo



Hình 11. Sơ đồ Demo

1.3. Bảng phân hoạch IP

Bảng 4. Phân hoạch IP

Thiết bị	Địa chỉ IP	Chức năng
Ubuntu Server	192.168.1.100	Giám sát, kiểm tra lưu lượng mạng
Kali Linux (Attacker)	192.168.1.151	Thực hiện tấn công
Windows 10 Client 01	192.168.1.152	Máy bị tấn công
Windows 10 Client 02	192.168.1.153	Máy bị tấn công
Windows 10 Client 03	192.168.1.154	Máy bị tấn công
Windows 10 Client 04	192.168.1.155	Máy bị tấn công
Windows 10 Client 05	192.168.1.156	Máy bị tấn công
Switch		Chuyển mạch mạng LAN nội bộ

1.4. Domain Controller

- Tên miền đã tạo group7.com.

```
doanh@ubuntu:~$ sudo samba-tool domain level show
Domain and forest function level for domain 'DC=group7,DC=com'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Hình 12. Tên miền trên Server

1.5. DHCP Server

- Trên hệ thống DHCP Server hiển thị các máy Client nhận DHCP.

```
lease 192.168.1.153 {
  starts 1 2025/07/21 15:33:38;
  ends 1 2025/07/21 15:43:38;
  cltt 1 2025/07/21 15:33:38;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 00:0c:29:0d:19:59;
  uid "\001\000\014)\015\031Y";
  set vendor-class-identifier = "MSFT 5.0";
  client-hostname "DESKTOP-NH8HM2J";
}
root@ubuntu:~#
```

Hình 13. Thông tin máy Client nhận IP

- Máy Client xin cấp IP từ Server thành công.

```

Command Prompt
Control-C
^C
C:\Users\Admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-NH8HM2J
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : group7.com

Ethernet adapter Ethernet0:

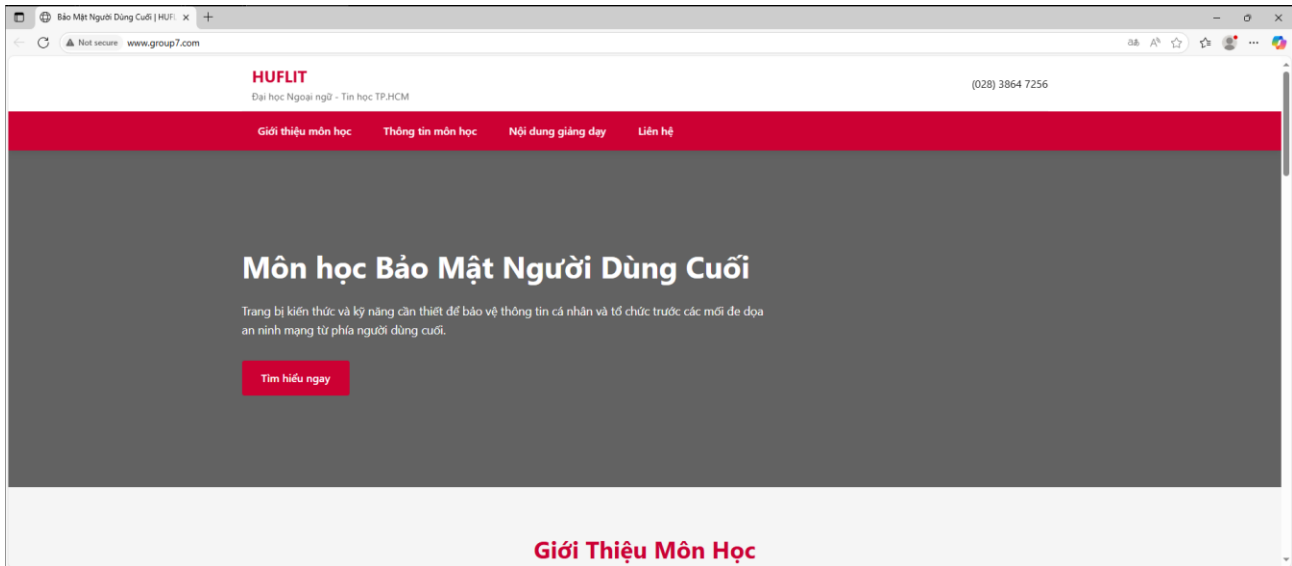
    Connection-specific DNS Suffix  . : group7.com
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-0C-29-0D-19-59
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2d14:b420:269c:b602%14(Preferred)
    IPv4 Address. . . . . : 192.168.1.153(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Tuesday, July 22, 2025 12:23:22 AM
    Lease Expires . . . . . : Tuesday, July 22, 2025 12:33:22 AM
    Default Gateway . . . . . : 192.168.1.100
    DHCP Server . . . . . : 192.168.1.100
    DHCPv6 IAID . . . . . : 100666409
    DHCPv6 Client DUID. . . . . : 00-01-00-01-30-0F-80-AB-00-0C-29-0D-19-59
    DNS Servers . . . . . : 192.168.1.100
                           8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Admin>
    
```

Hình 14. Máy Client nhận IP từ Server

1.6. Web Server

- Từ các máy Client thuộc mạng LAN đều có thể truy cập Web Server.

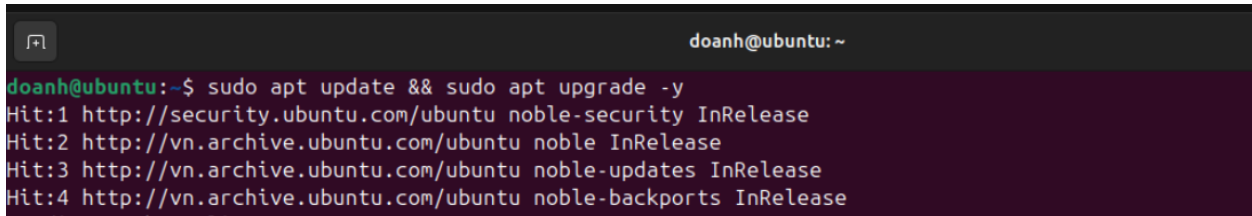


Hình 15. Truy cập Web Server trên Client

2. Triển khai IDS/IPS

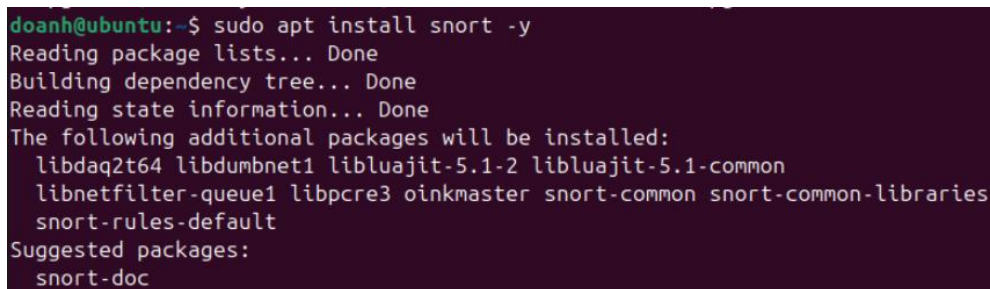
2.1. Cài đặt Snort

- Cập nhật danh sách các gói và nâng cấp lên phiên bản mới.



Hình 16. Cập nhật máy

- Cài đặt Snort.



Hình 17. Cài đặt Snort

- Tải về bộ rule cộng đồng từ trang chủ Snort.

```
doanh@ubuntu:~$ wget https://www.snort.org/rules/community -O ~/community.tar.gz
--2025-06-21 15:55:32-- https://www.snort.org/rules/community
Resolving www.snort.org (www.snort.org)... 104.16.92.19, 104.16.91.19, 2606:4700
::6810:5b13, ...
Connecting to www.snort.org (www.snort.org)|104.16.92.19|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files
/000/048/320/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-
Amz-Credential=AKIAU7AK5ITMF2NAGF7Y%2F20250621%2Fus-east-1%2Fs3%2Faws4_request&X-
Amz-Date=20250621T085532Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Sig-
nature=4b1a70227ed0f3841f99546f5cb1236ce8a5530f4846bcbef5bb14cc923096f6 [followi
ng]
```

Hình 18. Tải rule từ trang chủ

- Giải nén file rule vừa tải về và sao chép các rule vào thư mục cấu hình của Snort.

```
doanh@ubuntu:~$ sudo tar -xvf ~/community.tar.gz -C ~/
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
doanh@ubuntu:~$
```

Hình 19. Giải nén file

- Kiểm tra cấu hình Snort.

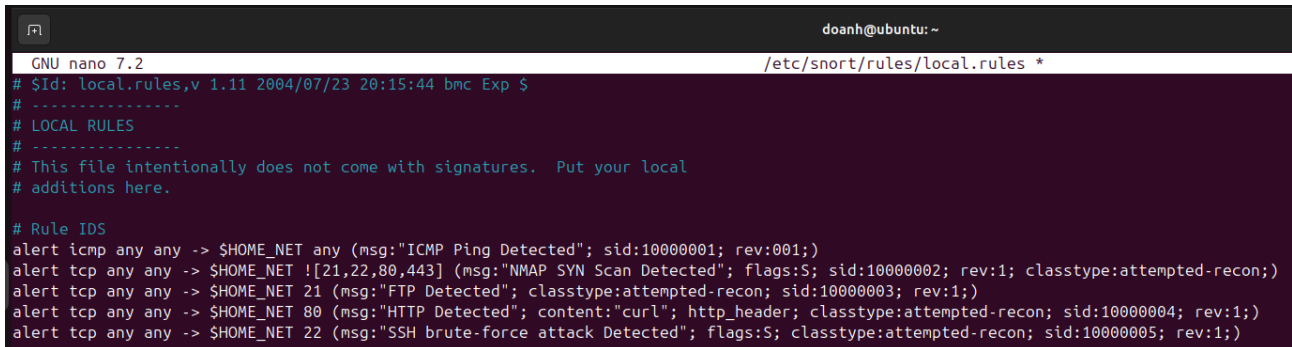
```
doanh@ubuntu:~$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
```

Hình 20. Kiểm tra Snort

2.2. Các rule IDS

- Viết một số rule khi phát hiện có tấn công từ bên ngoài.



```

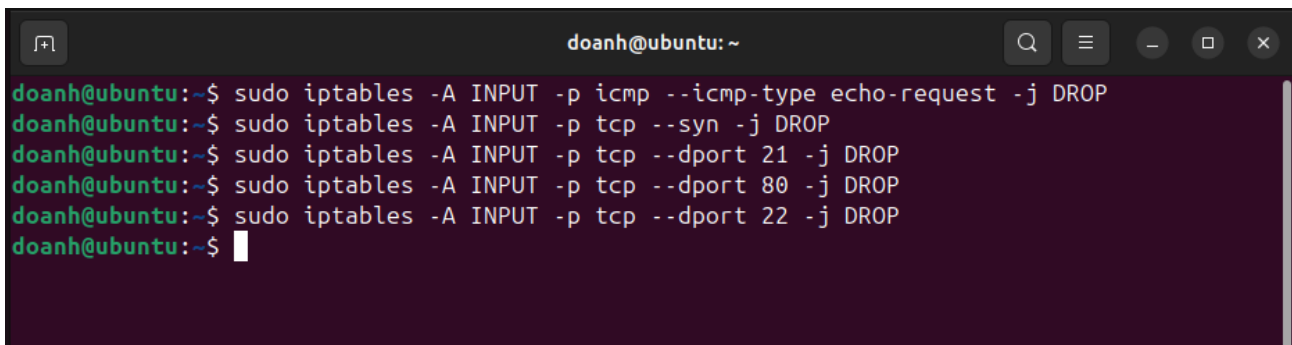
doanh@ubuntu: ~
GNU nano 7.2 /etc/snort/rules/local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

# Rule IDS
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:10000001; rev:001;)
alert tcp any any -> $HOME_NET ![21,22,80,443] (msg:"NMAP SYN Scan Detected"; flags:S; sid:10000002; rev:1; classtype:attempted-recon;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP Detected"; classtype:attempted-recon; sid:10000003; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP Detected"; content:"curl"; http_header; classtype:attempted-recon; sid:10000004; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH brute-force attack Detected"; flags:S; classtype:attempted-recon; sid:10000005; rev:1;)
  
```

Hình 21. Một số rule IDS

2.3. Các rule IPS

- Viết 1 số lệnh Iptables để chặn các cuộc tấn công.



```

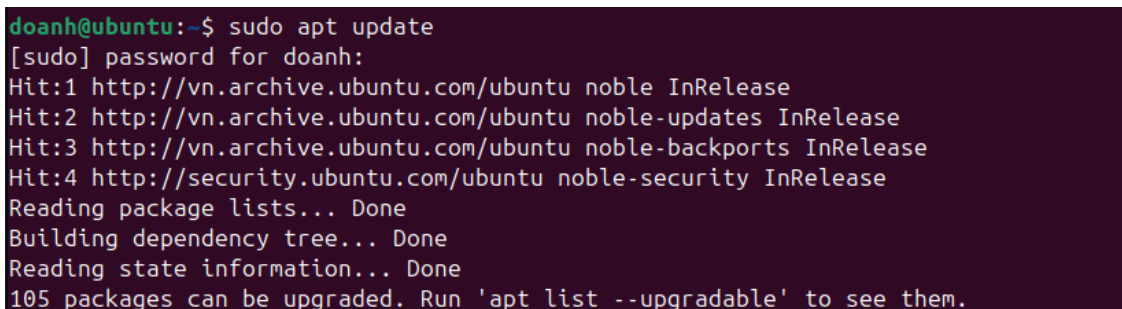
doanh@ubuntu: ~
doanh@ubuntu:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
doanh@ubuntu:~$ sudo iptables -A INPUT -p tcp --syn -j DROP
doanh@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 21 -j DROP
doanh@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
doanh@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
doanh@ubuntu:~$
  
```

Hình 22. Một số lệnh Iptables ngăn chặn tấn công

3. Triển khai System Endpoint

3.1. Cài đặt Wazuh

- Cập nhật hệ thống.



```

doanh@ubuntu:~$ sudo apt update
[sudo] password for doanh:
Hit:1 http://vn.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
105 packages can be upgraded. Run 'apt list --upgradable' to see them.
  
```

Hình 23. Cập nhật hệ thống

- Tải Wazuh về máy.

```
doanh@ubuntu:~$ curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
```

Hình 24. Tải gói Wazuh về máy

- Chạy script cài đặt Wazuh.

```
doanh@ubuntu:~$ sudo bash ./wazuh-install.sh -a
20/07/2025 01:42:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
20/07/2025 01:42:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
20/07/2025 01:42:13 INFO: Verifying that your system meets the recommended minimum hardware requirements.
20/07/2025 01:42:13 INFO: Wazuh web interface port will be 443.
```

Hình 25. Chạy script cài đặt Wazuh

- Tài khoản và mật khẩu dùng để truy cập Wazuh.

```
22/07/2025 04:01:15 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: XpUWEuw.SaWeL90GYLXCGI*H10Jgw0a+
22/07/2025 04:01:15 INFO: --- Dependencies ----
22/07/2025 04:01:15 INFO: Removing gawk.
22/07/2025 04:01:20 INFO: Installation finished.
```

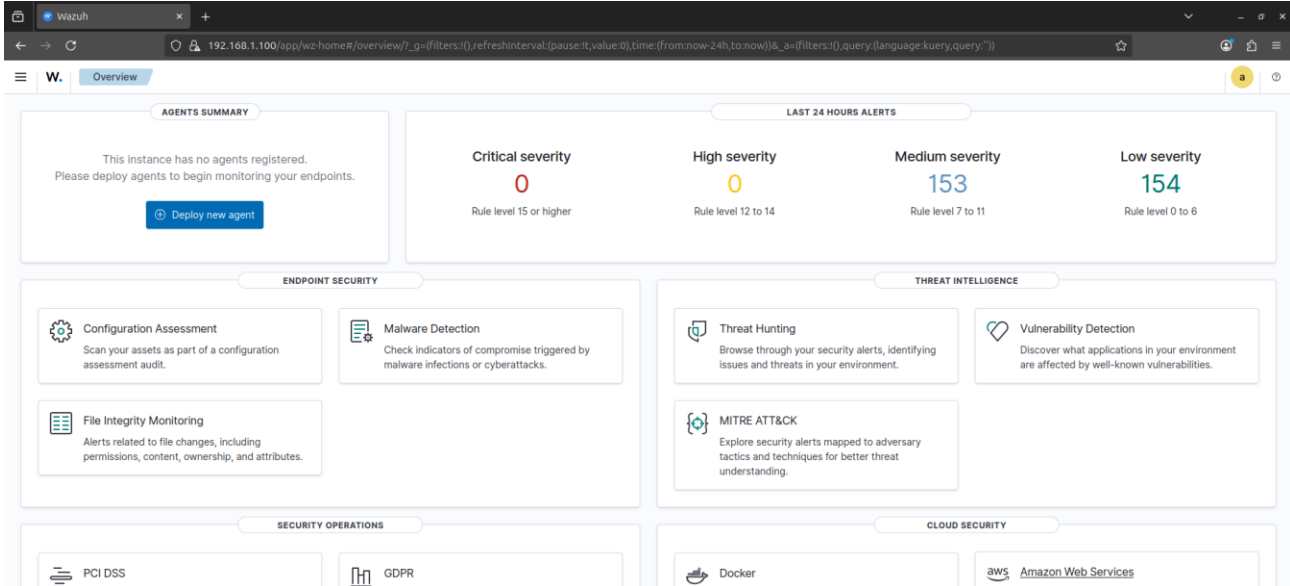
Hình 26. Thông tin đăng nhập

- Tắt cập nhật Wazuh để tránh xung đột.

```
root@ubuntu:/home/doanh# sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list
apt update
Hit:1 http://vn.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
```

Hình 27. Tắt cập nhật phiên bản mới

- Truy cập vào dashboard Wazuh.



Hình 28. Đăng nhập vào Wazuh

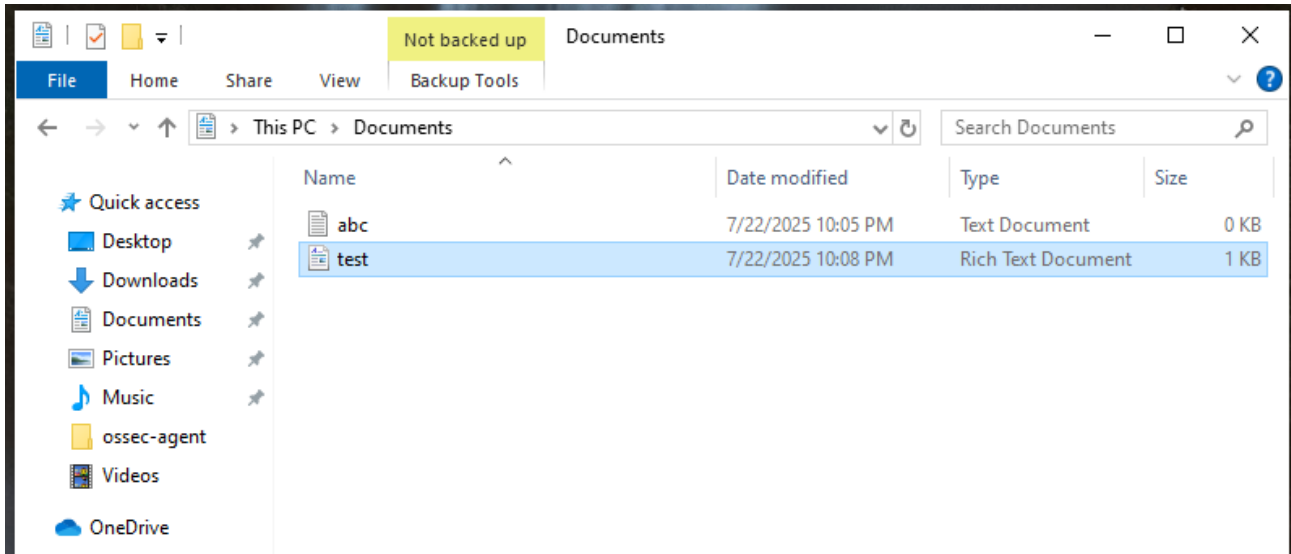
3.2. Cấu hình Wazuh

- Mở file ossec.conf trên Agent và thêm một số lệnh giúp giám sát người dùng.



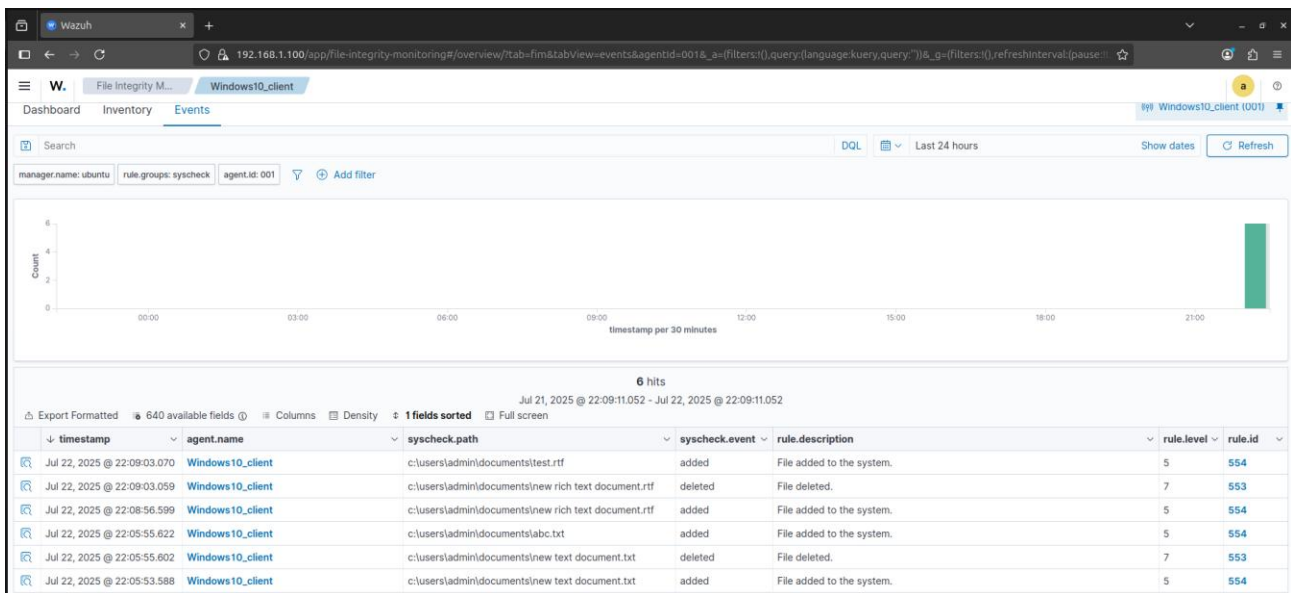
Hình 29. Mở file cấu hình ossec.conf

- Thực hiện tạo 2 file bất kỳ trên thư mục giám sát.



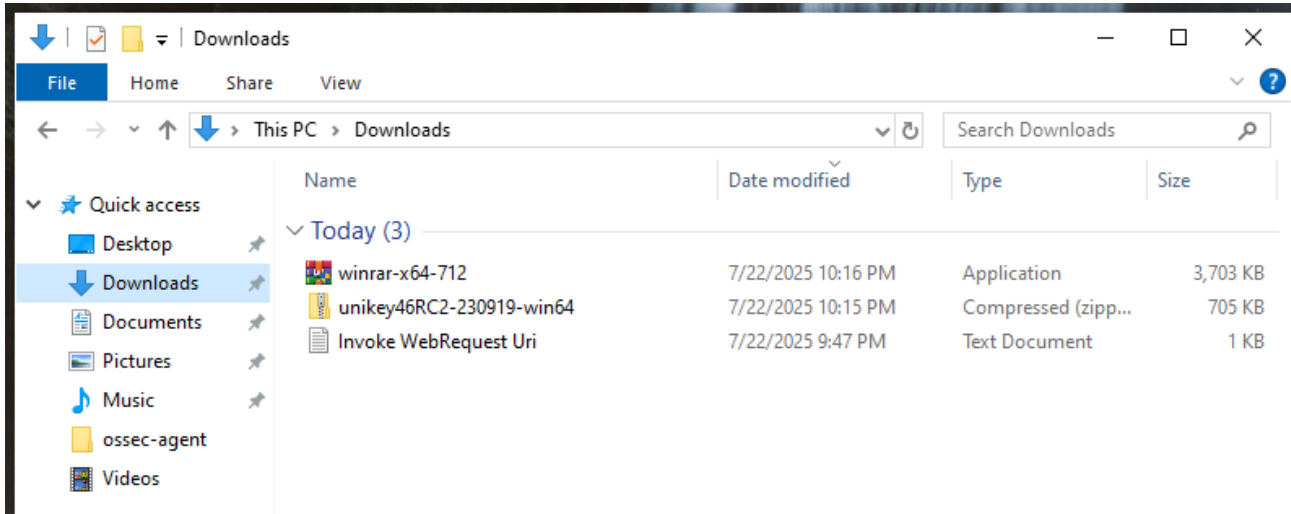
Hình 30. Thêm 2 file vào thư mục giám sát

- Hệ thống lúc này sẽ ghi nhận lại hành vi vừa thực hiện trong thư mục giám sát.



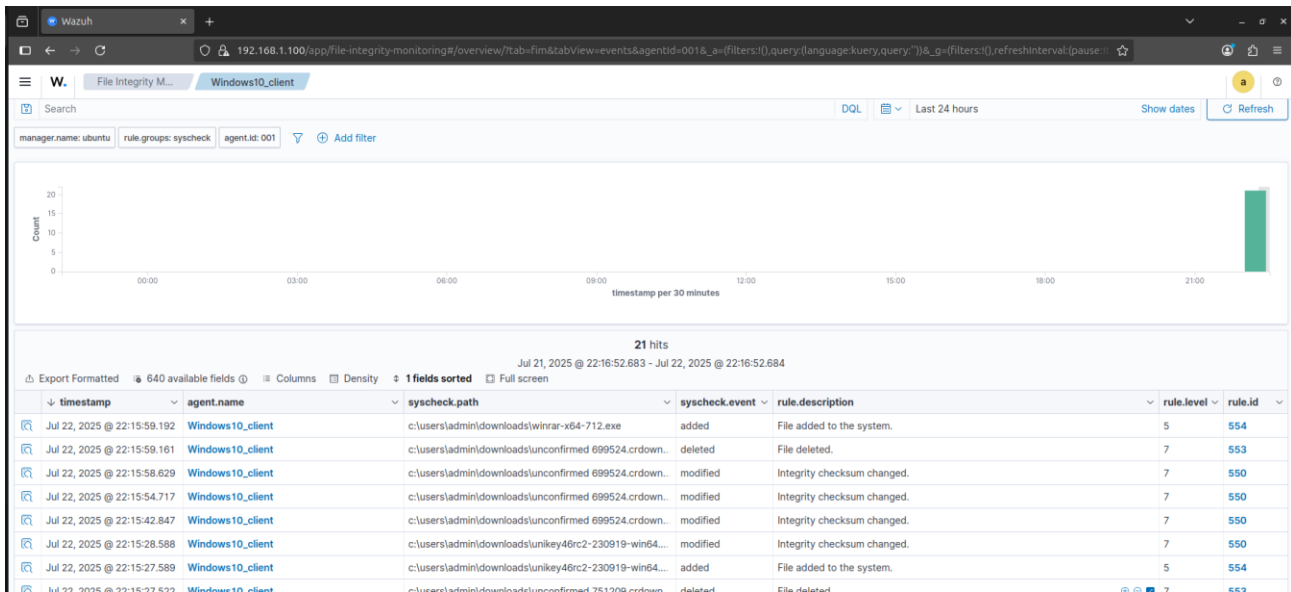
Hình 31. Hệ thống ghi lại các hành vi trên thư mục giám sát

- Tải 1 số phần mềm bất kỳ về máy.



Hình 32. Tải 1 số phần mềm về máy

- Hệ thống lúc này sẽ ghi nhận lại hành vi thực hiện tải phần mềm đó.



Hình 33. Hành vi tải phần mềm được hệ thống ghi lại

4. Mô tả sơ đồ và bối cảnh

Hệ thống mạng nội bộ của doanh nghiệp được triển khai với các thành phần chính gồm:

- Attacker: một máy tính cài hệ điều hành Kali Linux, đóng vai trò kẻ tấn công.
- Ubuntu Server: máy chủ cài đặt dịch vụ Snort để giám sát và ngăn chặn các cuộc tấn công từ mạng nội bộ hoặc bên ngoài. Máy chủ này đồng thời cung cấp các dịch vụ mạng như DNS, DHCP, Web Server cho các máy trạm.
- Client: các máy tính Windows 10 của người dùng trong mạng LAN, sử dụng các dịch vụ nội bộ từ server.
- Switch: thiết bị kết nối tất cả các máy tính và server lại với nhau trong cùng một hệ thống mạng nội bộ.
- Router và Cloud: đại diện cho kết nối ra internet hoặc mạng bên ngoài.

Toàn bộ các thiết bị nội bộ được kết nối qua switch và thông ra ngoài qua router.

Kẻ tấn công từ máy Kali Linux cố gắng:

- Kết nối thử vào dịch vụ FTP để dò mật khẩu hoặc truy cập trái phép.
- Thăm dò dịch vụ web đang chạy trên Ubuntu Server để thu thập thông tin hoặc khai thác lỗ hổng.
- Tấn công Brute-Force để dò mật khẩu người dùng.

5. Kịch bản 1 (Ping ICMP)

- Kẻ tấn công thực hiện các gói ping đến Ubuntu Server với mục đích kiểm tra trạng thái hoạt động và phản hồi mạng. Máy chủ Ubuntu Server với hệ thống Snort đang hoạt động đã nhanh chóng phát hiện ra các gói ICMP echo request và hiển thị cảnh báo trên console. Quản trị viên nhận diện dấu hiệu dò quét mạng và tiến hành cấu hình chặn toàn bộ gói ICMP echo request gửi đến server.

- Trên máy tấn công thực hiện ping tới máy server.

```
(kali㉿kali)-[~]
$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.572 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.559 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.458 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.400 ms
64 bytes from 192.168.1.100: icmp_seq=5 ttl=64 time=0.490 ms
64 bytes from 192.168.1.100: icmp_seq=6 ttl=64 time=0.400 ms
```

Hình 34. Trên máy Kali ping đến Ubuntu Server

- Hệ thống sẽ ghi nhận cảnh báo.

```
root@ubuntu:~# snort -q -A console -c /etc/snort/snort.conf -i ens33
07/22-03:10:40.704929  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.152 -> 192.168.1.100
07/22-03:10:40.705023  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.100 -> 192.168.1.152
07/22-03:10:41.711779  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.152 -> 192.168.1.100
07/22-03:10:41.711877  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.100 -> 192.168.1.152
07/22-03:10:42.736356  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.152 -> 192.168.1.100
07/22-03:10:42.736438  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.100 -> 192.168.1.152
07/22-03:10:43.759420  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.152 -> 192.168.1.100
07/22-03:10:43.759485  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.100 -> 192.168.1.152
```

Hình 35. Phát hiện Ping ICMP

- Thực hiện lệnh iptables chặn tấn công.

```
root@ubuntu:/home/doanh# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
root@ubuntu:/home/doanh#
```

Hình 36. Rule chặn Ping ICMP

- Máy tấn công bây giờ không thể gửi gói tin được nữa.

```
(kali㉿kali)-[~]
$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
— 192.168.1.100 ping statistics —
48 packets transmitted, 0 received, 100% packet loss, time 48109ms
```

Hình 37. Gửi gói tin thất bại

6. Kịch bản 2 (Thăm dò Web Server bằng Curl)

- Ở bước tiếp theo, kẻ tấn công sử dụng Curl để gửi yêu cầu HTTP đến máy chủ, thăm dò dịch vụ web và kiểm tra phản hồi từ server. Ngay lập tức, Snort trên máy chủ nhận biết các yêu cầu HTTP gửi từ Curl dựa vào thông tin trong HTTP header và phát đi cảnh báo trên console. Để ngăn chặn khả năng khai thác sâu vào ứng dụng web, quản trị viên thiết lập chặn các kết nối đến cổng dịch vụ HTTP từ bên ngoài.
- Trên máy tấn công thực hiện truy xuất Web Server.

```
(kali@kali)-[~]
$ curl http://www.group7.com
<!DOCTYPE html>
<html lang="vi">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Bảo Mật Người Dùng Cuối | HUFLIT</title>
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css">
  <style>
    :root {
      --huflit-red: #cc0033;
      --huflit-dark: #1a1a1a;
      --huflit-light: #f5f5f5;
      --huflit-blue: #0066cc;
    }

    * {
      margin: 0;
      padding: 0;
      box-sizing: border-box;
      font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
    }

    body {
      background-color: var(--huflit-light);
      color: var(--huflit-dark);
      line-height: 1.6;
    }
  </style>
</head>
```

Hình 38. Truy xuất Web nội bộ

- Hệ thống sẽ ghi nhận cảnh báo.

```
root@ubuntu:~# snort -q -A console -c /etc/snort/snort.conf -t ens33
07/22-03:12:39.068840  [**] [1:10000001:1] ICMP Ping Detected [**] [Priority: 0] [IPV6-ICMP] fe80::20c:29ff:fe16:2798 -> ff02::2
07/22-03:12:42.947763  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:68 -> 255.255.255.255:67
07/22-03:12:43.862019  [**] [1:10000004:1] HTTP Detected [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.152:51580 -> 192.168.1.100:80
```

Hình 39. Phát hiện truy xuất Web trái phép

- Thực hiện lệnh iptables chặn tấn công.

```
root@ubuntu:/home/doanh# iptables -A INPUT -p tcp --dport 80 -j DROP
root@ubuntu:/home/doanh#
```

Hình 40. Lệnh chặn truy xuất Web

- Máy tấn công bây giờ không thể gửi truy xuất được nữa.

```
(kali@kali)-[~]
$ curl http://www.group7.com
^C
```

Hình 41. Truy xuất Web thất bại

7. Kịch bản 3 (Truy cập trái phép FTP)

- Kẻ tấn công thực hiện kết nối đến dịch vụ FTP của Ubuntu Server mà không có tài khoản hợp lệ, với mục đích kiểm tra cổng dịch vụ và dò đoán thông tin đăng nhập. Hành động này tiếp tục được hệ thống Snort phát hiện với cảnh báo về truy cập trái phép vào cổng FTP. Nhằm đảm bảo an toàn cho dịch vụ FTP và tránh nguy cơ bị khai thác, quản trị viên thực hiện chặn hoàn toàn kết nối đến cổng 21 từ bên ngoài.
- Trên máy tấn công thực hiện kết nối đến máy server.

```
(kali@kali)-[~]
$ ftp 192.168.1.100
Connected to 192.168.1.100.
220 (vsFTPD 3.0.5)
Name (192.168.1.100:kali):
```

Hình 42. Kết nối FTP đến Server

- Hệ thống sẽ ghi nhận cảnh báo.

```
root@ubuntu:~# snort -q -A console -c /etc/snort/snort.conf -i ens33
07/22-03:14:21.981598  [**] [1:10000003:1] FTP Detected [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.152:55822 -> 192.168.1.100:21
07/22-03:14:21.981909  [**] [1:10000003:1] FTP Detected [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.152:55822 -> 192.168.1.100:21
07/22-03:14:21.987862  [**] [1:10000003:1] FTP Detected [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.1.152:55822 -> 192.168.1.100:21
```

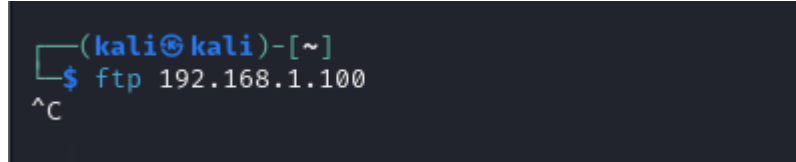
Hình 43. Phát hiện truy xuất FTP

- Thực hiện lệnh iptables chặn tấn công.

```
root@ubuntu:/home/doanh# iptables -A INPUT -p tcp --dport 21 -j DROP
root@ubuntu:/home/doanh#
```

Hình 44. Chặn kết nối FTP

- Máy tấn công bây giờ không thể kết nối đến được nữa.



```
(kali㉿kali)-[~]  
$ ftp 192.168.1.100  
^C
```

Hình 45. Kết nối qua FTP thất bại

CHƯƠNG III. KẾT LUẬN

1. Kết quả đạt được

Snort: <https://youtu.be/Nmv-YLeFY3c>

Wazuh: <https://youtu.be/dPxvNI5XSq4>

Demo tấn công: https://youtu.be/_k-SoOkjVBo

2. Đánh giá

Qua quá trình thực hiện đề tài, nhóm đã hoàn thành việc xây dựng một hệ thống mạng LAN theo mô hình Client-Server cơ bản, triển khai các thành phần mạng quan trọng như DHCP Server, Domain Controller, Web Server và đặc biệt là các giải pháp bảo mật bao gồm IDS/IPS (Snort) và Endpoint Security (Wazuh). Các kịch bản mô phỏng tấn công thực tế như Ping ICMP, truy xuất Web trái phép, và truy cập FTP không hợp lệ đã được thực hiện và hệ thống bảo mật đã phản ứng chính xác, phát hiện và ngăn chặn hiệu quả.

- Những điểm mạnh:
 - Nắm vững kiến thức lý thuyết về mạng LAN, mô hình Client-Server và các công nghệ bảo mật.
 - Biết cách cài đặt và cấu hình các công cụ bảo mật phổ biến như Snort và Wazuh.
 - Áp dụng được kiến thức vào thực hành thông qua các kịch bản mô phỏng.
 - Làm việc nhóm hiệu quả, phân công rõ ràng, trình bày báo cáo rõ ràng và logic.
- Tuy nhiên, nhóm cũng nhận thấy một số hạn chế:
 - Chưa triển khai nhiều rule nâng cao trong IDS/IPS để xử lý các loại tấn công phức tạp hơn như tấn công zero-day hoặc APT.
 - Việc mô phỏng vẫn còn giới hạn trong môi trường lab, chưa áp dụng được trên môi trường thực tế với quy mô lớn.
 - Còn phụ thuộc vào hướng dẫn, chưa hoàn toàn chủ động trong xử lý sự cố ngoài kịch bản.

3. Các phương án, giải pháp bảo mật người dùng cuối

Bảo mật người dùng cuối (Endpoint Security) là yếu tố quan trọng trong việc đảm bảo an toàn cho toàn bộ hệ thống mạng nội bộ. Ngoài việc triển khai các công cụ như Snort và Wazuh, nhóm đề xuất một số phương án và giải pháp bổ sung nhằm tăng cường bảo mật toàn diện như sau:

1. Thiết lập chính sách bảo mật nghiêm ngặt

- Phân quyền người dùng theo nguyên tắc tối thiểu (Least Privilege), chỉ cấp quyền cần thiết cho từng vai trò.
- Chính sách đặt mật khẩu mạnh: bắt buộc độ dài tối thiểu, sử dụng ký tự đặc biệt, thay đổi định kỳ.
- Khóa tự động màn hình khi người dùng không hoạt động trong khoảng thời gian nhất định.

2. Triển khai phần mềm bảo vệ thiết bị đầu cuối

- Sử dụng giải pháp EDR/EPP như ESET, Kaspersky, CyStack Endpoint để giám sát hành vi, phát hiện mã độc và cô lập thiết bị nếu cần.
- Thiết lập cơ chế tự động cập nhật phần mềm và hệ điều hành để giảm nguy cơ bị khai thác từ lỗ hổng bảo mật.

3. Giám sát và ghi nhật ký hoạt động

- Cài đặt hệ thống SIEM (Security Information and Event Management) để tập trung log từ các endpoint và server.
- Thiết lập cảnh báo khi phát hiện hành vi bất thường như đăng nhập ngoài giờ, truy cập tài nguyên nhạy cảm...

4. Kiểm soát thiết bị ngoại vi và phần mềm

- Chặn hoặc kiểm soát các thiết bị USB, ổ cứng di động nhằm ngăn chặn lây lan mã độc.
- Cấm cài đặt phần mềm không rõ nguồn gốc bằng chính sách GPO hoặc ứng dụng Application Whitelisting.

5. Tăng cường nhận thức bảo mật cho người dùng

- Tổ chức đào tạo định kỳ về nhận diện email lừa đảo, kỹ năng phòng tránh tấn công xã hội (social engineering).
- Phát triển văn hóa bảo mật nội bộ, khuyến khích người dùng báo cáo sớm nếu phát hiện dấu hiệu bất thường.

6. Sử dụng xác thực đa yếu tố (MFA)

- Bắt buộc người dùng sử dụng MFA (ví dụ: mật khẩu + mã OTP hoặc vân tay) để đăng nhập vào hệ thống nội bộ, email, ứng dụng quan trọng.

7. Phân vùng mạng nội bộ

- Áp dụng cơ chế VLAN để chia tách các nhóm thiết bị theo vai trò (nhân viên, quản lý, máy chủ...) giúp hạn chế lây lan khi có sự cố bảo mật.

4. Kết luận

Đề tài “Xây dựng hệ thống bảo mật người dùng cuối” đã giúp nhóm sinh viên tiếp cận và làm quen với quy trình thiết kế, triển khai và bảo mật một hệ thống mạng nội bộ doanh nghiệp. Qua đó, nhóm không chỉ củng cố kiến thức chuyên môn mà còn rèn luyện kỹ năng thực hành, giải quyết vấn đề và làm việc nhóm – những năng lực quan trọng trong ngành CNTT.

Dù còn một số hạn chế, nhưng kết quả đạt được cho thấy nhóm đã đạt được các mục tiêu đề ra ban đầu. Nhóm hy vọng đề tài sẽ là bước đệm hữu ích cho quá trình học tập và làm việc trong lĩnh vực bảo mật hệ thống sau này

CHƯƠNG IV. TÀI LIỆU THAM KHẢO

- [1]. <https://vietnix.vn/mang-lan-la-gi/>, Mạng LAN là gì? Chi tiết về công dụng và các kiểu kết nối của mạng LAN, truy cập lần cuối ngày 02/07/2025
- [2]. <https://viettelidc.com.vn/tin-tuc/ids-la-gi>, IDS là gì? So sánh IDS, IPS và tường lửa, truy cập lần cuối ngày 03/07/2025
- [3]. <https://vietnix.vn/ids-la-gi/>, IDS là gì? So sánh chi tiết giữa IDS và IPS, cập lần cuối ngày 03/07/2025
- [4]. <https://cystack.net/vi/blog/endpoint-security#khai-niem>, Endpoint Security là gì? Giới thiệu giải pháp quản lý thiết bị nhân viên CyStack Endpoint, cập lần cuối ngày 03/07/2025
- [5]. <https://aws.amazon.com/vi/what-is/endpoint-security/>, Bảo mật điểm cuối là gì?, cập nhật lần cuối ngày 14/07/2025
- [6]. <https://vnpro.vn/tin-tuc/su-quan-trong-cua-bao-mat-thiet-bi-nguoi-dung-cuoi-4795.html>, SỰ QUAN TRỌNG CỦA BẢO MẬT THIẾT BỊ NGƯỜI DÙNG CUỐI, cập nhật lần cuối ngày 08/07/2025