

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: MẠNG KHÔNG DÂY

ĐỀ TÀI: ỨNG DỤNG IDS/ IPS TRONG BẢO VỆ MẠNG KHÔNG DÂY

Giảng Viên Hướng Dẫn: ThS. Cao Tiến Thành
Thành Viên:

1. Nguyễn Thị Kim Doanh – MSSV: 22DH110511
2. Nguyễn Thúy Vy – MSSV: 22DH114363
3. Lê Tường Vi – MSSV: 22DH114421

Tp. Hồ Chí Minh, Ngày Tháng 03 Năm 2025

LỜI CẢM ƠN

Chúng em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến tất cả thầy cô Trường Đại Học Ngoại Ngữ - Tin Học TP. Hồ Chí Minh nói chung cùng thầy cô trong Khoa Công Nghệ Thông Tin nói riêng đã tận tình giảng dạy, truyền đạt những kiến thức và kinh nghiệm quý báu cho chúng em trong suốt quá trình học tập tại trường.

Trong suốt thời gian nhóm làm bài báo cáo đề tài môn Mạng Không Dây, chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến Thầy Cao Tiến Thành, người đã hết lòng giúp đỡ và theo sát nhóm chúng em trong suốt quá trình thực hiện đề tài đồ án môn học này, chỉ ra cho nhóm hướng đi để nhóm có thể hoàn thành tốt nhất bài báo cáo đề tài đồ án này đúng thời hạn quy định.

Trong quá trình thực hiện đề tài môn Mạng Không Dây, dù nhóm đã cố gắng hoàn thiện đề tài một cách tối ưu nhất nhưng do thời gian và kiến thức còn hạn chế nên sẽ không tránh khỏi những thiếu sót và sai sót nhất định, rất mong nhận được sự cảm thông từ những đóng góp chân thành từ quý thầy cô khoa Công Nghệ Thông Tin.

Sau cùng chúng em xin gửi lời cảm ơn đến tất cả các bạn đã tham gia đóng góp ý kiến và giúp đỡ chúng em trong suốt quá trình thực hiện đề tài môn Mạng Không Dây.

Em xin chân thành cảm ơn tất cả mọi người

MỤC LỤC

Thành Viên:	1
LỜI CẢM ƠN	2
MỤC LỤC	3
DANH MỤC HÌNH ẢNH.....	5
DANH MỤC BẢNG BIỂU.....	8
CHƯƠNG I: GIỚI THIỆU VỀ ĐỀ TÀI.....	9
1. Mục tiêu đề tài:	9
2. Đối tượng và phạm vi:	9
2.1. Đối tượng nghiên cứu:	9
2.2. Phạm vi:	9
3. Ý nghĩa:	10
CHƯƠNG II: CƠ SỞ LÝ THUYẾT	11
1. Lý thuyết	11
1.1. IDS là gì?	11
1.2. IPS là gì?	15
1.3. Công cụ Snort là gì?	19
1.4. Công cụ Zeek là gì?	21
1.5. So sánh hai công cụ Snort và Zeek	22
2. Các mối đe dọa	23
3. Cơ chế phát triển và ngăn chặn xâm nhập	24
4. Công nghệ và giải pháp IDS/IPS hiện tại	26
4.1. Các giải pháp thương mại hàng đầu	26
4.2. Giải pháp mã nguồn mở	27
4.3. Công nghệ tiên tiến trong IDS/IPS không dây	28
4.4. Xu hướng phát triển	28
5. Các tiêu chuẩn và quy định liên quan	29
5.1. Tiêu chuẩn quốc tế	29
5.2. Quy định tuân thủ ngành	30
5.3. Khung an ninh mạng và hướng dẫn	31
5.4. Quy định quốc gia	32
5.5. Thách thức tuân thủ	32
CHƯƠNG III: PHƯƠNG PHÁP THỰC HIỆN	33
1. Xây dựng môi trường thực nghiệm	33
2. Lựa chọn và triển khai công cụ	34

3. Cấu hình IDS/IPS	35
4. Thử nghiệm tấn công	35
5. Thu thập và phân tích dữ liệu.....	35
6. Tối ưu hóa hệ thống.....	35
7. Xây dựng quy trình triển khai	35
CHƯƠNG IV: TRIỂN KHAI.....	36
Cấu hình và cài đặt Snort	36
CHƯƠNG V: ĐÁNH GIÁ VÀ KẾT LUẬN	73
1. Bảng phân công.....	73
2.Tài liệu tham khảo.....	73
3. Link youtube	73
3.1 Quá trình cài đặt:.....	73
3.2 Test 1:	73
3.3 Test 2:	73

DANH MỤC HÌNH ẢNH

Hình 1. Mô hình IDS/IPS.....	11
Hình 2. IDS là gì?	12
Hình 3. Phân loại IDS.....	12
Hình 4. IPS là gì?	15
Hình 5. Phân loại IPS	15
Hình 6. So sánh IPS với IDS.....	18
Hình 7. Công cụ phát hiện xâm nhập mạng Snort.....	19
Hình 8. Công cụ Zeek	21
Hình 9. So sánh hai công cụ Snort và Zeek	22
Hình 10. Các mối đe dọa.....	23
Hình 11.Nâng cấp toàn bộ hệ thống	36
Hình 12. Cài đặt dịch vụ SSH Server	36
Hình 13. Cài đặt tất cả các công cụ cần thiết để biên dịch phần mềm từ mã nguồn.....	37
Hình 14. Cài đặt các thư viện phát triển (DEV) cần thiết cho việc biên dịch và xây dựng các công cụ an ninh mạng	38
Hình 15. Tạo thư mục “snort_src” và di chuyển đến thư mục đó.....	39
Hình 16. Tải gói mã nguồn của DAQ phiên bản 2.0.7, một thành phần bắt buộc khi muốn cài đặt Snort từ mã nguồn	39
Hình 17. Giải nén file	40
Hình 18.Di chuyển đến thư mục “daq - 2.0.7”.....	40
Hình 19. Biên dịch mã nguồn thành chương trình thực thi.....	41
Hình 20. Cài đặt chương trình đã Build vào hệ thống	41
Hình 21. Cài đặt các thư viện mã hóa và nén cần thiết.....	42
Hình 22. Cài đặt thư viện phát triển HTTP/2	42
Hình 23. Tải mã nguồn Snort phiên bản 2.9.20 về hệ thống.....	42
Hình 24. Giải nén file	43
Hình 25. Cấu hình Snort để kích hoạt tính năng Sourcefire trước khi biên dịch và cài đặt.	44
Hình 26. Tải xuống mã nguồn của LuaJIT	45
Hình 27. Biên dịch mã nguồn thành chương trình thực thi	45
Hình 28. Biên dịch mã nguồn thành công	46
Hình 29. Cài đặt chương trình đã Build vào hệ thống	46
Hình 30. Cấu hình phần mềm để sử dụng thư viện tirpc, vốn là một thư viện hỗ trợ giao tiếp qua Remote Procedure Call (RPC) trong hệ thống.....	46
Hình 31. Biên dịch mã nguồn thành chương trình thực thi	47
Hình 32.Cài đặt chương trình đã Build vào hệ thống	48

Hình 33. Cập nhật bộ nhớ cache của thư viện động trong hệ thống, tạo một liên kết mềm từ “/usr/local/bin/snort” đến “/usr/sbin/snort”. Điều này có nghĩa là có thể gọi snort từ bất kỳ đâu trong hệ thống. Cuối cùng là kiểm tra phiên bản hiện tại của Snort	49
Hình 34. Tạo ra một nhóm người dùng mới có tên là “snort” và tạo ra một người dùng hệ thống có tên là “snort”, nhưng không có quyền đăng nhập vào hệ thống, mục đích để quản lý hoặc chạy Snort mà không cần quyền truy cập trực tiếp vào shell	49
Hình 35. Tạo một số thư mục cấu hình và triển khai Snort.....	49
Hình 36. Tạo ra các tệp rỗng để cấu hình.....	49
Hình 37. Tạo một số thư mục mới trong hệ thống.....	50
Hình 38. Thay đổi quyền truy cập cho các thư mục. Với quyền “5775”, người sở hữu và nhóm có quyền đọc, ghi và thực thi trên các tệp và thư mục, trong khi người dùng khác chỉ có thể đọc và thực thi mà không có quyền thay đổi.....	50
Hình 39. Chỉ người dùng và nhóm Snort có quyền truy cập và quản lý	50
Hình 40.Sao chép các tệp cấu hình quan trọng, tệp bản đồ SID, và các tệp định nghĩa kiểu tài liệu vào thư mục cấu hình của Snort	51
Hình 41. Hiển thị cấu trúc thư mục của thư mục dưới dạng cây	51
Hình 42. Sửa dòng này thành ip của máy chủ	52
Hình 43. Thêm hướng dẫn	53
Hình 44. Yêu cầu Snort kiểm tra cấu hình mà không bắt đầu phân tích lưu lượng mạng thực tế	53
Hình 45. Cấu hình thành công	53
Hình 46. Mở file nano đến tệp “/etc/snort/rules/local.rules”	54
Hình 47. - Viết quy tắc gửi cảnh báo khi nhận được một gói ICMP từ bất kỳ nguồn nào đến mạng nội bộ	54
Hình 48. Mở file nano đến tệp “/etc/snort/sid-msg.map”.....	54
Hình 49. Viết một đoạn mô tả chi tiết quy tắc Snort	54
Hình 50. Yêu cầu Snort thực hiện kiểm tra cấu hình mà không thực sự bắt đầu giám sát lưu lượng mạng	54
Hình 51. Kiểm tra thành công	54
Hình 52. Thủ dùng máy Ubuntu ping đến 8.8.8.8 và kết quả thu được	55
Hình 53. Chỉnh sửa tệp “snort.conf”	55
Hình 54. Tại Step 6, thêm “output unified2: filename snort.u2, limit 128”	55
Hình 55. Tải tệp mã nguồn của Barnyard2 từ GitHub và lưu nó với tên barnyard2-Master.tar.gz trên hệ thống của bạn	56
Hình 56. Giải nén file	56
Hình 57.Di chuyển vào thư mục “barnyard2-master/” sau đó yêu cầu autoreconf tạo lại tất cả các tệp cấu hình cần thiết cho dự án phần mềm từ các tệp mẫu hiện có, sử dụng các macro tùy chỉnh từ thư mục ./m4/.....	57
Hình 58. Lệnh này tạo một liên kết tượng trưng (symlink) từ “/usr/include/dnet.h” đến “/usr/include/dumbnet.h”	57

Hình 59. Cấu hình phần mềm để nó có thể sử dụng MySQL trong quá trình biên dịch	58
Hình 60. Trình cấu hình sẽ tìm các thư viện MySQL cần thiết trong thư mục “/usr/lib/x86_64-linux-gnu/”	58
Hình 61. Đảm bảo rằng phần mềm có thể tích hợp với MySQL trong quá trình biên dịch và sử dụng	59
Hình 62. Kiểm tra phiên bản Barnyard2	59
Hình 63. Kiểm tra vị trí thư mục	59
Hình 64. Sao chép tệp “barnyard2.conf” từ thư mục của dự án Barnyard2 (ở “/home/doanh/barnyard2-master/etc/”) vào thư mục cấu hình của Snort (“/etc/snort/”)).....	59
Hình 65.Tạo thư mục và cấp quyền.....	60
Hình 66. Khởi chạy MySQL.....	60
Hình 67. Tạo CSDL	61
Hình 68. Người dùng chỉ có thể sử dụng các quyền này khi kết nối từ localhost.....	62
Hình 69. Cấp quyền cho tệp cấu hình.....	62
Hình 70. Khởi chạy Barnyard2 để xử lý các sự kiện và cảnh báo từ Snort.....	63
Hình 71. Thủ ping đến một địa chỉ và kiểm tra kết quả	64
Hình 72. Kết nối đến cơ sở dữ liệu “snort” với người dùng “snort”, sau đó thực hiện một câu truy vấn SQL để đếm số lượng bản ghi trong bảng event	65
Hình 73. Tạo tệp cấu hình “snort.service”	65
Hình 74. Thêm nội dung vào tệp và lưu lại	65
Hình 75. Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort	65
Hình 76. Tạo tệp cấu hình “barnyard2.serverce”	65
Hình 77. Tệp có nội dung sau	66
Hình 78. Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort	66
Hình 79. Thêm kho lưu trữ “ppa:ondrej/php” vào danh sách các kho lưu trữ của hệ thống	67
Hình 80. Cài đặt Apache và PHP 5.6 cùng với các phần mở rộng và mô-đun cần thiết để PHP hoạt động trên Apache	68
Hình 81. Tải về phiên bản ADODB 5.20.8 từ SourceForge, là thư viện hỗ trợ tương tác cơ sở dữ liệu trong PHP5	68
Hình 82. Giải nén file	69
Hình 83. Di chuyển thư mục “adodb5” vào thư mục “/var/adodb/” và thay đổi quyền truy cập của thư mục và các tệp bên trong	69
Hình 84. Tải về tệp BASE 1.4.5 từ SourceForge, là công cụ giúp phân tích và quản lý cảnh báo từ IDS	69
Hình 85. Giải nén tệp	70
Hình 86. Di chuyển thư mục “base-1.4.5/” vào thư mục “/var/www/html/base/”, nơi các tệp web sẽ được Apache phục vụ	70
Hình 87. Tạo tệp cấu hình “base_conf.php”	71
Hình 88. thay đổi quyền sở hữu thư mục	71
Hình 89. Loại bỏ quyền đọc đối với tệp “base_conf.php”	71
Hình 90. Khởi động Apache2	72

DANH MỤC BẢNG BIỂU

Bảng 1. So sánh các loại IDS	13
Bảng 2. So sánh các loại IPS.....	16
Bảng 3. So sánh giữa IDS và IPS	18

CHƯƠNG I: GIỚI THIỆU VỀ ĐỀ TÀI

1. Mục tiêu đề tài:

Hướng đến việc nghiên cứu và triển khai hiệu quả hệ thống phát hiện và ngăn chặn xâm nhập trong môi trường mạng không dây. Mục tiêu chính của đề tài là tìm hiểu sâu về cơ chế hoạt động của IDS/IPS, phân tích các phương thức tấn công phổ biến trên mạng không dây, và đề xuất giải pháp triển khai phù hợp. Thông qua việc xây dựng mô hình thử nghiệm và thực hiện các kịch bản đánh giá, đề tài hướng đến việc tối ưu hóa cấu hình IDS/IPS để nâng cao hiệu quả phát hiện và ngăn chặn các mối đe dọa an ninh mạng. Kết quả nghiên cứu sẽ cung cấp một quy trình triển khai và vận hành IDS/IPS toàn diện, góp phần tăng cường bảo mật cho hệ thống mạng không dây.

2. Đối tượng và phạm vi:

2.1. Đối tượng nghiên cứu:

- Hệ thống IDS/IPS là: các Cấu trúc và nguyên lý hoạt động của hệ thống phát hiện xâm nhập (IDS), Cơ chế phòng chống của hệ thống ngăn chặn xâm nhập (IPS), Các thành phần và mô-đun chính trong kiến trúc IDS/IPS, Quy trình xử lý và phân tích dữ liệu của hệ thống.
- Mạng không dây là những Cấu trúc và đặc điểm của mạng Wi-Fi, Các giao thức bảo mật không dây, Các điểm yếu và lỗ hổng tiềm ẩn trong mạng không dây, Các phương thức tấn công phổ biến trên mạng không dây.

2.2. Phạm vi:

- Phạm vi kỹ thuật là: Tập trung vào các giải pháp IDS/IPS chuyên dụng cho mạng không dây, Nghiên cứu các công nghệ phát hiện và ngăn chặn xâm nhập hiện đại, Đánh giá hiệu quả của các phương pháp phân tích và phát hiện tấn công, Giới hạn trong môi trường mạng Wi-Fi chuẩn IEEE 802.11.
- Phạm vi ứng dụng là: Áp dụng cho mạng không dây trong môi trường doanh nghiệp vừa và nhỏ, Tập trung vào các giải pháp có tính khả thi và hiệu quả về chi phí, Xem xét các trường hợp triển khai thực tế phổ biến, Giới hạn trong phạm vi bảo vệ mạng nội bộ.

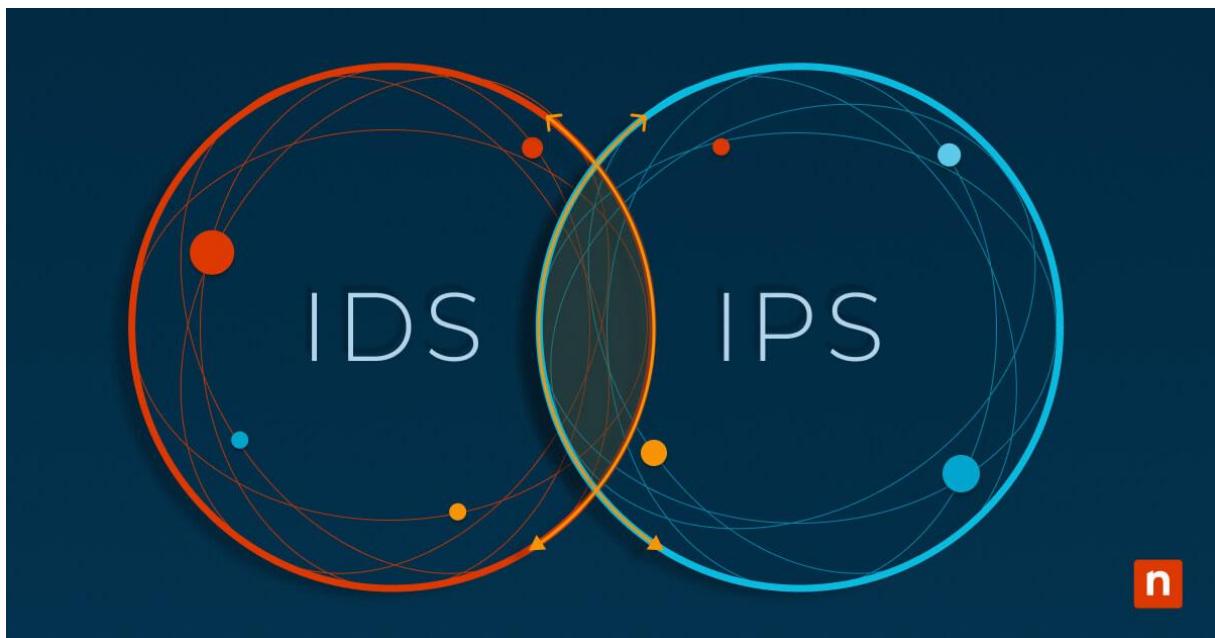
- Phạm vi thời gian là các: Nghiên cứu các công nghệ và giải pháp IDS/IPS hiện đại, Tập trung vào các mối đe dọa và phương thức tấn công mới nhất, Đánh giá xu hướng phát triển của công nghệ bảo mật không dây, Thời gian thực hiện nghiên cứu và triển khai trong khoảng 6-12 tháng.

3. Ý nghĩa:

Đề tài mang nhiều ý nghĩa quan trọng cả về mặt khoa học và thực tiễn. Về khía cạnh khoa học, nghiên cứu góp phần hệ thống hóa kiến thức về cơ chế hoạt động của IDS/IPS trong môi trường mạng không dây, đồng thời làm rõ mối quan hệ giữa các phương thức tấn công và giải pháp phòng chống, tạo nền tảng cho các nghiên cứu tiếp theo về bảo mật mạng không dây. Về mặt thực tiễn, đề tài cung cấp giải pháp bảo mật hiệu quả cho các tổ chức và doanh nghiệp, giúp giảm thiểu rủi ro bị tấn công và mất mát dữ liệu. Đối với người quản trị mạng, nghiên cứu cung cấp quy trình triển khai IDS/IPS chuẩn hóa, hỗ trợ việc phát hiện và xử lý sự cố bảo mật hiệu quả. Về phương diện phát triển, đề tài thúc đẩy việc áp dụng công nghệ mới trong bảo vệ mạng không dây, đồng thời mở ra hướng nghiên cứu về tích hợp AI trong hệ thống IDS/IPS, góp phần phát triển các giải pháp bảo mật thông minh và tự động hóa trong tương lai.

CHƯƠNG II: CƠ SỞ LÝ THUYẾT

1. Lý thuyết



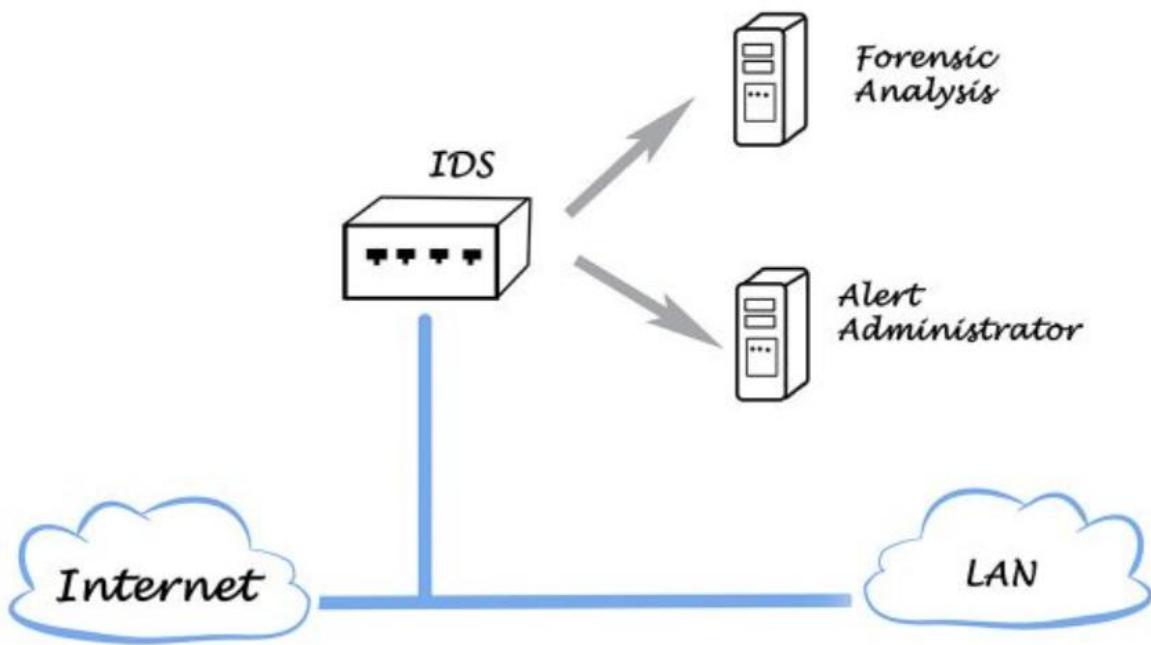
Hình 1. Mô hình IDS/IPS

1.1. IDS là gì?

1.1.1. Khái niệm:

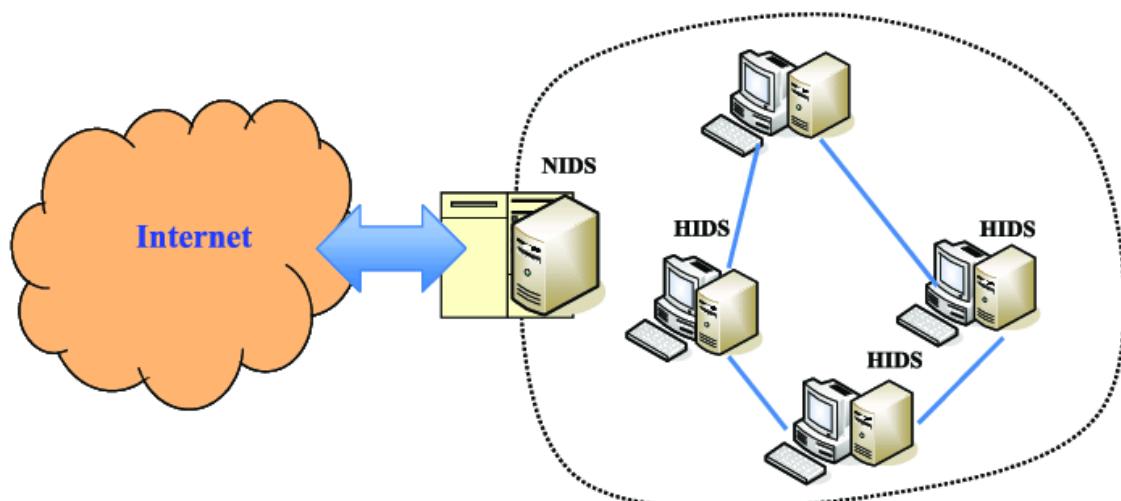
- IDS (Intrusion Detection System) là hệ thống phát hiện xâm nhập, đây là một giải pháp bảo mật quan trọng được sử dụng để giám sát và phát hiện các hoạt động đáng ngờ trong mạng.
 - Mục đích chính là phát hiện các hành vi xâm nhập trái phép hoặc vi phạm chính sách bảo mật
 - IDS hoạt động như một "camera an ninh" trong mạng máy tính
- IDS gồm các loại sau:*
- HIDS (Host-based IDS): Giám sát hoạt động trên từng máy chủ cụ thể
 - NIDS (Network-based IDS): Giám sát lưu lượng trên toàn bộ mạng
 - Hybrid IDS: Kết hợp cả HIDS và NIDS
 - WIDS (Wireless IDS): Chuyên dụng cho mạng không dây

Intrusion Detection System



Hình 2. IDS là gì?

1.1.2. Phân loại IDS



Hình 3. Phân loại IDS

Bảng 1. So sánh các loại IDS

Tiêu chí	HIDS	NIDS	Hybrid IDS	WIDS
Phạm vi bảo vệ	Máy chủ/máy trạm cụ thể	Toàn bộ mạng có dây	Kết hợp cả HIDS và NIDS	Mạng không dây
Cách thức hoạt động	Giám sát tiến trình, file, registry, nhật ký hệ thống	Giám sát lưu lượng mạng để phát hiện xâm nhập	Tích hợp cả phân tích lưu lượng mạng và giám sát host	Giám sát các thiết bị Wi-Fi, điểm truy cập, tấn công không dây
Ưu điểm	Phát hiện được tấn công zero-day, kiểm soát chặt chẽ	Bảo vệ cả hệ thống mạng, phát hiện tấn công từ bên ngoài	Toàn diện, giảm thiểu mù trong giám sát	Phát hiện rogue AP, tấn công MITM, giả mạo SSID
Nhược điểm	Không giám sát được lưu lượng mạng tổng thể	Có thể bỏ sót tấn công nội bộ hoặc mã hóa	Phức tạp, tốn tài nguyên triển khai	Hiệu quả phụ thuộc vào phạm vi phát hiện tín hiệu
Ứng dụng chính	Máy chủ quan trọng, hệ thống endpoint	Doanh nghiệp, trung tâm dữ liệu	Hệ thống cần bảo vệ tối đa, SOC	Mạng Wi-Fi công cộng, doanh nghiệp

1.1.3. Cơ chế hoạt động

- Thu thập dữ liệu: Log hệ thống, lưu lượng mạng, hoạt động người dùng
- Phân tích: So sánh với mẫu tấn công đã biết hoặc phát hiện hành vi bất thường
- Cảnh báo: Thông báo cho quản trị viên khi phát hiện nguy cơ
- Ghi nhận: Lưu trữ thông tin về các sự kiện để phân tích sau

1.1.4. Phương pháp phát hiện

- Signature-based: Dựa trên cơ sở dữ liệu các mẫu tấn công đã biết
- Anomaly-based: Phát hiện dựa trên hành vi bất thường so với baseline
- Specification-based: Dựa trên các quy tắc và chính sách bảo mật định sẵn
- Heuristic: Sử dụng các thuật toán học máy để phát hiện mối đe dọa mới

1.1.5. Ưu điểm

- Phát hiện sớm các cuộc tấn công
- Giám sát liên tục 24/7
- Tạo logs chi tiết phục vụ điều tra
- Hỗ trợ tuân thủ các quy định về bảo mật

1.1.6. Hạn chế

- Có thể tạo cảnh báo giả (false positives)
- Không thể ngăn chặn tấn công (chỉ phát hiện)
- Yêu cầu cập nhật thường xuyên
- Cần nguồn lực để quản lý và vận hành

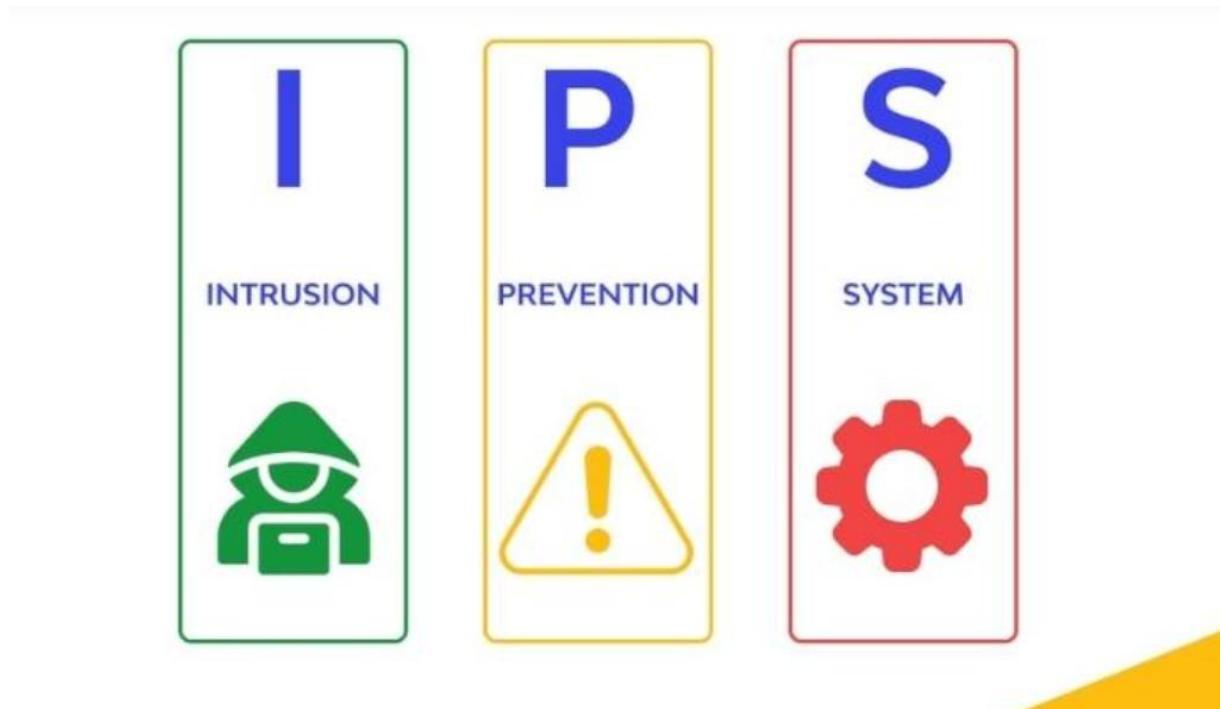
1.1.7. Vai trò trong bảo mật mạng không dây

- Phát hiện các điểm truy cập giả mạo
- Giám sát hoạt động đáng ngờ trong vùng phủ sóng
- Cảnh báo về các nỗ lực tấn công WPA/WEP
- Phát hiện các thiết bị không được phép

1.2. IPS là gì?

1.2.1. Khái niệm

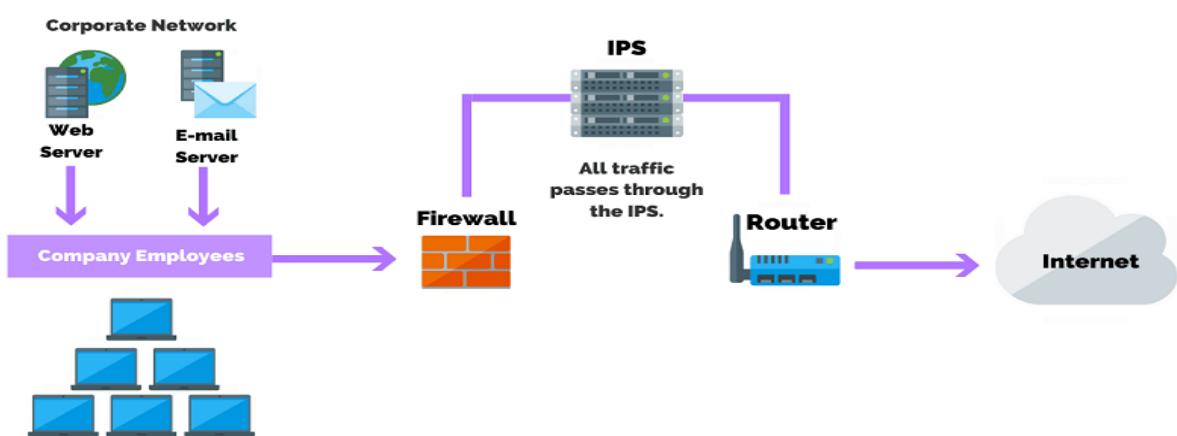
- IPS là hệ thống chủ động giám sát và ngăn chặn các hoạt động xâm nhập trái phép
- Không chỉ phát hiện mà còn có khả năng tự động phản ứng với các mối đe dọa
- Được tích hợp trực tiếp vào đường truyền mạng để kiểm soát lưu lượng.



Hình 4. IPS là gì?

1.2.2. Phân loại IPS

Network Intrusion Prevention System (NIPS)



Hình 5. Phân loại IPS

Phân loại IPS:

- Network-based IPS (NIPS): Bảo vệ toàn bộ mạng
- Host-based IPS (HIPS): Bảo vệ từng máy chủ cụ thể
- Wireless IPS (WIPS): Chuyên dụng cho mạng không dây
- NBA (Network Behavior Analysis): Phân tích hành vi mạng

Bảng 2. So sánh các loại IPS

Tiêu chí	NIPS	HIPS	WIPS	NBA
Phạm vi bảo vệ	Toàn bộ mạng	Máy chủ/máy trạm cụ thể	Mạng không dây	Cả mạng, tập trung vào hành vi
Cách thức hoạt động	Giám sát lưu lượng mạng và phát hiện/chặn mối đe dọa dựa trên quy tắc hoặc chữ ký	Giám sát tiến trình, file, registry của máy tính để phát hiện mối đe dọa	Giám sát các điểm truy cập không dây và thiết bị di động để phát hiện xâm nhập	Phân tích hành vi lưu lượng mạng, phát hiện bất thường thay vì dựa vào chữ ký
Ưu điểm	Bảo vệ nhiều thiết bị, phát hiện mối đe dọa từ sớm	Kiểm soát sâu vào từng thiết bị, phát hiện tấn công zero-day tốt hơn	Phát hiện tấn công trong mạng Wi-Fi (rogue AP, MITM, v.v.)	Nhận diện được các cuộc tấn công mới, không cần chữ ký có sẵn
Nhược điểm	Có thể bỏ sót các tấn công mã hóa hoặc nội bộ	Chỉ bảo vệ thiết bị cài đặt, không giám sát toàn mạng	Hiệu quả phụ thuộc vào vị trí triển khai và phạm vi bảo vệ	Có thể xảy ra báo động giả cao, cần phân tích kỹ hơn
Ứng dụng chính	Doanh nghiệp, trung tâm dữ liệu	Máy chủ, hệ thống quan trọng	Mạng Wi-Fi công cộng, doanh nghiệp	Phân tích an ninh mạng tổng thể, SOC (Security Operations Center)

1.2.3. Cơ chế hoạt động

- Giám sát lưu lượng mạng theo thời gian thực
- Phân tích và so sánh với cơ sở dữ liệu mối đe dọa
- Thực hiện hành động ngăn chặn khi phát hiện tấn công
- Ghi nhận và báo cáo các sự kiện bảo mật

1.2.4. Phương thức ngăn chặn

- Chặn/hủy các kết nối đáng ngờ
- Tái cấu hình tường lửa
- Chặn địa chỉ IP nguồn tấn công
- Đặt lại kết nối
- Khóa tài khoản người dùng đáng ngờ

1.2.5. Ưu điểm

- Bảo vệ chủ động và tự động
- Phản ứng nhanh với các mối đe dọa
- Giảm thiểu tác động của tấn công
- Tích hợp nhiều tính năng bảo mật

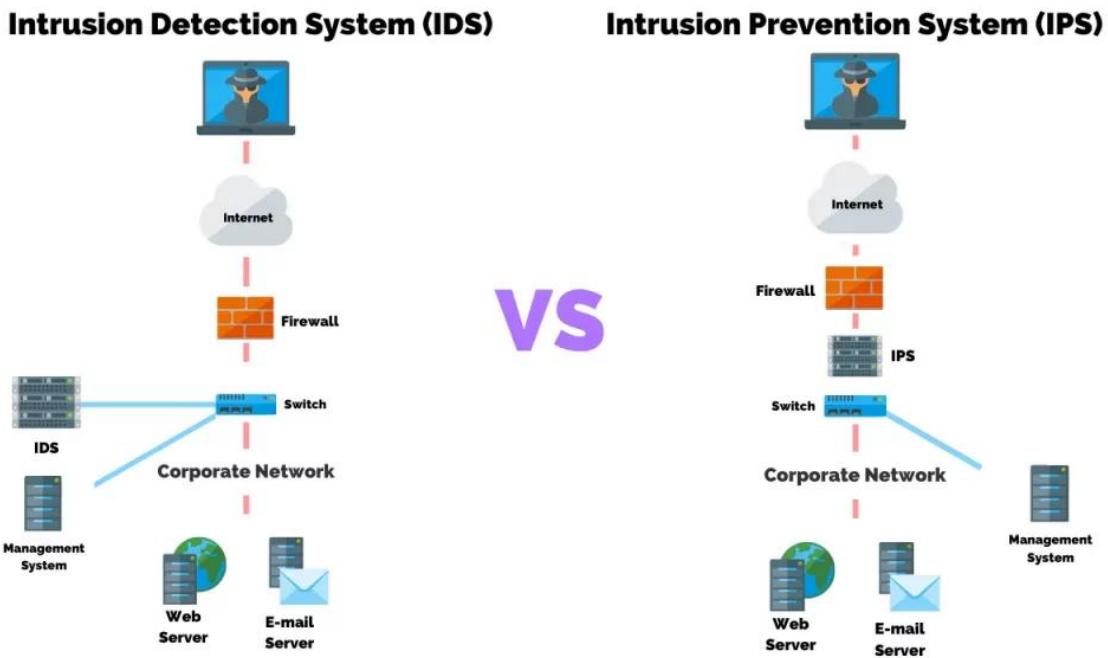
1.2.6. Hạn chế

- Chi phí triển khai cao
- Có thể ảnh hưởng đến hiệu năng mạng
- Nguy cơ chặn nhầm lưu lượng hợp lệ
- Yêu cầu cấu hình và quản lý phức tạp

1.2.7. Vai trò trong bảo vệ mạng không dây

- Ngăn chặn truy cập trái phép
- Chặn các cuộc tấn công DoS
- Bảo vệ chống lại man-in-the-middle
- Ngăn chặn việc sử dụng các công cụ hack không dây

1.2.8. So sánh với IDS



Hình 6. So sánh IPS với IDS

- IPS chủ động hơn IDS
- Có khả năng tự động phản ứng
- Đặt inline trong mạng (không phải passive)
- Chi phí và độ phức tạp cao hơn

Bảng 3. So sánh giữa IDS và IPS

Tiêu chí	IDS	IPS
Chức năng chính	Phát hiện và cảnh báo về các hoạt động xâm nhập	Phát hiện, cảnh báo và ngăn chặn các hoạt động xâm nhập
Phản ứng	Chỉ đưa ra cảnh báo, không can thiệp trực tiếp	Tự động can thiệp để ngăn chặn hoặc chặn các hoạt động xâm nhập
Vị trí triển khai	Thường được triển khai ngoài luồng (out-of-band)	Thường được triển khai trong luồng (inline)
Tác động đến lưu lượng	Không ảnh hưởng đến lưu lượng mạng	Có thể làm chậm lưu lượng mạng do can thiệp trực tiếp
Phát hiện xâm nhập	Dựa trên chữ ký hoặc hành vi, cảnh báo về các hành vi đáng ngờ	Dựa trên chữ ký hoặc hành vi, ngăn chặn ngay lập tức các hành vi đáng ngờ

Ứng dụng	Phù hợp cho việc giám sát và phân tích bảo mật	Phù hợp cho việc ngăn chặn và bảo vệ trực tiếp khỏi các mối đe dọa
Mức độ can thiệp	Thụ động (chỉ phát hiện và cảnh báo)	Chủ động (phát hiện và ngăn chặn)
Tích hợp với hệ thống	Có thể tích hợp với các hệ thống quản lý bảo mật	Có thể hoạt động độc lập hoặc tích hợp với các hệ thống bảo mật khác

1.3. Công cụ Snort là gì?

1.3.1. Khái niệm

Snort là một công cụ phát hiện xâm nhập mạng mã nguồn mở (Open Source Intrusion Detection System - IDS) được phát triển bởi Sourcefire. Nó có khả năng phân tích lưu lượng mạng theo thời gian thực và thực hiện ghi nhật ký các gói tin để phát hiện các cuộc tấn công, quét cổng, các dấu hiệu đáng ngờ và nhiều hành vi khác trên mạng.



Hình 7. Công cụ phát hiện xâm nhập mạng Snort

1.3.2. Chức năng chính của Snort

- Chế độ Sniffer: *Giám sát lưu lượng mạng theo thời gian thực.*
- Chế độ Packet Logger: *Lưu trữ dữ liệu gói tin để phân tích sau.*
- Chế độ IDS/IPS: *Phát hiện và ngăn chặn các cuộc tấn công mạng.*

Cách hoạt động của Snort

Snort hoạt động bằng cách phân tích gói tin, so sánh chúng với một bộ quy tắc (ruleset) để phát hiện các mối đe dọa. Khi phát hiện một gói tin nguy hiểm, nó sẽ cảnh báo hoặc chặn tùy theo cấu hình.

1.3.3. Một số kiểu tấn công Snort có thể phát hiện

- Quét cổng (Port Scanning)
- Tấn công DoS/DoS
- Tấn công buffer overflow
- Mã độc và backdoor
- Xâm nhập trái phép

1.4. Công cụ Zeek là gì?

1.4.1. Khái niệm:

Zeek (trước đây gọi là Bro) là một hệ thống giám sát bảo mật mạng (NSM – Network Security Monitoring) mạnh mẽ, mã nguồn mở. Không giống như Snort hay các IDS/IPS truyền thống, Zeek tập trung vào phân tích lưu lượng mạng, ghi log chi tiết và phát hiện các bất thường, thay vì chỉ dựa vào quy tắc chữ ký.

1.4.2. Các chức năng chính của Zeek

- Giám sát lưu lượng mạng theo thời gian thực
- Phân tích lưu lượng dữ liệu sâu (Deep Packet Inspection - DPI)
- Phát hiện các hành vi bất thường, mối đe dọa bảo mật
- Ghi log chi tiết các sự kiện mạng (HTTP, DNS, SSL, FTP, SSH, v.v.)
- Tích hợp với các hệ thống SIEM và công cụ bảo mật khác

1.4.3. Cách hoạt động của Zeek

- Zeek hoạt động trên 2 cấp độ:
 - Phân tích lưu lượng gói tin: Ghi lại thông tin chi tiết về các kết nối mạng.
 - Xử lý sự kiện: Dựa vào tập luật script để phát hiện các hoạt động đáng ngờ.



Hình 8. Công cụ Zeek

1.5. So sánh hai công cụ Snort và Zeek



Hình 9. So sánh hai công cụ Snort và Zeek

1.5.1. Điểm giống nhau:

- Đều là công cụ giám sát an ninh mạng mã nguồn mở.
- Hoạt động bằng cách phân tích lưu lượng mạng để phát hiện mối đe dọa.
- Được sử dụng rộng rãi trong bảo mật mạng doanh nghiệp.
- Có thể tích hợp với SIEM và các công cụ bảo mật khác.

1.5.2. Điểm khác nhau:

- Snort và Zeek đều là công cụ giám sát an ninh mạng, nhưng chúng có cách tiếp cận khác nhau.
- Snort là một hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), hoạt động dựa trên chữ ký (signature-based) để phát hiện các mối đe dọa đã biết, giúp ngăn chặn tấn công ngay lập tức.
- Zeek là một hệ thống giám sát bảo mật mạng (NSM), tập trung vào phân tích hành vi (behavior-based), ghi log chi tiết về các hoạt động mạng và phát hiện những bất thường thay vì chỉ dựa vào chữ ký.

-

-

-

- Snort có thể chặn lưu lượng độc hại, trong khi Zeek chỉ giám sát mà không ngăn chặn trực tiếp.
- Snort dễ cấu hình hơn nhờ sử dụng quy tắc có sẵn, còn Zeek yêu cầu người dùng viết script tùy chỉnh để phát hiện các mối đe dọa cụ thể.
- Snort thích hợp cho phát hiện tấn công theo thời gian thực, trong khi Zeek mạnh hơn trong phân tích và điều tra bảo mật chuyên sâu.

2. Các mối đe dọa



Hình 10. Các mối đe dọa

2.1. Tấn công DoS/DDoS vào hệ thống IDS/IPS

Tin tặc có thể làm quá tải IDS/IPS bằng cách gửi một lượng lớn gói tin độc hại, khiến hệ thống quá tải và không thể phát hiện xâm nhập thực sự.

Mối đe dọa nghiêm trọng đôi với an ninh mạng. Các tổ chức cần có chiến lược bảo vệ toàn diện, không chỉ tập trung vào việc phát hiện xâm nhập mà còn phải bảo vệ chính các hệ thống phát hiện và ngăn chặn xâm nhập. Việc xây dựng kiến trúc bảo mật có khả năng chống chịu cao là yếu tố quyết định để duy trì khả năng phòng thủ trước các cuộc tấn công ngày càng tinh vi.

2.2. Tấn công Evasion (Lẩn tránh IDS/IPS)

Hacker sử dụng các kỹ thuật che giấu dữ liệu như mã hóa, phân mảnh gói tin hoặc thay đổi mẫu tấn công để tránh bị IDS phát hiện.

Tấn công Evasion là tập hợp các kỹ thuật nhằm che giấu hoạt động tấn công để tránh bị

phát hiện bởi các hệ thống bảo mật như IDS (Intrusion Detection System) và IPS (Intrusion Prevention System). Mục tiêu là làm cho các gói tin độc hại trở nên "vô hình" đối với các cơ chế phát hiện.

2.3. Tấn công Spoofing (Mạo danh) để qua mặt IDS

Kẻ tấn công có thể giả mạo địa chỉ MAC/IP của các thiết bị hợp pháp để lừa IDS/IPS và thực hiện hành vi xâm nhập mà không bị phát hiện.

2.4. Tấn công vào chính hệ thống IDS/IPS (Exploiting IDS Vulnerabilities)

Nếu IDS/IPS có lỗ hổng bảo mật, tin tặc có thể khai thác để làm gián đoạn hoặc kiểm soát hệ thống giám sát này.

2.5. Tấn công Injection vào IDS/IPS

Kẻ tấn công có thể gửi dữ liệu giả mạo hoặc làm nhiễu loạn thông tin, khiến IDS/IPS nhận diện sai và đưa ra cảnh báo không chính xác.

2.6. Tấn công bằng Wi-Fi Rogue Access Point (AP)

Hacker thiết lập một điểm truy cập giả mạo để đánh lừa IDS/IPS, làm cho hệ thống không thể xác định được đâu là nguồn tấn công thực sự.

2.7. Lạm dụng cảnh báo sai (False Positives & False Negatives)

False Positive: IDS/IPS có thể phát hiện sai mối đe dọa, gây gián đoạn hoạt động bình thường.

False Negative: IDS/IPS không nhận diện được tấn công thực sự, làm giảm hiệu quả bảo mật.

2.8. Phần mềm độc hại tấn công IDS/IPS

Một số mã độc có thể được thiết kế để tắt hoặc vô hiệu hóa IDS/IPS, giúp hacker thực hiện các cuộc tấn công mà không bị phát hiện.

3. Cơ chế phát triển và ngăn chặn xâm nhập

3.1. Cơ chế phát hiện xâm nhập của IDS trong mạng không dây

3.1.1. Phát hiện dựa trên chữ ký (Signature-based Detection)

- IDS so sánh lưu lượng mạng với cơ sở dữ liệu chữ ký của các cuộc tấn công đã biết.
- Ví dụ: Nếu IDS phát hiện một mẫu gói tin trùng khớp với một cuộc tấn công brute-force đã được xác định trước, nó sẽ tạo cảnh báo.
- Hạn chế: Không phát hiện được các cuộc tấn công mới (zero-day attacks).

3.1.2. Phát hiện dựa trên hành vi (Anomaly-based Detection)

- IDS sử dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning) để xác định các hành vi bất thường so với hoạt động bình thường của hệ thống.
- Ví dụ: Nếu một thiết bị thường chỉ gửi 10MB dữ liệu/ngày, nhưng đột nhiên gửi 1GB dữ liệu trong một giờ, IDS sẽ coi đây là hành vi đáng ngờ.
- Ưu điểm: Phát hiện được các cuộc tấn công chưa biết (zero-day).
- Hạn chế: Dễ tạo cảnh báo sai (False Positives).

3.1.3. Phát hiện dựa trên trạng thái giao thức (Stateful Protocol Analysis)

- IDS phân tích trạng thái và hành vi của các giao thức mạng (Wi-Fi, TCP/IP, HTTP, DNS,...) để phát hiện vi phạm.
- Ví dụ: Nếu IDS phát hiện một thiết bị gửi quá nhiều yêu cầu xác thực WPA2 liên tục, có thể là dấu hiệu của tấn công brute-force.

3.2. Cơ chế ngăn chặn xâm nhập của IPS trong mạng không dây

IPS hoạt động chủ động hơn IDS, có thể tự động chặn hoặc ngăn chặn các cuộc tấn công theo nhiều cách:

3.2.1. Chặn lưu lượng độc hại (Packet Dropping)

- Nếu phát hiện một gói tin có dấu hiệu tấn công, IPS sẽ từ chối gói tin đó trước khi nó đến đích.
- Ví dụ: Nếu một máy tính bị nhiễm mã độc đang cố gửi dữ liệu đến máy chủ điều khiển (C2 Server), IPS sẽ ngăn chặn kết nối này.

3.2.2. Ngăn chặn truy cập vào các địa chỉ IP độc hại (IP Blacklisting)

- IPS có thể tự động chặn hoặc cảnh báo khi một thiết bị trong mạng kết nối với các địa chỉ IP đáng ngờ.
- Ví dụ: Nếu một thiết bị cố truy cập vào máy chủ có liên quan đến hacker, IPS sẽ ngăn chặn kết nối ngay lập tức.

3.2.3. Chặn hoặc cách ly thiết bị đáng ngờ (Quarantine Devices)

- Nếu một thiết bị có dấu hiệu bị nhiễm mã độc hoặc tấn công, IPS có thể ngăn chặn thiết bị đó kết nối vào mạng Wi-Fi hoặc chuyển nó vào một VLAN cách ly.
- Ví dụ: Nếu IPS phát hiện một thiết bị thực hiện quét cổng (port scanning), nó có thể tự động cô lập thiết bị này để tránh lây nhiễm.

3.2.4. Chặn tấn công từ chối dịch vụ (DoS & DDoS Mitigation)

- IPS có thể phát hiện mô hình tấn công DoS/DDoS và tự động giảm tải hoặc giới hạn băng thông của nguồn tấn công.
- Ví dụ: Nếu một thiết bị trong mạng gửi quá nhiều yêu cầu DNS trong thời gian ngắn, IPS có thể giới hạn tốc độ của nó hoặc chặn hẳn.

3.3. Kết hợp IDS/IPS với các giải pháp bảo mật khác

- IDS/IPS hiệu quả hơn khi kết hợp với các công nghệ bảo mật khác:
- Firewall thế hệ mới (Next-Gen Firewall - NGFW): Chặn lưu lượng độc hại ngay từ đầu.
- Hệ thống SIEM (Security Information and Event Management): Tích hợp cảnh báo IDS/IPS vào phân tích bảo mật tổng thể.
- VPN & Mã hóa WPA3: Bảo vệ dữ liệu trên mạng Wi-Fi trước tấn công nghe lén.
- Zero Trust Security: Chỉ cho phép các thiết bị được xác thực truy cập vào mạng.

4. Công nghệ và giải pháp IDS/IPS hiện tại

4.1. Các giải pháp thương mại hàng đầu

4.1.1. Cisco Wireless Intrusion Prevention System

- Tích hợp với hạ tầng mạng không dây Cisco
- Cung cấp khả năng phân tích phốt tàn và phát hiện các điểm truy cập giả mạo
- Tự động phân loại và ngăn chặn các mối đe dọa
- Quản lý tập trung thông qua Cisco DNA Center

4.1.2. Aruba WIPS (Wireless Intrusion Prevention System)

- Công nghệ Machine Learning để giảm cảnh báo giả
- Bảo vệ thông minh thích ứng với môi trường mạng
- Hỗ trợ đầy đủ các chuẩn mạng 802.11
- Tích hợp sâu với nền tảng Aruba ESP (Edge Services Platform)

4.1.3. Fortinet FortiWIPS

- Giải pháp IPS chuyên dụng cho mạng không dây
- Tích hợp với hệ sinh thái bảo mật Fortinet

- Phát hiện và ngăn chặn truy cập trái phép theo thời gian thực
- Hỗ trợ các tiêu chuẩn tuân thủ PCI, HIPAA, và GDPR

4.1.4. Check Point Wireless IPS

- Phân tích hành vi nâng cao
- Bảo vệ chống lại các cuộc tấn công zero-day
- Quản lý tập trung và báo cáo chi tiết
- Tích hợp với nền tảng bảo mật tổng thể Check Point

4.2. Giải pháp mã nguồn mở

4.2.1. Kismet

- Hệ thống phát hiện mạng không dây và IDS
- Hỗ trợ đa nền tảng (Linux, macOS, Windows)
- Phát hiện nhiều loại tấn công không dây
- Cộng đồng phát triển tích cực

4.2.2. Snort Wireless

- Bản mở rộng của Snort cho mạng không dây
- Quy tắc có thể tùy chỉnh cho các mối đe dọa không dây
- Hỗ trợ phân tích giao thức 802.11
- Tích hợp được với nhiều hệ thống SIEM

4.2.3. Suricata với module không dây

- Hỗ trợ đa luồng cho hiệu suất cao
- Khả năng phát hiện đe dọa nâng cao
- Tích hợp với các hệ thống phân tích bảo mật
- Cập nhật quy tắc thường xuyên từ cộng đồng

4.2.4. Zeek (trước đây là Bro)

- Phân tích giao thức mạng không dây chi tiết
- Ngôn ngữ kịch bản mạnh mẽ để tùy chỉnh
- Khả năng giám sát mạng quy mô lớn
- Tích hợp được với các hệ thống bảo mật khác

4.3. Công nghệ tiên tiến trong IDS/IPS không dây

4.3.1. Machine Learning và AI

- Phát hiện bất thường dựa trên học máy
- Giảm thiểu cảnh báo giả
- Tự động phân loại và phản ứng với mối đe dọa
- Khả năng thích ứng với các mẫu tấn công mới

4.3.2. Phân tích hành vi (Behavioral Analytics)

- Thiết lập đường cơ sở hành vi bình thường
- Phát hiện sai lệch và hành vi đáng ngờ
- Giám sát liên tục và học tập theo thời gian
- Cải thiện độ chính xác của phát hiện

4.3.3. Công nghệ SDR (Software-Defined Radio)

- Giám sát linh hoạt trên nhiều tần số
- Khả năng phát hiện tấn công tầng vật lý
- Phân tích phổ tần nâng cao
- Thích ứng với các công nghệ không dây mới

4.3.4. Điện toán biên (Edge Computing)

- Xử lý phát hiện xâm nhập tại điểm truy cập
- Giảm độ trễ trong phản ứng
- Phân tích phân tán cho hiệu suất cao
- Khả năng hoạt động khi mất kết nối với trung tâm

4.4. Xu hướng phát triển

4.4.1. Tích hợp với bảo mật Zero Trust

- Xác thực liên tục cho mọi thiết bị không dây
- Kiểm soát truy cập dựa trên ngữ cảnh
- Đánh giá rủi ro theo thời gian thực
- Kết hợp với các giải pháp NAC (Network Access Control)

4.4.2. Bảo vệ IoT không dây

- Nhận diện và phân loại thiết bị IoT
- Chính sách bảo mật tùy chỉnh cho từng loại thiết bị
- Phát hiện hành vi bất thường của thiết bị
- Cô lập nhanh các thiết bị bị xâm phạm

4.4.3. Tự động hóa phản ứng

- Kịch bản phản ứng tự động
- Tích hợp với SOAR (Security Orchestration, Automation and Response)
- Phối hợp với các hệ thống bảo mật khác
- Giảm thời gian phản ứng với sự cố

4.4.4. Bảo vệ mạng 5G và Wi-Fi 6

- Thích ứng với công nghệ không dây mới
- Xử lý tốc độ truyền dữ liệu cao hơn
- Bảo vệ cho mật độ thiết bị lớn hơn
- Giải quyết các lỗ hổng đặc thù của công nghệ mới

5. Các tiêu chuẩn và quy định liên quan

5.1. Tiêu chuẩn quốc tế

5.1.1. ISO/IEC 27001 và 27002

- Tiêu chuẩn quản lý an toàn thông tin
- Đưa ra các yêu cầu về kiểm soát truy cập mạng và giám sát hệ thống
- Quy định về quản lý sự cố an ninh mạng
- Hướng dẫn triển khai các hệ thống phát hiện và ngăn chặn xâm nhập

5.1.2. NIST Special Publication 800-53

- Khung an ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ
- Đưa ra các kiểm soát bảo mật cho hệ thống thông tin
- Quy định cụ thể về giám sát, phát hiện và phản ứng với xâm nhập
- Yêu cầu về bảo vệ mạng không dây

5.1.3. IEEE 802.11i

- Tiêu chuẩn bảo mật cho mạng không dây (Wi-Fi)
- Quy định về giao thức WPA2/WPA3
- Yêu cầu về xác thực và mã hóa
- Cơ sở cho việc phát hiện các vi phạm bảo mật

5.1.4. Common Criteria (ISO/IEC 15408)

- Khung đánh giá bảo mật cho sản phẩm CNTT
- Đưa ra các yêu cầu chức năng và đảm bảo cho IDS/IPS
- Phân loại các mức độ đảm bảo bảo mật
- Tiêu chí chứng nhận cho các sản phẩm bảo mật

5.2. Quy định tuân thủ ngành

5.2.1. PCI DSS (Payment Card Industry Data Security Standard)

- Yêu cầu bắt buộc sử dụng IDS/IPS (Yêu cầu 11.4)
- Quy định về giám sát mạng không dây (Yêu cầu 11.1)
- Yêu cầu kiểm tra và cập nhật hệ thống thường xuyênĐòi hỏi ghi nhận và phân tích các sự kiện bảo mật

5.2.2. HIPAA (Health Insurance Portability and Accountability Act)

- Quy định bảo vệ thông tin y tế
- Yêu cầu giám sát truy cập mạng và phát hiện xâm nhập
- Quy định về bảo vệ dữ liệu khi truyền qua mạng không dây
- Đòi hỏi đánh giá rủi ro và kiểm toán bảo mật

5.2.3. GDPR (General Data Protection Regulation)

- Quy định bảo vệ dữ liệu cá nhân tại EU
- Yêu cầu về phát hiện và thông báo vi phạm dữ liệu
- Đòi hỏi các biện pháp kỹ thuật phù hợp để bảo vệ dữ liệu
- Ảnh hưởng đến thiết kế và triển khai hệ thống IDS/IPS

5.2.4. SOX (*Sarbanes-Oxley Act*)

- Quy định về tính toàn vẹn của dữ liệu tài chính
- Yêu cầu kiểm soát nội bộ cho hệ thống CNTT
- Đòi hỏi giám sát và ghi nhận hoạt động truy cập
- Ảnh hưởng đến cấu hình và triển khai IDS/IPS

5.3. Khung an ninh mạng và hướng dẫn

5.3.1. NIST Cybersecurity Framework

- Khung tiêu chuẩn về nhận diện, bảo vệ, phát hiện, phản ứng và khôi phục
- Hướng dẫn triển khai các biện pháp giám sát và phát hiện
- Quy trình quản lý sự cố bảo mật
- Đánh giá hiệu quả của hệ thống bảo mật

5.3.2. CIS Controls (*Center for Internet Security*)

- Danh sách 20 biện pháp kiểm soát bảo mật quan trọng
- Hướng dẫn cụ thể về triển khai IDS/IPS (Kiểm soát 12)
- Yêu cầu về bảo vệ mạng không dây (Kiểm soát 15)
- Khuyến nghị về cấu hình và quản lý

5.3.3. ASP Wireless Security Testing Guide

- Hướng dẫn kiểm thử bảo mật không dây
- Phương pháp đánh giá hiệu quả của IDS/IPS không dây
- Danh sách các mối đe dọa phổ biến cần phát hiện
- Kỹ thuật kiểm tra tính hiệu quả của hệ thống

5.3.4. ENISA (*European Union Agency for Cybersecurity*) Guidelines

- Hướng dẫn về bảo mật mạng không dây
- Khuyến nghị về triển khai IDS/IPS
- Quy trình đánh giá rủi ro và quản lý sự cố
- Các biện pháp bảo mật tối thiểu cho mạng không dây

5.4. Quy định quốc gia

5.4.1. Việt Nam

- Luật An toàn thông tin mạng
- Nghị định về bảo vệ thông tin cá nhân
- Quy định về an ninh mạng cho các tổ chức tài chính
- Các tiêu chuẩn về bảo mật mạng không dây

5.4.2. Hoa Kỳ

- FISMA (Federal Information Security Modernization Act)
- Các hướng dẫn của DHS (Department of Homeland Security)
- FCC (Federal Communications Commission) về an toàn không dây
- Quy định riêng cho từng ngành như tài chính, y tế, giáo dục

5.4.3. Liên minh Châu Âu

- NIS Directive (Network and Information Systems Directive)
- eIDAS Regulation (Electronic Identification and Trust Services)
- Các quy định của ENISA về bảo mật mạng
- Luật an ninh mạng của từng quốc gia thành viên

5.5. Thách thức tuân thủ

5.5.1. Xung đột giữa các quy định

- Sự khác biệt giữa quy định các quốc gia
- Thách thức khi triển khai cho tổ chức đa quốc gia
- Cân bằng giữa các yêu cầu khác nhau

5.5.2. Cập nhật liên tục

- Thay đổi thường xuyên trong các quy định
- Nhu cầu cập nhật hệ thống IDS/IPS
- Chi phí và nguồn lực cho việc duy trì tuân thủ

5.5.3. Chứng minh tuân thủ

- Yêu cầu về ghi nhận và báo cáo
- Kiểm toán và đánh giá định kỳ
- Tài liệu hóa cấu hình và chính sách

CHƯƠNG III: PHƯƠNG PHÁP THỰC HIỆN

1. Xây dựng môi trường thực nghiệm

- Thiết lập mạng WiFi thử nghiệm với Access Points, các máy chủ giám sát và sensors
- Cài đặt các thiết bị phần cứng hỗ trợ monitor mode và packet injection
- Triển khai hệ điều hành Linux (Ubuntu Server/Kali Linux)

❖ Mục tiêu chính:

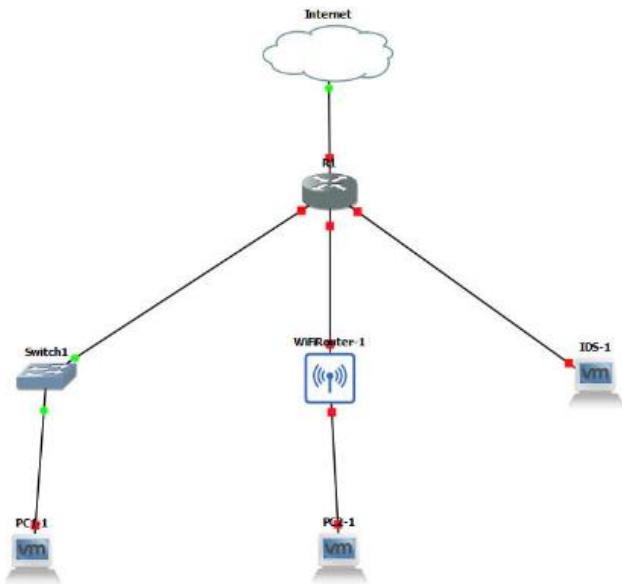
- Phát hiện và ngăn chặn các cuộc tấn công trên mạng không dây.
- Cấu hình Snort làm IDS/IPS để phân tích lưu lượng mạng.
- Sử dụng Zeek để ghi log, phân tích gói tin nâng cao.
- Kiểm tra hệ thống bằng cách mô phỏng các cuộc tấn công phổ biến (DoS, MITM, ARP Spoofing, v.v.).

2. Xây dựng mô hình mạng (Triển khai trên GNS3)

Thiết bị	Chức năng	IP
Router/Gateway	Cung cấp mạng internet	192.168.1.1/24
IDS1 (Ubuntu - Snort & Zeek)	Máy chủ giám sát, phát hiện tấn công	192.168.1.10/24
PC1 (Windows - Máy nạn nhân)	Máy bị tấn công	192.168.1.20/24
PC2 (Windows - Máy tấn công)	Máy thực hiện tấn công	192.168.1.30/24
Switch	Kết nối các thiết bị	-

Sơ đồ mô hình mạng trên GNS3:

- Router kết nối với Switch.
- IDS1 (Ubuntu) được đặt ở chế độ **promiscuous mode** để giám sát toàn bộ lưu lượng.
- PC1 và PC2 kết nối với Switch để mô phỏng tấn công và giám sát.



2. Lựa chọn và triển khai công cụ

- Cài đặt IDS/IPS: Suricata/Snort kết hợp với Kismet
- Cấu hình hệ thống giám sát: Wireshark, tcpdump
- Triển khai hệ thống quản lý log: ELK Stack (Elasticsearch, Logstash, Kibana)

3. Cấu hình IDS/IPS

- Thiết lập các rule phát hiện tấn công mạng không dây phổ biến
- Tích hợp hệ thống cảnh báo và phản ứng tự động
- Tối ưu ngưỡng phát hiện để giảm cảnh báo giả

4. Thủ nghiệm tấn công

- Thực hiện các kịch bản tấn công điển hình:
 - Tấn công WPA/WPA2 handshake
 - Rogue Access Point / Evil Twin
 - Deauthentication Attack
 - KRACK (Key Reinstallation Attack)
 - MITM (Man-in-the-Middle)
- Sử dụng công cụ: Aircrack-ng, Wifite, mdk3/mdk4

5. Thu thập và phân tích dữ liệu

- Ghi lại event logs và cảnh báo từ IDS/IPS
- Đánh giá hiệu suất phát hiện (tỷ lệ phát hiện, tỷ lệ báo động giả)
- Phân tích các chỉ số: True Positive Rate, False Positive Rate, Detection Accuracy

6. Tối ưu hóa hệ thống

- Điều chỉnh rule và cấu hình dựa trên kết quả thử nghiệm
- Xây dựng thêm rule tùy chỉnh cho các mối đe dọa mới
- Tích hợp cơ chế machine learning cải thiện khả năng phát hiện bất thường

7. Xây dựng quy trình triển khai

- Thiết lập quy trình phản ứng với sự cố
- Xây dựng chính sách giám sát và bảo trì hệ thống
- Lập tài liệu hướng dẫn triển khai và vận hành

CHƯƠNG IV: TRIỂN KHAI

Cấu hình và cài đặt Snort

- Nâng cấp toàn bộ hệ thống

```
v@v-VMware-Virtual-Platform:~$ sudo apt-get dist-upgrade -y
[sudo] password for v:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following upgrades have been deferred due to phasing:
  ubuntu-drivers-common
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

Hình 11.Nâng cấp toàn bộ hệ thống

- Cài đặt dịch vụ SSH server

```
v@v-VMware-Virtual-Platform:~$ sudo apt-get install -y openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 1 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,751 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server
amd64 1:9.6p1-3ubuntu13.8 [37.3 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64
  1:9.6p1-3ubuntu13.8 [509 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+2024011
3-1ubuntu2 [275 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 ssh-import-id all 5.
11-0ubuntu2.24.04.1 [10.1 kB]
Fetched 832 kB in 1s (1,325 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 150042 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.6p1-3ubuntu13.8_amd64.deb ...
Unpacking openssh-sftp-server (1:9.6p1-3ubuntu13.8) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.6p1-3ubuntu13.8_amd64.deb ...
Unpacking openssh-server (1:9.6p1-3ubuntu13.8) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.4+20240113-1ubuntu2_all.deb ...
Unpacking ncurses-term (6.4+20240113-1ubuntu2) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu2.24.04.1_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up openssh-sftp-server (1:9.6p1-3ubuntu13.8) ...
Setting up openssh-server (1:9.6p1-3ubuntu13.8) ...
```

Hình 12. Cài đặt dịch vụ SSH Server

- Cài đặt tất cả các công cụ cần thiết để biên dịch phần mềm từ mã nguồn

```
v@v-VMware-Virtual-Platform:~$ sudo apt-get install -y build-essential
[sudo] password for v:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 dpkg-dev fakeroot g++
  g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13
  gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libbinutils libcc1-0
  libctf-nobfd0 libctf0 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-13-dev
  libgprofng0 libhwasan0 libitm1 liblsan0 libquadmath0 libsframe1 libstdc++-13-dev
  libtsan2 libubsan1 lto-disabled-list make
Suggested packages:
  binutils-doc gprofng-gui bzip2-doc debian-keyring g++-multilib g++-13-multilib
  gcc-13-doc gcc-multilib autoconf automake libtool flex bison gcc-doc
  gcc-13-multilib gcc-13-locales gdb-x86-64-linux-gnu git bzr libstdc++-13-doc
  make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2 dpkg-dev
  fakeroot g++ g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13
  gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libbinutils libcc1-0
  libctf-nobfd0 libctf0 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-13-dev
  libgprofng0 libhwasan0 libitm1 liblsan0 libquadmath0 libsframe1 libstdc++-13-dev
  libtsan2 libubsan1 lto-disabled-list make
0 upgraded, 38 newly installed, 0 to remove and 1 not upgraded.
Need to get 55.2 MB of archives.
After this operation, 194 MB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-common amd64 2.42-4ubuntu2.4 [240 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libsframe1 amd64 2.42-4ubuntu2.4 [15.1 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libbinutils amd64 2.42-4ubuntu2.4 [576 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf-nobfd0 amd64 2.42-4ubuntu2.4 [97.3 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf0 amd64 2.42-4ubuntu2.4 [94.5 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libgprofng0 amd64 2.42-4ubuntu2.4 [849 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-x86-64-linux-gnu amd64 2.42-4ubuntu2.4 [2,464 kB]
```

Hình 13. Cài đặt tất cả các công cụ cần thiết để biên dịch phần mềm từ mã nguồn

- Cài đặt các thư viện phát triển (DEV) cần thiết cho việc biên dịch và xây dựng các công cụ an ninh mạng

```
v@v-VMware-Virtual-Platform:~$ sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdbus-1-dev libdumbnet1 libibverbs-dev libnl-3-dev libnl-route-3-dev
  libpcap0.8-dev libpcre16-3 libpcre3 libpcre32-3 libpcrecpp0v5 libpkgconf3 pkgconf
  pkgconf-bin
The following NEW packages will be installed:
  libdbus-1-dev libdumbnet-dev libdumbnet1 libibverbs-dev libnl-3-dev
  libnl-route-3-dev libpcap-dev libpcap0.8-dev libpcre16-3 libpcre3 libpcre3-dev
  libpcre32-3 libpcrecpp0v5 libpkgconf3 pkgconf pkgconf-bin
0 upgraded, 16 newly installed, 0 to remove and 1 not upgraded.
Need to get 2,787 kB of archives.
After this operation, 11.1 MB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 libpkgconf3 amd64 1.8.1-2build1 [30.7 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 pkgconf-bin amd64 1.8.1-2build1 [20.7 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 pkgconf amd64 1.8.1-2build1 [16.8 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libdbus-1-dev amd64 1.14.10-4ubuntu4.1 [190 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1ubuntu2 [30.7 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet-dev amd64 1.17.0-1ubuntu2 [64.5 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-3-dev amd64 3.7.0-0.3build1.1 [99.5 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-route-3-dev amd64 3.7.0-0.3build1.1 [216 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 libibverbs-dev amd64 50.0-2build2 [678 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 libpcap0.8-dev amd64 1.10.4-4.1ubuntu3 [269 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu noble/main amd64 libpcap-dev amd64 1.10.4-4.1ubuntu3 [3,324 B]
Get:12 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre16-3 amd64 2:8.39-1.9-15build1 [165 kB]
Get:13 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:8.39-1.9-15build1 [248 kB]
Get:14 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre32-3 amd64 2:8.39-1.9-15build1 [248 kB]
```

Hình 14. Cài đặt các thư viện phát triển (DEV) cần thiết cho việc biên dịch và xây dựng các công cụ an ninh mạng

- Tạo thư mục “snort_src” và di chuyển đến thư mục đó

```
v@v-VMware-Virtual-Platform:~$ mkdir ~/snort_src
v@v-VMware-Virtual-Platform:~$ cd ~/snort_src/
v@v-VMware-Virtual-Platform:~/snort_src$
```

Hình 15. Tạo thư mục “snort_src” và di chuyển đến thư mục đó

- Tải gói mã nguồn của DAQ phiên bản 2.0.7, một thành phần bắt buộc khi muốn cài đặt Snort từ mã nguồn.

```
v@v-VMware-Virtual-Platform:~/snort_src$ wget https://snort.org/downloads/snort/daq-2.0.7.tar.gz
--2025-03-20 21:54:15-- https://snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving snort.org (snort.org)... 104.16.91.19, 104.16.92.19, 2606:4700::6B10:5B13, ...
Connecting to snort.org (snort.org)|104.16.91.19|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMM0XGB2W5K2F20250320%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250320T145415Z&X-Amz-Expires=36008X-Amz-SignedHeaders=host&X-Amz-Signature=008daf288a38755513a4ed5b64b5db434a9248aa644a37c4b6bebedee0d07745a7 [following]
--2025-03-20 21:54:15-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/025/695/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMM0XGB2W5K2F20250320%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250320T145415Z&X-Amz-Expires=36008X-Amz-SignedHeaders=host&X-Amz-Signature=008daf288a38755513a4ed5b64b5db434a9248aa644a37c4b6bebedee0d07745a7
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|... 16.15.176.183, 3.5.29.75, 16.15.176.6, ...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|16.15.176.183|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515154 (503K) [binary/octet-stream]
Saving to: 'daq-2.0.7.tar.gz'

daq-2.0.7.tar.gz      100%[=====] 503.08K   394KB/s    in 1.3s

2025-03-20 21:54:18 (394 KB/s) - 'daq-2.0.7.tar.gz' saved [515154/515154]

v@v-VMware-Virtual-Platform:~/snort_src$
```

Hình 16. Tải gói mã nguồn của DAQ phiên bản 2.0.7, một thành phần bắt buộc khi muốn cài đặt Snort từ mã nguồn

- Giải nén file

```
v@v-VMware-Virtual-Platform:/snort_src$ tar -xvf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/api/
daq-2.0.7/api/daq.h
daq-2.0.7/api/Makefile.am
daq-2.0.7/api/daq_common.h
daq-2.0.7/api/daq_base.c
daq-2.0.7/api/daq_api.h
daq-2.0.7/api/daq_mod_ops.c
daq-2.0.7/api/Makefile.in
daq-2.0.7/config.sub
daq-2.0.7/ltnain.sh
daq-2.0.7/os-daq-modules/
daq-2.0.7/os-daq-modules/daq-modules-config.in
daq-2.0.7/os-daq-modules/daq_ipfw.c
daq-2.0.7/os-daq-modules/Makefile.am
daq-2.0.7/os-daq-modules/daq_static_modules.h
daq-2.0.7/os-daq-modules/daq_dump.c
daq-2.0.7/os-daq-modules/daq_lpq.c
daq-2.0.7/os-daq-modules/daq_static_modules.c
daq-2.0.7/os-daq-modules/daq_pcaps.c
daq-2.0.7/os-daq-modules/daq_nfq.c
daq-2.0.7/os-daq-modules/daq_nmap.c
daq-2.0.7/os-daq-modules/daq_afpacket.c
daq-2.0.7/os-daq-modules/Makefile.in
daq-2.0.7/compile
daq-2.0.7/install.sh
daq-2.0.7/missing
daq-2.0.7/Makefile.am
daq-2.0.7/aclocal.m4
daq-2.0.7/configure
daq-2.0.7/m4/
daq-2.0.7/m4/sf.m4
daq-2.0.7/m4/lt-obsolete.m4
daq-2.0.7/m4/ltoptions.m4
daq-2.0.7/m4/libtool.m4
daq-2.0.7/m4/ltsugar.m4
daq-2.0.7/m4/cflags_gcc_option.m4
```

Hình 17. Giải nén file

- Di chuyển đến thư mục “daq - 2.0.7”

```
v@v-VMware-Virtual-Platform:/snort_src$ cd daq-2.0.7
v@v-VMware-Virtual-Platform:/snort_src/daq-2.0.7$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for nawk... nawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name linker (nm)... /usr/bin/nm -B
checking the name linker (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-unknown-linux-gnu file names to x86_64-unknown-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-unknown-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dlltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
```

Hình 18. Di chuyển đến thư mục “daq - 2.0.7”

- Biên dịch mã nguồn thành chương trình thực thi

```
v@v-VMware-Virtual-Platform:/snort_src/daq-2.0.7$ make
make all-recursive
make[1]: Entering directory '/home/v/snort_src/daq-2.0.7'
Makign all in api
make[2]: Entering directory '/home/v/snort_src/daq-2.0.7/api'
/bin/bash ..../libtool --tag=CC -mode=compile gcc -DHAVE_CONFIG_H -I. -I. -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c -o daq_base.lo daq_base.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I. -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -fPIC -DPIC -o .libs/daq_base.o
daq_base.c: In function 'daq_load_modules':
daq_base.c:313:28: warning: the comparison will always evaluate as 'false' for the address of 'd_name' will never be NULL [-Waddress]
 313 |         if (de->d_name == NULL)
      |             ^
In file included from /usr/include/dirent.h:61,
                 from daq_base.c:27:
/usr/include/x86_64-linux-gnu/bits/dirent.h:33:10: note: 'd_name' declared here
 33 |     char d_name[256]; /* We must not include limits.h! */
      |
daq_base.c: In function 'daq_config_set_value':
daq_base.c:535:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
 535 |     __FUNCTION__, (unsigned long) sizeof(struct _daq_dict_entry));
      |             ^
daq_base.c:542:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
 542 |     __FUNCTION__, (unsigned long) (strlen(key) + 1));
      |             ^
daq_base.c:555:21: warning: ISO C does not support '__FUNCTION__' predefined identifier [-Wpedantic]
 555 |     __FUNCTION__, (unsigned long) (strlen(value) + 1));
      |             ^
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I. -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_base.lo -MD -MP -MF .deps/daq_base.Tpo -c daq_base.c -o daq_base.o >/dev/null 2>&1
mv -f .deps/daq_base.Tpo .deps/daq_base.Plo
/bin/bash ..../libtool --tag=CC -mode=compile gcc -DHAVE_CONFIG_H -I. -I. -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -MT daq_mod_ops.lo -MD -MP -MF .deps/daq_mod_ops.Tpo -c -o daq_mod_ops.
libtool: install: /usr/bin/install -c libdaq.so libdaq_static.so /usr/local/lib
libtool: install: /usr/bin/install -c libdaq.so.2.0.4 /usr/local/lib/libdaq.so.2.0.4
libtool: install: (cd /usr/local/lib && [ ln -s -f libdaq.so.2.0.4 libdaq.so.2 || { rm -f libdaq.so.2 && ln -s libdaq.so.2.0.4 libdaq.so.2; } ; })
libtool: install: (cd /usr/local/lib && [ ln -s -f libdaq.so.2.0.4 libdaq.so || { rm -f libdaq.so && ln -s libdaq.so.2.0.4 libdaq.so; } ; )
libtool: install: /usr/bin/install -c libls/libdaq_lai /usr/local/lib/libdaq_la
libtool: install: /usr/bin/install -c libls/libdaq_static_lai /usr/local/lib/libdaq_static_la
libtool: install: /usr/bin/install -c libls/libdaq_a /usr/local/lib/libdaq_a
libtool: install: chmod 644 /usr/local/lib/libdaq.a
libtool: install: ranlib /usr/local/lib/libdaq.a
libtool: install: /usr/bin/install -c libls/libdaq_static.a /usr/local/lib/libdaq_static.a
libtool: install: chmod 644 /usr/local/lib/libdaq_static.a
libtool: install: ranlib /usr/local/lib/libdaq_static.a
libtool: finish: PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/snap/bin:/sbin ldconfig -n /usr/local/lib
-----
Libraries have been installed in:
  /usr/local/lib

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:
- add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
  during execution
- add LIBDIR to the 'LD_RUN_PATH' environment variable
  during linking
- use the '-Wl,-rpath -Wl,LIBDIR' linker flag
- have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
-----
/usr/bin/mkdir -p '/usr/local/include'
/usr/bin/install -c -m 644 daq.h daq_api.h daq_common.h '/usr/local/include'
make[2]: Leaving directory '/home/v/snort_src/daq-2.0.7/api'
```

Hình 19. Biên dịch mã nguồn thành chương trình thực thi

- Cài đặt chương trình đã Build vào hệ thống

```
v@v-VMware-Virtual-Platform:/snort_src/daq-2.0.7$ sudo make install
Making Install in api
make[1]: Entering directory '/home/v/snort_src/daq-2.0.7/api'
make[2]: Entering directory '/home/v/snort_src/daq-2.0.7/api'
/usr/bin/mkdir -p '/usr/local/lib'
/bin/bash ..../libtool --mode=install /usr/bin/install -c libdaq.so libdaq_static.so /usr/local/lib
libtool: install: /usr/bin/install -c libdaq.so.2.0.4 /usr/local/lib/libdaq.so.2.0.4
libtool: install: (cd /usr/local/lib && [ ln -s -f libdaq.so.2.0.4 libdaq.so.2 || { rm -f libdaq.so.2 && ln -s libdaq.so.2.0.4 libdaq.so.2; } ; ])
libtool: install: (cd /usr/local/lib && [ ln -s -f libdaq.so.2.0.4 libdaq.so || { rm -f libdaq.so && ln -s libdaq.so.2.0.4 libdaq.so; } ; )
libtool: install: /usr/bin/install -c libls/libdaq_lai /usr/local/lib/libdaq_la
libtool: install: /usr/bin/install -c libls/libdaq_static_lai /usr/local/lib/libdaq_static_la
libtool: install: /usr/bin/install -c libls/libdaq_a /usr/local/lib/libdaq_a
libtool: install: chmod 644 /usr/local/lib/libdaq.a
libtool: install: ranlib /usr/local/lib/libdaq.a
libtool: install: /usr/bin/install -c libls/libdaq_static.a /usr/local/lib/libdaq_static.a
libtool: install: chmod 644 /usr/local/lib/libdaq_static.a
libtool: install: ranlib /usr/local/lib/libdaq_static.a
libtool: finish: PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/snap/bin:/sbin ldconfig -n /usr/local/lib
-----
Libraries have been installed in:
  /usr/local/lib

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:
- add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
  during execution
- add LIBDIR to the 'LD_RUN_PATH' environment variable
  during linking
- use the '-Wl,-rpath -Wl,LIBDIR' linker flag
- have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
-----
/usr/bin/mkdir -p '/usr/local/include'
/usr/bin/install -c -m 644 daq.h daq_api.h daq_common.h '/usr/local/include'
make[2]: Leaving directory '/home/v/snort_src/daq-2.0.7/api'
```

Hình 20. Cài đặt chương trình đã Build vào hệ thống

- Cài đặt các thư viện mã hóa và nén cần thiết

```
v@v-VMware-Virtual-Platform:~/snort_src/daq-2.0.7$ sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.13-0ubuntu3.5).
openssl set to manually installed.
Suggested packages:
  liblzma-doc libssl-doc
The following NEW packages will be installed:
  liblzma-dev libssl-dev zlib1g-dev
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 3,478 kB of archives.
After this operation, 15,5 MB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libssl-dev amd64 3.0.13-0ubuntu3.5 [2,408 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 zlib1g-dev amd64 1:1.3.dfsg-3.1ubuntu2.1 [894 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 liblzma-dev amd64 5.6.1+really5.4.5-1build0.1 [176 kB]
Fetched 3,478 kB in 1s (5,470 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 156213 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.0.13-0ubuntu3.5_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Selecting previously unselected package zlib1g-dev:amd64.
Preparing to unpack .../zlib1g-dev_1%3a1.3.dfsg-3.1ubuntu2.1_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.3.dfsg-3.1ubuntu2.1) ...
Selecting previously unselected package liblzma-dev:amd64.
Preparing to unpack .../liblzma-dev_5.6.1+really5.4.5-1build0.1_amd64.deb ...
Unpacking liblzma-dev:amd64 (5.6.1+really5.4.5-1build0.1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Setting up liblzma-dev:amd64 (5.6.1+really5.4.5-1build0.1) ...
Setting up zlib1g-dev:amd64 (1:1.3.dfsg-3.1ubuntu2.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
v@v-VMware-Virtual-Platform:~/snort_src/daq-2.0.7$
```

Hình 21. Cài đặt các thư viện mã hóa và nén cần thiết

- Cài đặt thư viện phát triển HTTP/2

```
v@v-VMware-Virtual-Platform:~/snort_src/daq-2.0.7$ sudo apt-get install -y libnghttp2-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libnghttp2-doc
The following NEW packages will be installed:
  libnghttp2-dev
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 116 kB of archives.
After this operation, 567 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 libnghttp2-dev amd64 1.59.0-1ubuntu0.2 [116 kB]
Fetched 116 kB in 0s (351 kB/s)
Selecting previously unselected package libnghttp2-dev:amd64.
(Reading database ... 156432 files and directories currently installed.)
Preparing to unpack .../libnghttp2-dev_1.59.0-1ubuntu0.2_amd64.deb ...
Unpacking libnghttp2-dev:amd64 (1.59.0-1ubuntu0.2) ...
Setting up libnghttp2-dev:amd64 (1.59.0-1ubuntu0.2) ...
v@v-VMware-Virtual-Platform:~/snort_src/daq-2.0.7$
```

Hình 22. Cài đặt thư viện phát triển HTTP/2

- Tải mã nguồn Snort phiên bản 2.9.20 về hệ thống

```
v@v-VMware-Virtual-Platform:~/snort_src$ wget https://snort.org/downloads/snort/snort-2.9.20.tar.gz
--2025-03-20 22:29:55-- https://snort.org/downloads/snort/snort-2.9.20.tar.gz
Resolving snort.org (snort.org)... 104.16.91.19, 104.16.92.19, 2606:4700:6810:5b13, ...
Connecting to snort.org (snort.org)|104.16.91.19|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort.org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXG82N5A2f28298328%Fus-east-1%2F3%2Faws4_request&X-Amz-Date=20250320T152956Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=d945df8acb5b8ea2b02c1bccae18f957d18e626d9f760a6fb0dd9e379cd9678 [following]
--2025-03-20 22:29:56-- https://snort.org-site.s3.amazonaws.com/production/release_files/files/000/025/687/original/snort-2.9.20.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXG82N5A2f28298328%Fus-east-1%2F3%2Faws4_request&X-Amz-Date=20250320T152956Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=d945df8acb5b8ea2b02c1bccae18f957d18e626d9f760a6fb0dd9e379cd9678
Resolving snort.org-site.s3.amazonaws.com (snort.org-site.s3.amazonaws.com)... 54.231.130.193, 16.182.98.1, 52.217.164.81, ...
Connecting to snort.org-site.s3.amazonaws.com (snort.org-site.s3.amazonaws.com)|54.231.130.193|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7009894 (6.7M) [binary/octet-stream]
Saving to: 'snort-2.9.20.tar.gz'

snort-2.9.20.tar.gz          100%[=====] 6.68M  2.62MB/s   in 2.6s

2025-03-20 22:30:00 (2.62 MB/s) - 'snort-2.9.20.tar.gz' saved [7009894/7009894]
v@v-VMware-Virtual-Platform:~/snort_src$
```

Hình 23. Tải mã nguồn Snort phiên bản 2.9.20 về hệ thống

- Giải nén file

```
daq-2.0.7  daq-2.0.7.tar.gz  snort-2.9.20.tar.gz
v@v-VMware-Virtual-Platform:~/snort_src$ tar -xzvf snort-2.9.20.tar.gz
snort-2.9.20/
snort-2.9.20/snort.8
snort-2.9.20/install-sh
snort-2.9.20/snort.pc.in
snort-2.9.20/aclocal.m4
snort-2.9.20/config.guess
snort-2.9.20/compile
snort-2.9.20/config.h.in
snort-2.9.20/missing
snort-2.9.20/LICENSE
snort-2.9.20/config.sub
snort-2.9.20/COPYING
snort-2.9.20/templates/
snort-2.9.20/templates/sp_template.c
snort-2.9.20/templates/sp_template.h
snort-2.9.20/templates/spp_template.c
snort-2.9.20/templates/Makefile.in
snort-2.9.20/templates/Makefile.am
snort-2.9.20/templates/spp_template.h
snort-2.9.20/verstuff.pl
snort-2.9.20/Makefile.in
snort-2.9.20/etc/
snort-2.9.20/etc/file_magic.conf
snort-2.9.20/etc/unicode.map
snort-2.9.20/etc/gen-msg.map
snort-2.9.20/etc/attribute_table.dtd
snort-2.9.20/etc/Makefile.in
```

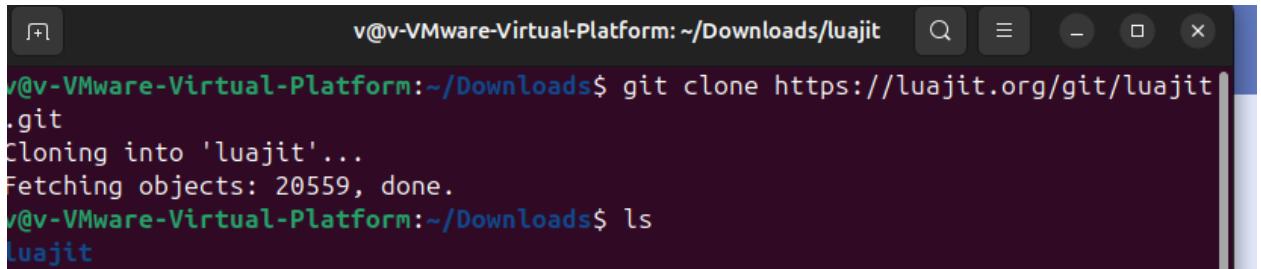
Hình 24. Giải nén file

- Cấu hình Snort để kích hoạt tính năng Sourcefire trước khi biên dịch và cài đặt

```
v@v-Virtual-Platform:~/snort_src/snort-2.9.20$ ./configure --enable-sourcefire
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name linker (nm)... /usr/bin/nm -B
checking the name linker (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
```

Hình 25. Cấu hình Snort để kích hoạt tính năng Sourcefire trước khi biên dịch và cài đặt

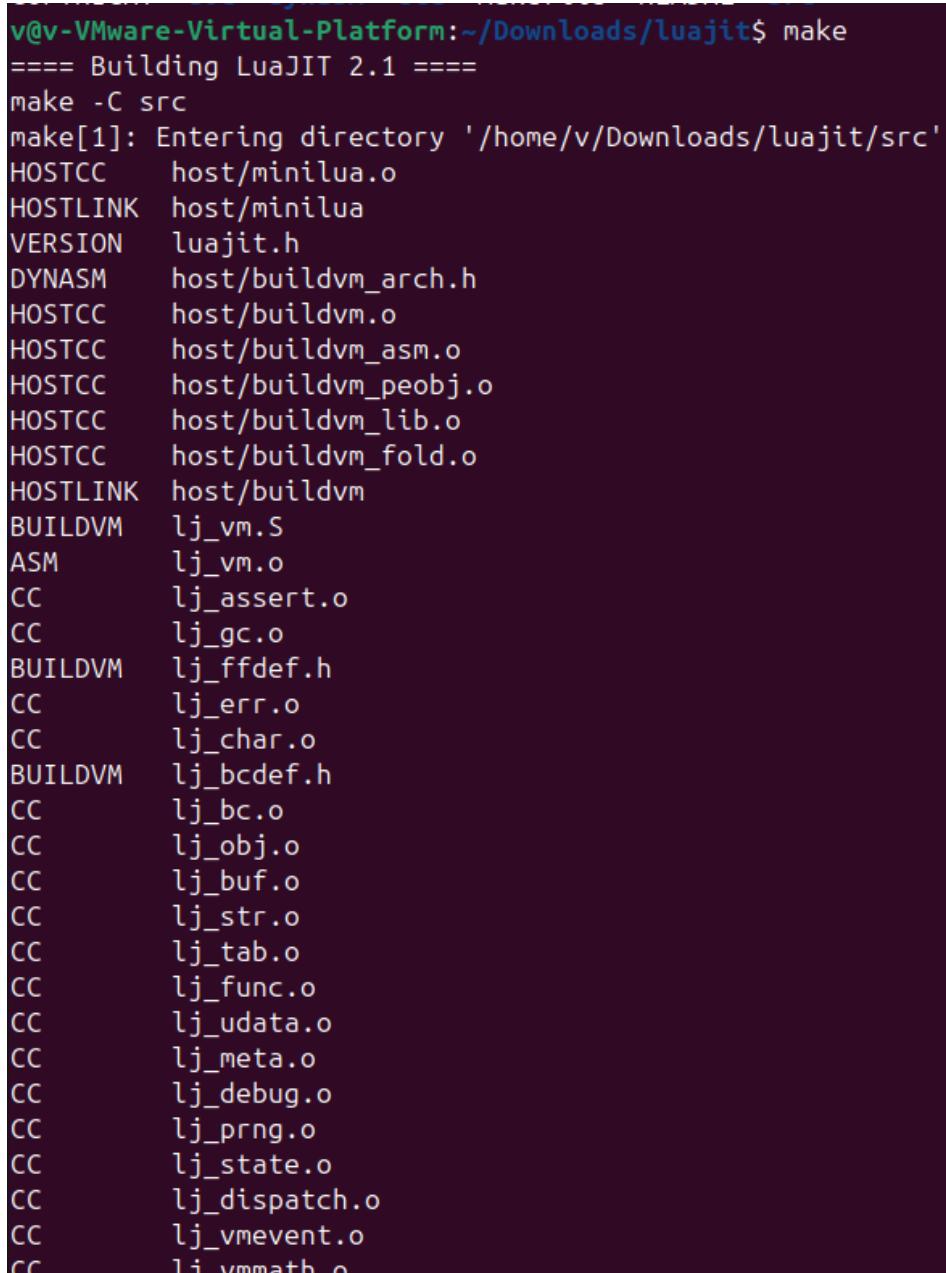
- Tải xuống mã nguồn của LuaJIT



```
v@v-VMware-Virtual-Platform:~/Downloads/luajit$ git clone https://luajit.org/git/luajit.git
Cloning into 'luajit'...
Fetching objects: 20559, done.
v@v-VMware-Virtual-Platform:~/Downloads$ ls
luajit
```

Hình 26. Tải xuống mã nguồn của LuaJIT

- Biên dịch mã nguồn thành chương trình thực thi



```
v@v-VMware-Virtual-Platform:~/Downloads/luajit$ make
==== Building LuaJIT 2.1 ====
make -C src
make[1]: Entering directory '/home/v/Downloads/luajit/src'
HOSTCC host/minilua.o
HOSTLINK host/minilua
VERSION luajit.h
DYNASM host/buildvm_arch.h
HOSTCC host/buildvm.o
HOSTCC host/buildvm_asm.o
HOSTCC host/buildvm_peobj.o
HOSTCC host/buildvm_lib.o
HOSTCC host/buildvm_fold.o
HOSTLINK host/buildvm
BUILDVM lj_vm.S
ASM lj_vm.o
CC lj_assert.o
CC lj_gc.o
BUILDVM lj_ffdef.h
CC lj_err.o
CC lj_char.o
BUILDVM lj_bcdef.h
CC lj_bc.o
CC lj_obj.o
CC lj_buf.o
CC lj_str.o
CC lj_tab.o
CC lj_func.o
CC lj_udata.o
CC lj_meta.o
CC lj_debug.o
CC lj_prng.o
CC lj_state.o
CC lj_dispatch.o
CC lj_vmevent.o
CC lj_vmmath.o
```

Hình 27. Biên dịch mã nguồn thành chương trình thực thi

- Biên dịch mã nguồn thành công

```
v@v-VMware-Virtual-Platform:~/Downloads/luaJIT$ sudo make install
[sudo] password for v:
==== Installing LuaJIT 2.1.1741730670 to /usr/local ====
mkdir -p /usr/local/bin /usr/local/lib /usr/local/include /luajit-2.1 /usr/local/share/man/man1 /usr/local/lib/pkgconfig /usr/local/share/luajit-2.1/jit /usr/local/share/luajit-5.1 /usr/local/lib/lua/5.1
cd src && install -0755 luajit /usr/local/bin/luajit-2.1.1741730670
cd src && test -f libluajit.a && install -m 0644 libluajit.a /usr/local/lib/libluajit-5.1.a || :
rm -f /usr/local/lib/libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so /usr/local/lib/libluajit-5.1.so.2
cd src && test -f libluajit.so && (
    install -m 0755 libluajit.so /usr/local/lib/libluajit-5.1.so.2.1.1741730670 && \
    ( lddconfig -n 2>/dev/null /usr/local/lib || : ) && \
    ln -sf libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so && \
    ln -sf libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so.2 || :
cd etc && install -m 0644 luajit.1 /usr/local/share/man/man1
cd etc && sed -e '$|^prefix=.*|prefix=/usr/local|' -e '$|multilib=.*|multilib=libl|' -e "s|relver=.*|relver=1741730670|" luajit.pc > luajit.pc.tmp && \
install -m 0644 luajit.pc.tmp /usr/local/lib/pkgconfig/luajit.pc && \
rm -f luajit.pc.tmp
cd src && install -m 0644 lua.h luaLlib.h luaLconf.h lua.hpp luajit.h /usr/local/include/luajit-2.1
cd src/jit && install -m 0644 bc.lua bcsave.lua dump.lua p.lua v.lua zone.lua dis_x86.lua dis_x64.lua dis_arm.lua dis_arm64be.lua dis_ppc.lua dis_mips.lua dis_mips64.lua dis_mips64el.lua dis_mips64r6el.lua dis_mips64r6el.lua vmdef.lua /usr/local/share/luajit-2.1/jit
ln -sf luajit-2.1.1741730670 /usr/local/bin/luajit
==== Successfully installed LuaJIT 2.1.1741730670 to /usr/local ====
v@v-VMware-Virtual-Platform:~/Downloads/luaJIT$
```

Hình 28. Biên dịch mã nguồn thành công

- Cài đặt chương trình đã Build vào hệ thống

```
v@v-VMware-Virtual-Platform:~/Downloads/luaJIT$ sudo make install
[sudo] password for v:
==== Installing LuaJIT 2.1.1741730670 to /usr/local ====
mkdir -p /usr/local/bin /usr/local/lib /usr/local/include /luajit-2.1 /usr/local/share/man/man1 /usr/local/lib/pkgconfig /usr/local/share/luajit-2.1/jit /usr/local/share/luajit-5.1 /usr/local/lib/lua/5.1
cd src && install -0755 luajit /usr/local/bin/luajit-2.1.1741730670
cd src && test -f libluajit.a && install -m 0644 libluajit.a /usr/local/lib/libluajit-5.1.a || :
rm -f /usr/local/lib/libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so /usr/local/lib/libluajit-5.1.so.2
cd src && test -f libluajit.so && (
    install -m 0755 libluajit.so /usr/local/lib/libluajit-5.1.so.2.1.1741730670 && \
    ( lddconfig -n 2>/dev/null /usr/local/lib || : ) && \
    ln -sf libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so && \
    ln -sf libluajit-5.1.so.2.1.1741730670 /usr/local/lib/libluajit-5.1.so.2 || :
cd etc && install -m 0644 luajit.1 /usr/local/share/man/man1
cd etc && sed -e '$|^prefix=.*|prefix=/usr/local|' -e '$|multilib=.*|multilib=libl|' -e "s|relver=.*|relver=1741730670|" luajit.pc > luajit.pc.tmp && \
install -m 0644 luajit.pc.tmp /usr/local/lib/pkgconfig/luajit.pc && \
rm -f luajit.pc.tmp
cd src && install -m 0644 lua.h luaLlib.h luaLconf.h lua.hpp luajit.h /usr/local/include/luajit-2.1
cd src/jit && install -m 0644 bc.lua bcsave.lua dump.lua p.lua v.lua zone.lua dis_x86.lua dis_x64.lua dis_arm.lua dis_arm64be.lua dis_ppc.lua dis_mips.lua dis_mips64.lua dis_mips64el.lua dis_mips64r6el.lua dis_mips64r6el.lua vmdef.lua /usr/local/share/luajit-2.1/jit
ln -sf luajit-2.1.1741730670 /usr/local/bin/luajit
==== Successfully installed LuaJIT 2.1.1741730670 to /usr/local ====
v@v-VMware-Virtual-Platform:~/Downloads/luaJIT$
```

Hình 29. Cài đặt chương trình đã Build vào hệ thống

- Cấu hình phần mềm để sử dụng thư viện tirpc, vốn là một thư viện hỗ trợ giao tiếp qua Remote Procedure Call (RPC) trong hệ thống

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ ./configure CFLAGS="-I/usr/include/tirpc" LDFLAGS="-L/usr/include/tirpc -ltirpc"
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets ${MAKE}... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to osidot,rgives... ,/usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
```

Hình 30. Cấu hình phần mềm để sử dụng thư viện tirpc, vốn là một thư viện hỗ trợ giao tiếp qua Remote Procedure Call (RPC) trong hệ thống

- Biên dịch mã nguồn thành chương trình thực thi

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ make
make all-recursive
make[1]: Entering directory '/home/v/snort_src/snort-2.9.20'
Making all in src
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src'
Making all in sfutil
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/sfutil'
gcc -DHAVE_CONFIG_H -I . -I .. -I ... -I ./src -I . -I ./src/portsutil -I /usr/include pcap -I . -I ./src/output-plugins -I . -I ./src/detection-plugins -I . -I ./src/dynamic-plugins -I . -I ./src/preprocessors -I . -I ./src/preprocessors/portscan -I . -I ./src/preprocessors/HttpInspect/include -I . -I ./src/preprocessors/session -I . -I ./src/preprocessors/Stream6 -I . -I ./src/target-based -I . -I ./src/control -I . -I ./src/file-process -I . -I ./src/file-process/libs -I . -I ./src/side-channel -I . -I ./src/side-channel/plugins -I . -I ./src/reload-adjust -DLZMA -DGRE -DMPLS -DPMM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -DFEAT_OPEN_APPID -DHAVE_LIBLUAJIT -I /usr/include/tirpc -DSF_VISIBILITY -fvisibility-hidden -Wall -c -o sfhash.c sfhash.c
gcc -DHAVE_CONFIG_H -I . -I .. -I ... -I ./src -I . -I ./src/sfutil -I /usr/include pcap -I . -I ./src/output-plugins -I . -I ./src/detection-plugins -I . -I ./src/dynamic-plugins -I . -I ./src/preprocessors -I . -I ./src/preprocessors/portscan -I . -I ./src/preprocessors/HttpInspect/include -I . -I ./src/preprocessors/session -I . -I ./src/preprocessors/Stream6 -I . -I ./src/target-based -I . -I ./src/control -I . -I ./src/file-process -I . -I ./src/file-process/libs -I . -I ./src/side-channel -I . -I ./src/side-channel/plugins -I . -I ./src/reload-adjust -DLZMA -DGRE -DMPLS -DPMM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -DFEAT_OPEN_APPID -DHAVE_LIBLUAJIT -I /usr/include/tirpc -DSF_VISIBILITY -fvisibility-hidden -Wall -c -o sfhashfcn.c sfhashfcn.c
gcc -DHAVE_CONFIG_H -I . -I .. -I ... -I ./src -I . -I ./src/sfutil -I /usr/include pcap -I . -I ./src/output-plugins -I . -I ./src/detection-plugins -I . -I ./src/dynamic-plugins -I . -I ./src/preprocessors -I . -I ./src/preprocessors/portscan -I . -I ./src/preprocessors/HttpInspect/include -I . -I ./src/preprocessors/session -I . -I ./src/preprocessors/Stream6 -I . -I ./src/target-based -I . -I ./src/control -I . -I ./src/file-process -I . -I ./src/file-process/libs -I . -I ./src/side-channel -I . -I ./src/side-channel/plugins -I . -I ./src/reload-adjust -DLZMA -DGRE -DMPLS -DPMM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -DFEAT_OPEN_APPID -DHAVE_LIBLUAJIT -I /usr/include/tirpc -DSF_VISIBILITY -fvisibility-hidden -Wall -c -o sfhashfcn.o sfhashfcn.c
gcc -DHAVE_CONFIG_H -I . -I .. -I ... -I ./src -I . -I ./src/sfutil -I /usr/include pcap -I . -I ./src/output-plugins -I . -I ./src/detection-plugins -I . -I ./src/dynamic-plugins -I . -I ./src/preprocessors -I . -I ./src/preprocessors/portscan -I . -I ./src/preprocessors/HttpInspect/include -I . -I ./src/preprocessors/session -I . -I ./src/preprocessors/Stream6 -I . -I ./src/target-based -I . -I ./src/control -I . -I ./src/file-process -I . -I ./src/file-process/libs -I . -I ./src/side-channel -I . -I ./src/side-channel/plugins -I . -I ./src/reload-adjust -DL7MA -DGRE -DMPLS -DPMM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -DFEAT_OPEN_APPID -DHAVE_LIBLUAJIT -I /usr/include/tirpc -DSF_VISIBILITY -fvisibility-hidden -Wall -c -o sfthd.o sfthd.c
gcc -DHAVE_CONFIG_H -I . -I .. -I ... -I ./src -I . -I ./src/sfutil -I /usr/include pcap -I . -I ./src/output-plugins -I . -I ./src/detection-plugins -I . -I ./src/dynamic-plugins -I . -I ./src/preprocessors -I . -I ./src/preprocessors/portscan -I . -I ./src/preprocessors/HttpInspect/include -I . -I ./src/preprocessors/session -I . -I ./src/preprocessors/Stream6 -I . -I ./src/target-based -I . -I ./src/control -I . -I ./src/file-process -I . -I ./src/file-process/libs -I . -I ./src/side-channel -I . -I ./src/side-channel/plugins -I . -I ./src/reload-adjust -DLZMA -DGRE -DMPLS -DPMM_MGR -DNDEBUG -DENABLE_REACT -DENABLE_RESPOND -DENABLE_RESPONSE3 -DSF_WCHAR -DTARGET_BASED -DPERF_PROFILING -DSNORT_RELOAD -DNO_NON_ETHER_DECODER -DNORMALIZER -DACTIVE_RESPONSE -DFEAT_OPEN_APPID -DHAVE_LIBLUAJIT -I /usr/include/tirpc -DSF_VISIBILITY -fvisibility-hidden -Wall -c -o sfhash.o sfhash.c
```

Hình 31. Biên dịch mã nguồn thành chương trình thực thi

- Cài đặt chương trình đã Build vào hệ thống

```
make: [snort] tclsh: no such file or directory, Error: 1  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo make install  
Making install in src  
make[1]: Entering directory '/home/v/snort_src/snort-2.9.20/src'  
Making install in sfutil  
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src/sfutil'  
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/sfutil'  
make[3]: Nothing to be done for 'install-exec-am'.  
make[3]: Nothing to be done for 'install-data-am'.  
make[3]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/sfutil'  
make[2]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/sfutil'  
Making install in win32  
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src/win32'  
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/win32'  
make[3]: Nothing to be done for 'install-exec-am'.  
make[3]: Nothing to be done for 'install-data-am'.  
make[3]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/win32'  
make[2]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/win32'  
Making install in output-plugins  
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src/output-plugins'  
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/output-plugins'  
make[3]: Nothing to be done for 'install-exec-am'.  
make[3]: Nothing to be done for 'install-data-am'.  
make[3]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/output-plugins'  
make[2]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/output-plugins'  
Making install in detection-plugins  
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
make[3]: install-am  
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
make[4]: Entering directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
make[4]: Nothing to be done for 'install-exec-am'.  
make[4]: Nothing to be done for 'install-data-am'.  
make[4]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
make[3]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
make[2]: Leaving directory '/home/v/snort_src/snort-2.9.20/src/detection-plugins'  
Making install in dynamic-plugins  
make[2]: Entering directory '/home/v/snort_src/snort-2.9.20/src/dynamic-plugins'  
Making install in sf_engine  
make[3]: Entering directory '/home/v/snort_src/snort-2.9.20/src/dynamic-plugins/sf_engine'  
make[3]: install-recursive  
make[4]: Entering directory '/home/v/snort_src/snort-2.9.20/src/dynamic-plugins/sf_engine'  
make[4]: install in examples
```

Hình 32.Cài đặt chương trình đã Build vào hệ thống

- Cập nhật bộ nhớ cache của thư viện động trong hệ thống, tạo một liên kết mềm từ “/usr/local/bin/snort” đến “/usr/sbin/snort”. Điều này có nghĩa là có thể gọi snort từ bất kỳ đâu trong hệ thống. Cuối cùng là kiểm tra phiên bản hiện tại của Snort.

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo ldconfig
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ snort -V

      -*> Snort! <-
o" )~ Version 2.9.20 GRE (Build 82)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.10.4 (with TPACKET_V3)
    Using PCRE version: 8.39 2016-06-14
    Using ZLIB version: 1.3

v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$
```

Hình 33. Cập nhật bộ nhớ cache của thư viện động trong hệ thống, tạo một liên kết mềm từ “/usr/local/bin/snort” đến “/usr/sbin/snort”. Điều này có nghĩa là có thể gọi snort từ bất kỳ đâu trong hệ thống. Cuối cùng là kiểm tra phiên bản hiện tại của Snort

- Tạo ra một nhóm người dùng mới có tên là “snort” và tạo ra một người dùng hệ thống có tên là “snort”, nhưng không có quyền đăng nhập vào hệ thống, mục đích để quản lý hoặc chạy Snort mà không cần quyền truy cập trực tiếp vào shell.

```
g: groupadd: cannot lock /etc/group, try again later.
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo groupadd snort
[sudo] password for v:
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ mkdir /etc/snort
```

Hình 34. Tạo ra một nhóm người dùng mới có tên là “snort” và tạo ra một người dùng hệ thống có tên là “snort”, nhưng không có quyền đăng nhập vào hệ thống, mục đích để quản lý hoặc chạy Snort mà không cần quyền truy cập trực tiếp vào shell

- Tạo một số thư mục cấu hình và triển khai Snort

```
mkutu: cannot create directory /etc/snort: permission denied
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort/rules
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort/rules/iplist
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort/preproc_rules
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /usr/local/lib/snort_dynamicrules
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort/so_rules
```

Hình 35. Tạo một số thư mục cấu hình và triển khai Snort

- Tạo ra các tệp rỗng để cấu hình

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo touch /etc/snort/rules/iplist/black_list.rules
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo touch /etc/snort/rules/iplist/white_list.rules
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo touch /etc/snort/rules/local.rules
```

Hình 36. Tạo ra các tệp rỗng để cấu hình

- Tạo một số thư mục mới trong hệ thống

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /etc/snort/sid-msg.map  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /var/log/snort  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo mkdir /var/log/snort/archived_logs
```

Hình 37. Tạo một số thư mục mới trong hệ thống

- Thay đổi quyền truy cập cho các thư mục. Với quyền “5775”, người sở hữu và nhóm có quyền đọc, ghi và thực thi trên các tệp và thư mục, trong khi người dùng khác chỉ có thể đọc và thực thi mà không có quyền thay đổi.

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /etc/snort/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /var/lo  
local/ lock/ log/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /var/log/snort/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /var/log/snort/archived_logs/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /etc/snort/snort_rules/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /usr/local/lib/snort  
snort/ snort_dynamicpreprocessor/  
snort_dynamicengine/ snort_dynamicrules/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules/
```

Hình 38. Thay đổi quyền truy cập cho các thư mục. Với quyền “5775”, người sở hữu và nhóm có quyền đọc, ghi và thực thi trên các tệp và thư mục, trong khi người dùng khác chỉ có thể đọc và thực thi mà không có quyền thay đổi

- Thay đổi chủ sở hữu và nhóm sở hữu của các thư mục và tệp liên quan đến Snort, đảm bảo rằng chỉ người dùng và nhóm snort có quyền truy cập và quản lý các tệp quan trọng của Snort.

```
try chmod +nhttp for more information.  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chown -R snort:snort /etc/snort/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chown -R snort:snort /var/log/snort/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chown -R 5775 /usr/local/lib/snort_dynamicrules/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ ls -ld /usr/local/lib/snort_dynamicrules/  
drwsrwxr-t 2 5775 root 4096 Mar 21 02:05 /usr/local/lib/snort_dynamicrules/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules/  
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$
```

Hình 39. Chỉ người dùng và nhóm Snort có quyền truy cập và quản lý

- Sao chép các tệp cấu hình quan trọng, tệp bản đồ SID, và các tệp định nghĩa kiểu tài liệu vào thư mục cấu hình của Snort

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/etc$ sudo cp *.config* /etc/snort/
[sudo] password for v:
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/etc$ sudo cp *.map /etc/snort/
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/etc$ sudo cp *.dtd /etc/snort/
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/etc$ cd ..
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$
```

Hình 40.Sao chép các tệp cấu hình quan trọng, tệp bản đồ SID, và các tệp định nghĩa kiểu tài liệu vào thư mục cấu hình của Snort

- Hiển thị cấu trúc thư mục của thư mục dưới dạng cây

```
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20$ cd src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ tree /etc/snort/
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ tree /etc/snort/
Command 'tree' not found, but can be installed with:
sudo snap install tree # version 2.1.3+pkg-5852, or
sudo apt install tree # version 2.1.1-2
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo apt install tree
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  tree
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 47.1 kB of archives.
After this operation, 111 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu noble/universe amd64 tree amd64 2.1.1-2ubuntu3 [47.1 kB]
Fetched 47.1 kB in 1s (83.6 kB/s)
Selecting previously unselected package tree.
(Reading database ... 157625 files and directories currently installed.)
Preparing to unpack .../tree_2.1.1-2ubuntu3_amd64.deb ...
Unpacking tree (2.1.1-2ubuntu3) ...
Setting up tree (2.1.1-2ubuntu3) ...
Processing triggers for man-db (2.12.0-4build2) ...
v@v-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ 
doanh@doanh-virtual-machine:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ tree /etc/snort/
/etc/snort/
└── attribute_table.dtd
    ├── classification.config
    ├── file_magic.conf
    ├── gen-msg.map
    └── preproc_rules
        ├── reference.config
        └── rules
            ├── iplists
            │   ├── black_list.rules
            │   └── white_list.rules
            └── local.rules
    └── sid-msg.map
    └── snort.conf
    └── so_rules
    └── threshold.conf
    └── unicode.map

4 directories, 12 files
```

Hình 41. Hiển thị cấu trúc thư mục của thư mục dưới dạng cây

- Tìm dòng có chứa include “\$RULES_PATH” trong tệp cấu hình snort.conf và thay thế nó thành “#include \$RULES_PATH”, tức là bình luận hóa dòng này, khiến Snort không bao gồm các tệp quy tắc từ đường dẫn “\$RULES_PATH” trong cấu hình.

```
vav-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor$ sudo sed -i "s/include \$RULES_PATH/#include \$RULES_PATH/" /etc/snort.conf  
[sudo] password for v:  
vav-VMware-Virtual-Platform:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicprocessor$ sudo nano /etc/snort/snort.conf
```

- Sửa dòng này thành ip của máy chủ

```
# Setup the network addresses you are protecting  
ipvar HOME_NET 192.168.71.150/24
```

Hình 42. Sửa dòng này thành ip của máy chủ

- Thêm đường dẫn

```
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplist
var BLACK_LIST_PATH /etc/snort/rules/iplist
```

Hình 43. Thêm hướng dẫn

- Yêu cầu Snort kiểm tra cấu hình mà không bắt đầu phân tích lưu lượng mạng thực tế

```
deanh@ubuntu:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ snort -T -L ens33 -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 8888 8899 9000 9066 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHLLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ODBC_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3555 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5006 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 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 8089 8090 8118 8123 8180:8181 8243 8280 8300 8888 8899 9000 9066 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search Method = AC_Full_O
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 26
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic rules found in /etc/snort/snort_dynamicrules.
WARNING: No dynamic detection libs from /usr/local/lib/snort_dynamicrules.
Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor...
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_ftptelnet_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_s7compplus_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_icmp6_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_gtp_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_dnp_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_dnp3_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_reputation_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_stp_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_dccp_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_dces_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so... done
Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor/libsf_appld_preproc.so... done
Finished loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
```

Hình 44. Yêu cầu Snort kiểm tra cấu hình mà không bắt đầu phân tích lưu lượng mạng thực tế

- Cấu hình thành công

```
Total snort Fixed Memory Cost - MaxRss:48000
Snort successfully validated the configuration!
Snort exiting
```

Hình 45. Cấu hình thành công

- Mở file nano đến tệp “/etc/snort/rules/local.rules”

```
$ sudo nano /etc/snort/rules/local.rules
```

Hình 46. Mở file nano đến tệp “/etc/snort/rules/local.rules”

- Viết quy tắc gửi cảnh báo khi nhận được một gói ICMP từ bất kỳ nguồn nào đến mạng nội bộ của.

```
doanh@ubuntu: ~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ nano /etc/snort/rules/local.rules
GNU nano 6.2
alert icmp any any -> $HOME_NET any (msg:"ICMP test Detected"; sid:10000001; rev:1; classtype:icmp-event;)
```

Hình 47. - Viết quy tắc gửi cảnh báo khi nhận được một gói ICMP từ bất kỳ nguồn nào đến mạng nội bộ

- Mở file nano đến tệp “/etc/snort/sid-msg.map”

```
$ sudo nano /etc/snort/sid-msg.map
```

Hình 48. Mở file nano đến tệp “/etc/snort/sid-msg.map”

- Viết một đoạn mô tả chi tiết quy tắc Snort

```
doanh@ubuntu: ~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ nano /etc/snort/sid-msg.map
GNU nano 6.2
gld,1 || sid,10000001 || ref,001 || classification, icmp-event || priority,0 || mgs, ICMP Test Detected || url,tools.ietf.org/html.rfc792,
```

Hình 49. Viết một đoạn mô tả chi tiết quy tắc Snort

- Yêu cầu Snort thực hiện kiểm tra cấu hình mà không thực sự bắt đầu giám sát lưu lượng mạng

```
doanh@ubuntu: ~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo nano /etc/snort/snort.conf
Running In Test mode
==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initialization Complete!
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 809
0 8118 8123 8180:8181 8243 8288 8300 8800 8888 8899 9000 9068 9980 9990:9991 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 'TELNET_PORTS' defined : [ 23 53 69 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 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 8288 8300 8800 8888 8899 9000 9068 9980 9990:9991 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method=Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
```

Hình 50. Yêu cầu Snort thực hiện kiểm tra cấu hình mà không thực sự bắt đầu giám sát lưu lượng mạng

- Kiểm tra thành công

```
Total snort Fixed Memory Cost - MaxRss:48256
Snort successfully validated the configuration!
Snort exiting
```

Hình 51. Kiểm tra thành công

- Thử dùng máy Ubuntu ping đến 8.8.8.8 và kết quả thu được

The screenshot shows two terminal windows side-by-side. The left window displays Snort test results for ICMP events on interface ens33, with many entries for ICMP test detected from 192.168.71.152 to 8.8.8.8. The right window shows ping statistics from 8.8.8.8 to 8.8.8.8, with a minimum average round-trip time (RTT) of 28.30 ms.

```

doanh@ubuntu: ~
Snort exiting
doanh@ubuntu: /snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ cd ..
doanh@ubuntu: /snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib$ cd
doanh@ubuntu: $ sudo snort -A console -q -u snort -c /etc/snort/snort.conf -l ens3
ERROR: Can't start DAQ (-1) - SIOCDEVIFNAME: No such device!
Fatal Error. Quitting...
doanh@ubuntu: $ sudo /usr/local/bin/snort -A console -q -u snort -c /etc/snort/snort.conf -l ens33
04/05/11:37:39.400096 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:40.504374 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:41.503333 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:42.402716 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:43.416957 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:44.388475 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:45.388464 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:46.401479 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:47.415855 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:48.539506 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:49.397600 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:50.418436 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:51.415706 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:52.552433 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority y: 3] [(ICMP) 8.8.8.8 -> 192.168.71.152]
04/05/11:37:53.487779 [**] [1:1000000001:1] ICMP test Detected [**] [Classification: Generic ICMP event] [Priority
doanh@ubuntu: ~
rtt min/avg/max/mdev = 28.30/48.018/185.167/39.133 ms
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=51.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=153 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=279 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=153 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=63.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=34.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=30.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=43.7 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=128 time=75.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=128 time=178 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=128 time=36.5 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=128 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=128 time=53.1 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=128 time=187 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=128 time=122 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=128 time=62.7 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=128 time=179 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=128 time=181 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=128 time=28.9 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=128 time=33.8 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=128 time=36.7 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=128 time=29.7 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=128 time=29.7 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=128 time=36.6 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=128 time=29.1 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=128 time=31.4 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=128 time=28.4 ms
64 bytes from 8.8.8.8: icmp_seq=28 ttl=128 time=29.8 ms
64 bytes from 8.8.8.8: icmp_seq=29 ttl=128 time=46.6 ms
64 bytes from 8.8.8.8: icmp_seq=30 ttl=128 time=50.4 ms
64 bytes from 8.8.8.8: icmp_seq=31 ttl=128 time=38.7 ms
64 bytes from 8.8.8.8: icmp_seq=32 ttl=128 time=35.3 ms
64 bytes from 8.8.8.8: icmp_seq=33 ttl=128 time=34.6 ms
--- 8.8.8.8 ping statistics ---

```

Hình 52. Thử dùng máy Ubuntu ping đến 8.8.8.8 và kết quả thu được

- Chính sửa tệp “snort.conf”



Hình 53. Chính sửa tệp “snort.conf”

- Tại Step 6, thêm “output unified2: filename snort.u2, limit 128”

```

#####
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuration
#####

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128,
output unified2: filename snort.u2, limit 128

```

Hình 54. Tại Step 6, thêm “output unified2: filename snort.u2, limit 128”

- Tải tệp mã nguồn của Barnyard2 từ GitHub và lưu nó với tên barnyard2-Master.tar.gz trên hệ thống của bạn

```
doanh@ubuntu:~$ wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-Master.tar.gz
--2025-03-24 16:11:35-- https://github.com/firnsy/barnyard2/archive/master.tar.gz
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/firnsy/barnyard2/tar.gz/refs/heads/master [following]
--2025-03-24 16:11:36-- https://codeload.github.com/firnsy/barnyard2/tar.gz/refs/heads/master
Resolving codeload.github.com (codeload.github.com)... 20.205.243.165
Connecting to codeload.github.com (codeload.github.com)|20.205.243.165|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: 'barnyard2-Master.tar.gz'

barnyard2-Master.tar.gz      [ =>                               ] 433,66K   650KB/s   in 0,7s

2025-03-24 16:11:37 (650 KB/s) - 'barnyard2-Master.tar.gz' saved [444071]
```

Hình 55. Tải tệp mã nguồn của Barnyard2 từ GitHub và lưu nó với tên barnyard2-Master.tar.gz trên hệ thống của bạn

- Giải nén file

```
doanh@ubuntu:~$ tar zxvf barnyard2-Master.tar.gz
barnyard2-master/
barnyard2-master/.gitignore
barnyard2-master/COPYING
barnyard2-master/LICENSE
barnyard2-master/Makefile.am
barnyard2-master/README
barnyard2-master/RELEASE.NOTES
barnyard2-master/autogen.sh
barnyard2-master/configure.ac
barnyard2-master/doc/
barnyard2-master/doc/INSTALL
barnyard2-master/doc/Makefile.am
barnyard2-master/doc/README.aruba
barnyard2-master/doc/README.database
barnyard2-master/doc/README.sguil
barnyard2-master/doc/README.sig_suppress
barnyard2-master/doc/README.snortsam
barnyard2-master/etc/
barnyard2-master/etc/Makefile.am
barnyard2-master/etc/barnyard2.conf
barnyard2-master/m4/
barnyard2-master/m4/Makefile.am
barnyard2-master/m4/libprelude.m4
barnyard2-master/rpm/
barnyard2-master/rpm/Makefile.am
```

Hình 56. Giải nén file

- Di chuyển vào thư mục “barnyard2-master/” sau đó yêu cầu autoreconf tạo lại tất cả các tệp cấu hình cần thiết cho dự án phần mềm từ các tệp mẫu hiện có, sử dụng các macro tùy chỉnh từ thư mục ./m4/

```
doanh@ubuntu:~$ cd barnyard2-master/
doanh@ubuntu:~/barnyard2-master$ autoreconf -fvi -I ./m4/
autoreconf: export WARNING=_
autoreconf: Entering directory '.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal -I ./m4/ --force -I m4
autoreconf: configure.ac: tracing
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
autoreconf: configure.ac: not using Intltool
autoreconf: configure.ac: not using Gtkdoc
autoreconf: running: aclocal -I ./m4/ --force -I m4
autoreconf: running: /usr/bin/autoconf --include=./m4/ --force
configure.ac:7: warning: 'AM_CONFIG_HEADER': this macro is obsolete.
configure.ac:7: You should use the 'AC_CONFIG_HEADERS' macro instead.
./lib/autoconf/general.m4:2434: AC_DIAGNOSE is expanded from...
aclocal.m4:781: AM_CONFIG_HEADER is expanded from...
configure.ac:7: the top level
configure.ac:26: warning: The macro `AC_PROG_CC_STDC' is obsolete.
configure.ac:26: You should run autoupdate.
./lib/autoconf/c.m4:1666: AC_PROG_CC_STDC is expanded from...
configure.ac:26: the top level
configure.ac:28: warning: The macro `AC_PROG_LIBTOOL' is obsolete.
configure.ac:28: You should run autoupdate.
```

Hình 57. Di chuyển vào thư mục “barnyard2-master/” sau đó yêu cầu autoreconf tạo lại tất cả các tệp cấu hình cần thiết cho dự án phần mềm từ các tệp mẫu hiện có, sử dụng các macro tùy chỉnh từ thư mục ./m4/

- Lệnh này tạo một liên kết tượng trưng (symlink) từ “/usr/include/dnet.h” đến “/usr/include/dumbnet.h”

```
doanh@ubuntu:~/barnyard2-master$ sudo ln -s /usr/include/dumbnet.h /usr/include/dnet.h
doanh@ubuntu:~/barnyard2-master$ sudo ldconfig
sudo: ldconfig: command not found
doanh@ubuntu:~/barnyard2-master$ sudo ldconfig
doanh@ubuntu:~/barnyard2-master$
```

Hình 58. Lệnh này tạo một liên kết tượng trưng (symlink) từ “/usr/include/dnet.h” đến “/usr/include/dumbnet.h”

- Cấu hình phần mềm để nó có thể sử dụng MySQL trong quá trình biên dịch. Trình cấu hình sẽ tìm các thư viện MySQL cần thiết trong thư mục “`/usr/lib/x86_64-linux-gnu`” và đảm bảo rằng phần mềm có thể tích hợp với MySQL trong quá trình biên dịch và sử dụng

```
doanh@ubuntu:~/barnyard2-master$ ./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu/
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk...
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether the compiler supports GNU C... yes
checking whether gcc accepts -g... yes
checking for gcc option to enable C11 features... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... none
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
```

Hình 59. Cấu hình phần mềm để nó có thể sử dụng MySQL trong quá trình biên dịch

```

make[1]: Entering directory '/home/doanh/barnyard2-master'
Making all in src
make[2]: Entering directory '/home/doanh/barnyard2-master/src'
make[3]: Entering directory '/home/doanh/barnyard2-master/src/sfutil'
make[3]: Nothing to be done for 'all'.
make[3]: Leaving directory '/home/doanh/barnyard2-master/src/sfutil'
make[2]: Leaving directory '/home/doanh/barnyard2-master/src'
make[1]: Leaving directory '/home/doanh/barnyard2-master'
make[1]: Entering directory '/home/doanh/barnyard2-master/src/output-plugins'
gcc -DHAVE_CONFIG_H -I../../ -I.. -I../sfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o spo_database.o spo_database.c
gcc -DHAVE_CONFIG_H -I.. -I.. -I.. -I../sfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o spo_database_cache.o spo_database_cache.c
spo_database_cache.c: In function 'signatureReferenceCacheUpdateOld':
spo_database_cache.c:1301:13: warning: 'memset' used with length equal to number of elements without multiplication by element size [-Wmemset-elt-size]
5301 |         memset(sigRefArr, '\0', MAX_REF_OBJ);
|             ^
rm -f libbspp.a
ar cr libbspp.a spo_alert_arubacontrol.o spo_alert_bro.o spo_alert_csv.o spo_alert_fast.o spo_alert_full.o spo_alert_fwsan.o spo_alert_prelude.o spo_alert_syslog.o spo_alert_test.o spo_alert_untsock.o spo_common.o spo_log_ascii.o spo_log_null.o spo_log_tcpdump.o spo_sgull.o spo_echidna.o spo_syslog_full.o spo_database.o spo_database_cache.o
ar: 'u' modifier ignored since 'D' is the default (see 'U')
ranlib libbspp.a
make[3]: Leaving directory '/home/doanh/barnyard2-master/src/output-plugins'
make[1]: Entering directory '/home/doanh/barnyard2-master/src/input-plugins'
make[3]: Entering directory '/home/doanh/barnyard2-master/src/input-plugins'
gcc -DHAVE_CONFIG_H -I../../ -I.. -I../sfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o spi_unified2.o spi_unified2.c
spi_unified2.c: In function 'Unfiled2ReadRecord':
spi_unified2.c:166:25: warning: variable 'record_type' set but not used [-Wunused-but-set-variable]
166 |     uint32_t record_type;
|             ^
rm -f libbspi.a
ar cr libbspi.a spi_unified2.o
ar: 'u' modifier ignored since 'D' is the default (see 'U')
ranlib libbspi.a
make[3]: Leaving directory '/home/doanh/barnyard2-master/src/input-plugins'
make[3]: Entering directory '/home/doanh/barnyard2-master/src'
make[3]: Entering directory '/home/doanh/barnyard2-master/src'
gcc -DHAVE_CONFIG_H -I.. -I.. -Isfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o barnyard2.o barnyard2.c
gcc -DHAVE_CONFIG_H -I.. -I.. -Isfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o debug.o debug.c
gcc -DHAVE_CONFIG_H -I.. -I.. -Isfutil -I/usr/include/mysql -DENABLE_MYSQL -g -O2 -Wall -c -o decode.o decode.c
|
|           const struct DAQ_PktHdr_t *
In file included from decode.c:41:
decode.h:1851:29: note: expected 'const DAQ_PktHdr_t *' [aka 'const struct _daq_pkthdr *'] but argument is of type 'const struct DAQ_PktHdr_t *'
1851 | void DecodeEtherPkt(Packet_t, const DAQ_PktHdr_t *, const uint8_t *);
|
decode.c:95:35: warning: passing argument 2 of 'DecodeIEEE80211Pkt' from incompatible pointer type [-Wincompatible-pointer-types]

```

Hình 60. Trình cấu hình sẽ tìm các thư viện MySQL cần thiết trong thư mục “/usr/lib/x86_64-linux-gnu/”

```

doanh@ubuntu:~/barnyard2-master$ sudo make install
Making install in src
make[1]: Entering directory '/home/doanh/barnyard2-master/src'
  Making install in sfutil
  make[2]: Entering directory '/home/doanh/barnyard2-master/src/sfutil'
    make[3]: Entering directory '/home/doanh/barnyard2-master/src/sfutil'
      make[3]: Nothing to be done for 'install-exec-am'.
      make[3]: Nothing to be done for 'install-data-am'.
    make[3]: Leaving directory '/home/doanh/barnyard2-master/src/sfutil'
  make[2]: Leaving directory '/home/doanh/barnyard2-master/src/sfutil'
  Making install in output-plugins
  make[2]: Entering directory '/home/doanh/barnyard2-master/src/output-plugins'
  make[3]: Entering directory '/home/doanh/barnyard2-master/src/output-plugins'
    make[3]: Nothing to be done for 'install-exec-am'.
    make[3]: Nothing to be done for 'install-data-am'.
  make[3]: Leaving directory '/home/doanh/barnyard2-master/src/output-plugins'
  make[2]: Leaving directory '/home/doanh/barnyard2-master/src/output-plugins'
  Making install in input-plugins
  make[2]: Entering directory '/home/doanh/barnyard2-master/src/input-plugins'
  make[3]: Entering directory '/home/doanh/barnyard2-master/src/input-plugins'
    make[3]: Nothing to be done for 'install-exec-am'.
    make[3]: Nothing to be done for 'install-data-am'.
  make[3]: Leaving directory '/home/doanh/barnyard2-master/src/input-plugins'
  make[2]: Leaving directory '/home/doanh/barnyard2-master/src/input-plugins'
  make[2]: Entering directory '/home/doanh/barnyard2-master/src'
  make[3]: Entering directory '/home/doanh/barnyard2-master/src'
    make[3]: Nothing to be done for 'install-exec-am'.
    make[3]: Nothing to be done for 'install-data-am'.
  make[3]: Leaving directory '/home/doanh/barnyard2-master/src'
  make[2]: Leaving directory '/home/doanh/barnyard2-master/src'
  make[2]: Entering directory '/home/doanh/barnyard2-master/usr/local/bin'
    /bin/install/mkdir -p /usr/local/bin
    /bin/install/lbtool --mode=install /usr/bin/install -c barnyard2 /usr/local/bin/barnyard2
  make[3]: Nothing to be done for 'install-data-am'.
  make[3]: Leaving directory '/home/doanh/barnyard2-master/src'
  make[2]: Leaving directory '/home/doanh/barnyard2-master/src'
  make[1]: Leaving directory '/home/doanh/barnyard2-master/src'
  Making install in etc
  make[1]: Entering directory '/home/doanh/barnyard2-master/etc'
  make[2]: Entering directory '/home/doanh/barnyard2-master/etc'

```

Hình 61. Đảm bảo rằng phần mềm có thể tích hợp với MySQL trong quá trình biên dịch và sử dụng

- Kiểm tra phiên bản Barnyard2

```

doanh@ubuntu:~/barnyard2-master$ /usr/local/bin/barnyard2 -V

      _-*> Barnyard2 <*-_
 / ,,_ \ Version 2.1.14 (Build 337)
 |o" )~| By Ian Firns (SecurixLive): http://www.securixlive.com/
 + ' ' + (C) Copyright 2008-2013 Ian Firns <firnsy@securixlive.com>

doanh@ubuntu:~/barnyard2-master$
```

Hình 62. Kiểm tra phiên bản Barnyard2

- Kiểm tra vị trí thư mục

```

doanh@ubuntu:~/barnyard2-master$ sudo cp -r ~/snort_src/ ./
doanh@ubuntu:~/barnyard2-master$ pwd
/home/doanh/barnyard2-master
doanh@ubuntu:~/barnyard2-master$
```

Hình 63. Kiểm tra vị trí thư mục

- Sao chép tệp “**barnyard2.conf**” từ thư mục của dự án Barnyard2 (ở “**/home/doanh/barnyard2-master/etc/**”) vào thư mục cấu hình của Snort (“**/etc/snort/**”)

```

doanh@ubuntu:~/barnyard2-master$ sudo cp /home/doanh/barnyard2-master/etc/barnyard2.conf /etc/snort/

```

Hình 64. Sao chép tệp “**barnyard2.conf**” từ thư mục của dự án Barnyard2 (ở “**/home/doanh/barnyard2-master/etc/**”) vào thư mục cấu hình của Snort (“**/etc/snort/**”)

- Tạo thư mục và cấp quyền

```
doanh@ubuntu:~/barnyard2-master$ sudo mkdir /var/log/barnyard2
doanh@ubuntu:~/barnyard2-master$ sudo chown snort.snort /var/log/barnyard2/
doanh@ubuntu:~/barnyard2-master$ sudo touch /var/log/snort/barnyard2.waldo
doanh@ubuntu:~/barnyard2-master$ sudo chown snort.snort /var/log/barnyard2.waldo
chown: cannot access '/var/log/barnyard2.waldo': No such file or directory
doanh@ubuntu:~/barnyard2-master$ sudo chown snort.snort /var/log/snort/barnyard2.waldo
doanh@ubuntu:~/barnyard2-master$ █
```

Hình 65.Tạo thư mục và cấp quyền

- Khởi chạy MySQL

```
ERROR 1045 (28000): Access denied for user 'doanh'@'localhost' (using password: YES)
doanh@ubuntu:~/barnyard2-master$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.41-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

Hình 66. Khởi chạy MySQL

- Tạo cơ sở dữ liệu

Hình 67. Tao CSDL

- Tạo một người dùng mới tên “**snort**” trong MySQL hoặc MariaDB với mật khẩu “**“snortpass”**”. Người dùng này chỉ có thể kết nối với cơ sở dữ liệu từ **localhost**
- Cấp cho người dùng **snort** quyền **tạo, chèn, chọn, xóa và cập nhật** trên tất cả các bảng trong cơ sở dữ liệu **snort**. Người dùng này chỉ có thể sử dụng các quyền này khi kết nối từ **localhost**

```
mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'snortpass';
Query OK, 0 rows affected (0,00 sec)

mysql> grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';
Query OK, 0 rows affected (0,00 sec)

mysql>
```

Hình 68. Người dùng chỉ có thể sử dụng các quyền này khi kết nối từ localhost

```
Examples:
output database: log, mysql, user=snort password=snortpass dbname=snort host=localhost sensor_name=sensor01
      output database: alert, postgresql, user=snort dbname=snort
```

- Cấp quyền cho tệp cấu hình

```
doanh@ubuntu:~/barnyard2-master$ sudo chmod o-r /etc/snort/barnyard2.conf
[sudo] password for doanh:
```

Hình 69. Cấp quyền cho tệp cấu hình

- Khởi chạy Barnyard2 để xử lý các sự kiện và cảnh báo từ Snort

```
doanh@ubuntu:/var/log/snort$ sudo /usr/local/bin/barnyard2 -c /etc/snort/snort.conf -v -d /var/log/snort/ -f snort.u2
Running in Continuous mode

    --== Initializing Barnyard2 ==-
Initializing Input Plugins!
Initializing Output Plugins!
Parsing config file "/etc/snort/snort.conf"
ERROR: /etc/snort/snort.conf(45) Unknown rule type: ipvar.
Fatal Error, Quitting..
Barnyard2 exiting
=====
Record Totals:
  Records:          0
  Events:          0 (0.000%)
  Packets:         0 (0.000%)
  Unknown:         0 (0.000%)
  Suppressed:      0 (0.000%)
=====
Packet breakdown by protocol (includes rebuilt packets):
  ETH: 0          (0.000%)
  ETHdisc: 0       (0.000%)
  VLAN: 0          (0.000%)
  IPV6: 0          (0.000%)
  IP6 EXT: 0       (0.000%)
  IP6opts: 0        (0.000%)
  IP6disc: 0        (0.000%)
  IP4: 0          (0.000%)
  IP4disc: 0        (0.000%)
  TCP 6: 0          (0.000%)
  UDP 6: 0          (0.000%)
  ICMP6: 0          (0.000%)
  ICMP-IP: 0        (0.000%)
  TCP: 0          (0.000%)
  UDP: 0          (0.000%)
  ICMP: 0          (0.000%)
  TCPdisc: 0        (0.000%)
  UDPdisc: 0        (0.000%)
  ICMPdis: 0        (0.000%)
  FRAG: 0          (0.000%)
  FRAG 6: 0          (0.000%)
  ARP: 0          (0.000%)
  EAPOL: 0          (0.000%)
  ETHLOOP: 0        (0.000%)
  IPX: 0          (0.000%)
  OTHER: 0          (0.000%)
  DISCARD: 0        (0.000%)
  InvChkSum: 0        (0.000%)
  S5 G 1: 0          (0.000%)
  S5 G 2: 0          (0.000%)
  Total: 0          (0.000%)
=====

doanh@ubuntu:/var/log/snort$
```

Hình 70. Khởi chạy Barnyard2 để xử lý các sự kiện và cảnh báo từ Snort

- Thủ ping đến một địa chỉ và kiểm tra kết quả

```

doanh@ubuntu:/var/log/snort$ sudo /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort -a /var/log/snort/archived_log
Running in continuous mode

    === Initializing Barnyard2 ===
Initializing Input Plugins!
Initializing Output Plugins!
Parsing config file "/etc/snort/barnyard2.conf"

+[ Signature Suppress list ]
-----+
+[No entry in Signature Suppress List]+
-----+
+[ Signature Suppress list ]+
-----+
Barnyard2 spooler: Event cache size set to [2048]
Log directory = /var/log/barnyard2
INFO database: Defaulting Reconnect/Transaction Error limit to 10
INFO database: Defaulting Reconnect sleep time to 5 second
[SignatureReferencePullDatabaseStore(): No Reference found in database ...]
database: compiled support for (mysql)
database: configured to use mysql
database: scheme version = 10
database: default host = localhost
database: user = snort
database: database name = snort
database: sensor name = sensor01
database: sensor id = 1
database: sensor ctd = 16
database: data encoding = hex
database: detail level = full
database: ignore_bpf = no
database: using the "log" facility

    === Initialization Complete ===

/`--> Barnyard2 <=.
`--> Version 2.1.14 (Build 337)
`--> By Ian Frans (SecurixLive): http://www.securixlive.com/
`--> + (C) Copyright 2008-2013 Ian Frans <ifrsy@securixlive.com>

Using waldo file '/var/log/snort/barnyard2.waldo':
spool directory = /var/log/snort
spool filebase = snort.u2
time_stamp = 1743830323
record_id = 0
Opening log file '/var/log/snort/snort.u2.1743830323'
Waiting for new data
04/05/13:12:43.802150 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:44.803166 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:45.796260 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:46.812054 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:47.822813 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:48.823052 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
04/05/13:12:49.826398 [**] [1:1000000001:1] Snort Alert [1:1000000001::1] [**] [Classification: Generic ICMP event] [Priority: 3] [ICMP] 8.8.8.8 -> 192.168.71.152
`*** Caught Int-Signal
Barnyard2 exiting
database: Closing connection to database "snort"
=====
Record totals:
  Records: 14
  Events: 7 (50.000%)
  Packets: 7 (50.000%)
  Unknown: 0 (0.000%)
  Suppressed: 0 (0.000%)
=====
Packet breakdown by protocol (includes rebuilt packets):
  IP: 7 (100.000%)
  ETH: 0 (0.000%)
  VLAN: 0 (0.000%)
  IPV6: 0 (0.000%)
  IP6 EXT: 0 (0.000%)
  IP6opts: 0 (0.000%)
  IP6disc: 0 (0.000%)
  IP4: 7 (100.000%)
  IP4disc: 0 (0.000%)
  TCP: 0 (0.000%)
  UDP: 0 (0.000%)
  ICMP: 0 (0.000%)
  ICMP-IP: 0 (0.000%)
  TCP: 0 (0.000%)
  UDP: 0 (0.000%)
  ICMP: 7 (100.000%)
  TCPdisc: 0 (0.000%)
  UDPdisc: 0 (0.000%)
  ICMPdisc: 0 (0.000%)
  FRAG: 0 (0.000%)
  FRAG: 0 (0.000%)
  ARP: 0 (0.000%)
  ARP: 0 (0.000%)
  EAPOL: 0 (0.000%)
  EAPOL: 0 (0.000%)
  ETH: 0 (0.000%)
  IPVX: 0 (0.000%)
  OTHER: 0 (0.000%)
  DISCARD: 0 (0.000%)
  InvChkSum: 0 (0.000%)
  SS G 1: 0 (0.000%)
  SS G 2: 0 (0.000%)
  Total: 7
=====
Closing spool file '/var/log/snort/snort.u2.1743830323'. Read 14 records
doanh@ubuntu:/var/log/snort$
```

- Kết nối đến cơ sở dữ liệu “snort” với người dùng “snort”, sau đó thực hiện một câu truy vấn SQL để đếm số lượng bản ghi trong bảng event

```
doanh@ubuntu:/var/log/snort$ sudo mysql -u snort -p -D snort -e "select count(*) from event"
Enter password:
+-----+
| count(*) |
+-----+
|      22 |
+-----+
doanh@ubuntu:/var/log/snort$
```

Hình 72. Kết nối đến cơ sở dữ liệu “snort” với người dùng “snort”, sau đó thực hiện một câu truy vấn SQL để đếm số lượng bản ghi trong bảng event

- Tạo tệp cấu hình “snort.service”

```
doanh@ubuntu:/var/log/snort$ sudo nano /lib/systemd/system/snort.service
```

Hình 73. Tạo tệp cấu hình “snort.service”

- Thêm nội dung sau vào tệp và lưu lại

```
GNU nano 6.2
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

[Install]
WantedBy=multi-user.target
```

Hình 74. Thêm nội dung vào tệp và lưu lại

- Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort

```
doanh@ubuntu:/var/log/snort$ sudo systemctl enable snort
doanh@ubuntu:/var/log/snort$ sudo systemctl start snort
doanh@ubuntu:/var/log/snort$ sudo systemctl status snort
● snort.service - Snort NIDS Daemon
   Loaded: loaded (/lib/systemd/system/snort.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-04-05 12:18:43 +07; 57min ago
     Main PID: 21370 (sudo)
        Tasks: 3 (limit: 4549)
       Memory: 40.8M
          CPU: 163ms
         CGroup: /system.slice/snort.service
                   ├─21370 sudo /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
                   └─21371 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

Th 4 05 12:18:43 ubuntu systemd[1]: Started Snort NIDS Daemon.
Th 4 05 12:18:43 ubuntu sudo[21370]:      root : PMD=/ ; USER=root ; COMMAND=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
Th 4 05 12:18:43 ubuntu sudo[21370]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
doanh@ubuntu:/var/log/snort$
```

Hình 75. Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort

- Tạo tệp cấu hình “barnyard2.serverce”

```
doanh@ubuntu:/var/log/snort$ sudo nano /lib/systemd/system/barnyard2.service
```

Hình 76. Tạo tệp cấu hình “barnyard2.serverce”

- Tệp có nội dung như sau



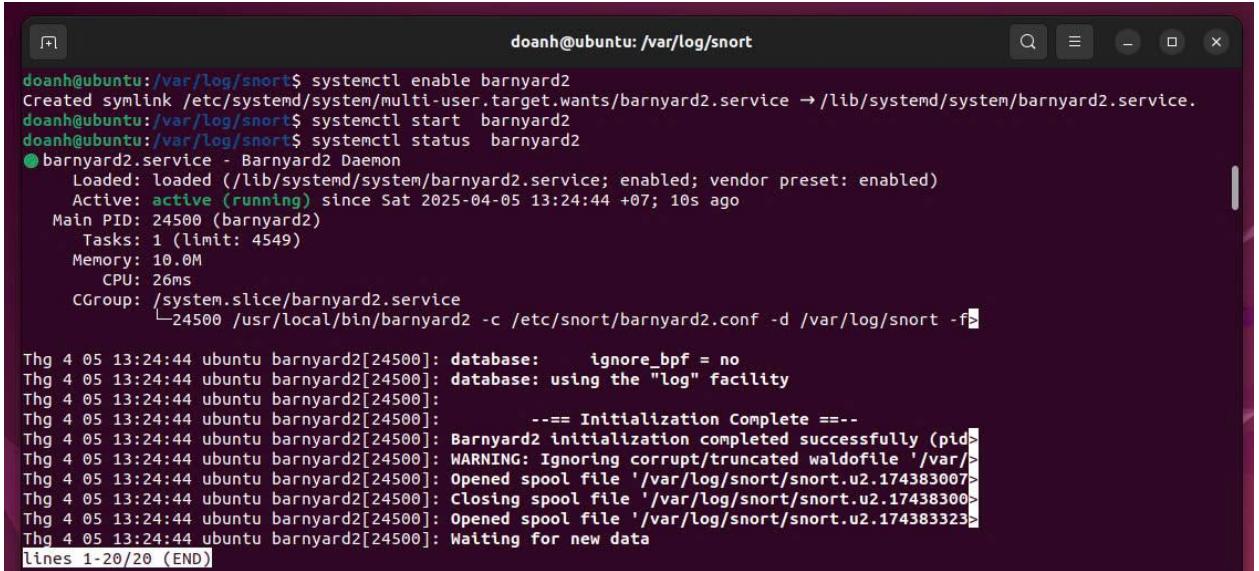
```
doanh@ubuntu:/var/log/snort
[doanh]
Description=Barnyard2 Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -q -w /var/log/snort/barnyard2.waldo -g snort -u snort -D -a /var/log/snort/archived_logs

[Install]
WantedBy=multi-user.target
```

Hình 77. Tệp có nội dung sau

- Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort



```
doanh@ubuntu:/var/log/snort$ systemctl enable barnyard2
Created symlink /etc/systemd/system/multi-user.target.wants/barnyard2.service → /lib/systemd/system/barnyard2.service.
doanh@ubuntu:/var/log/snort$ systemctl start barnyard2
doanh@ubuntu:/var/log/snort$ systemctl status barnyard2
● barnyard2.service - Barnyard2 Daemon
   Loaded: loaded (/lib/systemd/system/barnyard2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-04-05 13:24:44 +07; 10s ago
     Main PID: 24500 (barnyard2)
        Tasks: 1 (limit: 4549)
       Memory: 10.0M
          CPU: 26ms
        CGroup: /system.slice/barnyard2.service
               ↳ 24500 /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f

Thg 4 05 13:24:44 ubuntu barnyard2[24500]: database: ignore_bpf = no
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: database: using the "log" facility
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: === Initialization Complete ===
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: Barnyard2 initialization completed successfully (pid
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: WARNING: Ignoring corrupt/truncated walofile '/var/
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: Opened spool file '/var/log/snort/snort.u2.174383007>
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: Closing spool file '/var/log/snort/snort.u2.17438300>
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: Opened spool file '/var/log/snort/snort.u2.174383323>
Thg 4 05 13:24:44 ubuntu barnyard2[24500]: Waiting for new data
lines 1-20/20 (END)
```

Hình 78. Kích hoạt dịch vụ Snort, khởi động lại dịch vụ và kiểm tra, hiển thị trạng thái hiện tại của dịch vụ Snort

- Thêm kho lưu trữ “ppa:ondrej/php” vào danh sách các kho lưu trữ của hệ thống

```
doanh@ubuntu:/var/log/snort$ sudo add-apt-repository ppa:ondrej/php
PPA publishes dbgsym, you may need to include 'main/debug' component
Repository: deb https://ppa.launchpadcontent.net/ondrej/php/ubuntu/ jammy main
Description: Co-installable PHP versions: PHP 5.6, PHP 7.x, PHP 8.x and most requested extensions are included. Only supported Ubuntu Releases (https://wiki.ubuntu.com/Releases) are provided.
Debian oldstable and stable packages are provided as well: https://deb.sury.org/#debian-dpa
You can get more information about the packages at https://deb.sury.org
BUG&FEATURES: This PPA now has a issue tracker:
https://deb.sury.org/#bug-reporting

CAVEATS:
1. If you are using php-gearman, you need to add ppa:ondrej/pkg-gearman
2. If you are using apache2, you are advised to add ppa:ondrej/apache2
3. If you are using nginx, you are advised to add ppa:ondrej/nginx-mainline
or ppa:ondrej/nginx

PLEASE READ: If you like my work and want to give me a little motivation, please consider donating regularly: https://donate.sury.org/
WARNING: add-apt-repository is broken with non-UTF-8 locales, see
https://github.com/oerdnj/deb.sury.org/issues/56 for workaround:
# LC_ALL=C.UTF-8 add-apt-repository ppa:ondrej/php
More info: https://launchpad.net/~ondrej/+archive/ubuntu/php
Adding repository...
Press [ENTER] to continue or Ctrl-c to cancel.
Adding deb entry to /etc/apt/sources.list.d/ondrej-ubuntu-php-jammy.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/ondrej-ubuntu-php-jammy.list
Adding key to /etc/apt/trusted.gpg.d/ondrej-ubuntu-php.gpg with fingerprint BBDC7E53946656EFBCE4C1DD710AEAA84AD4CAB6
Http: http://ppa.launchpadcontent.net/ondrej/ubuntu/jammy/main InRelease
Http: http://ppa.launchpadcontent.net/ondrej/ubuntu/jammy-security InRelease
Http: http://ppa.launchpadcontent.net/ondrej/ubuntu/jammy-updates InRelease
Http: http://ppa.launchpadcontent.net/ondrej/ubuntu/jammy-backports InRelease
Hit:4 https://deb.nodesource.com/node\_18.x nodistro InRelease
Get:5 https://security.ubuntu.com/ubuntu/jammy-security InRelease [129 kB]
Hit:6 https://repo.mongodb.org/apt/ubuntu/focal/mongodb-org/6.0 InRelease
Get:7 https://ppa.launchpadcontent.net/ondrej/php/ubuntu/jammy InRelease [24,6 kB]
Hit:8 https://ppa.launchpadcontent.net/ondrej/ubuntu/jammy InRelease
Hit:9 https://ppa.launchpadcontent.net/ondrej/ubuntu/jammy/universe InRelease
Get:10 https://ppa.launchpadcontent.net/ondrej/ubuntu/jammy/main amd64 Packages [43,3 kB]
Get:11 https://ppa.launchpadcontent.net/ondrej/ubuntu/jammy/main amd64 Packages [137 kB]
Get:12 https://security.ubuntu.com/ubuntu/jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Get:13 https://security.ubuntu.com/ubuntu/jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
Get:14 https://ppa.launchpadcontent.net/ondrej/php/ubuntu/jammy/main i386 Packages [37,1 kB]
Get:15 https://ppa.launchpadcontent.net/ondrej/php/ubuntu/jammy/main Translation-en [42,8 kB]
Fetched 544 kB in 226 ms (226 kB/s)
Reading package lists... Done
W: https://repo.mongodb.org/apt/ubuntu/dists/focal/mongodb-org/6.0/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
```

Hình 79. Thêm kho lưu trữ “ppa:ondrej/php” vào danh sách các kho lưu trữ của hệ thống

- Cài đặt Apache và PHP 5.6 cùng với các phần mở rộng và mô-đun cần thiết để PHP hoạt động trên Apache

Hình 80. Cài đặt Apache và PHP 5.6 cùng với các phần mở rộng và mô-đun cần thiết để PHP hoạt động trên Apache

- Tải về phiên bản ADODB 5.20.8 từ SourceForge, là thư viện hỗ trợ tương tác cơ sở dữ liệu trong PHP5

```
[root@ubuntu ~]# 5 wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz
--2025-04-05 13:55:37... https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz
Resolving sourceforge.net (sourceforge.net)... 104.18.13.149, 104.18.12.149, 2606:4700::6812:d95, ...
Connecting to sourceforge.net (sourceforge.net)|104.18.13.149|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz/ [following]
--2025-04-05 13:55:38... https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz/
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz/download [following]
--2025-04-05 13:55:39... https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-5.20.8.tar.gz/download
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://downloads.sourceforge.net/project/adodb/adodb-php5-only/adodb-5.20.8.tar.gz?ts=gAAAAABnBPrQcZDmZlsVlFAeRTPJ9N2PEwfBrBfDvUlu272gs9lcw_SKVOEUB70diWGoP7c2zeHbx8yH
N2knpfrqV0Kq3Dk3DwMs...&mirror=cyfuture&r=[following]
--2025-04-05 13:55:40... https://downloads.sourceforge.net/project/adodb/adodb-php5-only/adodb-5.20.8.tar.gz?ts=gAAAAABnBPrQcZDmZlsVlFAeRTPJ9N2PEwfBrBfDvUlu272gs9lcw_SKVOEUB70diW
GorZrczZrJnMjNpquKg3Kp...&mirror=cyfuture&r=[following]
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 104.18.12.149, 104.18.13.149, 2606:4700::6812:c95, ...
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)|104.18.12.149|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://cyfuture.dl.sourceforge.net/project/adodb/adodb-php5-only/adodb-5.20.8.tar.gz?vlasf=1 [following]
--2025-04-05 13:55:40... https://cyfuture.dl.sourceforge.net/project/adodb/adodb-php5-only/adodb-5.20.8.tar.gz?vlasf=1
Resolving cyfuture.dl.sourceforge.net (cyfuture.dl.sourceforge.net)... 49.50.119.27
Connecting to cyfuture.dl.sourceforge.net (cyfuture.dl.sourceforge.net)|49.50.119.27|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 420255 (410K) [application/x-gzip]
saving to: 'adodb-5.20.8.tar.gz'

adodb-5.20.8.tar.gz          100%[=====] 410,41K 496KB/s   in 0,8s

2025-04-05 13:55:45 (496 KB/s) - 'adodb-5.20.8.tar.gz' saved [420255/420255]
```

Hình 81. Tải về phiên bản ADODB 5.20.8 từ SourceForge, là thư viện hỗ trợ tương tác cơ sở dữ liệu trong PHP5

- Giải nén file

```
doanh@ubuntu:~/snort_src$ tar -xvzf adodb-5.20.8.tar.gz
adodb/
adodb/xmlschema.dtd
adodb/adodb_pager.inc.php
adodb/adodb_csvlib.inc.php
adodb/adodb_time.inc.php
adodb/adodb_exceptions.inc.php
adodb/cute_icons_for_site/
adodb/cute_icons_for_site/adodb.gif
adodb/cute_icons_for_site/adodb2.gif
adodb/adodb-lib.inc.php
adodb/pivottable.inc.php
adodb/adodb-active-recordx.inc.php
adodb/datadict/
adodb/datadict/datadict-generic.inc.php
adodb/datadict/datadict-mssqlnative.inc.php
adodb/datadict/datadict-postgres.inc.php
adodb/datadict/datadict-sqlite.inc.php
adodb/datadict/datadict-mysql.inc.php
adodb/datadict/datadict-mssql.inc.php
adodb/datadict/datadict-sybase.inc.php
adodb/datadict/datadict-ibase.inc.php
adodb/datadict/datadict-oci8.inc.php
adodb/datadict/datadict-access.inc.php
adodb/datadict/datadict-informix.inc.php
adodb/datadict/datadict-sapdb.inc.php
adodb/datadict/datadict-db2.inc.php
adodb/datadict/datadict-firebird.inc.php
adodb/adodb_xmlschema.inc.php
adodb/session/
adodb/session/old/
adodb/session/old/adodb_cryptsession.php
adodb/session/old/adodb_session_clob.php
adodb/session/old/adodb_session.php
adodb/session/adodb_encrypt_md5.php
adodb/session/adodb_sessions_oracle_clob.sql
adodb/session/adodb_encrypt_secret.php
adodb/session/adodb_cryptsession.php
adodb/session/adodb_encrypt_mcrypt.php
adodb/session/adodb_session_clob2.php
adodb/session/adodb_session2.php
adodb/session/adodb_sess.txt
adodb/session/adodb_session_clob.php
adodb/session/adodb_sessions_mysql.sql
adodb/session/adodb_session.php
adodb/session/adodb_compress_bztp2.php
adodb/session/adodb_sessions_oracle.sql
adodb/session/adodb_compress_gzlp.php
adodb/session/crypt.inc.php
adodb/session/session_schema2.xml
adodb/session/adodb_cryptsession2.php
adodb/session/session_schema.xml
```

Hình 82. Giải nén file

- Di chuyển thư mục “adodb5” vào thư mục “/var/adodb/” và thay đổi quyền truy cập của thư mục và các tệp bên trong

```
doanh@ubuntu:~/snort_src$ sudo mv adodb5/ /var/adodb
doanh@ubuntu:~/snort_src$ sudo chmod -R 755 /var/adodb/
doanh@ubuntu:~/snort_src$ █
```

Hình 83. Di chuyển thư mục “adodb5” vào thư mục “/var/adodb/” và thay đổi quyền truy cập của thư mục và các tệp bên trong

- Tải về tệp BASE 1.4.5 từ SourceForge, là công cụ giúp phân tích và quản lý cảnh báo từ IDS

```
doanh@ubuntu:~/snort_src$ wget https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
--2025-04-05 14:05:06- https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
Resolving sourceforge.net (SourceForge.net)... 104.18.13.149, 104.18.12.149, 2006:4700::0:812:d99, ...
Connecting to sourceforge.net (sourceforge.net)[104.18.13.149]:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/ [following]
--2025-04-05 14:05:06- https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/download [following]
--2025-04-05 14:05:07- https://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz/download
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://downloads.sourceforge.net/project/secureideas/BASE/base-1.4.5/base-1.4.5.tar.gz?ts=gAAAAAA8nBNYJhZusYpJq-18eVrny2VruhxVQ1t6qslQW2sPLZPGXbrgzvyvz90y_vw3LkDLvT6g-Puo4_g4BoAg3Ap3NzPng%3D0
30use_mirror=cyfuture=> [following]
--2025-04-05 14:05:07- https://downloads.sourceforge.net/project/secureideas/BASE/base-1.4.5/base-1.4.5.tar.gz?ts=gAAAAAA8nBNYJhZusYpJq-18eVrny2VruhxVQ1t6qslQW2sPLZPGXbrgzvyvz90y_vw3LkDLvT6g-Puo4_g4Bo
Add header: X-SourceForge-Header: mirror=cyfuture
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 104.18.13.149, 104.18.12.149, 2006:4700::0:812:d99, ...
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)[104.18.13.149]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 958567 (936K) [application/x-gzip]
Saving to: 'base-1.4.5.tar.gz'

base-1.4.5.tar.gz          100%[=====] 936,10K  1,23MB/s   in 0,7s
2025-04-05 14:05:09 (1,23 MB/s) - 'base-1.4.5.tar.gz' saved [958567/958567]
```

Hình 84. Tải về tệp BASE 1.4.5 từ SourceForge, là công cụ giúp phân tích và quản lý cảnh báo từ IDS

- Giải nén tệp

```
doanh@ubuntu:~/snort_src$ tar -xvzf base-1.4.5.tar.gz
base-1.4.5/
base-1.4.5/admin/
base-1.4.5/admin/base_roleadmin.php
base-1.4.5/admin/base_useradmin.php
base-1.4.5/admin/index.php
base-1.4.5/base_ag_common.php
base-1.4.5/base_ag_main.php
base-1.4.5/base_common.php
base-1.4.5/base_conf.php.dist
base-1.4.5/base_db_common.php
base-1.4.5/base_db_setup.php
base-1.4.5/base_denied.php
base-1.4.5/base_footer.php
base-1.4.5/base_graph_common.php
base-1.4.5/base_graph_display.php
base-1.4.5/base_graph_form.php
base-1.4.5/base_graph_main.php
base-1.4.5/base_hdr1.php
base-1.4.5/base_hdr2.php
base-1.4.5/base_local_rules.php
base-1.4.5/base_logout.php
base-1.4.5/base_mac_prefixes.map
base-1.4.5/base_main.php
base-1.4.5/base_maintenance.php
base-1.4.5/base_payload.php
base-1.4.5/base_qry_alert.php
base-1.4.5/base_qry_common.php
base-1.4.5/base_qry_form.php
base-1.4.5/base_qry_main.php
base-1.4.5/base_qry_sqlcalls.php
base-1.4.5/base_stat_alerts.php
base-1.4.5/base_stat_class.php
base-1.4.5/base_stat_common.php
base-1.4.5/base_stat_ipaddr.php
base-1.4.5/base_stat_iplink.php
base-1.4.5/base_stat_ports.php
base-1.4.5/base_stat_sensor.php
base-1.4.5/base_stat_time.php
base-1.4.5/base_stat_uaddr.php
base-1.4.5/base_user.php
base-1.4.5/contrib/
base-1.4.5/contrib/barnyard-base.patch
base-1.4.5/contrib/base-rss-core.php
base-1.4.5/contrib/base-rss.php
base-1.4.5/contrib/custom_base_footer.php
base-1.4.5/contrib/SnortUnified/
base-1.4.5/contrib/SnortUnified/LICENSE
base-1.4.5/contrib/SnortUnified/pcaptodb.pl
```

Hình 85. Giải nén tệp

- Di chuyển thư mục “**base-1.4.5/**” vào thư mục “**/var/www/html/base/**”, nơi các tệp web sẽ được Apache phục vụ

```
doanh@ubuntu:~/snort_src$ sudo mv base-1.4.5/ /var/www/html/base/
```

Hình 86. Di chuyển thư mục “**base-1.4.5/**” vào thư mục “**/var/www/html/base/**”, nơi các tệp web sẽ được Apache phục vụ

- Tạo tệp cấu hình “base_conf.php”

```
doanh@ubuntu:/var/www/html/base$ sudo nano /var/www/html/base/base_conf.php
```

Hình 87. Tạo tệp cấu hình “base_conf.php”

Sửa các nội dung như sau:

```
/*
$BASE_urlpath = '/base';
```

```
/*
$DBlib_path = '/var/adodb';
```

```
/*
$alert_dbname    = 'snort';
$alert_host      = 'localhost';
$alert_port      = '';
$alert_user      = 'snort';
$alert_password  = 'snortpass';
```

```
//$graph_font_name = "DejaVuSans";
```

```
// $graph_font_name = "Image";
$graph_font_name = "";
```

- Thay đổi quyền sở hữu thư mục

```
doanh@ubuntu:/var/www/html/base$ sudo chown -R www-data:www-data /var/www/html/base/
```

Hình 88. thay đổi quyền sở hữu thư mục

- Loại bỏ quyền đọc đối với tệp “base_conf.php”

```
doanh@ubuntu:/var/www/html/base$ sudo chmod o-r /var/www/html/base/base_common.php
doanh@ubuntu:/var/www/html/base$ sudo chmod o-r /var/www/html/base/base_conf.php
doanh@ubuntu:/var/www/html/base$ sudo chmod o-r /var/www/html/base/base_conf.dist
```

Hình 89. Loại bỏ quyền đọc đối với tệp “base_conf.php”

- Khởi động lại dịch vụ Apache2 để áp dụng các thay đổi cấu hình và Kiểm tra trạng thái hiện tại của Apache2 để đảm bảo dịch vụ đang hoạt động đúng.

```
doanh@ubuntu:/var/www/html/base$ service apache2 restart
doanh@ubuntu:/var/www/html/base$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-04-05 14:21:35 +07; 12s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 41361 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 41365 (apache2)
    Tasks: 6 (limit: 4549)
   Memory: 14.8M
      CPU: 46ms
     CGroup: /system.slice/apache2.service
             └─41365 /usr/sbin/apache2 -k start
                 ├─41368 /usr/sbin/apache2 -k start
                 ├─41369 /usr/sbin/apache2 -k start
                 ├─41370 /usr/sbin/apache2 -k start
                 ├─41371 /usr/sbin/apache2 -k start
                 └─41372 /usr/sbin/apache2 -k start

Thg 4 05 14:21:35 ubuntu systemd[1]: Starting The Apache HTTP Server...
Thg 4 05 14:21:35 ubuntu apachectl[41364]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for Port 80
Thg 4 05 14:21:35 ubuntu systemd[1]: Started The Apache HTTP Server.

doanh@ubuntu:/var/www/html/base$
```

Hình 90. Khởi động Apache2

CHƯƠNG V: ĐÁNH GIÁ VÀ KẾT LUẬN

1. Bảng phân công

Họ và tên	Công việc
Nguyễn Thị Kim Doanh	100%
Nguyễn Thúy Vy	100%
Lê Tường Vi	100%

2. Tài liệu tham khảo

[1] <https://tenten.vn/tin-tuc/ids-la-gi/>

[2] https://quantrimang.com/cong-nghe/he-thong-phat-hien-xam-pham-ids-phan-1-37334?utm_source=chatgpt.com

[3] https://quantrimang.com/cong-nghe/ips-he-thong-ngan-nga-xam-nhap-tuong-lua-the-he-ke-tiep-6377?utm_source=chatgpt.com

[4]

https://vi.wikipedia.org/wiki/H%E1%BB%87_th%E1%BB%91ng_ng%C4%83n_ng%E1%BB%ABa_x%C3%A2m_nh%E1%BA%ADp?utm_source=chatgpt.com

[5] <https://quangviet.edu.vn/tuong-lua-the-he-moi-ngfw-voi-ids-ips-ket-hop-cisco-ai-la-gi.html>

[6] <https://www.hackingloops.com/a-beginners-guide-to-snort-deploying-and-writing-rules-for-intrusion-detection-system/>

https://blog.desdelinux.net/vi/zeek/?utm_source=chatgpt.com

3. Link youtube

3.1 Quá trình cài đặt:

<https://youtu.be/0HvSAkJTBC>

3.2 Test 1:

<https://youtu.be/SA9mdgbjj68>

3.3 Test 2:

<https://youtu.be/OJ8PnAaYnSg>