IDPS cho wireless network

Bùi Quốc Huy
19520588
ATCL2019.1
19520588@gm.uit.edu.vn

Bùi Đức Anh
19521190
ATCL2019.1
19521190@gm.uit.edu.vn

Ngô Đức Trí
19521044
ATCL2019.1
19521044@gm.uit.edu.vn

Bao Gia Bảo
19520398
ATCL2109.1
19520398@gm.uit.edu.vn

I. GIỚI THIỆU

Trong những thập kỷ gần đây, việc sử dụng công nghệ không dây đã gia tăng đáng kể, cả với các cá nhân hay tổ chức. Sự phát triển của công nghệ không dây cũng kéo theo nhiều thách thức mới, khiến người dùng đối mặt với những rủi ro về quyền riêng tư. Trên thực tế, mạng không dây rất dễ bị tấn công và đe dọa. Ví dụ như tấn công từ chối dịch vụ (DoS), nghe trộm hoặc truy cập trái phép vào hệ thống nhằm làm hỏng hệ thống. Khi công nghệ không dây trở nên phổ biến hơn, các thiết bị không dây càng ngày càng tăng hiệu suất và rẻ hơn, việc xâm nhập vào mạng không dây đã trở nên rất phổ biến. Cùng với độ tin cậy yếu của công nghệ không dây, mạng không dây và mạng di động thường phải đối mặt với những thách thức mới. Kẻ tấn công vào hệ thống không dây cũng có thể được tấn công ở một vị trí địa lý khác gần đó vào bất cứ lúc nào mà chúng ta không hề hay biết.

Vì vậy, vấn đề bảo vệ các mạng không dây khỏi các tác nhân xấu là 1 điều rất cần thiết trong một hệ thống mạng sử dụng mạng không dây. Để làm được điều đó mà không ảnh hưởng tới các hành vi thông thường của hệ thống thì ta sẽ sử dụng IDPS. Đồ án này sẽ thảo luận về cách triển khai Wireless IDPS và cải tiến IDPS để làm cho nó trở nên hữu ích hơn, khắc phục các cuộc xâm nhập và tấn công hiện có, đồng thời giảm thiểu rủi ro trong tương lai trong mạng không dây.

II. MỤC TIÊU

Mục tiêu của đề tài này là: giúp ta hiểu thêm về hệ thống mạng không dây; giới thiệu một số hình thức tấn công vào hệ thống mạng không dây; vai trò của hệ thống IDPS trong việc ngăn chặn tấn công; đưa ra mô hình bảo mật giúp cải thiện hệ thống Wireless IDPS và ứng dụng của nó.

III. PHƯƠNG PHÁP THỰC HIỆN

A. Tìm hiểu về WIDPS

- Phương pháp thực hiện: xem lại các kiến thức giảng viên đã dạy kết hợp với việc tham khảo các bài báo khoa học.

B. Sự khác biệt giữa IDPS trên wireless và standard network

- Phương pháp thực hiện: Tham khảo qua các bài báo khoa học trên trang scholar.google.com.

C. Các hình thức tấn công vào wireless network

- Phương pháp thực hiện: Nghiên cứu tài liệu về các hình thức tấn công vào mạng không dây.

D. Mô hình được đề xuất cải thiện hệ thống IDPS

- Phương pháp thực hiện: Nghiên cứu các bài báo khoa học về các đề xuất để tăng hiệu suất làm việc của hệ thống idps trên wireless network, đồng thời khắc phục được những hạn chế của IDPS trên wireless network.

E. Thiết kế giải pháp, triển khai mô hình WIDPS với hệ thống mạng Wifi, thực nghiệm ngăn chặn tấn công với WIDPS

- Phương pháp thực hiện: Sử dụng công cụ Mininet-wifi để tạo mô hình mạng không dây ảo. Ta sử dụng Snort để phát hiện xâm nhập và ngăn ngừa nó bằng phương pháp deauthentication với công cụ Aireplay-ng, cố gắng loại bỏ người dùng bất hợp pháp ra khỏi mạng.

IV. NỘI DUNG THỰC HIỆN

A. WIDPS là gì?

WIDPS hoặc Wireless IDPS là một thiết bị mạng giám sát tính hiệu vô tuyến để biết đến sự hiện diện của các điểm truy cập trái phép, các gói tin tấn công (phát hiện xâm nhập) và có thể tự động thực hiện các biện pháp đối phó với sự tấn công đó (ngăn chặn xâm nhập). WIDPS giúp bảo vệ các hệ thống mạng không dây như hệ thống Wifi, mạng điện thoại khỏi sự xâm nhập trái phép.

Mục đích chính của WIDPS là ngăn chặn truy cập mạng trái phép vào mạng cục bộ và các tài sản thông tin khác trong hệ thống bằng các thiết bị không dây. Các hệ thống này thường được triển khai dưới dạng 1 lớp bao phủ nằm trong hệ thống mạng LAN không dây, mặc dù WIDPS có thể được triển khai độc lập để thực thi các chính sách trong một tổ chức. Cũng có một số hệ thống không dây tiên tiến hơn có khả năng tích hợp sẵn WIDPS trong hệ thống.

B. Sự khác biệt giữa IDPS trên wireless và standard network

Trên hệ thống mạng bình thường, việc triển khai hệ thống IDPS để phát hiện và ngăn chặn tấn công bằng cách triển khai IDPS ở vị trí có thể thấy được tất cả các traffic trong hệ thống mạng, nó có thể thấy tất cả các traffic vào và ra hệ thống mạng, việc phát hiện và ngăn chặn các cuộc tấn công cũng trở nên dễ dàng hơn. Tuy nhiên, đối với việc triển khai IDPS trên wireless network để đạt được hiệu quả thì lại gặp nhiều khó khăn hơn:

- Sóng không ổn định: do người dùng thường xuyên di chuyển, thiết bị không ở 1 vị trí nhất định làm cường độ của mạng không ổn định, cũng gây khó khăn cho việc phát hiện các mối đe dọa.
- Khó khăn trong việc phát hiện những clients lạ: Những client kết nối tới wireless network có thể sử dụng wireless cards có địa chỉ MAC khác. Hơn nữa, đa số các địa chỉ MAC của wireless cards có thể bị thay đổi bằng các phần mềm, vì vậy sẽ rất khó khăn để phát hiện những kết nối lạ vào hệ thống. Một hệ thống IDPS trên wireless cần phải có khả năng phân

biệt giữa 2 clients với cùng địa chỉ MAC: 1 là client thật còn 1 là hacker.

- Vấn đề về vị trí đặt sensor: Sensor trong wireless network có một phạm vi hoạt động nhất định, nếu đặt ở vị trí không thích hợp sẽ làm giảm hiệu quả của hệ thống, đồng thời làm tốn chi phí lắp đặt hơn.
- Vấn đề về thông tin khi sử dụng nhiều sensor: Cần phải tìm cách để kết hợp các thông tin của nhiều Sensor khác nhau trong wireless network để tạo nên thông tin hoàn chỉnh về traffic trong wireless network để phát hiện chính xác các cuộc xâm nhập.

C. Một số cách tấn công vào hệ thống mạng không dây

Hacker có thể xâm nhập vào mạng thông qua:

- Các node trong hệ thống mạng.
- Bằng các công nghệ như wireless card do các phần mềm như Kismet hoặc Tumbler cung cấp. những phần mềm này cho phép hacker xâm nhập vào mạng của nạn nhân và thay đổi, phá hủy những thông tin của họ.

Một số loại tấn công đối với mạng không dây:

- DoS vs DDoS là nổi bật nhất: đây là loại attack đã được học nhiều nên em sẽ không nhắc đến.
- Tấn công Man in The Middle Attack: tương tự như DoS và DDoS Attack, loại tấn công này cũng đã được học rồi
- Một loại tấn công khác là wormhole attack: là một kiểu tấn công lớp mạng được thực hiện bằng cách sử dụng nhiều node độc hại. Các node được sử dụng để thực hiện cuộc tấn công này vượt trội hơn so với những node bình thường và có khả năng thiết lập các kênh liên lạc tốt hơn trên phạm vi dài.

  Wormhole attack có thể được phân theo 3 loại chính:

  1. Tấn công Wormhole mở: trong trường hợp này, các gói dữ liệu lần đầu tiên được gửi từ nguồn đến một wormhole để chuyển chúng đến wormhole khác, sau đó mới đến đích. Các node khác trong mạng bị bỏ qua và không được sử dụng để truyền dữ liệu

  2. Tấn công Wormhole nửa mở: trong trường hợp này, các gói dữ liệu được gửi từ nguồn đến một wormhole để truyền trực tiếp chúng đến đích.

  3. Tấn công Wormhole đóng: trong trường hợp này, các gói dữ liệu được chuyển trực tiếp từ nguồn đến đích trong một hop (chặng) duy nhất, khiến chúng trở thành những neighbour giả mạo.
- MAC Spoofing cũng là 1 trong những phương thức mà hacker thực hiện để tấn công các hệ thống mạng không dây hiện nay. Loại tấn công này có thể được thực hiện như sau:

  1. Attacker sử dụng tool để scan các địa chỉ MAC của những máy khách khác trong wireless network

  2. Attacker thay đổi địa chỉ MAC của hắn thành 1 trong những địa chỉ mà hắn scan được

  3. Sau đó Attacker tiến hành deauth client mà hắn đã giả dạng để khiến client đó không thể truy cập vào mạng

  4. Attacker tiến hành giao tiếp với Access Point và tìm hiểu các thông tin của mạng nội bộ và đăng nhập vào mạng nội bộ

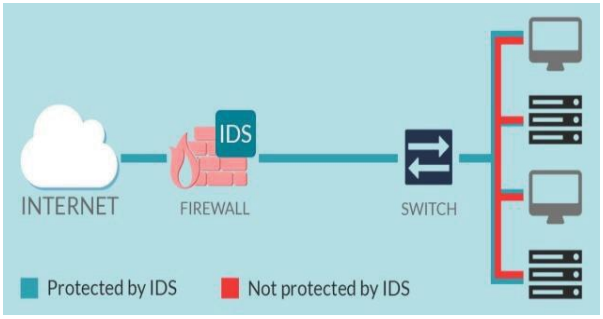
  5. Sau đó attacker có thể tiến hành nghe lén các thông tin trong mạng hoặc thực hiện các cuộc tấn công khác

- Tấn công bằng Tần số Radio: Wireless network thường hoạt động ở băng tần 2.4GHz và 5GHz. Nếu kẻ tấn công sử dụng sóng Radio có tần số cao thì có thể khiến access point của wireless network trở nên vô dụng.

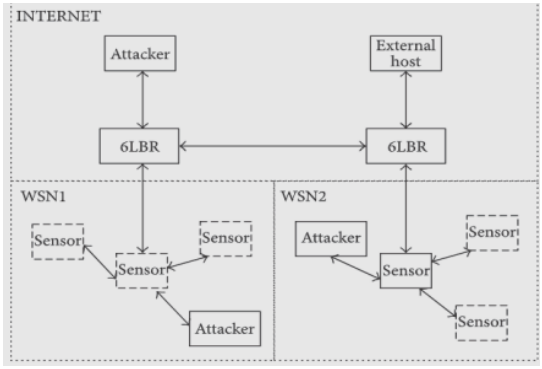
D. Mô hình đề xuất để cải thiện hệ thống Wireless IDPS

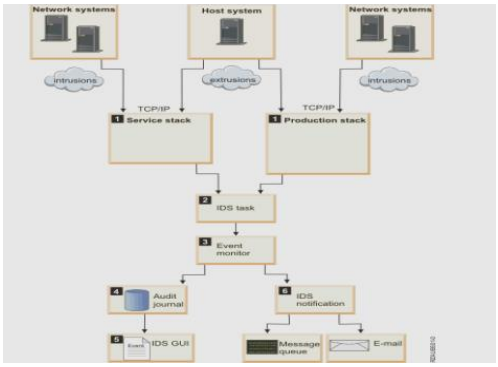
Mô hình IPDS của một môi trường Internet tích hợp của một WSN nên được giám sát bằng tài nguyên có sẵn để cảm nhận được sự ràng buộc và vận hành các nền tảng trong khi nó có thể hữu ích hơn với các tài nguyên khả dụng với các lớp khác của thiết bị, cụ thể là Border Router. Hybrid attitude được thể hiện đối với xâm nhập và phát hiện để tất cả các thiết bị trong mạng giao tiếp theo nó.

Giả sử các thiết bị thực hiện phát hiện đều đáng tin cậy và cả hai cổng vào và các thiết bị cảm biến tương thích với nó. Hình dưới diễn tả kiến trúc cho sự xâm nhập và ngăn chặn.



Unsocial boby ở hình dưới có thể có sẵn trong cùng một miền của WSN hoặc nó có thể có sẵn ở một bên ngoài nguồn hoặc mạng lưới internet. Tất cả các thiết bị sẽ hoạt động cùng nhau để giúp phát hiện trong thời gian thích hợp bằng cách chặn giao tiếp giữa miền WSN và Internet với sự trợ giúp của gateway. Gateway cũng có thể gửi message tới các sensorcó sẵn trong mạng để tránh thông điệp đến từ non-social agencies. Khuôn khổ của gateway và sensor được thể hiện ở 2 hình dưới:

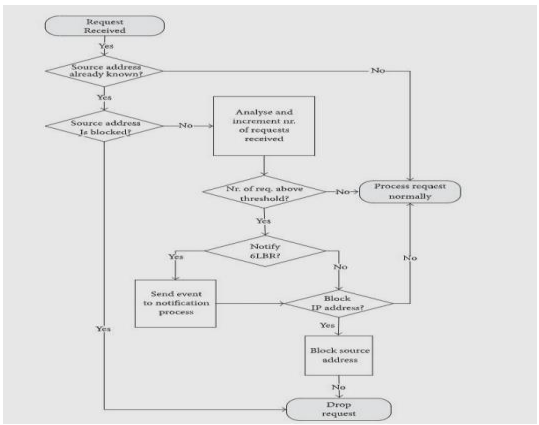


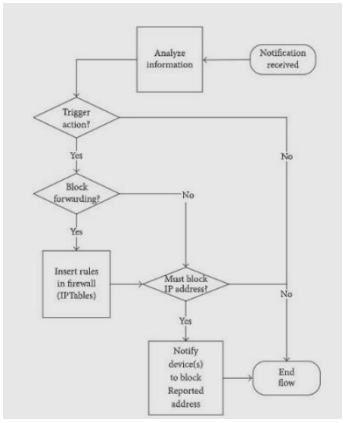


Bằng cách cố gắng kích hoạt để encrypt dữ liệu ở data link layer và physical layer được sử dụng trong giao tiếp bên trong miền WSN với sự trợ giúp của phương pháp mã hóa đối xứng ở cấp độ cao hơn của sự giao tiếp chủ yếu giữa các sensor và gateway với sự trợ giúp của CoAP. Ngoài ra, sửa đổi firewall để chặn thông báo không mong muốn đến với mạng ở các level khác nhau của việc truyền thông điệp thông qua các nguồn khác nhau với sự trợ giúp của gateway và các thiết sensor. Kỹ thuật này giúp ngăn chặn thông báo không mong muốn đến từ các nguồn không mong muốn ngay khi được tìm thấy.

Application (COAP)	IDS and Firewall	Application (HTTP)
Network/routing (RPL, IPv6)		Network/routing (TCP/UDP)
6LoWPAN		IPv6
MAC (IEEE 802.15.4, IEEE 802.15.4e)	802.15.4 Firewall	MAC (IEEE 802.3, 802.11, 802.16, LTE)
PHY (IEEE 802.15.4, IEEE 802.15.4e)		PHY (IEEE 802.3, 802.11, 802.16, LTE)

Đầu tiên, khi 1 message đến sensor, nó sẽ xác nhận địa chỉ IP của nguồn và ngoài ra, cũng xác nhận thêm số lượng packet nhận được trong cùng một nguồn trong cùng một khoảng thời gian nhằm để kiểm tra có phải tấn công DOS hay không. Không chỉ vậy, xem xét thêm sự sụt giảm các thông báo không mong muốn ở phía gateway nhằm cảnh báo bảo mật mạng. Đồng thời kích hoạt thêm biện pháp bảo mật bằng các từ chối các message không mong muốn và chuyển tiếp thông báo gateway để chặn ngăn chặn người dùng không mong muốn và bổ sung vào database. Hai lưu đồ dưới đây cho chúng ta thấy về tấn công cũng như hệ thống bảo mật sẽ làm gì khi bị tấn công:





Thực hiện các phương pháp phòng ngừa và phát hiện tại các sensor, thiết bị lưu trữ địa chỉ IP cùng với digital signature của friendly intrusion từ đó nó sẽ giúp mạng cung cấp cảnh báo khi việc phát hiện mối đe dọa khi được thực hiện. Ngoài ra còn duy trì dữ liệu trong WSN của cảm biến thiết bị trong domain cụ thể và điều này được thực hiện với sự trợ giúp của tài nguyên bởi sự ứng dụng CoAP và khi biết địa chỉ IP của nguồn, nó sẽ tăng sự ổn định cho mô hình được đề xuất. Theo mô hình khi một message được gửi qua thiết bị cảm biến tới cổng có sẵn, một thông báo về loại message request được nhận và địa chỉ IP của người gửi cũng sẽ được gửi đến gateway. Sau khi thông báo được nhận, gateway quyết định hành động bảo mật nào nên được thực hiện cho một hành động hoặc thông điệp cụ thể.

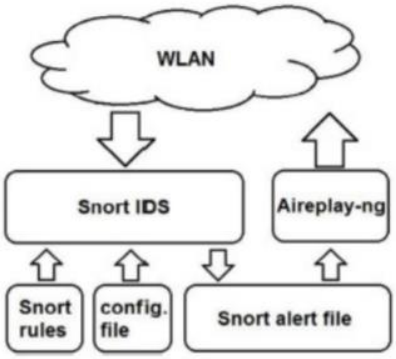
Để đạt được mục tiêu về thử nghiệm đề xuất mô hình, tác giả đã sử dụng hệ điều hành của Contiki. Các bước đầu tiên để đạt được mục tiêu, tác giả đã gắn sensor và gateway vào mạng. Như đã phân tích, nó cho kết quả là phân tích loại yêu cầu đến với mạng, lớp ứng dụng và định tuyến. Vì vậy, điều này giúp tác giả thực hiện các phương pháp kỹ thuật phát hiện xâm nhập khác nhau.

E. Thiết kế giải pháp, triển khai mô hình WIDPS với hệ thống mạng Wifi, thực nghiệm ngăn chặn tấn công với WIDPS.

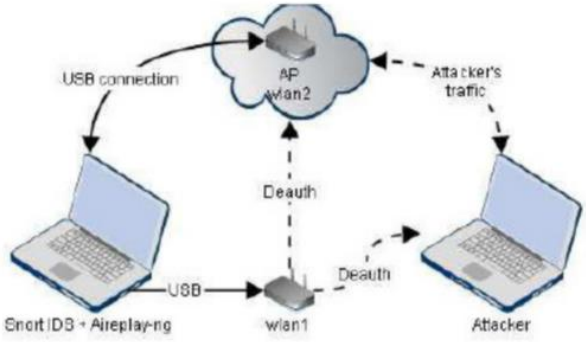
Ở phần demo thực nghiệm này, phương pháp mà ta sẽ sử dụng để ngăn chặn xâm nhập là phương pháp deauthentication được những kẻ tấn công sử dụng để lấy thông tin cần thiết dùng cho bẻ khóa WPA-PSK, và đây là cách tiếp cận khá mới của việc sử dụng vũ khí của kẻ tấn công để chống lại kẻ tấn công. Mục tiêu cơ bản của phương pháp này là cố gắng loại bỏ người dùng ra khỏi mạng bằng cách gửi các tín hiệu ngắt liên kết lặp đi lặp lại liên tục để ngăn người dùng đó gửi bất kỳ gói tín nào trong hệ thống mạng không dây được bảo vệ. Gói frame disassociation là một phần của tập hợp các frame quản lí được dùng trong hệ thống mạng không dây. Các access point sẽ gửi các frame này cho người dùng để ngắt kết nối. Công cụ để chèn gói tin mà ta sử dụng trong quá trình này là công cụ Aireplay-ng, nó được sử dụng để tạo và đưa các gói disassociation đến các phương tiện không dây.

Giải pháp bao gồm hai thành phần chính. Đầu tiên là hệ thống IDS phát hiện xâm nhập và thứ hai là phần chèn các gói tin vào hệ thống mạng. Với phần IDS ta sẽ sử dụng Snort, lí do sử dụng chủ yếu là do sự phổ biến của nó đối với các chuyên gia mạng và nó có tài liệu phong phú hơn các giải pháp khác. Như đã đề cập trước, để chèn các gói tin công cụ Aireplay-ng sẽ được ta sử dụng. Hình dưới đây mô tả kiến trúc hệ thống cơ bản. Snort được sử dụng để giám sát lưu lượng

trong phương tiện không dây và báo các cảnh báo khi phát hiện một số hành vi độc hại. Trong tệp conf ta ghi các thông tin quan trọng, ví dụ: quy tắc Snort nào sẽ được sử dụng, bộ xử lý trước nào nên được kích hoạt hoặc tiền tố IP của mạng được bảo vệ là gì.



Mininet-WiFi là một nhánh mở rộng của công cụ mô phỏng mạng Mininet SDN mã nguồn mở. Mininet-WiFi có thêm thêm các WiFi station và các Access point ảo hóa dựa trên trình điều khiển không dây tiêu chuẩn của Linux và trình điều khiển mô phỏng không dây 80211_hwsim. Điều này có nghĩa là các đối tượng mới đã được thêm vào để hỗ trợ việc tạo các thiết bị không dây này trong mạng ảo Mininet. Từ đó mô phỏng các thuộc tính của các thiết bị kết nối không dây như vị trí và chuyển động chuyển động của nó liên quan đến các access point.

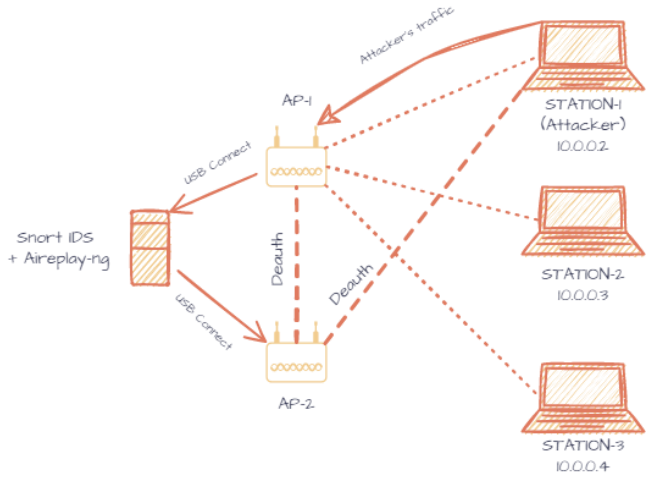


Và với trình tạo mạng ảo Mininet-WiFi ta sẽ tạo 1 hệ thống mạng không dây ảo trên máy tính của ta. Hệ thống này sẽ có các thiết bị là 2 thiết bị station trong đó 1 cho attacker và 1 cho ta cài đặt snort và aireplay-ng trên nó; 2 thiết bị phát tín hiệu không dây trong đó có 1 thiết bị là router wifi cho phép máy attacker kết nối và xâm nhập hệ thống của ta. Máy snort sẽ có cổng kết nối tới thiết bị router này bài giám sát, phân tích các tín hiện gửi tới nó, nếu có sự xâm nhập, tấn công nó sẽ gửi tín hiện tới 1 thiết bị phát wifi khác, thiết bị này sẽ gửi các tín hiệu deauth liên tục nhắm tới mục tiêu để cố gắng ngăn cản máy attacker tiếp tục tấn công hệ thống.

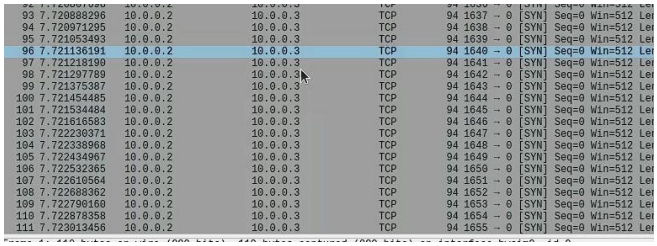
V. THỰC HIỆN DEMO

Về việc demo tấn công vào hệ thống idps trên wireless network, nhóm em quyết định sẽ demo SYN flood DDoS Attack bằng công cụ hping3, sau đó Snort sẽ phát hiện và gửi tín hiệu deauth bằng công cụ Aireplay-ng đến máy attacker để ngăn chặn quá trình tấn công của attacker.

Nhóm em đã thiết kế và triển khai mạng ảo trên công cụ Mininet-wifi theo mô hình mạng sau:



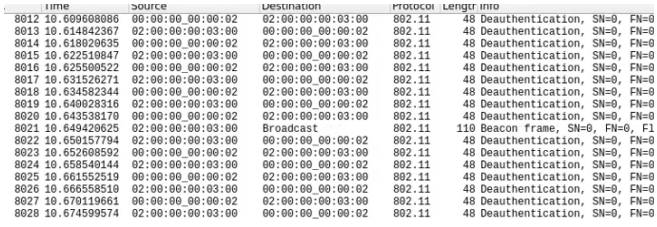
Máy Attacker sẽ tấn công TCP Syn flood đến máy station-2 hoặc station-3. Các gói tin tấn công sẽ gây làm tràn bộ nhớ đệm cảu máy victim và cả access point 1. Lúc này ta không kết nối tới các máy trong mạng được nữa do access point đã bị treo hoặc bị tắt đột ngột.



93	7.720888296	10.0.0.2	10.0.0.3	TCP	94 1637 → 0 [SYN] Seq=0 Win=512 Le
94	7.720971295	10.0.0.2	10.0.0.3	TCP	94 1638 → 0 [SYN] Seq=0 Win=512 Le
95	7.721053493	10.0.0.2	10.0.0.3	TCP	94 1639 → 0 [SYN] Seq=0 Win=512 Le
96	7.721136191	10.0.0.2	10.0.0.3	TCP	94 1640 → 0 [SYN] Seq=0 Win=512 Le
97	7.721218190	10.0.0.2	10.0.0.3	TCP	94 1641 → 0 [SYN] Seq=0 Win=512 Le
98	7.721297789	10.0.0.2	10.0.0.3	TCP	94 1642 → 0 [SYN] Seq=0 Win=512 Le
99	7.721375387	10.0.0.2	10.0.0.3	TCP	94 1643 → 0 [SYN] Seq=0 Win=512 Le
100	7.721454485	10.0.0.2	10.0.0.3	TCP	94 1644 → 0 [SYN] Seq=0 Win=512 Le
101	7.721534484	10.0.0.2	10.0.0.3	TCP	94 1645 → 0 [SYN] Seq=0 Win=512 Le
102	7.721616583	10.0.0.2	10.0.0.3	TCP	94 1646 → 0 [SYN] Seq=0 Win=512 Le
103	7.722230371	10.0.0.2	10.0.0.3	TCP	94 1647 → 0 [SYN] Seq=0 Win=512 Le
104	7.722338968	10.0.0.2	10.0.0.3	TCP	94 1648 → 0 [SYN] Seq=0 Win=512 Le
105	7.722434967	10.0.0.2	10.0.0.3	TCP	94 1649 → 0 [SYN] Seq=0 Win=512 Le
106	7.722532365	10.0.0.2	10.0.0.3	TCP	94 1650 → 0 [SYN] Seq=0 Win=512 Le
107	7.722610564	10.0.0.2	10.0.0.3	TCP	94 1651 → 0 [SYN] Seq=0 Win=512 Le
108	7.722688362	10.0.0.2	10.0.0.3	TCP	94 1652 → 0 [SYN] Seq=0 Win=512 Le
109	7.722790160	10.0.0.2	10.0.0.3	TCP	94 1653 → 0 [SYN] Seq=0 Win=512 Le
110	7.722878358	10.0.0.2	10.0.0.3	TCP	94 1654 → 0 [SYN] Seq=0 Win=512 Le
111	7.723013456	10.0.0.2	10.0.0.3	TCP	94 1655 → 0 [SYN] Seq=0 Win=512 Le

Và trong demo này nhóm em sẽ sử dụng dụng snort để nhận các gói tin trong traffic đi qua access point 1 và phân tích nó nếu có dấu hiệu tấn công dựa theo rules được thiết lập sẵn thì sẽ thông báo. Nhóm em đã xây dựng 1 chương trình script python để tự động nhận thông báo và gửi các gói Deauth từ access point 2 tới máy kẻ tấn công ngay lập tức.

```
Lasted alert time:11/21-05:27:00
----------10.0.0.2----------
Found MAC address for 10.0.0.2
00:00:00:00:00:02
Start deauth STMAC: 00:00:00:00:00:02 in 10 second
Finished deauth station
```



	Time	Source	Destination	Protocol	Length	Info
8012	10.609608086	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8013	10.614842367	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8014	10.618020635	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8015	10.622510847	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8016	10.625500522	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8017	10.631526271	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8018	10.634582344	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8019	10.640028316	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8020	10.643538170	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8021	10.649420625	02:00:00:00:03:00	Broadcast	802.11	110	Beacon frame, SN=0, FN=0, F1
8022	10.650157794	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8023	10.652608592	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8024	10.658540144	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8025	10.661552519	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8026	10.666558519	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0
8027	10.670119661	00:00:00_00:00:02	02:00:00:00:03:00	802.11	48	Deauthentication, SN=0, FN=0
8028	10.674599574	02:00:00:00:03:00	00:00:00_00:00:02	802.11	48	Deauthentication, SN=0, FN=0

Kết quả của việc ngăn chặn tấn công TCP Syn Flood: giúp cho access point 1 và máy victim không bị quá tải, các traffic mạng đi qua access point vẫn di chuyển được bình thường. Quá trình từ lúc xuất hiện các gói TCP Syn để attack tới lúc gửi các gói Deauth chặn thành công diễn ra trong vòng 3 giây, với hệ thống mạng trong mininet-wifi, việc ngăn chặn này hoàn toàn có thể giúp hệ thống chống lại cuộc tấn công DdoS TCP Syn Flood.

Link video demo:

https://drive.google.com/file/d/1Jya6ShIpmRy6fuOfSrccv9MBez-PDc6r/view?usp=sharing

TÀI LIỆU THAM KHẢO

[1] Yadav, H. Gupta and S. K. Khatri, "A Security Model for Intrusion Detection and Prevention over Wireless Network," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019, pp. 12-16, doi: 10.1109/ISCON47742.2019.9036288.

[2] Al-Janabi, Samaher & AlShourbaji, Ibrahim. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. Kurdistan Journal for Applied Research. 2. 6. 10.24017/science.2017.3.48.t

[3] Tao, Zhiqi; Ruighaver, A. (2005). [IEEE TENCON 2005 - 2005 IEEE Region 10 Conference - Melbourne, Australia (2005.11.21-2005.11.24)] TENCON 2005 - 2005 IEEE Region 10 Conference - Wireless Intrusion Detection: Not as easy as traditional network intrusion detection. , (), 1–5. doi:10.1109/tencon.2005.300907

[4] Korcak, Michal & Lamer, Jaroslav & Jakab, Frantisek. (2014). Intrusion Prevention/Intrusion Detection System (IPS/IDS) for Wifi Networks. International journal of Computer Networks & Communications. 6. 77-89. 10.5121/ijcnc.2014.6407.