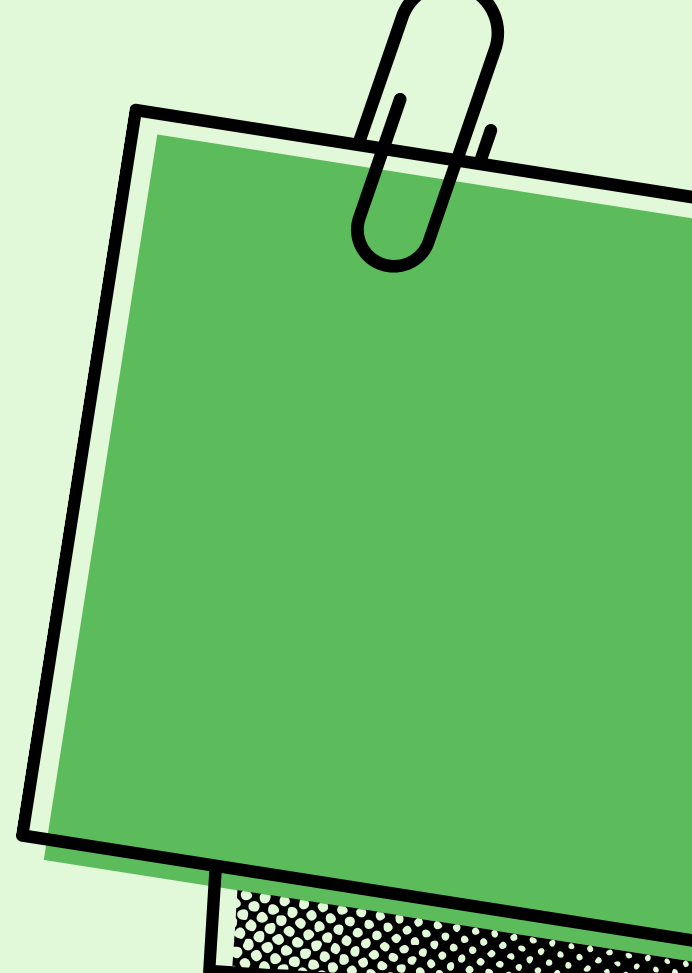




BÁO CÁO PBL4

Dự án hệ điều hành và mạng máy tính



ĐỀ TÀI: TÌM HIỂU HỆ ĐIỀU HÀNH LINUX VÀ XÂY
DỰNG ỨNG DỤNG PHÁT HIỆN XÂM NHẬP

Giảng viên hướng dẫn: ThS. Nguyễn Thế Xuân Ly

Sinh viên thực hiện:

Võ Hoàng Bảo

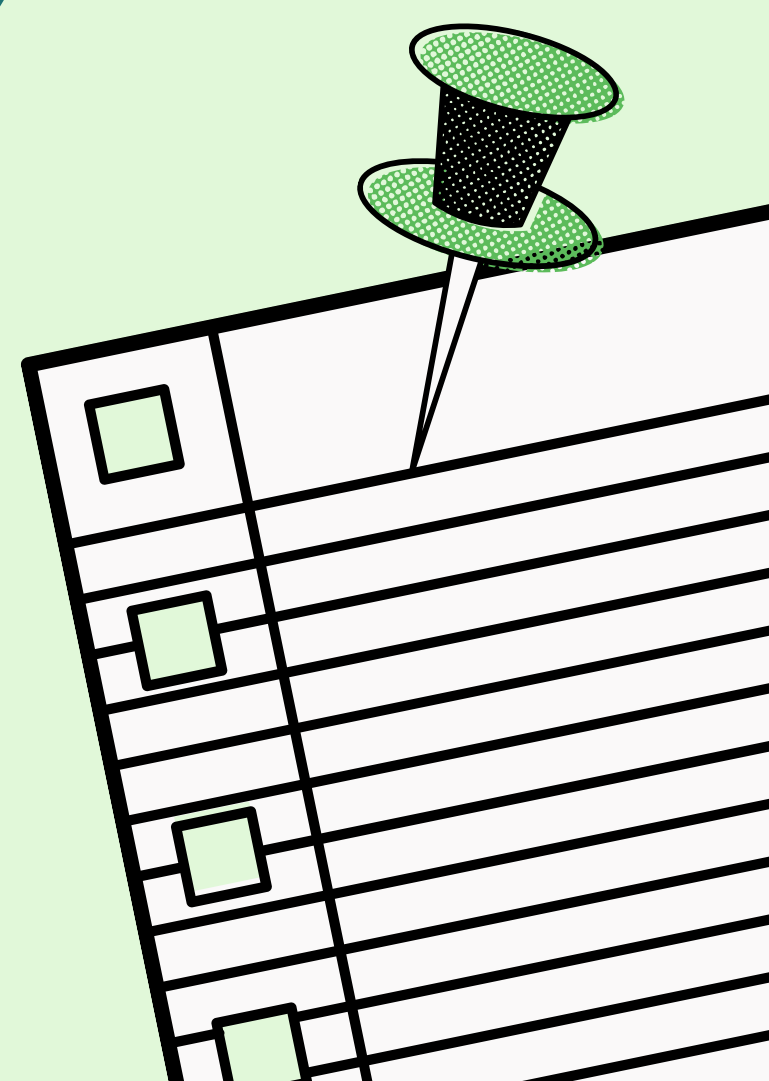
102200246

Bùi Hải Nam

102200273

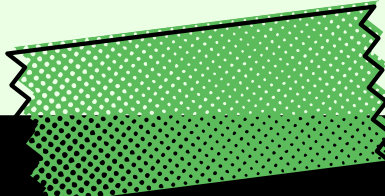
Nguyễn Hoàng Quân

102200281





Nội dung trình bày



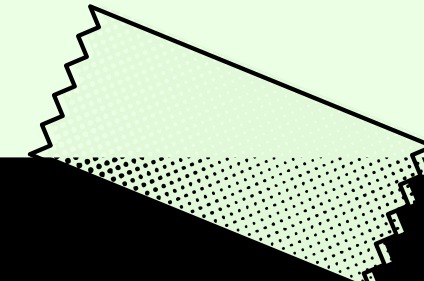
1. Giới thiệu về
hệ điều hành
Linux



2. Hệ thống IDS
Snort



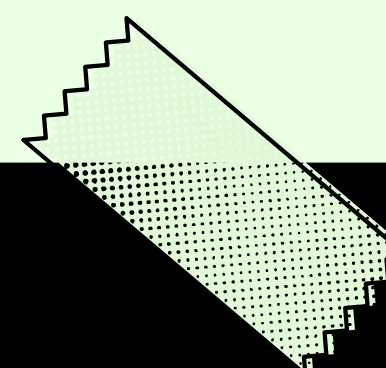
3. Giới thiệu về
IPTABLE



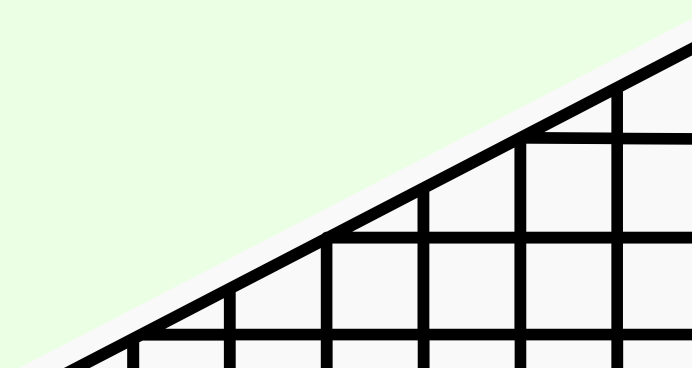
4. Phân tích
thiết kế hệ thống



5. Triển khai kết
quả và đánh giá



6. Kết luận và
hướng phát triển



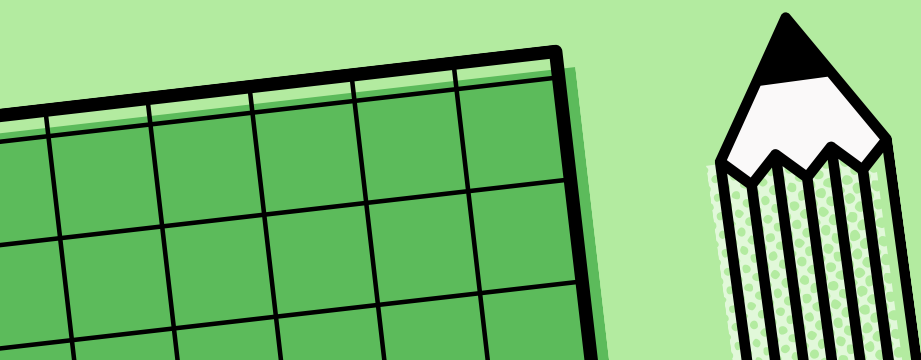
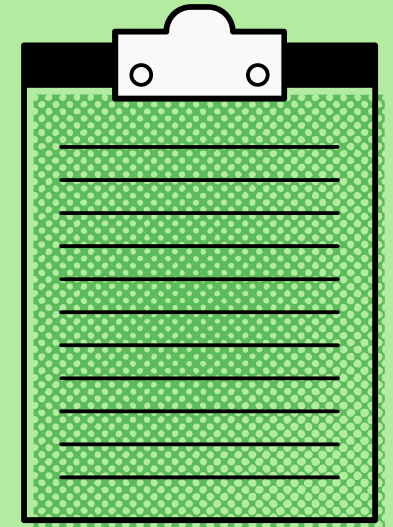


I. Giới thiệu về hệ điều hành Linux

Linux là tên gọi của một hệ điều hành máy tính và cũng là tên hạt nhân của hệ điều hành. Nó là một ví dụ nổi tiếng nhất của phần mềm tự do và của việc phát triển mã nguồn mở. Linux được phát triển từ năm 1991 dựa trên hệ điều hành Unix và bằng viết bằng ngôn ngữ C.

Cấu trúc:

- Kernel: hay được gọi là phần Nhân vì đây là phần quan trọng trong máy tính.
- Shell: là phần có chức năng thực thi các lệnh.
- Application: là phần để cài đặt và chạy ứng dụng.



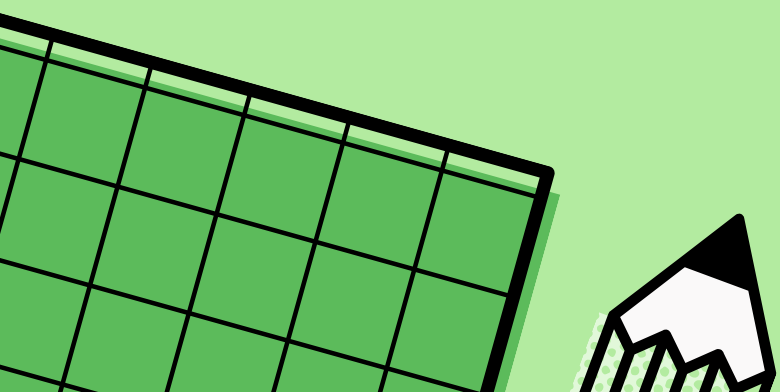


2. Hệ thống IDS Snort



2.1 Snort là gì?

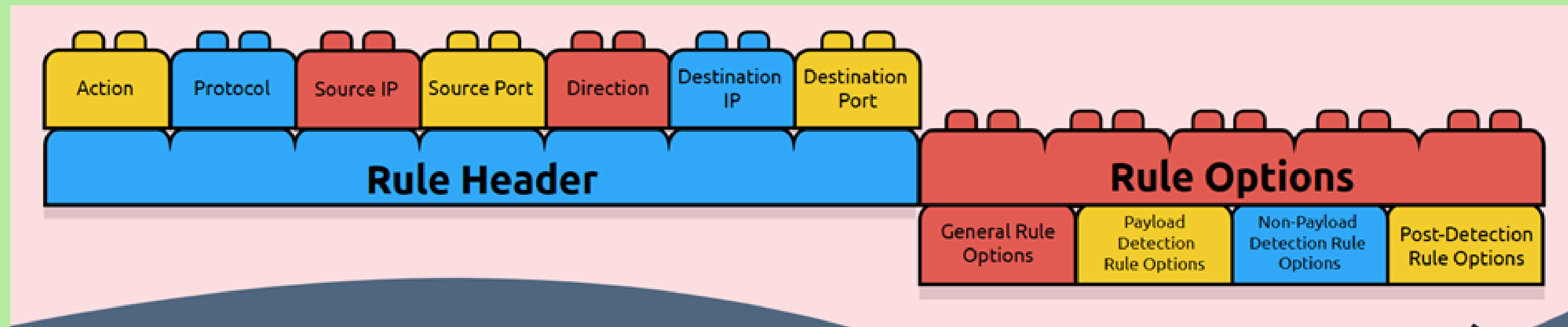
Snort là một NIDS/NIPS mã nguồn mở, hoạt động dựa trên một tập luật linh hoạt, thông qua phân tích các protocol, tìm kiếm nội dung và các bộ tiền xử lý (preprocessor) để phát hiện ra hàng ngàn loại sâu (worm), các kiểu tấn công, quét cổng và những hành động đáng ngờ khác trên mạng. Nó được phát triển và bảo trì bởi Martin Roesch, các nhà đóng góp mã nguồn mở và Cisco Talos team.



2. Hệ thống IDS Snort



2.2 Cấu trúc luật của Snort

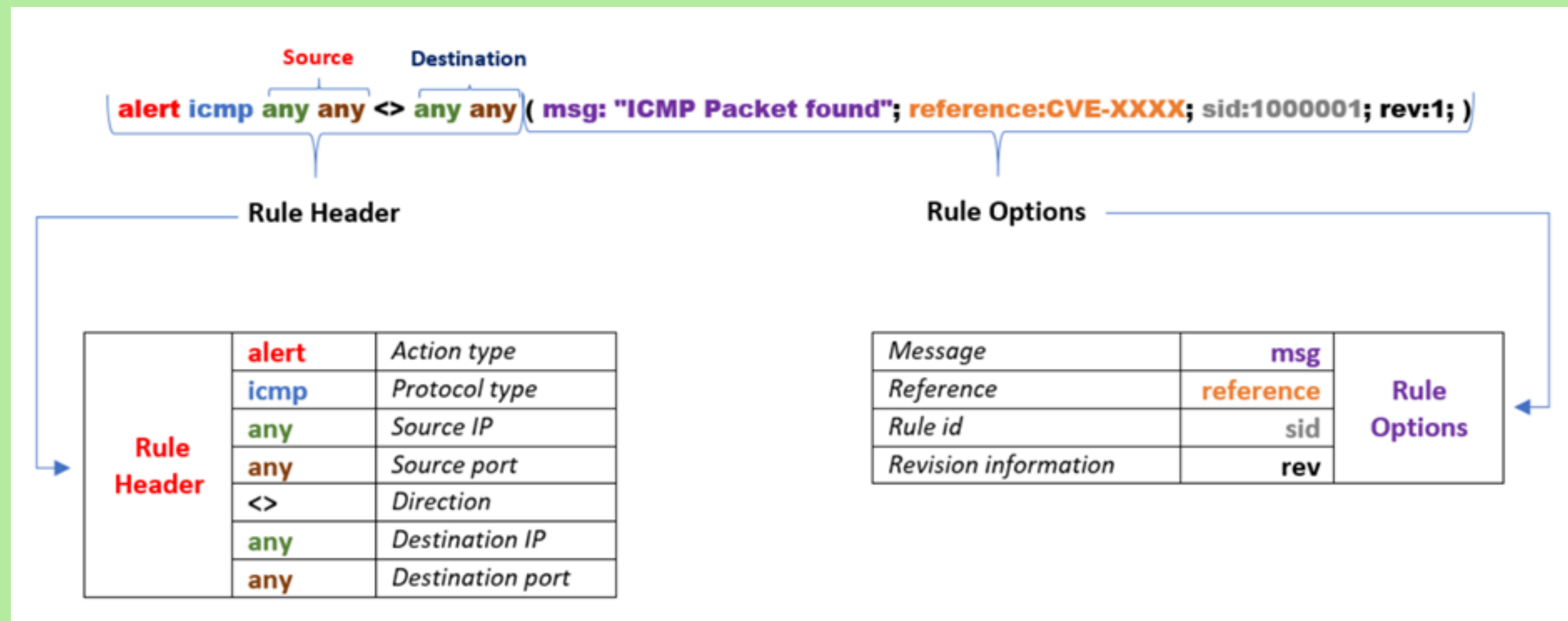


Hình 2: Cấu trúc luật của Snort

2. Hệ thống IDS Snort

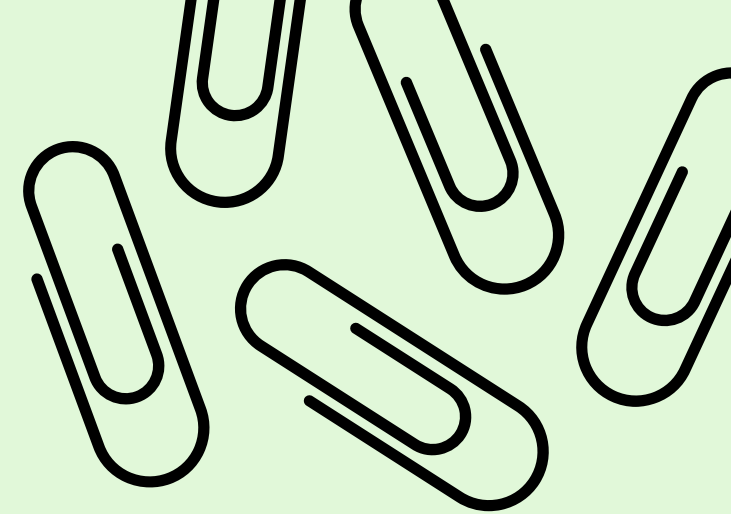


2.2 Cấu trúc luật của Snort



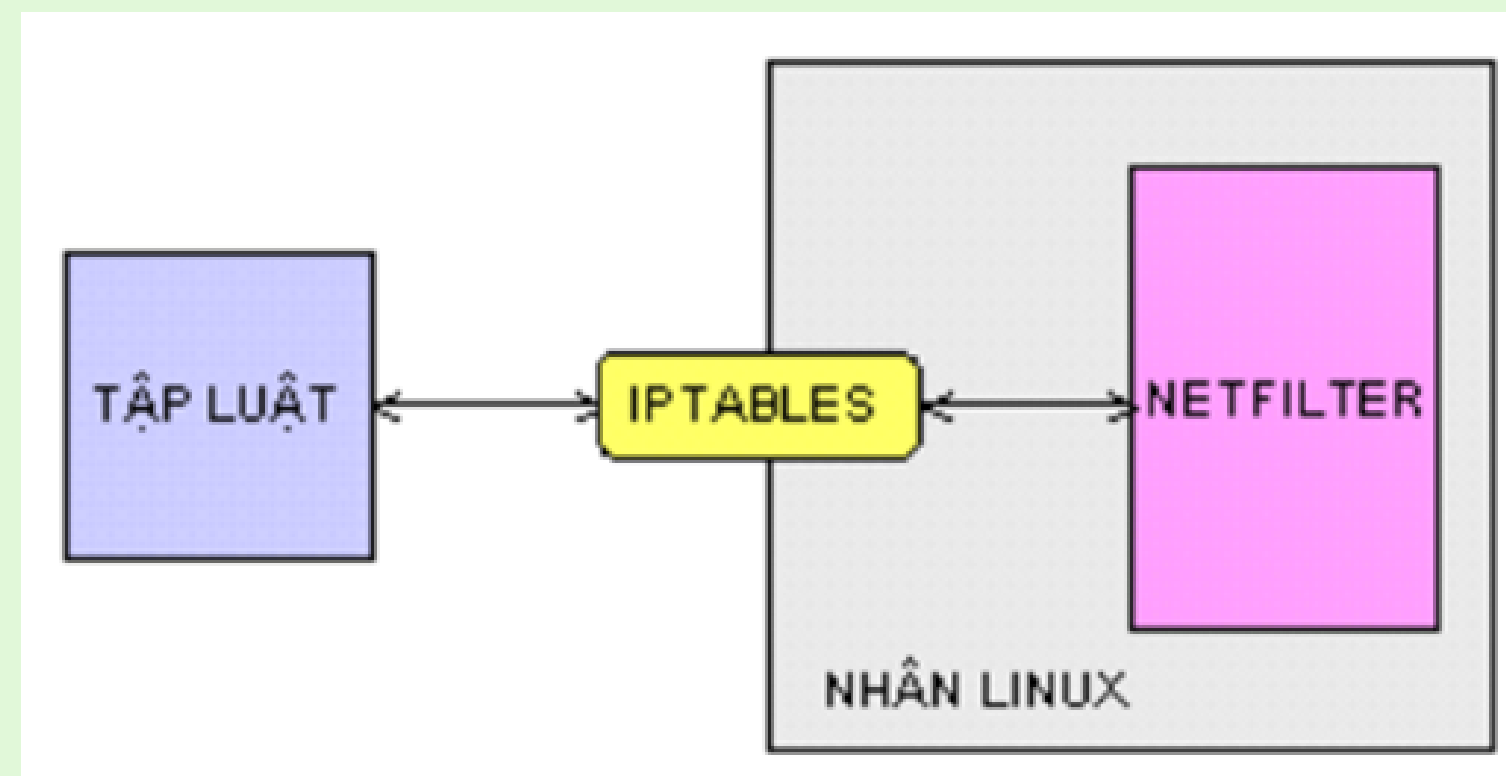
Hình 3: Ví dụ

3. Giới thiệu về IPtables



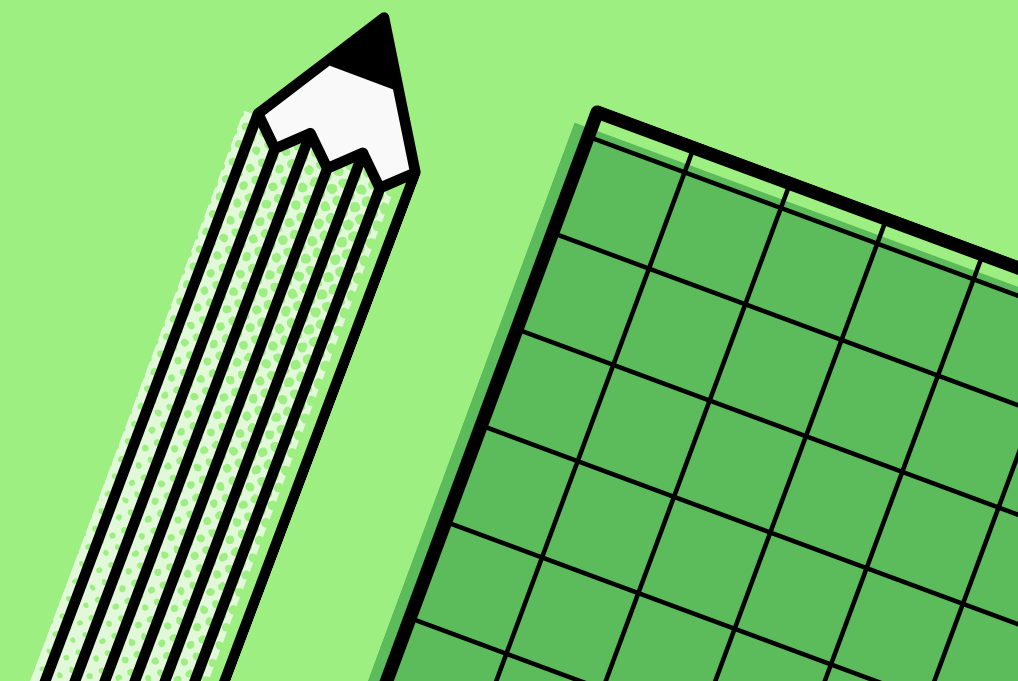
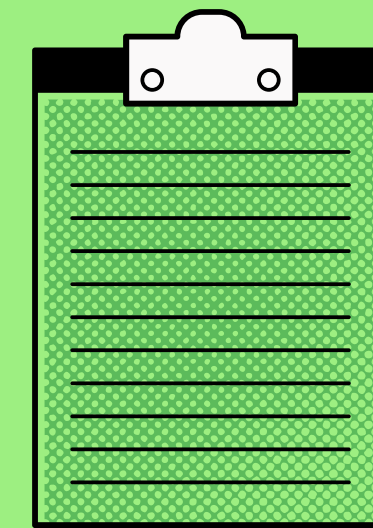
3.1 Khái niệm:

Iptables là một tường lửa ứng dụng lọc gói dữ liệu rất mạnh, miễn phí và có sẵn trên Linux. Netfilter/Iptables gồm 2 phần là Netfilter ở trong nhân Linux và Iptables nằm ngoài nhân. Iptables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter để đẩy các luật của người dùng vào cho Netfilter xử lý. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống.



Hình 4: Sơ đồ Netfilter/Iptables

4. Phân tích thiết kế hệ thống



5. Kết quả triển khai và đánh giá

Ví dụ như cuộc tấn công Ping of death, thông thường các gói tin ping rất nhỏ, nhưng gói tin IP4 lại có dung lượng có thể chứa rất lớn, có thể vượt quá dung lượng tối đa cho phép của 1 gói tin, việc gửi đến các ping có dung lượng lớn khiến cho hệ thống không thể hoạt động bình thường thậm chí là ngưng hoạt động vì bị chiếm tài nguyên.

Phát hiện bằng cách đặt ngưỡng thông báo khi gặp gói tin ICMP với dung lượng lớn:

```
alert icmp any any -> $HOME_NET any(msg:"ICMP Ping Of Dead attack"; itype:8; dsize>1000; sid:1000000003; rev:1)
```

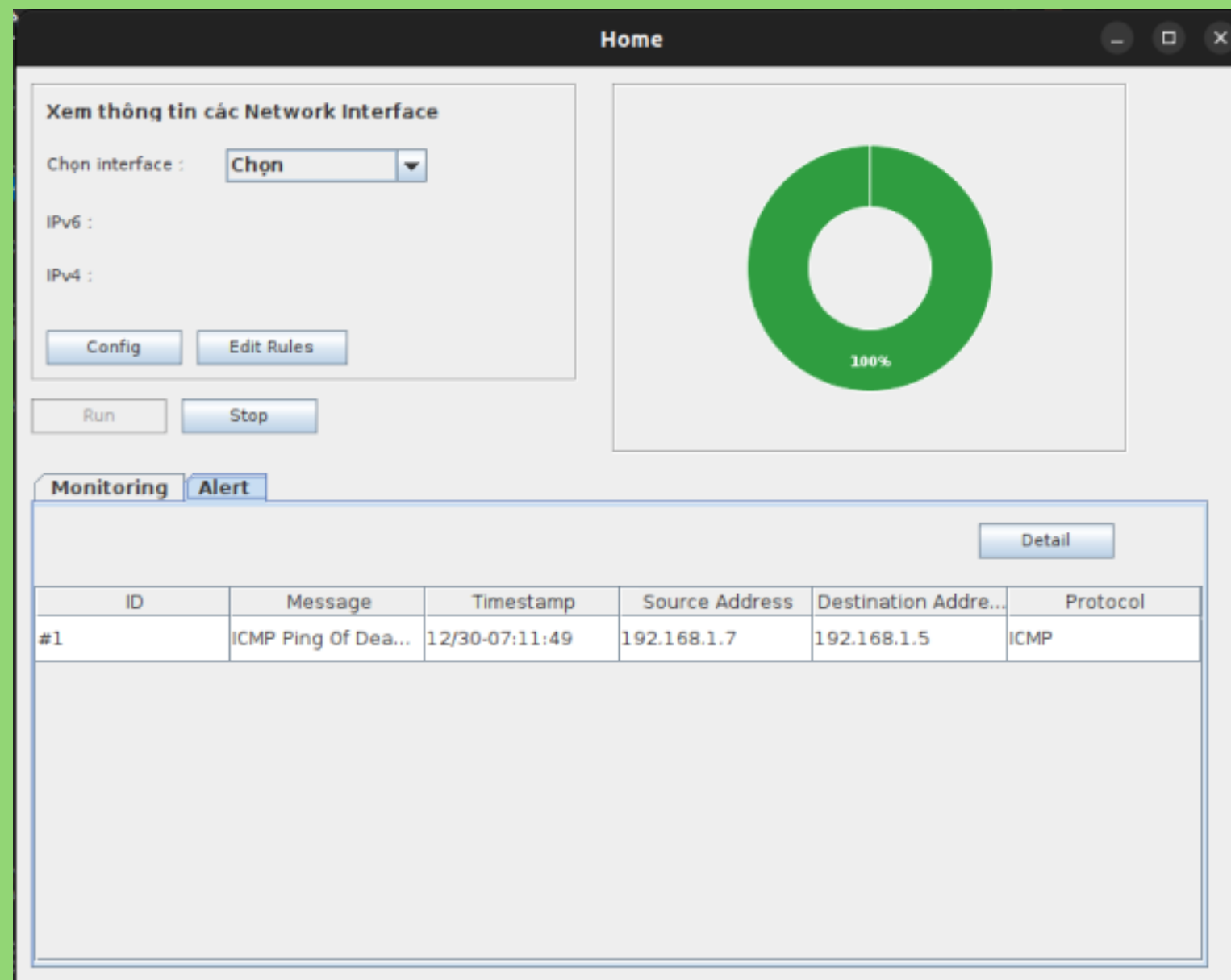
Ngăn chặn bằng cách chặn các Ping tự tiện Ping tới máy chủ.

```
iptables -I INPUT -p icmp -j DROP
```

5. Kết quả triển khai và đánh giá

```
C:\Users\HP>ping -l 65500 192.168.1.5 -t

Pinging 192.168.1.5 with 65500 bytes of data:
Reply from 192.168.1.5: bytes=65500 time=5ms TTL=64
Reply from 192.168.1.5: bytes=65500 time=7ms TTL=64
Reply from 192.168.1.5: bytes=65500 time=7ms TTL=64
Reply from 192.168.1.5: bytes=65500 time=7ms TTL=64
```



ID	Message	Timestamp	Source Address	Destination Addr...	Protocol
#35	ICMP Ping Of De...	12/30-07:11:56	192.168.1.7	192.168.1.5	ICMP
#36	ICMP Ping Of De...	12/30-07:11:56	192.168.1.7	192.168.1.5	ICMP
#37	ICMP Ping Of De...	12/30-07:11:57	192.168.1.7	192.168.1.5	ICMP
#38	ICMP Ping Of De...	12/30-07:11:57	192.168.1.7	192.168.1.5	ICMP
#39	ICMP Ping Of De...	12/30-07:11:58	192.168.1.7	192.168.1.5	ICMP
#40	ICMP Ping Of De...	12/30-07:11:58	192.168.1.7	192.168.1.5	ICMP
#41	ICMP Ping Of De...	12/30-07:11:59	192.168.1.7	192.168.1.5	ICMP
#42	ICMP Ping Of De...	12/30-07:11:59	192.168.1.7	192.168.1.5	ICMP
#43	ICMP Ping Of De...	12/30-07:12:00	192.168.1.7	192.168.1.5	ICMP
#44	ICMP Ping Of De...	12/30-07:12:00	192.168.1.7	192.168.1.5	ICMP
#45	ICMP Ping Of De...	12/30-07:12:01	192.168.1.7	192.168.1.5	ICMP
#46	ICMP Ping Of De...	12/30-07:12:01	192.168.1.7	192.168.1.5	ICMP



5. Kết quả triển khai và đánh giá

Nhằm lợi dụng việc sau khi nhận gói tin SYN, Server phải trả lời bằng gói tin SYN/ACK và đợi chờ việc xác nhận từ Client. Việc tấn công diễn ra như thế này

- Người tấn công sẽ gửi một lượng lớn các gói tin SYN cho Server
- Server phải trả lời hết tất cả các gói tin và dùng mỗi cổng riêng biệt để đợi chờ trả lời từ Client
- Vì chờ đợi gói tin ACK từ Client (thứ sẽ không bao giờ đến), việc sử dụng tài nguyên cổng cứ thế diễn ra cho đến khi các cổng hiện có được sử dụng hết, lúc đó hệ thống sẽ không thể làm việc bình thường được.

Cách phát hiện: Đặt thông báo khi số lượng cờ SYN tới vượt quá ngưỡng quy định.

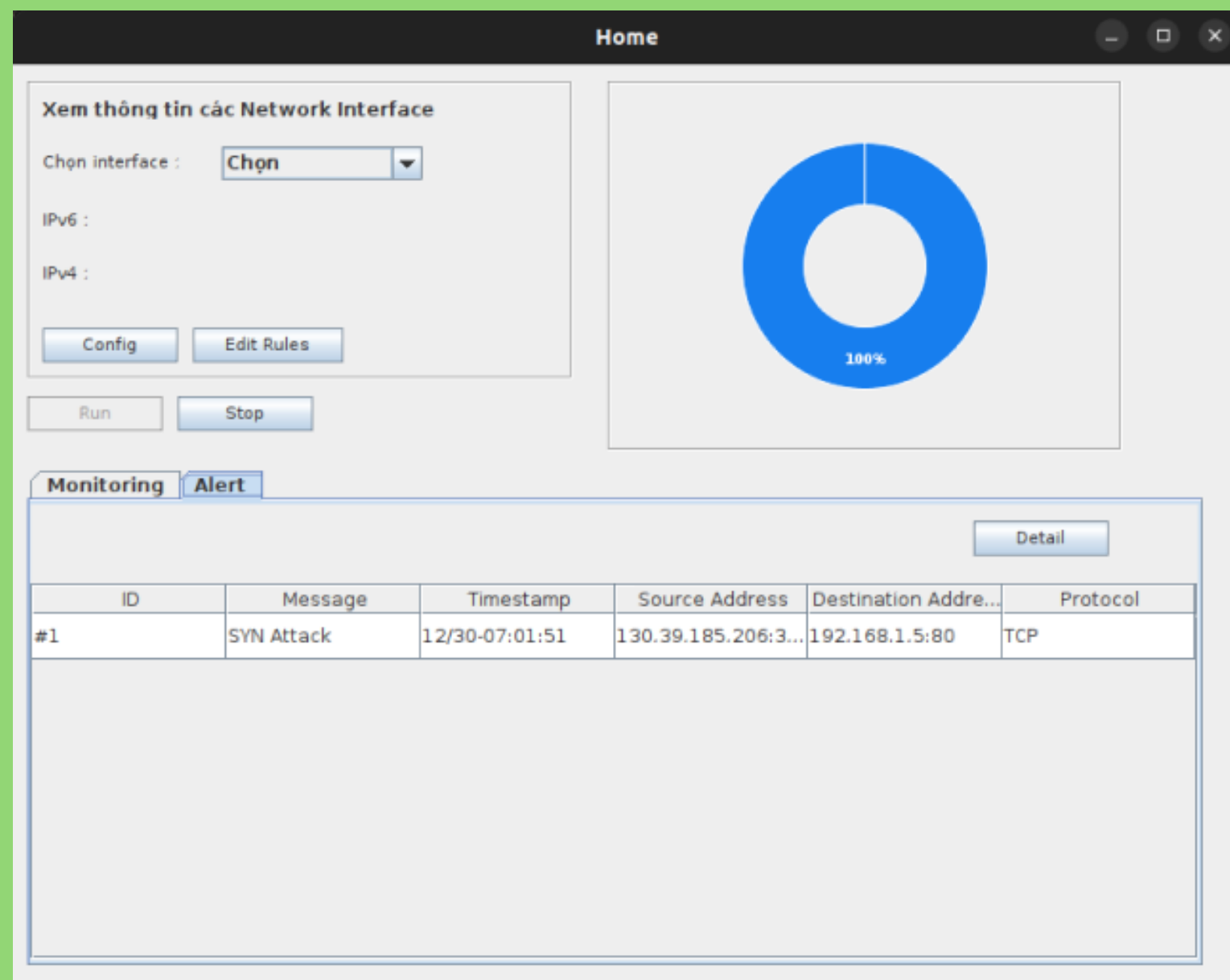
```
alert tcp any any -> $HOME_NET any (msg:"SYN attack"; flags:S; threshold: type threshold, track by_dst, count 1000, seconds 60; sid:10004; rev:1;)
```

Cách ngăn chặn: Giới hạn số lượng gói tin SYN chấp nhận được trong một thời gian cố định.

```
sudo iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
```

5. Kết quả triển khai và đánh giá

```
(kali@kali)-[~/Desktop]
$ sudo hping3 -S -p 80 --flood --rand-source 192.168.1.5
[sudo] password for kali:
HPING 192.168.1.5 (eth0 192.168.1.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



ID	Message	Timestamp	Source Address	Destination Addr...	Protocol
#85	SYN Attack	12/30-07:01:51	171.215.86.174:...	192.168.1.5:80	TCP
#86	SYN Attack	12/30-07:01:51	171.215.86.174:...	192.168.1.5:80	TCP
#87	SYN Attack	12/30-07:01:51	171.215.86.174:...	192.168.1.5:80	TCP
#88	SYN Attack	12/30-07:01:51	52.172.123.134:...	192.168.1.5:80	TCP
#89	SYN Attack	12/30-07:01:51	52.172.123.134:...	192.168.1.5:80	TCP
#90	SYN Attack	12/30-07:01:51	52.172.123.134:...	192.168.1.5:80	TCP
#91	SYN Attack	12/30-07:01:51	136.185.171.18...	192.168.1.5:80	TCP
#92	SYN Attack	12/30-07:01:51	136.185.171.18...	192.168.1.5:80	TCP
#93	SYN Attack	12/30-07:01:51	136.185.171.18...	192.168.1.5:80	TCP
#94	SYN Attack	12/30-07:01:51	130.39.185.206:...	192.168.1.5:80	TCP
#95	SYN Attack	12/30-07:01:51	130.39.185.206:...	192.168.1.5:80	TCP
#96	SYN Attack	12/30-07:01:51	130.39.185.206:...	192.168.1.5:80	TCP

6. Kết luận và hướng phát triển

Kết luận:

Thông qua nghiên cứu và triển khai hệ thống IDS SNORT, chúng em đã rút ra được các kết luận về ưu và nhược điểm của kết quả mà bọn em đã hoàn thành:

Ưu điểm:

- Thành thực sử dụng Linux, Snort và iptables
- Kết quả cho ra chương trình Snort có giao diện dễ tiếp cận, thân thiện với người dùng.

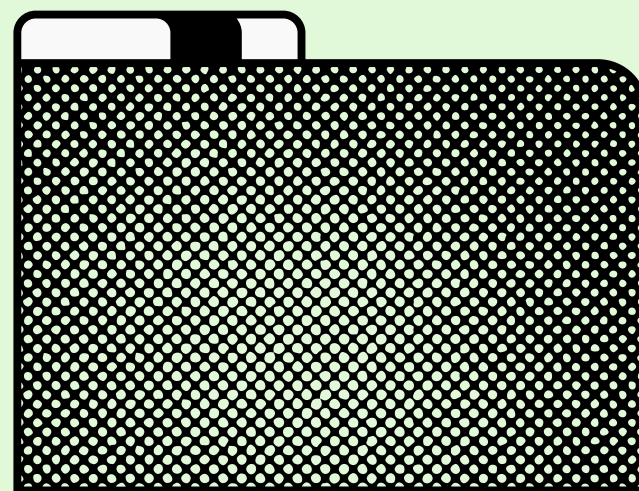
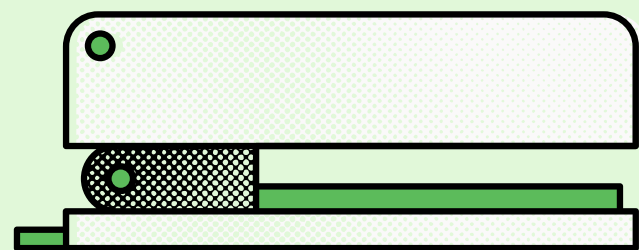
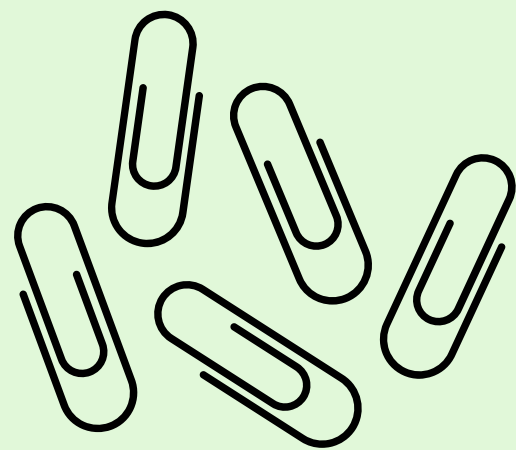
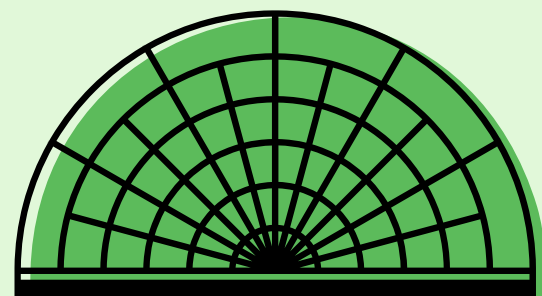
Nhược điểm:

- Các cuộc tấn công tìm hiểu được quá ít, chưa đầy đủ bảo mật cho một hệ thống có thể hoạt động tốt.

Hướng phát triển:

Thông qua bài PBL lần này, chúng em đã có một vài hướng phát triển cho đề án trở nên hoàn thiện hơn:

- Trao dồi thêm kiến thức về các giao thức khác
- Tìm hiểu thêm về các hình thức tấn công khác, về công cụ tấn công cũng như biện pháp chống lại nó



**THANK
YOU**