1. Thay đổi nội dung tấn công :
2. Giao thức tầng network : ip ,icmp,arp
3. Biết cách bypass => Phòng chống
4. Kiểm thử : biết cách bypass IDS cho hệ thống của mình
5. Scan không phải là tấn công
6. "fall-open" : tình trạng của các thiết bị bảo mật (firewall, IPS, IDS,..) khi không thể hoạt động chính xác

A picture containing text, screenshot, font

Description automatically generated

18 kỹ thuật bypass :

Vd : viết payload ngoài định nghĩa của signature

1.**Insertion Attack**

- Attacker gửi 

Qua mặt đc IDS do có nhiều kí tự lạ khác signature

Qua hệ thống đầu cuối nó sẽ xóa các kí tự lạ => 

 là payload tấn công

2.**Evasion**

- IDS loại bỏ 1 số byte => k phát hiện đc (tránh bị chặn hoặc báo động bởi IDS)

IDS nhận ít gói tin hơn hệ thống đầu cuối

NIC -> kernel -> application (ids)

Kernel,hardwire khác nhau => xử lý khác nhau

1 số data đến kernel sẽ bị loại bỏ

Cắt nhỏ gói tin : đảm bảo tính linh hoạt và hiệu quả của mạng.

**03. Denial-of-Service Attack (DoS)**

Hệ thống bị treo = > k ghi đc logs

* Ng phân tích k có đủ data

Làm hệ thống quá tải => làm sao , bỏ sót

**04. False Positive Generation**

- Tạo ra các cảnh báo sai

- Scan nhiều vào mạng => sinh ra các cảnh báo (ping) nhưng k phải tấn công thực sự

**DoS và False Positive Generation**

**05. Obfuscating – Làm rối mã**

- encode payload tấn công

- IDS đọc k hiểu , chỉ có hệ thống đầu cuối

**06. Session Splicing**

chia nhỏ traffic tấn công thành nhiều gói tin để không 1 gói nào bật cảnh báo trên IDS

K lắp thì k biết đc tấn công

Delay nhiều hơn timeout của bộ lắp ráp => k lắp ráp đc để kiểm tra => IDS k nhận biết đc

A picture containing text, font, screenshot, line

Description automatically generated

**07. Fragmentation Attack**

A picture containing text, human face, website, web page

Description automatically generated

**07. Fragmentation Attack (tt)**

A picture containing text, screenshot, software, web page

Description automatically generated

**08. Overlapping Fragments**

tạo ra loạt các fragment nhỏ với các sequence number chồng chéo nhau

vd : 123 , 345 (3 bị chồng)

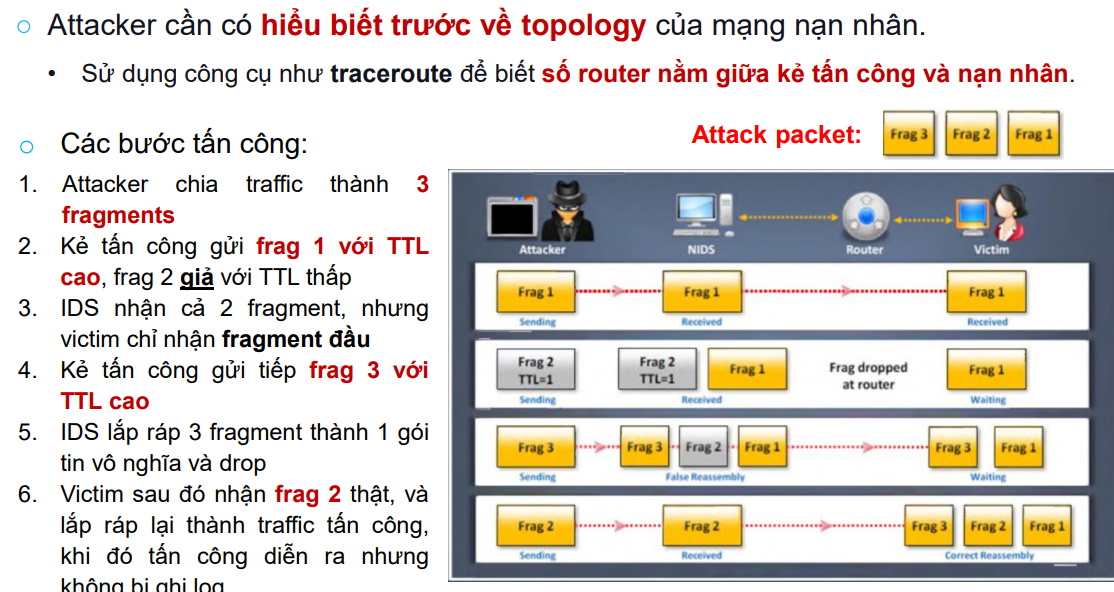
Win : giữ gói đầu

Cisco : giữ gói sau

A screenshot of a computer

Description automatically generated with medium confidence

**09. Time-To-Live Attacks**

****

**10. Invalid RST Packets**

- Gói reset : Tự động ngắt session

A picture containing text, screenshot, font

Description automatically generated

**11. Urgency Flag**

- Nhiều IDS không xem xét urgent pointer và xử lý tất cả gói tin trong traffic trong khi victim chỉ xử lý dữ liệu khẩn cấp

A picture containing text, font, screenshot, line

Description automatically generated

**12. Unicode Evasion**

Viết signature : chặn #

Attacker mã hóa # duoi dạng unicode

**13. Polymorphic Shellcode – Đa hình**

- Decryptor khác nhau

IDS : string thường

Attacker dùng string đc encode

=> Dùng decode để giải => Shell đc giải mã thì khác hoàn toàn lúc IDS nhận đc

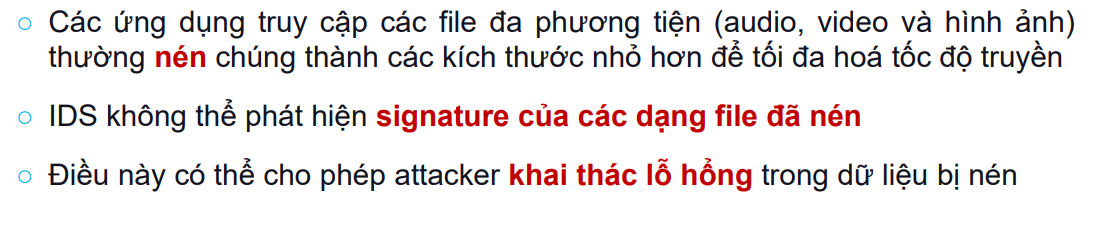
=> Qua mặt string shell code signature

**14. ASCII Shellcode**

- shellcode : dạng byte

Attacker đổi thành dạng chữ => By pass

**15. Application-Layer Attacks**



**16. Desynchronization**

- Attacker gửi gói syn với sequence number giả :

Đang là 6 , gửi 1 , IDS k tốt => reset về 1

* Khớp với phiên của attacker
* Attacker dùng phiên khác gửi tới victim
* IDS vô dụng

A picture containing text, screenshot, font

Description automatically generated

A screenshot of a computer

Description automatically generated with low confidence