**BỘ THÔNG TIN TRUYỀN THÔNG**



**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

----------

**Kỹ thuật giấu tin trong văn bản**

**Sử dụng CFG để giấu tin vào văn bản và truyền tin**

**LAB: cfg-lab-detect**

**Sinh viên:** Lê Văn Tuấn

**Mã sinh viên:** B21DCAT208

**Bộ môn:** Kỹ thuật giấu tin

**Giảng viên hướng dẫn:** PGS.TS. Đỗ Xuân Chợ

**Hà Nội – 2025**

1. **Mục đích**

Giúp sinh viên hiểu hơn về thuật toán sử dụng phương pháp giấu tin CFG (Context Free Grammar), và vận dụng các thức tấn công người đứng giữa (MITM) để thực hiện bắt và phát hiện một văn bản có bị giấu tin bằng CFG không

1. **Yêu cầu đối với sinh viên**

Có kiến thức về mật mã học cơ sở và kĩ thuật giấu tin, sử dụng thành thạo linux

1. **Nội dung lý thuyết**

Văn phạm phi ngữ cảnh là một tập hợp hữu hạn các biến (còn được gọi là các ký hiệu chưa kết thúc), mỗi biến biểu diễn một ngôn ngữ. Ngôn ngữ được biểu diễn bởi các biến được mô tả một cách đệ quy theo thuật ngữ của một khái niệm khác gọi là ký hiệu kết thúc. Quy tắc quan hệ giữa các biến gọi là luật sinh. Mỗi luật sinh. Mỗi luật sinh có dạng một biết, ở vế trái sinh ra một chuối có thể gồm biến lẫn các ký hiệu là văn phạm G (V, T, P, S), trong đó:

* V là tập hợp hữu hạn các biến
* T là tập hợp hữu hạn các ký tự kết thúc V ∩ T = ∅
* P là tập hợp hữu hạn các luật sinh mà mỗi luật sinh có dạng A → α (với A là biến và α là chuỗi các ký hiệu ∈ (V∪T)\*)
* S là một biến đặc biệt gọi là ký hiệu bắt đầu văn phạm.

Các quy tắc sau chỉ ra cách để tạo ra một chuỗi (gồm các kí hiệu kết thúc) từ một CFG cho trước:

* Sử dụng 1 kí hiệu bắt đầu để khởi đầu. Chọn một luật có kí hiệu khởi đầu ở bên trái và chọn một kí hiệu ở phần bên phải của luật để thay thế kí hiệu khởi đầu này. Kí hiệu được sử dụng sẽ là một thành tố của văn bản sẽ được tạo sao này.
* Chọn 1 kí hiệu chưa kết thúc trong văn bản, tìm một luật có kí hiệu chưa kết thúc này ở bên trái và thay thế kí hiệu này bằng một kí hiệu ở phần bên phải của luật.
* Lặp lại bước 2 cho đến khi văn bản chỉ còn lại toàn các kí hiệu kết thúc.

Sau khi giấu tin xong sẽ gửi văn bản đến một máy client sau đó client giải mã thông điệp.

1. **Nội dung thực hành**

Add module file lab:

Khởi động bài lab:

Vào terminal gõ:

labtainer -r cfg-lab-detect

(Chú ý: Sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu để sử dụng khi chấm điểm)

**Nhiệm vụ 1: Thử với văn bản không giấu tin**

Trên máy attacker sẽ có 1 file detect.py, file này thực hiện tính xác suất khả năng giấu tin của 1 văn bản bằng cách kiểm tra cấu trúc ngữ pháp, do khi giấu tin bằng CFG, sẽ rất dễ tồn tại rất nhiều lỗi ngữ pháp cũng như lặp từ. Thử với 1 file message có nội dung là “Hello I am Test”

echo “Hello I am Test” > message.txt

python3 detect.py -m message.txt

**Nhiệm vụ 2: Giấu tin**

Nhiệm vụ của user1 sẽ là gửi thông điệp cho user2, user2 nhận và giải mã thông điệp. Chạy lệnh

python3 CFG\_encode.py -m “Hello”

**Nhiệm vụ 3: Cài đặt môi trường**

Bây giờ ta cần chạy dịch vụ ftp server để user1 có thể gửi thông điệp cho user2. Ở máy user2 chạy:

python3 ftp\_server.py

Đồng thời cùng lúc này attacker sẽ khởi động dịch vụ arpspoof để thực hiện ARP spoofing, giả mạo địa chỉ MAC của user2. Ở máy attacker chạy đồng thời arpspoof và attack.py:

sudo arpspoof -i eth0 -t 192.168.0.10 192.168.0.20

sudo python3 attack.py

**Nhiệm vụ 4: Nghe lén**

Ở máy user1, tiến hành gửi file message.txt cho user2 (username là user và password là 123456):

ftp 192.168.0.20

put message.txt

Cùng lúc đó ở bên máy attacker, ta có thể thấy được thông tin của user2 đã được ghi lại ở giao diện attack.py

**Nhiệm vụ 4: Nhận file**

Sau khi có được thông tin của user2, tại máy attacker ta tiến hành ftp và get các file cần thiết về để phân tích

ftp 192.168.0.20

get message.txt

**Nhiệm vụ 5: Phát hiện giấu tin**

Chạy lại file detect.py 1 lần nữa để xem lần này nó có thể phát hiện được văn bản trong file message.txt bị giấu tin hay không

python3 detect.py -m message.txt

**Kết thúc bài thực hành**

* Kiểm tra checkwork

checkwork

* Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab

stoplab

Khởi động lại bài lab

labtainer -r cfg-lab-detect