HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ

ĐỀ TÀI: TẤN CÔNG CHÈN BLOCK GIẢ VÀO BLOCKCHAIN KHI KIỂM TRA POW KHÔNG ĐẦY ĐỦ

Sinh viên thực hiện:

B22DCAT239 Phạm Đức Quân

Tên nhóm: 05

Tên lớp: N4

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

HÀ NỘI 5-2025

TẤN CÔNG CHÈN BLOCK GIẢ VÀO BLOCKCHAIN KHI KIỂM TRA POW KHÔNG ĐẦY ĐỦ

CHƯƠNG 1. GIỚI THIỆU VỀ BÀI THỰC HÀNH

1.1 Proof of Work (PoW) là gì?

Proof of Work (PoW - Bằng chứng công việc) là cơ chế đồng thuận đầu tiên được tạo ra trên Blockchain và khá phổ biến trong thế giới tiền điện tử. Proof of Work được Satoshi Nakamoto áp dụng thành công cho Bitcoin vào năm 2009. Từ đó đến nay, PoW là một trong những cơ chế đồng thuận phổ biến nhất trong hệ sinh thái Cryptocurrency.

Proof of Work tập hợp các thợ đào (hay còn gọi là node) tham gia cạnh tranh xác thực các giao dịch, sau đó đưa giao dịch vào các block trong Blockchain để nhận phần thưởng tùy theo mạng lưới.

Ví dụ: Các thợ đào của Ethereum sẽ xác nhận các giao dịch trên Ethereum, đưa vào block và nhận về ETH làm phần thưởng.

Bản chất của Proof of Work chính là xác nhận bằng chứng làm việc của ai đó là hợp lệ đến toàn bộ mạng lưới blockchain, thông qua việc tiêu tốn tài nguyên trong thế giới thực.

1.2 Giới thiệu chung về bài thực hành

Bài thực hành tấn công PoW-Fake giúp sinh viên tìm hiểu cách một attacker có thể gửi block giả vào hệ thống blockchain nếu nút mạng (node victim) kiểm tra thuật toán Proof of Work không đầy đủ. Cụ thể, attacker sẽ không thực hiện quá trình tính toán khai thác block như bình thường, mà dùng một block giả có hash "trông hợp lệ" (bắt đầu bằng 0000) để đánh lừa victim.

Mục đích:

- Hiểu bản chất của **thuật toán PoW (Proof of Work)** trong blockchain.
- Phân tích lỗ hổng khi node chỉ kiểm tra hash.startswith("0000").
- Viết mã tấn công gửi block giả từ attacker → victim.
- Thực hành kiểm tra nonce, kiểm thử block hợp lệ và đánh giá hệ thống.

Yêu cầu đối với sinh viên:

- Hiểu cơ bản về thuật toán băm SHA256, nonce, thuật toán đồng thuận PoW.
- Biết sử dụng Linux Terminal, chỉnh sửa file Python, sử dụng labedit, checkwork.
- Biết cách xác định địa chỉ IP, giao tiếp socket giữa hai máy (attacker ↔ victim).

1.3 Nội dung thực hành

Sinh viên tải bài lab bằng lệnh

imodule https://github.com/PoPo502/mmh2025/raw/main/imodule.tar

Sinh viên khởi động bài lab bằng lệnh :

labtainer pow-fake

(Chú ý: sinh viên sử dụng MÃ SINH VIÊN của mình để nhập thông tin người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động bài lab thành công sẽ hiện ra hai terminal một của attacker một của victim.

TASK 1: Kiểm tra kết nối thành công giữa máy attacker và server

- Trên hai terminal thực hiện câu lệnh ***ifconfig*** kiểm tra địa chỉ ip của hai máy
- Từ terminal attacker thực hiện lệnh: ***ping <địa chỉ IP máy server>*** để kiểm tra kết nối giữa 2 máy.

TASK 2: Tìm nonce hợp lệ

Trên terminal attacker sinh viên kiểm tra file ***find_nonce.py*** và chạy file ***find_nonce.py*** để tìm nonce hợp lệ:

python3 find_nonce.py

TASK 3: Sửa mã attacker và gửi block giả

Sinh viên mở file fake_block_sender.py để sửa mã sao cho phần nonce là nonce hợp lệ vừa tìm được ở bên trên và sửa phần "host" là ip của victim

nano fake_block_sender.py

Trên terminal victim chạy file victim_node.py để victim lắng nghe thông điệp

Trên terminal attacker chạy file fake_block_sender.py để gửi block giả sang máy victim.

Block sẽ được gửi, victim sẽ ghi lại log vào file fake_pow.log:

cat fake_pow.log

Nếu gửi thành công thì thông điệp sẽ là "Victim accepted fake block" nếu không thành công sẽ là "Victim rejected fake block".

Kết thúc lab:

Trên terminal khởi động lab, sinh viên sử dụng lệnh:

stoplab

Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab. Sinh viên cần nộp file .lab để chấm điểm.

Để kiểm tra kết quả khi trong khi làm bài thực hành sử dụng lệnh:

checkwork <tên bài thực hành>

Sinh viên cần nộp file .lab để chấm điểm.

Kiểm tra kết quả trong quá trình làm bài:

checkwork <tên bài lab>

Khởi động lại bài lab: Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer -r pow-fake