Bài thực hành: Sử dụng RsaCtfTool để tấn công với khóa bí mật nhỏ

1. Mục đích

Giúp hiểu được cách sử dụng công cụ rsactftool cho tấn công RSA, sử dụng openssl cho mã hóa, giải mã thuật toán mã hóa RSA.

2. Yêu cầu đối với sinh viên

Có kiến thức về mã hóa RSA, tấn công wiener. Sử dụng công cụ rsactftool và openssl.

3. Nội dung bài thực hành

Khởi động bài lab:

imodule https://github.com/baprang186/labtainer/raw/main/imodule_cryp-attk-rsa_rsactftool.tar

Vào terminal, gõ:

labtainer cryp-attk-rsa_rsactftool

(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)

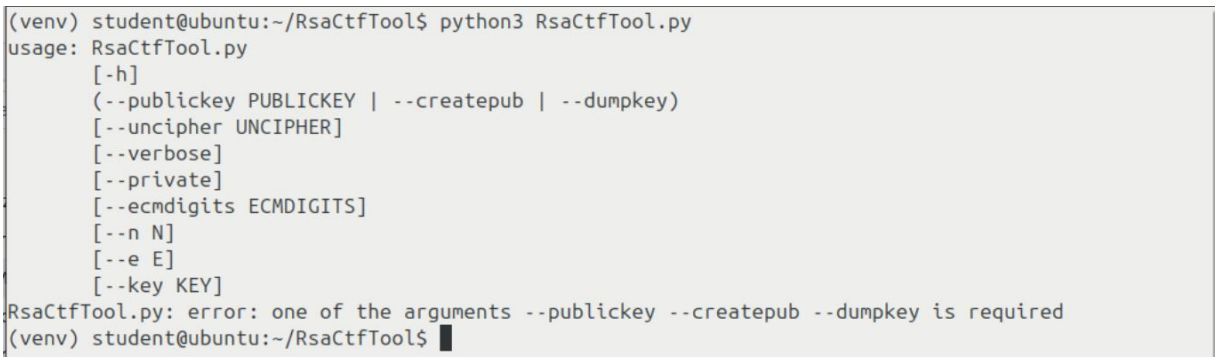
Sau khi khởi động xong, màn hình sẽ xuất hiện 1 terminal với người dùng **student**. Khởi động môi trường ảo để thực hiện bài lab, thực hiện lệnh:

source venv/bin/activate

Bài lab cho sẵn 1 file value.txt chứa giá trị khóa công khai n, e. Để thực hiện được công cụ rsactftool cho tấn công wiener tìm khóa bí mật. RsaCtfTool là một công cụ mạnh mẽ hỗ trợ giải mã RSA trong các bài tập CTF và thực tế. Nó được thiết kế để khai thác các điểm yếu thường gặp trong việc triển khai thuật toán RSA, chẳng hạn như:

- **Yếu tố hóa nhanh:** Tự động phân tích và tìm các thừa số của mô-đun n khi có khóa yếu.
- **Tấn công Wiener:** Nhắm vào trường hợp khóa riêng d quá nhỏ.
- **Tìm khóa riêng từ thông tin bổ sung:** Ví dụ như khi có p,q,d,n hoặc các thông tin khác liên quan.
- **Khai thác các lỗ hổng RSA phổ biến khác:** Như tấn công module chung, tấn công số mũ khóa công khai e nhỏ.

Các chức năng của công cụ RsaCtfTool



Ta cần đổi giá trị khóa công khai về dạng khóa pem. Thực hiện lệnh sinh khóa công khai, gõ:

python3 rsactftool.py --createpub --n <giá trị n> --e <giá trị e>

Thực hiện tạo 1 bản rõ bất kì bằng nano hoặc touch. Sử dụng openssl để mã hóa bản rõ:

openssl pkeyutl -encrypt -inkey <file publickey> -pubin -in <file plaintext> -out <file mã hóa>

Tiếp tục sử dụng công cụ rsactftool để tìm khóa bí mật, thực hiện lệnh:

python3 rsactftool.py --publickey <file publickey> --verbose --private

Kết quả tìm được sẽ trả về khóa bí mật dạng pem. Sử dụng openssl để tìm lại bản rõ:

openssl pkeyutl -decrypt -inkey <file privatekey> -in <file ciphertext> -out <file bản rõ khác>

Thực hiện kiểm tra bản rõ bằng lệnh cat.

Kết thúc bài lab:

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

stoplab cryp-attk-rsa_rsactftool

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

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

startlab –r cryp-attk-rsa_rsactftool