**Báo cáo bài tập số 3**

**Phần lý thuyết:**

**Cách hoạt động của ssh:**

Tạo kết nối đến một ssh server khác, tiến hành xác thực để có thể truy cập vào server dưới quyền một user nào đó.

**Cách hoạt động của sshd:**

Tạo một cổng để lắng nghe request từ ssh client, tiến hành xác thực tài khoản và mật khẩu của client thông qua pam modules để cấp quyền cho client.

**Cơ chế xác thực của PAM:**

Pam (Pluggable Authentication Modules) làm cấu nối trung gian giúp các bộ phận khác xác thực với hệ thống quản trị bằng mật khẩu, dấu vân tay,… Khi có yêu cầu truy cập gửi đến sshd, nó sẽ chuyển đến pam module rồi được pam truy vấn về file /etc/shadow để tiến hành xác thực.

**Cơ chế xác thực của strace và ptrace:**

Strace có nhiệm vụ theo dõi các system call đang được chạy của một tiến trình trong khi ptrace cho biết phương thức để một tiến trình quan sát và điểu khiển tiến trình khác.

**Phần thực hành:**

**Cách hoạt động của sshtrojan1:**

1. Tìm kiếm process có người đăng nhập sudo ps aux | grep "\[priv\]"
2. Từ lệnh này, lấy tên Username và id của tiến trình
3. Tiến hành đọc thông tin trao đổi từ tiến trình vào file foo sudo strace -p [ppid] 2> foo
4. Hàm check có chức năng kiểm tra xem đã có mật khẩu nhập đúng hay chưa
5. Nếu có mật khẩu đúng, tiến hành truy vết input và lấy mật khẩu

**Lưu ý**: Trong sshd\_config để 2 dòng sau ở trạng thái uncommented PubkeyAuthentication no và PasswordAuthentication yes

**Cách hoạt động của sshtrojan2:**

1. Phát hiện process được dùng để đăng nhập nơi khác pgrep -a -f '^ssh '
2. Tại bước này ta lấy được username và pid
3. Tiến hành đọc thông tin trao đổi từ tiến trình vào file foo sudo strace -p [ppid] 2> foo
4. Dựa trên trạng thái trong reply message của máy tính kết nối (=28 cho password đúng)
5. Khi có tín hiệu mất khẩu đúng, truy vết file và lấy mật khẩu

**Kiến thức nắm được sau bài tập:**

* Cài đặt SSH trên Windows và Linux, thiết lập config SSH server thông qua file 'sshd\_config'
* Lấy thông tin từ tiến trình
* Đọc dữ liệu từ file lưu trữ nội dung tương tác giữa client và server của SSH
* Chạy lệnh song song để thu thập thông tin mà không ảnh hưởng đến trạng thái hoạt động của tiến trình
* Thực hiện code và compile trên và cấp quyền root cho Sublime-Text