**CHƯƠNG TRÌNH ĐÀO TẠO SINH VIÊN**

# PROG03: LẬP TRÌNH SSH LOGGER

| **Path** | Ứng dụng/Lập trình /SSH Logger |
| --- | --- |
| **Phụ trách** | KhanhPV6 |
| **Thời gian** | 1 tuần |

**Lý Thuyết (2đ):**

* Tìm hiểu cách hoạt động của dịch vụ sshd và tiến trình ssh.
* Tìm hiểu cơ chế xác thực pam của hệ điều hành linux.
* Tìm hiểu cách hoạt động của strace, ptrace.

# Thực Hành (8đ):

Trường hợp đang có quyền root để truy cập vào 1 máy tính linux. Xây dựng chương trình để lấy được username, password ssh trong 2 trường hợp sau mà không thay đổi luồng hoạt động bình thường:

* Một user tiến hành truy cập vào máy tính đó thông qua ssh (chương trình sshtrojan1 - 4đ). Yêu cầu:
  + Username, password log vào file /tmp/.log\_sshtrojan1.txt
  + Trong báo cáo có mô tả lại cách hoạt động, cách sử dụng của sshtrojan1.
  + Chỉ log lại username và password đúng.
* Một người dùng đứng trên máy tính đó ssh đi một máy tính khác (chương trình sshtrojan2 - 4đ). Yêu cầu:
  + Username, password log vào file /tmp/.log\_sshtrojan2.txt
  + Trong báo cáo có mô tả lại cách hoạt động, cách sử dụng của sshtrojan2.

# Output:

* File báo cáo (docx, zip) đặt theo format sau: <username>\_challenge3.docx(.zip). Ví dụ khanhpv6\_challenge3.docx
* Link Github mã nguồn các chương trình sshtrojan1, sshtrojan2. Lập trình rõ ràng, sạch đẹp (code convention chuẩn)
* Quay video demo chạy thử các chương trình trên (có thể dùng Bandicam để quay màn hình): <username>\_demochallenge3.mp4

# Tài liệu tham khảo:

* https://en.wikipedia.org/wiki/Hooking
* <https://github.com/openssh/openssh-portable>
* Linux PAM Module

Tài liệu này thuộc sở hữu của Viettel. Việc phát tán, sử dụng trái phép bị nghiêm cấm 1/1