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 bài lab:
    - Vào terminal, gõ:

startlab ptit-netcat-shellscript

(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 khách: ***client***, một cái là đại diện cho máy chủ: ***server.*** Biết rằng 2 máy nằm cùng mạng LAN.

- Trên terminal ***client*** sử dụng lệnh

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

Để tạo 1 file gửi đi có nội dung bất kỳ có 20 ký tự.

Trên terminal **server** sử dụng lệnh

nc -l -p 12345 > receive.txt

Để mở một kết nối netcat lắng nghe (listening) trên cổng 12345

Tiếp tục sử dụng Netcat để gửi dữ liệu từ file sendfile.txt tới máy server đang lắng nghe trên cổng 12345 sử dụng lệnh:

nc <IP máy server> 12345 < sendfile.txt

Sau đó mở và đọc nội dung file receive.txt

-
    -
        -
            - Trên máy khách ***server*** mở một kết nối Netcat (qua Ncat, một phiên bản mở rộng và an toàn hơn của Netcat) trên cổng 12345 và khi có kết nối được thiết lập, nó sẽ thực thi một phiên shell trên máy chủ.

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

Trên máy ***client*** mở một kết nối đến một máy chủ tại địa chỉ IP được chỉ định và cổng 12345 bằng cách sử dụng Netcat.

Sau khi kết nối được với máy chủ sử dụng lệnh "*whoami*" và "*ifconfig*" để chứng minh kết nối thành công.

-
    -
        -
            - Trên máy ***client*** tạo 1 file chứa các cổng cần đọc trong đó có cổng 22 bằng lệnh touch và nano (ví dụ ports.txt)

Tiếp tục trên máy ***client*** tạo một tệp script (ví dụ: scanning.sh) bằng trình soạn thảo văn bản. Trong tệp script sử dụng lệnh để đọc cổng trong file chưa cổng tạo ở trên:

#!/bin/bash

server_ip="<ip máy 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

Cấp quyền thực thi và chạy file script, sau đó đọc kết quả nhận được.

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

stoplab ptit-netcat-shellscript

-
    - 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:

stoplab –r ptit-netcat-shellscript