- Root-me.org là cổng thông tin cho phép thực hiện các bài thi CTF (Capture of Flag) hay gọi là Cướp cờ

- Các bài CTF trên root-me.org được phân nhóm. Ta chú ý tới 2 nhóm: App-script và CryptAnalysis

**I. Các bài tập mục App-Script**

- Bài Bash system 1: khai thác một nguy cơ về gán quyền cho file thực thi trên linux cụ thể như sau:

- Một số câu lệnh linux cần nhớ:

Whoami: xem tài khoản đang đăng nhập

Ls: xem nội dung thư mục hiện tại có những file nào, thuộc tính ra rao

Cat: đọc nội dung file

Mkdir: tạo thư mục

Cp: copy file

Cd: chuyển thư mục

Pwd: xem đường dẫn thư mục hiện thời

**Xem xét bài Bash System 1 ta nhận thấy một số điều sau:**

1. Chương trình ch11.c chỉ có một câu lệnh ls …/.passwd, lệnh ls là lệnh xem thư mục do đó thực hiện chương trình trên chỉ cho phép hiển thị đường dẫn của file .passwd

2. Xem thuộc tính của các file nhận thấy: file .passwd chỉ có thể đọc bởi quyền root hoặc owner bởi vì 3 bit permission tương ứng là r-- (r: là read, nếu dấu gạch thứ hai là w thì có quyền ghi write, dấu gạch thứ ba là x thì có quyền thực thi execute)

3. Xem permission của file ch11 nhận thấy root có quyền x-s. Bít s thể hiện rằng người sử dụng bình thường (không phải root, chẳng hạn là app-script-ch11) có thể thực thi file này và trong lúc thực thi file này, các câu lệnh trong chương trình ch11 sẽ được kế thừa quyền root có nghĩa là có thể xem được file .passwd bằng các lệnh trong file ch11 lúc nó thực thi

Từ đó ta rút ra cách giải như sau:

Chương trình ch11 có một lệnh ls (xem nội dung thư mục), ta sẽ làm lệnh ls này, mặc dù tên là ls nhưng sẽ chạy chương trình cat (xem nội dung file). Cách làm như sau:

Bước 1: Vì trong thư mục hiện tại ta không có quyền tạo thư mục và file nên ta sẽ tạo một thư mục của riêng ta ở trong /tmp bằng lệnh: mkdir /tmp/lagi

Bước 2: Copy chương trình cat của hệ thống nằm trong /bin vào trong thư mục vừa tạo với tên là ls bằng lệnh

cp /bin/cat /tmp/lagi/ls

Bước 3: Để hệ thống có thể tìm kiếm đến ls trong /tmp/lagi ta thêm đường dẫn tới /tmp/lagi vào biến môi trường $PATH bằng lệnh

export PATH=/tmp/lagi:$PATH

Bước 4: Chạy chương trình ch11 để hiển thị mật khẩu bằng lệnh

./ch11

Sinh viên có thể xem thêm cách giải ở mục solution của bài tập

**Cách giải bài Bash System 2**

Bước 1: Tạo thư mục tên là “tenla” trong thư mục /tmp bằng lệnh:

mkdir /tmp/tenla

Bước 2: Tạo một file shell-script với tên là ls trong thư mục vừa tạo bằng trình soạn thảo văn bản nano (file shell trên linux là file kịch bản, giống file .bat trên dos)

nano /tmp/tenla/ls

Bước 3: Sau khi trình soạn thảo nano xuất hiện ta soạn thảo file shell với hai lệnh: lệnh thứ nhất khai báo /bin/sh, lệnh thư hai là chạy trình đọc file /bin/cat với tham số là tham số thứ hai trên dòng lệnh (tham số này khi chạy lệnh ./ch12 chính là đường dẫn tới file chứa mật khẩu). Sau đây là nội dung file ls cần soạn thảo

#!/bin/sh

/bin/cat “$2”

Bước 4: Lưu nội dung file ls bằng phím nóng Ctrl – O rồi thoát khỏi nano bằng phím nóng Ctrl – X

Bước 5: Thêm quyền thực thi cho file shell tên là ls vừa soạn thảo bằng lệnh

chmod +x /tmp/tenla/ls

Bước 6: Để hệ thống có thể tìm kiếm đến ls trong /tmp/tenla ta thêm đường dẫn tới /tmp/tenla vào biến môi trường $PATH bằng lệnh

export PATH=/tmp/tenla:$PATH

Bước 7: Chạy chương trình ch11 để hiển thị mật khẩu bằng lệnh

./ch12

Sinh viên có thể xem thêm cách giải ở mục solution của bài tập

**II. Các bài tập mục Cryptanalysis**

1. Bài mã Ascii cho một chuỗi mã các ký tự dạng hexa, yêu cầu chuyển về chuỗi ký tự. Bài này rất đơn giản chỉ cần so sánh mã ascii tra ra ký tự tương ứng, hoặc dùng các hàm chuyển đổi mã trong các ngôn ngữ lập trình để hiển thị chuỗi

2. Bài mã Uuencode đã từng làm trên lớp, sinh viên có thể giải bằng tay hoặc viết chương trình máy tính để hiển thị chuỗi cần tìm

3. Bài mã băm Md5. Về nguyên tắc hàm băm là anh xạ một chiều chuyển từ một chuỗi ký tự sang chuỗi băm là chuỗi nhị phân có chiều dài cố định (ví dụ như Md5 thì chuỗi băm có độ dài 256 bit). Đếm số ký tự hexa ở chuỗi băm cho trong bài ta thấy đúng 32 byte tức là 256 bit của chuỗi nhị phân Md5. Về nguyên tắc ta không thể giải mã ngược từ chuỗi băm sang chuỗi ký tự bị băm ban đầu. Ý nghĩa của bài tập này nhắc chúng ta ghi nhớ điều này. Việc giải mã băm chỉ đơn thuần là việc so sánh chuỗi băm trong một cơ sở dữ liệu rất lớn đã có để tìm ra một số chuỗi mật khẩu phổ biến. Vậy để giải bài này ta có thể tìm một số Md5 decoder online cung cấp một cơ sở dữ liệu lớn các mã băm Md5 sau đó dán mã băm cần giải vào để tìm kiếm

4. Bài mã băm SHA-2