PRIVILEGE ESCALATION LAB (Linux)

I. Lý thuyết

\* Enumerating Linux

+ Hiểu về file và user privileges trong Linux

- File trong Linux: + Mọi đối tượng trong Linux đều là file (vì các yếu tố như thư mục, thiết bị, giao tiếp mạng,.. đều được đại diện bởi filesystem)

-

II. LAB

1. Editing /etc/passwd

\* Các tình huống

+ TH1: Thay password hash cho người dùng hiện tại trong file /etc/passwd bằng mật khẩu được mã hóa của chúng ta

+ TH2: Thêm một người dùng đặc quyền root vào file /etc/passwd với mật khẩu được mã hóa của chúng ta

+ TH3: Kiểm tra mật khẩu của root hoặc người dùng có đặc quyền cao trong tệp /etc/passwd

\* Sử dụng OpenSSL:

Method 1 (OpenSSL được sử dụng trên máy hacker):



Sử dụng lệnh:

**echo aarti: $1$rHGNLne3$R.Adl7iyNfmZeVs4utq/d1:0:0:root:/root:/bin/bash**

gid và uid là 0 => tương đương quyền root

A computer screen with white text and blue text

Description automatically generated

A screen shot of a computer

Description automatically generated

Method 2 (OpenSSL được sử dụng trên máy nạn nhân – nếu trên máy nạn nhân có openssl):

A screen shot of a computer

Description automatically generated

\* Mkpasswd

+ Là công cụ dòng lệnh được sử dụng để tạo ra các hàm băm mật khẩu dành cho nhiều hệ thống xác thực khác nhau



Options -m: method muốn sử dụng (MD5, SHA-512,…)

+ Tạo user như ở trên hoặc chỉnh sửa thủ công file /etc/passwd

A screen shot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

\* Python:

+ Sử dụng python để thêm 1 trường salt vào mật khẩu muốn tạo, điều này sẽ tạo ra mật khẩu chứa giá trị salt (Giá trị salt giống như $1 khi mã hóa MD5)



Lưu ý:

* Giá trị salt $6$salt, giá trị $6 là đại diện cho phiên bản của hàm băm (cụ thể là hàm SHA-512), không thể sửa thành một giá trị không tồn tại (giá trị đó không đại diện cho hàm băm nào)

+ Chỉnh sửa vào trong tệp /etc/passwd:

A screenshot of a computer

Description automatically generated

\* Perl:

A blue and orange text

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

\* PHP:



php -r: chạy script PHP từ dòng lệnh

crypt(‘aarti’,’123’): crypt nhận hai tham số

+ aarti: Chuỗi cần được mã hóa (trong TH này là mật khẩu)

+ 123: salt được sử dụng trong quá trình mã hóa (Có thể hiểu là giá trị được thêm kết hợp với mk trước khi băm => làm giá trị được mã hóa trở nên khó giải mã)

A screenshot of a computer

Description automatically generated

\* Ruby:



A screen shot of a computer code

Description automatically generated

Bonus:

A screen shot of a computer screen

Description automatically generated



1. Using SUID binaries:

A diagram of a group

Description automatically generated

+ Số bit tối đa được sử dụng để thiết lập cho người dùng là 7 (r-4; w-2; x-1)

+ THĐB: SUID, SGID

A diagram of a network

Description automatically generated with medium confidence

Khi bit bổ sung “4” được đặt thành Owner => thành SUID; khi bit “2” được đặt thành group => thành SGID

\* Quyền SUID:

+ Thường được sử dụng trên các file thực thi. Cho phép file được thực thi với đặc quyền của chủ sở hữu file đó (VD: file thuộc root, được set SUID, thì mọi user thực thi file đều chạy với đặc quyền root)

\* Leo thang:

- Bằng lệnh copy:

Method 1:

A computer screen shot of a computer code

Description automatically generated

A computer screen with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

Method 2:

- Bằng lệnh find:

A black background with white text

Description automatically generated

A computer screen shot of a computer

Description automatically generated

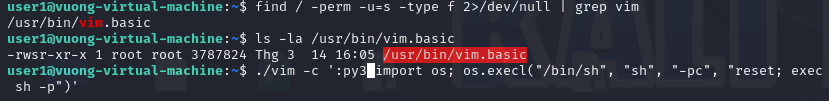


A screen shot of a computer

Description automatically generated

- Bằng Vim editor:

+ Cách 1:



(chuyển đến thư mục /usr/bin trước khi thực hiện)

A close up of a black background

Description automatically generated

+ Cách 2:

A screenshot of a computer screen

Description automatically generated

(Chỉnh sửa trong file sudoers:

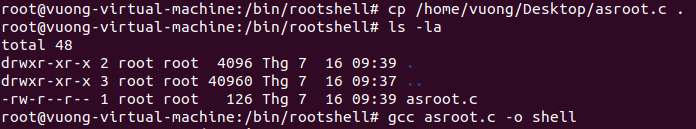
A screenshot of a computer

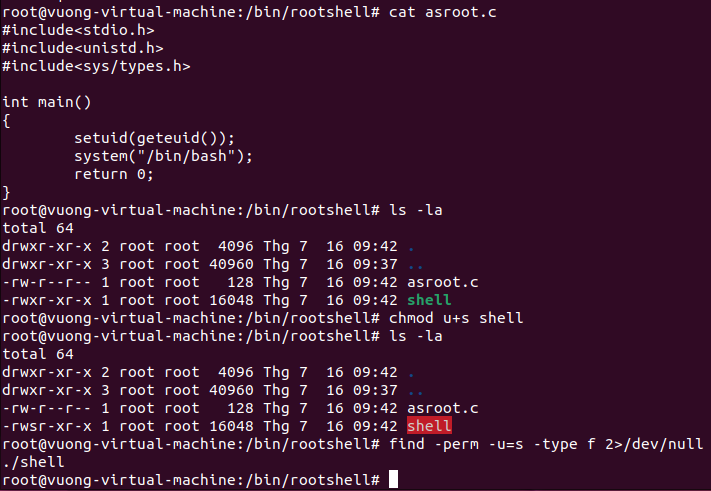
Description automatically generated

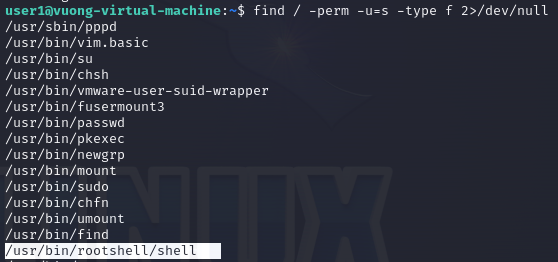
Cấp quyền cho user1)

- Sử dụng Save Script:









A computer screen shot of a computer code

Description automatically generated

- Sử dụng nano editor

+ Method 1: Chỉnh sửa file /etc/passwd



A screen shot of a computer code

Description automatically generated



A screen shot of a computer code

Description automatically generated

(Trong file /etc/passwd, thêm 1 tài khoản với đặc quyền root

)

+ Method 2: Lấy mật khẩu từ file /etc/shadow:

A screenshot of a computer screen

Description automatically generated

1. Using Sudo Rights

+ Tệp sudoers: Cấu hình cho quyền sudo; Lưu trữ người dùng+nhóm đặc quyền root để chạy lệnh với tư cách là root hoặc người dùng khác

+ Cú pháp tập tin:

- cấp quyền sudo cho user khác: nhập visudo, chỉnh sửa file sudoers

A diagram of a group of people

Description automatically generated with medium confidence

A close up of text

Description automatically generated

+ Traditional Method

A screenshot of a computer program

Description automatically generated

- Spawn Root Access:

A computer screen shot of a computer program

Description automatically generated

+ Default Method:

A blue and white text

Description automatically generated

- Spawn Root Access:

A screen shot of a computer

Description automatically generated

+ Quyền Root cho các lệnh nhị phân (Binary Commands)

(thực thi bất kỳ tệp/lệnh nào của 1 thư mục cụ thể)

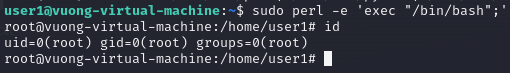
A screen shot of a computer

Description automatically generated

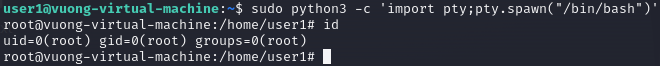
+ Quyền Root cho các chương trình nhị phân (Binary Programs)



- Tạo shell bằng Perl:



- Tạo shell bằng Python:



- Tạo shell bằng less:



A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

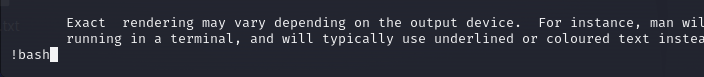
- Tạo shell bằng Awk:

A black background with white text

Description automatically generated

- Tạo shell bằng Man





A black background with white text

Description automatically generated

- Tạo shell bằng Vi-editor

A screenshot of a computer

Description automatically generated

A screen shot of a computer code

Description automatically generated

+ Sử dụng Shell Script (Các tệp ngôn ngữ bash, python, c):

- File asroot.c:

A computer screen shot of white text

Description automatically generated

- File asroot.sh:

A computer screen with text

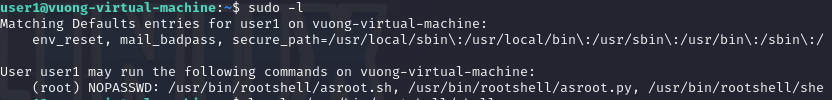
Description automatically generated

- File asroot.py:

A computer screen with text

Description automatically generated

- Cấu hình file sudoers:



A screenshot of a computer

Description automatically generated

- File .c:

Sử dụng gcc biên dịch file asroot.c (file mới có tên là shell)



- File .sh:



- File .py:



+ Một số chương trình khác:



- Env:



- Ftp:

A blue and white text

Description automatically generated

- Scp (Truyền file giữa các máy):

A computer screen with white text

Description automatically generated



- socat:



A screenshot of a computer program

Description automatically generated

1. NFS (Network File System):

+ NFS cho phép người dùng trên máy client gắn các tệp hoặc thư mục được chia sẻ qua mạng. NFS sử dụng

+ NFS sử dụng RPC (Remote Procedure Calls) để định tuyến các yêu cầu giữa máy khách và máy chủ

+ Sử dụng cổng TCP/UDP 2049

- Thiết lập NFS Lab:

+ 3 tệp cấu hình cốt lõi (/etc/export, /etc/hosts.allow, /etc/hosts.deny)

* Cấu hình yếu: /etc/export

+ Cú pháp cấu hình:

A black text on a white background

Description automatically generated

Một số options dể xác định loại quyền mà máy sẽ có đối với thư mục chia sẻ:

- **rw**: Cho phép máy client có quyền đọc + ghi vào thư mục chia sẻ

- **ro**: Cho phép máy khách truy cập chỉ đọc vào thư mục chia sẻ

- **root\_squash**: ngăn chặn yêu cầu tệp do người dùng root thực hiện trên máy khách (vì chia sẻ NFS thay đổi người dùng root thành nfsnobody- tài khoản người dùng không có đặc quyền)

- **no\_root\_squash**: cấp quyền cho người dùng root trên client để truy cập các tệp trên máy chủ NFS với tư cách là root.

- **async**: tăng tốc độ truyền dữ liệu nhưng có thể gây hỏng dữ liệu vì máy chủ NFS không đợi cho đến khi toàn bộ hoạt động ghi trên bộ lưu trữ ổn định hoàn tất trước khi trả lời máy khách

- **sync**: Thực hiện ngược lại với tùy chọn không đồng bộ, máy chủ NFS sẽ chỉ trả lời máy khách sau khi dữ liệu cuối cùng được ghi vào bộ lưu trữ ổn định

+ Lab:

Tạo thư mục chia sẻ nfs:

A screen shot of a computer screen

Description automatically generated

Tạo thư mục raj trong thư mục /tmp, gán thư mục chia sẻ /home vào /tmp/raj

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Sử dụng Bash file

- Sử dụng C program

File asroot.c:

A screen shot of a computer

Description automatically generated

Biên dịch thành file shell:

A screenshot of a computer

Description automatically generated

Cấp SUID cho file shell:

A screenshot of a computer program

Description automatically generated

Tại thư mục bên user1

A screen shot of a computer

Description automatically generated

Chạy shell:

A blue and white text

Description automatically generated

- Sử dụng Nano/vi

+ Chỉnh sửa file passwd (tương tự với file sudoers)

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated







A screen shot of a computer

Description automatically generated

1. LD\_Preload

+ Shared Libraries:

- Là thư viện được chương trình tải khi khởi động.

- Khi thư viện chia sẻ được cài đặt đúng cách, tất cả các chương trình khởi động sau đó sẽ tự động sử dụng thư viện chia sẻ mới

+ Shared Libraries Names:

- Mỗi thư viện chia sẻ đều có một tên gọi đặc biệt gọi là “soname”

- Soname có tiền tố “lib”, tên của thư viện, cụm “.so”, theo sau là dấu chấm và phiên bản

+ LD\_Preload:

- Là biến môi trường liệt kê các thư viện chia sẻ với các hàm ghi đè lên bộ chuẩn, giống như /etc/ld.so.preload. Những hàm này được triển khai bởi trình tải /lib/ld-linux.so

+ Lab:

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

A computer screen shot of a program code

Description automatically generated

1. Using PATH Variable

A screenshot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

1. Using Zip

A screen shot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a computer program

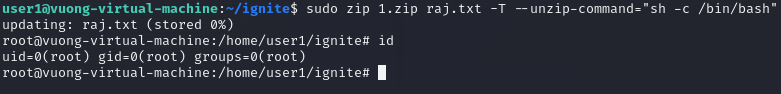
Description automatically generated

A computer screen with text on it

Description automatically generated

A screen shot of a computer

Description automatically generated



1. Ádasd
2. Ádasd
3. Ádasd
4. Ádasd
5. Ádasd
6. Ádasd
7. Ádasd