

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



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484**

**NHÓM LỚP: 01
TÊN BÀI:
HẠN CHẾ TRUY CẬP SSH BẰNG CÔNG CỤ DENYHOST**

Sinh viên thực hiện:
B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

<i>MỤC LỤC</i>	2
<i>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</i>	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
<i>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</i>	6
2.2.1 Xem các tệp cấu hình	6
2.2.2 Khóa một người dùng hợp lệ bằng cách sử dụng một bot.....	8
2.2.3 Khôi phục khả năng đăng nhập của người dùng hợp lệ.....	9
2.2.4 Khóa người dùng không hợp lệ	11
<i>TÀI LIỆU THAM KHẢO</i>	13

DANH MỤC HÌNH ẢNH

Hình ảnh 1 : <code>sudo tail -f /var/log/auth.log</code>	6
<u>Hình ảnh 2: <code>ssh hank@172.20.0.3</code></u>	6
Hình ảnh 3: <code>ssh hank@172.20.0.3</code>	7
Hình ảnh 4: <code>sudo less /etc/denyhosts.conf</code>	7
Hình ảnh 5: <code>cat /etc/hosts.deny</code>	8
Hình ảnh 6: <code>sudo tail -f /var/log/auth.log</code>	8
Hình ảnh 7: <code>./bot.py hank</code>	9
Hình ảnh 8: <code>sudo cat /etc/hosts.deny</code>	9
Hình ảnh 9: <code>sudo nano /etc/hosts.allow</code>	10
Hình ảnh 10: <code>sudo iptables -L -n</code>	10
Hình ảnh 11: <code>sudo iptables -D INPUT -s 172.20.0.2 -j DROP</code>	10
Hình ảnh 12: <code>ssh hank@172.20.0.3</code>	10
Hình ảnh 13: <code>sudo ifconfig eth0 172.20.0.9</code>	11
Hình ảnh 14: <code>./bot.py tony</code>	11
TÀI LIỆU THAM KHẢO	13

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Mục đích của bài thực hành: Khám phá việc sử dụng tiện ích denyhosts trên một máy chủ SSH để giới hạn số lần đăng nhập SSH từ một địa chỉ IP.

1.2 Tìm hiểu lý thuyết

DenyHosts là một phần mềm mã nguồn mở được viết bằng Python, dùng để tăng cường bảo mật cho dịch vụ SSH trên hệ điều hành Linux/Unix. Công cụ này có chức năng chính là ngăn chặn các cuộc tấn công brute-force vào dịch vụ SSH thông qua việc theo dõi các đăng nhập không thành công và tự động chặn các địa chỉ IP có hành vi đáng ngờ.

1.2.1 Mục đích và Nguyên lý hoạt động:

Mục đích: DenyHosts được thiết kế để theo dõi các nỗ lực đăng nhập SSH không thành công và chặn các địa chỉ IP có hành vi đáng ngờ.

Nguyên lý:

- DenyHosts phân tích các tệp nhật ký SSH (thường là /var/log/auth.log hoặc /var/log/secure) để tìm kiếm các nỗ lực đăng nhập không thành công.
- Khi phát hiện một số lượng nỗ lực đăng nhập không thành công từ một địa chỉ IP cụ thể vượt quá một ngưỡng nhất định, DenyHosts sẽ chặn địa chỉ IP đó bằng cách thêm nó vào tệp /etc/hosts.deny.
- Tệp /etc/hosts.deny được sử dụng bởi TCP Wrappers, một hệ thống kiểm soát truy cập dựa trên máy chủ, để từ chối các kết nối đến các dịch vụ mạng.

1.2.2 Các thành phần chính

1. Tệp cấu hình (/etc/denyhosts.conf): Tệp này chứa các cài đặt cấu hình cho DenyHosts, bao gồm:

- SECURE_LOG: Đường dẫn đến tệp nhật ký SSH
- HOSTS_DENY: Đường dẫn đến tệp /etc/hosts.deny
- BLOCK_SERVICE: Dịch vụ cần chặn (thường là sshd)
- DENY_THRESHOLD_INVALID: Số lần đăng nhập không thành công với tên người dùng không hợp lệ trước khi chặn IP.
- DENY_THRESHOLD_VALID: Số lần đăng nhập không thành công với người dùng hợp lệ trước khi chặn IP.
- DENY_THRESHOLD_ROOT: Số lần đăng nhập không thành công với người dùng root trước khi chặn IP.

- MAX_DENY_FROM: Thời gian (tính bằng giây) mà một địa chỉ IP bị chặn.

2. Tập nhật ký SSH: Tập này ghi lại các hoạt động đăng nhập SSH, bao gồm các nỗ lực đăng nhập thành công và không thành công.

3. Tập */etc/hosts.deny*: Tập này chứa danh sách các địa chỉ IP bị chặn.

1.2.3 Ưu điểm của DenyHosts

- Tự động hóa: DenyHosts tự động theo dõi và chặn các địa chỉ IP có hành vi đáng ngờ, giảm thiểu công việc thủ công của quản trị viên hệ thống.
- Hiệu quả: DenyHosts có thể chặn các cuộc tấn công brute-force một cách hiệu quả, giúp bảo vệ máy chủ SSH khỏi các truy cập trái phép.
- Dễ sử dụng: DenyHosts tương đối dễ cài đặt và cấu hình.

1.2.4 Hạn chế:

- Chỉ bảo vệ SSH: DenyHosts chỉ bảo vệ dịch vụ SSH và không bảo vệ các dịch vụ mạng khác.
- Có thể chặn nhầm: Trong một số trường hợp, DenyHosts có thể chặn nhầm các địa chỉ IP hợp lệ.
- Không còn được duy trì: DenyHosts đã không còn được duy trì và phát triển. Vì vậy hiện nay các quản trị viên hệ thống có xu hướng sử dụng Fail2ban nhiều hơn. Fail2ban cũng là công cụ tương tự DenyHosts.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

- Khởi động lab:

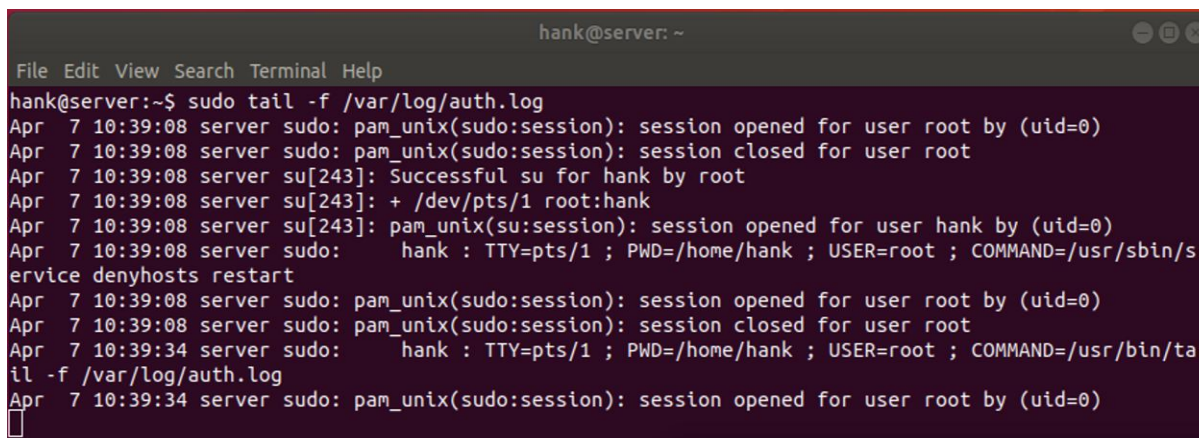
labtainer -r denyhost

- Các nhiệm vụ

2.2.1 Xem các tệp cấu hình

Theo dõi tệp `/var/log/auth.log`

1. Trên máy chủ (server terminal): *sudo tail -f /var/log/auth.log*

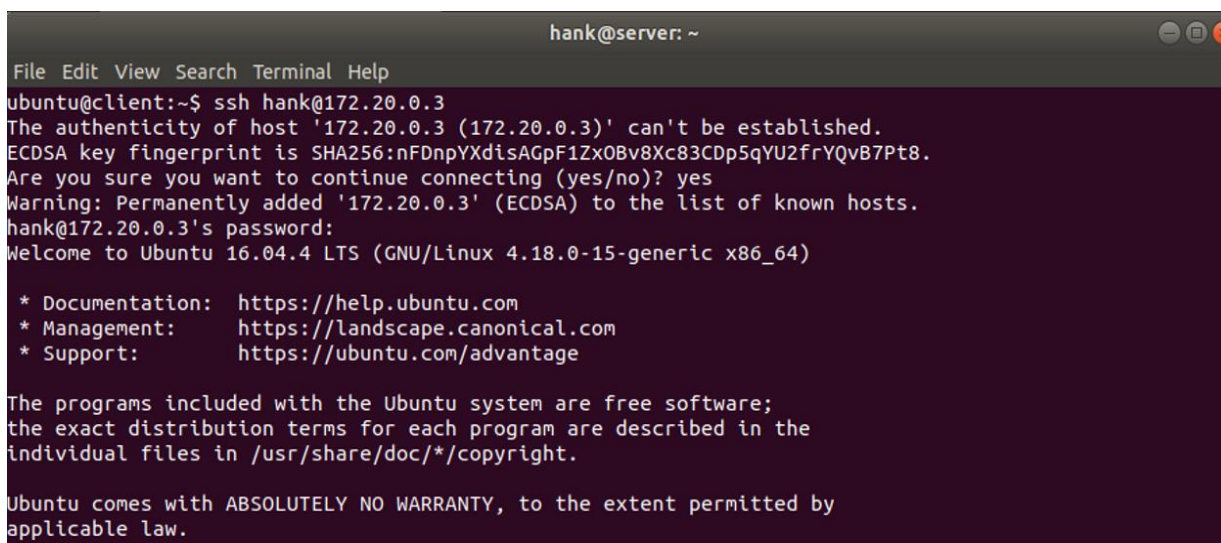


```
hank@server: ~  
File Edit View Search Terminal Help  
hank@server:~$ sudo tail -f /var/log/auth.log  
Apr  7 10:39:08 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)  
Apr  7 10:39:08 server sudo: pam_unix(sudo:session): session closed for user root  
Apr  7 10:39:08 server su[243]: Successful su for hank by root  
Apr  7 10:39:08 server su[243]: + /dev/pts/1 root:hank  
Apr  7 10:39:08 server su[243]: pam_unix(su:session): session opened for user hank by (uid=0)  
Apr  7 10:39:08 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart  
Apr  7 10:39:08 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)  
Apr  7 10:39:08 server sudo: pam_unix(sudo:session): session closed for user root  
Apr  7 10:39:34 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log  
Apr  7 10:39:34 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
```

Hình ảnh 1 : *sudo tail -f /var/log/auth.log*

SSH từ máy khách vào máy chủ

1. Trên máy khách (client terminal): *ssh [hank@172.20.0.3](#)*
2. Nhập mật khẩu: hank21



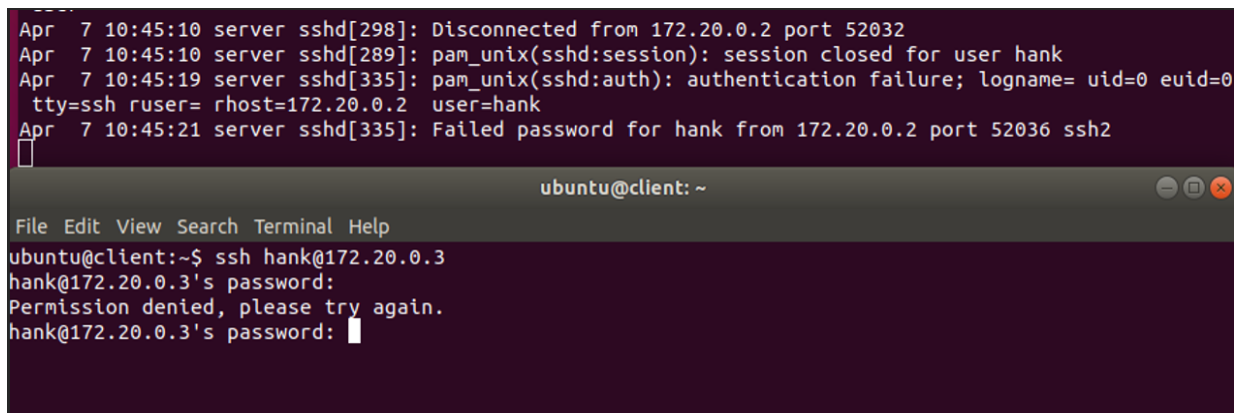
```
hank@server: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ ssh hank@172.20.0.3  
The authenticity of host '172.20.0.3 (172.20.0.3)' can't be established.  
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1Zx0Bv8Xc83CDp5qYU2frYQvB7Pt8.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '172.20.0.3' (ECDSA) to the list of known hosts.  
hank@172.20.0.3's password:  
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.18.0-15-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.
```

Hình ảnh 2: *ssh [hank@172.20.0.3](#)*

SSH lại và nhập sai mật khẩu

```
Apr  7 10:45:10 server sshd[298]: Disconnected from 172.20.0.2 port 52032
Apr  7 10:45:10 server sshd[289]: pam_unix(sshd:session): session closed for user hank
Apr  7 10:45:19 server sshd[335]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 10:45:21 server sshd[335]: Failed password for hank from 172.20.0.2 port 52036 ssh2

```

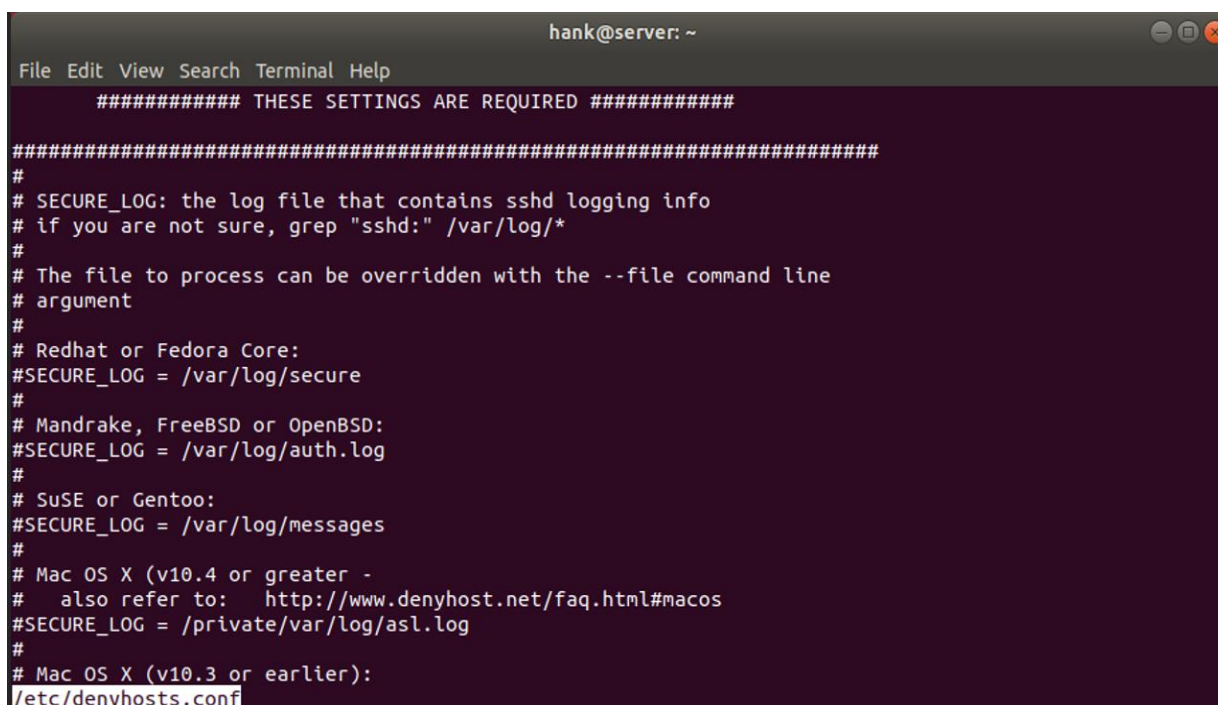


The image shows two terminal windows. The top window displays system logs for an SSH server, showing a disconnection, session closure, and an authentication failure for user 'hank' from IP 172.20.0.2. The bottom window is a terminal titled 'ubuntu@client: ~' showing a user attempting to SSH into 'hank@172.20.0.3'. The password prompt is shown, followed by 'Permission denied, please try again.' and another password prompt.

Hình ảnh 3: *ssh hank@172.20.0.3*

Xem nội dung cấu hình denyhosts

Trên máy chủ, chạy: *sudo less /etc/denyhosts.conf*



The image shows a terminal window titled 'hank@server: ~' displaying the contents of the file `/etc/denyhosts.conf` using the `less` command. The file contains configuration settings for the denyhosts package, including comments and the `SECURE_LOG` variable set to `/var/log/secure`.

Hình ảnh 4: *sudo less /etc/denyhosts.conf*

Kiểm tra nội dung `/etc/hosts.deny`

1. Trên máy chủ: *cat /etc/hosts.deny*


```
hank@server: ~  
File Edit View Search Terminal Help  
hank@server:~$ sudo less /etc/denyhosts.conf  
hank@server:~$ cat /etc/hosts.deny  
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.  
# See the manual pages hosts_access(5) and hosts_options(5).  
#  
# Example: ALL: some.host.name, .some.domain  
# ALL EXCEPT in.fingerd: other.host.name, .other.domain  
#  
# If you're going to protect the portmapper use the name "rpcbind" for the  
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.  
#  
# The PARANOID wildcard matches any host whose name does not match its  
# address.  
#  
# You may wish to enable this to ensure any programs that don't  
# validate looked up hostnames still leave understandable logs. In past  
# versions of Debian this has been the default.  
# ALL: PARANOID
```

Hình ảnh 5: `cat /etc/hosts.deny`

- Khi denyhosts phát hiện quá ngưỡng đăng nhập sai, nó sẽ tự động thêm dòng như: `sshd: 172.20.0.2`

2.2.2 Khóa một người dùng hợp lệ bằng cách sử dụng một bot

Trên máy chủ – theo dõi log

`sudo tail -f /var/log/auth.log`

```
hank@server: ~  
File Edit View Search Terminal Help  
hank@server:~$ sudo tail -f /var/log/auth.log  
Apr  7 10:45:21 server sshd[335]: Failed password for hank from 172.20.0.2 port 52036 ssh2  
Apr  7 10:46:39 server sshd[335]: Failed password for hank from 172.20.0.2 port 52036 ssh2  
Apr  7 10:46:46 server sshd[335]: Connection closed by 172.20.0.2 port 52036 [preauth]  
Apr  7 10:46:46 server sshd[335]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh r  
user= rhost=172.20.0.2 user=hank  
Apr  7 10:47:06 server sudo: pam_unix(sudo:session): session closed for user root  
Apr  7 10:47:11 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/le  
ss /etc/denyhosts.conf  
Apr  7 10:47:11 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)  
Apr  7 10:48:37 server sudo: pam_unix(sudo:session): session closed for user root  
Apr  7 10:56:33 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/ta  
il -f /var/log/auth.log  
Apr  7 10:56:33 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
```

Hình ảnh 6: `sudo tail -f /var/log/auth.log`

Trên máy khách chạy : `./bot.py hank`


```
Apr 7 10:57:14 server sshd[469]: Connection closed by 172.20.0.2 port 52054 [preauth]
Apr 7 10:57:14 server sshd[471]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr 7 10:57:16 server sshd[471]: Failed password for hank from 172.20.0.2 port 52056 ssh2
Apr 7 10:57:16 server sshd[471]: Connection closed by 172.20.0.2 port 52056 [preauth]
Apr 7 10:57:16 server sshd[473]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr 7 10:57:18 server sshd[473]: Failed password for hank from 172.20.0.2 port 52058 ssh2
Apr 7 10:57:18 server sshd[473]: Connection closed by 172.20.0.2 port 52058 [preauth]
Apr 7 10:57:18 server sshd[475]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr 7 10:57:19 server sshd[475]: Failed password for hank from 172.20.0.2 port 52060 ssh2

ubuntu@client: ~
File Edit View Search Terminal Help
ubuntu@client:~$ cd ~
ubuntu@client:~$ ./bot.py hank

try user: hank passwd: hank1 -- permission denied, count=1
try user: hank passwd: hank2 -- permission denied, count=2
try user: hank passwd: hank3 -- permission denied, count=3
try user: hank passwd: hank4 -- permission denied, count=4
try user: hank passwd: hank5 -- permission denied, count=5
try user: hank passwd: hank6 -- permission denied, count=6
try user: hank passwd: hank7 -- permission denied, count=7
try user: hank passwd: hank8 -- permission denied, count=8
try user: hank passwd: hank9 -- permission denied, count=9
```

Hình ảnh 7: `./bot.py hank`

- Bot sẽ thử lần lượt các mật khẩu: hank1, hank2, hank3,...
- Bot sẽ dừng lại vì IP đã bị chặn — kiểm tra lại `/etc/hosts.deny`.

2.2.3 Khôi phục khả năng đăng nhập của người dùng hợp lệ

Kiểm tra `/etc/hosts.deny`

Trên máy chủ chạy : `sudo cat /etc/hosts.deny`

```
hank@server: ~
File Edit View Search Terminal Help
hank@server:~$ sudo cat /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

sshd: 172.20.0.2
```

Hình ảnh 8: `sudo cat /etc/hosts.deny`

Thêm IP vào whitelist

`sudo nano /etc/hosts.allow`

Thêm dòng: `ALL: 172.20.0.2`

```
hank@server: ~
File Edit View Search Terminal Help
GNU nano 2.5.3 File: /etc/hosts.allow

ALL: 172.20.0.2
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: LOCAL @some_netgroup
# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
```

Hình ảnh 9: `sudo nano /etc/hosts.allow`

Kiểm tra iptables

`sudo iptables -L -n`

```
hank@server: ~
File Edit View Search Terminal Help
hank@server:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP all -- 172.20.0.2 0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Hình ảnh 10: `sudo iptables -L -n`

Xóa bằng `sudo iptables -D INPUT -s 172.20.0.2 -j DROP`

```
hank@server: ~
File Edit View Search Terminal Help
hank@server:~$ sudo iptables -D INPUT -s 172.20.0.2 -j DROP
hank@server:~$
```

Hình ảnh 11: `sudo iptables -D INPUT -s 172.20.0.2 -j DROP`

Thử SSH lại từ máy khách

`ssh hank@172.20.0.3`

```
hank@server: ~
File Edit View Search Terminal Help
ubuntu@client:~$ ssh hank@172.20.0.3
hank@172.20.0.3's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.18.0-15-generic x86_64)

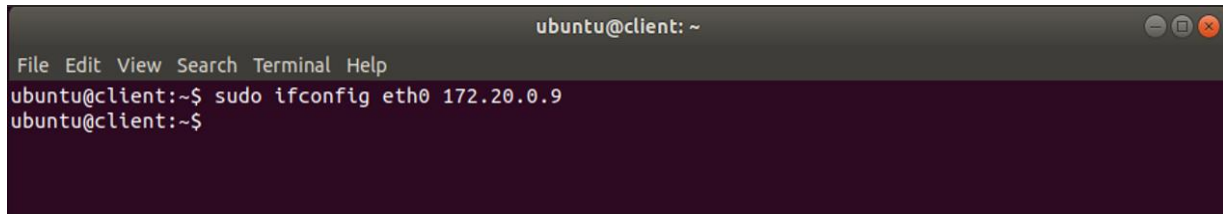
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Mon Apr  7 10:43:54 2025 from 172.20.0.2
hank@server:~$
```

Hình ảnh 12: `ssh hank@172.20.0.3`

- Đăng nhập thành công lại.

2.1.4 Khóa người dùng không hợp lệ

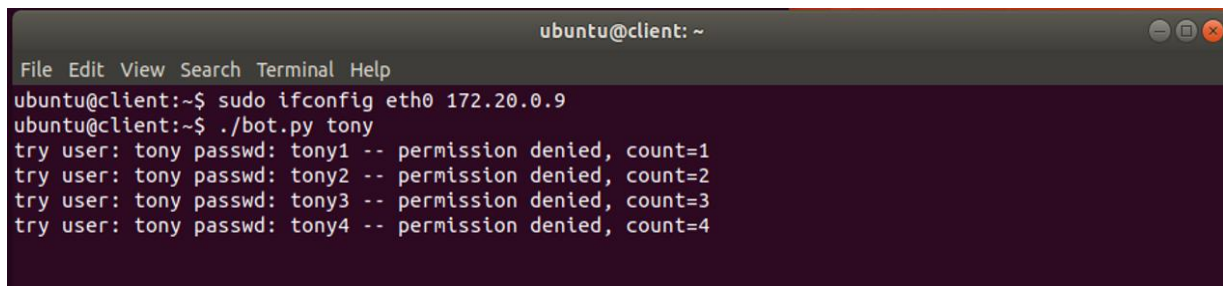
- Đổi địa chỉ IP máy khách



```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ sudo ifconfig eth0 172.20.0.9  
ubuntu@client:~$
```

Hình ảnh 13: `sudo ifconfig eth0 172.20.0.9`

- Chạy bot với user không hợp lệ



```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ sudo ifconfig eth0 172.20.0.9  
ubuntu@client:~$ ./bot.py tony  
try user: tony passwd: tony1 -- permission denied, count=1  
try user: tony passwd: tony2 -- permission denied, count=2  
try user: tony passwd: tony3 -- permission denied, count=3  
try user: tony passwd: tony4 -- permission denied, count=4
```

Hình ảnh 14: `./bot.py tony`

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab denyhosts

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 denyhosts

CHƯƠNG 3: KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/denyhost
Labname denyhost
```

Student	deny_valid	deny_invalid	hank_login	hosts_allow
B22DCAT176	11	4	2	Y

What is automatically assessed for this lab:

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.