

**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**

**CA THỰC HÀNH: 01
NHÓM LỚP: INT1484-02
TÊN BÀI: DENYHOST – HẠN CHẾ TRUY CẬP SSH BẰNG
CÔNG CỤ DENYHOST**

Sinh viên thực hiện:

B22DCAT063 Lê Tiến Dương

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết	5
1.2.1 Mục đích và nguyên lý hoạt động	5
1.2.2 Các thành phần chính	5
1.2.3 Ưu điểm của DenyHosts	6
1.2.4 Hạn chế của DenyHosts	6
1.2.5 Các lưu ý về bảo mật SSH	6
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	7
2.1 Chuẩn bị môi trường	7
2.2 Các bước thực hiện.....	7
2.2.1 Khởi động lab	7
2.2.2 Các nhiệm vụ.....	7
2.2.3 Kết thúc lab	14
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH	15
TÀI LIỆU THAM KHẢO	16

DANH MỤC CÁC HÌNH VẼ

Hình 1 – Khởi động bài lab	7
Hình 2 – Theo dõi tệp auth.log.....	8
Hình 3 – SSH vào 172.20.0.3.....	8
Hình 4 – Quan sát tệp /var/log/auth.log	8
Hình 5 – SSH lại vào 172.20.0.3.....	9
Hình 6 – Quan sát các sự kiện trong auth.log	9
Hình 7 – Xem nội dung /etc/denysthosts.conf	9
Hình 8 – Kiểm tra file /var/log/auth.log.....	10
Hình 9 – Vào máy chủ và chạy lệnh	10
Hình 10 – Kiểm tra địa chỉ ip.....	11
Hình 11 – Khởi chạy bot	11
Hình 12 – Quan sát kết quả	12
Hình 13 – Xem tác động của DAEMON_SLEEP.....	12
Hình 14 – Xem tệp /etc/hosts.deny	13
Hình 15 – Thêm mục nhập vào tệp /etc/hosts.allow	13
Hình 16 – Kiểm tra địa chỉ bị chặn	13
Hình 17 – Xóa khỏi chặn.....	14
Hình 18 – SSH từ máy khách.....	14
Hình 19 – Thay đổi địa chỉ IP máy khách.....	14
Hình 20 – Thử lại bot.py	14
Hình 21 – Kết quả checkwork.....	15

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SSH	Secure Shell	Giao thức bảo mật

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

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 công cụ bảo mật mã nguồn mở được sử dụng để ngăn chặn các cuộc tấn công brute-force vào máy chủ SSH (Secure Shell). Dưới đây là lý thuyết cơ bản về cách DenyHosts hoạt động:

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

- **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 tên 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.
- **Tệp nhật ký SSH:** Tệp này ghi lại các hoạt động đăng nhập SSH, bao gồm cả các nỗ lực đăng nhập thành công và không thành công.
- **Tệp `/etc/hosts.deny`:** Tệp 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 của DenyHosts

- 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.

1.2.5 Các lưu ý về bảo mật SSH

- Sử dụng mật khẩu mạnh: Mật khẩu mạnh là một yếu tố bảo mật cơ bản.
- Sử dụng khóa SSH: Xác thực khóa SSH an toàn hơn xác thực mật khẩu.
- Thay đổi cổng SSH mặc định: Thay đổi cổng SSH mặc định có thể giảm thiểu nguy cơ bị tấn công tự động.
- Cập nhật phần mềm SSH: Luôn cập nhật phần mềm SSH lên phiên bản mới nhất để vá các lỗ hổng bảo mật.
- Sử dụng Fail2ban: Fail2ban là một công cụ bảo mật mạnh mẽ hơn DenyHosts và được duy trì tích cực.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

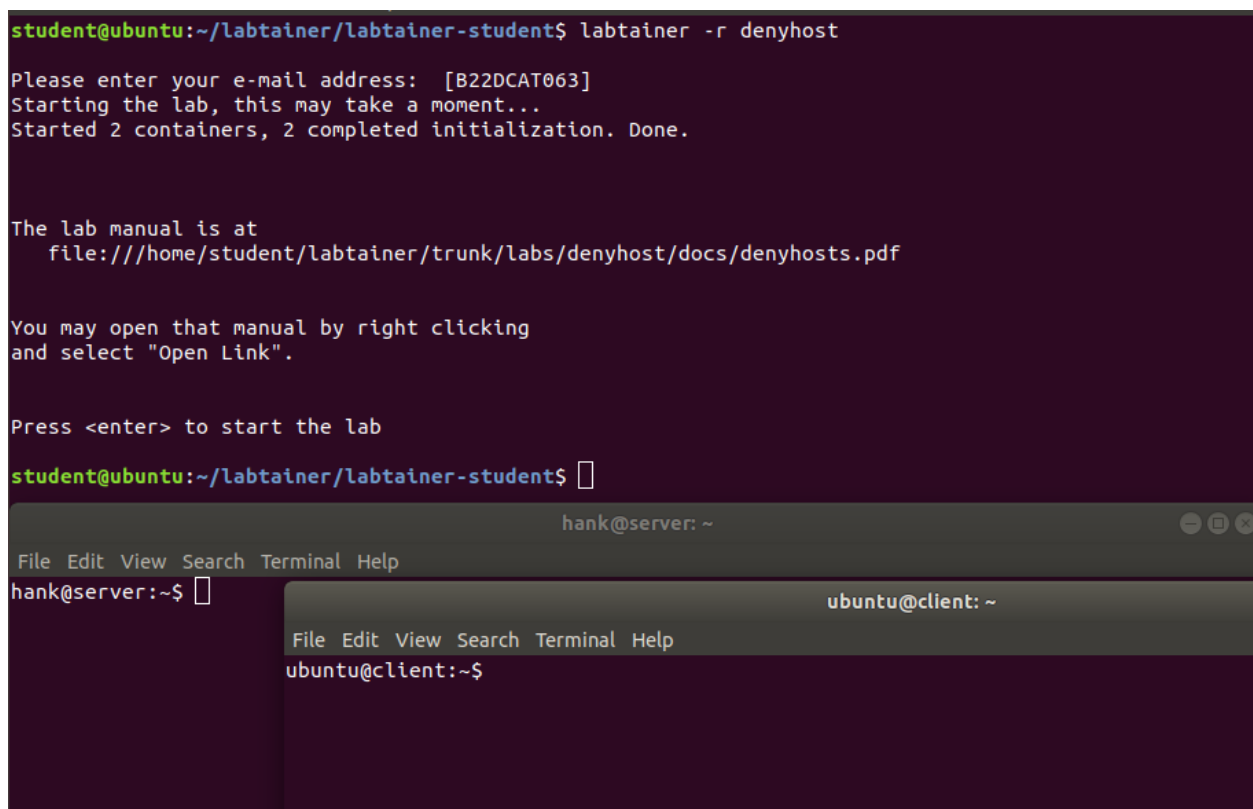
- Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
- Máy trạm chạy hệ điều hành linux: đã cài đặt labtainer.

2.2 Các bước thực hiện

2.2.1 Khởi động lab

labtainer -r denyhost

Các cửa sổ terminal kết quả bao gồm hiển thị các hướng dẫn này, một terminal kết nối với một máy khách và một terminal kết nối với một máy chủ SSH.



```
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r denyhost
Please enter your e-mail address: [B22DCAT063]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.

The lab manual is at
  file:///home/student/labtainer/trunk/labs/denyhost/docs/denyhosts.pdf

You may open that manual by right clicking
and select "Open Link".

Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$

hank@server: ~
File Edit View Search Terminal Help
hank@server:~$

ubuntu@client: ~
File Edit View Search Terminal Help
ubuntu@client:~$
```

Hình 1 – Khởi động bài lab

2.2.2 Các nhiệm vụ

2.2.2.1 Nhiệm vụ 1: Xem các tệp cấu hình

Chúng ta sẽ xem xét ba tệp quan trọng liên quan đến tiện ích denyhosts.

Tệp quan trọng #1: auth.log

Tệp /var/log/auth.log phản ánh kết quả của các lần đăng nhập thành công. Theo dõi tệp đó bằng cách sử dụng lệnh:

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 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr 7 19:36:38 server su[237]: Successful su for hank by root
Apr 7 19:36:38 server su[237]: + /dev/pts/1 root:hank
Apr 7 19:36:38 server su[237]: pam_unix(su:session): session opened for user hank by (uid=0)
Apr 7 19:36:38 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr 7 19:37:47 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Apr 7 19:37:47 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
```

Hình 2 – Theo dõi tệp auth.log

Sau đó, ssh vào 172.20.0.3 với tài khoản "hank" và mật khẩu là hank21

Lưu ý: Khi hệ thống hiển thị "Bạn có chắc chắn muốn tiếp tục kết nối (yes/no)?", nhập "yes".

```
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.

hank@server:~$
```

Hình 3 – SSH vào 172.20.0.3

Quan sát điều gì xảy ra trong tệp /var/log/auth.log

```
hank@server:~$ sudo tail -f /var/log/auth.log
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr 7 19:36:38 server su[237]: Successful su for hank by root
Apr 7 19:36:38 server su[237]: + /dev/pts/1 root:hank
Apr 7 19:36:38 server su[237]: pam_unix(su:session): session opened for user hank by (uid=0)
Apr 7 19:36:38 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr 7 19:37:47 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Apr 7 19:37:47 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 7 19:38:38 server sshd[283]: Accepted password for hank from 172.20.0.2 port 42276 ssh2
Apr 7 19:38:38 server sshd[283]: pam_unix(sshd:session): session opened for user hank by (uid=0)
Apr 7 19:38:38 server sudo: hank : TTY=pts/2 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart
Apr 7 19:38:38 server sudo: pam_unix(sudo:session): session opened for user root by hank(uid=0)
Apr 7 19:38:38 server sudo: pam_unix(sudo:session): session closed for user root
```

Hình 4 – Quan sát tệp /var/log/auth.log

Sau đó, thoát và ssh lại vào 172.20.0.3, nhưng lần này nhập mật khẩu không chính xác. Quan sát kết quả trong tệp /var/log/auth.log.

Tiện ích denyhosts quan sát các sự kiện trong auth.log để phát hiện các lần đăng nhập không thành công.

```
ubuntu@client:~$ ssh hank@172.20.0.3
hank@172.20.0.3's password:
Permission denied, please try again.
hank@172.20.0.3's password: █
```

Hình 5 – SSH lại vào 172.20.0.3

```
hank@server:~$ sudo tail -f /var/log/auth.log
Apr  7 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr  7 19:36:38 server su[237]: Successful su for hank by root
Apr  7 19:36:38 server su[237]: + /dev/pts/1 root:hank
Apr  7 19:36:38 server su[237]: pam_unix(su:session): session opened for user hank by (uid=0)
Apr  7 19:36:38 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart
Apr  7 19:36:38 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:36:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr  7 19:37:47 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Apr  7 19:37:47 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:38:38 server sshd[283]: Accepted password for hank from 172.20.0.2 port 42276 ssh2
Apr  7 19:38:38 server sshd[283]: pam_unix(sshd:session): session opened for user hank by (uid=0)
Apr  7 19:38:38 server sudo: hank : TTY=pts/2 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/sbin/service denyhosts restart
Apr  7 19:38:38 server sudo: pam_unix(sudo:session): session opened for user root by hank(uid=0)
Apr  7 19:38:38 server sudo: pam_unix(sudo:session): session closed for user root
Apr  7 19:39:12 server sshd[292]: Received disconnect from 172.20.0.2 port 42276:11: disconnected by user
Apr  7 19:39:12 server sshd[292]: Disconnected from 172.20.0.2 port 42276
Apr  7 19:39:12 server sshd[283]: pam_unix(sshd:session): session closed for user hank
Apr  7 19:39:18 server sshd[329]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:39:20 server sshd[329]: Failed password for hank from 172.20.0.2 port 42278 ssh2
```

Hình 6 – Quan sát các sự kiện trong auth.log

Tệp quan trọng #2: denyhosts.conf

Xem nội dung của /etc/denyhosts.conf:

```
sudo less /etc/denyhosts.conf
```

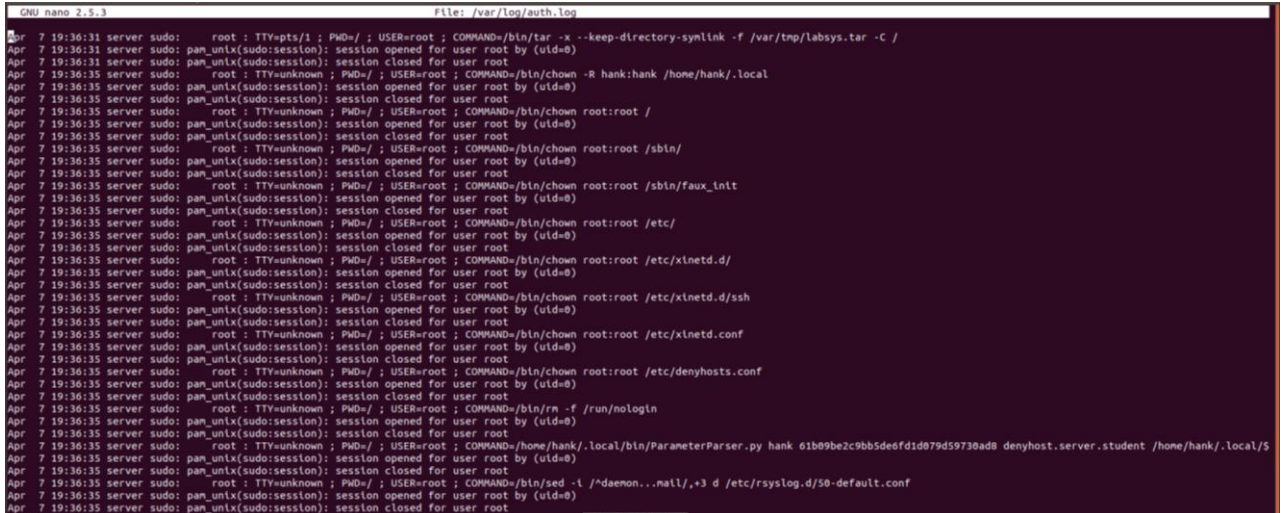
Lưu ý đặc biệt mô tả và giá trị cho "DENY_THRESHOLD_INVALID và DENY_THRESHOLD_VALID".

```
##### THESE SETTINGS ARE REQUIRED #####
#####
#
# SECURE_LOG: the log file that contains sshd logging info
# if you are not sure, grep "sshd:" /var/log/*
#
# The file to process can be overridden with the --file command line
# argument
#
# Redhat or Fedora Core:
#SECURE_LOG = /var/log/secure
#
# Mandrake, FreeBSD or OpenBSD:
#SECURE_LOG = /var/log/auth.log
#
# SuSE or Gentoo:
#SECURE_LOG = /var/log/messages
#
# Mac OS X (v10.4 or greater -
# also refer to: http://www.denyhost.net/faq.html#macos
#SECURE_LOG = /private/var/log/asl.log
#
# Mac OS X (v10.3 or earlier):
#SECURE_LOG=/private/var/log/system.log
#
# Debian and Ubuntu
#SECURE_LOG = /var/log/auth.log
#####
#####
#
# HOSTS_DENY: the file which contains restricted host access information
#
# Host operating systems:
#HOSTS_DENY = /etc/hosts.deny
#
# Some BSD (FreeBSD) Unixes:
#HOSTS_DENY = /etc/hosts.allow
#
# Another possibility (also see the next option):
#HOSTS_DENY = /etc/hosts.evil
#####
/etc/denyhosts.conf
```

Hình 7 – Xem nội dung /etc/denyhosts.conf

Tệp quan trọng #3: *hosts.deny*

Tệp hệ thống này được sử dụng bởi các chức năng mạng để chặn kết nối từ các địa chỉ IP được chọn. Một mục nhập trong tệp này sẽ chặn kết nối trước khi nó đến được dịch vụ đích. Do đó, tiến trình SSH sẽ không nhìn thấy các nỗ lực kết nối từ các nguồn này, giúp tránh tình trạng tiêu thụ tài nguyên hệ thống. Tiện ích denyhosts thêm các mục nhập vào tệp này khi số lần đăng nhập không thành công ghi lại trong `/var/log/auth.log` vượt quá ngưỡng được xác định trong `/etc/denyhosts.conf`.

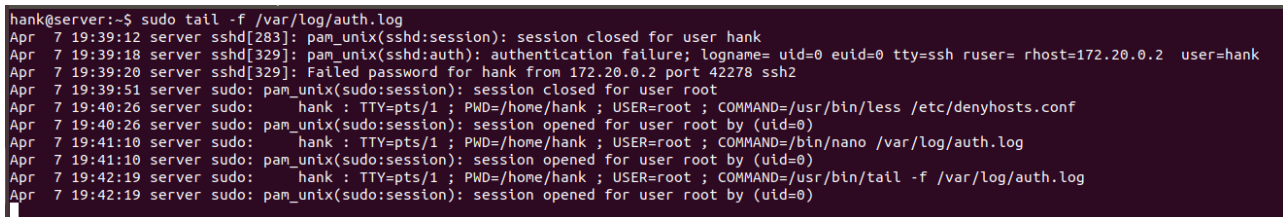


Hình 8 – Kiểm tra file `/var/log/auth.log`

2.2.2.2 Nhiệm vụ 2: Khóa một người dùng hợp lệ bằng cách sử dụng một bot

Chương trình bot.py trong thư mục home của máy khách là một bot thử đăng nhập SSH bằng cách lặp lại các mật khẩu đơn giản dựa trên ID người dùng. Ví dụ, nếu cho một ID người dùng là "hank", nó sẽ thử các mật khẩu như: hank1, hank2, hank3, và cứ tiếp tục cho đến khi tìm được mật khẩu chính xác. Trước khi bạn bắt đầu chạy bot, hãy vào máy chủ và chạy lệnh:

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



Hình 9 – Vào máy chủ và chạy lệnh

Trên máy khách, ghi lại địa chỉ IP của bạn:

`ifconfig`

```
ubuntu@client: ~  
File Edit View Search Terminal Help  
ubuntu@client:~$ ls  
bot.py  
ubuntu@client:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:02  
          inet addr:172.20.0.2  Bcast:172.20.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:115 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:59 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:16399 (16.3 KB)  TX bytes:7896 (7.8 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
ubuntu@client:~$
```

Hình 10 – Kiểm tra địa chỉ ip

Sau đó, khởi chạy bot, cung cấp người dùng "hank".

./bot.py hank

```
ubuntu@client: ~  
File Edit View Search Terminal Help  
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  
try user: hank passwd: hank10 -- permission denied, count=10  
try user: hank passwd: hank11 -- permission denied, count=11
```

Hình 11 – Khởi chạy bot

Quan sát kết quả, chương trình sẽ dường như treo lại sau khi vượt quá ngưỡng đăng nhập không hợp lệ.

```

Apr  7 19:39:12 server sshd[283]: pam_unix(sshd:session): session closed for user hank
Apr  7 19:39:18 server sshd[329]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:39:20 server sshd[329]: Failed password for hank from 172.20.0.2 port 42278 ssh2
Apr  7 19:39:51 server sudo: pam_unix(sudo:session): session closed for user root
Apr  7 19:40:26 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/less /etc/denyhosts.conf
Apr  7 19:40:26 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:41:10 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/bin/nano /var/log/auth.log
Apr  7 19:41:10 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:42:19 server sudo: hank : TTY=pts/1 ; PWD=/home/hank ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Apr  7 19:42:19 server sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr  7 19:44:13 server sshd[436]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:14 server sshd[436]: Failed password for hank from 172.20.0.2 port 42282 ssh2
Apr  7 19:44:14 server sshd[436]: Connection closed by 172.20.0.2 port 42282 [preauth]
Apr  7 19:44:17 server sshd[438]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:17 server sshd[438]: Failed password for hank from 172.20.0.2 port 42284 ssh2
Apr  7 19:44:17 server sshd[438]: Connection closed by 172.20.0.2 port 42284 [preauth]
Apr  7 19:44:17 server sshd[440]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:19 server sshd[440]: Failed password for hank from 172.20.0.2 port 42286 ssh2
Apr  7 19:44:19 server sshd[440]: Connection closed by 172.20.0.2 port 42286 [preauth]
Apr  7 19:44:19 server sshd[442]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:21 server sshd[442]: Failed password for hank from 172.20.0.2 port 42288 ssh2
Apr  7 19:44:21 server sshd[442]: Connection closed by 172.20.0.2 port 42288 [preauth]
Apr  7 19:44:21 server sshd[444]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:24 server sshd[444]: Failed password for hank from 172.20.0.2 port 42290 ssh2
Apr  7 19:44:24 server sshd[444]: Connection closed by 172.20.0.2 port 42290 [preauth]
Apr  7 19:44:24 server sshd[446]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:26 server sshd[446]: Failed password for hank from 172.20.0.2 port 42292 ssh2
Apr  7 19:44:26 server sshd[446]: Connection closed by 172.20.0.2 port 42292 [preauth]
Apr  7 19:44:28 server sshd[448]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:28 server sshd[448]: Connection closed by 172.20.0.2 port 42294 [preauth]
Apr  7 19:44:28 server sshd[450]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:31 server sshd[450]: Failed password for hank from 172.20.0.2 port 42296 ssh2
Apr  7 19:44:31 server sshd[450]: Failed password for hank from 172.20.0.2 port 42296 ssh2
Apr  7 19:44:31 server sshd[450]: Connection reset by 172.20.0.2 port 42296 [preauth]
Apr  7 19:44:31 server sshd[452]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:33 server sshd[452]: Failed password for hank from 172.20.0.2 port 42298 ssh2
Apr  7 19:44:33 server sshd[452]: Connection closed by 172.20.0.2 port 42298 [preauth]
Apr  7 19:44:33 server sshd[454]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:35 server sshd[454]: Failed password for hank from 172.20.0.2 port 42300 ssh2
Apr  7 19:44:35 server sshd[454]: Connection closed by 172.20.0.2 port 42300 [preauth]
Apr  7 19:44:35 server sshd[456]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 19:44:37 server sshd[456]: Failed password for hank from 172.20.0.2 port 42302 ssh2

```

Hình 12 – Quan sát kết quả

Dựa trên việc xem xét địa chỉ IP của máy khách để thêm vào tệp `hosts.deny`, liệu kết nối đã bị từ chối vào thời điểm bạn mong đợi chưa? Nếu chưa, hãy xem xét tác động của giá trị `DAEMON_SLEEP` trong tệp `denyhosts.conf`.

```

#####
#
# DAEMON_SLEEP: when DenyHosts is run in daemon mode (--daemon flag)
# this is the amount of time DenyHosts will sleep between polling
# the SECURE_LOG. See the comments in the PURGE_DENY section (above)
# for details on specifying this value or for complete details
# refer to: http://denyhost.sourceforge.net/faq.html#timespec
#
#
DAEMON_SLEEP = 3s
#
#####

#####
#
# DAEMON_PURGE: How often should DenyHosts, when run in daemon mode,
# run the purge mechanism to expire old entries in HOSTS_DENY
# This has no effect if PURGE_DENY is blank.
#
DAEMON_PURGE = 1h

```

Hình 13 – Xem tác động của `DAEMON_SLEEP`

2.2.2.3 Nhiệm vụ 3: Khôi phục khả năng đăng nhập của người dùng hợp lệ

Xem tệp `/etc/hosts.deny` và ghi nhận mục nhập cho địa chỉ IP của bạn. Điều đó sẽ ngăn ai đó từ địa chỉ IP đó kết nối vào máy chủ SSH.


```
GNU nano 2.5.3 File: /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 14 – Xem tệp */etc/hosts.deny*

Nếu việc đăng nhập không thành công là một sự nhầm lẫn, việc chỉ xóa mục nhập trong tệp */etc/hosts.deny* thường không đủ vì denyhosts lưu giữ các cơ sở dữ liệu bổ sung khác.

Một tùy chọn là "whitelist" máy tính khách bằng cách thêm một mục nhập vào tệp */etc/hosts.allow* trên máy chủ, ví dụ:

ALL: 172.20.0.2

```
GNU nano 2.5.3 File: /etc/hosts.allow Modified

# /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.
#
ALL: 172.20.0.2
```

Hình 15 – Thêm mục nhập vào tệp */etc/hosts.allow*

Địa chỉ IP bị cấm cũng có thể bị chặn bằng cách sử dụng "iptables". Trên máy chủ, bạn có thể kiểm tra xem điều này có xảy ra không bằng cách sử dụng lệnh:

sudo iptables -L -n

```
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
hank@server:~$
```

Hình 16 – Kiểm tra địa chỉ bị chặn

Nếu địa chỉ IP xuất hiện trong kết quả, bạn có thể xóa khỏi chặn bằng cách sử dụng lệnh:

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

```
hank@server:~$ sudo iptables -D INPUT -s 172.20.0.2 -j DROP
hank@server:~$
```

Hình 17 – Xóa khỏi chặn

Sau đó, xác nhận rằng bạn có thể SSH từ máy khách.

```
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 19:38:38 2025 from 172.20.0.2
hank@server:~$
```

Hình 18 – SSH từ máy khách

2.2.2.4 Nhiệm vụ 4: Khóa người dùng không hợp lệ

Trước tiên, thay đổi địa chỉ IP của máy khách để máy khách của chúng ta không còn trong danh sách cho phép whitelist. Trên máy khách:

```
sudo ifconfig eth0 172.20.0.9
```

```
ubuntu@client:~$ sudo ifconfig eth0 172.20.0.9
ubuntu@client:~$
```

Hình 19 – Thay đổi địa chỉ IP máy khách

Sau đó, hãy thử lại bot.py, nhưng lần này cung cấp một người dùng khác, ví dụ:

```
./bot.py tony
```

```
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 20 – Thử lại bot.py

2.2.3 Kết thúc lab

```
stoplab denyhost
```

CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

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

Student | deny_valid | deny_invalid | hank_login | hosts_allow |
===== | ===== | ===== | ===== | ===== |
B22DCAT063 | 9 | 2 | 2 | Y |
What is automatically assessed for this lab:
```

Hình 21 – Kết quả checkwork

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] Wikipedia: <https://en.wikipedia.org/wiki/DenyHosts>
- [3] Devopsedu: <https://devopsedu.vn/10-cach-bao-mat-ssh-tren-linux-thuc-te/>