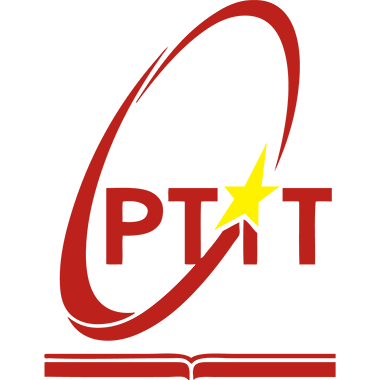
**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**TP.HCM**

****

**Đề tài:**

**TÌM HIỂU DỊCH VỤ FINGER**

**VÀ LỢI DỤNG DỊCH VỤ ĐỂ CÀI SHELLCODE**

**LÊN MÁY NẠN NHÂN**

|  |  |
| --- | --- |
| **GVHD:** | **Nguyễn Hồng Sơn** |
| **SVTH:** | **Phan Văn Tấn** |
|  | **Tạ Hồng Trung** |

***Tp.Hồ Chí Minh, tháng 11, năm 2017***

* [Introduction](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html#SEC1)

* + [Why Another Finger?](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC2)

* [Using Finger](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC3)

* + [Arguments to GNU Finger](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC4)

* + [Command Line Options](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC5)

* + [Special User Names](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC6)

* [Advanced Use](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC7)

* + [How Finger Works](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC8)

* + [The `~/.fingerrc' Script](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC9)

* + [User-defined Targets](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC10)

* + [How Finger Picks a Port](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC11)

* [Security Issues](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC12)

* [Installation](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC14)

* + [Basic Installation](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC15)

* + [Configuration Files](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC16)

* + - [The `clients' file](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC17)

* + - [The `serverhost' file](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC18)

* + - [The `mailhost' file](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC19)

* + - [The `forwardhost' file](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC20)

* + - [The `ttylocs' file](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC21)

* + [Site Specific Functions](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC22)

* + [Configuration Options](https://ftp.gnu.org/old-gnu/Manuals/finger-1.37/html_mono/finger.html" \l "SEC23)

**I.Tìm hiểu dịch vụ finger**

**1. Giới thiệu**

GNU Finger là một chương trình tiện ích được thiết kế để cho phép người dùng máy chủ Unix trên mạng Internet có được thông tin về nhau. Nó là một sự thay thế trực tiếp cho thuận toán finger Berkeley 4.3, mặc dù nó cho ra nhiều kết quả tìm kiếm khác nhau và được thiết kế để chạy trên nhiều hệ thống khác nhau.

**Tại sao cần một finger khác?**

Ban đầu, mỗi máy chủ trên mạng Internet bao gồm một máy tính duy nhất, có sức mạnh hợp lý, có khả năng xử lý nhiều người dùng cùng một lúc. Thông thường, một vị trí (vị trí thực tế của người dùng máy tính) sẽ chỉ có một hoặc hai máy tính, ngay cả khi họ có 20 người hoặc nhiều hơn sử dụng chúng. Nếu người dùng tại vị trí A muốn biết về người dùng đã đăng nhập tại vị trí B, một chương trình đơn giản có thể được gọi đến truy vấn máy chủ lưu trữ tại vị trí B về người dùng đã đăng nhập.

Với sự khởi đầu của tính toán điện tử, máy tính lớn (mainframe ) đã được đặt sang một bên. Một cơ sở máy tính hiện đại thường bao gồm một người dùng trên mỗi máy chủ, và nhiều máy chủ tại mỗi vị trí. Điều này nhằm để kiểm tra và tìm hiểu về người dùng đăng nhập tại các vị trí khác nhau, vì bạn phải truy vấn mỗi máy chủ để tìm hiểu về người dùng duy nhất đã đăng nhập. Nếu vị trí đó có 20 máy chủ, bạn sẽ phải gọi một chương trình finger 20 lần chỉ để tìm ra ai đã đăng nhập!

GNU Finger là một cách đơn giản và hiệu quả về vấn đề này. Đối với những vị trí có nhiều máy chủ, một máy chủ duy nhất có thể được chỉ định là finger *server* host . Máy chủ này lưu trữ thu thập thông tin về ai đăng nhập vào các máy chủ khác tại vị trí đó. Nếu người dùng tại vị trí A muốn biết về người dùng đăng nhập tại vị trí B, chỉ server host được yêu cầu, thay vì mỗi máy chủ tại vị trí đó. Điều này rất thuận tiện.

GNU Finger là một thay thế trực tiếp cho các chương trình finger hiện có. Vì giao thức finger (các quy tắc cho truyền thông) rất đơn giản nên GNU Finger tuân theo giao thức đó để đáp ứng các yêu cầu đơn giản. Nhưng GNU Finger cũng thực hiện một giao thức khác cho phép hai chương trình finger trao đổi thông tin theo một cách xác định trước, nhanh hơn và rộng hơn.

Finger cung cấp thông tin về người dùng ở các định dạng khác nhau, tùy thuộc vào cách nó được gọi. Finger được gọi mà không cần bất kỳ yêu cầu thực hiện nào của một finger nào ở vị trí khác, cho dù nó được gọi từ đâu. Chuyển đối số tồn tại để nhận dạng thông tin finger "long" và chỉ để biết thông tin máy địa phương.

Nếu người dùng trên máy chủ A muốn biết về người dùng trên máy chủ B, finger phải tạo kết nối mạng với máy chủ B. Nếu máy chủ B đang chạy chương trình finger, chương trình đó sẽ được yêu cầu chuyển tiếp thông tin về người dùng đang được hỏi thông qua kết nối trở lại máy chủ A, nơi finger có thể hiển thị nó.

GNU Finger cũng chạy một tiến trình máy chủ daemon trên server host, công việc của nó là để theo dõi người dùng đăng nhập vào máy địa phương.

Một tính năng tùy chọn và hiện không được hỗ trợ là truyền hình ảnh. Nó được xây dựng trên giao thức mới. Người dùng tại vị trí A (ví dụ: PTIT Hà Nội) có thể thấy hình ảnh của người dùng ở vị trí B (ví dụ nh: PTIT HCM), bằng cách gõ một finger request. Việc chuyển đổi dữ liệu đồ hoạ từ một định dạng này sang dạng khác được thực hiện thông qua GNU Finger; không nơi nào cần biết nơi hay cách những hình ảnh được lưu trữ ở nơi khác để có thể hiển thị những hình ảnh. Bạn nên yêu cầu quản trị viên hệ thống của mình để tìm hiểu xem đã chọn bao gồm chức năng này trên mạng của bạn hay không.

**2. Sử dụng finger**

**Đối số của finger**

Đối số cơ bản của Finger là cặp *user@host*. Phần *user* là tên của người dùng, người mà bạn muốn biết thông tin. *host* là máy tính mà người dùng có tài khoản trên. Khi được gọi theo cách này, GNU Finger hiển thị danh sách các máy chủ mà người dùng này hiện đang đăng nhập hoặc nếu người dùng không đăng nhập thì sẽ hiển thị lần cuối cùng (thời gian) và địa điểm mà người đó đã đăng nhập. *host* có thể được trình bày dưới bất kỳ địa chỉ Internet hợp lệ nào (ví dụ: dot-notation, host.domain ..).

Nếu *host* không tồn tại, máy chủ địa phương(localhost) sẽ được giả định. Nếu *user* bị bỏ trống hoặc không xác định, thì sẽ được giả định rằng bạn muốn có thông tin về tất cả người dùng.

Nội dung và định dạng đầu ra của GNU finger phụ thuộc vào những gì đang được fingered:

*User*

Hiển thị thông tin đăng nhập về người dùng. Nếu `--info' hay `--l' được chỉ định, finger sẽ hiển thị tên đầy đủ, thư mục chính, shell, chuyển tiếp thư, file `.plan' và `.project'. Ví dụ:

bash$ finger --info bson@gnu.ai.mit.edu

[apple-gunkies.gnu.ai.mit.edu]

Jan Brittenson (bson)

Home: /home/fsf/bson

Shell: /usr/local/bin/bash

Mail forwarded to bson@ai.mit.edu.

No mail.

User Real Name What Idle TTY Host Console Location

bson Jan Brittenson fgrep \*p0 apple-gu (nutrimat.gnu.ai.)

bson Jan Brittenson 1:57 \*sb nutrimat

Plan:

To hack GNU Finger

*Mailing List or Alias*

Mở rộng danh sách gửi thư hoặc bí danh và hiển thị người nhận. Bạn luôn phải sử dụng `--info ' (hoặc` -l') khi fingering một danh sách gửi thư hoặc bí danh thư, nếu không các bí danh thư sẽ không được nhìn lên do quá trình xử lý thêm. Ví dụ:

% finger --info postmaster@gnu.ai.mit.edu

postmaster is an alias for the following:

Roland McGrath <roland>,

<tower@prep.ai.mit.edu>,

Noah Friedman <friedman>,

Michael I Bushnell <mib>

*User-defined Target*

Cho phép máy chủ từ xa hiển thị thông tin cụ thể, chẳng hạn như danh sách giá, tài liệu hoặc dự báo thời tiết. Ví dụ:

% finger .site@gnu.ai.mit.edu

This is the FSF GNU Project. For more information, please contact

"postmaster". For information about guest accounts, please contact

"request".

**Tuỳ chọn dòng lệnh (Command line)**

Có một số tùy chọn dòng lệnh mà bạn có thể sử dụng trên GNU Finger:

`--face'

`-f'

Yêu cầu Finger đối mặt với tất cả thông tin người dùng đã được yêu cầu. Phải cung cấp danh sách người dùng rõ ràng. `--info'

`-l'

`-i'

Hiển thị hình thức "đầy đủ" của thông tin cho người dùng finger. Thông tin chính xác được trả lại phụ thuộc vào phần mềm finger được chạy trên máy chủ từ xa - ví dụ như GNU Finger trả về thông tin cụ thể. `-l 'được cung cấp cho khả năng tương thích ngược; finger kế thừa từ Berkeley có tùy chọn này.

`--brief'

`-b'

Hiển thị hình thức "tóm tắt" của thông tin cho người dùng finger. Ngược lại của `--info '.

`--port port*'*

`-P port*'*

Thực hiện kết nối đến cổng, có thể là một số cổng(80, 79, 8080..) hoặc tên dịch vụ từ `/ etc / services '.

`--help'

`-h'

Hiển thị mô tả về tất cả các lựa chọn.

**Tên người dùng đặc biệt**

Bạn có thể cho GNU Finger một số tên người dùng "đặc biệt". Những tên người dùng này bắt đầu bằng một dấu chấm (`. ') Và hướng dẫn daemon finger nhận thực hiện một việc mà chỉ có một daemon Finger của GNU mới có thể làm được. Các tên đặc biệt hiện tại là:

`.free'

Trả về một danh sách các máy trống. Máy "Free" là những máy không có người dùng đăng nhập, hoặc đã không sử dụng trong một thời gian dài. Thông tin trả lại rất rõ ràng, true là trống

`.all'

Trả lại thông tin về mọi máy mà máy chủ Finger biết. `.all 'tương đương với việc ban hành lệnh finger mà không chỉ rõ tên người dùng.

`.site'

Trả lại thông tin về vị trí, chẳng hạn như công ty và địa điểm.

`.clients'

Trả về một danh sách các máy khách mà máy chủ Finger GNU biết. Cũng liệt kê những người đã đăng nhập vào giao diện điều khiển.

`.faces'

Trả về một danh sách các mặt mà máy chủ này đã có. Dòng cuối cùng xuất ra cho bạn biết có bao nhiêu dòng được liệt kê trước đó.

`.local'

Finger chỉ ở máy cụ thể. Điều này cho phép finger tiếp tục hữu ích ngay cả trong trường hợp máy chủ bị tắt. Nó cũng cho phép bạn kiểm tra tất cả các hồ sơ đăng nhập của người dùng. Thông thường, máy chủ chỉ theo dõi hồ sơ đăng nhập hoạt động gần đây nhất cho mỗi người dùng.

`.help'

Mô tả các dịch vụ được cung cấp bởi finger server.

**3. Sử dụng nâng cao**

**Cách hoạt động của Finger**

GNU Finger là tên chung của một tập hợp các chương trình:

* `finger'
* `fingerd'
* `in.fingerd'
* `in.cfingerd'

**Tập lệnh `~ / .fingerrc '**

Khi máy chủ Finger GNU nhận được yêu cầu thông tin về người dùng, nó sẽ tìm xem người dùng có tệp `.fingerrc 'trong thư mục chính hay không. Nếu tập tin đó tồn tại, và là tập tin thực thi, thì tập tin này được thực hiện, và đầu ra finger bình thường được truyền vào nó như đầu vào.

Đầu ra của nó trở thành những gì được trả lại cho yêu cầu. Do đó, nó có thể được sử dụng để:

Vô hiệu hóa finger người dùng cụ thể bằng cách liên kết `~ user / .fingerrc' đến ` / bin / true'.

Hoàn toàn thay thế đầu ra của finger bằng cách bỏ qua đầu vào của nó. Dưới đây là một tập lệnh mẫu có thể đặt trong `~ price-info / .fingerrc '.

#! /bin/sh

#

# This sample script replaces the output of GNU Finger

#

echo Hack-O-Matic Consulting Services, Inc. " " `date`

cat <<ETX

Hi, thanks for asking us about prices on our newly introduced support

services for Free Software. Below is a list of new services; for a list

of our previous services, please send mail to this address and someone

will contact you. Please don't forget to tell us how to reach you.

ETX

cat ~/info/new-stuff

Lọc đầu ra để thực hiện thay đổi. Nếu tập lệnh dưới đây được đặt trong `~ bson / .fingerrc 'trên máy chủ của máy chủ finger cho miền` gnu.ai.mit.edu':

**Mục tiêu Người dùng được định nghĩa**

Nhiều mục tiêu đặc biệt khác có thể được thêm vào như các tập tin thực thi trong thư mục `fingerdir / target '. Mỗi tên tập tin trong thư mục này bắt đầu với một lá thư mô tả khi nào thực hiện nó, theo sau là một dấu gạch nối và tên mục tiêu.

`l' Gửi lại thông tin đầy đủ finger, gõ `finger -l'.

`s' Gửi lại thông tin tóm tắt finger, gõ `finger -s', tuỳ chọn này thường được mặc định, nếu không có chỉ định nào cho nó.

`x' Gửi lại yêu cầu đầy đủ hoặc tóm tắt.

**Cách finger chọn port**

Khi được gọi, GNU Finger máy khách sẽ xem có hay không một tùy chọn `--port 'đã được chỉ định trên dòng lệnh. Nếu có thì sẽ trở thành số cổng mà dịch vụ được sử dụng. Nếu không, máy khách sẽ nhìn thấy tên nó được bắt đầu dưới, loại bỏ bất kỳ đường dẫn thư mục hàng đầu, và bất kỳ hậu tố đuôi. Hậu tố là một phần của tên tệp theo một dấu chấm, bao gồm cả dấu chấm. Đây là tên dịch vụ được sử dụng. Ví dụ, nếu GNU Finger được cài đặt tại `/usr/local/bin/finger.new ', thì dịch vụ` finger' được dùng. Nếu nó được cài đặt tại `/ usr / local / bin / gfinger ', thì dịch vụ' gfinger 'sẽ được sử dụng. Đường dẫn này có thể được thay đổi bởi quản trị viên hệ thống trong quá trình cài đặt.

**4. Các vấn đề về bảo mật**

Một câu hỏi thường phát sinh khi cài đặt phần mềm mạng bổ sung thêm chức năng mới là liệu nó có được coi là an toàn không. Chức năng mới quan trọng nhất trong GNU Finger về bảo mật là khả năng người dùng có một tập tin `.fingerrc 'trong thư mục chính. Sau đây là các biện pháp phòng ngừa của GNU Finger:

Kiểm tra xem `.fingerrc 'có thể ghi bởi bất cứ ai ngoại trừ chủ sở hữu hay không. Lưu ý rằng kiểm tra không được kích hoạt theo mặc định, vì người dùng FSF như bất cứ ai để có thể viết bất kỳ tệp nào - bật kiểm tra này trong quá trình cài đặt bằng cách chỉnh sửa `config.h '.

Kiểm tra xem `.fingerrc 'thuộc sở hữu của người dùng có trong thư mục chính của nó. Điều này, giống như kiểm tra trước đó, bị vô hiệu theo mặc định. Nó thực sự chỉ có ý nghĩa đối với các hệ thống mà người dùng thông thường không thể cho đi các tập tin của họ.

Thực hiện kịch bản thông qua trình bao đăng nhập của người dùng, sử dụng lệnh "shell -c script". Điều này có nghĩa là người dùng đã vô hiệu hoá tài khoản của mình (ví dụ: trình bao được thiết lập cho chương trình in thông báo hoặc chỉ chết) không thể chạy tập lệnh `.fingerrc '. Hành vi này có thể được thay đổi bằng cách mã hóa vỏ trong `config.h '.

**5. Cài đặt finger**

**Cài đặt cơ bản**

Dưới đây là các bước cần thực hiện để cài đặt GNU Finger.

1. Chọn một máy sẽ là máy chủ finger địa phương cho mạng của bạn. Tạo tập tin `clients ', và cài đặt nó trong` / usr / local / etc / fingerdir' (hoặc EtcDir như được chỉ định trong `config.h '). Đặt tên của tất cả các máy cần báo cáo lên máy chủ fingertrong tệp này. Đừng quên bao gồm máy chủ fingercủa chính nó.
2. Đối với mỗi máy khách (máy chủ được chỉ định cũng là máy khách), hãy làm như sau,
3. Thay đổi thư mục làm việc của bạn để trở thành đầu nguồn GNU Finger. Ví dụ, nếu bạn đã đặt nguồn trong `/ src / gnu / finger 'bạn sẽ gõ` cd / src / gnu / finger'.
4. Trong thư mục nguồn, gõ `make clean 'và` ./configure' nếu máy chủ này khác với máy chủ cũ. Nếu bạn đang sử dụng csh trên một phiên bản cũ của Hệ thống V, bạn có thể cần phải nhập `sh ./configure 'thay vì để ngăn csh cố gắng thực hiện cấu hình chính nó. Cấu hình shell script cố gắng đoán các giá trị chính xác cho các biến hệ thống khác nhau được sử dụng trong quá trình biên dịch và tạo Makefile (một trong mỗi thư mục con của thư mục nguồn). Trong một số gói nó tạo ra một tập tin tiêu đề C có chứa các định nghĩa phụ thuộc hệ thống. Nó cũng tạo một tập tin «config.status» mà bạn có thể chạy trong tương lai để tạo lại cấu hình hiện tại. Chạy cấu hình mất một hoặc hai phút. Trong khi nó đang chạy, nó in một số thông báo cho biết nó đang làm gì. Nếu bạn không muốn nhìn thấy các tin nhắn, chạy cấu hình với đầu ra tiêu chuẩn của nó chuyển hướng đến `/ dev / null '; ví dụ, `./configure> / dev / null '. Để biên dịch gói trong một thư mục khác với thư mục chứa mã nguồn, bạn phải sử dụng một phiên bản làm cho hỗ trợ biến VPATH, chẳng hạn như GNU make `cd 'vào thư mục nơi bạn muốn các tệp đối tượng và tệp thi hành đi và chạy cấu hình. cấu hình kiểm tra tự động cho mã nguồn trong thư mục cấu hình có trong và trong `.. '. Nếu vì lý do nào đó cấu hình không nằm trong thư mục mã nguồn mà bạn đang cấu hình, thì nó sẽ báo cáo rằng nó không thể tìm thấy mã nguồn. Trong trường hợp đó, chạy cấu hình với tùy chọn `--srcdir = DIR ', trong đó DIR là thư mục có chứa mã nguồn. Bạn có thể nói `configure 'để tìm ra cấu hình cho hệ thống của bạn, và ghi nó trong« config.status », mà không thực sự cấu hình gói (tạo` Makefile' và có lẽ là một tập tin tiêu đề cấu hình). Để thực hiện việc này, hãy cấu hình tùy chọn `--no-create '. Sau đó, bạn có thể chạy ./config.status để thực sự định cấu hình gói cho một máy chủ cụ thể. Tùy chọn này hữu ích chủ yếu trong các quy tắc `Makefile 'để cập nhật` config.status' và `Makefile '. Bạn cũng có thể cho `config.status 'tùy chọn` --recheck', làm cho nó chạy lại cấu hình với cùng một đối số bạn đã sử dụng trước đó. Điều này rất hữu ích nếu bạn thay đổi cấu hình. `configure 'bỏ qua các đối số khác mà bạn đưa ra. Nếu bạn muốn cài đặt các tập tin cấu hình fingerGNU khác với `/ usr / local / etc / fingerdir ', thì bạn nên chỉnh sửa tập tin` ./config.h' và `include / fingerpaths.h 'ngay bây giờ. Bạn cần phải xác định vị trí thay thế nơi mà các tập tin cấu hình sẽ được giữ. Nếu bạn muốn bao gồm mã không được hỗ trợ cho mugshots, sau đó bạn cũng nên chọn một trong các định dạng mặt, cũng như chỉnh sửa `lib / Makefile.in ',` lib / trang web / Makefile.in', và `src / Makefile .in 'để biên dịch và liên kết trong các file cần thiết . Nếu hệ thống của bạn đòi hỏi các tùy chọn bất thường để biên dịch hoặc liên kết mà cấu hình không biết, bạn có thể cho cấu hình các giá trị ban đầu cho một số biến bằng cách đặt chúng trong môi trường. Trong trình bao tương thích Bourne, bạn có thể thực hiện điều đó trên dòng lệnh như sau:

CC='gcc -traditional' DEFS=-D\_POSIX\_SOURCE ./configure

Các biến `make 'mà bạn có thể muốn ghi đè bằng các biến môi trường khi chạy cấu hình là: (Đối với các biến này, bất kỳ giá trị nào được đưa ra trong môi trường sẽ ghi đè giá trị mà` configure' sẽ chọn :)

1. Để xây dựng và / hoặc cài đặt GNU Finger executable và các mục tiêu chuẩn, hãy thực hiện một trong các lệnh sau:

`make server'

`make client'

`make all'

1. Sửa đổi cấu hình hệ thống để máy khách có (tham khảo tài liệu hệ thống để biết chi tiết về cách thực hiện việc này trên một hệ thống cụ thể):
2. Khi bạn đã thực hiện các bước trên cho mỗi máy khách, đăng nhập vào máy chủ được chỉ định của GNU Finger.
3. Start the server daemon, fingerd. You should arrange to have fingerd started every time the server host is rebooted. For exact details on how to do this, please refer to the server host's system documentation.
4. Nếu bạn chọn để bao gồm các tùy chọn mugshots, bây giờ có thể là một thời điểm tốt để cài đặt mugshots. Nhưng trước tiên, hãy thử gặp mặt từ một trang web khác đang chạy GNU Finger! Ví dụ: bạn có thể thử

finger --face bfox@aurel.cns.caltech.edu

1. Sửa đổi tệp `x-help 'và` x-.site' trong `/ usr / local / etc / fingerdir / target 'cho trang web của bạn.

**Cấu hình file**

* `clients' file
* `serverhost' file
* `mailhost' file
* `forwardhost' file
* `ttylocs' file

**Chức năng cụ thể site**

Nếu bạn quan tâm đến việc tùy biến output của GNU Finger, thì thư mục `lib / site 'là nơi thích hợp để bắt đầu. Nếu bạn muốn thêm mã mới để hiển thị khuôn mặt hoặc có định dạng đầu ra thông tin "dài" đặc biệt thú vị, tôi sẽ vui lòng đưa nó vào mã không được hỗ trợ trong lần phát hành tiếp theo của GNU Finger. (Tôi sẽ trực tiếp liên lạc về mã code của bạn.) Bạn có thể tìm thấy mã đóng góp khác trong `lib / site ', các định dạng và thông tin người dùng khác nhau đáng chú ý nhất để xử lý định dạng tệp tin bản đồ bit khác nhau. Tệp duy nhất được hỗ trợ trong `lib / site 'là` userinfo.c'.

**Cấu hình tuỳ chọn**

Các định nghĩa sau trong `config.h 'kiểm soát hành vi của GNU Finger:

SUPPORT\_FINGERRC

Undefine to prevent users from writing `.fingerrc' scripts. Defined by default.

CHECK\_OWNER\_FINGERRC

Define to make sure `.fingerrc' is owned by the user in whose directory it's found.

CHECK\_RDONLY\_FINGERRC

Define to make sure `.fingerrc' isn't writable by anyone other than its owner.

FINGERRC\_SHELL

The shell to use to execute `.fingerrc'. Undefine to use user's login shell.

DEFAULT\_POLL\_INTERVAL

Define to be the delay between polls, in seconds, unless an interval is explicitly given to fingerd with the `--interval' option.

BASENAME\_IS\_SERVICE

Undefine if you always want the finger client to use the `finger' service. Otherwise the service is deduced from the basename of the client. Defined by default.

INFO\_IS\_DEFAULT

Define if you prefer `finger --info' to be the default, undefine if you prefer `finger --brief' to be the default.

**II.Cài shellcode lên máy nạn nhân bằng finger (Demo)**

**1. Xây dựng mô hình kịch bản.**

- Máy attacker là máy unix có cài dịch vụ finger, máy client cũng vậy.

- Máy attacker gọi dịch vụ finger request, máy client trả lời.

**2. Demo**