**Giao thức và những máy chủ**

Bài này sẽ giới thiệu cho người dùng những giao thức phổ biến như:

* HTTP
* FTP
* POP3
* SMTP
* IMAP

**Telnet:**

Giao thức telnet là 1 giao thức lớp ứng dụng được dùng để kết nối terminal ảo của máy tính khác. Dùng telnet, người dùng có thể đăng nhập vào máy tính khác và truy cập terminal để chạy những chương trình và quản trị hệ thống từ xa.

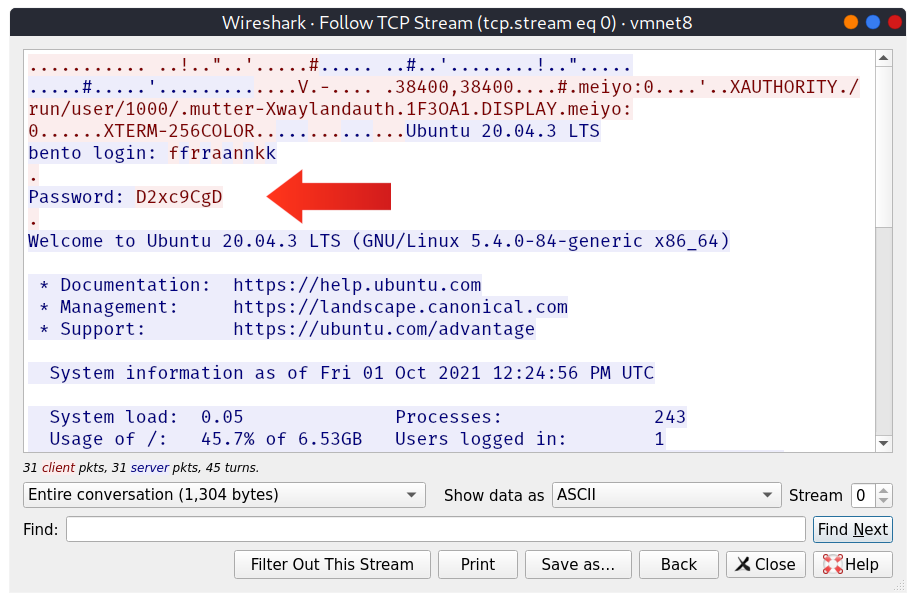
Giao thức telnet khá đơn giản. Khi 1 người dùng kết nối, sẽ được yêu cầu tài khoản và mật khẩu. Khi xác thực thành công, họ sẽ truy cập terminal của máy tính khác. Không may mắn, tất cả những giao tiếp giữa máy khách Telnet và máy chủ không được mã hóa, rất dễ trở thành mục tiêu của kẻ tấn công.

Một máy chủ telnet sử dụng giao thức telnet để nghe những kết nối đến cổng 23. Ví dụ, một người dùng đang kết nối đến telnetd, 1 máy chủ telnet. Các bước thực hiện như sau:

* Đầu tiên anh ấy được yêu cầu cung cấp tên người dùng. Chúng ta có thể thấy người dùng nhập frank.
* Sau đó, anh ấy được yêu cầu mật khẩu, D2xc9CgD. Mật khẩu không được hiển thị trên màn hình.
* Khi hệ thống kiểm tra thông tin đăng nhập, máy chủ từ xa cấp cho anh ấy 1 giao diện thực hiện lệnh frank@bento:~$. $ chỉ rằng nó không phải root terminal.



Mặc dù Telnet cho chúng ta truy cập terminal của hệ thống từ xa không giới hạn thời gian, nó không phải là 1 giao thức đáng tin cậy để quản trị từ xa vì dữ liệu được gửi ở dạng văn bản. Ở hình bên dưới, chúng ta thu thập được lưu lượng tạo ra bởi Telnet, và nó rất dễ để tìm mật khẩu. Chữ màu đỏ là chữ chúng ta đang gửi đến hệ thống từ xa, trong khi chữ màu xanh là chữ hệ thống đang gửi. Chú ý là tên người dùng đã được gửi lại; tuy nhiên, mật khẩu thì không. Nói cách khác, nếu một ai đó đang xem chúng ta đánh chữ, họ sẽ không thể xem những kí tự mật khẩu trên màn hình.

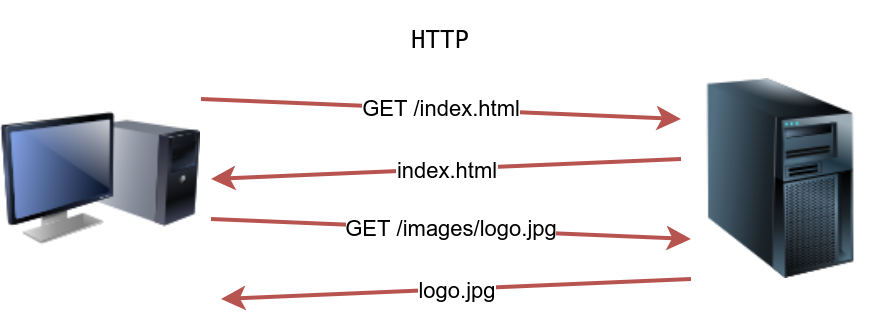


Telnet không phải là 1 lựa chọn bảo mật, đặc biệt bất cứ ai có thể bắt được lưu lượng mạng sẽ có thể khám phá tên người dùng và mật khẩu của bạn. Giải pháp thay thế an toàn hơn là SSH.

**HTTP**

Hypertext Transfer Protocol (HTTP) là giao thức dùng để vận chuyển những trang web. Trình duyệt của bạn kết nối đến máy chủ web và dùng HTTP để yêu cầu những trang HTML và hình ảnh. Bất cứ lúc nào bạn duyệt world wide web (www), bạn chắc chắn đang dùng giao thức HTTP.

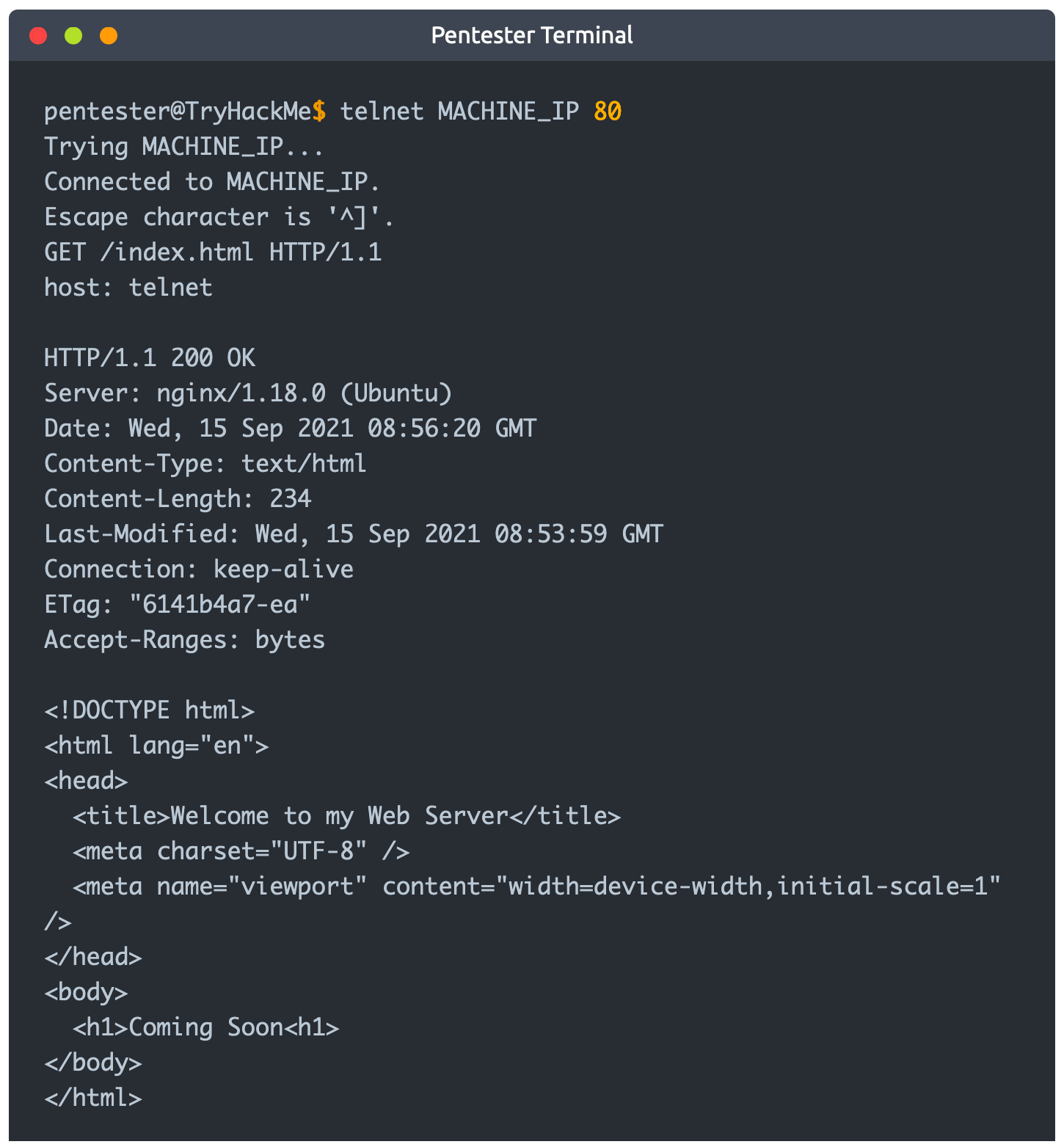
Hình dưới cho thấy máy khách đang yêu cầu trang HTML index.html, cái mà máy chủ web cung cấp. Sau đó máy khách yêu cầu 1 hình ảnh, logo.jpg và máy chủ web gửi nó.



HTTP gửi và nhận dữ liệu ở dạng văn bản (không mã hóa); Do đó, bạn có thể dùng 1 công cụ đơn giản như telnet (hay netcat) để giao tiếp với máy chủ web như trình duyệt. Điểm khác biệt chính là bạn cần nhập những lệnh liên quan đến HTTP thay vì trình duyệt làm điều đó cho bạn.

Ở ví dụ sau, chúng ta sẽ thấy cách chúng ta có thể yêu cầu 1 trang web; Hơn nữa, sẽ khám phá được phiên bản của máy chủ web. Để làm được điều đó, chúng ta sẽ dùng máy khách telnet. Các bước thực hiện như sau:

1. Đầu tiên chúng ta kết nối đến cổng 80 bằng telnet MACHINE\_IP 80
2. Tiếp theo, chúng ta cần nhập GET /index.html HTTP/1.1 để truy suất trang index.html .
3. Cuối cùng, bạn cần cung cấp 1 vài giá trị cho máy chủ như host:telnet



Chúng ta cần 1 máy chủ HTTP (máy chủ web) và HTTP client (trình duyệt web) để sử dụng giao thức HTTP. Máy chủ web sẽ vận chuyển 1 danh sách tập tin cho trình duyệt đang yêu cầu.

Ba lựa chọn phổ biến cho máy chủ web:

* Apache
* Internet Information Services (IIS)
* nginx

Apache và nginx là phần mềm miễn phí và mã nguồn mở. Tuy nhiên, IIS là phần mềm đóng và mất phí.

Những trình duyệt web phổ biến nhất:

* Chrome của Google
* Edge của Microsoft
* Firefox của Mozilla
* Safari của Apple

**File Transfer Protocol (FTP)**

FTP được phát triển để vận chuyển tập tin giữa những máy tính khác nhau.

FTP cũng gửi và nhận dữ liệu ở dạng văn bản; do đó, chúng ta có thể dùng telnet để giao tiếp với máy chủ ftp. Những bước thực hiện như sau:

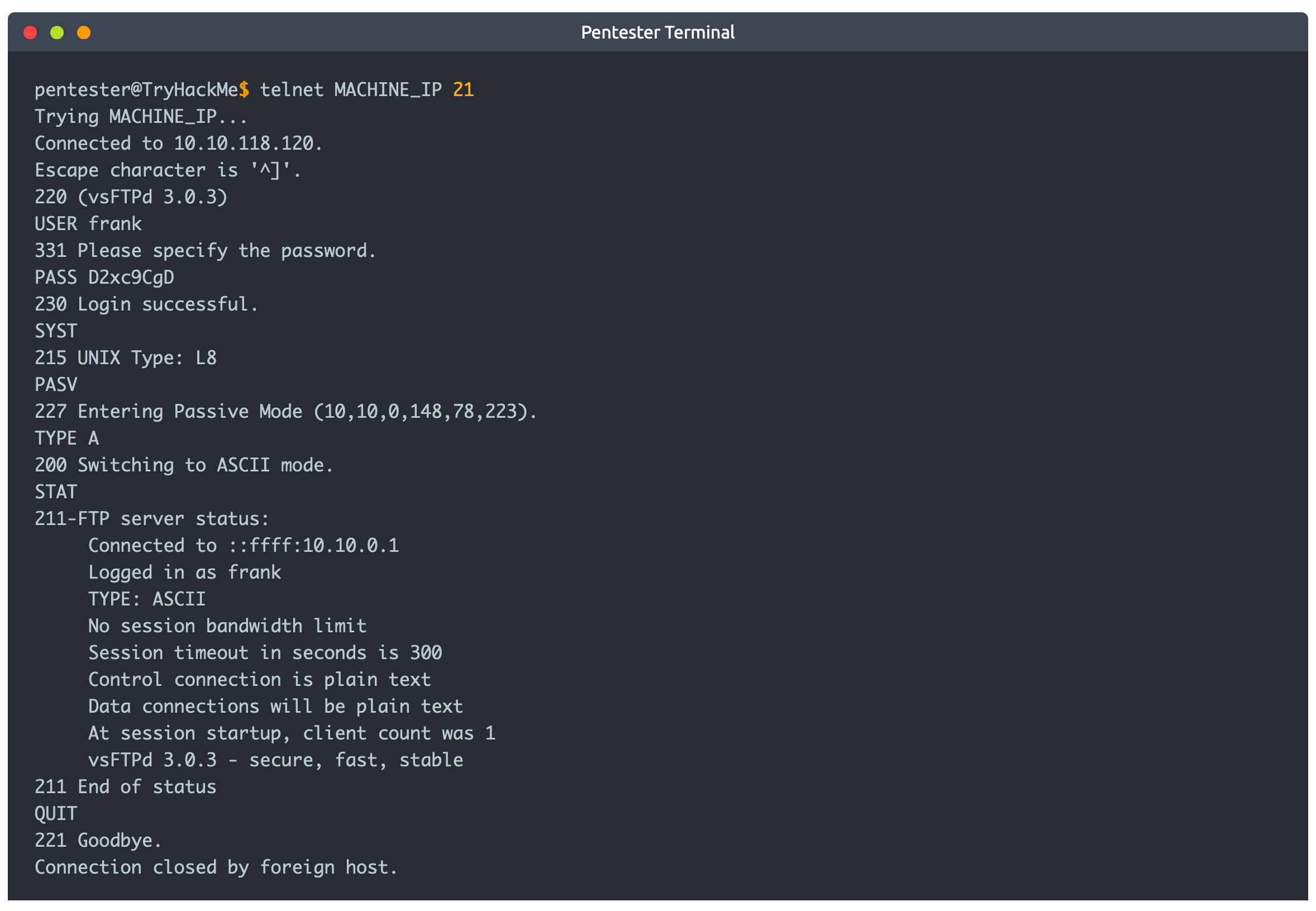
1. Kết nối đến máy chủ FTP bằng việc dung máy khách telnet. FTP lắng nghe trên cổng 21.
2. Chúng ta cần cung cấp tên người dùng với lệnh USER frank
3. Sau đó, cung cấp mật khẩu với lệnh PASS D2xc9CgD
4. Vì chúng ta cung cấp đúng tài khoản và mật khẩu nên được đăng nhập.

Lệnh STAT có thể cung cấp thêm thông tin. Lệnh SYST hiển thị loại hệ thống của đối tượng (Unix). PASV điều chỉnh chế độ sang bị động. FTP có hai chế độ:

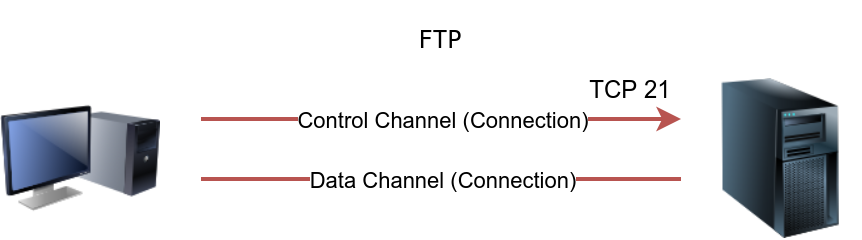
Active: dữ liệu được gửi qua 1 kênh riêng có nguồn gốc từ máy chủ FTP ở cổng 20

Passive: dữ liệu được gửi qua 1 kênh riêng có nguồn gốc từ máy khách FTP có cổng lớn hơn 1023

Lệnh TYPE A điều chỉnh vận chuyển tập tin ở ASCII, trong khi TYPE I điều chỉnh tập tin ở dạng nhị phân. Tuy nhiên, chúng ta không thể vận chuyển tập tin bằng telnet được vì FTP tạo 1 kết nối riêng để vận chuyển.

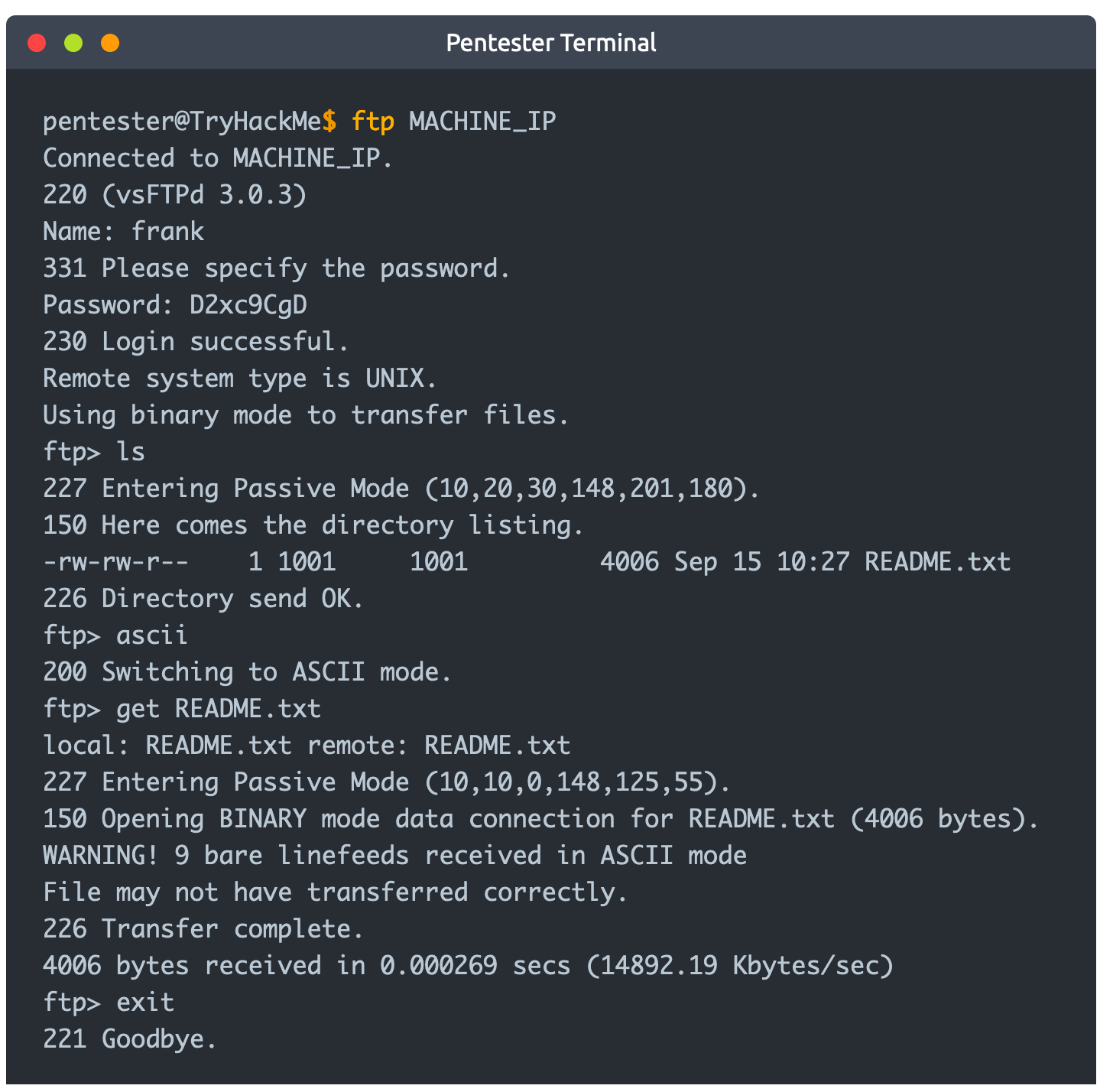


Hình bên dưới cho thấy cách vận chuyển tập tin bằng FTP. Máy khách sẽ khởi tạo 1 kết nối đến máy chủ FTP, lắng nghe trên cổng 21. Tất cả lệnh sẽ được gửi qua kênh điều khiển. Khi máy khách yêu cầu 1 tập tin, 1 kết nối TCP khác sẽ được thiết lập giữa chúng.



Để truy suất tập tin dễ dàng hơn, hãy sử dụng ứng dụng FTP thực tế.

Sau khi đăng nhập thành công, chúng ta có giao diện ftp>. ls để liệt kê các tập tin; sau đó điều chỉnh sang ascii. Cuối cùng ,GET FILENAME làm cho máy khách và máy chủ thiết lập 1 kênh mới để vận chuyển.



Những máy khách và máy chủ FTP dùng giao thức FTP.

Một số máy chủ FTP:

* vsftpd
* ProFTPD
* uFTP

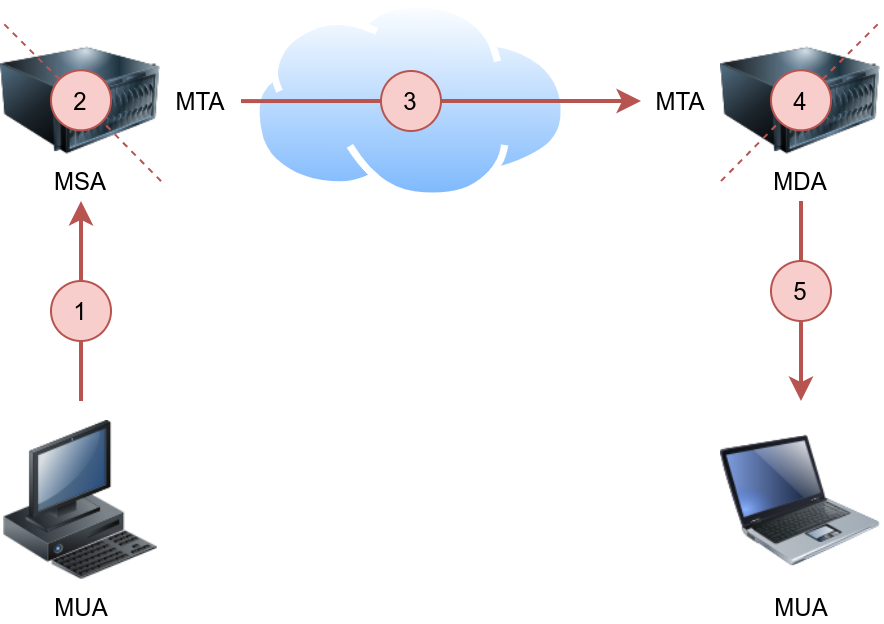
Đối với máy khách FTP, ngoài FTP client được tìm thấy phổ biến trên những hệ thống Linux, bạn có thể dùng FTP client với GUI như FileZilla. Một vài trình duyệt web cũng hỗ trợ giao thức FTP.

**Simple Mail Transfer Protocol (SMTP)**

Thư là 1 trong những dịch vụ được dùng nhiều nhất trong Internet. Có rất nhiều cấu hình cho máy chủ email; Ví dụ, bạn có thể thiết lập hệ thống email cho phép những người dùng cục bộ trao đổi thư với những người khác mà không truy cập vào Internet. Tuy nhiên, chúng ta sẽ xem xét thiết lập tổng quát hơn nơi các máy chủ email khác nhau kết nối qua Internet.

Vận chuyển thư qua internet yêu cầu những thành phần sau:

1. Mail Submission Agent (MSA)
2. Mail Transfer Agent (MTA)
3. Mail Delivery Agent (MDA)
4. Mail User Agent (MUA)



Hình trên hiển thị 5 bước mà 1 bức thư cần đi qua để đến hộp thư của người nhận.

1. A Mail User Agent (MUA) hoặc chỉ đơn giản là 1 ứng dụng email, có 1 email được gửi. MUA kết nối với MSA để gửi thư.

2. MSA nhận được thư, kiểm tra lỗi trước khi truyền nó đến máy chủ MTA, thường được lưu trữ trong cùng máy chủ.

3. MTA sẽ gửi thư đến MTA của người nhận. MTA cũng có thể hoạt động như MSA.

4. 1 thiết lập cơ bản sẽ làm cho máy chủ MTA cũng hoạt động như MDA.

5. Người nhận sẽ thu thập email từ MDA bằng việc dùng ứng dụng email.

Nếu những bước trên làm bạn bối rối, xem xét sự tương tự sau đây:

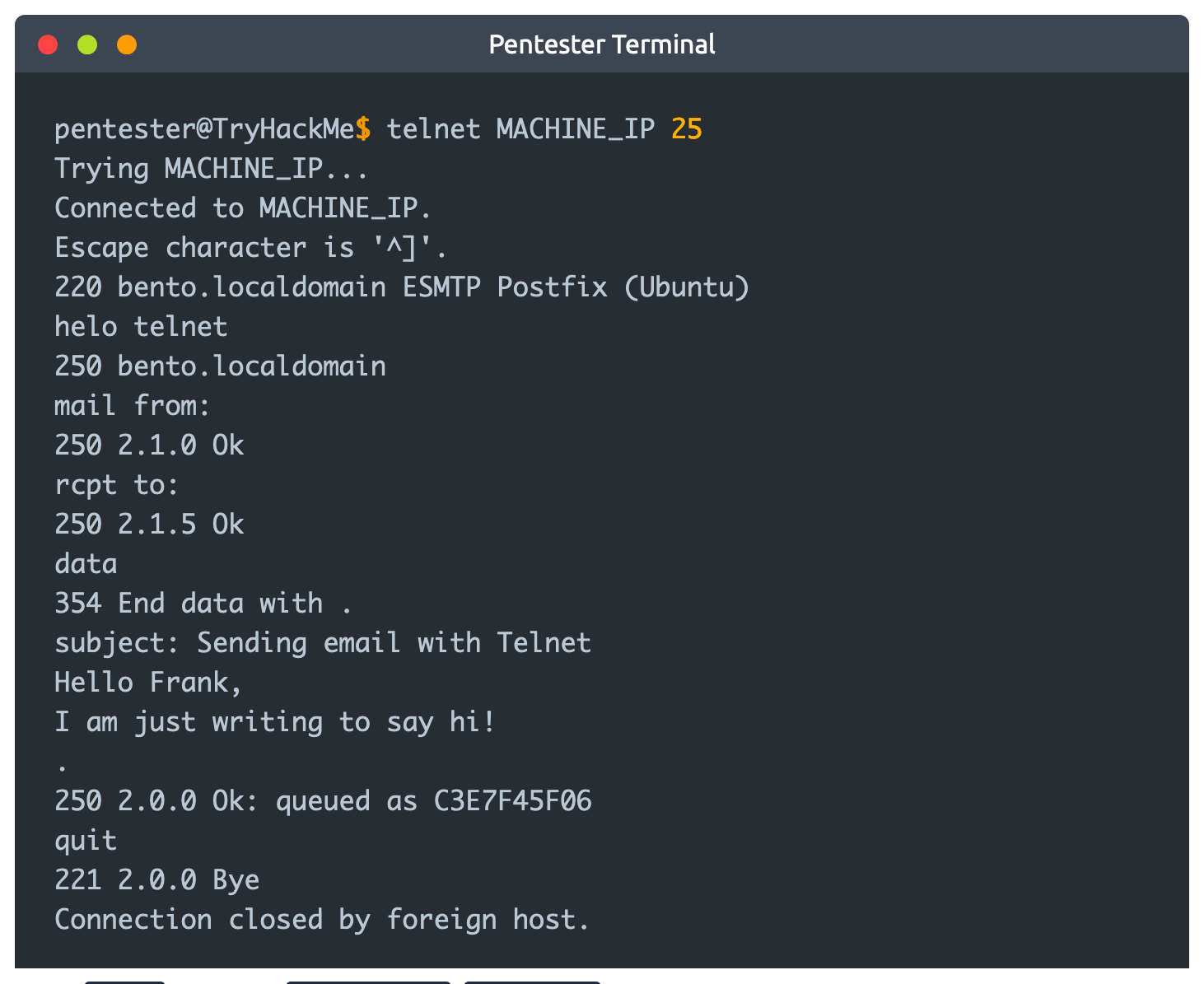
1. Bạn (MUA) muốn gửi thư bưu điện.
2. Nhân viên bưu điện (MSA) kiểm tra thư xem có lỗi gì không trước khi bưu điện A(MTA) chấp nhận nó .
3. Bưu điện A kiểm tra địa chỉ và gửi nó đến đúng bưu điện B (MTA)
4. Bưu điện B (MTA) vận chuyển thư đến hộp thư của người nhận (MDA)
5. Người nhận (MUA) thường xuyên kiểm tra hộp thư xem có thư mới không.

Theo cách tương tự, chúng ta cần tuân theo 1 giao thức để giao tiếp với máy chủ HTTP và chúng ta cần dựa vào những giao thức email để nói chuyện với MTA và MDA. Những giao thức đó là:

1. SMTP
2. POP3 hoặc IMAP

SMTP được dùng để giao tiếp với máy chủ MTA. Vì SMTP dùng văn bản rõ ràng, khi tất cả lệnh được gửi đi không có mã hóa, chúng ta có thể dùng công cụ telnet để kết nối với máy chủ SMTP và ứng dụng email (MUA) để gửi thư.

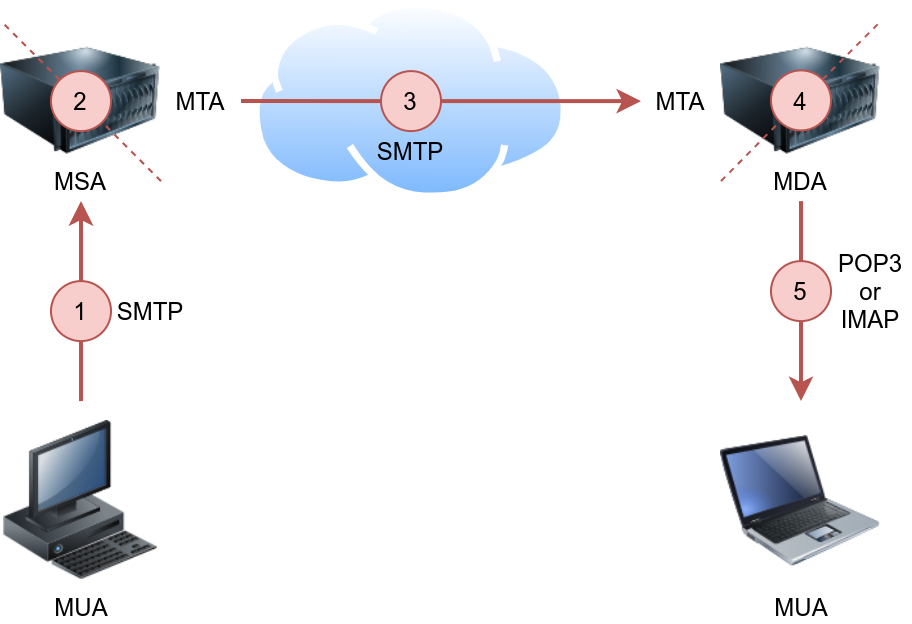
Máy chủ SMTP mặc định lắng nghe trên cổng 25. Khi kết nối, chúng ta phát hành helo hostname và sau đó bắt đầu viết thư.



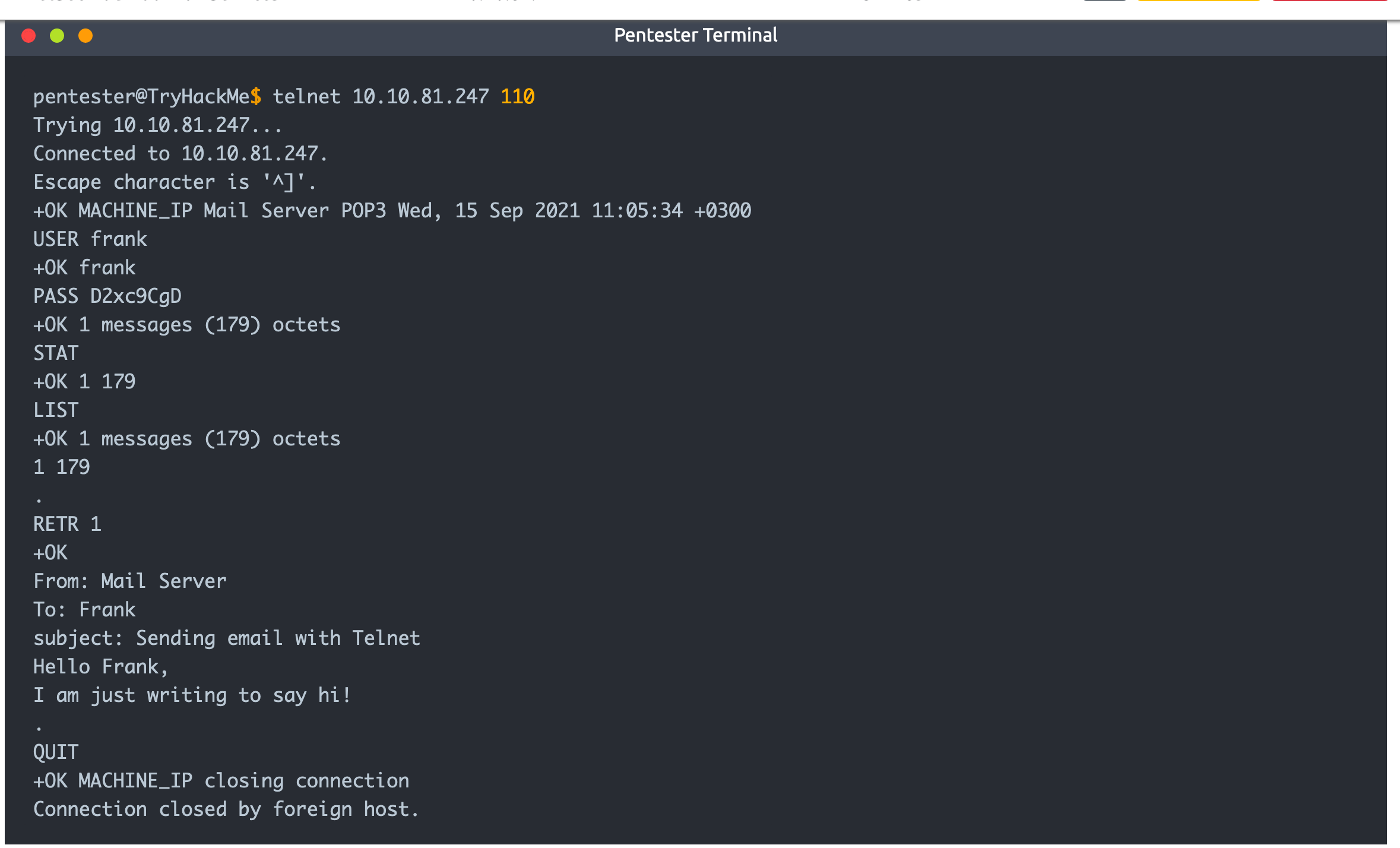
Sau khi helo, chúng ta phát hành mail from:, rcpt to: để chỉ định người gửi và người nhận. Khi chúng ta gửi thư, chúng ta phát hành lệnh data và viết thư. Chúng ta phát hành <CR><LF>.<CR><LF> (hoặc Enter . Enter) . Tiếp theo, máy chủ SMTP xếp tin nhắn.

**Post Office Protocol 3 (POP3)**

POP3 là 1 giao thức được dùng để tải những tin nhắn từ máy chủ MDA. Ứng dụng mail kết nối đến máy chủ POP3, xác thực và tải những tin nhắn mới trước khi xóa chúng.



Ví dụ dưới cho thấy phiên của POP3 sẽ như thế nào nếu được thực hiện qua máy khách telnet. Đầu tiên người dùng kết nối với máy chủ POP3 ở cổng 110. Xác thực được yêu cầu để truy cập những tin nhắn; Sử dụng lệnh STAT, chúng ta nhận được phản hồi +OK 1 179; dựa trên RFC 1939, 1 phản hồi tích cực cho STAT có định dạng +OK nn mm, nn là số tin nhắn trong hộp thư, mm là kích thức hộp thư theo bytes. Lệnh LIST cung cấp 1 danh sách thư mới trên máy chủ và RETR 1 đã truy suất thư đầu tiên trong danh sách.



Ví dụ trên hiển thị những lệnh được gửi ở dạng văn bản. Dùng telnet đủ để xác thực và truy suất tin nhắn. Vì tên người dùng và mật khẩu được gửi ở dạng văn bản, bất cứ bên thứ ba nào xem được lưu lượng mạng có thể đánh cắp thông tin đăng nhập.

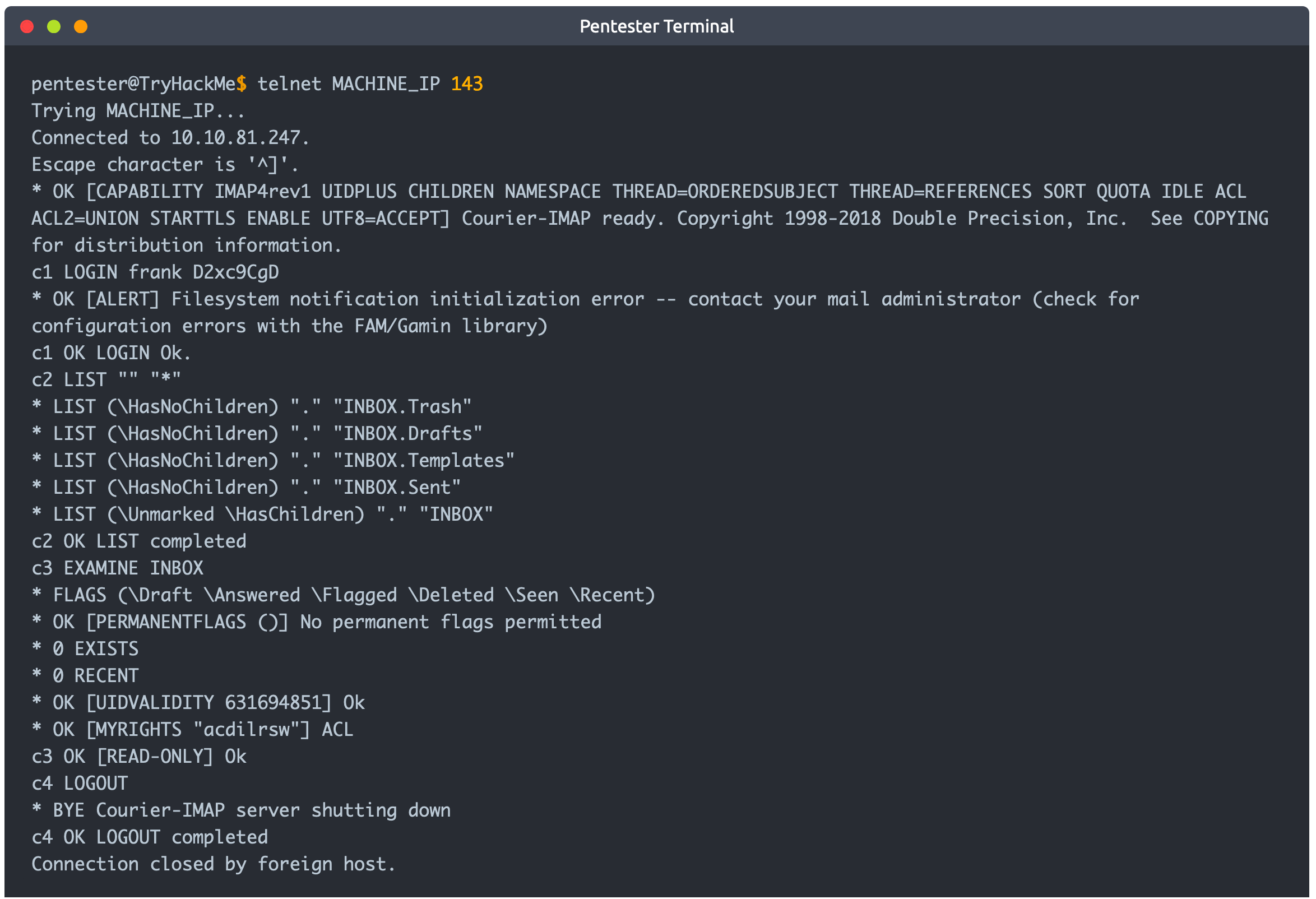
Nhìn chung, ứng dụng mail của bạn (MUA) sẽ kết nối đến máy chủ POP3 (MDA), xác thực và tải tin nhắn.

Dựa vào cài đặt mặc định, ứng dụng mail sẽ xóa tin nhắn sau khi nó được tải. Hành vi này có thể được thay đổi từ ứng dụng mail nếu bạn muốn tải thư 1 lần nữa từ ứng dụng khác. Việc truy cập 1 tài khoản mail qua nhiều ứng dụng bằng POP3 thường không tiện vì người ta thường mất dấu các thư đã đọc và chưa đọc. Để giữ cho hộp thư được đồng bộ hóa, chúng ta cần xem xét 1 giao thức khác như IMAP.

**Internet Message Access Protocol (IMAP)**

IMAP là giao thức phức tạp hơn POP3. IMAP có thể đồng bộ hóa thư qua nhiều thiết bị. Nói cách khác, nếu bạn đánh dấu 1 tin nhắn đã đọc khi kiểm tra thư trên điện thoại, sự thay đổi sẽ được lưu trữ trên máy chủ IMAP (MDA) và được lặp lại trên laptop khi bạn đổng bộ hóa hộp thư.

Chúng ta dùng telnet để kết nối đến máy chủ IMAP sau đó xác thực bằng LOGIN username password. IMAP yêu cầu mỗi câu lệnh bắt đầu bằng 1 chuỗi ngẫu nhiên để theo dõi phản hồi. Vì vậy chúng ta thêm c1, c2 và tiếp tục. Sau đó chúng ta liệt kê những thư mục thư bằng LIST “” “\*”, trước khi kiểm tra xem chúng ta có tinh nhắn mới không bằng EXAMINE INBOX.



**Tóm tắt:**

| **Protocol** | **TCP Port** | **Application(s)** | **Data Security** |
| --- | --- | --- | --- |
| FTP | 21 | File Transfer | Cleartext |
| HTTP | 80 | Worldwide Web | Cleartext |
| IMAP | 143 | Email (MDA) | Cleartext |
| POP3 | 110 | Email (MDA) | Cleartext |
| SMTP | 25 | Email (MTA) | Cleartext |
| Telnet | 23 | Remote Access | Cleartext |