Passive recon cho phép bạn thu thập thông tin về đối tượng không cần kết nối trực tiếp. Giống như bạn quan sát từ xa để thu thập thông tin công khai.

Active recon yêu cầu bạn kết nối với đối tượng. Cách kết nối có thể chỉ là cuộc gọi điện thoại hay giả vờ đi đến công ty đối tượng để nhận được nhiều thông tin hơn, giống như social engineering. Ngoài ra, nó có thể là 1 kết nối trực tiếp đến hệ thống đích.

Nó giống như bạn đang phá khóa. Do vậy, hãy nhớ không recon active trước khi được phân quyền hợp pháp từ khách hàng.

Active recon là những kết nối trực tiếp với đối tượng. Bất cứ kết nối nào cũng có thể để lại manh mối trên logs trong địa chỉ IP của khách hàng. Tuy vậy, không phải kết nối nào cũng đáng nghi. Xem xét việc duyệt web, không ai sẽ điều tra trình duyệt kết nối với máy chủ web trong số hàng trăm người dùng hợp pháp. Bạn có thể dùng nhiều kĩ thuật như vậy khi làm việc trong red team và không cảnh báo cho đội xanh.

Chúng ta sẽ bắt đầu với trình duyệt web và những công cụ phát triển của nó; Trình duyệt web là 1 thư viện thu thập thông tin rất hiệu quả. Sau cùng, chúng ta sẽ thảo luận về những công cụ nhẹ khác như ping, traceroute, telnet.

**Trình duyệt web**

Trình duyệt web có thể là 1 công cụ rất tuyệt vời, đặc biệt nó khả thi trên tất cả hệ thống.

Có một vài cách bạn có thể dùng trình duyệt web để thu thập thông tin về 1 đối tượng.

Ở mức độ vận chuyển, trình duyệt kết nối:

* TCP cổng 80 khi trang web được truy suất qua HTTP
* TCP cổng 443 khi trang web được truy suất qua HTTPs

Vì 80 và 443 là những cổng mặc định cho HTTP và HTTPs, trình duyệt web không hiển thị nó trên thanh địa chỉ.

Tuy nhiên, vẫn có thể dùng 1 cổng khác để truy cập 1 dịch vụ. Ví dụ, https://127.0.0.1:8834 sẽ kết nối đến 127.0.0.1 (localhost) ở cổng 8834 qua giao thức https. Nếu có một máy chủ https lắng nghe trên cổng đó, chúng ta sẽ nhận được 1 trang web.

Trong khi duyệt một trang web, bạn có thể nhấn Option+ Command+ I để mở công cụ phát triển trên Firefox. Những công cụ phát triển cho phép bạn điều tra rất nhiều thứ mà trình duyệt của bạn đã nhận và trao đổi với máy chủ từ xa. Ví dụ, bạn có thể xem và điều chỉnh tập tin JS, phân tích cookies trên hệ thống và khám phá cấu trúc thư mục của trang.

Có rất nhiều tiện ích mà Firefox và Chrome có thể giúp trong quá trình kiểm thử. Đây là 1 vài ví dụ:

* FoxyProxy
* User-Agent Switcher and Manager
* Wappalyzer

**Ping**

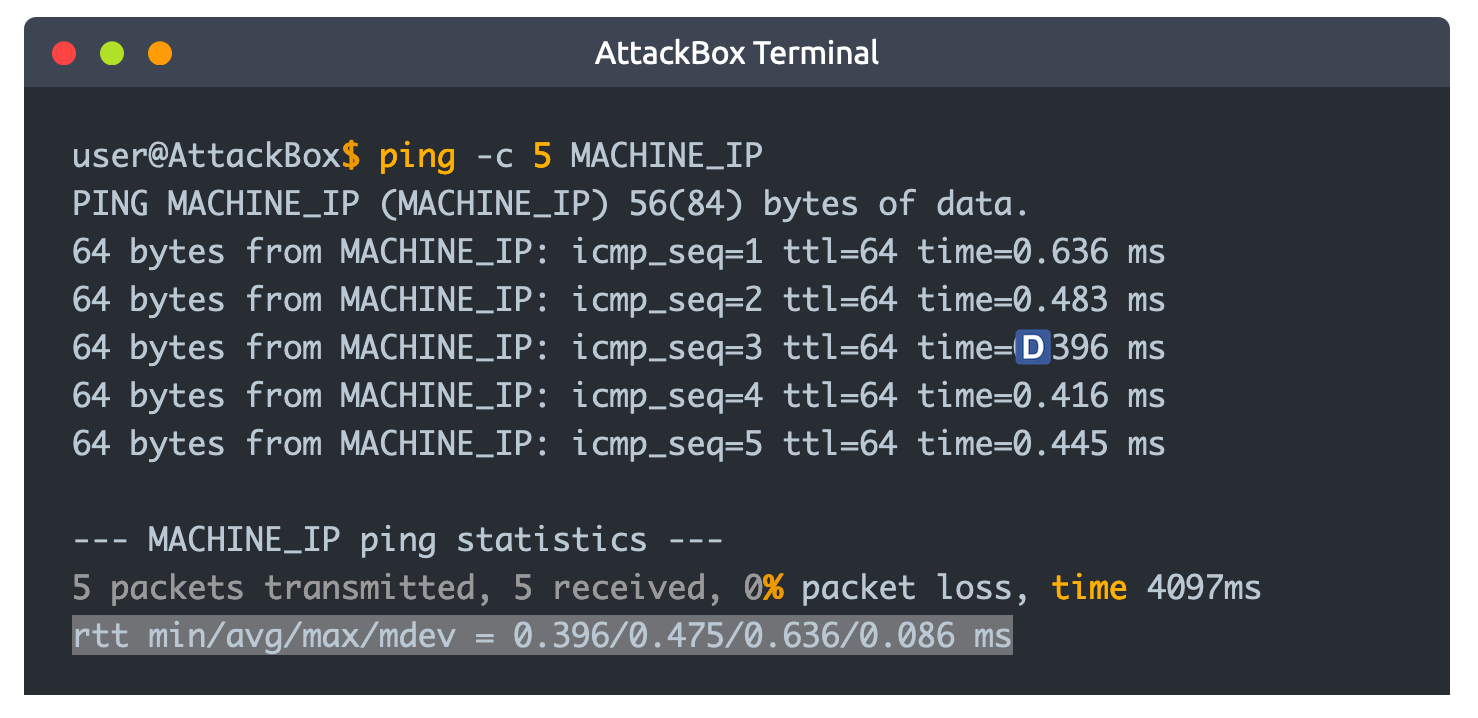
Mục đích chính của ping là kiểm tra xem bạn có thể truy cập hệ thống từ xa không và hệ thống có thể kết nối lại với bạn không.

Nói cách khác, nó được dùng để kiểm tra kết nối mạng; tuy nhiên, chúng ta hứng thứ với mục đích sử dụng khác của nó: kiểm tra xem hệ thống từ xa có trực tuyến không.

Lệnh ping gửi 1 gói tin đến hệ thống từ xa và nó phản hồi. Bằng cách này, bạn có thể kết luận rằng hệ thống từ xa đang trực tuyến và mạng vẫn còn hoạt động giữa hai thiết bị.

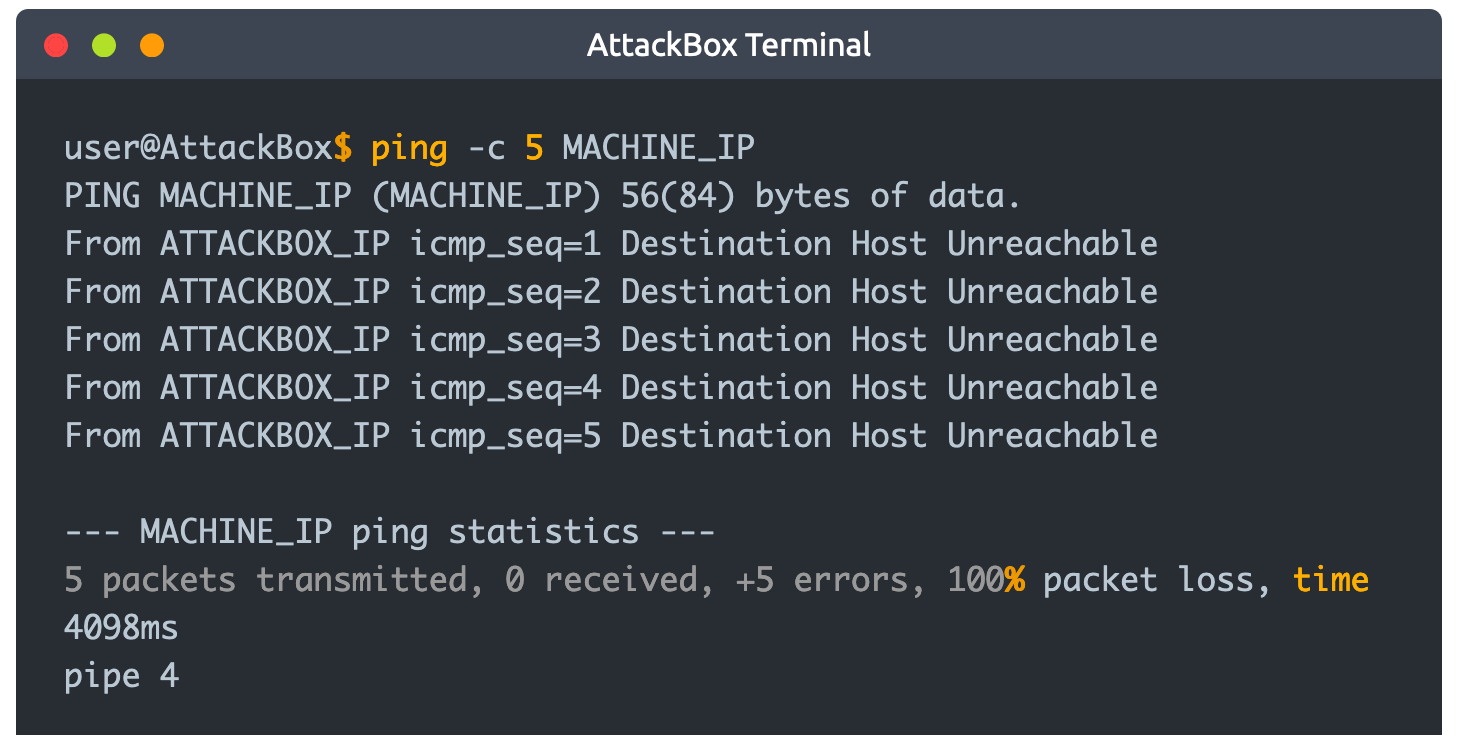
Mục tiêu của câu lệnh này là đảm bảo hệ thống đích trực tuyến trước khi chúng ta tốn thời gian để scan chi tiết để khám phá hệ điều hành và dịch vụ đang chạy.

Trong ví dụ sau, chúng ta chỉ định gửi đi 5 gói tin icmp.



Hệ thống đích đang phản hồi. Chúng ta để ý thấy, trung bình mất 0.475 ms để chúng ta nhận được trả lời, tối đa là 0.636 ms

Cùng khám phá trường hợp sau: chúng ta tắt máy ảo và sau đó thử ping địa chỉ IP của nó.



Nhìn chung mà nói, khi chúng ta không nhận được phản hồi, đó là vì:

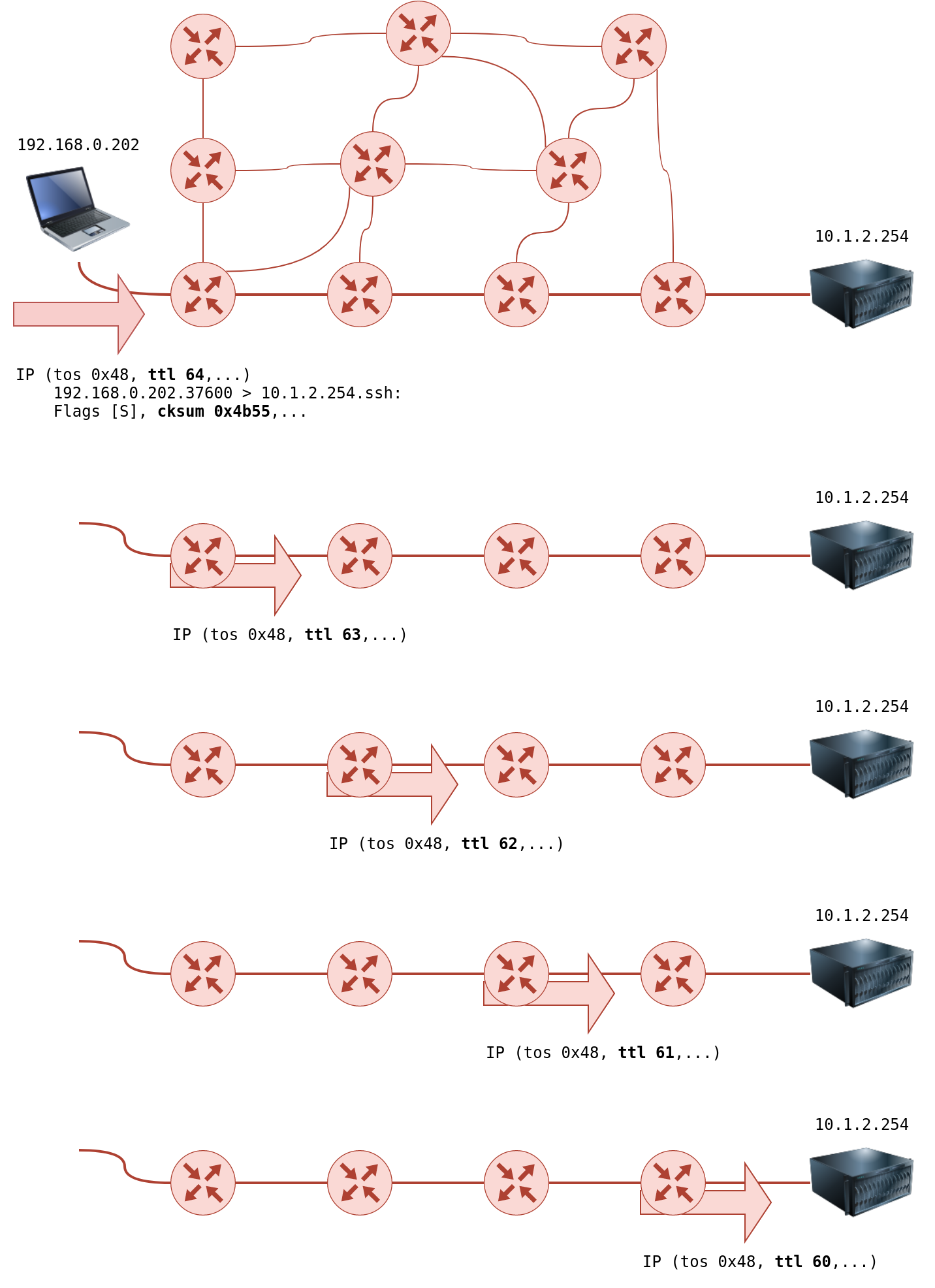
* Máy tính đích không phản hồi; có thể đang khởi động hoặc tắt, hệ điều hành bị hư.
* Nó đã bị rút ra khỏi mạng hoặc thiết bị mạng bị lỗi.
* Tường lửa được cấu hình để chặn những gói tin như vậy. Chú ý là tường lửa MS Windows mặc định chặn ping.
* Hệ thống của bạn bị rút ra khỏi mạng.

**Traceroute**

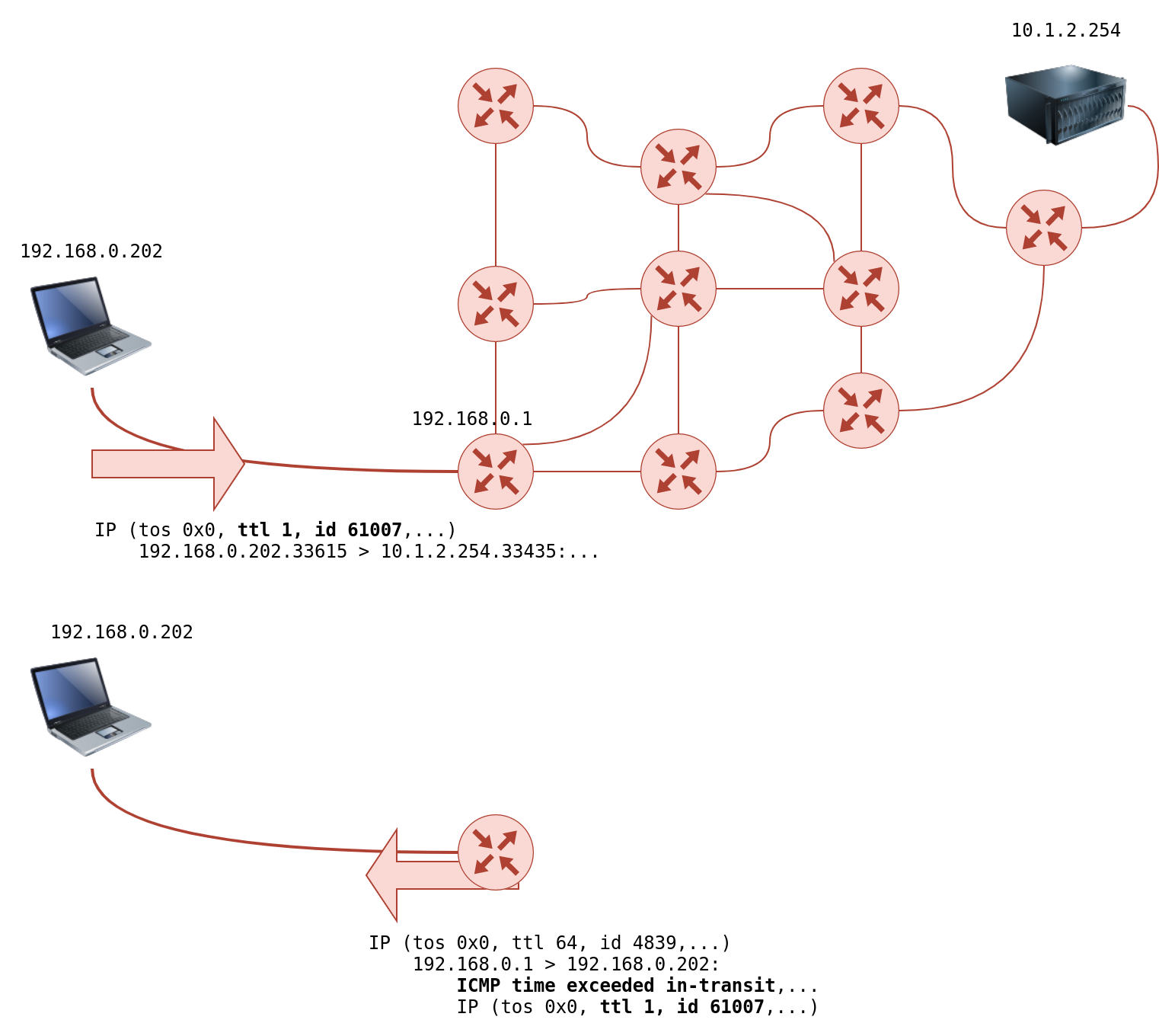
Lệnh traceroute theo dõi tuyến đường giữa hai thiết bị của những gói tin. Mục đích của traceroute là tìm kiếm địa chỉ IP của những routers hoặc hubs mà gói tin truyền qua. Nó cũng tiết lộ số routers giữa hai hệ thống. Tuy nhiên, tuyến đường mà những gói tin truyền đi có thể thay đổi vì rất nhiều routers sử dụng giao thức định tuyến động để phù hợp với sự thay đổi của mạng.

Cú pháp: traceroute MACHINE\_IP

Không có cách trực tiếp nào để khám phá đường dẫn từ hệ thống của bạn đến mục tiêu. Chúng ta dựa vào ICMP để lừa những routes tiết lộ địa chỉ IP của chúng. Chúng ta có thể làm điều này bằng việc sử dụng TTL trong IP header. Mặc dù T trong TTL đại diện cho thời gian,TTL chỉ ra số lượng routers tối đa mà 1 gói tin có thể truyền qua; Khi 1 router nhận 1 gói tin, nó giảm TTL đi một trước khi chuyển nó đến 1 router khác.



Tuy vậy, nếu TTL đạt đến 0, nó sẽ bị hủy và ICMP time exceeded sẽ được gửi đến người gửi ban đầu. Trong hình sau, hệ thống đặt TTL bằng 1 trước khi gửi nó đến router. Router đầu tiên trên đường truyền giảm TTL còn 0. Cuối cùng, router này sẽ hủy bỏ gói tin và gửi 1 thông báo lỗ: ICMP time exceeded. Lưu ý, một vài routers được cấu hình không gửi thông báo icmp như vậy khi hủy bỏ 1 gói tin.



Với Linux, traceroute sẽ bắt đầu gửi UDP datagrams trong gói tin IP với TTL bằng 1. Do đó, router đầu tiên sẽ làm cho TTL bằng 0 và gửi ICMP exceeded time. TTL bằng 1 sẽ tiết lộ địa chỉ IP đầu tiên cho bạn. Sau đó nó gửi gói tin khác với TTL bằng 2; gói tin này sẽ bị hủy bỏ ở router thứ hai; tiếp tục như vậy.

**Telnet**

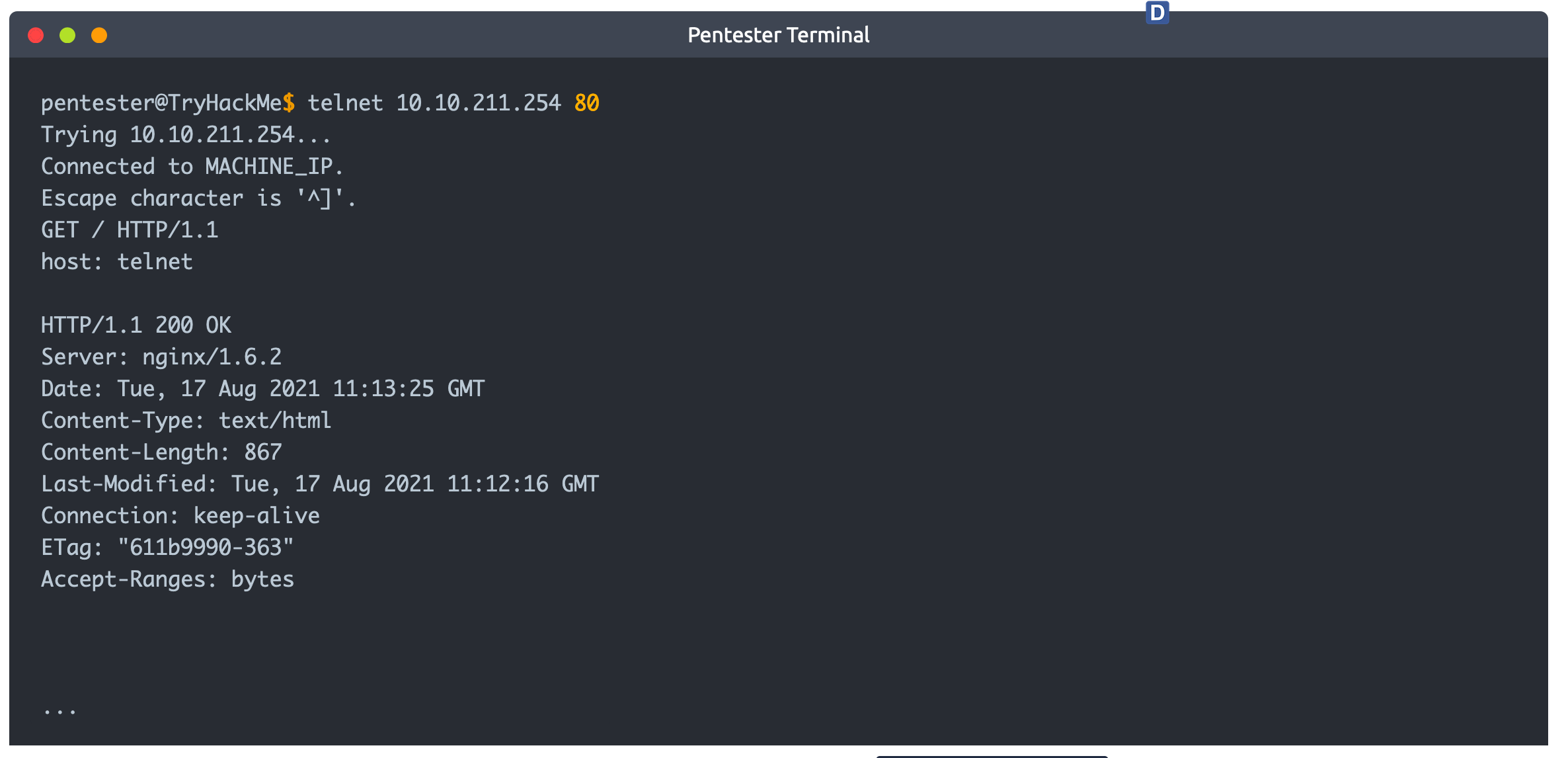
Giao thức Telnet được phát triển năm 1969 để giao tiếp với hệ thống từ xa qua giao diện dòng lệnh (CLI). Do đó, câu lệnh telnet sử dụng giao thức telnet để quản trị từ xa. Cổng mặc định là 23.

Từ góc độ bảo mật, telnet gửi tất cả dữ liệu, bao gồm tên người dùng và mật khẩu trong văn bản rõ ràng. Việc gửi văn bản rõ ràng làm cho bất cứ ai cũng có thể truy cập kênh giao tiếp để đánh cắp thông tin đăng nhập. Giải pháp thay thế an toàn hơn là SSH.

Tuy vậy, máy khách telnet có thể được dùng với nhiều mục đích khác nhau. Bạn có thể dùng telnet để kết nối bất cứ dịch vụ nào.

Cú pháp: telnet MACHINE\_IP PORT

Chúng ta muốn khám phá thêm thông tin về máy chủ web, lắng nghe trên cổng 80. Chúng ta kết nối đến máy chủ ở cổng 80, sau đó chúng ta giao tiếp bằng giao thức http. Bạn không cần hiểu sâu về giao thức đó, chỉ cần phát hành GET / HTTP/1.1 . Để chỉ định một vài thứ khác trang mặc định, bạn có thể dùng GET /page.html HTTP/1.1, sẽ yêu cầu trang page.html. Chúng ta cũng có thể chỉ định máy chủ web từ xa chúng ta muốn dùng HTTP phiên bản 1.1 để giao tiếp. Để nhận được phản hồi hợp lệ, bạn cần nhập tên máy chủ host: example và đánh enter hai lần.



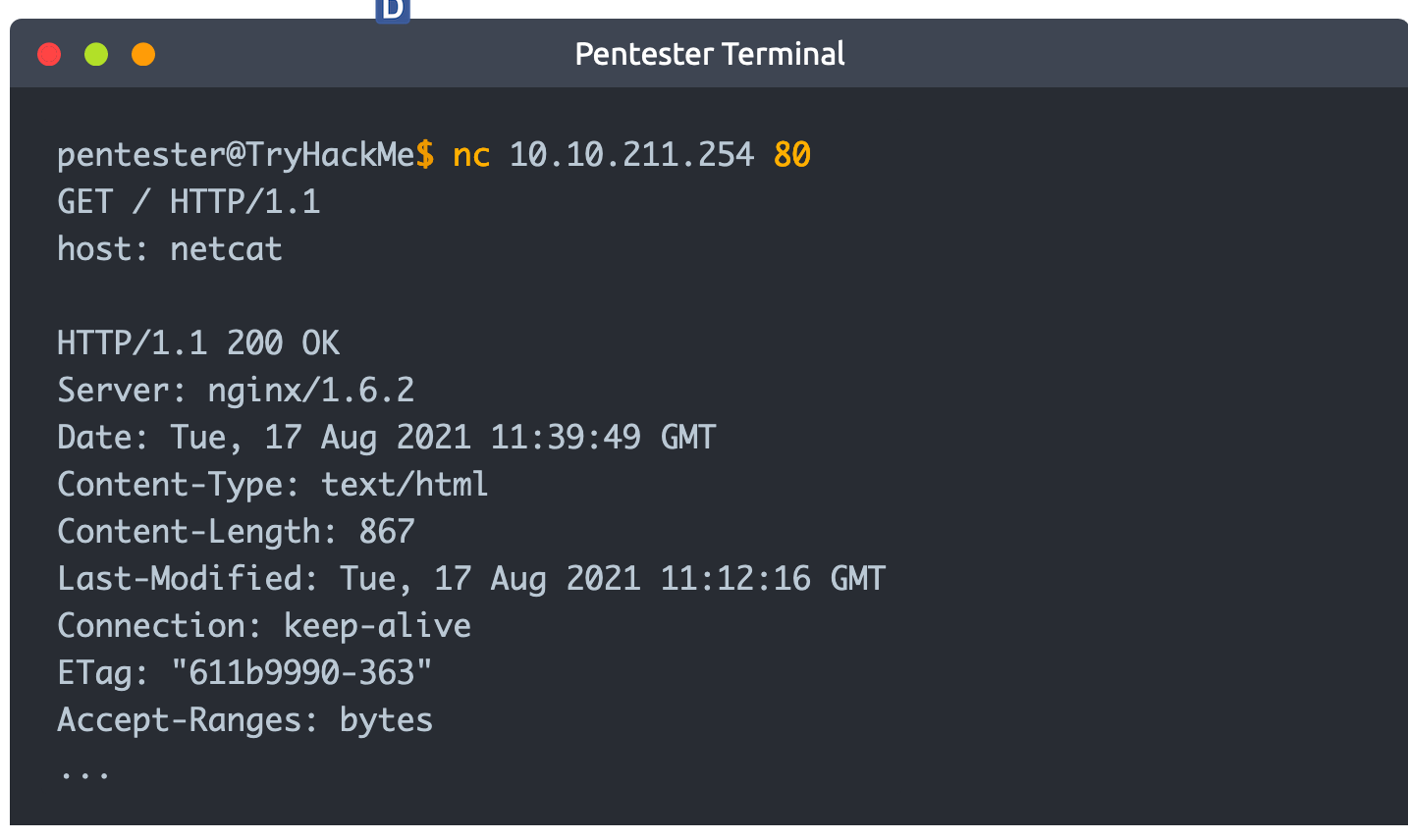
Điều thú vị là chúng ta đã khám phá loại và phiên bản của máy chủ web Server: nginx/1.6.2. Ở ví dụ này, chúng ta giao tiếp với máy chủ web. Nếu chúng ta kết nối với máy chủ mail, chúng ta cần dùng những lệnh phù hợp với giao thức như SMTP hay POP3.

**Netcat**

Netcat có nhiều ứng dụng khác nhau trong kiểm thử. Netcat hỗ trợ cả hai giao thức TCP và UDP. Nó có thể hoạt động như máy khách kết nối với cổng đang lắng nghe; ngoài ra, nó có thể hoạt động như máy chủ lắng nghe cổng bạn muốn.

Đầu tiên, bạn có thể kết nối đến 1 máy chủ, như bạn làm với telnet để thu thập banner của 1 dịch vụ bằng việc sử dụng câu lệnh sau:

nc 10.10.211.254 PORT



Trong hình trên, chúng ta dùng netcat để kết nối đến 10.10.211.254 ở cổng 80. Kế tiếp, chúng ta dùng lệnh GET để lấy trang web mặc định

Bạn có thể dùng netcat để lắng nghe cổng TCP và kết nối đến 1 cổng đang lắng nghe ở 1 hệ thống khác.

Ở máy chủ bạn có thể mở 1 cổng và lắng nghe trên đó, bạn có thể dùng nc -lp 1234 hoặc tốt hơn nc -vnlp 1234. Thứ tự chữ cái không quan trọng miễn là cổng được đặt trực tiếp với -p

| **option** | **meaning** |
| --- | --- |
| -l | Listen mode |
| -p | Specify the Port number |
| -n | Numeric only; no resolution of hostnames via DNS |
| -v | Verbose output (optional, yet useful to discover any bugs) |
| -vv | Very Verbose (optional) |
| -k | Keep listening after client disconnects |

* Lựa chọn -p nên xuất hiện trước cổng bạn muốn lắng nghe
* Lựa chọn -n sẽ tránh tra cứu DNS và những cảnh báo
* Số cổng ít hơn 1024 yêu cầu quyền root để lắng nghe

Ở máy khách, bạn sẽ dùng nc 10.10.211.254 PORT\_NUMBER. Sau khi bạn thiết lập 1 kết nối đến máy chủ thành công, những cái bạn đánh trên máy khách sẽ được lặp lại ở phía máy chủ và ngược lại.

Xem xét 1 ví dụ sau. Trên máy chủ, chúng ta sẽ lắng nghe cổng 1234. Máy chủ có địa chỉ IP là 10.10.211.254, vì vậy chúng ta có thể kết nối đến nó từ máy khách bằng cách thực thi nc 10.10.211.254 1234.