ACTIVE RECONNAISSANCE

1. Introduction

- Trong căn phòng thứ hai này, chúng tôi tập trung vào hoạt động **active reconnaissance** và các công cụ thiết yếu liên quan đến nó. Chúng tôi học cách sử dụng trình duyệt web để thu thập thêm thông tin về mục tiêu của chúng tôi. Ngoài ra, chúng tôi thảo luận về việc sử dụng các công cụ đơn giản như **ping**, **traceroute, telnet** và **nc** để thu thập thông tin về mạng, hệ thống và dịch vụ.

- Như chúng ta đã học trong phòng trước**, passive reconnaissance** cho phép bạn thu thập thông tin về mục tiêu của mình mà không cần bất kỳ hình thức tương tác hoặc kết nối trực tiếp nào. Bạn đang xem từ xa hoặc kiểm tra thông tin có sẵn công khai.

- **Active reconnaissance** yêu cầu bạn thực hiện một số hình thức liên lạc với mục tiêu của mình. Liên hệ này có thể là một phần của kỹ thuật xã hội. Ngoài ra, đó có thể là kết nối trực tiếp đến hệ thống đích, cho dù truy cập trang web của họ hay kiểm tra xem tường lửa của họ có mở cổng SSH hay không. Hãy nghĩ về nó giống như bạn đang kiểm tra chặt chẽ các cửa sổ và khóa cửa. Do đó, điều cần thiết là phải nhớ không tham gia vào công việc **active reconnaissance** trước khi nhận được sự ủy quyền hợp pháp có chữ ký từ khách hàng.

- Active bắt đầu bằng các kết nối trực tiếp được thực hiện với máy mục tiêu. Bất kỳ kết nối nào như vậy có thể để lại thông tin trong nhật ký hiển thị địa chỉ IP của máy khách, thời gian kết nối và thời lượng kết nối, cùng những thông tin khác. Tuy nhiên, không phải tất cả các kết nối đều đáng ngờ. Có thể để hoạt động do thám tích cực của bạn xuất hiện dưới dạng hoạt động của khách hàng thông thường. Xem xét duyệt web không ai có thể nghi ngờ một trình duyệt được kết nối với máy chủ web mục tiêu trong số hàng trăm người dùng hợp pháp khác.

2. Web Browser

- Trình duyệt web có thể là một công cụ tiện lợi, đặc biệt là nó có sẵn trên tất cả các hệ thống. Có một số cách mà bạn có thể sử dụng trình duyệt web để thu thập thông tin về mục tiêu.

- Ở cấp độ truyền tải, trình duyệt kết nối với:

+ Cổng TCP 80 theo mặc định khi trang web được truy cập qua HTTP

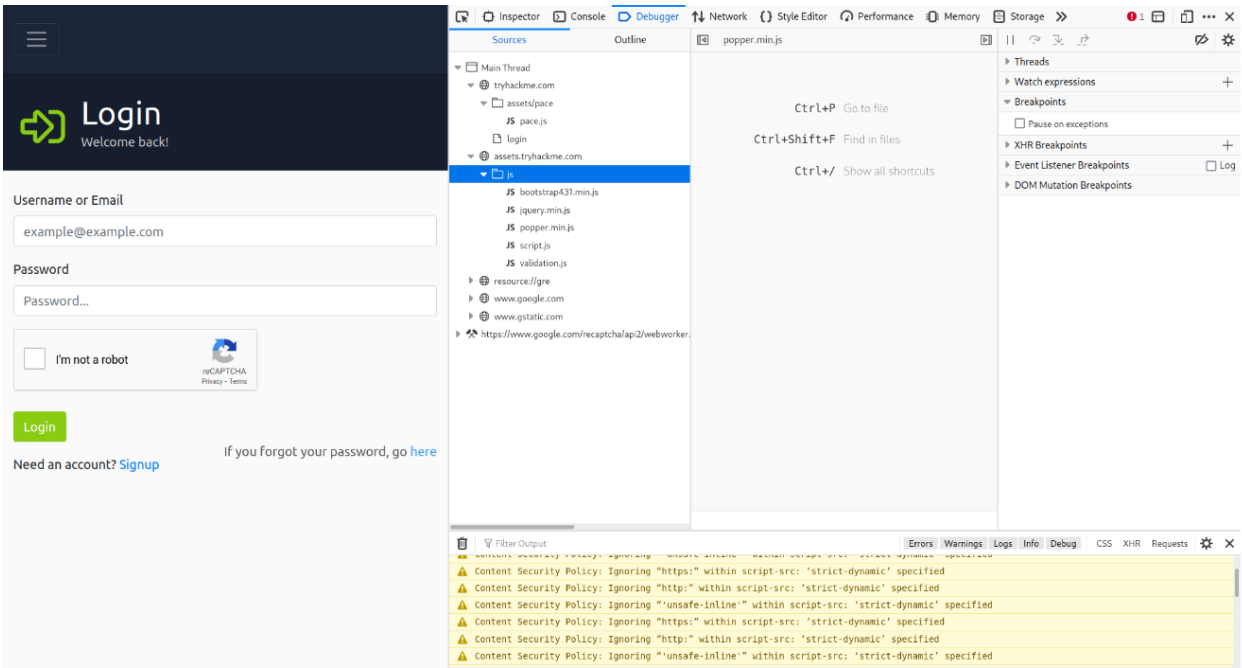
+ Cổng TCP 443 theo mặc định khi trang web được truy cập qua HTTPS

+ Vì 80 và 443 là các cổng mặc định cho HTTP và HTTPS nên trình duyệt web không hiển thị chúng trên thanh địa chỉ. Tuy nhiên, có thể sử dụng các cổng tùy chỉnh để truy cập một dịch vụ. Chẳng hạn, https://127.0.0.1:8834/ sẽ kết nối với 127.0.0.1 (localhost) tại cổng 8834 thông qua giao thức HTTPS. Nếu có một máy chủ HTTPS lắng nghe trên cổng đó, chúng tôi sẽ nhận được một trang web.

- Trong khi duyệt trang web, bạn có thể nhấn Ctrl+Shift+I trên PC hoặc Option + Command + I (⌥ + ⌘ + I) trên máy Mac để mở công cụ dành cho nhà phát triển trên Firefox. Các phím tắt tương tự cũng sẽ giúp bạn bắt đầu với Google Chrome hoặc Chromium. Công cụ dành cho nhà phát triển cho phép bạn kiểm tra nhiều thứ mà trình duyệt của bạn

đã nhận và trao đổi với máy chủ từ xa. Chẳng hạn, bạn có thể xem và thậm chí sửa đổi các tệp JavaScript (JS), kiểm tra cookie được đặt trên hệ thống của bạn và khám phá cấu trúc thư mục của nội dung trang web.

- Dưới đây là ảnh chụp màn hình của Firefox Developer Tools. Chrome DevTools khá giống nhau.

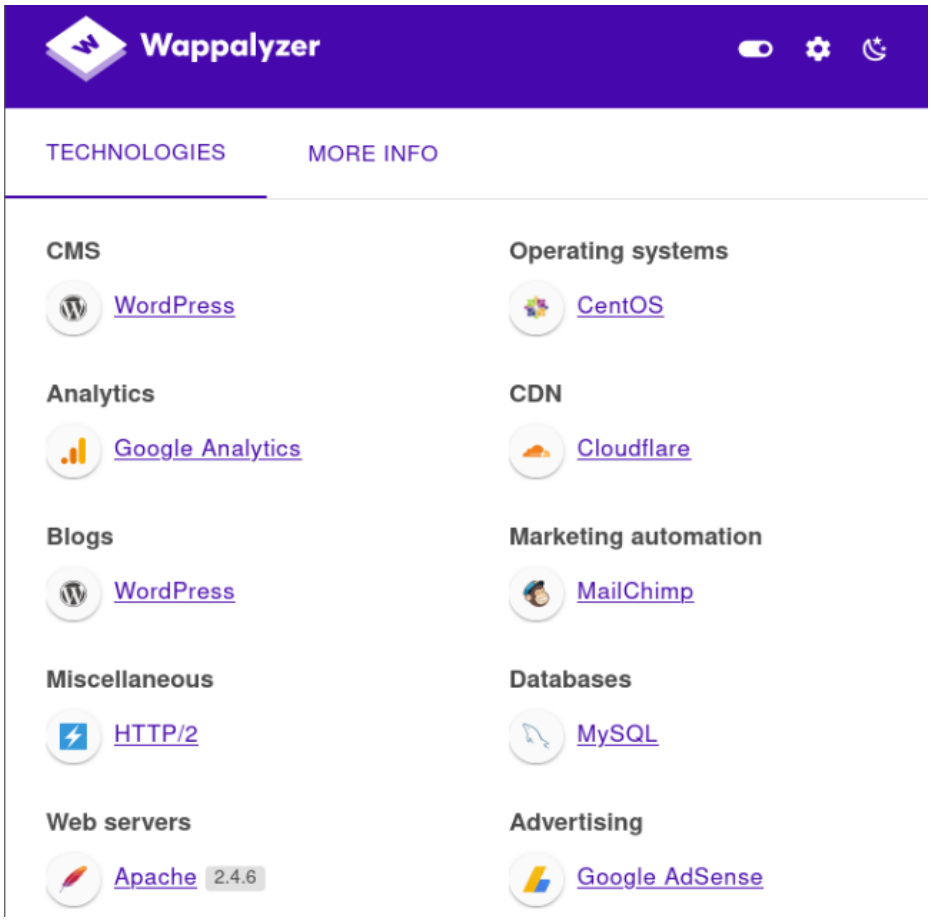


- Ngoài ra còn có rất nhiều tiện ích bổ sung dành cho Firefox và Chrome có thể giúp kiểm tra thâm nhập. Dưới đây là một vài ví dụ:

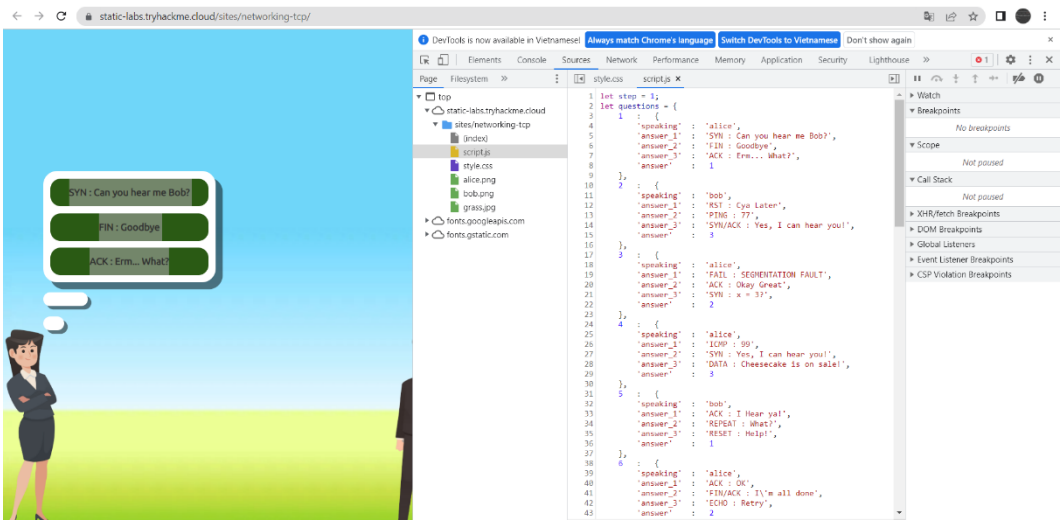
• **FoxyProxy**: cho phép bạn nhanh chóng thay đổi máy chủ proxy mà bạn đang sử dụng để truy cập trang web mục tiêu. Tiện ích mở rộng trình duyệt này thuận tiện khi bạn đang sử dụng một công cụ như Burp Suite hoặc nếu bạn cần chuyển đổi máy chủ proxy thường xuyên. Bạn có thể tải FoxyProxy cho Firefox từ đây.

• **User-Agent Switcher and Manager**: cung cấp cho bạn khả năng giả vờ rằng bạn đang truy cập trang web từ một hệ điều hành khác hoặc trình duyệt web khác. Nói cách khác, bạn có thể giả vờ đang duyệt một trang web bằng iPhone trong khi thực tế, bạn đang truy cập trang đó từ Mozilla Firefox. Bạn có thể tải xuống nó cho Firefox tại đây.

• **Wappalyzer**: cung cấp thông tin chi tiết về các công nghệ được sử dụng trên các trang web đã truy cập. Tiện ích mở rộng như vậy rất tiện dụng, chủ yếu khi bạn thu thập tất cả thông tin này trong khi duyệt trang web giống như bất kỳ người dùng nào khác. Ảnh chụp màn hình của Wappalyzer được hiển thị bên dưới. Bạn có thể tìm Wappalyzer cho Firefox tại đây.



➔ Nhìn thông tin hình ảnh trả về của Wappalyzer ta có thể thu thập được một vài thông tin rất hữu ích như trang web đang sử dụng hệ thống quản lí nội dung là WordPress, nhà phân phối mạng phân phối nội dung là Cloudflare, hệ quản trị cơ sở dữ liệu là MySQL.



3. Ping

- Ping sẽ nhắc bạn về trò chơi ping-pong (bóng bàn). Bạn ném bóng và mong lấy lại được. Mục đích chính của ping là kiểm tra xem bạn có thể kết nối với hệ thống từ xa hay không và hệ thống từ xa có thể liên hệ lại với bạn hay không. Nói cách khác, ban đầu, điều này được sử dụng để kiểm tra kết nối mạng; tuy nhiên, chúng tôi quan tâm nhiều hơn đến các mục đích sử dụng khác nhau của nó: kiểm tra xem hệ thống từ xa có trực tuyến hay không.

Nói một cách đơn giản, lệnh ping sẽ gửi một gói đến một hệ thống từ xa và hệ thống từ xa sẽ trả lời. Bằng cách này, bạn có thể kết luận rằng hệ thống từ xa đang trực tuyến và mạng đang hoạt động giữa hai hệ thống.

- Nếu bạn thích một định nghĩa cầu kỳ hơn, ping là một lệnh gửi gói ICMP Echo đến một hệ thống từ xa. Nếu hệ thống từ xa đang trực tuyến và gói ping được định tuyến chính xác và không bị chặn bởi bất kỳ tường lửa nào, thì hệ thống từ xa sẽ gửi lại ICMP Echo Reply. Tương tự, phản hồi ping sẽ đến được hệ thống đầu tiên nếu được định tuyến phù hợp và không bị chặn bởi bất kỳ tường lửa nào.

- Mục tiêu của một lệnh như vậy là để đảm bảo rằng hệ thống đích đang trực tuyến trước khi chúng tôi dành thời gian thực hiện các lần quét chi tiết hơn để khám phá hệ điều hành và các dịch vụ đang chạy.

- Trên thiết bị đầu cuối AttackBox của bạn, bạn có thể bắt đầu sử dụng ping như **ping MACHINE_IP** hoặc **ping HOSTNAME**. Sau này, hệ thống cần phân giải HOSTNAME thành địa chỉ IP trước khi gửi gói ping. Nếu bạn không chỉ định số đếm trên hệ thống Linux, bạn sẽ cần nhấn CTRL+C để buộc hệ thống dừng lại. Do đó, bạn có thể xem xét ping -c 10 MACHINE_IP nếu bạn chỉ muốn gửi mười gói. Điều này tương đương với ping -n 10 MACHINE_IP trên hệ thống MS Windows.

- Về mặt kỹ thuật, ping thuộc giao thức ICMP (Internet Control Message Protocol). ICMP hỗ trợ nhiều loại truy vấn, nhưng đặc biệt, chúng tôi quan tâm đến ping (ICMP echo/type 8) và ping reply (ICMP echo reply/type 0). Không bắt buộc phải truy cập chi tiết ICMP để sử dụng ping.

- Trong ví dụ sau, chúng tôi đã chỉ định tổng số gói tin là 5. Từ thiết bị đầu cuối của AttackBox, chúng tôi bắt đầu ping MACHINE_IP. Chúng tôi đã biết rằng MACHINE_IP đã hoạt động và không chặn các **Echo ICMP Requests**. Ngoài ra, bất kỳ tường lửa và bộ định tuyến nào trên tuyến gói cũng không chặn các yêu cầu đó.

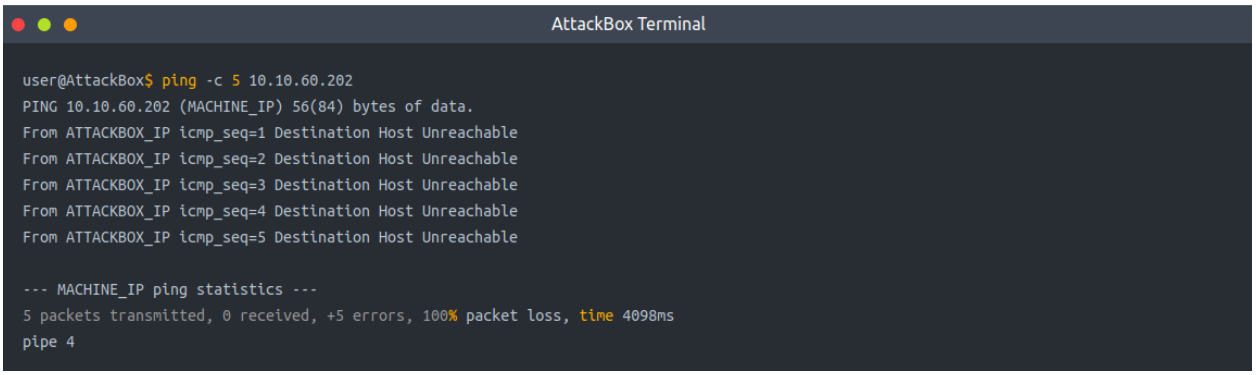
```
user@AttackBox$ ping -c 5 MACHINE_IP
PING MACHINE_IP (MACHINE_IP) 56(84) bytes of data.
64 bytes from MACHINE_IP: icmp_seq=1 ttl=64 time=0.636 ms
64 bytes from MACHINE_IP: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from MACHINE_IP: icmp_seq=3 ttl=64 time=0.396 ms
64 bytes from MACHINE_IP: icmp_seq=4 ttl=64 time=0.416 ms
64 bytes from MACHINE_IP: icmp_seq=5 ttl=64 time=0.445 ms

--- MACHINE_IP ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4097ms
rtt min/avg/max/mdev = 0.396/0.475/0.636/0.086 ms
```

-> Nhìn vào kết quả trên, lệnh ping gửi một gói dữ liệu nhỏ đến máy đích và chờ phản hồi. Đầu ra hiển thị kích thước của gói được gửi (56 byte), số byte nhận được trong phản hồi (84 byte) và thời gian khứ hồi (tính bằng mili giây) cho mỗi gói được gửi và nhận.

Trong trường hợp này, đầu ra cho thấy máy đích (MACHINE_IP) đã phản hồi từng gói trong số năm gói được gửi, với thời gian khứ hồi nằm trong khoảng từ 0,396 đến 0,636 mili giây. Điều này cho thấy kết nối mạng giữa hai máy đang hoạt động tốt và thời gian phản hồi rất nhanh.

- Từ quan điểm thử nghiệm thâm nhập, chúng tôi sẽ cố gắng khám phá thêm về mục tiêu này. Chúng tôi sẽ cố gắng tìm hiểu càng nhiều càng tốt, chẳng hạn như cổng nào đang mở và dịch vụ nào đang chạy.

- Hãy xem xét trường hợp sau: chúng tôi tắt máy ảo mục tiêu và sau đó thử ping 10.10.60.202. Như bạn mong đợi trong ví dụ sau, chúng tôi không nhận được bất kỳ phản hồi nào.



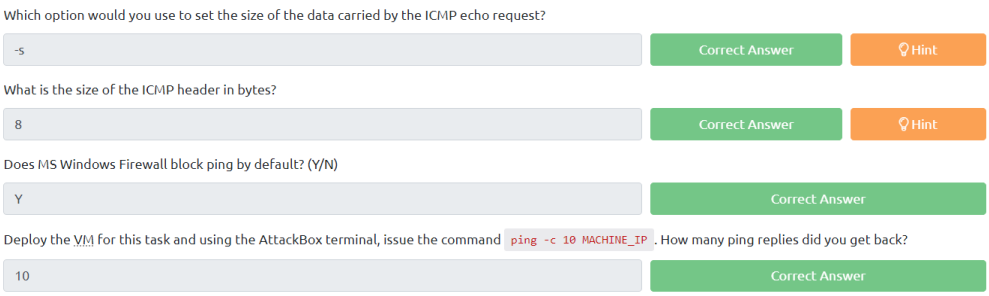
- Ở đây chúng ta đã tắt máy tính mục tiêu có ip 10.10.60.202, đối với mỗi lần gửi tin ta đều nhận được phản hồi “Destination Host Unreachable”. Chúng tôi có thể thấy rằng chúng tôi đã truyền năm gói nhưng không nhận được gói nào, dẫn đến mất gói 100%. Nói chung, khi chúng tôi không nhận được phản hồi ping, có một số giải thích có thể giải thích tại sao chúng tôi không nhận được phản hồi ping, ví dụ:

+ Máy tính đích không phản hồi có thể vẫn khởi động nhưng đang bị tắt, hoặc hệ điều hành đã bị hỏng.

+ Nó bị rút khỏi mạng hoặc có một thiết bị mạng bị lỗi trên đường dẫn.

+ Tường lửa được cấu hình để chặn các gói như vậy. Tường lửa có thể là một phần mềm chạy trên chính hệ thống hoặc một thiết bị mạng riêng biệt. Lưu ý rằng tường lửa MS Windows chặn ping theo mặc định.

+ Hệ thống của bạn đã được rút phích cắm khỏi mạng.

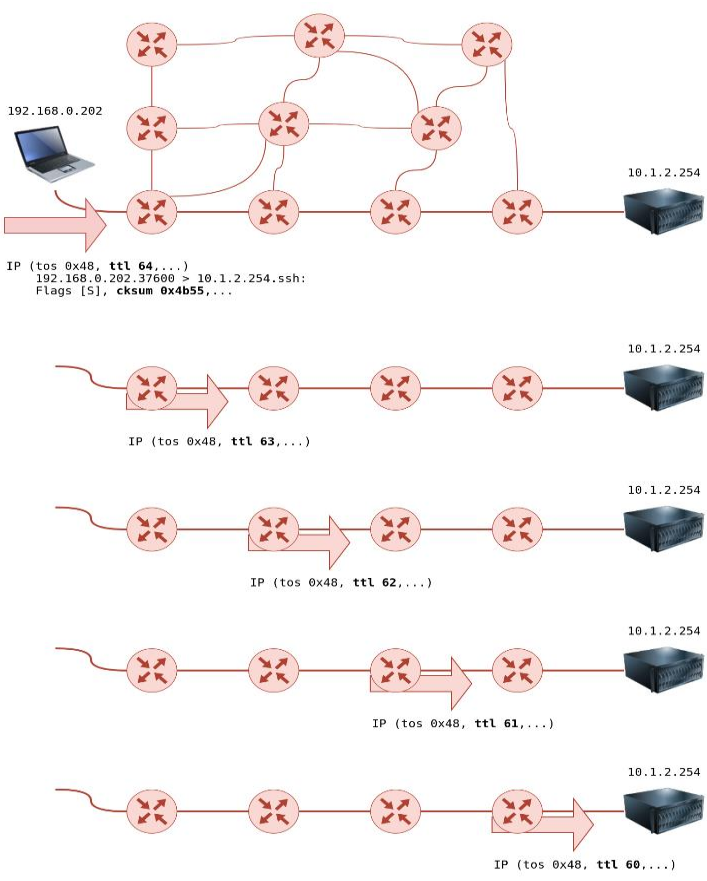


4. Traceroute

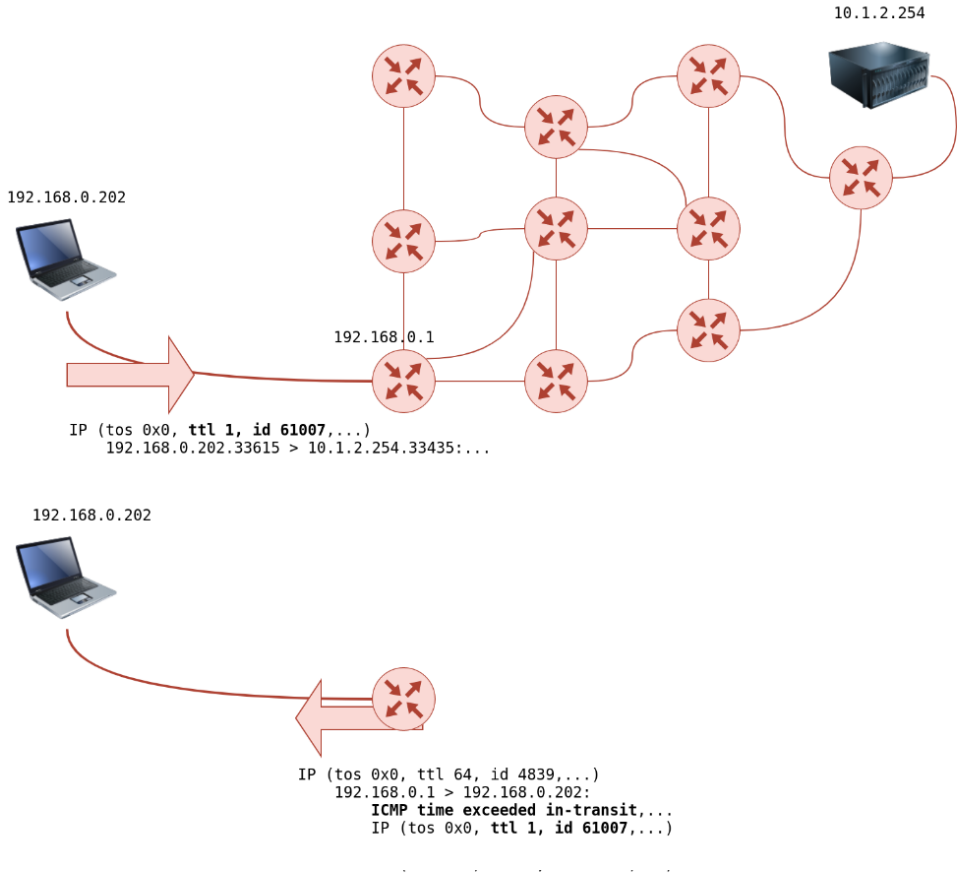
- Như tên gợi ý, lệnh theo dõi tuyến đường được thực hiện bởi các gói từ hệ thống của bạn đến máy chủ khác. Mục đích của theo dõi là tìm địa chỉ IP của bộ định tuyến hoặc bước nhảy mà gói đi qua khi nó đi từ hệ thống của bạn đến máy chủ đích. Lệnh này cũng tiết lộ số lượng bộ định tuyến giữa hai hệ thống. Nó rất hữu ích vì nó cho biết số bước nhảy (bộ định tuyến) giữa hệ thống của bạn và máy chủ đích. Tuy nhiên, lưu ý rằng đường đi của các gói có thể thay đổi vì nhiều bộ định tuyến sử dụng các giao thức định tuyến động thích ứng với các thay đổi của mạng.

- Trên Linux và macOS, lệnh sử dụng là tracerroute MACHINE_IP và trên MS Windows, đó là tracert MACHINE_IP. Traceroute cố gắng khám phá các bộ định tuyến trên đường dẫn từ hệ thống của bạn đến hệ thống đích.

- Không có cách nào trực tiếp để khám phá đường dẫn từ hệ thống của bạn đến hệ thống mục tiêu. Chúng tôi dựa vào ICMP để "lừa" các bộ định tuyến tiết lộ địa chỉ IP của chúng. Chúng ta có thể thực hiện điều này bằng cách sử dụng một Time To Live (TTL) nhỏ trong trường tiêu đề IP. Mặc dù T trong TTL là viết tắt của thời gian, nhưng TTL cho biết số lượng bộ định tuyến/bước nhảy tối đa mà một gói có thể đi qua trước khi bị loại bỏ; TTL không phải là số đơn vị thời gian tối đa. Khi một bộ định tuyến nhận được một gói, nó sẽ giảm TTL xuống một trước khi chuyển nó đến bộ định tuyến tiếp theo. Hình dưới đây cho thấy mỗi khi gói IP đi qua một bộ định tuyến, giá trị TTL của nó giảm đi 1. Ban đầu, nó rời khỏi hệ thống với giá trị TTL là 64; nó đến hệ thống đích với giá trị TTL là 60 sau khi đi qua 4 bộ định tuyến.



- Tuy nhiên, nếu TTL đạt đến 0, nó sẽ bị hủy và ICMP Time-to-Live vượt quá sẽ được gửi đến người gửi ban đầu. Trong hình dưới đây, hệ thống đặt TTL thành 1 trước khi gửi đến bộ định tuyến. Bộ định tuyến đầu tiên trên đường dẫn giảm TTL đi 1, dẫn đến TTL bằng 0. Do đó, bộ định tuyến này sẽ loại bỏ gói và gửi thông báo lỗi quá trình truyền quá thời gian ICMP. Lưu ý rằng một số bộ định tuyến được cấu hình để không gửi các thông báo ICMP như vậy khi loại bỏ một gói.



- Trên Linux, traceroute sẽ bắt đầu bằng cách gửi các gói dữ liệu UDP trong các gói IP có TTL là 1. Do đó, nó khiến bộ định tuyến đầu tiên gặp TTL=0 và gửi ngược lại ICMP Time-to-Live đã vượt quá. Do đó, TTL bằng 1 sẽ tiết lộ địa chỉ IP của bộ định tuyến đầu tiên cho bạn. Sau đó, nó sẽ gửi một gói khác với TTL=2; gói này sẽ bị loại bỏ ở bộ định tuyến thứ hai. Và như thế. Hãy thử điều này trên các hệ thống trực tiếp.

- Trong các ví dụ sau, chúng tôi chạy cùng một lệnh, theo dõi tryhackme.com từ AttackBox của TryHackMe. Chúng tôi nhận thấy rằng các lần chạy khác nhau có thể dẫn đến các tuyến đường khác nhau được thực hiện bởi các gói.

- Traceroute A:

```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
 1  ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5)  2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com
(3.248.240.13)  7.468 ms
 2  100.66.8.86 (100.66.8.86)  43.231 ms 100.65.21.64 (100.65.21.64)  18.886 ms 100.65.22.160 (100.65.22.160)  14.556 ms
 3  * 100.66.16.176 (100.66.16.176)  8.006 ms *
 4  100.66.11.34 (100.66.11.34)  17.401 ms 100.66.10.14 (100.66.10.14)  23.614 ms 100.66.19.236 (100.66.19.236)  17.524 ms
 5  100.66.7.35 (100.66.7.35)  12.808 ms 100.66.6.109 (100.66.6.109)  14.791 ms *
 6  100.65.14.131 (100.65.14.131)  1.026 ms 100.66.5.189 (100.66.5.189)  19.246 ms 100.66.5.243 (100.66.5.243)  19.805 ms
 7  100.65.13.143 (100.65.13.143)  14.254 ms 100.95.18.131 (100.95.18.131)  0.944 ms 100.95.18.129 (100.95.18.129)  0.778 ms
 8  100.95.2.143 (100.95.2.143)  0.680 ms 100.100.4.46 (100.100.4.46)  1.392 ms 100.95.18.143 (100.95.18.143)  0.878 ms
 9  100.100.20.76 (100.100.20.76)  7.819 ms 100.92.11.36 (100.92.11.36)  18.669 ms 100.100.20.26 (100.100.20.26)  0.842 ms
10  100.92.11.112 (100.92.11.112)  17.852 ms * 100.92.11.158 (100.92.11.158)  16.687 ms
11  100.92.211.82 (100.92.211.82)  19.713 ms 100.92.0.126 (100.92.0.126)  18.603 ms 52.93.112.182 (52.93.112.182)  17.738 ms
12  99.83.69.207 (99.83.69.207)  17.603 ms  15.827 ms  17.351 ms
13  100.92.9.83 (100.92.9.83)  17.894 ms 100.92.79.136 (100.92.79.136)  21.250 ms 100.92.9.118 (100.92.9.118)  18.166 ms
14  172.67.69.208 (172.67.69.208)  17.976 ms  16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms
```

- Trong đầu ra theo dõi ở trên, chúng tôi có 14 dòng được đánh số, mỗi dòng đại diện cho một bộ định tuyến/hop. Hệ thống của chúng tôi sẽ gửi ba gói có TTL được đặt thành 1, sau đó ba gói có TTL được đặt thành 2, v.v. Tùy thuộc vào cấu trúc liên kết mạng, chúng tôi có thể nhận được phản hồi từ tối đa 3 bộ định tuyến khác nhau, tùy thuộc vào tuyến đường mà gói tin thực hiện. Xem xét dòng số 12, bộ định tuyến thứ mười hai có địa chỉ IP được liệt kê đã bỏ gói ba lần và gửi một thông báo quá thời gian ICMP trong quá trình chuyển tiếp. Dòng 12 99.83.69.207 (99.83.69.207) 17.603 ms 15.827 ms 17.351 ms hiển thị thời gian tính bằng mili giây để mỗi câu trả lời đến được hệ thống của chúng tôi.

- Mặt khác, chúng ta có thể thấy rằng chúng ta chỉ nhận được một câu trả lời duy nhất ở dòng thứ ba. Hai dấu sao trong đầu ra 3 * 100.66.16.176 (100.66.16.176) 8.006 ms * cho biết hệ thống của chúng tôi không nhận được hai thông báo vượt quá thời gian ICMP dự kiến trong quá trình truyền.

- Cuối cùng, trong dòng đầu tiên của kết quả, chúng ta có thể thấy rằng các gói tin rời khỏi AttackBox có các tuyến đường khác nhau. Chúng ta có thể thấy hai bộ định tuyến phản hồi TTL là một. Hệ thống của chúng tôi chưa bao giờ nhận được thông báo ICMP dự kiến thứ ba.

-> Note lại: ICMP (Internet Control Message Protocol) là một giao thức được sử dụng bởi các thiết bị mạng, chẳng hạn như bộ định tuyến, để gửi thông báo lỗi và thông tin vận hành về tình trạng mạng. Một trong các loại thông báo ICMP là thông báo "Time-to-Live exceeded".

+ Trường Time-to-Live ,(TTL) là một giá trị trong header IP của gói giới hạn số bước nhảy (bộ định tuyến) tối đa mà gói có thể đi qua trước khi bị loại bỏ. Mỗi khi một gói được chuyển tiếp bởi một bộ định tuyến, trường TTL sẽ giảm đi một. Khi trường TTL về 0, gói bị loại bỏ và thông báo "Time-to-Live exceeded" của ICMP được gửi trở lại máy chủ nguồn.

+ Mục đích của trường TTL là để ngăn các gói lặp lại vô tận trong mạng. Nếu một gói bị mắc kẹt trong một vòng lặp, trường TTL cuối cùng sẽ bằng 0 và gói sẽ bị loại bỏ.

+ Tóm lại, thông báo "Time-to-Live exceeded" là thông báo ICMP được bộ định tuyến gửi đến máy chủ nguồn khi trường TTL của gói bằng 0. Nó chỉ ra rằng gói đã bị loại bỏ và giúp ngăn các gói lặp lại vô tận trong mạng.

5. Telnet

- Giao thức **TELNET** (Teletype Network) được phát triển vào năm 1969 để liên lạc với một hệ thống từ xa thông qua giao diện dòng lệnh (CLI). Do đó, lệnh telnet sử dụng giao thức TELNET để quản trị từ xa. Cổng mặc định được telnet sử dụng là 23. Từ góc độ bảo mật, telnet gửi tất cả dữ liệu, bao gồm tên người dùng và mật khẩu, ở dạng văn bản rõ ràng. Gửi ở dạng văn bản rõ ràng giúp bất kỳ ai có quyền truy cập vào kênh liên lạc dễ dàng đánh cắp thông tin đăng nhập. Giải pháp thay thế an toàn là giao thức **SSH (Secure Shell).**

- Tuy nhiên, ứng dụng khách telnet, với sự đơn giản của nó, có thể được sử dụng cho các mục đích khác. Biết rằng ứng dụng khách telnet dựa trên giao thức TCP, bạn có thể sử dụng Telnet để kết nối với bất kỳ dịch vụ nào và lấy biểu ngữ của dịch vụ đó. Sử dụng **telnet MACHINE_IP PORT**, bạn có thể kết nối với bất kỳ dịch vụ nào chạy trên TCP và thậm chí trao đổi một số tin nhắn trừ khi dịch vụ đó sử dụng mã hóa.

- Giả sử chúng ta muốn khám phá thêm thông tin về máy chủ web, nghe trên cổng 80. Chúng tôi kết nối với máy chủ ở cổng 80, sau đó chúng tôi giao tiếp bằng giao thức HTTP. Bạn không cần phải đi sâu vào giao thức HTTP, bạn chỉ cần phát hành **GET/HTTP/1.1**. Để chỉ định một cái gì đó khác với trang chỉ mục mặc định, bạn có thể đưa ra lệnh **GET /page.html HTTP/1.1**, trang này sẽ yêu cầu **page.html**. Chúng tôi cũng đã chỉ định cho máy chủ web từ xa rằng chúng tôi muốn sử dụng HTTP phiên bản 1.1 để liên lạc. Để nhận được phản hồi hợp lệ, thay vì báo lỗi, bạn cần nhập một số giá trị cho máy chủ lưu trữ như **host: example** và nhấn enter hai lần. Thực hiện các bước này sẽ cung cấp trang chỉ mục được yêu cầu.

```
pentester@TryHackMe$ telnet MACHINE_IP 80
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
GET / HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:13:25 GMT
Content-Type: text/html
Content-Length: 867
Last-Modified: Tue, 17 Aug 2021 11:12:16 GMT
Connection: keep-alive
ETag: "611b9990-363"
Accept-Ranges: bytes
```

- Mối quan tâm đặc biệt đối với chúng tôi là khám phá các loại và phiên bản của máy chủ web đã cài đặt, Máy chủ: nginx/1.6.2. Trong ví dụ này, chúng tôi đã giao tiếp với một máy chủ web, vì vậy chúng tôi đã sử dụng các lệnh HTTP

cơ bản. Nếu chúng tôi kết nối với máy chủ thư, chúng tôi cần sử dụng các lệnh thích hợp dựa trên giao thức, chẳng hạn như SMTP và POP3.

- Note thêm: **SSH (Secure Shell)** là một giao thức mạng được sử dụng để thiết lập kết nối mạng an toàn giữa hai thiết bị, ví dụ như máy tính và máy chủ, cho phép truyền tải dữ liệu một cách bảo mật.

+ Giao thức SSH cung cấp khả năng mã hóa dữ liệu và xác thực người dùng một cách an toàn bằng cách sử dụng các thuật toán mật mã mạnh, bao gồm RSA, DSA, và ECDSA. SSH cho phép người dùng thiết lập kết nối mạng từ xa đến các thiết bị khác một cách an toàn mà không cần sử dụng các phương tiện truyền thông không bảo mật như Telnet hay FTP.

Một số ứng dụng phổ biến của SSH bao gồm:

- Truy cập từ xa đến máy tính hoặc máy chủ: SSH cho phép người dùng truy cập từ xa đến máy tính hoặc máy chủ thông qua một kết nối an toàn.
- Chuyển tệp tin qua mạng: SSH cho phép người dùng chuyển tệp tin an toàn giữa các thiết bị.
- Tạo máy chủ ảo: SSH có thể được sử dụng để tạo các máy chủ ảo trên các thiết bị.

➔ SSH là một giao thức rất quan trọng trong việc bảo vệ an ninh mạng, đặc biệt là khi truy cập từ xa vào các thiết bị như máy chủ. SSH được sử dụng rộng rãi trong các ứng dụng truyền thông an toàn, bao gồm truyền tệp tin, điều khiển từ xa, và truyền dữ liệu qua mạng.

```
┌──(kali㉿kali)-[~/Desktop/VPN_THM]
└─$ telnet 10.10.235.15 80
Trying 10.10.235.15...
Connected to 10.10.235.15.
Escape character is '^]'.
GET / HTTP/1.1
host: telnet
HTTP/1.1 408 Request Timeout
Date: Tue, 28 Feb 2023 09:00:42 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 303
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80.
What is the name of the running server?

apache — Correct Answer

What is the version of the running server (on port 80 of the VM)?

2.4.10 — Correct Answer

6. Netcat

- Netcat hoặc đơn giản là **nc** có các ứng dụng khác nhau có thể có giá trị lớn đối với một pentester. Netcat hỗ trợ cả giao thức TCP và UDP. Nó có thể hoạt động như một máy khách kết nối với cổng nghe, cách khác, nó có thể hoạt động như một máy chủ lắng nghe trên cổng bạn chọn. Do đó, nó là một công cụ thuận tiện mà bạn có thể sử dụng như một máy khách hoặc máy chủ đơn giản qua TCP hoặc UDP.

- Đầu tiên, bạn có thể kết nối với một máy chủ, như bạn đã làm với Telnet, để thu thập biểu ngữ của nó bằng cách sử dụng **nc MACHINE_IP PORT**, khá giống với **telnet MACHINE_IP PORT** trước đây của chúng tôi. Lưu ý rằng bạn có thể cần nhấn SHIFT+ENTER sau dòng GET.

- Trong thiết bị đầu cuối được hiển thị ở trên, chúng tôi đã sử dụng netcat để kết nối với cổng MACHINE_IP 80 bằng cách sử dụng nc MACHINE_IP 80. Tiếp theo, chúng tôi đã đưa ra một trang mặc định bằng cách sử dụng GET / HTTP/1.1; chúng tôi đang chỉ định cho máy chủ đích mà máy khách của chúng tôi hỗ trợ phiên bản HTTP 1.1. Cuối cùng, chúng ta cần đặt tên cho máy chủ của mình, vì vậy chúng tôi đã thêm vào một dòng mới, host: netcat; bạn có thể đặt tên cho máy chủ của mình bất cứ thứ gì vì điều này không ảnh hưởng đến bài tập này.

- Dựa trên đầu ra server: nginx/1.6.2 chúng tôi nhận được, chúng tôi có thể nói rằng trên cổng 80, chúng tôi có Nginx phiên bản 1.6.2 lắng nghe các kết nối đến.

- Bạn có thể sử dụng netcat để nghe trên cổng TCP và kết nối với cổng nghe trên hệ thống khác.

- Trên hệ thống máy chủ, nơi bạn muốn mở cổng và lắng nghe trên đó, bạn có thể ra lệnh **nc -lp 1234** hoặc tốt hơn là **nc -vnlp 1234**, tương đương với **nc -v -l -n -p 1234**, như bạn sẽ nhớ từ phòng Linux. Thứ tự chính xác của các chữ cái không quan trọng miễn là số cổng được đặt trước trực tiếp bằng -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

- Ghi chú:

+ -p sẽ xuất hiện ngay trước số cổng bạn muốn nghe.

+ -n sẽ tránh các cảnh báo và tra cứu DNS.

+ số cổng nhỏ hơn 1024 yêu cầu quyền root để nghe.

+ Về phía máy khách, bạn sẽ cấp **nc MACHINE_IP PORT_NUMBER**. Đây là một ví dụ về việc sử dụng nc để lặp lại. Sau khi bạn thiết lập thành công kết nối với máy chủ, bất kỳ nội dung nào bạn nhập ở phía máy khách sẽ được lặp lại ở phía máy chủ và ngược lại.

+ Hãy xem xét ví dụ sau. Về phía máy chủ, chúng tôi sẽ lắng nghe trên cổng 1234. Chúng tôi có thể đạt được điều này bằng lệnh **nc -vnlp 1234** (giống như **nc -lvnp 1234**). Trong trường hợp của chúng tôi, máy chủ lắng nghe có địa chỉ IP MACHINE_IP, vì vậy chúng tôi có thể kết nối với nó từ phía máy khách bằng cách thực thi nc MACHINE_IP 1234. Thiết lập này sẽ lặp lại bất kỳ nội dung nào bạn nhập ở bên này sang bên kia của đường hầm TCP. Bạn có thể tìm thấy một bản ghi của quá trình dưới đây. Lưu ý rằng máy chủ lắng nghe nằm ở bên trái màn hình.

```
┌──(kali㉿kali)-[~/Desktop/VPN_THM]
└─$ nc 10.10.78.48 21
220 debra2.thm.local FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
```

7. Summary

Command	Example
ping	`ping -c 10 MACHINE_IP` on Linux or macOS
ping	`ping -n 10 MACHINE_IP` on MS Windows
traceroute	`traceroute MACHINE_IP` on Linux or macOS
tracert	`tracert MACHINE_IP` on MS Windows
telnet	`telnet MACHINE_IP PORT_NUMBER`
netcat as client	`nc MACHINE_IP PORT_NUMBER`
netcat as server	`nc -lvnp PORT_NUMBER`