Active reconnaissance

1. **Nội dung học**

Thu thập thông tin về mạng, hệ thống và dịch vụ qua các công cụ:

* Ping
* Traceroute
* telnet
* nc

1. **Web Browser**

* Trình duyệt kết nối tới TCP port 80 khi sử dụng HTTP hoặc TCP port 443 khi sử dụng HTTPS
* Sử dụng Ctrl+Shift+I (Windows) hoặc Option + Command + I (Mac) để mở Developer Tools trên các browser
* Những tiện ích giúp pentest:
* 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 rất tiện lợi khi bạn 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 cho phép bạn giả vờ đang truy cập trang web từ một hệ điều hành khác hoặc một 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 web đó từ Mozilla Firefox. Bạn có thể tải xuống User-Agent Switcher and Manager 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 là khi bạn thu thập tất cả thông tin này trong khi duyệt trang web như bất kỳ người dùng nào khác. Ảnh chụp màn hình của Wappalyzer được hiển thị bên dưới. Bạn có thể tìm thấy Wappalyzer cho Firefox tại đây.

A screenshot of a computer

Description automatically generated

1. **Ping**

A screenshot of a computer program

Description automatically generated

1. **Traceroute**

* Trên Linux và macOS, lệnh sử dụng là traceroute 10.10.242.218, còn trên MS Windows, lệnh là tracert 10.10.242.218. traceroutecố gắng khám phá các bộ định tuyến trên đường dẫn từ hệ thống của bạn đến hệ thống mục tiêu.
* Tóm lại, chúng ta có thể nhận thấy những điều sau:
* Số lượng hop/router giữa hệ thống của bạn và hệ thống đích phụ thuộc vào thời gian bạn chạy traceroute. Không có gì đảm bảo rằng các gói tin của bạn sẽ luôn theo cùng một tuyến đường, ngay cả khi bạn ở cùng một mạng hoặc bạn lặp lại lệnh traceroute trong một thời gian ngắn.
* Một số bộ định tuyến trả về địa chỉ IP công khai. Bạn có thể kiểm tra một số bộ định tuyến này dựa trên phạm vi thử nghiệm thâm nhập dự định.
* Một số bộ định tuyến không trả lời.

1. **Telnet**

Giao thức TELNET (Teletype Network) được phát triển vào năm 1969 để giao tiếp với hệ thống từ xa thông qua giao diện dòng lệnh ( CLI ). Do đó, lệnh telnetsử dụng giao thức TELNET để quản trị từ xa. Cổng mặc định được telnet sử dụng là 23. Về mặt bảo mật, telnetgửi tất cả dữ liệu, bao gồm tên người dùng và mật khẩu, dưới dạng văn bản thuần túy. Việc gửi dưới dạng văn bản thuần túy khiến bất kỳ ai có quyền truy cập vào kênh giao tiếp đều có thể dễ dàng đánh cắp thông tin đăng nhập. Giải pháp thay thế an toàn là giao thức SSH (Secure SHell).

A computer screen shot of a computer program

Description automatically generated

1. **Netcat**

Netcat hoặc đơn giản là nccó 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 một cổng lắng nghe; hoặc có thể hoạt động như một máy chủ lắng nghe trên một cổng mà bạn lựa chọn. Do đó, nó là một công cụ tiện lợi mà bạn có thể sử dụng như một máy khách hoặc máy chủ đơn giản qua TCP hoặc UDP

1. **Putting It All Together**

Trong phòng này, chúng ta đã đề cập đến nhiều công cụ khác nhau. Thật dễ dàng để kết hợp một số công cụ trong số chúng thông qua một tập lệnh shell để xây dựng một máy quét hệ thống và mạng thô sơ. Bạn có thể sử dụng tracerouteđể lập bản đồ đường dẫn đến mục tiêu, pingđể kiểm tra xem hệ thống mục tiêu có phản hồi ICMP Echo không và telnetđể kiểm tra xem cổng nào đang mở và có thể truy cập được bằng cách cố gắng kết nối với chúng. Các máy quét có sẵn thực hiện việc này ở các cấp độ tiên tiến và tinh vi hơn nhiều, như chúng ta sẽ thấy trong bốn phòng tiếp theo với nmap.

| **Command** | **Example** |
| --- | --- |
| ping | **ping -c 10 10.10.55.45** on Linux or macOS |
| ping | **ping -n 10 10.10.55.45** on MS Windows |
| traceroute | **traceroute 10.10.55.45** on Linux or macOS |
| tracert | **tracert 10.10.55.45** on MS Windows |
| telnet | **telnet 10.10.55.45 PORT\_NUMBER** |
| netcat as client | **nc 10.10.55.45 PORT\_NUMBER** |
| netcat as server | **nc -lvnp PORT\_NUMBER** |

Mặc dù đây là những công cụ cơ bản, nhưng chúng có sẵn trên hầu hết các hệ thống. Đặc biệt, trình duyệt web được cài đặt trên hầu hết mọi máy tính và điện thoại thông minh và có thể là công cụ thiết yếu trong kho vũ khí của bạn để tiến hành trinh sát mà không gây báo động. Nếu bạn muốn có thêm kiến ​​thức sâu sắc về Công cụ dành cho nhà phát triển, chúng tôi khuyên bạn nên tham gia Walking An Application .

| **Hệ điều hành** | **Phím tắt Công cụ dành cho nhà phát triển** |
| --- | --- |
| Linux hoặc MS Windows | **Ctrl+Shift+I** |
| macOS | **Option + Command + I** |