*Reconnaissance*

“Biết địch, biết ta. Trăm trận, trăm thắng”. Khi muốn khai thác hoặc tấn công vào một trang web hay server(target) thì điều đầu tiên chúng ta cần là thu thập thông tin về mục tiêu. Càng nhiều thông tin chúng ta có được, khả năng khai thác thành công càng cao. Reconnaissance (recon) được định nghĩa là thu thập hoặc quan sát mục tiêu mà không cảnh báo cho họ về hoạt động của chúng ta. Mục tiêu của chúng ta sẽ bao gồm:

* Phát hiện subdomains có liên quan đến target.
* Thu thập thông tin được công khai về host và địa chỉ IP
* Tìm kiếm địa chỉ email của target.
* Phát hiện thông tin đăng nhập và mật khẩu bị rò rỉ.
* Định vị các tài liệu và thông tin bảo mật bị rò rỉ.

Recon có thể được chia thành 2 phần – passive recon và active recon. Lưu ý: active recon có thể sẽ hơi “ồn ào” và khả năng cao chúng ta sẽ bị chặn trong quá trình khai thác.

Chúng ta sẽ đi sâu hơn về kĩ thuật thu thập thông tin (recon):

**Passive recon:** Với phương pháp này, chúng ta không cần tương tác với mục tiêu. Thay vào đó chúng ta dựa vào những thông tin có sẵn công khai được thu thập và duy trì bởi một bên thứ 3. Open Source Intelligence (OSINT) được sử dụng để thu thập thông tin và xem như hồ sơ truyền thông xã hội có sẵn công khai của mục tiêu. Thông tin ví dụ mà chúng ta có thể thu thập bao gồm tên miền, khối địa chỉ IP, địa chỉ email, tên nhân viên và bài đăng công việc, bla bla… Một số tools giúp bạn thu thập thông tin của target:

- whois: Thu thập nhà đăng kí server, nhà đăng kí URL, ngày tạo, ngày update, thông tin và địa chỉ đăng kí ( trừ khi có chính sách bảo mật sẽ không được public), thông tin liên hệ và địa chỉ admin (trừ khi được giữ lại vì vấn đề bảo mật ), thông tin và địa chỉ công nghệ (như 2 ông trước đó :))) )

- nslookup: Sử dụng default DNS server để lấy địa chỉ ipv4 và ipv6 liên quan đến tên miền của target.

- dig: Giống như nslookup nhưng dig cung cấp nhiều tùy chọn truy vấn và thậm chí cho phép chúng ta chỉ định một máy chủ DNS khác nhau để sử dụng.

- host: Một tools khác để lấy Ipv4 và Ipv6 của target.

- Shodan.io: Shodan.io thu thập thông tin liên quan đến bất kỳ thiết bị nào mà nó có thể tìm thấy được kết nối trực tuyến.

- Google advanced search: sử dụng một số thủ thuật nâng cao của google để có được đầu ra mong muốn. Google cung cấp giao diện web cho các tìm kiếm nâng cao, bạn có thể tham khảo tại đây <https://www.google.com/advanced_search> ( không có virus mô đừng lo :))) ).

**Active recon:** Trái ngược với passvie recon, chúng ta sẽ cần phải tương tác với target thông qua gửi request hoặc packets và quan sát responds. Các phản hồi được thu thập – or phản hồi bị thiếu có thể mở rộng thêm bức tranh mà chúng ta phát hiện ở Passive recon. Một số thông tin chúng ta muốn tìm kiếm bao gồm máy chủ hiện hành, servers, version,….Một số tools hỗ trợ bạn:

-Web browser: Đôi khi chúng ta sẽ tìm thấy vài điều thú vị khi đọc source code của một web, có thể là dev quên xóa những comment có chứa thông tin nhạy cảm hoặc các file, bla bla. Ngoài ra chúng ta có thể cài các extension để thu thập thông tin. Wappalyzer là một tool được sử dụng rất nhiều. Nó có thể thu thập OS, databases, web server đang chạy, bla bla.

- traceroute (Unix system)/ tracert (Window system): nó theo dõi tuyến đường thực hiện bởi các gói từ hệ thống của chúng ta đến máy chủ đích.

- nmap: Đây có thể là tool được dùng nhiều nhất. Nmap có thể thu thập được dịch vụ nào đang chạy ở port nào, version, hệ điều hành. Nmap thậm chí có thể chèn script để khai thác nếu lỗ hỏng đó có tồn tại ở phía target.

Và còn rất nhiều tools nữa hỗ trợ bạn trong quá trình thu thập thông tin, việc của bạn là tìm hiểu các hoạt động và làm quen với nó. Hãy nhớ rằng, càng nhiều thông tin bạn thu thập được, khả năng khai thác lỗi của bạn càng cao. Vì vậy đừng bỏ qua bước recon này nhé, hãy take note thật nhiều, và kiên nhẫn vì đôi khi nó có thể mất của bạn hàng giờ, thậm chí cả ngày.

Bài viết đến đây cũng dài rồi, cảm ơn bạn nếu bạn kiên nhẫn đọc hết đến đây. Hi vọng với series này sẽ cho bạn cái nhìn tổng quát về ngành ATTT. Hẹn gặp lại các bạn vào một bài viết khác.

“Information and patience are key”.

“Stay secure, stay vigilant”.

T.