|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **KHOA CÔNG NGHỆ THÔNG TIN 1** |
|  |
| **BÀI THỰC HÀNH 14**  **THỰC TẬP CƠ SỞ** |
| **Họ và tên : Đinh Quang Hiếu**  **Mã sinh viên: B19DCAT065**  **Giảng viên giảng dạy: Hoàng Xuân Dậu** |
| **HÀ NỘI, THÁNG 5/2022** |

**Bài 14: Phát hiện lỗ hổng với công cụ tìm kiếm**

**I. Lý thuyết**

**1.Shodan**

Shodan là một công cụ tìm kiếm khác nhiều so với các công cụ tìm kiếm nội dung như Google, Yahoo hoặc Bing. Shodan là một công cụ tìm kiếm để tìm các thiết bị trực tuyến trên internet như: máy tính, server, webcam, các thiết bị routers... Nó hoạt động bằng cách quét toàn bộ các các thiết bị trên internet có mở cổng public ra internet và thực hiện phân tích các dấu hiệu được phản hồi về từ các thiết bị. Sử dụng thông tin đó, Shodan có thể cho bạn biết những thứ như máy chủ web (và phiên bản) nào phổ biến nhất hoặc có bao nhiêu máy chủ FTP ẩn danh tồn tại ở một vị trí cụ thể, hay trả về danh sách các camera có thể truy cập trực tuyến qua internet. Nói chung, với shodan bạn có thể tìm kiếm bất cứ thiết bị nào trên internet miễn là chúng đang có kết nối internet và mở cổng public.

- Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:

* Tạo một địa chỉ IPv4 (IPV4 là gì) một cách ngẫu nhiên.
* Chọn port (cổng dịch vụ) ngẫu nhiên và thực hiện gửi câu lệnh kiểm tra
* Xem nội dung phản hồi của thiết bị (Service Banner) từ đó xác định xem đó là loại thiết bị gì và chạy cổng gì
* Lặp lại quá trình trên nhưng với ip và port mới. Điều này giúp tạo ra sự ngẫu nhiên cũng như đảm bảo tránh gây ra lượng kết nối quá lớn tới một thiết bị một cách liên tục.

Các cổng dịch vụ mà shodan thường xuyên rà quét: (Port 554 – Real Time Streaming Protocol, Port 5060 – SIP, Port 25 – SMTP, Port 161 – SNMP, Port 23 - Telnet, Port 993 – IMAP, Port 22 – SSH, Port 21 – FTP, Ports 8443, 443, 8080, and 80 – HTTPS/HTTP)

**2. Google hacking**

Google Hacking là một thuật ngữ mà gói gọn một loạt các kĩ thuật cho phép truy vấn trên công cụ tìm kiếm Google.com, đôi khi được dùng để xác định các lổ hổng trong các ứng dụng web cụ thể.(Cụ thể như thế nào thì mình sẽ cố gắng giải thích tiếp trong giới hạn kiến thức mà mình biết). Bên cạnh việc truy vấn từ google có thể tiết lộ các lỗ hổng trong các ứng dụng web, Google Hacking cho phép bạn tìm các dữ liệu nhạy cảm, có ích cho giai đoạn Reconnaissance để attack ứng dụng, chẳng hạn như email liên kết với một trang web nào đó, cơ sở dữ liệu hoặc các file khác với tên người dùng và mật khẩu, các thư mục không được bảo vệ với các tập tin nhạy cảm, URL để đăng nhập cổng thông tin, các loại khác nhau của các bản ghi hệ thống như tường lửa và truy cập các bản ghi.…

- Google hacking database chia thành nhiều loại khác nhau như: thông tin các file bị tổn thương, các file chứa mật khẩu, thông tin về máy chủ và phần mềm trên đó, tìm kiếm các thiết bị trực tuyến...etc. Một Dork chỉ là một truy vấn Google đã tìm ra kết quả hữu ích như khai thác dữ liệu nhạy cảm. Khi duyệt qua các kết quả, bạn nên tham khảo đến thời gian update hoặc thời gian được lữu trữ, Google hỗ trợ điều đó rất tốt từ các kết quả mà nó mang lại cho bạn. Một vài kết quả từ lâu sẽ bao gồm là các thông tin phiên bản ứng dụng gặp lỗi, lỗi ứng dụng code,…

- Hiện tại chúng tôi ngày càng có nhiều IOT Thiết bị (Internet of Things), tự động hóa gia đình và nhiều hơn nữa được kết nối với Internet. Vấn đề mà họ gặp phải là chúng bị xử lý bởi những người không có đủ kiến thức hoặc thiết bị này không được trang bị các biện pháp bảo mật cần thiết. Sau đó, chúng tôi tìm thấy các lỗi như mật khẩu mặc định, cấu hình xấu và thiết bị do thiếu bản cập nhật nên ngày càng trở nên không an toàn.

Một số ví dụ có thể bị ảnh hưởng là camera giám sát video, TV thông minh, máy in, v.v. Ví dụ, đối với camera giám sát video, chúng tôi có thể sử dụng:

* máy ảnh linksys inurl: main.cgi
* intitle: ”camera mạng toshiba - Đăng nhập người dùng”

Thay vào đó, đối với máy in:

* inurl: webarch / mainframe.cgi
* intitle: "network print server" filetype: shtm
* Các chức năng Hacking khác của Google mà chúng tôi có thể thực hiện thông qua việc sử dụng các toán tử sẽ là:
* Tìm kiếm các máy chủ lỗi thời và dễ bị tấn công.
* Thực hiện tìm kiếm người dùng và mật khẩu của các trang web, máy chủ và cơ sở dữ liệu.

Để kết thúc với Google Hacking, cần lưu ý rằng thông tin này có sẵn do cấu hình máy chủ hoặc thiết bị không tốt, thiếu các bản cập nhật và cũng vì Google đôi khi lập chỉ mục những thông tin không nên

**II.Thực Hành**

1. **Thử nghiệm với Shodan**

* tìm máy chủ apache và có hostname .ptit.edu.vn

Graphical user interface, text

Description automatically generated

Graphical user interface, application

Description automatically generated

* tìm máy chủ web IIS ở hà nội

Graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* tìm những thiết bị mở port 22 tại việt nam

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

* tìm máy chủ có hostname là .ptit.edu.vn

Graphical user interface

Description automatically generated

Graphical user interface, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* tìm những thiết bị chạy win 7 tại VN

Graphical user interface, text

Description automatically generated

* Dùng metasploit để quét webcamxp

Graphical user interface

Description automatically generated

Text

Description automatically generated

Graphical user interface, website

Description automatically generated

1. **Thử nghiệm với Google Hacking**

- Filter theo Vulnerable Servers

Graphical user interface, website

Description automatically generated

Graphical user interface, application

Description automatically generated

- Chọn một mục để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác.

Graphical user interface, application

Description automatically generated

- Thử nghiệm với ví dụ: www.exploit-db.com/ghdb/4057 . Với truy vấn tìm kiếm intitle: “Index of” “DCIM”, Google sẽ trả về kết quả của các bộ sưu tập ảnh mà mọi người không biết ở đó. Sinh viên cần tìm hiểu các từ khóa trong câu lệnh: intitle, DCIM.

* intitle: giúp Google giới hạn kết quả tìm kiếm về những trang có chứa từ đó trong tiêu đề. VD: intitle: “Index of” “DCIM” sẽ trả về những trang có từ “Index of”, “DCIM” trong tiêu đề
* Mục DCIM thực chất là từ viết tắt của Digital Camera Images. Đó là tên thư mục trong Quy tắc thiết kế cho hệ thống Tệp máy ảnh, là một phần của hệ thống tệp máy ảnh kỹ thuật số

Graphical user interface, text, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

- Tìm hiểu lệnh (còn gọi là Google dork) tại www.exploitdb.com/ghdb/6322 để tìm các khóa SSH.

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

- Tìm hiểu Google dork tại www.exploit-db.com/ghdb/6412 tìm log có tên người dùng và mật khẩu, có thể có các mục khác như địa chỉ e-mail, URL mà những thông tin đăng nhập này được sử dụng, v.v

Graphical user interface, application

Description automatically generated

- Thư mục gốc của máy chủ ftp.riken.jp

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

- Xem các file log của máy chủ ftp

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

- Xem thư mục backup của máy chủ ftp

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated