Môn học Thực tập cơ sở

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

1.1 Mục đích

Bài thực hành này giúp sinh viên hiểu được mối đe dọa đến từ các công cụ tìm kiếm bao gồm Shodan và Google.

1.2 Nội dung thực hành

1.2.1 Tìm hiểu lý thuyết

- Tìm hiểu về shodan và google hack. Tài liệu tham khảo:

  https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most- dangerous-internet-searches/index.html

  Principles of Computer Security: CompTIA Security+ and Beyond

1.2.2 Các bước thực hiện và kết quả cần đạt

1.2.2.1 Thử nghiệm với Shodan

a) Các bước thực hiện

- Vào website shodan và tạo tài khoản, đăng nhập sử dụng
- Tìm hiểu và thử nghiệm các bộ lọc trong danh sách: https://beta.shodan.io/search/filters
- Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://beta.shodan.io/search/examples
- Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://help.shodan.io/the-basics/search-query-fundamentals
- Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://www.yeahhub.com/shodan-search-examples/
- Tìm hiểu và thử nghiệm các ví dụ trong danh sách: https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/

b) Kết quả cần đạt được

- Thử nghiệm thành công 10 ví dụ tìm kiếm trong shodan để tìm kiếm các lỗ hổng, các thiết bị hay dịch vụ, sử dụng các bộ lọc đã tìm hiểu bên trên. Mô tả các tìm hiểu và quá trình thực hiện trong file báo cáo.

- Minh chứng: Chụp ảnh minh chứng màn hình cho 10 kết quả tìm kiếm trên, trong ảnh có tên và mã sinh viên của mình trong trang quản lý đào tạo PTIT.

1.2.2.2 Thử nghiệm với Google Hacking

Google Hacking Database (GHDB) là một chỉ mục được phân loại gồm các truy vấn của công cụ tìm kiếm trên Internet được thiết kế để khám phá thông tin thú vị, và thường là nhạy cảm, được công bố công khai trên Internet. Các thông tin này không bao giờ được công khai nhưng do chúng được liên kết trong một tài liệu web, được thu thập và lập chỉ mục bởi một công cụ tìm kiếm. Chúng ta có thể sử dụng các phương pháp tìm kiếm nâng cao của Google để khai thác các thông tin này.

a) Các bước thực hiện

- Vào website www.exploit-db.com/google-hacking-database và tìm hiểu
- Nhấn vào nút Filters đầu bên phải của trang và mũi tên xổ menu để khai thác các mục. Các mục ở đây bao gồm Footholds, Files Containing Usernames, Sensitive Directories, Web Server Detection, và các thứ khác.
- 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.
- 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.
- Tìm hiểu lệnh (còn gọi là Google dork) tại www.exploit-db.com/ghdb/6322 để tìm các khóa SSH.
- 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.
- Quay lại GHDB (www.exploit-db.com/google-hacking-database) và trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP).
- Chọn 5 Google dork, mỗi loại thuộc một danh mục khác nhau và giải thích cách chúng có thể có nguy hiểm như thế nào. Theo tùy chọn, hãy nhấp vào siêu liên kết cho các dork thực tế của Google để xem kết quả nào được trả

về. Sinh viên không sử dụng các kết quả trả về do đó có thể là một hành vi không hợp pháp.

b) Kết quả cần đạt được

- Thử nghiệm thành công 10 ví dụ Google hacking như đã tìm hiểu bên trên. Mô tả các tìm hiểu và quá trình thực hiện trong file báo cáo.
- Minh chứng: Chụp ảnh minh chứng màn hình cho 10 kết quả tìm kiếm trên, trong ảnh có tên và mã sinh viên của mình trong trang quản lý đào tạo PTIT.

1.3 Yêu cầu đối với file báo cáo

- File báo cáo dưới dạng pdf được trình bày rõ ràng theo cấu trúc: trang bìa, mục lục, các phần lý thuyết và thực hành riêng, tài liệu tham khảo nếu có. Báo cáo được đánh số trang trừ trang bìa.
- Đặt tên file theo định dạng kiểu như sau: Ví dụ đối với bài thực hành 1, tên file báo cáo là: *Bài thực hành 14_Họ tên SV_Mã SV*