BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật web và ứng dụng**

**Lab 3: Reconnaissance**

*GVHD: Ngô Khánh Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Tất cả các bài tập | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Bài tập 1: Liệt kê ra ít nhất 100 tên miền phụ của rmit.edu.vn, kết quả được lưu trong file csv**

* Để liệt kê các tên miền phụ của rmit.edu.vn, ta sử dụng virustotal.com:

**A screenshot of a computer

Description automatically generated**

* Kết quả cho thấy có hơn 100 subdomain ở đây, tiến hành lưu sang csv:

**A screenshot of a computer

Description automatically generated**

1. **Bài tập 2: Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác.**

* Truy cập vào trang web rmit.edu.vn để tìm tên miền phụ thông qua browser của burpsuite để ghi nhận HTTP history, sau đó send request này vào intruder:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Thêm subdomain vào url để tìm kiếm, sử dụng nút Add$, để dễ lấy tra hơn thì em sẽ tìm kiếm trên toàn bộ domain

A close-up of a computer screen

Description automatically generated

* Qua tab payload, tiến hành load list domain vào:

A screenshot of a computer

Description automatically generated

* Start attack và kiểm tra kết quả trả về, có thể tuỳ chỉnh thời gian giữa 2 câu request tại Resource pool để phù hợp với tốc độ trả về của trang web cần tìm kiếm, tránh việc trang web bị ddos.

A screenshot of a computer

Description automatically generated

1. **Bài tập 3: Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của \*.rmit.edu.vn. Kết quả lưu trong file csv.**

* Có thể dùng nslookup để xem địa chỉ IP tương ứng với tên miền, bài này chúng ta sẽ sử dụng bash script để tìm địa chỉ IP tương ứng với các tên miền đã tìm thấy ở bài tập 1.
* Tiến hành lưu các tên miền vào file domain.txt:

A screenshot of a computer

Description automatically generated

* Thực thi bash script:

A computer screen with text and numbers

Description automatically generated

* Tiến hành lưu vào file csv:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Bài tập 4: Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của \*.rmit.edu.vn. Báo cáo kết quả tìm được trong file csv**

* Sử dụng tool naabu:

<https://github.com/projectdiscovery/naabu?tab=readme-ov-file> <https://hub.docker.com/r/projectdiscovery/naabu>

* Sử dụng bash script tiến hành scan 1000 port phổ biển của các IP đã tìm được:

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Bài tập 5: Sử dụng https://web.archive.org/ tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của \*.rmit.edu.vn**

* Dưới đây là dữ liệu quá khứ của tên miền phụ staff.rmit.edu.vn không còn tồn tại của \*.rmit.edu.vn khi tra trên **https://web.archive.org/:**

A screenshot of a computer

Description automatically generated

1. **Bài tập 6: Tìm kiếm các tập tin pdf, excel, word, trên \*.rmit.edu.vn.**

* Sử dụng google dork để tìm kiểm các tập tin pdf, excel, word trên \*.rmit.edu.vn như sau:

**site:alumninetwork.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls**

**A screenshot of a computer

Description automatically generated**

1. **Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain \*.rmit.edu.vn. (lưu ý: không sử dụng thông tin này để khai thác thông tin cá nhân có thể có, mọi hành vi sử dụng không được phép sẽ chịu trách nhiệm trước pháp luật)**

* Sử dụng github search để tra cứu thông tin với .rmit.edu.vn và password:

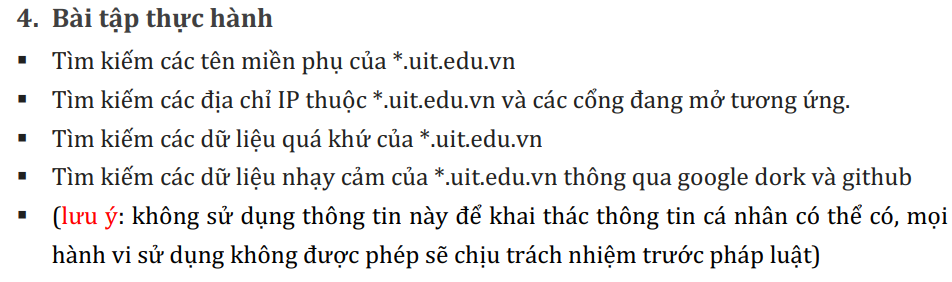
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Từ đây ta sẽ biết thêm thông tin về username và password liên quan đến rmit.edu.vn



* Các subdomain của uit.edu.vn

A screenshot of a computer

Description automatically generated

* IP thì có thể xem ở bên cạnh hoặc sử dụng nsloohup để xem địa chỉ Ip ứng với tên miền tương ứng

A screenshot of a computer program

Description automatically generated

* Các port thì có thể dùng tool naabu hoặc dùng nmap để scan

A screenshot of a computer program

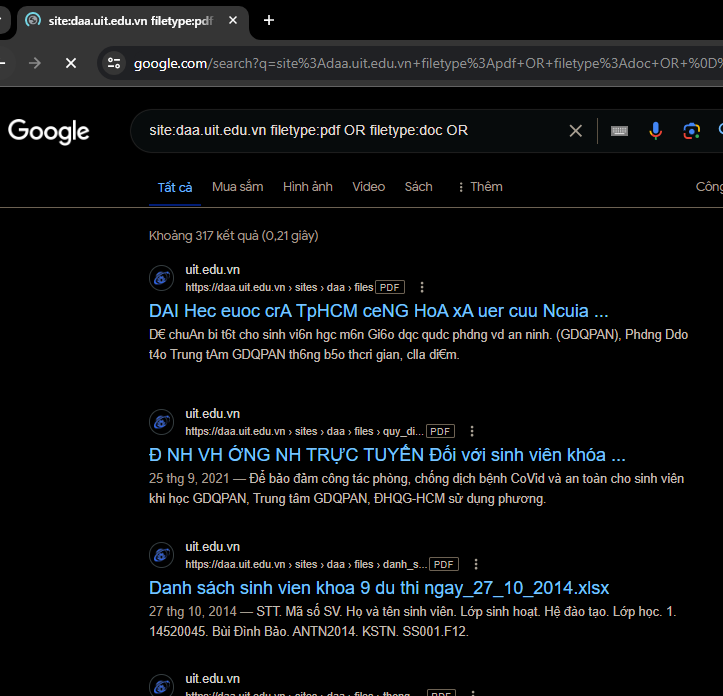
Description automatically generated

* Tìm kiếm dữ liệu trong quá khứ

A screenshot of a computer

Description automatically generated

* Tìm kiếm thông tin nhạy cảm trên google dork hoặc github search



A screenshot of a computer

Description automatically generated

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)