BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng – NT140.O11.ANTT**

**Tên chủ đề: – The Kaminsky Attack Lab**

*GV: Nghi Hoàng Khoa*

**Nhóm: 13**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT140.O11.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 01 | Đinh Bùi Huy Phương | 21520090 | 21520090@gm.uit.edu.vn |
| 02 | Nguyễn Thị Thanh Mai | 21521112 | 21521112@gm.uit.edu.vn |
| 03 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |
| 04 | Nguyễn Phương Trinh | 21521581 | 21521581@gm.uit.edu.vn |

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

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung |  | Trang |
| 01 | Task 1: Lab Environment Setup | | 02 – 07 |
| 02 | Task2: Construct DNS request | | 07 – 08 |
| 03 | Task 3: Spoof DNS Replies | | 08 – 09 |
| 04 | Task 4: Launch the Kaminsky Attack | | 09 – 12 |
| 05 | Task 5: Result Verification | | 13 |

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

BÁO CÁO CHI TIẾT

**1. Task 1: Lab Environment Setup**

- Tiến hành cài đặt môi trường bằng docker-compose.yml trong Labsetup.zip:

A screen shot of a computer program

Description automatically generated

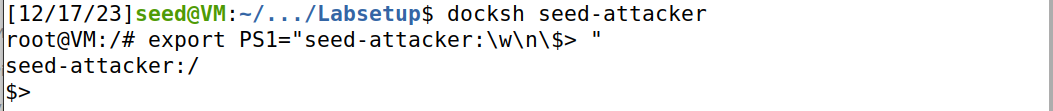
A screenshot of a computer program

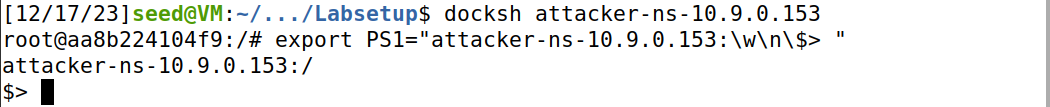
Description automatically generated

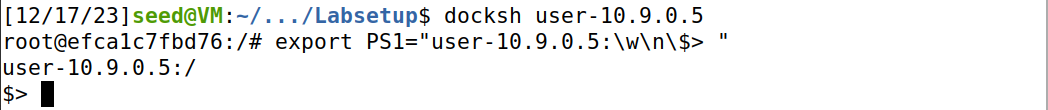
A computer screen shot of a computer error

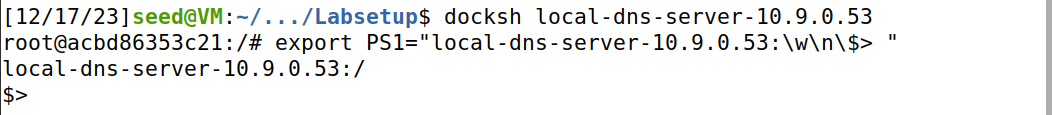
Description automatically generated

- Tiến hành truy cập vào shell của các container và thay đôi biến môi trường PS1 để xác nhận rõ ràng đang làm việc trong môi trường container đó:

****

****

****

****

**\* Trên máy Local DNS Server:**

**A screenshot of a computer

Description automatically generated**

**\* Trên máy user:**

**A white background with black and white clouds

Description automatically generated**

**\* Trên máy Attacker’s Nameserver:**

**A screenshot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A computer screen shot of a computer code

Description automatically generated**

**\* Kiểm tra DNS Setup**

- Trên máy user, thực hiện:

**A computer screen shot of a computer code

Description automatically generated**

→ Kết quả chạy lệnh dig ns.attacker32.com là IP của Nameserver của Attacker.

A computer screen shot of a code

Description automatically generated

→ Kết quả chạy lệnh dig [www.example.com](http://www.example.com) được trả về từ nameserver hợp pháp của miền.

A computer screen shot of a computer code

Description automatically generated

→ Kết quả chạy lệnh dig @ns.attacker32.com [www.example.com](http://www.example.com) nhận được kết quả giả từ attacker.

**2. Task2: Construct DNS request**

- Trong task2, tập trung vào việc gửi các yêu cầu DNS, attacker kích hoạt máy chủ DNS mục tiêu gửi các truy vấn DNS để có cơ hội giả mạo các câu trả lời.

- Hoàn thiện chương trình:

A computer screen with numbers and symbols

Description automatically generated

Code này tạo một gói tin DNS request có địa chỉ nguồn từ máy attacker ’10.9.0.1’, địa chỉ đích '10.9.0.53' và trường qname là ‘www.example.com'.

- Kết quả thu được trên wireshark:

A screenshot of a computer

Description automatically generated

**3. Task 3: Spoof DNS Replies**

- Kiểm tra IP của các nameservers của domain example.com:

**A screenshot of a computer

Description automatically generated**

- Hoàn thiện chương trình:

A screenshot of a computer

Description automatically generated

Đoạn mã này có chức năng tạo một câu trả lời DNS giả mạo cho tên miền [www.example.com](http://www.example.com)

- Kết quả thu được trên Wireshark:

A screenshot of a computer

Description automatically generated

→ Thành công với địa chỉ “1.2.3.4”

**4. Task 4: Launch the Kaminsky Attack**

- Khởi tạo các DNS packet:

+ DNS request:

A computer screen with text

Description automatically generated

+ DNS Spoof reply:

A computer screen shot of a computer code

Description automatically generated

- Hoàn thiện file attack.c được cung cấp kèm theo Labsetup.zip

A close-up of a computer code

Description automatically generated

A computer screen shot of text

Description automatically generated

A screen shot of a computer code

Description automatically generated

**A screenshot of a computer code

Description automatically generated**

→ Hàm send\_dns\_request được sử dụng để tạo và gửi một yêu cầu DNS giả mạo. Đầu vào của hàm bao gồm pkt (mảng unsigned char) là gói tin DNS cơ bản, pktsize là kích thước của gói tin, và name là tên miền muốn giả mạo. Hàm này thay thế một phần của tên miền trong gói tin DNS để tạo thành yêu cầu DNS giả mạo, sau đó gửi gói tin đi bằng cách sử dụng hàm send\_raw\_packet.

Hàm send\_dns\_response được sử dụng để tạo và gửi một câu trả lời DNS giả mạo. Đầu vào của hàm bao gồm pkt (mảng unsigned char) là gói tin DNS cơ bản, pktsize là kích thước của gói tin, src là địa chỉ IP nguồn giả mạo, name là tên miền muốn giả mạo, và id là Transaction ID. Hàm này thay đổi địa chỉ IP nguồn, tên miền trong gói tin DNS, cũng như Transaction ID để tạo thành câu trả lời DNS giả mạo, sau đó gửi gói tin đi bằng cách sử dụng hàm send\_raw\_packet.

- Tiến hành chạy task2.py và task3.py để lấy các template packet:

A screenshot of a computer

Description automatically generated A screenshot of a computer code

Description automatically generated

- Thực thi file attack.c, một phần nội dung hiển thị trên màn hình

A screenshot of a computer

Description automatically generated A screenshot of a computer code

Description automatically generated

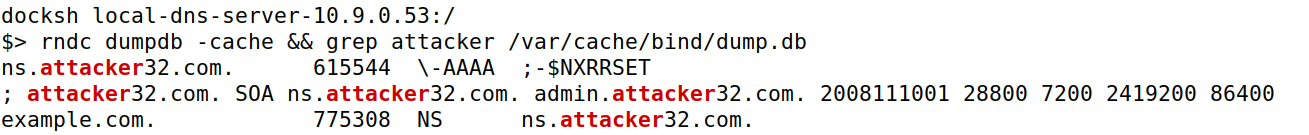
- Thực hiện tấn công:

- Trên máy local dns server, thực thi lệnh:

+ rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db

A screenshot of a computer code

Description automatically generated



**5. Task 5: Result Verification**

- Chứng minh tấn công thành công:

*A computer screen shot of a computer code

Description automatically generated*

*A screenshot of a computer screen

Description automatically generated*→ Kết quả của 2 lệnh dig @ns.attacker32.com [www.example.com](http://www.example.com) và dig [www.example.com](http://www.example.com) đều cho ra cùng địa chỉ giả mạo của attacker nameserver 1.2.3.5 (ns.attack32.com).

**---HẾT ---**

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