BÁO CÁO THỰC HÀNH

**Môn học: AN TOÀN MẠNG**

**Tên chủ đề: TẤN CÔNG DNS**

**DNS Attack**

*GVHD: Tô Trọng Nghĩa*

**Nhóm: 09**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT140.P11.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Trần Anh Khôi | 22520701 | [22520701@gm.uit.edu.vn](mailto:22520701@gm.uit.edu.vn) |
| 2 | Hồ Vỉ Khánh | 22520633 | [22520633@gm.uit.edu.vn](mailto:22520633@gm.uit.edu.vn) |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| STT | Nội dung | Tình trạng |
| 1 | Yêu cầu 1 | 100% |
| 2 | Yêu cầu 2 | 100% |
| 3 | Yêu cầu 3 | 100% |
| 4 | Yêu cầu 4 | 100% |
| 5 | Yêu cầu 5 | 100% |
| 6 | Yêu cầu 6 | 100% |
| 7 | Yêu cầu 7 | 100% |
| Điểm tự đánh giá 10/10 | | |

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

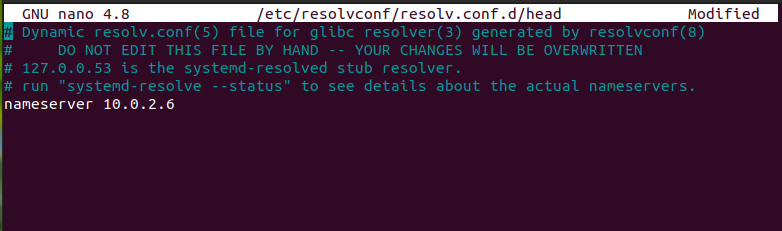
BÁO CÁO CHI TIẾT

# Cài đặt môi trường thực hành

### Cài đặt máy User VM

**Trên máy User**

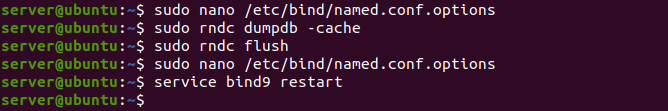




*Cài đặt UserVM*

### Cài đặt máy Local DNS Server

**Trên máy DNS-Server:**





*Cài đặt Local DNS Server*

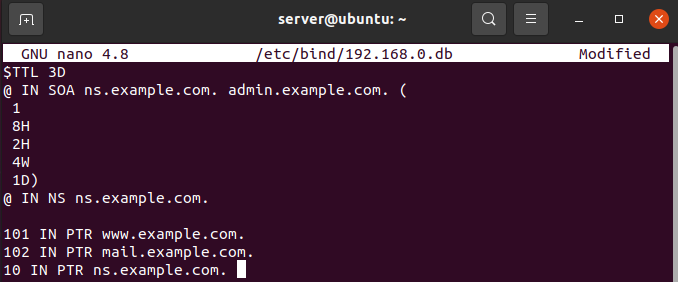
### Cấu hình DNS Zone



*Tạo DNS Zone*



*Thiết lập Forward lookup zone file*



*Thiết lập Reverse lookup zone file*

#### **1. Trước khi thực hiện bài thực hành, sinh viên tìm hiểu và cho biết: Khi người dùng thực hiện truy vấn phân giải tên miền sang địa chỉ IP, quá trình này sẽ được thực hiện như thế nào (tại máy người dùng, trong cùng mạng LAN, DNS Servers,…)**

Khi người dung thực hiện truy vấn phân giải tên miền sang địa chỉ IP, quá trình này sẽ được thực hiện:

- **Tại máy User**: Gửi gói request DNS đến DNS server cục bộ trên mạng LAN.

- **Tại máy DNS server cục bộ**:

+ Nhận yêu cầu DNS từ máy người dùng.

+ Tìm thông tin phân giải trong filehosts – file text trong hệ điều hành chịu trách

nhiệm chuyển hostname thành địa chỉ IP.

+ Nếu không thấy thông tin, kiểm tra Cache của DNS Server cục bộ DNS Resolver kiểm tra cache của mình. Nếu có, trả kết quả cho người dùng.

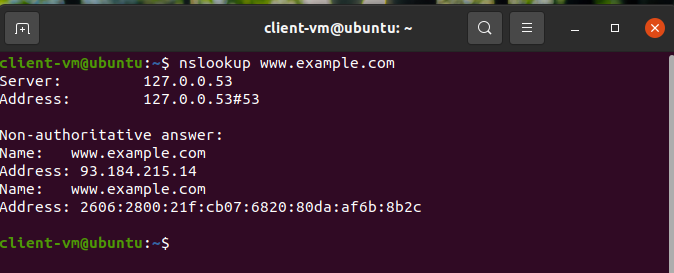
+ Nếu không có record nào được lưu lại, DNS server cục bộ sẽ truy vấn đến những DNS Servers ở tầng cao hơn, máy chủ DNS quản lý tên miền để lấy thông tin. Sẽ liên hệ lần lượt với Root DNS, TLD DNS, và Authoritative DNS để lấy địa chỉ IP.

+ Sau khi biết kết quả, sẽ trả kết quả cho máy người dùng để truy cập vào server.

# Thực hành

## Tấn công giả mạo phản hồi trực tiếp đến người dùng (Directly Spoofing Response to User)

#### **2. Mô tả kết quả nhận được từ quá trình phân giải tên miền www.example.com khi sử dụng và không sử dụng netwox 105.**



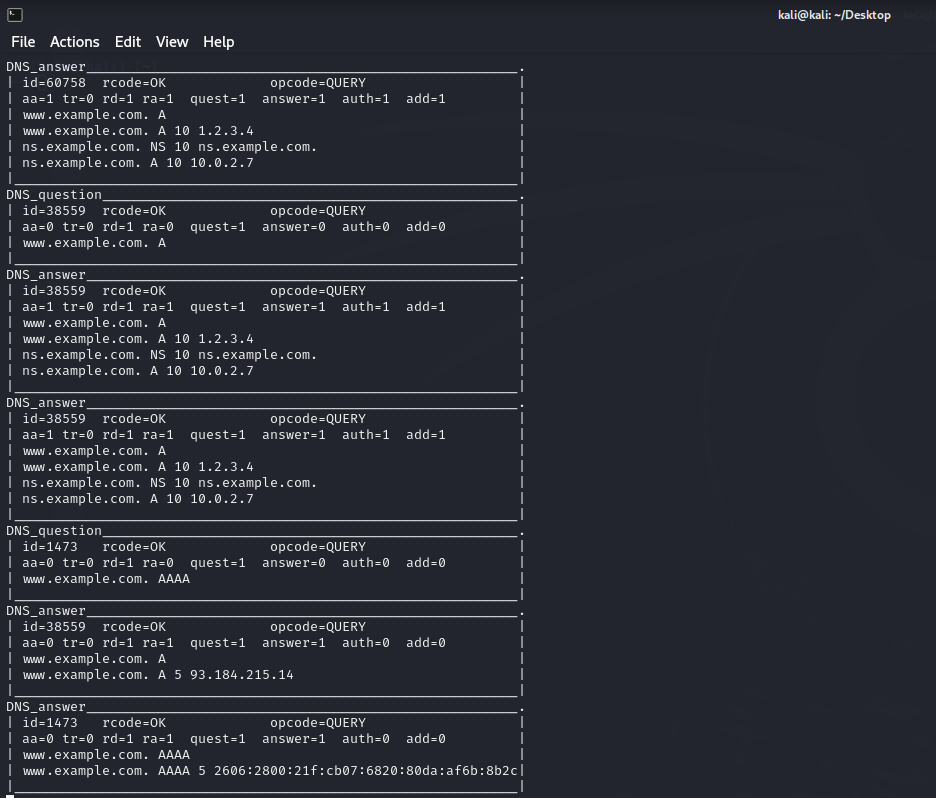
*Kết quả thực thi lệnh nslookup với tên miền www.example.com trước khi mở chạy netwox 105*

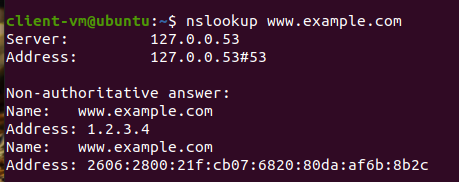
**- Trên máy Attacker:**

Sử dụng netwox để nghe lén các DNS request:

**sudo netwox 105 -h “www.example.com” -H “1.2.3.4” -a “ns.example.com” -A “10.0.2.7”**

- Thu được các kết quả trên máy Attacker:

****

**

*Kết quả thực thi lệnh nslookup với tên miền www.example.com khi đã mở chạy netwox 105*

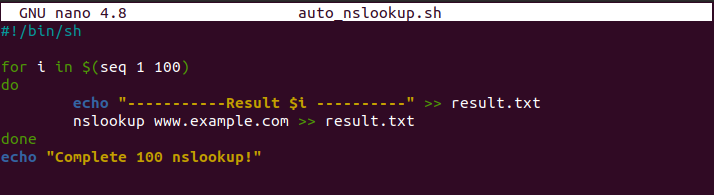
#### **3. Xác suất tấn công thành công là bao nhiêu (với số lần thử > 30). Đề xuất giải pháp để nâng cao tỉ lệ tấn công thành công.**

- Đầu tiên ta tiếp tục thực hiện netwox 105

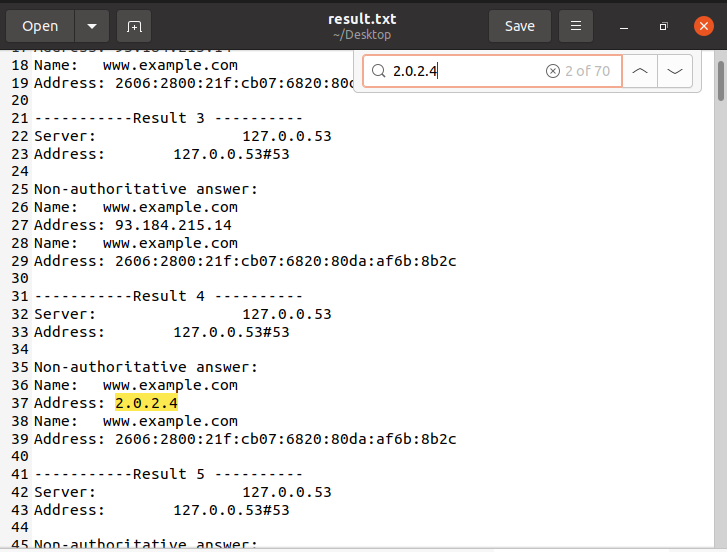


- Ở máy user thì ta sẽ viết 1 file bash chạy 100 lần tự động nslookup đến

www.example.com



- Sau khi ta thực hiện chạy file bash thì nhận được ít kết quả thành công.



* Sau khi hoàn thành thực hiện kiểm tra 100 lần thực hiện thì sẽ có được từ 69 đến 70 lần thành công như vậy là tỉ lệ thành công chưa được cao. Giải pháp để nâng cao tỉ lệ thành công là nâng số lần thực hiện, đặt thời gian chờ sau mỗi lệnh để đạt được kết quả thành công cao hơn và tìm hiểu cách hoạt động của giao thức DNS và các triển khai cụ thể để tìm ra các lỗ hổng bảo mật có thể được khai thác. Sử dụng các công cụ và kỹ thuật tấn công mạnh mẽ như DNS spoofing, cache poisoning, amplification attacks, hay các phương pháp khác nhằm tận dụng các lỗ hổng trong hệ thống DNS.

#### 4. Cần làm gì để hạn chế được nguy cơ tấn công của cơ chế này.

- Sử dụng DNSSEC (DNS Security Extensions - công nghệ an toàn mở rộng cho hệ thống tên miền DNS, cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau và xác thực cho từng zone dữ liệu để đảm bảo toàn vẹn dữ liệu), Firewall,...

- Sử dụng các công cụ phát hiện tấn công mạng (IDS/IPS)

- Xác thực hai yếu tố (2FA): Áp dụng xác thực hai yếu tố để tăng cường bảo mật cho các tài khoản người dùng, giảm thiểu nguy cơ bị tấn công giả mạo.

- Đặt Time to Live thấp để ngăn chặn cách tấn công nghe lén và giả mạo.

- Phân tích các log mạng để phát hiện và ngăn chặn kịp thời.

- Không để public IP của máy Local DNS Server cho mạng bên ngoài.

- Giáo dục người dùng: Đào tạo người dùng về cách nhận biết các dấu hiệu của tấn công giả mạo và cách xử lý khi gặp phải các tình huống nghi ngờ.

- Sử dụng giao thức mã hóa an toàn: Đảm bảo rằng các giao thức mã hóa như HTTPS được sử dụng để bảo mật các kết nối mạng, ngăn chặn việc giả mạo thông tin.

- Sử dụng các phần mềm uy tín có khả năng phát hiện và cảnh báo các mối đe dọa tiềm

ẩn. Ngăn chặn tải xuống và ngăn phần mềm độc hại xâm nhập vào hệ thống.

- Thường xuyên cập nhật phiên bản và các bản vá lỗ hổng.

## Tấn công DNS Cache Poisoning

#### 5. Tại sao khi thiết lập spoofip với giá trị raw, tỉ lệ thành công khi thực hiện hình thức tấn công này sẽ cao hơn?

|  |  |
| --- | --- |
| Khi không sử dụng spoofip với giá trị raw | Khi sử dụng spoofip với giá trị raw |
| - Netwox 105 cố gắng giả mạo địa chỉ MAC cho IP giả mạo  - Gửi ARP request để lấy địa chỉ MAC  - Thường không nhận được phản hồi do IP giả mạo là máy DNS bên ngoài  - Thời gian chờ đợi lâu, có thể dẫn đến thất bại nếu DNS local phản hồi trước | - Bỏ qua quá trình xác định địa chỉ MAC qua ARP  - Giảm thời gian chờ, tăng tỷ lệ tấn công thành công  - Không kiểm tra tính hợp lệ của địa chỉ IP nguồn  - Tăng khả năng tùy chỉnh gói tin, khó bị phát hiện hơn |

**Lợi ích khi sử dụng giá trị raw**

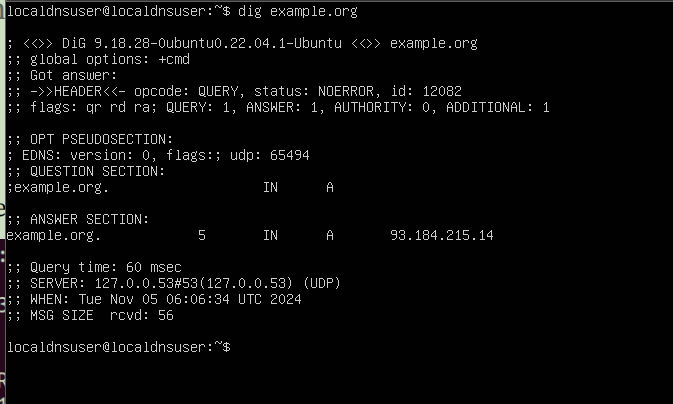
- Bỏ qua một số biện pháp bảo mật dựa trên kiểm tra tính hợp lệ

- Tăng tốc độ gửi gói tin, hiệu quả hơn trong các cuộc tấn công DoS/DDoS

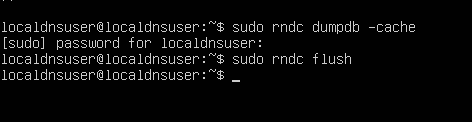
=> Việc sử dụng spoofip với giá trị raw trong Netwox 105 giúp tăng hiệu quả của các cuộc tấn công giả mạo IP bằng cách bỏ qua các bước kiểm tra và xác thực, đồng thời tăng tốc độ và khả năng tùy chỉnh của các gói tin giả mạo.

**Ví dụ:**

*Kết quả truy vấn* ***example.org*** *trước khi tấn công*



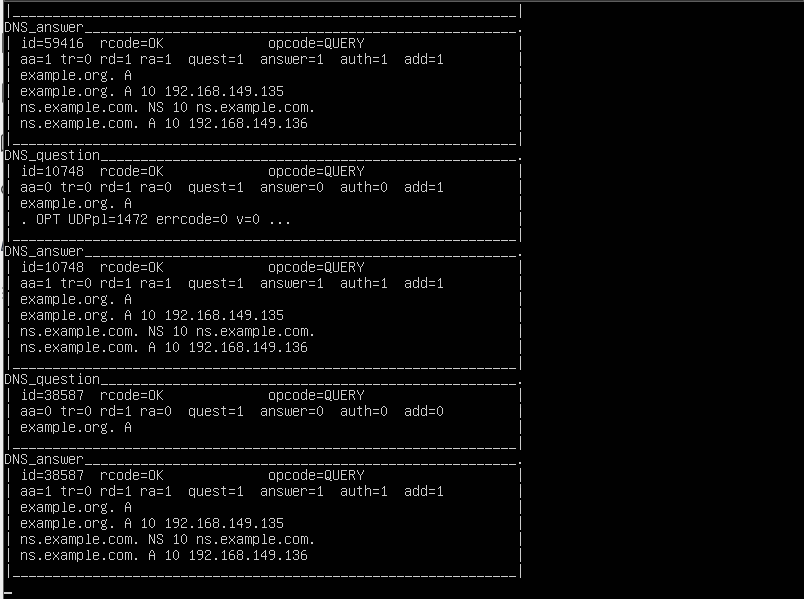
- Xóa rỗng DNS cache tại server



Tại máy tấn công, sử dụng Netwox 105 như trong bài trước để thực hiện

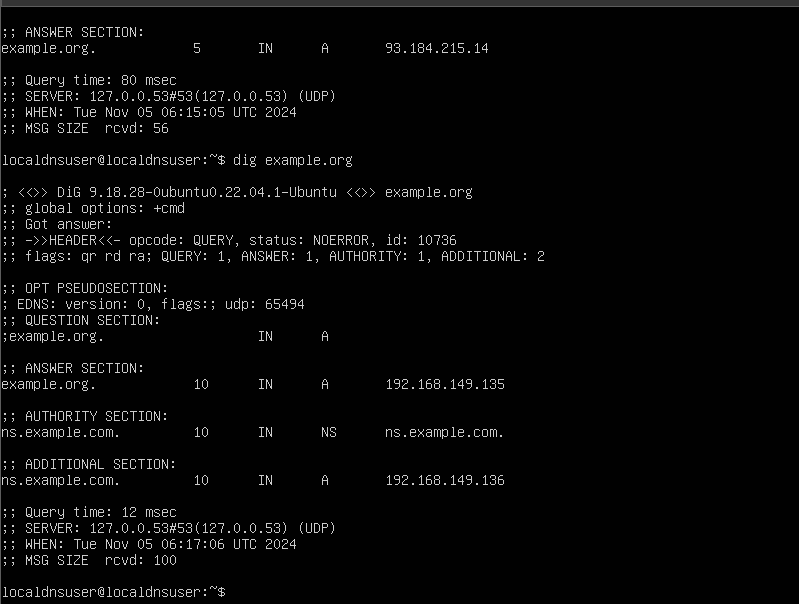
tấn công. Sử dụng filter với nội dung “src host 10.0.2.6” (sử dụng địa chỉ IP của DNS server). Có thể sử dụng thêm ttl (time-to-live) để chỉ định thời gian tồn tại trong bộ nhớ cache.



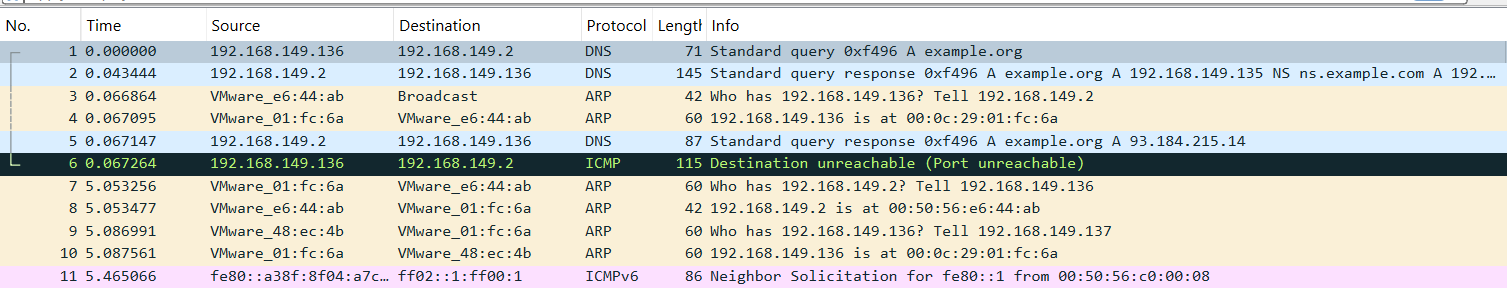


Sau khi tấn công ta được kết quả như sau khi truy vấn đến tên miền example.org

ở user

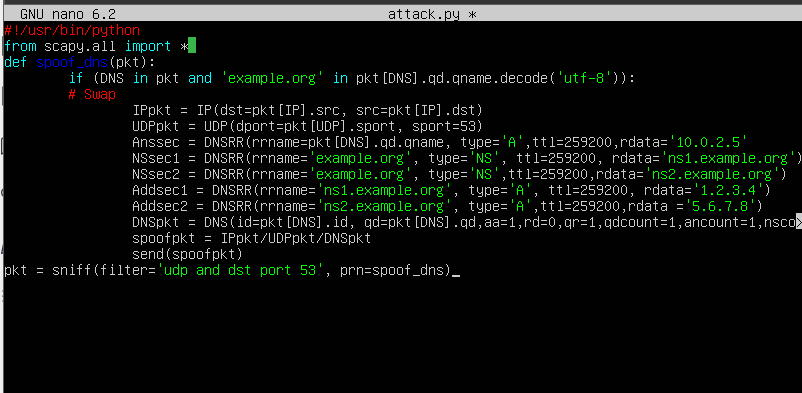


- Thực hiện bắt gói tin bằng wireshark để xem quá trình truy vấn phân giải tên miền

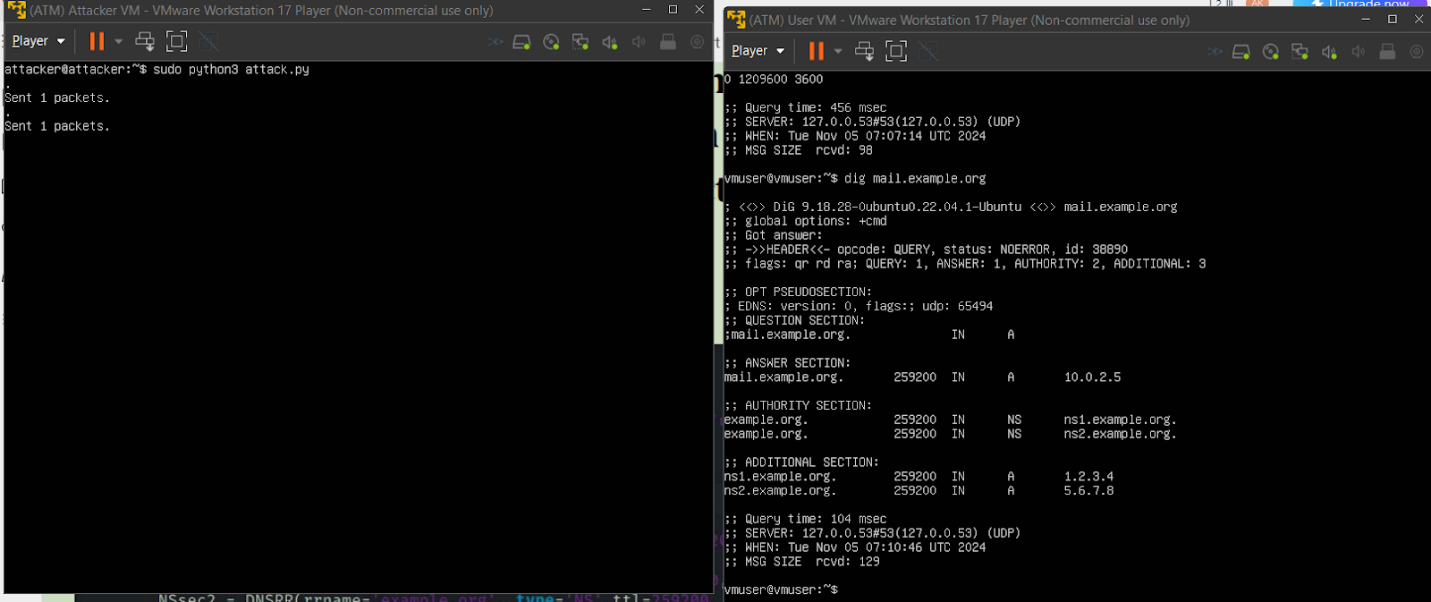


#### 6. Cách thức tấn công này có nhược điểm chỉ áp dụng trên các hostname cụ thể đã xác định trước (example.org). Nếu người dùng truy cập vào hostname khác (mail.example.org) thì không thể tấn công được. Sinh viên thực hiện tìm hiểu và thực hiện tấn công Authority Section để DNS servers lưu cache thông tin nameserver giả mạo.

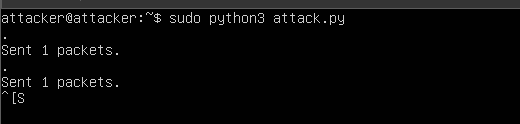
- Code tấn công:



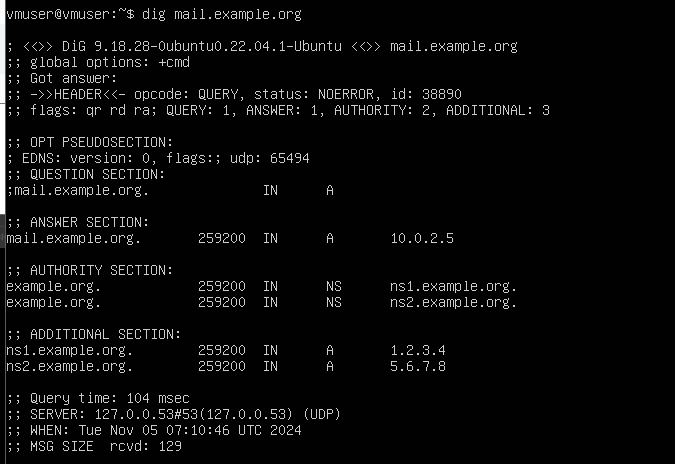
- Thực thi code trên máy attacker:

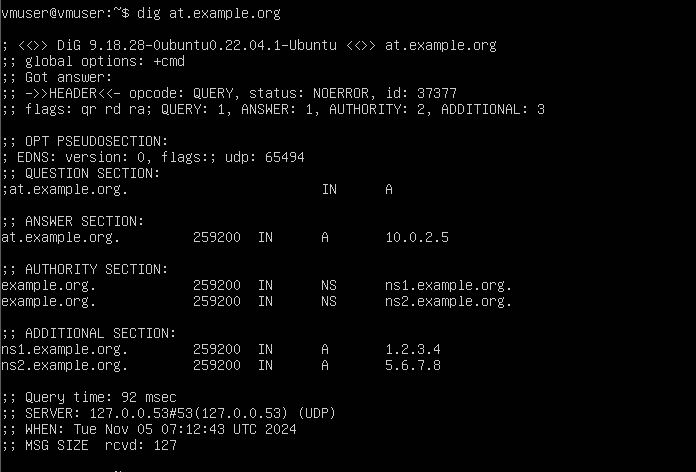


* Attacker

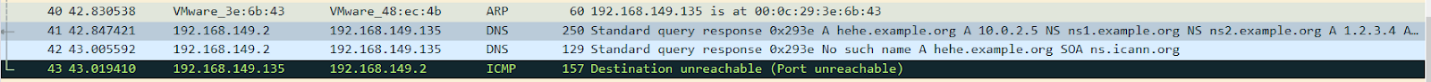


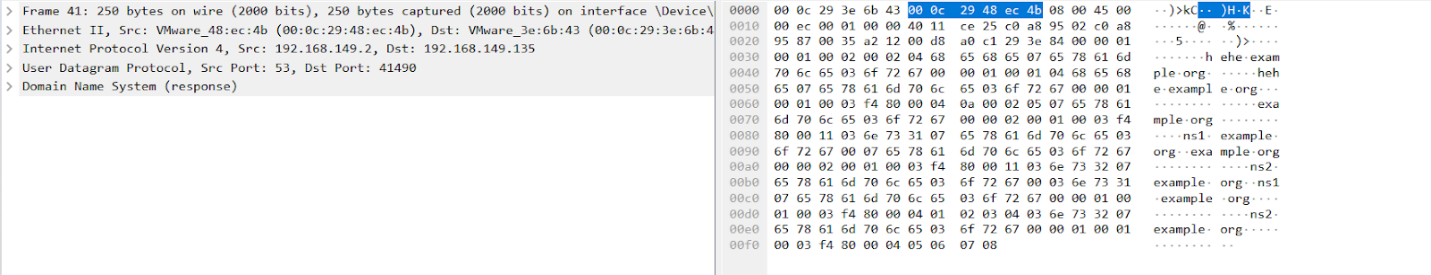
* User





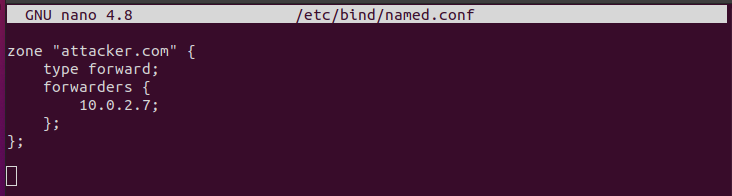
- Chạy wireshark để kiểm tra gói tin bắt được



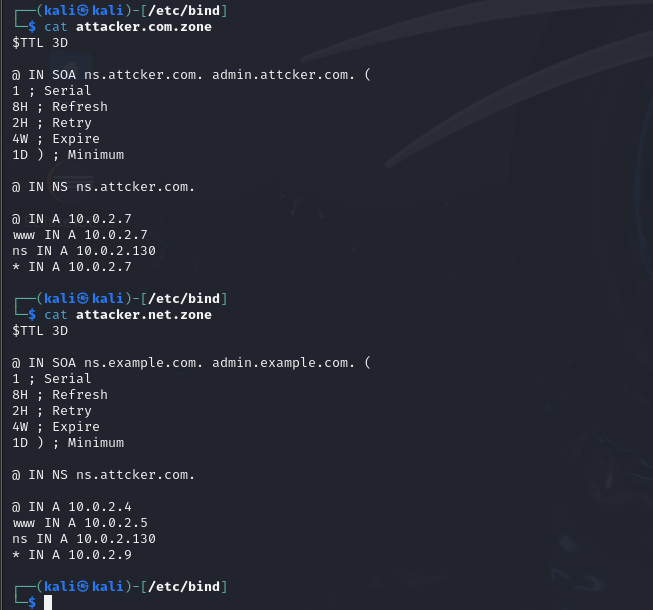


## Tấn công Kaminsky

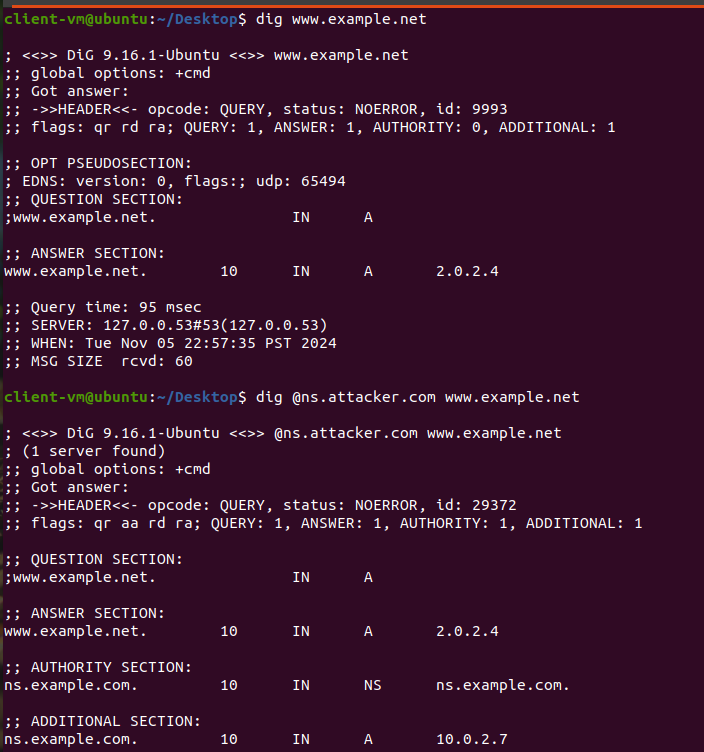
### Thiết lập Forward zone



### Thiết lập trên máy Attacker



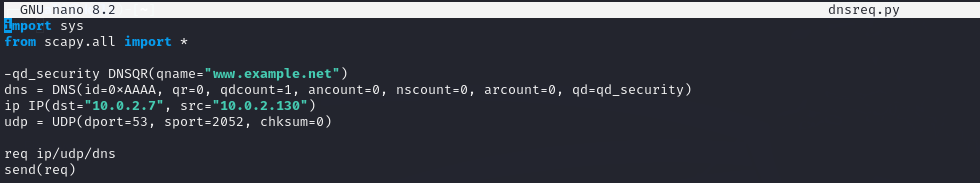
### Kiểm tra việc thiết lập



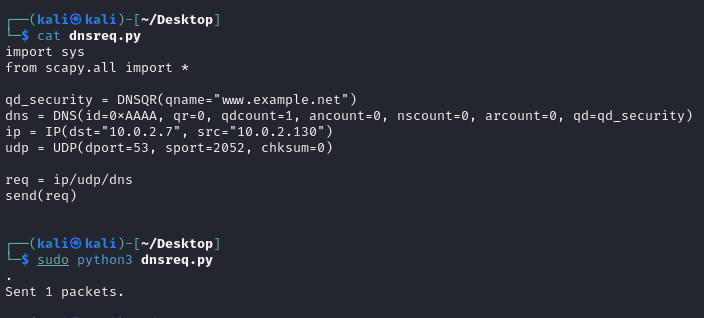
### Thực hiện tấn công

**Chức năng tạo ra DNS request**

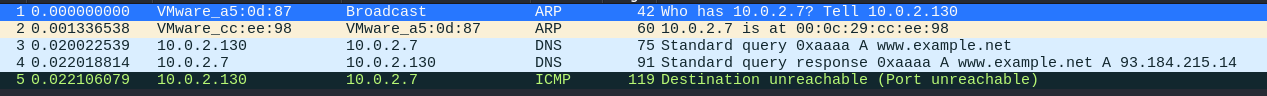
Code request:



Thực hiện:

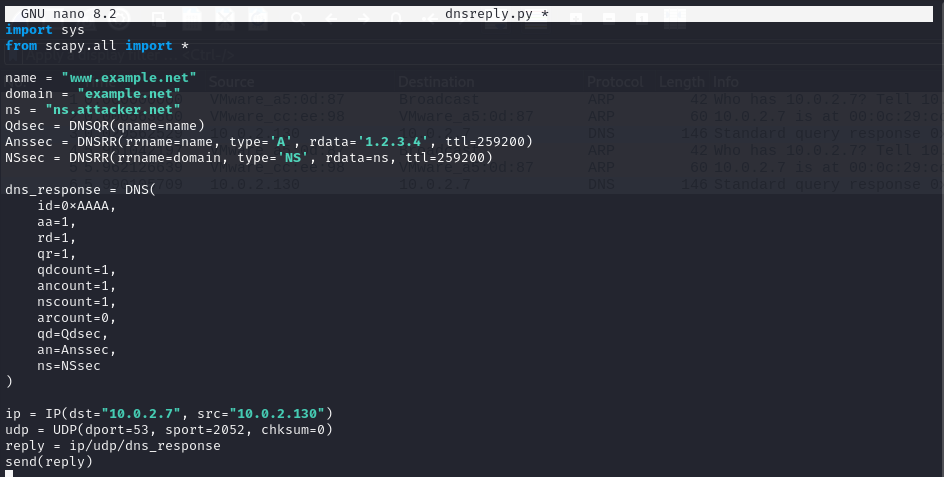


Bắt gói tin bằng Wireshark:

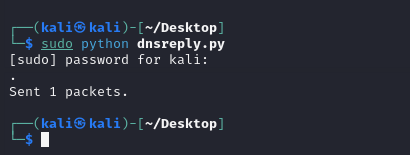


**Chức năng gửi DNS reply giả mạo**

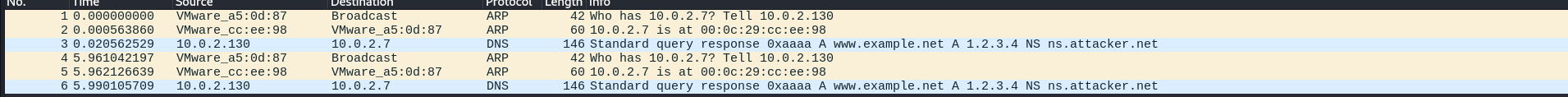
Code request:



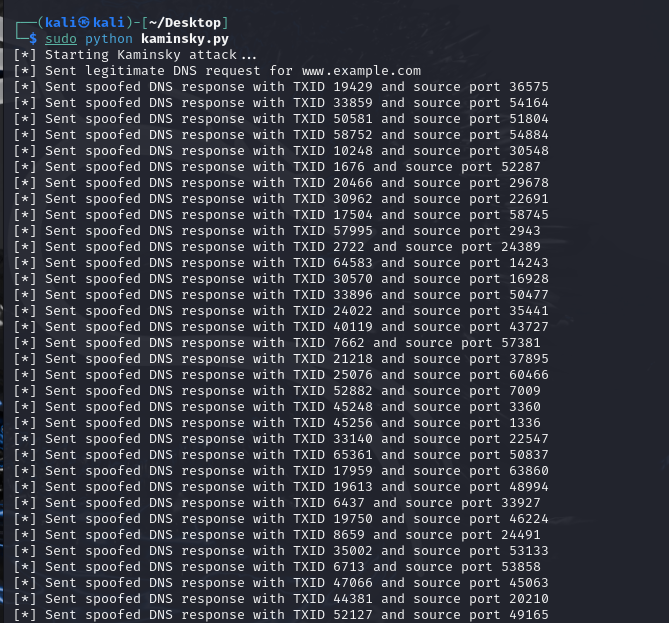
Thực hiện:



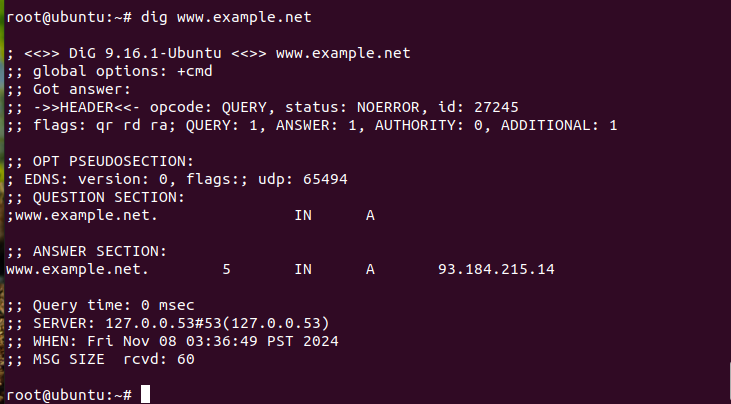
Bắt gói tin bằng Wireshark:



**Thực hiện chức năng tấn công Kaminsky (Bài tập mở rộng / cộng điểm)**



**Kiểm tra**

****

**Challenges Network (CTF)**

#### **7. DNS - zone transfert (Viết writeup chi tết)**

**Statement**

A not really dutiful administrator has set up a DNS service for the "ch11.challenge01.root-me.org" domain...

Challenge connection informations:

- Host: challenge01.root-me.org

- Protocol: DNS

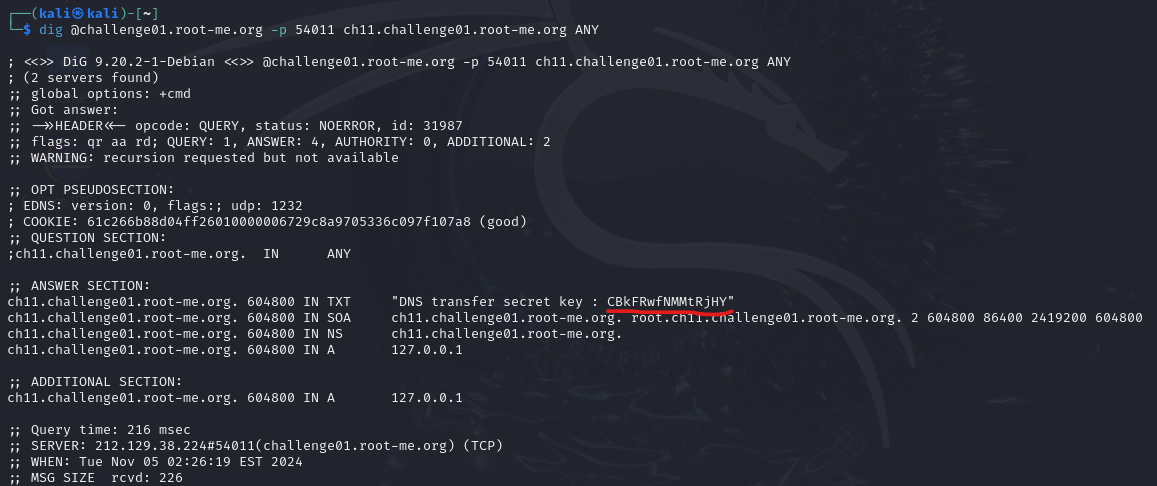
- Port: 54011

**Trả lời:**

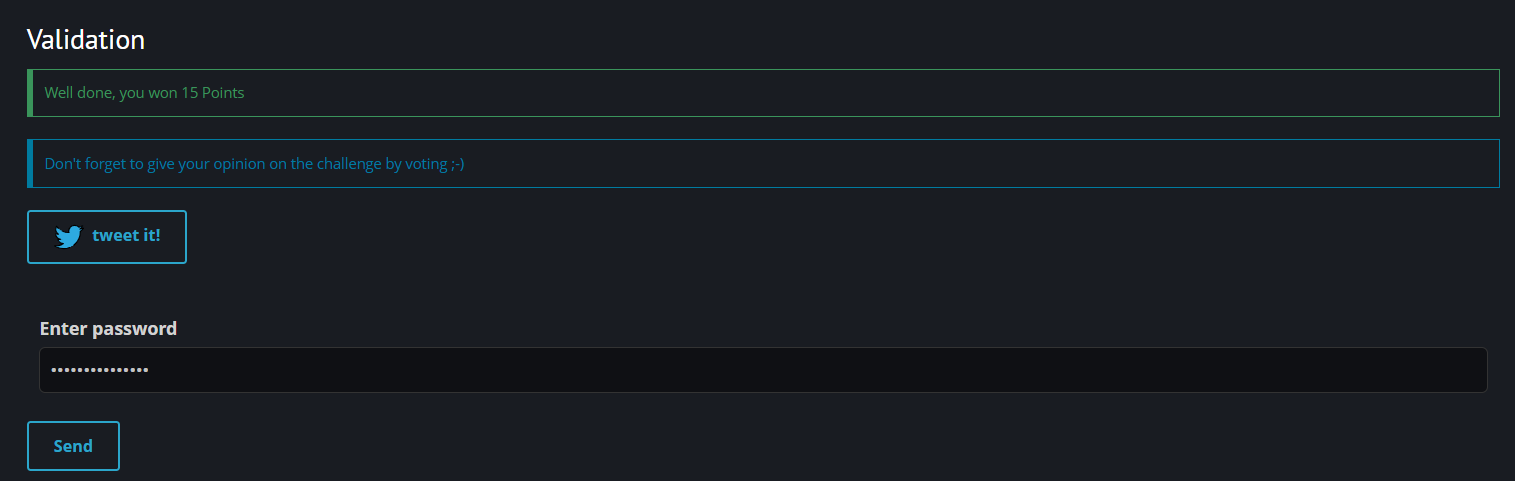
- Dựa vào Statement ta biết được domain của challenge DNS – zone transfert là: "ch11.challenge01.root-me.org"

- Sử dụng lệnh “**dig**” để truy vấn thông tin về các bản ghi DNS.

**dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org ANY**



* Flag: CBkFRwfNMMtRjHY



1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)