BÁO CÁO THỰC HÀNH

**Bài thực hành số xx: Tên bài thực hành**

**Môn học:** Nhập môn Mạng máy tính

**Lớp:** NT100.ATTT.2

**THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Nguyễn Thị A | 20520001 |
| 2 | Phan Văn B | 20520002 |
|  |  |  |

|  |
| --- |
| **Điểm tự đánh giá** |
|  |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện |  |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

MỤC LỤC

[BÁO CÁO CHI TIẾT 2](#_Toc116939715)

[1. ARP Cache Poisoning 2](#_Toc116939716)

[a. Using ARP request 2](#_Toc116939717)

[b. Using ARP reply 4](#_Toc116939718)

[c. Using ARP gratuitous message 7](#_Toc116939719)

[2. MITM Attack on Telnet using ARP Cache Poisoning 9](#_Toc116939720)

[+ Mục tiêu bài này ta sẽ viết code để trong ARP cache của Server thì IP của Client sẽ là MAC của Attacker, và trong ARP cache của Client IP của Server sẽ là MAC của Attacker 9](#_Toc116939721)

[3. MITM Attack on Netcat using ARP Cache Poisoning 15](#_Toc116939722)

[**B.** TÀI LIỆU THAM KHẢO 15](#_Toc116939723)

# BÁO CÁO CHI TIẾT

## ARP Cache Poisoning

### Using ARP request

Mô hình mạng của từng máy như sau:

+ Attacker:

* IP: 10.0.2.15
* MAC: 08:00:27:76:9D:B4

+ Server:

* IP: 10.0.2.4
* MAC: 08:00:27:2C:B5:41

+ Client

* IP: 10.0.2.5
* MAC: 08:00:27:1A:EE:B2
* Đầu tiên ta cần đầu độc ARP Cache
* Tại máy của attacker ta viết 1 chương trình

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Với hwsrc là địa chỉ máy MAC của attacker còn psrc là địa chỉ ip máy cilent, hwdst là MAC của server, pdst là địa chỉ ip của server

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Kiểm tra arp của máy server ta thấy lúc chưa bị đầu độc thì ip và mac của attacker đều đúng

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tại máy attacker ta chạy file đầu độc

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

+ Kiểm tra lại bảng arp của máy server ta thấy địa chỉ ip của client đã được xác định là MAC của máy attacker

### Using ARP reply

+ Trên máy attacker ta viết 1 chương trình để giả mạo gói tin ARP reply

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Thêm 1 biến op=2 nghĩa là gói arp reply

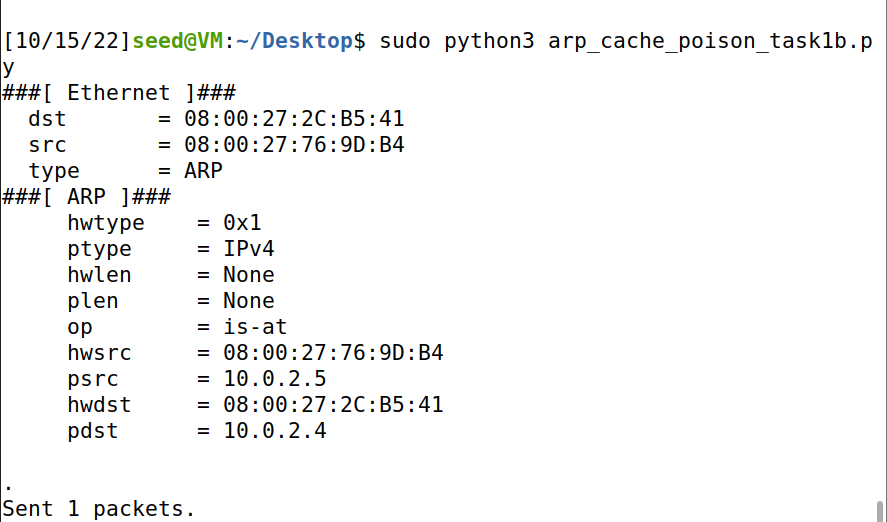
Ảnh có chứa văn bản

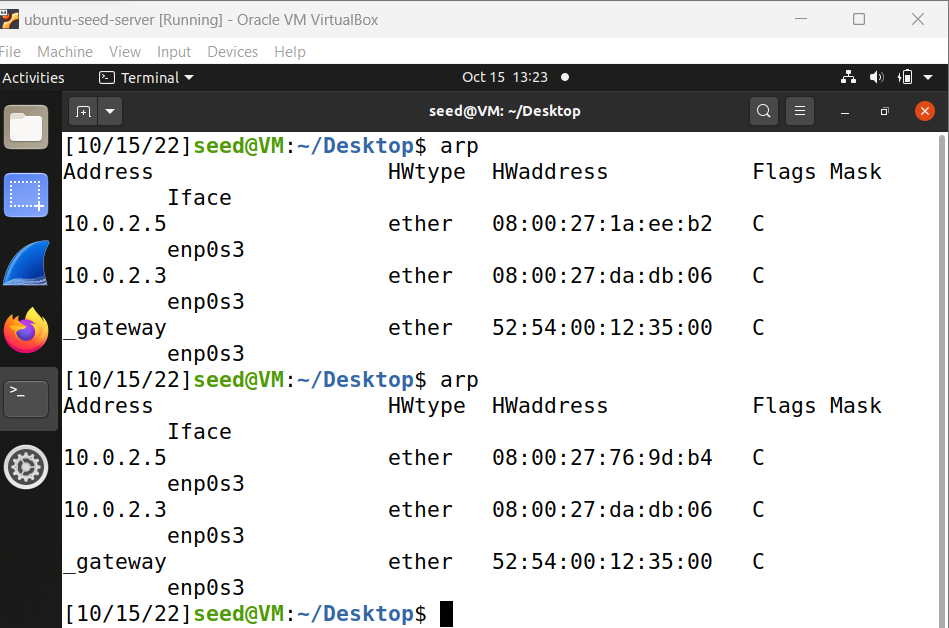
Mô tả được tạo tự động

+ Kiểm tra arp máy server thì tất cả đều bình thường

+ Tại máy attacker ta thực hiện chạy đoạn code để gửi đi gói tin arp reply

* Lưu ý: máy server phải có ip của máy client nhưng chưa có MAC thì mới thực hiện được. Hoặc có ip và MAC đúng thì ta mới đổi MAC thành của attacker được





+ Tại máy server ta kiểm tra bảng arp

+ Ở trên là trước khi attacker thực hiện ARP reply thì địa chỉ IP và MAC vẫn đúng là của client

+ Ở dưới sau khi thực hiện ARP reply thì ip của client nhưng MAC lại là của attacker

### Using ARP gratuitous message

+ Trên máy attacker tha viết 1 chương trình để nói cho mọi người(ở đây là server) mình chính là địa chỉ MAC và IP đó

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tại máy server ta kiểm tra bảng arp

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Địa chỉ MAC và ip vẫn tương ứng và bình thường

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tại máy attacker ta thực hiện chạy đoạn lệnh

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta thấy địa chỉ MAC của máy client đã được thay bằng máy của attacker

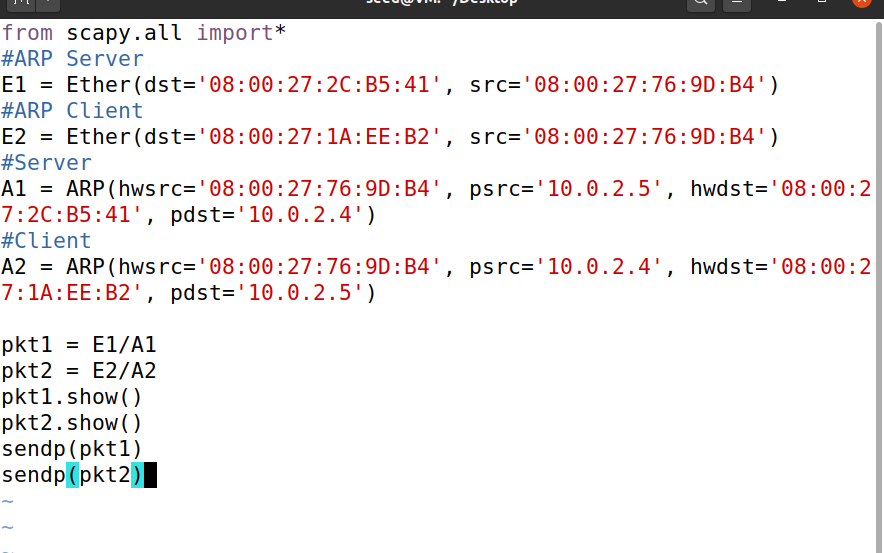
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Kiểm tra bảng arp của máy client không thấy địa chỉ của server do không thực hiện gửi gói tin ARP đi

## MITM Attack on Telnet using ARP Cache Poisoning

### + Mục tiêu bài này ta sẽ viết code để trong ARP cache của Server thì IP của Client sẽ là MAC của Attacker, và trong ARP cache của Client IP của Server sẽ là MAC của Attacker



+ Tại máy của attacker ta viết chương trình để trong ARP cache của client và server đều có MAC của attacker nhưng đĩa chỉ IP tại máy server lại là của client và ngược lại

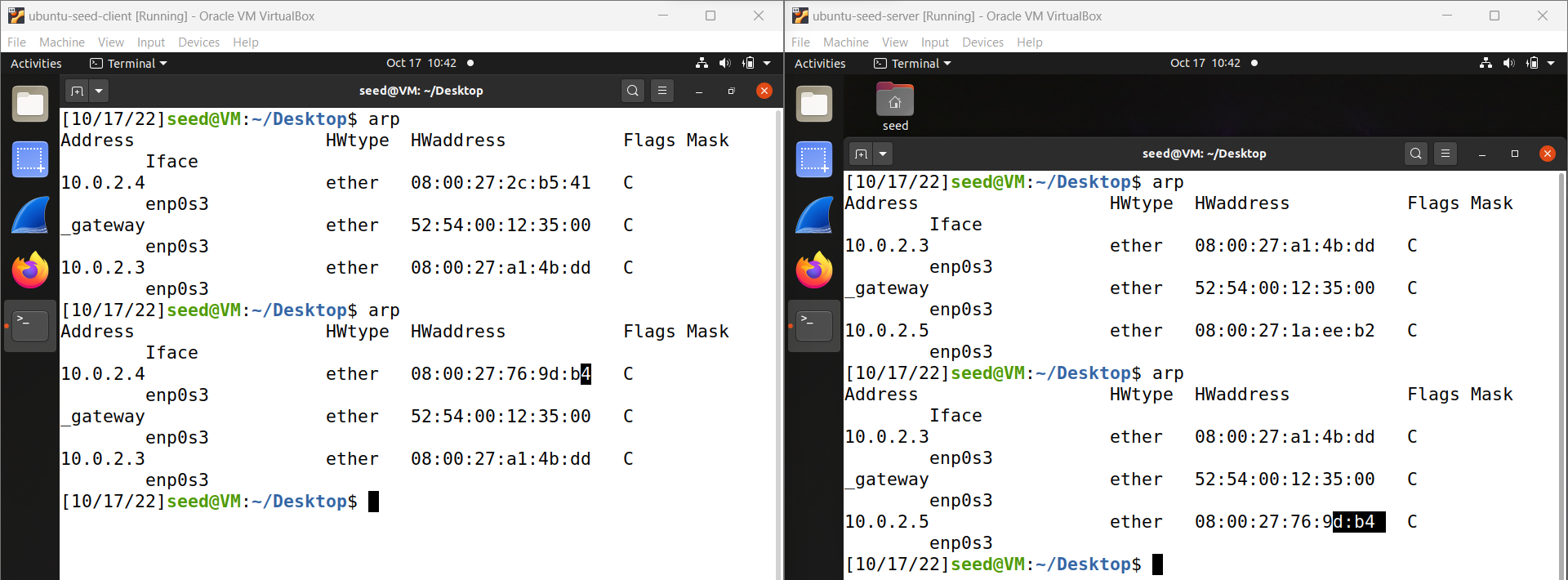
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Kiểm tra bảng ARP của client và server đều bình thường

Ảnh có chứa văn bản

Mô tả được tạo tự động+ Tại máy attacker ta chạy chương trình



+ Kiểm tra lại ARP cache của client và server thì MAC đã bị đổi thành của attacker

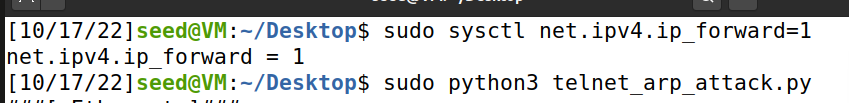
+ Giờ đây khi cả 2 giao tiếp với nhau thì nghĩa là đang giao tiếp với attacker

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

+ Nhưng khi ta thử ping từ máy client sang server thì bảng ARP lại được cập nhật lại

* Do bên máy attacker ta chưa bật chế độ để chuyển tiếp gói tin



+ Giờ ta bật chế độ chuyển tiếp gói tin bên máy attacker sau đó thực hiện chạy lại chương trình

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta kết nối telnet tới máy của server từ client

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Sau đó tại máy attacker ta viết 1 chương trình giả mạo gói tin ta lấy được từ client sau đó sửa thành thông tin ta muốn client cung cấp

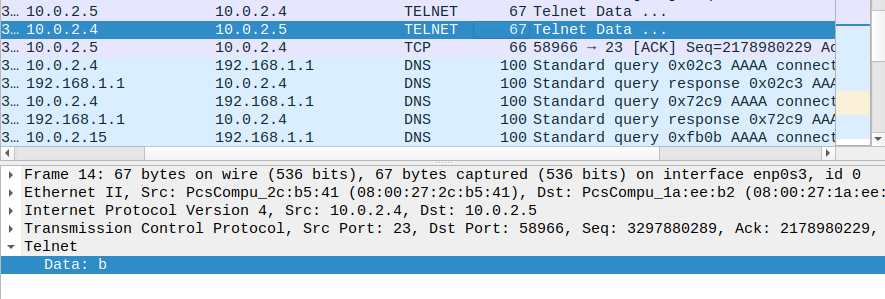
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Chạy chương trình



+ Tại máy client ta viết thử ký tự ‘b’ lúc này client vẫn đang kết nối tới server qua telnet



+ Bên máy attacker ta bắt được gói tin từ nguồn là client ip 10.0.2.4 và dest là 10.0.2.5 và data là ký tự b ta vừa gõ bên máy client dù máy client vẫn đang telnet tới máy server

## MITM Attack on Netcat using ARP Cache Poisoning

+ Mục tiêu tương tự task 2 ở trên nhưng ở đây clietn và server giao tiếp với nhau thông qua netcat

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tại máy attacker ta viết chương trình tương tự task 2 để bắt gói tin và sau đó giả mạo gói đã bắt được

Ảnh có chứa văn bản

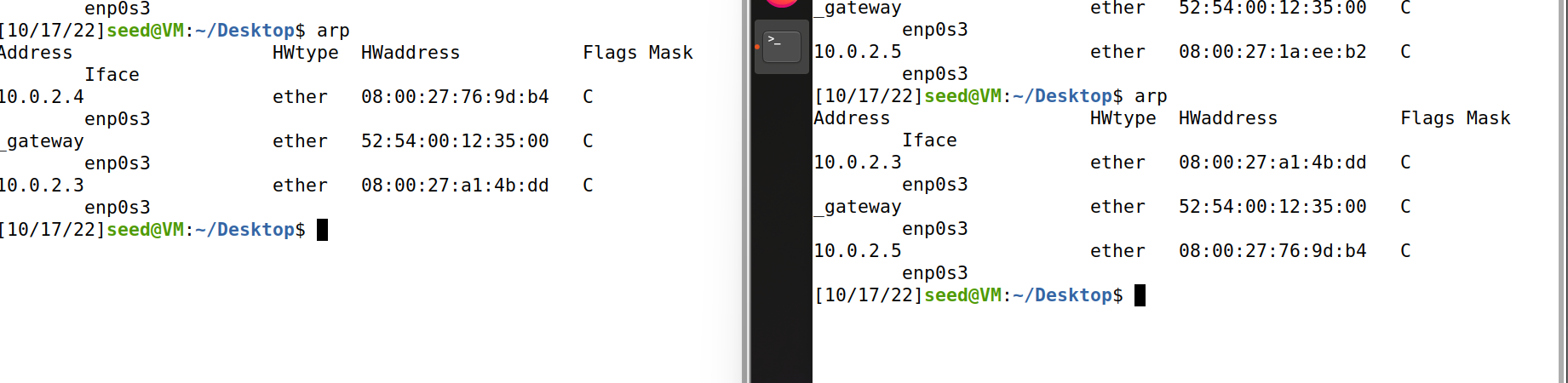
Mô tả được tạo tự động

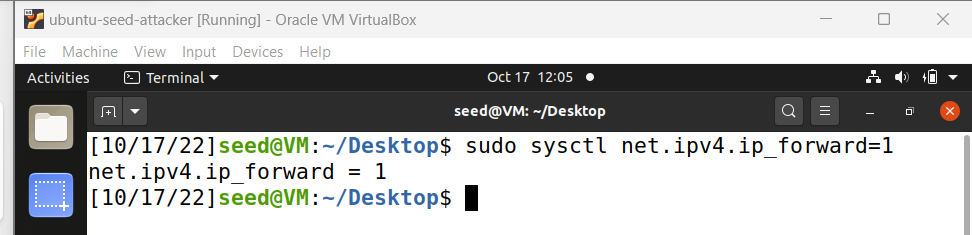
+ Tại máy client và server kiểm tra ARP cache đều bình thường

Ảnh có chứa văn bản

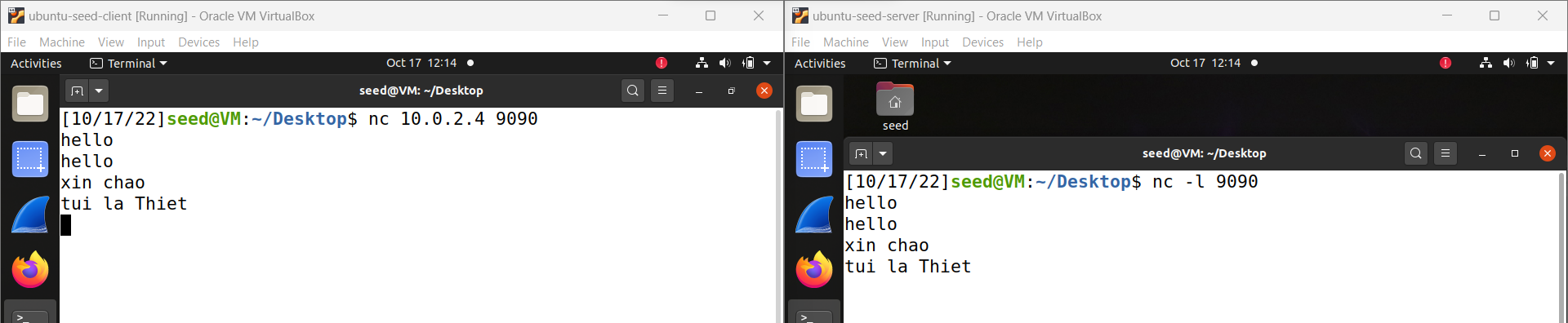
Mô tả được tạo tự động

+ Tại máy attacker ta chạy lại chương trình để tahy thế IP của client và server trong ARP cache tương ứng thành MAC của attacker

+ Ta đã thay thế được IP của của server và client tương ứng thành MAC của attacker



+ Tại máy attacker ta mở chế độ chuyển tiếp gói tin để attkacer có thể đứng giữa cuộc giao tiếp



+ Khi ta kết nối netcat giữa client và server qua port 9090 thì giao tiếp giữa 2 bên đều bình thường

+ Do bên attacker ta vẫn để chế độ chuyển tiếp gói tin

# TÀI LIỆU THAM KHẢO