BÀI THỰC HÀNH SỐ 2

**Phân tích kỹ thuật tấn công ARP Cache Poisoning**

1. **Giới thiệu chung**
   1. **Mục đích**

ARP là giao thức mạng được sử dụng để tìm kiếm địa chỉ MAC của một nút trong mạng LAN khi đã biết địa chỉ IP của nút đó. ARP là một giao thức đơn giản và không triển khai bất kỳ cơ chế an toàn bảo mật nào. Tấn công ARP Cache Poisoning(hay còn gọi là ARP Spoofing) là một kỹ thuật tấn công phổ biến mà đối phương đánh lừa các máy nạn nhân chấp nhận một ánh xạ giả mạo từ địa chỉ IP sang địa chỉ MAC của một máy khác nằm dưới quyền điều khiển của hắn. Điều đó khiến cho lưu lượng mạng tới máy đích được chuyển hướng sang máy của đối phương.

Mục đích của bài thực hành này là để sinh viên thử nghiệm kịch bản tấn công ARP Cache Poisoning và các tấn công leo thang khác. Trên cơ sở đó, sinh viên có thể phân tích để xác định các đặc điểm của dạng tấn công này. Sau khi hoàn thành bài thực hành này, sinh viên được tích lũy các kiến thức và kỹ năng liên quan đến tấn công ARP Cache Poisoning.

* 1. **Môi trường thực hành**
* Hệ điều hành: Linux Ubuntu
* Các công cụ: Docker, Wireshark, Python

**1.3. Chuẩn bị thực hành**

* Đọc lại bài giảng và các tài liệu về tấn công ARP Cache Poisoning
* Đọc tài liệu thực hành
* Hoàn thành đúng >50% số câu hỏi trắc nghiệm chuẩn bị thực hành
* Luyện tập sử dụng các công cụ trong bài thực hành

1. **Một số thao tác căn bản với Docker**

Môi trường thực hành được triển khai trên các máy ảo Linux Ubuntu trong Docker được gọi là container. Các container này được thi trên một máy chứa gọi là host. Sau đây là một số lệnh thao tác căn bản cần sử dụng trong bài thực hành:

* Xây dựng các container: $ docker-compose build
* Khởi động các container: $ docker-compose up

Có thể tắt container bằng cách nhấn tổ hợp phím Ctrl + C nhưng file ảnh (image) của container không bị xóa.

* Tắt container và xóa file ảnh: $ docker-compose down
* Liệt kê các container: $ dockps
* Truy cập và thực thi lệnh shell trên container: $ docksh <container\_id>

Trong đó <container\_id> chỉ cần một vài ký tự đầu tiên trong ID của container. Có thể mở nhiều cửa sổ Terminal để kết nối tới cùng một container.

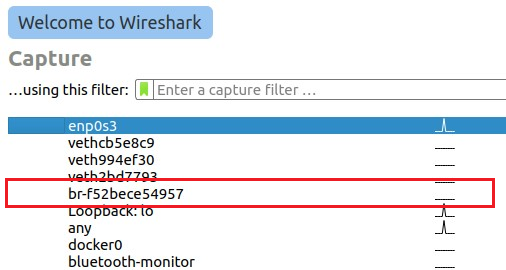
* Khởi động lại container: $ docker restart <container\_id>
* Sao chép file từ máy host sang thư mục /tmp trên Docker container

$ docker cp <file\_on\_host> <container\_id>:/tmp

* Sao chép file từ thư mục /tmp trên Docker container sang máy host

$ docker cp <container\_id>:/tmp/<filename> <file\_on\_host>

* Bắt gói tin trong mạng ảo hóa của Docker bằng Wireshark: chọn cạc mạng bắt đầu bằng **br-**



* Bắt gói tin trong máy ảo container và lưu lại

# tcpdump -i eth0 -n -w <file\_name.pcap>

1. **Tổ chức thực hành**

* Sinh viên làm bài thực hành theo nhóm đã phân công.
* Mỗi nhóm thực hiện các kịch bản tấn công đã mô tả sau đây.
* Mỗi nhóm viết báo cáo theo mẫu dựa trên kết quả thực hiện các kịch bản tấn công

Trên máy tính tại phòng thực hành, các bạn được cung cấp một máy ảo VM chạy hệ điều hành Ubuntu 20.04 trong phần mềm ảo hóa Virtualbox. Máy ảo VM này đóng vai trò là máy chứa (host) cho các Docker container. Các kịch bản tấn công được thực hiện trên mạng ảo hóa bằng Docker như sau:

A picture containing shape

Description automatically generated

1. **Nội dung thực hành**
   1. **Triển khai hệ thống (1 điểm)**

Triển khai hệ thống ảo hóa cho bài thực hành theo các bước sau:

* **Bước 1:** Trên máy host, truy cập vào thư mục ~/it4263lab/lab02
* **Bước 2:** Sửa thông số địa chỉ IP cho các container trong file docker-compose.yml với x là 2 số cuối trong mã lớp thực hành, y là số thứ tự của nhóm.
* **Bước 3:** Xây dựng các container cho bài thực hành và khởi động chúng
* **Bước 4:** Truy cập vào các container để thực thi các lệnh shell
* **Bước 5:** Xác định các thông số địa chỉ của các container bằng lệnh **$ ifconfig**

Ghi nhận các thông số vào báo cáo

* **Bước 6:** Kiểm tra kết nối giữa các container bằng lệnh ping
* **Bước 7:** Hiển thị các ánh xạ trong bảng ARP Table của máy User và Server bằng lệnh **$ arp -n**

Chụp ảnh màn hình kết quả và chèn vào báo cáo.

* 1. **Kịch bản tấn công 1 (2 điểm)**

Trong kịch bản này, các bạn được cung cấp file thực thi kịch bản tấn công **scenario1.py**.

* **Bước 1:** Sửa các tham số trong file thực thi tấn công ~/it4263lab/lab02/attack/scenario1.py sao cho phù hợp với các thông số của máy ảo container.
* **Bước 2:** Khởi động Wireshark trên máy host VM và chọn cạc mạng để bắt lưu lượng trong mạng của Docker
* **Bước 3:** Thực thi tấn công trên máy Attacker **$ python3 scenario1.py**
* **Bước 4:** Hiển thị các ánh xạ trong bảng ARP Table của máy User và Server. Chụp ảnh màn hình kết quả và chèn vào báo cáo.
* **Bước 5:** Dừng bắt gói tin trên Wireshark.

Viết báo cáo giải thích quá trình tấn công.

* 1. **Kịch bản tấn công 2 (2 điểm)**

Trong kịch bản này, các bạn được cung cấp file thực thi kịch bản tấn công **scenario2.py**.

* **Bước 1:** Sửa các tham số trong file thực thi tấn công ~/it4263lab/lab02/attack/scenario2.py sao cho phù hợp với các thông số của máy ảo container.
* **Bước 2:** Khởi động Wireshark trên máy host VM và chọn cạc mạng để bắt lưu lượng trong mạng của Docker
* **Bước 3:** Thực thi tấn công trên máy Attacker **$ python3 scenario2.py**
* **Bước 4:** Hiển thị các ánh xạ trong bảng ARP Table của máy User và Server. Chụp ảnh màn hình kết quả và chèn vào báo cáo.
* **Bước 5:** Dừng bắt gói tin trên Wireshark.

Viết báo cáo giải thích quá trình tấn công.

* 1. **Kịch bản tấn công 3 (3 điểm)**

Trong kịch bản này, các bạn thực hiện tấn công man-in-the-middle để can thiệp vào quá trình truyền tin giữa máy User và Server. Các bạn được cung cấp file thực thi tấn công **mitm.py** nhằm sửa đổi thông điệp mà máy User gửi cho máy Server.

* **Bước 1:** Sửa các tham số trong file thực thi tấn công **mitm.py** sao cho phù hợp với các thông số của máy ảo container.
* **Bước 2:** Trên cửa sổ thực thi shell tại máy User, thực hiện lệnh tcpdump để bắt lưu lượng
* **Bước 3:** Trên cửa sổ thực thi shell tại máy Server, thực hiện lệnh tcpdump để bắt lưu lượng
* **Bước 4:** Trên máy Server thực hiện lệnh **$ nc -lp 10101**
* **Bước 5:** Trên máy User thực hiện lệnh **$ nc <Server\_IP\_address>** **10101** và gửi thông điệp bất kỳ tới Server sau khi kết nối được thiết lập.
* **Bước 6:** Trên máy Attacker, thực hiện tấn công ARP Cache Poisoning tới máy User và Server sao cho khi mỗi máy gửi dữ liệu cho bên kia thì đều bị chuyển hướng tới máy Attacker
* **Bước 7:** Trên máy Attacker thực hiện lệnh sau để máy này có thể chuyển tiếp dữ liệu giữa User và Attacker

**$ sysctl net.ipv4.ip\_forward=1**

* **Bước 8:** Trên máy Attacker, thực thi kịch bản tấn công **mitm.py**
* **Bước 9:** Trên máy User, gửi một số thông điệp bất kỳ tới Server và quan sát kết quả.
* **Bước 10:** Dừng bắt gói tin trên các máy.

Viết báo cáo giải thích quá trình tấn công.

* 1. **Phòng chống tấn công (2 điểm)**

Trên máy User, thực hiện lệnh sau để thiết lập một ánh xạ cố định trong bảng ARP Table

**$ arp -s <Server\_IP\_address> <Server\_MAC\_address>**

Thực hiện lại một kịch bản tấn công bất kỳ và cho biết đối phương có thành công không?