BÁO CÁO BÀI TẬP

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

**Tên chủ đề: – ICMP Recirect 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 |

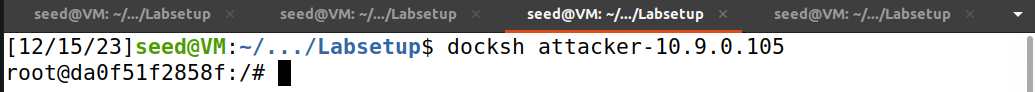
1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

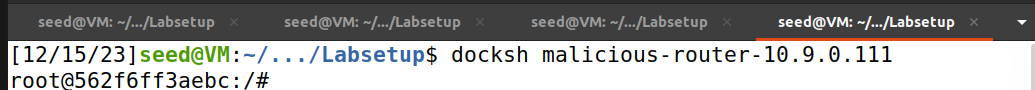
|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung |  | Trang |
| 01 | Task 1: Launching ICMP Redirect Attack | | 02 - 07 |
| 02 | Task 2: Launching the MITM Attack | | 07 - 11 |

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

BÁO CÁO CHI TIẾT

\* Tiến hành thiết lập môi trường dựa trên Labsetup.zip được cung cấp sẵn:





A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

*Hình 1, 2, 3, 4. Thiết lập môi trường và kiểm tra kết nối giữa host và victim*

**1. Task 1: Launching ICMP Redirect Attack** - Trong thiết lập hiện tại, nạn nhân sử dụng bộ chứa router (192.168.60.11) để truy cập vào mạng 192.168.60.0/24.

A close up of black text

Description automatically generated

*Hình 5. Kết quả trả về của ip route tên máy victim*

- Thực hiện tấn công: ở trên máy attacker, thực hiện tạo file tấn công như sau:

A screenshot of a computer

Description automatically generated

*Hình 6. Nội dung file thực thi tấn công*

Đoạn code này tạo ra gói tin ICMP Redirect để thông báo với victim ('10.9.0.5') sẽ chuyển hướng (type = 5 (Redirect)) vì mạng đích đã thay đổi/không còn khả dụng (code = 1) và sẽ sử dụng router độc hại malicious-router ('10.9.0.111') của attacker như là gateway để truy cập vào mạng '192.168.60.0/24' thay vì sử dụng router mặc định '10.9.0.11'.

- Trên máy victim tiến hành ping đến máy host và các hoạt động được ghi lại trong log.txt: 

- Tiến hành chạy file icmp-task1 trên máy attacker:

**A white background with black text

Description automatically generated**

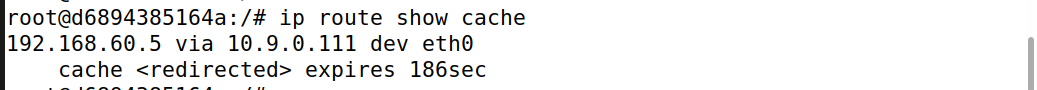
*Hình 7. Attacker thực hiện tấn công*

- Trên máy victim, thực hiện  để thực hiện một cuộc truy vấn traceroute đến địa chỉ IP 192.168.60.5

A screenshot of a computer screen

Description automatically generated

*Hình 8. Kết quả truy vấn traceroute của máy victim*

**

*Hình 9. Kết quả ip route show cache của victim*

***\* Câu hỏi:***

***1. Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation. (Có thể sử dụng các cuộc tấn công chuyển hướng ICMP để chuyển hướng đến một máy từ xa không? Cụ thể, địa chỉ IP được gán cho icmp.gw là một máy tính không nằm trong mạng LAN cục bộ. Hãy trình bày kết quả thí nghiệm và giải thích quan sát.)***

***→*** Không thể sử dụng các tấn công chuyển hướng ICMP để chuyển hướng đến một máy từ xa, bởi vì các cuộc tấn công chuyển hướng ICMP thường chỉ áp dụng trong mạng LAN và không được thiết kế để chuyển hướng lưu lượng đến các máy tính từ xa không nằm trong mạng LAN. Có nghĩa là nếu địa chỉ IP được gán cho icmp.gw không thuộc mạng LAN, thì việc thực hiện cuộc tấn công chuyển hướng ICMP có thể không có hiệu quả.

\* Thực hiện chỉnh sửa lại file icmp-task1, icmp thành 192.168.0.111 (ip nằm ngoài mạng LAN) như sau:

***A screenshot of a computer

Description automatically generated***

*Hình 10. Nội dung file thực thi tấn công, icmp.gw là một ip ngoài mạng LAN*

- Thực hiện tấn công như lúc nãy và kiểm tra mtr -n 192.168.60.5 và ip route show cache thu được

A white background with black text

Description automatically generated

***A screen shot of a computer

Description automatically generated***

*Hình 11, 12. Kết quả kiểm tra, nhận thấy đã không xuất hiện ip của malicious-router, tức cuộc tấn công không thành công*

***2. Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation. (Có thể sử dụng các cuộc tấn công chuyển hướng ICMP để chuyển hướng đến máy không tồn tại trên cùng mạng? Cụ thể, địa chỉ IP được gán cho icmp.gw là một máy tính cục bộ là ngoại tuyến hoặc không tồn tại. Vui lòng hiển thị kết quả thử nghiệm của bạn và giải thích quan sát.)***

***→*** Không thể sử dụng các tấn công chuyển hướng ICMP để chuyển hướng đến một máy không tồn tại hoặc ngoại tuyến. Khi gửi gói tin ICMP redirect, đang cố gắng thông qua thông báo chuyển hướng ICMP rằng có một đường đi tốt hơn thông qua địa chỉ IP được chỉ định trong icmp.gw. Tuy nhiên, nếu địa chỉ IP đó không tồn tại hoặc không hoạt động, hệ thống đích có thể không chấp nhận hoặc bỏ qua thông báo này.

***A computer screen with numbers and symbols

Description automatically generated***

*Hình 13. Nội dung file thực thi tấn công, icmp.gw là một ip không tồn tại*

- Thực hiện tấn công như lúc nãy và kiểm tra mtr -n 192.168.60.5 và ip route show cache thu được

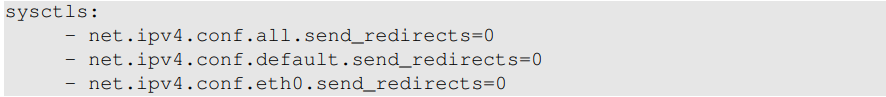
******

***A close-up of a graph

Description automatically generated***

*Hình 14, 15. Kết quả kiểm tra, nhận thấy đã không xuất hiện ip của malicious-router, tức cuộc tấn công không thành công*

***3.*** ***If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation (Nhìn vào tệp docker-compose.yml, sẽ tìm thấy các mục cho vùng chứa bộ định tuyến độc hại. Mục đích của những mục này là gì? Hãy thay đổi giá trị của chúng thành 1 và thực hiện lại cuộc tấn công. Hãy mô tả và giải thích quan sát.)***

******

- Các mục này được sử dụng để tắt chức năng gửi các thông báo chuyển hướng ICMP trên giao diện mạng eth0 của vùng chứa bộ định tuyến độc hại. Khi giá trị của các mục này được đặt thành 0, chức năng gửi các thông báo chuyển hướng sẽ bị vô hiệu hóa.

- Thực hiện sửa file và tấn công lại:

A screen shot of a computer

Description automatically generated

*Hình 16. Thực hiện chỉnh sửa trong file docker-compose.yml*

A screenshot of a computer

Description automatically generated

*Hình 17. File thực thi tấn công*

**A screen shot of a computer

Description automatically generated**

**A black text on a white background

Description automatically generated**

*Hình 18, 19. Kết quả thực hiện, cuộc tấn công không thành công*

**2. Task 2: Launching the MITM Attack**

- Thực hiện tắt chuyển tiếp trên file docker-compose.yml:

A screenshot of a computer

Description automatically generated

*Hình 20. Thực hiện tắt chuyển tiếp*

- Hoàn thiện file MITM.py trên malicious-router

- Thực hiện tấn công theo các bước hướng dẫn:

- Trên máy host 192.168.60.5 thực hiện bật netcat server và trên máy victim thực hiện kết nối đến server:

***\*Câu hỏi:***

***4. In your MITM program, you only need to capture the traffics in one direction. Please indicate which direction, and explain why (Trong chương trình MITM của bạn, bạn chỉ cần bắt các gói tin theo một hướng. Vui lòng chỉ ra hướng nào và giải thích tại sao).***

→ Cần thực hiện lọc các gói từ victim đến máy chủ vì các gói cần thay đổi đều theo hướng này.

***5. In the MITM program, when you capture the nc traffics from A (10.9.0.5), you can use A’s IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion (Trong chương trình MITM, khi bắt các gói tin từ A (10.9.0.5), có thể sử dụng địa chỉ IP hoặc địa chỉ MAC của A trong bộ lọc. Một trong những lựa chọn không tốt và sẽ tạo ra vấn đề. Vui lòng thử cả hai và sử dụng kết quả thử nghiệm của bạn để cho thấy lựa chọn nào đúng và hãy giải thích kết luận của bạn)***

*a, Địa chỉ IP*

***A screen shot of a computer

Description automatically generated***

*Hình 21. Code với bộ lọc là địa chỉ IP*

*A white background with black text

Description automatically generated*

*Hình 22. Kết nối đến nc Server và gửi thông tin trên máy victim*

*A white background with black and white clouds

Description automatically generated*

*Hình 23. Kết quả nhận được trên máy host*

***A screenshot of a computer

Description automatically generated***

*Hình 24. Kết quả ở malicious-router: hiện thị loạn xạ và trong một vòng lặp vô hạn*

*b, Địa chỉ MAC*

*A screen shot of a computer

Description automatically generated*

*Hình 25. Code với bộ lọc là địa chỉ MAC*

*A number of numbers on a white background

Description automatically generated*

*Hình 26. Kết nối đến nc Server và gửi thông tin trên máy victim*

**

*Hình 27. Kết quả nhận được trên máy host*

*A white background with black text

Description automatically generated*

*Hình 28. Kết quả ở malicious-router: các gói tin được gửi lần lượt và không bị lặp vô hạn*

**→ Nhận xét:** Nên chọn cách lọc theo địa chỉ MAC sẽ tốt hơn, tránh bị rơi vào lặp vô hạn và nhảy liên tục như địa chỉ IP.

**---HẾT---**

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