|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **KHOA CÔNG NGHỆ THÔNG TIN 1** |
|  |
| **BÀI THỰC HÀNH 8**  **THỰC TẬP CƠ SỞ** |
| **Họ và tên : Đinh Quang Hiếu**  **Mã sinh viên: B19DCAT065**  **Giảng viên giảng dạy: Hoàng Xuân Dậu** |
| **HÀ NỘI, THÁNG 4/2022** |

**Bài 8: Bắt dữ liệu mạng**

**I. Giới thiệu chung**

**1. Mục đích**

• Tìm Sử dụng tcpdump để bắt gói tin mạng

• Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP/TCP/IP)

• Sử dụng Network Miner để bắt và phân tích gói tin mạng

**2. Yêu cầu**

• Tìm hiểu lý thuyết o Tcpdump

▪ Là công cụ được phát triển nhằm mục đích nhận diện và phân tích các gói dữ liệu mạng theo dòng lệnh.

▪ Cho phép người dùng hiển thị TCP/IP và các gói khác đang được truyền hoặc nhận qua mạng mà máy tính được gắn vào.

▪ Tcpdump hoạt động trên hầu hết các hệ điều hành Unix : Linux , Solaris , FreeBSD,… o Wireshark

▪ Là một ứng dụng dùng để bắt (capture), phân tích và xác định các vấn đề liên quan đến network như: rớt gói tin, kết nối chậm, hoặc các truy cập bất thường.

▪ Cho phép bắt các packet trong thời gian thực (realtime), lưu trữ chúng lại và phân tích offline. Ngoài ra, nó bao gồm các tính năng filter, color coding,...

▪ Có thể sử dụng trên Linux, MacOS và Windows o Network Miner

▪ Là một công cụ phân tích pháp y mạng (NFAT) mã nguồn mở

▪ Có thể phân tích cú pháp tệp PCAP để phân tích ngoại tuyến và tái tạo/tập hợp lại các tệp PCAP.

▪ Dễ dàng thực hiện phân tích lưu lượng mạng nâng cao bằng cách cung cấp các tạo tác được trích xuất trong giao diện người dùng trực quan.

• Chuẩn bị o Phần mềm VMWare Workstation o File máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 5 o Topo mạng như đã cấu hình trong bài 5

**3. Các bước thực hiện**

-Sử dụng tcpdump

a) Các bước thực hiện

o Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#ifconfig -a), kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp.

Text

Description automatically generated

* Khởi động tcpdump. Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file(thời gian chờ dữ liệu trong khoảng 2 phút)

Text

Description automatically generated

* Đăng nhập Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external.

Text

Description automatically generated

* Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap

Text

Description automatically generated

b) Kết quả cần đạt được

o Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump

Text

Description automatically generated

**- Sử dụng Wireshark để bắt và phân tích các gói tin**

a) Các bước thực hiện

o Có thể tải Wireshark ở đây: <http://www.wireshark.org/download.html>

o Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0

Graphical user interface

Description automatically generated

* Trên máy Windows 7 Attack kết nối tới ftp server (C:\ftp 192.168.100.201) trên máy Window Server Internal Victim

Text

Description automatically generated

* Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp

A screenshot of a computer

Description automatically generated

* Trên máy Windows attack, trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0

Graphical user interface, text, application, email

Description automatically generated

* Trên máy Window Server 2003 victim, kết nối với ftp server (root@bt:~#ftp 10.10.19.202)

Text

Description automatically generated

Text

Description automatically generated

* Trên Window 7 dừng quá trình bắt gói tin và lọc theo giao thức ftp

Graphical user interface, application

Description automatically generated

**- Sử dụng Network Miner để bắt và phân tích các gói tin**

a) Các bước thực hiện

o Trên máy Windows 7 Internal Attack khởi động và chọn Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) và bắt đầu bắt gói tin.

Graphical user interface, text, application

Description automatically generated

* Sử dụng Internet Explorer để kết nối đến trang web của Windows Server Internal Victim: http://192.168.100.201/ Sau đó dừng quá trình bắt gói tin

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Graphical user interface, application, Word

Description automatically generated