**Môn học Thực tập cơ sở**

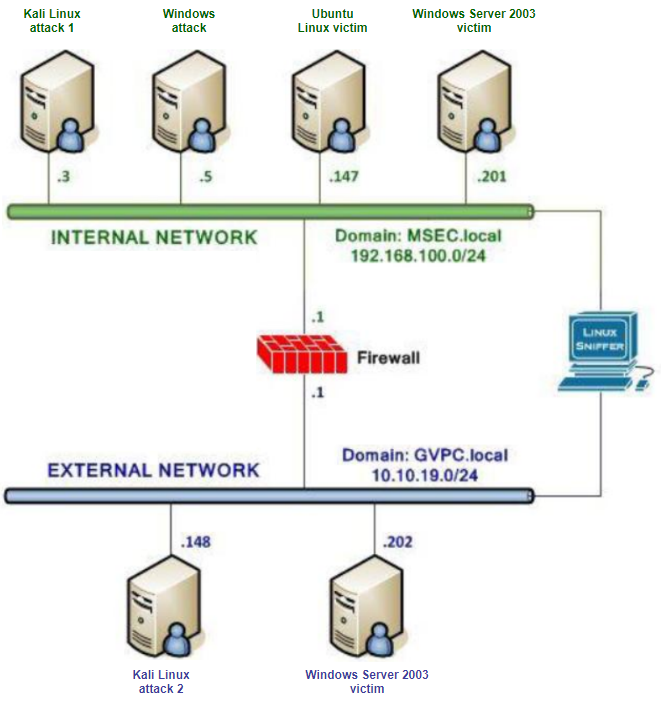
**Bài 8: Bắt dữ liệu mạng**

1. ***Mục đích***

Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ liệu mạng, bao gồm:

1. Sử dụng tcpdump để bắt gói tin mạng
2. Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)
3. Sử dụng Network Miner để bắt và phân tích gói tin mạng
4. ***Nội dung thực hành***
   1. *Tìm hiểu lý thuyết*

* Tìm hiểu về tính năng và hoạt động của một số công cụ bắt dữ liệu mạng như: tcpdump, Wireshark, Network Miner…
* Một số tài liệu tham khảo:
  + Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021
  + <https://www.tcpdump.org/index.html#documentation>
  + <https://www.wireshark.org/docs/wsug_html/>
  + <https://docs.securityonion.net/en/2.3/networkminer.html#>
  1. *Chuẩn bị môi trường*
* Phần mềm VMWare Workstation( hoặc các phần mềm hỗ trợ ảo hóa khác).
* Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
* Topo mạng như đã cấu hình trong bài 5.



* 1. *Các bước thực hiện và kết quả cần đạt*
     1. *Sử dụng tcpdump*

*a) Các bước thực hiện*

* Trên máy Windows attack trong mạng Internal, đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#**ifconfig -a**)
* Trên máy Windows attack trong mạng Internal, kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp, sau đó 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 5 phút).
* Trên máy Window victim, đăng nhập Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external
* Trên máy Window attack, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.

*b) Kết quả cần đạt được*

* Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump
* Minh chứng:

- Chụp ảnh minh chứng màn hình với các lệnh trong cmd trong máy Windows attack:

+ echo %USERNAME%

+ date

+ Kết quả chạy #**tcpdump –i eth0 icmp**

+ Kết quả chạy **#tcpdump –i eth1 icmp**

+ Các file pcap tương ứng

* + 1. *Sử dụng Wireshark để bắt và phân tích các gói tin*

*a) Các bước thực hiện*

* Có thể tải Wireshark ở đây: http://www.wireshark.org/download.html
* Trên máy Windows attack, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong **Capture Interfaces** chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0
* Trên máy Windows 7 victim kết nối tới ftp server (C:\**ftp 192.168.100.201)**
* Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp
* Trên máy Windows attack, trong **Capture Interfaces** chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0
* Trên máy Window Server 2003 victim, kết nối với ftp server(root@bt:~#**ftp 10.10.19.202)**
* Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp

*b) Kết quả cần đạt được*

* Sử dụng Wireshark để bắt và lọc ra được các gói tin ftp, các file pcap tương ứng
* Minh chứng:

- Chụp ảnh minh chứng với các lệnh trong cmd: Trong máy Windows attack mạng Internal, gõ lệnh:

+ echo %USERNAME%

+ date

+ Kết quả bắt gói tin từ máy Window 7, và máy Window Server 2003

+ Các file pcap tương ứng

* + 1. *Sử dụng Network Miner để bắt và phân tích các gói tin*

a) Các bước thực hiện

* Trên máy Windows 7 Internal Attack khởi động Network Miner và chọn **Socket: Intel® PRO/1000MT Network Connection(192.168.100**.**5)** và bắt đầu bắt gói tin. Sử dụng Internet Explorer để kết nối đến trang web của Windows 2003 Server Internal Victim: <http://192.168.100.201/>. Sau đó dừng quá trình bắt gói tin.
* Trong Network Miner, chọn File/ index.html để xem dữ liệu gói tin vừa bắt được.

*b) Kết quả cần đạt được*

* Bắt được các dữ liệu trong file index.html.
* Minh chứng:

- Chụp ảnh minh chứng với các lệnh trong cmd: Trong máy Windows attack mạng Internal, gõ lệnh:

+ echo %USERNAME%

+ date

+ Kết quả bắt gói tin từ máy Window 7, và máy Window Server 2003

+ File index.html chứa dữ liệu của máy victim.

1. ***Các yêu cầu với báo cáo bài thực hành***

Báo cáo bài thực hành cần có đầy đủ các nội dung/thành phần sau:

* Trang bìa (ghi rõ môn học, bài thực hành, mã sv và họ và tên.
* Trình bày vắn tắt về các nội dung lý thuyết đã tìm hiểu được trong mục 2.1.
* Các nội dung thực hành cần kèm ảnh minh chứng theo thứ tự thực hiện các bước.
* Đặt tên file theo định dạng kiểu như sau: *Bài thực hành 8\_Họ tên SV\_Mã SV*