**Nội dung và hướng dẫn thực hành**

**Mục đích**

* Giúp sinh viên hiểu được kỹ thuất tấn công MAN-IN-THE-MIDDEL, cách sử dụng công cụ tấn công ETTERCAP để nghe lén

**Yêu cầu đối với sinh viên**

* Có kiến thức cơ bản về hệ điều hành LINUX

**Nội dung bài lab**

* Khởi động bài lab

*labtainer  -r ptit-ettercap*

(chú ý: sinh viên sử dụng email stu.ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong  ba terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách là victim, một  cái đại diện cho máy chủ là : server, một cái đại diện cho hacker là attacker. Biết rằng ba máy nằm trong cùng mạng lan

**Task 1 : Enable IP Forward trên máy attacker**

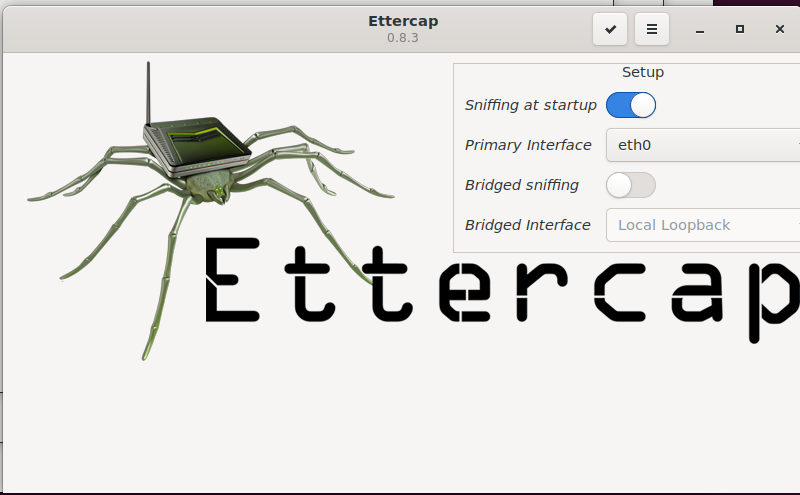
* Tạo một folder logging

mkdir logging

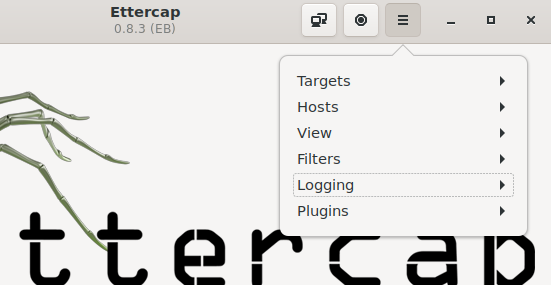
chmod -R 777 logging

* Khởi động Ettercap với người dùng root

*sudo ettercap -G &*



* Tiếp tục bằng cách click vào nút dấu tick



* Logging 🡪 Chọn ghi lại file log

Log user message

* Sau đó lưu tại thư mục */home/ubuntu/logging* với tên là *log*

*/home/ubuntu/logging/log*

* Trên máy attacker Enable ip forward :

*sudo sysctl net.ipv4.conf.all.forwarding=1*

**Task 2: Scan host**

* Hosts 🡪 Scan for hosts
* Quét host và hiển thị ip máy được quét

Scan for hosts

* Trên máy server Config server database tại đường dẫn /*var/www/mutillidae/config.inc* sửa mục dbname

*$dbname = 'owasp10';*

* Khởi động lại webserver:

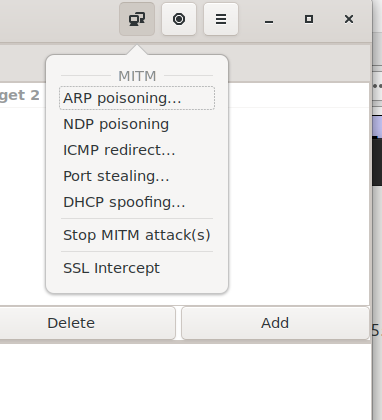
*sudo /etc/init.d/apache2 reload*

**Task 3: Lấy thông tin username và password**

* Trên máy victim mở trình duyệt firefox truy cập web server:

*http://192.168.1.2/mutillidae/index.php?page=login.php*

* Trên ettercap chọn kỹ thuật tấn công ARP poisoning và bắt đầu tấn công



* Trên vicim đăng nhập với tài khoản (email đăng nhập) và mật khẩu (trước đó hãy đăng ký tài khoản và mật khẩu tương ứng với mã sinh viên nhập vào làm bài lab) (chú ý: nếu nhập sai username không đúng với mail làm bài lab thì sẽ phải làm lại từ đầu)
* Bắt được username và password của victim trên ettercap
* Kết thúc bài lab:

Kiểm tra checkwork:

*checkwork*

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thục bài lab:

*Stoplab*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạp và lưu vào một vị trí hiển thị dưới stoplab

* Khởi động lại bài lab:

*Labtainer -r ptit-ettercap*