BÀI THỰC HÀNH SỐ 2
Môn: MẬT MÃ & AN NINH MẠNG
-o0o-

I. MỤC TIÊU
Mục tiêu của bài thực hành này cung cấp kiến thức liên quan đến dò quét mạng, nghe lén thông tin, dữ liệu và xâm nhập một máy chủ.
Các nội dung chính trong bài thực hành gồm:
- Tìm hiểu và sử dụng Kali Linux và các công cụ liên quan
- Thu thập thông tin mạng bằng cách quét mạng
- Nghe lén thông tin, dữ liệu
- Cài đặt máy chủ CentOS 7 trên Virtual Box
- Tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7
- Giải pháp giảm thiểu tấn công vét cạn nói trên

II. TÀI LIỆU THAM KHẢO
[1]. How to Install Kali Linux on VirtualBox
[2]. How to Install CentOS7 on VirtualBox
[3]. VirtualBox Networking

III. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH
Trang thiết bị và các phiên bản phần mềm sử dụng:
- 01 máy tính.
- Hệ điều hành: MS Windows 7/10.
- Download Virutal Box, máy ảo Kali Linux tương ứng, Tập tin ISO của hệ điều hành CentOS 7

IV. CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI
- Sinh viên trả lời tất cả các câu hỏi trong bài thực hành vào file **<MSSV>_Lab02.docx** và nộp bài theo deadline của bài Lab02 ở Bkel, không nhận bài nộp qua email hay các hình thức khác.
- Thời gian để thực hiện bài Lab là 14 ngày.

V. NỘI DUNG THỰC HIỆN
1. Tìm hiểu Kali Linux và các công cụ liên quan

- Kali Linux là gì ?

……
……
……

- Hãy cho biết các nhóm công cụ liên quan hiện có trên Kali Linux

……
……
……

2. Cài đặt máy ảo Kali Linux

- Cài đặt môi trường ảo hóa (Virtual Box). Hãy cho biết các bước và một số hình ảnh:

……
……
……

- Dowload và tạo máy ảo Kali Linux. Hãy cho biết các bước và một số hình ảnh:

……
……
……

3. Thu thập thông tin mạng bằng cách quét mạng

- Sử dụng công cụ Nmap/Zenmap. Hãy cho biết các bước và một số hình ảnh:

……
……
……

- Sử dụng Angry IP Scanner. Hãy cho biết các bước và một số hình ảnh:

……
……
……

- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

……
……
……

- Biện pháp đối phó đối với loại hình tấn công là gì ?

……
……
……

4. Nghe lén thông tin, dữ liệu

- Dùng Wireshark để bắt gói, phân tích gói tin bắt được. Hãy cho biết các bước và một số hình ảnh:

……
……
……

- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

……
……
……

- Biện pháp đối phó đối với loại hình tấn công là gì ?

……
……
……

5. Cài đặt máy chủ CentOS 7

- Hệ điều hành CentOS là gì ?

……
……
……

- Hãy cho biết các bước cài đặt máy chủ CentOS 7 trên Virtual Box bao gồm vài hình ảnh:

……
……
……

- Cấu hình để máy chủ CentOS và Kali Linux có thể ”thấy” nhau. Cho biết kết quả kiểm tra kết nối từ máy Kali linux đến máy chủ CentOS bằng lệnh ping:

……
……
……

6. Tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7

- Tìm hiểu và cho biết cách sử dụng công cụ `hydra` trên Kali Linux:

……
……

- Dùng công cụ `hydra` tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 với tự điển hiện có:

……
……

- Tạo danh sách các mật khẩu (wordlist) bằng `crunch` và dùng `hydra` tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 dùng danh sách mật khẩu đã tạo ra:

……
……
……

- Đánh giá mức độ nguy hiểm của loại hình tấn công này:

……
……
……

7. Giải pháp giảm thiểu tấn công vét cạn

- Tìm hiểu `fail2ban` và cho biết nó được sử dụng để làm gì ?

……
……
……

- Cài đặt và cấu hình `fail2ban` đối với dịch vụ SSH trên máy chủ CentOS 7:

……
……

- Dùng công cụ `hydra` tấn công vét cạn trên dịch vụ SSH của máy chủ CentOS 7 và cho biết kết quả:

……
……

-HẾT-