Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

6

Lab

Cloud Security

Thực hành môn An toàn mạng máy tính nâng cao

Tháng 3/2025
Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu public cloud AWS và các dịch vụ Security của AWS
- Thực hành khai thác các lỗ hổng từ AWS IAM

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Máy tính kết nối Internet

C. THỰC HÀNH

1. AWS IAM

AWS Identity and Access Management (IAM) là một dịch vụ cốt lõi trong nền tảng đám mây Amazon Web Services (AWS), cho phép quản trị và kiểm soát quyền truy cập vào các dịch vụ và tài nguyên AWS một cách an toàn và tập trung. IAM cung cấp các công cụ để quản lý người dùng, nhóm người dùng, vai trò (roles), cũng như các thông tin xác thực như khóa truy cập (access keys) và mật khẩu. Thông qua IAM, các tổ chức có thể xác định **ai** có quyền truy cập vào **tài nguyên nào**, có thể thực hiện **hành động gì**, và **trong điều kiện nào**.
Một thành phần quan trọng trong IAM là **policy** (chính sách truy cập). Các chính sách này được định nghĩa dưới dạng tài liệu JSON, cho phép xác thực và ủy quyền truy cập chi tiết cho người dùng, nhóm người dùng hoặc vai trò đối với các dịch vụ cụ thể trong AWS. Tuy nhiên, nếu các policy này được cấu hình không đúng cách, chúng có thể tạo ra **lỗ hổng bảo mật nghiêm trọng**, cho phép kẻ tấn công truy cập trái phép, leo thang đặc quyền (privilege escalation), hoặc kiểm soát hoàn toàn môi trường đám mây.
Trong thực hành này, chúng ta sẽ tìm hiểu sâu hơn về các lỗi cấu hình phổ biến trong IAM policies – một trong những nguyên nhân hàng đầu dẫn đến **rò rỉ dữ liệu và tấn công nội bộ** (**insider threats**) trong môi trường Cloud.

Task: Thực hiện các challenge của Big IAM Challenge tại link sau: https://bigiamchallenge.com/
Để thực hiện được các challenge này, các bạn cần tham khảo các câu lệnh của AWS CLI:
Dịch vụ S3: https://docs.aws.amazon.com/cli/latest/reference/s3/
Dịch vụ SQS: https://docs.aws.amazon.com/cli/latest/reference/sqs/

Dịch vụ SNS: https://docs.aws.amazon.com/cli/latest/reference/sns/

Dịch vụ Cognito: https://docs.aws.amazon.com/cli/latest/reference/cognito-idp/

Note:

- Không thực hiện challenge 3, nhập flag sau để bỏ qua challenge 3: {wiz:always-suspect-asterisks}
- Challenge 1, 2, 4 là bắt buộc, challenge 5, 6 là bonus

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
  - Ví dụ: [NT534.K11.ANTN.1]-Lab1_1852xxxx_1852yyyy.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!