ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Nguyễn Hoàng Dương

XÂY DỰNG HỆ THỐNG QUẢN LÝ BỀ MẶT TẤN CÔNG CHO KIỂM THỬ XÂM NHẬP

Báo cáo dự án công nghệ - INT3132

Ngành: Khoa học máy tính

Lớp khoá học: QH-2022-I/CQ-I-CS4

Mã sinh viên: 22028007

Cán bộ hướng dẫn: TS. Nguyễn Đại Thọ

HÀ NỘI - 2025

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Nguyễn Hoàng Dương

XÂY DỰNG HỆ THỐNG QUẢN LÝ BỀ MẶT TẤN CÔNG CHO KIỂM THỬ XÂM NHẬP

Báo cáo dự án công nghệ - INT3132

Ngành: Khoa học máy tính

Lớp khoá học: QH-2022-I/CQ-I-CS4

Mã sinh viên: 22028007

Cán bộ hướng dẫn: TS. Nguyễn Đại Thọ

HÀ NỘI - 2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

Chương 1

Giới thiệu

1.1. Tổng quan

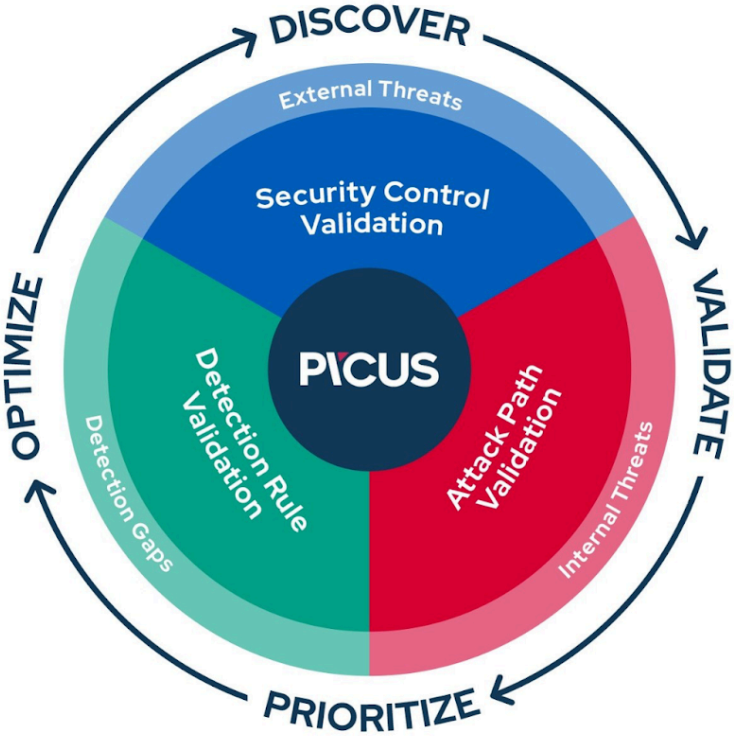
Kiểm thử xâm nhập (Pentesting) là hình thức mô phỏng các cuộc tấn công thực tế lên mạng, ứng dụng hoặc thiết bị để phát hiện, khai thác lỗ hổng và đưa ra khuyến nghị khắc phục trước khi bị kẻ xấu lợi dụng. Quá trình này bao gồm các bước thu thập thông tin, phân tích lỗ hổng, khai thác và báo cáo kết quả, cho phép tổ chức chủ động vá lỗi.

Red Team là nhóm chuyên gia đóng vai hacker trong môi trường mô phỏng, sử dụng kết hợp tấn công kỹ thuật và phi kỹ thuật như social engineering hay xâm nhập vật lý. Mục tiêu là đánh giá khả năng phát hiện, phản ứng và khôi phục của tổ chức dưới áp lực tấn công sát thực tế.

Trong bối cảnh an ninh mạng đầy biến động, Red Team truyền thống có nhiều sự hạn chế, nhất là trong bối cảnh tài nguyên công khai của tổ chức luôn thay đổi và phát triển theo thời gian, dẫn đến việc các lỗ hổng mới trong tài nguyên của tổ chức xuất hiện liên tục và khó kiểm soát. Các phương pháp kiểm thử xâm nhập truyền thống thường chỉ tập trung vào các lỗ hổng đã biết và không thể theo kịp tốc độ phát triển của công nghệ và các mối đe dọa mới, cũng như chỉ xem xét được một thời điểm trong suốt quá trình hoạt động của tổ chức. Điều này dẫn đến việc tổ chức có thể bỏ sót những lỗ hổng nghiêm trọng, và để lộ các tài nguyên điểm mù mà kẻ tấn công có thể khai thác.

Trước tình hình đó, có xuất hiện một xu hướng mới trong cách hoạt động của các tổ chức Red Team là Red Team chủ động (Continuous Automated Red Teaming), trong đó có sự tích hợp với hệ thống quản lý bề mặt tấn công (Attack Surface Management – ASM). ASM là quy trình liên tục nhằm phát hiện, theo dõi và giảm thiểu các lỗ hổng mà kẻ tấn công có thể khai thác để xâm nhập vào hệ thống. Thay vì chỉ tập trung vào việc vá lỗ hổng đã biết, ASM mở rộng phạm

vi giám sát từ tầng hạ tầng mạng, ứng dụng web, API, đến các tài nguyên đám mây và cả những thiết bị IoT, bằng cách kết hợp phương pháp quét thụ động (thu thập thông tin từ DNS, logs chứng chỉ số), quét chủ động (port scanning, web crawling) và tích hợp API từ các nhà cung cấp dịch vụ.



Hình 1.1 — Mô tả quy trình của Red Team chủ động kết hợp ASM

Xử lý dữ liệu trong ASM thường bao gồm ba bước chính: thu thập và hợp nhất thông tin tài sản, phân tích và đánh giá mức độ rủi ro dựa trên các chỉ số như độ phổ biến exploit, mức độ phơi bày và tầm quan trọng của tài sản, rồi cuối cùng là cảnh báo và gợi ý hành động. Nền tảng ASM hiện đại thường dùng cơ sở dữ liệu thời gian thực và các mô-đun học máy để tự động nhận diện tài sản mới, so sánh dấu vân (fingerprint) và cập nhật điểm rủi ro một cách linh hoạt khi môi trường thay đổi.

Lợi ích rõ nét nhất của ASM là khả năng phát hiện sớm tài sản "ẩn" hoặc cấu hình sai (misconfiguration) trước khi kẻ tấn công khai thác, giúp tổ chức giảm thiểu thời gian phản ứng (MTTR) và cải thiện tuân thủ các tiêu chuẩn bảo mật. Bên cạnh đó, các dashboard trực quan và báo cáo tự động cho phép lãnh đạo dễ dàng theo dõi tiến độ khắc phục, cân nhắc đầu tư và ưu tiên nguồn lực.

Chương 2

Các khái niệm cơ sở

3. Penetration Testing

ádfash ádfhiu

Tài liệu tham khảo