HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

KỊCH BẢN BÀI TẬP LỚN

MÔN HỌC: KIỂM THỬ XÂM NHẬP

Giảng viên: **Đinh Trường Duy**

Lớp: **03**

Nhóm: **02**

Thành viên:

Nguyễn Quốc Khánh	**B20DCAT103**
Nguyễn Quý Dũng	**B20DCAT031**
Phạm Thanh Tùng	**B20DCAT171**
Chu Quang Long	**B20DCAT111**

Hà Nội, tháng 2 năm 2024

Kịch bản leo thang đặc quyền (system hacking):

Mục tiêu: Dùng tài khoản của người dùng nâng cao đặc quyền của người dùng đó trong hệ thống.

Các bước thực hiện:

I. Trước khi tấn công

Thu thập thông tin người dùng

- Đầu vào: Tên, địa chỉ email, tên công ty.
- Công cụ: Google Hacking, tìm kiếm dữ liệu công khai.
- Đầu ra: Dữ liệu về người dùng như tên, vị trí công việc, địa chỉ email.

Xác định các cổng và dịch vụ mà người dùng sử dụng

- Đầu vào: IP hoặc tên miền.
- Công cụ: Nmap, Shodan.
- Đầu ra: Các cổng mở và dịch vụ đang chạy trên máy chủ.

Xác định các lỗ hổng và điểm yếu của dịch vụ mà nạn nhân sử dụng

- Đầu vào: IP hoặc tên miền.
- Công cụ: Nessus, OpenVAS.
- Đầu ra: Danh sách lỗ hổng và điểm yếu.

Phân tích các lỗ hổng và điểm yếu

- Đầu vào: Danh sách lỗ hổng và điểm yếu.
- Công cụ: Nessus, OpenVAS, Metasploit.
- Đầu ra: Danh sách các lỗ hổng có thể khai thác.

Chọn phương pháp tấn công phù hợp với lỗ hổng hoặc điểm yếu trên

- Đầu vào: Danh sách lỗ hổng có thể khai thác.
- Công cụ: Metasploit, Aircrack-ng, THC-Hydra.
- Đầu ra: Access vào hệ thống, lấy thông tin hoặc tiến hành tấn công.

II. Tấn công

A. Tấn công người dùng:

Tiến hành phishing:

- Đầu vào: Danh sách email địa chỉ của nạn nhân.
- Công cụ: Các trang web giả mạo (phishing site), công cụ gửi email tự động.

- Đầu ra: Tạo ra một trang web giả mạo, lấy thông tin đăng nhập của nạn nhân.

Tấn công về phần mềm:

- Đầu vào: Nạn nhân click vào trang web giả mạo
- Công cụ: Ngrok.
- Đầu ra: Gửi 1 reverse shell đến máy của nạn nhân

B. Tấn công hệ thống:

Tấn công đánh cắp thông tin:

- Đầu vào: Đoạn mã Shell được thực hiện trên máy nạn nhân.
- Công cụ: PowerShell, Metasploit.
- Đầu ra: Kẻ tấn công sử dụng kết nối reverse shell để thực hiện các hành động chiếm quyền và kiểm soát hệ thống mục tiêu từ xa.

Nâng cao đặc quyền:

- Đầu vào: Reverse shell access vào hệ thống.
- Công cụ: Metasploit, PowerUpSQL.
- Đầu ra: Tăng cao quyền hạn của tài khoản, trở thành người dùng quản trị.

III. Kịch bản phòng thủ

A. Phòng thủ chống tấn công người dùng:

Phishing Protection:

- Đầu vào: Triển khai giải pháp như Microsoft Defender for Office 365 hoặc Proofpoint.
- Công cụ: Microsoft Defender for Office 365, Proofpoint.
- Đầu ra: Phát hiện và chặn email phishing trước khi chúng đến hòm thư đến của người dùng, tự động chuyển các email đáng ngờ vào thùng rác hoặc cảnh báo người dùng, giáo dục nhân viên về cách nhận diện và tránh các kỹ thuật lừa đảo như phishing.

Phishing Site Detection:

- Đầu vào: Sử dụng dịch vụ quét web như Google Safe Browsing API hoặc PhishTank.
- Công cụ: Google Safe Browsing API, PhishTank.
- Đầu ra: Phát hiện và chặn truy cập đến các trang web giả mạo, giám sát liên tục của các đường dẫn URL trong email và các tệp đính kèm để phát hiện sớm các liên kết độc hại.

Network Segmentation:

- Đầu vào: Tạo ra các vùng mạng ảo (VLANs).
- Công cụ: Cấu hình VLAN trên thiết bị mạng.
- Đầu ra: Cô lập các phòng ban và dịch vụ khác nhau, giảm thiểu khả năng lan truyền của các tấn công từ bên trong mạng. Sử dụng cơ chế cấu hình và quản lý truy cập (ACLs) trên thiết bị mạng để kiểm soát và giới hạn luồng dữ liệu giữa các segment mạng.

B. Phòng thủ chống tấn công hệ thống:

1. Thực hiện Phân quyền:

- Đầu vào: Sử dụng các nhóm người dùng và vai trò để quản lý quyền truy cập.
- Công cụ: Quản lý hệ thống quyền truy cập, ví dụ như Active Directory.
- Đầu ra: Đảm bảo người dùng chỉ nhận được quyền cần thiết để thực hiện công việc của họ theo nguyên tắc tối thiểu.

2. Quản lý Phần mềm:

- Đầu vào: Triển khai giải pháp quản lý cập nhật tự động.
- Công cụ: Hệ thống quản lý cập nhật tự động, ví dụ như WSUS (Windows Server Update Services).
- Đầu ra: Đảm bảo tất cả các máy tính và phần mềm trên hệ thống được cập nhật đầy đủ và kiểm soát quá trình triển khai phần mềm.

3. Giám sát Hoạt động Hệ thống:

- Đầu vào: Sử dụng các giải pháp giám sát hệ thống.
- Công cụ: Splunk, ELK Stack.
- Đầu ra: Theo dõi và phân tích các hoạt động đáng ngờ, cũng như cấu hình cảnh báo để phản ứng với các sự kiện quan trọng.

4. Mạng ảo (Virtual Private Network - VPN):

- Đầu vào: Triển khai một giải pháp VPN chặt chẽ.
- Công cụ: Phần mềm hoặc thiết bị VPN, cơ chế xác thực hai yếu tố.
- Đầu ra: Bảo vệ thông tin khi người dùng kết nối từ xa và tăng cường bảo mật thông qua xác thực hai yếu tố.

5. Tường lửa (Firewall) và Hệ thống Phát hiện Xâm nhập (Intrusion Detection System - IDS):

- Đầu vào: Cấu hình tường lửa và triển khai cảm biến IDS trên mạng.
- Công cụ: Tường lửa, IDS.
- Đầu ra: Chặn lưu lượng không mong muốn và phát hiện các hành vi xâm nhập, cũng như cung cấp báo cáo và cảnh báo về các hoạt động đáng ngờ.

6. Hệ thống Antivirus và Antimalware:

- Đầu vào: Sử dụng giải pháp diệt virus và phần mềm độc hại hiện đại.
- Công cụ: Phần mềm diệt virus và phần mềm độc hại.
- Đầu ra: Bảo vệ hệ thống khỏi các mối đe dọa từ virus và phần mềm độc hại thông qua quét định kỳ và loại bỏ các tệp và thư mục có vấn đề.

IV. Sau tấn công

Lập tài liệu.

Làm báo cáo.