**BÀI TẬP AN TOÀN MẠNG MÁY TÍNH**

**BUỔI 1**

Lê Ngọc Kiều Anh - 22520047

Lớp: NT101.P11

1. **Lập bảng tổng hợp các kỹ thuật tấn công cơ bản (tên gọi, cơ chế hoạt động, công cụ sử dụng, kết quả đạt được, biện pháp phòng chống,…).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên gọi** | **Cơ chế hoạt động** | **Công cụ sử dụng** | **Kết quả đạt được** | **Biện pháp phòng chống** |
| **Eavesdropping** | Giám sát lưu lượng mạng và bắt các gói tin đi qua các thiết bị. | Sử dụng thiết bị mạng (router, card mạng,…) và chương trình ứng dụng (Tcpdump, Ethereal, Wireshark…). | Nghe trộm được các thông tin nhạy cảm như mật khẩu, dữ liệu các nhân. | Mã hóa dữ liệu trước khi truyền chúng lên mạng.  Không sử dụng mạng công cộng không bảo mật. |
| **Cryptanalysis** | Tìm kiếm thông tin hữu ích từ dữ liệu đã mã hóa mà không cần biết khóa. | Sử dụng công cụ toán học và máy tính có hiệu suất cao. | Phá vỡ được hệ thống bảo mật, truy cập trái phép vào hệ thống. | Dùng các giải thuật mã hóa không thể hiện cấu trúc thống kê trong chuỗi mật mã.  Dùng khóa có độ dài lớn để chống Brute-force attacks. |
| **Password Pilfering** | Lấy cắp mật khẩu thông qua việc dò tìm username và password, đoán mật khẩu, sd các kỹ năng xã hội để ăn cắp thông tin của người khác. | Các phần mềm tấn công, các chương trình password sniffing như Cain & Abel. | Lấy được mật khẩu, tài khoản của người dùng, xâm nhập vào hệ thống, đánh cắp thông tin cá nhân. | Sử dụng xác thực hai yếu tố, xác thực sinh trắc học, dùng mật khẩu mạnh và thường xuyên thay đổi, không tiết lộ mật khẩu cho người khác, không sử dụng phần mềm đăng nhập từ xa, không click vào các liên kết khả nghi,.. |
| **Identity Spoofing** | Cho phép kẻ tấn công mạo nhận nạn nhân mà không cần sử dụng mật khẩu của nạn nhân.  Chặn và sửa đổi, làm giả dữ liệu truyền giữa những người sử dụng. | Các công cụ  để thực hiện tấn công Man-in-the-  middle, replay  message, network  spoofing và  khai thác lỗ hỏng  phần mềm. | Đánh lừa hệ thống và người dùng sau đó truy cập trái phép. | Mã hóa và chứng thực các gói IP, kiểm tra và xác minh giấy phép hoặc chứng thực, kiểm tra IP và tên miền, sử dụng các biện pháp bảo mật mạng và phần cứng như Firewall, VPN. |
| **Buffer-Overflow Exploitations** | Gửi dữ liệu quá lớn đến bộ đệm của hệ thống để thực thi mã độc hoặc phá vỡ bảo mật. | Các trình biên dịch, trình gỡ lỗi, các công cụ tìm lỗi. | Thực thi mã độc, kiểm soát hệ thống từ xa, gây treo hoặc sập hệ thống. | Kiểm tra kích thước bộ đệm, kiểm tra đầu vào, cập nhật phần mềm, sử dụng các công cụ bảo mật. |
| **Repudiation** | Kẻ tấn công từ chối hành động đã thực hiện (như gửi email, chuyển dữ liệu), gây khó khăn trong việc truy xuất nguồn gốc. | Để ngăn chặn repudiation, các công cụ sử dụng các thuật toán mã hóa và xác thực để bảo vệ tính toàn vẹn của dữ liệu. | Khó khăn trong việc kiểm tra và xử lý sự cố, mất tính minh bạch và bảo mật thông tin. | Sử dụng chữ ký số, xác thực mạnh mẽ, lưu nhật ký hệ thống, hành động rõ ràng. |
| **Intrusion** | Xâm nhập bất hợp pháp vào một mạng với mục đích đánh cắp thông tin và tài nguyên máy tính hoặc băng thông của nạn nhân. | IP scan và Port scan  Do cấu hình sơ hở, giao thức sai sót, tác dụng phụ của phần mềm. | Đánh cắp thông tin quan trọng, truy cập và thay đổi dữ liệu, làm suy yếu hệ thống. | Đóng các cổng UDP hoặc TCP không cần thiết để giảm thiểu việc xâm nhập, kiểm tra bảo mật thường xuyên, áp dụng cac chính sách phân quyền chặt chẽ. |
| **Denial of Service Attacks** | Ngăn chặn người dùng hợp pháp sử dụng dịch vụ bằng cách tạo ra một lưu lượng lớn yêu cầu không hợp lệ dẫn đến quá tải và làm hỏng hệ thống. | Jolt2, Bubonic.c, Land and LaTierra, Targa, Blast20, Nemesy, Panther2, Crazy Pinger, Some Trouble, UDP Flood, FSMax,… | Dịch vụ không khả dụng, mất kết nối hoặc giảm hiệu suất hệ thống với người dùng. | Cấu hình hệ  thống và mạng  để chống lại các loại tấn công từ chối dịch vụ phổ  biến, giới hạn số  lượng yêu cầu đến từ một nguồn duy  nhất trong một  khoảng thời gian nhất định, sử dụng các giải pháp băng  thông rộng và cân bằng tải để phân phối tải đồng đều  và chống lại tấn công DDoS. |
| **Malicious Software** | Gồm các phần mềm độc hại: virus, worms, trojan horses, logic bombs, backdoors, spyware. Các loại phần mềm này thường được tạo ra để xâm nhập vào hệ thống mà không được người dùng cho phép hoặc người dùng không biết. | Các phần mềm độc hại được tạo ra và phân tán thông qua email, các trang web, tệp tin đính kèm, các đường link không nguồn gốc,… | Tạo ra lỗ hỏng bảo mật, đánh cắp thông tin cá nhân, kiểm soát máy của người dùng từ xa, tấn công mạng. | Cài đặt các phần mềm chống virus, cập nhật hệ điều hành, không click vào các đường link hay mở các tập tin đáng nghi ngờ, không rõ nguồn gốc,… |

1. **Phân tích mô hình phòng thủ theo chiều sâu**

Mô hình phòng thủ theo chiều sâu là một phương pháp bảo mật mạng dựa trên việc triển khai nhiều lớp phòng thủ khác nhau, tập trung xây dựng các khối phòng thủ từ bên trong mạng và mở rộng ra ngoài để ngăn chặn và phát hiện các cuộc tấn công mạng.

Các chức năng của các layer:

* **Data:** layer bảo vệ dữ liệu, quản lí quyền truy cập dữ liệu, giám sát và phát hiện các cuộc tấn công từ bên trong mạng, dữ liệu cần được mã hóa, sao lưu thường xuyên, truyền dữ liệu cần các phương thức bảo mật (SSL, TLS…).
* **Application:** layer bảo vệ các ứng dụng, ứng dụng cần phải đảm bảo tính an toàn, khó xâm nhập, được bảo mật, có các chính sách quản lý truy cập dữ liệu, phát hiện và chặn các cuộc tấn công từ các ứng dụng.
* **Host:** cài đặt mất khẩu cho các host, bao gồm các hệ điều hành, các ứng dụng, các cơ chế phát hiện xâm nhập.
* **Internal network:** layer bảo vệ mạng nội bộ của tổ chức, bao gồm các hệ thống giám sát mạng, phát hiện xâm nhập, các chính sách quản lý quyền truy cập, sử dụng VPN cho các kết nối từ xa, bảo mật mạng nội bộ.
* **Perimeter:** cài đặt tường lửa cho mạng diện rộng, kiểm tra các kết nối đáng ngờ, giúp ngăn chặn các cuộc tấn công từ bên ngoài mạng.
* **Physical**: layer vật lý bảo vệ môi trường vật lý của các thiết bị và hệ thống mạng, bảo vệ máy chủ, ổ cứng, bảo vệ các cổng vào ra,…dùng các biện pháp vật lý như bảo mật sinh trắc học, ngăn các cá nhân không có thẩm quyền xâm nhập.
* **Policies, procedures, and awareness:** layer chính sách, cho phép nhân viên sử dụng tài nguyên vừa đủ với thẩm quyền, huấn luyện cho nhân viên về nhận thức các mối nguy hại để kịp xử lí.