**Câu 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…).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Tên gọi | Cơ chế hoạt động | Công cụ sử dụng | Kết quả đạt được | Biện pháp phòng chống |
| 1 | Eavesdropping | Sử dụng một thiết bị mạng và một chương trình ứng dụng để giám sát lưu lượng mạng, bắt các gói tin đi qua thiết bị này | +) Thiết bị mạng (router, card  mạng…)  +) Chương trình ứng dụng (Tcpdump, Ethereal, Wireshark…) | Đánh cắp thông tin, dữ liệu nhạy cảm | +) Không có cách nào ngăn chận việc nghe trộm trong một mạng công cộng  +) Cách tốt nhất là mã hoá dữ liệu trước khi truyền chúng trên mạng |
| 2 | Cryptanalysis | Nghệ thuật tìm kiếm thông tin hữu ích từ dữ liệu đã mã hoá mà không cần biết khoá giải mã | Các công cụ toán học và máy tính có hiệu suất cao | Đánh cắp thông tin, dữ liệu đã được mã hóa | +) Sử dụng những giải thuật mã hoá không thể hiện cấu trúc thống kê trong chuỗi mật mã.  +) Khoá có độ dài lớn để chống Brute-force attacks. |
| 3 | Password Pilfering | +) Lấy cắp mật khẩu của người dùng  +) Các phương pháp thông dụng bao gồm:  - Guessing  - Social engineering: sử dụng các kỹ năng xã hội để ăn cắp thông tin mật của người khác  - Dictionary Attacks: duyệt tìm từ một từ điển (thu được từ các file SAM…) các username và password đã được mã hoá.  - Password sniffing: một phần mềm dùng để bắt các thông tin đăng nhập từ xa như username và password đối với các ứng dụng mạng phổ biến | +) Mạo danh, lừa đảo qua email, tạo web đăng nhập giả …  +) Cain & Abel, Phishing, keylogger, trojan horse | Truy cập trái phép vào tài khoản, hệ thống | +) Sử dụng mật khẩu bí mật, sinh trắc học  +) Sử dụng mật khẩu kết hợp nhiều kí tự  +) Thay đổi mật khẩu định kì  +) Không sử dụng một mật khẩu cho các tài khoản khác nhau  +) Không click vào các đường link lạ |
| 4 | Identity Spoofing | +) Phương pháp tấn công cho phép kẻ tấn công  mạo nhận nạn nhân mà không cần sử dụng mật  khẩu của nạn nhân  +) Các phương pháp phổ biến bao gồm:  – Man-in-the-midle attacks: dàn xếp với thiết bị mạng sửa đổi hay làm giả dữ liệu truyền giữa những người sử dụng rồi truyền chúng như chưa từng bị tác động bởi kẻ tấn công.  – Message replays attacks: tấn công lấy bản sao của giấy phép của một số giao thức nhằm mạo nhận người dung để có được các dịch vụ từ hệ thống  – Network spoofing attacks: IP Spoofing bao gồm:  \* SYN flooding: kẻ tấn công lấp đầy bộ đệm TCP của máy tính mục tiêu với một khối lượng lớn các gói SYN, làm cho máy tính mục tiêu không thể thiết lập các thông tin liên lạc với các máy tính khác.  \* TCP hijacking: sử dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích  \* ARP spoofing (ARP poisoning): thay đổi địa chỉ MAC đích hợp pháp của một địa chỉ IP đến một địa chỉ MAC khác được lựa chọn bởi những kẻ tấn công.  – Software exploitation attacks | +)Man-in-the-midle attacks: Ettercap, Wireshark…  +)Message replay attacks: Wireshark, Scapy, Burp Suite…  +)Network spoofing attacks: Ettercap, Scapy, Nmap, Hping…  +)Software exploitation attacks: GDB, Metasploit Framework, Burp Suite… | Truy cập trái phép vào tài khoản, hệ thống | +) Man-in-the-midle attacks: Mã hoá và chứng thực các gói IP  +) Message replay attacks: Sử dụng các giao thức mã hóa, để bảo vệ dữ liệu trong quá trình truyền và đảm bảo tính toàn vẹn của dữ liệu.  +) Network spoofing attacks:  \* TCP hijacking: sử dụng phần mềm như TCP Wrappers để kiểm tra địa chỉ IP tại tầng TCP (tầng Transport).  \* ARP spoofing (ARP poisoning): cần phải tăng cường kiểm tra các tên miền, và chắc chắn rằng địa chỉ IP nguồn và địa chỉ IP đích trong một gói tin IP không được thay đổi trong khi truyền.  +) Software exploitation attacks: Luôn cập nhật và vá lỗi các phần mềm, chỉ cài đặt các phần mềm từ nguồn tin cậy |
| 5 | Buffer-Overflow Exploitations | Một lỗ hổng phần mềm phổ biến. Lỗi này xảy ra khi quá trình ghi dữ liệu vào bộ đệm nhiều hơn kích thước khả dụng của nó | Sử dụng phần mềm độc hại, mã độc... | Chạy mã độc, chiếm quyền điều khiển hệ thống | Sử dụng phần mềm bản quyền, cập nhật phần mềm bảo mật |
| 6 | Repudiation | Chủ sở hữu của dữ liệu có thể không thừa nhận quyền sở hữu của dữ liệu để tránh hậu quả pháp lý | Công nghệ xóa dữ liệu | Lừa đảo, trốn tránh trách nhiệm | Các thuật toán mã hóa và xác thực có thể giúp ngăn ngừa các cuộc tấn công bác bỏ. |
| 7 | Intrusion | Xâm nhập bất hợp pháp vào một mạng với mục đích truy cập vào hệ thống máy tính của người khác, đánh cắp thông tin và tài nguyên máy tính hoặc băng thông của nạn nhân. | IP scan và Port scan | Truy cập trái phép vào tài khoản, hệ thống | IP scan và Port scan cũng là những công cụ giúp người dùng kiểm tra được các lỗ hổng trong hệ thống. |
| 8 | Denial of Service Attacks | +) Ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ  +) DoS có các hình thức cơ bản sau:   * Smurf * Buffer Overflow Attack * Ping of death * Teardrop * SYN Attack | Jolt2, Bubonic.c, Land and LaTierra, Targa,  Blast20, Nemesy, Panther2, Crazy Pinger,  Some Trouble, UDP Flood, FSMax… | Làm ngừng hoạt động của hệ thống | Sử dụng tường lửa hoặc những phần mềm diệt virus uy tín, hạn chế băng thông truy cập,... |
| 9 | Malicious Software | Sử dụng các phần mềm độc hại để tấn công vào hệ thống của nạn nhân | +) Virus  +) Worms  +) Trojan horses  +) Logic bombs  +) Backdoors  +) Spyware. | Đánh cắp dữ liệu, chiếm quyền điều khiển hệ thống | Sử dụng phần mềm diệt virus uy tín, cập nhật thường xuyên, cảnh giác với những tin nhắn, email, đường link lạ |

**Câu 2: Phân tích mô hình phòng thủ theo chiều sâu**

* Mô hình phòng thủ theo chiều sâu (defense in depth) là một chiến lược bảo mật mạng trong đó một hệ thống được bảo vệ bởi nhiều lớp bảo mật khác nhau. Mỗi lớp bảo mật sẽ có một vai trò riêng, giúp ngăn chặn các cuộc tấn công mạng.
* Mô hình phòng thủ theo chiều sâu dựa trên nguyên tắc rằng không có biện pháp bảo mật nào là hoàn hảo. Bằng cách triển khai nhiều lớp bảo mật, các tổ chức có thể giảm thiểu rủi ro bị tấn công thành công.
* Các lớp bảo mật trong mô hình phòng thủ theo chiều sâu có thể bao gồm:
* **Dữ liệu:** Dữ liệu là tài sản quan trọng nhất của nhiều tổ chức. Do đó, việc bảo vệ dữ liệu là một trong những ưu tiên hàng đầu của mô hình phòng thủ theo chiều sâu. Các biện pháp bảo vệ dữ liệu phổ biến bao gồm mã hóa, quản lý truy cập, sao lưu dữ liệu.
* **Ứng dụng:** Ứng dụng là một mục tiêu hấp dẫn đối với các cuộc tấn công mạng. Do đó, việc bảo vệ ứng dụng là một lớp bảo mật quan trọng trong mô hình phòng thủ theo chiều sâu. Các biện pháp bảo vệ ứng dụng phổ biến bao gồm kiểm tra bảo mật, xác thực hai yếu tố, mã hóa.
* **Máy chủ:** Máy chủ là trung tâm của nhiều hệ thống mạng. Do đó, việc bảo vệ máy chủ là một lớp bảo mật quan trọng trong mô hình phòng thủ theo chiều sâu. Các biện pháp bảo vệ máy chủ phổ biến bao gồm cập nhật hệ điều hành và phần mềm, cài đặt tường lửa, sử dụng phần mềm diệt virus.
* **Vùng biên mạng nội bộ:** Vùng biên mạng nội bộ là khu vực phân cách giữa mạng nội bộ và mạng internet. Do đó, việc bảo vệ vùng biên mạng nội bộ là một lớp bảo mật quan trọng trong mô hình phòng thủ theo chiều sâu. Các biện pháp bảo vệ vùng biên mạng nội bộ phổ biến bao gồm tường lửa, kiểm soát truy cập, thiết bị mạng.
* **Perimeter (Ranh giới):** Ranh giới là điểm tiếp xúc giữa mạng nội bộ và mạng bên ngoài. Để bảo vệ mạng nội bộ, cần triển khai các biện pháp bảo vệ ranh giới như tường lửa, hệ thống phát hiện xâm nhập (IDS/IPS) và quản lý bằng chứng số (SIEM).
* **Vật lý:** Mô hình phòng thủ theo chiều sâu cũng bao gồm các biện pháp bảo vệ vật lý, chẳng hạn như kiểm soát truy cập vật lý, camera an ninh, hệ thống báo động.
* **Chính sách, quy trình và nhận thức:** Chính sách, quy trình và nhận thức của người dùng cũng là một phần quan trọng của mô hình phòng thủ theo chiều sâu. Các chính sách và quy trình bảo mật rõ ràng sẽ giúp nhân viên hiểu rõ về các yêu cầu bảo mật và thực hiện các biện pháp bảo mật một cách hiệu quả. Nhận thức của người dùng về bảo mật cũng là một yếu tố quan trọng, giúp người dùng phát hiện và báo cáo các hoạt động đáng ngờ.