1. **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 |
| **Eavesdropping** | Sử dụng một thiết bị mạng (router, card mạng…) và một chương trình ứng dụng (Tcpdump, Ethereal, Wireshark…) để giám sát lưu lượng mạng, bắt các gói tin đi qua thiết bị này. | Các thiết bị mạng như (router, card mạng…) và một chương trình ứng dụng (Tcpdump, Ethereal, Wireshark…) | Các gói tin chứa nội dung, thông tin giao tiếp giữa các đối tượng với nhau. | Mã hoá dữ liệu trước khi truyền chúng trên mạng. |
| **Cryptanalysis** | Sử dụng các phương pháp thống kê để xác định tần suất xuất hiện của các ký tự, từ hoặc cụm từ có thể có trong mã khoá. | Thường sử dụng các công cụ toán học và máy tính có hiệu suất cao. | Mã khoá để có thể truy cập mà không cần sự cho phép của chính chủ. | 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. |
| **Password Pilfering** | Phương pháp thông dụng bao gồm:  - **Guessing**: hiệu quả đối với các mật khẩu ngắn hoặc người dùng quên đổi mật khẩu ngầm định.  - **Social engineering**: sử dụng các kỹ năng xã hội để ăn cắp thông tin mật của người khác như mạo danh, lừa đảo qua email, websites…  - **Dictionary attacks**: duyệt tìm từ một từ điển (thu được từ các file SAM, /etc/passwd…) các username và password đã được mã hoá.  - **Password Sniffing**: bắt các thông tin đăng nhập từ xa như username và password đối với các ứng dụng mạng phổ biến như Telnet, FTP, SMTP, POP3. | - Cain & Abel là một công cụ khôi phục mật khẩu trong hệ điều hành Microsoft và cũng là một công cụ password sniffing có thể bắt và phá mã các password đã được mã hoá. | - Thông tin quan trọng chứa username và password của người dùng cho các tài khoản quý giá. | Đối với từng phương pháp sẽ có những cách ngăn chặn khác nhau:  - **Guessing và Dictionary attacks**: Sử dụng mật khẩu dài kết hợp giữa chữ thường, chữ hoa, số và các ký tự đặc biệt như $ # & %. Không dùng các từ có trong từ điển, các tên và mật khẩu thông dụng. Thay đổi mật khẩu định kỳ và không sử dụng trở lại những mật khẩu cũ để chống lại những cuộc tấn công từ điển hoặc mật khẩu cũ đã được nhận diện.  - **Social engineering**: Không tiết lộ mật khẩu với những người không có thẩm quyền hoặc qua điện thoại, thư điện tử…  - **Password Sniffing**: dùng những chương trình đặc biệt (như SSH trong HTTPS…) để mã hoá tất cả các thông điệp truyền đi. |
| **Identity Spoofing** | 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 giữa hai hoặc nhiều người sử dụng, sau đó chặn và 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**: những kẻ tấn công có thể ngăn chặn việc giấy phép được cấp cho người dùng đăng nhập vào hệ thống được mã hoá sau đó giữ một bản sao, và sử dụng nó sau này để mạo nhận (đóng vai) người dùng để có được các dịch vụ từ hệ thống.  - **Network Spoofing**: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. 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**: dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích. Máy nạn nhân bị treo và hacker có thể truyền thông với máy đích như hacker chính là nạn nhân.  + **ARP spoofing (ARP poisoning):** kẻ tấn công thay đổi địa chỉ MAC  đích hợp pháp của một địa chỉ IP đến một địa chỉ  MAC khác được lựa chọn bởi họ. |  | Kẻ tấn công có thể truy cập vào thông tin cá nhân, tài khoản ngân hàng, hoặc dữ liệu nhạy cảm khác bằng cách giả mạo danh tính của một người khác.  Việc giả mạo danh tính có thể làm cho việc xác định kẻ tấn công trở nên phức tạp, gây khó khăn cho việc điều tra và truy tố. | Đối với từng phương pháp sẽ có những cách ngăn chặn khác nhau:  - Mã hoá và chứng thực các gói IP là biện pháp chính để ngăn chận các cuộc tấn công **Man-in-the-midle**. Những kẻ tấn công không thể đọc hoặc sửa đổi một gói tin IP đã được mã hoá mà không phải giải mã nó.  - Để ngăn chặn **TCP hijacking**, có thể sử dụng phần mềm như TCP Wrappers để kiểm tra địa chỉ IP tại tầng TCP (tầng Transport).  - Để ngăn chặn các cuộc tấn công **ARP spoofing**, 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. |
| **Buffer-Overflow Exploitations** | - Là 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. |  | Kẻ tấn công có thể chiếm quyền điều khiển máy tính hoặc ứng dụng, cho phép họ thực hiện các hành độngkhông được phép.  Mất mát hoặc hư hỏng dữ liệu, ảnh hưởng đến tính toàn vẹn của thông tin. | Kiễm tra kĩ xem bộ đệm đủ khoảng trống để dữ liệu có thể được sao chép vào mà không gây ra tràn bộ đệm. |
| **Repudiation** | - Trong một số trường hợp chủ sở hữu của dữ liệu có thể không thừa nhận quyền sở hữu của dữ liệu để tránh hậu quả pháp lý. Người này có thể cho rằng chưa bao giờ gửi hoặc nhận các dữ liệu đó.  Ngay cả khi dữ liệu đã được chứng thực, chủ sở  hữu của dữ liệu xác thực có thể thuyết phục quan  tòa rằng vì những sơ hở, bất cứ ai cũng có thể dễ  dàng chế tạo tin nhắn và làm cho nó trông giống  như thật. |  | Mất mát thông tin  Khó khăn trong điều tra  Các bên liên quan có thể rơi vào tranh chấp về trách nhiệm, dẫn đến mâu thuẫn nội bộ hoặc giữa các tổ chức. | Sử dụng các thuật toán mã hóa và xác thực có thể giúp ngăn ngừa các cuộc tấn công bác bỏ. |
| **Intrusion** | - Xâm nhập bất hợp pháp vào một mạng nhờ vào lỗ hổng từ các cấu hình cơ sở, giao thức sai sót, tác dụng phụ của phần mềm 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 là những công cụ hack phổ biến thuộc dạng này và cũng là những công cụ giúp người dùng kiểm tra được các lỗ hổng trong hệ thống. | Mất mát dữ liệu  Gián đoạn dịch vụ  Hỏng hóc hệ thống  Tạo ra lỗ hổng bảo mật mới  Truy cập trái phép kéo dài  Thay đổi dữ liệu | Đóng các cổng UDP hoặc TCP không cần thiết này lại có thể giảm thiểu việc xâm nhập. |
| **Denial of Service Attacks** | - Mục tiêu là ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ. Các cuộc tấn công như vậy thường buộc máy tính mục tiêu phải xử lý một số lượng lớn những thứ vô dụng, hy vọng máy tính này sẽ tiêu thụ tất cả các nguồn tài nguyên quan trọng.  - DoS có các hình thức cơ bản sau:  + Smurf  + Buffer Overflow Attack  + Ping of death  + Teardrop  + SYN Attack  - **DoS: Smurf** là một loại tấn công DoS điển hình. Máy của attacker sẽ gởi rất nhiều lệnh ping đến một số lượng lớn máy tính trong một thời gian ngắn trong đó địa chỉ IP nguồn của gói ICMP echo sẽ được thay thế bởi địa chỉ IP của nạn nhân. Các máy tính này sẽ trả lại các gói ICMP reply đến máy nạn nhân. Buộc phải xử lý một số lượng quá lớn các gói ICMP reply trong một thời gian ngắn khiến tài nguyên của máy bị cạn kiệt và máy sẽ bị sụp đổ.  - Đối với **DDoS (Distributed DoS)**: Attackers thường sử dụng Trojan để kiểm soát cùng lúc nhiều máy tính nối mạng. Attacker cài đặt một phần mềm đặc biệt (phần mềm zombie) lên các máy tính này (máy tính zombie) để tạo ra một đội quân zombie (botnet)  nhằm tấn công DoS sau này trên máy nạn nhân. | - Cuộc tấn công được phát sinh từ một máy tính duy nhất (DoS), hoặc từ một nhóm các máy tính phân bố trên mạng Internet  (DDoS).  - Công cụ để thực hiện tấn công DoS có thể là Jolt2, Bubonic.c, Land and LaTierra, Targa, Blast20, Nemesy, Panther2, Crazy Pinger,  Some Trouble, UDP Flood, FSMax…  - Trojan để kiếm soát mạng botnet | - **Gián đoạn dịch vụ**: Người dùng không thể truy cập vào dịch vụ hoặc trang web, dẫn đến mất mát về doanh thu cho doanh nghiệp.  - **Hỏng hóc hệ thống**: Tài nguyên hệ thống bị quá tải, có thể dẫn đến treo máy chủ hoặc hỏng hóc phần cứng.  - **Tổn thất tài chính**: Doanh nghiệp có thể phải chi phí cho việc khắc phục sự cố, bảo trì hệ thống và tăng cường bảo mật.  - **Mất uy tín**: Khách hàng có thể mất lòng tin vào doanh nghiệp nếu dịch vụ không ổn định. | -Sử dụng tường lửa lọc lưu lượng truy cập không hợp lệ và hệ thống phát hiện xâm nhập cũng như các hoạt động bất thường (IDS).  -Thiết lập giới hạn băng thông cho từng IP để ngăn chặn lưu lượng truy cập quá mức từ một nguồn duy nhất.  -Sử dụng dịch vụ CDN (Content Delivery Network) để phân phối lưu lượng truy cập và giảm tải cho máy chủ chính.  -Sử dụng các thiết bị cân bằng tải để phân phối lưu lượng truy cập đồng đều đến nhiều máy chủ. |
| **Malicious Software** | - **Virus:** Là một phần mềm có thể sao chép chính nó. Nó không đứng một mình mà phải gắn vào một tập tin hoặc một chương trình khác. Khi được thực hiện virus có thể làm hại máy tính và sao chép chính nó để lây nhiễm sang máy khác trong hệ thống.  - **Worms:***là một chương trình có thể tự sao chép chính nó. Nhưng không giống như virus, Worm là một*  *chương trình đứng một mình (stand alone program). Worm có thể tự thực thi tại bất kỳ thời điểm nào nó muốn. Khi thực thi, Worm có thể gây nguy hiểm cho hệ*  *thống nơi nó thường trú hoặc tái sinh chính nó trên các hệ thống qua mạng.*  - **Trojan horses:** Thường nguỵ trang mình kèm theo những chương trình ứng dụng thông thường và vô hại như trò chơi hoặc những công cụ miễn phí để người dùng tải về máy. Chức năng chính của Trojan là điểu khiển máy tính từ xa, ăn cắp thông tin của nạn nhân hoặc làm nhiệm vụ backdoor.  - **Logic bombs:**Bom logic là chương trình con hoặc lệnh được nhúng trong một chương trình. Sự thi hành của nó được kích hoạt bởi câu lệnh điều kiện.  - **Backdoors:**Khi được chạy trên máy nạn nhân, Backdoors sẽ thường trực trong bộ nhớ, mở một port (mặc định hoặc do kẻ tấn công quy định) giúp kẻ tấn công dễ dàng đột nhập vào máy nạn nhân thông qua port này.  - **Spyware:** là một loại phần mềm tự cài đặt chính nó trên máy tính của người dùng.  Spyware thường được sử dụng để theo dõi xem người dùng làm gì và quấy rối họ với  những thông điệp thương mại xuất hiện trong những cửa sổ popup.  + Browser Hijacking: là một kỹ thuật có thể thay đổi các thiết lập của trình duyệt của người dùng. Nó có thể thay thế Website mặc định của người dùng với một trang web khác được lựa chọn bởi kẻ tấn công. Hoặc nó có thể ngăn chặn người dùng truy  cập vào các Websites họ muốn đến thăm.  + Zombieware: là phần mềm có trên máy tính của  người dùng và biến nó thành một zombie để khởi động các cuộc tấn công DDoS hoặc thực hiện các hoạt động có hại như gửi thư rác hoặc phát tán virus. |  | - **Virus:** Lây lan đến các tệp và hệ thống khác. Gây hỏng hoặc xóa dữ liệu. Làm giảm hiệu suất hệ thống. Có thể dẫn đến mất mát tài chính nếu không khôi phục được dữ liệu.  - **Worms:** Tự động lây lan qua mạng mà không cần sự can thiệp của người dùng.  Tiêu tốn băng thông mạng.  Làm tê liệt hoặc làm chậm hệ thống và mạng. Có thể tạo ra các lỗ hổng bảo mật cho các cuộc tấn công khác.  - **Trojan horses:** Giả mạo thành phần hữu ích để lừa người dùng cài đặt. Có thể cài đặt phần mềm độc hại khác hoặc tạo ra backdoor để truy cập hệ thống. Có thể đánh cắp thông tin nhạy cảm, như mật khẩu hoặc dữ liệu tài chính.  - **Logic bombs:** Kích hoạt khi một điều kiện cụ thể xảy ra, gây hại cho hệ thống. Thường gây ra mất mát dữ liệu hoặc cho phép truy cập trái phép. Có thể dẫn đến tổn thất tài chính và giảm uy tín.  - **Backdoors:** Tạo ra lối vào bí mật cho kẻ tấn công để truy cập vào hệ thống. Cho phép kẻ tấn công kiểm soát hệ thống mà không bị phát hiện. Có thể dẫn đến mất mát thông tin nhạy cảm và quyền riêng tư.  - **Spyware:** Theo dõi hoạt động của người dùng mà không có sự đồng ý.  Đánh cắp thông tin cá nhân, mật khẩu và dữ liệu tài chính. Gây ra rủi ro về bảo mật và quyền riêng tư cho người dùng. | - Sử dụng phần mềm diệt virus để quét và loại bỏ virus.  - Khôi phục dữ liệu từ bản sao lưu nếu dữ liệu bị hỏng.  - Cài đặt và cập nhật phần mềm diệt virus thường xuyên.  - Tránh mở tệp đính kèm từ nguồn không rõ ràng.  - Sử dụng tường lửa để kiểm soát lưu lượng mạng.  - Thực hiện các biện pháp bảo mật cho mạng LAN.  - Quét hệ thống bằng phần mềm diệt virus để phát hiện và loại bỏ trojan.  - Thay đổi mật khẩu và thông tin nhạy cảm nếu bị xâm phạm.  - Không tải xuống hoặc cài đặt phần mềm từ nguồn không đáng tin cậy.  - Sử dụng phần mềm bảo mật có khả năng phát hiện trojan. |

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

* Mô hình có nhiều lớp bảo vệ **nhiều lớp bảo vệ**: Mỗi lớp bảo vệ có chức năng riêng, giúp tăng cường an ninh tổng thể bằng cách không phụ thuộc hoàn toàn vào một lớp duy nhất.
* Nguyên tắc ngăn chặn của mô hình: Nếu một lớp bảo vệ bị phá vỡ, các lớp khác vẫn có thể bảo vệ hệ thống.
* Các lớp có trong mô hình:
  + Lớp dữ liệu: Có tác dụng bảo vệ thông tin dữ liệu bằng cách biện pháp như mã hóa dữ liệu khi lưu trữ và truyền tải, sao lưu dữ liệu định kỳ, kiểm soát quyền truy cập
  + Lớp ứng dụng: Bảo vệ các ứng dụng và phần mềm bằng các biện pháp như: Thực hiện kiểm tra bảo mật ứng dụng, cập nhật và vá lỗi thường xuyên, sử dụng mã hóa cho dữ liệu quan trọng.
  + Lớp host: bảo vệ các thiết bị cá nhân và máy chủ trong mạng bằng cách quản lý quyền truy cập, sử dụng và liên tục cập nhật các phần mềm diệt virus, tường lửa…
  + Lớp mạng nội bộ: bảo vệ các mạng nội bộ, nơi mà dữ liệu và ứng dụng quan trọng được lưu trữ và xử lý.
  + Lớp mạng ngoại vi: bảo vệ giới hạn giữa mạng nội bộ và bên ngoài, nhằm ngăn chặn các cuộc tấn công từ Internet.
  + Lớp vật lí: Bảo vệ các thiết bị vật lý, như máy chủ và mạng qua các phương pháp như: Khóa phòng máy chủ, giám sát video, kiểm soát truy cập vật lý.
  + Lớp chính sách thủ tục, con người: Đào tạo và nâng cao nhận thức về an ninh cho người tham gia hệ thống như về các mối đe dọa an ninh, tổ chức các buổi tập huấn, thực hiện chính sách kiểm tra an ninh nội bộ