What Are Risks, Threats, and Vulnerabilities?

Lương Gia Hân - 51403087
Trần Gia Thái - 51703184

Đại học Tôn Đức Thắng

TPHCM

Overview

1. 1. Nguy cơ, mối đe dọa, lỗ hổng:
   - Mục tiêu của các mối đe dọa
   - Các loại mối đe dọa cho hệ thống
2. 2. Các cuộc tấn công độc hại:
3. 3. Các phần mềm độc hại:
4. 4. Các loại tấn công chung:
5. 5. Biện pháp đối phó:

Nguy cơ, mối đe dọa, lỗ hổng

Nguy cơ, đe dọa và lỗ hổng luôn đi chung với nhau.
+ Nguy cơ: thứ gì đó tệ có thể xảy ra.
+ Đe dọa: hành động gây nguy hiểm cho hệ thống và tài nguyên.
+ Lỗ hổng: có thể bị khai thác từ 1 tác nhân đe dọa nào đó.
Không thể loại bỏ nguy cơ nhưng có thể ngăn ngừa các lỗ hổng bảo mật.
Chìa khóa để bảo vệ tài nguyên khỏi các nguy cơ của cuộc tấn công là loại bỏ hoặc đánh dấu các lỗ hổng càng nhiều càng tốt.
Có thể tìm ra nhiều mối đe dọa cũng như lỗ hổng bảo mật trong các tài nguyên cơ sở hạ tầng IT. Bảng sau liệt kê một số lỗi chung thường xảy ra khi sử dụng các cơ sở hạ tầng IT dưới đây.

Cơ sở hạ tầng	Mục tiêu
Con người	- Vi phạm chính sách sử dụng.
Máy trạm	- Các lỗ hổng trên máy trạm, laptop, smart phone. Đây chính là điểm mấu chốt để truy cập vào hệ thống.
LAN	- Kiến trúc quản lý điều tiết trong server, IP đăng nhập.
LAN to WAN	- Truy cập các tài liệu hệ thống mạng từ bên ngoài. - Quảng cáo phần mềm độc hại - Mất lượt truy cập do mất kết nối Internet
WAN	- Truyền dữ liệu không được mã hóa - Các cuộc tấn công nặc danh - Tấn công từ chối dịch vụ - Lỗ hổng trong phần mềm
Quyền truy cập từ xa	- Tấn công Brute - Force để truy cập vào dữ liệu riêng tư - Truy cập trái phép vào nguồn - Rò rỉ dữ liệu hoặc mất thiết bị lưu trữ
Hệ thống / Ứng dụng	- Sử dụng các phần cứng và phần mềm trái phép - Lỗ hổng trong hệ điều hành hoặc phần mềm - Rò rỉ dữ liệu do lỗi hoặc thiên tai

Nguy cơ, mối đe dọa, lỗ hổng

Các mối đe doa phổ biến

- Phần mềm độc hại.
- Lỗi phần cứng hoặc phần mềm.
- Tấn công từ nội bộ bên trong.
- Mất cắp thiết bị.
- Tấn công từ bên ngoài.
- Thiên tai.
- Gián điệp.
- Khủng bố.

Các loại đe dọa cho hệ thống

Mối đe dọa tiết lộ thông tin

Tiết lộ xảy ra bất cứ khi nào người dùng trái phép truy cập thông tin cá nhân hoặc bí mật được lưu trữ trên tài nguyên mạng hoặc trong khi nó đang truyền tải giữa các tài nguyên mạng. . Hai kỹ thuật sau được kẻ tấn công sử dụng trái phép có được hoặc sửa đổi dữ liệu:

- Sabotage (Phá hoại ngầm): Phá hủy tài sản hoặc cản trở những hoạt động bình thường.
- Espionage (Gián điệp): là hành động do thám để có được thông tin bí mật, điển hình là để hỗ trợ cho quốc gia khác.

Mối đe dọa thay đổi thông tin

Vi phạm tính toàn vẹn thông tin. Kiểu tấn công này làm hại hệ thống bằng cách thực hiện các thay đổi trái phép dữ liệu trên một hệ thống do cố ý hoặc vô ý. Thay đổi có chủ ý thường là độc hại.

- Mối đe dọa từ chối và phá hủy

- Các mối đe dọa từ chối hoặc phá hủy làm cho tài sản hoặc tài nguyên không có sẵn hoặc không thể sử dụng được.
- Vi phạm nguyên lý sẵn có của bảo mật thông tin.
- Một cuộc tấn công từ chối hoặc phá hủy thành công khi nó ngăn người dùng được ủy quyền truy cập tài nguyên tạm thời hoặc vĩnh viễn.
- Tấn công DoS là một ví dụ về mối đe dọa từ chối hoặc phá hủy.

Tấn công khai thác lỗ hổng

Các cuộc tấn công có thể bao gồm cả 4 phương thức sau:

1. Giả mạo: tạo ra một số mánh khóe để người dùng không nghi ngờ hệ thống đã bị tấn công.
2. Chặn thông tin: Liên quan đến việc nghe lén các truyền và chuyển hướng chúng để sử dụng trái phép.
3. Gián đoạn thông tin: Gây ra sự gián đoạn trong một kênh truyền thông, ngăn chặn việc truyền dữ liệu.
4. Thay đổi thông tin: thay đổi dữ liệu có trong các đường truyền hoặc tập tin.

2 nhóm tấn công:

1. Tấn công nhằm thay đổi các dữ liệu.
2. Tấn công nhằm nghe lén và theo dõi các dữ liệu.

Các tấn công độc hại

Birthday attacks:

- Tấn công Ngày sinh là một loại tấn công mật mã dựa trên sự khai thác vấn đề Ngày sinh (Birthday problem)- một hiện tượng xác suất tạo ra nghịch lý đối với cảm giác của con người, do vậy còn được gọi là "Nghịch lý Ngày sinh"(Birthday paradox). Áp dụng lí thuyết xác suất thống kê, giả sử trong 1 phòng có 23 người ngẫu nhiên, xác suất có ít nhất 2 người trùng ngày sinh là 50%.
- Công thức tổng quát để tính xác suất có ít nhất 2 người trùng ngày sinh trong n người ngẫu nhiên:

$$p(n) = 1 - \frac{365!}{365^n (365-n)!}$$

- Với n = 70 người ngẫu nhiên, p(n) 99%, nghĩa là gần như chắc chắn trong 70 người ngẫu nhiên có 2 người trùng ngày sinh.

Các tấn công độc hại

Brute – force:

- Kẻ tấn công sẽ thử các mật khẩu khác nhau tr6en một hệ thống cho đến khi thành công.
- Kiểu tấn công này không có kỹ năng hay sự lén lút chỉ dùng vũ lực mà cuối cùng phá vỡ mã.
- Với máy tính quy mô lớn ngày nay, có thể thử hàng triệu kết hợp mật khẩu trong một khoảng thời gian ngắn. Nếu đủ thời gian và đủ máy tính, có thể bẻ khóa hầu hết các thuật toán..

Các tấn công độc hại

Dictionary password attacks

- Là một cuộc tấn công đơn giản dựa vào người dùng thực hiện các lựa chọn mật khẩu kém. Chương trình bẻ khóa mật khẩu đơn giản sẽ lấy tất cả các từ trong tệp từ điển và cố gắng đăng nhập bằng cách nhập từng mục từ điển làm mật khẩu.
- Một chính sách mật khẩu thực thi mật khẩu phức tạp là cách bảo vệ tốt nhất đối với kiểu tấn công từ điển mật khẩu. Người dùng nên tạo mật khẩu gồm một tổ hợp các chữ cái và số và mật khẩu không được bao gồm bất kỳ thông tin cá nhân nào về người dùng.

Các tấn công độc hại

IP Address Spoofing:

- Kĩ thuật này áp dụng khi một máy bên ngoài hệ thống muốn liên kết vào hệ thống đó mà không thông báo trước. Máy tính bên ngoài phải giành được 1 IP để đánh lừa hệ thống. Khi đã xâm nhập thành công, hacker có thể thực hiện tấn công từ chối dịch vụ để làm máy chủ bị nghẽn.

Các tấn công độc hại

Hijacking:

Là một kiểu tấn công trong đó kẻ tấn công chiếm quyền kiểm soát phiên giữa hai máy và giả mạo là một trong số chúng. Có một số loại Hijacking:

- Man-in-the-middle hijacking: Kẻ tấn công sử dụng một chương trình để kiểm soát kết nối bằng cách giả mạo như mỗi đầu của kết nối.
- Browser/ URL hijacking: Chiếm quyền điều khiển trình duyệt hoặc URL Kẻ tấn công có thể sử dụng cuộc tấn công này để lừa đảo để lừa người dùng cung cấp thông tin cá nhân như mật khẩu.(Phising).
- Session Hijacking: Là hình thức tấn công vào phiên làm việc giữa client và server bằng cách đánh cắp cookie của người sử dụng sau khi họ đã qua bước xác thực với máy chủ sau đó sẽ chiếm quyền điều khiển của phiên làm việc này.

Các tấn công độc hại

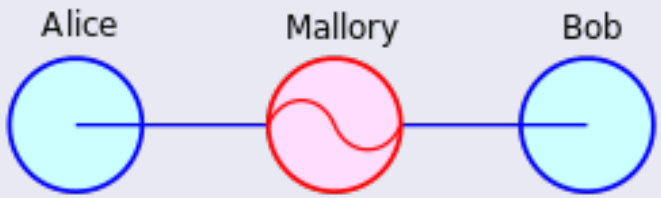
Replay Attacks:

- Tấn công mạng lưới trong đó các thực thể độc hại chặn và lặp lại việc truyền tải một dữ liệu hợp lệ đi vào trong mạng lưới. Nhờ có tính hợp lệ của dữ liệu ban đầu (thường đến từ người dùng đã được cấp quyền), các giao thức bảo mật của mạng lưới sẽ xử lý vụ việc tấn công này chỉ giống như một hình thức truyền tải dữ liệu thông thường. Do các tệp tin ban đầu đã bị ngăn chặn và được truyền tải lại nguyên văn nên hacker thực hiện vụ tấn công sẽ không cần giải mã chúng.

Các tấn công độc hại

Main in the middle:

- Hành động xen giữa cuộc giao tiếp giữa 2 thiết bị mà chúng không hề biết. 2 thiết bị cho rằng đang giao tiếp trong môi trường riêng tư, nhưng thực ra các trao đổi giữa 2 bên lại bị bên thứ 3 nghe lén và thu thập được. Trong kiểu tấn công này, kẻ tấn công chặn tin nhắn giữa hai bên trước khi chuyển chúng đến đích dự định.



Các tấn công độc hại

Masquerading:

- Máy tính và người dùng giả vờ là một máy tính hoặc người dùng khác.
- Các cuộc tấn công giả trang thường bao gồm một trong các hình thức tấn công hoạt động khác, chẳng hạn như giả mạo địa chỉ IP hoặc phát lại. Kẻ tấn công có thể nắm bắt các chuỗi xác thực và sau đó phát lại chúng để đăng nhập lại vào một ứng dụng hoặc hệ điều hành.

Eavesdropping

Tạo ra các gói tin có địa chỉ IP giả mạo không là địa chỉ máy gửi gói tin

Vượt qua các kiểm soát về nguồn gốc địa chỉ IP.

Phục vụ các mô hình tấn công khác.

- Tấn công về phiên Tấn công về session.
- Tấn công kiểu phản xạ.

Giải pháp:

- Không sử dụng xác thực là địa chỉ IP.
- Phát hiện các bất thường về kết nối Phát hiện các bất thường về kết nối mạng.

Các tấn công độc hại

Social Engineering:

- Là kỹ thuật tác động đến con người, nhằm mục đích lấy được thông tin hoặc đạt được một mục đích mong muốn.
- Dựa trên nền tảng là điểm yếu tâm lý, nhận thức sai lầm của con người về việc bảo mật thông tin, sử dụng sự ảnh hưởng và thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công, hoặc thuyết phục nạn nhân thực hiện một hành động nào đó
- Tiến hành khai thác các thói quen tự nhiên của người dùng, hơn việc khai thác các lỗ hổng bảo mật của hệ thống. Người dùng được trang bị kém về kiến thức bảo mật sẽ là cơ sở để tin tặc thực hiện tấn công.

Các tấn công độc hại

Phreaking:

- Phreaking là nghệ thuật khai thác lỗi và trục trặc tồn tại trong hệ thống điện thoại.
- • Bằng cách phreaking, những người này có thể thực hiện một cuộc gọi dài miễn phí hoặc thậm chí là thực hiện cuộc gọi trên máy của người khác.

Các tấn công độc hại

Phishing

- Kẻ tấn công cố gắng lừa nạn nhân cung cấp thông tin cá nhân thông qua email hoặc tin nhắn tức thời.
- Thông điệp hướng dẫn nạn nhân cung cấp thông tin được yêu cầu hoặc nhấp vào một liên kết được cung cấp trong tin nhắn nạn nhân của một trang web giả mạo trông giống hệt với chính thức nhưng trên thực tế thuộc về kẻ lừa đảo. Thông tin cá nhân đã nhập vào trang web này đi trực tiếp đến kẻ lừa đảo.

Các tấn công độc hại

Pharming

- Một loại tấn công khác nhằm tìm cách lấy thông tin tài chính cá nhân hoặc riêng tư thông qua việc giả mạo tên miền.

Phần mềm độc hại

Phreaking:

- Phreaking là nghệ thuật khai thác lỗi và trục trặc tồn tại trong hệ thống điện thoại.
- Bằng cách phreaking, những người này có thể thực hiện một cuộc gọi dài miễn phí hoặc thậm chí là thực hiện cuộc gọi trên máy của người khác.

Phần mềm độc hại

Cương trình lây nhiễm:

- Cố gắng sao chép bản thân sang các máy tính khác. Mục đích chính của nó là để thực hiện một hướng dẫn tấn công của kẻ tấn công vào các mục tiêu mới. Bao gồm:Virues, worms

Cương trình ẩn:

- Ngầm phá hủy, thu thập thông tin trên thiết bị mà không để bị phát hiện. Bao gồm: Trojan horses,Rootkits, spyware.

Phần mềm độc hại

Viruses

Chương trình thâm nhập vào máy tính và tự nhân lên mà không có tác động của người dùng. Có nhiều loại virus khác nhau dựa trên mức độ phá hoại và mục tiêu của nó.

Worms

Là môt dạng kết hợp giữa sức phá hoại, lây lan của virus và tính âm thầm của Trojan. 1 số các worm tồn tại như 1 tập tin, số khác nằm trong bộ nhớ máy tính.

Trojan Horses

Trojan không tự nhân bản được.Bên ngoài trông có vẻ là phần mềm có ích, nhưng nó chỉ tạo lớp ỏ bên ngoài để thâm nhập và phá hủy từ bên trong.

Phần mềm độc hại

Rootkits

Là biến thể mới của phần mềm độc hại, được thiết kế để ẩn mình và vượt qua được nhiều phần mềm bảo vệ. Cần các phần mềm đủ mạnh mới diệt được nó.

Spyware

Được đóng gói như một thành phần ẩn của phần mềm miễn phí hoặc phần mềm chia sẻ các chương trình mà người dùng tải xuống từ Internet, tương tự như Trojan. Nó cũng có thể lây lan thông qua trao đổi tập tin ngang hàng

Các loại tấn công phổ biến

Tấn công vào tính sẵn sàng

Làm ảnh hưởng hoặc tê liệt hoàn toàn các hoạt động tương tác giữa hệ thống với người dùng.

Tấn công vào con người

Đánh vào sự tò mò hoặc ép người dùng phải tiết lộ thông tin hay nhấp vào 1 đường link chứa mã độc nào đó hay dc gửi từ 1 mai không xác định.

Tấn công vào hệ thống IT

Xâm nhập sử dụng tài nguyên trái phép, sửa hoặc xóa các dữ liệu.

Social Engineering Attacks

- Dưới đây là tóm tắt về các cuộc tấn công kỹ thuật xã hội
  - Authority: Sử dụng một vị trí của chính quyền để ép buộc hoặc thuyết phục một cá nhân tiết lộ thông tin.
  - Đồng thuận / bằng chứng xã hội: Dựa vào việc mà mọi người khác đã và đang thực hiện.rằng nó ổn hoặc có thể chấp nhận.
  - Dumpsters-diving: Tìm kiếm những mảnh giấy có thể chứa dữ liệu nhạy cảm hoặc dữ liệu riêng tư để lấy cắp danh tính
  - Hoaxes: Tạo một lừa đảo hoặc nhận thức sai lầm để khiến một cá nhân làm điều gì đó hoặc tiết lộ thông tin.
  - Impersonation: Giả vờ là một người khác.
  - Khẩn cấp: Sử dụng khẩn cấp hoặc một tình huống căng thẳng khẩn cấp để khiến ai đó làm gì đó hoặc tiết lộ thông tin.
  - Vishing: Thực hiện một cuộc tấn công lừa đảo qua điện thoại để lấy thông tin cá nhân sử dụng sự ép buộc bằng lời nói và thuyết phục.

Wireless network attacks

- Các dạng của cuộc tấn công mạng không dây:
  - Bluejacking: Chiếm quyền kiểm soát giữa thiết bị Bluetooth và smartphone.
  - Bluesnarfing: Nghe lén thông tin giữa các thiết bị Bluetooth
  - Evil twin: Giả mạo 1 mạng mục tiêu nào đó, chuyển hướng thiết bị muốn kết nối vào mạng đó sang 1 nơi chuẩn bị trước và yêu cầu nhập lại mật khẩu của mạng thật, khi đó sẽ chiếm dc mật khẩu của mạng thật.
  - Jamming/interference: gửi tần số vô tuyến cùng tần số với các điểm truy cập mạng gây nghẽn mạng.
  - Impersonation: Giả vờ là một người khác.
  - Near field communication attack: NFC: xen giữa giao tiếp NFC giữa 2 smartphone.
  - Packet sniffing: Bắt các gói IP khỏi mạng không dây và phân tích TCP / IP dữ liệu gói bằng cách sử dụng một công cụ như Wireshark®..

Web Aplication acttacks

- Thực thi mã tùy ý / từ xa: Có được quyền truy cập đặc quyền hoặc quyền quản trị hệ thống truy cập, kẻ tấn công có thể chạy các lệnh hoặc thực hiện một lệnh theo ý muốn trên điều khiển hệ thống từ xa.
- Bufferred overflow: Cố gắng đẩy nhiều dữ liệu hơn khả năng lưu trữ để thay đổi hành vi của chương trình dẫn đến các hiệu ứng không muốn hoặc ghi đè địa chỉ trả về.
- Cross-site scripting (XSS): Thêm script vào máy chủ ứng dụng web để chuyển hướng tấn công trở lại máy khác.
- SQL Injection: Thêm các lệnh sql để lấy thông tin và dữ liệu trong cơ sở dữ liệu SQL phía back-end.
- Watering-hole attack: Lôi kéo người dùng đến một trang web thường truy cập trên đó đã được cài mã độc hoặc phần mềm độc hại với hy vọng người dùng sẽ kích hoạt tấn công với một cú nhấp chuột không biết.

Biện pháp ngăn ngừa

- Tạo một chương trình giáo dục (nhận thức bảo mật thông tin) để ngăn người dùng khỏi cài đặt phần mềm độc hại trên hệ thống.
- Đăng các bản tin thường xuyên về các vấn đề về phần mềm độc hại.
- Không bao giờ chuyển tệp từ một nguồn không xác định hoặc không đáng tin trừ khi máy tính có một tiện ích chống phần mềm độc hại được cài đặt.
- Cài đặt phần mềm chống phần mềm độc hại, đảm bảo phần mềm và dữ liệu hiện tại và lên lịch quét phần mềm độc hại thường xuyên.
- Sử dụng quy trình xác thực và đăng nhập an toàn.

Các biện pháp ngăn ngừa

- Một số phần mềm anti malware: BitDefender, Kaspersky Anti-Virus, Webroot Antivirus, Norton Antivirus,...
- Bảo vệ hệ thống với tường lửa: Có rất nhiều giải pháp tường lửa có sẵn. Các nhà cung cấp tường lửa nổi bật bao gồm: Palo Alto Networks, Cisco System, SonicWALL,...

The End