Tổng hợp các kiểu tấn công mạng phổ biến hiện nay

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

1. Tấn công bị động (Passive attack)

Trong một cuộc tấn công bị động, các hacker sẽ kiểm soát traffic không được mã hóa và tìm kiếm mật khẩu không được mã hóa (Clear Text password), các thông tin nhạy cảm có thể được sử dụng trong các kiểu tấn công khác. Các cuộc tấn công bị động bao gồm phân tích traffic, giám sát các cuộc giao tiếp không được bảo vệ, giải mã các traffic mã hóa yếu, và thu thập các thông tin xác thực như mật khẩu.

Các cuộc tấn công chặn bắt thông tin hệ thống mạng cho phép kẻ tấn công có thể xem xét các hành động tiếp theo. Kết quả của các cuộc tấn công bị động là các thông tin hoặc file dữ liệu sẽ bị rơi vào tay kẻ tấn công mà người dùng không hề hay biết.

2. Tấn công rải rác (Distributed attack)

Đối với các cuộc tấn công rải rác yêu cầu kẻ tấn công phải giới thiệu mã, chẳng hạn như một chương trình Trojan horse hoặc một chương trình back-door, với một thành phần "tin cậy" hoặc một phần mềm được phân phối cho nhiều công ty khác và tấn công user bằng cách tập trung vào việc sửa đổi các phần mềm độc hại của phần cứng hoặc phần mềm trong quá trình phân phối,... Các cuộc tấn công giới thiệu mã độc hại chẳng hạn như back door trên một sản phẩm nhằm mục đích truy cập trái phép các thông tin hoặc truy cập trái phép các chức năng trên hệ thống.

3. Tấn công nội bộ (Insider attack)

Các cuộc tấn công nội bộ (insider attack) liên quan đến người ở trong cuộc, chẳng hạn như một nhân viên nào đó "bất mãn" với công ty của mình,…các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại.

Người trong cuộc cố ý nghe trộm, ăn cắp hoặc phá hoại thông tin, sử dụng các thông tin một cách gian lận hoặc truy cập trái phép các thông tin.

4. Tấn công Phishing

Trong các cuộc tấn công phising, các hacker sẽ tạo ra một trang web giả trông "giống hệt" như các trang web phổ biến. Trong các phần tấn công phising, các hacker sẽ gửi một email để người dùng click vào đó và điều hướng đến trang web giả mạo. Khi người dùng đăng nhập thông tin tài khoản của họ, các hacker sẽ lưu lại tên người dùng và mật khẩu đó lại.

5. Các cuộc tấn công của không tặc (Hijack attack)

Trong các cuộc tấn công của không tặc, các hacker sẽ giành quyền kiểm soát và ngắt kết nối cuộc nói chuyện giữa bạn và một người khác.

6. Tấn công mật khẩu (Password attack)

Đối với các cuộc tấn công mật khẩu, các hacker sẽ cố gắng "phá" mật khẩu được lưu trữ trên cơ sở dữ liệu tài khoản hệ thống mạng hoặc mật khẩu bảo vệ các tập tin.

Các cuộc tấn công mật khẩu bao gồm 3 loại chính: các cuộc tấn công dạng từ điển (dictionary attack), brute-force attack và hybrid attack.

Cuộc tấn công dạng từ điển sử dụng danh sách các tập tin chứa các mật khẩu tiềm năng.

7. Khai thác lỗ hổng tấn công (Exploit attack)

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

8. Buffer overflow (lỗi tràn bộ đệm)

Một cuộc tấn công buffer attack xảy ra khi các hacker gửi dữ liệu tới một ứng dụng nhiều hơn so với dự kiến. Và kết quả của cuộc tấn công buffer attack là các hacker tấn công truy cập quản trị hệ thống trên Command Prompt hoặc Shell.

9. Tấn công từ chối dịch vụ (denial of service attack)

Không giống như các cuộc tấn công mật khẩu (Password attack), các cuộc tấn công từ chối dịch vụ (denial of service attack) ngăn chặn việc sử dụng máy tính của bạn hoặc hệ thống mạng theo cách thông thường bằng valid users.

Sau khi tấn công, truy cập hệ thống mạng của bạn, các hacker có thể:

- Chặn traffic.

- Gửi các dữ liệu không hợp lý tới các ứng dụng hoặc các dịch vụ mạng, dẫn đến việc thông báo chấm dứt hoặc các hành vi bất thường trên các ứng dụng hoặc dịch vụ này.

- Lỗi tràn bộ nhớ đệm.

10. Tấn công theo kiểu Man-in-the-Middle Attack

Đúng như cái tên của nó, một cuộc tấn công theo kiểu Man-in-the-Middle Attack xảy ra khi cuộc nói chuyện giữa bạn và một người nào đó bị kẻ tấn công theo dõi, nắm bắt và kiểm soát thông tin liên lạc của bạn một cách minh bạch.

Các cuộc tấn công theo kiểu Man-in-the-Middle Attack giống như một người nào đó giả mạo danh tính để đọc các tin nhắn của bạn. Và người ở đầu kia tin rằng đó là bạn, bởi vì kẻ tấn công có thể trả lời một cách tích cực để trao đổi và thu thập thêm thông tin.

11. Tấn công phá mã khóa (Compromised-Key Attack)

Mã khóa ở đây là mã bí mật hoặc các con số quan trọng để "giải mã" các thông tin bảo mật. Mặc dù rất khó để có thể tấn công phá một mã khóa, nhưng với các hacker thì điều này là có thể. Sau khi các hacker có được một mã khóa, mã khóa này sẽ được gọi là mã khóa gây hại.

Hacker sử dụng mã khóa gây hại này để giành quyền truy cập các thông tin liên lạc mà không cần phải gửi hoặc nhận các giao thức tấn công. Với các mã khóa gây hại, các hacker có thể giải mã hoặc sửa đổi dữ liệu.

12. Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò tìm tên người sử dụng và mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không

đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một chương trình tự động hoá về việc dò tìm mật khẩu này.

Một chương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của hệ thống unix có tên là crack, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.

Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (root hay administrator).

Hai ví dụ thường xuyên được đưa ra để minh hoạ cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.

Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.

Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

13. Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên, mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa card giao tiếp mạng (Network

Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

14. Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

15. Vô hiệu các chức năng của hệ thống

Đây là kiểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

Ví dụ sử dụng lệnh ping với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

16. Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

17. Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.