**Kiểm tra thâm nhập không dây**

* Định nghĩa: Quá trình kiểm tra tính bảo mật của mạng không dây và thiết bị bằng cách mô phỏng các cuộc tấn công và xác định các lỗ hổng.
* Mục tiêu: Để đánh giá hiệu quả của các biện pháp bảo mật mạng không dây và xác định các điểm yếu tiềm ẩn có thể bị khai thác bởi những kẻ tấn công.
* Phạm vi: Bao gồm nhiều loại công nghệ không dây, bao gồm Wi-Fi, Bluetooth, di động và liên lạc vệ tinh.
* Các bước chính:
  + Trinh sát: Thu thập thông tin về mạng mục tiêu, bao gồm SSID, địa chỉ MAC và cường độ tín hiệu.
  + Liệt kê: Xác định loại bảo mật không dây được sử dụng (WEP, WPA, WPA2, v.v.), khóa mã hóa và bất kỳ biện pháp bảo mật nào khác được áp dụng.
  + Khai thác: Cố gắng khai thác bất kỳ lỗ hổng nào được tìm thấy trong mạng hoặc thiết bị, chẳng hạn như mật khẩu yếu, điểm truy cập được định cấu hình sai hoặc phần mềm chưa được vá.
  + Báo cáo: Ghi lại các phát hiện và đưa ra các khuyến nghị để cải thiện tính bảo mật của mạng và thiết bị.
* Công cụ: Các công cụ phổ biến được sử dụng để thử nghiệm thâm nhập mạng không dây bao gồm Aircrack-ng, Wireshark, Metasploit và Kali Linux.
* Tầm quan trọng: Mạng không dây ngày càng phổ biến và dễ bị tấn công, điều quan trọng là các tổ chức phải kiểm tra và cải thiện các biện pháp bảo mật của họ để ngăn chặn vi phạm dữ liệu và các sự cố bảo mật khác.

**Kiểm tra thâm nhập mạng cục bộ không dây (WLAN)**

* Định nghĩa: Quá trình kiểm tra tính bảo mật của mạng cục bộ không dây (WLAN) bằng cách mô phỏng các cuộc tấn công và xác định các lỗ hổng trong mạng và các thiết bị của mạng.
* Mục tiêu: Để xác định các điểm yếu tiềm ẩn và lỗ hổng bảo mật trong mạng WLAN và đưa ra các khuyến nghị để cải thiện tính bảo mật của mạng.
* Phạm vi: Bao gồm kiểm tra tính bảo mật của mạng WLAN, có thể bao gồm các điểm truy cập, bộ định tuyến không dây, máy khách không dây và chính giao thức truyền thông không dây.
* Các bước chính:
  + Do thám: Thu thập thông tin về mạng WLAN, bao gồm SSID, địa chỉ MAC và cường độ tín hiệu.
  + Liệt kê: Xác định loại bảo mật không dây được sử dụng (WEP, WPA, WPA2, v.v.), khóa mã hóa và bất kỳ biện pháp bảo mật nào khác được áp dụng.
  + Khai thác: Cố gắng khai thác bất kỳ lỗ hổng nào được tìm thấy trong mạng WLAN, chẳng hạn như mật khẩu yếu, điểm truy cập được định cấu hình sai hoặc phần mềm chưa được vá.
  + Báo cáo: Ghi lại các phát hiện và đưa ra các đề xuất để cải thiện tính bảo mật của mạng WLAN và các thiết bị của nó.
* Công cụ: Các công cụ phổ biến được sử dụng để kiểm tra thâm nhập mạng WLAN bao gồm Aircrack-ng, Wireshark, Metasploit và Kali Linux.
* Tầm quan trọng: Mạng WLAN ngày càng phổ biến trong cả môi trường gia đình và doanh nghiệp và dễ bị tấn công, điều quan trọng là các tổ chức phải kiểm tra và cải thiện các biện pháp bảo mật của họ để ngăn chặn vi phạm dữ liệu và các sự cố bảo mật khác. Thử nghiệm thâm nhập mạng WLAN có thể giúp xác định các lỗ hổng bảo mật tiềm ẩn trong mạng và đưa ra các đề xuất để cải thiện tính bảo mật của mạng WLAN và các thiết bị của nó.

**Khám phá mạng không dây**

Khám phá các mạng không dây là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó giúp xác định các mục tiêu tấn công tiềm năng. Có một số công cụ và kỹ thuật có thể được sử dụng để khám phá các mạng không dây, bao gồm:

* Quét các điểm truy cập Wi-Fi: Các điểm truy cập Wi-Fi thường được định cấu hình để phát SSID (Mã định danh bộ dịch vụ) của chúng và có thể dễ dàng phát hiện bằng cách sử dụng các trình quét Wi-Fi, chẳng hạn như inSSIDer hoặc NetStumbler. Những công cụ này cho phép người kiểm tra thâm nhập xác định sự hiện diện, vị trí và độ mạnh của các điểm truy cập Wi-Fi.
* Lái xe chiến tranh: Lái xe chiến tranh là một kỹ thuật được sử dụng để khám phá các mạng không dây bằng cách lái xe quanh một khu vực địa lý bằng máy quét Wi-Fi, chẳng hạn như máy tính xách tay hoặc điện thoại thông minh. Phương pháp này hữu ích để xác định các điểm truy cập Wi-Fi nằm ngoài vị trí trực tiếp của người kiểm tra thâm nhập.
* Sử dụng bộ dò tìm không dây: Có thể sử dụng bộ dò tìm không dây, chẳng hạn như Wireshark, để nắm bắt lưu lượng truy cập không dây và phân tích lưu lượng truy cập không dây đó để lấy thông tin về mạng không dây, bao gồm SSID, loại mã hóa và bất kỳ điểm truy cập mở hoặc dễ bị tấn công nào.
* Sử dụng máy phân tích phổ không dây: Máy phân tích phổ không dây, chẳng hạn như AirMagnet hoặc Wi-Spy, có thể được sử dụng để phân tích phổ tần số được sử dụng bởi các mạng không dây, cung cấp thông tin về loại và cường độ của tín hiệu không dây trong một khu vực nhất định.

Khám phá các mạng không dây là một bước quan trọng trong thử nghiệm thâm nhập không dây vì nó cung cấp thông tin cần thiết để xác định các mục tiêu tấn công tiềm năng. Bằng cách xác định các mạng không dây trong một khu vực nhất định, người kiểm tra thâm nhập có thể đánh giá tính bảo mật của các mạng và thiết bị này và đưa ra các khuyến nghị để cải thiện các biện pháp bảo mật của họ.

**Kiểm tra bảo mật vật lý của các điểm truy cập (AP)**

Bảo mật vật lý là một khía cạnh quan trọng của thử nghiệm thâm nhập mạng không dây, vì kẻ tấn công có thể cố gắng giành quyền truy cập vào mạng của tổ chức bằng cách giả mạo vật lý hoặc đánh cắp Điểm truy cập (AP). Dưới đây là một số bước có thể thực hiện để kiểm tra tính bảo mật vật lý của các AP:

* Xác minh vị trí AP: Xác minh rằng các AP được đặt ở những vị trí an toàn, chẳng hạn như tủ khóa hoặc phòng máy chủ, để ngăn truy cập trái phép.
* Kiểm tra các kết nối cáp: Kiểm tra các kết nối cáp của AP để đảm bảo rằng chúng được buộc chặt an toàn và người dùng trái phép không thể truy cập được.
* Kiểm tra các dấu hiệu giả mạo: Kiểm tra các dấu hiệu giả mạo hoặc hư hỏng vật lý đối với AP, chẳng hạn như con dấu bị hỏng, vít hoặc tấm che, điều này có thể cho thấy rằng ai đó đã cố gắng truy cập trái phép vào AP.
* Xác minh địa chỉ MAC: Xác minh rằng địa chỉ MAC của các AP khớp với địa chỉ MAC của các thiết bị được ủy quyền trên mạng, để đảm bảo rằng các AP giả mạo không được thêm vào mạng.
* Xác minh phiên bản chương trình cơ sở: Kiểm tra phiên bản chương trình cơ sở của các AP để đảm bảo rằng chúng được cập nhật và không có các lỗ hổng đã biết có thể bị kẻ tấn công khai thác.
* Tiến hành thử nghiệm thâm nhập vật lý: Tiến hành thử nghiệm thâm nhập vật lý để mô phỏng một cuộc tấn công vào bảo mật vật lý của các AP, để xác định bất kỳ điểm yếu hoặc lỗ hổng nào có thể bị kẻ tấn công khai thác.

Kiểm tra bảo mật vật lý của các AP là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó giúp đảm bảo rằng mạng được bảo vệ khỏi các cuộc tấn công vật lý. Bằng cách thực hiện các bước để xác minh tính bảo mật vật lý của các AP, các tổ chức có thể giúp ngăn chặn truy cập trái phép vào mạng và bảo vệ khỏi các vi phạm bảo mật tiềm ẩn.

**Phát hiện kết nối không dây**

Phát hiện các kết nối không dây là một khía cạnh quan trọng của thử nghiệm xâm nhập không dây, vì nó giúp xác định các mục tiêu tấn công tiềm năng. Có một số công cụ và kỹ thuật có thể được sử dụng để phát hiện các kết nối không dây, bao gồm:

* Máy quét không dây: Máy quét không dây, chẳng hạn như inSSIDer hoặc NetStumbler, có thể được sử dụng để phát hiện mạng không dây và cung cấp thông tin về tên mạng (SSID), loại mã hóa, cường độ tín hiệu và các chi tiết khác.
* Trình nghe lén gói không dây: Trình nghe lén gói không dây, chẳng hạn như Wireshark, có thể được sử dụng để nắm bắt và phân tích lưu lượng không dây, cung cấp thông tin về mạng không dây, các thiết bị được kết nối với mạng và lưu lượng truy cập qua mạng.
* Hệ thống phát hiện xâm nhập không dây (WIDS): Các hệ thống WIDS, chẳng hạn như Cisco Meraki hoặc Aruba Networks, được thiết kế để phát hiện và cảnh báo quản trị viên về truy cập không dây trái phép vào mạng.
* Bộ điều khiển điểm truy cập không dây: Bộ điều khiển điểm truy cập không dây, chẳng hạn như Aruba ClearPass hoặc Cisco Identity Services Engine (ISE), có thể được sử dụng để giám sát và kiểm soát quyền truy cập vào mạng bằng cách xác định các thiết bị trái phép và chặn quyền truy cập.

Bằng cách sử dụng các công cụ và kỹ thuật này để phát hiện các kết nối không dây, những người kiểm tra thâm nhập có thể hiểu rõ hơn về các mạng không dây trong môi trường mục tiêu và xác định các mục tiêu tấn công tiềm năng. Bằng cách xác định các mạng không dây trong một khu vực nhất định, người kiểm tra thâm nhập có thể đánh giá tính bảo mật của các mạng và thiết bị này và đưa ra các khuyến nghị để cải thiện các biện pháp bảo mật của họ.

Điều quan trọng cần lưu ý là việc phát hiện các kết nối không dây phải được thực hiện theo cách được kiểm soát và cho phép, đồng thời tuân thủ mọi cân nhắc về pháp lý và đạo đức. Người kiểm tra thâm nhập phải có được sự cho phép và đồng ý thích hợp trước khi tiến hành bất kỳ hoạt động kiểm tra thâm nhập không dây nào và phải tuân theo tất cả các luật, quy định và nguyên tắc đạo đức hiện hành.

**Đánh hơi lưu lượng giữa AP và các thiết bị được liên kết**

Đánh hơi lưu lượng mạng là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó cho phép người kiểm tra thâm nhập nắm bắt và phân tích lưu lượng mạng giữa các điểm truy cập không dây (AP) và các thiết bị được liên kết. Dưới đây là một số bước có thể được thực hiện để đánh hơi lưu lượng giữa AP và các thiết bị được liên kết:

* Chọn công cụ thích hợp: Chọn một công cụ để theo dõi lưu lượng truy cập tương thích với giao thức không dây đang được sử dụng bởi AP và các thiết bị được liên kết, chẳng hạn như Wireshark hoặc Aircrack-ng.
* Thiết lập bộ dò tìm: Định cấu hình bộ dò tìm để nắm bắt lưu lượng trên mạng không dây, chọn kênh và băng tần thích hợp.
* Nắm bắt lưu lượng: Nắm bắt lưu lượng giữa AP và các thiết bị được liên kết để phân tích lưu lượng mạng để tìm các dấu hiệu của lỗ hổng hoặc điểm yếu.
* Phân tích lưu lượng bị bắt: Phân tích lưu lượng bị bắt để xác định các lỗ hổng tiềm ẩn, chẳng hạn như mã hóa yếu, lưu lượng không được mã hóa hoặc thiết bị mạng được định cấu hình không đúng.
* Sử dụng lưu lượng truy cập bị bắt cho các cuộc tấn công tiếp theo: Sử dụng lưu lượng truy cập bị bắt để khởi chạy các cuộc tấn công tiếp theo, chẳng hạn như tấn công phát lại, liên quan đến việc phát lại lưu lượng truy cập bị bắt để giành quyền truy cập trái phép vào mạng.

Đánh hơi lưu lượng giữa AP và các thiết bị được liên kết là một bước quan trọng trong thử nghiệm thâm nhập mạng không dây, vì nó cho phép người thử nghiệm thâm nhập xác định các lỗ hổng và điểm yếu tiềm ẩn trong mạng. Bằng cách nắm bắt và phân tích lưu lượng mạng, người kiểm tra thâm nhập có thể xác định các lỗ hổng và đề xuất các biện pháp bảo mật để ngăn chặn vi phạm bảo mật và các sự cố bảo mật khác.

**Tạo một điểm truy cập giả mạo**

Điểm truy cập giả mạo là điểm truy cập không dây trái phép được kết nối với mạng mà quản trị viên mạng không biết hoặc không cho phép. Tạo điểm truy cập giả mạo là một kỹ thuật phổ biến được sử dụng trong thử nghiệm xâm nhập không dây để kiểm tra tính bảo mật của mạng không dây. Dưới đây là một số bước có thể được thực hiện để tạo một điểm truy cập giả mạo:

* Lấy điểm truy cập không dây: Lấy điểm truy cập không dây không thuộc mạng đang được kiểm tra. Đây có thể là một thiết bị độc lập hoặc thiết bị đã được định cấu hình để hoạt động ở chế độ giả mạo.
* Định cấu hình điểm truy cập: Định cấu hình điểm truy cập bằng SSID tương tự với SSID của mạng hợp pháp đang được thử nghiệm. Điều này có thể giúp đánh lừa các máy khách không dây kết nối với điểm truy cập lừa đảo.
* Kết nối với mạng: Kết nối điểm truy cập giả mạo với mạng đang được kiểm tra, bằng cách cắm điểm truy cập đó vào cổng có dây hoặc kết nối không dây.
* Giám sát lưu lượng mạng: Giám sát lưu lượng mạng để xác định bất kỳ thiết bị nào kết nối với điểm truy cập giả mạo. Điều này có thể giúp xác định các mục tiêu tiềm năng để tấn công.

Tạo một điểm truy cập giả mạo có thể là một kỹ thuật hữu ích trong thử nghiệm thâm nhập mạng không dây, vì nó có thể giúp xác định các lỗ hổng bảo mật tiềm ẩn trong mạng.

**Tạo một khách hàng lăng nhăng**

Máy khách hỗn tạp là một thiết bị được định cấu hình để nắm bắt tất cả lưu lượng không dây trong phạm vi của nó, bất kể nó có dành cho thiết bị hay không. Tạo một ứng dụng khách bừa bãi là một kỹ thuật phổ biến khác được sử dụng trong thử nghiệm thâm nhập không dây để kiểm tra tính bảo mật của mạng không dây. Dưới đây là một số bước có thể được thực hiện để tạo một khách hàng lăng nhăng:

* Lấy thẻ giao diện mạng không dây (NIC): Lấy một NIC không dây có khả năng ở chế độ hỗn hợp. Đây có thể là USB dongle hoặc thẻ PCI.
* Định cấu hình NIC: Định cấu hình NIC để hoạt động ở chế độ hỗn tạp. Điều này có thể được thực hiện bằng cách sử dụng một công cụ như Wireshark hoặc bằng cách sửa đổi các tệp cấu hình của trình điều khiển NIC.
* Nắm bắt lưu lượng mạng: Nắm bắt tất cả lưu lượng không dây trong phạm vi của thiết bị, sử dụng công cụ như Wireshark hoặc tcpdump. Điều này có thể giúp xác định các mục tiêu tiềm năng để tấn công.

Tạo một ứng dụng khách hỗn tạp có thể là một kỹ thuật hữu ích trong thử nghiệm thâm nhập mạng không dây, vì nó có thể giúp xác định các lỗ hổng bảo mật tiềm ẩn trong mạng và cung cấp thông tin chi tiết về hành vi của các thiết bị không dây trên mạng.

Honeypot không dây là một cơ chế bảo mật được sử dụng để thu hút và phát hiện các nỗ lực xâm phạm mạng không dây. Nó bắt chước một điểm truy cập không dây hợp pháp, nhưng thay vì cung cấp quyền truy cập vào mạng thực, nó cung cấp một mạng giả được sử dụng để thu thập thông tin về những kẻ tấn công hoặc lỗ hổng.

Dưới đây là các bước chung để sử dụng một honeypot không dây để khám phá các máy khách không dây dễ bị tấn công:

1. Thiết lập honeypot không dây: Để tạo honeypot không dây, bạn cần một thiết bị có thể bắt chước điểm truy cập không dây. Bạn có thể sử dụng phần mềm chuyên dụng như Kismet, Wireshark hoặc OpenWRT để thiết lập một điểm truy cập không dây giả có thể nắm bắt và phân tích lưu lượng. Bạn cũng sẽ cần tạo một tên mạng giả (SSID) và mật khẩu.
2. Thu hút khách hàng đến với honeypot: Sau khi thiết lập xong honeypot, bạn cần thu hút các khách hàng không dây dễ bị tổn thương kết nối với nó. Một cách để thực hiện điều này là làm cho tên mạng (SSID) và mật khẩu giả trông hợp pháp, chẳng hạn như sử dụng các tên mạng phổ biến như "Starbucks" hoặc "Wi-Fi miễn phí". Bạn cũng có thể thử phát SSID để xem có thiết bị nào tự động kết nối với nó không.
3. Nắm bắt lưu lượng và phân tích nó: Khi một máy khách dễ bị tổn thương kết nối với honeypot, thì honeypot sẽ nắm bắt lưu lượng và phân tích nó. Bạn có thể sử dụng các công cụ như Wireshark để phân tích lưu lượng truy cập và tìm kiếm bất kỳ dấu hiệu dễ bị tổn thương hoặc tấn công nào. Ví dụ: bạn có thể thấy lưu lượng truy cập không được mã hóa, mật khẩu yếu hoặc dấu hiệu của một cuộc tấn công vũ phu.
4. Bảo mật mạng: Khi bạn đã xác định được các máy khách dễ bị tấn công, bạn có thể sử dụng thông tin này để bảo mật mạng. Điều này có thể liên quan đến việc vá các lỗ hổng, thay đổi mật khẩu hoặc triển khai mã hóa mạnh hơn.
5. Giám sát mạng: Để tiếp tục bảo vệ mạng, bạn nên giám sát mạng thường xuyên và đảm bảo rằng không có lỗ hổng hoặc cuộc tấn công mới nào được phát hiện. Bạn có thể sử dụng honeypot không dây để tiếp tục thu hút những kẻ tấn công tiềm năng và xác định các lỗ hổng mới.

Thực hiện tấn công từ chối dịch vụ (DoS), cụ thể là tấn công hủy xác thực, liên quan đến việc gửi các gói hủy xác thực giả mạo đến một điểm truy cập không dây hoặc thiết bị khách. Kiểu tấn công này có thể ngăn người dùng hợp pháp truy cập mạng không dây hoặc có thể khiến thiết bị ngắt kết nối khỏi mạng và cố gắng kết nối lại nhiều lần, do đó gây ra tình trạng từ chối dịch vụ.

Dưới đây là các bước chung liên quan đến việc thực hiện một cuộc tấn công hủy xác thực:

1. Lấy bộ điều hợp không dây: Để thực hiện tấn công hủy xác thực, bạn sẽ cần một bộ điều hợp không dây có khả năng chèn gói. Điều này cho phép bạn gửi các gói hủy xác thực giả mạo đến thiết bị hoặc mạng đích.
2. Chọn mục tiêu: Mục tiêu có thể là một thiết bị cụ thể được kết nối với mạng không dây hoặc toàn bộ mạng. Bạn có thể sử dụng các công cụ như Kismet, Airodump-ng hoặc Wireshark để xác định mạng không dây và các thiết bị được kết nối với mạng đó.
3. Sử dụng công cụ hủy xác thực: Hiện có nhiều công cụ hủy xác thực khác nhau, chẳng hạn như Aireplay-ng hoặc MDK3, có thể tự động hóa quá trình gửi các gói hủy xác thực. Các công cụ này sẽ gửi các gói hủy xác thực đến thiết bị hoặc mạng đích, khiến thiết bị hoặc mạng đó bị ngắt kết nối khỏi mạng không dây.
4. Theo dõi cuộc tấn công: Trong cuộc tấn công, bạn có thể sử dụng các công cụ như Wireshark hoặc tcpdump để theo dõi lưu lượng và xác nhận rằng các gói hủy xác thực đang được gửi và nhận.
5. Dừng cuộc tấn công: Để dừng cuộc tấn công, bạn chỉ cần ngừng gửi các gói xác thực.

Điều quan trọng cần lưu ý là thực hiện tấn công hủy xác thực mà không được phép là bất hợp pháp và có thể dẫn đến hậu quả nghiêm trọng. Kiểu tấn công này có thể làm gián đoạn người dùng hợp pháp truy cập mạng không dây và có thể gây hư hỏng cho thiết bị hoặc mạng. Ngoài ra, điều quan trọng là phải thận trọng khi thử nghiệm hoặc thực hành các kiểu tấn công này vì chúng có thể vô tình gây hại.

"Tạo lưu lượng truy cập nhanh" là một kỹ thuật được sử dụng trong thử nghiệm xâm nhập không dây để đánh giá hiệu suất và tính bảo mật của mạng không dây. Kỹ thuật này liên quan đến việc tạo ra một lưu lượng truy cập lớn trong một khoảng thời gian ngắn để kiểm tra khả năng xử lý và phản hồi lưu lượng của mạng.

Trong quá trình thử nghiệm thâm nhập không dây, việc tạo lưu lượng truy cập nhanh có thể được sử dụng để kiểm tra hiệu suất tổng thể của mạng không dây, xác định các tắc nghẽn hiệu suất tiềm ẩn và kiểm tra cách mạng phản ứng với các loại lưu lượng khác nhau. Kỹ thuật này cũng có thể được sử dụng để xác định các lỗ hổng bảo mật, chẳng hạn như các cuộc tấn công từ chối dịch vụ (DoS), bằng cách làm mạng quá tải lưu lượng và quan sát cách mạng phản hồi.

Tuy nhiên, điều quan trọng cần lưu ý là việc tạo lưu lượng truy cập nhanh có thể làm gián đoạn hoạt động bình thường của mạng không dây và do đó chỉ nên được thực hiện bởi các chuyên gia bảo mật có trình độ trong môi trường được kiểm soát. Việc sử dụng trái phép các kỹ thuật tạo lưu lượng truy cập nhanh có thể gây gián đoạn dịch vụ, vi phạm chính sách mạng và thậm chí dẫn đến hậu quả pháp lý.

Giải mã gói đơn là một kỹ thuật được sử dụng trong thử nghiệm thâm nhập không dây để bẻ khóa lưu lượng mạng không dây được mã hóa. Trong các mạng không dây, dữ liệu thường được truyền qua mạng ở dạng mã hóa để ngăn chặn việc nghe lén và truy cập trái phép. Để giải mã dữ liệu này, kẻ tấn công cần nắm bắt các gói được mã hóa, sau đó sử dụng các công cụ và kỹ thuật để phá vỡ mã hóa.

Giải mã gói đơn là phương pháp liên quan đến việc nắm bắt một gói lưu lượng truy cập mạng và sau đó cố gắng bẻ khóa mã hóa của nó. Kỹ thuật này rất hữu ích trong các tình huống mà kẻ tấn công có thời gian hoặc tài nguyên hạn chế, vì nó không yêu cầu bắt một số lượng lớn các gói hoặc một phiên hoàn chỉnh.

Có một số công cụ và kỹ thuật có sẵn để thực hiện giải mã gói đơn, bao gồm các công cụ như Aircrack-ng, Wireshark và Cain and Abel. Các công cụ này sử dụng nhiều phương pháp khác nhau để bẻ khóa mã hóa, bao gồm tấn công từ điển, tấn công vũ phu và tấn công bảng cầu vồng. Mỗi phương pháp đều có điểm mạnh và điểm yếu riêng và có thể ít nhiều hiệu quả tùy thuộc vào loại mã hóa được sử dụng.

Cần lưu ý rằng việc cố gắng giải mã một gói không phải lúc nào cũng hợp pháp và nó chỉ nên được thực hiện trong môi trường được kiểm soát với sự cho phép hợp pháp thích hợp. Thử nghiệm thâm nhập và hack đạo đức chỉ nên được thực hiện với sự cho phép rõ ràng của tổ chức mục tiêu và dưới sự hướng dẫn của một chuyên gia có kinh nghiệm.

Ngộ độc ARP (còn được gọi là giả mạo ARP) là một kỹ thuật được sử dụng để chặn lưu lượng mạng. Trong cuộc tấn công này, kẻ tấn công gửi thông báo Giao thức phân giải địa chỉ (ARP) giả mạo tới mạng, liên kết địa chỉ MAC của kẻ tấn công với địa chỉ IP của thiết bị hợp pháp trên mạng. Do đó, tất cả lưu lượng truy cập mạng dành cho thiết bị hợp pháp thay vào đó được gửi đến kẻ tấn công.

Thực hiện một cuộc tấn công đầu độc ARP thường bao gồm các bước sau:

1. Xác định thiết bị đích: Xác định địa chỉ IP của thiết bị mà bạn muốn chặn lưu lượng truy cập.
2. Bật chuyển tiếp IP: Trên máy tấn công của bạn, hãy bật chuyển tiếp IP để nó có thể hoạt động như một bộ định tuyến và chuyển tiếp lưu lượng truy cập từ thiết bị đích đến đích dự kiến. Trong Linux, bạn có thể sử dụng lệnh sau để bật chuyển tiếp IP:

tiếng vang 1 > /proc/sys/net/ipv4/ip\_forward

1. Thực hiện giả mạo ARP: Sử dụng công cụ giả mạo ARP như Ettercap hoặc arpspoof để gửi thông báo ARP giả mạo đến mạng. Những thông báo này sẽ liên kết địa chỉ MAC của bạn với địa chỉ IP của thiết bị đích. Ví dụ: để thực hiện đầu độc ARP bằng Ettercap, bạn có thể sử dụng lệnh sau:

ettercap -T -M arp:remote /targetIP// /gatewayIP//

Trong lệnh này, **/targetIP/** là địa chỉ IP của thiết bị đích và **/gatewayIP/** là địa chỉ IP của cổng mặc định của mạng.

1. Chặn lưu lượng: Sau khi bạn đã đầu độc thành công bộ đệm ARP của thiết bị đích, bạn có thể chặn lưu lượng của nó bằng cách sử dụng trình thám thính mạng như Wireshark. Trình thám thính sẽ nắm bắt tất cả lưu lượng mạng dành cho thiết bị đích, có thể bao gồm thông tin xác thực đăng nhập, dữ liệu nhạy cảm hoặc thông tin có giá trị khác.

Điều quan trọng cần lưu ý là việc thực hiện một cuộc tấn công đầu độc ARP mà không được phép là bất hợp pháp và phi đạo đức. Nó chỉ nên được thực hiện trong một môi trường được kiểm soát với sự cho phép của chủ sở hữu mạng như một phần của đánh giá bảo mật hoặc thử nghiệm thâm nhập.

Tiêm một gói được mã hóa yêu cầu kiến thức về thuật toán mã hóa và khóa được sử dụng để mã hóa gói. Không có thông tin này, không thể tiêm một gói được mã hóa hợp lệ.

Giả sử bạn có khóa và thuật toán mã hóa, bạn có thể thực hiện các bước sau để cố gắng đưa vào một gói tin được mã hóa:

1. Chụp gói mã hóa hợp lệ: Sử dụng trình nghe trộm mạng như Wireshark để chụp gói mã hóa hợp lệ được gửi giữa hai thiết bị trên mạng.
2. Giải mã gói bị bắt: Sử dụng khóa mã hóa và thuật toán để giải mã gói bị bắt. Điều này sẽ cho phép bạn xem nội dung của gói tin.
3. Sửa đổi gói đã giải mã: Sau khi gói được giải mã, hãy sửa đổi nội dung của gói để bao gồm tải trọng hoặc dữ liệu mong muốn.
4. Mã hóa gói tin đã sửa đổi: Sử dụng khóa mã hóa và thuật toán để mã hóa gói tin đã sửa đổi.
5. Tiêm gói đã mã hóa: Sử dụng một công cụ như Scapy để đưa gói đã sửa đổi và mã hóa vào mạng.

Việc bẻ khóa WPA-PSK (Khóa chia sẻ trước) yêu cầu bắt một gói bắt tay và sau đó thực hiện một cuộc tấn công vũ phu để đoán mật khẩu. Các bước sau đây có thể được sử dụng để bẻ khóa các khóa WPA-PSK:

1. Thiết lập giao diện không dây ở chế độ màn hình: Điều này là cần thiết để nắm bắt lưu lượng giữa máy khách và điểm truy cập.
2. Xác định điểm truy cập mục tiêu: Sử dụng một công cụ như airodump-ng để liệt kê các mạng không dây khả dụng và xác định kênh và BSSID (địa chỉ MAC) của mạng mục tiêu.
3. Bắt tay bốn bước: Bắt đầu nắm bắt lưu lượng truy cập trên kênh mục tiêu và đợi máy khách kết nối với mạng. Khi một máy khách kết nối với mạng, điểm truy cập sẽ gửi một cái bắt tay bốn bên có chứa thông tin cần thiết để bẻ khóa mật khẩu. Sử dụng một công cụ như airodump-ng hoặc tcpdump để ghi lại quá trình bắt tay.
4. Sử dụng một công cụ như aireplay-ng để hủy xác thực ứng dụng khách: Việc hủy cấp phép ứng dụng khách sẽ khiến ứng dụng kết nối lại với mạng, điều này sẽ tạo ra một quá trình bắt tay bốn chiều khác có thể bị bắt.
5. Sử dụng công cụ như aircrack-ng để bẻ khóa bắt tay: Sau khi bắt tay, hãy sử dụng aircrack-ng để bẻ khóa mật khẩu. Aircrack-ng sử dụng một cuộc tấn công vét cạn để đoán mật khẩu bằng cách thử các tổ hợp ký tự khác nhau cho đến khi tìm được mật khẩu chính xác. Sự thành công của phương pháp này phụ thuộc vào độ phức tạp của mật khẩu và tốc độ của máy tính được sử dụng để tấn công.

Bẻ khóa WPA/WPA2 ở chế độ Doanh nghiệp khó hơn bẻ khóa WPA/WPA2 ở chế độ Cá nhân (PSK) vì chế độ này sử dụng một phương thức xác thực khác. Trong chế độ Doanh nghiệp, người dùng được xác thực bằng máy chủ RADIUS, yêu cầu tên người dùng và mật khẩu, ngoài khóa chia sẻ trước (PSK) được sử dụng trong chế độ Cá nhân. Dưới đây là các bước chung liên quan đến việc bẻ khóa WPA/WPA2 ở chế độ Doanh nghiệp:

1. Xác định phương thức EAP: Bước đầu tiên trong việc bẻ khóa WPA/WPA2 ở chế độ Doanh nghiệp là xác định phương thức Giao thức xác thực mở rộng (EAP) được sử dụng để xác thực. Thông tin này có thể được lấy từ lưu lượng mạng bằng cách sử dụng công cụ chụp gói chẳng hạn như Wireshark.
2. Lấy địa chỉ máy chủ RADIUS: Bước tiếp theo là lấy địa chỉ IP của máy chủ RADIUS được sử dụng để xác thực. Điều này cũng có thể thu được từ lưu lượng mạng bằng Wireshark.
3. Tạo một máy chủ RADIUS giả: Khi bạn đã xác định được địa chỉ máy chủ RADIUS, bạn có thể tạo một máy chủ RADIUS giả sẽ chặn và ghi nhật ký các yêu cầu xác thực. Để tạo máy chủ RADIUS giả, bạn có thể sử dụng các công cụ như FreeRADIUS-WPE, đây là phiên bản sửa đổi của máy chủ FreeRADIUS có thể được sử dụng cho mục đích kiểm tra và kiểm tra bảo mật.
4. Tạo danh sách từ: Bước tiếp theo là tạo danh sách từ sẽ được sử dụng để bẻ khóa kết hợp tên người dùng và mật khẩu được sử dụng để xác thực. Điều này có thể được thực hiện bằng cách sử dụng các công cụ như Crunch hoặc CeWL, có thể tạo danh sách từ dựa trên từ khóa hoặc nội dung trang web.
5. Khởi động cuộc tấn công: Khi bạn đã thiết lập một danh sách từ và máy chủ RADIUS giả mạo, bạn có thể khởi động cuộc tấn công. Điều này liên quan đến việc gửi yêu cầu xác thực đến thiết bị nạn nhân và thu thập phản hồi bằng máy chủ RADIUS giả mạo. Sau đó, dữ liệu bị bắt có thể được sử dụng để cố gắng bẻ khóa mật khẩu bằng một công cụ như John the Ripper hoặc Hashcat.

Lọc MAC là một tính năng bảo mật được sử dụng trong các mạng không dây để hạn chế truy cập mạng bằng cách cho phép hoặc từ chối các thiết bị dựa trên địa chỉ MAC của chúng. Để kiểm tra lọc MAC, hãy làm theo các bước sau:

1. Xác định địa chỉ MAC của thiết bị: Bạn có thể thực hiện việc này bằng cách sử dụng lệnh "ipconfig /all" trên Windows hoặc "ifconfig" trên Linux hoặc macOS.
2. Truy cập cài đặt bộ định tuyến không dây: Nhập địa chỉ IP của bộ định tuyến vào trình duyệt web của bạn và đăng nhập bằng thông tin xác thực quản trị viên của bộ định tuyến.
3. Điều hướng đến cài đặt lọc MAC: Tùy thuộc vào bộ định tuyến, cài đặt này có thể nằm trong phần Không dây, Bảo mật hoặc Kiểm soát truy cập.
4. Kiểm tra cài đặt lọc MAC: Tìm các tùy chọn như "Lọc MAC", "Bộ lọc MAC không dây" hoặc "Kiểm soát truy cập". Nếu tính năng lọc MAC được bật, bạn có thể thấy danh sách các địa chỉ MAC được phép hoặc bị từ chối.
5. Xác định xem thiết bị của bạn có được phép hay không: Nếu địa chỉ MAC của bạn không được liệt kê hoặc được liệt kê là bị từ chối, bạn có thể bị lọc MAC.

Giả mạo MAC là một kỹ thuật được sử dụng để thay đổi địa chỉ Điều khiển truy cập phương tiện (MAC) của giao diện mạng. Điều này có thể hữu ích trong một số tình huống chẳng hạn như bỏ qua bộ lọc MAC hoặc để tiến hành một cuộc tấn công trung gian (MitM). Dưới đây là các bước để giả mạo địa chỉ MAC của bạn:

1. Xác định giao diện mạng: Trước tiên, bạn cần xác định giao diện mạng có địa chỉ MAC mà bạn muốn giả mạo. Bạn có thể sử dụng lệnh **ifconfig** trên Linux hoặc **ipconfig /all** trên Windows để xác định giao diện mạng.
2. Tắt giao diện mạng: Tiếp theo, bạn cần tắt giao diện mạng để thay đổi địa chỉ MAC. Bạn có thể dùng lệnh **ifconfig <interface> down** trên Linux hoặc **netsh interface set interface "<interface>" admin=disable** trên Windows để tắt giao diện.
3. Thay đổi địa chỉ MAC: Sau khi tắt giao diện, bạn có thể thay đổi địa chỉ MAC. Bạn có thể sử dụng lệnh **macchanger -m <new\_mac\_address> <interface>** trên Linux hoặc **getmac /v /fo list** trên Windows để thay đổi địa chỉ MAC.
4. Bật giao diện mạng: Sau khi thay đổi địa chỉ MAC, bạn cần bật lại giao diện mạng. Bạn có thể dùng lệnh **ifconfig <interface> up** trên Linux hoặc **netsh interface set interface "<interface>" admin=enable** trên Windows để bật giao diện.

Để tạo kết nối trực tiếp đến điểm truy cập không dây, bạn có thể làm theo các bước sau:

1. Xác định SSID và loại bảo mật của điểm truy cập không dây mà bạn muốn kết nối.
2. Đảm bảo rằng bộ điều hợp mạng không dây của bạn được bật và hoạt động bình thường.
3. Quét các mạng không dây khả dụng và tìm điểm truy cập bạn muốn kết nối.
4. Nếu điểm truy cập đang sử dụng bảo mật, bạn sẽ cần cung cấp thông tin đăng nhập phù hợp để kết nối. Điều này có thể bao gồm khóa bảo mật mạng hoặc tên người dùng và mật khẩu cho chế độ Doanh nghiệp WPA/WPA2.
5. Khi bạn đã kết nối thành công với điểm truy cập không dây, bạn sẽ có thể truy cập internet và các tài nguyên mạng khác.

Cần lưu ý rằng một số điểm truy cập không dây có thể có các biện pháp bảo mật bổ sung, chẳng hạn như lọc MAC hoặc cách ly máy khách, điều này có thể ngăn bạn kết nối trực tiếp. Trong những trường hợp như vậy, bạn có thể cần sử dụng các kỹ thuật bổ sung như giả mạo địa chỉ MAC hoặc giả mạo ARP để có quyền truy cập.

Công cụ kiểm tra thâm nhập không dây bổ sung: Kismet

Kismet là một hệ thống phát hiện mạng không dây, nghe trộm và phát hiện xâm nhập cho mạng LAN không dây 802.11. Nó là một công cụ nguồn mở được sử dụng rộng rãi để giám sát mạng không dây, đánh hơi gói tin và xử lý sự cố mạng.

Kismet có thể phát hiện các mạng không dây trong khu vực và hiển thị thông tin như SSID, địa chỉ MAC, kênh, loại mã hóa và cường độ tín hiệu. Nó cũng có thể chụp và giải mã các gói, đồng thời cung cấp phân tích thời gian thực về lưu lượng không dây.

Kismet hỗ trợ nhiều loại giao diện mạng không dây, bao gồm bộ điều hợp Wi-Fi, bộ điều hợp Bluetooth và một số thiết bị radio được xác định bằng phần mềm (SDR). Nó có thể chạy trên nhiều hệ điều hành khác nhau như Linux, macOS và Windows.

Ngoài chức năng cơ bản, Kismet cũng có thể được mở rộng bằng các plugin, cho phép người dùng thêm các tính năng và tùy chỉnh bổ sung vào công cụ. Một số plugin phổ biến cho Kismet bao gồm theo dõi GPS, lập bản đồ mạng và khả năng IDS/IPS không dây.

Kismet là một công cụ mạnh mẽ để phân tích mạng không dây và được sử dụng rộng rãi bởi các quản trị viên mạng, chuyên gia bảo mật và tin tặc cho các mục đích khác nhau như khắc phục sự cố mạng, kiểm tra thâm nhập và kiểm tra an ninh mạng.

Thử nghiệm thâm nhập RFID (Nhận dạng tần số vô tuyến) là quá trình đánh giá tính bảo mật của hệ thống RFID. Công nghệ RFID được sử dụng cho nhiều ứng dụng, bao gồm theo dõi hàng tồn kho, kiểm soát truy cập, hệ thống thanh toán, v.v. Tuy nhiên, nếu không được bảo mật đúng cách, các hệ thống RFID có thể dễ bị tấn công, chẳng hạn như nghe lén, chặn dữ liệu và truy cập trái phép.

Kiểm tra thâm nhập là một phương pháp đánh giá tính bảo mật của hệ thống bằng cách mô phỏng một cuộc tấn công vào nó. Trong trường hợp hệ thống RFID, thử nghiệm thâm nhập thường liên quan đến việc cố gắng khai thác các lỗ hổng trong hệ thống để có quyền truy cập vào dữ liệu nhạy cảm hoặc các tài nguyên khác.

Thử nghiệm thâm nhập RFID có thể được thực hiện bởi một chuyên gia bảo mật lành nghề hoặc một nhóm chuyên gia quen thuộc với các công nghệ và giao thức được sử dụng bởi hệ thống RFID. Quá trình thử nghiệm thường bao gồm một số giai đoạn, bao gồm trinh sát, quét lỗ hổng, khai thác và báo cáo.

Trong giai đoạn trinh sát, người thử nghiệm sẽ thu thập thông tin về hệ thống RFID, chẳng hạn như các thành phần, giao thức và các vectơ tấn công tiềm năng của nó. Thông tin này sẽ được sử dụng để xác định các lỗ hổng trong hệ thống.

Giai đoạn quét lỗ hổng liên quan đến việc sử dụng các công cụ tự động để quét hệ thống RFID để tìm các lỗ hổng đã biết, chẳng hạn như mật khẩu mặc định, kênh liên lạc không an toàn và mã hóa yếu.

Khi các lỗ hổng đã được xác định, giai đoạn khai thác liên quan đến việc cố gắng khai thác chúng để có quyền truy cập vào dữ liệu nhạy cảm hoặc các tài nguyên khác. Điều này có thể liên quan đến việc sử dụng các công cụ phần cứng hoặc phần mềm chuyên dụng để chặn và giải mã tín hiệu RFID hoặc cố gắng vượt qua các cơ chế bảo mật và kiểm soát truy cập.

Cuối cùng, kết quả của thử nghiệm thâm nhập được ghi lại trong một báo cáo, thường bao gồm phân tích chi tiết về các lỗ hổng được tìm thấy, cùng với các đề xuất khắc phục.

Nhìn chung, thử nghiệm thâm nhập RFID là một công cụ quan trọng để đảm bảo tính bảo mật của hệ thống RFID và bảo vệ chống lại các cuộc tấn công tiềm tàng. Bằng cách xác định và giải quyết các lỗ hổng, các tổ chức có thể giúp ngăn chặn truy cập trái phép vào dữ liệu nhạy cảm và đảm bảo chức năng liên tục cũng như độ tin cậy của hệ thống RFID của họ.

Kỹ thuật đảo ngược Công nghệ RFID (Nhận dạng qua tần số vô tuyến) liên quan đến việc kiểm tra hệ thống RFID hiện có để hiểu cách thức hoạt động, cách thức thiết kế và cách thức sửa đổi hoặc cải thiện hệ thống. Mục đích của kỹ thuật đảo ngược RFID là thu thập kiến thức về hoạt động bên trong của hệ thống, có thể giúp các nhà phát triển, chuyên gia bảo mật và nhà nghiên cứu nâng cao hiệu suất của hệ thống RFID hoặc xác định các lỗ hổng hoặc điểm yếu tiềm ẩn.

RFID là công nghệ không dây sử dụng sóng vô tuyến để giao tiếp giữa thẻ (còn được gọi là bộ phát đáp) và đầu đọc (còn được gọi là bộ thẩm vấn). Thẻ RFID chứa một vi mạch lưu trữ thông tin và một ăng-ten gửi và nhận dữ liệu bằng sóng vô tuyến. Đầu đọc phát ra sóng vô tuyến mà ăng-ten trên thẻ nhận được và vi mạch trong thẻ sử dụng năng lượng từ sóng vô tuyến để cấp nguồn và truyền dữ liệu được lưu trữ của nó trở lại đầu đọc.

Kỹ thuật đảo ngược RFID có thể liên quan đến một loạt các hoạt động, bao gồm phân tích các thành phần phần cứng và phần mềm của hệ thống RFID, chặn và phân tích tín hiệu vô tuyến được truyền giữa thẻ và đầu đọc, đồng thời kiểm tra tính bảo mật và quyền riêng tư của hệ thống. Nó có thể được sử dụng để đánh giá hiệu suất và tính bảo mật của các hệ thống RFID hiện có hoặc để phát triển các hệ thống mới và cải tiến.

Một số lợi ích tiềm năng của kỹ thuật đảo ngược RFID bao gồm:

* Xác định các lỗ hổng trong hệ thống RFID có thể bị kẻ tấn công khai thác
* Phát triển các hệ thống RFID mới và cải tiến hiệu quả hơn, an toàn hơn hoặc bảo vệ quyền riêng tư
* Giúp chuẩn hóa công nghệ RFID và đảm bảo khả năng tương tác giữa các hệ thống khác nhau
* Cải thiện hiệu suất của hệ thống RFID trong môi trường đầy thách thức

Tấn công phân tích năng lượng là một loại tấn công kênh bên nhằm vào mức tiêu thụ năng lượng của thiết bị điện tử để trích xuất thông tin bí mật, chẳng hạn như khóa mật mã hoặc dữ liệu nhạy cảm khác. Kiểu tấn công này cũng có thể được áp dụng cho các hệ thống RFID để trích xuất thông tin từ các thẻ RFID.

Thực hiện một cuộc tấn công phân tích năng lượng trên một hệ thống RFID liên quan đến việc đo mức tiêu thụ năng lượng của thẻ RFID trong khi nó đang được đầu đọc sử dụng. Mục tiêu là để tương quan các biến thể trong mức tiêu thụ điện năng với dữ liệu được truyền đi, điều này có thể tiết lộ thông tin bí mật được lưu trữ trên thẻ.

Dưới đây là một số bước chung có thể được thực hiện để thực hiện một cuộc tấn công phân tích sức mạnh trên hệ thống RFID:

1. Thiết lập thiết bị: Để thực hiện tấn công phân tích công suất trên hệ thống RFID, bạn sẽ cần thiết bị chuyên dụng như máy hiện sóng, máy phân tích công suất và đầu dò. Bạn cũng sẽ cần quyền truy cập vào hệ thống RFID mà bạn muốn phân tích.
2. Ghi lại dấu vết năng lượng: Sử dụng máy hiện sóng để ghi lại dấu vết năng lượng của thẻ RFID trong khi nó đang được đầu đọc sử dụng. Điều này sẽ cung cấp cho bạn một bản ghi về mức tiêu thụ năng lượng của thẻ theo thời gian.
3. Phân tích dấu vết nguồn điện: Sử dụng bộ phân tích nguồn điện để phân tích dấu vết nguồn điện và xác định bất kỳ biến thể nào trong mức tiêu thụ điện năng tương ứng với dữ liệu được thẻ truyền đi. Đây có thể là một quá trình tốn nhiều thời gian, đòi hỏi phải phân tích cẩn thận và tương quan giữa dấu vết năng lượng với dữ liệu được truyền đi.
4. Trích xuất thông tin bí mật: Khi bạn đã xác định được các biến thể trong mức tiêu thụ năng lượng tương ứng với thông tin bí mật được lưu trữ trên thẻ, bạn có thể sử dụng thông tin này để trích xuất khóa hoặc dữ liệu nhạy cảm khác khỏi thẻ.

Nghe lén là hành động bí mật lắng nghe cuộc trò chuyện hoặc liên lạc giữa hai hoặc nhiều người. Nghe lén có thể được sử dụng cho nhiều mục đích khác nhau, từ giám sát và gián điệp cho đến sự tò mò hoặc giải trí cá nhân. Tuy nhiên, nó thường được coi là phi đạo đức và trong nhiều trường hợp là bất hợp pháp.

Dưới đây là một số bước để thực hiện nghe lén trên RFID:

1. Mua đầu đọc và ăng-ten RFID: Bạn sẽ cần một đầu đọc và ăng-ten RFID chuyên dụng để nhận tín hiệu RFID. Có một số sản phẩm thương mại có sẵn hoặc bạn có thể tự tạo một đài phát thanh do phần mềm xác định.
2. Xác định tần số: Xác định tần số của hệ thống RFID mà bạn muốn nghe trộm. RFID hoạt động trên các tần số khác nhau, tùy thuộc vào ứng dụng. Ví dụ: tần số cho chip RFID thẻ tín dụng thường là 13,56 MHz.
3. Đặt ăng-ten: Đặt ăng-ten gần khu vực mà bạn muốn truyền thông tin RFID, chẳng hạn như quầy thanh toán, điểm kiểm soát truy cập hoặc lối vào nhà kho.
4. Thu thập dữ liệu: Bắt đầu thu thập dữ liệu bằng cách lắng nghe tín hiệu RFID. Sử dụng đầu đọc RFID để thu thập và phân tích dữ liệu. Bạn có thể nắm bắt nhiều loại thông tin, chẳng hạn như ID thẻ, thời gian giao dịch và bất kỳ dữ liệu bổ sung nào được truyền đi.
5. Phân tích dữ liệu: Khi bạn đã thu được các tín hiệu RFID, bạn có thể phân tích dữ liệu để hiểu cách thức hoạt động của hệ thống và thông tin nào đang được truyền đi. Điều này có thể giúp xác định các lỗ hổng và các vectơ tấn công tiềm năng.

Thực hiện một cuộc tấn công trung gian (MITM) vào hệ thống RFID (Nhận dạng qua tần số vô tuyến) có thể là một thách thức, nhưng có thể thực hiện được nếu đáp ứng một số điều kiện nhất định. Trước khi thực hiện một cuộc tấn công MITM, điều quan trọng là phải hiểu những điều cơ bản về cách thức hoạt động của hệ thống RFID.

Hệ thống RFID bao gồm đầu đọc (hoặc bộ dò tín hiệu) và thẻ (hoặc bộ phát đáp). Đầu đọc phát ra một trường điện từ cung cấp năng lượng cho thẻ và thẻ phản hồi bằng cách truyền dữ liệu của nó trở lại đầu đọc. Tùy thuộc vào loại hệ thống RFID, giao tiếp giữa đầu đọc và thẻ có thể được mã hóa, khiến việc chặn và thao tác trở nên khó khăn hơn.

Để thực hiện một cuộc tấn công MITM vào hệ thống RFID, bạn cần chặn và điều khiển giao tiếp giữa đầu đọc và thẻ. Điều này có thể đạt được bằng cách đặt một trình đọc giả mạo (hoặc "giả mạo" trình đọc) giữa trình đọc hợp pháp và thẻ và chuyển tiếp giao tiếp giữa chúng. Trình đọc giả mạo sau đó có thể nắm bắt và sửa đổi dữ liệu được truyền bởi thẻ trước khi chuyển tiếp nó tới trình đọc hợp pháp và ngược lại.

Dưới đây là các bước chung để thực hiện một cuộc tấn công MITM RFID:

1. Xác định loại hệ thống RFID đang sử dụng và băng tần của nó.
2. Có được hoặc xây dựng một trình đọc giả mạo có thể hoạt động trên cùng một dải tần số và bắt chước hành vi của trình đọc hợp pháp.
3. Đặt đầu đọc giả mạo giữa đầu đọc hợp pháp và thẻ, bằng cách đặt nó gần đầu đọc và thẻ hoặc bằng cách chặn giao tiếp không dây.
4. Nắm bắt dữ liệu do thẻ truyền tới đầu đọc hợp pháp và sửa đổi dữ liệu đó khi cần thiết.
5. Chuyển tiếp dữ liệu đã sửa đổi tới đầu đọc hợp pháp và lặp lại quy trình đối với dữ liệu được truyền bởi đầu đọc hợp pháp tới thẻ.
6. Theo dõi thông tin liên lạc và trích xuất bất kỳ thông tin nhạy cảm nào có thể đã được truyền đi.

Tấn công từ chối dịch vụ (DoS) là một loại tấn công mạng trong đó kẻ tấn công cố gắng phá vỡ hoạt động bình thường của hệ thống hoặc mạng được nhắm mục tiêu bằng cách áp đảo hệ thống đó bằng một lượng lớn lưu lượng truy cập hoặc yêu cầu. Một cuộc tấn công DoS có thể được sử dụng để vô hiệu hóa một trang web, làm sập máy chủ hoặc làm cho một dịch vụ không khả dụng.

Thực hiện một cuộc tấn công DoS thường bao gồm các bước sau:

1. Xác định mục tiêu: Bước đầu tiên trong một cuộc tấn công DoS là xác định hệ thống hoặc mạng mà bạn muốn phá vỡ. Đây có thể là một trang web, một máy chủ hoặc toàn bộ mạng.
2. Chọn phương pháp tấn công: Có nhiều phương pháp khác nhau có thể được sử dụng để khởi động một cuộc tấn công DoS, bao gồm làm tràn ngập mục tiêu bằng lưu lượng truy cập mạng, áp đảo mục tiêu bằng các yêu cầu hoặc khai thác các lỗ hổng trong phần mềm hoặc phần cứng của mục tiêu.
3. Khởi động cuộc tấn công: Khi bạn đã chọn phương thức tấn công của mình, bạn có thể bắt đầu khởi động cuộc tấn công bằng cách gửi một loạt lưu lượng truy cập hoặc yêu cầu đến mục tiêu. Điều này có thể được thực hiện bằng cách sử dụng phần mềm chuyên dụng, chẳng hạn như công cụ kiểm tra mức độ căng thẳng của mạng hoặc bằng cách gửi một số lượng lớn yêu cầu đến mục tiêu theo cách thủ công.
4. Theo dõi kết quả: Khi cuộc tấn công diễn ra, bạn sẽ muốn theo dõi kết quả để xem mức độ hiệu quả của cuộc tấn công và điều chỉnh chiến lược của mình nếu cần. Điều này có thể liên quan đến việc theo dõi lưu lượng mạng hoặc yêu cầu, giám sát nhật ký hệ thống để tìm lỗi hoặc bất thường hoặc sử dụng các công cụ khác để đánh giá tác động của cuộc tấn công đối với mục tiêu.

Nhân bản hoặc giả mạo RFID (Nhận dạng tần số vô tuyến) là một loại tấn công mạng trong đó kẻ tấn công sao chép dữ liệu từ một thẻ RFID và sử dụng nó để tạo một thẻ mới có thể được sử dụng để mạo danh thẻ ban đầu. Điều này có thể được sử dụng để giành quyền truy cập trái phép vào một khu vực an toàn, đánh cắp thông tin nhạy cảm hoặc thực hiện hành vi gian lận.

Việc thực hiện sao chép hoặc giả mạo RFID thường bao gồm các bước sau:

1. Có được một đầu đọc: Bước đầu tiên trong quá trình nhân bản RFID là có được một đầu đọc RFID có khả năng đọc dữ liệu từ thẻ gốc. Có nhiều loại đầu đọc RFID có sẵn, từ thiết bị cầm tay đến các hệ thống phức tạp hơn.
2. Quét thẻ gốc: Khi bạn đã có đầu đọc RFID, bạn có thể sử dụng nó để quét thẻ gốc và lấy dữ liệu của nó. Dữ liệu này thường bao gồm mã định danh duy nhất và thông tin khác dành riêng cho thẻ và mục đích sử dụng của thẻ.
3. Ghi dữ liệu vào thẻ mới: Sau khi quét thẻ ban đầu, bạn có thể sử dụng đầu đọc RFID để ghi dữ liệu vào thẻ mới có thể được sử dụng để mạo danh thẻ ban đầu. Điều này có thể được thực hiện bằng phần mềm chuyên dụng, phần mềm này cho phép bạn ghi dữ liệu vào thẻ mới và định cấu hình để thẻ hoạt động giống như thẻ ban đầu.
4. Sử dụng thẻ mới: Khi bạn đã tạo thẻ mới, bạn có thể sử dụng thẻ đó để có quyền truy cập vào khu vực an toàn hoặc thực hiện các hành động khác thường yêu cầu sử dụng thẻ ban đầu. Điều này có thể được thực hiện bằng cách trình bày thẻ mới cho đầu đọc RFID, đầu đọc này sẽ đọc dữ liệu từ thẻ và cho phép bạn thực hiện hành động mong muốn.

Tấn công phát lại RFID (Nhận dạng tần số vô tuyến) là một loại tấn công mạng trong đó kẻ tấn công ghi lại giao tiếp giữa thẻ RFID và đầu đọc và sau đó phát lại giao tiếp tương tự để mạo danh thẻ. Điều này có thể được sử dụng để giành quyền truy cập trái phép vào một khu vực an toàn, đánh cắp thông tin nhạy cảm hoặc thực hiện hành vi gian lận.

Thực hiện một cuộc tấn công phát lại RFID thường bao gồm các bước sau:

1. Có được đầu đọc: Bước đầu tiên trong một cuộc tấn công phát lại RFID là có được đầu đọc RFID có khả năng đọc giao tiếp giữa thẻ RFID và đầu đọc. Có nhiều loại đầu đọc RFID có sẵn, từ thiết bị cầm tay đến các hệ thống phức tạp hơn.
2. Ghi lại giao tiếp: Khi bạn đã nhận được đầu đọc RFID, bạn có thể sử dụng nó để ghi lại giao tiếp giữa thẻ RFID và đầu đọc. Điều này có thể được thực hiện bằng phần mềm chuyên dụng, cho phép bạn chụp và lưu trữ dữ liệu được truyền giữa thẻ và đầu đọc.
3. Phát lại giao tiếp: Sau khi ghi lại giao tiếp, bạn có thể sử dụng đầu đọc RFID để phát lại cùng một dữ liệu cho đầu đọc để giả mạo thẻ RFID. Điều này có thể được thực hiện bằng cách sử dụng cùng một phần mềm được sử dụng để ghi lại giao tiếp, phần mềm này có thể phát lại dữ liệu cho đầu đọc như thể nó đến từ thẻ gốc.
4. Sử dụng thẻ mạo danh: Khi bạn đã phát lại thành công giao tiếp, bạn có thể sử dụng thẻ mạo danh để có quyền truy cập vào khu vực an toàn hoặc thực hiện các hành động khác thường yêu cầu sử dụng thẻ gốc. Điều này có thể được thực hiện bằng cách trình bày thẻ mạo danh tới đầu đọc RFID, đầu đọc này sẽ đọc dữ liệu từ thẻ và cho phép bạn thực hiện hành động mong muốn.

Tấn công phát lại RFID là một loại tấn công bảo mật liên quan đến việc bắt tín hiệu RFID và sau đó phát lại tín hiệu đó để giành quyền truy cập vào các khu vực, dữ liệu hoặc thông tin bị hạn chế. Trong kiểu tấn công này, kẻ tấn công chặn tín hiệu nhận dạng tần số vô tuyến (RFID) từ thiết bị hỗ trợ RFID bằng máy quét tần số vô tuyến (RF). Sau khi bắt được tín hiệu, kẻ tấn công có thể truyền lại tín hiệu đó để giành quyền truy cập vào hệ thống, thông tin hoặc dữ liệu.

Cuộc tấn công có thể xảy ra vì hầu hết các hệ thống RFID không được mã hóa và không có tính năng bảo mật. Kẻ tấn công cần có kiến thức về giao thức và tín hiệu RFID để thực hiện cuộc tấn công. Kẻ tấn công có thể sử dụng tín hiệu RFID từ người dùng hợp pháp để giành quyền truy cập vào các khu vực hoặc dữ liệu bị hạn chế. Tín hiệu phát lại được hệ thống coi là hợp lệ vì nó giống với tín hiệu ban đầu.

Để ngăn chặn các cuộc tấn công phát lại RFID, hệ thống nên sử dụng mã hóa và triển khai các tính năng bảo mật như xác thực và ủy quyền. Ngoài ra, sử dụng tín hiệu gây nhiễu cũng có thể giúp ngăn chặn kiểu tấn công này.

Máy hiện sóng, Anten RFID và Đầu đọc RFID

1. Máy hiện sóng: Máy hiện sóng là một loại dụng cụ kiểm tra điện tử được sử dụng để đo và hiển thị tín hiệu điện áp và dạng sóng. Nó hiển thị tín hiệu dưới dạng biểu đồ, với thời gian trên trục X và điện áp trên trục Y. Nó thường được sử dụng trong các lĩnh vực điện tử, viễn thông và kỹ thuật để chẩn đoán và khắc phục sự cố với các mạch điện tử.
2. Ăng-ten RFID: Ăng-ten RFID là một thiết bị được sử dụng để truyền và nhận tín hiệu vô tuyến để liên lạc với các thẻ RFID. Nó thường được sử dụng trong các hệ thống RFID để cho phép trao đổi dữ liệu giữa thẻ và đầu đọc. Anten RFID có nhiều kích cỡ và hình dạng khác nhau, tùy thuộc vào ứng dụng cụ thể và tần suất của hệ thống RFID.
3. Đầu đọc RFID: Đầu đọc RFID là một thiết bị được sử dụng để giao tiếp với các thẻ RFID bằng cách truyền và nhận tín hiệu vô tuyến. Nó thường được sử dụng trong các hệ thống RFID để đọc và ghi dữ liệu vào thẻ, cũng như để kiểm soát hành vi của thẻ. Đầu đọc RFID có nhiều loại và cấu hình khác nhau, tùy thuộc vào ứng dụng cụ thể và tần suất của hệ thống RFID. Một số đầu đọc cầm tay, trong khi những đầu đọc khác cố định và được tích hợp vào máy móc hoặc thiết bị.

Tóm lại, máy hiện sóng được sử dụng để đo và hiển thị tín hiệu điện áp và dạng sóng, trong khi ăng-ten và đầu đọc RFID được sử dụng trong các hệ thống RFID để liên lạc và kiểm soát các thẻ RFID.

Thử nghiệm thâm nhập NFC (Giao tiếp trường gần) là một quá trình đánh giá tính bảo mật của các thiết bị và hệ thống hỗ trợ NFC bằng cách mô phỏng các cuộc tấn công và lỗ hổng trong thế giới thực. NFC là công nghệ giao tiếp không dây tầm ngắn cho phép hai thiết bị trao đổi dữ liệu khi chúng được đặt gần nhau. NFC thường được sử dụng cho thanh toán di động, hệ thống kiểm soát truy cập và các ứng dụng khác yêu cầu liên lạc an toàn giữa các thiết bị.

Thực hiện kiểm tra thâm nhập NFC thường bao gồm các bước sau:

1. Trinh sát: Điều này liên quan đến việc thu thập thông tin về các thiết bị và hệ thống hỗ trợ NFC đang được nhắm mục tiêu cho thử nghiệm thâm nhập. Điều này có thể bao gồm việc xác định các loại thiết bị và hệ thống, phiên bản phần mềm của chúng và loại thẻ NFC hoặc thẻ mà chúng hỗ trợ.
2. Đánh giá lỗ hổng bảo mật: Điều này liên quan đến việc kiểm tra các thiết bị và hệ thống hỗ trợ NFC để tìm lỗ hổng bảo mật mà kẻ tấn công có thể khai thác. Điều này có thể bao gồm quét các cổng mở, kiểm tra mật khẩu mặc định và kiểm tra mã hóa yếu.
3. Khai thác: Khi các lỗ hổng đã được xác định, bước tiếp theo là cố gắng khai thác chúng để giành quyền truy cập trái phép hoặc thực hiện các hành động độc hại khác. Điều này có thể bao gồm giả mạo thẻ hoặc thẻ NFC, thực hiện các cuộc tấn công trung gian hoặc đánh cắp dữ liệu nhạy cảm.
4. Báo cáo: Cuối cùng, một báo cáo được tạo để tóm tắt các phát hiện của thử nghiệm thâm nhập và đưa ra các khuyến nghị để khắc phục. Báo cáo phải xác định bất kỳ lỗ hổng nào đã được phát hiện, giải thích tác động tiềm ẩn của những lỗ hổng này và cung cấp hướng dẫn về cách giải quyết chúng.

Nghe trộm NFC (Giao tiếp trường gần) là một kiểu tấn công cho phép kẻ tấn công nghe trộm giao tiếp NFC giữa hai thiết bị. Kiểu tấn công này thường được sử dụng để chặn dữ liệu nhạy cảm, chẳng hạn như thông tin thẻ tín dụng, chi tiết liên hệ hoặc mật khẩu.

Nghe lén NFC được thực hiện bằng cách đặt một thiết bị NFC giả mạo giữa hai thiết bị hợp pháp đang giao tiếp với nhau. Thiết bị lừa đảo hoạt động như một "người trung gian", chặn liên lạc và đánh cắp mọi dữ liệu nhạy cảm đang được truyền đi.

Để thực hiện một cuộc tấn công nghe lén NFC, kẻ tấn công thường cần có quyền truy cập vật lý vào các thiết bị hỗ trợ NFC đang được nhắm mục tiêu. Khi đã có thiết bị giả mạo, kẻ tấn công có thể sử dụng phần mềm chuyên dụng để chặn và phân tích giao tiếp giữa hai thiết bị.

Để ngăn nghe lén NFC, điều quan trọng là phải giữ an toàn cho các thiết bị hỗ trợ NFC của bạn và chỉ sử dụng các đầu đọc NFC an toàn, đáng tin cậy cũng như các thiết bị khác. Tránh sử dụng NFC ở những nơi công cộng hoặc ở những khu vực có nguy cơ bị chặn cao, chẳng hạn như khu vực đông đúc hoặc gần những kẻ tấn công tiềm tàng. Ngoài ra, điều quan trọng là luôn cập nhật các thiết bị NFC của bạn với các bản vá và cập nhật bảo mật mới nhất để giúp bảo vệ khỏi các mối đe dọa mới và đang nổi lên.

Thực hiện một cuộc tấn công sửa đổi dữ liệu trên NFC (Giao tiếp trường gần) liên quan đến việc thao túng dữ liệu được truyền giữa hai thiết bị hỗ trợ NFC. Kiểu tấn công này có thể được sử dụng để sửa đổi thông tin nhạy cảm, chẳng hạn như chi tiết tài khoản ngân hàng, mật khẩu và dữ liệu cá nhân khác.

Để thực hiện một cuộc tấn công sửa đổi dữ liệu trên NFC, kẻ tấn công thường cần phải ở gần thiết bị mục tiêu. Cuộc tấn công có thể được thực hiện bằng cách sử dụng thiết bị giả mạo hỗ trợ NFC hoặc bằng cách chặn và sửa đổi dữ liệu được truyền giữa hai thiết bị hợp pháp.

Một phương pháp thực hiện tấn công sửa đổi dữ liệu NFC là sử dụng phần mềm chuyên dụng để chặn và sửa đổi dữ liệu được truyền giữa hai thiết bị. Điều này có thể được thực hiện bằng cách chặn liên lạc giữa hai thiết bị và sửa đổi các gói dữ liệu đang truyền. Sau đó, dữ liệu đã sửa đổi có thể được gửi đến thiết bị đích, có khả năng dẫn đến việc truyền dữ liệu nhạy cảm cho kẻ tấn công.

Để ngăn chặn các cuộc tấn công sửa đổi dữ liệu trên NFC, điều quan trọng là phải sử dụng các thiết bị hỗ trợ NFC an toàn, đáng tin cậy và chỉ sử dụng NFC trong môi trường an toàn. Bạn cũng nên cập nhật các thiết bị hỗ trợ NFC của mình với các bản vá và cập nhật bảo mật mới nhất để giúp bảo vệ khỏi các mối đe dọa mới và đang nổi lên. Ngoài ra, hãy cảnh giác với mọi dấu hiệu hoạt động đáng ngờ, chẳng hạn như các yêu cầu bất thường về thông tin cá nhân hoặc hành vi bất thường trên thiết bị hỗ trợ NFC của bạn.

Lỗi dữ liệu trong NFC (Giao tiếp trường gần) xảy ra khi kẻ tấn công cố ý hoặc vô ý sửa đổi dữ liệu được truyền giữa hai thiết bị hỗ trợ NFC. Kiểu tấn công này có thể dẫn đến mất mát, thay đổi hoặc thao túng dữ liệu được truyền qua NFC.

Các cuộc tấn công làm hỏng dữ liệu trên NFC có thể được thực hiện theo một số cách, bao gồm thông qua việc sử dụng trình đọc NFC giả mạo hoặc bằng cách khai thác các lỗ hổng trong giao thức NFC. Trong một số trường hợp, kẻ tấn công có thể làm hỏng dữ liệu chỉ bằng cách làm gián đoạn tín hiệu giao tiếp NFC, gây ra lỗi trong quá trình truyền dữ liệu.

Hậu quả của việc hỏng dữ liệu trong NFC có thể rất nghiêm trọng. Ví dụ: nếu kẻ tấn công làm hỏng dữ liệu trong một giao dịch thanh toán NFC, thì giao dịch đó có thể không thành công hoặc số tiền thanh toán có thể bị thay đổi. Tương tự, nếu kẻ tấn công làm hỏng dữ liệu trong quá trình truyền tệp NFC, thì tệp có thể bị mất hoặc bị hỏng, dẫn đến mất hoặc hỏng dữ liệu.

Để bảo vệ chống lại các cuộc tấn công làm hỏng dữ liệu trong NFC, điều quan trọng là phải sử dụng các thiết bị NFC an toàn, đáng tin cậy và chỉ sử dụng NFC trong các môi trường an toàn, được kiểm soát. Ngoài ra, điều quan trọng là luôn cập nhật các thiết bị hỗ trợ NFC của bạn với các bản vá và cập nhật bảo mật mới nhất để giúp bảo vệ chống lại các mối đe dọa mới và đang nổi lên. Bạn cũng nên thường xuyên kiểm tra các thay đổi trái phép đối với dữ liệu hoặc theo dõi các dấu hiệu làm hỏng dữ liệu để giúp phát hiện và giảm thiểu bất kỳ cuộc tấn công nào có thể xảy ra.

Tấn công MITM (Man-In-The-Middle) là một kiểu tấn công trong đó kẻ tấn công chặn liên lạc giữa hai thiết bị hỗ trợ NFC. Trong một cuộc tấn công NFC MITM, kẻ tấn công đặt một thiết bị NFC giả mạo giữa hai thiết bị hợp pháp và có thể theo dõi, sửa đổi hoặc thao túng thông tin liên lạc được trao đổi giữa chúng.

Kẻ tấn công có thể thực hiện nhiều hoạt động độc hại khác nhau như đánh cắp dữ liệu nhạy cảm, thay đổi hoặc sửa đổi dữ liệu được truyền, đưa vào các lệnh giả mạo hoặc chuyển hướng giao tiếp đến thiết bị của chính chúng.

Có nhiều kỹ thuật khác nhau mà kẻ tấn công có thể sử dụng để thực hiện tấn công NFC MITM, chẳng hạn như NFC Relay, NFC Spoofing, NFC Emulation và NFC Eavesdropping. Những kẻ tấn công có thể sử dụng các công cụ phần cứng và phần mềm được thiết kế đặc biệt để thực hiện các cuộc tấn công này.

Để ngăn chặn các cuộc tấn công MITM vào NFC, điều quan trọng là phải giữ an toàn cho các thiết bị hỗ trợ NFC của bạn và chỉ sử dụng các đầu đọc NFC đáng tin cậy và an toàn cũng như các thiết bị khác. Việc cập nhật các bản vá và cập nhật bảo mật mới nhất cho các thiết bị NFC của bạn cũng rất cần thiết để bảo vệ khỏi các mối đe dọa mới và đang nổi lên.

Một cách hiệu quả khác để bảo vệ chống lại các cuộc tấn công MITM là sử dụng mã hóa, chữ ký số và các giao thức bảo mật khác trong giao tiếp NFC. Bằng cách triển khai các biện pháp bảo mật này, khả năng kẻ tấn công thực hiện thành công cuộc tấn công MITM vào NFC có thể giảm đáng kể.