

I. GIỚI THIỆU TỔNG QUAN

1. TỔNG QUAN VỀ BẢO MẬT MẠNG:

1.1. Giới thiệu về bảo mật:

Hiện nay, vấn đề bảo mật và an toàn thông tin đã và đang được áp dụng phổ biến ở khắp mọi nơi. Vì thế đây là một lĩnh vực được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo sự an toàn cho các hệ thống thông tin. Tuy nhiên không có một hệ thống thông tin nào được bảo mật hoàn toàn, bất kỳ hệ thống nào cũng có những lỗ hổng về bảo mật an toàn mà chưa được phát hiện.

Vấn đề về an toàn và bảo mật thông tin phải đảm bảo các yếu tố sau:

* Tính bảo mật: chỉ cho phép những người có quyền hạn được truy cập đến nó.
* Tính toàn vẹn: dữ liệu không bị sửa đổi, bị xóa một cách bất hợp pháp.
* Tính sẵn sàng: bất cứ khi nào chúng ta cần thì dữ liệu luôn sẵn sàng.

1.2. Sự kiện bảo mật năm 2014

1.2.1. Heartbleed (Trái tim rỉ máu):

Heartbleed, phát hiện trong tháng 4, là lỗ hổng bảo mật đầu tiên trong hai lỗ hổng nghiêm trọng làm chấn động thế giới Internet năm qua. Heartbleed cho phép kẻ tấn công đột nhập vào các máy chủ có tính năng “the heartbeat extension” trong thư viện OpenSSL được kích hoạt, lấy đi những dữ liệu nhạy cảm như thông tin thẻ tín dụng, tài khoản ngân hàng và các giao dịch trực tuyến khác của người dùng được bảo mật bằng mã hóa SSL. Heartbleed buộc hàng triệu người dùng phải đổi mật khẩu trên nhiều website. Mặc dù Heartbleed có thể được bịt lại nhanh chóng bằng một bản vá phần mềm, nhưng các chuyên gia bảo mật cho rằng Heartbleed sẽ vẫn còn tồn tại trong nhiều năm tới. Nguy cơ lớn nhất nằm ở chỗ nhiều chủ website nhỏ chưa quan tam tới việc cập nhật phần mềm cho máy chủ của họ.

1.2.2. Shellshock

Chỉ vài tháng sau khi “Trái tim rỉ máu” được hàn gắn, cả thế giới lại hoảng lên với một lỗ hổng bảo mật nghiêm trọng khác mang tên Shellshock. Shellshock là tên của một loạt các lỗ hổng bảo mật ảnh hưởng trên Unix Bash shell. Rất nhiều dịch vụ Internet sử dụng Bash để xử lí các yêu cầu cụ thể, đồng nghĩa với việc tin tặc có thể thực thi lệnh tùy ý và đoạt quyền truy cập vào hệ thống. Lỗ hổng đẩu tiên (CVE-2014-6271) được phát hiện vào tháng chín, và sau đó là hàng loạt các lỗ hổng CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE2014-7186, CVE-2014-7187.

1.2.3. Mã độc mã hoá dữ liệu & tống tiền

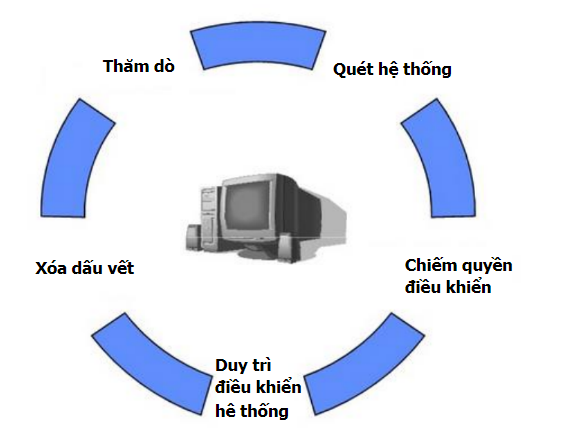
Trong thời gian vừa qua hàng loạt điện thoại thông minh, máy tính tại Việt Nam bị nhiễm một loại mã độc tống tiền. Loại mã độc này tìm cách xâm nhập vào thiết bị của người dùng và mã hoá dữ liệu trên đó, sau đó buộc nạn nhân phải nộp tiền chuộc để nhận lại dữ liệu đã bị mã hoá. Dữ liệu đã bị mã hoá không thể khôi phục lại vì hacker đã dùng các thuật toán bí mật để mã hoá, công cụ giải mã lại lưu trữ tại máy chủ do hacker quản lý.

Loại mã độc này thuộc dòng Ransomware (một loại mã độc khoá dữ liệu tống tiền người dùng) mang tên Critroni hay còn gọi là CTB Locker (Curve-Tor-Bitcoin Locker) xuất hiện từ tháng 7-2014.

1.2.4. Sony Pictures bị hack

Cuối tháng 11, một nhóm hacker tự xưng là Guardians of Peace (GOP) – “Những người bảo vệ hòa bình”, tấn công mạng làm tê liệt toàn bộ máy tính của nhân viên tại hãng phim Sony Pictures. Nhóm này còn lấy được một lượng lớn thông tin nhạy cảm, theo tường thuật dung lượng dữ liệu đánh cắp lớn hơn 100 terabyte, bao gồm nhiều kịch bản phim, một số phim chưa phát hành, hợp đồng của hãng với nhiều ngôi sao, thông tin nhân viên, và nhiều tài liệu nội bộ. Vài tuần sau đó, GOP đã đưa ra yêu cầu Sony dừng phát hành bộ phim The Interview (Cuộc phỏng vấn) có nội dung nói về cuộc ám sát giả tưởng lãnh tụ Kim Jong-un của Triều Tiên, khiến người ta nghi ngờ Bình Nhưỡng hậu thuẫn cho cuộc tấn công tàn nhẫn này. Rốt cục Sony cũng đã quyết định hoãn phát hành bộ phim do lo ngại các rạp phim sẽ bị tấn công khủng bố theo như những lời đe dọa đã được hacker tung ra.

2. GIỚI THIỆU VỀ CÁC GIAI ĐOẠN TẤN CÔNG



2.1. Thăm dò

Thăm dò mục tiêu là một trong những bước quan trọng để biết những thông tin trên hệ thống mục tiêu. Hacker sử dụng kỹ thuật này để khám phá hệ thống mục tiêu đang chạy hệ điều hành nào, có bao nhiêu dịch vụ đang chạy, cổng dịch vụ nào đang mở, cổng nào đóng.

Gồm 2 loại:

Passive: thu thập thông tin chung như vị trí, điện thoại, email cá nhân, người điều hành trong tổ chức.

Active: thu thập thông tin về địa chỉ IP, domain, DNS, … của hệ thống.

2.2. Quét hệ thống

Quét thăm dò hệ thống là phương pháp quan trọng mà Attacker thường sử dụng để tìm hiểu hệ thống và thu thập các thông tin như: địa chỉ IP cụ thể, hệ điều hành, kiến trúc hệ thống.

Một số phương pháp quét thông dụng: quét cổng, quét mạng, quét các điểm yếu trên mạng.

2.3. Chiếm quyền điều khiển

Giai đoạn này Hacker bắt đầu xâm nhập được hệ thống, tấn công nó, và truy cập nó bằng các lệnh khai thác. Các lệnh khai thác nằm ở bất cứ đâu, từ mạng LAN tới Internet và lan rộng ra mạng không dây.

Hacker có thể chiếm quyền điều khiển tại:

 Mức hệ điều hành / mức ứng dụng

 Mức mạng

 Từ chối dịch vụ

2.4. Duy trì điều khiển hệ thống

Giai đoạn này hacker bắt đầu phá hỏng làm hại, cài trojan, rootkit, backdoor để lấy thông tin. Thường được sử dụng nhằm mục đích đánh cắp tài khoản tín dụng, dữ liệu quan trọng, thông tin cá nhân, …

2.5. Xóa dấu vết

Sau khi bị tấn công thì hệ thống sẽ lưu lại những dấu vết do hacker để lại. Hacker cần xoá chúng đi nhằm tránh bị phát hiện bằng các phương thức như: Steganography, tunneling và altering log file.

3. CÁC PHƯƠNG THỨC TẤN CÔNG MẠNG

3.1. Tấn công vào hệ điều hành

Thông thường việc cài đặt một hệ thống thường có một số lượng lớn các dịch vụ cùng chạy và các cổng kết nối. Điều này làm cho hacker có nhiều cơ hội tấn công hơn. Tìm kiếm một bản vá lỗi rất khó khăn trong một hệ thống mạng phức tạp như ngày nay. Hacker luôn nghiên cứu rất kỹ các hệ điều hành, tìm các lệnh khai thác lỗ hỏng để truy xuất, xâm nhập hệ thống.

3.2. Tấn công ở mức ứng dụng

Tấn công ở mức ứng dụng. Những kiểu tấn công phổ biến như: tấn công từ chối dịch vụ, tấn công SOL Injection, tấn công XSS, …

3.2.1. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ là một kiểu tấn công làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng.

3.2.2. Tấn công SQL Injection

SQL Injection là một kĩ thuật cho phép hacker thi hành các câu lệnh truy vấn SQL bất hợp pháp (người phát triển không lường trước được) bằng cách lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập từ các ứng dụng web. Hậu quả này rất tai hại vì nó cho phép kẻ tấn công có toàn quyền, hiệu chỉnh… trên cơ sở dữ liệu của ứng dụng. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị CSDL như SQL Server, Oracle, DB2, Sysbase.

3.2.3. Tấn công XSS

Cross-Site Scripting (XSS) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây nguy hại cho những người sử dụng. Những đoạn mã nguy hiểm này hầu hết được viết bằng các Client-Site Script như: JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML.

3.3. Tấn công vào lỗi cấu hình hệ thống

Tấn công dựa vào các lỗi cấu hình hệ thống như:

 Hệ thống cấu hình không chính xác, ít bảo mật.

 Hệ thống phức tạp nhưng người quản trị không có đủ kỹ năng để sửa các lỗi.

 Khi cấu hình hệ thống thường chọn Default để dễ làm, điều này có thể bị hacker khai thác.

4. TỔNG QUAN VỀ KALI LINUX

4.1. Giới thiệu

Kali Linux là phiên bản mới nhất của hệ điều hành Linux do Offensive Security phát hành. Không giống như những hệ điều hành Linux khác, Kali Linux thường được dùng để thử nghiệm xâm nhập hệ thống mạng. Đó là cách để đánh giá mức độ an toàn của một hệ thống máy tính hoặc mạng bằng cách mô phỏng một cuộc tấn công mạng.

Kali Linux một OS tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến.

4.2. Lịch sử phát triển

Kali phát triển trên nền tảng hệ điều hành Debian, tiền thân của Kali là hệ điều hành BackTrack xuất hiện năm 2006, và nó đã không ngừng cải tiến để đạt được vị trí nhất định trong cộng đồng bảo mật. Kali Linux đã được phát hành chính thức vào ngày 13 tháng ba năm 2013.

4.3. Đặc điểm

Kali Linux được cài đặt sẵn với hơn 600 công cụ để thử nghiệm thâm nhập hệ thống. Tính tương thích kiến trúc: Kali có khả năng tương thích với kiến trúc ARM. Chúng ta có thể xây dựng phiên bản Kali trên một Raspberry Pi hoặc trên Samsung Galaxy Note.

Hỗ trợ mạng không dây tốt hơn

Khả năng tùy biến cao: Kali rất linh hoạt khi đề cập đến giao diện hoặc khả năng tuỳ biến hệ thống.

Dễ dàng nâng cấp giữa các phiên bản: Kali đã dễ dàng hơn trong việc nâng cấp hệ thống khi phiên bản mới xuất hiện, và không cần phải cài đặt lại mới hoàn toàn.

II. TÌM HIỂU KIẾN THỨC

1. Giới thiệu về các công cụ trên Kali Linux

Kali được cài đặt hơn 600 công cụ tùy theo nhu cầu đánh giá và nó đã được sắp xếp, phân loại rõ ràng dựa trên mục đích sử dụng để người dùng có thể sử dụng những công cụ này một cách tối ưu nhất.

1.1.Thu thập thông tin - Information Gathering

Nhóm phân loại này gồm những công cụ tập trung vào việc thu thập thông tin về mục tiêu. Trong phân loại này có một số lượng lớn các công cụ được phân chia theo loại thông tin cần thu thập như:

 OS Fingerprinting (Thu thập thông tin về hệ điều hành).

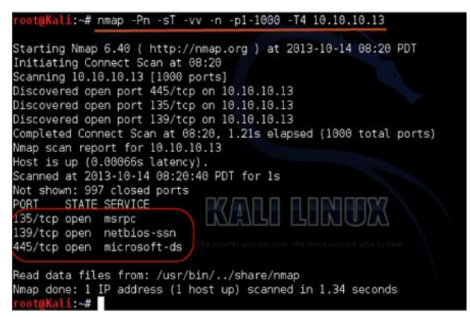
 Network Scanners (Dò quét cổng, dò quét mạng, dò quét phiên bản dịch vụ).

 SSL Analysis (Phân tích giao thức SSL).

 VoIP Analysis (Phân tích giao thức VoIP).

Trong số các công cụ trên có một công cụ rất nổi tiếng, cực hữu ích khi thực hiện đánh giá bảo mật hạ tầng mạng lưới điện toán, đó chính là Nmap.

Với Nmap, chúng ta có thể biết được Ports (Cổng dịch vụ) nào đang Open, Filtered hoặc Closed, ngoài ra còn có thể xác định được phiên bản dịch vụ (Banner version) và cũng có thể thực hiện phán đoán phiên bản hệ điều hành mà mục tiêu đang sử dụng.



Hình 1. Quét port với nmap trên Kali

Một công cụ khác cũng nổi trội không kém là theHarvester. Công cụ này dựa vào nhiều nguồn tìm kiếm như google, google-profiles, bing, Linkedin hoặc Shodan để thu thập thông

tin, ví dụ: thu thập thông tin về một công ty ABC nào đó, tìm kiếm địa chỉ email, tên máy chủ và nhiều thông tin liên quan đến công ty đó bằng theHarvester.



Hình 2. Thu thập thông tin với theHarvester

1.2.Phân tích lỗ hổng - Vulnerability Analysis

Những công cụ nằm trong nhóm này tập trung vào việc phát hiện các lỗ hổng bảo mật như: lỗ hổng ứng dụng, lỗ hổng trong hạ tầng, mạng lưới cho đến phần cứng chuyên dụng. Vì vậy ở đây có rất nhiều các công cụ Vulnerability Scanner (Dò quét lỗ hổng) và Fuzzers (Kiểm thử). Một số công cụ có thể kể đến như:

Sqlmap: Đây là một công cụ tuyệt vời mà thực sự có thể giúp bạn tìm kiếm và khai thác các lỗ hổng SQL Injection. Với công cụ này, bạn chỉ định các ứng dụng web và các thông số bạn muốn kiểm tra, phần còn lại phần mềm sẽ tự động hóa thực hiện

OpenVAS: OpenVAS là một nền tảng dành cho việc dò quét phát hiện các lỗ hổng. Nó được tạo ra như một nhánh của Nessus khi Nessus trở nên thương mại hóa.

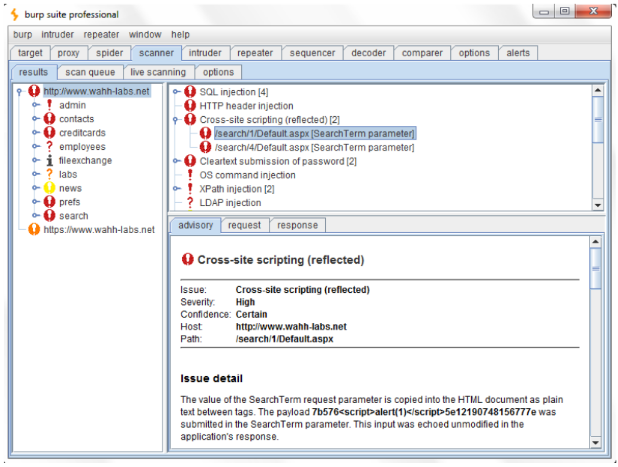
1.3.Ứng dụng Web - Web Applications

Nhóm phân loại này gồm những công cụ dùng để phát hiện và tấn công các lỗ hổng ứng dụng Web. Trong đó có một công cụ rất đáng để chúng ta quan tâm, chính là Burp Suite (Có hai phiên bản Free và Pro).

Một trong những tính năng chính và cơ bản của Burp Suite là khả năng Intercept (đánh chặn) tất cả các HTTP Request được gửi đến các ứng dụng Web, nhờ đó chúng ta có thể chỉnh sửa, thay đổi, kiểm thử tham số và gửi đến ứng dụng.

Burp Suite không chỉ là một công cụ đánh chặn, mà còn là một trong những công cụ tốt nhất để thực hiện các phân tích lỗ hổng ứng dụng Web tự động hoặc thủ công.

Ví dụ, với Burp bạn có thể để tải nhiều Payloads từ một file và sửa đổi các tham số (Parameters), gửi các Payload đó đến cho các ứng dụng Web. Điều này giúp cho bạn có thể thực hiện những cuộc tấn công Brute force.



Hình 3. Giao diện của công cụ Burp Suite

Ngoài ra chúng ta có thể sử dụng các công cụ khác như XSSer. Công cụ này tương tự như Sqlmap, dùng để tìm các lỗ hổng XSS.

1.4.Tấn công mật khẩu - Password Attacks

Trong nhóm này chúng ta có thể tìm thấy những công cụ bẻ khóa mật khẩu Offline hay khởi tạo các cuộc tấn công mật khẩu vào các giao thức. Công cụ đáng chú ý trong phân loại này là John the Ripper, oclhashcat-plus, Medusa và THC-Hydra. John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix. Nó là một trong những chương trình testing/breaking mật khẩu phổ biến nhất vì có kết hợp một số bộ cracker mật khẩu, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh. Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản

Unix khác (dựa trên DES, MDS hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash. Bên cạnh đó còn có các modul bổ sung mở rộng khả năng gồm có cả các kiểu mật khẩu MD4 và các mật khẩu được lưu trong LDAP, MySQL và các thành phần khác.

Oclhashcat-plus là công cụ dùng để giải mã md5crypt, phpass, mscash2 và WPA / WPA2. Medusa và THC-Hydra có thể giúp khởi tạo các cuộc tấn công Brute Force đối với các giao thức như HTTP, FTP, SSH, RDC.

1.5.Tấn công mạng không dây - Wireless Attacks

Trong phân loại này bạn có thể tìm thấy các công cụ dùng để phân tích và tấn công các giao thức mạng không dây như IEEE 802.11, RFID / NFC hay Bluetooth.

Công cụ hữu dụng nhất trong phần này để thực hiện phân tích giao thức IEEE 802.11 (WiFi) là aircrack-ng. Công cụ này cho phép thực hiện nhiều kiểu tấn công khác nhau với các cơ chế xác thực (authentication) và ủy quyền (authorization) của mạng WiFi.

1.6.Nghe lén/Giả mạo - Sniffing/Spoofing

Sniffing/Spoofing (Nghe lén/Giả mạo) cung cấp các công cụ để intercept lưu lượng mạng trên đường truyền, Web hoặc lưu lượng VoIP. Một trong những chương trình Sniffer tốt nhất hiện nay chính là Wireshark.

Với Wireshark bạn sẽ có thể intercept lưu lượng mạng và có thể xác định giao thức được sử dụng, phân tích và highlight các dữ liệu quan trọng.

Một công cụ thú vị khác là Dsniff. Công cụ này được chia thành nhiều ứng dụng giúp intercept và xác định những loại dữ liệu nhạy cảm như mật khẩu, e-mail, PII hoặc sniff các dữ liệu đã mã hóa SSL.

1.7.Duy trì kết nối - Maintaining Access

Phân loại này tập hợp tất cả các công cụ giúp duy trì khả năng truy cập đến mục tiêu, sau khi đã chiếm được quyền kiểm soát hệ thống và đánh cắp các thông tin quan trọng được lưu trữ trong đó.

1.8.Kiểm tra hiệu năng - Stress Testing

Stress Testing (Kiểm tra hiệu năng), trong nhóm phân loại này chúng ta có thể tìm thấy những công cụ khác nhau để kiểm tra hiệu năng của Network, ứng dụng Web, WLAN hay

VoIP khi xử lý một lượng lớn lưu lượng. Ví dụ, với những công cụ này chúng ta có thể dùng để mô phỏng tấn công từ chối dịch vụ - DoS.

1.9.Các công cụ báo cáo - Reporting Tools

Reporting Tools (Các công cụ dành cho việc báo cáo): gồm các công cụ để giúp tạo ra những bản báo cáo sau khi hoàn tất công việc đánh giá bảo mật, dựa trên các kết quả mà chúng ta đã tìm thấy.

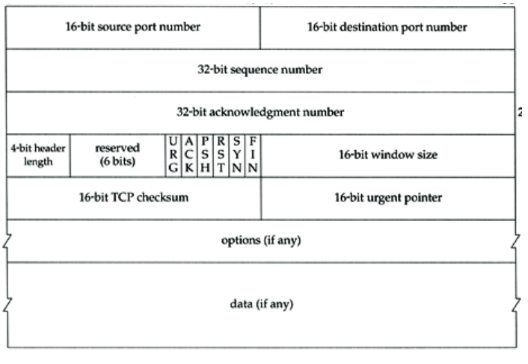
Ví dụ, công cụ recordMyDesktop, nhiệm vụ đơn giản của nó chính là tạo ra các File video ghi lại những hoạt động của bạn trên máy tính.

Một công cụ quan trọng khác không kém là TrueCrypt. Nó không liên quan trực tiếp tới việc lập các tài liệu báo cáo, là một chuyên gia đánh giá bảo mật bạn luôn phải thực sự cẩn thận với nơi lưu trữ các kết quả đánh giá bảo mật của bạn. TrueCrypt cung cấp cho bạn khả năng lưu trữ an toàn các kết quả đánh giá bảo mật và mã hóa để không ai có thể đọc chúng ngoài bạn.

2. Tìm hiểu vế công cụ thu thập thông tin (Nmap)

2.1.Nguyên tắc truyền thông tin TCP/IP

2.1.1. Cấu tạo gói tin TCP



Hình 4. Cấu trúc gói TCP

Trong phần này chúng ta chỉ quan tâm tới các thiết lập Flag trong gói tin TCP nhằm mục đích sử dụng để Scan Port:

 Thông số SYN để yêu cầu kết nối giữa hai máy tính.

 Thông số ACK để trả lời kết nối giữa hai máy có thể bắt đầu được thực hiện.

 Thông số FIN để kết thúc quá trình kết nối giữa hai máy.

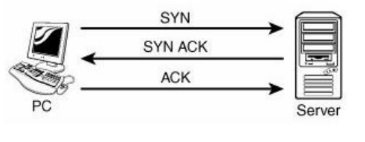
 Thông số RST từ Server để nói cho Client biết rằng giao tiếp này bị cấm (không thể sử

dụng).

 Thông số PSH sử dụng kết hợp với thông số URG.

 Thông số URG sử dụng để thiết lập độ ưu tiên cho gói tin này.

2.1.2. Khi Client muốn thực hiện một kết nối TCP với Server



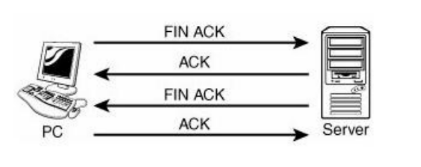
Hình 5. Cách thức Client kết nối với Server

+ Bước 1: Client gửi đến Server một gói tin SYN.

+ Bước 2: Server trả lời tới Client một gói tin SYN/ACK.

+ Bước 3: Khi Client nhận được gói tin SYN/ACK sẽ gửi lại server một gói ACK và quá trình trao đổi thông tin giữa hai máy bắt đầu.

2.1.3. Khi Client muốn kết thúc một phiên làm việc với Server



Hình 6. Cách thức Client kết thúc phiên làm việc với Server

+ Bước 1: Client gửi đến Server một gói tin FIN ACK.

+ Bước 2: Server gửi lại cho Client một gói tin ACK.

+ Bước 3: Server lại gửi cho Client một gói FIN ACK.

+ Bước 4: Client gửi lại cho Server gói ACK và quá trình ngắt kết nối giữa Server và Client được thực hiện.

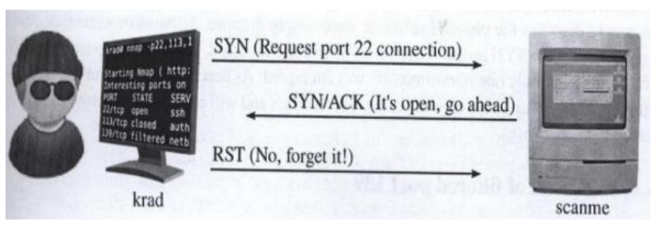
2.2.Nguyên tắc Scan port trong một hệ thống

2.2.1. TCP Scan

Trên gói TCP/UDP có 16 bit dành cho Port Number, điều này có nghĩa là nó có từ 1 – 65535 port. Thông thường chúng ta chỉ sử dụng từ port 1 đến port 1024, nên khi một hacker muốn thu thập thông tin thì cũng tập trung scan những port đó. Dựa vào các nguyên tắc truyền thông tin của TCP, chúng ta có thể Scan Port nào mở trên hệ thống bằng những phương thức sau đây:

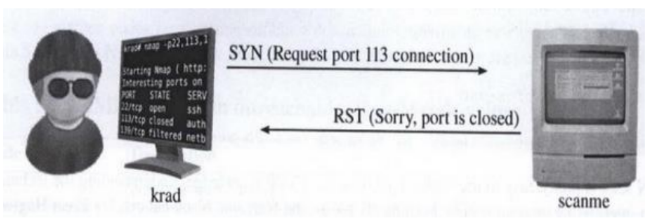
SYN Scan: Khi Client gửi gói SYN với một thông số Port nhất định tới Server nếu server gửi về gói SYN/ACK thì Client biết Port đó trên Server được mở. Nếu Server gửi về cho Client gói RST/SYN tôi biết port đó trên Server đóng.

Ví dụ: SYN scan với port 22 đang mở



Hình 7. SYN Scan với port 22

Ví dụ: SYN scan với port 113 đang đóng



Hình 8. Syn scan với port 113

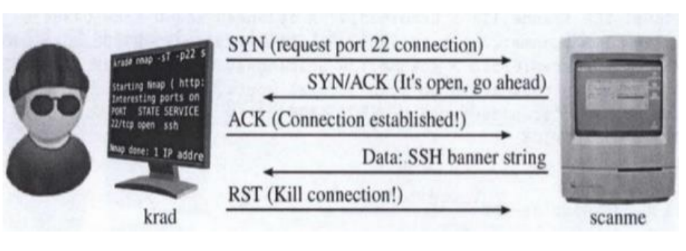
FIN Scan: Khi Client chưa có kết nối tới Server nhưng vẫn tạo ra gói FIN với số port nhất định gửi tới Server cần Scan. Nếu Server gửi về gói ACK thì Client biết Server mở port đó, nếu Server gửi về gói RST thì Client biết Server đóng port đó.

NULL Scan: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì Client biết port đó trên Server bị đóng.

XMAS Scan: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST thì Client biết port đó trên Server bị đóng.

TCP Connect: Phương thức này rất thực tế. Client gửi đến Server những gói tin yêu cầu kết nối thực tế tới các port cụ thể trên server. Nếu server trả về gói SYN/ACK thì Client biết port đó mở, nếu Server gửi về gói RST/ACK Client biết port đó trên Server bị đóng.

Ví dụ: Client scan kết nối với port 22 đang mở



Hình 9. Client kết nối với port 22 đang mở

ACK Scan: phương thức Scan này nhằm mục đích tìm những Access Controll List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP nếu nhận được gói tin là Host Unreachable thì Client sẽ hiểu port đó trên server đã bị lọc.

Có vài dạng Scan cho các dịch vụ điển hình dễ bị tấn công như:

- RPC Scan: Cố gắng kiểm tra xem hệ thống có mở port cho dịch vụ RPC không.

- Windows Scan: tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.

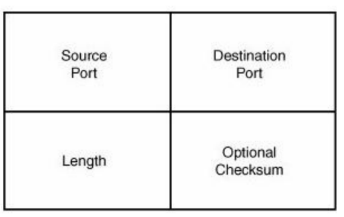
- FTP Scan: dùng để xem dịch vụ FTP có được sử dụng trên Server hay không.

- IDLE : cho phép kiểm tra tình trạng của máy chủ.

2.2.2. UDP Scan

Đối với những gói tin truyền bằng TCP thì sẽ đảm bảo được sự toàn vẹn của gói tin, gói tin sẽ luôn được truyền tới đích. Còn đối với những gói tin truyền bằng UDP sẽ đáp ứng được nhu cầu truyền tải dữ liệu nhanh với các gói tin nhỏ. Khi thực hiện truyền tin bằng TCP kẻ tấn công dễ dàng Scan được hệ thống đang mở những port nào dựa trên các thông số Flag trên gói TCP.

Cấu tạo gói tin UDP



Hình 10. Cấu tạo gói tin UDP

Ta thấy rằng trong gói tin UDP không chứa các thông số Flag, cho nên không thể sử dụng các phương thức Scan port của TCP được. Tuy nhiên hầu hết hệ thống đều cho phép gói ICMP.

Nếu một port bị đóng, khi Server nhận được gói ICMP từ client nó sẽ cố gắng gửi một gói ICMP với nội dung là "Unreachable" về Client. Khi thực hiện UDP Scan các kết quả nhận được không có độ tin cây cao.

2.3. Sử dụng Nmap để scan port

2.3.1. Các giai đoạn của Nmap scan

Target enumeration: Nmap tìm kiếm các máy chủ được cung cấp bởi người dùng.

Host disovery (ping scan): quét mạng. Đầu tiên là khai thác các máy mục tiêu có

đang hoạt động không. Nmap có nhiều kỹ thuật để phát hiện máy chủ, sử dụng ARP kết hợp TCP, ICMP và các kiểu khác.

Reverse DNS: Nmap tìm kiếm reverse-DNS name của toàn bộ host đang online.

Port scanning: thăm dò gửi và trả lời.

Version detection: nếu port được xác định là mở, Nmap có thể xác định phần mềm

máy chủ đang chạy (-sV).

OS detection: nếu yêu cầu với lựa chọn là –O, Nmap sẽ phát hiện hệ điều hành đang

sử dụng.

Traceroute: Nmap chứa 1 thành phần traceroute. Có thể tìm kiếm các route mạng tới

nhiều host.

Script scanning: sử dụng kịch bản để có nhiều thông tin hơn.

Output: thu thập toàn bộ thông tin và xuất ra một file.

2.3.2. Các dạng scan mà Nmap hỗ trợ

Nmap –sT: trong đó chữ s – là Scan, còn chữ T là dạng TCP scan.

Nmap –sU: đó là sử dụng UDP Scan.

Nmap –sP: sử dụng Ping để scan.

Nmap –sF: sử dụng FIN Scan.

Nmap –sX: sử dụng phương thức XMAS Scan.

Nmap –sN: sử dụng phương thức NULL Scan.

Nmap –sV: sử dụng để Scan tên các ứng dụng và version của nó.

Nmap –SR /I RPC sử dụng để scan RPC.

2.3.3. Các option kết hợp với các dạng Scan trong Nmap.

- O: sử dụng để biết hệ điều hành chạy trên máy chủ. Ví dụ sử dụng Nmap với phương thức scan là XMAS Scan và đoán biết hệ điều hành của: <www.abc.com> ta dùng câu lệnh: nmap – sX –o <www.abc.com>.

- P: dãy port sử dụng để scan.

- F: Chỉ những port trong danh sách scan của Nmap.

- V: Sử dụng Scan hai lần nhằm tăng độ tin cậy và hiệu quả của phương thức scan mà ta sử dụng.

- P0: không sử dụng ping để Scan nhằm mục đích giảm thiểu các quá trình quét ngăn chặn scan trên các trang web hay máy chủ.

3. Tìm hiểu công cụ phân tích lỗ hỏng (Nessus)

Một trong những mối quan tâm hàng đầu của các nhà quản trị hệ thống là làm sao biết được hệ thống của mình bị hổng ở chổ nào để có thể vá lại hoặc để tấn công hay đột nhập vào nếu người quan tâm đến chúng là các hacker. Có rất nhiều công cụ trợ giúp trong việc xác định các lỗi bảo mật và những điểm nhạy cảm của hệ thống như Retina của Eeye, hay Nexpose… Nhưng một trong các công cụ được các hacker và những nhà quản trị hệ thống yêu thích là nessus, công cụ được xếp hạng thứ nhất trong nhiều công cụ bảo mật được đánh giá bởi tổ chức Insecure

(<www.insecure.org>).

Với tính năng phát hiện nguy hiểm nhanh, thống kê toàn diện về hệ thống đầy đủ, phát hiện dữ liệu nhạy cảm và phân tích lỗ hổng, đáp ứng yêu cầu cao về bảo mật.

Nessus kiểm soát toàn bộ toàn hệ thống mạng doanh nghiệp bao gồm cả bên trong những khu vực DMZs (thường là những vùng chứa Email server, Web server) và từng đoạn mạng vật lý riêng biệt.

Nessus hỗ trợ kiểm tra các kiểu bảo mật sau đây:

 Quét các cổng đáng tin và không đáng tin.

 Quét lỗ hổng bảo mật mạng.

 Kiểm tra bản vá tin cậy cho Windows và hầu hết nền tảng Unix.

 Kiểm tra cấu hình tiêu chuẩn cao cho hầu hết nền tảng Windows và Unix.

 Kiểm tra độ tin cậy bảo mật một cách toàn diện cho các ứng dụng của phần mềm thứ 3 như iTunes, Java, Skype và Firefox.

 Kiểm tra lỗ hổng ứng dụng web được nhúng và tùy biến.

Kiểm tra cấu hình CSDL SQL.

 Kiểm tra cấu hình Cisco Route.

 Thống kê phần mềm trên Unix và Windows.

 Kiểm tra phần cài đặt chữ ký số hết hạn và những lỗi cấu hình của phần mềm.

 Anti-virus.

Có cả phiên bản cho Windows, Linux, MacOS…Nessus không được cài mặc định trên Kali Linux. Nessus bao gồm cả phiên bản miễn phí và tính phí.

4. Tìm hiểu công cụ crack password

4.1. Giới thiệu

Crack password là quá trình bẻ khóa mật khẩu mà những kẻ tấn công đều muốn thực hiện nhất trong quá trình tấn công hệ thống. Nếu bẻ khóa thành công thì mọi thông tin, tài khoản người dùng đều bị nguy hiểm. Các kiểu crack password.

Hình 11. Các kiểu crack password

Passive Online: Nghe lén sự thay đổi mật khẩu. Cuộc tấn công dạng này bao gồm: sniffing, man-in-the-middle, và replay attacks.

Active online: đoán trước mật khẩu. Các cuộc tấn công này bao gồm việc đoán trước password tự động.

Offline: các kiểu tấn công dạng này gồm có: dictionary, hybrid, và brute-force.

Non-Electronic: Các cuộc tấn công dạng này dựa vào yếu tố con người như: Social engineering, Phising, …

4.2. Passive Online attack