Module 5
SYSTEM HACKING

Các Chủ Đề Chính Trong Chương Này

Bẻ Khóa Mật Khẩu

Leo Thang Đặc Quyền

Thực Thi Chương Trình

Che Dấu Tập Tin

Xóa Dấu Vết

Trong chương này chúng ta sẽ thảo luận về chủ đề System Hacking bao gồm các thao tác tấn công vào hệ thống. Như đã trình bày trong phần *Scanning* và *Enumeration* tiến trình System Hacking sẽ gồm sáu bước , đầu tiên là *Enumration* và các bước còn lại là :

- Bẻ Khóa Mật Khẩu
- Leo Thang Đặc Quyền
- Thực Thi Chương Trình
- Che Dấu Tập Tin
- Xóa Dấu Vết

Các bài giảng về chủ đề System Hacking

- Giới thiệu về System Hacking http://youtu.be/Qgh43mNbbPg
- Leo thang đặc quyền http://youtu.be/DNpZzOwz-Rs
- Thực thi ứng dụng http://youtu.be/lr0lEOuh8ts

Phần 1 - Bẻ Khóa Mật Khẩu

Rất nhiều tình huống tấn công hệ thống bắt đầu với việc phá mật khẩu vì đây là một trong những thông tin quan trọng nhất để truy cập vào hệ thống. Có nhiều dạng mật khẩu khác nhau nhưng thông thường khi người dùng muốn truy cập vào hệ thống của mình như hệ điều hành Windows 7 thì anh ta cần phải cung cấp thông tin gồm tài khoản cùng với mật khẩu liên quan. Vì nhiều lý do cá nhân mà người sử dụng thường đặt mật khẩu khá dễ nhớ và liên quan đến các thông tin đặc biệt của mình như ngày sinh, số điện thoại hay là tên người yêu, thú cưng của mình. Do đó mà việc tấn công mật khẩu thường có tỉ lệ thành công cao. Đặc biệt, các mật khẩu lại thường được dùng chung cho nhiều dịch vụ khác nhau cho nên khi một mật khẩu hệ thống bị phá vỡ thì các hệ thống khác cũng chịu chung số phận như tình huống mà các hacker thuộc nhóm Luzsec khi tấn công vào diễn đàn của công ty bảo mật danh tiếng là BKIS đã công bố trên blog. Một khi việc bẻ khóa thành công thì hacker sẽ tiến hành các thao tác leo thang đặc quyền, chạy những chương trình nguy hiểm trên hệ thống bị tấn công và sau đó là tiến hành che dấu tập tin, xóa dấu vết để phòng chống bị điều tra.

Có nhiều kỹ thuật bẻ khóa khác nhau từ các phương pháp thủ công cho đến tự động dựa trên cơ chế dò từ điển hay tấn công *brute-force*. Để tấn công theo dạng thủ công thì hacker sẽ đoán mật khẩu của tài khoản (thường là *Administrator*) dựa trên các đặc điểm của người dùng như số điện thoại, ngày sinh, … và tiến hành thử nghiệm cho đến khi đăng nhập thành công. Với phương pháp này, hacker cần phải tìm hiểu thông tin của người dùng khá kỹ thông qua các cơ sở dữ liệu được công bố trên internet hay những mối quan hệ thân quen của nạn nhân.

Còn có các cách thức hiệu quả hơn, đó là hacker tìm cách đánh cắp những tập tin mật khẩu được lưu trữ trên máy tính như tập tin /etc/passwd trên Linux, tập tin SAM trên hệ thống Windows. Các tập tin này chứa thông tin người dùng và mật khẩu đã được mã hóa một chiều theo các thuận toán băm (MD5, SHA) sau đó sử dụng công cụ để tiến hành bẻ khóa theo dạng *brute-force* hay dò từ điển.

Một cách tổng quan, có bốn dạng tấn công mật khẩu là :

- **Passive Online:** Nghe trôm sự thay đổi mật khẩu trên mạng. Cuộc tấn công thụ động trực tuyến bao gồm: sniffing, man-in-the-middle, và replay attacks (tấn công dựa vào phản hồi)
- **Active Online:** Đoán trước mật khẩu người quản trị. Các cuộc tấn công trực tuyến bao gồm việc đoán password tự động.
- **Offline:** Các kiểu tấn công như Dictionary, hybrid, và brute-force.

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

Passive Online Attack

Một cuộc tấn công thụ động trực tuyến là đánh hơi (sniffing) để tìm các dấu vết, các mật khẩu trên một mạng. Mật khẩu là bị bắt (capture) trong quá trình xác thực và sau đó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách từ (word list). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa (encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng. Nếu mật khẩu được bảo vệ bằng cách trên,một số công cụ đặc biệt giúp hacker có thể phá vỡ các thuật toán mã hóa mật khẩu.

Active Online Attack

Cách dễ nhất để đạt được cấp độ truy cập của một quản trị viên hệ thống là phải đoán từ đơn giản thông qua giả định là các quản trị viên sử dụng một mật khẩu đơn giản. Mật khẩu đoán là để tấn công. Active Online Attack dựa trên các yếu tố con người tham gia vào việc tạo ra mật khẩu và cách tấn công này chỉ hữu dụng với những mật khẩu yếu. Trong chương 6, khi chúng ta thảo luận về các giai đoạn Enumeration, bạn đã học được những lỗ hổng của NetBIOS Enumeration và Null Session. Giả sử rằng NetBIOS TCP mở port 139, phương pháp hiệu quả nhất để đột nhập vào Win NT hoặc hệ thống Windows 2000 là đoán mật khẩu. Cái này được thực hiện bằng cách cố gắng kết nối đến hệ thống giống như một quản trị viên thực hiện. Tài khoản và mật khẩu được kết hợp để đăng nhập vào hệ thống.
Một hacker, đầu tiên có thể thử để kết nối với tài nguyên chia sẽ mặc định là Admin$, C$ hoặc C:\Windows. Để kết nối tới các ổ đĩa máy tính, ổ đĩa chia sẻ, gõ lệnh sau đây trong Start > Run:

```
\\ ip_address \ c$
```

Các chương trình tự động có thể nhanh chóng tạo ra file từ điển, danh sách từ, hoặc kết hợp tất cả có thể có của các chữ cái, số và ký tự đặc biệt và cố gắng để đăng nhập vào. Hầu hết các hệ thống ngăn chặn kiểu tấn công này bằng cách thiết lập một số lượng tối đa của các nỗ lực đăng nhập vào một hệ thống trước khi tài khoản bị khóa. (ví dụ khi bạn đăng nhập vào một trang web mà bạn nhập sai password 5 lần thì tài khoản bạn từ động bị khóa lại 1 ngày)

Offline Attack

Cuộc tấn công Offline được thực hiện tại một vị trí khác hơn là hành động tại máy tính có chứa mật khẩu hoặc nơi mật khẩu được sử dụng. Cuộc tấn công Offline yêu cầu phần cứng để truy cập vật lý vào máy tính và sao chép các tập tin mật khẩu từ hệ thống lên

phương tiện di động. Hacker sau đó có file đó và tiếp tục khai thác lỗ hổng bảo mật. Bảng sau minh họa vài loại hình tấn công offline:

Các kiểu tấn công Offline

Type of Attack	Characteristics	Example Password
Dictionary attack	Nỗ lực để sử dụng mật khẩu từ từ điển	Administrator
Hybrid attack	Thay thế một vài ký tự của mật khẩu	Adm1n1strator
Brute-force-attack	Thay đổi toàn bộ ký tự của mật khẩu	Ms!tr245@F5a

Dictionary Attack là cách tấn công đơn giản và nhanh nhất trong các loại hình tấn công. Nó được sử dụng để xác định một mật khẩu từ thực tế, và mật khẩu có thể được tìm thấy trong từ điển. Thông thường nhất, cuộc tấn công sử dụng một tập tin từ điển các từ có thể, sau đó sử dụng một thuật toán được sử dụng bởi quá trình xác thực. Các hàm băm (hash) của các từ trong từ điển được so sánh với hàm băm của mật khẩu người dùng đăng nhập vào, hoặc với các mật khẩu được lưu trữ trong một tập tin trên máy chủ. Dictionary Attack chỉ làm việc nếu mật khẩu là một thực thể có trong từ điển. Nhưng kiểu tấn công này có một số hạn chế là nó không thể được sử dụng với các mật khẩu mạnh có chứa số hoặc ký hiệu khác .

Hybrid Attack là cấp độ tiếp theo của hacker, một nỗ lực nếu mật khẩu không thể được tìm thấy bằng cách sử dụng Dictionary Attack. Các cuộc tấn công Hybrid bắt đầu với một tập tin từ điển và thay thế các con số và các ký hiệu cho các ký tự trong mật khẩu. Ví dụ, nhiều người sử dụng thêm số 1 vào cuối mật khẩu của họ để đáp ứng yêu cầu mật khẩu mạnh. Hybrid được thiết kế để tìm những loại bất thường trong mật khẩu.

Brute Force Attack là một cuộc tấn công bằng thuật toán brute-force, mà mọi cố gắng kết hợp có thể có của chữ hoa và chữ thường, chữ cái, số, và biểu tượng. Một cuộc tấn công bằng thuật toán brute-force là chậm nhất trong ba loại tấn công vì có thể kết hợp nhiều ký tự trong mật khẩu. Tuy nhiên, cách này có hiệu quả, cần có đủ thời gian và sức mạnh xử lý tất cả.

Noneelectronic Attack

Các cuộc tấn công nonelectronic là dạng tấn công mà không sử dụng bất kỳ kiến thức kỹ thuật nào. Loại tấn công có thể bao gồm các kỹ thuật như *social engineering, shoulder surfing, keyboard sniffing, dumpster diving.*

Công Cụ Tấn Công

Legion : Đây là công cụ có khả năng quét nhiều máy tính cùng lúc thông qua các dãy địa chỉ IP để tìm ra các tài nguyên chia sẽ và đoán mật khẩu của người dùng tự động.

L0pht Crack : là ứng dụng thường được đề cập trong các câu hỏi của kì thi lấy chứng chỉ CEH, L0pht Crack (còn gọi tắt với các tên LC5 hay LC6 tùy theo phiên bản của ứng dụng) có khả năng bẻ khóa mật khẩu rất mạnh mẽ dựa trên dữ liệu từ điển có sẵn của ứng dụng hay tiến hành bẻ khóa theo dạng brute-force (quét cạn) nếu như dò tìm điển không thành công. Với ứng dụng này, những máy tính có cấu hình càng mạnh thì tỉ lệ thành công càng cao.

Join The Riper : Ứng dụng dạng dòng lệnh này có thể bẻ khóa mật khẩu của các hệ thống Unix và Windows.

KerbCrack : Chương trình này gồm hai thành phần là : kerbsniff và kerbcrack, trong đó kerbsniff sẽ lắng nghe và bắt giữ các thông tin đăng nhập của hệ thống Windows 2000 / XP / 2003 / Vista sau đó sẽ gởi đến cho kerbcrack bẻ khóa thông qua các phương pháp quét cạn hay dùng từ điển.

Thế Nào Là LanManager Hash ?

Windows 2000 sử dụng NT Lan Manager (NTLM) để tiến hành băm và bảo vệ mật khẩu khi truyền trên mạng. Tuy nhiên đây là một phương pháp bảo vệ yếu dễ dàng bị bẻ khóa, vì dụ ta có mật khẩu là *123456abcdef* được mã hóa với NTLM thì trước tiên nó sẽ được chuyển đổi thành kí tự chữ hoa là *123456ABCDEF* và sau đó điền vào các khoảng trắng cho đủ 14 kí tự ***123456ABCDEF__.*** Trước khi mật khẩu này được mã hóa thì chuỗi kí tự trên sẽ được chia đôi thành **123456A** và **BCDEF__** rồi tiến hành mã hóa riêng cho từng nhóm với kết quả như sau :

123456A = 6BF11E04AFAB197F
BCDEF__ = F1E9FFDCC75575B15

Và ghép lại thành chuỗi kết quả đích là ***6BF11E04AFAB197FF1E9FFDCC75575B15***

Với mật khẩu này, phần đầu tiên của mật khẩu được mã hóa bao gồm các kí tự và chữ số gây đôi chút khó khăn cho *L0phtCrack*, vì vậy ứng dụng này có thể cần tối đa 24 tiếng để bẻ khóa trong khi phần còn lại chỉ gồm các kí tự đơn giãn nên *L0phtCrack* chỉ cần 60 giây để tìm được kết quả.

Bẻ Khóa Mật Khẩu Hệ Thống Windows 2000

Trên hệ điều hành windows 2000 và XP thì thông tin tài khoản và mật khẩu được mã hóa với hàm băm lưu trong tập tin SAM tại thư mục Windows\system32\config. Tuy nhiên, tập tin này bị khóa khi hệ thống đang hoát động, do đó hacker sẽ không thể nào tương tác

vào đươc tập tin trên khi hệ điều hành đang chạy. Vì vậy, để có thể lấy được tập tin trên các hacker thường sử dụng các chương trình khởi động từ hệ thống DOS / Linux hay dùng đĩa khởi động HirenBoot. Ngoài ra, tập tin *SAM* còn có thể được lấy từ bản sao đã được nén của nó là *SAM._* trong thư mục *C:\windows\repair*, sau khi lấy về hacker giải nén băng lệnh expand như sau :

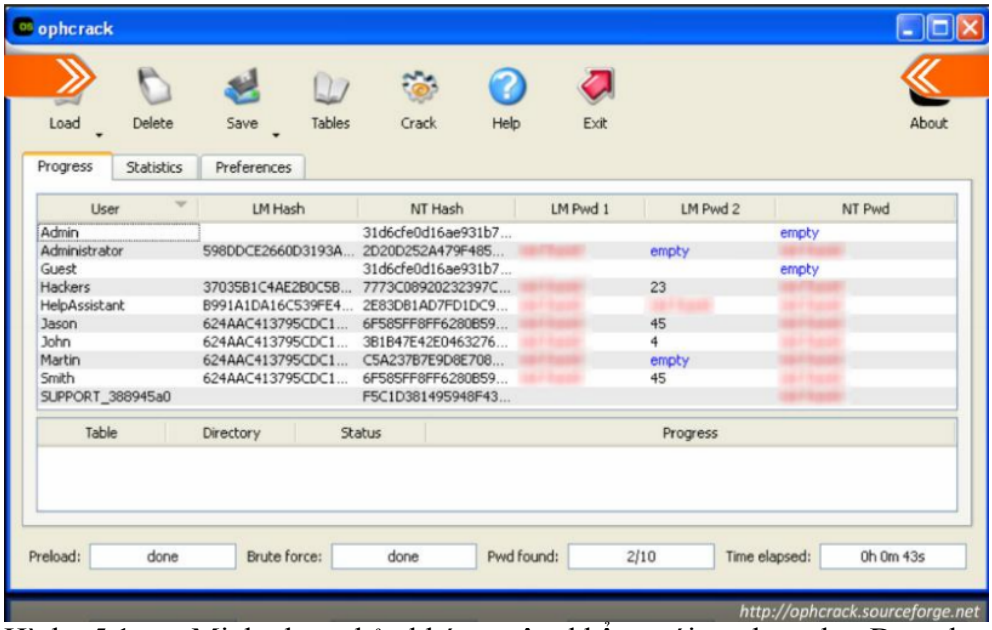
C:\>expand sam._ sam

Một khi tập tin này được giả nén thì các bạn có thể sử dụng các chương trình bẻ khóa theo dạng *brute-force* hay dò từ điển như *L0phtCrack* để dò tìm mật khẩu.

Công Cụ Bẻ Khóa Hay Xóa Trắng Mật Khẩu Thông Dụng

NT Offline Password Recovery : Đây là chương trình khá mạnh mẽ dùng để bẻ khóa mật khẩu, và là ứng dụng đầu tiên tôi đã từng sử dụng để bẻ khóa cho chính hệ thống Domain Controller trên hệ thống máy chủ Windows Server 2003 của mình vào năm 2003, và tỉ lệ thành công rất cao. Bên cạnh chức năng bẻ khóa mật khẩu thông thường thì NT Offlien Password Recovery còn cho phép vô hiệu hóa dịch vụ Syskey. Hiện nay ứng dụng này đã được tích hợp trên bộ đĩa Hiren Boot CD (http://www.hirensbootcd.org/download/)

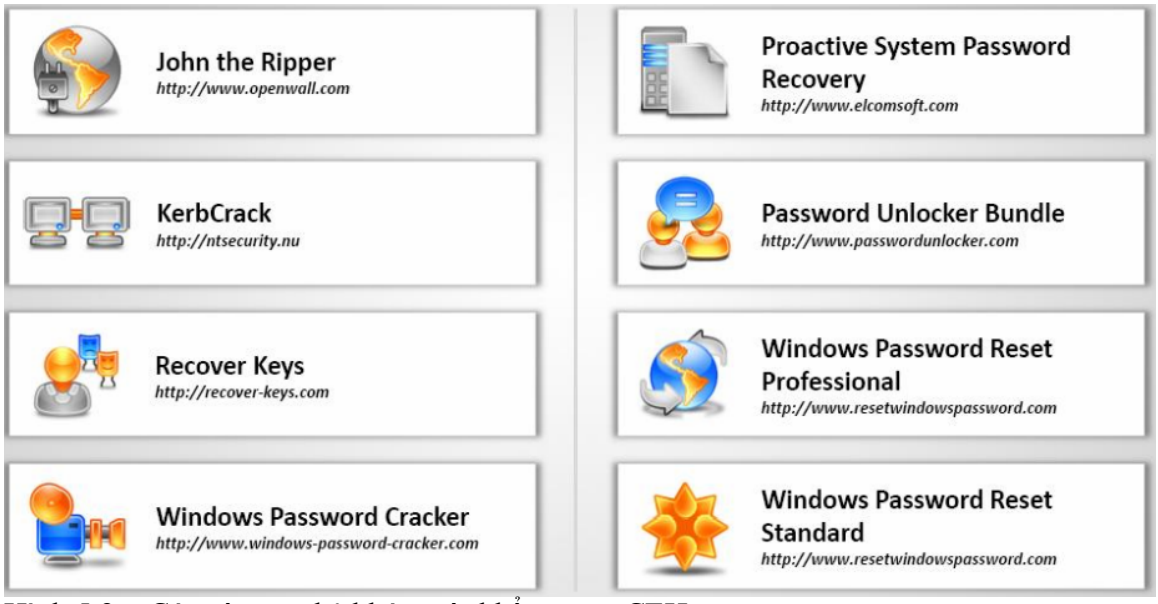
OphCrack : Đây là Live CD dùng để bẻ khóa hệ thống mật khẩu Windows khá mạnh và miễn phí.



Hình 5.1 - Minh họa bẻ khóa mật khẩu với ophcrack. Download tại http://ophcrack.sourceforge.net

Active Pasword Change : Ứng dụng này cho phép chạy trực tiếp từ Live CD với giao diện trực quan rất dễ sử dụng, có thể download tập tin iso tại địa chỉ http://www.netpro.edu.vn/download/activepasswordchange.iso . Demo minh họa tại

Hình 5.2 là danh sách một số công cụ bẻ khóa mật khẩu thông dụng hiện nay :



Hình 5.2 – Các công cụ bẻ khóa mật khẩu trong CEH

Chuyển Hướng SMB Logon Đến Attacker

Một phương pháp tấn công mật khẩu khác của hacker là chuyển hướng trang đăng nhập mật khẩu của dịch vụ SMB đến máy tính của attacker với mục tiêu chuyển các mật khẩu đến cho kẻ tấn công. Để thực hiện điều này thì các hacker cần phải nghe lén các phản hồi NTML (response) từ máy chủ xác thực và dẫn dụ nạn nhân xác thực với máy chủ qua máy tính của mình. Ví dụ như khi các hacker gởi một emailo chứa đường link dẫn đến máy chủ SMB giả mạo, khi nạn nhân click vào đường link trên sẽ bị điều hướng các giao dịch dựa trên SMB đến máy tính của attacker.

Công Cụ Tấn Công SMB Dựa Trên Cơ Chế Điều Hướng

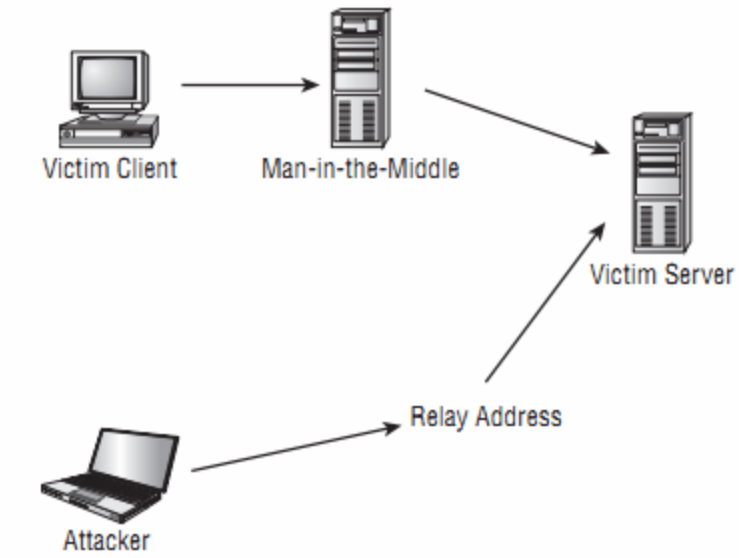
Có một số công cụ có thể thực hiện tấn công dựa trên cơ chế này, thường được sử dụng là SMB Relay. Đây là một máy chủ SMB dùng để bắt giữ thông tin tài khoản và mật khẩu truy cập (đã được mã hóa với hàm băm) từ các luồng dữ liệu SMB, và có khả năng tấn công theo cơ chế man in the middle (sẽ được trình bày trong phần Sniffer).

Phiên bản nâng cao của SMB Relay là SMB Relay 2 có thể tiến hành nghe lén dựa trên tên NetBios thay vì dùng địa chỉ IP như SMB Relay.

Ngoài ra, khi tương tác trực tiếp vào hệ thống các hacker còn dùng công cụ *samdump* hay *pwdump2* để xem các thông tin tài khoản và mật khẩu mã hóa, sau đó chuyển tập tin này cho ứng dụng *L0phtCrack* xử lý. Đây cũng là một ví dụ mà tôi có trình bày trong chương trình đào tạo của mình về an toàn thông tin cho tổng công ty VNPT, khi đó các học viên sẽ sử dụng Metasploit để đột nhập vào một hệ thống Windows Server 2003 bị lỗi, tiếp theo là nạp dll có chứa công cụ pwdump để lấy thông tin mật khẩu rồi chuyển đến cho chương trình LC 5 (L0phtCrack 5, phiên bản mới nhất vào lúc đó) để bẻ khóa mật khẩu.

Tấn Công SMB Relay MITM Và Giải Pháp Phòng Chống

Trong mô hình tấn công SMB Relay MITM các hacker sẽ đặt giữa máy chủ SMB và client một hệ thống giả mạo với mục tiêu bắt giữ tất cả các thông tin tài khoản của người dùng trong giao dịch SMB, sau đó mới chuyển các thông tin này về cho máy chủ thật sự nhằm bảo đảm cho quá trình truyền thông vẫn diễn ra bình thường, nhưng thực sự thì các thông tin đã bị lấy cắp. Cách tấn công này thường ứng dụng trong các mạng xung đột (broadcast domain) sử dụng Hub để liên kết các máy trạm, Đối với những hệ thống mạng sử dụng thiết bị như Switch thì hacker cần phải tiến hành quá trình đầu độc ARP (arp posioning) trước khi bắt giữ các gói tin khác.



Hình 5.3 – Mô hình tấn công SMB Relay MITM

Để phòng chống lại dạng tấn công SMB Relay MITM cần cấu hình các máy tính sử dụng *SMB signing* trong chính sách bảo mật (có thể cấu hình trên từng máy trong mục *Security Policies/Security Options* hay cấu hình chính sách vùng trên *domain controller* rồi áp đặt cho các máy tính thuộc vùng).

Các Công Cụ Tấn Công MITM Thông Dụng

Có khá nhiều công cụ tấn công MITM hiện nay có chức năng đầu độc ARP như arpspoof, dfsniff, ettercap. Trong đó, ettercap là ứng dụng mạnh mẽ nhất từng được mệnh danh là "vua của các mạng tokenring" với biệt hiệu Lord Of The TokenRing lấy theo tựa đề phim chúa nhẫn.

NetBIOS DoS Attacks

Dạng tấn công *NetBISO Denial of Service (DoS)* gởi các thông điệp *NetBIOS Name Release* đến máy chủ *NetBIOS Name Service* như máy chủ WINS trên các hệ thống Windows của nạn nhân và ép hệ thống mục tiêu luôn ở trong tình trạng xung đột tên. Điều này sẽ ngăn chặn không cho phép các máy tính client liên hệ và kết nối đến máy chủ thông qua tên NetBIOS, gây nên tình trạng từ chối dịch vụ trên hệ thống mạng.

Công cụ tấn công dạng này như *NBName* có thể vô hiệu hóa toàn bộ hệ thống mạng LAN, ngăn không cho các máy tính gia nhập mạng vì các máy trạm trên hệ thống sử dụng NetBISO cho rằng đã có một máy tính khác sử dụng tên của mình.

Phòng Chống Bị Bẻ Khóa Mật Khẩu

Để ngăn ngừa bị bẻ khóa mật khẩu chúng ta cần áp đặt các chính sách mật khẩu mạnh có độ dài trên 8 kí tự, với sự kết hợp của nhiều dạng kí tự khác nhau gồm kí tự đặc biệt, chữ hoa, chữa thường và các số sẽ làm cho quá trình tấn công dò từ điển hay brute-force trở nên khó khăn. Bên cạnh đó, quản trị mạng nên ứng dụng *Syskey* trên Windows, một chức năng bảo vệ và mã hóa mật khẩu nâng cao có thể phòng chống rất tốt các công cụ như *L0phtCrack, Ron The Ripper*.

Để sử dụng Syskey các bạn chỉ cần thực thi dòng lệnh Syskey trên cữa sổ dòng lệnh và chọn Update (Encryption Enable) như Hình 5.4

Hình 5.4 - Ứng dụng Syskey

Sau đây là một số quy tắt đặt mật khẩu cần tuân theo để phòng chống bị bẻ khóa :

1. Không bao giờ sử dụng mật khẩu mặc định.

2. Không bao giờ sử dụng các mật khẩu đơn giãn có thể bị tìm kiếm thông qua dò từ điển, như các mật khẩu là ***password, abcdef, 123456*** là những mật khẩu được thống kê là bị tấn công nhiều nhất.
3. Không bao giờ sử dụng mật khẩu liên quan đến hostname, domain name hay những thông tin mà hacker dễ dàng tìm kiếm qua Whois.

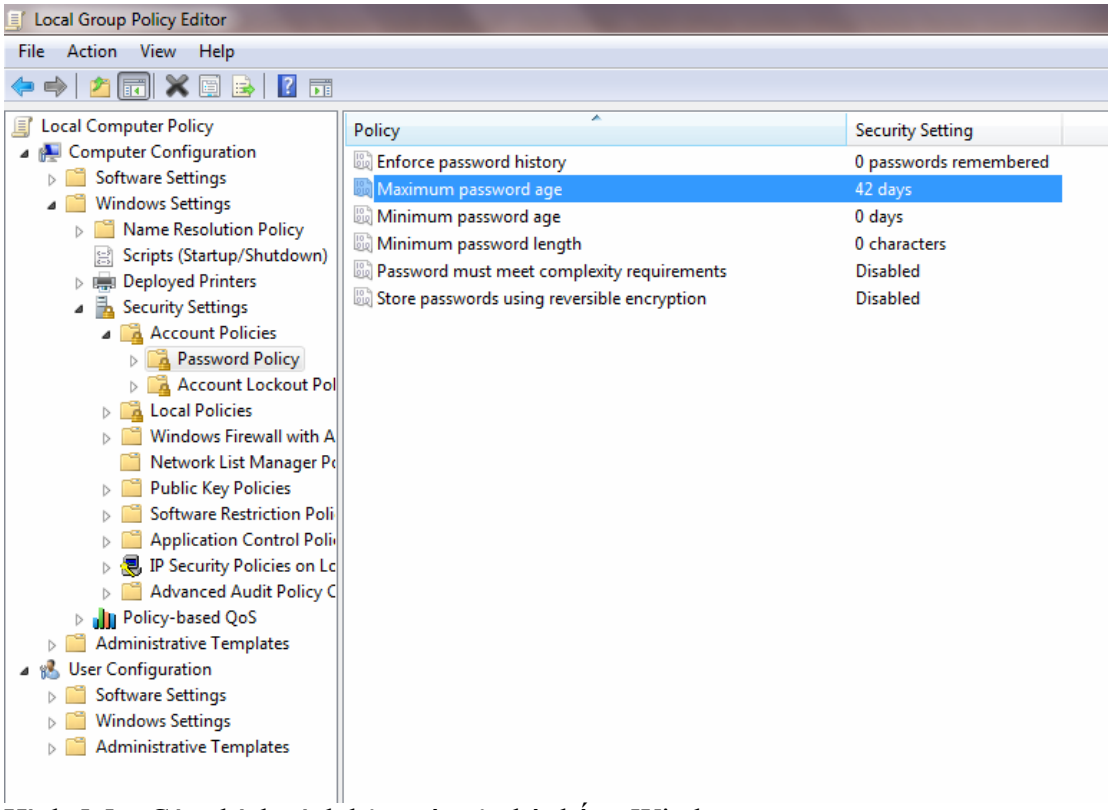
4. Không bao giờ sử dụng mật khẩu liên quan đến thú cưng, ngày sinh của bạn hay người yêu vì đây là những đối tượng mà hacker sẽ nghĩ đến đầu tiên khi dò mật khẩu của bạn.

5. Sử dụng các mật khẩu có độ dài trên 21 kí tự sẽ khiên cho hacker không thể bẻ khóa bằng cách dò từ điển.

Trong phần tiếp theo, chúng ta sẽ thảo luận về hai phương pháp giúp gia tăng độ mạnh của mật khẩu và ngăn ngừa bị tấn công.

Thay Đổi Mật Khẩu Thường Xuyên

Thay đổi mật khẩu thường xuyên là một trong những tiêu chí hàng đầu trong việc bảo vệ mật khẩu, thoe khuyến nghĩ của chính sách an toàn thông tin ISO 27001 : 2005 thì chúng ta nên thay đổi mật khẩu sau 24 ngày hoặc 48 ngày tùy vào nhu cầu của tổ chức. Mặc dù điều này sẽ gây ra đôi chút bất tiện cho người dùng nhưng sẽ hạn chế rất nhiều khả năng các hacker bẻ khóa được mật khẩu và tái sử dụng để truy cập bất hợp pháp vào hệ thống. Việc thiết lập các chính sách này có thể thực hiện qua Group Policy Editor trong phần Security Setttings\Account Policies như Hình 5.5



Hình 5.5 – Các chính sách bảo mật của hệ thống Windows.

Hình trên mình họa vị trí chính sách dùng để thay đổi thời gian tồn tại của một mật khẩu trên Windows 7. Đối với các hệ thống Windows phiên bản khác các bạn cũng có thể thực hiện thông qua Local Group Policy Editor dễ dàng. Tuy nhiên, để đạt hiệu quả cao hơn các bạn nên thiết lập chính sách này chung cho toàn bộ hệ thống thông qua Domain Controller.

Mặc dù với phương pháp này chúng ta không thể hoàn toàn ngăn ngừa bị tấn công mật khẩu dạng brute-force vì hacker nhưng sẽ gây ra trở ngại lớn cho chúng khi siết chặt Security Policy (chính sách bảo mật) ví dụ nếu đăng nhập sai mật khẩu quá 5 lần sẽ bị khóa trong vòng 15 phút sẽ nãn chí những kẻ tấn công.

Theo Dõi Event Viewer Log

Trong vai trò quản trị hệ thống hay người phụ trách vấn đề an ninh mạng của tổ chức các bạn cần thường xuyên theo dõi tập tin nhật kí Event View, điều này sẽ giúp chúng ta phát hiện ra những hành động khả nghi như xâm nhập trái phép của hacker, hoặc có các virus đang lây lan trên mạng đang cố gắng kết nối đến những máy tính khác nhau bằng tên *netbios* và các mật khẩu mặc định. Có nhiều công cụ giám sát Event Log chuyên dụng cho từng hệ thống máy chủ riêng biệt như các sản phẩm của GFI (www.gfi.com) hay chương trình VisualLast (http://www.ntobjectives.com/) hỗ trợ các quản trị mạng trong công việc phân tích log file thông qua các báo cáo về tình trạng đăng nhập tương đối rõ

ràng. Đối với những chương trình chuyên dụng thì khi hệ thống có sự cố xảy ra sẽ có những cảnh báo thích hợp bằng mail, sms hay cả gọi điện thoại tự động đến cho quản trị viên.

Tập tin nhật kí được lưu trữ tại c:\\windows\system32\config\ , cần lưu ý trong một số tình huống tập tin này rỗng do các bạn không hiệu lực chúng trong chính sách bảo mật. hãy thiết lập chúng trong mục **Security Settings\ Local Policies.**

Phần 2 – Leo Thang Đặc Quyền

Leo thang đặc quyền hay *Escalating Privilege* là bước thứ ba trong chu trình Hacking System, leo thang đặc quyền về cơ bản có nghĩa là thêm nhiều quyền hơn hoặc cho phép một tài khoản người dùng thêm quyền, leo thang đặc quyền làm cho một tài khoản người dùng có quyền như là tài khoản quản trị.

Nói chung, các tài khoản quản trị viên có yêu cầu mật khẩu nghiêm ngặt hơn, và mật khẩu của họ được bảo vệ chặt chẽ hơn. Nếu không thể tìm thấy một tên người dùng và mật khẩu của một tài khoản với quyền quản trị viên, một hacker có thể chọn sử dụng một tài khoản với quyền thấp hơn. Tại trường hợp này, các hacker sau đó phải leo thang đặc quyền để có nhiều quyền như quyền của quản trị.

Cái này được thực hiện bằng cách nắm lấy quyền truy cập bằng cách sử dụng một tài khoản người dùng không phải là quản trị viên. Thường bằng cách thu thập các tên người dùng và mật khẩu thông qua một bước trung gian để gia tăng các đặc quyền trên tài khoản với mức độ quản trị viên.

Một khi hacker đã có một tài khoản người dùng hợp lệ và mật khẩu, các bước tiếp theo là để thực thi các ứng dụng nói chung hacker cần phải có một tài khoản có quyền truy cập cấp quản trị viên để cài đặt chương trình. Đó là lý do tại sao leo thang đặc quyền là rất quan trọng. Trong các phần kế tiếp , chúng tôi sẽ xem những gì hacker có thể làm với hệ thống của bạn một khi họ có quyền quản trị.

Công Cụ Leo Thang Đặc Quyền

> **Getadmin.exe** là một chương trình nhỏ nó có thể thêm một người dùng vào nhóm Local Administrator. Một vài kernel NT cấp thấp, thường xuyên truy cập để cho phép quá trình chạy. Một đăng nhập vào giao diện điều khiển máy chủ là cần thiết để thực hiện chương trình. Getadmin.exe được chạy từ dòng lệnh và chỉ hoạt động trên Win NT 4.0 Service Pack 3.

Tiện ích **HK.exe** để lộ ra kẽ hở trong giao thức gọi hàm cục bộ (Local Procedure Call) của Windows NT. Một người dùng có thể là không phải người quản trì có thể leo thang vào nhóm quản trị viên bằng cách sử dụng công cụ này.

Phần 3: Thực Thi Ứng Dụng

Một khi hacker đã có thể truy cập tài khoản với quyền quản trị, điều tiếp theo cần làm là thực thi các ứng dụng trên hệ thống đích. Mục tiêu của việc thực thi ứng dụng có thể cài đặt một cửa sau trên hệ thống, cài đặt một keylogger để thu thập thông tin bí mật, sao chép các tập tin, hoặc chỉ gây thiệt hại cơ bản cho hệ thống, bất cứ điều gì hacker muốn làm trên hệ thống.

Khi hacker có thể thực thi các ứng dụng, họ có thể chiếm toàn quyền trên hệ thống hệ thống này.

Công Cụ

PsExec là một chương trình kết nối vào và thực thi các tập tin trên hệ thống từ xa. Phần mềm không cần phải được cài đặt trên hệ thống từ xa.

Remoxec thực thi một chương trình bằng cách sử dụng dịch vụ RPC (Task Scheduler) hoặc WMI (Windows Management Instrumentation). Administrators với mật khẩu rỗng hay yếu có thể khai thác thông qua lịch trình công việc (Task Scheduler - 1025/tcp) hoặc chế độ phân phối thành phần đối tượng (Distributed Component Object Mode; 135/tcp).

Buffer Overflow

Hacker cố gắng khai thác một lỗ hổng trong mã ứng dụng (Application). Về bản chất, cuộc tấn công tràn bộ đệm gửi quá nhiều thông tin cho một biến nào đó trong ứng dụng, có thể gây ra lỗi ứng dụng. Hầu hết các lần, ứng dụng không biết hành động tiếp theo bởi vì nó được ghi đè bằng các dữ liệu bị tràn. Vì thế nó hoặc thực thi các lệnh trong các dữ liệu bị tràn hoặc giảm trong một dấu nhắc lệnh để cho phép người dùng nhập lệnh tiếp theo này. Dấu nhắc lệnh (command prompt hoặc shell) là chìa khóa cho hacker có thể được sử dụng để thực thi các ứng dụng khác.

Chuyên đề về Buffer Overflows sẽ được thảo luận chi tiết trong *chương 17: Buffer Overflow*

Rootkit

Rootkit là một loại chương trình thường được sử dụng để che dấu các tiện ích trên hệ thống bị xâm nhập. Rootkit bao gồm cái gọi là *back doors*, nó giúp cho kẻ tấn công đó truy cập vào hệ thống sẽ dễ dàng hơn trong lần sau. Ví dụ, các rootkit có thể ẩn một ứng dụng, ứng dụng này có thể sinh ra một lệnh kết nối vào một cổng mạng cụ thể trên hệ thống. *Back door* cho phép các quá trình bắt đầu bởi một người không có đặc quyên, dùng để thực hiện chức năng thường dành cho các quản trị viên. Rootkit thường xuyên được sử dụng để cho phép lập trình viên ra rootkit có thể xem và truy cập vào tên người dùng và thông tin đăng nhập trên các trang site có yêu cầu họ.

Khái niệm Site ở đây không phải là website, mà là một miền (domain) trong hệ thống các máy tính.

Một Số Loại Rootkit Thường Gặp:

Kernel-level rootkit: Rootkit ở cấp độ Kernel thường thêm hoặc thay thế một vài thành phần của nhân hệ thống, thay bằng mã được sửa đổi để giúp che giấu một chương trình trên hệ thống máy tính. Điều này thường được thực hiện bằng cách thêm mã mới cho nhân hệ thống thông qua một thiết bị ổ đĩa có khả năng nạp mô-đun, chẳng hạn như các kernel mô-đun có thể nạp được trong linux hoặc các thiết bị điều khiển trong Microsoft Windows. Rootkit đặc biệt nguy hiểm bởi vì nó có thể khó phát hiện mà không có phần mềm phù hợp.

Library-level rootkit: Rootkit ở cấp độ thư viện thường chắp vá, sữa chữa, hoặc thay thế hệ thống. Một số phiên bản có thể giấu thông tin tùy theo mục đích của hacker.

Application-level rootkits Rootkit ở cấp ứng dụng thì có thể thay thế những chương trình ứng dụng giống trojan độc hại, hoặc họ có thể thay đổi hành vi của các ứng dụng hiện có bằng cách sử dụng các móc (hook), các bản vá lỗi (patch), mã độc hại (injected code), hoặc các phương tiện khác.

Triển khai Rootkits trên Windows 2000 & XP

Trong hệ điều hành Window NT/2000 thì rookit được xây dựng như một trình điều khiển ở chế độ kernel của driver, có thể được tự động nạp trong chế độ runtime. Rootkit có thể chạy với đặc quyền hệ thống (system privileges) trong NT Kernel. Do đó, nó đã truy cập vào tất cả các nguồn tài nguyên của hệ điều hành. Các rootkit cũng có thể ẩn các quy trình, ẩn các tập tin, ẩn các mục đăng ký, tổ hợp phím tắt trên hệ thống, giao diện điều

khiển, phát hành gián đoạn từng bước để gây ra một màn hình màu xanh của sự chết chốc (death) và chuyển các tập tin EXE.
Rootkit này có chứa một trình điều khiển hoạt động ở chế độ kernel *(kernel mode device driver)* có tên gọi là *_root_.sys* và khởi chạy chương trình có tên là *DEPLOY.EXE*. Sau khi đạt được quyền truy cập vào hệ thống, chúng copy file *-root-.sys* và *DEPLOY.EXE* thành nhiều file vào hệ thống và thực thi file *DEPLOY.EXE*. Sau đó sẽ cài đặt trình điều khiển thiết bị rootkit và kẻ tấn công bắt đầu xóa *DEPLOY.EXE* từ các máy tính mục tiêu. Những kẻ tấn công sau đó có thể dừng lại và khởi động lại các rootkit bằng cách sử dụng lệnh *net stop _root_and _root_* và các tập tin *_root_.sys* không còn xuất hiện trong danh sách thư mục. Rootkit chặn không cho hệ thống gọi tập tin trong danh sách và giấu tất cả các file bắt đầu với *_root_* .

```
Trong hệ điều hành, có hai chế độ hoạt động là usermode
và kernel mode. Với Kernel mode, các trình ứng dụng có
toàn quyền truy cập vùng nhớ của RAM, các chỉ lệnh
CPU…nói chung là toàn quyền.
```

Rootkit được nhúng vào giao thức TCP/IP

Một tính năng mới của rootkit trong window NT/2000 là nó hoạt động bằng cách xác định tình trạng kết nối dựa trên các dữ liệu trong gói dữ liệu đến (incoming). Rootkit có một địa chỉ IP cố định mà nó sẽ trả lời. Rootkit sử dụng các kết nối Ethernet qua hệ thống card mạng, vì thế nó rất mạnh mẽ. Một hacker có thể kết nối đến port bất kỳ trên hệ thống. Ngoài ra, nó cho phép nhiều người có thể đăng nhập cùng một lúc.

Phòng chống Rootkit

Tất cả các rootkit truy cập hệ thống đích có quyền giống như quản trị viên (administrator), do đó, bảo mật mật khẩu là rất quan trọng. Nếu bạn phát hiện một rootkit, lời khuyên rằng bạn nên sao lưu dữ liệu quan trọng và cài đặt lại hệ điều hành và các ứng dụng từ một nguồn đáng tin cậy. Các quản trị viên cũng nên giữ sẵn một nguồn đáng tin cậy để cài đặt và phục hồi tự động.

Biện pháp đối phó khác là sử dụng thuật toán mã hóa MD5, checksum MD5 của một tập tin là một giá trị 128-bit, nó giống như là dấu vân tay tập tin. Thuật toán này được thiết kế để phát hiện sự thay đổi, ngay cả một chút trong tập tin dữ liệu, để kiểm tra các nguyên nhân khác nhau. Thuật toán này có tính năng rất hữu ích để so sánh các tập tin và đảm bảo tính toàn vẹn của nó. Một tính năng hay là kiểm tra chiều dài cố định, bất kể kích thước của tập tin nguồn là như thế nào.

Việc tổng kiểm tra MD5 đảm bảo một file đã không thay đổi này có thể hữu ích trong việc kiểm tra tính toàn vẹn file nếu rootkit đã được tìm thấy trên hệ thống. Các công cụ như **Tripwire** được thực hiện để kiểm tra MD5, để xác định các tập tin có bị ảnh hưởng bởi rootkit hay không.

Công Cụ Phòng Chống

Tripwire là một chương trình kiểm tra tính toàn vẹn hệ thống tập tin hệ điều hành Unix, Linux, thêm vào kiểm tra mật mã một hoặc nhiều nội dung trong mỗi thư mục và tập tin. Tripwire có cơ sở dữ liệu chứa thông tin cũng cho phép bạn xác minh, cho phép truy cập và cài đặt chế độ tập tin, tên người dùng chủ sở hữu tập tin, ngày tháng và thời gian tập tin đã được truy cập lần cuối, và sửa đổi cuối.

Keylogger và Phần Mềm Gián Điệp

Nếu tất cả những nỗ lực để thu thập mật khẩu không thành công, thì keylogger là công cụ lựa chọn cho các hacker. Được thực hiện như là phần mềm được cài đặt trên máy tính hoặc là phần cứng gắn vào máy tính. Keylogger là các phần mềm ẩn, ngồi giữa phần cứng (bàn phím) và hệ điều hành, để họ có thể ghi lại mọi phím tắt. Keylogger phần mềm có thể phá hoại hệ thống như Trojans hoặc viruses.

Keylogger là phần mềm gián điệp có dung lượng nhỏ, giúp kết nối các bàn phím máy tính và lưu tất cả các thao tác phím vào một file. Hacker có thể cài thêm tính năng là tự động gửi nội dung file đó đến máy chủ của hacker.

Đối vối kiểu keylogger cứng, có một thiết bị, giống usb, được gắn vào máy tính. Quá trình thao tác phím được ghi lại trong usb đó. Để làm được điều này thì một hacker phải có quyền truy cập vật lý vào hệ thống.

```
Keylogger cứng thường được cài ở các điểm internet công
cộng có ý đồ xấu. Do đó khi truy cập net tại nơi công
cộng, bạn nên quan sát kỹ lưỡng các thiết bị bất thường
được cắm vào máy tính.
```

Công Cụ Tấn Công

Spector là phần mềm gián điệp ghi lại mọi điều từ hệ thống nào đó trên mạng Internet, giống như một camera giám sát tự động. Spector có hàng trăm bức ảnh chụp mỗi giờ của bất cứ thứ gì trên màn hình máy tính và lưu những bức ảnh chụp ở một vị trí ẩn trên ổ đĩa cứng của hệ thống. Spector có thể được phát hiện và loại bỏ bởi phần mềm chống Spector.

eBlaster là phần mềm gián điệp internet để chụp các email gửi đến và gửi đi, và ngay lập tức chuyển chúng đến một địa chỉ email. Eblaster cũng có thể chụp cả hai mặt của một cuộc hội thoại nhắn tin tức thời (Instant Messenger), thực hiện tổ hợp phím đăng nhập và các trang web truy cập thường xuyên.

Spyanywhere là một công cụ cho phép bạn xem các hoạt động hệ thống và hành động của người sử dụng, tắt/khởi động lại máy, khóa/đóng băng, và ngay cả trình duyệt gỡ bỏ tập tin hệ thống. Spyanywhere cho phép bạn kiểm soát chương trình mở và đóng cửa sổ trên hệ thống từ xa và xem lịch sử internet và các thông tin liên quan.

Kkeylogger là một phần mềm gián điệp hiệu suất cao, trình điều khiển thiết bị ảo, chạy âm thầm ở mức thấp nhất của hệ điều hành Windows 95/98/ME. Tất cả các tổ hợp phím được ghi lại trong một tập tin.

Email keylogger là phần mềm ghi lại tất cả các email được gửi và nhận trên một hệ thống. Mục tiêu các hacker là có thể xem người gửi, người nhận, chủ đề, và thời gian/ngày…. nội dung email và bất kỳ file đính kèm cũng được ghi lại.

Phần 4: Hiding Files

Một hacker có thể muốn che dấu các tập tin trên một hệ thống, để ngăn chặn bị phát hiện, sau đó có thể được dùng để khởi động một cuộc tấn công khác trên hệ thống. Có hai cách để ẩn các tập tin trong Windows.

Đầu tiên là sử dụng lệnh **attrib**. Để ẩn một tập tin với lệnh attrib, gõ như sau tại dấu nhắc lệnh:

```
attrib +h [file/directory]
```

Cách thứ hai để ẩn một tập tin trong Windows là với luồng dữ liệu xen kẽ NTFS (*alternate data streaming - ADS)*.

NTFS File Streaming

NTFS sử dụng bởi Windows NT, 2000, 2003, 2008 và cả các hệ thống Windows XP, Windows 7 có một tính năng gọi là *ADS* cho phép dữ liệu được lưu trữ trong các tập tin liên kết ẩn một cách bình thường, có thể nhìn thấy được tập tin. Streams không giới hạn về kích thước, hơn nữa một stream có thể liên kết đến một file bình thường.
Để tạo và kiểm tra NTFS file stream, ta thực hiện các bước sau:

1. Tại dòng lệnh, nhập vào **notepad test.txt**
2. Đặt một số dữ liệu trong tập tin, lưu tập tin, và đóng notepad
3. Tại dòng lệnh, nhập **dir test.txt** và lưu ý kích thước tập tin
4. Tại dòng lệnh, nhập vào **notepad test.txt:hidden.txt** thay đổi một số nội dung vào Notepad, lưu các tập tin, và đóng nó lại.
5. Kiểm tra kích thước tập tin lại (giống như ở bước 3).
6. Mở lại **test.txt**. bạn chỉ nhìn thấy những dữ liệu ban đầu.
7. Nhập **type test.txt:hidden.txt** tại dòng lệnh một thông báo lỗi được hiển thị. *"The filename, directory name, or volume label syntax is incorrect."*

Các bạn có thể tham khảo bài hướng dẫn về chủ đề này tại http://youtu.be/0knTHa61Q0E.

Công Cụ Tấn Công

Makestrm.exe là một tiện ích chuyển dữ liệu từ một tập tin vào một tập tin liên kết ADS và thay thế liên kết với các tập tin ban đầu.

Phòng Chống NTFS File Streaming

Để xóa một stream file, đầu tiên là copy nó đến phân vùng FAT, và sau đó cpoy nó trởvào phân vùng NTFS. Stream bị mất khi tập tin được chuyển đến phân vùng FAT, vì nó có một tính năng của phân vùng NTFS và do đó chỉ tồn tại trên một phân vùng NTFS.

Công Cụ Phòng Chống

Bạn có thể sử dụng LNS.exe để phát hiện ra Stream. LNS báo cáo sự tồn tại và vị trí của những file chứa dữ liệu stream.

Steganography

Steganography là quá trình giấu dữ liệu trong các loại dữ liệu khác như hình ảnh hay tập tin văn bản.

```
Các phương pháp phổ biến nhất của dữ liệu ẩn trong các tập tin là sử dụng hình ảnh đồ họa như là nơi để cất giấu. Kẻ tấn công có thể nhúng các thông tin trong một tập tin hình ảnh bằng cách sử dụng steganography. Các hacker có thể ẩn các chỉ dẫn thực hiện một quả bom, số bí mật của tài khoản ngân hàng... Hành động bất kỳ có thể được ẩn trong hình ảnh.
```

Công Cụ Tấn Công

1. **Imagehide** là một chương trình *steganography*, nó giấu số lượng lớn văn bản trong hình ảnh. Ngay cả sau khi thêm dữ liệu,vẫn không có sự gia tăng kích thước hình ảnh, hình ảnh trông giống như trong một chương trình đồ họa bình thường. Nó nạp và lưu các tập tin và do đó là có thể tránh được nghe lén.

2. **Blindside** là một ứng dụng *steganography* mà giấu thông tin bên trong ảnh BMP (bitmap). Đó là một tiện ích dòng lệnh.

3. **MP3stego** giấu thông tin trong file mp3 trong quá trình nén. Dữ liệu được nén, mã hóa, và chúng ẩn trong các dòng bit MP3.

4. **Snow** là một chương trình *whitespace steganography* có nghĩa là che giấu thông điệp trong ASCII text, bằng cách phụ thêm các khoảng trắng ở cuối file. Vì spaces and tabs không thể nhìn thấy ở người xem văn bản. Nếu được sử dụng một thuật toán mã hóa, tin nhắn không thể đọc ngay cả khi nó bị phát hiện.

5. **Camera/shy** làm việc với Window và trình duyệt Internet Explorer, cho phép người dùng chia sẻ tìm kiếm hoặc thông tin nhạy cảm được lưu giữ trong một hình ảnh GIF thường.

6. **Stealth** là một công cụ lọc, cho các tập tin PGP. Nó loại bỏ thông tin nhận dạng từ tiêu đề, sau đó các tập tin có thể được sử dụng cho *steganography*.

Chống lại Steganography

Steganography có thể được phát hiện bởi một số chương trình, mặc dù làm như vậy là khó khăn. Bướcđầu tiên trong việc phát hiện là để xác định vị trí các tập tin với các văn bản ẩn, có thể được thực hiện bằng cách phân tích các mẫu trong các hình ảnh và thay đổi bảng màu.

Công Cụ Phòng Chống

Stegdetect là một công cụ tự động để phát hiện nội dung *steganographic* trong hình ảnh.

Dskprobe là một công cụ trên đĩa CD cài đặt trên Windows 2000/2003. Dùng để quét đĩa cứng ở cấp độ thấp có thể phát hiện steganography.

Phần 5: Clear Track – Xóa Dấu Vết

Một khi kẻ xâm nhập thành công, đã đạt được quyền truy cập quản trị viên trên một hệ thống, cố gắng để che dấu vết của chúng để ngăn chặn bị phát hiện. Một hacker cũng có thể cố gắng để loại bỏ các bằng chứng hoặc các hoạt động của họ trên hệ thống, để ngăn ngừa truy tìm danh tính hoặc vị trí của cơ quan hacker. Xóa bất kỳ thông báo lỗi hoặc các sự kiện an ninh đã được lưu lại, để tránh phát hiện.

Trong các phần sau đây, chúng tôi sẽ xem xét việc vô hiệu hóa kiểm toán (auditing) và xóa bỏ các bản ghi sự kiện (event log), đó là hai phương pháp được sử dụng bởi hacker để bao bọc dấu vết và tránh bị phát hiện.

Auditing là tính năng ghi lại *Event Log*. *Windows Event Viewer* là chương trình dùng để quản lý Auditing trên windows.

Vô hiệu hóa Auditing

Những việc làm đầu tiên của kẻ xâm nhập sau khi giành được quyền quản trị là vô hiệu hóa auditing. Auditing trong Windows ghi lại tất cả các sự kiện nhất định *Windows Event Viewer*. Sự kiện có thể bao gồm đăng nhập vào hệ thống, một ứng dụng, hoặc một sự kiện. Một quản trị viên có thể chọn mức độ ghi nhật ký trên hệ thống. Hacker cần xác định mức độ ghi nhật ký để xem liệu họ cần làm gì để xóa những dấu vết trên hệ thống.

Công Cụ Tấn Công

auditPol là một công cụ có trong bộ Win NT dành cho các quản trị tài nguyên hệ thống. Công cụ này có thể vô hiệu hóa hoặc kích hoạt tính năng kiểm toán từ cửa sổ dòng lệnh. Nó cũng có thể được sử dụng để xác định mức độ ghi nhật ký được thực hiện bởi một quản trị viên hệ thống.

Xóa Nhật Ký Sự Kiện

Những kẻ xâm nhập có thể dễ dàng xóa bỏ các bản ghi bảo mật trong *Windows Event Viewer*. Một bản ghi sự kiện có chứa một hoặc một vài sự kiện là đáng ngờ bởi vì nó thường cho thấy rằng các sự kiện khác đã bị xóa. Vẫn còn cần thiết để xóa các bản ghi sự kiện sau khi tắt Auditing, bởi vì sử dụng công cụ *AuditPol* thì vẫn còn sự kiện ghi nhận việc tắt tính năng Auditing.

Công Cụ Tấn Công

Một số công dụ để xóa các bản ghi sự kiện, hoặc một hacker có thể thực hiện bằng tay trong *Windows Event Viewer*.

Tiện ích **elsave.exe** là một công cụ đơn giản để xóa các bản ghi sự kiện.

Winzapper là một công cụ mà một kẻ tấn công có thể sử dụng để xóa các bản ghi sự kiện, chọn lọc từ các cửa sổ đăng nhập bảo mật trong năm 2000. Winzapper cũng đảm bảo rằng không có sự kiện bảo mật sẽ được lưu lại trong khi chương trình đang chạy.

Evidence Eliminator là một trình xóa dữ liệu trên máy tính Windows. Nó ngăn ngừa không cho dữ liệu trở thành file ẩn vĩnh viễn trên hệ thống. Nó làm sạch thùng rác, bộ nhớ cache internet, hệ thống tập tin, thư mục temp... *Evidence Eliminator* cũng có thể được hacker sử dụng để loại bỏ các bằng chứng từ một hệ thống sau khi tấn công.

Tổng Kết

Qua chương này chúng ta đã nắm được tầm quan trọng của bảo mật mật khẩu. Các biện pháp thay đổi mật khẩu trong khoảng thời gian thích hợp, độ mạnh của mật khẩu, và các biện pháp bảo mật khác là rất quan trọng đối với an ninh mạng.

Nhận biết các loại tấn công mật khẩu khác nhau. *Passive online* bao gồm *sniffing*, *man-in-the-middle*, và *replay*. *Active online* bao gồm đoán mật khẩu tự động. *Offline attacks* bao gồm *dictionary*, *hybrid*, và *brute force*. *Nonelectronic* bao gồm *surfing*, *keyboard sniffing*, và *social engineering.*
Biết làm thế nào để có bằng chứng về activite hacking là loại bỏ bởi những kẻ tấn công. Xoá bản ghi sự kiện và vô hiệu hoá phương pháp kiểm tra của những kẻ tấn công sử dụng để che dấu vết của chúng.

Nhận ra rằng các tập tin ẩn là phương tiện được sử dụng để lấy ra những thông tin nhạy cảm. Steganography, NTFS File, và các lệnh attrib là những cách tin tặc có thể ẩn và ăn cắp các tập tin.