Module 6
Trojan Và Backdoor

Những Nội Dung Chính Trong Chương Này

Giới Thiệu Về Backdoor

Trojan Là Gì

Overt Và Covert Channel

Netcat

Cách Nhận Biết Máy Tính Bị Nhiễm Trojan

Thế Nào Là "Wrapping" ?

Phòng Chống Trojan

Để kiểm soát mục tiêu các hacker thường sử dụng trojan và backdoor, giữa chúng có một số điểm khác biệt nhưng đều có chung một cách thức lây nhiễm đó là cần được cài đặt thông qua một chương trình khác hay người dùng phải bị dẫn dụ để click vào một tập tin đính kèm mã độc trong email, hay truy cập vào đường link liên kết đến trang web đã được chèn mã khai thác, và mã độc chứa trojan hay backdoor sẽ được nhúng kèm trong *shellcode* (chúng ta sẽ trình bày khái niệm này ở phần sau) cài đặt trên máy của nạn nhân.

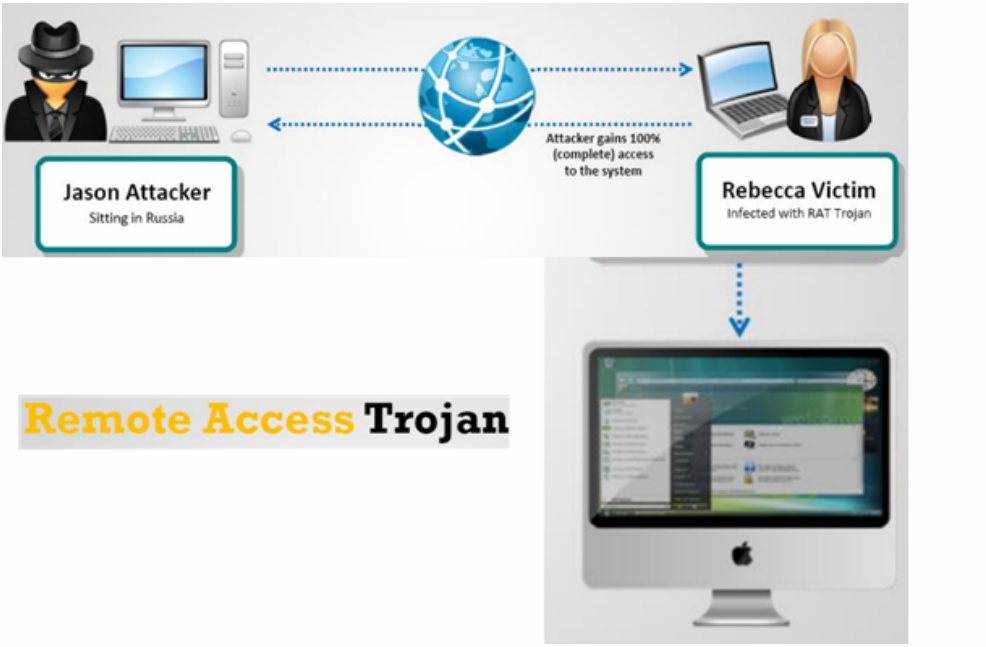
Một số tài liệu tham khảo về trojan và backdoor

- Virus Construction Kit : http://youtu.be/r0PKMNeMIfI
- ICMP Shell Backdoor : http://youtu.be/C0j7Df3xQrQ

Backdoor

Backdoor hay còn gọi là "cổng sau" là chương trình mà hacker cài đặt trên máy tính của nạn nhân để có thể điều khiển hay xâm nhập lại dễ dàng. Một chức năng khác của backdoor là xóa tất cả những thông tin hay các chứng cứ mà hacker có thể để lại khi họ xâm nhập trái phép vào hệ thống, các backdoor tinh vi đôi khi tự nhân bản hay che dấu để có thể duy trì "cổng sau" cho phép các hacker truy cập hệ thống ngay cả khi chúng bị phát hiện. Kỹ thuật mà backdoor thường thực hiện đó là thêm một dịch vụ mới trên các hệ điều hành Windows, và dịch vụ này càng khó nhận dạng thì hiệu quả càng cao. Do đó tên của chúng thường đặt giống với tên của những dịch vụ của hệ thống hay thậm chi các hacker sẽ tìm tên các tiến trình hệ thống nào không hoạt động (hay tắt những tiến trình này) và dùng tên này đặt cho các backdoor của mình. Điều này sẽ qua mặt được cả những chuyên gia hệ thống giàu kinh nghiệm.

Một trong các backdoor thường được đề cập trong CEH là Remote Administration Trojan (RAT) cho phép các hacker kiểm soát những máy tính đã bị chiếm quyền điều khiển với những chức năng xem và quản lý toàn bộ desktop, thực thi các tập tin, tương tác vào registry hay thậm chí tạo ra các dịch vụ hệ thống khác. Không như các backdoor thông thường RAT neo chúng và hệ điều hành của nạn nhân để khó bị xóa đi và luôn có hai thành phần trong mô hình hoạt động của backdoor này là thành phần client và thành phần server. Trong đó server là tập tin sẽ được cài vào máy tính bị lây nhiễm còn client là ứng dụng mà các hacker dùng để điều khiển server.



Hình 6.1 – RAT backdoor

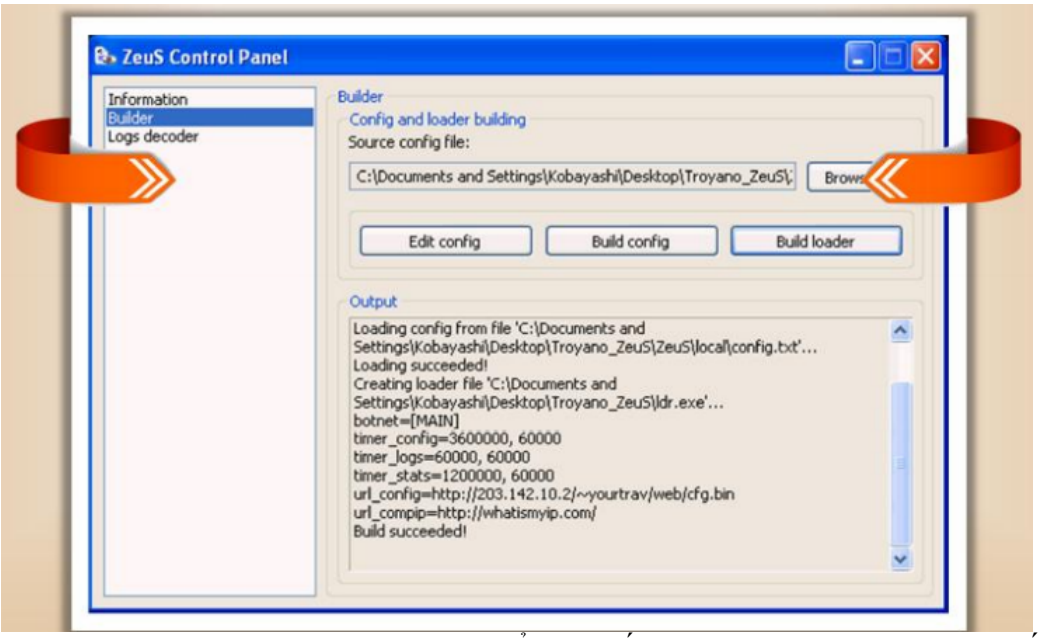
Trojan là gì ?

Đôi khi không có sự phân biệt giữa chức năng của Backdoor và Trojan vì các công cụ cao cấp thuộc dạng này luôn có những chức năng giống nhau. Sự phân biệt chính liên quan đến những hành động của chúng mà hacker sẽ thực hiện, ví dụ hacker cần tiến hành các cuộc tấn công từ chối dịch vụ thì các thành phần mã độc trên máy tính của nạn nhân được gọi là trojan, còn khi hacker thâm nhập vào một máy chủ qua mã độc được cài sẵn thì chương trình nguy hiểm được xem là backdoor. Và một trojan cũng có thể là backdoor hay ngược lại. Trojan ban đầu chỉ là một ý tưởng điều khiển máy tính liên phòng ban trong quân sự, nhưng về sau đã được các hacker phát triển thành một công cụ tấn công nguy hiểm

Tên gọi trojan lấy ý tưởng từ cuộc chiến thành Troy với tên gọi là Trojan Hoorse, có lẽ các bạn cũng đã xem qua hay nghe nói đến bộ phim cuộc chiến thành Troy do tài tử Brad Pitt thể hiện rất xuất sắc trong vài anh hùng Achil, mặc dù với quân lực mạnh mẽ nhưng vẫn không thể nào hạ thành, vì vậy bọn họ đã lập mưu tặng một món quà là con ngựa gỗ khổng lồ có các chiến binh núp ở bên trong để nữa đêm xuất hiện công phá thành từ phía bên trong. Hình 6.2

là giao diện điều khiển của một trojan điển hình Zeus.

Trojan trên máy tính cũng vậy, được cài vào hệ thống của chúng ta thông qua các hình thức "tặng quà" hay những cách tương tự. Ví dụ ta cần kiếm một chương trình nào đó phục vụ công việc và tìm chúng qua các mạng chia sẽ, các diễn đàn hay tìm kiếm *torrent* của ứng dụng này. Các hacker biết rõ điều này nên họ đã tạo sẵn các chương trình trên với tập tin *crack* đã được "khuyến mãi" thêm mã độc (*trojan*/backdoor). Nếu bất cẩn các bạn có thể bị nhiễm trojan theo hình thức này, một khi bị nhiễm thì các tìn hiệu bàn phím chúng ta gõ vào hay những hành động trên máy tính của mình sẽ được thông báo đến hộp thư của hacker hay đẩy lên một máy chủ FTP nào đó trên mạng internet. Đối với các trojan phức tạp và tinh vi còn được trang bị thêm các cơ chế nhận lệnh từ kênh IRC để các hacker dễ dàng điều khiển và phát động các cuộc "tổng tấn công" gây ra tình trạng từ chối dịch vụ của website hay máy chủ của cơ quan hay tổ chức.



Hình 6.1 - ZeuS là trojan thường dùng để đánh cắp tài khoản ngân hàng trực tuyến

Trong bảng 6.1 là danh sách một số trojan thông dụng và cổng tương ứng mà chúng hoạt động :

Trojan	Protocol (Giao thức vận chuyển)	Port / Cổng
BackOrifice	UDP	31337, 31338
Deep Throat	UDP	2140, 3150
NetBus	TCP	12345, 12346
Whack-a-mole	TCP	12361, 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544

Masters Paradise	TCP	3129, 40421, 40422, 40423, 40426

Bảng 6.1 – Các trojan thông dụng và số hiệu cổng tương ứng

Overt Và Covert Channel

Có hai cơ chế truyền thông trên máy tính hay hệ thống mạng là hợp lệ và bất hợp lệ. Những ứng dụng trò chơi hay các chương trình nghe nhạc, xem phim khi truyền dữ liệu sử dụng co chế truyền hợp lệ qua những kênh truyền gọi là Overt Chennel. Ngược lại, khi hacker điều khiển máy tính của nạn nhân thướng sử dụng các kênh truyền bất hợp lệ Covert Channel. Thành phần client (điều khiển) của Trojan sử dụng covert channel để gởi các chỉ thị đến server (thành phần trojan được cài trên các máy tính bị điều khiển, hay các zombie).

Covert channel dựa trên lỹ thuật gọi là tunneling,trong kỹ thuật này một giao thức sẽ được gói bởi giao thức khác nhằm vượt qua sự kiểm soát của firewall như ICMP tunneling là phương pháp dùng ICMP ECHOrequest và ECHO reply để mang theo các paypload (chương trình mà hacker muốn chạy trên máy nạn nhân). Hoặc các phương pháp tunnling qua giao thức http gọi lại http tunnling, còn nếu như một giao thức được bao bọc bởi giao thức SSH thì gọi là SSh tunneling, một kỹ thuật vượt firewall rất hay được các hacker sử dụng. Các bạn có thể tham khảo một bài viết của tôi về chủ đề này trên Pcworld với tựa đề *"Cách Không Chỉ Điểm" Với SSH Tunneling !*

Công Cụ Tấn Công

> **Loki** là một công cụ tấn công cho phép truy cập ở mức cao vào trình điều khiển lệnh dựa trên ICMP, khiến cho việc phát hiện chúng trở nên khó khăn hơn các backdoor thông thường dựa trên TCP hay UDP.

Các Loại Trojan

Trojan có thể được sử dụng cho nhiều dạng tấn công khác nhau từ đánh cắp dữ liệu cho đến chạy chương trình từ xa, tấn công từ chối dịch vụ …Có nhiều dạng trojan khac nhau mà các bạn cần lưu ý trong chương trình CEH :

- **Remote Access Trojan (RAT)** — dùng để truy cập từ xa vào hệ thống

- **Data-Sending Trojan** — dùng để đánh cắp dữ liệu trên hệ thống và gởi về cho hacker.

- **Destructive Trojan** — sử dụng để phá hủy tập tin trên hệ thống

- **Denial of Service Trojan** — dùng để phát động các đợt tấn công từ chối dịch vụ.

└ **Proxy Trojan** —được dùng để tạo ra các vỏ bọc truyền thông (tunnel) hay phát động tấn công từ một hệ thống khác.

└ **FTP Trojan** — dùng để tạo ra dịch vụ FTP nhằm sao chép dữ liệu lên hệ thống bị nhiễm.

└ **Security software disabler Trojan** — dùng để tắt các dịch vụ phòng chống virus, trojan.

Các Trojan Và Backdoor Cần Quan Tâm

TROJ_OAZ là một trojan thay đổi tên chương trình notepad.cexe thanh note.com sau đó sao chép chính nó thành notepad.exe vào thự mục hệ thống của Windows. Như vậy mỗi khi chúng ta mở chương trình notepad thì trojan cũng hoạt động và mở công hậu (backdoor) 7597 để hacker có thể thâm nhập vào máy tính từ xa. TROJ_OAZ còn nhiễm vào registry để nạp khi máy tính khởi động.

Tini là một trojan có kích thươc rất nhỏ và đơn giãn hoạt động trên hệ điều hành Windows chuyên lắng nghe trên cổng 7777 cho phép hacker chạy lệnh từ xa thông qua chương trình telnet đến cổng này trên các máy tính bị lây nhiễm.

Donald Disk là một dạng backdoor Trojan trên hệ thống Windows cho phép hacker toàn quyền kiểm soát qua môi trường internet. Hacker có thể đọc, ghi, xoa hay chạy bất kì ứng dụng nào trên hệ thống. Donald Disk kèm thoe cả keylogger để bắt tín hiệu bàn phím và thay đổi registry để thực hiện các hành động như đóng mở khay CD-ROM. . Donald Disk hoạt động trên các cổng mặc định 23476 hay 23477

NetBus là một chương trình Trojan với giao diện đồ họa (đa số các trojan ngày nay đều dùng các cữa sở đồ họa được thiết kế rõ ràng giúp cho hacker dễ dàng sử dụng), netbus có chức năng tương tự như Donald Disk trong việc điều khiển máy tính từ xa. Đây cũng là một ứng dụng tôi đã dùng để "nghịch" một chút trên máy tính của đồng nghiệp trước đây làm cho chủ nhân của máy tính bị nhiễm rất ngạc nhiên khi thấy khe CD-ROM bị đóng mở liên tục mà không biết tại sao, cứ cho rằng bị hư phần cứng. Trong tình huống thử nghiệm này tôi sử dụng một file hình ảnh để đính kèm trojan. Netbus thêm một khóa vào registry tại *HKEY_CURRENT_USER\NetBus Server* và thay đổi giá trị cổng tại *HKEY_CURRENT_USER\NetBus Server\General\TCPPort* . Nếu NetBus được cấu hình chạy tự động trên máy tính bị nhiễm sẽ xuất hiện khóa tên là NetBus Server Pro tại HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

ComputerSpy Key Logger đây là ứng dụng lưu lại các tín hiệu bàn phím để thu thập các thông tin đăng nhập của người dùng và các trang như ICQ, MSN, AOL, AIM và Yahoo Messenger hay webmail. Ngoài ra công cụ này có thể màn hình theo những khoảng thời gian xác định.

Beast là trojan chạy tại bộ nhớ cấp phát cho dịch vụ WinLogon.exe, một khi được cài chương trình sẽ tự chèn chính nó vào Windows Explorer hay Internet Explorer. Beast thuộc dạng trojan tất cả trong một (all in one) vì các thành phần server, client và server editor đề nằm trên cùng một ứng dụng.

CyberSpy thuộc dạng telnet trojan có khả năng sao chép chính nó vào thư mục hệ thống của Windows cũng như tự đăng kí trong registry để có thể chạy khi hệ thống khởi động. Một khi được cài CyberSpy sẽ thông báo cho hacker biết cổng đang lắng nghe qua email hay ICQ.

SubRoot là trojan quản trị từ xa mà hacker có thể dùng để điều khiển máy tính bị nhiễm qua cổng 1700

LetMeRule cũng thuộc loại trojan quản trị từ xa (RAT) và có thể lắng nghe trên bất kì cổng nào trên máy tính bị lây nhiễm, cho phép hacker xóa hay thực thi tập tin trên máy tính nạn nhân, xem và sữa đổi registry hay điều khiển máy tính này thông qua dòng lệnh.

Firekiller 2000 có chức năng tắt các chương trình chống virus và ứng dụng tường lữa. Một khi bị nhiễm mã độc này các chương trình phòng vệ sẽ mất tác dụng, buộc lòng phải gỡ ra và cài lại chúng sau khi đã quét trojan/backdoor sạch sẽ từ chế độ safemode hay trên các đĩa khởi động DVD/CD.

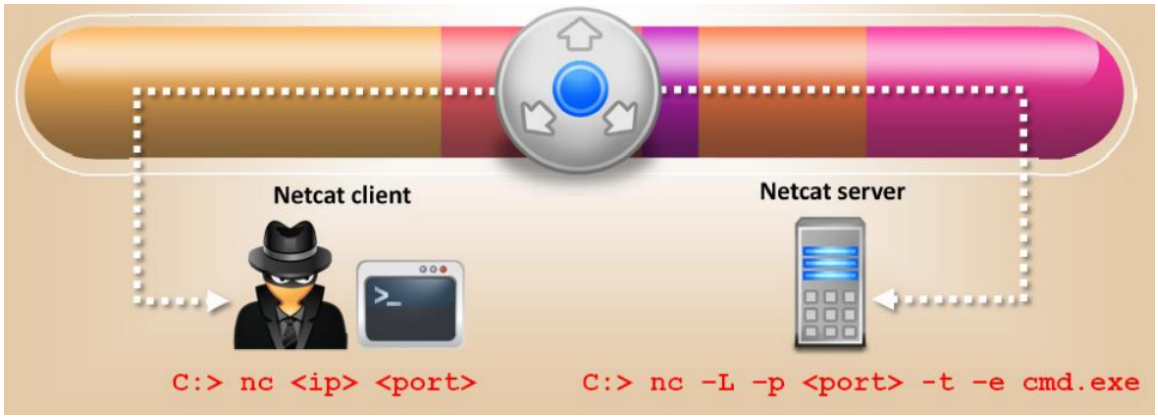
Hard Drive Killer Pro có chứ cna8ng phá hũy toàn bộ dữ liệu trên các hệ thống DOS hay Windows.

BackOrifice 2000 là một công cụ điều khiển từ xa với giao diện đồ họa, BackOrifice không xuất hiện trong danh sách các tiến trình hay tasklist. Cũng như các trojan mạnh mẽ khác no có khả năng thêm các khóa trong registry để chạy khi máy tính khởi động. Bên cạnh đó BackOrifice còn có các plug in hỗ trỡ nhưng chức năng như mã hóa với giao thức mạnh mẽ 3DES, điều khiển desktop từ xa bằng chuột hay bàn phím …

Netcat Trojan Và Những Chức Năng Thông Dụng

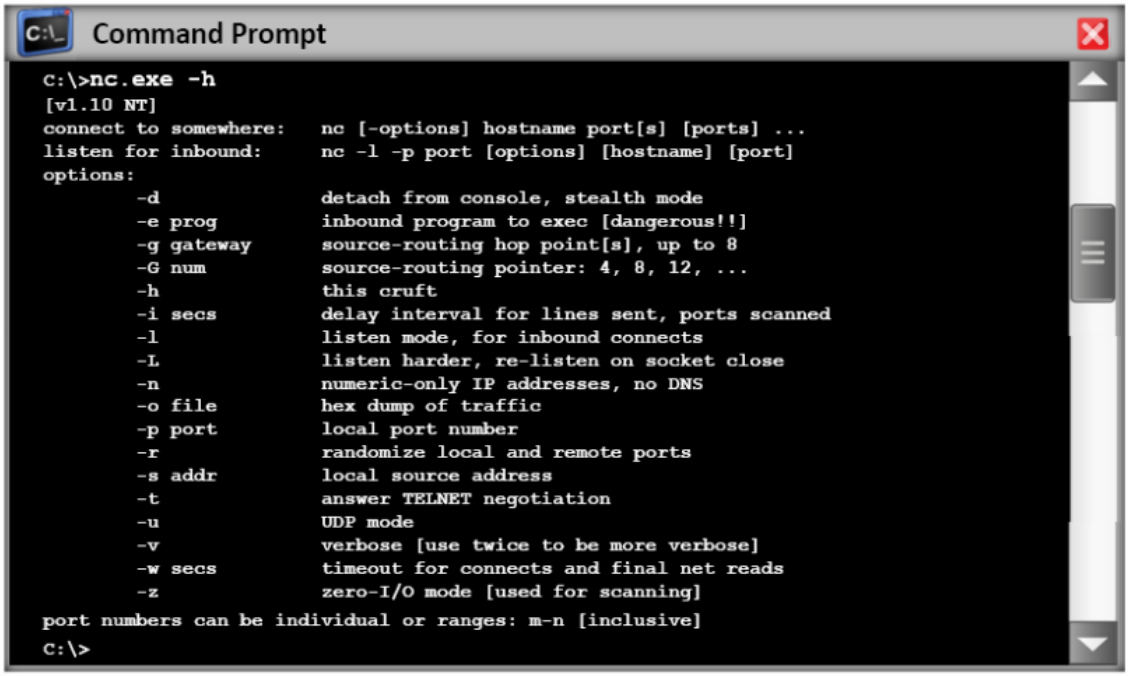
Netcat là một trojan dạng dòng lệnh nhưng khá mạnh mẽ và dễ sử dụng. Trước đây, Netcat được xem như một công cụ "sạch" nhưng do bị các hacker sử dụng nhiều vào các mục tiêu không trong sáng nên hiện nay hầu hết chương trình phòng chống virus đều đưa Netcat vào danh sách đen. Công cụ này có khả năng mở những cổng TCP hay UDP trên máy tính bị nhiễm, và hacker sử dụng chương trình telnet để kết nối tới các cổng đã mở

và thực hiện nhiều thao tác nguy hiểm như truyền file, thực thi lệnh. Netcat có thể chạy trên hệ thống Windows cũng như Linux, tương tác theo mô hình client / server như minh họa trong Hình 6.2 :



Hình 6.2 – Netcat

Để xem các tùy chọn của Netcat hãy chạy lệnh nc.exe –h như Hình 6.3 :



Hình 6.3 – Các tùy chọn của Netcat

Ví dụ các bạn muốn tạo một kênh chat giữa hai máy với netcat server (có IP là192.168.0.1) và netcat client thì chúng ta sẽ lắng nghe trên cổng xác định ví dụ 3333 trên máy có địa chỉ là 192.168.0.1 với lệnh :

```
C:\nc.exe -l 3333
```

Trên máy còn lại hãy kết nối thông qua lệnh :

```
C:\nc.exe 192.168.0.1 3333
```

Truyền Tập Tin Với Netcat

Với Netcat ta có thể truyền tập tin dễ dàng, lấy ví dụ hai máy ở trên cần truyền tập tin backup.iso từ máy 192.168.0.1 (server) về máy 192.168.0.1 thì đầu tiên chúng ta chạy lệnh trên máy đóng vai trò server

```
C:\ cat backup.iso | nc -l 3333
```

Để nhận tập tin backup.iso trên client hãy chạy lệnh:

```
C:\ nc 192.168.0.1 3333 > backup.iso
```

Dùng Netcat Như Là Công Cụ Quét Cổng

Một chức năng thú vị khác của Netcat là khả năng quét các cổng đang mở trên những ma1yti1nh ở xa thông qua tùy chọn –z. Không như các ứng dụng quét cổng khác Netcat không khởi tạo kết nối đến máy từ xa mà chỉ nhận dạng những cổng đang mở, ví dụ ta muốn kiểm tra xem các cổng từ 80 đến 90 trên máy 192.168.0.1 hãy sử dụng lệnh :

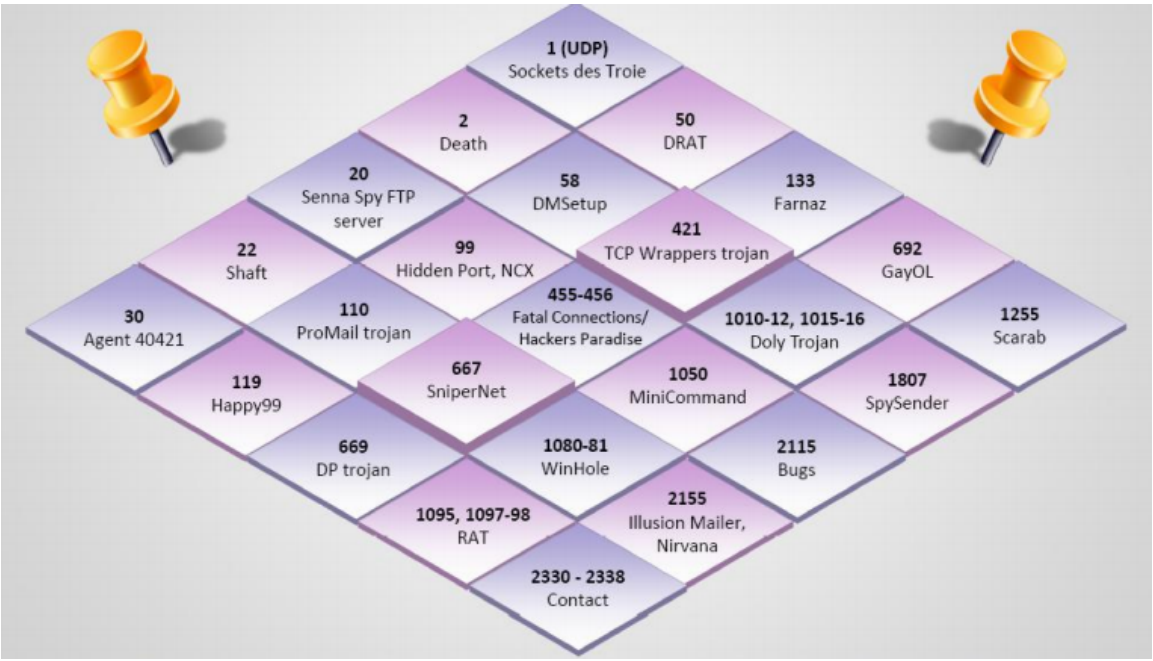
```
C:\ nc -z 192.168.0.1 80-90
Connection to 192.168.0.1 80 port [tcp/http] succeeded!
```

Kết quả cho thấy cổng 80 đang mở và dịch vụ tcp/http đang hoạt động.

Nhận Biết Máy Tính Bị Nhiễm Trojan Như Thế Nào ?

Ngoài việc sử dụng các chương trình diệt virus được cập nhật đầy đủ như Avast, Kaspersky, Nob32 …thì chúng ta có thể căn cứ vào những hành vi bất thường của máy tính như các thông báo lỗi lạ, CDROM hoạt động đóng mở tự động cho chúng ta biết máy tính đang có vấn đề và có khả năng bị lây nhiễm trojan / backdoor.

Chúng ta còn có thể giám sát các cổng trên hệ thống Windows với lệnh như ***C:\netstat –na*** để xem những cổng lạ nào đang mở, nếu có những cổng như trong hình minh họa sau thì có lẽ máy tính đa bị nhiễm mã độc.



Hình 6.4 – Các cổng tương ứng với chương trình nguy hiểm

Ngoài ra, việc sử dụng các chương trình giám sát mạng như Wireshark để phát hiện những kết nối bất hợp lý, những truyền thông khả nghi là biện pháp rất tốt để phát hiện các trojan / backdoor tinh vi. Vì nhiều mã độc có khả năng ẩn mình qua mặt cả những chương trình diệt virus, không xuất hiện trong danh sách task list hay các tiến trình đang chạy nhưng khi chúng truyền thông với hacker để nhận lệnh thì các gói tin này không thể nào qua mặt được những ứng dụng giám sát đường truyền như Wireshark, đây cũng là phương pháp tôi tư vấn cho một số học viên trước đây làm việc tại Bộ tài chính để phát hiện ra các trojan nguy hiểm chuyên đánh cắp dữ liệu và gởi sang một máy chủ đặt tại nước ngoài. Cũng vì sự hữu ích của mình mà hiện nay Wireshark được xếp số 1 trong 125 công cụ bảo mật hàng đầu trên trang www.sectools.org. Các bạn có thể xem phần giới thiệu về những công cụ bảo mật hàng đầu thế giới tại đây http://youtu.be/R3CUulCG1tA

Thế Nào Là “Wrapping” ?

Để có thể phát tán các mã độc hay trojan / backdoor hacker thường đính kèm những công cụ này vào những công cụ hợp lệ khác, ví dụ như thời gian gần đây website unikey.org bị hacker tấn công và chèn mã độc vào chương trình này để khi người dùng download ứng dụng unikey về máy cài đặt sẽ vô tình cài luôn chương trình nguy hiểm của hacker. Và những ứng dụng cho phép gắn một trojan hay backdoor vào một chương trình khác được gọi là các wrapper và quá trình này gọi là Wrapping hay đóng gói.

Những công cụ đóng gói trojan :

- **Graffiti** là một chương trình game hoạt họa có thể dùng để gói một trojan và khi người dùng tải về máy tính để chơi thì sẽ cài luôn cả trojan được đóng gói.
- **Silk Rope 2000** là một wrapper kết hợp *BackOrifice* server và một ứng dụng thông thường khác.
- **EliTeWrap** là ứng dụng cao cấp chuyên đóng gói các chương trình .exe hoạt động trên hệ thống Windows. EliteWrap có thể tạo ra những ứng dụng cài đặt để có thể bung nén vào những thư mục đã được chỉ định.
- **IconPlus** là ứng dụng dùng để chuyển đổi các icon theo nhiều định dạng khác nhau cũng được các hacker dùng cho việc phân tán các mã độc nguy hiểm.
- Ngoài ra, có một ứng dụng hữu ích là chương trình **AutoIT** cho phép người dùng tạo ra các công cụ hay những script theo các lệnh và hàm thư viên của Windows. Mặc dù đây là một công cụ hữu ích nhưng lại bị nhiều hacker Việt Nam lạm dụng để tạo ra các công cụ nguy hiểm như virus Yahoo! Messenger trước đây. Và AutoIt tích hợp sẵn một wrapper là UPX để đóng gói các kịch bản được tạo ra vì vậy ứng dụng diệt virus BKAV đã mặc nhiên xem các chương trình được tạo bằng Auto IT là virus do phát hiện có header của UPX. Tuy nhiên, đây là một dạng "diệt nhầm hơn bỏ sót" vì nhiều chương trình hữu ích được viết bằng Auto IT chứ không phải tất cả ứng dụng tạo bởi Auto It đều xấu ví dụ như kịch bản *lockscreen.exe* do tôi tạo ra để người dùng có thể nhanh chóng khóa màn hình khi rời khỏi bàn làm việc chỉ với một cái click chuột.

Trojan Construction Kit và Trojan Maker

Trojan construction kit va trojan maker là những công cụ mà các hacker dùng để t75 tạo ra các biến thể trojan / backdoor nguy hiểm của riêng mình , với các cấu hình riêng như khởi tạo kết nối trên những kênh IRC riêng, dựa vào các số hiệu cổng mà những chương trình diệt virus hay trojan scanning tool có thể không nhận biết được vì không có những dấu hiệu trùng lắp trong cơ sở dữ liệu do mới được tạo ra.

Một số công cụ dùng để tạo trojan như *Senna Spy Generator, Trojan Horse Construction Kit, Pandora's Box.*

Phòng Chống Trojan

Hầu hết các ứng dụng phòng và diệt virus hiện nay đều có khả năng phòng chống trojan, ngăn ngừa chúng lây nhiễm trên hệ thống máy tính. Tuy nhiên, các bạn nên sử dụng các chương trình antivirus được cập nhật đầy đủ để có thể phát hiện ra các biến thể mới nhất của mã độc. Trong trường hợp sử dụng các chương trình diệt virus miễn phí nên chọn các ứng dụng được đánh giá tốt nhất, như *AVAST ! Antivirus Free* có thể cài trên các hệ

thống Windows XP, Windows 7, Windows Vista hiện tôi đang sử dụng với hiệu quả cao, cảnh báo đầy đủ những virus mới và những website chứa mã độc.

Tuy nhiên, các phiên bản thương mại vẫn có nhiều tính năng mạnh mẽ hơn, khả năng phòng chống trojan cao hơn so với các bản miễn phí. Do đó, nếu đặt yếu tố hiệu quả lên hàng đầu thì nên chọn các sản phẩm thương mại của *AVAST, Kaspersky hay NOB 32*. Bên cạnh đó, kết hợp thêm một phiên bản *BKAV, CMC* miễn phí (hay có phí) nhằm ngăn ngừa những virus nội cũng là một giải pháp đáng quan tâm.

Ngoài ra, chúng ta nên cẩn thận khi sử dụng những phần mềm crack hay chạy các tập tin vá, chương trình lấy *keygen* vì đây là những nguồn lây nhiễm trojan, virus hàng đầu. Trong trường hợp cần cài đặt thử nghiệm những ứng dụng không tin cậy hãy cài trước trên máy ảo để xem có tác hại hay hành động khả nghi nào không (giám sát với các chương trình Wiresharke, Process Monitor, dùng lệnh netstat –na để kiểm soát các session trên máy tính…)

Những Công Cụ Giám Sát Port Và Dò Tìm Trojan

Fport : Công cụ miễn phí của Foundstone báo cáo về tình trạng của tất cả các cổng TCP / UDP đang mở cùng với dịch vụ tương ứng hoạt động trên những cổng này. Hãy ứng dụng Fport để nhanh chóng phát hiện tình trạng hoạt động của cổng và dịch vụ trên máy tính của bạn.

TCP View : Chương trình hoạt động trên hệ điều hành Windows hiển thị chi tiết các điểm đầu cuối tham gia truyền thông trên TCP / UDP bao gồm các địa chỉ local và remote cũng như tình trạng của các kết nối TCP (tại sao chúng ta không nói đến tình trạng của "kết nối UDP", đ1o là do UDP không phải là một giao thức hướng liên kết, cần ghi nhớ để tránh bị bẫy trong các câu hỏi của CEH)

PrcView : Là ứng dụng dùng để giám sát các tiến trình đang hoạt động, đây là công cụ dạng dòng lệnh rất hay, có khả năng kill (đóng) các tiến trình nguy hiểm.

Inzider : Là một ứng dụng hữu ích liệt kê những tiến trình đang hoạt động trên hệ thống Windows và các cổng tương ứng, Inzider có thể phát hiện một số trojan như BackOrifice mặc dù chúng tự chèn vào trong các tiến trình của hệ thống để ẩn trên danh sách của Task list nhưng trojan này vẫn phải mở các cổng xác định.

Tripwire : Ứng dụng trên Linux dùng để kiểm tra tính toàn vẹn của hệ thống tập tin, sử dụng một thuật toán băm để có thể xác định được tình trạng của các tập tin hệ thống và nhận biết khi có sự thay đổi xảy ra. Tripwire tạo ra một thiết lập chuẩn (baseline) của hệ thống và thường xuyên quét các tập tin nếu có sự thay đổi xảy ra sẽ cảnh báo cho quản trị hệ thống.

Phòng Chống Trojan Bằng Cách Kiểm Tra Tính Toàn Vẹn Của tập Tin

Trên hệ thống Windows Server 2003 trở về sau có một tính năng gọi là Windows File Protection (WFP) giúp ngăn ngừa việc thay thế các tập tin được bảo vệ. WFP kiểm tra tính toàn vẹn của tập tin khi có sự tác động đến các tập tin SYS, DLL, OCX, TTF hay EXE. Điều này bảo đảm chỉ có các tập tin đã được xác thực bởi Microsoft mới thay đổi được các tập tin hệ thống.

Ngoài ra, chúng ta có thể sử dụng công cụ sigverif xem các tập tin có được xác thực bởi Microsoft hay không thông qua các thao tác sau :

1. *Click vào nút **Start**.*
2. *Click vào **Run**.*
3. *Nhập vào lệnh **sugverif** và nhấn **Start** kết quả các tập tin được xác thực sẽ hiển thị.*

Hoặc tiến hành kiểm tra tình trạng các tập tin với *System File Checker* qua lệnh ***sfc / scannow*** để phát hiện những tập tin nào bị trojan thay đổi, nếu phát hiện ra *System File Checker* sẽ phục hồi chúng từ thư mục *Windows\system32\dllcache* .

Tổng Kết

Như vậy, trong chương này chúng ta đã tìm hiểu về ***trojan*** và ***backdoor*** với những đặc điểm khác biệt của chúng. Các bạn cần ghi nhớ những cổng thông dụng mà trojan hay backdoor thường sủ dụng cũng như các phương pháp dùng để kiểm tra sự có mặt của các phần mềm độc hại này.

Trong các câu hỏi của bài thi chứng chỉ CEH thường hay đề cập đến những cổng mà trojan như *Subseven, BackOrofice* hay *Netbus* hoạt động, và những điểm lưu ý khác là các tùy chọn quan trọng của trojan Netcat.