Module 6

Enumeration

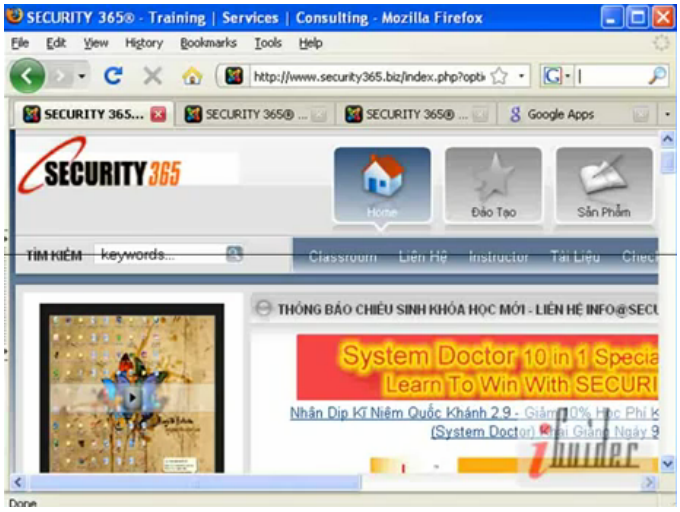
Những Nội Dung Chính Được Trình Bày

Enumeration Là Gì?

Null Session

SNMP Enumeration

Active Directory Enumeration



Enumeration hay Liệt kê là bước tiếp theo trong quá trình tìm kiếm thông tin của tổ chức, xảy ra sau khi đã scanning được dùng để tập hợp và phân tích tên người dùng, tên máy, tài nguyên chia sẽ cùng các dịch vụ. Quá trình này cũng chủ động truy vấn hoặc kết nối tới mục tiêu để có được những thông tin mà các hacker quan tâm.

Enumeration Là Gì?

Enumeration có thể được định nghĩa là quá trinh trích xuất những thông tin có được trong phần scan ra thành một hệ thống có trật tự. Những thông tin được trích xuất bao gồm những thứ có liên quan đến mục tiêu cần tấn công, như tên người dùng (user name), tên máy tính (host name), dịch vụ (service), tài nguyên chia sẽ (share).

Các bạn có thể tham khảo thêm về Enumeration tại bài giảng http://youtu.be/r6wP_yi-dak

Những kỹ thuật liệt kê được điều khiển từ môi trường bên trong.

Enumeration bao gồm cả công đoạn kết nối đến hệ thống và trực tiếp rút trích ra các thông tin.

Mục đích của kĩ thuật liệt kê là xác định tài khoản người dùng và tài khoản hệ thống có khả năng sử dụng vào việc hack một mục tiêu. Không cần thiết phải tìm một tài khoản quản trị vì chúng ta có thể tăng tài khoản này lên đến mức có đặc quyền nhất để cho phép truy cập vào nhiều tài khoản hơn đã cấp trước đây.

Các kỹ thuật được sử dụng trong liệt kê có thể kể ra như:

Kỹ thuật Win2k Enumeration : dùng để trích xuất thông tin tài khoản người dùng (user name).

Kỹ thuật SNMP (Simple Network Management Protocol) để liệt kê thông tin người dùng.

Kỹ thuật Active Directory Enumeration dùng trong liệt kê hệ thống Active Directory.

Null Session là gì?

Khi người dùng đăng nhập vào hệ điều hành, hệ thống sẽ yêu cầu chứng thực với các thông tin username và password. Sau quá trình chứng thực, một danh sách truy cập – ACL – được tải về để xác định quyền hạn của user đăng nhập. Nó một cách khác, quá trình đó tạo cho user một phiên làm việc rõ ràng. Tuy nhiên, có những dịch trong hệ điều hành được kích hoạt tự chạy, với một user ẩn danh nào đó, chẳng hạn như SYSTEM USER. Các user này không cần có password được dùng để khởi chạy các dịch vụ ví dụ dịch vụ tìm kiếm tài nguyên chia sẽ khi các bạn chọn chức năng duyệt trong Explorer, lúc này chúng ta đang sử dụng các dịch vụ thuộc dạng Null Session.

Những dịch vụ sử dụng giao thức NetBIOS cũng sử dụng kết nối thuộc dạng Null Session. Một trong những phương pháp kết nối Null Session, hay được gọi là IPC$ trên máy chủ nền tảng Windows, là một dạng kết nối nặc danh tới một mạng chia sẻ cho phép người dùng trong mạng truy cập tự do.

Tấn công Null Session đã xuất hiện kể từ khi Windows 2000 được sử dụng rộng rãi. Tuy nhiên, hình thức tấn công này không được các quản trị viên hệ thống chú ý khi áp dụng các biện pháp bảo mật mạng. Điều này có thể dẫn đến kết cục khôn lường vì tin tặc có thể sử dụng hình thức tấn công này để lấy mọi thông tin hữu dụng cần thiết để giành quyền truy cập từ xa vào hệ thống. Mặc dù không còn mới mẻ, nhưng tấn công Null Session vẫn phổ biến và nguy hiểm như những năm trước đây. Xét về một khía cạnh nào đó, mặc dù khả năng bảo mật của các hệ thống hiện đại không phải quá yếu nhưng khi thực hiện các cuộc thử nghiệm xâm nhập trên máy tính Windows thì kết quả cho thấy Null Session vẫn là một trong những hình thức cần lưu ý.

Phương thức hoạt động của Null Session

Một phiên truy cập từ xa được tạo lập khi người dùng đăng nhập từ xa vào một máy tính sử dụng một tên người dùng và mật khẩu có quyền truy cập vào tài nguyên hệ thống. Tiến trình đăng nhập này được thực hiện qua giao thức SMB (Server Message Block) và dịch vụ Windows Server. Những kết nối này hoàn toàn hợp pháp khi những thông tin đăng nhập chính xác được sử dụng.

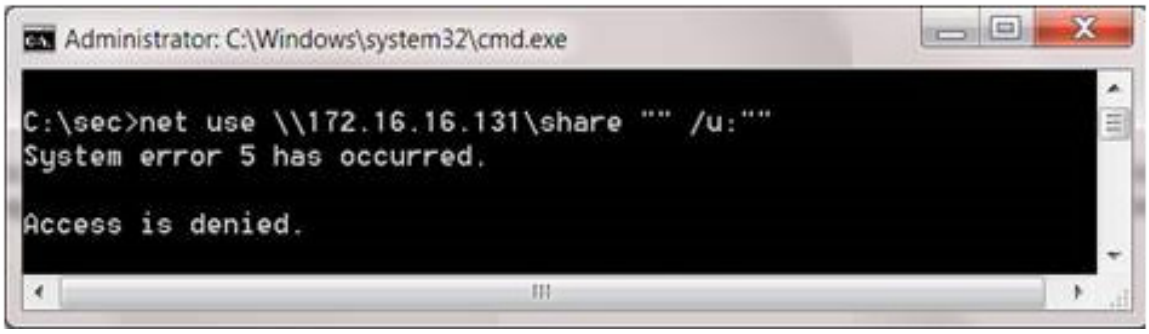
Một Null Session xảy ra khi người dùng thực hiện kết nối tới một hệ thống Windows mà không sử dụng tên người dùng hay mật khẩu. Hình thức kết nối này không thể thực hiện trên bất kỳ hình thức chia sẻ Windows thông thường nào, tuy nhiên lại có thể thực hiện trên chia sẻ quản trị IPC (Interprocess Communication). Chia sẻ IPC được các tiến trình của Windows sử dụng (với tên người dùng là SYSTEM) để giao tiếp với các tiến trình khác qua mạng này. Chia sẻ IPC chỉ được giao thức SMB sử dụng.

Chia sẻ không yêu cầu thông tin đăng nhập IPC thường được sử dụng cho những chương trình giao tiếp với một chương trình khác, tuy nhiên không có gì đảm bảo rằng người dùng không thể kết nối tới một máy tính bằng kết nối IPC này. Kết nối IPC không chỉ cho phép truy cập không giới hạn vào máy tính, mà còn trao quyền truy cập vào tất cả các máy tính trên mạng, và đây là những gì mà tin tặc cần để xâm nhập hệ thống.

Tham khảo bài trình bày về Null Session tôi trình bày tại địa chỉ http://youtu.be/Tqb_IVKCROU

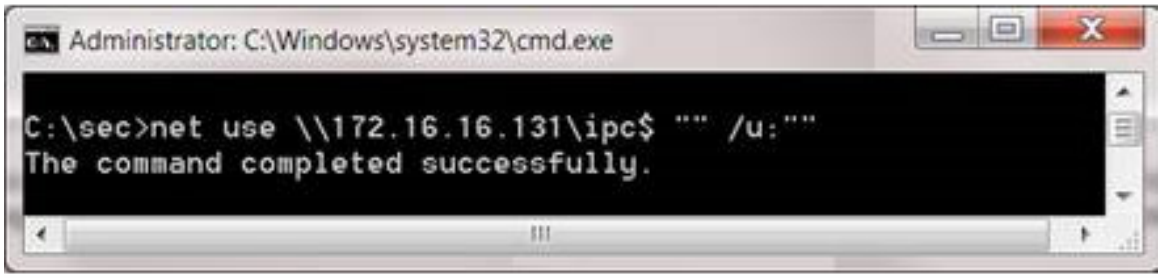
Phương thức tấn công sử dụng Null Session

Giờ đây chúng ta đã biết cách thức hoạt động của Null Session, tuy nhiên ‘liệu tin tặc có thể sử dụng hình thức tấn công này dễ dàng hay không?’ Câu trả lời là ‘khá dễ dàng’. Kết nối Null Session có thể được thiết lập trực tiếp từ một lệnh Windows mà không cần sử dụng công cụ bổ sung, đó chính là lệnh NET. Lệnh NET có thể thực hiện nhiều chức năng quản trị, khi sử dụng lệnh này chúng ta có thể tạo một kết nối tới một chia sẻ tiêu chuẩn trên máy chủ đích, tuy nhiên kết nối này sẽ thất bại do những thông tin đăng nhập không chính xác.



Hình 4. 1: Kết nối thất bại vào một mạng chia sẻ sử dụng lệnh NET.

Khi sử dụng lệnh NET, chúng ta có thể thay đổi tên chia sẻ kết nối tới chia sẻ quản trị IPC$. Khi đó kết quả sẽ khả quan hơn.



Hình 4 2: Kết nối Null Session thành công với lệnh NET.

Lúc này, chúng ta đã thiết lập một kết nối Null Session tới máy tính nạn nhân. Tuy nhiên, chúng ta vẫn chưa có quyền truy cập quản trị trên máy tính này do đó chưa thể bắt đầu duyệt tìm ổ cứng hay lấy mật khẩu. Cần nhớ rằng, chia sẻ IPC được sử dụng để giao tiếp giữa các tiến trình, do đó quyền truy cập của chúng ta sẽ bị giới hạn xuống quyền truy cập của tên người dùng SYSTEM. Chúng ta có thể sử dụng lệnh NET để lấy nhiều thông tin hơn từ máy tính mục tiêu, tuy nhiên có nhiều công cụ tự động hóa sẽ thực hiện các công việc rắc rối này.

Công Cụ

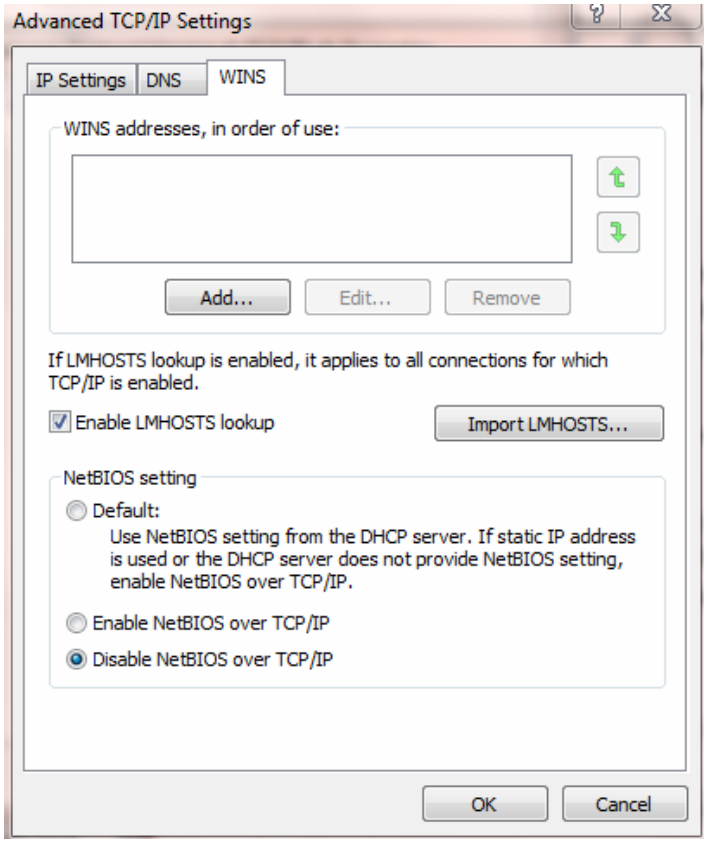
Null Session có thể dễ dàng tấn công với công cụ có sẵn trong windows như Net, Netview.

Tuy nhiên, như đã trình bày ở trên, chúng ta cần một quá trình phúc tập hơn để làm được nhiều việc, như liệt kê thư mục, user…Công cụ Nbtstat và Enum sẽ giúp chúng ta thực hiện hàng loạt các công việc phức tạp, để cuối cùng chúng ta xâp nhập được vào hệ thống. Dumpsec và Superscan là hai công cụ đồ họa hổ trợ thực hiện các công việc này.

Chống tấn công bằng Null Session

Null Session sử dụng các cổng TCP 135, 137,139, hay 445 vì vậy đóng các cổng này là một trong những cách để chặn các kết nối null session. Tuy nhiên, máy tính của chúng ta sẽ không thể chia sẽ tài nguyên cho người dùng khác khi đóng những cổng này. Trên các hệ thống tường lữa hay gateway của hệ thống

mạng các quản trị hệ thống hay tắt chức năng NetBIOS bằng cách mở trang thuộc tính của card mạng và chọn tab WINS trong Advance TCP/IP Settings và chọn Disable NetBIOS over TCP/IP như Hình 4.1



Hình 4.1 – Disable NetBIOS over TCP/IP

Chặn Null Session Trong Registry

Chúng ta có thể chặn Null Session bằng cách thêm vào một khóa có kiểu REG_WORD với giá trị bằng 2 trong Registry như sau :

1. Mở regedt32, di chuyển đến HKLM\SYSTEM\CurrentControlSet\LSA.

2. Chọn Edit ┘ Add Value. Và nhập vào giá trị :

└ Tên : RestrictAnonymous

└ Kiểu : REG_WORD

└ Giá trị: 2

Phát Hiện Null Session với IDS

Nếu những thay đổi trong Registry hay Firewall loại bỏ chức năng của các ứng dụng mạng thì chúng ta phải sử dụng một phương pháp khác. Thay vì chặn thống kê qua Null Session, một trong những biện pháp hữu hiệu nhất đó là phát hiện ra tấn công Null Session một cách sớm nhất để có thể triển khai những biện pháp khắc phục kịp thời như khi thực hiện một sự kiện bảo mật mạng thông thường.

Nếu đang sử dụng Snort, một IDS/IPS (Hệ thống phát hiện và chặn xâm nhập mạng) phổ biến nhất hiện nay trong môi trường sản xuất, thì rule sau đây sẽ phát hiện thống kê Null Session:

alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"NETBIOS NT NULL session"; flow:to_server.establshed;

content: '|00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4E 00 54 00 20 00 31 00 33 00 38 00 31|'; classtype:attempted-recon;)

Rule này sẽ không ngăn chặn các kết nối Null Session, tuy nhiên nó sẽ thông báo khi Null Session xảy ra.

Nâng cấp hệ điều hành

Giải pháp cuối cùng như đã đề cập ở trên là nâng cấp hệ điều hành. Null Session chỉ dễ dàng thực hiện với hệ điều hành đời cũ trước năm 2000. Còn sau đó như Windows XP, Windows 2003 thì việc này đã được Microsoft tích hợp trong sản phẩm. Do đó, nâng cấp hệ điều hành làm chúng ta yên tâm hơn.

Bài giới thiệu về NetBIOS Nul Session tại http://youtu.be/iiNNPI6xs98

Kĩ thuật liệt kê SNMP (Simple Network Management Protocol)

Tìm hiểu về SNMP

SNMP là "giao thức quản lý mạng đơn giản", viết tắc của "Simple Network Management Protocol". Thế nào là giao thức quản lý mạng đơn giản ? Giao thức là một tập hợp các thủ tục mà các bên tham gia cần tuân theo để có thể giao tiếp được với nhau. Trong lĩnh vực thông tin, một giao thức quy định cấu trúc, định dạng (format) của dòng dữ liệu trao đổi với nhau và quy định trình tự, thủ tục để trao đổi dòng dữ liệu đó. Nếu một bên tham gia gửi dữ liệu không đúng định dạng hoặc không theo trình tự thì các bên khác sẽ không hiểu hoặc từ chối trao đổi thông tin. SNMP là một giao thức, do đó nó có những quy định riêng mà các thành phần trong mạng phải tuân theo. Một thiết bị hiểu được và hoạt động tuân theo giao thức SNMP được gọi là "có hỗ trợ SNMP" (SNMP supported) hoặc "tương thích SNMP" (SNMP compartible).

SNMP dùng để quản lý, nghĩa là có thể theo dõi, có thể lấy thông tin, có thể được thông báo, và có thể tác động để hệ thống hoạt động như ý muốn. VD một số khả năng của phần mềm SNMP:

Theo dõi tốc độ đường truyền của một router, biết được tổng số byte đã truyền/nhận.

Lấy thông tin máy chủ đang có bao nhiêu ổ cứng, mỗi ổ cứng còn trống bao nhiêu.

Tự động nhận cảnh báo khi switch có một port bị down.

Điều khiển tắt (shutdown) các port trên switch.

SNMP Enumeration

Kĩ thuật SNMP Enumeration là quá trình sử dụng SNMP để liệt kê các tài khoản người dùng trên một hệ thống mục tiêu. Hầu hết tất cả các thiết bị hạ tầng mạng, như router,switch và bao gồm cả hệ thống Windows, chứa đựng một SNMP agent để quản lý hệ thống hoặc thiết bị. Các trạm quản lý SNMP gửi yêu cầu tới các agent và agent trả lời lại.Các yêu cầu và các sự trả lời được gửi đến các biến truy cập cấu hình bởi phần mềm agent. Các trạm quản lý có thể luôn gửi các yêu cầu để thiết lập giá trị cho các biến nhất định. Các trạm quản lý nhận gói Trap từ agent để biết một vài điều quan trọng vừa xảy ra trên phần mềm agent như có sự khởi động lại hay một lỗi giao diện.

SNMP có hai password sử dụng để truy cập và cấu hình SNMP agent từ trạm quản lý. Cái đầu tiên được gọi là "read community string", password này cho phép bạn xem cấu hình của thiết bị hoặc hệ thống. Cái thứ hai được gọi là "read/write community string", nó được dùng để thay đổi hay chỉnh sức cấu hình trên thiết bị. Nói chung, mặc định read community string là public, còn read/write community string là private. Một lỗ hổng bảo mật phổ biến xảy ra khi các community string không thay đổi so với các thiết lập mặc định. Một hacker có thể sử dụng những password mặc định để xem hoặc thay đổi cấu hình trên thiết bị.

Nếu bạn có bất kì câu hỏi về việc làm cách nào để xác định password mặc định của các thiết bị ,truy cập vào www.defaultpassword.com.

Công Cụ

SNMPUtil và Network Browser là các công cụ liệt kê SNMP.

SNMPUtil tập trung thông tin về tài khoản người dùng qua SNMP trong các hệ thống Windows. Một vài thông tin như các bảng về các công việc hàng ngày,các bảng ARP,địa chỉ IP,địa chỉ MAC, các cổng mở TCP và UDP, tài khoản người dùng và các phần chia sẽ có thể bị đọc từ một hệ thống Windows nơi SNMP cho phép sử dụng công cụ SNMPUtil.

IPNetworkBrowser từ các công cụ SolarWinds cũng sử dụng SNMP để thu thập thêm thông tin về một thiết bị có một SNMP agent.

Đối phó với kỹ thuật liệt kê SNMP

Cách đơn giản nhất để ngăn chặn kỹ thuật liệt kê SNMP là gỡ bỏ các SNMP agent hoặc tắt dịch vụ SNMP. Nếu không được chọn tắt SNMP, hãy thay đổi tên mặc định read và read/write community. Thực thi bảo mật trong "Group Policy" thêm điều kiện ngăn ngừa kết nối người dùng nặc danh.

Active Directory Enumeration

Active Directory (AD) là gì ?

Active Directory là một cơ sở dữ liệu của các tài nguyên trên mạng (còn gọi là đối tượng) cũng như các thông tin liên quan đến các đối tượng đó. Tuy vậy, Active Directory không phải là một khái niệm mới bởi Novell đã sử dụng dịch vụ thư mục (directory service) trong nhiều năm rồi.

Mặc dù Windows NT 4.0 là một hệ điều hành mạng khá tốt, nhưng hệ điều hành này lại không thích hợp trong các hệ thống mạng tầm cỡ xí nghiệp. Đối với các hệ thống mạng nhỏ, công cụ Network Neighborhood khá tiện dụng, nhưng khi dùng trong hệ thống mạng lớn, việc duyệt và tìm kiếm trên mạng sẽ là một ác mộng (và càng tệ hơn nếu bạn không biết chính xác tên của máy in hoặc Server đó là gì). Hơn nữa, để có thể quản lý được hệ thống mạng lớn như vậy, bạn thường phải phân chia thành nhiều domain và thiết lập các mối quan hệ uỷ quyền thích hợp. Active Directory giải quyết được các vấn đề như vậy và cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp. Lúc này, dịch vụ thư mục trong mỗi domain có thể lưu trữ hơn mười triệu đối tượng, đủ để phục vụ mười triệu người dùng trong mỗi domain.

Chức năng của Active Directory

Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.

Cung cấp một Server đóng vai trò chứng thực (authentication server) hoặc Server quản lý đăng nhập (logon Server), Server này còn gọi là domain controller (máy điều khiển vùng).

Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (index) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng.

Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (rights) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền backup dữ liệu hay shutdown Server từ xa…

Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (subdomain) hay các đơn vị tổ chức OU (Organizational Unit). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

Active Directory Enumeration

Liệt kê trong AD có nghĩa là truy vấn tìm kiếm những thông tin có liên quan đến AD và các server trong Windows ứng dụng qua AD. Những kỹ thuật dưới đây chúng ta sẽ tìm hiểu các kỹ thuật liệt kê NTP, WEB, DNS, LDAP…

User Account Enumeration

Có nghĩa là liệt kê những thông tin có liên quan đến user, như username, phone, mail, first name, address…Những thông tin có liên quan khi bạn thực hiện một hình thức tấn công khác. Ví dụ như bạn muốn dò tìm mật khẩu của user thì hãy nhớ một quy tắc, user thường đặt mật khẩu là những gì có liên quan đến mình như ngày sinh, số điện thoại, số nhà, số xe…

Các bạn xem thêm bài trình bày về User Account Enumeration tại http://youtu.be/kcc51MiKXho

Công Cụ

Sid2user và User2sid là hai công cụ dạng dòng lệnh giúp bạn liệt kê các thông tin có liên đến user.

GetAcct là chương trình dạng đồ họa, cho phép bạn tìm kiếm thông tin user trên hệ điều hành Win NT và 2000

Tổng kết

Sau khi kết thúc chương này bạn cần nắm rõ các vấn đề sau:

Hiểu rỏ về liệt kê thông tin user account: Bằng cách tạo ra kết nối đến hệ thống đích bằng giao thức NetBIOS để truy vấn thông tin hệ thống. Trình bày được những thông nào có thể liệt kê từ hệ thống. Những thông đó bao gồm tài nguyên mạng chia sẽ, user, group và những ứng dụng.

Lý giải Null Session là gì? Và những kỹ tấn công dựa trên null session. Kết nối đến hệ thống bằng password trắng là Null Session. Hacker kết nối đến hệ thống đích để thực thi những ứng dụng.

Các công cụ dùng để liệt kê. Có thể chia hai loại. Loại dùng NetBIOS, loại dùng SNMP như SNMP Until, Enum….