



# Ethical Hacking and Countermeasures

Version 6



## Module VI

## Enumeration

Dennis has just joined a Security Sciences Certification program. During his research on organizational security, Dennis came through the term enumeration. While reading about enumeration, a wild thought flashed in his mind.

Back home he searched over the Internet for enumeration tools. He downloaded several enumeration tools and stored them in a flash memory. Next day in his library when nobody was around he ran enumeration tools across library intranet.

He got user names of several library systems and fortunately one among them was the user name used by one of his friends who was a premium member of the library. Now it was easy for Dennis to socially engineer his friend to extract his password.

**How will Dennis extract his friend's password?**

**What kind of information Dennis can extract?**

## Computer Memory Vulnerable to Hacking

By JORDAN ROBERTSON – 3 days ago

SAN FRANCISCO (AP) — Want to break into a computer's encrypted hard drive? Just blast the machine's memory chip with a burst of cold air.

That's the conclusion of new research out of Princeton University demonstrating a novel, low-tech way hackers can access even the most well-protected computers, provided they have physical access to the machines.

The Princeton report shows how encryption, long considered a vital shield against hacker attacks, can be defeated by manipulating the way memory chips work. The researchers say the ease of their attack raises fears about the security of laptop computers increasingly used to store sensitive information, from personal banking data, to company trade secrets, to national security documents.

Freezing a dynamic random access memory, or DRAM, chip, the most common type of memory chip in personal computers, causes it to retain data for minutes or even hours after the machine loses power, the report found. That data includes the keys to unlock encryption. Without freezing, the chip loses its contents within seconds.

Hackers can steal information stored in memory by rebooting the compromised machine with a simple program designed to copy the memory contents — before the computer has a chance to purge sensitive data, according to the study.

Laptops left in hibernation or sleep mode, or simply not turned off at all, are the most vulnerable to the new type of attack.

"These risks imply that disk encryption on laptops may do less good than widely believed," according to the report, which was published this week by researchers from Princeton, the Electronic Frontier Foundation digital rights group, and Wind River

Source: <http://ap.google.com/>

Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited

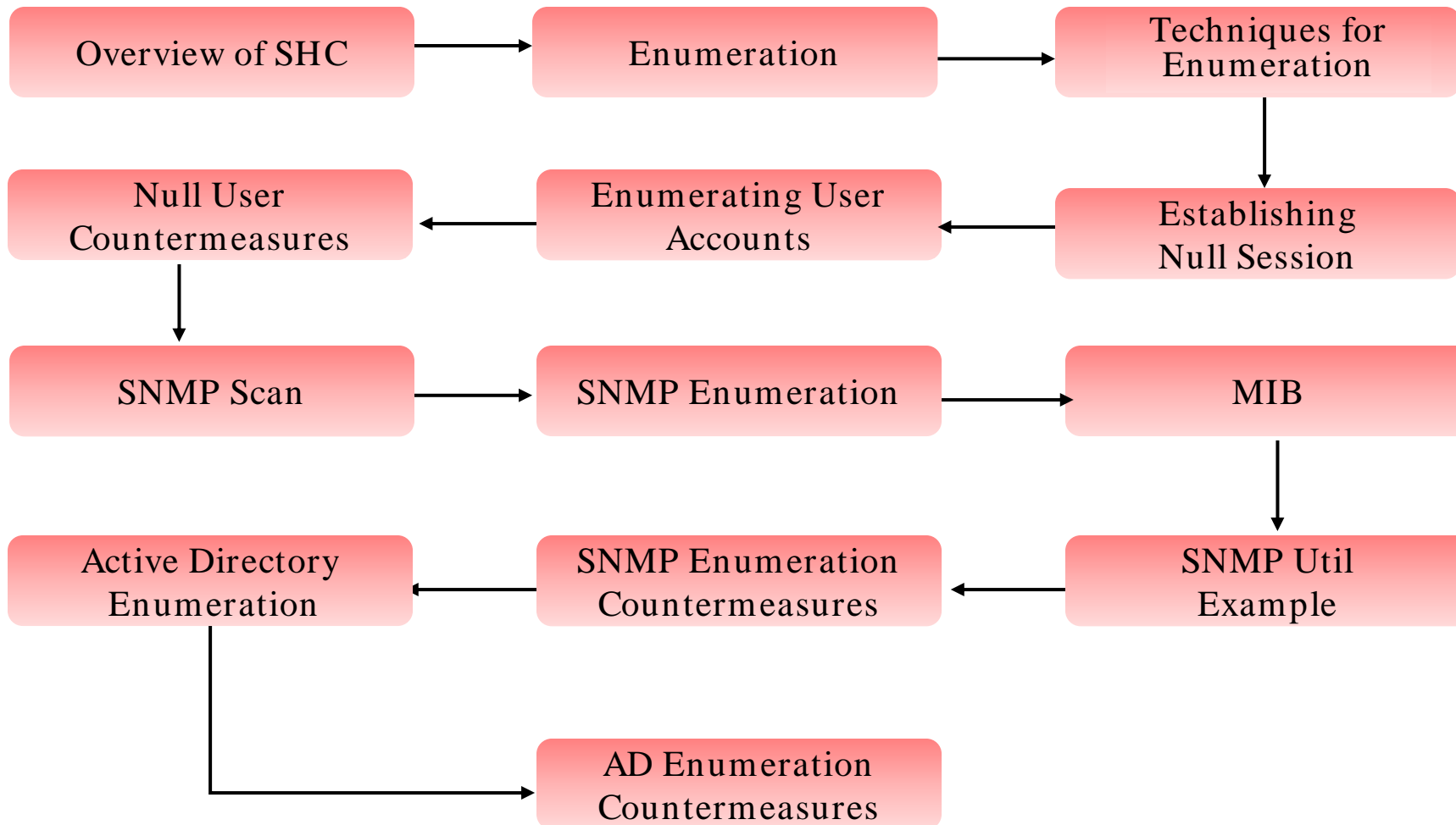
# Module Objective

This module will familiarize you with:

- Overview of System Hacking Cycle
- Enumeration
- Techniques for Enumeration
- Establishing Null Session
- Enumerating User Accounts
- Null User Countermeasures
- SNMP Scan
- SNMP Enumeration
- MIB
- SNMP Util Example
- SNMP Enumeration Countermeasures
- Active Directory Enumeration
- AD Enumeration Countermeasures



# Module Flow



# Overview of System Hacking Cycle

## Step 1: Enumerate users

- Extract user names using Win2K enumeration and SNMP probing

## Step 2: Crack the password

- Crack the password of the user and gain access to the system

## Step 3: Escalate privileges

- Escalate to the level of the administrator

## Step 4: Execute applications

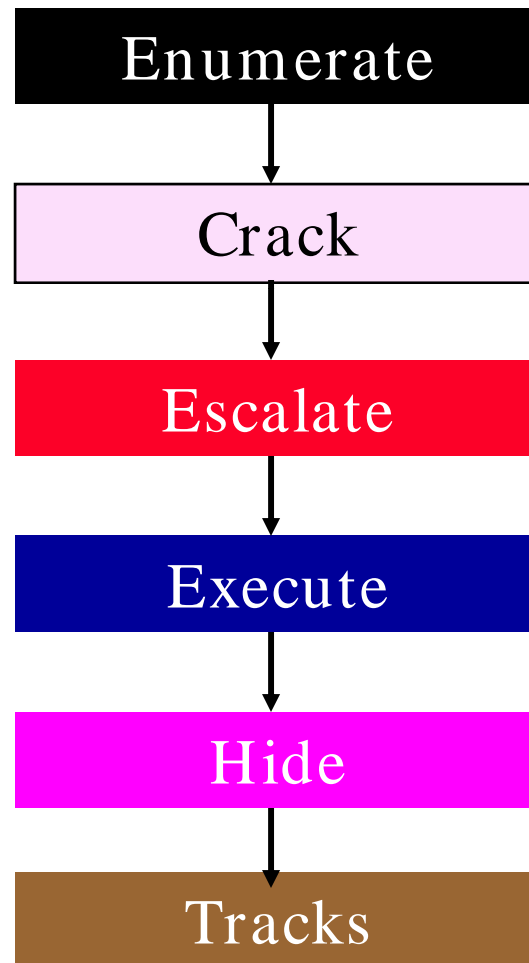
- Plant keyloggers, spywares, and rootkits on the machine

## Step 5: Hide files

- Use steganography to hide hacking tools and source code

## Step 6: Cover your tracks

- Erase tracks so that you will not be caught



# What is Enumeration

Enumeration is defined as extraction of user names, machine names, network resources, shares, and services

Enumeration techniques are conducted in an intranet environment

Enumeration involves active connections to systems and directed queries

The type of information enumerated by intruders:

- Network resources and shares
- Users and groups
- Applications and banners
- Auditing settings

Some of the techniques for enumeration are:

- Extract user names using Win2k enumeration
- Extract user names using SNMP
- Extract user names using email IDs
- Extract information using default passwords
- Brute force Active Directory





# Netbios Null Sessions

The null session is often referred to as the Holy Grail of Windows hacking. Null sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/ Server Messaging Block)

You can establish a null session with a Windows (NT/2000/XP) host by logging on with a null user name and password

Using these null connections, you can gather the following information from the host:

- List of users and groups
- List of machines
- List of shares
- Users and host SIDs (Security Identifiers)



# So What's the Big Deal

Anyone with a NetBIOS connection to your computer can easily get a full dump of all your user names, groups, shares, permissions, policies, services, and more using the null user

The following syntax connects to the hidden Inter Process Communication 'share' (IPC\$) at IP address 192.34.34.2 with the built-in anonymous user (/u:"") with a (") null password

The attacker now has a channel over which to attempt various techniques

The CIFS/ SMB and NetBIOS standards in Windows 2000 include APIs that return rich information about a machine via TCP port 139—even to the unauthenticated users

This works on Windows 2000/ XP systems, but not on Win 2003

**Windows:** `C:\>net use \\192.34.34.2\IPC$ "" /u:""`

**Linux:** `$ smbclient \\\target\ipc$ "" -U ""`

# Tool: DumpSec

DumpSec reveals shares over a null session with the target computer

```

Somarsoft DumpSec (formerly DumpAcl) - \\AI200
File Edit Search Report View Help
Share and path Account Own Permission
NETLOGON=D:\WINNT\system32\Repl\Import\Scripts (disktree) Everyone read
ADMIN$=D:\WINNT (special admin share) admin-only (no dacl)
IPC$= (special admin share) admin-only (no dacl)
C$=C:\ (special admin share) admin-only (no dacl)
D$=D:\ (special admin share) admin-only (no dacl)
E$=E:\ (special admin share) admin-only (no dacl)
F$=F:\ (special admin share) admin-only (no dacl)
G$=G:\ (special admin share) admin-only (no dacl)
users=G:\users (disktree) unprotected (no dacl)
print$=D:\WINNT\system32\spool\drivers (disktree) Everyone read
print$=D:\WINNT\system32\spool\drivers (disktree) BENTO\Administrators all
print$=D:\WINNT\system32\spool\drivers (disktree) BENTO\Print Operators all
print$=D:\WINNT\system32\spool\drivers (disktree) BENTO\Server Operators all
WebFiles=G:\ (disktree) BENTO\Administrators read
WebFiles=G:\ (disktree) BENTO\abento all
00001
  
```

# NetBIOS Enumeration Using Netview

The Netview tool allows you to gather two essential bits of information:

- List of computers that belong to a domain
- List of shares on individual hosts on the network

The first thing a remote attacker will try on a Windows 2000 network is to get a list of hosts attached to the wire

- `net view /domain`
- `Net view \\<some-computer>`
- `nbstat -A <some IP>`



# NetBIOS Enumeration Using Netview (cont'd)

```
C:\WINNT\System32\cmd.exe
Doing NBT name scan for addresses from 192.168.2.0/24
192.168.2.0      Sendto failed: Cannot assign requested address
192.168.2.1      Recvfrom failed: Connection reset by peer

NetBIOS Name Table for Host 192.168.2.4:
Name           Service        Type
-----
USER           Workstation Service
WORKGROUP      Domain Name
USER           Messenger Service

Adapter address: 00-0b-2b-0e-af-59
-----

NetBIOS Name Table for Host 192.168.2.7:
Name           Service        Type
-----
JCITR02       Workstation Service
RANGE2        Domain Name
JCITR02       Messenger Service
JCITR02       File Server Service
RANGE2        Browser Service Elections
RANGE2        Master Browser
@@_MSBROWSE_@ Master Browser

Adapter address: 00-80-ad-83-a5-2e
-----

NetBIOS Name Table for Host 192.168.2.24:
Name           Service        Type
-----
COMPUTRE1     Workstation Service
COMPUTRE1     Messenger Service

Adapter address: 00-c1-26-10-d4-2d
-----
```

# Nbtstat Enumeration Tool

Nbtstat is a Windows command-line tool that can be used to display information about a computer's NetBIOS connections and name tables

- Run: `nbtstat -A <some ip address>`

C:\>nbtstat

- Displays protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP).  
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S]  
[interval] ]

```
C:\Documents and Settings\Haja>nbtstat -A 10.0.0.11

Umware Network Adapter UMnet8:
Node IpAddress: [192.168.87.1] Scope Id: []

    NetBIOS Remote Machine Name Table

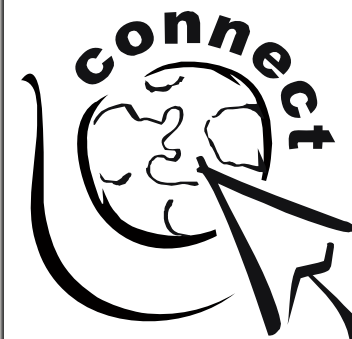
    Name                Type             Status
    -----
    HAJAXP                <00>    UNIQUE         Registered
    MSHOME                <00>    GROUP          Registered
    MSHOME                <1E>    GROUP          Registered
    MSHOME                <1D>    UNIQUE         Registered
    .._MSBROWSE_..       <01>    GROUP          Registered

    MAC Address = 00-C0-9F-2C-36-30

Umware Network Adapter UMnet1:
Node IpAddress: [192.168.159.1] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
```



# Tool: SuperScan

A powerful connect-based TCP port scanner, pinger, and hostname resolver

Performs ping scans and port scans by using any IP range or by specifying a text file to extract addresses

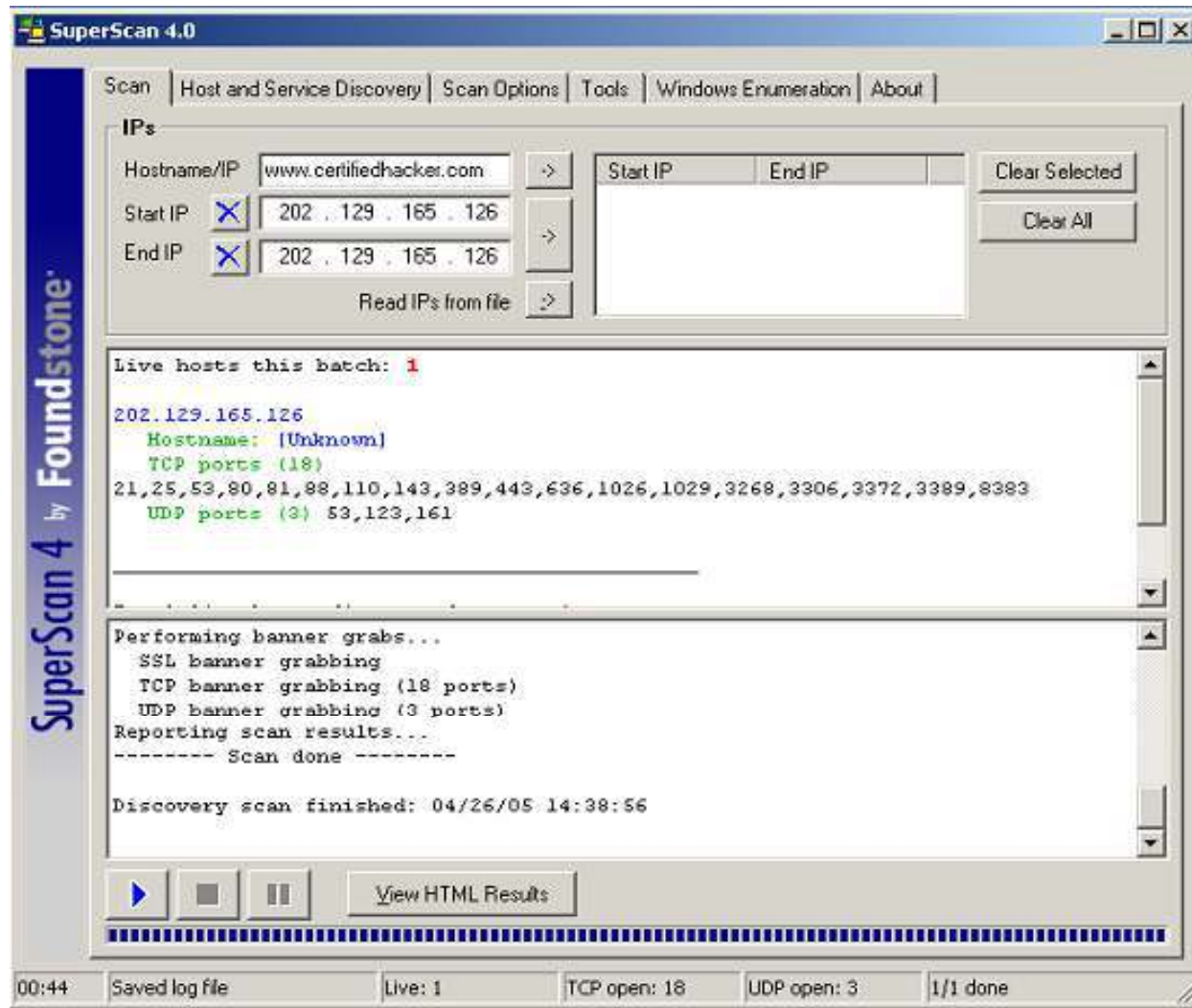
Scans any port range from a built-in list or specified range

Resolves and reverse-lookup any IP address or range

Modifies the port list and port descriptions using the built-in editor

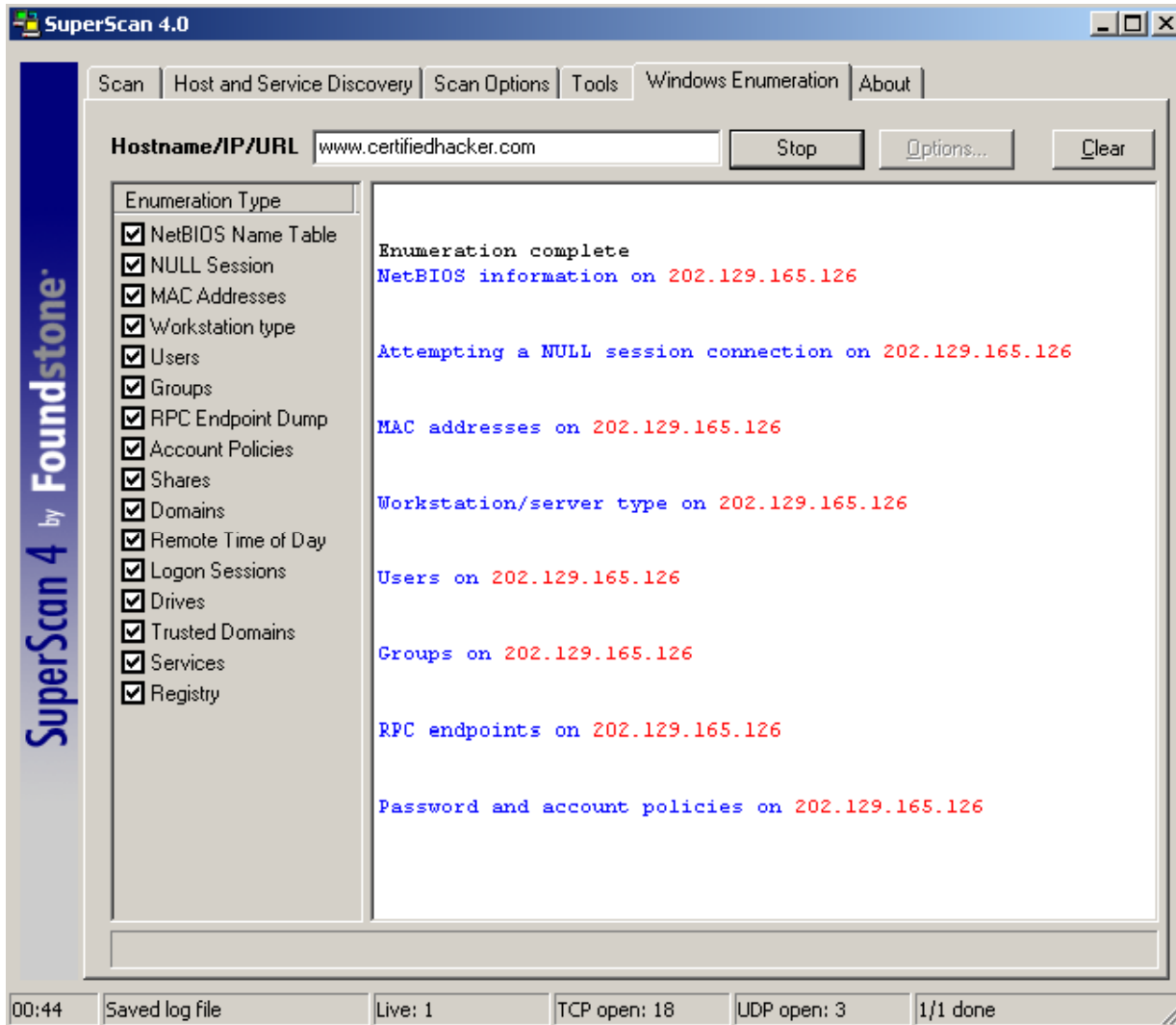
Connects to any discovered open port using user-specified "helper" applications (e.g., Telnet, web browser, FTP), and assigns a custom helper application to any port

# SuperScan: Screenshot





# Screenshot for Windows Enumeration



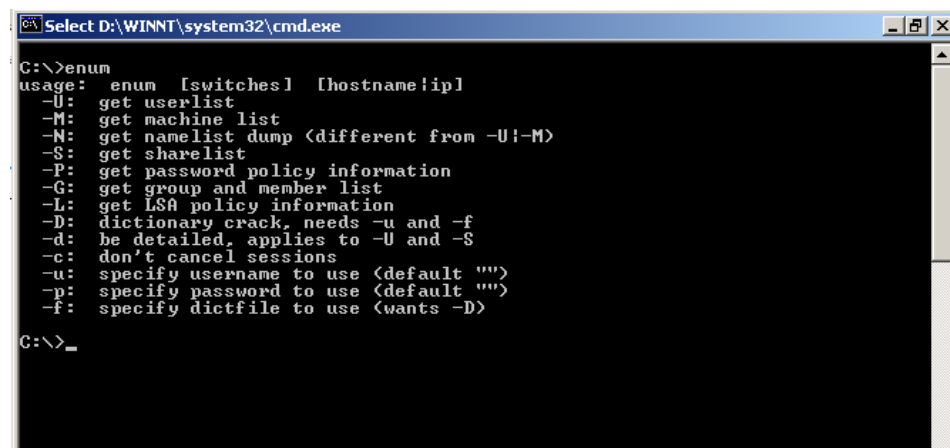
# Tool: enum

Available for download from  
<http://razor.bindview.com>

enum is a console-based Win32  
information enumeration utility

Using null sessions, enum can retrieve  
user lists, machine lists, share lists, name  
lists, group and membership lists, and  
password and LSA policy information

enum is also capable of rudimentary  
brute-force dictionary attacks on the  
individual accounts



```
Select D:\WINNT\system32\cmd.exe
C:\>enum
usage: enum [switches] [hostname!ip]
-U: get userlist
-M: get machine list
-N: get namelist dump <different from -U|-M>
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use <default "">
-p: specify password to use <default "">
-f: specify dictfile to use <wants -D>
C:\>_
```

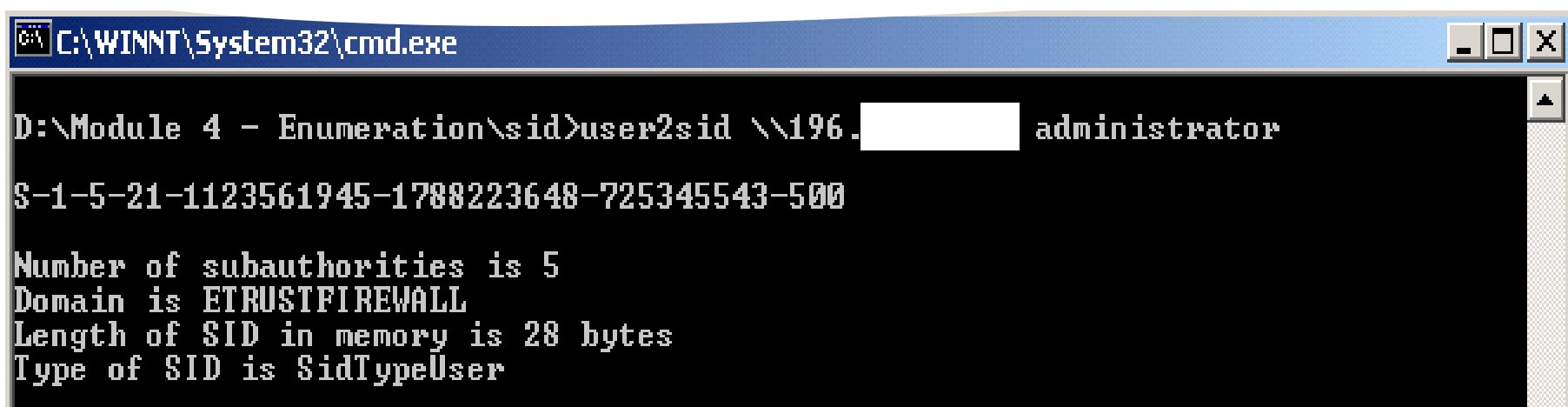
# Enumerating User Accounts

Two powerful NT/2000 enumeration tools are:

- 1.sid2user
- 2.user2sid

They can be downloaded at [www.chem.msu.edu/~rudnyi/NT/](http://www.chem.msu.edu/~rudnyi/NT/)

These are command-line tools that look up NT SIDs from user name input and vice versa



```
C:\WINNT\System32\cmd.exe

D:\Module 4 - Enumeration\sider>user2sid \\196. [redacted] administrator

S-1-5-21-1123561945-1788223648-725345543-500

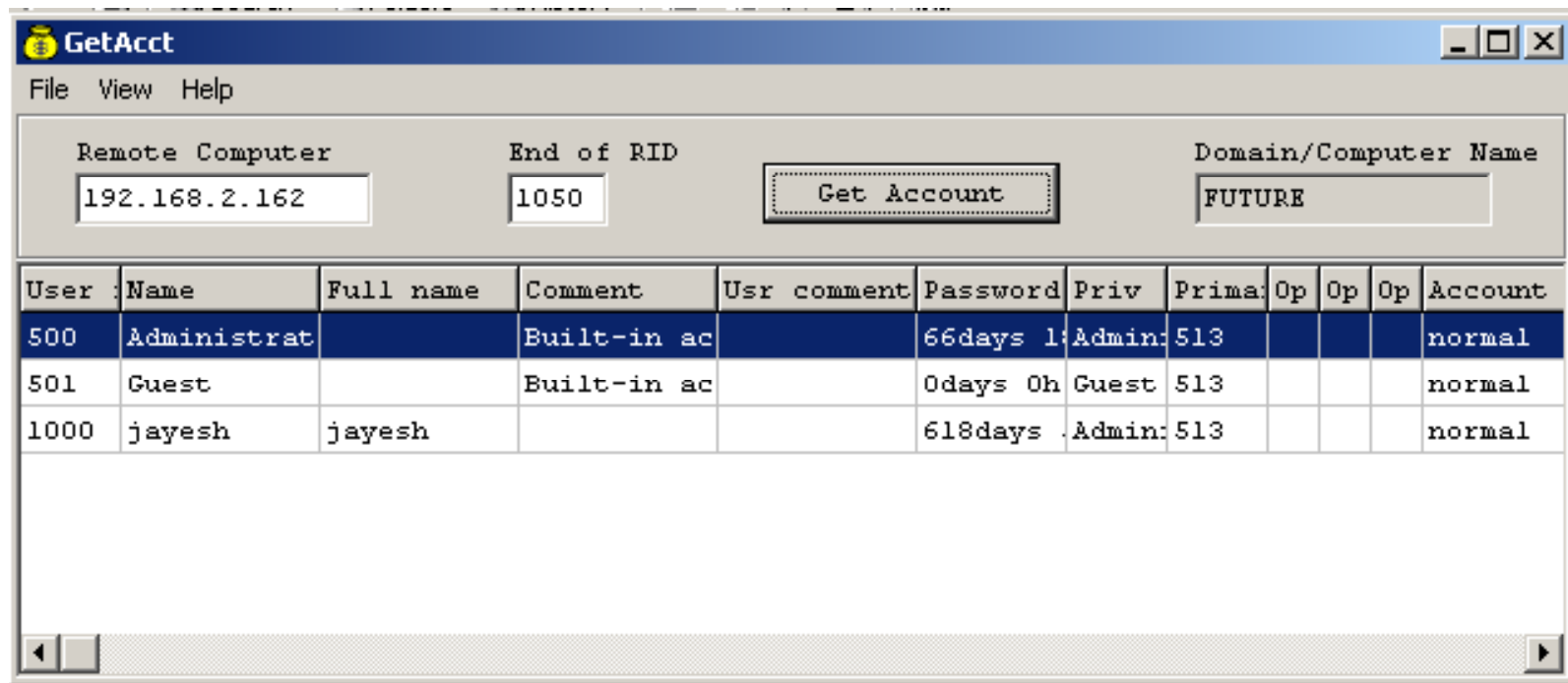
Number of subauthorities is 5
Domain is ETRUSTFIREWALL
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

# Tool: GetAcct

GetAcct sidesteps "Restrict Anonymous=1" and acquires account information on Windows NT/2000 machines



Downloadable from [www.securityfriday.com](http://www.securityfriday.com)



# Null Session Countermeasures

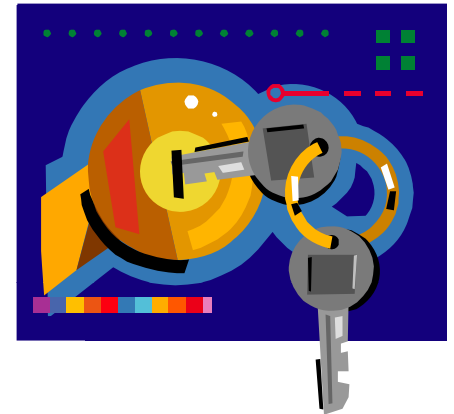
Null sessions require access to TCP 139 and/or TCP 445 ports

Null sessions do not work with Windows 2003

You could also disable SMB services entirely on individual hosts by unbinding the WINS Client TCP/IP from the interface

Edit the registry to restrict the anonymous user:

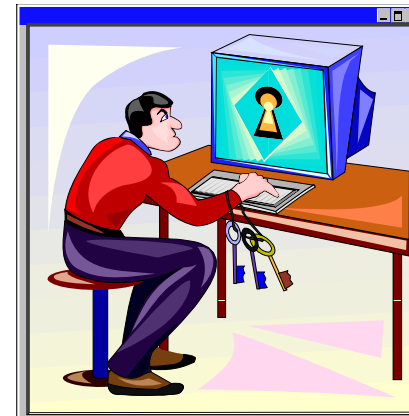
- Step1: Open regedt32 and navigate to `HKLM\SYSTEM\CurrentControlSet\LSA`
- Step2: Choose edit | add value
  - value name: Restrict Anonymous
  - Data Type:REG\_WORD
  - Value: 2



PS Tools was developed by Mark Russinovich of SysInternals and contains a collection of enumeration tools.

Some tools require user authentication to the system:

- PsExec - Remotely executes processes
- PsFile - Shows remotely opened files
- PsGetSid - Displays the SID of a computer or a user
- PsKill - Kills processes by name or process ID
- PsInfo - Lists information about a system
- PsList - Lists detailed information about processes
- PsLoggedOn - Shows who is logged on locally and via resource sharing
- PsLogList - Dumps event log records
- PsPasswd - Changes account passwords
- PsService - Views and controls services
- PsShutdown - Shuts down and optionally reboots a computer
- PsSuspend - Suspends processes
- PsUptime - Shows how long a system has been running since its last reboot



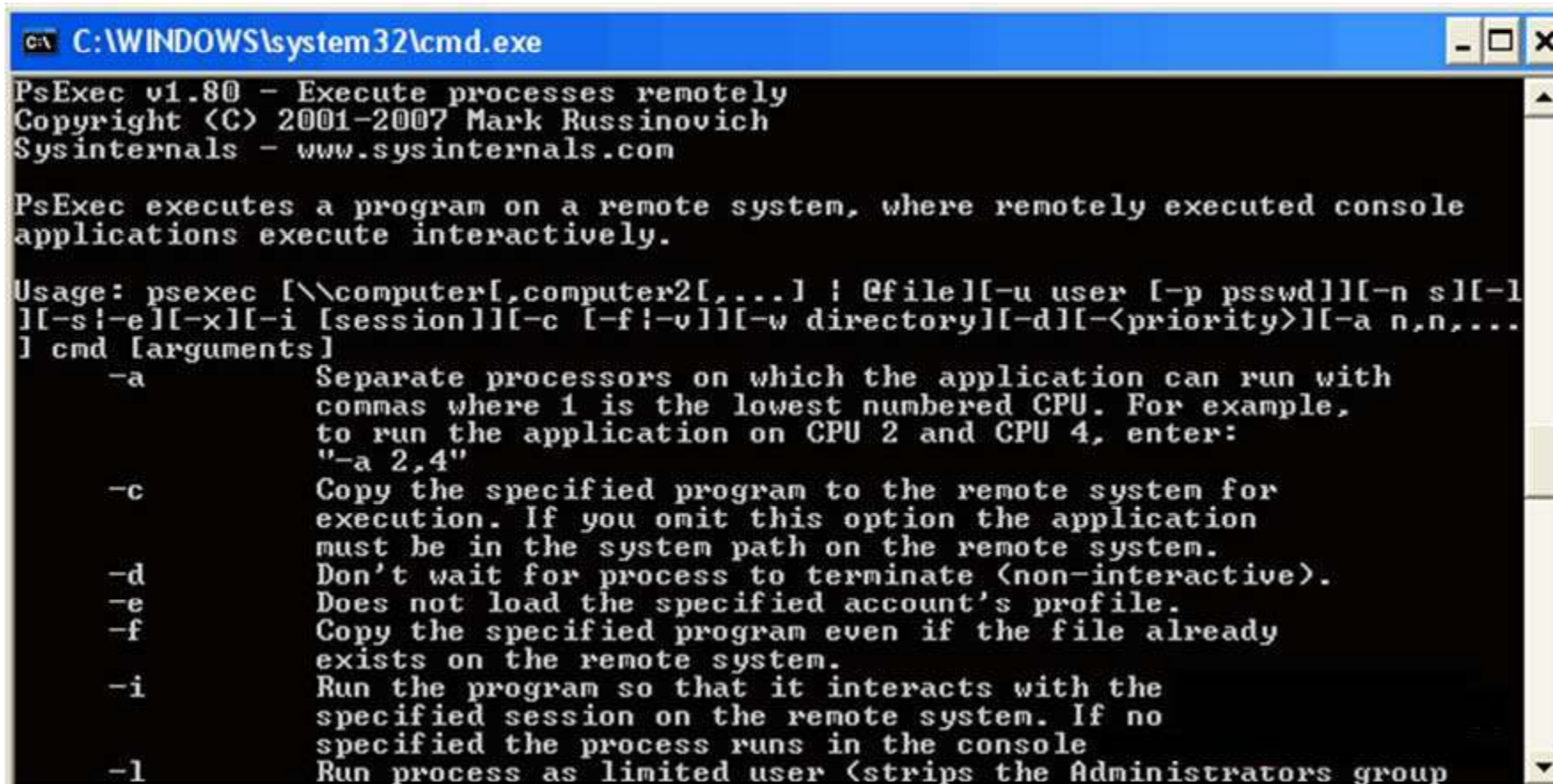
PsExec is a lightweight telnet replacement that allows you to execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software

PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig



```
Usage: psexec
[\\computer[,computer[,...]] | @file
][-u user [-p psswd]][-n s][-l][-s|-
e][-i][-c [-f|-v]][-d][-w
directory][-<priority>][-a n,n,...]
cmd [arguments]
```

# PsExec: Screenshot



```
C:\WINDOWS\system32\cmd.exe
PsExec v1.80 - Execute processes remotely
Copyright (C) 2001-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

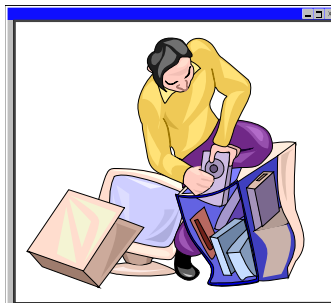
Usage: psexec [\\computer[,computer2[,...]] ; @file][-u user [-p psswd]][-n s][-l
][-s!-e][-x][-i [session]][-c [-f!-v]][-w directory][-d][-<priority>][-a n,n,...
] cmd [arguments]
  -a          Separate processors on which the application can run with
              commas where 1 is the lowest numbered CPU. For example,
              to run the application on CPU 2 and CPU 4, enter:
              "-a 2,4"
  -c          Copy the specified program to the remote system for
              execution. If you omit this option the application
              must be in the system path on the remote system.
  -d          Don't wait for process to terminate (non-interactive).
  -e          Does not load the specified account's profile.
  -f          Copy the specified program even if the file already
              exists on the remote system.
  -i          Run the program so that it interacts with the
              specified session on the remote system. If no
              specified the process runs in the console
  -l          Run process as limited user (strips the Administrators group
```



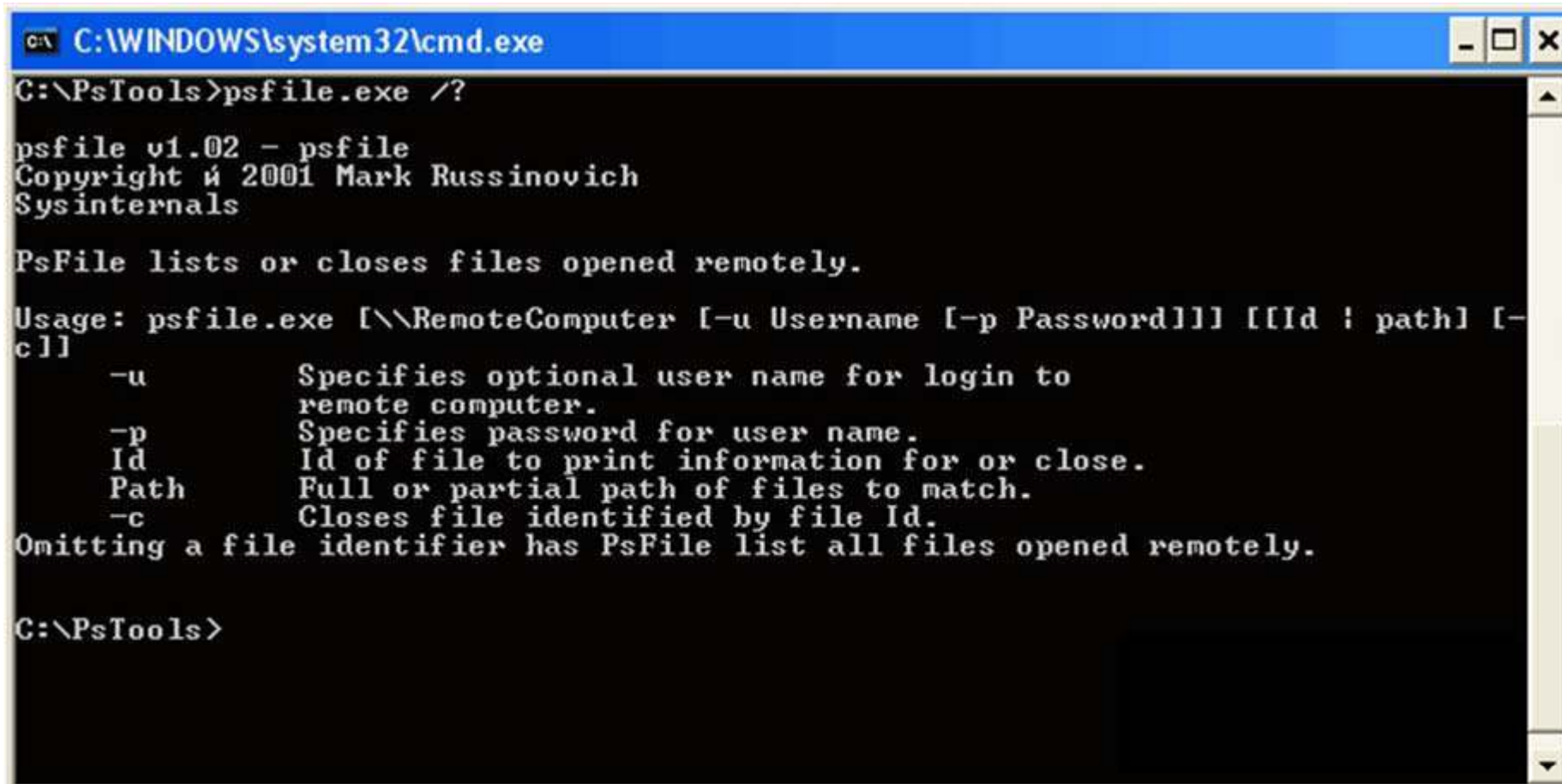
The "net file" command shows you a list of files that other computers have opened on their systems, upon which you execute the command

*PsFile* is a command-line utility that shows a list of files on a system that are opened remotely, and it also allows you to close opened files either by name or by file identifier

```
Usage: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]
```



# PsFile: Screenshot



```
C:\WINDOWS\system32\cmd.exe
C:\PsTools>psfile.exe /?

psfile v1.02 - psfile
Copyright © 2001 Mark Russinovich
Sysinternals

PsFile lists or closes files opened remotely.

Usage: psfile.exe [\\RemoteComputer [-u Username [-p Password]]] [[Id : path] [-c]]
    -u          Specifies optional user name for login to
                remote computer.
    -p          Specifies password for user name.
    Id         Id of file to print information for or close.
    Path       Full or partial path of files to match.
    -c         Closes file identified by file Id.
Omitting a file identifier has PsFile list all files opened remotely.

C:\PsTools>
```

Have you performed a rollout only to discover that your network might suffer from the SID duplication problem?

*PsGetSid* allows you to see the SIDs of user accounts and translate SIDs into the names that represent them

```
Usage: psgetsid [\\computer[,computer[,...]] | @file]  
[-u username [-p password]] [account|SID]
```



# PsGetSid: Screenshot

```
C:\WINDOWS\system32\cmd.exe
PsGetSid v1.43 - Translates SIDs to names and vice versa
Copyright (C) 1999-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: psgetsid.exe [\\computer[,computer2[,...]] ! @file] [-u Username [-p Password]] [account ! SID]
    -u      Specifies optional user name for login to remote computer.
    -p      Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
    account PsGetSid will report the SID for the specified user account rather than the computer.
    SID     PsGetSid will report the account for the specified SID.
    computer Direct PsGetSid to perform the command on the remote computer or computers specified. If you omit the computer name PsGetSid runs the command on the local system, and if you specify a wildcard (\\*), PsGetSid runs the command on all computers in the current domain.
    @file   PsGetSid will execute the command on each of the computers listed in the file.

C:\PsTools>
```

Windows NT/2000 does not come with a command-line 'kill' utility

*PsKill* is a kill utility that can kill processes on remote systems

```
Usage: pskill [-?]
[-t] [\\computer
[-u username] [-p
password]]
<process name |
process id>
```



# PsKill: Screenshot



```
C:\WINDOWS\system32\cmd.exe

C:\PsTools>pskill.exe

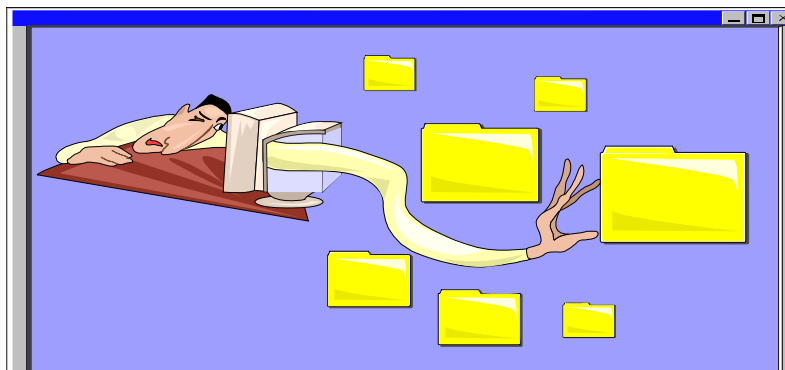
PsKill v1.12 - Terminates processes on local or remote systems
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pskill [-t] [\\computer [-u username [-p password]]] <process ID : name>
  -t      Kill the process and its descendants.
  -u      Specifies optional user name for login to
          remote computer.
  -p      Specifies optional password for user name. If you omit this
          you will be prompted to enter a hidden password.

C:\PsTools>
```

*PsInfo* is a command-line tool that gathers key information about the local or remote Windows NT/2000 system, including the type of installation, kernel build, registered organization and owner, number of processors and their types, amount of physical memory, install date of the system and if it's a trial version, and expiration date

```
Usage: psinfo [[\\computer[,computer[,...]] | @file [-u  
user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]]  
[filter]
```



# PsInfo: Screenshot

```
C:\WINDOWS\system32\cmd.exe

PsInfo v1.74 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

PsInfo returns information about a local or remote Windows NT/2000/XP system.

Usage: psinfo [-h] [-s] [-d] [-c [-t delimiter]] [filter] [\\computer[,computer[
,..]]!@file [-u Username [-p Password]]
  -u      Specifies optional user name for login to
         remote computer.
  -p      Specifies password for user name.
  -h      Show installed hotfixes.
  -s      Show installed software.
  -d      Show disk volume information.
  -c      Print in CSV format
  -t      The default delimiter for the -c option is a comma,
         but can be overridden with the specified character. Use
         "\t" to specify tab.
  filter  Psinfo will only show data for the field matching the filter.
         e.g. "psinfo service" lists only the service pack field.
  computer Direct PsInfo to perform the command on the remote
         computer or computers specified. If you omit the computer
         name PsInfo runs the command on the local system,
         and if you specify a wildcard (\\*), PsInfo runs the
         command on all computers in the current domain.
  @file   PsInfo will run against the computers listed in the file
         specified.

C:\PsTools>
```

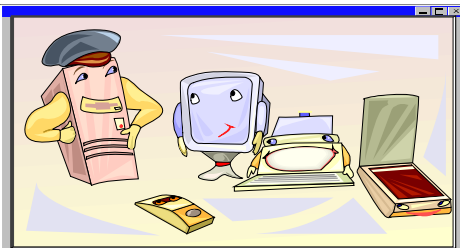


# PsList

Most UNIX operating systems ship with a command-line tool called "ps" (or something equivalent) that administrators use to view detailed information about process CPU and memory usage

*PsList* is utility that shows a combination of the information obtainable individually with *ps* and *psstat*

```
Usage: pslist [-?] [-d] [-m] [-x] [-t] [-s [n] [-r n]][\computer [-u username] [-p password]] [name | pid]
```



# PsList: Screenshot

```
C:\WINDOWS\system32\cmd.exe

pslist v1.28 - Sysinternals PsList
Copyright © 2000-2004 Mark Russinovich
Sysinternals

Usage: pslist.exe [-d][-m][-x][-t][-s [n] [-r n] [\\computer [-u username][-p pa
ssword]][name|pid]
  -d          Show thread detail.
  -m          Show memory detail.
  -x          Show processes, memory information and threads.
  -t          Show process tree.
  -s [n]     Run in task-manager mode, for optional seconds specified.
             Press Escape to abort.
  -r n       Task-manager mode refresh rate in seconds (default is 1).
  \\computer Specifies remote computer.
  -u         Optional user name for remote login.
  -p         Optional password for remote login. If you don't present
             on the command line pslist will prompt you for it if necessary.
  name       Show information about processes that begin with the name
             specified.
  -e         Exact match the process name.
  pid        Show information about specified process.

All memory values are displayed in KB.
Abbreviation key:
  Pri        Priority
  Thd        Number of Threads
  Hnd        Number of Handles
  UM         Virtual Memory
  WS         Working Set
  Priv       Private Virtual Memory
  Priv Pk    Private Virtual Memory Peak
  Faults     Page Faults
  NonP       Non-Paged Pool
  Page       Paged Pool
  Cswtch     Context Switches

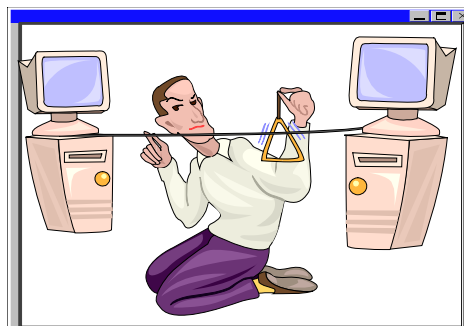
C:\PsTools>
```

# PsLoggedOn

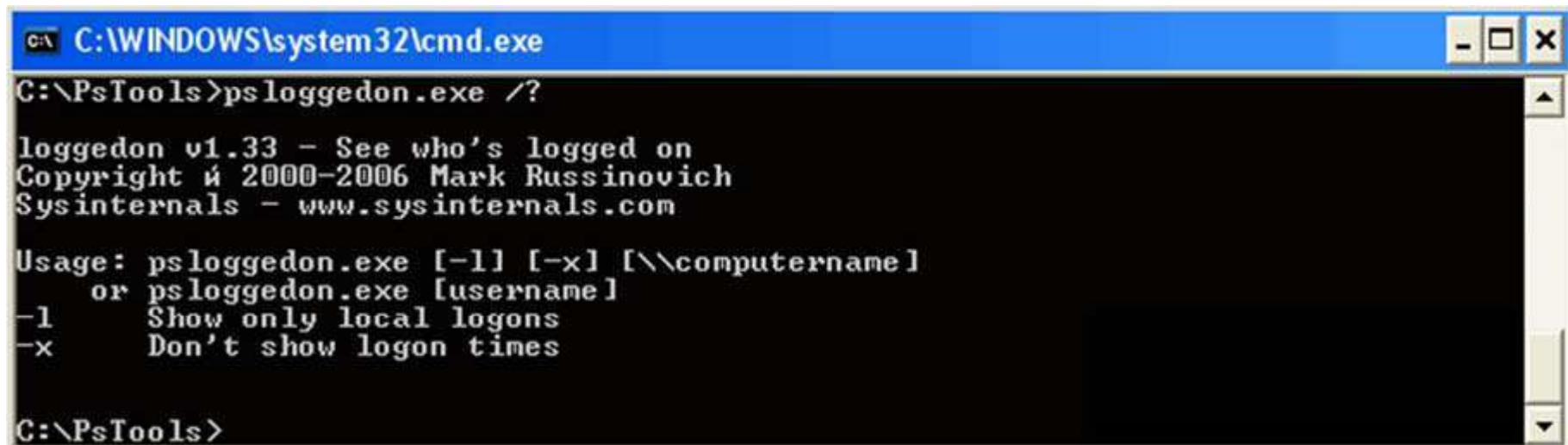
You can determine who is using resources on your local computer with the "net" command ("net session"); however, there is no built-in way to determine who is using the resources of a remote computer

*PsLoggedOn* searches the computers in the network neighborhood and tells you if the user is currently logged on

Usage: `psloggedon [-?] [-l] [-x] [\\computername | username]`



# PsLoggedOn: Screenshot



```
C:\WINDOWS\system32\cmd.exe
C:\PsTools>psloggedon.exe /?

loggedon v1.33 - See who's logged on
Copyright © 2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: psloggedon.exe [-l] [-x] [\\computername]
       or psloggedon.exe [username]
-l      Show only local logons
-x      Don't show logon times

C:\PsTools>
```

*PsLogList* allows you to log into remote systems in situations where your current set of security credentials would not permit access to the Event Log, and *PsLogList* retrieves message strings from the computer on which the event log that you view resides

```
Usage: psloglist [-?] [\\computer[,computer[,...]] | @file  
[-u username [-p password]] [-s [-t delimiter]] [-m #|-  
n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy][-b  
mm/dd/yy][-f filter] [-i ID[,ID[,...]] | -e  
ID[,ID[,...]]] [-o event source[,event source][,...]] [-  
q event source[,event source][,...]] [-l event log file]  
<eventlog>
```



# PsLogList: Screenshot

```
C:\WINDOWS\system32\cmd.exe

PsLoglist v2.64 - local and remote event log viewer
Copyright (C) 2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

PsLogList dumps event logs on a local or remote NT system.

Usage: psloglist [\\computer[.computer2[,...]] | @file] [-u username [-p password
]] [-s [-t delimiter]] [-m #!-n #!-d #!-h #!-w][-c][-x][-r][-a mm/dd/yy][-b mm/
dd/yy] [-f filter] [-i ID,[ID,...]] [-e ID,[ID,...]] [-o event source[,event so
urce[,...]]] [-q event source[,event source[,...]]] [-g!-l] event log file <ev
ent log>
  @file      Psloglist will execute the command on each of the computers
             listed in the file.
  -a        Dump records timestamped after specified date.
  -b        Dump records timestamped before specified date.
  -c        Clear event log after displaying.
  -d        Only display records from previous n days.
  -e        Exclude events with the specified ID or IDs (up to 10).
  -f        Filter event types, using starting letter
             (e.g. "-f we" to filter warnings and errors).
  -g        Export an event log as an evt file. This can only be used
             with the -c switch (clear log).
  -h        Only display records from previous n hours.
  -i        Show only events with the specified ID or IDs (up to 10).
  -l        Dump the contents of the specified saved event log file.
  -m        Only display records from previous n minutes.
  -n        Only display n most recent records.
  -o        Show only records from the specified event source or sources
             (e.g. "-o cdrom").
  -p        Specifies password for user name.
  -q        Omit records from the specified event source or sources
             (e.g. "-q cdrom").
  -r        Dump log from least recent to most recent.
  -s        Records are listed on one line each with delimited
             fields, which is convenient for string searches.
             The default delimiter for the -s option is a comma,
             but can be overridden with the specified character. Use "\t"
             to specify tab.
  -u        Specifies optional user name for login to
             remote computer.
  -w        Wait for new events, dumping them as they generate (local system
             only.)
  -x        Dump extended data.
  eventlog Specifies event log to dump. Default is system. If the
             -l switch is present then the event log name specifies
             how to interpret the event log file.

C:\PsTools>
```

Systems administrators who manage local administrative accounts on multiple computers regularly need to change the account password as a part of the standard security practices

*PsPasswd* is a tool that allows you to change an account password on local or remote systems

## Usage:

- `pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] Username [NewPassword]`



# PsPasswd: Screenshot

```
C:\WINDOWS\system32\cmd.exe
C:\PsTools>pspasswd.exe

PsPasswd v1.22 - Local and remote password changer
Copyright (C) 2003-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

PsPasswd changes passwords on a local or remote system.

Usage: pspasswd [\\[computer[,computer[,...]]!Domain]!@file] [-u Username [-p Password]] Username [NewPassword]
    computer      Direct PsPasswd to perform the command on the remote
                  computer or computers specified. If you omit the computer
                  name PsPasswd runs the command on the local system,
                  and if you specify a wildcard (\\*), PsPasswd runs the
                  command on all computers in the current domain.
    @file         PsPasswd will change the password on the computers listed
                  in the file.
    -u           Specifies optional user name for login to remote
                  computer.
    -p           Specifies optional password for user name. If you omit this
                  you will be prompted to enter a hidden password.
    Username     Specifies name of account for password change.
    NewPassword  New password. If omitted a NULL password

C:\PsTools>
```



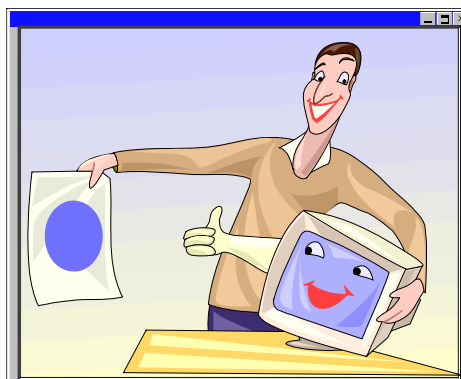
# PsService

*PsService* includes a unique service-search capability that identifies active instances of a service on your network

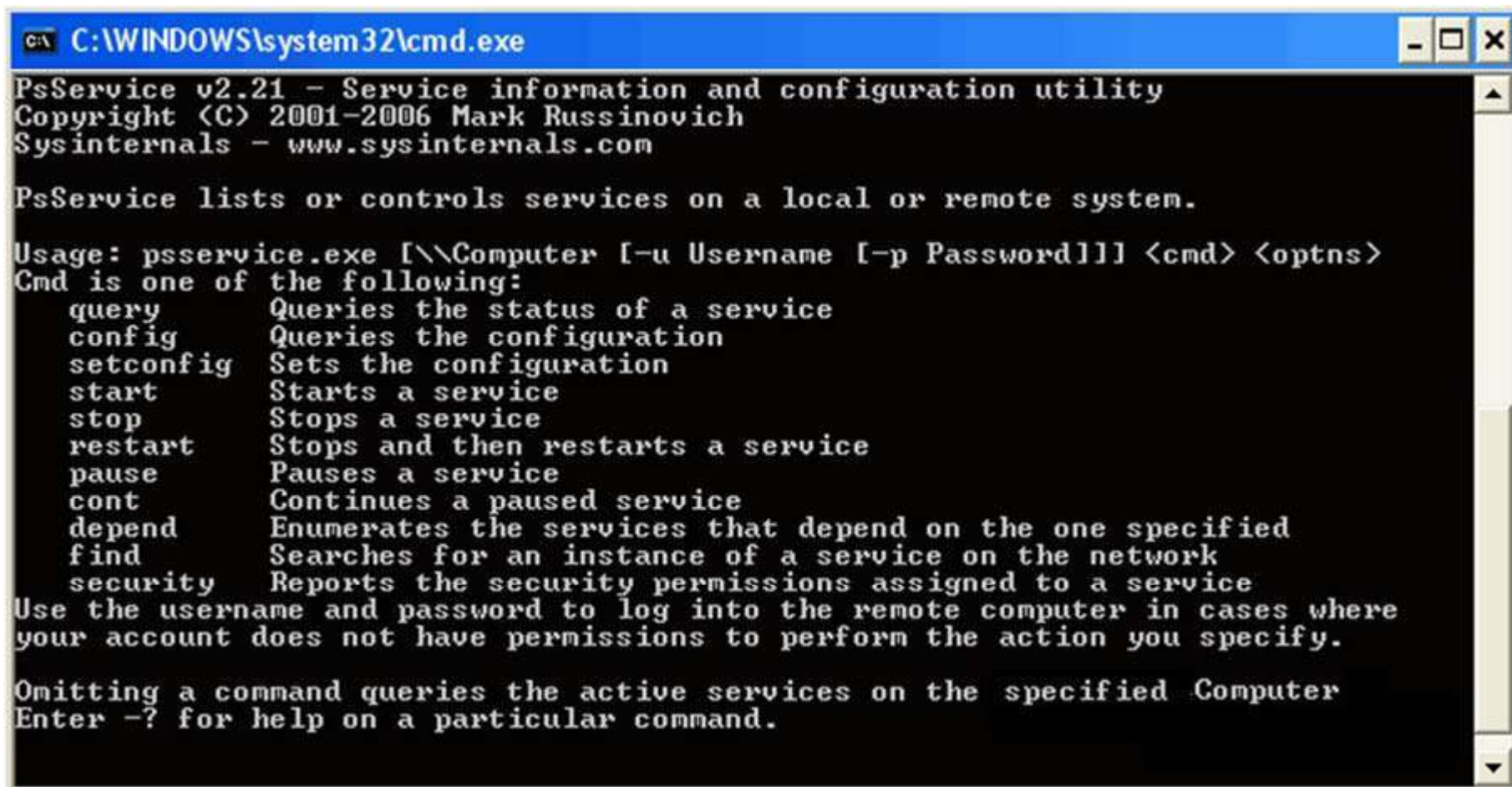
For instance, you would use the search feature if you wanted to locate systems running on DHCP servers

Usage:

- `psservice [\\computer [-u username] [-p password]] <command> <options>`



# PsService: Screenshot



```
C:\WINDOWS\system32\cmd.exe
PsService v2.21 - Service information and configuration utility
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

PsService lists or controls services on a local or remote system.

Usage: psservice.exe [\\Computer [-u Username [-p Password]]] <cmd> <opts>
Cmd is one of the following:
  query      Queries the status of a service
  config     Queries the configuration
  setconfig  Sets the configuration
  start      Starts a service
  stop       Stops a service
  restart    Stops and then restarts a service
  pause      Pauses a service
  cont       Continues a paused service
  depend     Enumerates the services that depend on the one specified
  find       Searches for an instance of a service on the network
  security   Reports the security permissions assigned to a service
Use the username and password to log into the remote computer in cases where
your account does not have permissions to perform the action you specify.

Omitting a command queries the active services on the specified Computer
Enter -? for help on a particular command.
```

# PsShutdown

*PsShutdown* is a command-line utility similar to the shutdown utility from the Windows 2000 Resource Kit, but with the ability to do much more

*PsShutdown* can log off the console user or lock the console

```
Usage: psshutdown [[\\computer[,computer[,...]] | @file [-u user [-p psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]
```



# PsShutdown: Screenshot

```

C:\WINDOWS\system32\cmd.exe
PsShutdown v2.52 - Shutdown, logoff and power manage local and remote systems
Copyright (C) 1999-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

usage:
psshutdown -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t [min]:[h]:[m]] [-v nn] [-e [uipl]:xx:yy] [-n "message"] [-u Username [-p password]] [-n s1 [\computer[,computer[...]]|@file]
-a          Abort a shutdown (only possible while countdown is in progress)
-c          Allow the shutdown to be aborted by the interactive user
-d          Suspend the computer
-e          Shutdown reason code (available on Windows XP and higher).
           Specify 'u' for unplanned and 'p' for planned
           shutdown reason codes.
           xx is the major reason code (must be less than 256)
           yy is the minor reason code (must be less than 65536)
-f          Forces running applications to close
-h          Hibernate the computer
-k          Poweroff the computer (reboot if poweroff is not supported)
-l          Lock the computer
-n          Message to display to logged on users
-n          Specifies timeout in seconds connecting to remote computers
-o          Logoff the console user
-p          Specifies optional password for user name. If you omit this
           you will be prompted to enter a hidden password.
-r          Reboot after shutdown
-s          Shutdown without poweroff
-t          Specifies countdown in seconds until shutdown (default is 20) or
           the time of shutdown (in 24 hour notation)
-u          Specifies optional user name for login to remote
           computer.
-v          Display message for the specified number of seconds before
           the shutdown. If you omit this parameter the shutdown
           notification dialog displays and specifying a value of 0
           omits the dialog.
computer  Shutdown the computer or computers specified
@file     Shutdown the computers listed in the file specified

Reasons defined on this computer (U = unplanned, P = planned):
Type  Major  Minor  Title
U      0      0      Other (Unplanned)
P      0      0      Other (Planned)
U      1      1      Hardware: Maintenance (Unplanned)
P      1      1      Hardware: Maintenance (Planned)
U      1      2      Hardware: Installation (Unplanned)
P      1      2      Hardware: Installation (Planned)
U      2      3      Operating System: Upgrade (Unplanned)
P      2      3      Operating System: Upgrade (Planned)
U      2      4      Operating System: Reconfiguration (Unplanned)
P      2      4      Operating System: Reconfiguration (Planned)
U      4      1      Application: Maintenance (Unplanned)
P      4      1      Application: Maintenance (Planned)
U      4      5      Application: Unresponsive
U      4      6      Application: Unstable
  
```

# PsSuspend

*PsSuspend* allows you to suspend processes on a local or remote system, which is desirable in cases where a process is consuming a resource (e.g., network, CPU, or disk) that you want to allow different processes to use

Rather than kill the process that is consuming the resource, suspending it permits you to continue operation at some later point of time

Usage:

- `pssuspend [-?] [-r] [\\computer [-u username] [-p password]] <process name | process id>`



# PsSuspend: Screenshot



```
C:\WINDOWS\system32\cmd.exe

PsSuspend v1.06 - Process Suspender
Copyright © 2001-2003 Mark Russinovich
Sysinternals

PsSuspend suspends or resumes processes on a local or remote NT system.

Usage: pssuspend [-r] [\\RemoteComputer [-u Username [-p Password]]] <process Id
or name>
  -r    Resume.
  -u    Specifies optional user name for login to
        remote computer.
  -p    Specifies optional password for user name. If you omit this
        you will be prompted to enter a hidden password.

C:\PsTools>
```

# SNMP Enumeration

SNMP stands for Simple Network Management Protocol

Managers send requests to agents and the agents send back replies

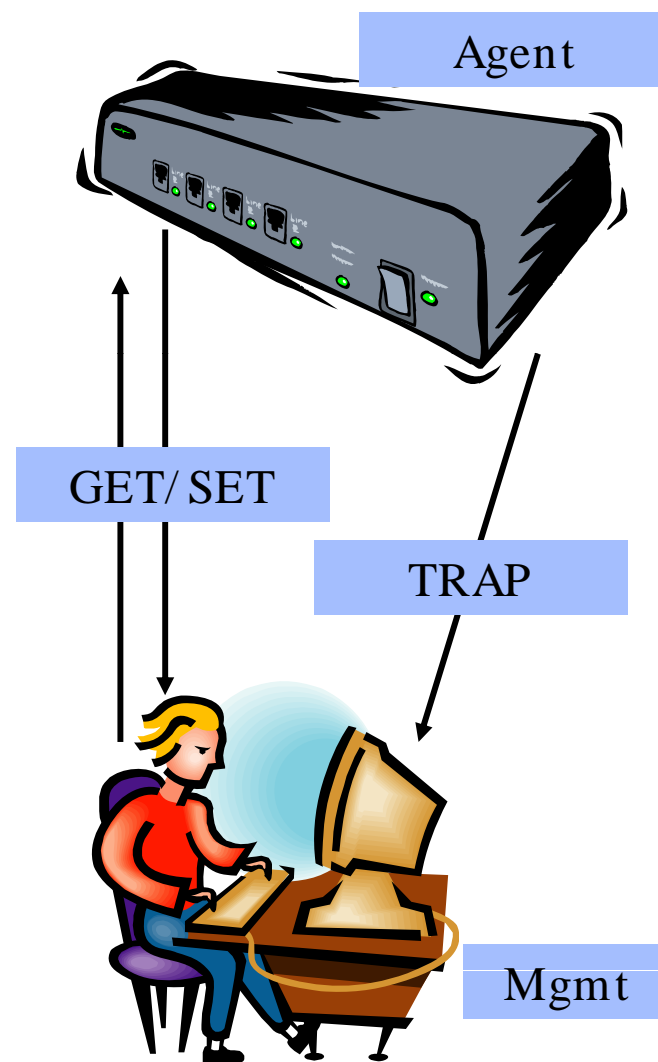
The requests and replies refer to variables accessible to the agent software

Managers can also send requests to set values for certain variables

Traps makes the manager aware that something significant has happened at the agent's end of things:

- A reboot
- An interface failure
- Or, something else that is potentially bad has occurred

Enumerating NT users via SNMP protocol is easy using snmputil



# Management Information Base

MIB provides a standard representation of the SNMP agent's available information and where it is stored

It is the most basic element of network management

It is the updated version of the standard MIB

It adds new SYNTAX types and adds more manageable objects to the MIB tree

Look for SNMP systems with the community string "public," which is the default for most systems



# SNMPutil Example

```
C:\>snmputil get 210.212.69.129 public .1.3.6.1.2.1.1.2.0
Variable = system.sysObjectID.0
Value = ObjectID 1.3.6.1.4.1.9.1.27

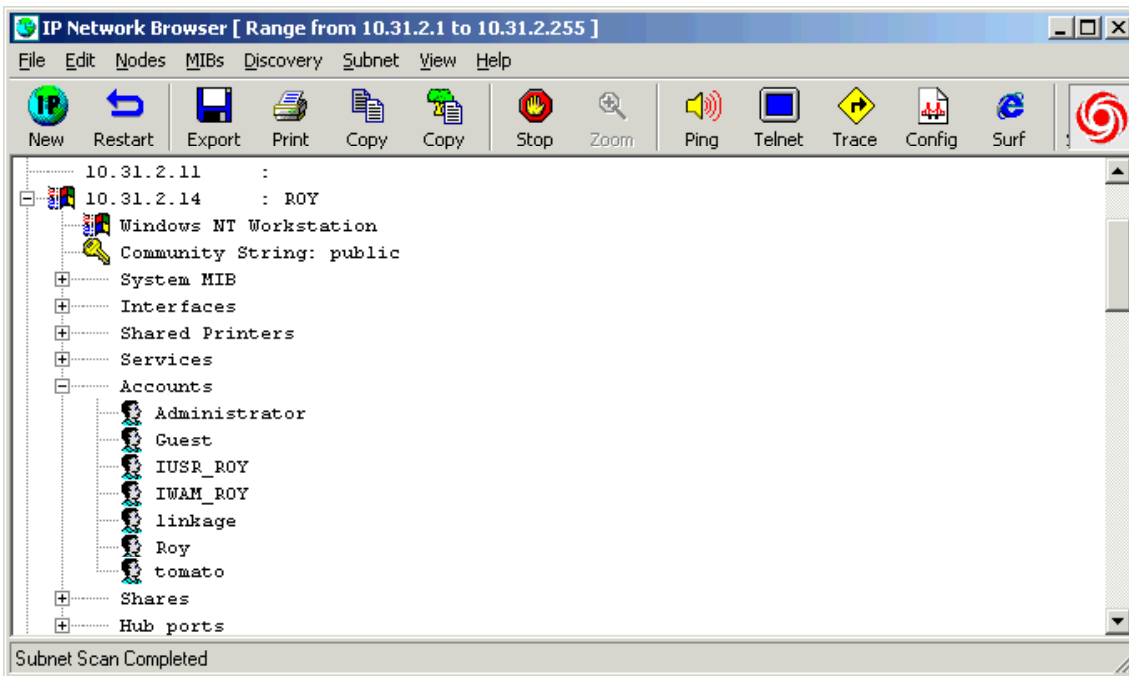
C:\>snmputil getnext 210.212.69.129 public interfaces.ifNumber.0
Variable = interfaces.ifTable.ifEntry.ifIndex.1
Value = Integer32 1

C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.1
Variable = interfaces.ifTable.ifEntry.ifIndex.2
Value = Integer32 2

C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.2
Variable = interfaces.ifTable.ifEntry.ifIndex.3
Value = Integer32 3

C:\>snmputil getnext 210.212.69.129 public 0.0
Variable = system.sysDescr.0
Value = String <0x43><0x69><0x73><0x63><0x6f><0x20><0x49><0x6e><0x74><0x65><0x72><0x6e><0x65><0x74><0x77><0x6f><0x72><0x6b><0x20><0x4f><0x70><0x65><0x72><0x61><0x74><0x69><0x6e><0x67><0x20><0x53><0x79><0x73><0x74><0x65><0x6d><0x20><0x53><0x6f><0x66><0x74><0x77><0x61><0x72><0x65><0x20><0x0d><0x0a><0x49><0x4f><0x53><0x20><0x28><0x74><0x6d><0x29><0x20><0x32><0x35><0x30><0x30><0x20><0x53><0x6f><0x66><0x67><0x74><0x77><0x61><0x72><0x65><0x20><0x28><0x43><0x32><0x35><0x30><0x30><0x2d><0x49><0x2d><0x4c><0x29><0x2c><0x20><0x56><0x65><0x72><0x73><0x69><0x6f><0x6e><0x20><0x31><0x31><0x2e><0x32><0x28><0x31><0x30><0x61><0x29><0x2c><0x20><0x52><0x45><0x4c><0x45><0x41><0x53><0x45><0x20><0x53><0x4f><0x46><0x54><0x57><0x41><0x52><0x45><0x20><0x28><0x66><0x63><0x31><0x29><0x0d><0x0a><0x43><0x6f><0x70><0x79><0x72><0x69><0x67><0x68><0x74><0x20><0x28><0x63><0x29><0x20><0x31><0x39><0x38><0x36><0x2d><0x31><0x39><0x39><0x37><0x20><0x62><0x79><0x20><0x63><0x69><0x73><0x63><0x6f><0x20><0x53><0x79><0x73><0x74><0x65><0x6d><0x73><0x2c><0x20><0x49><0x6e><0x63><0x2e><0x0d><0x0a><0x43><0x6f><0x6d><0x70><0x69><0x6c><0x65><0x64><0x20><0x54><0x75><0x65><0x20><0x30><0x32><0x2d><0x44><0x65><0x63><0x2d><0x39><0x37><0x20><0x31><0x36><0x3a><0x30><0x32><0x20><0x62><0x79><0x20><0x63><0x6b><0x72><0x61><0x6c><0x69><0x6b>
```

# Tool: Solarwinds



Solarwinds is a set of network management tools

The tool set consists of the following:

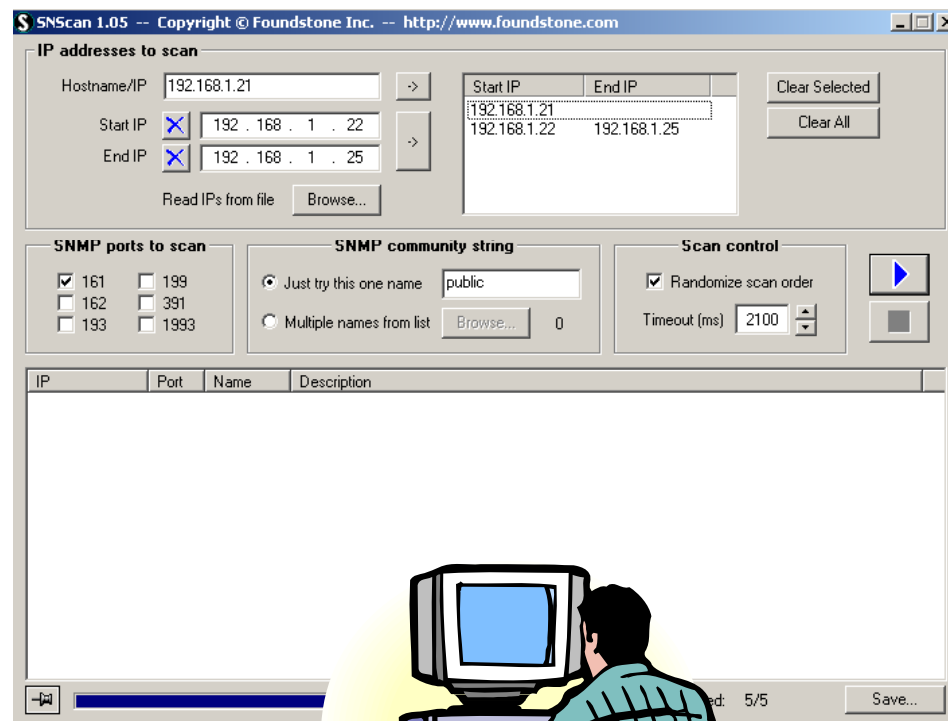
- Discovery
- Cisco Tools
- Ping Tools
- Address Management
- Monitoring
- MIB Browser
- Security
- Miscellaneous

# Tool: SNScan

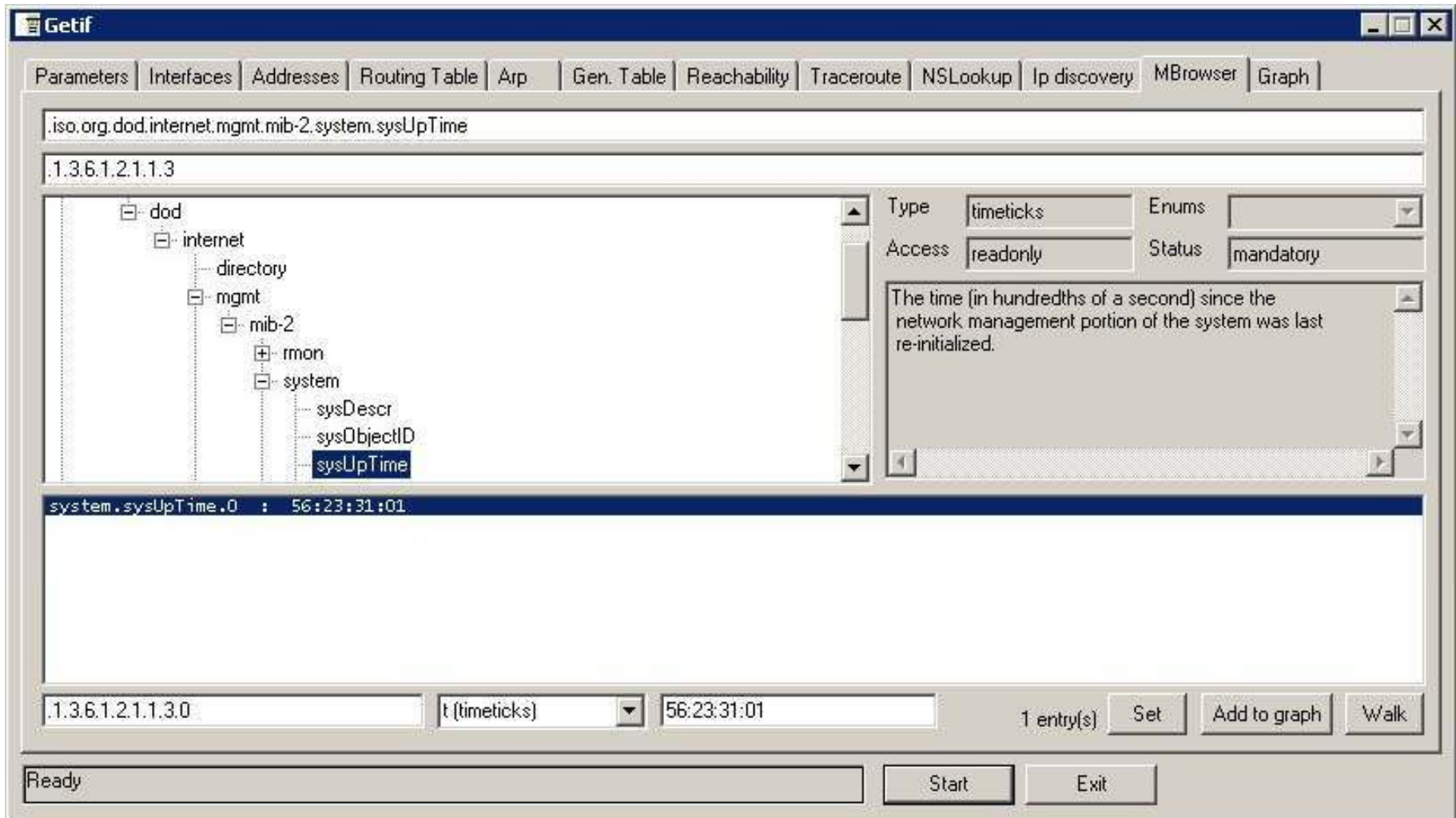
SNScan is a windows-based SNMP scanner that can effectively detect SNMP-enabled devices on the network

It scans specific SNMP ports and uses public and user-defined SNMP community names

It is a handy tool for information gathering



# Getif SNMP MIB Browser



Commands used to enumerate Unix network resources are as follows:

## showmount:

- Finds the shared directories on the machine
  - [root \$] showmount -e 19x.16x. xxx.xx

## Finger:

- Enumerates the user and host
- Enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail
  - [root\$] finger -l @target.hackme.com

## rpcinfo:

- Helps to enumerate Remote Procedure Call protocol
- RPC protocol allows applications to talk to one another over the network
  - [root] rpcinfo -p 19x.16x.xxx.xx

# SNMP UNIX Enumeration

An SNMP agent in the Unix platform can be enumerated using the snmpwalk tool

SNMP running on UDP port 161 can be enumerated using the command:

- [root] # nmap -sU -p161 19x.16x.1.60
- Query is passed to any MIB agent with snmpget:
  - [root] # snmpwalk 19x.16x.x.xx public system.  
Sysname.x

Countermeasures:

- Ensure proper configuration with required names “PUBLIC” and “PRIVATE.”
- Implement SNMP v3 version which is a more secure version

# SNMP Enumeration Countermeasures

Simplest way to prevent such activity is to remove the SNMP agent or turn off the SNMP service

If shutting off SNMP is not an option, then change the default “public” community’s name

Implement the Group Policy security option called “Additional restrictions for anonymous connections.”

Access to null session pipes, null session shares, and IPsec filtering should also be restricted



# LDAP Enumeration

The Lightweight Directory Access Protocol is a protocol used to access directory listings within Active Directory or from other Directory Services

A directory is compiled in an hierarchical and logical format, like the levels of management and employees in a company

It tends to be tied into the Domain Name System to allow integrated quick lookups and fast resolution of queries

It runs on port 389, and tends to usually conform to a distinct set of rules (RFC's) like other protocols





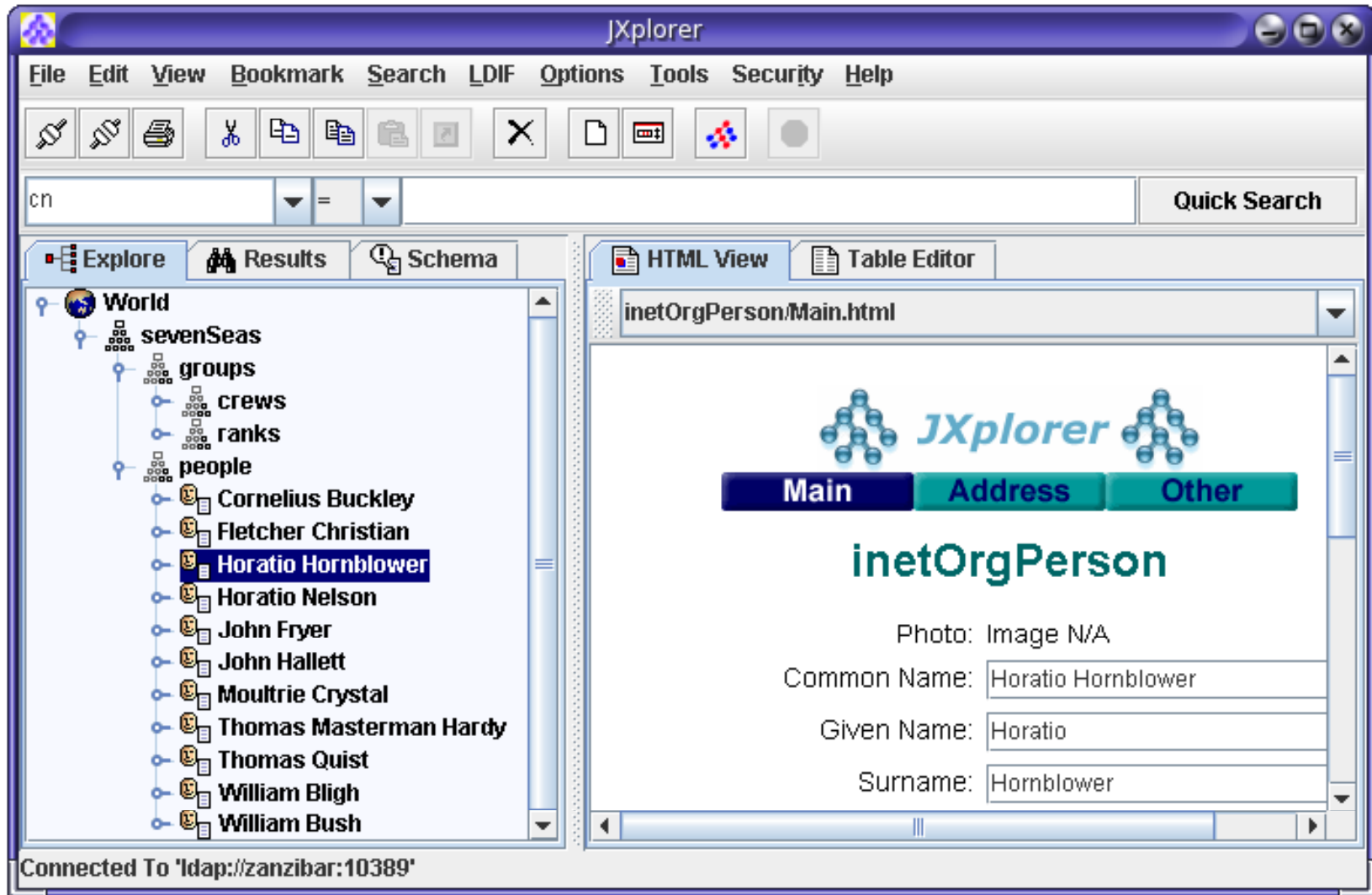
JXplorer is a free general purpose LDAP browser used to read and search any LDAP directory, or any X500 directory with an LDAP interface

### Features:

- Standard LDAP operations: add/ delete/ copy/ modify
- Complex operations: tree copy and tree delete
- Optional GUI based search filter construction
- SSL and SASL authentication
- Pluggable editors/ viewers
- Pluggable security providers
- HTML templates/ forms for data display
- LDIF file format support
- DSML Support



# Jxplorer: Screenshot



LdapMiner is a tool that collects information from different LDAP Server implementations

LDAP is a protocol used to access directory listings within active directory

It is implemented in web browsers and e-mail programs to enable lookup queries

```
ldapminer.exe -h host option  
-p [port] : default to 389  
-B [bind dn] : user. default null  
-w [password] : user password. default null  
-b [base search] : base for searching for user, group, ...  
-F [output format] : 0 for ldif, 1 for clean  
-d : dump all data you can grab
```



# LdapMiner: Screenshot

## Expected output:

```
checking if server is alive
Connected to : 192.169.1.119
server type is : netscape
Netscape Checks enabled
Problem getting some server config info, results might not be 100% reliable

Netscape Admin server checks
=====

Netscape server checks
=====

Netscape base checks
=====
Netscape users
CN=Schema,CN=Configuration,DC=kev,DC=local:
CN=Configuration,DC=kev,DC=local:
DC=kev,DC=local:
Netscape groups :

CN=Schema,CN=Configuration,DC=kev,DC=local:

CN=Configuration,DC=kev,DC=local:

DC=kev,DC=local:
Netscape ACL :

LDAP server data available (clean output)
=====
dn: CN=Schema,CN=Configuration,DC=kev,DC=local
dn: CN=Configuration,DC=kev,DC=local
dn: CN=Everyone,CN=WellKnown Security Principals,CN=Configuration,DC=kev,DC=local
attribute: cn
```

# Softerra LDAP Browser

Softerra LDAP Browser is a free lightweight version of Softerra's LDAP Administrator with reduced functionality

It does not allow its users to modify discovered LDAP directories

It allows to access:

- OpenLDAP
- Netscape/ iPlanet
- Novell eDirectory
- Oracle Internet Directory
- Lotus Domino or Microsoft Active Directory

It supports the following open standards:

- DSML v1
- DSML v2
- XML-RPC
- XSLT



# Softerra LDAP Browser: Screenshot

The screenshot shows the Softerra LDAP Browser interface. The window title is "dc=OpenLDAP,dc=org". The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar with navigation and search icons, and a search filter set to "(objectClass=\*)".

The left pane shows a tree view of the LDAP directory structure:

- Browser root
  - OpenLDAP
    - dc=OpenLDAP
      - cn=Directory Manager
      - ou=People
        - uid=kurt
        - uid=kdz
        - uid=hyc
        - uid=venaas
      - ou=Groups

Name	Value	Type	Size
cn	Directory Manager	entry	267
ou	People	entry	52
ou	Groups	entry	52
objectClass	top	text ...	3
objectClass	organization	text ...	12
objectClass	OpenLDAPorg	text ...	11
objectClass	dcObject	text ...	8
objectClass	domainRelatedObject	text ...	19
dc	OpenLDAP	text ...	8
displayName	OpenLDAP Project	text ...	16
o	OpenLDAP Project	text ...	16
o	OpenLDAP Foundation	text ...	19
o	OpenLDAP	text ...	8
l	Internet	text ...	8
description	OpenLDAP - community developed software	text ...	39

Output

```
Successfully connected to ldap.openldap.org
Schema cache does not exist or expired. Fetching new one...
LDAP Syntaxes: Total: 31 Invalid: 0 Duplicated: 0
AttributeTypes: Total: 231 Invalid: 0 Duplicated: 0
LDAPObjectClasses: Total: 65 Invalid: 0 Duplicated: 0
MatchingRules: Total: 36 Invalid: 0 Duplicated: 0
MatchingRulesUse: Total: 27 Invalid: 0 Duplicated: 0
```

Messages

Ready. For Help, press F1

Anonymous

Schema loaded

# NTP Enumeration

Network Time Protocol is designed to synchronize clocks of networked computers

NTP uses UDP port 123 as its primary means of communication

It is designed to resist the effects of the variable latency

The following commands are used against an NTP server:

`ntpdate`

`ntptrace`

`ntpdc`

`ntpq`



# SMTP Enumeration

Simple Mail Transport Protocol is used to send email messages as opposed to POP3 or IMAP which can be used to both send and receive messages

It generally relies on using Mail Exchange (MX) servers to direct the mail via the Domain Name Service

It operates over TCP port 25

On Unix-based systems, sendmail is the most widely-used SMTP server for e-mail





It is possible to directly interact with SMTP via the use of a telnet prompt:

```
telnet 192.168.0.1 25
220 uk03.cak.uk ESMTP Sendmail 8.9.3; Wed, 9 Nov 2005 15:29:50 GMT
EXPN ROOT
250 <root@uk03.nu.cak.uk>
250 <smith.j@uk03.nu.cak.uk>
EXPN BIN
250 <bin@uk03.nu.cak.uk>
VRFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VRFY ORACLE
550 ORACLE... User unknown
QUIT
```

Smtpscan is a remote SMTP server version detector

It is used to identify which mail software is used on a remote server, especially when banner obfuscation is taking place

It works by testing the remote SMTP server reaction using a series of predefined tests

After completion of testing, the remote server returns a SMTP Error Message

Fingerprints are made of SMTP error messages corresponding to these test requests and responses

Smtpscan tries to find the nearest fingerprint if there is no exact match, that is it finds the fingerprint that has fewer error messages



# Web Enumeration

Hyper Text Transfer Protocol is used by World Wide Web to display and distribute the information

A client usually sends a request and the server duly responds

The means of access to the specific information using HTTP is usually by means of user supplied Uniform Resource Locators (URL's)

The DNS will then look up the URL and translate this to the URL's corresponding IP Address and the message is then sent to the server

HTTP uses TCP Port 80 and HTTPS uses TCP Port 443 as its communications channels



Asnumber extension displays an Internet Service Provider of every website visited along with some additional information

For Firefox, it displays the Asnumber

All data are updated daily and the prefix to AS number mapping is from a real DFZ BGP feed

```
AS15169  
Prefixes : 67  
IP addrs : 70912  
IP/Prefix : 1058  
AS name : GOOGLE  
AS descr : Google Inc.  
Country : US  
Allocated : 20000330  
RIR : ARIN  
BGP Prefix  
Prefix : 64.233.182.0/23
```

AS15169

Lynx is the text web browser

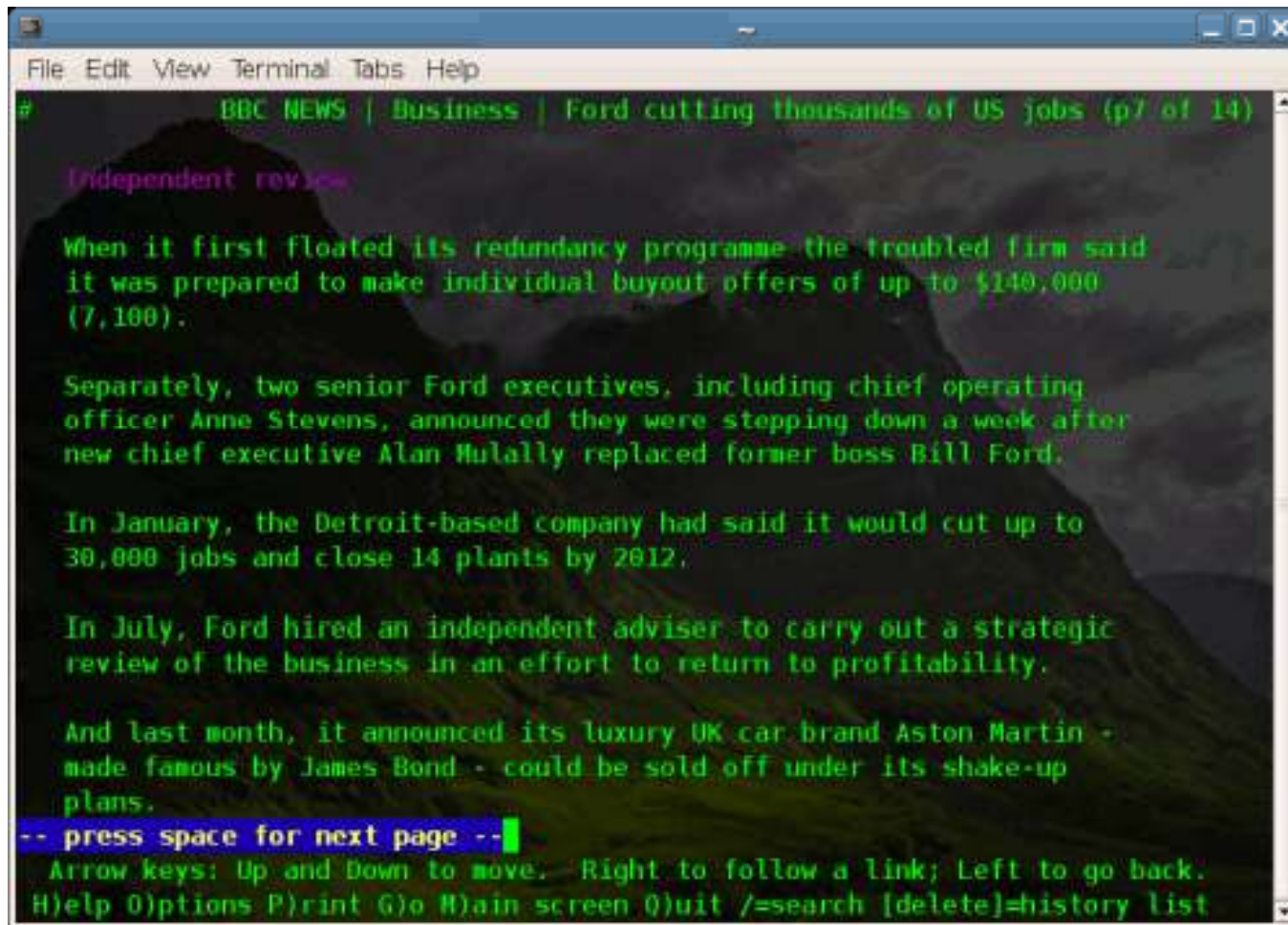
This browser will not display any images, so web pages are loaded very quickly

It allows pen tester to create a list of available pages within a particular website



# Lynx: Screenshot

Screenshot of the BBC News viewed with Lynx



```
File Edit View Terminal Tabs Help
#      BBC NEWS | Business | Ford cutting thousands of US jobs (p7 of 14)

Independent review

When it first floated its redundancy programme the troubled firm said
it was prepared to make individual buyout offers of up to $140,000
(7,100).

Separately, two senior Ford executives, including chief operating
officer Anne Stevens, announced they were stepping down a week after
new chief executive Alan Mulally replaced former boss Bill Ford.

In January, the Detroit-based company had said it would cut up to
30,000 jobs and close 14 plants by 2012.

In July, Ford hired an independent adviser to carry out a strategic
review of the business in an effort to return to profitability.

And last month, it announced its luxury UK car brand Aston Martin -
made famous by James Bond - could be sold off under its shake-up
plans.

-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

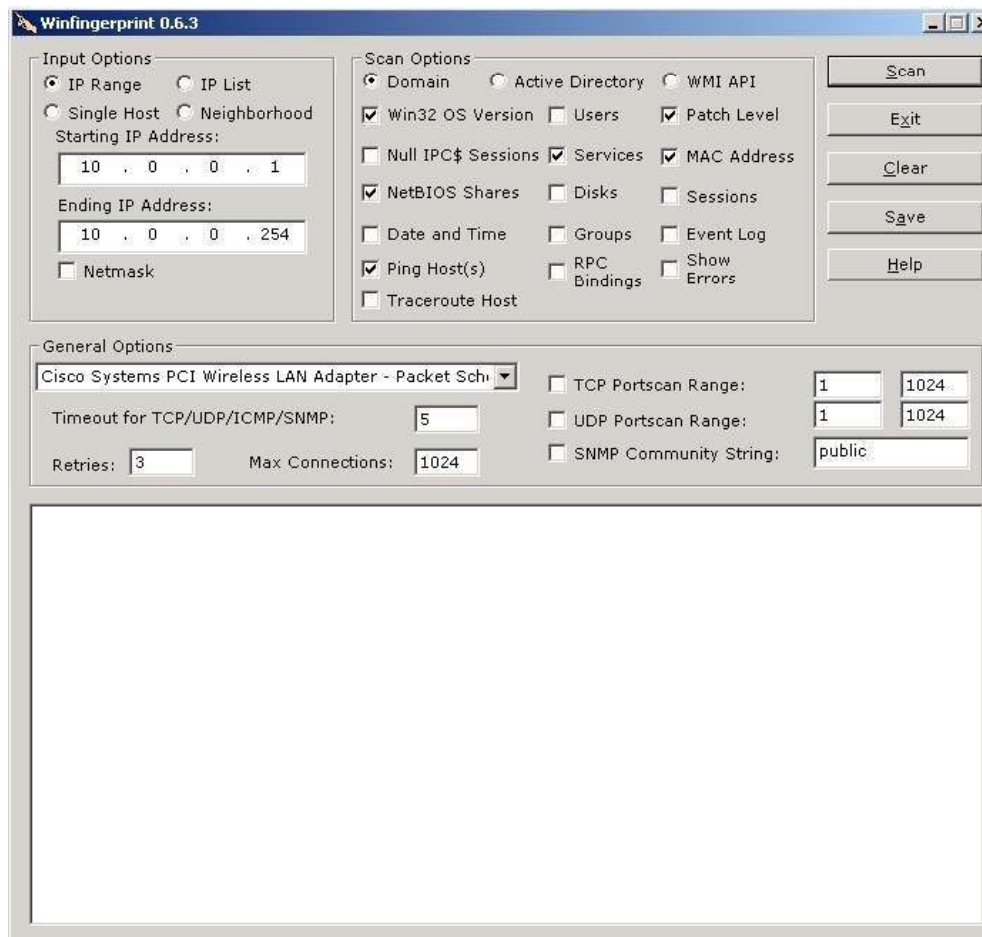
# Tool: Winfingerprint

Winfingerprint is GUI-based

It has the option of scanning a single host or a continuous network block

Has two main windows:

- IP address range
- Windows options



# Windows Active Directory Attack Tool

w2kdad.pl is a perl script that attacks Windows 2000/2003 against Active Directory

Enumerates users and passwords in a native W2k AD

There is an option to use SNMP to gather user data, as well as a DoS option to lock out every user found

A successful DoS attack will depend on whether or not the domain has account lockout enabled

```
#####
# End of Subroutine LoadPasswordFile
#####
# IP_check
# Description:
# IP_check checks the IP-address and returns "1" for a valid :
# or "0" for an invalid IP-address to the calling routine
#####

sub IP_check {

#####
### Declare local variables start
#####

    my $A;
    my $B;
    my $C;
    my $D;
    my $IP_address;
    my $error=0;
    my $success=1;
    my @number_of_groups;

#####
### Declare local variables end
#####

# Grab the IP-address to scan

    $IP_address = <@_>;

# Check that the IP-address consists of 4 groups divided by dots
# For some reason Perl wants an array here, instead of a scalar otherwise
```





# How To Enumerate Web Application Directories in IIS Using Directory Services

This work is accomplished by `DirectoryEntry` class

Specify the `ADsPath` for the web server and the object you are looking for and then call `Children` property to get the list of children items

A general `ADsPath` can be specified as `IIS://MachineName/W3SVC/N/Root`

This path returns list of all `IISWebVirtualDir` and `IISWebDirectory` containers

Check `SchemaClassName` value for each child `DirectoryEntry` object returned by `Children` property

The objects whose class name matches "`IISWebDirectory`" is added to the `StringCollection` for later display

# How To Enumerate Web Application Directories in IIS Using DirectoryServices (cont'd)

```
public stringCollection GetIISVirtualFolders(string strServer)
{
    stringCollection strColl = null;
    DirectoryEntry objDirEntry = null;
    DirectoryEntries objDirEntList = null;
    try
    {
        objDirEntry = new DirectoryEntry("IIS://" + strServer + "/w3svc/1/Root");
        objDirEntList = objDirEntry.Children;

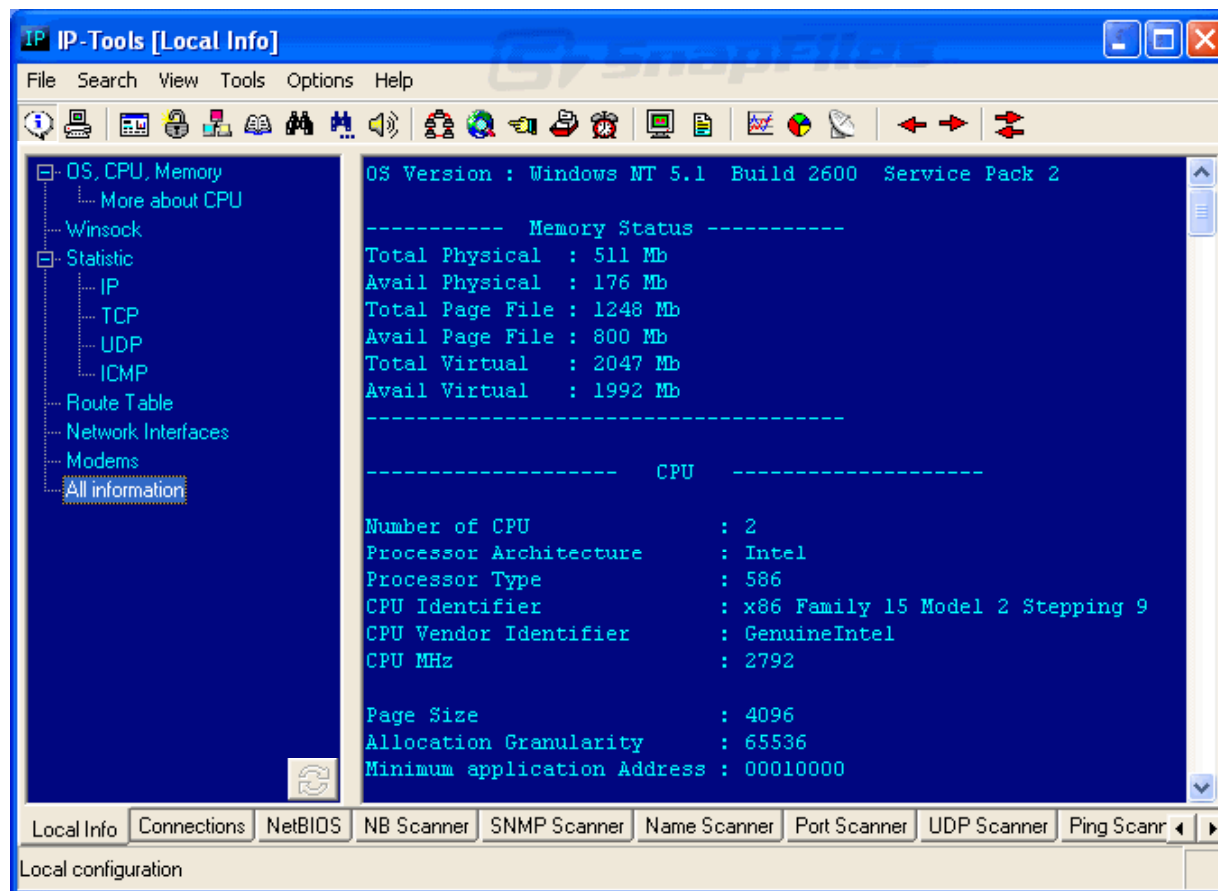
        // Process each child entry and add the name of virtual folder
        // to string collection.
        strColl = new stringCollection();
        foreach(DirectoryEntry objChildDE in objDirEntList)
        {
            ProcessSDEFForIISVFolder(objChildDE, strColl);
        }
    }
    catch (Exception ex)
    {
        Trace.Write(ex.Message);
        return null;
    }
    return strColl;
}

private void ProcessSDEFForIISVFolder(DirectoryEntry ob, stringCollection strColl)
{
    try
    {
        // Check if the schema class is Iiswebvirtualdir or not.
        if (0 == String.Compare( ob.SchemaClassName, "Iiswebdirectory"))
        {
            strColl.Add(ob.Name);
        }
    }
    catch (Exception ex)
    {
        Trace.WriteLine(ex.Message);
    }
}
```

# IP Tools Scanner

IP Tools is a complete suite of 19 essential TCP/IP networking utilities that include :

- Local Info
- Connections Monitor
- NetBIOS Scanner
- Shared resources
- Scanner, SNMP
- Scanner, HostName
- Scanner, Ports
- Scanner, UDP Scanner
- Ping Scanner
- Trace, LookUp
- Finger
- WhoIs
- Time Synchronizer
- Telnet client
- HTTP client
- IP-Monitor
- Hosts Monitor and SNMP Trap Watcher



# Enumerate Systems Using Default Passwords

## Default Password List

2006-09-14

Manufacturer	Product	Revision	Protocol	User ID	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LANplex	2500	Telnet	tech	tech
3COM	LinkSwitch	2000/2700	Telnet	tech	tech

Many devices like switches/hubs/routers might still be enabled with a “default password”

Try to gain access using default passwords

[www.phenoelit.de/dpl/dpl.html](http://www.phenoelit.de/dpl/dpl.html) contains interesting list of passwords

# Tool: NBTScan

NBTscan is a program for scanning IP networks for NetBIOS name information

It sends NetBIOS status query to each address in supplied range and lists received information in human readable form

For each responded host it lists:

IP address

NetBIOS computer name

Logged-in user name

MAC address

# NBTScan: Screenshot

```
Command Prompt
D:\security\nbtscan>nbtscan

NBTscan version 1.0.2. Copyright (C) 1999-2000 Alla Bezroutchko.
This is a free software and it comes with absolutely no warranty.
You can use, distribute and modify it under terms of GNU GPL.

Usage:
nbtscan [-v] [-d] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] <scan_range>
-v          verbose output. Print all names received from each host
-d          dump packets. Print whole packet contents. Cannot be used with -v, -s or -h options.
-t timeout  wait timeout seconds for response. Default 1.
-b bandwidth Output throttling. Slow down output so that it uses no more that bandwidth bps. Useful on slow links, so that outgoing queries don't get dropped.
-r          use local port 137 for scans. Win95 boxes respond to this only. You need to be root to use this option on Unix.
-q          Suppress banners and error messages.
-s separator Script-friendly output. Don't print column and record headers, separate fields with separator.
-h          Print human-readable names for services. Can only be used with -v option.
-m retransmits Number of retransmits. Default 0.
<scan_range> what to scan. Can either be single IP like 192.168.1.1 or range of addresses in one of two forms: xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.

Examples:
nbtscan -r 192.168.1.0/24
Scans the whole C-class network.
nbtscan 192.168.1.25-137
Scans a range from 192.168.1.25 to 192.168.1.137
nbtscan -v -s : 192.168.1.0/24
Scans C-class network. Prints results in script-friendly format using colon as field separator.
Produces output like that:
192.168.0.1:NT_SERVER:00U
```

# Tool: NetViewX

NetViewX is a tool to list the servers in a domain or workgroup

It is a bit like the NT "net view / domain" command

It allows to list only servers with specific services

It uses a list format that is easily parsable



```
command prompt
C:\tools\netviewx>netviewx
Server1_5.1.500.nt\workstation\server\printq_server\potential_brouser\master_bro
user, ""
DevComputer_5.1.500.nt\workstation\server\potential_brouser, ""
Server2_5.0.500.nt\workstation\server_nt\server\dialin_server\backup_brouser\200
0000, ""
WIN2K3_5.2.500.nt\workstation\server_nt\server\dfs, ""
C:\tools\netviewx>
```

# Tool: FreeNetEnumerator

FreeNetEnumerator is a tool to enumerate computers in a domain

This tool can work in different ways depending on the enumeration parameters provided

It can enumerate:

- All computers ( if all computers are selected )
- All SQL servers only (if Microsoft SQL Servers are selected)
- All primary domain controllers only(if Primary domain controllers is selected )
- Backup domain controllers only (f Backup domain controllers is selected)
- Primary domains only (if Primary domains is selected)



# FreeNetEnumerator: Screenshot



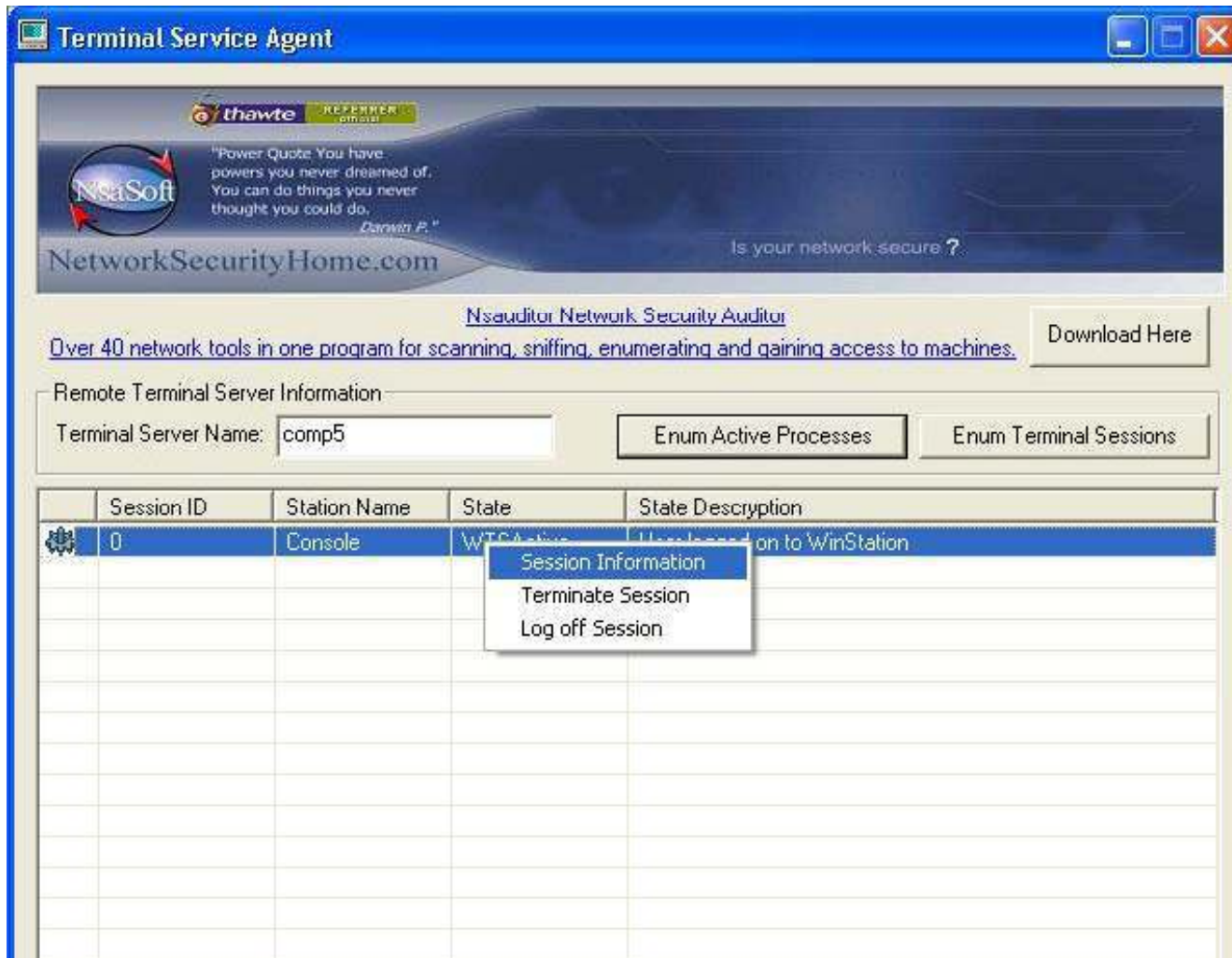
# Terminal Service Agent

Terminal Service Agent allows to enumerate and control network terminal services and processes and allows to terminate or log off remotely

It shows remote network terminal service information like Initial Program, Application Name, Working Directory, OEM Id, Session Id, User Name, Windows Station Name, Domain Name, Connect State, Client Build Number, Client Name, Client Directory, Client Product Id, Client Hardware Id, Client Address, Client Display Resolution, and Client Protocol Type



# Terminal Service Agent: Screenshot



The screenshot shows the 'Terminal Service Agent' application window. At the top, there is a banner for 'thawte' and 'NsaSoft' with a quote from Darwin P. and the text 'Is your network secure?'. Below the banner, there is a link to 'Nsauditor Network Security Auditor' and a 'Download Here' button. The main section is titled 'Remote Terminal Server Information' and contains a text box for 'Terminal Server Name' with the value 'comp5'. To the right of this text box are two buttons: 'Enum Active Processes' and 'Enum Terminal Sessions'. Below these buttons is a table with the following columns: Session ID, Station Name, State, and State Description.

Session ID	Station Name	State	State Description
0	Console	WTCActive	Used based on WinStation

A context menu is open over the first row of the table, showing the following options:

- Session Information
- Terminate Session
- Log off Session

# Tool: TXDNS

TXDNS is a Win32 aggressive multithreaded DNS digger

It is capable of placing thousands of DNS queries per minute on the wire

Its main goal is to expose a domain namespace through a number of techniques

Use the following techniques:

Typos

TLD rotation

Dictionary attack

Brute force

# Tool: Unicornscan

Unicornscan is a new information gathering and correlation engine

It was designed to provide an engine that is scalable, accurate, flexible, and efficient

This tool is an attempt at a user-land distributed TCP/IP stack for and by members of the security research and testing communities



# Unicornscur: Screenshot

```
Eterm Font Background Terminal
root@rel:~# unicornscur
what host(s) should i scan?
unicornscur [dyadsecurity] (Version 0.4.2)
Usage: unicornscur [options `b;B;d;De;EFhi;L;m;M;pP;q;r;R;s;St;T;w;W;vWZ:' ] X.X.X.X/YY;S-E
  -b, --broken-crc      *[Set broken crc sums on [T]ransport layer, [N]etwork layer, or both[TN]]
  -B, --source-port    *[Set source port? or whatever the scan module expects as a number]
  -d, --delay-type     *[Set delay type (numeric value, valid options are `1:tsc 2:gtod 3:sleep'')]
  -D, --no-defpayload  [No default Payload, only probe known protocols]
  -e, --enable-module  *[enable modules listed as arguments (output and report currently)]
  -E, --show-errors    [for tracking icmp errors (*non-firewalled hosts normally) and rst packets]
  -h, --help           [help (you are reading it)] <---- YOU ARE HERE
  -i, --interface      *[interface name, like eth0 or fxp1, not normally required]
  -m, --mode           *[scan mode, tcp (syn) scan is default, U for udp T for tcp `sf' for tcp connect scan and A for arp]
                       for -mT you can also specify tcp flags following the T like -mTsFpU for example
                       that would send tcp syn packets with (NO Syn|FIN|NO Push|URG)
  -M, --module-dir     *[directory modules are found at (defaults to /usr/libexec/unicornscur/modules)]
  -p, --no-patience   [No patience, display things as we find them]
  -P, --pcap-filter    *[Extra pcap filter string for receiver]
  -q, --covertiness    *[Covertiness value from 0 to 255]
  -r, --pps            *[packets per second (total, not per host, and as you go higher it gets less accurate)]
  -R, --repeats        *[Repeat packet scan N times]
  -s, --source-addr    *[Source address for packets `r' for random]
  -S, --no-shuffle     [DON'T shuffle ports]
  -t, --ip-ttl         *[Set TTL on sent packets]
  -T, --ip-tos         *[set TOS on sent packets]
  -w, --safefile       *[Write pcap file of recieved packets]
  -W, --fingerprint   *[OS fingerprint 0=cisco(def) 1=openbsd 2=WindowsXP 3=p0fsendsyn 4=FreeBSD 5=nmap]
                       [6=linux 7:Crazy lint tcp header (use with p0f hopefully)]
  -v, --verbose        [verbose (each time more verbose so -vvvvv is really verbose)]
  -V, --version        [Display version]
  -Z, --drone-type     *[L or S]
*: Options with `*' require an argument following them

Address ranges are cidr like 1.2.3.4/8 for all of 1.?.?.?
if you omit the cidr mask then /32 is implied
port ranges are like 1-4096 with 53 only scanning one port, a for all 65k and p for 1-1024
example: unicornscur -i eth1 208.47.125.0/24:1-4000 -pr 160 -E
root@rel:~#
```

# Tool: Amap

Amap is a next-generation scanning tool for pentesters

It is used to identify applications even if they are running on a different port than normal

It also identifies non-ascii based applications

This is achieved by sending trigger packets, and looking up for the responses in a list of response strings



# Tool: Netenum

Netenum comes as a part of the IRPAs suite of tools

It can be used to produce lists of hosts for other programs

It is a basic ping sweeper and enumeration tool

While giving a timeout, it uses ICMP echo request to find the available hosts

It just prints an IP address per line, if you do not give the timeout. So you can use them in shell scripts



# Netenum: Screenshot



# Steps to Perform Enumeration

Extract user names using win 2k enumeration

Gather information from the host using null sessions

Perform Windows enumeration using the tool Super Scan4

Get the users' accounts using the tool GetAcct

Perform an SNMP port scan using the tool SNScan



# What Happened Next

Dennis applied different social engineering techniques on his friend to guess his password correctly. He was surprised to see that he could access all the classified information available over the library intranet which was available only for US\$ 500 premium membership subscriptions



Enumeration involves active connections to systems and directed queries

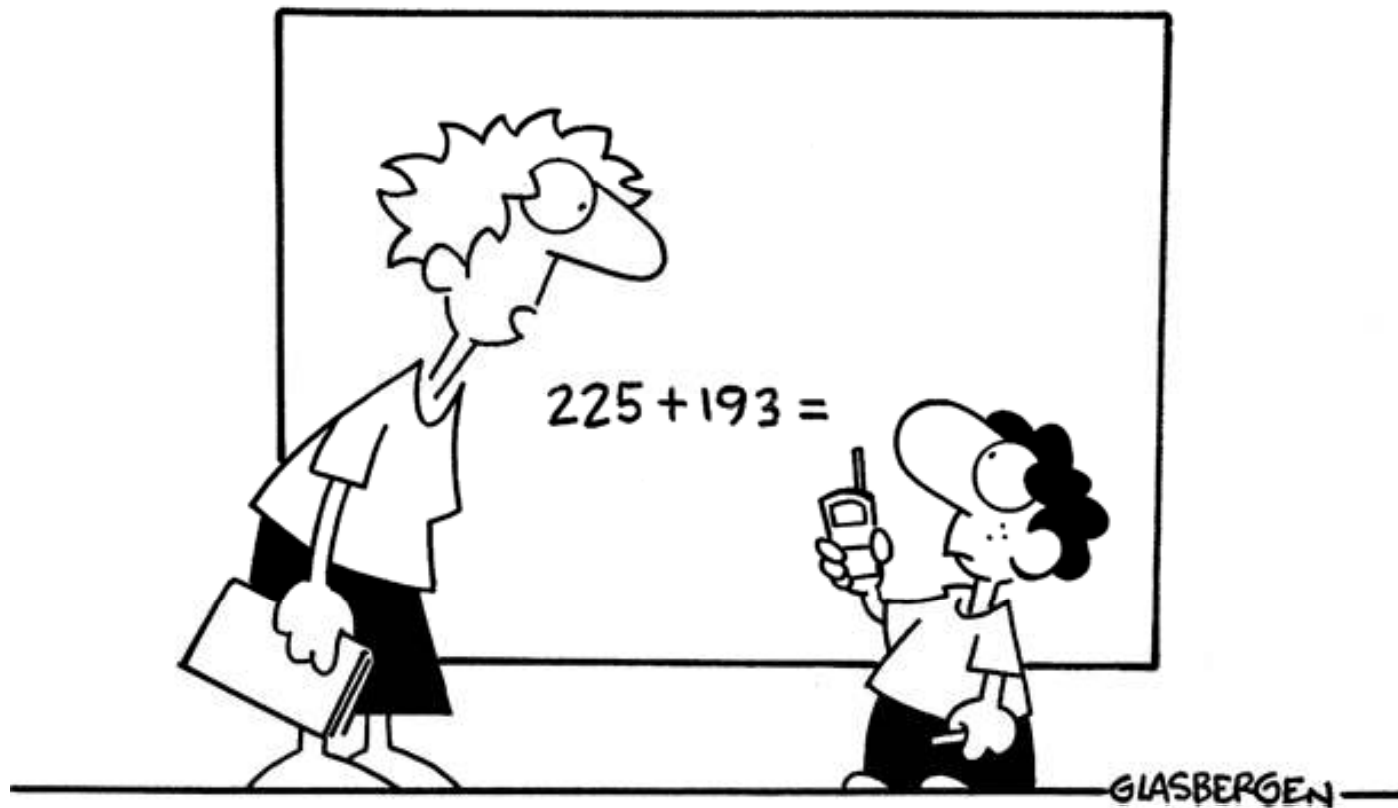
The type of information enumerated by intruders includes network resources and shares, users and groups, and applications and banners

Crackers often use Null sessions to connect to the target systems

NetBIOS and SNMP enumerations can be disguised using tools such as snmputil, and nat

Tools such as user2sid, sid2user, and userinfo can be used to identify vulnerable user accounts

Copyright 2005 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“You have to solve this problem by yourself. You can’t call tech support.”**

Copyright 2002 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



**“Someone got my Social Security number off the internet  
and stole my identity. Thank God — *I hated being me!*”**