Ethical Hacking and Countermeasures

Version 6

Module VI

Enumeration

Scenario

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?

Associated Press

Go to Google News

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

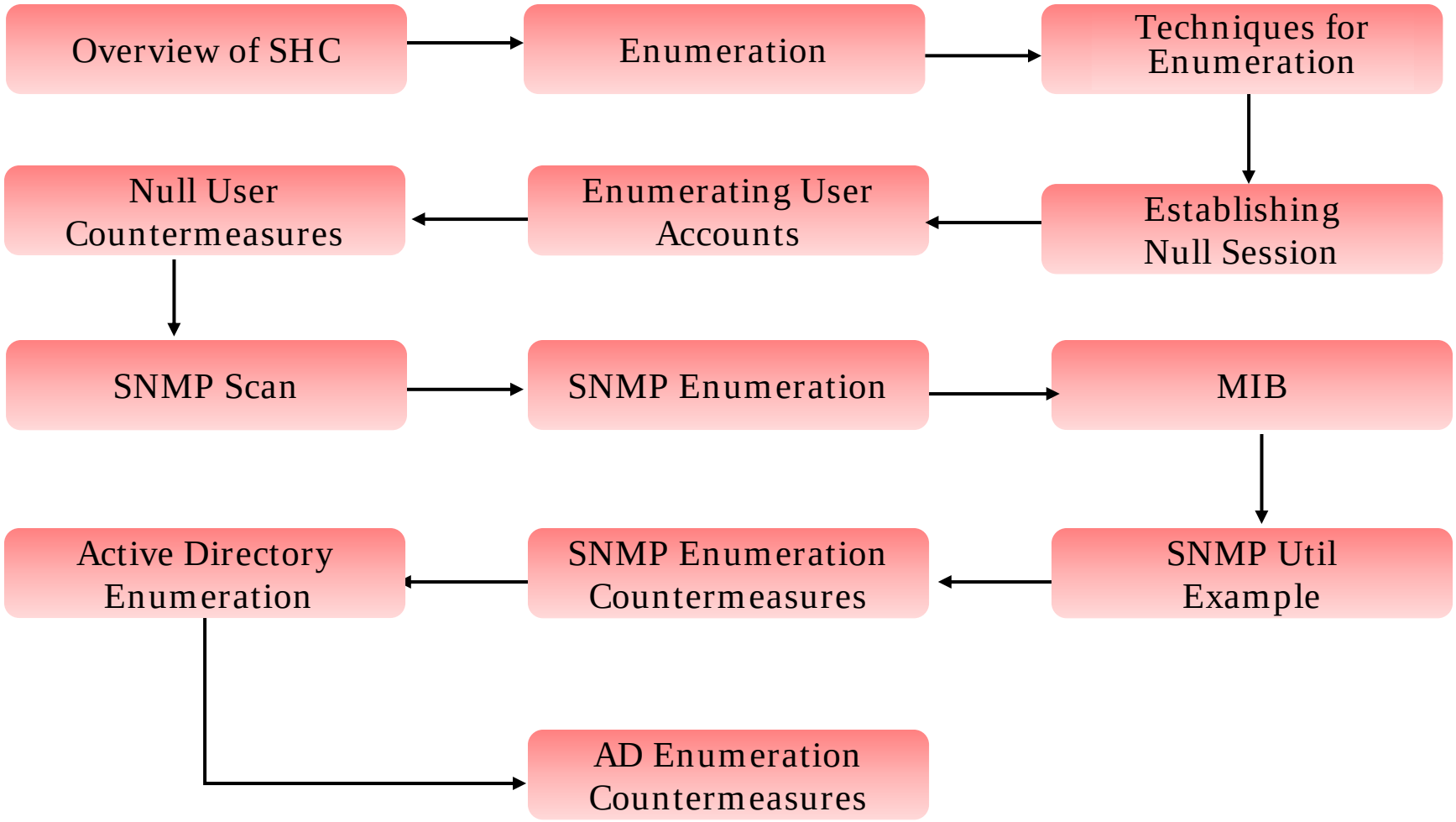
Source: *http://ap.google.com/*

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

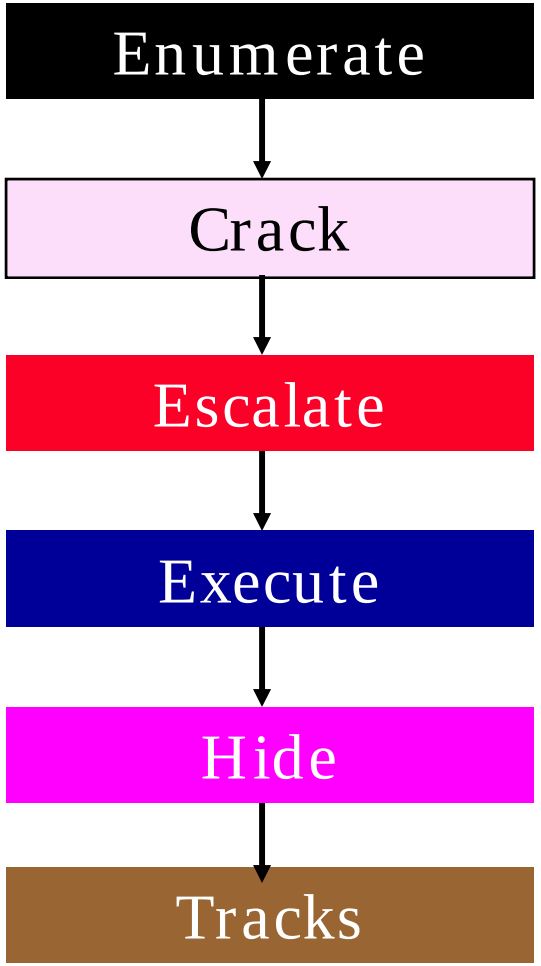
- Plant keyloggers, spywares, and rootkits on the machine

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

Techniques for Enumeration

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 refereed 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

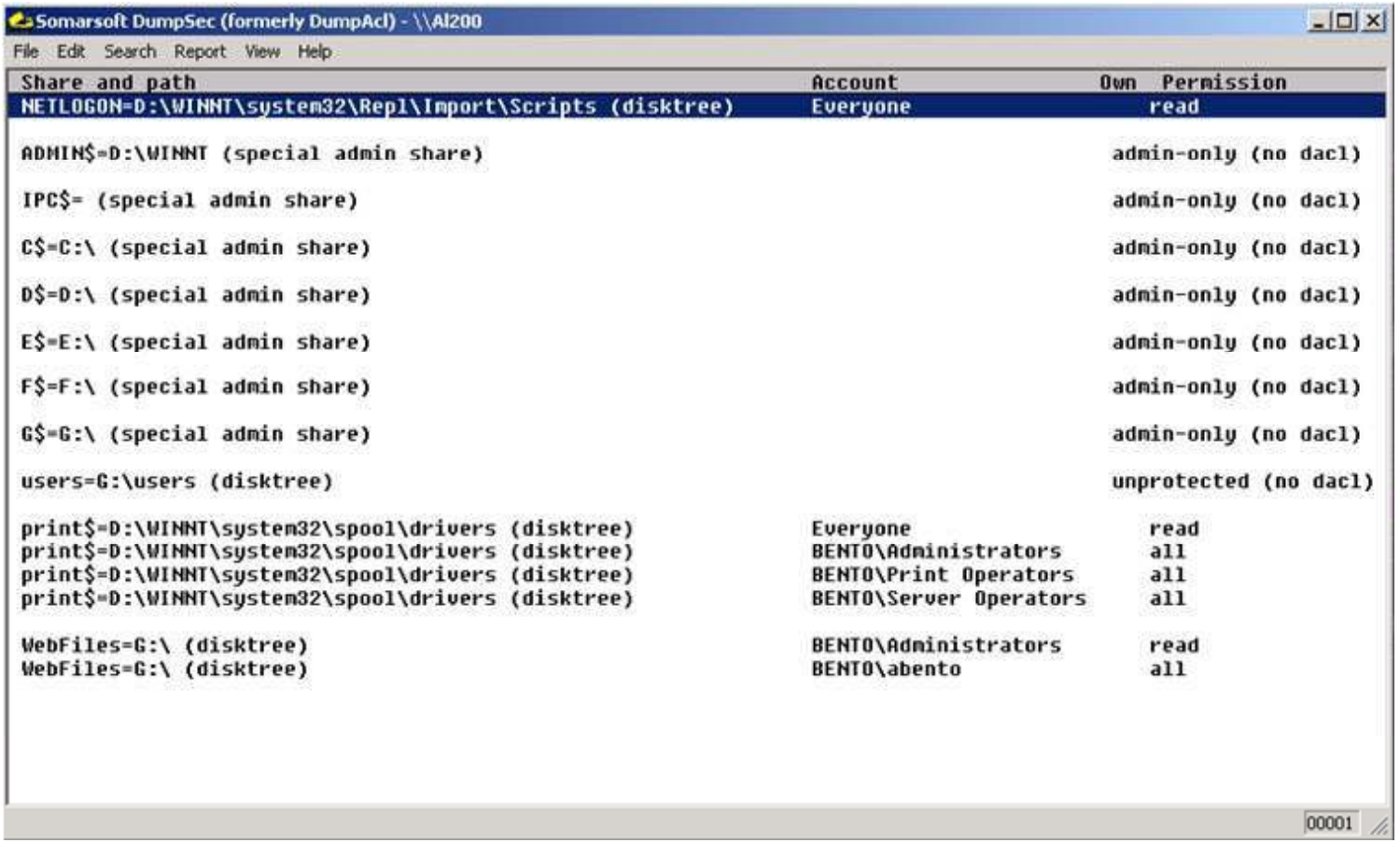
The CIFS/SMB and NetBIOS standards in Windows 2000 include APIs that return rich information about a machine via TCP port 139—even to the unauthenticated users

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



NetBIOS Enumeration Using Netview

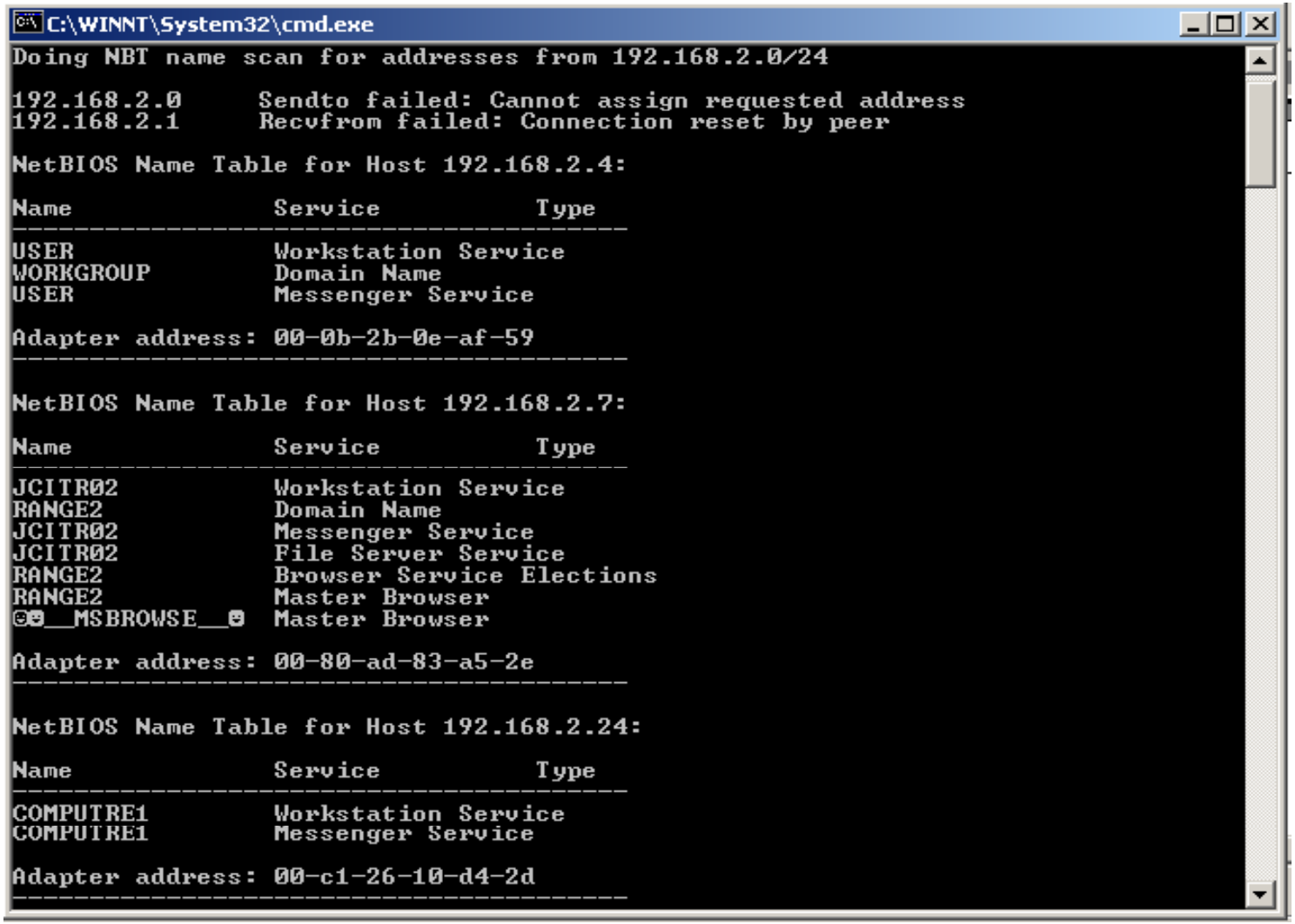
The Netview tool allows you to gather two essential bits of information:

- 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)



Nbtstat Enumeration Tool

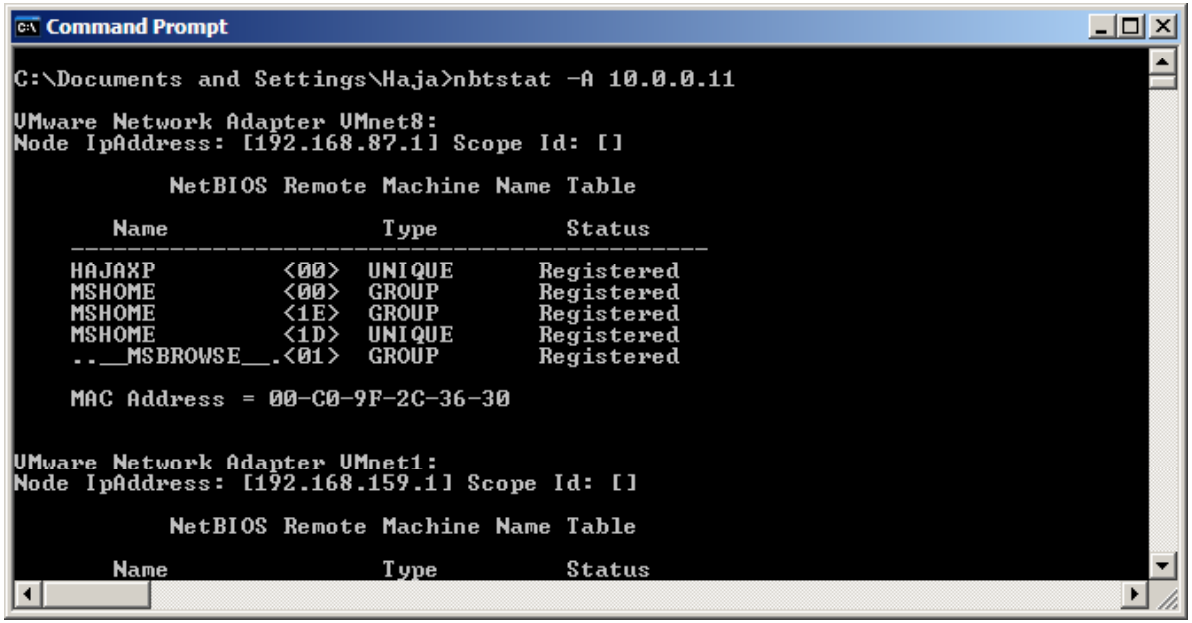
Nbtstat is a Windows command-line tool that can be used to display information about a computer's NetBIOS connections and name tables

- Run:`nbtstat –A <some ip address>`

C:\nbtstat

- Displays protocol statistics and current TCP/IPconnections using NBT(NetBIOS over TCP/IP).

```
NBTSTAT [-a      RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S]
     [interval] ]
```



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

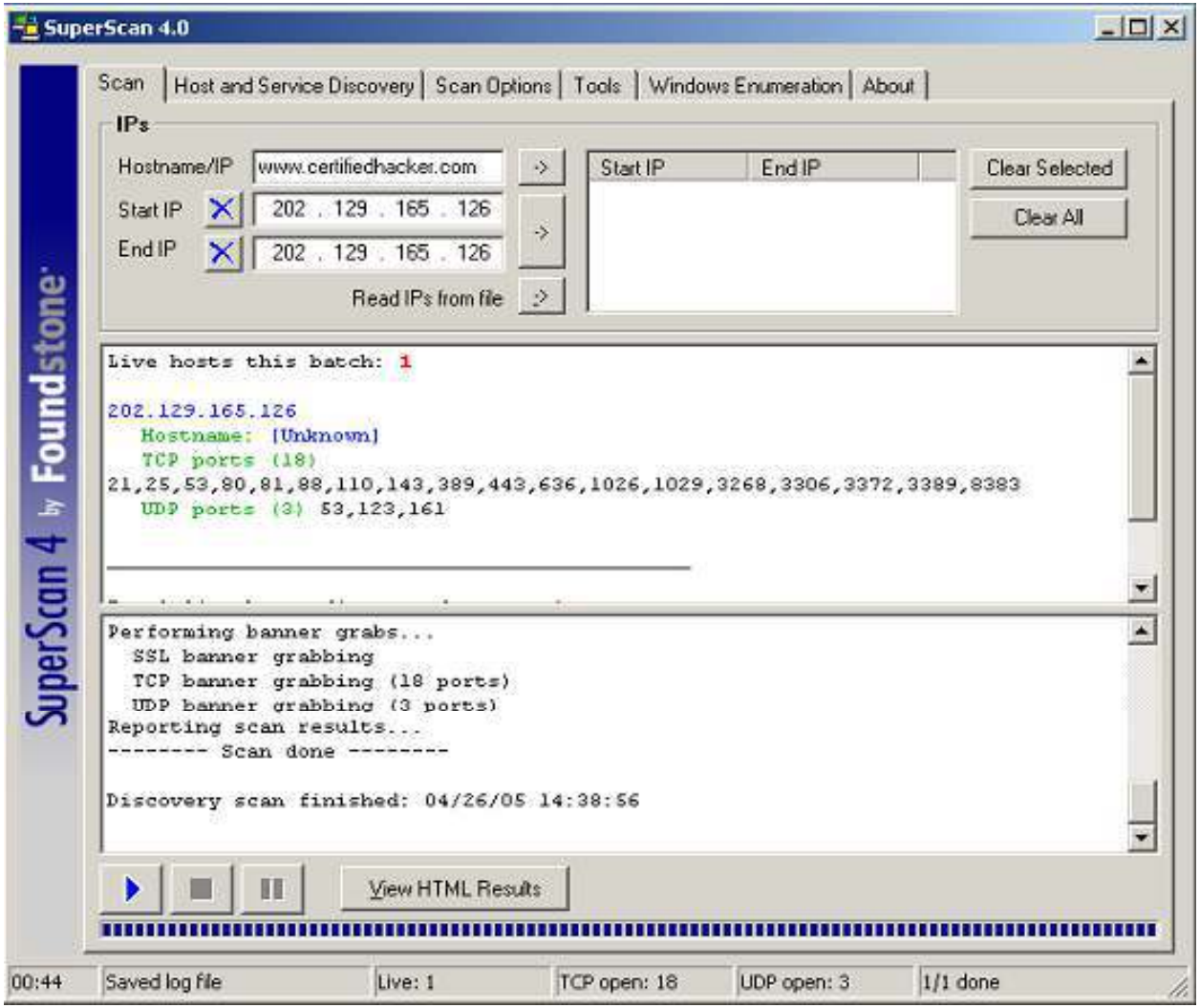
Scans any port range from a built-in list or specified range

Resolves and reverse-lookup any IP address or range

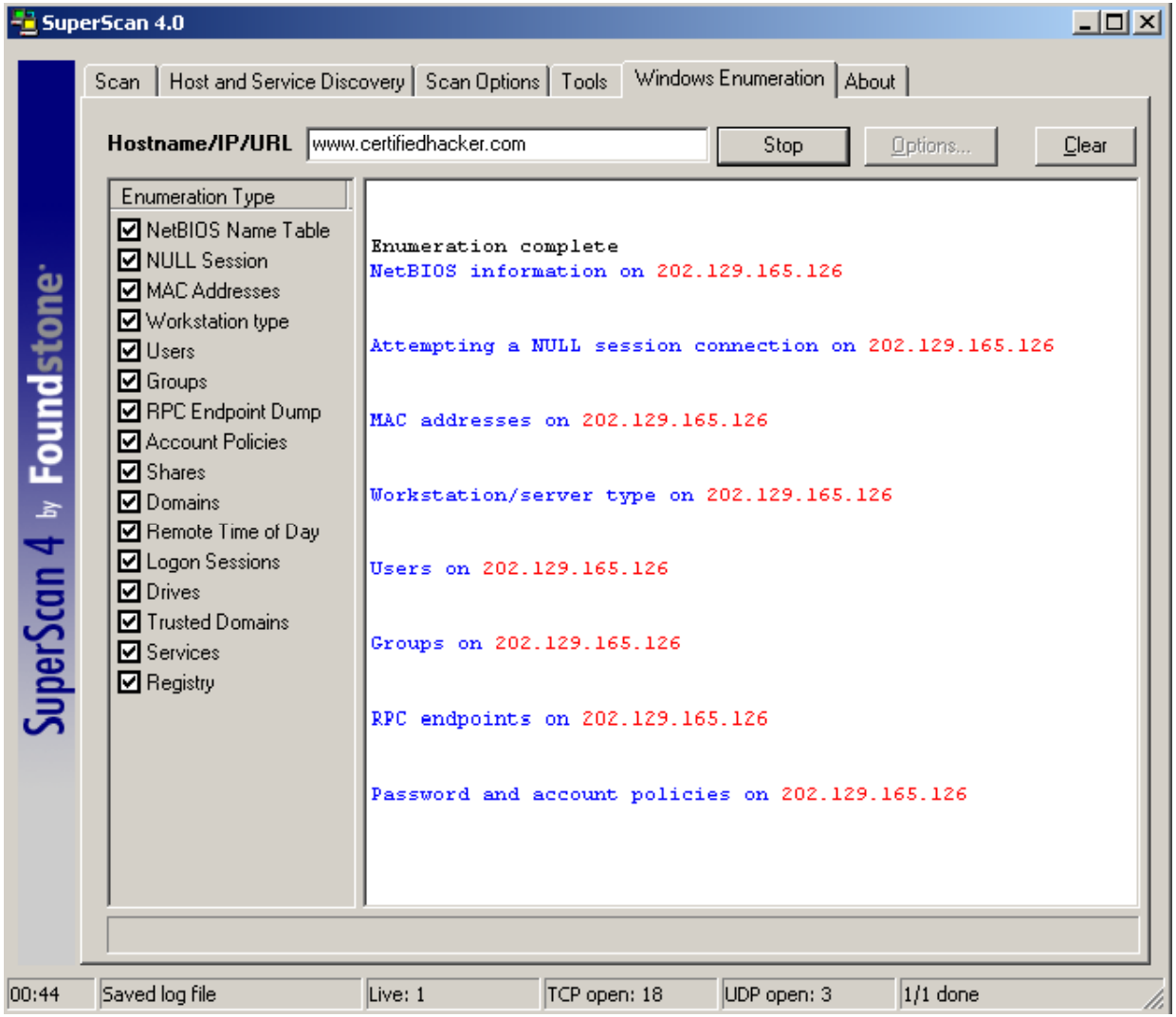
Modifies the port list and port descriptions using the built-in editor

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



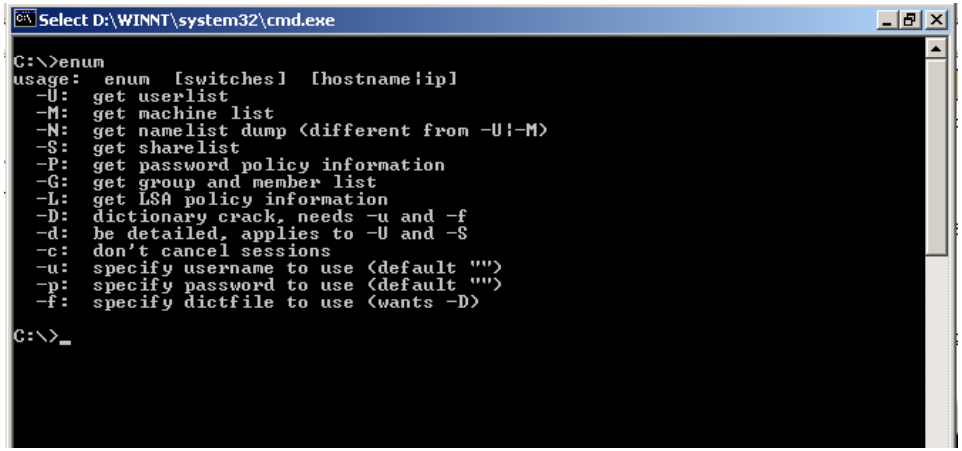
Tool: enum

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



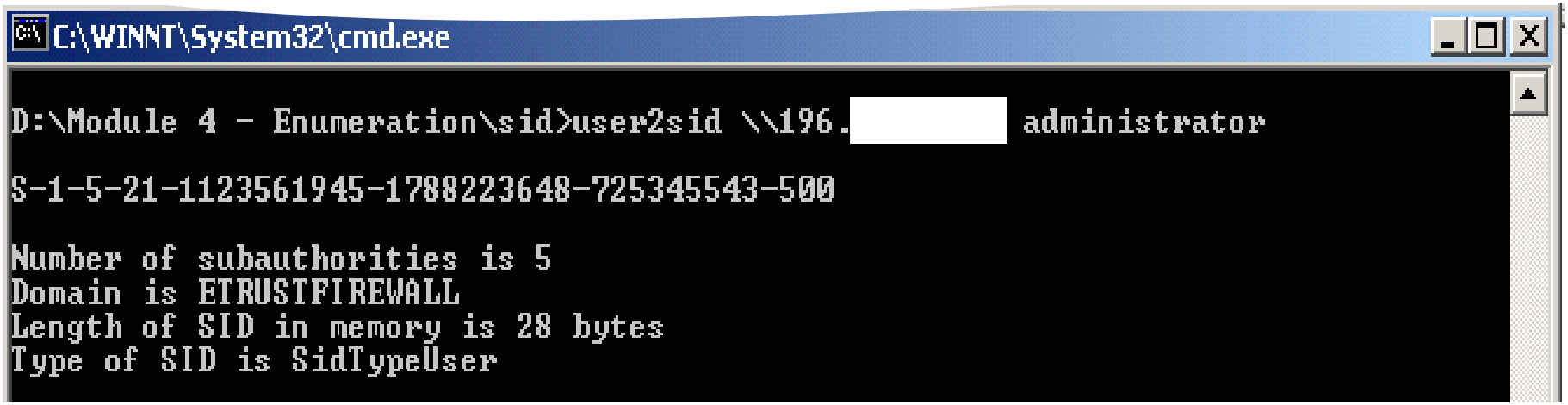
Enumerating User Accounts

Two powerful NT/2000 enumeration tools are:

- 1.sid2user
- 2.user2sid

They can be downloaded at www.chem.msu.su/~rudnyi/NT/

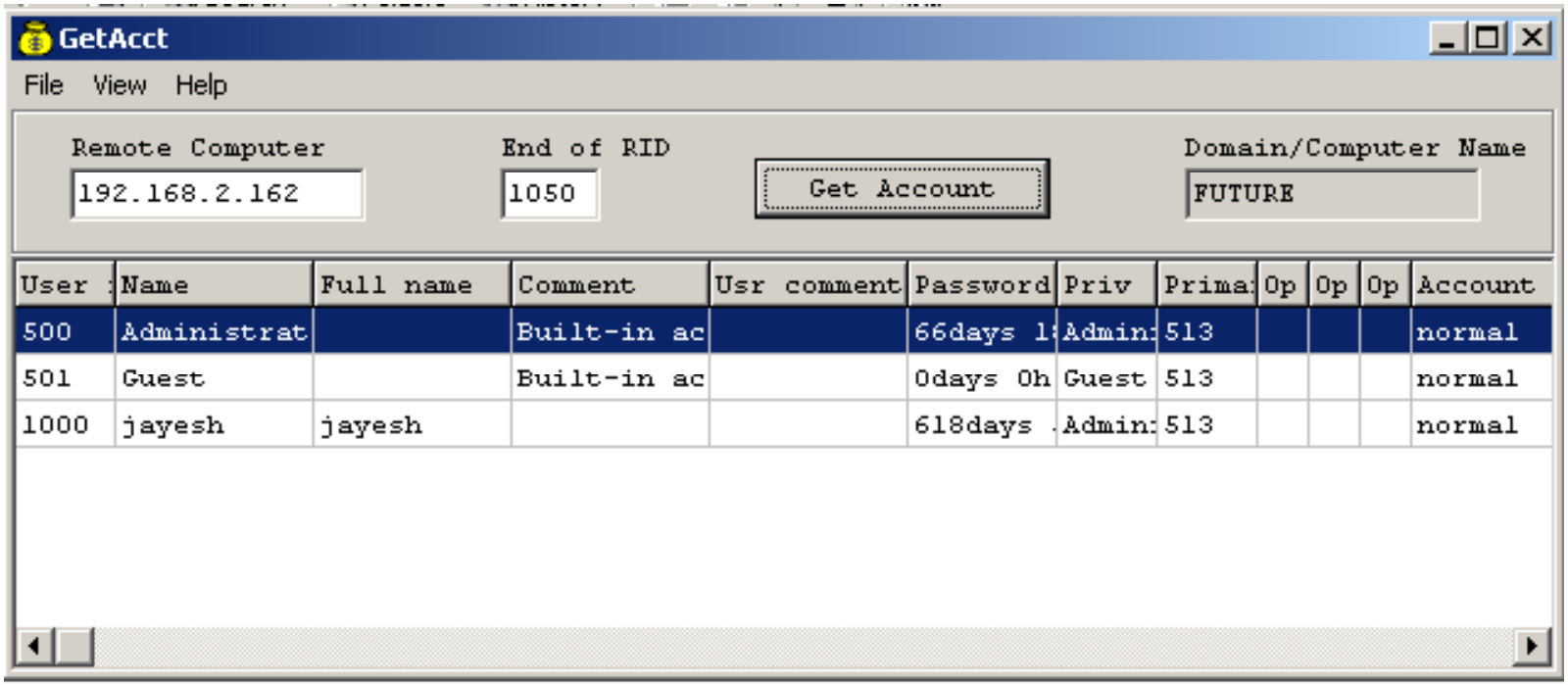
These are command-line tools that look up NT SIDs from user name input and vice versa



Tool: GetAcct

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

Downloadable from www.securityfriday.com



Null Session Countermeasures

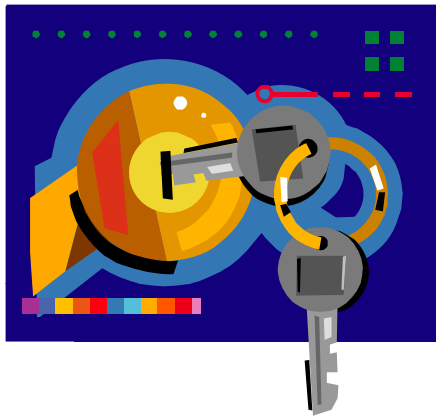
Null sessions require access to TCP 139 and/or TCP 445 ports

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

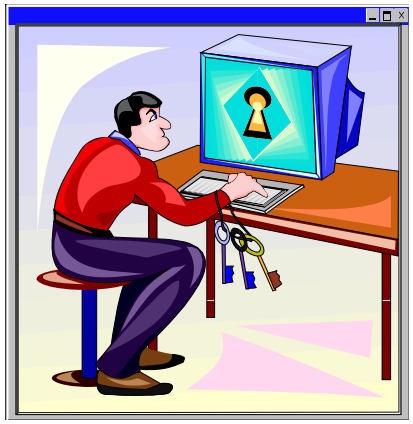


PS Tools

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



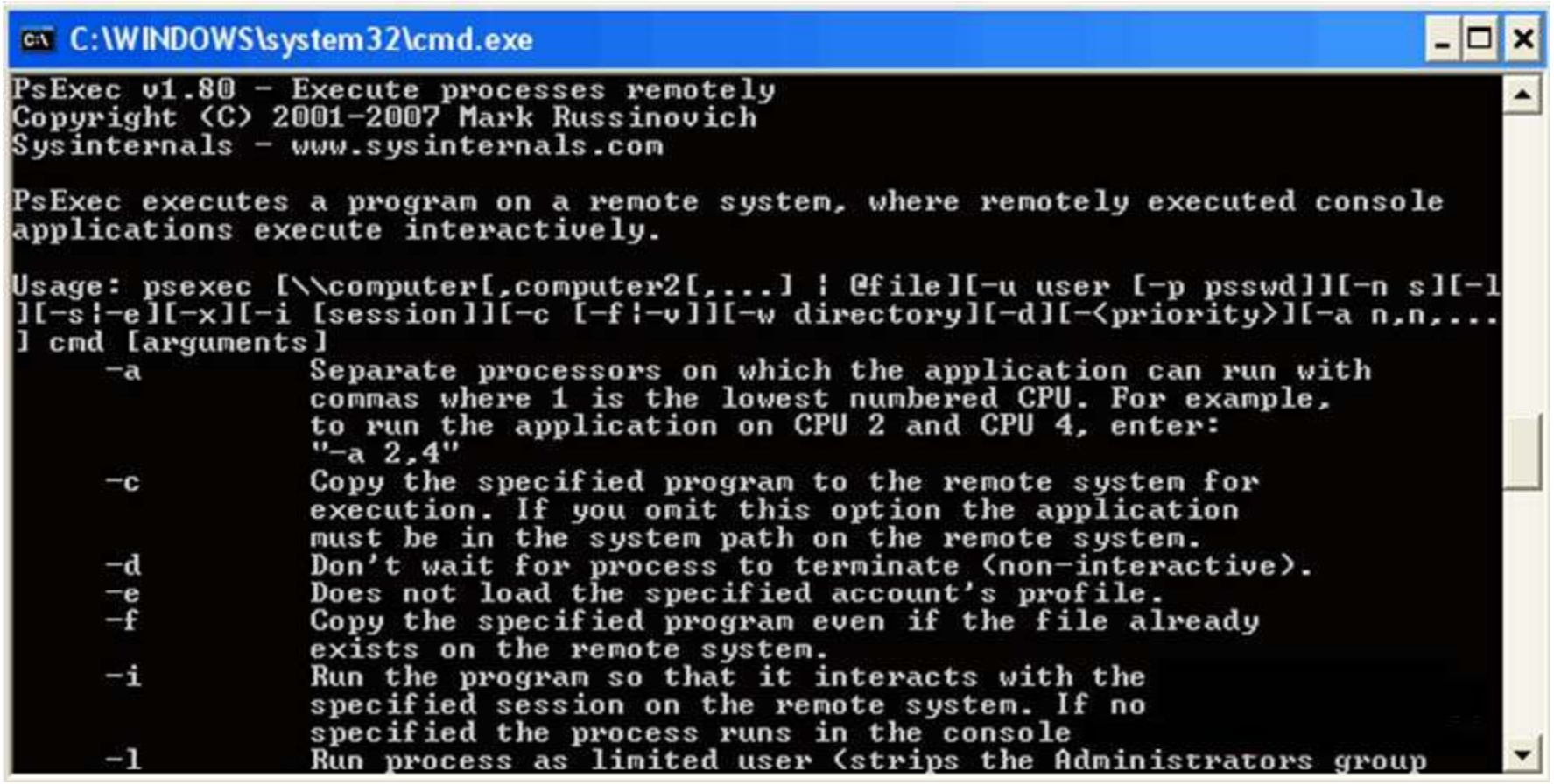
PsExec

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

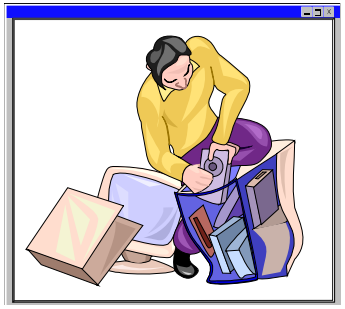


PsFile

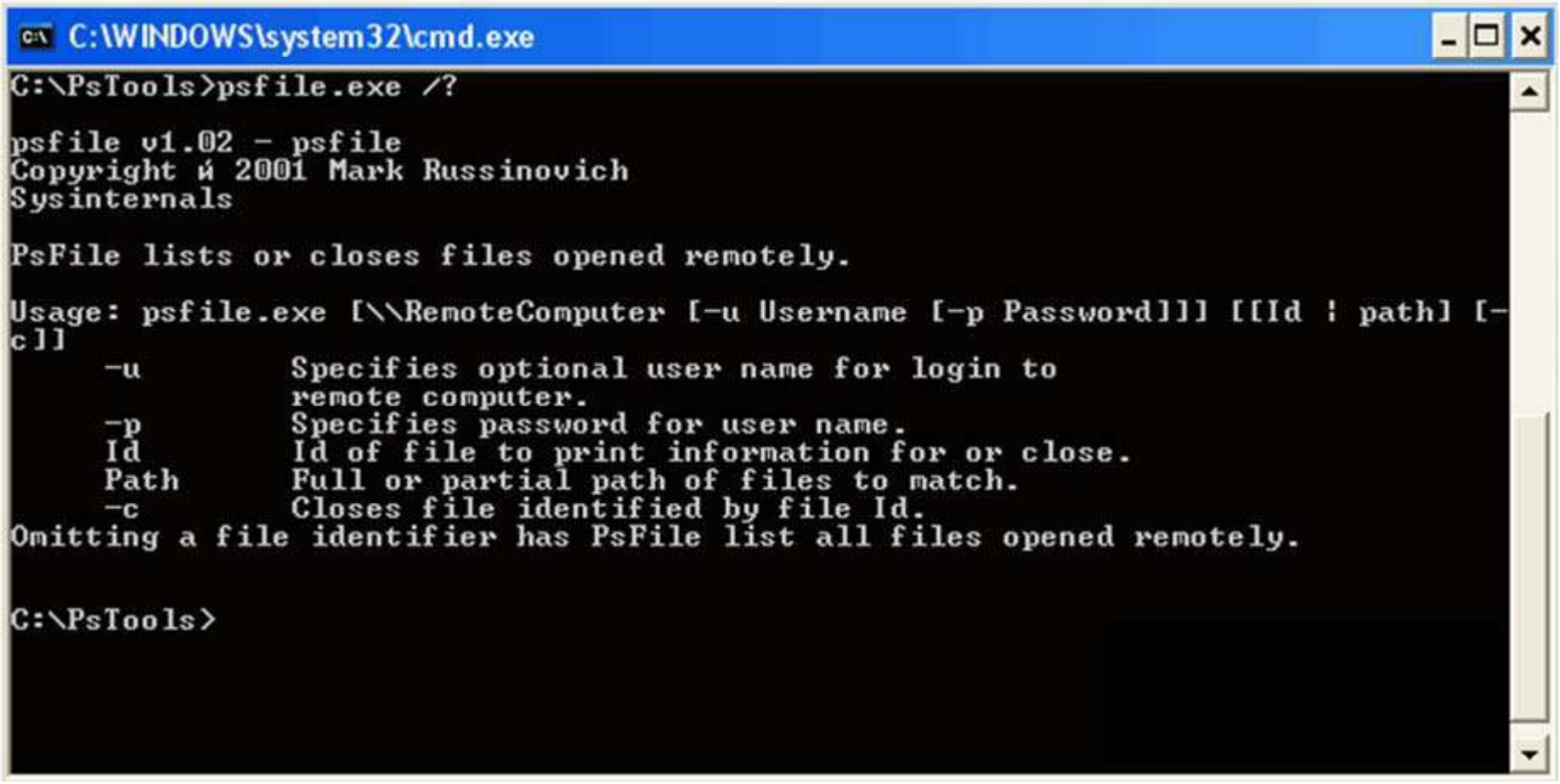
The "net file" command shows you a list of files that other computers have opened on their systems, upon which you execute the command

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



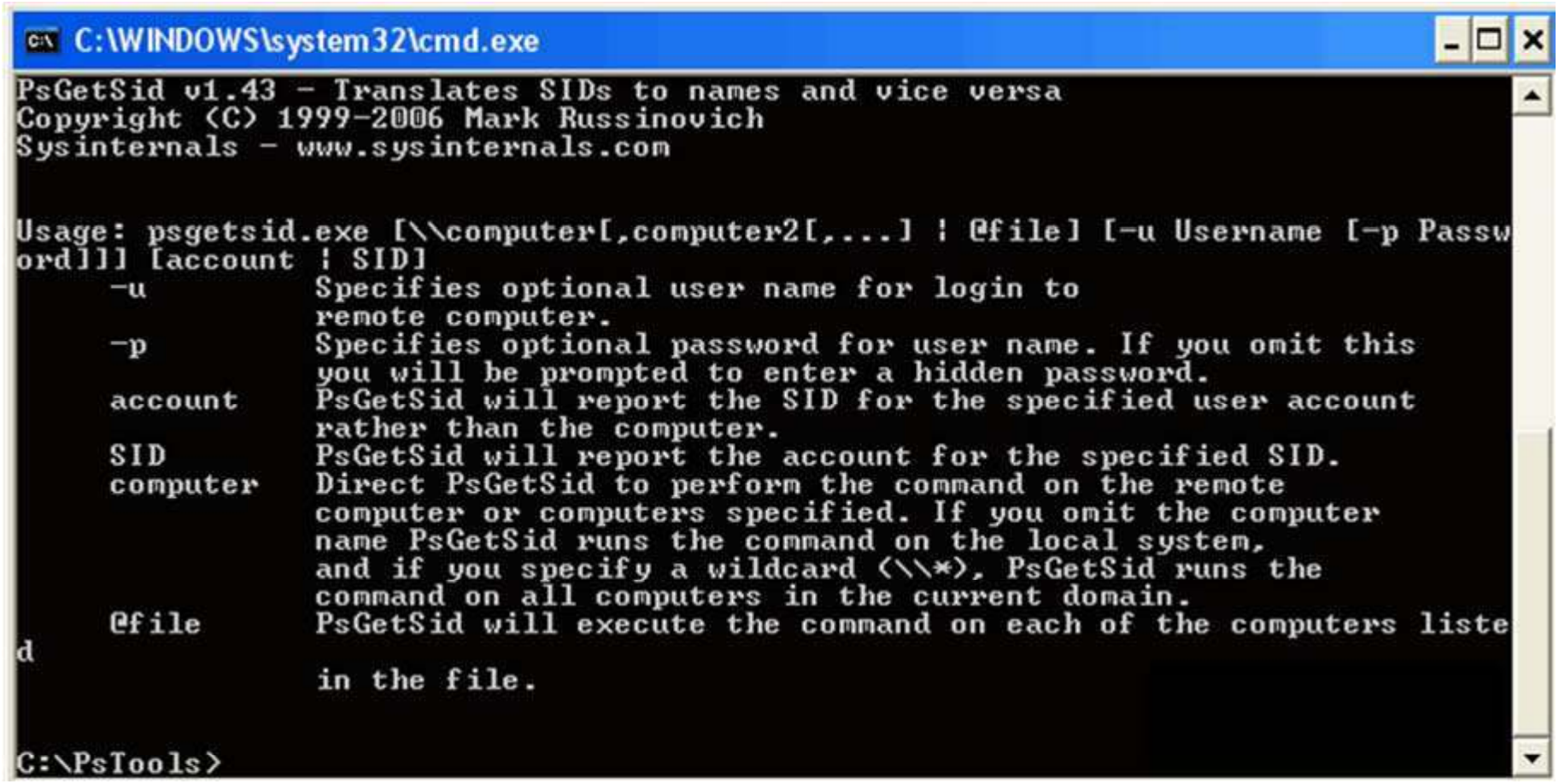
PsGetSid

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

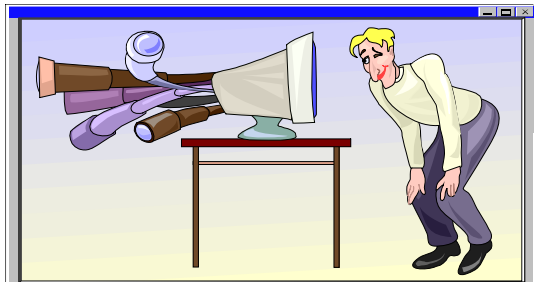


PsKill

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>`

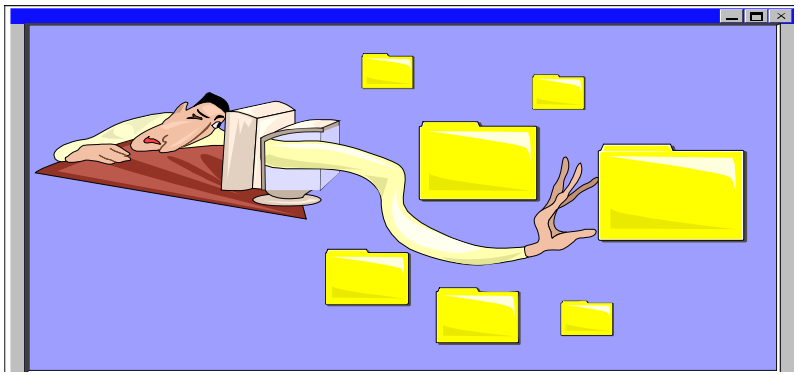


PsKill: Screenshot

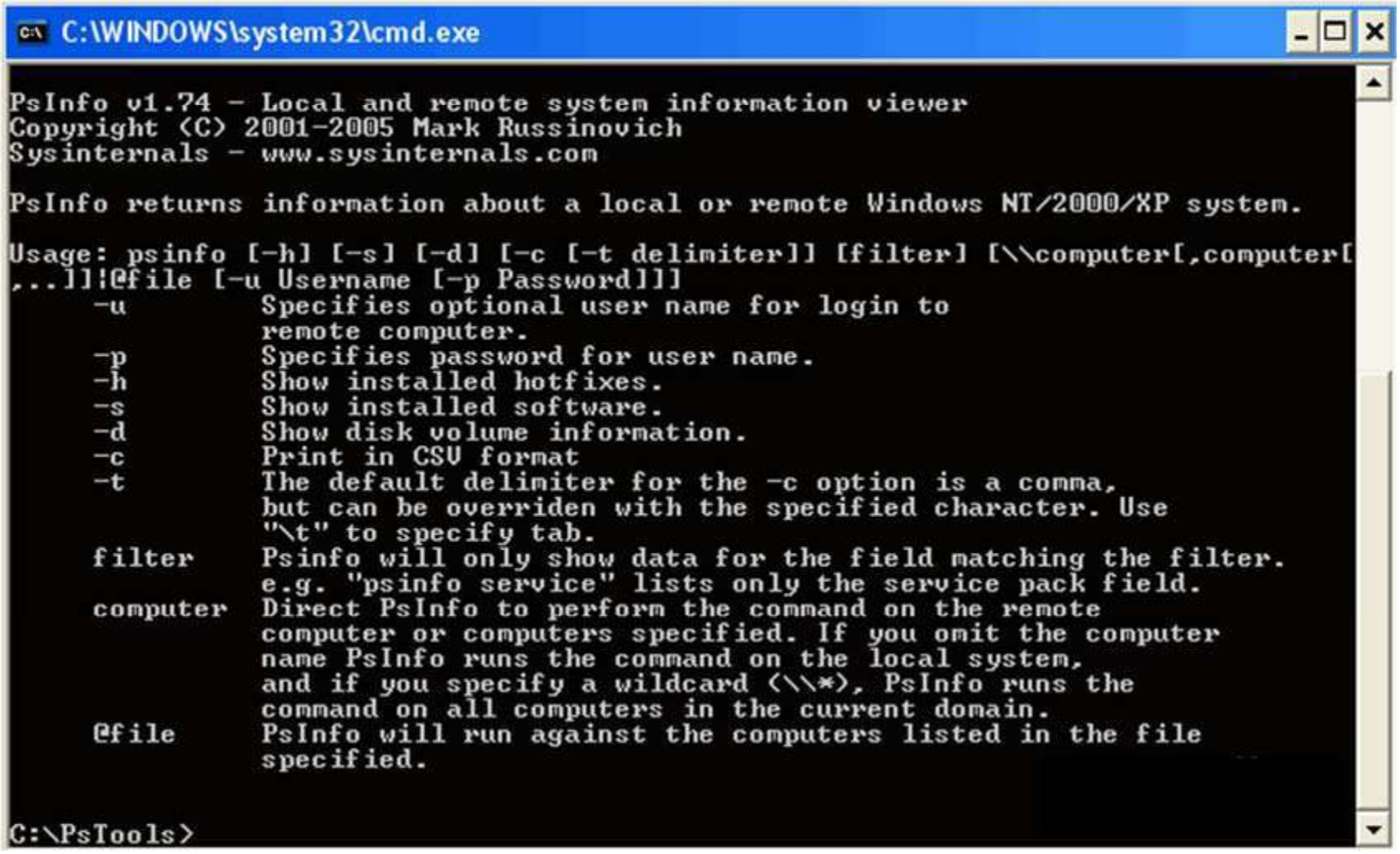
PsInfo

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

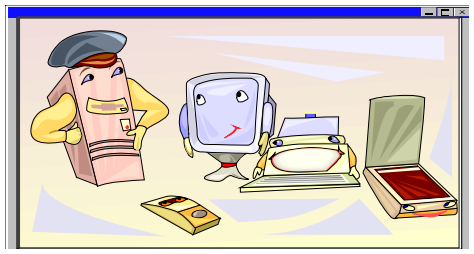


PsList

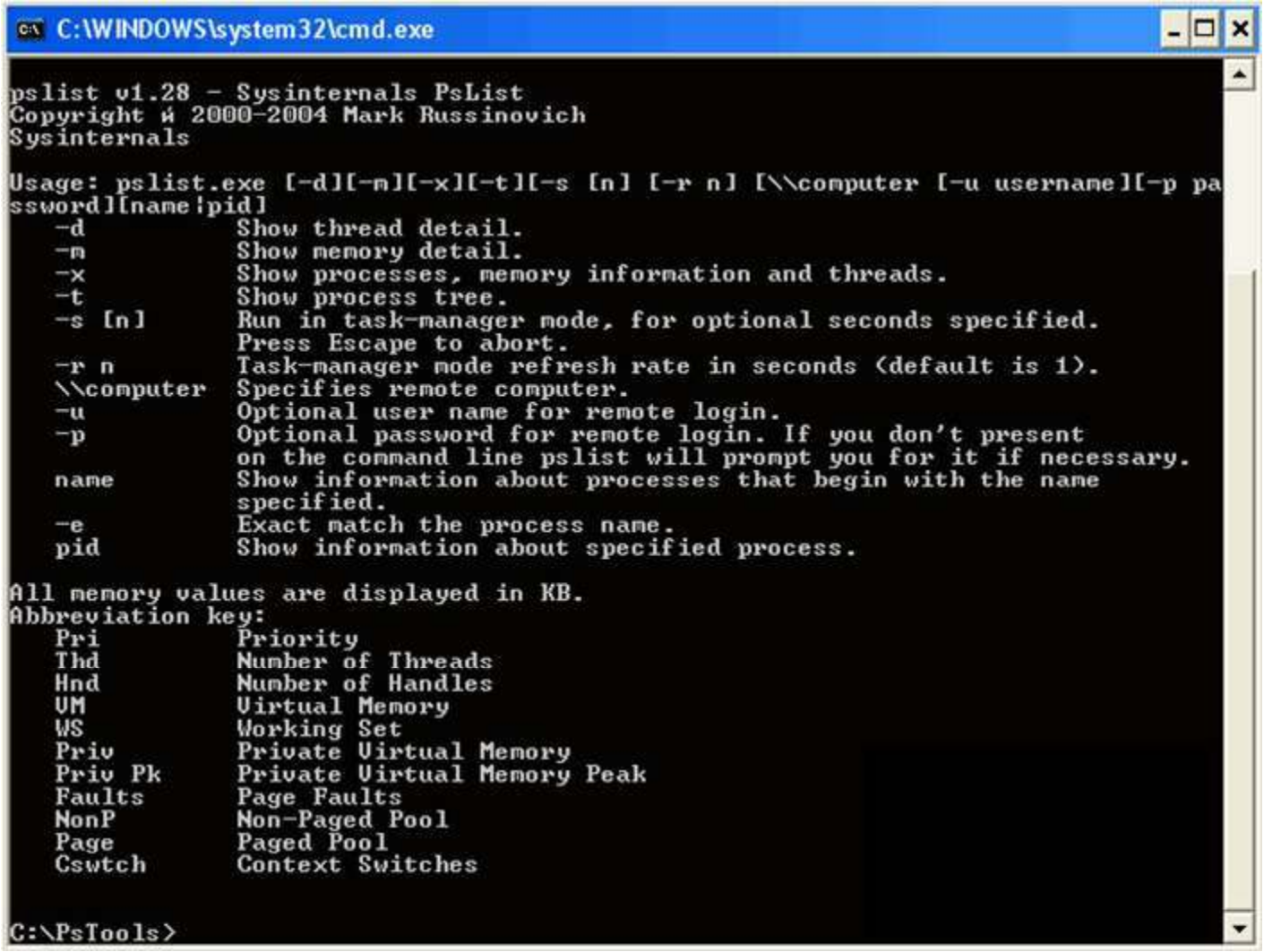
Most UNIX operating systems ship with a command-line tool called "ps" (or something equivalent) that administrators use to view detailed information about process CPU and memory usage

PsList is utility that shows a combination of the information obtainable individually with *pmon* and *pstat*

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



PsList: Screenshot

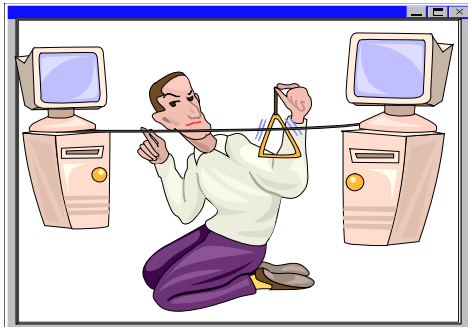


PsLoggedOn

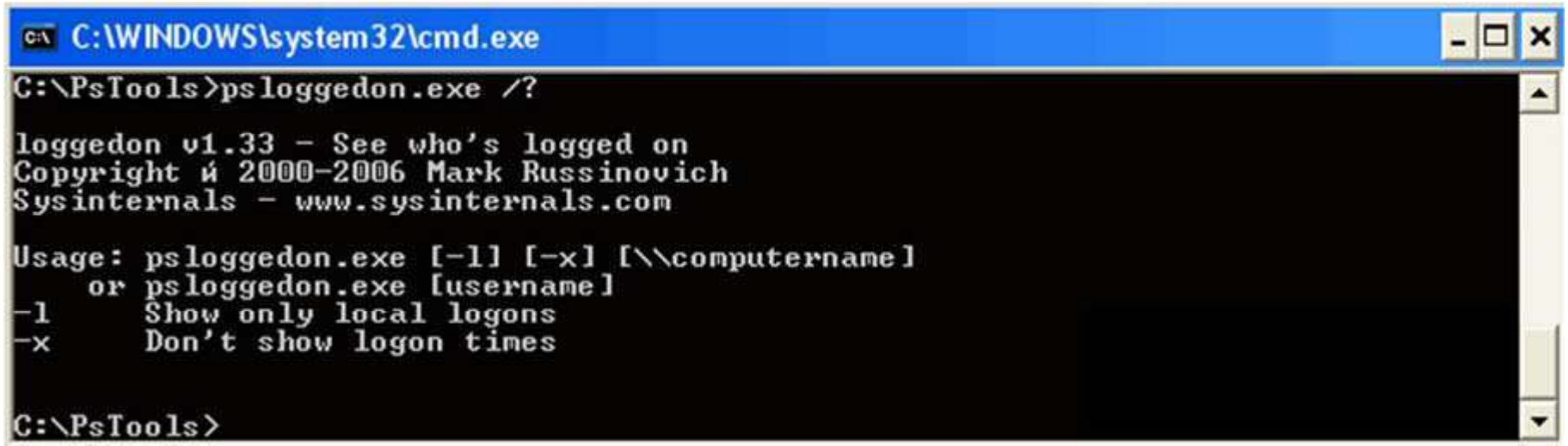
You can determine who is using resources on your local computer with the "net" command ("net session"); however, there is no built-in way to determine who is using the resources of a remote computer

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



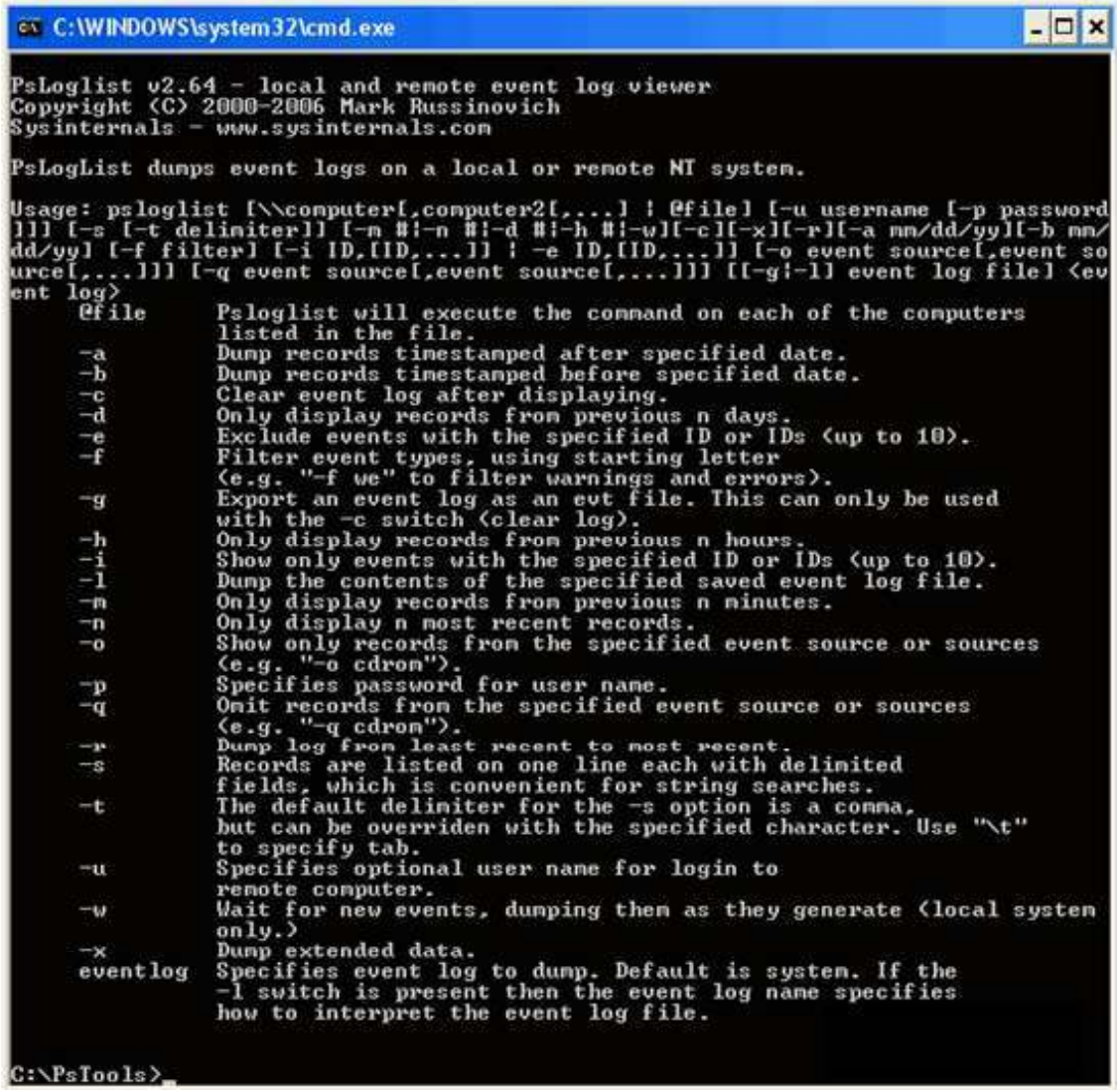
PsLogList

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



PsPasswd

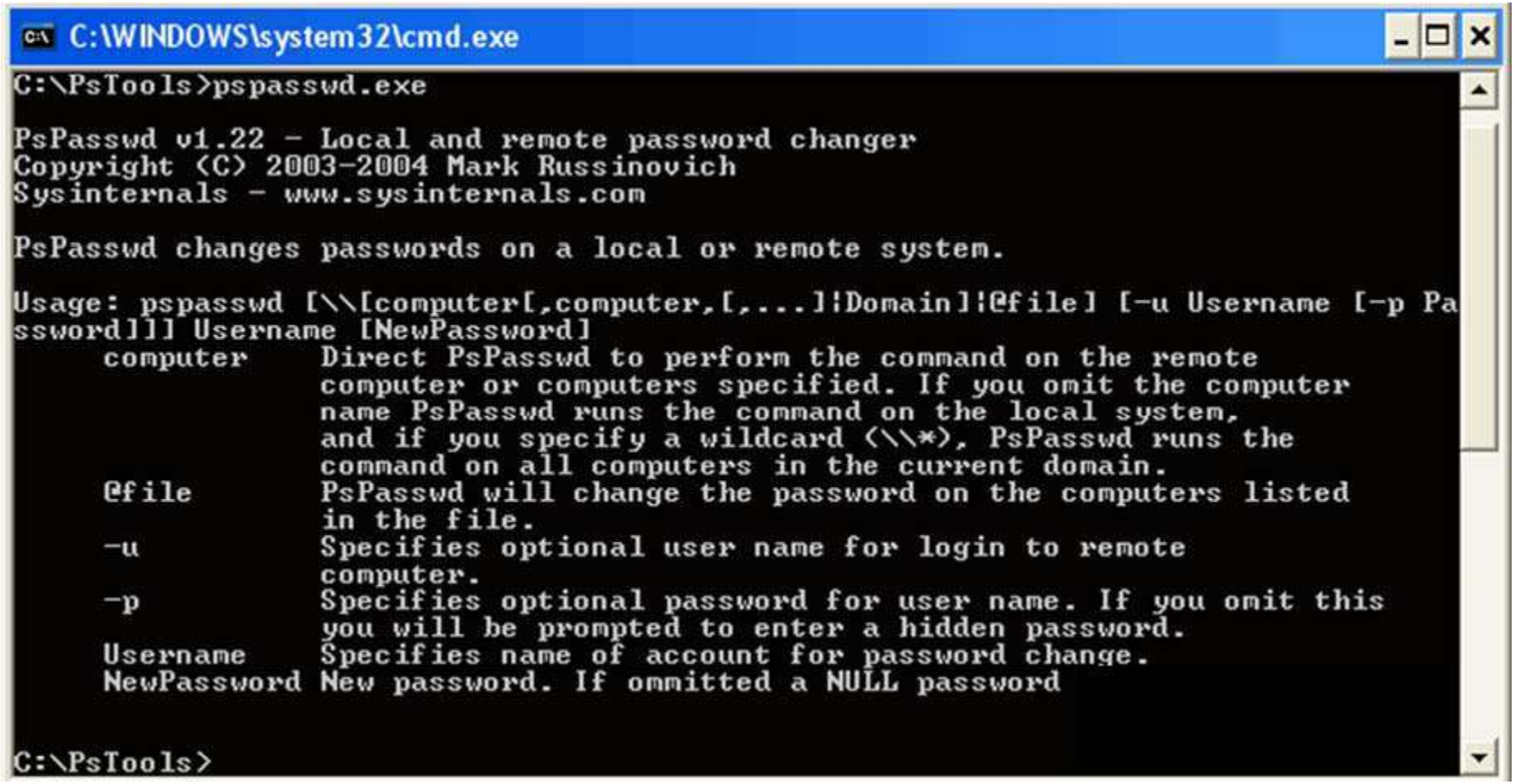
Systems administrators who manage local administrative accounts on multiple computers regularly need to change the account password as a part of the standard security practices

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



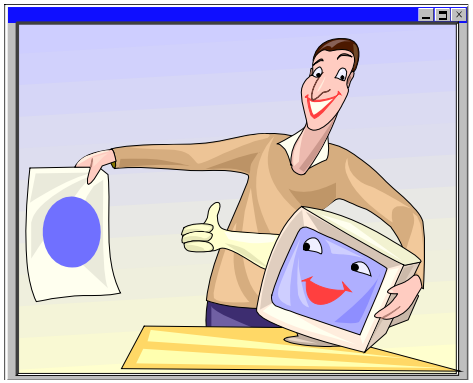
PsService

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

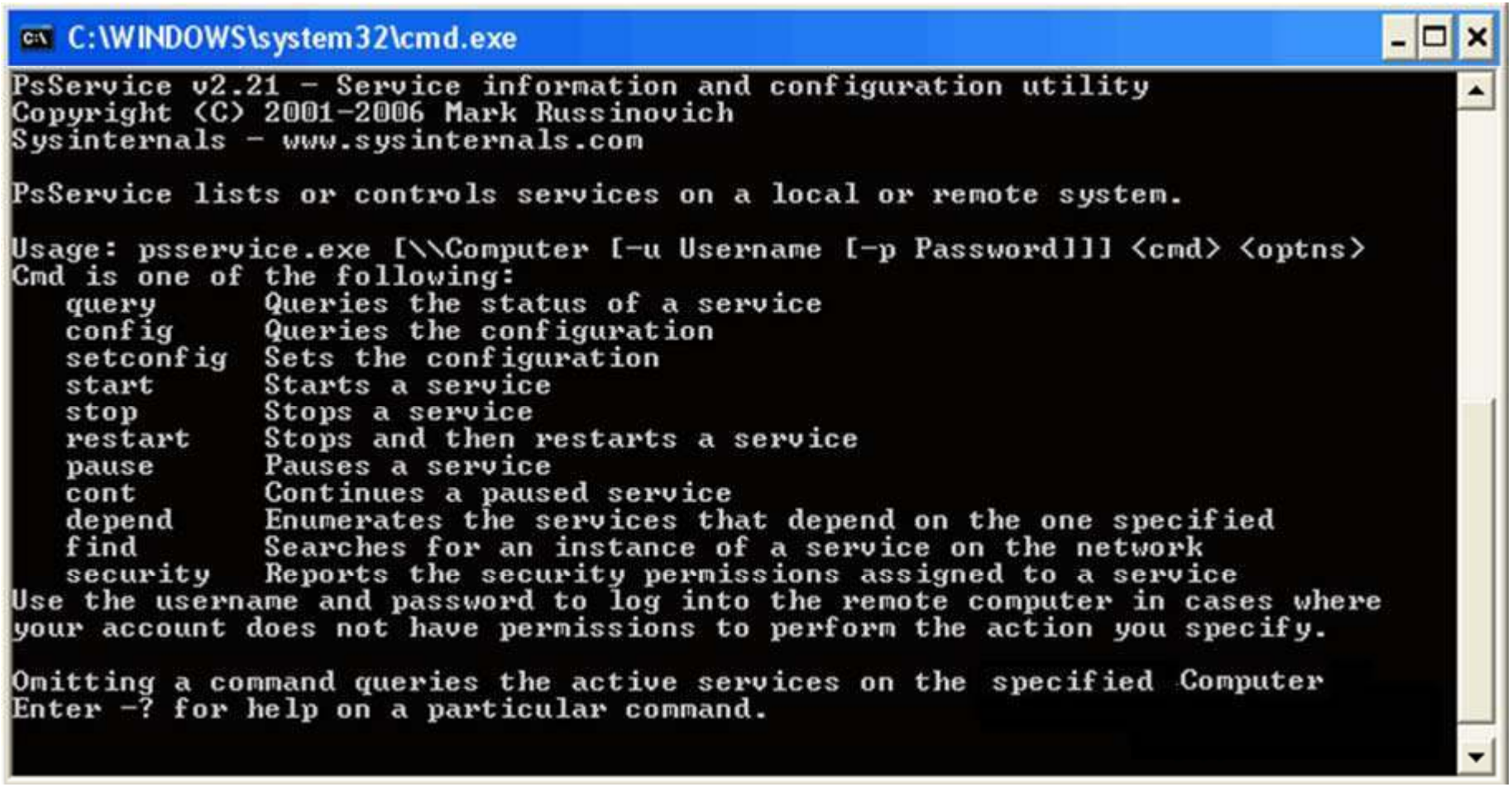
For instance, you would use the search feature if you wanted to locate systems running on DHCP servers

Usage:

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



PsService: Screenshot

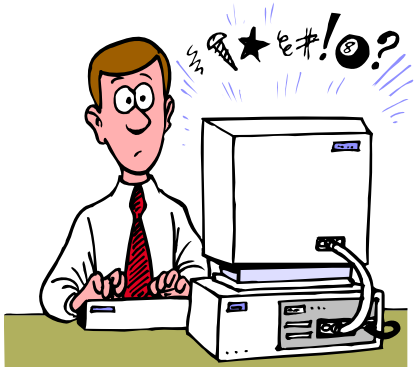


PsShutdown

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

PsSuspend

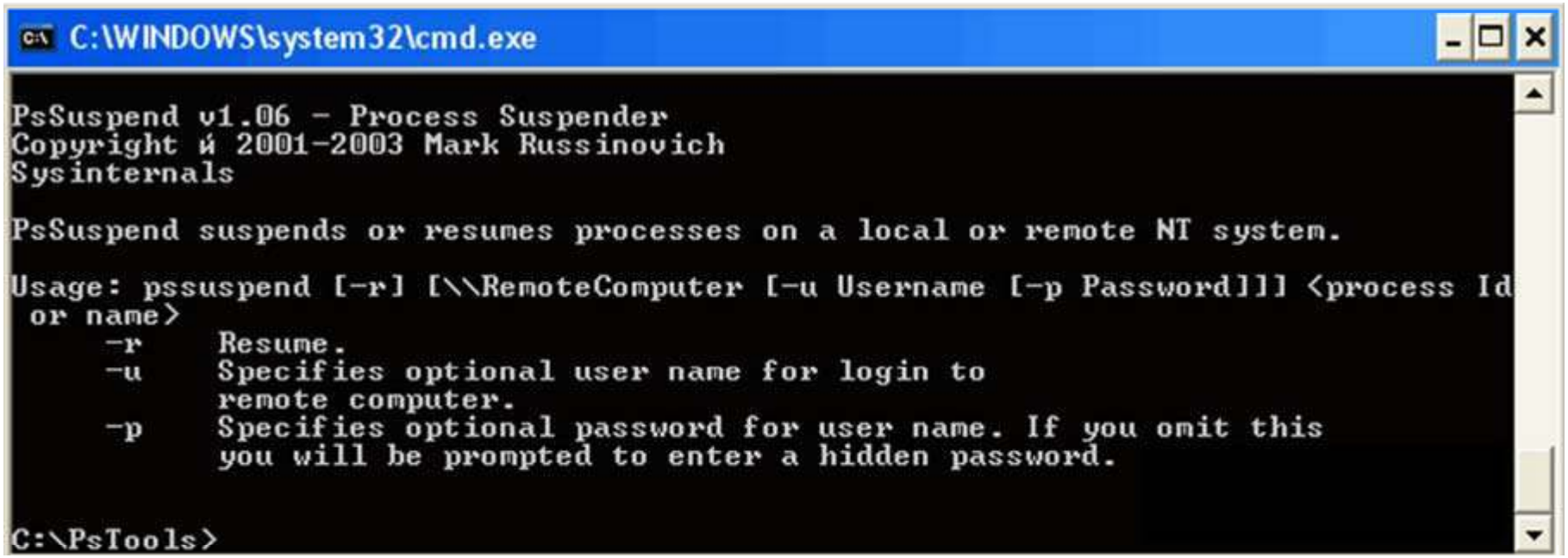
PsSuspend allows you to suspend processes on a local or remote system, which is desirable in cases where a process is consuming a resource (e.g., network, CPU, or disk) that you want to allow different processes to use

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



SNMP Enumeration

SNMP stands for Simple Network Management Protocol

Managers send requests to agents and the agents send back replies

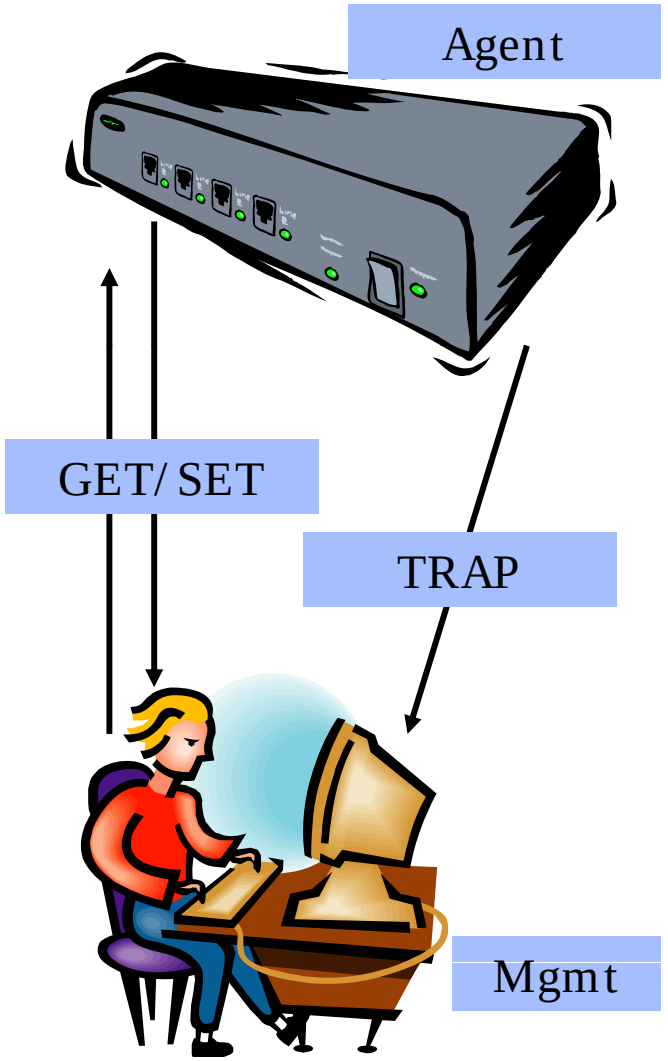
The requests and replies refer to variables accessible to the agent software

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 ispotentially 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

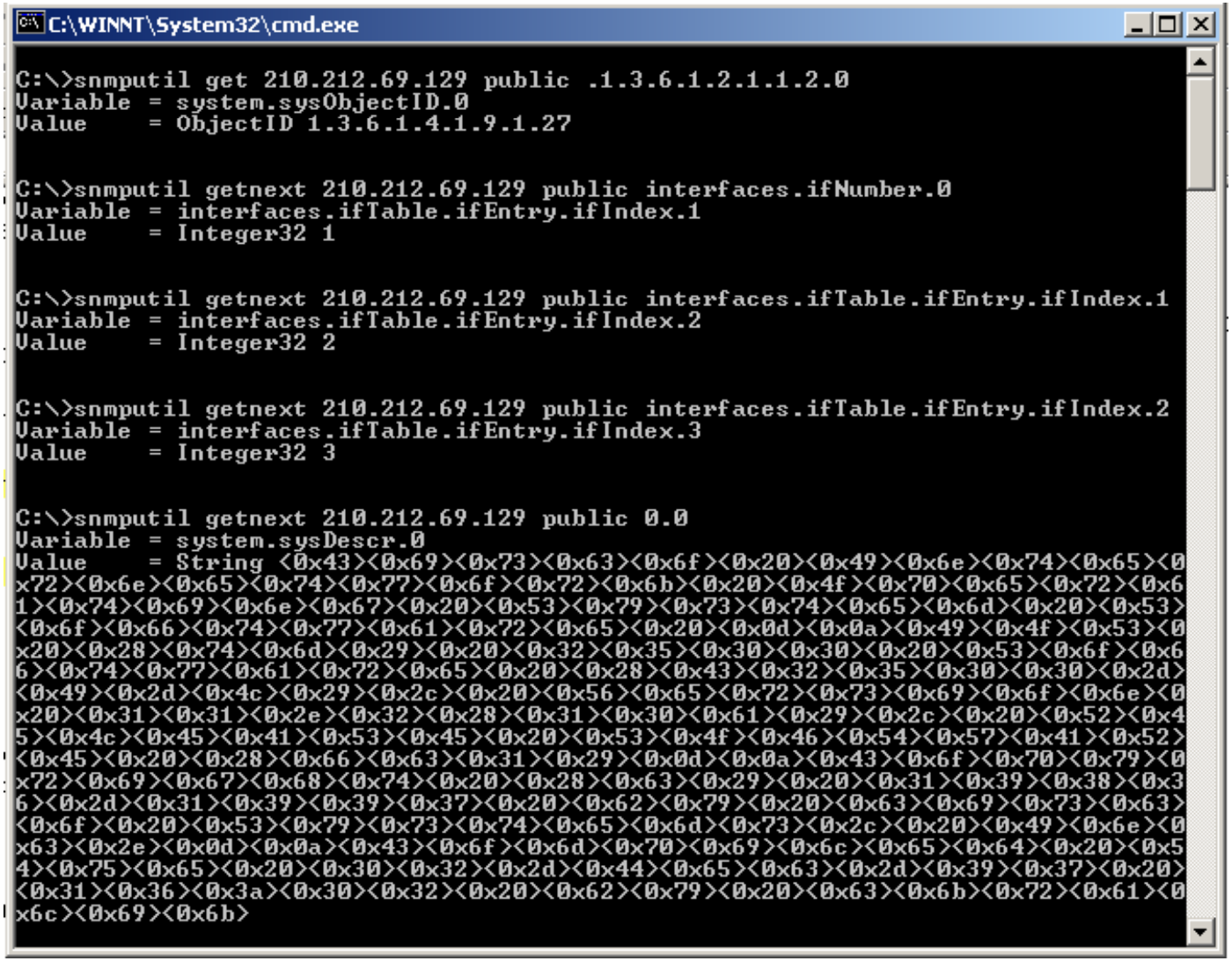
It is the most basic element of network management

It is the updated version of the standard MIB

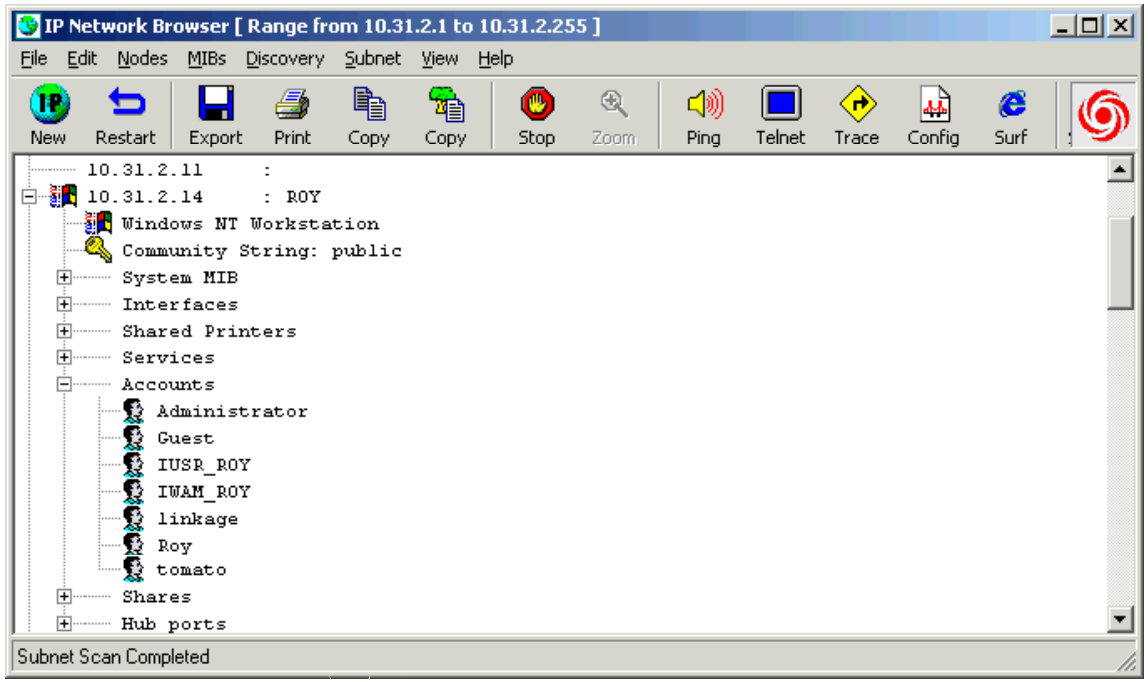
It adds new SYNTAX types and adds more manageable objects to the MIB tree

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

SNMPutil Example



Tool: Solarwinds



Solarwinds is a set of network management tools

The tool set consists of the following:

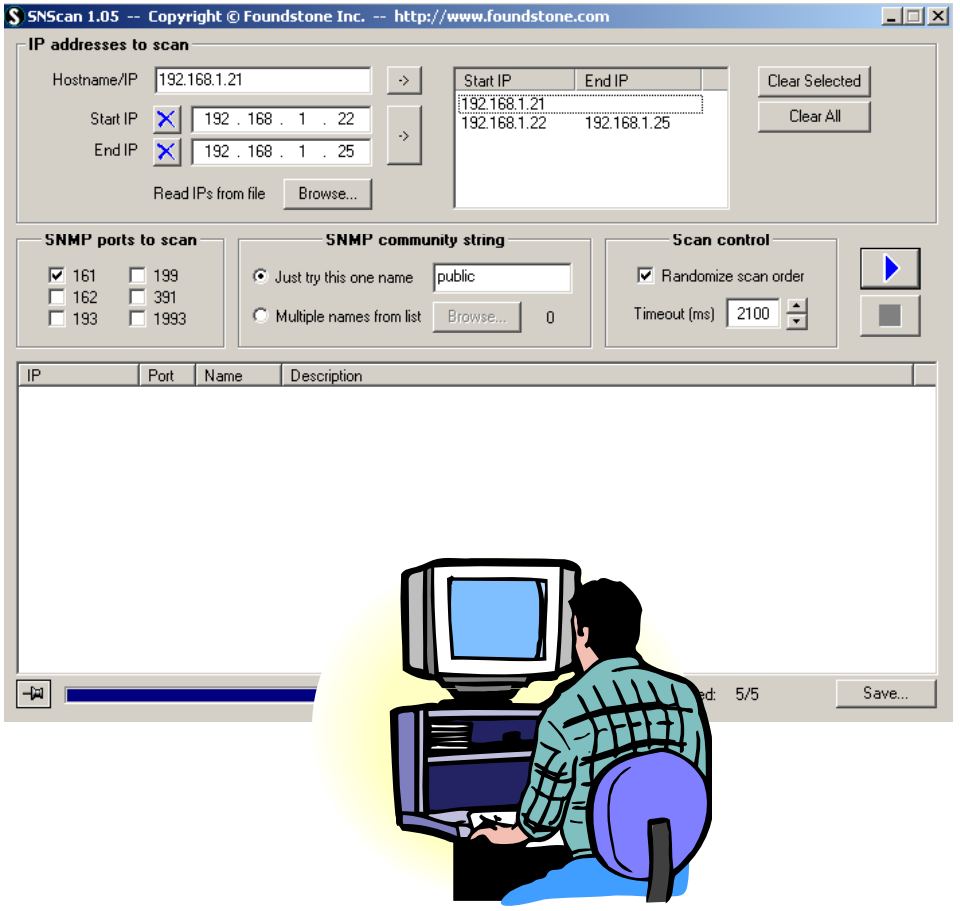
- Discovery
- Cisco Tools
- Ping Tools
- Address Management
- Monitoring
- MIB Browser
- Security
- Miscellaneous

Tool: SNScan

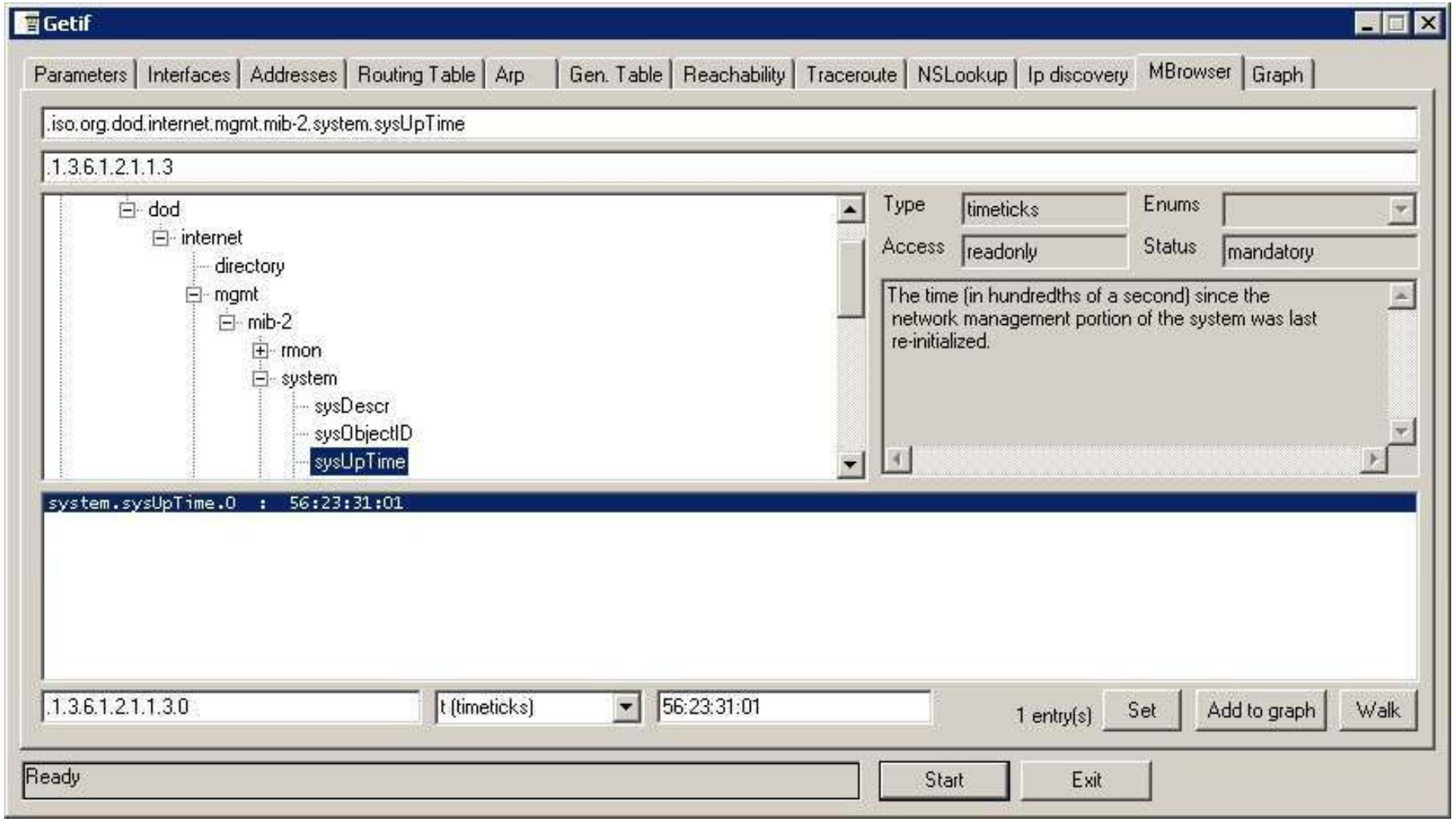
SNScan is a windows-based SNMP scanner that can effectively detect SNMP-enabled devices on the network

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



UNIX Enumeration

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 –1 @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

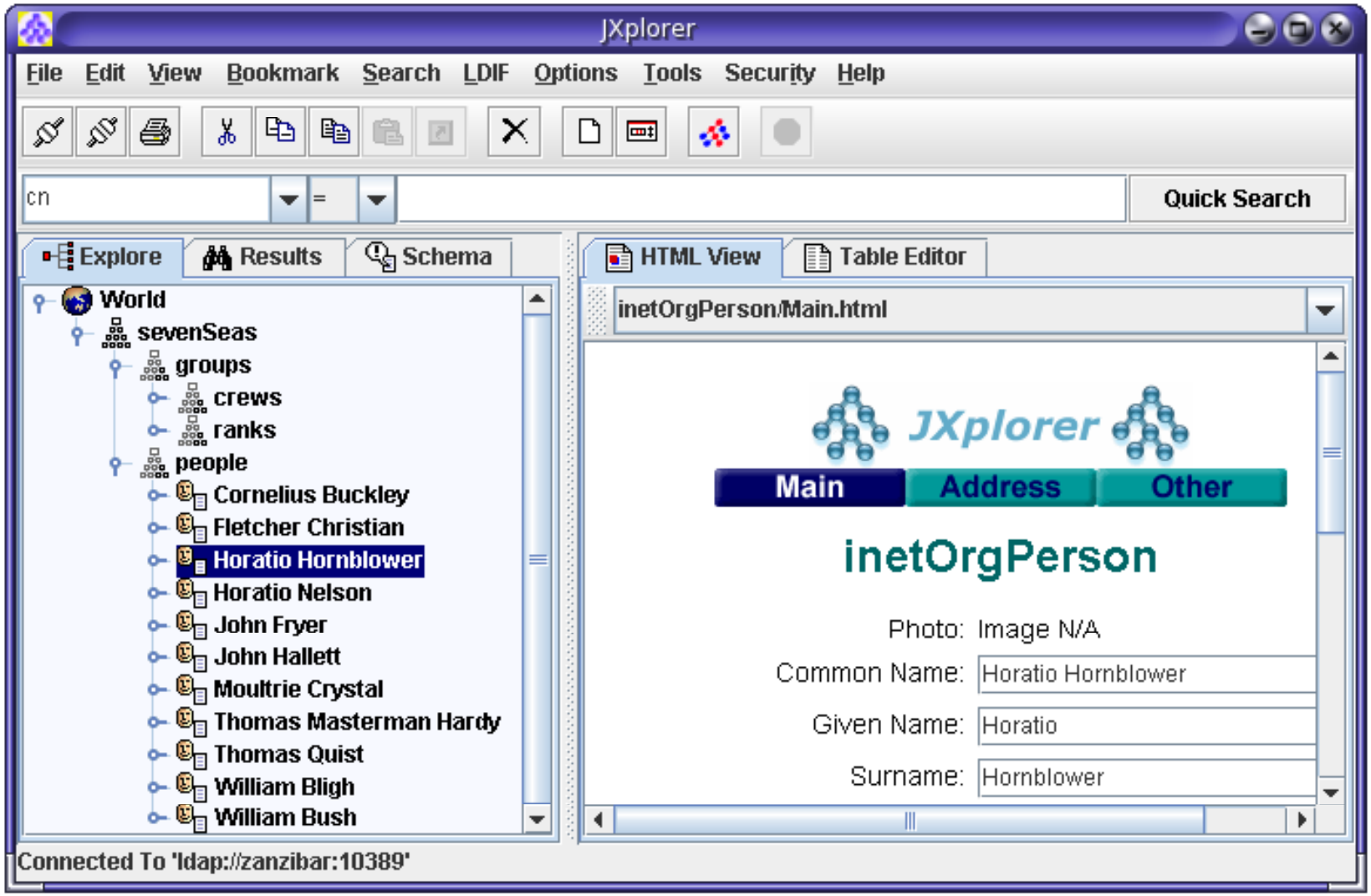
JXplorer

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

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

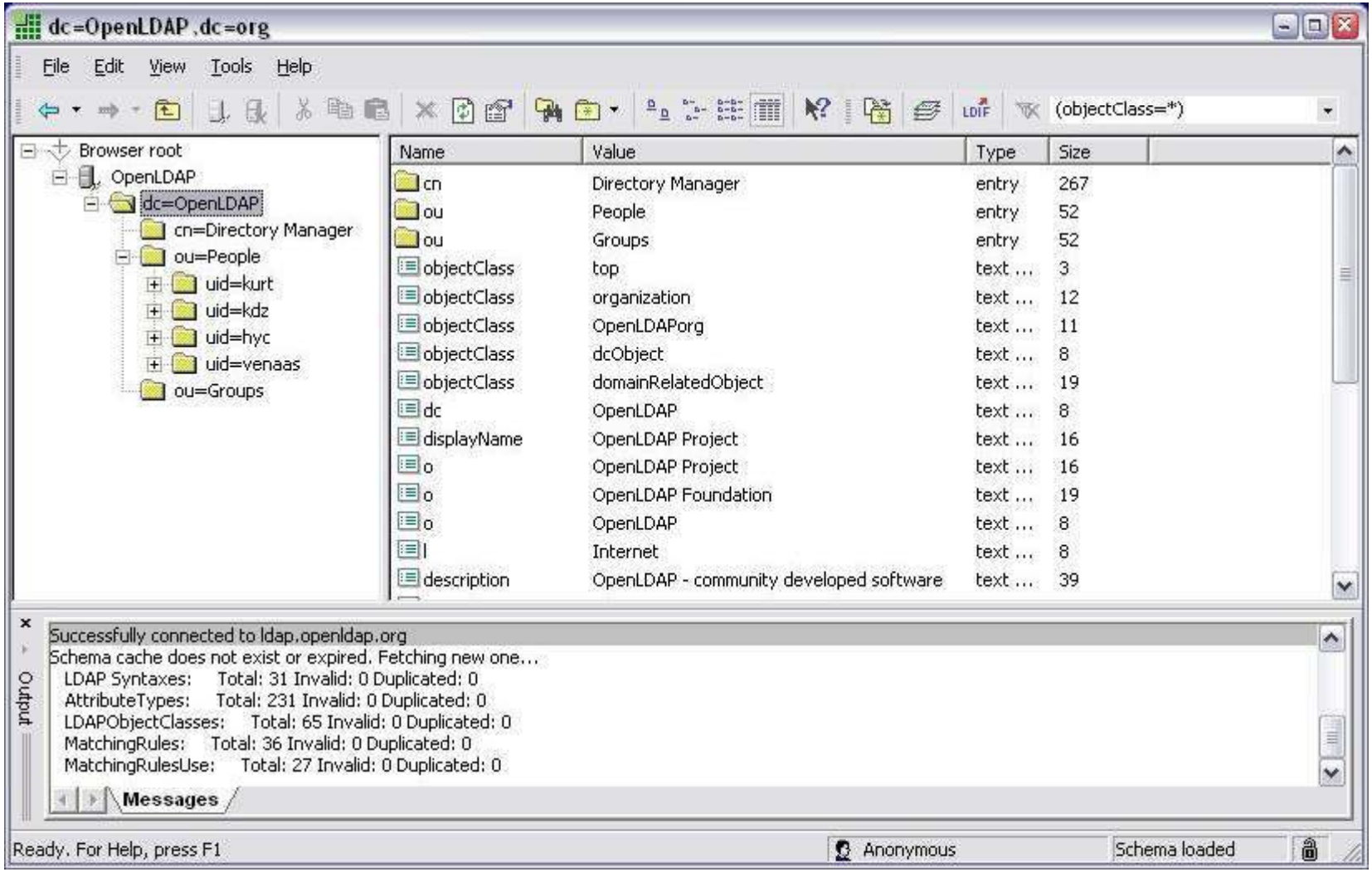
It allows to access:

- 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



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 port25

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

SMTP Enumeration(cont'd)

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

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

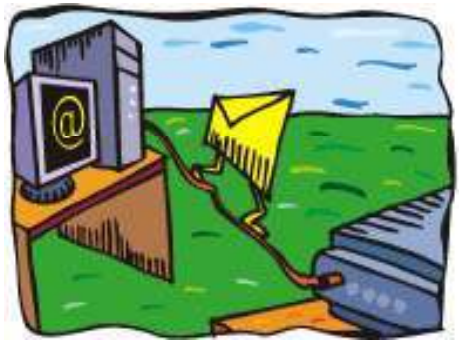
Hyper Text Transfer Protocol is used by World Wide Web to display and distribute the information

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

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

Lynx

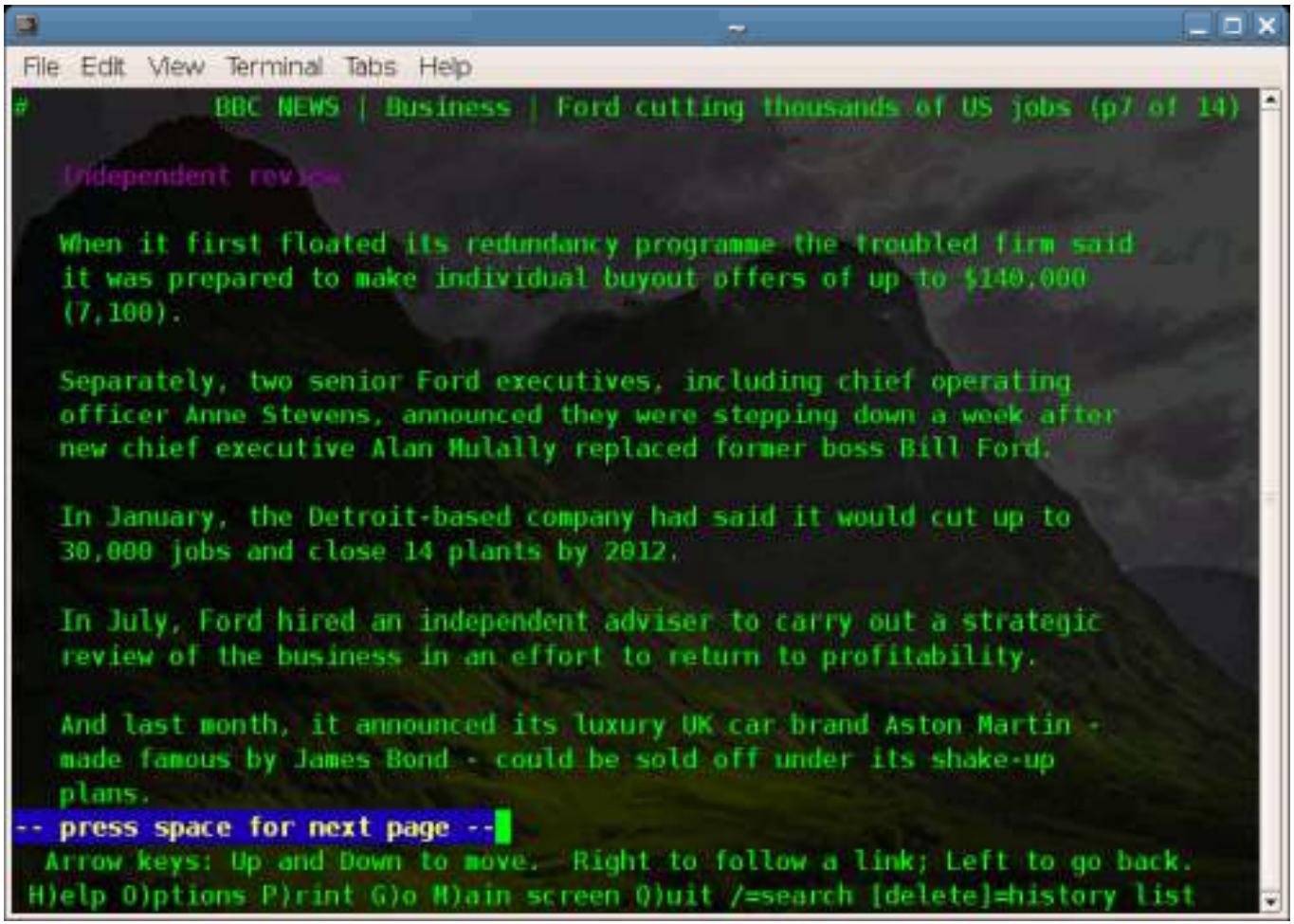
Lynx is the text web browser

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



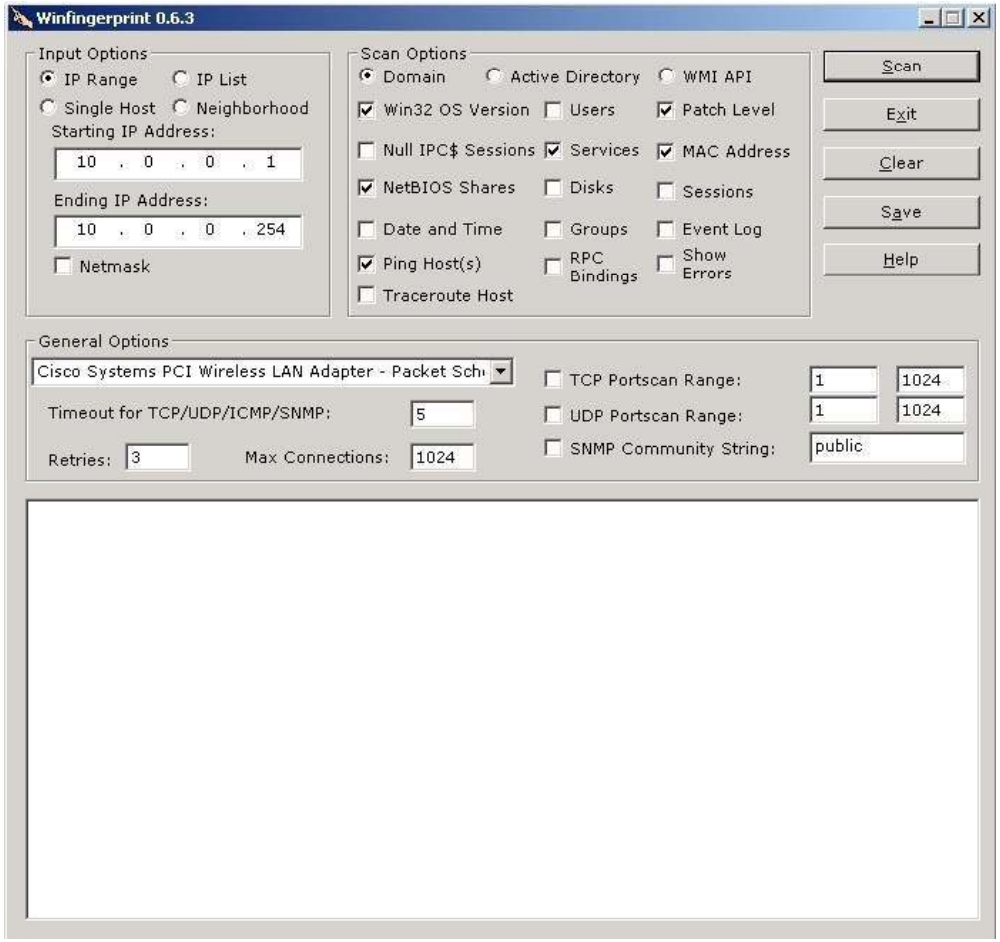
Tool: Winfingerprint

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 I
# 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
```

w2kdad.pl

How To Enumerate Web Application Directories in IIS Using Directory Services

This work is accomlished 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

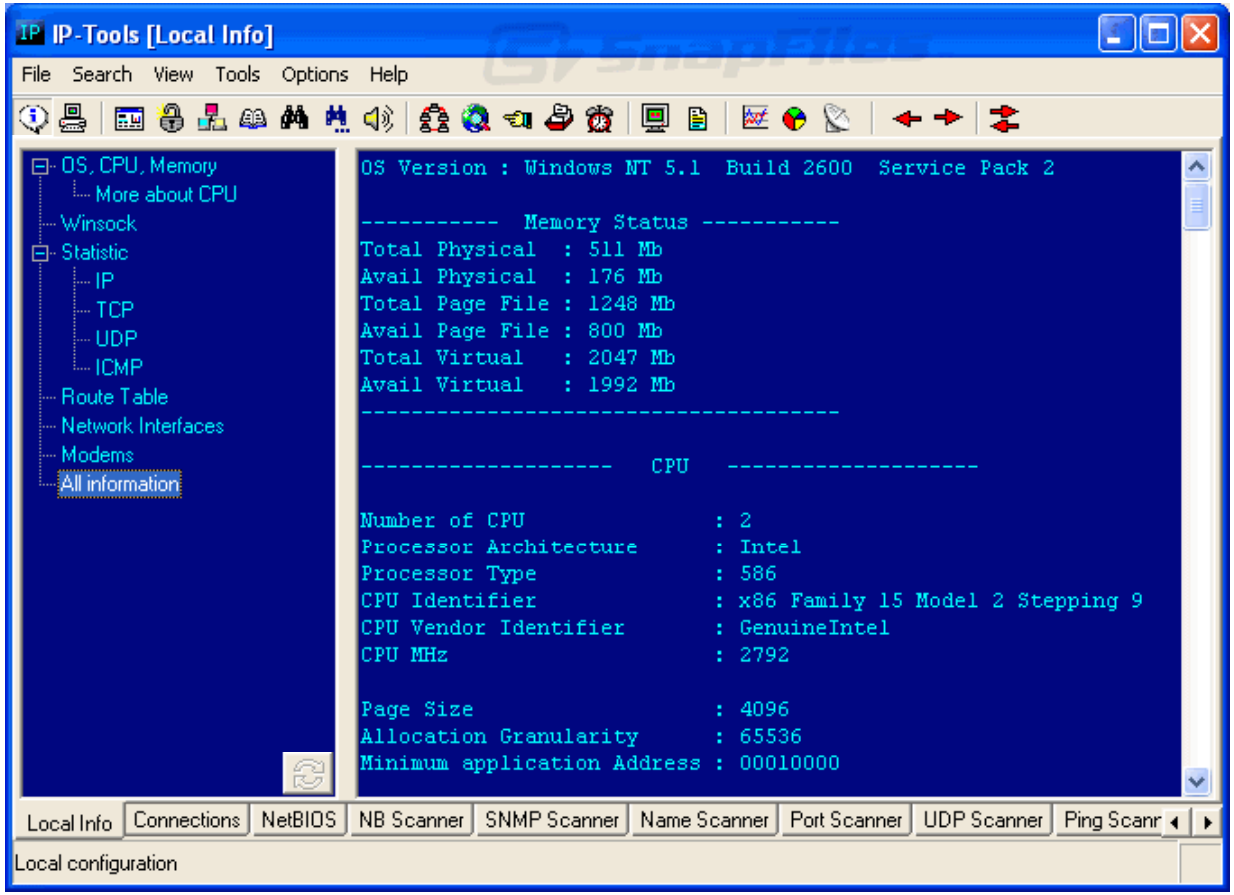
How To Enumerate Web Application Directories in IIS Using DirectoryServices (cont'd)

```
public StringCollection GetIISVirtualFolders(string strServer)
{
        StringCollection strColl = null;
        DirectoryEntry obDirEntry = null;
        DirectoryEntries obDirEntList = null;
        try
        {
                obDirEntry = new DirectoryEntry("IIS://" + strServer + "/W3svc/1/Root");
                obDirEntList= obDirEntry.Children;

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

private void ProcessDEForIISVFolder(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



EC-Council

Enumerate Systems Using Default Passwords

Default Password List

2006-09-14

Manufactor	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 contains interesting list of passwords

Tool: NBTScan

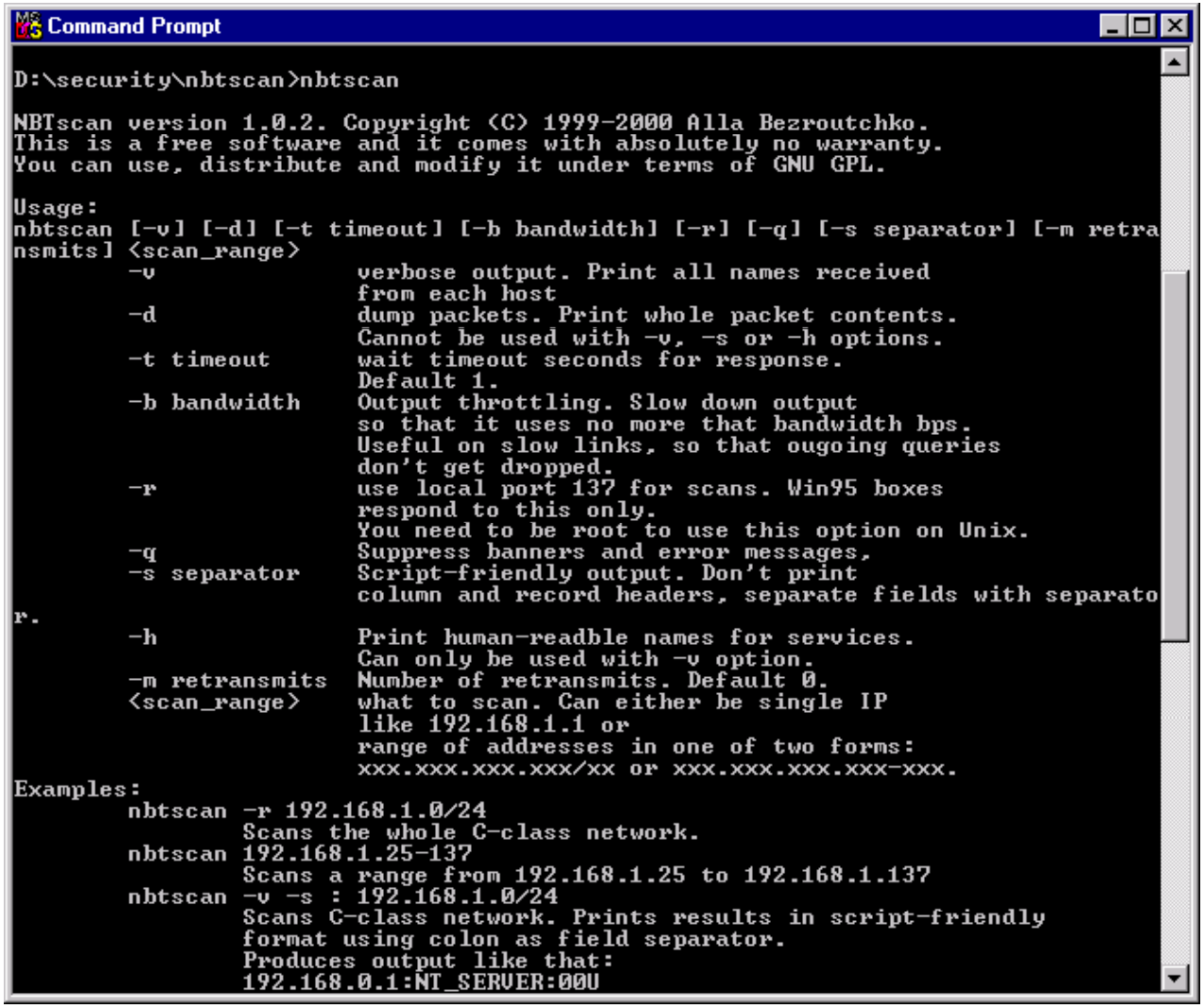
NBTscan is a program for scanning IP networks for NetBIOS name information

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



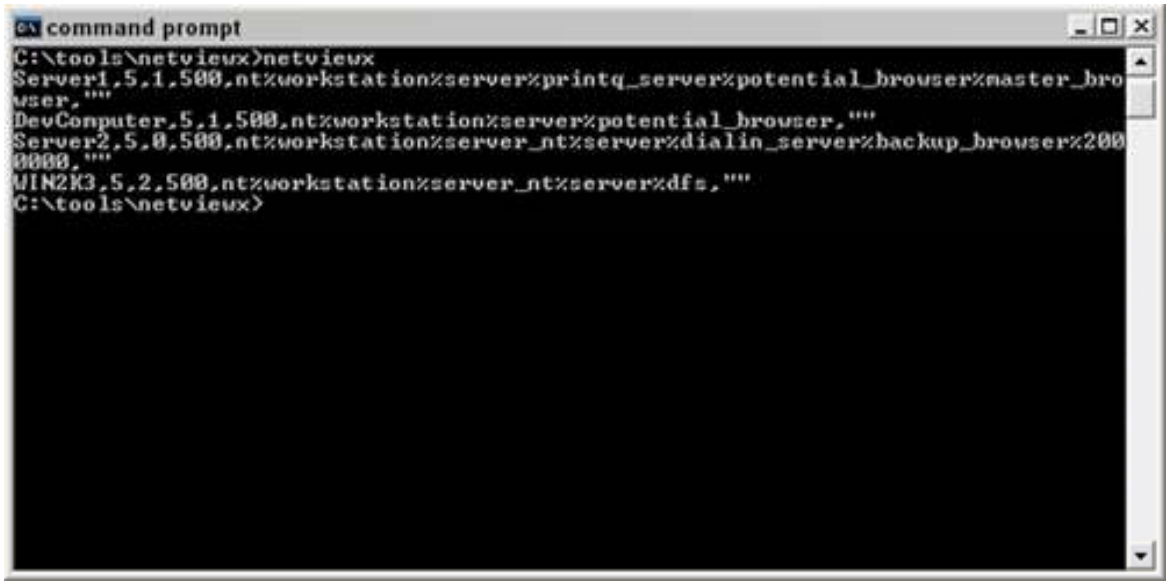
Tool: NetViewX

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



Tool: FreeNetEnumerator

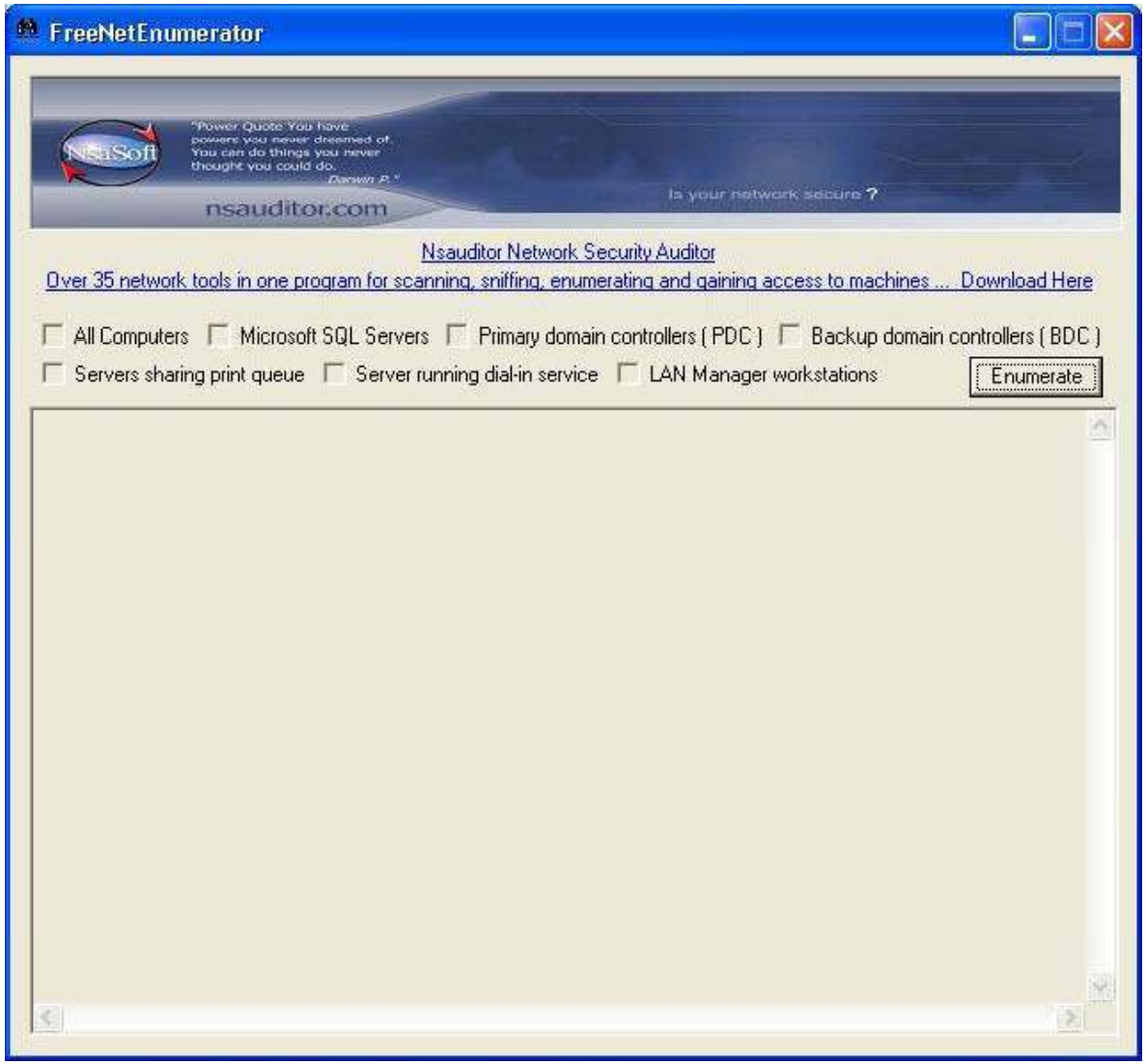
FreeNetEnumerator is a tool to enumerate computers in a domain

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: Sceenshot

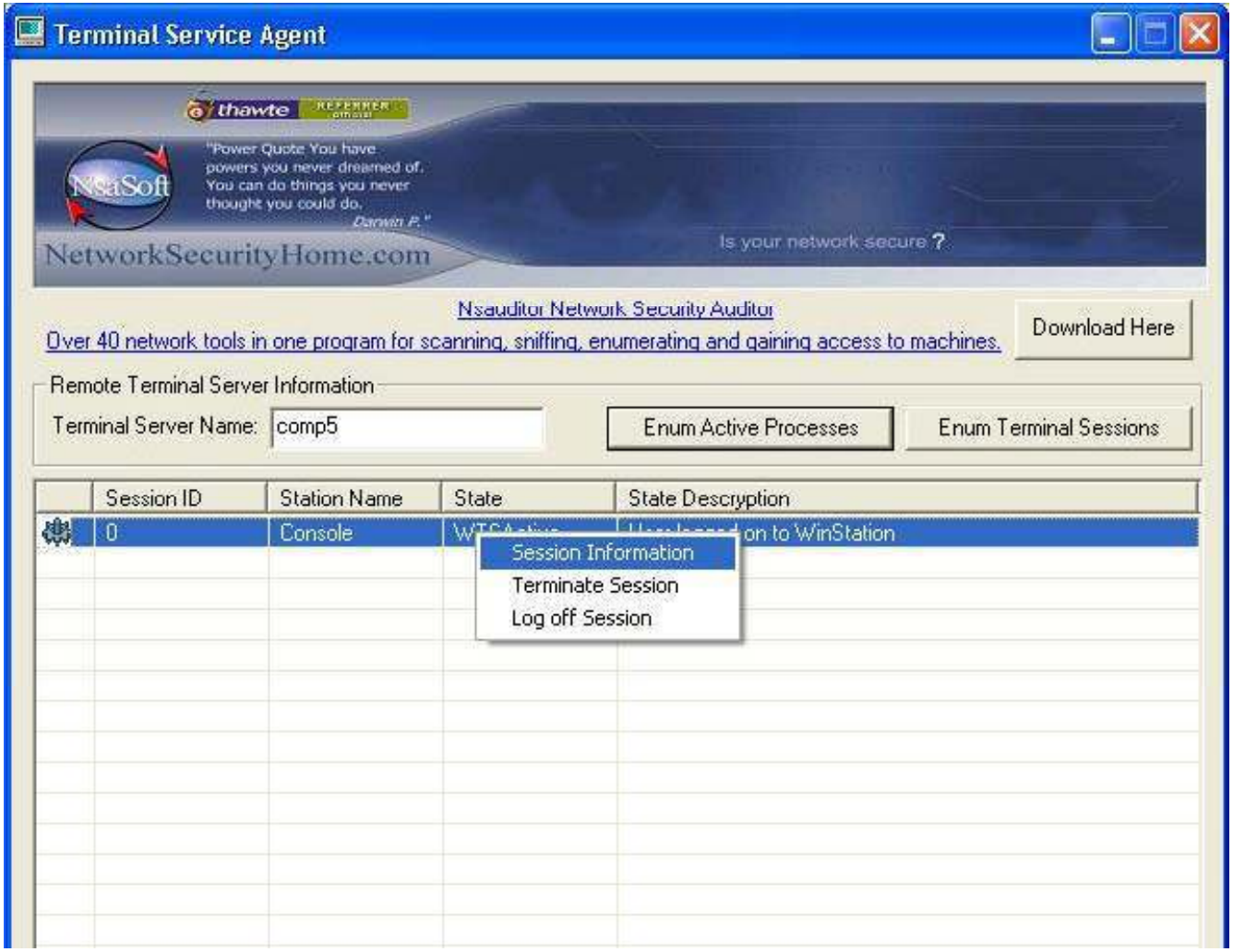


Terminal Service Agent

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



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

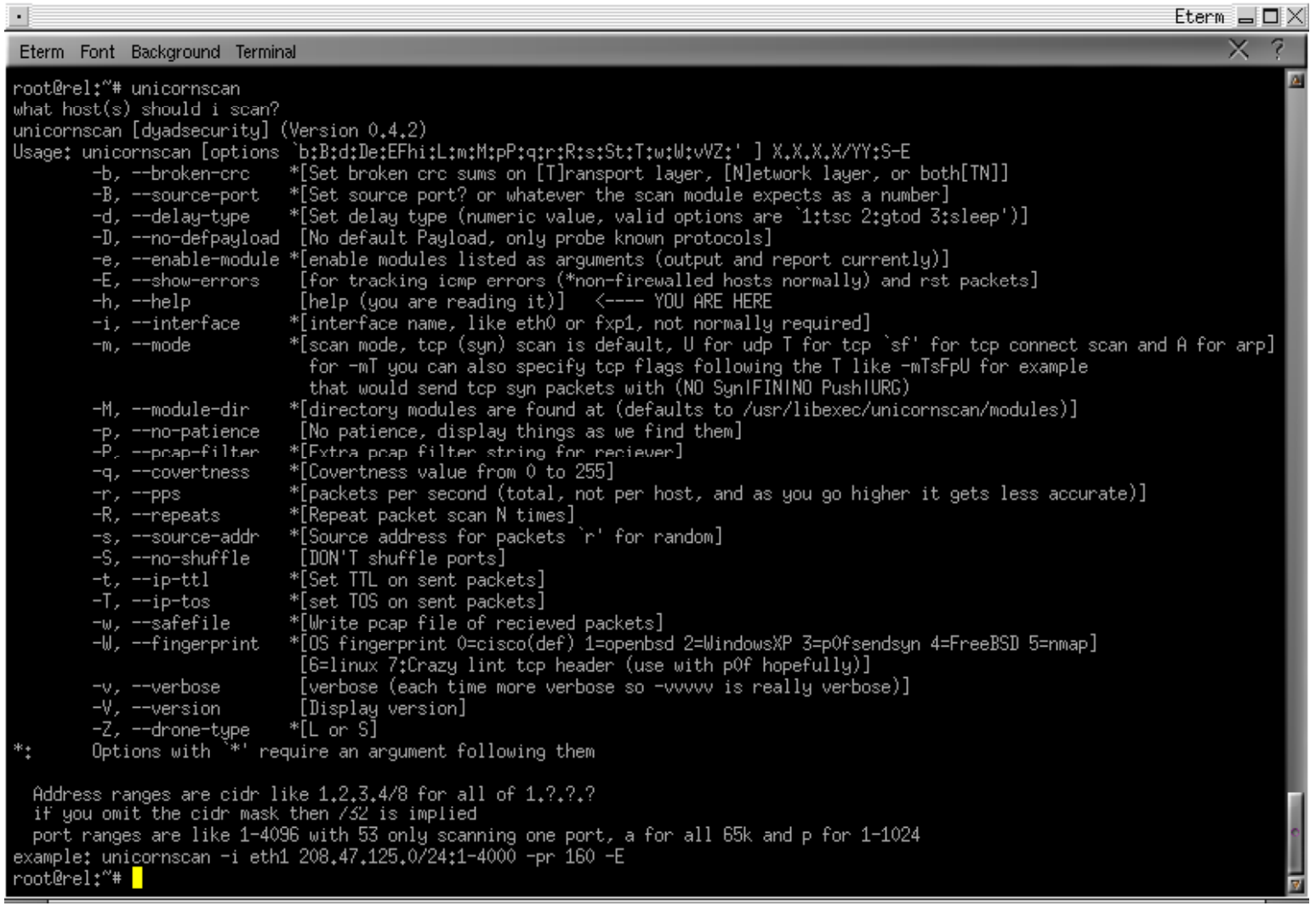
Tool: Unicornscan

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

Unicornscan: Screenshot



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

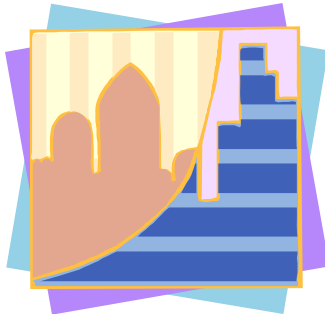
While giving a timeout, it uses ICMP echo request to find the available hosts

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

Summary

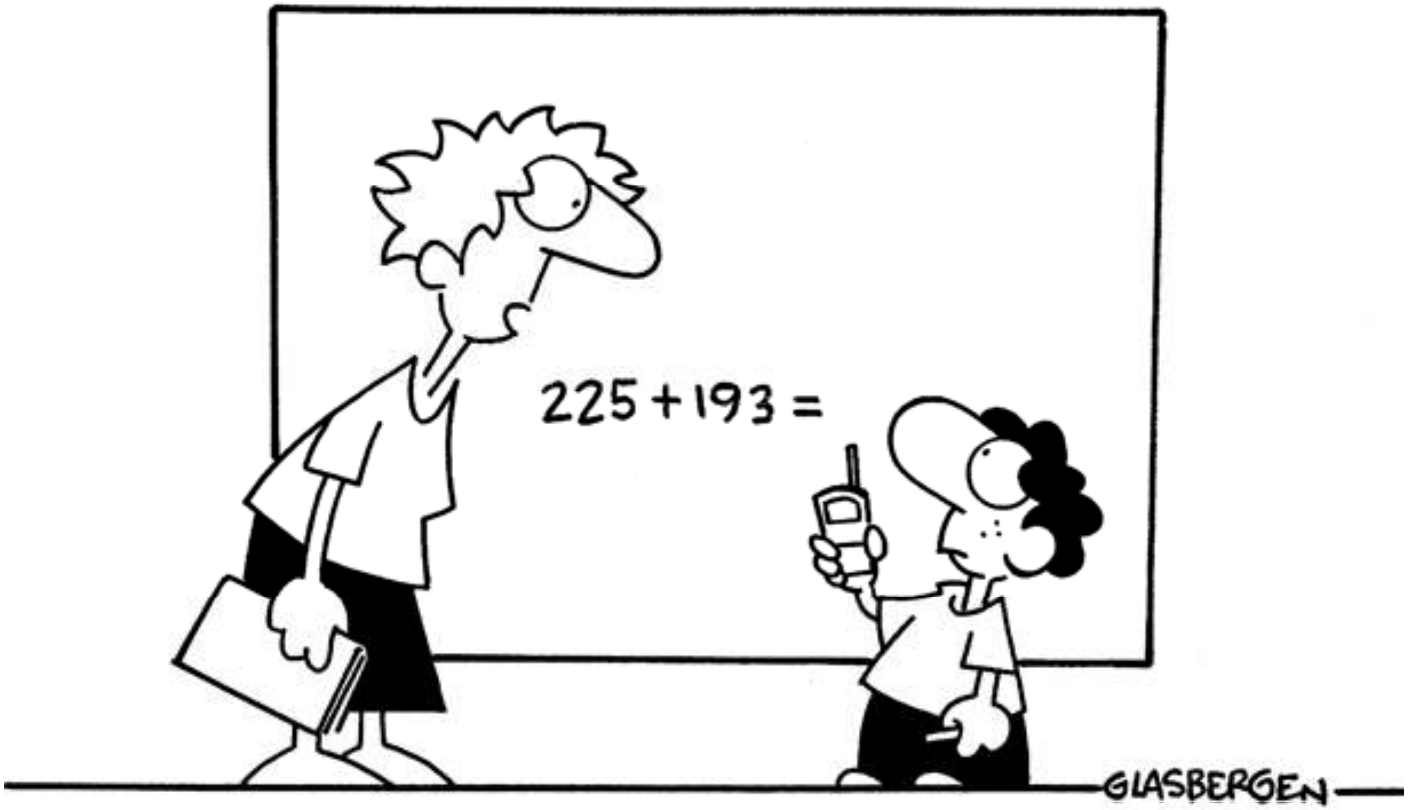
Enumeration involves active connections to systems and directed queries

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



"You have to solve this problem by yourself. You can't call tech support."

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