Remote Access and Management

Ideas, Thoughts, Do' and Don'ts

Don Murdoch, CISSP

MCSE, MCSD

Presented on behalf of Compass Technology Management

Agenda

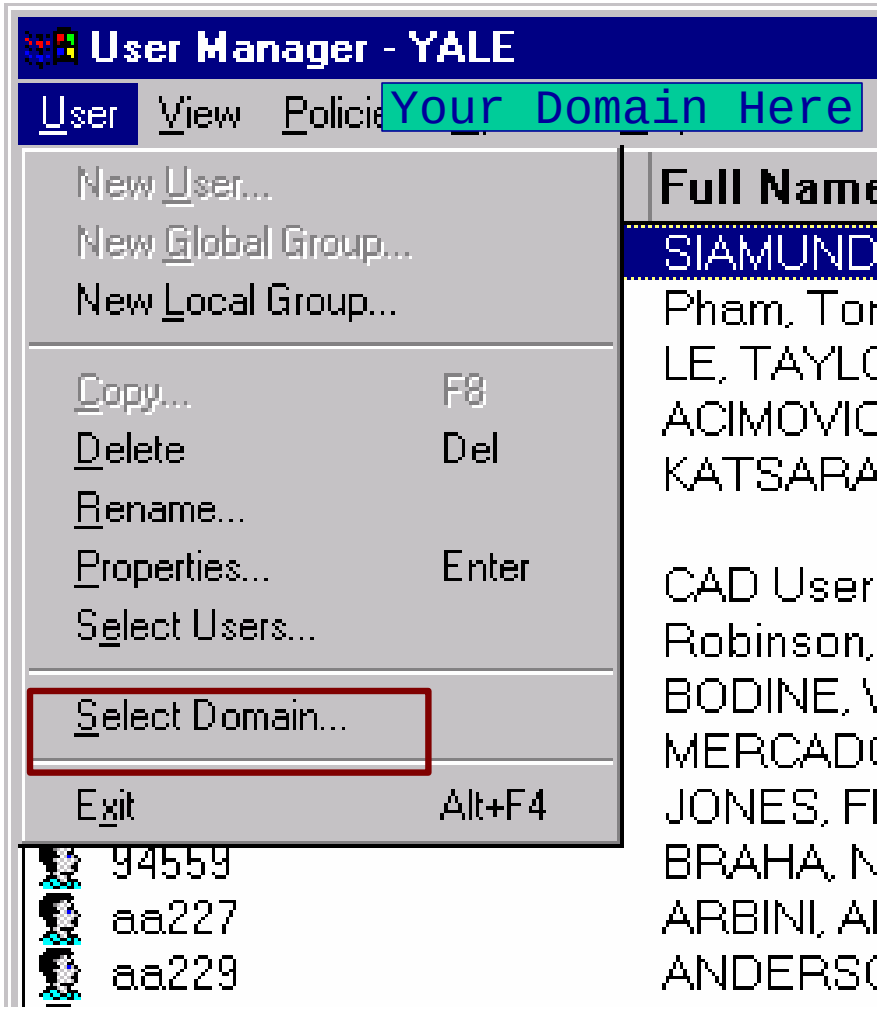
- Discuss Remote Admin / Management
  - Windows NT/2000 Native Capabilities
  - Resource Kits
  - Terminal Server
- SSH for Unix and Linux
- Security issues involved with remote management
- Thoughts from real life

Past and Present

- Past – desktop control
  - PCAnywhere
  - Carbon Copy
  - Remotely Possible
  - MSFT RAS (dial in to an NT/2000 network)
- Present - remote access servers
  - IP Remote Access Cards
  - Microsoft Terminal Services
  - Web based Admin for the Unix / Linux world
  - Thin Client and/or Fat Client
  - Some sort of VPN

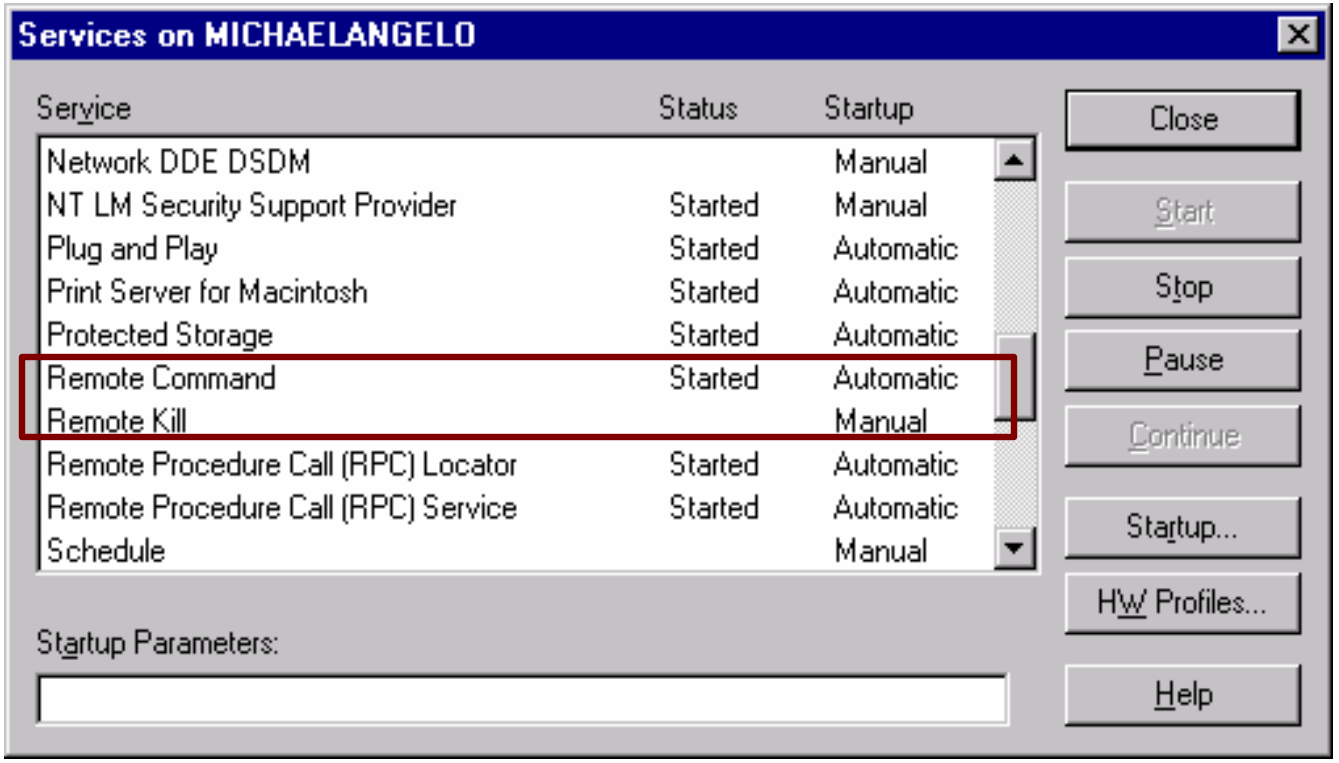
WinNT4 Server Tools

- Most have a “Select Computer” or “Select Domain” option
- On the Server CD \clients\srvtools\OS
- Common management tools are available
- User Manager for Domains can also manage local WinNT user lists



NT4 Remote Services

- View connections to a remote server
- Remote Shutdown
- Service Installation Wizard
- Process Viewer
- Control schedule service on a remote machine



NT4 Command Line Tools

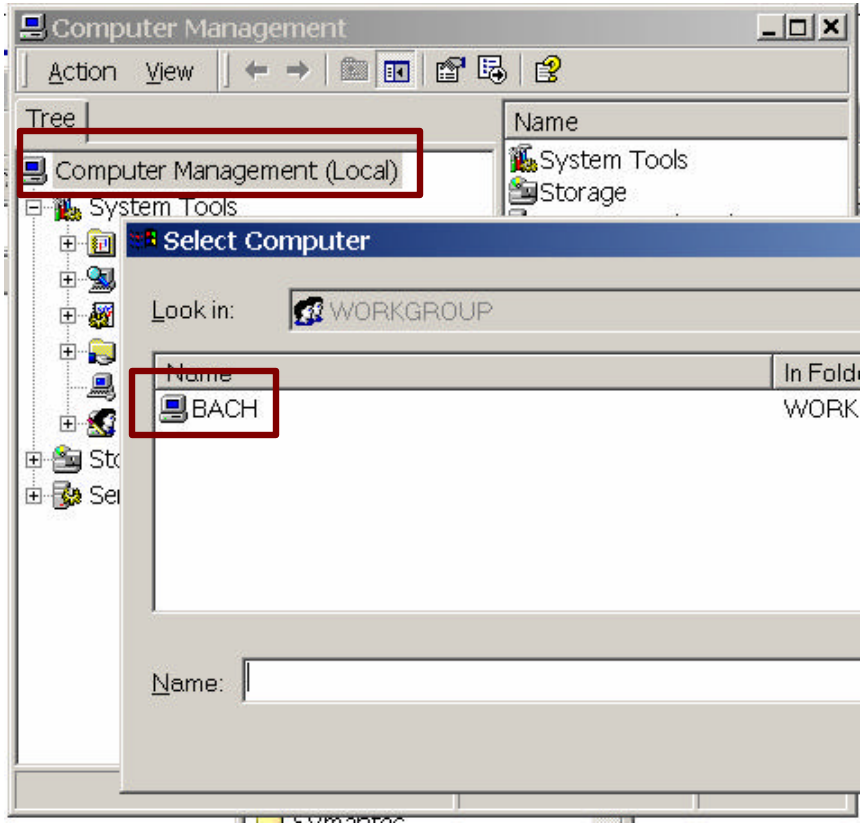
- netsvc - control services on a remote machine
- rcmd - can also execute a single command on a remote machine
- rmtshare - manage shares on a remote machine
- addusers - add/delete users or change group memberships in a computer/domain
- dumpel - dump event log(s) from a specified machine to a file

General Remote Topics

- Windows drives are shared as hidden
- File system can be manipulated remotely
- Registry can be viewed / edited remotely in regedit and regedt32
- Win2000 Computer Management can fully manage 2000 systems and mostly/partly manage NT4 SP6 systems

Win2000 Administration Tools

- Many Windows 2000 administration tools allow for selecting a computer to manage
- Most will popup a workgroup or domain dialog – or you can type in a name or IP address



NT/2000 Resource Kits

- Resource Kit - Many functions can be remotely monitored and/or managed with tools.
- Numerous command line tools -including scripts to control users, services, sharing and security.
- Quality may be a little off - because they are mostly projects by the developers of NT.

Resource Kit Tools

- Command Line Service Utilities
  - Netsvc.exe, Sc.exe, sclist.exe
- Pulist.exe
  - Command-line tool displays processes running on local/remote computers.
- Svcmon.exe
  - Service Monitoring Tool
- Uptime.exe
  - Analyzes a single server by processing the event log to determine reliability, availability, and current uptime.

More Resource Kit Tools

- Browmon.exe: Browser Monitor
- Dommon.exe: Domain Monitor
- Logevent.exe: Event Logging Utility
- Qtcp.exe: measures end-to-end network service quality
- Rpinc.exe (RPC Ping): RPC Connectivity Verification Tool
- Srvinfo.exe: General server info utility
- Robocoyp.exe: Robust File Copy Utility

Even More Resource Kit Tools

- Httpcmd.exe: Command-line HTTP client
- Httpmon.exe: HTTP Monitoring Tool
- Cusrmgr.exe: Console User Manager
- Rassrvmon.exe: RAS Server Monitor
- Rcmd.exe & Rcmdsvc.exe: Remote Command Service
- Shutdown.exe: Remote Shutdown

Great tools, but how ...

Do we get there from here?

NT RAS Supported Connection Types

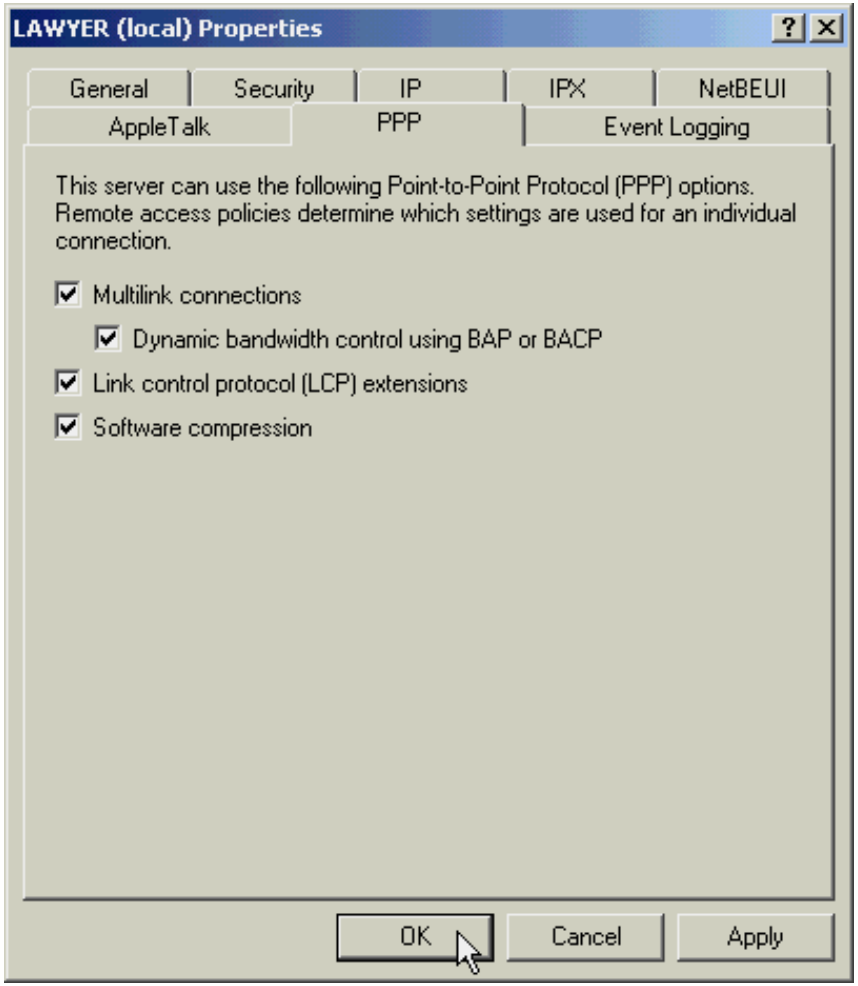
- Modems
  - Asynchronous modems
  - Synchronous modems via access server
  - Null modem connections
  - Regular dial-up telephone lines
- Leased telecommunications lines; T-carrier
  - ISDN lines (and digital modems)
  - X.25 lines
  - Frame relay lines (?)
- Protocols
  - TCP/IP, NWLink, NetBEUI, PPP, PPTP, L2TP

MultiLink Support

- Multilink:
  - RAS can aggregate multiple data streams into one logical network connection for the purpose of using more than one modem, ISDN channel, or other communication line in a single logical connection
- Bandwidth Allocation Protocol (BAP):
  - A protocol that works with Multilink in Windows 2000 Server that enables the bandwidth or speed of a remote connection to be allocated on the basis of the needs of an application (max = number of available devices)
- Bandwidth Allocation Control Protocol:
  - Similar to BAP, but BACP is able to select a preferred client when two or more clients compete for the same bandwidth

Enabling Multilink

- Use the Routing and Remote Access Tool
  - Right-click the RAS server
  - RAS server prop's
  - Specific to each RAS Server



Windows 2000 Terminal Services

Once I’m there, lets do something really useful!

TSE Basics

- Extend MSFT apps to variety of desktops
- Two usage scenarios
  - Remote Admin
    - Server management from anywhere e
  - Application Sharing
    - Deploy apps to legacy PC's
    - Centralized app management
    - Involved licensing and system setup
    - Several RK tools to help along the way

New TSE features

- Printer redirection
  - Auto detection & install of printers
  - Supports printing from Windows applications
- Session Remote Control
  - Administrators can shadow a client's session
  - Provide help or intervene from remote location
- Clipboard redirection
  - Cut & paste between apps running locally and those running in the remote session

TSE Remote Admin Mode

- Scheduling for background services
- TS App Compatibility code disabled
- No Client Licensing Requirements
  - Two built-in per-server connections
- Minimal Performance Impact
  - ~85K non-paged, ~175K paged kernel memory, ~2.25Mb overall commit
- Must be enabled (not on be default)

Administering TSE

- TS functions integrated with Win2000 tools
  - Task Manager, User Manager, DS Admin
- TS Specific Tools
  - TS Protocol Configuration Tool
  - TS License Manager
  - Terminal Services Manager
    - Monitors users and their processes
    - Disconnect and logoff user sessions
    - Used to initiate session remote control
- Command-line interfaces
- Performance Counters

Securing Windows Term Server

- Make use of the allowed IP addresses feature – limit admin hosts
- Enable TCPIPHostBindMode to only listen on admin interface
- Change default port
- Make sure the Windows NT user is logged off after session disconnect (normal and abnormal)
- Enable event logging and session recording (if disk space permits)

Securing Windows Term Server

- If possible, use X.509 for host authentication
- Disable response to PCAnywhere query broadcasts
- Configure clients to only use TCP to connect (rather than a UDP query – reduces firewall ruleset)
- Use separate user account for each admin with strong passwords
- Limit login attempts
- Only use PCAnywhere user with PCAnywhere privileges

The Secure SHell

Managing Linux and Unix systems remotely

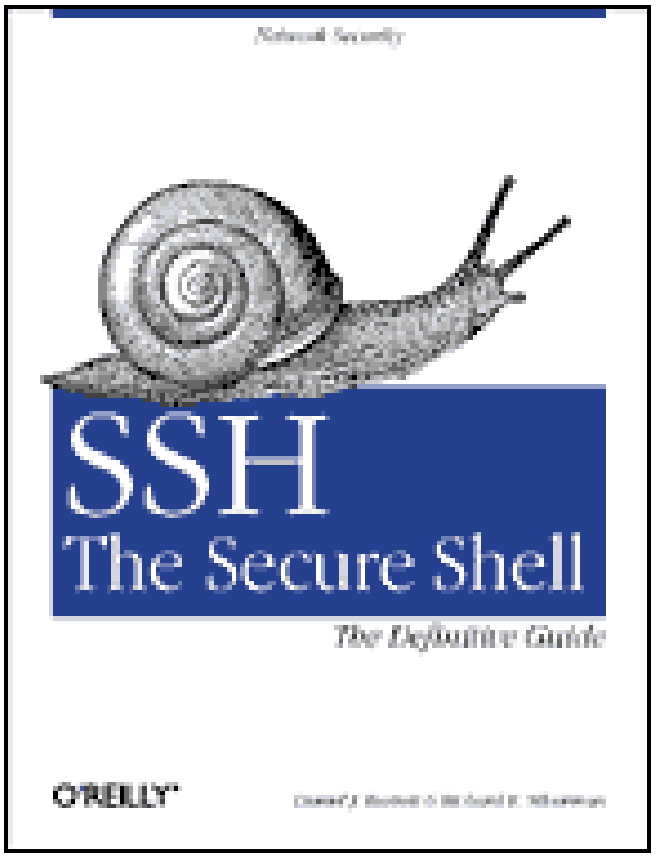
Section Agenda

- Explain how to use SSH
- Demo client software
- Explain server side configuration

- Sources of Information
  - OpenSSH.ORG
  - Cory L. Scott, Lead Security Consultant Securify, Inc.
  - Heidi and Bruce Potter, Shmoo Group

SSH – One of the Best Things Going

- Secure SHell.
- Replacement for Telnet, r-commands, and ftp
- Public/Private based keying for high security
- Variety of clients and servers available



Why do this?

- Using older *nix remote tools is inherently insecure
  - Telnet and FTP transfer username, password, and commands in clear text
  - Berkley “r” commands are vulnerable to trust relationship exploitation
- Variety of network based vulnerabilities possible
- SSH can use public/private key methods of encryption

So – what is SSH?

- Practically, a “Drop In” replacement for “r” commands, telnet, and ftp
- Strong authentication
  - User can be validated against public/private key pair; can require user to have private key
- Data encryption
  - Data is encrypted on the wire
  - Port forwarding encrypts other traffic as well

What does it consist of?

- sshd
  - Server side program
- ssh
  - Client program
- scp
  - Command line file copy
- ssh-keygen
  - Create Pubkey Authentication (RSA or DSA) keys
- ssh-agent
  - Authentication agent (keyholder)

What else?

- ssh-add
  - Registers new keys with the agent.
- sftp-server
  - Secure FTP server subsystem.
- sftp
  - Secure file transfer program.
- ssh-keyscan
  - Gather ssh public keys.
- ssh-keysign
  - ssh helper program for hostbased authentication.

SSH Architecture

- SSH works in three distinct layers
  - Transport layer protocol
  - Authentication protocol
  - Connection protocol

- IETF working group page
  - http://www.ietf.org/html.charters/secsh-charter.html

Transport Layer

- Runs over TCP/IP
- Negotiates and handles
  - Shared secret (Diffie Helman Key Exchange)
  - Encryption and algorithm usage
  - Key management
- Client – uses public key algorithm to identify the server (trust but verify)
- Tunnels other protocols

Authentication Protocol

- Multiple methods supported
  - Username / Password
  - Client Keying
  - Encryption negotiation
- Preauthentication banners supported
  - “Your use of this system …”

Authentication Protocol

- Channel management
  - Open / Close and direction
- Port management
  - Pseudo-tty
  - X11 forwarding
  - Authentication agent forwarding,
  - Environment variable passing,
  - Window commands
  - TCP/IP port forwarding

Where can you use it?

- Server side
  - Open Source – most *nix systems that are in the main stream
  - Purchase Source – 600 to 800 for Windows NT/2000
- Client Side
  - Open Source – most *nix systems, Windows 98/NT/2000 and Mac OS/X (PuTTy)
  - Purchase Source – Windows (FSecure)

Unix / Linux installation

- Most recent distributions include ssh
- Build from scratch –
  - Likely to need RSA reference source
  - Download from openssh.org/.com
  - tar, configure, make, make install

Login process

- Client side
  - Will default to current logged in name -or-
  - xsh -l userjoe@host.name.edu (port 22)
- Server side
  - Responds with public host keys, rand, and supported encryption types
- Process side
  - Client/server use keys to authenticate - because both compute session key

SSH common options

-l	Use specific logon name
-F	Use specific config file
-X	Enable X11 forwarding
-i	Identity for public key
-v	Verbose output (several screens worth)
-c	Set the encryption cipher algorithm
-p	Server port number (default 22)
-D	Enable dynamic port forwarding

SSH protects against

- Intercepting passwords
- Protocol eavesdropping

RSA KeyGen Process

- User needs to generate a set of RSA keys using ssh-keygen
- A pass phrase s used to encrypt the user's private key
- Public key goes on the server in ~user/.ssh/authorized_keys
- The server checks to see if the connecting user@hostname is listed in auth keys

Web based management of Linux Systems

WebMin

- Self contained web server
- Web based GUI tools
  - HTML front end, sh/perl back end
- Extendable for other management tools
  - Example on www.snort.org
- 239 add in modules
- Runs on non-standard port
- Should only be made Internet accessible when using SSL

A Few Other Ideas

(are we done yet?)

Windows GUI – PCAnywhere

- Risks
  - Runs on well-known port – juicy target for attackers
  - Previous versions have been vulnerable to DoS attacks and weak password encryption
  - Typical configuration binds to all interfaces
  - Should avoid exposing on an untrusted network segment
  - Typical configuration bypasses Windows login mechanism

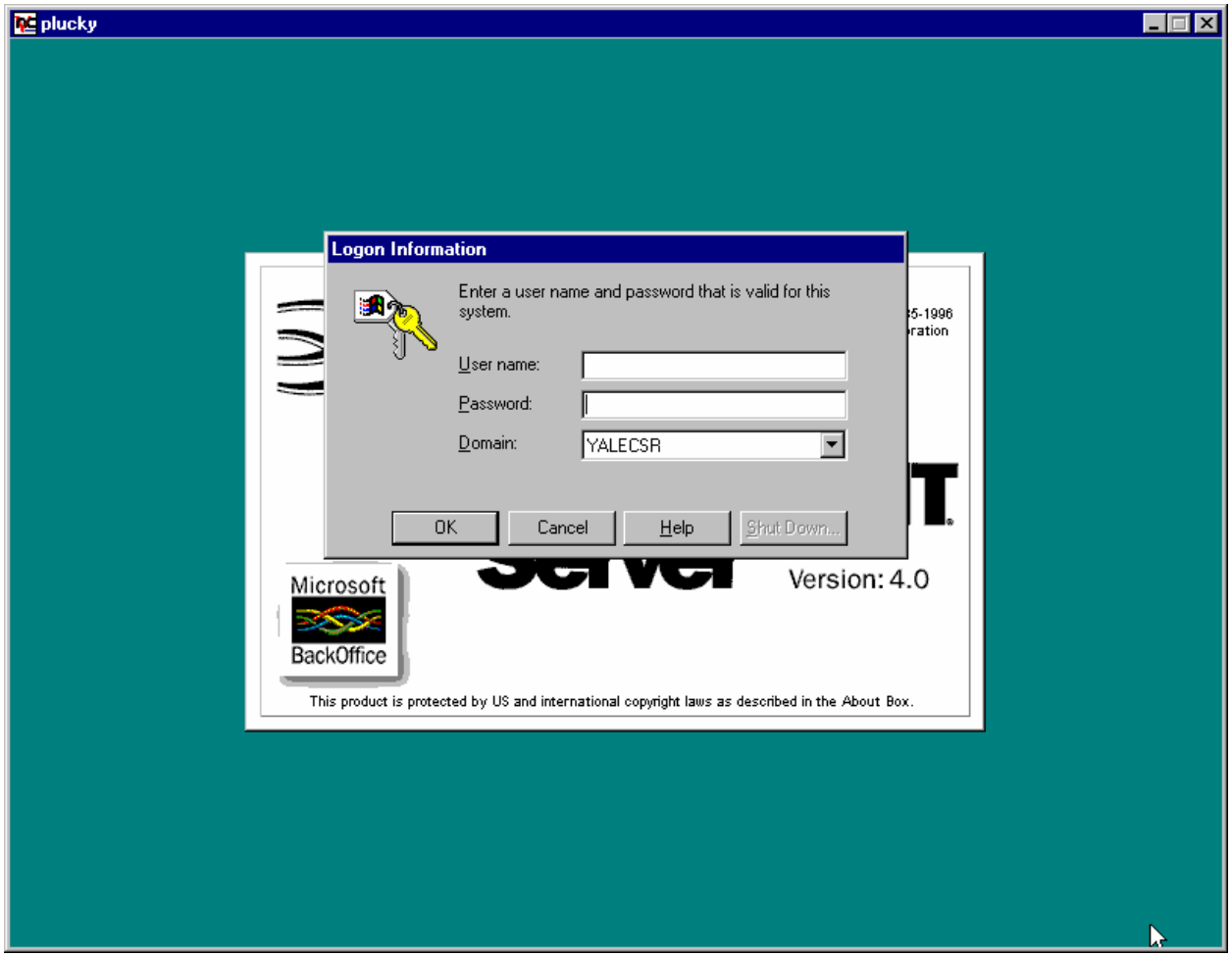
Securing PCanywhere

- Make use of the allowed IP addresses feature – limit admin hosts
- Enable TCPIPHostBindMode to only listen on admin interface
- Change default port
- Make sure the Windows NT user is logged off after session disconnect (normal and abnormal)
- Enable event logging and session recording (if disk space permits)
- Utilize Symmetric encryption / Deny lower-level
- If possible, use X.509 for host authentication
- Disable response to PCAnywhere query broadcasts
- Configure clients to only use TCP to connect (rather than a UDP query – reduces firewall ruleset)
- Use separate user account for each admin with strong passwords
- Limit login attempts
- Only use PCAnywhere user with PCAnywhere privileges

VNC

http://www.uk.research.att.com/vnc/index.html

- Some say yes, some say no…
- Cross Platform!!!



VNC over SSH? GRRREAT!

- URL:
  - http://www.uk.research.att.com/vnc/sshvnc.html
  - http://web.mit.edu/pismere/ssh/vnc-over-ssh.html
  - Putty: http://login.hmdc.harvard.edu/~mathpre/vnc/putty/