COMP 175

System Administration and Security

Network Neighborhood

SAMBA SERVER

Course Topics

- Protocol History
- Windows Networking Overview
- Overview of Samba
  - The different protocols
  - Samba functions
- Configuration of Samba
  - Server side
  - Client side
  - SWAT

Objectives

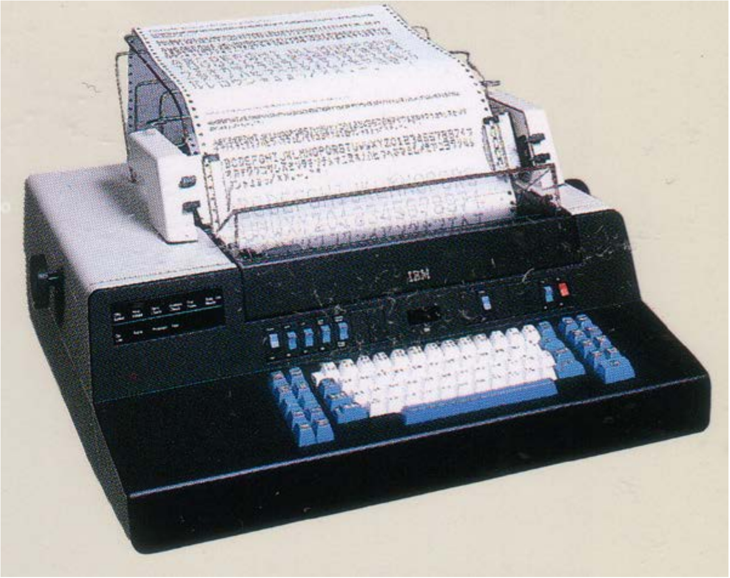
Upon completion you should be able to:

- Set up a SAMBA server for various clients
  - Login clients
  - Shared Resources
- Troubleshoot configurations
- Understand Network Attached Storage (NAS)

History 101

Vendor-based LAN standards

- DEC – DECnet to connect PDP-11's (1975)
- Apple – Appletalk to connect Macintosh's (1985)
- IBM – Systems Network Architecture (SNA) (1975)



History 101

- IBMs' SNA describes formats and protocols
- SNA implementation is VTAM software
- Network Control Program (NCP)
- Synchronous Data Link control (SDLC)
- Customer Information Control System (CICS)
- Still in use in financial industry
- SNA was too big for early PC's
- IBM hired Sytek to create **PC Network**
- NetBIOS (Network Basic Input Output System)
  - Software interface to PC Network hardware
  - Max-nodes=80   security not considered

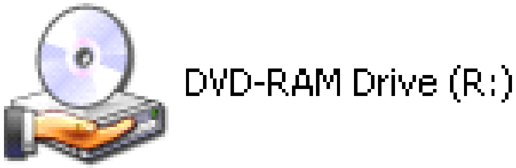
History 101

- NetBIOS API – commands
  - Could control the hardware
  - Establish and delete sessions
  - Transfer data
- Starting with DOS 3.1 NetBIOS API was used to transport Server Message Block (SMB) file service messages providing shared access to:
  - Files
  - Printers
  - Serial Ports

History 101

Windows network shares

- Microsoft built into Windows 3.1 the ability for Windows boxes to have ***shares***
- Shares are files, directories, and drives for which users have enabled sharing (right-click on the icon, etc. A hand appears holding the shared item)
- Microsoft wrote NetBIOS (Network Basic Input Output System) to run all this *
- NetBIOS is not routable over the Internet, and everyone on the LAN is presumed trustworthy so Microsoft did not concern itself a great deal with security



NetBIOS Formative Years

Vendors implement NetBIOS API on other protocols

- 1985 IBM NetBIOS ExtendedUser Interface: NetBEUI
  - Provides NetBIOS over Token Ring (IEEE 802.2 LLC)
  - 1985 MS creates NetBIOS MS-NET (IEEE 802.2 LLC)
- 1986 Novell NetWare – NetBIOS over IPX/SPX
- 1987 NetBIOS encapsulation over TCP/IP
  - Name service (lookup, add name, ...)
  - Session service for connections (TCP) call, listen, send
  - Datagram distribution mechanism (UDP) send, bcast

Whoops! Encapsulation happened!

Its an insecure day in the neighborhood...

Windows Network Shares

- Message format is Server Message Block (SMB)
- Protocol is Common Internet File System (CIFS)
- CIFS/SMB used for printer and file sharing
- UDP Ports 137, 139
- Messages transfer using TCP Port 139
- W2K –> on uses TCP 139 and/or TCP 445

- MS SMB2 – Vista, Windows 7, Windows 2008
  - Better asynch support, larger r/w sizes
  - Huge BSOD vulnerability – Epic Fail

SAMBA

Samba - xNIX implementation of SMB/CIFS

- Integrates Linux/Unix servers and desktops
- Provides:
  - File & print services
  - Authentication and Authorization
  - Name resolution
  - Service announcement (browsing)

More on this later

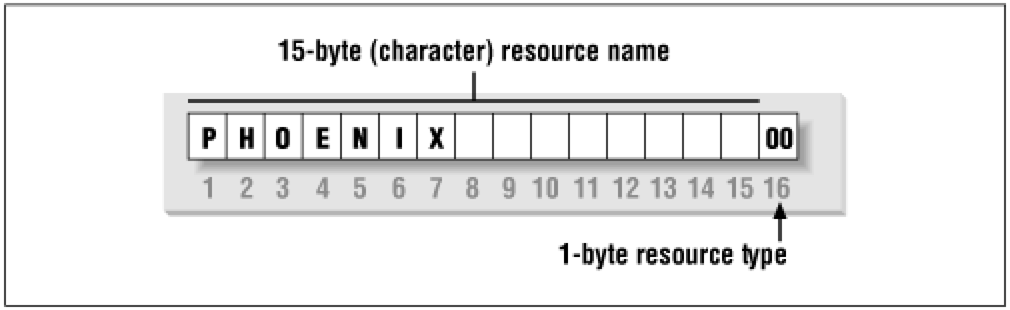
NetBIOS LANs

NetBIOS LAN emulation requires: (RFC 1001/1002)

- Name Service: map NetBIOS names (addresses) to IP addresses in the underlying IP network
- Datagram Service: provides for the delivery of NetBIOS datagrams via UDP
- Session Service: establish and maintain point-to-point, connection-oriented NetBIOS sessions over TCP

NetBIOS

- NAME = 15 char (16th char is Suffix)
- WINS for name service (like DNS)
- LMHOSTS file for statics (like HOSTS file)
- Node type: how names resolve to IP address
- Suffix map service to record type
  - 1B Domain Master Browser (PDC)
  - 1C Domain Controller (record w/ up to 25 IP's)
  - 01 Master Browser
  - 1E Browser service elections



Names

As each machine comes online

  - It claims a name for itself

- The NetBIOS Name Server (NBNS) keeps track of which hosts have registered a NetBIOS name
- Each machine on the network defends its name in the event that another machine tries to use it

Name Resolution (In this order for Hybrid mode)

- NBNS resolves NetBIOS names to IP addresses
- Each machine echos its IP address when it "hears" a broadcast request for its NetBIOS name

Windows Networking

- Primary function of **browser service** is to:
  - Provide a list of shared resources in domain
  - List of other domain, workgroup names across the wide-area network (WAN)
- View network resources
  - Network Neighborhood
  - NET VIEW command
  - Tools using APIs

- Microsoft Active Directory (AD) services in Win2K and XP replaced the browser name service
  - Backwardly compatible

Browser Service

- At startup – the OS sends a host announcement frame. This is repeated at 4 minutes, 8 minutes, then repeated every 12 minutes thereafter.
- Browser service maintains a list of domain or workgroup names along with the protocol used for each computer on the network segment
- Graceful shutdowns notify the master browser and are removed from the list (non-graceful?)
- Computers running the browser service elect a master browser for each Lan segment

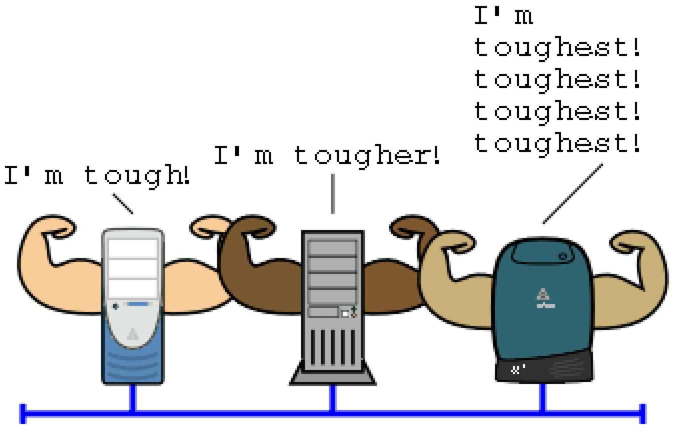
```
process_local_master_announce: Server NEON at IP 10.0.0.7 is
announcing itself as a local master browser for workgroup
ELEMENTS and we think we are master. Forcing election.
```

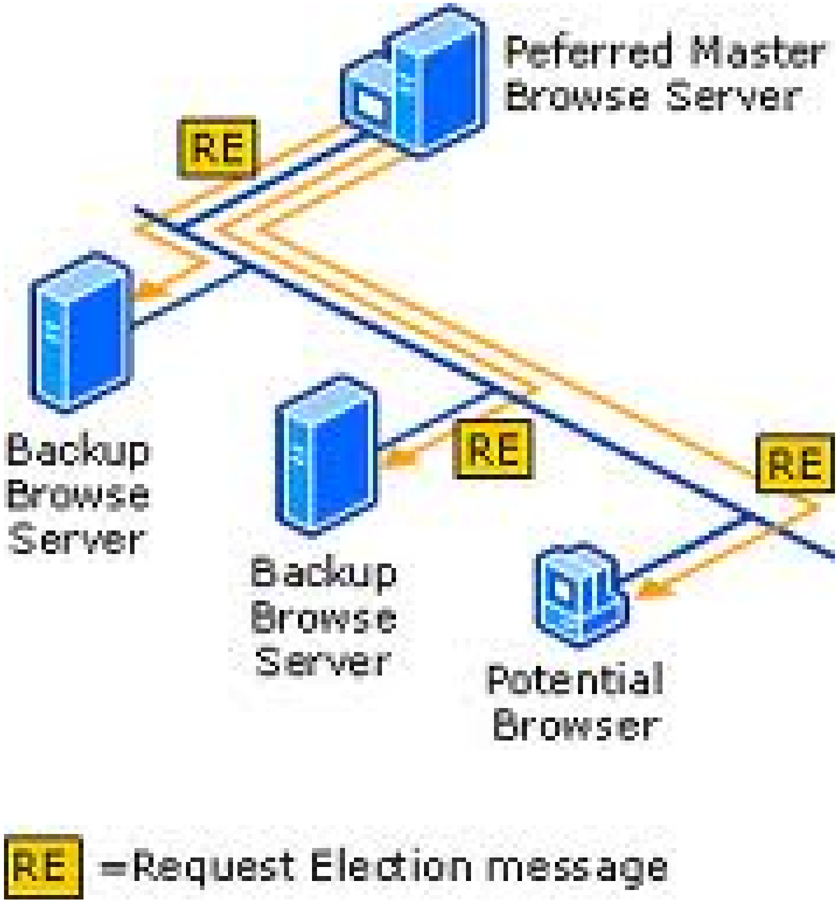
Windows Networking

- If there is a Primary Domain Controller (PDC) it is the master browser for the domain
- Backup Domain Controllers (BDC) are backup domain browsers
- On a given network segment, there is only one master browser. The master browser designates one backup browser for every 32 computers on the segment
- If no domain controller is present on a segment, an election occurs for master browser and backup browser from the computers on the segment

"¿Quien es mas macho?"

- Determination progression is based on:
  - Version level of the browser protocol
  - Server and Desktop OS in the MS hierarchy
  - Uptime
  - Alpha sort order
  - ~~Scissors paper rock~~





Windows Networking

- A new master browser and each workgroup and domain master browser broadcast a:
    - DomainAnnouncement datagram every minute for five minutes, followed by a
    - DomainAnnouncement once every 12 minutes
- A workgroup or domain that has not announced itself for three periods is removed from the list
- Thus a workgroup or domain can appear in the browse list 45 minutes after the workgroup or domain has failed or been shut down
- *…that is a long timeout when debugging network issues*

Windows Networking

- The PDC connects to the primary Windows Internet Name Service (WINS) server every 12 minutes
  - Get a list of all the DomainName entries
  - Adds the workgroup announcements collected by the master browsers, creating:
  - A full list of domain and workgroup names
- Every 12 minutes the master browsers request the list from the PDC

Windows Networking

- The browser service relies on server broadcasts
  - The communication is connectionless
  - By definition – unreliable
- Allowing the loss of a few datagram frames, the host announcement frame to the master browser should be on the browse list within 12 minutes after startup
- In a multi-segment WAN environment, the **max.** time for all domain clients to see new host is 48 minutes (12+12+12+12). On a well-managed network – the average time should be 24 minutes

Windows Networking

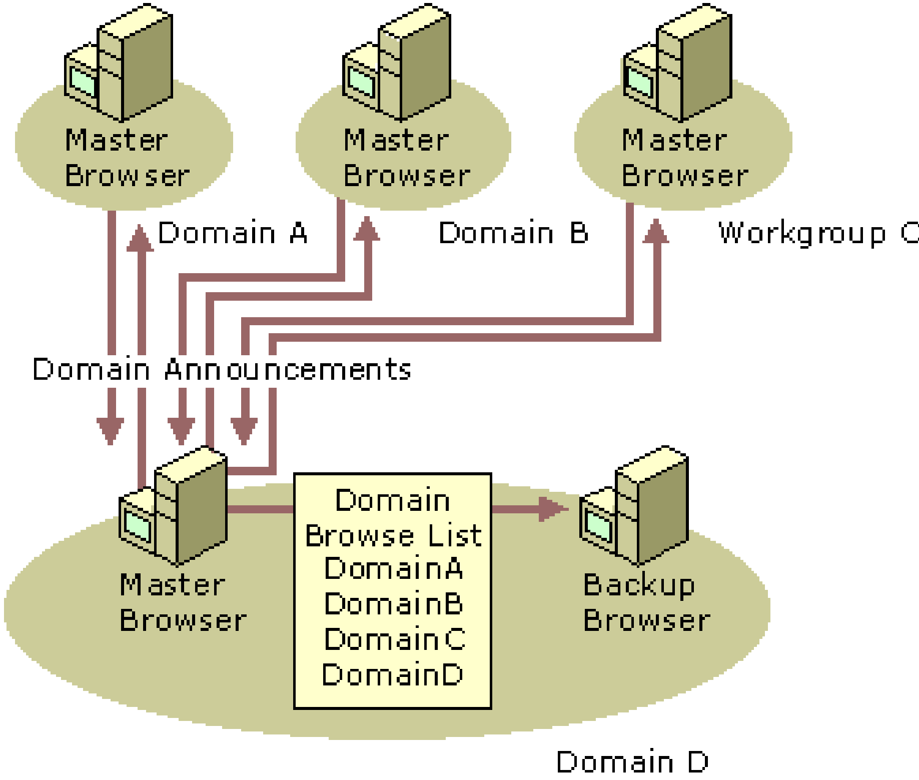
- Allowing for lost datagram frames, the master browser does not remove a host from list until 3 announcement periods pass.
- Non-graceful shutdowns or network outages? Host still in master browser's list up to 36 min. until PDC notified to remove host name.
- Within 12 min. a master browser on remote segment gets the domain-wide list from PDC, and within 12 min. each backup browser connects to master browser. Process can take as long as 72 min. to finish (36 + 12 + 12 + 12)

Windows Networking

- If master browser 'blue screens', it may take up to 12 minutes for a backup browser to discover that no master browser is present

- Very chatty network
- Visibility latency 12-36m

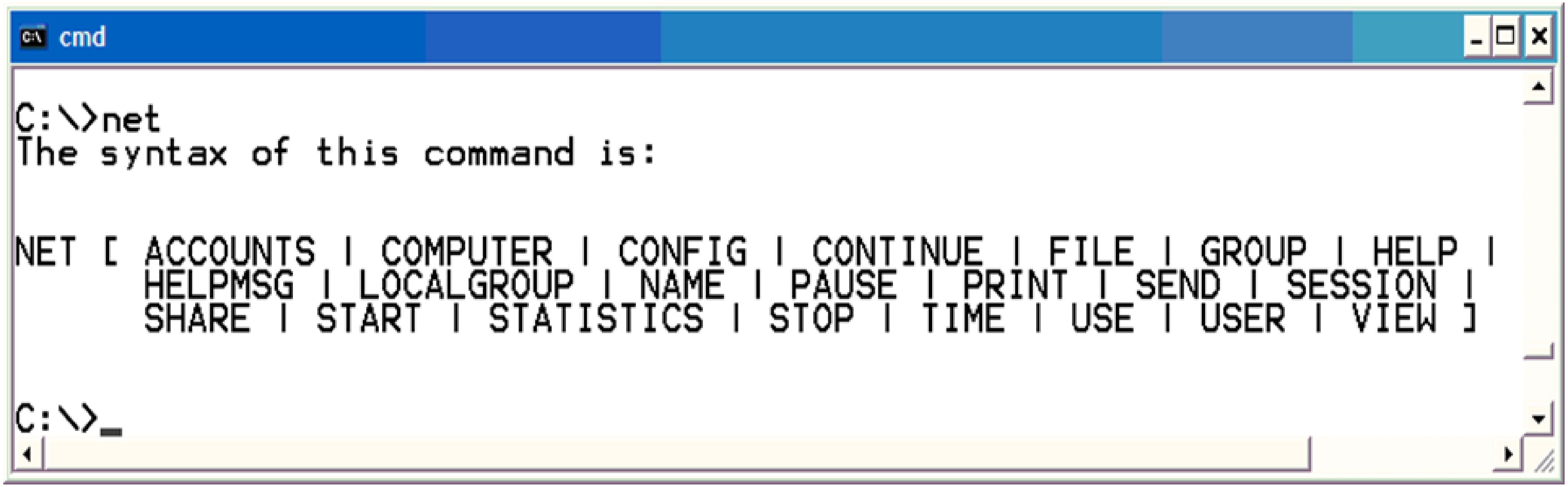
- Networking is non-trivial



Next: What can be seen?

Net Commands

- nbtstat -n   netstat for SMB
- A list of all of Windows’ net commands
  - net statistics [workstation | server]
  - net view (wait for it)
  - net user



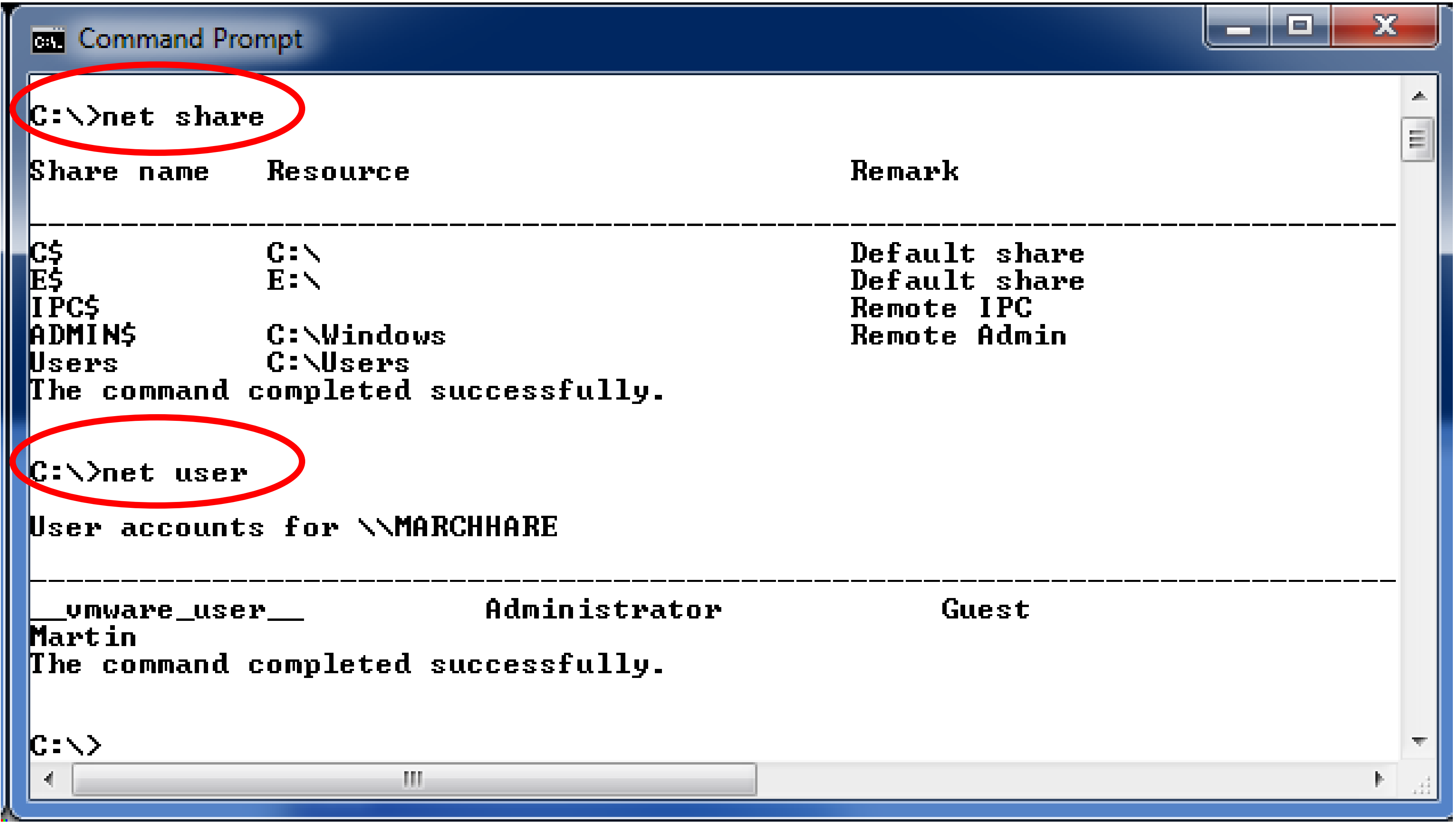
```
C:\>net
The syntax of this command is:


NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]


C:\>_
```

Enumeration

- List of Windows hosts on the LAN
- For each Windows host
  - List of groups
  - List of shares – files, printers
  - List of users & their account information

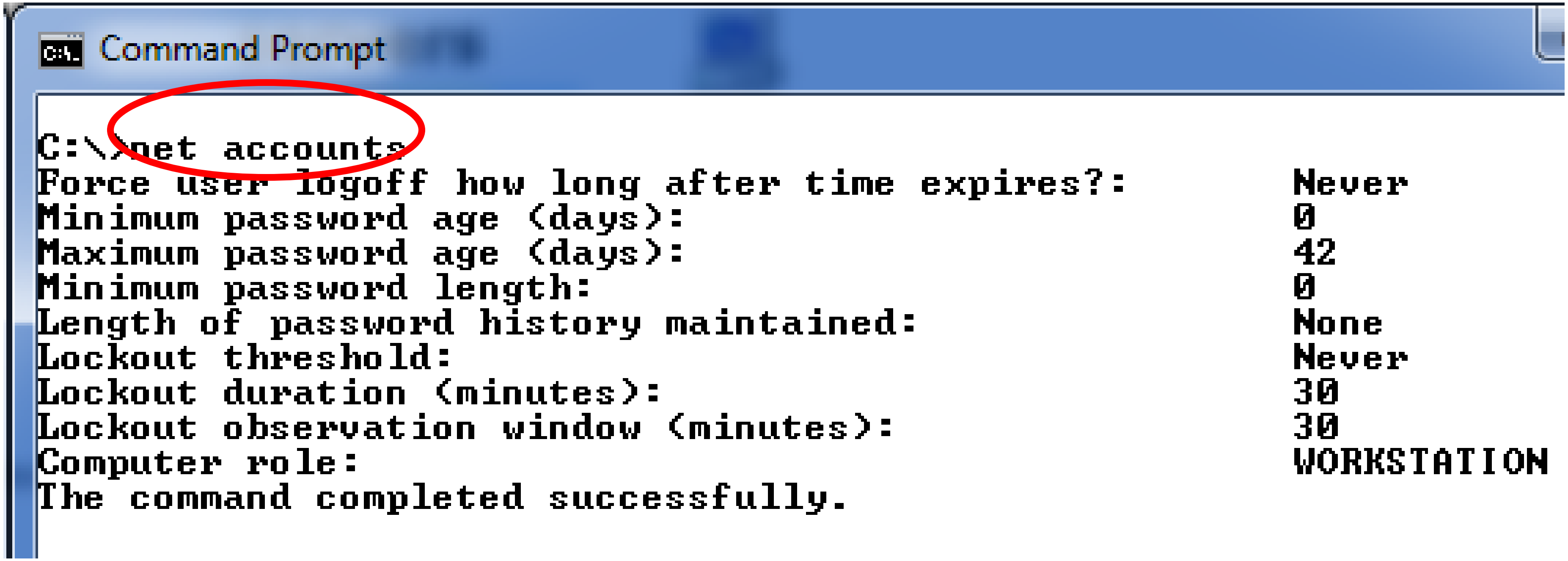
Note: The above could be obtained using a null session: an anonymous connection to shares (IPC$) that allowed read/write access on Windows NT/2000 and read-access on XP and 2003.

Net Commands



```
C:\>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
E$           E:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
Users        C:\Users
The command completed successfully.


C:\>net user

User accounts for \\MARCHHARE

-------------------------------------------------------------------------------
__vmware_user__          Administrator            Guest
Martin
The command completed successfully.


C:\>
```

Password Policy

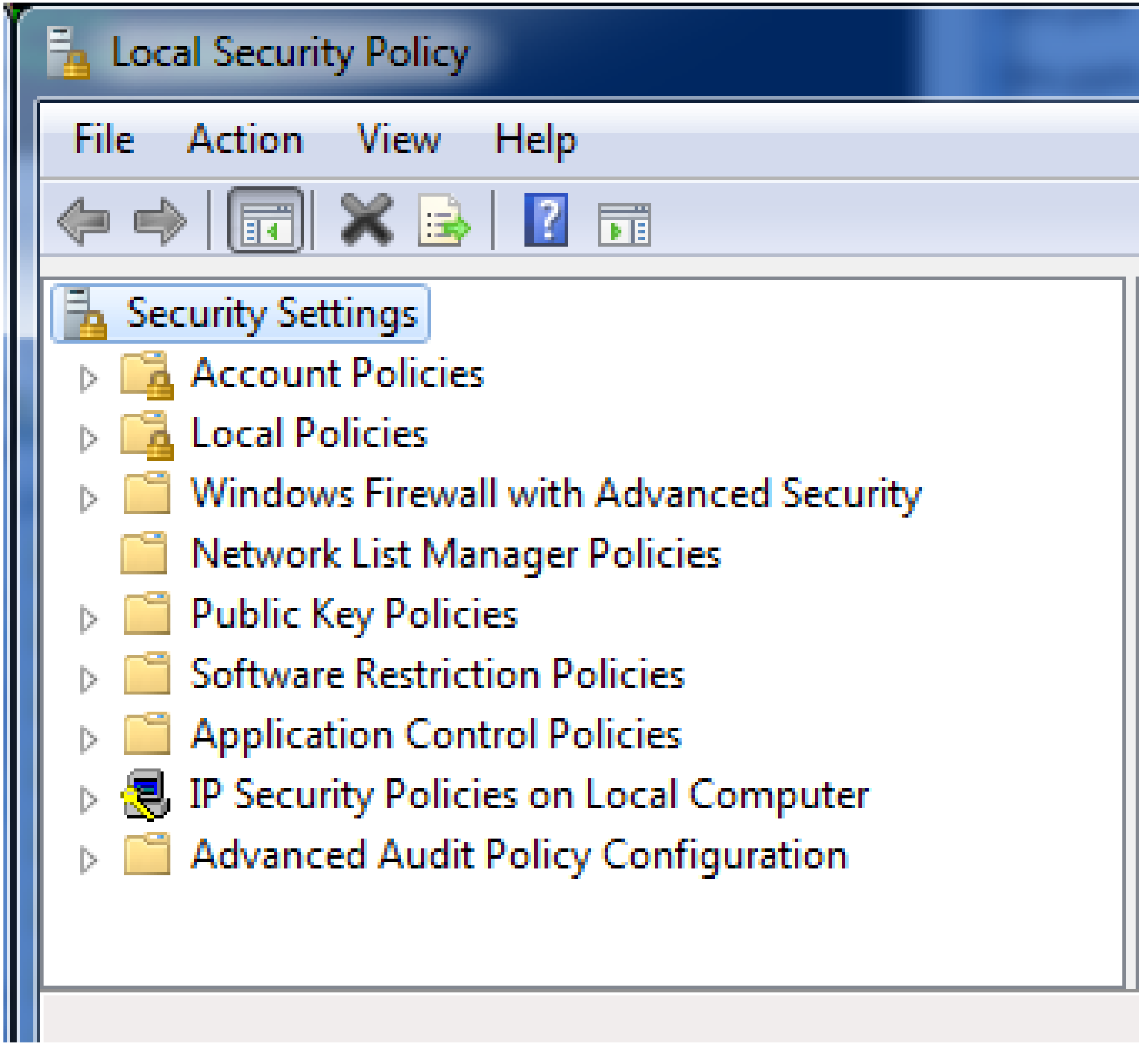


```
C:\>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

Local Security Policy

also:

Group Security Policy



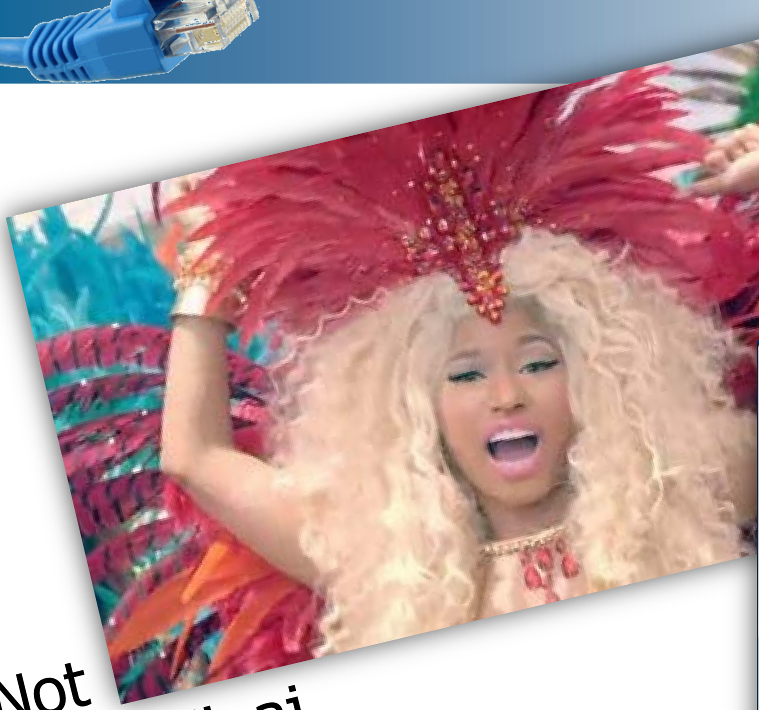
Security Settings
- Account Policies
- Local Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Windows Networking

- Protocol and design was vulnerable to exploits
- Golden age of computer hacking

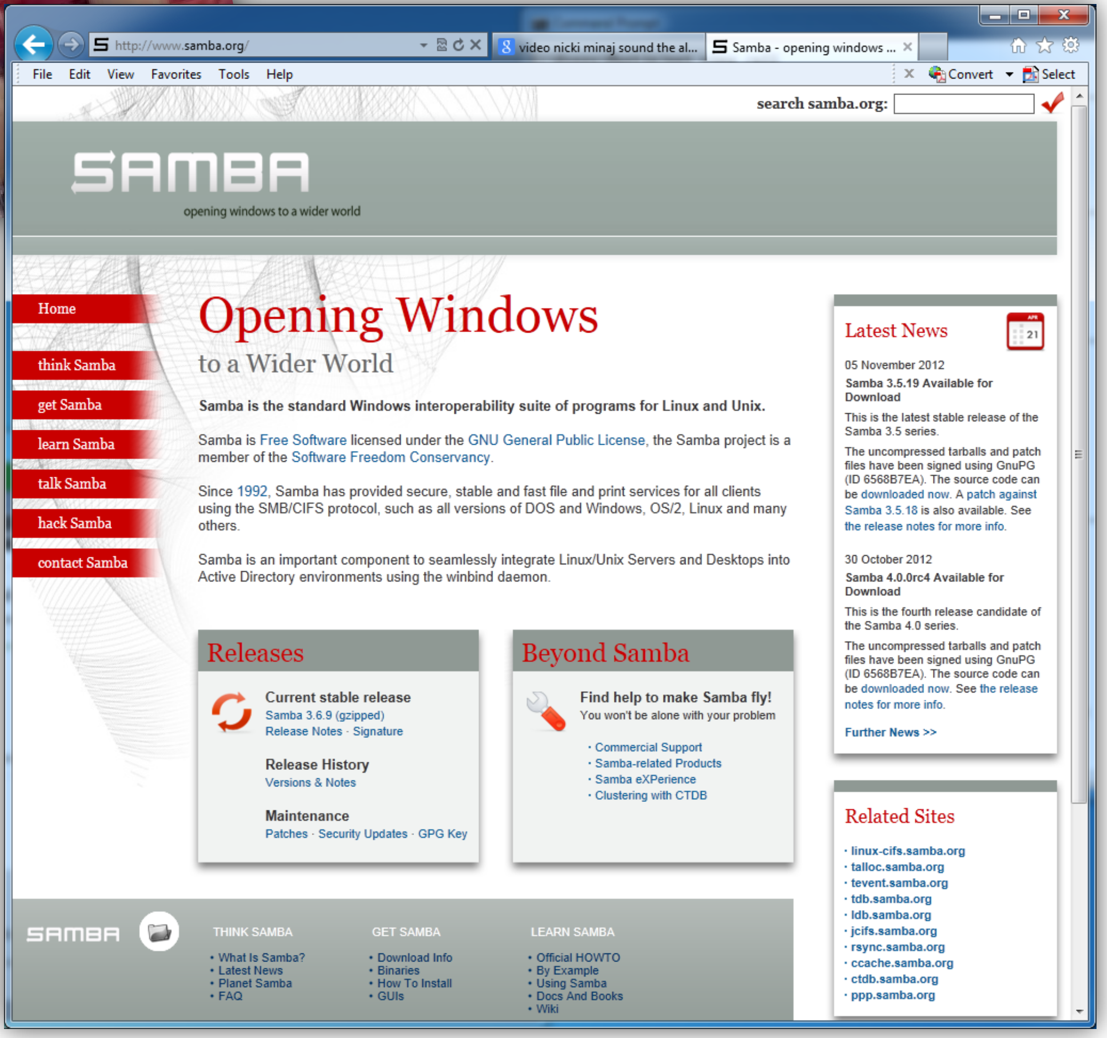
- Null session very helpful
  - Could call API's
  - Use RPC's

- Can we have the functionality...
- Add interoperability with UNIX...
  - Securely? → **Samba**



Not
Nicki Minaj
music video of
Samba

samba.org



SAMBA
opening windows to a wider world

Opening Windows
to a Wider World

Samba is the standard Windows interoperability suite of programs for Linux and Unix.

Samba is Free Software licensed under the GNU General Public License, the Samba project is a member of the Software Freedom Conservancy.

Since 1992, Samba has provided secure, stable and fast file and print services for all clients using the SMB/CIFS protocol, such as all versions of DOS and Windows, OS/2, Linux and many others.

Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops into Active Directory environments using the winbind daemon.

Releases

Current stable release
Samba 3.6.9 (gzipped)
Release Notes · Signature

Release History
Versions & Notes

Maintenance
Patches · Security Updates · GPG Key

Beyond Samba

Find help to make Samba fly!
You won't be alone with your problem

- Commercial Support
- Samba-related Products
- Samba eXPerience
- Clustering with CTDB

Latest News

05 November 2012
Samba 3.5.19 Available for Download

This is the latest stable release of the Samba 3.5 series.

The uncompressed tarballs and patch files have been signed using GnuPG (ID 6568B7EA). The source code can be downloaded now. A patch against Samba 3.5.18 is also available. See the release notes for more info.

30 October 2012
Samba 4.0.0rc4 Available for Download

This is the fourth release candidate of the Samba 4.0 series.

The uncompressed tarballs and patch files have been signed using GnuPG (ID 6568B7EA). The source code can be downloaded now. See the release notes for more info.

Further News >>

Related Sites

- linux-cifs.samba.org
- talloc.samba.org
- tevent.samba.org
- tdb.samba.org
- ldb.samba.org
- jcifs.samba.org
- rsync.samba.org
- ccache.samba.org
- ctdb.samba.org
- ppp.samba.org

SAMBA

THINK SAMBA
- What Is Samba?
- Latest News
- Planet Samba
- FAQ

GET SAMBA
- Download Info
- Binaries
- How To Install
- GUIs

LEARN SAMBA
- Official HOWTO
- By Example
- Using Samba
- Docs And Books
- Wiki

Samba Overview

- Samba is a free open source re-implementation of the SMB/CIFS networking protocol
- Samba runs on most Unix-like systems
- Samba provides file and print services for Windows clients
- Samba can be:
  - a Primary Domain Controller (PDC)
  - a domain member
  - part of an Active Directory domain

August 08, 2022 release 4.17.0rc1

Samba Roles

- Domain Controller
  - Primary Domain Controller (PDC)
  - Backup Domain Controller (BDC)
  - Active Directory Domain Controller
- Domain Member Server
  - Active Directory Domain Server
  - NT4 Style Domain Domain Server
- Standalone Server
- Samba security modes
  - User level security (Default Mode) *security = user*
  - Share level security **>** *security = share* **<**
  - Domain security mode *security = domain*
  - ADS security mode *security = ADS*

    realm = your.kerberos.REALM

Samba Components

Samba consists of two programs:

- **smbd** provides file and print services, handles share mode and user mode authentication and authorization
- **nmbd** provides name resolution and browsing
  Name resolution: broadcast and point-to-point
  - Clients can use either or both methods
- smbd and nmbd implement the four basic CIFS (Common Internet File System) services:
  - File and print services
  - Authentication and Authorization
  - Name resolution
  - Service announcement (browsing)

Server Configuration

- Samba configuration file: smb.conf
  - Typically in: /etc/samba
- Start with the minimal configuration
- Create a workgroup, name the server, and add a simple file share
- Many parameters - flexible and complicated
- Password issues [cleartext, encrypted]

- samba-swat GUI interface for configuring Samba
  - Will overwrite custom file – back it up first
- webmin - has Samba management component

Configuration

smb.conf has different sections:

- [global] for global server settings and default settings that may apply to the other shares
- [homes] user access to their home directories
- [printers] for printer services
- [share] for shared folders

The following may not be created by default

- [netlogon] options for logon scripts
- [profile] storage for domain logon information desktop icons, favorites

Server Configuration

[global] section

- Set environment parameters for the server
- Some basic parameters:
  - Workgroup: defines the workgroup
  - netbios name: defines host's netbios name
  - Invalid users: user level ACL *speak to the hand*
  - Hosts deny/allow: host level ACL
  - guest account: specifies guest account
- Activate the WINS server:
  - name resolve order = wins host lmhosts bcast
  - wins support = yes

Server Configuration

[global] section

- Three security levels (authentication)
  - security = user
    - per user account
  - security = share
    - legacy – considered deprecated
    - still useful in a small home network
  - security = server or domain
    - legacy – considered deprecated

Server Configuration

```
[global]
workgroup = ELEMENTS      Must match clients
netbios name= HYDROGEN
server string = %h FREE ELECTRONS
interfaces = eth0 10.0.0.2/24 255.255.255.0
bind interfaces only = Yes
security = SHARE
OS level = 255
guest account = nobody
invalid users = root
```

%h hostname - %v Samba version number

guest nobody – ACL in services section

checks against -/etc/passwd - add nobody

nobody:x:99:99:nobody:/:

Server Configuration

[share] section:

- Each shared folder needs this section
- Replace [Share] with name of the share
- Share sections parameters
  - comment: shared folder description
  - path: path to the folder to share
  - valid users: defines the list of authorized users
  - browseable: explore the shared folder
  - read only: access in read only mode.

Share Configuration

```
[Hassium]
    comment = SYS-STOR
    path = /
    writeable = yes
    browseable = yes
    guest ok = yes
    guest account = nobody
    guest only = yes
```

Note: This is not a secure example

Server Configuration

[homes] Section

- Configure sharing for user share folders
- valid users = %s   (user at home folder only)

```
[homes]
   comment = Home Directories
   valid users = %s
```

Server Configuration

[printers] Section

- Allows for shared and private printers.
- printable directive : activates the shared folder.
- Path: /var/spool/samba (printing queue path)

[print$] Section

- Shared folder containing printing drivers.
- Path: /var/lib/samba/printer, path to the drivers.

Server Configuration

```
[printers]
   comment = All Printers
   browseable = no
   path = /tmp
   printable = yes
   public = no
   writable = no
   create mode = 0700
```

Testing Configuration

- Test Samba configurations via `testparm`

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[share]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
```

Samba As Client

- Samba provides tools to add host to a Windows network as a client
- Client tools include:

smbclient connect to a server

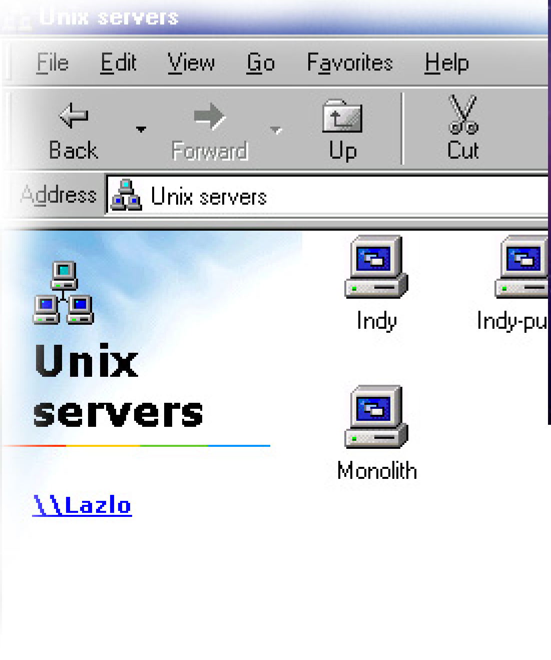
smbmount add remote shares to local file system

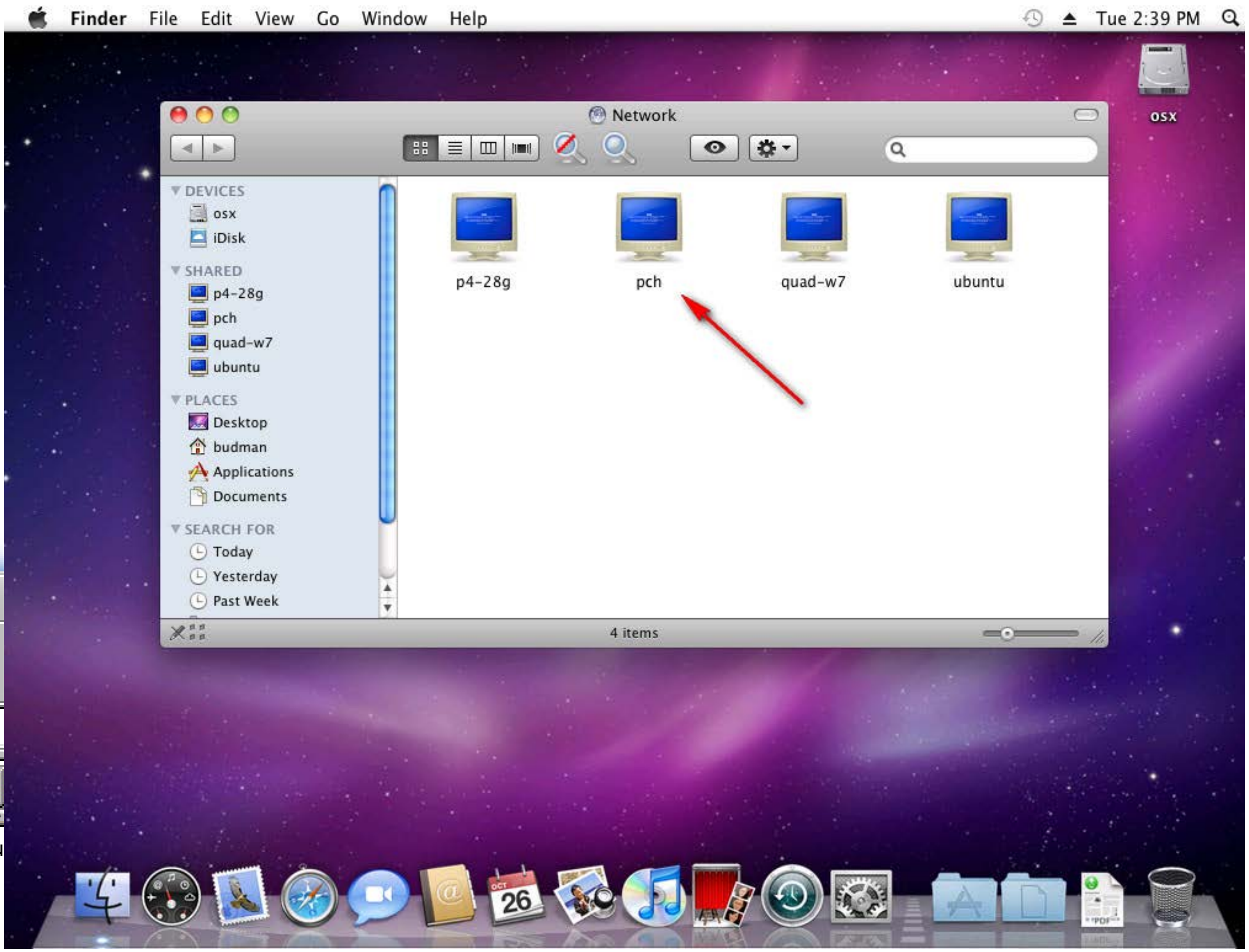
nmblookup get IP address from NetBIOS name

Why

- Free file server for SOHO
- Provide RAID reliability
- Centralize file storage for backup
- NAS alternative
- Shared media server for home
    - MP3 Music collection
    - Recorded video
- Print server (for non-networked printers)
- Authentication server

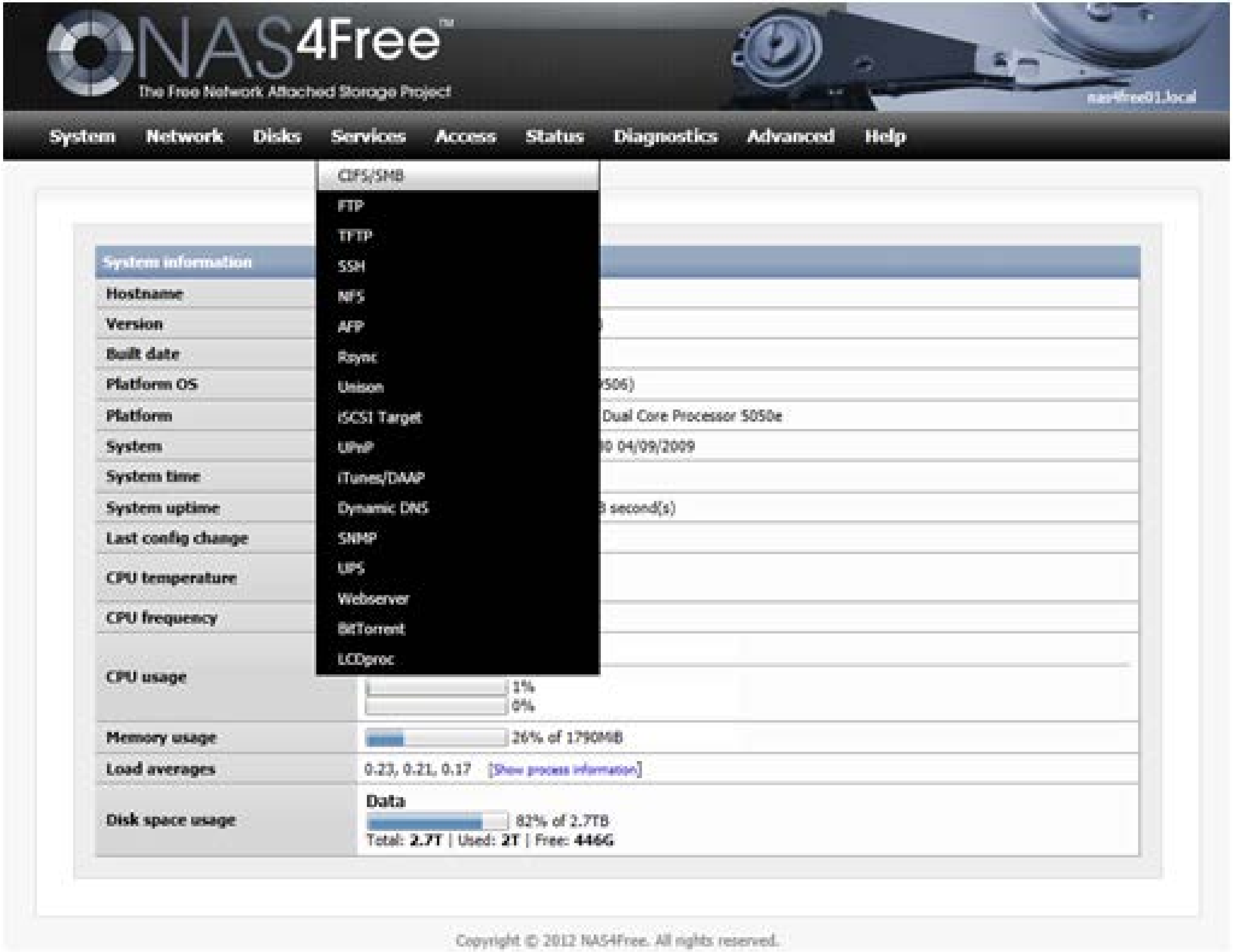
Interoperability





Network Attached Storage

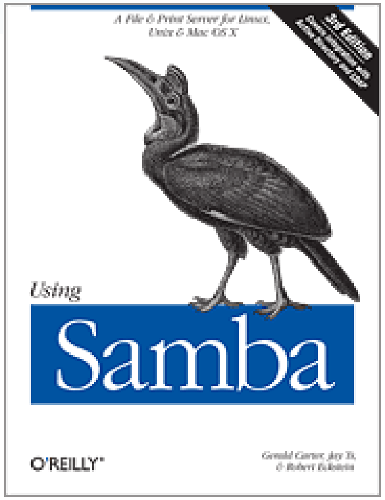
NAS



System information	
Hostname	
Version	)
Built date	
Platform OS	506)
Platform	Dual Core Processor 5050e
System	0 04/09/2009
System time	
System uptime	second(s)
Last config change	
CPU temperature	
CPU frequency	
CPU usage	1% 0%
Memory usage	26% of 1790MB
Load averages	0.23, 0.21, 0.17 [Show process information]
Disk space usage	Data 82% of 2.7TB Total: 2.7T | Used: 2T | Free: 446G

Copyright © 2012 NAS4Free. All rights reserved.

Additional References

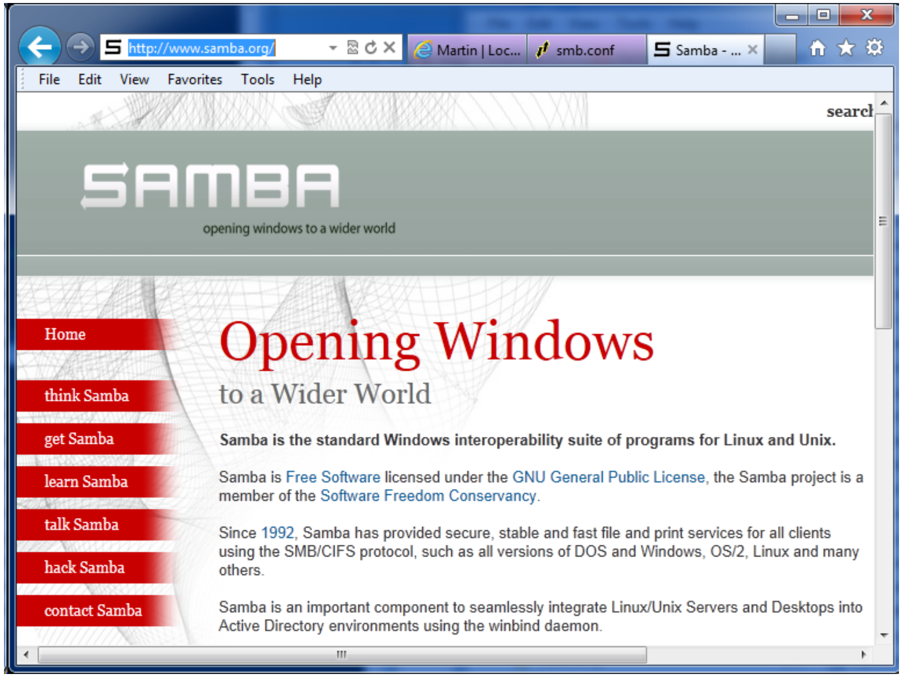

A File & Print Server for Linux, Unix & Mac OS X
Using
Samba
O'REILLY
Gerald Carter, Jay Ts, & Robert Eckstein

Using Samba 3rd Edition
Jan 2007 448 pages
O'Reilly Publishing

2nd Edition free online

http://samba.org/samba/docs/man/using_samba/toc.html

www.samba.org



Opening Windows
to a Wider World

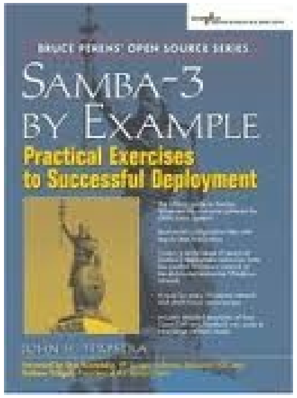
Samba is the standard Windows interoperability suite of programs for Linux and Unix.

Samba is Free Software licensed under the GNU General Public License, the Samba project is a member of the Software Freedom Conservancy.

Since 1992, Samba has provided secure, stable and fast file and print services for all clients using the SMB/CIFS protocol, such as all versions of DOS and Windows, OS/2, Linux and many others.

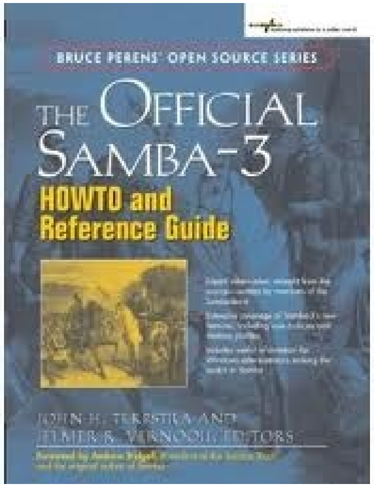
Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops into Active Directory environments using the winbind daemon.

Free Reference Manuals



- Samba-3 By Example
- 638 pages   2009
- http://www.samba.org/samba/docs/Samba3-ByExample.pdf

Combined over 1500 pages



- Samba 3.2x Howto and Reference Guide
- 964 pages 2009
- http://www.samba.org/samba/docs/Samba3-HOWTO.pdf

Samba on CentOS

Default: Installed But Not Started

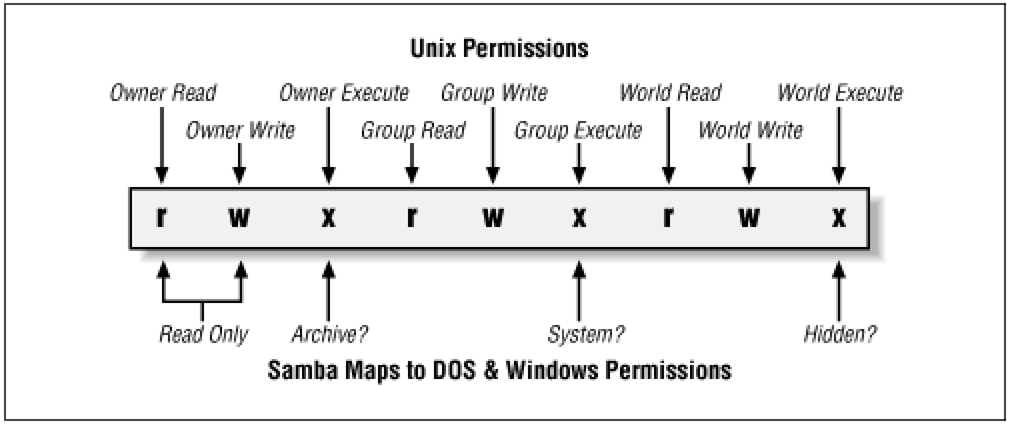
/etc/samba/

```
[root@helius samba]# ls -al
total 64
drwxr-xr-x   2 root root  4096 Sep  7 21:54 .
drwxr-xr-x 106 root root 12288 Nov  5 21:16 ..
-rw-r--r--   1 root root    20 Apr 10  2012 lmhosts
-rw-------   1 root root  4096 Sep  7 21:54 passdb.tdb
-rw-r--r--   1 root root  9733 Apr 10  2012 smb.conf
-rw-r--r--   1 root root    97 Apr 10  2012 smbusers
```

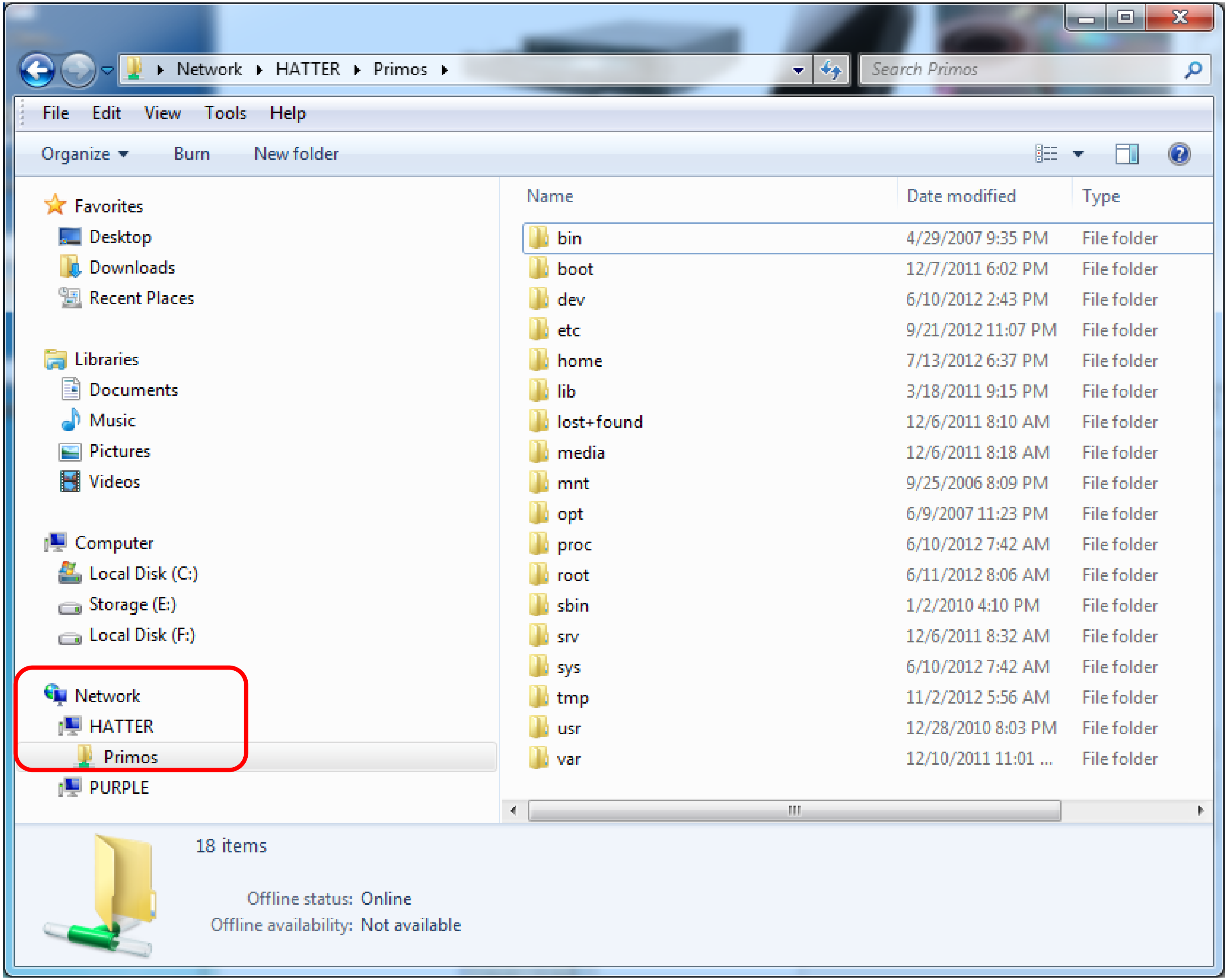
- The smb.conf file is well commented (; or #)
- Read the man page, e.g. man smb.conf 5
- Start simple, test, add complexity
- Understand what the options/changes are

Considerations

- Legacy file name compatibility (8.3)
- Windows max. length 127 chars, case sensitive
- Unix max. length 255 chars, case sensitive
- Case issues
- LFN (Long File Names)
  - Name mangling options
- File permissions and attributes differ



Linux File System



Name	Date modified	Type
bin	4/29/2007 9:35 PM	File folder
boot	12/7/2011 6:02 PM	File folder
dev	6/10/2012 2:43 PM	File folder
etc	9/21/2012 11:07 PM	File folder
home	7/13/2012 6:37 PM	File folder
lib	3/18/2011 9:15 PM	File folder
lost+found	12/6/2011 8:10 AM	File folder
media	12/6/2011 8:18 AM	File folder
mnt	9/25/2006 8:09 PM	File folder
opt	6/9/2007 11:23 PM	File folder
proc	6/10/2012 7:42 AM	File folder
root	6/11/2012 8:06 AM	File folder
sbin	1/2/2010 4:10 PM	File folder
srv	12/6/2011 8:32 AM	File folder
sys	6/10/2012 7:42 AM	File folder
tmp	11/2/2012 5:56 AM	File folder
usr	12/28/2010 8:03 PM	File folder
var	12/10/2011 11:01 ...	File folder

18 items

Offline status: Online
Offline availability: Not available

Certificate of Completion

YOUR NAME HERE

Has successfully completed the
Systems Administration and Security
Samba course module

A Signature Here

A Date Here