



Authentication Directory Auditing

Sean K. Lowder

Email: Sean@Lowder.com

CISSP / MCSE / CNE / CCNA



Brief Intro

■ Who am I?

- I've been in the IT industry for about 12 years
- Worked with authentication directories for 9 years
- Focused on Security in the enterprise for last 8 years



What are authentication directories?

- Typically designed like a folder structure (think Windows explorer)
- A Database in disguise
 - Tweaked to store user and application data
 - Easily modified to contain additional information.
- Just a useful way to store user data



What is the use of directories

- Applications can use them for storing data
 - Phone numbers
 - Email addresses
- Systems use them to verify credentials
 - Password
 - Usernames



Many types of directories

- X.400
 - Old Email systems
- X.500
 - Novell's NDS (or e-Directory)
 - Microsoft Active Directory
 - Sun Microsystems Directory One
- X.509
 - PKI (Public Key Infrastructure)



LDAP

- **Stands for Lightweight Directory Access Protocol**
 - LDAP was defined in order to encourage adoption of X.500 directories. LDAP defines a relatively simple Protocol for updating and searching directories running over TCP.
- **NOT a directory in itself**
 - This is just the method that is used to communicate with the directory
 - Yes, there is a DAP, (Directory Access Protocol)



What am I looking for?

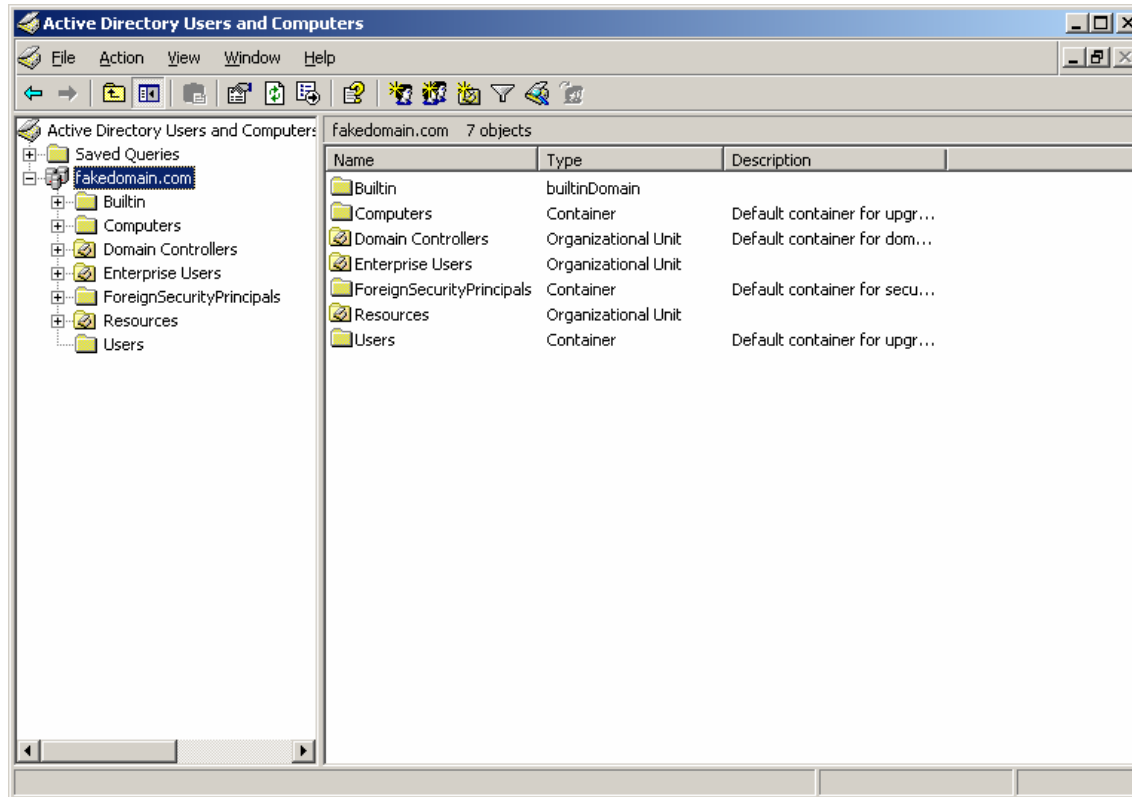
- How things are organized
 - Where are the users located?
 - Where are the groups located?
 - Where are the resources (printers and such)?
- Who has access
 - Who are your admins?
- What Groups are used



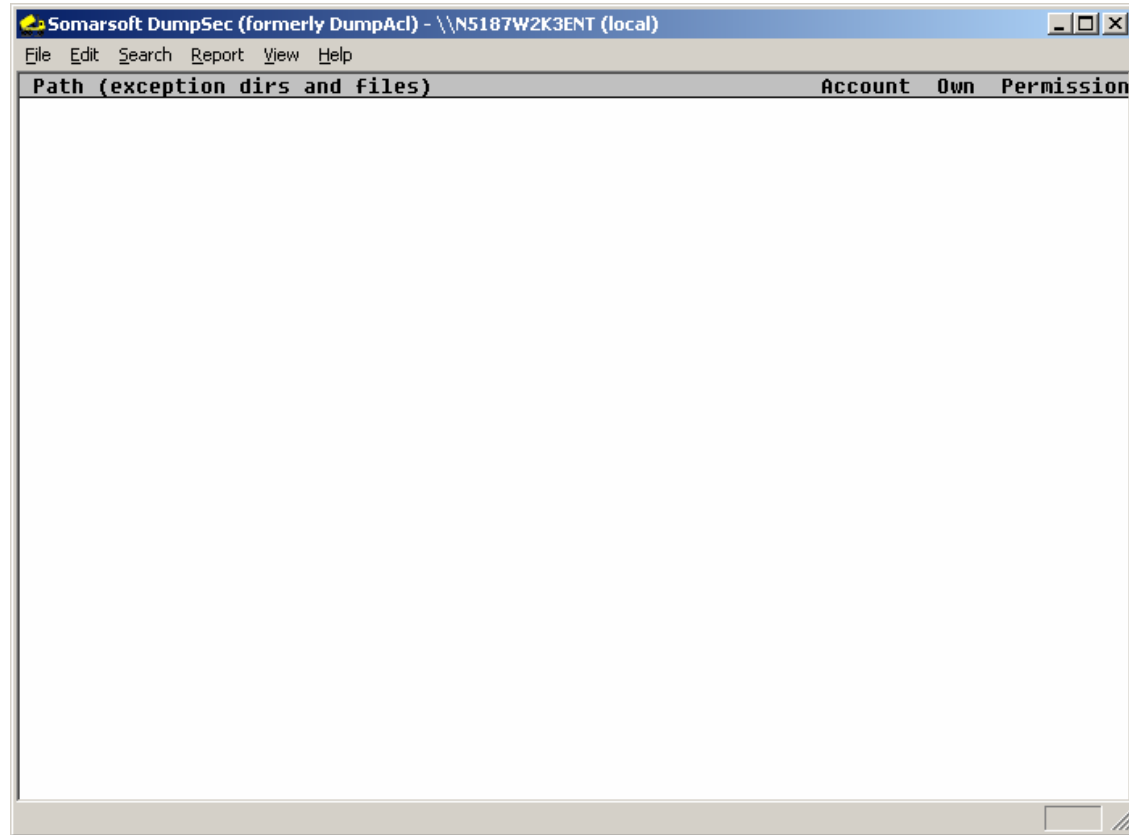
Basic tools to use

- Active Directory for Users and Computers
 - Native tool for Windows 2000 and higher servers
- System Tools DumpSec
 - (It's FREE!!!)
- Hyena
 - (It's not ☹)
- ADSI Edit
 - Another native tool

Active Directory Users and Computers



DumpSec

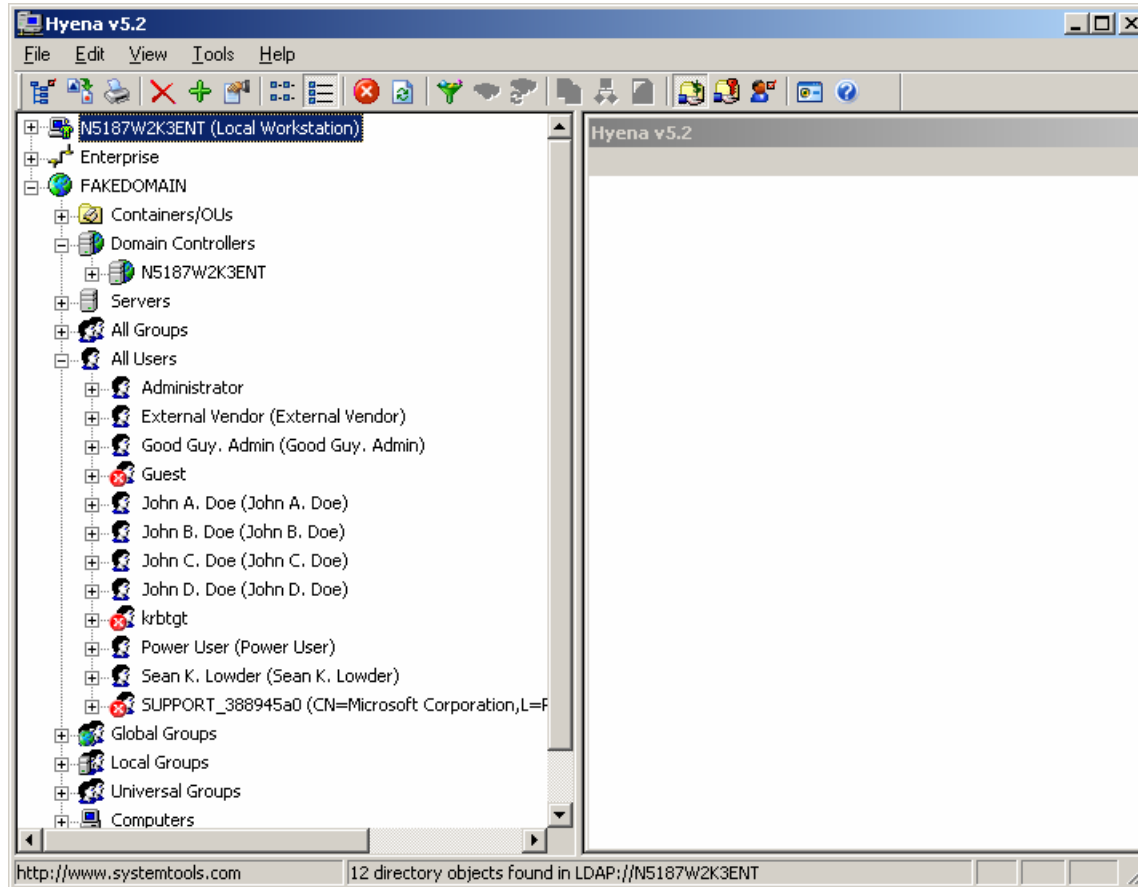


3/10/2004

Authentication Directory Tips - Sean K. Lowder ©2004

10

Hyena



3/10/2004

Authentication Directory Tips - Sean K. Lowder ©2004

11



Group Policy Objects are Your Friend

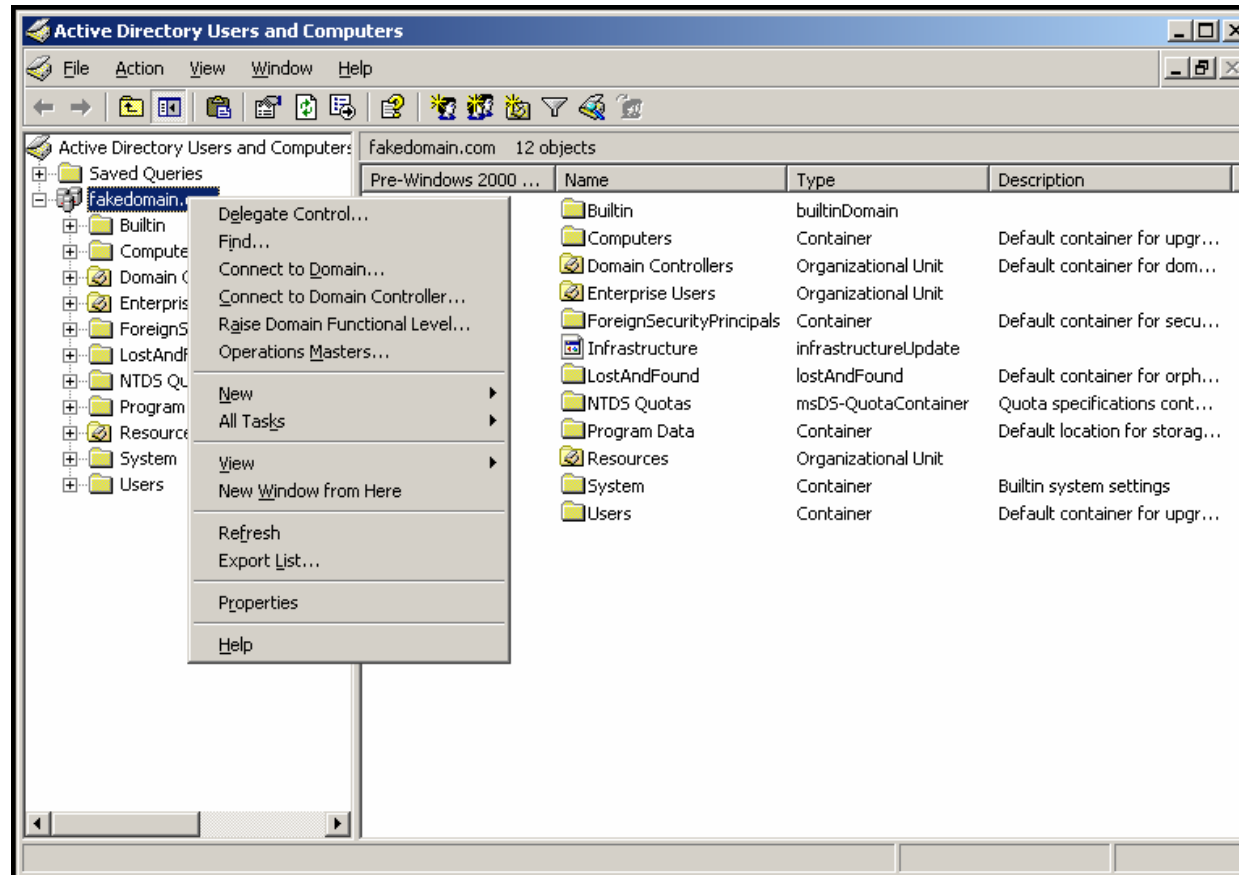
- Group Policy Objects allow for method to distribute various settings to multiple objects.
 - User objects
 - Computer objects
- The First place to check for general account and computer settings.



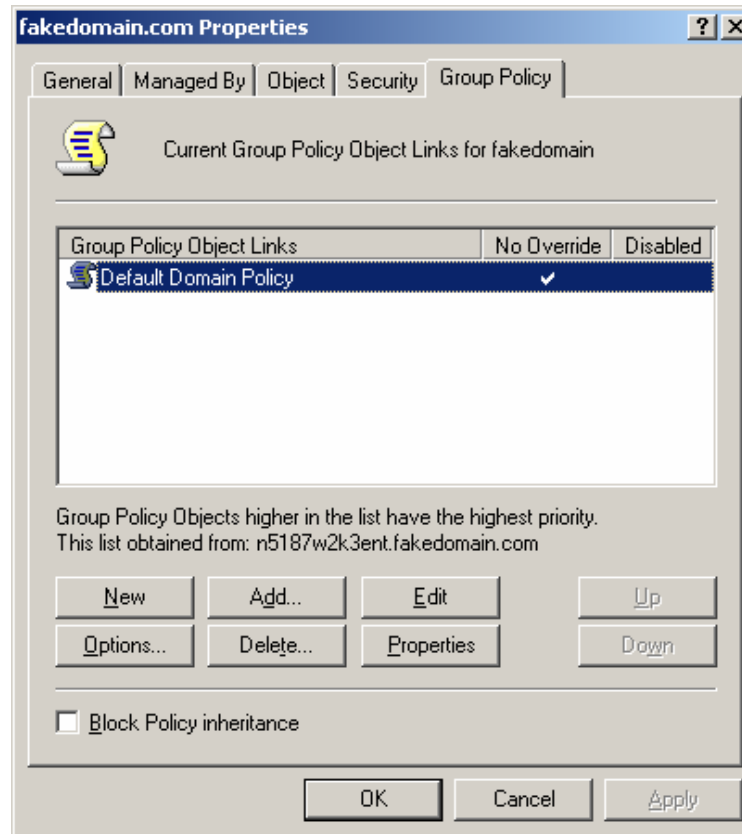
Group Policy Objects (2)

- GPO's have two pieces
 - Settings
 - What will be applied
 - Rights
 - Who (or what) will get the settings
- Both must be configured for the GPO to work correctly

AD Users and Computers

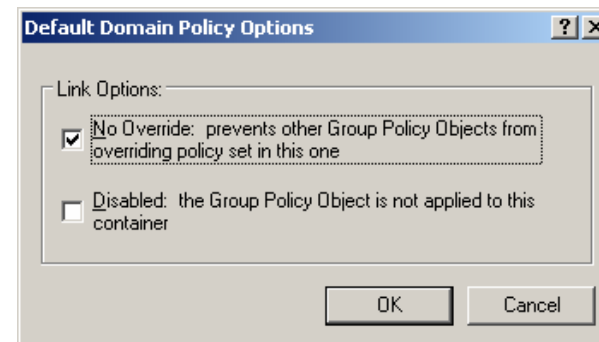


Default Domain Group Policy

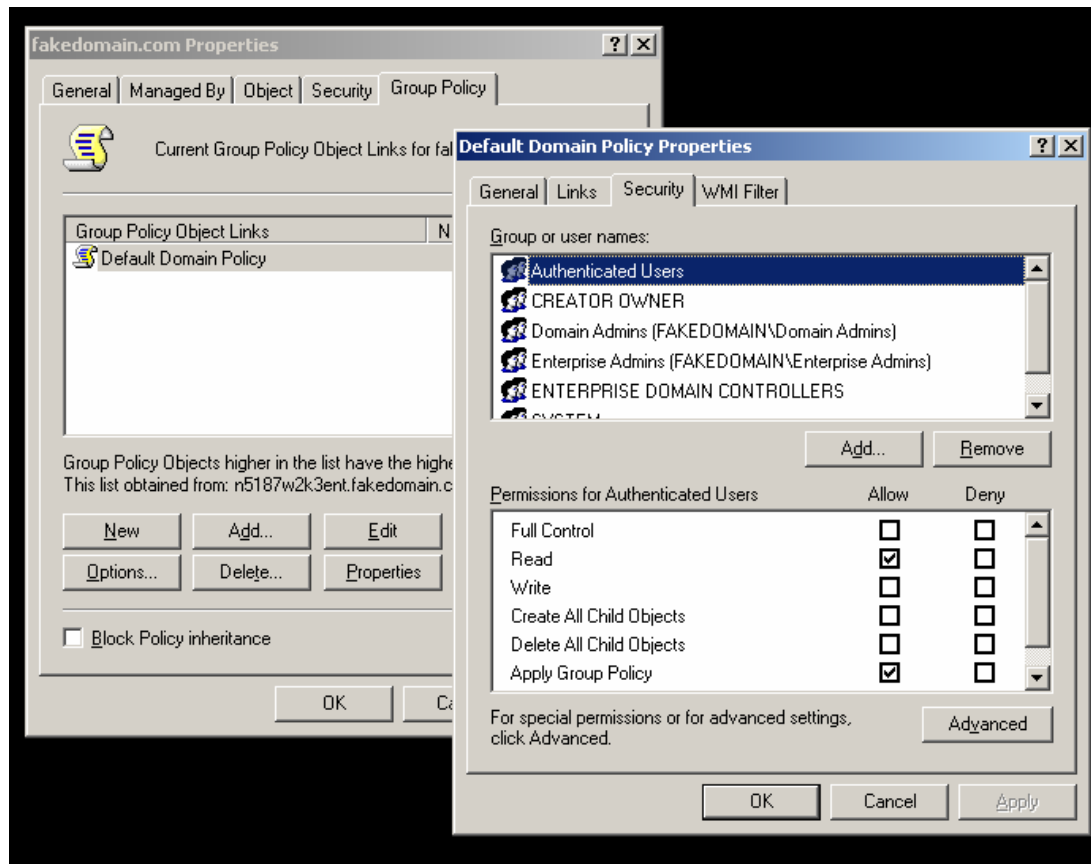


No Override options

- On all “Global” settings, ensure this is checked.
 - This ensures these settings are inherited throughout the domain
 - If this is checked the settings should be limited to mandatory configurations (e.g. password length, password age)



Default Domain Policy / Security settings

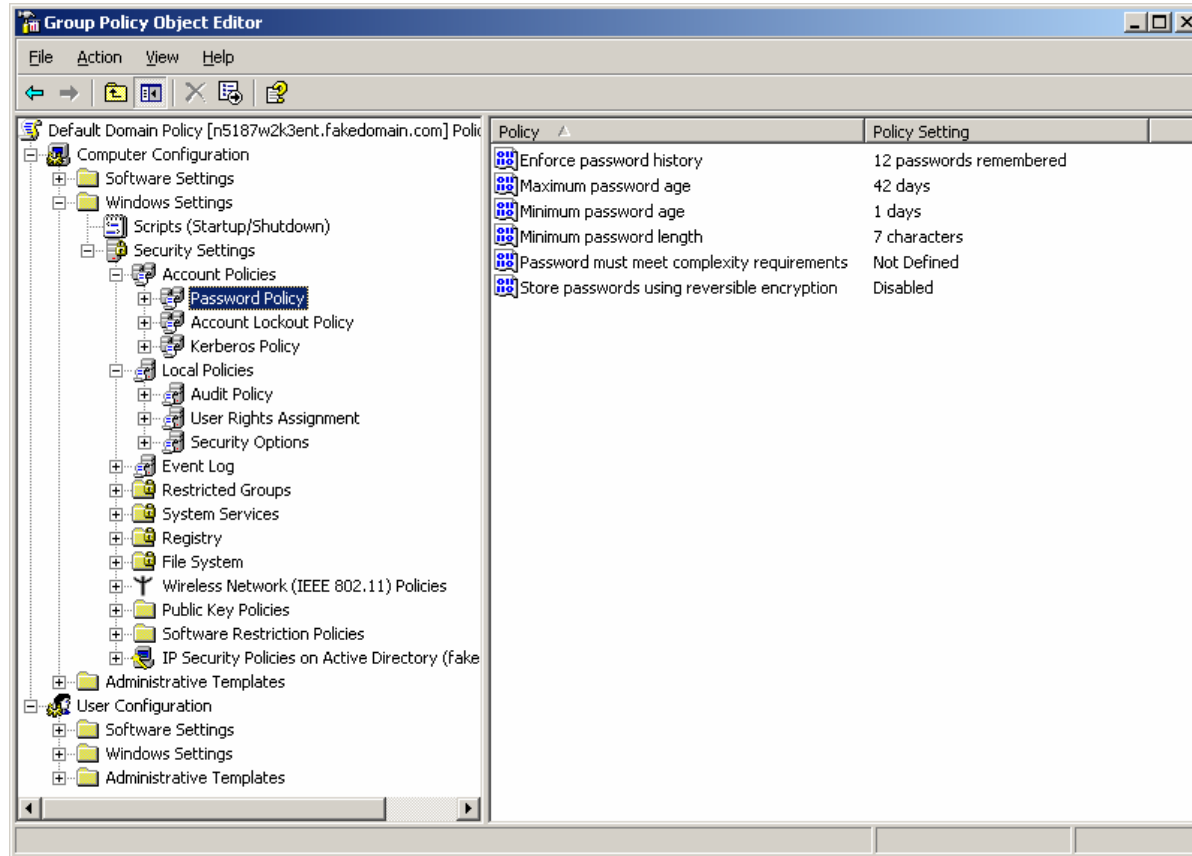




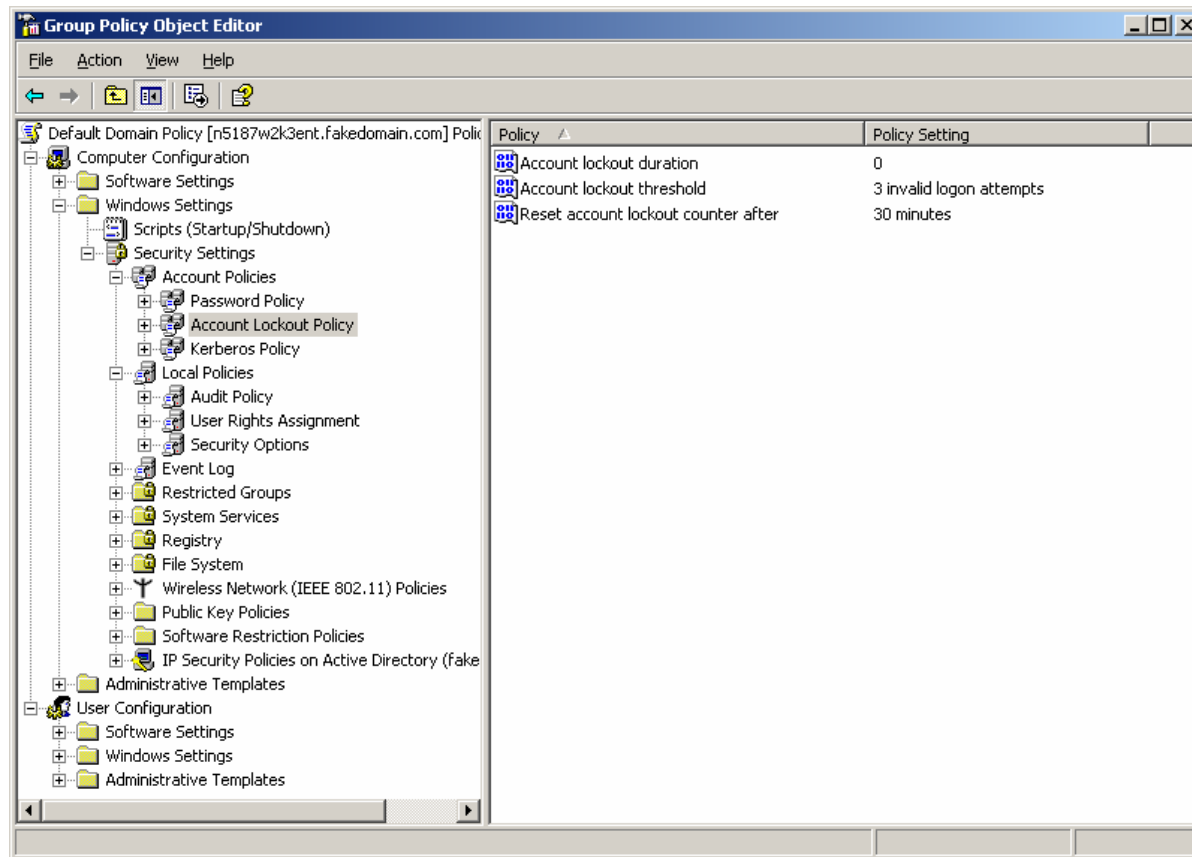
Account Policies

- Password Reset times
- Password Lengths
- Password complexity
- Change frequency
- Account lockout threshold and features

Default Domain Policy / Password settings



Default Domain Policy / Account Lockout settings





Administrative Groups

- Local Administrators Group
 - Gives total access to machine / domain by default.
- Group “Domain Admins”
 - Gives you NO rights / access by default
 - Added to the “Local Administrators Group” in all member servers and member PCs



Rogue accounts

- First and foremost, “DON’T PANIC”
- These are not that well known or used
 - The hiding technique is a carry over from a NDS “hack”
 - I’ve only seen this once in all my audits
- To implement this “Administrator” privileges are necessary.



What's the big deal?

- Island hopping
 - Think beach-head warfare
- Port redirection
 - This will get around most firewalls
- Windows environments like to share
 - Cached credentials



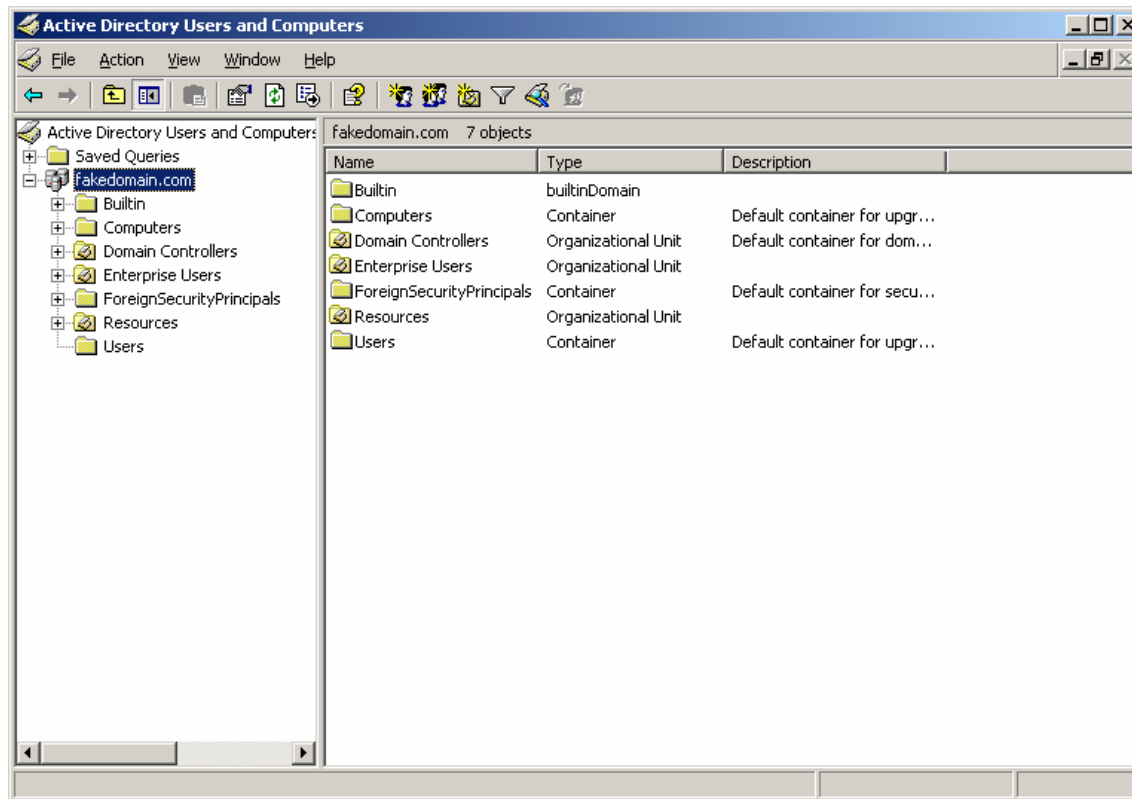
How to “Hide” accounts

- All directory entries are objects that have access control lists (ACLs).
- These ACLs can be utilized to “hide” accounts from normal users or even ADMIN users.

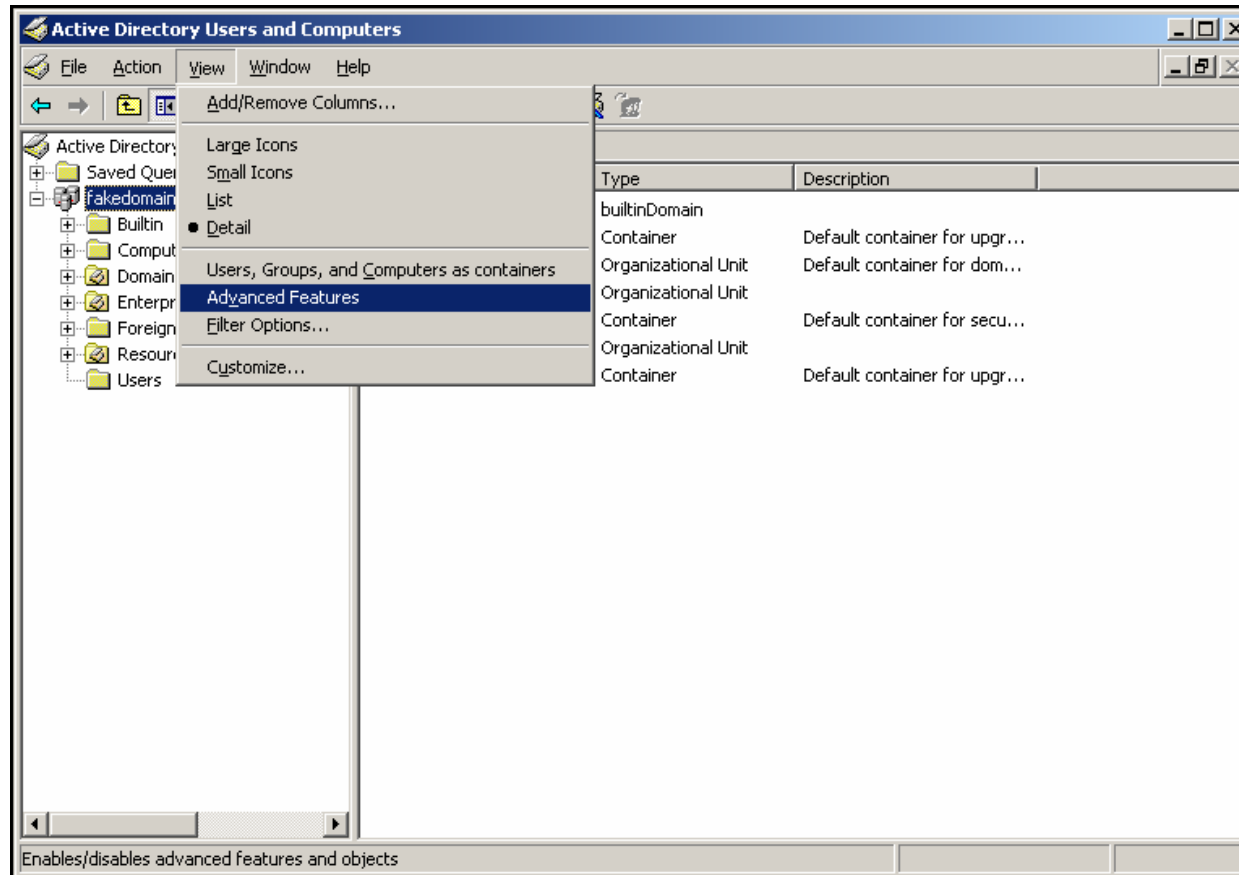
Demo

- First thing...a WARNING
 - It is VERY easy to make modifications to your directories that will render it unusable.
 - Use the “Two-sets” of eyes principle when doing the following type of directory review.
- Next thing...this is fairly advanced hiding to demonstrate the concept. There are other ways as well. ☹

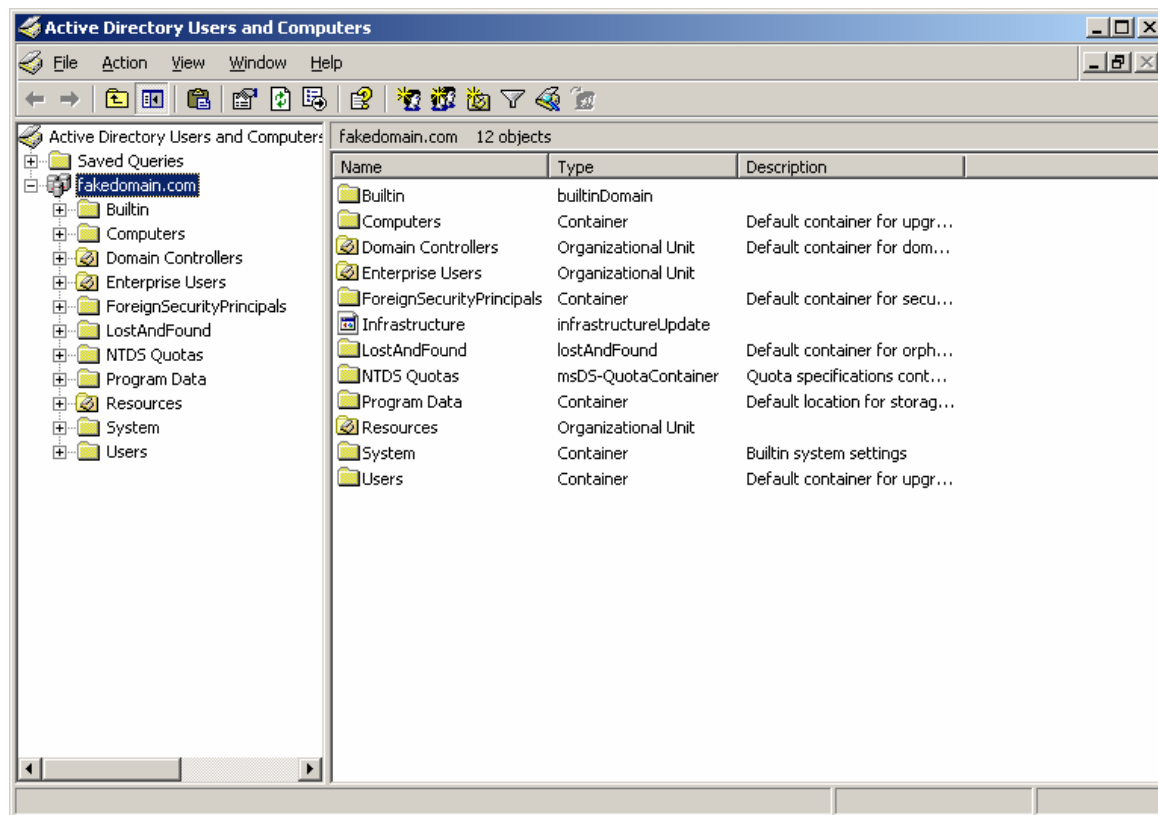
Active Directory Users and Computers (default view)



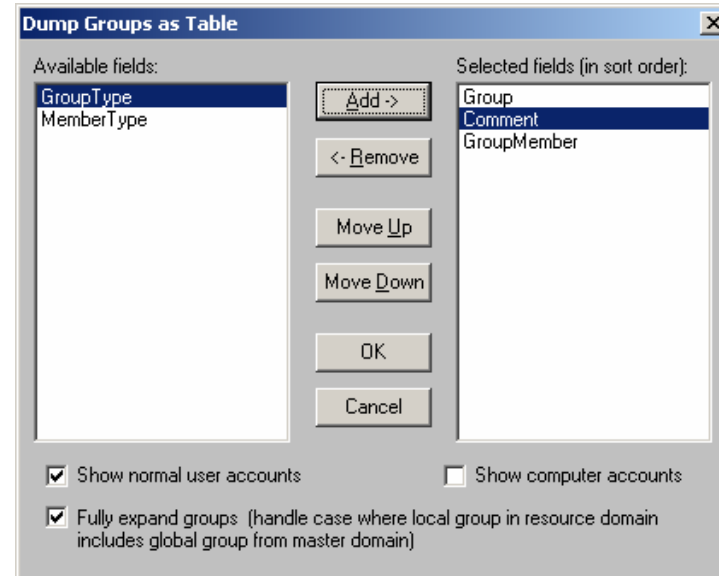
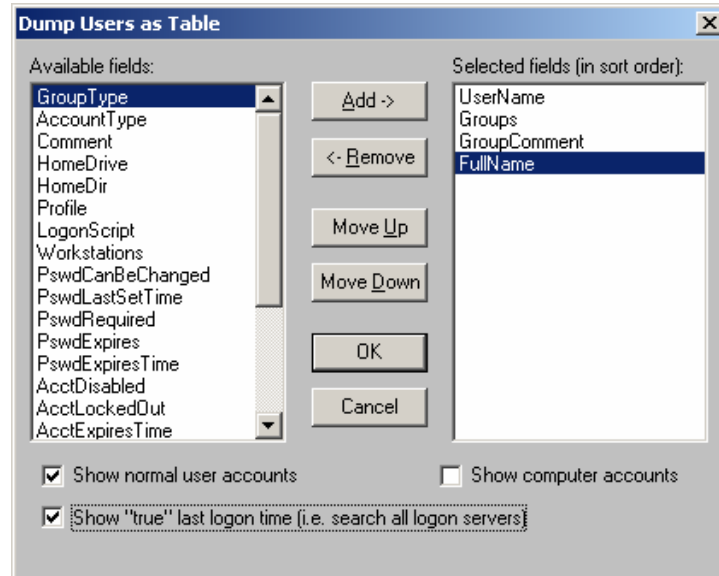
Active Directory Users and Computers



Active Directory Users and Computers (Advanced view)



DumpSec Users & Groups



Differences from DumpSec report

UserName	Groups	GroupComment
Administrator	Administrators	Administrators have complete and unrestr
Administrator	Domain Admins	Designated administrators of the domain
Administrator	Domain Users	All domain users
Administrator	Enterprise Admins	Designated administrators of the enterpr
Administrator	Group Policy Creator Owners	Members in this group can modify group p
Administrator	Schema Admins	Designated administrators of the schema
BADDude	Administrators	Administrators have complete and unrestr
BADDude	Domain Users	All domain users
ExtVendor	Domain Users	All domain users
GoodAdmin	Domain Admins	Designated administrators of the domain
GoodAdmin	Domain Users	All domain users
Guest	Domain Guests	All domain guests
Guest	Guests	Guests have the same access as members o
JDoeA	Domain Users	All domain users
JDoeB	Domain Users	All domain users
JDoeC	Domain Users	All domain users
JDoeD	Domain Users	All domain users
krbtgt	Domain Users	All domain users
PowerU	Domain Users	All domain users
SLOWder	Administrators	Administrators have complete and unrestr
SLOWder	Domain Admins	Designated administrators of the domain
SLOWder	Domain Users	All domain users
SUPPORT_388945a0	Domain Users	All domain users
SUPPORT_388945a0	HelpServicesGroup	Group for the Help and Support Center

Found 13 users

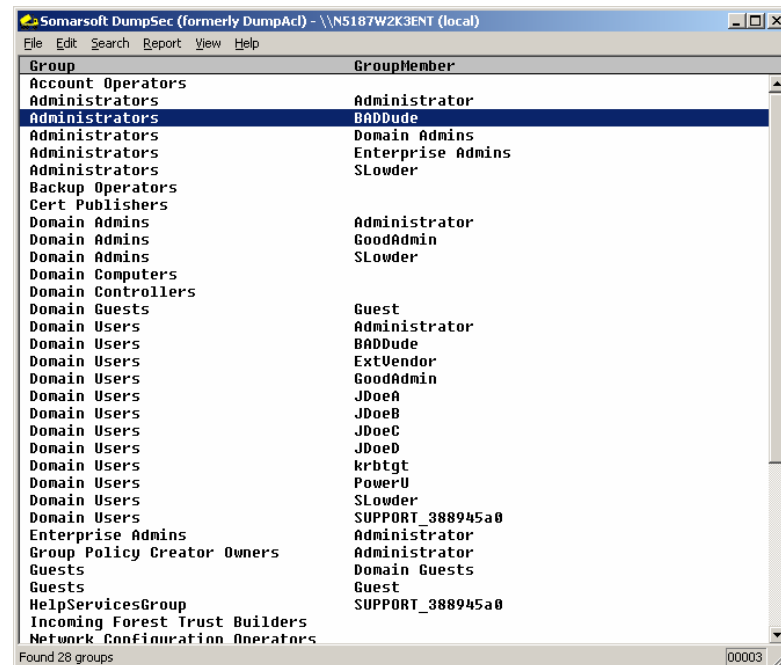
UserName	FullName	AccountType
Administrator		User
ExtVendor	External Vendor	User
GoodAdmin	Good Guy. Admin	User
Guest		User
JDoeA	John A. Doe	User
JDoeB	John B. Doe	User
JDoeC	John C. Doe	User
JDoeD	John D. Doe	User
krbtgt		User
PowerU	Power User	User
SLOWder	Sean K. Lowder	User
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	User

Found 12 users

- Report on left run with Admin privileges, report on right run with GoodAdmin privileges, note number of users
- Any problem here???

One place to look

- Remember, Groups are objects too!!!
- Just because you don't have access to the ID, you MIGHT have access to the group.
- Report on right run as GoodAdmin ID.



Somarsoft DumpSec (formerly DumpAcl) - \\NS187W2K3ENT (local)

Group	GroupMember
Account Operators	
Administrators	Administrator
Administrators	BADDude
Administrators	Domain Admins
Administrators	Enterprise Admins
Administrators	SLowder
Backup Operators	
Cert Publishers	
Domain Admins	Administrator
Domain Admins	GoodAdmin
Domain Admins	SLowder
Domain Computers	
Domain Controllers	
Domain Guests	Guest
Domain Users	Administrator
Domain Users	BADDude
Domain Users	ExtVendor
Domain Users	GoodAdmin
Domain Users	JDoeA
Domain Users	JDoeB
Domain Users	JDoeC
Domain Users	JDoeD
Domain Users	krbtgt
Domain Users	PowerU
Domain Users	SLowder
Domain Users	SUPPORT_388945a0
Enterprise Admins	Administrator
Group Policy Creator Owners	Administrator
Guests	Domain Guests
Guests	Guest
HelpServicesGroup	SUPPORT_388945a0
Incoming Forest Trust Builders	
Network Configuration Operators	

Found 28 groups 00003



Other places to look

- Member servers and workstations
 - Check the group membership on these as well.
- Remember, if it JDLR (just doesn't look right), there is probably something there.



Questions???

Email: Sean@Lowder.com

References and Additional Resources

- Hacking Exposed Network Security Secrets & Solutions Forth Edition
 - Stuart McClure, Joel Scambray and George Kurtz
 - McGraw Hill / Osborne Publishers
 - ISBN 0-07-222742-7
- Hacking Exposed Windows Server 2003
 - Stuart McClure, Joel Scambray
 - McGraw Hill / Osborne Publishers
 - ISBN 0-07-223061-4
- Windows 2000 Active Directory Survival Guide
 - Richard Schwartz
 - John Wiley & Sons, Inc. Publishers
 - ISBN 0-471-35600-X
- Windows 2000 Administration
 - George Spalding
 - McGraw Hill / Osborne Publishers
 - ISBN 0-07-882582-2
- Hyena and DumpSec available at www.systemtools.com
- <http://dret.net/glossary> (look up X.400, X.500, X.509, LDAP)