INFO-6003

# O/S & Application Security

Week 05

# Agenda

- Test Details
- Group Policy
- Primary Security Policy Settings
- NTFS

# Test 01 - Details

# Test 01

- Week-06
  - Date Feb 10  Rm R1020
  - Regular class start time
- Content
  - Lectures & Labs from Weeks 1-5

# Test 01

- FOL via Respondus LockDown Browser
- You will be able to move forward and backward through the test questions
- The in class students will have 60 minutes to write the test
  - If you need to reboot, you need to let me know, otherwise I will sign you out at 60

# Test 01

- No communication is allowed during the test period
  - As soon as I give you the password to access the test there will be no further communication allowed
- Any form of communication during the test will result in a zero
  - You will be asked to submit your test and leave the room

# What to Bring to the Test

- Your Laptop with the current version of Respondus LockDown Browser
- Network Cable
- Student Card
  - You need to have this on you desk while writing the test
- Nothing else is allowed on the desk
  - No phones, notes, etc.

# Test Topics & Format

- Topics
  - Anything from weeks 1 to 5
  - Includes both lectures, text book and labs
- Format
  - Multiple Choice, True False, Matching
    - Around 80%
    - Covers the more factual information
      - How do you force the update of group policy
  - Long Answer
    - Around 20%
    - Covers the larger concepts
      - Why do we use group policy objects

# Group Policy

# Group Policy

- Group policy has been a feature of Windows Networks and OS's since the Windows NT days
- Group Policy is a set of rules allowing administrators the ability to control computer configuration and the behavior of a user's working environment
- Key method for deploying security configurations across a Windows Network
- At the Domain level, allows administrators to centrally manage the configuration settings for computers, users, groups, etc.

# Group Policy Vs. Registry Edits

- The Registry is the central configuration database for the Windows operating system
  - Not user friendly and Dangerous to Edit directly
- Group Policy is used as a front end tool to edit the Registry
- Hundreds of settings can be configured through Group Policy
  - These settings are then applied to the registry

# Registry Edits

- Regular users should not have permissions to change the registry settings
- There are tools available for attackers to alter the registry locally or remotely
- Typically used by attackers to mask Malware or set certain malicious scripts to run on system boot up

# Challenges

- Hardening the operating system requires knowledge of the current default security settings and the options that can be set to increase security
- For Example:
  - Security includes the protection of user data files and system files
  - Many settings in group policy control access to configuration options
  - An inexperienced administrator could make configuration errors that allow unauthorized access to, or deletion of, important files

# Access Restriction

- Group Policy can be used to control or restrict account activities
  - Restrict access to Task Manager
  - Restrict access to Control Panel
  - Restrict the downloading of executable files
  - Control sharing of folders
  - Control access to installed programs
- There are many more involved

# Types of Group Polices

- 2 Main Types
- Local
  - A policy that exists on, and is applied to, a single pc
- Domain
  - A policy that exists on Domain Controllers and can be applied to objects in the domain

- Note on Terminology: Generally when we refer to a "Group Policy" we are talking about the domain type

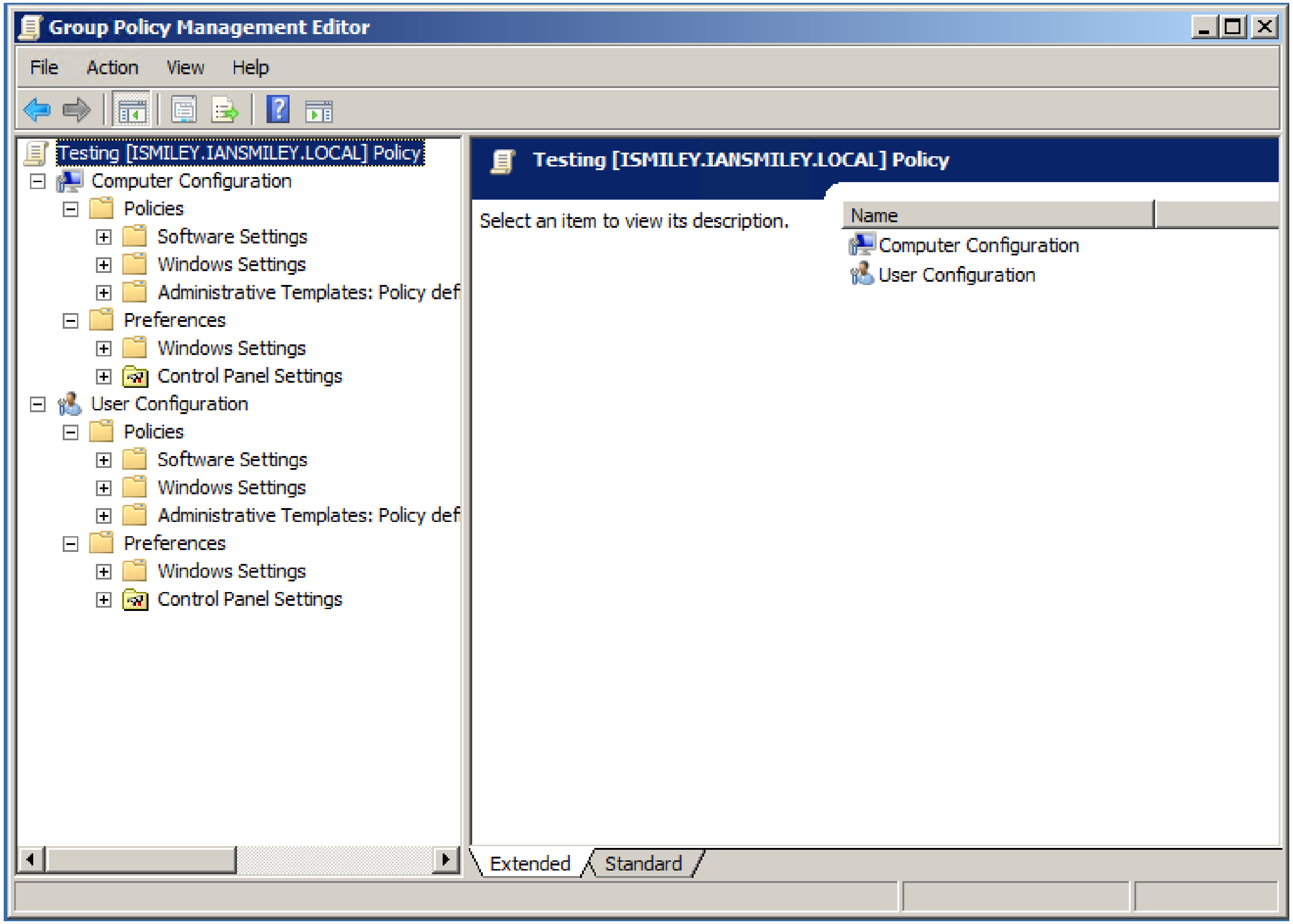
# Two Main Areas of Control

- Policies apply to two main areas
  - Computer Configuration
  - User Configuration
- Each area has two main sub-areas
  - Policies
  - Preferences

# Divisions

- Under Policies there are:
  - Software Settings
  - Windows Settings
  - Administrative Templates
- Under Preferences there are:
  - Windows Settings
  - Control Panel Settings

# Divisions



- Testing [ISMILEY.IANSMILEY.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy def
    - Preferences
      - Windows Settings
      - Control Panel Settings
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy def
    - Preferences
      - Windows Settings
      - Control Panel Settings

Testing [ISMILEY.IANSMILEY.LOCAL] Policy

Select an item to view its description.

| Name |
|---|
| Computer Configuration |
| User Configuration |

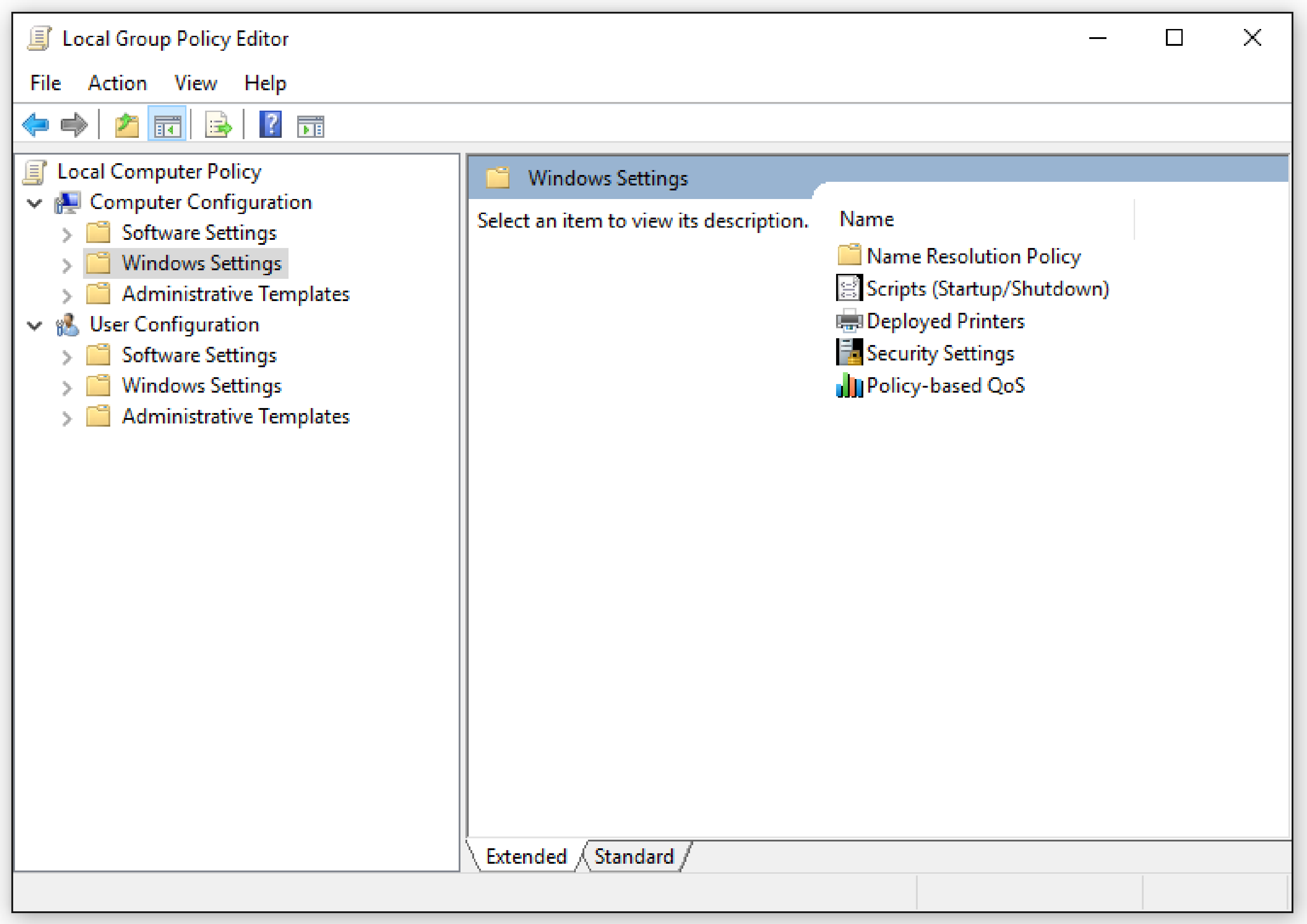
# Local Group Policy

- In the past, Local Group Policy could only be applied to the computer, not individual accounts
  - Limited users & administrators got the same policy
  - Was applied to the HKLM registry hive
- In current systems you can have multiple Local Group Policies
  - Computer in HKLM
  - Administrators in HKCU
  - Non-Administrators in HKCU
  - Individual Users in HKCU

# Local Group Policy

- Processing order
  - Local Computer Group Policy
  - Administrator or Non-Administrator Group policy
  - Per-User Group Policy
- Since the Per-User Group Policy is read last it will take precedence over the other settings
  - Last writer wins

# Local Group Policy in Windows 10 Pro



Local Group Policy Editor

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Windows Settings

Select an item to view its description.

| Name |
|---|
| Name Resolution Policy |
| Scripts (Startup/Shutdown) |
| Deployed Printers |
| Security Settings |
| Policy-based QoS |

# Active Directory Group Policy

- Active Directory Group Policy can “link” to
  - Sites
  - Domains
    - We linked our WSUS GPO at this level
  - OUs (Organizational Units)
- Active Directory Group Policy can “apply” to Objects, such as:
  - Computers
    - Our WSUS GPO applied to our W7 VM
  - Users
  - Groups

# Domain Group Policy Processing Order

- Local GPO
  - Computer based GPO
  - Least Influential
- Site GPOs
  - Order of GPOs can be specified
- Domain GPOs
  - Order of GPOs can be specified
- OU GPOs
  - GPOs are processed from top OU to bottom OU
  - Order of multiple GPOs can be specified

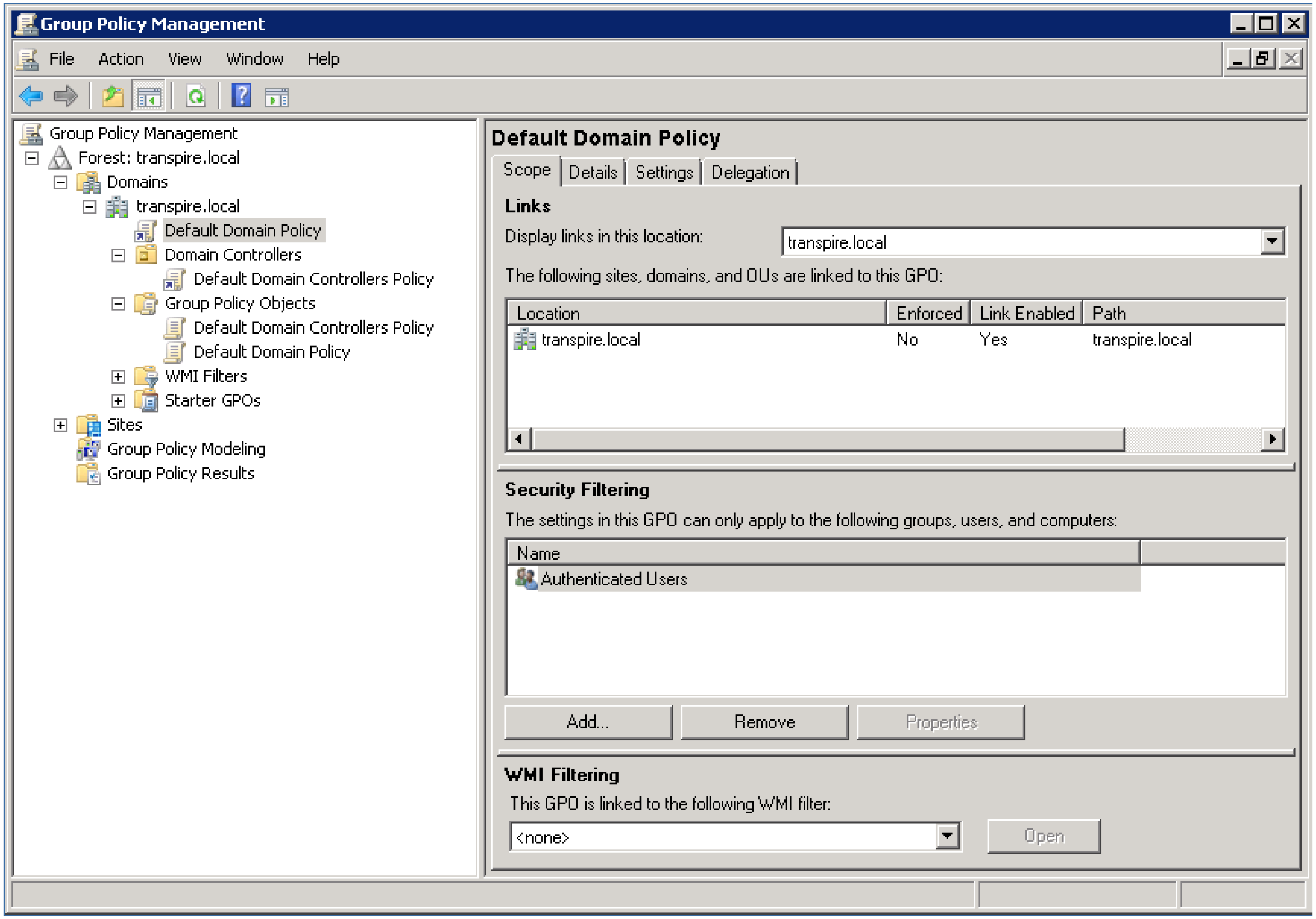
# Exceptions to Processing Order

- An AD container can be set to **Block Policy Inheritance**
  - GPOs from above will not apply
- An AD GPO can be set to **No Override**
  - Cannot be overwritten by GPOs that are below
  - No Override GPOs CANNOT be blocked
- GPOs can also be disabled or unlinked
  - Unlinking a GPO does not delete it!

# GPO Permissions

- GPO’s have permissions (Delegations)
- For a GPO to apply, Users/Groups must have Read permissions for the GPO
- Users/Groups are set in GPMC under Scope, Security Filtering
- Permissions are changed from the Delegation tab

# GPO Permissions



Default Domain Policy

Links

Display links in this location: transpire.local

The following sites, domains, and OUs are linked to this GPO:

| Location | Enforced | Link Enabled | Path |
|---|---|---|---|
| transpire.local | No | Yes | transpire.local |

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

| Name |
|---|
| Authenticated Users |

WMI Filtering

This GPO is linked to the following WMI filter: <none>

# Domain Client Application

- With Active Directory, GPOs can be pushed out to computers automatically from Domain Controllers
  - The policies refresh every 90min by Default
    - 0-30 minute random offset interval so all systems are not processing policies at the same time
  - When a computer boots up and connects to the Domain controller the computer configuration settings from the GPO are downloaded
  - When a user logs on the user configuration GPO settings are downloaded
  - Both can be forced with **gpupdate /force**

# Domain Client Application

- The client computer will poll the domain controller for the current version number of the GPO for that computer and user
- If the version number is unchanged there is no need to reapply the settings
- If the client can’t connect to the domain controller at the 90 min interval the timer is reset for the next 90 min
- Client downloads when it finally connects to the domain

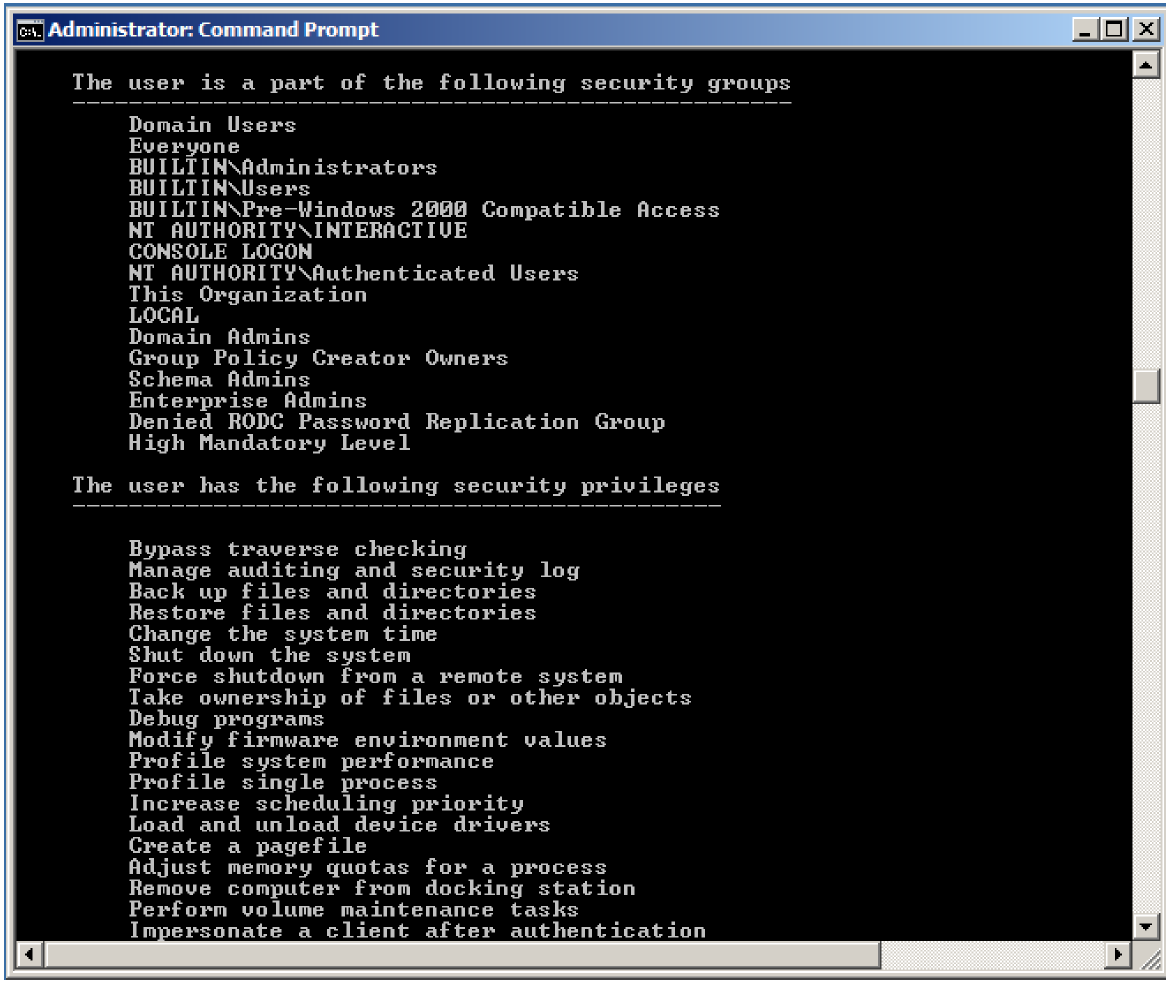
# Group Policy Tools

- Local Group Policies can be accessed through a Microsoft Management Console (MMC) snap-in
  - Group Policy Object Editor snap-in
  - MS does not provide a built in shortcut for this.
- When adding the snap-in, the author is prompted for which computer to add.
  - Secondary Users tab allows selection of Administrators, Non-Administrators, or users
  - You can control what can be edited with the Edit Extensions option

# Group Policy Tools

- Group Policies in Active Directory are managed with the Group Policy Management Console
  - Built in since Server 2008
- gpresult.exe will give a text based output of the current GPO settings
  - gpresult.exe /z will give a more verbose output
- The utility rsop.msc will start a user friendly GUI similar to the MMC snap-in or GPMC
  - The tree will show the policy settings that have been applied
  - Resultant Set Of Policy

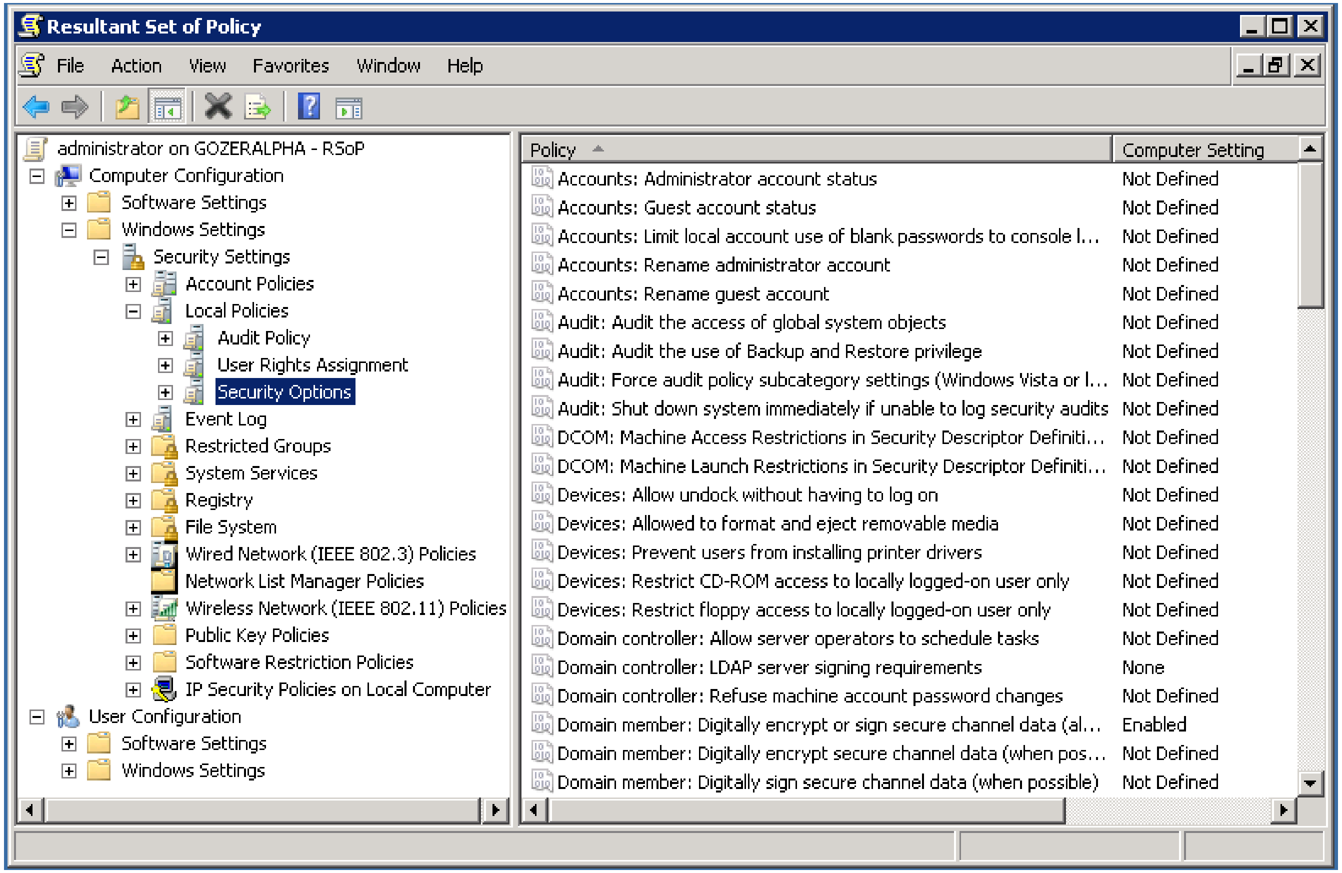
# Partial Output of gpresult /z



```
    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        BUILTIN\Pre-Windows 2000 Compatible Access
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Domain Admins
        Group Policy Creator Owners
        Schema Admins
        Enterprise Admins
        Denied RODC Password Replication Group
        High Mandatory Level

    The user has the following security privileges
    ----------------------------------------------

        Bypass traverse checking
        Manage auditing and security log
        Back up files and directories
        Restore files and directories
        Change the system time
        Shut down the system
        Force shutdown from a remote system
        Take ownership of files or other objects
        Debug programs
        Modify firmware environment values
        Profile system performance
        Profile single process
        Increase scheduling priority
        Load and unload device drivers
        Create a pagefile
        Adjust memory quotas for a process
        Remove computer from docking station
        Perform volume maintenance tasks
        Impersonate a client after authentication
```

# rsop.msc

- Security settings and how they are assigned (Win2k8 R2)



- administrator on GOZERALPHA - RSoP
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - IP Security Policies on Local Computer
  - User Configuration
    - Software Settings
    - Windows Settings

| Policy | Computer Setting |
|---|---|
| Accounts: Administrator account status | Not Defined |
| Accounts: Guest account status | Not Defined |
| Accounts: Limit local account use of blank passwords to console l... | Not Defined |
| Accounts: Rename administrator account | Not Defined |
| Accounts: Rename guest account | Not Defined |
| Audit: Audit the access of global system objects | Not Defined |
| Audit: Audit the use of Backup and Restore privilege | Not Defined |
| Audit: Force audit policy subcategory settings (Windows Vista or l... | Not Defined |
| Audit: Shut down system immediately if unable to log security audits | Not Defined |
| DCOM: Machine Access Restrictions in Security Descriptor Definiti... | Not Defined |
| DCOM: Machine Launch Restrictions in Security Descriptor Definiti... | Not Defined |
| Devices: Allow undock without having to log on | Not Defined |
| Devices: Allowed to format and eject removable media | Not Defined |
| Devices: Prevent users from installing printer drivers | Not Defined |
| Devices: Restrict CD-ROM access to locally logged-on user only | Not Defined |
| Devices: Restrict floppy access to locally logged-on user only | Not Defined |
| Domain controller: Allow server operators to schedule tasks | Not Defined |
| Domain controller: LDAP server signing requirements | None |
| Domain controller: Refuse machine account password changes | Not Defined |
| Domain member: Digitally encrypt or sign secure channel data (al... | Enabled |
| Domain member: Digitally encrypt secure channel data (when pos... | Not Defined |
| Domain member: Digitally sign secure channel data (when possible) | Not Defined |

# Security Scripts

- Both Computer and User Scripts are found under Windows Settings
- Computer Scripts run at start up and/or shutdown
- User Scripts run at logon and/or logoff
- Can be used to schedule special repetitive tasks

# Security Scripts

- Scripts can be:
  - Batch files
  - Visual Basic
  - JavaScript
  - Interpreters available for scripts written in Perl & Python
  - PowerShell Scripts are also supported in current versions
    - Script Processing Order can be controlled

# Security Scripts

- Can also be used by attackers to automatically run on start up and launch Trojans, etc.
- Malware may launch when user reboots the system and listen to command server on a predetermined port number for incoming instructions

# Group Policy Summary

- Group Policy is the main tool to set security or environment settings for almost every part of Windows and Windows Networks
- Allows us to take centralized measures to:
  - Restrict Access
  - Remove or Disable unused Services
  - Control Updates through Policy, such as WSUS GPO we set up
- Note: you should recognize that these match up with the steps to harden an OS

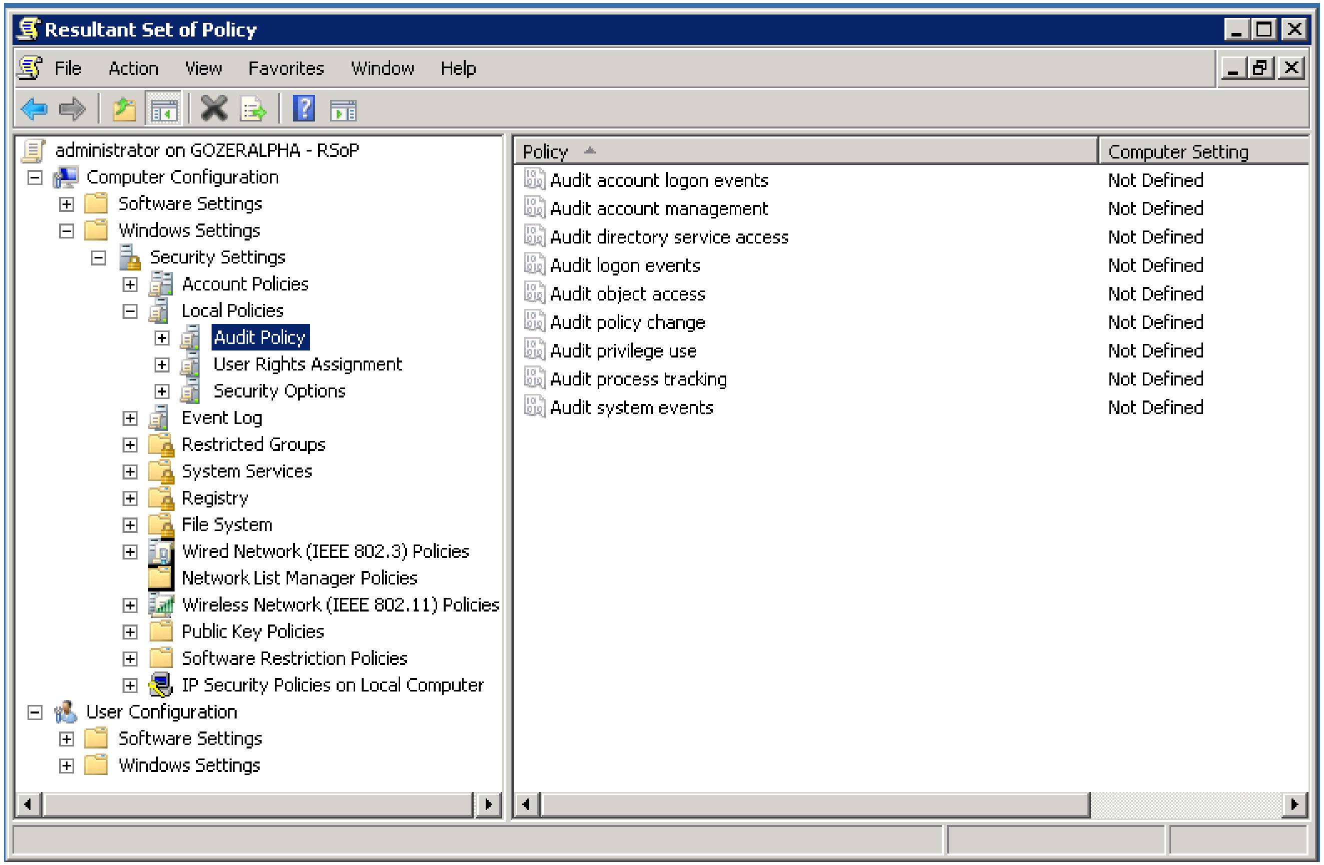
# Specific Security Settings

# Audit Policy

- The Audit Policy section has options to log events
  - Changes to User accounts
  - Changes to User rights & privileges
  - Access to objects
  - Logon attempts
- By default audit items are disabled
  - Hacking activities such as password guessing attacks or creation of new user accounts can be detected by logging

# Audit Policy

- The Audit Policy section in Win2k8_R2



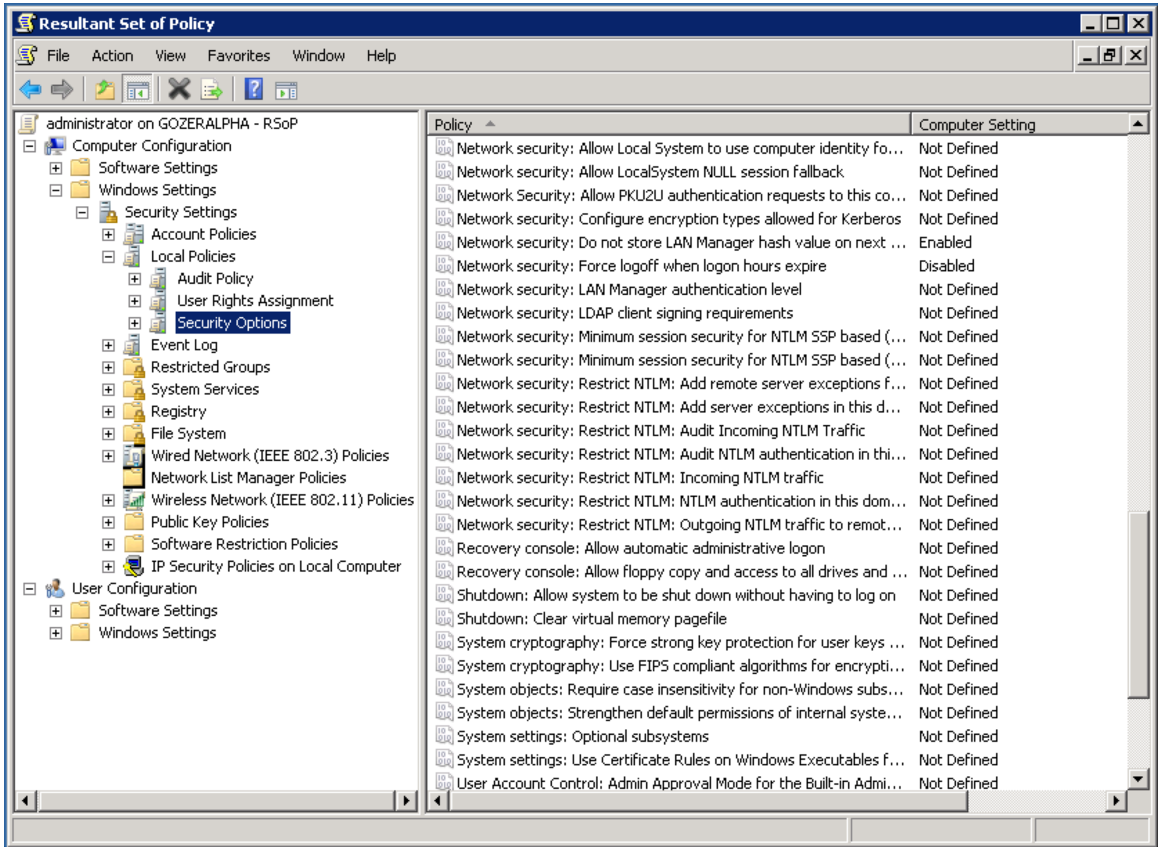
| Policy | Computer Setting |
|---|---|
| Audit account logon events | Not Defined |
| Audit account management | Not Defined |
| Audit directory service access | Not Defined |
| Audit logon events | Not Defined |
| Audit object access | Not Defined |
| Audit policy change | Not Defined |
| Audit privilege use | Not Defined |
| Audit process tracking | Not Defined |
| Audit system events | Not Defined |

# Security Options

- The Administrator & Guest accounts cannot be deleted
- To prevent hackers from gaining access through these accounts they can be disabled
- The accounts can also be renamed
- Several items set the options to determine the messages displayed on the console when a user logs on

# Audit Policy

- The Security Options section in Win2k8_R2



| Policy | Computer Setting |
|---|---|
| Network security: Allow Local System to use computer identity fo… | Not Defined |
| Network security: Allow LocalSystem NULL session fallback | Not Defined |
| Network Security: Allow PKU2U authentication requests to this co… | Not Defined |
| Network security: Configure encryption types allowed for Kerberos | Not Defined |
| Network security: Do not store LAN Manager hash value on next … | Enabled |
| Network security: Force logoff when logon hours expire | Disabled |
| Network security: LAN Manager authentication level | Not Defined |
| Network security: LDAP client signing requirements | Not Defined |
| Network security: Minimum session security for NTLM SSP based (… | Not Defined |
| Network security: Minimum session security for NTLM SSP based (… | Not Defined |
| Network security: Restrict NTLM: Add remote server exceptions f… | Not Defined |
| Network security: Restrict NTLM: Add server exceptions in this d… | Not Defined |
| Network security: Restrict NTLM: Audit Incoming NTLM Traffic | Not Defined |
| Network security: Restrict NTLM: Audit NTLM authentication in thi… | Not Defined |
| Network security: Restrict NTLM: Incoming NTLM traffic | Not Defined |
| Network security: Restrict NTLM: NTLM authentication in this dom… | Not Defined |
| Network security: Restrict NTLM: Outgoing NTLM traffic to remot… | Not Defined |
| Recovery console: Allow automatic administrative logon | Not Defined |
| Recovery console: Allow floppy copy and access to all drives and … | Not Defined |
| Shutdown: Allow system to be shut down without having to log on | Not Defined |
| Shutdown: Clear virtual memory pagefile | Not Defined |
| System cryptography: Force strong key protection for user keys … | Not Defined |
| System cryptography: Use FIPS compliant algorithms for encrypti… | Not Defined |
| System objects: Require case insensitivity for non-Windows subs… | Not Defined |
| System objects: Strengthen default permissions of internal syste… | Not Defined |
| System settings: Optional subsystems | Not Defined |
| System settings: Use Certificate Rules on Windows Executables f… | Not Defined |
| User Account Control: Admin Approval Mode for the Built-in Admi… | Not Defined |

# Null Sessions & NetBIOS

# Security Options

- Security Options can be used to control the connection of anonymous users
  - Many Windows services connect to a computer to retrieve data without formally logging on
  - Null session or anonymous logon
- Options will control what information can be retrieved
  - Tools have been written that can retrieve information from the Local Security Authority (LSA) such as user accounts and security policy
    - Winfingerprint

# Windows Shares

- Windows has a number of special shares
  - C$
  - ADMIN$
  - IPC$
  - Print$
- Shares with the $ are hidden from normal user
- Can be deleted but reappear when system rebooted

# Windows Shares

- C$
  - The root of each volume on the hard drive is shared automatically to allow administrators to connect across the network for administrative tasks
  - Administrators group has full control of the share
- ADMIN$
  - Represents the system root folder
  - %SYSTEMROOT% variable
  - C:\windows
  - Administrators group has full control of the share

# Windows Shares

- IPC$
  - Used by named pipes that allow communication between services
  - Used for remote administration and to view resources
  - Used for the anonymous logon
    - Null Session Attacks start here
- Print$
  - Used for remote administration of printers

# Anonymous Access

- Does not require a username or password
- Used by many Windows applications and services
- IPC$ allows anonymous access for a variety of purposes
  - Used for remote administration
  - Used to access shared folders
  - Named Pipes
  - Used for RPC connections
  - Cannot be deleted

# Anonymous Access

- Security Options Settings
  - Network Access: Do not Allow Anonymous Enumeration of SAM Accounts
  - Network Access: Do not Allow Anonymous Enumeration of SAM Accounts and Shares
  - Network Access: Let Everyone Permission Apply to Anonymous User
  - Network Access: Named Pipes that can be Accessed
    - List of services that are used for Inter Process Communication

# NetBIOS

- NetBIOS was an early version of software used by Windows Operating Systems to interact with network resources
- Newer versions of Windows can communicate with each other without the need for NetBIOS, however it is usually used for backwards compatibility
- Network resources were identified with 16-byte NetBIOS names
- Allowed packets to be transmitted over TCP/IP and various other network topologies

# NetBIOS

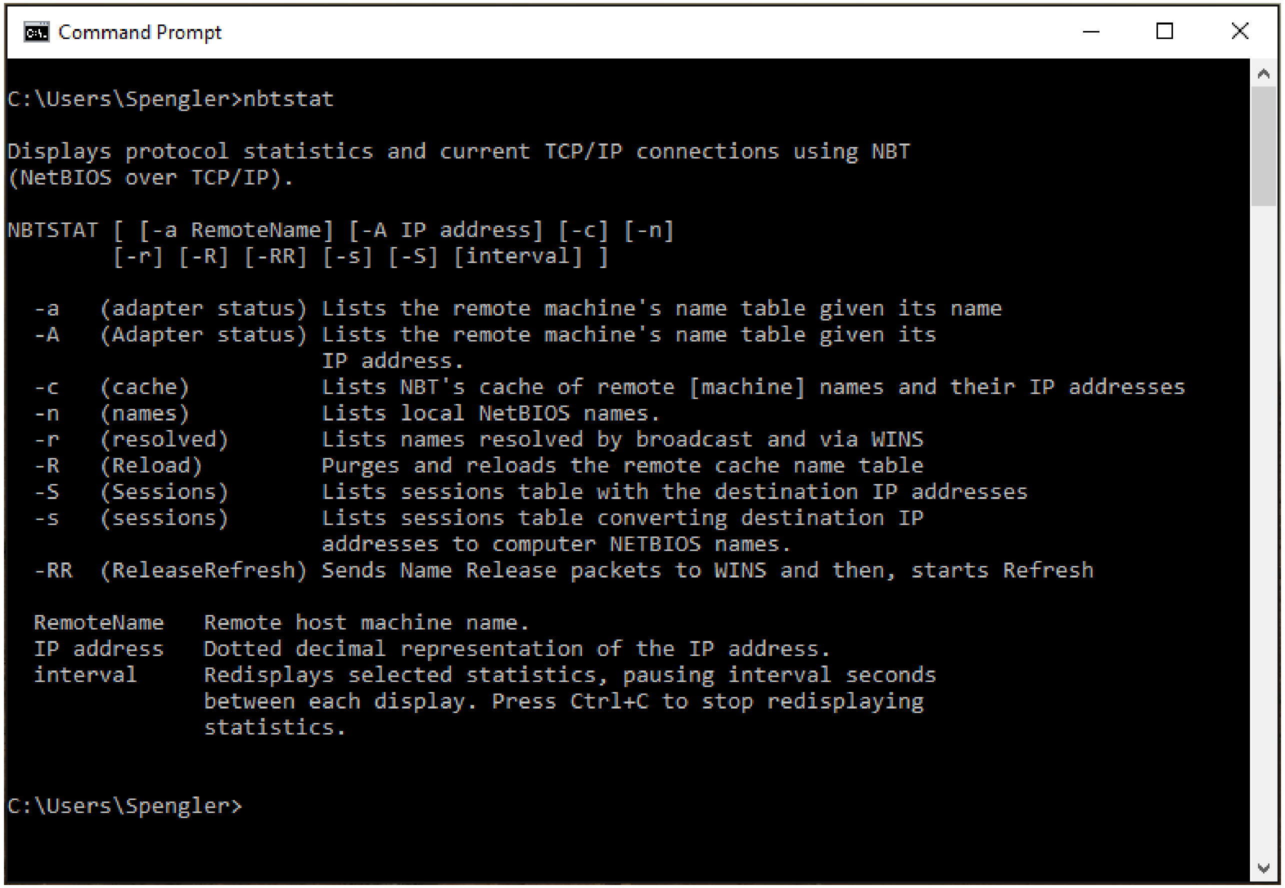
- Customers demand that newer systems can interact with older systems, especially when corporate budgets don't allow for all systems to be upgraded at the same time
- As long as newer Microsoft Operating Systems have to work with older NetBIOS based systems, security will always be a problem
  - Since Server 2000, it is referred to as NetBT running on ports:
    - UDP port 137 (name services)
    - UDP port 138 (datagram services)
    - TCP port 139 (session services)

# Enumerating NetBIOS

- The following commands can be used to enumerate NetBIOS vulnerabilities:
  - Nbtstat
  - Net view
  - Netstat
  - Ping
  - Pathping
  - Telnet

# Audit Policy

- Example of Nbtstat options in Windows 10

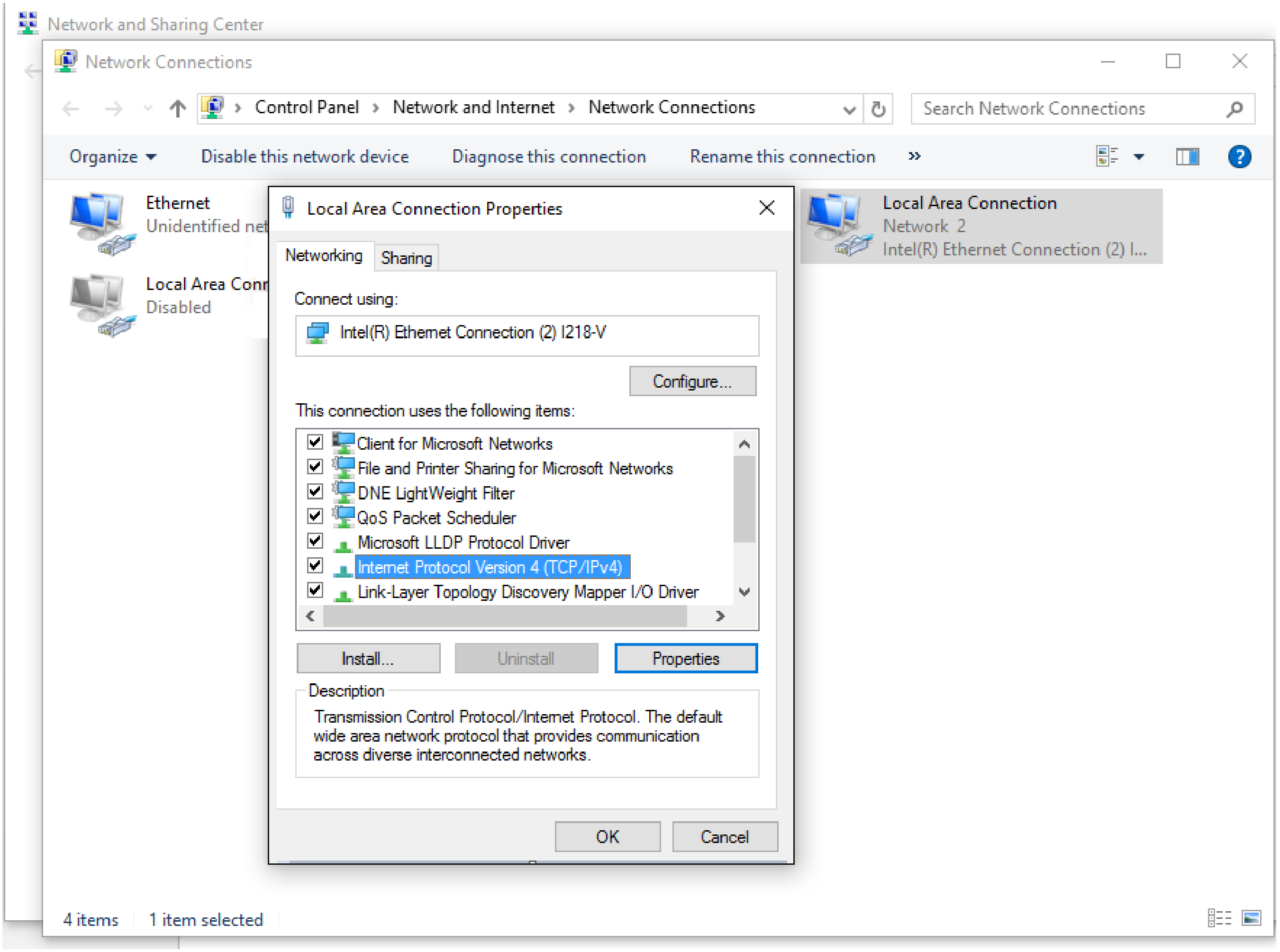


```
C:\Users\Spengler>nbtstat

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

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

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.


C:\Users\Spengler>
```

# Disabling NetBIOS on TCP/IP in Windows 10

- Go to Control Panel -> Network and Internet -> Network Connections
- Right click on the Network Connection that you wish to disable NetBIOS on and select Internet Protocol Version 4 (TCP/IPv4)
- Click on Properties

# Disabling NetBIOS on TCP/IP



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) Ethernet Connection (2) I218-V

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ DNE LightWeight Filter
- ☑ QoS Packet Scheduler
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Install... | Uninstall | Properties

Description

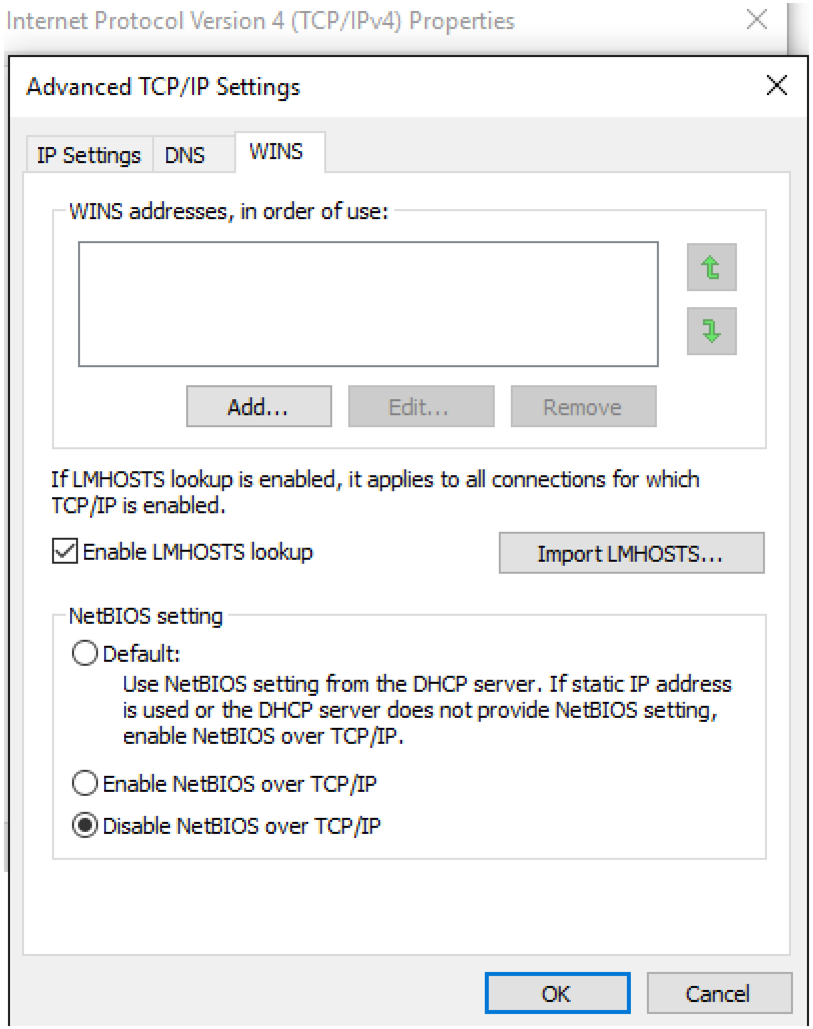
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

# Disabling NetBIOS on TCP/IP in Windows 10

- Under the Internet Protocol Version 4 (TCP/IPv4) Properties menu, select Advanced
- Click on the WINS tab
- You will see several options on the bottom for the NetBIOS setting
- Unless NetBIOS is required, you should select “Disable NetBIOS over TCP/IP”

# Disabling NetBIOS on TCP/IP in Windows 10



Internet Protocol Version 4 (TCP/IPv4) Properties

Advanced TCP/IP Settings

WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

# NTFS

# NTFS Permissions

- New Technology File System permissions are applied to folders and files
- Reasonably easy to set in the GUI interface
- Determining what is exactly set as well as the effective, inherited and explicit permissions is more complicated
- NTFS security issues
  - What permissions are to be assigned
    - Large set of permissions for files & folders
  - What users and groups should be given permissions

# NTFS Permissions

- Standard file permissions for NTFS
- Full Control
  - All permissions plus and take ownership & change permission
- Read
  - View file and attributes
- Modify
  - Read, write, execute plus delete
- Read & Execute
  - Run an application
- Write
  - Change file content and attributes
  - View file ownership

# NTFS Permissions

- Standard folder permissions
- Full Control
  - All permissions as well as change permissions and take ownership
- List content
  - View names of files and sub folders
- Modify
  - Delete folders & read, write, execute
- Read & Execute
  - Move folders
- Write
  - Create new files and sub folders

# NTFS Special Permissions

- Each permission is actually composed of several special permissions
- The special permissions can be granted individually to fine tune permissions
  - Either Allow or Deny
- Full Control for example includes the complete set of special permissions
- Read permission for example includes
  - List Folder/Read Data
  - Read Attributes
  - Read Extended Attributes
  - Read Permissions

# NTFS Special Permissions

- Explicit & inherited permissions
- Be default, permissions are inherited by all sub folders (child objects) of the parent folder
- If the inheritance box in the Advanced properties is unchecked then permission can be assigned explicitly to the folder
- Inherited permissions are shown in the Allow or Deny box with a shaded grey background
  - Explicit permissions have a white background

# NTFS Permissions

- Permissions can be explicitly assigned to an object, or inherited from parent folders
- Any permission not explicitly assigned or inherited is assumed to be denied
- If a person is a member of multiple groups and the groups have different permissions an equal  Deny permission overrides an Allow permission
  - If one group is granted read but another group is denied read then the user is denied
- Exceptions: An explicit Allow permission will override an inherited Deny permission

# NTFS Permissions

- Effective permissions
- If a user is a member of 3 groups
  - Group 1 – allow read
  - Group 2 – allow write
  - Group 3 – allow full control
- The user will be granted full control

# NTFS Permissions

- If a permission is not inherited or explicitly Allowed it is denied
- Permissions have a hierarchy or precedence order in how they are applied
  - Explicit Deny
  - Explicit Allow
  - Inherited Deny
  - Inherited Allow

# NTFS Permissions

- Deny permissions do not always override Allow permissions
  - An explicit Allow will take precedence over an inherited Deny
- Explicit Deny will take precedence over an inherited Allow
- Permissions applied directly to the object (explicit) are applied before inherited permissions

# NTFS Permissions

- Permissions are set in the precedence order automatically
- When a Deny permission is set for a user or group through the GUI it is automatically set or moved to the top of the list by the operating system
- It is possible to use scripts to set permissions for users and groups
  - The OS will not check the script for the proper precedence and could list Allow permissions before Deny permissions

# NTFS Permissions

- The user that creates a folder & file becomes the owner
- Folders and files created during installation are owned by the admin group
- By default, the owner can change permissions on the folder or file
- Since Vista, Win7, and Win 2008 server is the owner/creator where the owner can be denied the permission to change permissions

# Shared Folder Permissions

# Windows Shares

- Windows allows users to share folders across a network
- Permissions are applied to the shared folder
- Three permissions can be granted to shared folders
  - Full control
  - Change
  - Read

# Windows Shares

- These permissions apply to network access only and not to a local console logon
- The access control on a shared folder is the combination of the shared and NTFS permissions
- The most restrictive control is applied

# Windows Shares

- If the share permission is Allow Read, and the NTFS permission is Allow Full Control then only Read access is granted across the network to the shared folder
- If the share permission is Allow Full Control, and the NTFS folder permission is Allow Read Write then the effective permissions are Read & Write to the shared folder

# Share Permissions

- When creating a shared folder in WinXP & Win2003 server by default the Everyone group is granted Read permissions
    - This does not follow the Principle of Least Privilege
- Even worse, Windows NT & Windows 2000 gave the Everyone group Full Control
    - Since Vista, Windows does not give the Everyone group permissions

# Share Permissions - Old

- Older FAT file systems with shared folders did not allow for the setting of share permissions
  - The only access control was a password
  - Connection to the share allowed full access to all the data

# Server Message Block (SMB)

- Previous versions of Windows (NT and older) used SMB to share files
- It usually ran on top of NetBIOS, NetBEUI, or TCP/IP
- There are many hacking tools available to exploit the vulnerabilities associated with SMB

# Common Internet File System (CIFS)

- Replaced SMB starting with Windows 2000, XP, and Server 2003
- Uses an enhanced version of SMB
- Server may listen on many ports including:
    - FTP port 21
    - SMTP port 25
    - DNS port 53
    - HTTP port 80
    - Kerberos port 88
    - RPC port 135
    - LDAP port 389
    - HTTPS port 443
    - SMB/CIFS port 445
    - LDAP over SSL port 636
    - AD global catalogue port 3268
    - Terminal Server port 3389

# Common Internet File System (CIFS)

- Linux O/S clients are able to communicate with Microsoft file shares by “tricking” the MS server
- The Linux O/S is able to browse and mount a Windows share or connect to a Samba Server
- Typical commands in Linux will look like this:

```
mount –t cifs //share/folder /local/dir –o username=example
smbclient //server/share -U user
```

# Common Internet File System (CIFS)

- The user will be prompted with a password and if they exist in the list of users, they will have access
- When sharing across networks, you may have to substitute the server's name (share) with the IP address in case DNS is being blocked by a firewall

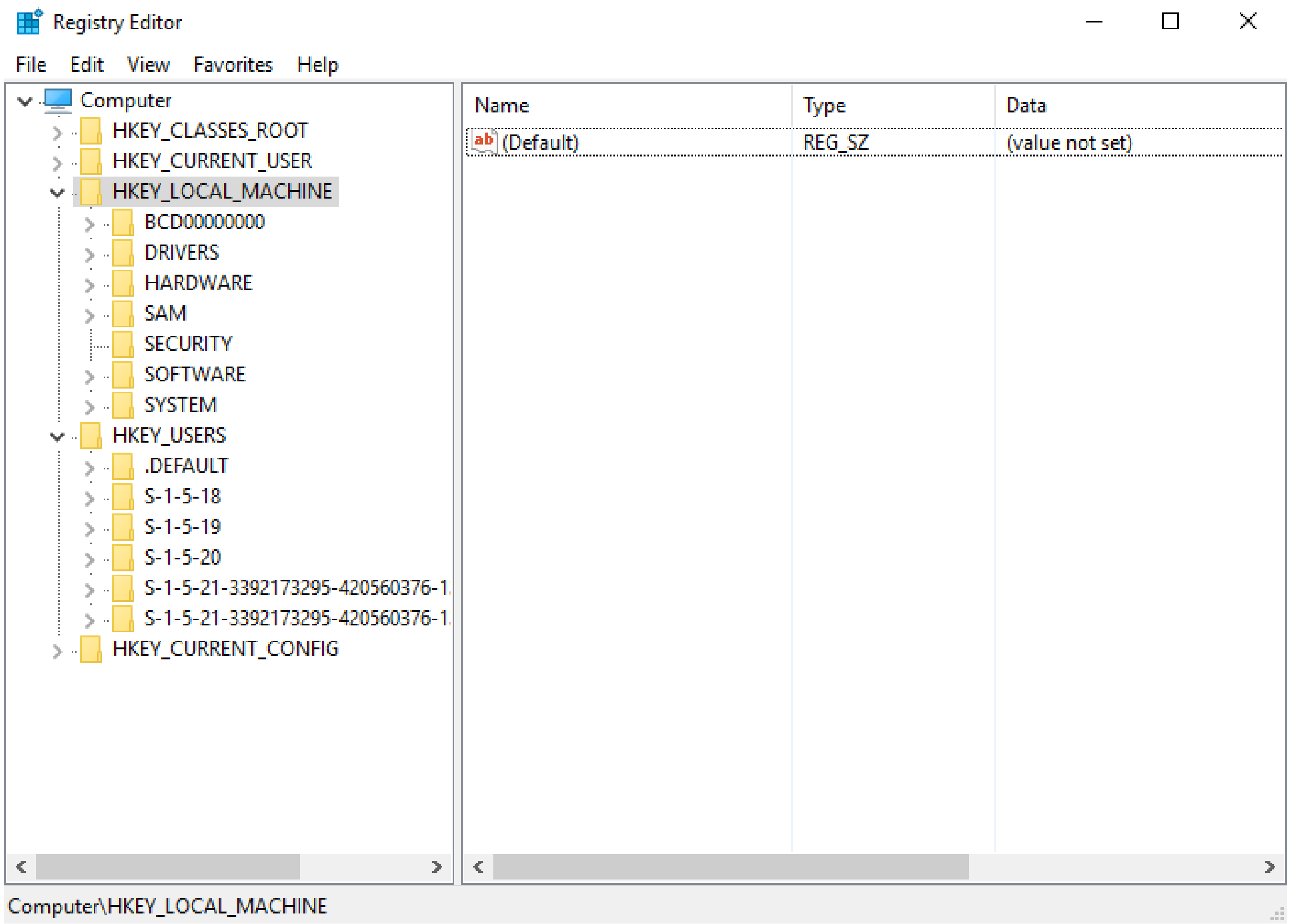
```
mount –t cifs //192.168.10.11/folder /local/dir –o username=example
```

# Registry Permissions

# Registry Permissions

- The Registry is a database that stores configuration settings and options for the Windows OS
- The database is a hierarchical file system
- The registry data store is known as a Hive
- User-specific data is stored in the appropriate user section of Hive Key Users (HKEY_USERS)
- System and machine information is stored in the HKEY_LOCAL_MACHINE (HKLM) hive

# Windows 10 Registry Editor



Registry Editor

File Edit View Favorites Help

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    DRIVERS
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
    .DEFAULT
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-3392173295-420560376-1
    S-1-5-21-3392173295-420560376-1
  HKEY_CURRENT_CONFIG
```

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |

Computer\HKEY_LOCAL_MACHINE

# Registry Permissions

- A Registry key is similar to a folder and can contain sub keys
- Each registry key can be assigned values which determine the configuration option
- Registry permissions can be viewed through the regedit Registry editor tool

# Registry Permissions

- Regedit will display the Registry as a hierarchical file system
- Registry permissions are inherited similar to the NTFS folder & file permissions
- By selecting a registry key (folder) the values and permissions can be viewed

# Registry Security

- The Windows registry will typically be altered when new software or updates are installed
- Many Patch Management scanners will look for Windows O/S updates by searching the registry
- Windows releases updates that are numbered and begin with KB
- These KB numbers are used to determine if a system is patched

# Registry Security

- There are some handy tools to compare registry settings
- Sometimes it is good to take a copy of the HIVE before and after an update or software installation
- Regshot is a great tool for this:

http://sourceforge.net/projects/regshot/

# Lab 04 – Permissions

# Lab 04 Details

- Explore Windows Permissions
- Access Control Lists
- Changing Permissions
- Registry Permissions