Advanced Scripting   
Security Settings for User Rights

Last Updated: 4/13/2024 9:52 AM Version 1  
Document Prepared for: CYBER360 Student

# Name Click here to enter name ID Click here to enter id

# Instructions

Answer all questions directly in this document. You will save and upload this completed document as your homework submission.

# Overview

One of the most effective things a defender can do to harden a Windows workstation or server is configure users’ operating capabilities according to the principle of least privilege. Chapter 5 mentions several of these settings. Available tools for this purpose include the Local Security Policy management console, the SecEdit command-line tool, and PowerShell. For user rights management purposes, each of these requires administrator privilege.

# Requirements

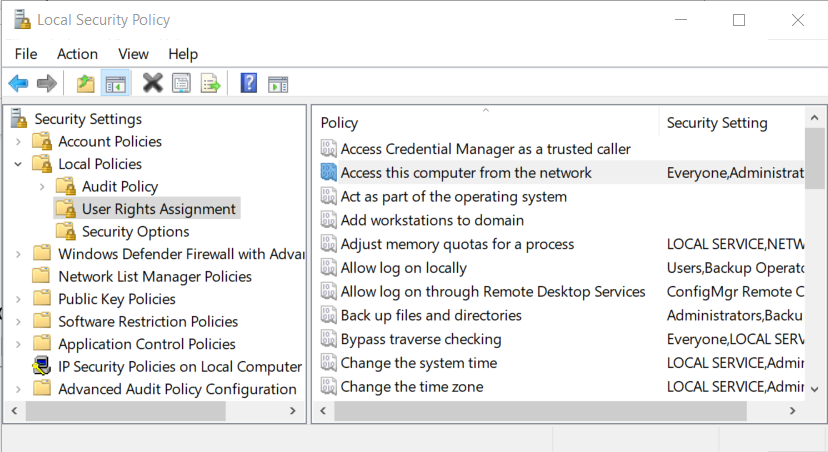
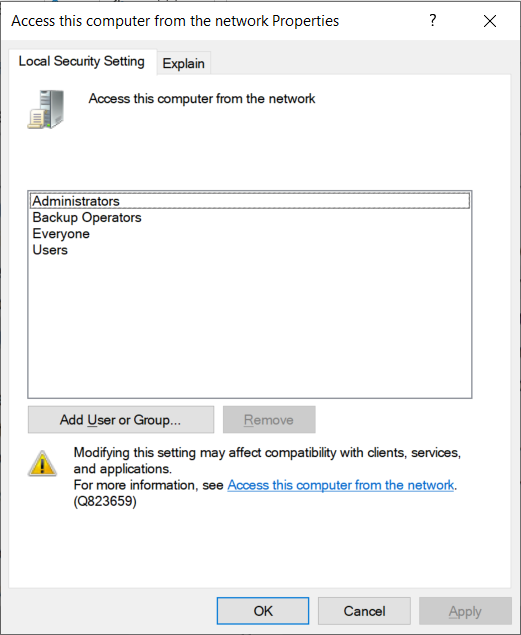
PowerShell (Core or Desktop) for Windows, with elevated administrator privilege.

Local Security Policy Editor, **SecPol.msc**. (*If you’re running an education, enterprise, pro, or server edition of Windows, you already have this, but if you’re running a “home” edition of Windows, visit* <https://www.itechtics.com/enable-secpol-msc/> *to find a script that will add necessary tools for group and local policies.*)

# Task 1—Local Security Policy Management Console

Type **secpol.msc** and press [Enter] to launch the *Local Security Policy* Management Console GUI utility. *Caution: be careful! It is possible to make careless changes that can accidentally render a Windows host unusable.*

## Steps

1. The Local Security Policy management console looks a bit like the File Explorer app, with settings organized as expandable folders in the left pane:   
   
2. Expand the *Local Policies* folder, then click *User Rights Assignment* (as illustrated above). In the right pane, for each *Policy*, The *Security Setting* column contains a list of user groups and individual users.
   1. Double-click the policy labeled **Access this computer from the network** to view its Properties dialog:  
      
   2. Tap the *Explain* tab. What are the four default user groups on a server or workstation for this user rights setting? Click or tap here to enter text.
   3. Tap the [Local Security Setting] tab. Select the user group *Everyone*, then click [Remove].
   4. Choose: tap [OK] to commit this change and close the Properties dialog, or tap [Cancel] to abort the change and close the Properties dialog.
3. Show the current groups and users in each of the following user rights settings on your computer:
   1. **Allow log on locally**: Click or tap here to enter text.
   2. **Allow log on through Remote Desktop Services**: Click or tap here to enter text.
   3. **Log on as a batch job**: Click or tap here to enter text.
   4. **Log on as a service**: Click or tap here to enter text.
   5. Do any of the settings that start with ***Deny access*** or ***Deny log on*** have configured groups or users? If so, which settings? Click or tap here to enter text. (These ***Deny*** rules override any settings that might be configured in any of the other rules that allow access.)
4. Show the current groups and users in each of the following user rights settings on your computer:
   1. **Back up files and directories**: Click or tap here to enter text. (Users/Groups with this privilege can misuse it to *read* any file.)
   2. **Restore files and directories**: Click or tap here to enter text. (Users/Groups with this privilege can misuse it to *write* to any file.)
   3. **Generate security audits**: Click or tap here to enter text.
   4. **Manage auditing and security log**: Click or tap here to enter text.
   5. **Debug programs**: Click or tap here to enter text.
   6. **Load and unload device drivers**: Click or tap here to enter text.
   7. **Change the system time**: Click or tap here to enter text.
   8. **Change the time zone**: Click or tap here to enter text.
   9. Do any of these four settings have configured groups or users? If so, which settings?  
      **Enable computer and user accounts to be trusted for delegation**  
      **Impersonate a client after authentication**  
      **Act as part of the operating system**  
      **Add workstations to domain**  
       Click or tap here to enter text.
5. Close the Local Security Policy management console.

# Task 2—Examine user rights with **secedit.exe**

**SecEdit.exe** is a Windows command-line tool that interfaces with User Rights Assignment settings.

## Steps

1. At your (administrator privileged) PowerShellCore (Windows) prompt, enter:   
   **SecEdit /?**   
   to see a few of the command’s options.
2. Enter:   
   **$env:Temp**   
   to see your account’s unique temporary directory. We’ll save some output to that folder.
3. Enter:   
   **secedit /export /areas USER\_RIGHTS /cfg $Env:Temp\secedit.txt**.  
   This will save all of your machine’s local user rights settings to a text file.
4. View the results of the file:   
   **more $Env:Temp\secedit.txt**   
   or  
   **notepad $Env:Temp\secedit.txt**
5. The file contains lists of key-value pairs, and is organized into stanzas. Each stanza starts with a square bracketed identifier. The first stanza probably looks something like this:   
   **[Unicode]**   
   **Unicode=yes**   
   (So this stanza’s identifier is *[Unicode]*, and it has one setting: the key *Unicode* has the value *yes*.)
   1. Find the [Privilege Rights] stanza, then find its setting *SeRemoteShutdownPrivilege*. What is the value of that setting? Click or tap here to enter text. *Hint: if the value isn’t empty, it should be a sequence of characters starting with* **\*S** *(“splat S”) and followed by some hyphen-delimited numbers.*
   2. Notice that almost all of the groups and users for these settings are represented by *security ID* codes (SIDs) rather than the actual group names and user names. You can probably figure out what some of the SIDs represent, but you’ll prefer a more helpful tool to show actual group or user names. Let’s look at one way to do that.
   3. Enter the following three PowerShell command lines:   
      **$t = "***<insert your answer to step 5.1 here, starting with the capital* **S** *(omit the leading splat* **\****)>***"**   
      **$s = New-Object System.Security.Principal.SecurityIdentifier($t)**   
      **$s.Translate([System.Security.Principal.NTAccount]).Value**   
      Your result: Click or tap here to enter text.

# Deliverable

Upload this document with completed answers to I-Learn Canvas.