Unit OS7: Security

7.4. Lab Manual

Roadmap for Section 7.4.

Lab experiments investigating:

- Viewing Security Processes
- Looking at the SAM
- Viewing Access Tokens
- Looking at Security Identifiers (SIDs)
- Viewing a Security Descriptor structure
- Investigating ordering of Access Control Entries (ACEs)
- Investigating Privileges

Looking at the SAM

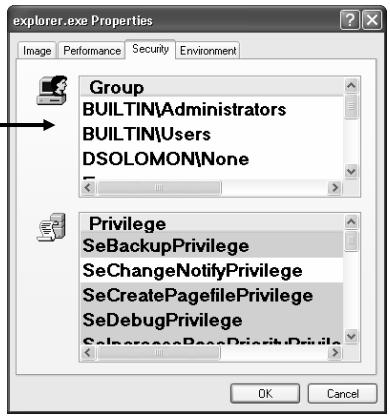
- Look at HKLM\SAM permissions
  - SAM security allows only the local system account to access it
  - Run Regedit
  - Look at HKLM\SAM - nothing there?
  - Check permissions (right click->Permissions)
  - Close Regedit
- Look in HKLM\SAM
  - Running Regedit in the local system account allows you to view the SAM:

    psexec –s –i –d c:\windows\regedit.exe
  - View local usernames under HKLM\SAM\SAM\Domains\Account\Users\Names
  - Passwords are under Users key above Names

4

Viewing Access Tokens

- Process Explorer: double click on a process and go to Security tab
  - Examine groups list
- Use RUNAS to create a CMD process running under another account (e.g. your domain account)
  - Examine groups list
- Viewing tokens with the Kernel Debugger
  - Run !process 0 0 to find a process
  - Run !process PID to dump the process
  - Get the token address and type !token –n <token address>
  - Type dt _token <token address> to see all fields defined in a token



5

Using PsGetSid to View Account SIDs

- Example SIDs

Domain SID: **S-1-5-21-34125455-5125555-1251255**
First account: **S-1-5-21-34125455-5125555-1251255-1000**
Admin account: **S-1-5-21-34125455-5125555-1251255-500**

- Lab: run PsGetSid (Sysinternals) to view the SID of your username and of the computer

6

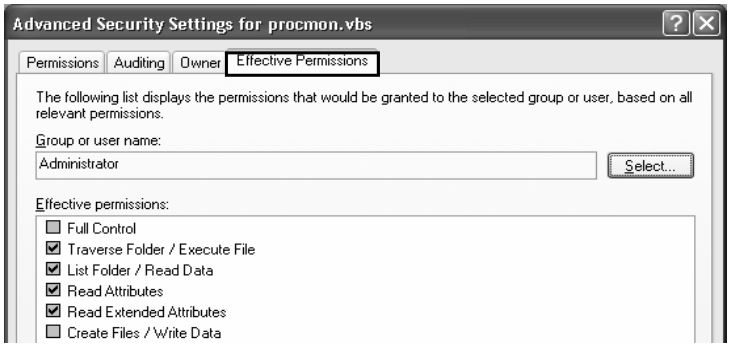
Viewing a Security Descriptor Structure

- Get the address of an EPROCESS block with !process
- Type !object on that address
- Type “dt _OBJECT_HEADER” on the object header address to get the security descriptor address
- Type !sd <security descriptor address> & -8 1

7

Understanding permissions as presented by GUI Security Editors

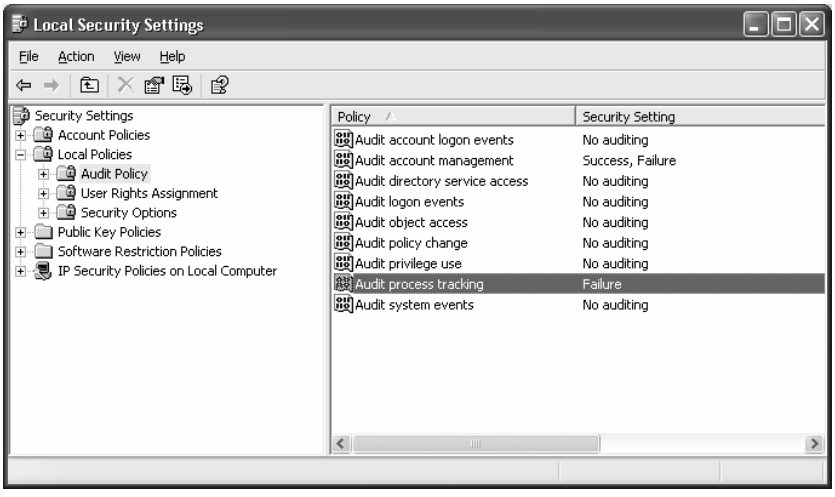
- Go to a NTFS file
- Add an Everyone deny-all to a file
- Will the Administrator be able to look at the file?
  - Verify your answer by checking Effective Permissions



8

View Audit Options

- Run Secpol.msc and view Local Policies->Audit Policy



9

Seeing a Privilege Get Enabled

- Run Secpol.msc and examine full list
  - Click on Local Policies->User Rights assignment
- Process Explorer: double click on a process, go to security tab, and examine privileges list
- Watch changes to privilege list:
  1. Run Process Explorer – put in paused mode
  2. Open Control Panel applet to change system time
  3. Go back to Process Explorer & press F5
  4. Examine privilege list in new process that was created
  5. Notice in privilege list that system time privilege is enabled

10

Observe the Bypass Traverse Checking Privilege

- View the use of the backup privilege:
  - Make a directory
  - Create a file in the directory
  - Use the security editor to remove inherited security and give Everyone full access to the file
  - Remove all access to the directory (do not propagate)
  - Start a command-prompt and do a “dir” of the directory
  - Run PView and enable the Backup privilege for the command prompt
  - Do another “dir” and note the different behavior
- View the use of the Bypass-Traverse Checking privilege (internally called “Change Notify”)
  - From the same command prompt run notepad to open the file (give the full path) in the inaccessible directory
  - Extra credit: disable Bypass-Traverse Checking so that you get access denied trying to open the file (hint: requires use of secpol.msc and then RUNAS)

11