Windows 7 Access Control Lab

Goal

Use Windows 7 security subsystem to protect elements on a NTFS file system

Due

Submit your final report on compass by midnight Tues, February 2. Each student must submit a report individually.

Scenario

You need to set up a file system for CosaNostra Pizza. This company has three sets of employees

- Deliverators
- Financial folks
- System Administrators

Each set of folks would like a place on the file system where in general they have full control and other folks have read-only access. But each group of folks would like to have the following subareas with different access:

- A public area that gives all users read and write access.
- A private area that blocks everyone except for folks of the same set.

The lab machines have been populated with the following users

- Ellen – Currently an deliverator, but she used to be a financial person and she still sometimes fulfills that role.
- Bob – A deliverator.
- Carol and Dave are both Financial folks
- Alice and Gus are both sys admins

Each user's password is their name plus "-test", e.g., alice's password is alice-test.

The following groups are also on these machines

- Delivery
- Financial
- Administrators

Things you need to know

You will need to adjust the audit policies for the SACLS to have any effect. Go to Control Panel -> System and Security -> Administrative Tools ->Local Security Policy -> Audit Policies. Be careful of enabling too many audit policies. They can get very verbose.

The event viewer is in Control Panel -> System and Security -> Administrative Tools -> Event Viewer

You can look at assigned privileges in Control Panel -> System and Security-> Administrative Tools ->Local Policy ->User Rights Assignment.

You can manipulate the ACL's either graphically through the file explorer or textually through the icacls utility. You can also adjust integrity levels with the icacls or chml utilities installed on the Windows image.

You can also use the Process Explorer (procexp.exe) to look at the attributes of the processes running on the machine. You need to run this program as Administrator to see all of the available information.

The lab environment

The machines in the lab are running Fedora Core 12. Windows 7 is running as a virtual machine under VirtualBox.

You may also complete this lab on a Windows 7 machine outside of the lab as long as you have administrative access on that machine.

Deliverables

Uncle Ezno of CosaNostra Pizza is contracting you to perform the following actions.

1. Implement the directory structure that satisfies the security requirements described above.
2. Augment the scenario to block Ellen from access to the financial private area (Ellen is a member of the Financial group).
3. Cause audit messages to be sent to the event viewer when people without access attempt to access one of the private areas.
4. Explore the mandatory integrity control mechanism.
    - View the integrity levels of the processes and files.
    - Make a copy of the cmd.exe program. Set its integrity level to Low.
    - Figure out how to make the “no read up” policy work.

Write a report that includes the following elements.

1. Describe your solution to items 1 and 2 above.
2. How do you block access from one of the administrative users? Can a member of the Administrative group by-pass your controls? How or why not?
3. Include a system log entry generated from your item three deliverable.
4. In the private directories, can you create directories or files that can be accessed by non-group users?
5. What is the common integrity level of the processes and files? What are the exceptions?
6. Who can assign integrity labels to files?
7. What is the result of your low integrity cmd.exe? Can it traverse any of the file system? Can it execute other programs?
8. How did no read up policy work? What did you have to do to make this work?