Lab2

Windows & Linux Access Control and Hardening Exercises

Goal

Use Windows 7 security subsystem to protect elements on a NTFS file system. Use Linux access controls to protect elements of a Linux file system. Use the CIS-CAT tool to harden your Windows, Windows Server and Ubuntu images.

Due

Submit your final report on Compass by 11:59 PM on Monday, February 5.

PART 1

Scenario

You will need to set up Active Directory on your Windows Server and join your Windows 7 image to it. Then you need to set up a file system for collaboration between different elements of the Ankh-Morpork society. In particular, you are asked to design a file system control for the following groups.

- The Nightwatch
- Assassins' Guild
- Unseen University

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.

You need to create the following users in Active Directory in your Windows Server.

- Ellen – Currently on the staff of the Unseen University. She used to be a member of the Nightwatch and still sometimes works on their behalf.
- Gus – On staff of the Unseen University.
- Carol and Dave are both members of the Nightwatch.
- Alice and Bob are both members of the Assassins Guild.

Each user's password is **Lab02-staff-test!**

In addition there is a user named **boss** which is in the admin group.

The following groups need to be created in Active Directory:

- Nightwatch
- Assassin
- Unseen

Things you need to know

Run this exercise in two parts, Windows first, then Linux (Linux obviously will NOT be joined to AD, use local groups and users). Performance will be less then optimal if everyone runs three images simultaneously.

For Windows:

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 > Local Policies > Audit Policy. 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.
You can use the “runas” command to test some of your scenarios without logging in and out multiple times.

Lab Environment

Use your VMs from the last lab.

Deliverables

The government of Anhk-Morpork is contracting you to perform the following actions.

1. Create an active directory domain (use NETID-DOMAIN.LOCAL) where NETID is your NETID. Create users and groups in Active Directory, do NOT use local users.
2. Implement the directory structure that satisfies the security requirements described above.

PART 2

Download the attached CIS-CAT tool, which provides an automated mechanism to benchmark a system's security configuration.
Take a screenshot of the CIS-CAT tool output for each of your VMs before performing any hardening. Using the OS hardening guides and the tool's report output, make a minimum of 10 changes each (of your choosing) to your Windows, Windows Server, and Ubuntu images, then take another screenshot of the CIS-CAT tool output for each of the three VMs.

Deliverables

Submit before and after screenshots of the CIS-CAT tool output for each of your VMs. The output should reflect at least 10 additional hardening steps.