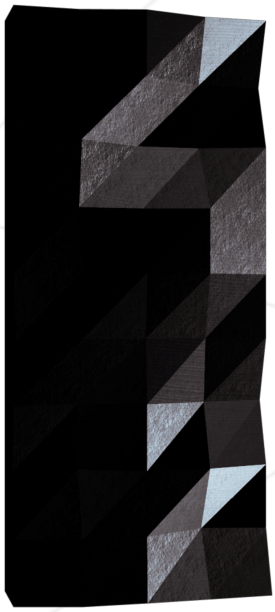

Administrative Directory

Introduction to GPO and SIEM.

Summary: This subject will introduce you to ActiveDirectory's GPO, and to SIEM to analyse your event log.

Version: 1.00

Contents

Chapter I

Preamble

Domolia is really happy with the deployement you've made for them, and now want to securize what users can and can't do, and monitorize what happen on the network. For this, they want you to use two build-in feature of Active Directory, GPO and SIEM.

GPO are "rules" applied to the network and users, and SIEM are a logging system, saving everything that did happen on the network

Chapter II

Mandatory part

II.1 Preparation

You must process to certain preparation/Creation :

- Organisation Unit "Workspace"
- Organisation Unit "Administration"
- Group "Worker"
- Group "Direction"
- Group "Secretary"
- Group "Administrator"
- Disk "D:"
- Disk "E:"
- Folder "D:/WorkPlan"
- Folder "D:/Management"
- Folder "E:/HumanResources"
- Folder "E:/Estimate"
- Folder "E:/Client"

II.2 GPOs creation

Now that the preparation are done, there is the list of GPO they want you to create.

- Define screen desktop
- Define OpenOffice program deployement if required by each user
- Define Slack non-optionnal installation for each new user
- Allow groups to access certain disk, and automaticaly connect to them
  Every groups should access the two mandatory disks
- Allow groups to access certain folders, with example as :
  Worker : Access to folders :
  - D:/WorkPlan
  - D:/Management
  - E:/HumanResources

  Direction : Access to folders :
  - D:/WorkPlan
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Secretary : Access to folders :
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Administrator : Access to every folder
- Allow groups to edit certain folders/files
  Worker : Edit folder :
  - D:/WorkPlan

  Direction : Edit folders :
  - D:/WorkPlan
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Secretary : Edit folders :
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Administrator : Can edit every folders
- Allow groups to create certain folders/files
  Worker : Create files in :
  - D:/WorkPlan

  Direction : Create files in :

- D:/WorkPlan
- D:/Management
- E:/HumanResources
- E:/Estimate
- E:/Client

Secretary : Create files in :
- D:/Management
- E:/HumanResources
- E:/Estimate
- E:/Client

Administrator : Can create files in every folders

- Allow groups to delete certain folders/files
  Worker : Nothing
  Direction : Delete files in
  - D:/WorkPlan,
  - D:/Management,
  - E:/HumanResources,
  - E:/Estimate
  - E:/Client

  Secretary : Delete files in
  - D:/Management,
  - E:/HumanResources
  - E:/Estimate
  - E:/Client Administrator : Can delete files in every folders

II.3 Network event logging

To work in parallele with your GPO and your installation, Domolia asked you to implement, by any mean, a way for them to be notified of what happen in their network.

They desire to get information about the following activities :

- Computer Account Management Activity
- Distribution Group Management Activity
- Security Group Management Activity
- User Account Management Activity
- Directory Service Access Activity
- Logoff Activity
- Logon Activity

`The Domolia manager has heard the term SIEM used without necessarily understanding why.`

II.4 Logging scripts

In addition of the monitorisation, you're asked to create any scripts necessary to read logs with ease. Domolia requested at least the following operation to performable via a script.

- A script that list who's connected between 2 time tag
- A script to show event concerning one user between 2 time tag
- A script to isolate access and modification one certain folder
- A script to list of IPs used by users
- A script listing security incidents

Chapter III

Bonuses

Find below a few ideas of interesting bonuses you could create. Some could even be useful. You can, of course, invent your own, which will then be evaluated by your correctors according to their own taste.

- Some GPO
- Some SIEM necessary log
- Some script to activate/deactivate SIEM log type
- Some script to automatize actions over SIEM log

The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter IV

Submission and peer-evaluation

You only have to turn in a `signatures.txt` file at the root of your `Git` repository. It must contain the signature of each of your machine's virtual disk, following this format :

```
> cat signatures.txt
# VM AD 1
6e657c4619944be17df3c31faa030c25e43e40af
# VM AD 2
6e657c4619944be17df3c31faa030c25e43e40af
# VM USER 1
6e657c4619944be17df3c31faa030c25e43e40af
# VM USER 2
```

To get a signature of one of your VM, you first have to open the default installation folder (it is the folder where your VMs are saved):

- Windows: `%HOMEDRIVE%%HOMEPATH%\VirtualBox VMs\`
- Linux: `~/VirtualBox VMs/`
- MacM1: `~/Library/Containers/com.utmapp.UTM/Data/Documents/`
- MacOS: `~/VirtualBox VMs/`

Then, retrieve the signature from the `".vdi"` file (or `".qcow2` for `UTM`'users) of your virtual machine in `sha1` format. Below are 4 command examples for a `centos_serv.vdi` file:

- Windows: `certUtil -hashfile centos_serv.vdi sha1`
- Linux: `sha1sum centos_serv.vdi`
- For Mac M1: `shasum Centos.utm/Images/disk-0.qcow2`
- MacOS: `shasum centos_serv.vdi`

This is an example of what kind of output you will get:

- `6e657c4619944be17df3c31faa030c25e43e40af`

Please note that your virtual machine's signature may be altered after your first evaluation. To solve this problem, you can duplicate your virtual machine or use save state.

It is of course FORBIDDEN to turn in your virtual machine in your Git repository. During the defense, the signature of the signature.txt file will be compared with the one of your virtual machine. If the two of them are not identical, your grade will be 0.

.

The evaluation process will happen on the computer of each student of the evaluated group.