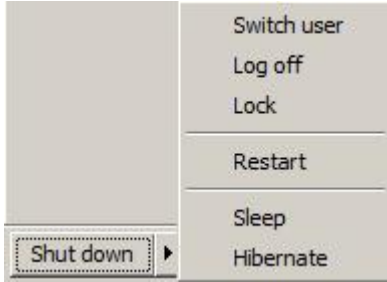


Labo Windows (90 min)

| | | |
|---------------|--|------------|
| 0 | Objectifs & poste de travail | sudo ./c 2 |
| | Depuis Vista, Microsoft implémente <i>User Account Control (UAC)</i> qui respecte le principe du moindre privilège afin de limiter l'impact d'une éventuelle attaque. | |
| Cadre | Ce labo s'effectue individuellement avec un PC Windows 7 situé dans l'intranet | |
| Action | Ouvrir une session avec Username= albert password= admin Copier le dossier \\10.2.1.1\doclabo\Secu\Windows sur le bureau Créer un compte ursula password= user à partir de du §1.1 du Labo Hacking | |

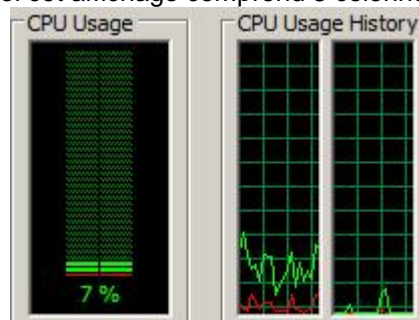
| | | |
|---|--|--------|
| 1 | User Account Control (UAC) & whoami | 10 min |
|---|--|--------|

| | |
|-----------------|--|
| Objectif | Configurer UAC pour notifier les changements effectués sur la configuration système |
| Action | Control Panel – User Accounts – Change User Account Control settings Selectionner Always notify. OK |
| But 1a | Déterminer l'appartenance à un groupe |
| Action | Dans <i>Local Users and Groups – Users</i> clic-droit sur ursula – <i>Properties – Member of</i> |
| Q_1a | A quel(s) groupe(s) appartient ursula ? A quel(s) groupe(s) appartient albert ? |
| But 1b | Ouvrir la configuration des paramètres TCP/IP |
| Action | <i>Start – Control Panel – Network and Sharing Center – Change adapter settings</i> Clic sur <i>Local Area Connection - Properties</i> |
| Q_1b | Que se passe-t-il ? Quelles sont les différences avec XP ? |
| Remarque | Lorsque cette fenêtre s'affiche, l'écran se noircit et il n'est plus possible d'effectuer une tâche avant l'acceptation ou le refus d'élévation de privilèges. Cette fenêtre ne s'affiche pas sur le même bureau que l'utilisateur mais dans un bureau isolé appelé Secure Desktop . |
| But 1c | Déterminer le contexte de sécurité |
| Action | Lancer une fenêtre en ligne de commande à l'aide du raccourci bureau <i>Command Prompt</i> Typer : <code>whoami /all</code> |
| Q_1c | Combien y a-t-il de privilèges disponibles (consulter les <i>PRIVILEGES INFORMATION</i>) ? |
| But 1d | Effectuer un Switch User pour établir une session avec le compte ursula |
| Action | Ouvrir la configuration des paramètres TCP/IP <i>Start – Shut Down... - Switch User</i> |
| |  |
| | <i>Start – Control Panel – Network and Sharing Center – Change adapter settings</i> Clic sur <i>Local Area Connection - Properties</i> |
| Q_1d | Que se passe-t-il ? |

- But 1e** Déterminer le contexte de sécurité
- Action** Lancer une fenêtre en ligne de commande à l'aide du raccourci bureau *Command Prompt*
Typer : `whoami /all`
- Q_1e** Combien y a-t-il de privilèges disponibles (consulter les *PRIVILEGES INFORMATION*) ?
- Action** Lancer une fenêtre en ligne de commande avec privilèges administrateur :
Clic droit sur *Command Prompt* (raccourci bureau) – *Run As Administrator*
Typer : `whoami /all`
- Q_1f** Combien y a-t-il de privilèges disponibles (consulter les *PRIVILEGES INFORMATION*) ?

| | | |
|----------|--|---------------|
| 2 | Task Manager & Resource Monitor | 10 min |
|----------|--|---------------|

- Objectifs** Identifier les charges et activités
- But 2a** Observer les charges CPU et RAM lorsque l'utilisateur ouvre des nouvelles fenêtres dans Chrome
- Action** Utiliser le raccourci <Ctrl-Maj-Esc> pour ouvrir Task Manager
Lancer le navigateur Google Chrome
Typer plusieurs Ctrl+N à intervalles réguliers
- Q_2a** Quelles charges observez-vous ?
- Q_2b** Pourquoi cet affichage comprend 3 colonnes ?



Charge CPU Moyenne + Charge CPU de chaque cœur

- Action** Dans Task Manager, sélectionner onglet Performance puis 

- Q_2c** Qu'apporte Resource Monitor en plus de Task Manager pour la charge CPU ?

- But 2b** Observer les charges disque (en ouvrant plusieurs fenêtres avec Chrome)

| Processes with Disk Activity | | | | |
|-------------------------------------|-------|--------------|---------------|-----------------|
| <input type="checkbox"/> Image | PID | Read (B/sec) | Write (B/sec) | Total (B/sec) ▾ |
| <input type="checkbox"/> chrome.exe | 12192 | 3'789 | 1'213'158 | 1'216'947 |
| <input type="checkbox"/> System | 4 | 6'007 | 92'202 | 98'209 |

| Storage | | | | | |
|--------------|---------------|-----------------|----------------------|------------------|---------------------|
| Logical Disk | Physical Disk | Active Time (%) | Available Space (MB) | Total Space (MB) | Disk Queue Length ▾ |
| C: Q: D: E: | 0 | 6.40 | 148'599 | 475'436 | 0.06 |

- But 2c** Observer les charges réseau (en ouvrant plusieurs fenêtres avec Chrome)

Parcourir le dernier tiers de <http://www.7tutorials.com/how-use-resource-monitor-windows-7>

- Learn How the Memory is Used by Windows
- What's Got the Disk? Monitor Disk Activity
- What's Using the Network and the Internet

Objectifs Identifier les principaux éléments du système Windows : processus, PID, *user name*, session, *integrity level*, *handle*, *dll*,

Action Effectuer un *Switch User* pour passer dans la session **albert**
Important Ne pas fermer la session **ursula**
 Exécuter **procexp.exe** (depuis dossier copié sur bureau) avec les droits administrateur (Run as administrator)

Repérer la ligne qui définit les paramètres affichés

| Process | PID | CPU | Description | Company Name | Session | User Name | Integrity |
|---------|-----|-----|-------------|--------------|---------|-----------|-----------|
|---------|-----|-----|-------------|--------------|---------|-----------|-----------|

Clic-droit sur cette ligne, pour ajouter les colonnes *User Name*, *Session* et *Integrity Level*

Select the columns that will appear on the Process view of Process Explorer.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Process Name | <input type="checkbox"/> Window Title |
| <input checked="" type="checkbox"/> PID (Process Identifier) | <input type="checkbox"/> Window Status |
| <input checked="" type="checkbox"/> User Name | <input checked="" type="checkbox"/> Session |
| <input checked="" type="checkbox"/> Description | <input type="checkbox"/> Command Line |
| <input checked="" type="checkbox"/> Company Name | <input type="checkbox"/> Comment |
| <input type="checkbox"/> Verified Signer | <input type="checkbox"/> DEP Status |
| <input type="checkbox"/> Version | <input checked="" type="checkbox"/> Integrity Level |
| <input type="checkbox"/> Image Path | <input type="checkbox"/> Virtualized |
| <input type="checkbox"/> Image Type (64 vs 32-bit) | <input type="checkbox"/> ASLR Enabled |

Par défaut, les processus sont classés dans l'ordre chronologique de démarrage (*boot*). Vous pouvez retrouver cet affichage en sélectionnant *View – Show Process Tree*

Q_3a Identifier les principaux processus à partir du *slide* 15

Q_3b Lesquels utilisent le CPU ?

Q_3c Utiliser les colonnes *Session* et *User Name* pour regrouper ces processus dans des catégories

Q_3d Identifier les processus associés à des services, aidez-vous des lignes en rose



Action Démarrer *Notepad* (*Start – All Programs – Accessories – Notepad*) pour visualiser l’affichage dynamique vert.

Recherche ce processus dans procexp

Effectuer un clic-droit – *Propriétés* pour parcourir les onglets suivants



Q_3e Qu’avez-vous appris ?

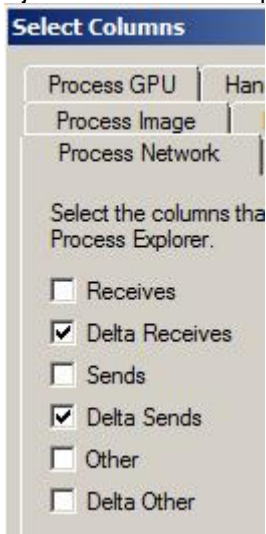
Action Utiliser   pour activer l’affichage du bas et visualiser les *DLLs* et *Handles*

Q_3f Quelles sont les clés de registre utilisées par ce processus ?

Q_3g Quelle est la version utilisée de kernel32.dll ?

Action Fermer *Notepad* pour visualiser l’affichage dynamique rouge

Action Ajouter 2 colonnes supplémentaires pour afficher l’activité réseau



Lancer Le navigateur Internet Explorer

Q_3h Quel est le processus Internet Explorer qui communique ?

Remarque Vous pouvez observer une activité réseau sur divers services

- Introduction** *Mandatory Integrity Control* implémente l'axiome **no write up** du modèle Biba avec 4 niveaux : *System – High – Medium – Low*
- Chaque processus possède un niveau d'intégrité (niveau de confiance) hérité du compte qui l'a démarré ; ainsi un processus ayant le niveau *High* ne peut pas écrire (modifier) un processus de niveau *System*.
- Contrôle** Vous avez besoin pour la suite de ce travail de
- Une session établie avec compte **ursula**
 - Une session établie avec compte **albert**
 - Un *Command Prompt* ouvert dans la session **ursula**
 - Un *Command Prompt* ouvert dans la session **albert**
 - Un *Command Prompt* ouvert avec les droits administrateur dans la session **albert**
 - *Process Explorer* dans la session **albert**
- Objectif** Consulter le niveau d'intégrité des processus en cours d'exécution à partir de la colonne *Integrity Level*
- Q_4a** Quel est le niveau d'intégrité d'explorer.exe appartenant à ursula ?
- Q_4b** Quel est le niveau d'intégrité d'explorer.exe appartenant à albert ?
- Q_4c** Quel est le niveau d'intégrité de *cmd.exe* lancé par ursula ?
- Q_4d** Quel est le niveau d'intégrité de *cmd.exe* lancé sans élévation de privilèges par albert ?
- Q_4e** Quel est le niveau d'intégrité de *cmd.exe* lancé avec élévation de privilèges par albert ?
- Q_4f** Quel est le niveau d'intégrité de *procexp.exe* lancé par albert ?
- Q_4g** Quel est le niveau d'intégrité de *csrss.exe* appartenant à la session d'ursula ?
- Q_4h** Quel est le niveau d'intégrité de *csrss.exe* appartenant à la session d'albert ?
- Q_4i** Quelle conclusion tirer de ces différents tests ?

- Objectif** Supprimer le droit *Change the time zone* à ursula
- Action** Dans la session **albert**
Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Continue – Security Settings – Local Policies – User Rights Assignment
 Retirer le groupe *Users* du droit *Change the time zone*
Redémarrer le poste
- Test** Ouvrir une session **ursula**
 Constater qu'il n'est plus possible de changer *time zone*
 (clic sur heure – *Change date and time settings...* - *Change time zone...*)
- Q_5a** Proposer une autre méthode pour contrôler que cet utilisateur ne dispose plus de ce droit

- Introduction** Les documents des utilisateurs sont souvent stockés sur un serveur de fichiers pour des raisons de sécurité (confidentialité, disponibilité, sauvegarde, administration,...).
 Il est conseillé de créer une partition pour ce type de données afin qu'elles ne se trouvent pas dans la partition système (C:) puis de donner des autorisations spécifiques grâce aux mécanismes du système de fichiers NTFS.
- Remarque** Les autorisations NTFS seront effectuées en local sur votre PC, le principe étant exactement identique sur un serveur de fichiers.
- But 6a** Réduire la taille de la partition C: et créer une partition E :
- Action** Dans la session **albert**, clic-droit sur Computer – Manage – Storage – Disk Management
 Clic-droit sur Windows (C:), Shrink Volume, space to shrink in MB = 100000, valider par shrink
 Clic-droit sur l'espace non alloué – New Simple Volume – Next – Next – Assign letter = E – Next – Format this volume, FS = NTFS, Quick format = true – Next - Finish
 Ouvrir la partition E:, puis clic-droit *New – Folder puis créer votre dossier E:\Test*
- But 6b** Visualiser les autorisations (qui peut accéder à ce dossier ?)
- Action** Clic-droit sur ce dossier Test – *Properties – Security*
- Q_6b** Déterminer les autorisations NTFS pour chaque groupe ?
 Quel groupe possède le minimum d'autorisations ?
- But 6c** Créer un fichier texte dans le dossier Test
- Action** Ouvrir le dossier E:\Test puis clic-droit *New – Text Document*
- But 6d** Contrôler les autorisations NTFS du fichier créé
- Action** Clic-droit sur ce fichier texte – *Properties – Security*
- Q_6d** Quelles sont les différences sur les autorisations NTFS de ce fichier par rapport à son dossier parent ?
- But 6e** Comprendre l'appartenance à plusieurs groupes d'autorisations NTFS
- Action** Ouvrir le fichier texte puis taper abc
 Sauver les modifications
 Retourner dans la session **ursula**
 Tenter de modifier le fichier texte créé ci-dessus

- Q_6e** Le fichier texte peut-il être modifié avec un compte utilisateur ? Pourquoi ?
- But 6f** Contrôler les autorisations d'un utilisateur
- Action** Dans la session **albert**
Clic-droit sur le fichier texte puis *Properties – Security – Advanced – Effective Permissions Select – Advanced – Find Now*
Choisir Ursula puis *OK*
- Q_6f** Quelle autorisation ne possède pas Ursula pour ce fichier ?
- But 6g** Supprimer le principe d'héritage à l'arborescence de E:\Test
- Action** Dans la session **albert**
Clic-droit sur le dossier Test puis *Properties – Security Advanced... Change Permissions...*
Décocher *Include inheritable permissions from this object's parent*
Puis *Remove – OK – Yes – OK – OK*
- Constat** Tous les groupes ont disparu
- But 6h** Ajouter albert pour lui donner toutes les autorisations sur ce dossier E:\Test
- Action** Clic-droit sur le dossier E:\Test puis *Properties – Security Edit - Add... - Advanced... - Find Now*, choisir le compte albert, puis *OK – OK*
Donner toutes les autorisations au compte albert (*Full Control*)
Fermer toutes les fenêtres de propriétés NTFS en cliquant sur *OK*
- Remarque** Utiliser, pour ce travail, les autorisations NTFS standards :
- Full control
 - Modify
 - Read & execute
 - List folder contents
 - Read
 - Write
- But 6i** Donner à Ursula les autorisations NTFS minimales sur le dossier et les fichiers suivants
E:\Test pour parcourir ce dossier
E:\Test\Read.txt pour lire ce fichier
E:\Test\calc.exe pour exécuter calc.exe copié depuis C:\Windows\System32\calc.exe
E:\Test\ReadWrite.txt pour lire & écrire dans ce fichier
- Q_6j** Ursula peut-elle créer un fichier ou un dossier dans E:\Test ?
- Q_6k** Ursula peut-elle copier un fichier dans E:\Test ?
- Q_6l** Ursula peut-elle supprimer un fichier situé dans E:\Test ?
- Q_6m** Quelles autorisations avez-vous données à E:\Test ?
- Q_6n** Quelles autorisations avez-vous données à E:\Test\Read.txt ?
- Q_6o** Quelles autorisations avez-vous données à E:\Test\calc.exe ?
- Q_6p** Quelles autorisations avez-vous données à E:\Test\ReadWrite.txt ?
- But 6q** Déterminer les autorisations sur la partition système C:\Windows
- Q_6q** Indiquer les valeurs pour le groupe Users
- But 6r** Déterminer toutes les autorisations sur la partition système C:\Windows
- Actions** Sélectionner *Advanced* puis *Effective Permissions*
- Q_6r** Indiquer toutes les valeurs pour le groupe Users

- Remarque** Bien que Win7 améliore la sécurité de WinXP, les utilisateurs ont toujours accès à certains exécutables comme l'éditeur de la base de registre regedit dont ils n'ont pas besoin.
- But 7a** Constater qu'un membre du groupe Users peut exécuter regedit
- Action** Dans une session **ursula**
Start – Run... – regedit.exe
- Remarque** Avec Windows 7, un propriétaire « TrustedInstaller »(Owner) est assigné pour les exécutables du système. Il s'agit d'un service qui est utilisé lors de la mise à jour des fichiers systèmes par Windows Update ou lors de l'application d'une mise à jour par un autre moyen.
- But 7b** Prendre possession de l'exécutable **regedit.exe**
- Action** Retourner dans la session **albert**
Dans **c:\windows**
Clic droit sur **regedit.exe** – *Propriétés*
Onglet *Security – Advanced* – Onglet *Owner – Edit*
Sélectionner l'utilisateur albert – OK (4 fois)
- Q_7b** Peut-il y avoir plusieurs propriétaires d'un objet NTFS ?
- But 7c** Interdire l'usage de regedit au groupe Users
- Action** Dans **c:\windows**, clic droit sur **regedit.exe** – *Propriétés*
Onglet *Security – Advanced* – *Permissions – Change Permissions...*
Supprimer le groupe *Users*
OK – Yes – OK (2 fois)
- Test 7c** Tester avec le compte ursula
Tester avec le compte albert
- But 7d** Déterminer la raison pour laquelle albert ne peut plus exécuter regedit ?
- Q_7d** Quelles sont les propriétés effectives du groupe Administrators ?
- Explication** **albert ne peut plus faire d'élévation de privilège en cliquant sur regedit mais il peut lancer regedit.exe depuis un cmd – run as administrator !!!
Ce comportement est bizarre A tester avec SP1**
- But 7e** Ajouter l'utilisateur albert dans les autorisations
Clic droit sur **regedit.exe** – *Propriétés*
Onglet *Security – Advanced* – *Permissions – Change Permissions...*
Add – Advanced – Find Now – albert – OK – OK
OK – Yes – OK (2 fois)
- | Permissions: | Allow |
|--------------------------------|-------------------------------------|
| Full control | <input type="checkbox"/> |
| Traverse folder / execute file | <input checked="" type="checkbox"/> |
| List folder / read data | <input checked="" type="checkbox"/> |
| Read attributes | <input checked="" type="checkbox"/> |
| Read extended attributes | <input checked="" type="checkbox"/> |
| Create files / write data | <input type="checkbox"/> |
| Create folders / append data | <input type="checkbox"/> |
| Write attributes | <input type="checkbox"/> |
| Write extended attributes | <input type="checkbox"/> |
| Delete | <input type="checkbox"/> |
| Read permissions | <input checked="" type="checkbox"/> |
- Test 7e** Tester avec le compte ursula puis avec celui d'albert

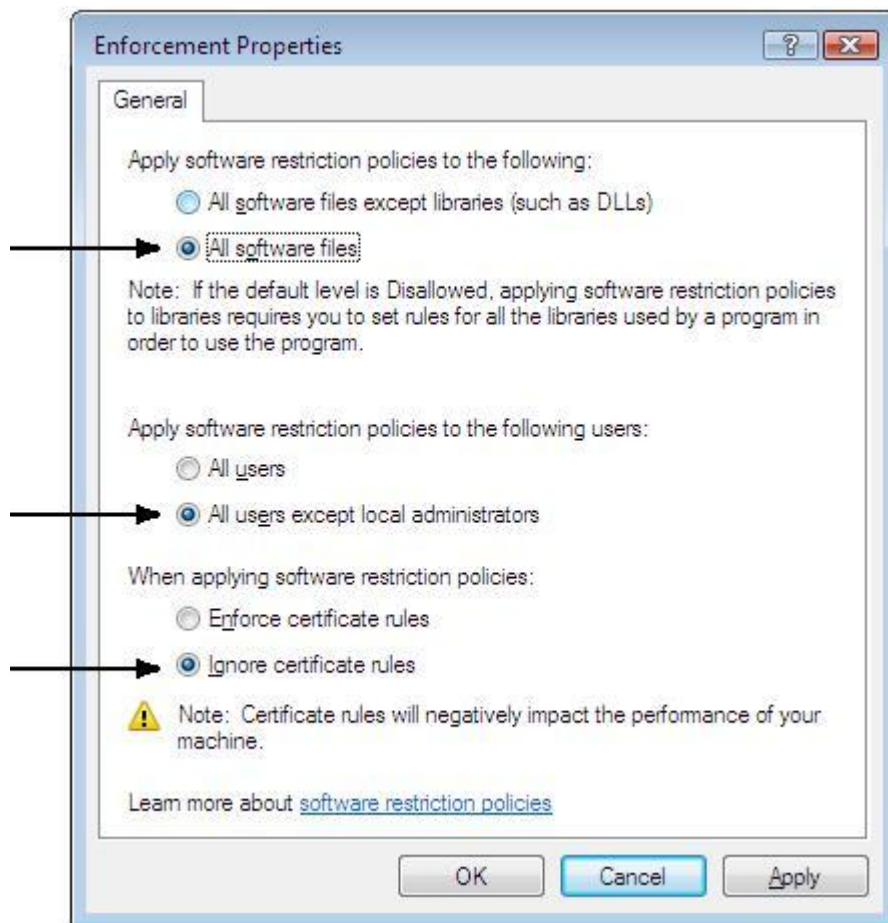
| | |
|-----------------|---|
| But 8a | Auditer les événements des catégories <i>Audit policy change</i> et <i>Audit system events</i> |
| Action | Dans la session albert <i>Start – Administrative Tools – Local Security Policy</i> <i>Security Settings – Local Policies – Audit Policy</i> Définir les valeurs suivantes : <i>Audit policy change : Success & Failure</i> <i>Audit system events : Success & Failure</i> |
| But 8b | Réinitialiser le journal d'événement (<i>Event Viewer</i>) : |
| Action | Exécuter le journal d'événement dans <i>Start –Administratives Tools - Event Viewer</i> <i>Windows Logs - clic-droit sur Application puis Clear Log... - Clear</i> Répéter l'opération sur <i>Security</i> et <i>System</i> |
| Remarque | On constate que la suppression des <i>logs</i> est consignée dans <i>Security</i> et <i>System</i> |
| But 8c | Auditer les événements des catégories <i>Audit logon events</i> et <i>Audit account management</i> |
| Action | Définir les valeurs suivantes : <i>Audit logon events : Success & Failure</i> <i>Audit account management : Success & Failure</i> |
| Remarque | On constate que les changements sont consignés dans <i>Security</i> (presser <i>F5</i> pour rafraîchir le journal d'évènement). |
| But 8d | Désactiver le compte ursula |
| Action | Fermer la session <i>ursula</i> si elle est encore ouverte : Sur le bureau, clic-droit sur <i>Computer</i> puis <i>Manage – Local Users and Groups – Users</i> . Dans les propriétés du compte <i>ursula</i> , sélectionner <i>Account is disabled</i> . |
| Remarque | On constate que la désactivation du compte <i>ursula</i> est consignée dans <i>Security</i> . |
| Test | Effectuer les points suivants : <ul style="list-style-type: none">▪ Réactivez le compte <i>ursula</i>▪ Essayer d'ouvrir une session avec le compte utilisateur <i>ursula</i>▪ Ouvrir une session albert Consulter les <i>Security</i> du journal d'événement (<i>Start – Settings – Control Panel – Administrative Tools - Event Viewer</i>) |
| But 8e | Activer les logs sur le fichier <i>E:\Test\Read.txt</i> |
| Action | Dans une session albert Clic-droit sur l'objet – <i>Properties – Security – Advanced – Auditing - Continue</i> <i>Add – Advanced – Find Now</i> Sélectionner un compte ou un groupe Définir le type d'accès (<i>read, write, ...</i>) et le résultat (<i>success</i> et/ou <i>failure</i>) Dans <i>Audit Policy</i> , configurer correctement le paramètre <i>Audit object access</i> |
| Test | Contrôler que vous obtenez bien une trace des activités dans <i>Event Viewer</i> |

But 9a Constaté qu'il est possible de lancer un exécutable depuis le bureau d'un utilisateur

Action Dans la session **utilisateur**
Double cliquer sur **procexp.exe** situé sur le bureau

But 9b Implémenter SRP pour autoriser uniquement l'exécution de programmes situés dans le « système root » (C:\Windows) ou dans le répertoire C:\Program Files

Action Dans la session **albert**
Start – Administrative Tools – Local Security Policy – Security Settings,
clic droit sur *Software Restriction Policies* puis *New Software Restriction Policies*
Double-cliquer sur *Enforcement* et appliquer les paramètres suivants :



Double-clic sur *Trusted Publisher*

Sélectionner *Define these policies settings* et conserver les paramètres par défaut.

(Si les certificats sont utilisés, sélectionner également les deux cases de la partie *Certificate verification*)

OK

Dans *Security Levels* double-cliquer sur *Disallowed – Set as Default – Yes – OK*

Dans *Additional Rules*, laisser les deux règles :

```
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%
```

Clic droit sur *Additional Rules* puis *New Path Rule...*

Dans *Path:* entrer **.lnk* (Cette règle doit être ajoutée, car les raccourcis font partie des exécutables.)

Dans *Security level* sélectionner *Unrestricted*

OK

Redémarrer le poste

Test Vérifier qu'il n'est plus possible de lancer un exécutable depuis le bureau d'un utilisateur