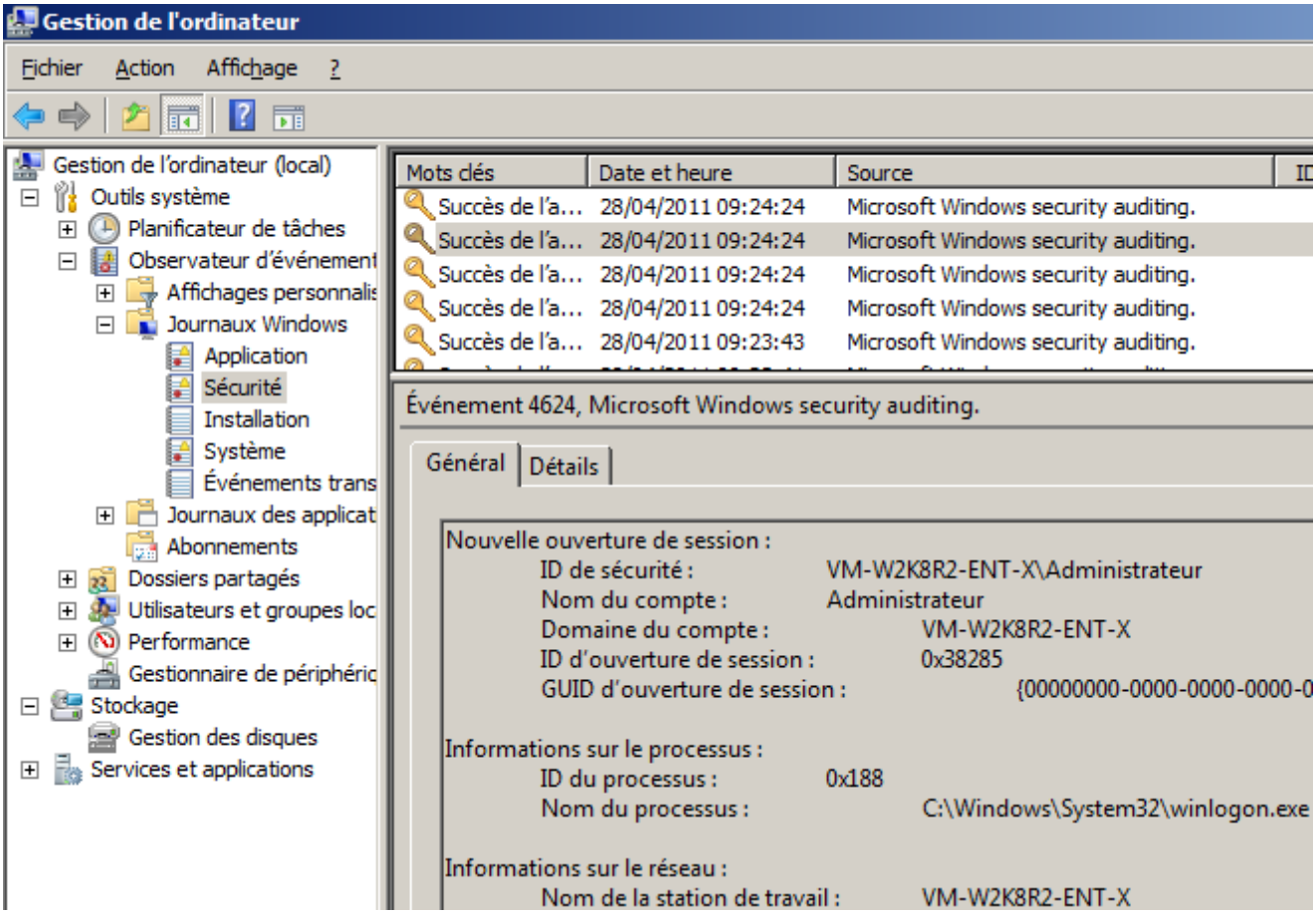
Un observateur d’événements aveugle…

blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle

gentilkiwi 28/04/2011

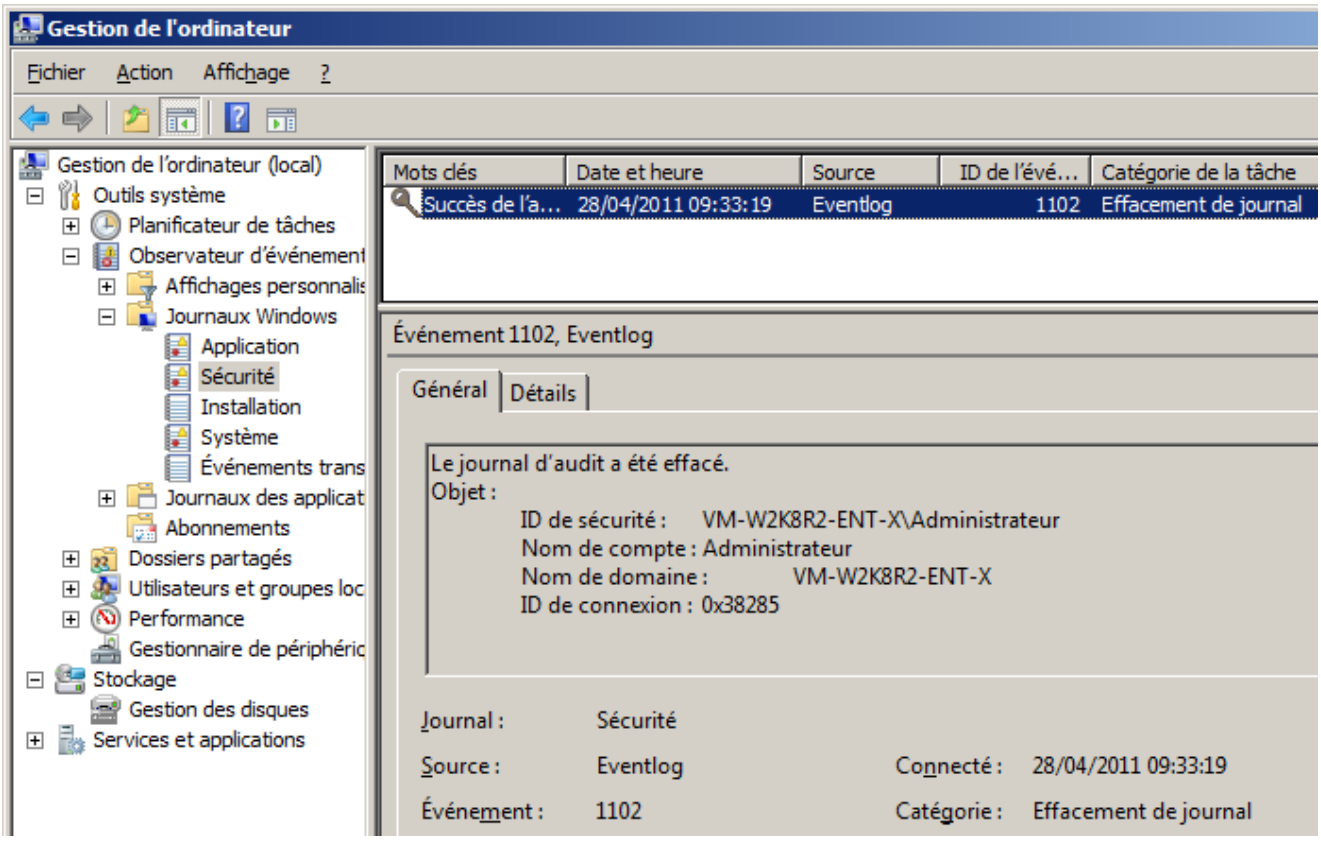
L’observateur d’événements de Windows est un service permettant au système et programmes de centraliser leurs remontées d’informations.

Par exemple, l’audit de sécurité du poste y est ainsi consigné pour la plus grande joie des administrateurs :



Un rapporteur

Ce service est aussi un rapporteur, il n'hésitera pas à vous trahir lorsque vous voudrez faire disparaitre vos traces…



Il est ainsi *difficile* d'avoir un journal de sécurité vide.

Le code

Que ce soit par un callback RPC ou lors de l'effacement d'un journal, une fonction traître est appelée…

En NT 5

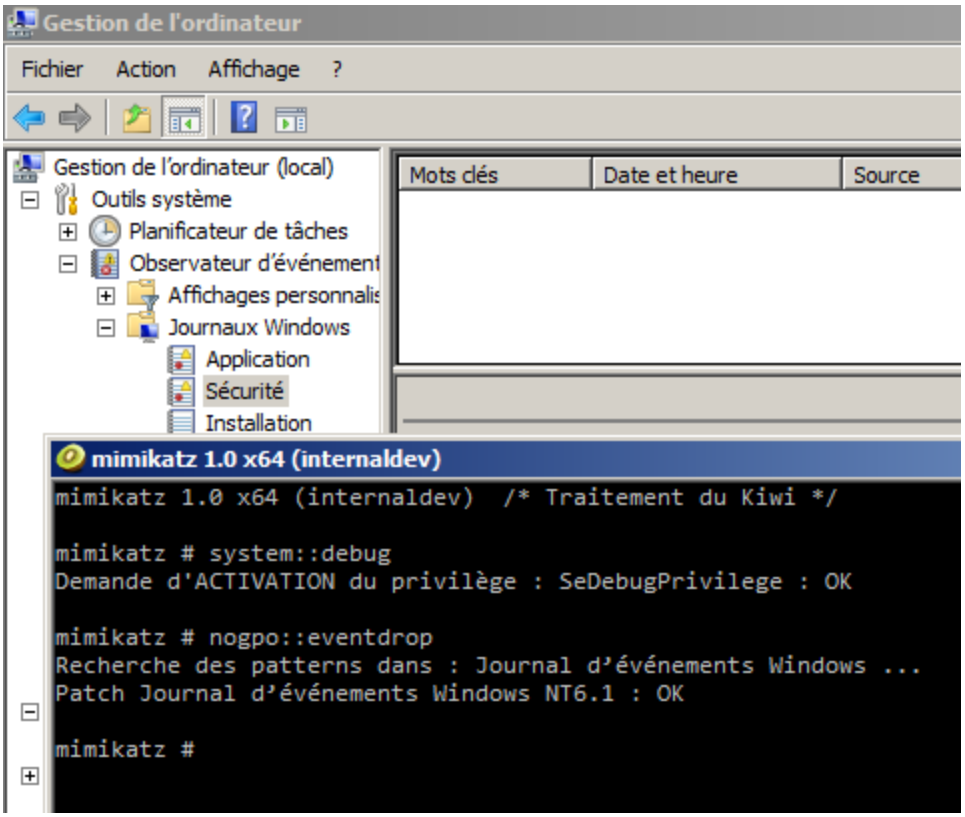
```
.text:756F2F8D ; __stdcall PerformWriteRequest(x)
.text:756F2F8D _PerformWriteRequest@4 proc near         ; CODE XREF:
ElfPerformRequest(x)+48p
.text:756F2F8D                                          ; WriteQueuedEvents()+70p
```

En NT 6

```
.text:715D2841 ; private: void __thiscall Channel::ActualProcessEvent(class
BinXmlReader &)
.text:715D2841 ?ActualProcessEvent@Channel@@AAEXAAVBinXmlReader@@@Z proc near
.text:715D2841                                          ; CODE XREF:
Channel::ProcessEvent(BinXmlReader &)+52p
.text:715D2841                                          ;
Channel::FireEventIntoLog(Buffer &,_EVENT_DESCRIPTOR const &,void *)+15Cp
.text:715D2841                                          ;
Channel::ProcessLogFull(BinXmlReader &)+1A2p
.text:715D2841
```

Sous NT 6, la fonction doit être interceptée à moins bas niveau que NT 5 afin d'éviter au maximum les programmes et tâches pouvant êtres liés à l'écriture de l'événement. L'événement n'ayant pas été réellement créé, cela peut vexer notre service…

Aidons l'observateur à moins observer



Et voilà un journal d'événements beaucoup moins bavard :), même lors de son arrêt… le premier événement au reboot sera donc : `Windows démarre.`

…comme toujours, ça sera dans `mimikatz 1.0` *…*