

# Un observateur d'événements aveugle...

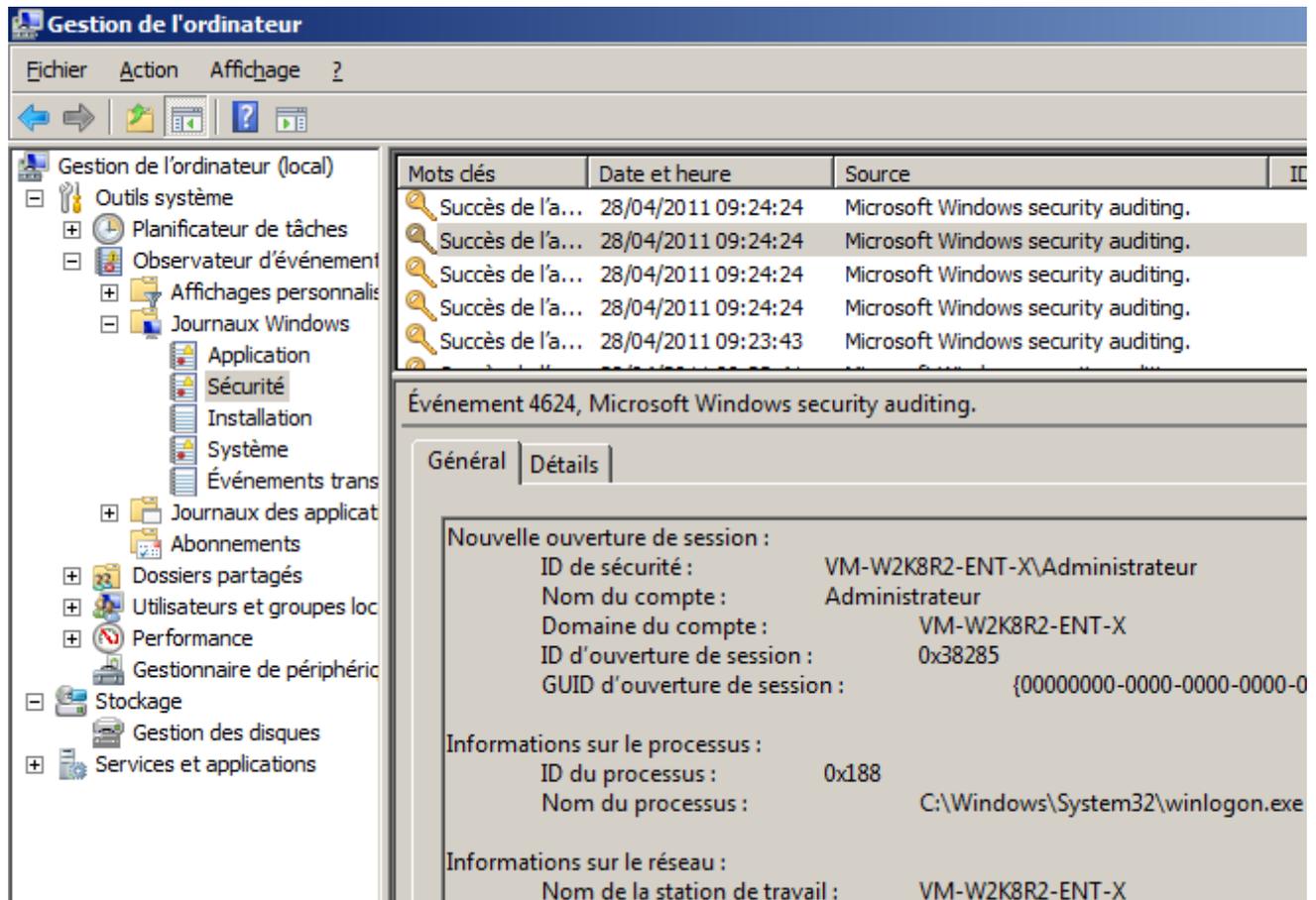
[blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle](http://blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle)

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 :



The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Gestion de l'ordinateur' tree with 'Observateur d'événement' expanded to 'Journaux Windows' > 'Sécurité'. The main pane shows a list of events with the following columns: Mots clés, Date et heure, Source, and ID. The selected event is 'Événement 4624, Microsoft Windows security auditing.' The details pane shows the following information:

Nouvelle ouverture de session :	
ID de sécurité :	VM-W2K8R2-ENT-X\Administrateur
Nom du compte :	Administrateur
Domaine du compte :	VM-W2K8R2-ENT-X
ID d'ouverture de session :	0x38285
GUID d'ouverture de session :	{00000000-0000-0000-0000-0000-0000-0000-0000-0000}

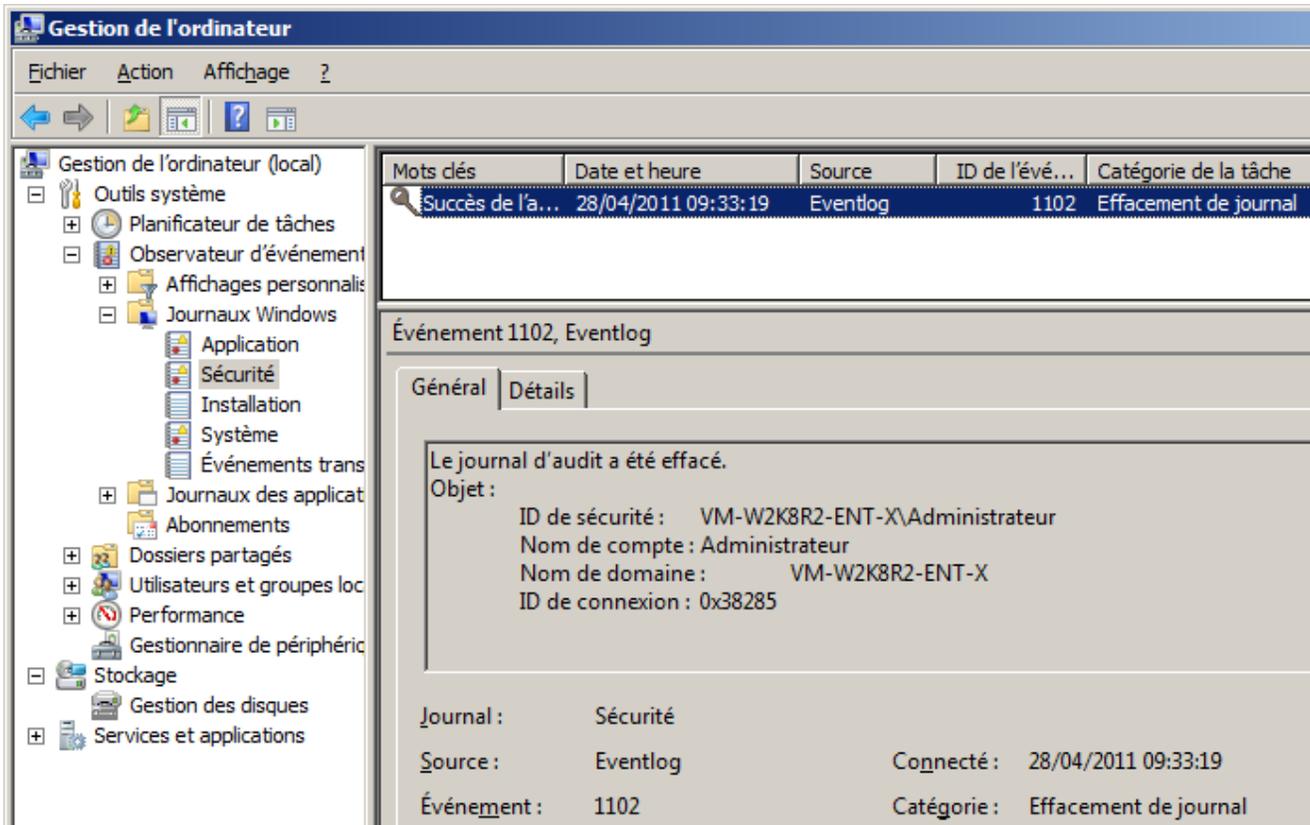
Informations sur le processus :	
ID du processus :	0x188
Nom du processus :	C:\Windows\System32\winlogon.exe

Informations sur le réseau :	
Nom de la station de travail :	VM-W2K8R2-ENT-X

## Un rapporteur

Ce service est aussi un rapporteur, il n'hésitera pas à vous trahir lorsque vous voudrez faire disparaître 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

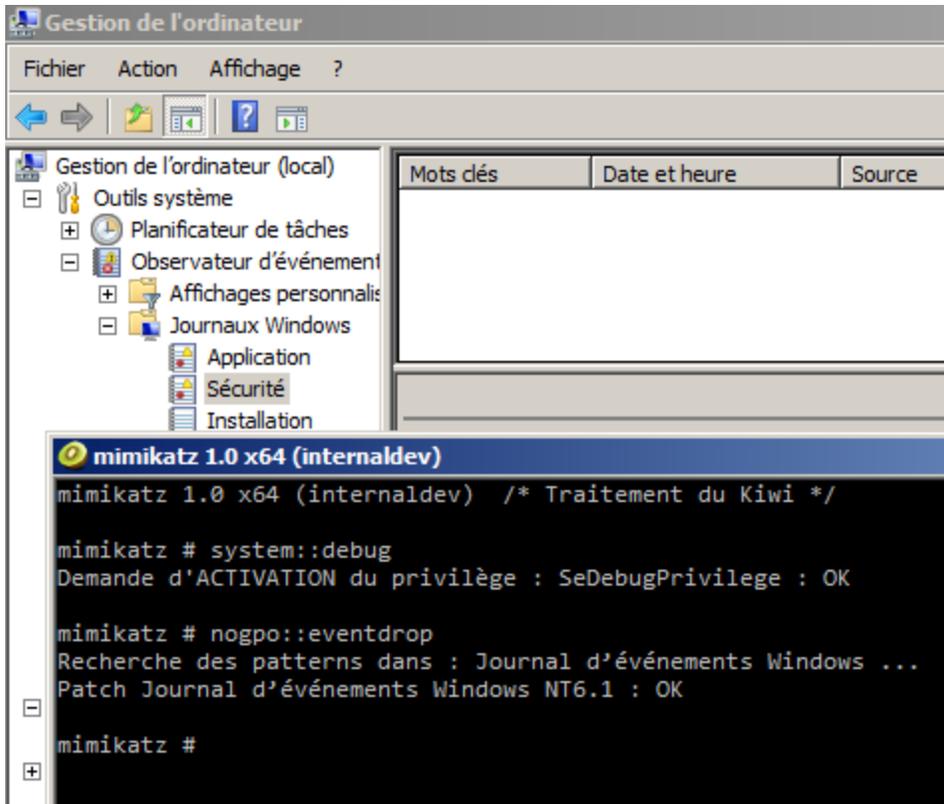
```
.text:756F2F8D ; __stdcall PerformWriteRequest(x)
.text:756F2F8D _PerformWriteRequest@4 proc near ; CODE XREF:
ElfPerformRequest(x)+48p
.text:756F2F8D ; WriteQueuedEvents()+70p
```

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 être 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** ...