

squad



MIX YOUR  
**TALENT**

Forensics Windows, Mac et Linux



Windows



Mac



Linux



## Windows

### Historique du système de fichier de Windows

#### Histoire [\[ modifier \]](#) [\[ modifier le code \]](#)

Dans le milieu des années 1980 Microsoft et IBM ont formé un projet conjoint visant à créer la prochaine génération de [système d'exploitation](#) graphique. Il en résulta OS/2, mais Microsoft et IBM, en désaccord sur de nombreux points, se sont finalement séparés. OS/2 est resté un projet d'IBM. Microsoft a commencé à travailler sur Windows NT. Le système de fichiers de OS/2, [HPFS](#), comportait de nombreuses nouvelles fonctionnalités importantes. Lors de la création de son nouveau système d'exploitation, Microsoft a emprunté beaucoup de ces concepts pour NTFS<sup>2</sup>. Probablement en raison de cette origine commune, NTFS et HPFS partagent le même code d'identification de type de [partitionnement de disque](#) (07). Partager un identifiant est inhabituel, car il y avait des dizaines de codes disponibles, et d'autres systèmes de fichiers importants ont leur propre code. FAT en a plus de neuf (un pour chacune des [FAT12](#), [FAT16](#), [FAT32](#), etc.). Des algorithmes permettant d'identifier le système de fichiers dans un type de partition 07 doivent effectuer des contrôles supplémentaires. Il est également clair que NTFS doit une partie de sa conception architecturale à [Files-11](#) utilisé par [VMS](#). Cela est sûrement dû au fait que [Dave Cutler](#) fut le chef principal des Windows NT et VMS à la fois.

#### Versions [\[ modifier \]](#) [\[ modifier le code \]](#)

Le format sur disque de NTFS a cinq versions publiées :

- v1.0 avec [Windows NT 3.1](#), publiée mi-1993 ;
- v1.1 avec [Windows NT 3.5](#), publiée en automne 1994 ;
- v1.2 avec [Windows NT 3.51](#) (mi-1995) et [Windows NT 4.0](#) (mi-1996) (parfois dénommé « NTFS 4.0 » parce que la version du pilote du système de fichiers est la 4.0) ;
- v3.0 à partir de [Windows 2000](#) (« NTFS v5.0 » ou « NTFS5 »)<sup>3</sup> ;
- v3.1 à partir de [Windows XP](#) (automne 2001 ; « NTFS v5.1 »).



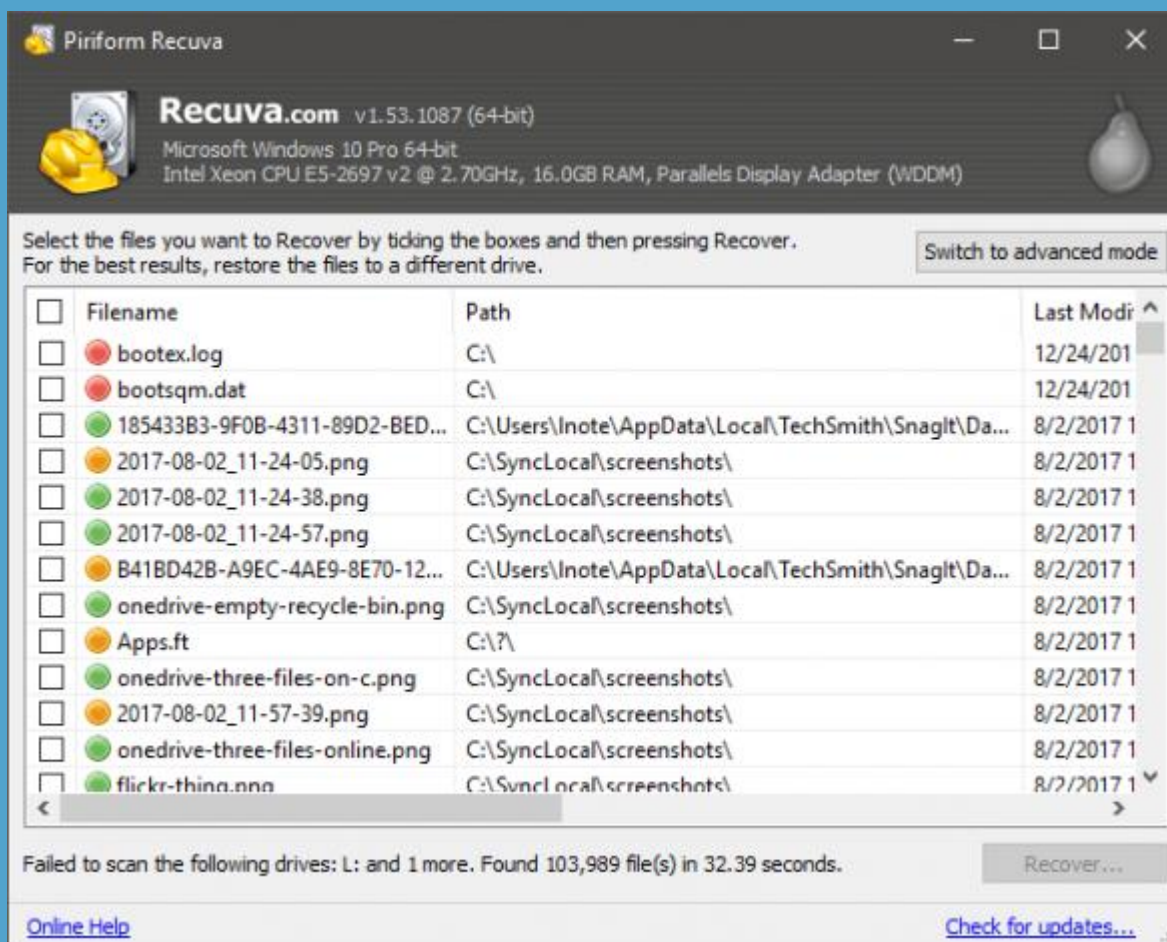


## Windows

### Récupération de fichiers effacés de la Corbeille

Pourquoi il est possible de récupérer des fichiers effacés de la corbeille sur Windows ?

- A. Car la corbeille est dans une partition dédiée
- B. Car le fichier est encore accessible dans la mémoire vive
- C. Car lors de la suppression d'un fichier, Windows se contente de modifier l'index
- D. Car une sauvegarde du fichier est effectué par Windows avant sa suppression





## Windows

### Récupération de fichiers effacés de la Corbeille

Pourquoi il est possible de récupérer des fichiers effacés de la corbeille sur Windows ?

- A. Car la corbeille est dans une partition dédiée
- B. Car le fichier est encore accessible dans la mémoire vive
- C. Car lors de la suppression d'un fichier, Windows se contente de modifier l'index
- D. Car une sauvegarde du fichier est effectué par Windows avant sa suppression

## Approche logicielle [ [modifier](#) | [modifier le code](#) ]

La récupération de données par logiciel a de multiples motivations : les plus courantes vont de l'erreur humaine aux virus, en passant par les différents degrés de malveillance, d'espionnage et d'enquêtes policières. Par exemple, dans l'[affaire Clearstream](#), une partie de l'enquête s'est appuyée sur les données récupérées sur l'ordinateur du [général Rondot](#), données que ce dernier avait simplement effacées<sup>1</sup>.

En informatique, le [système d'exploitation](#) découpe en morceaux les ressources auxquelles il accède, et les retrouve grâce à un index. Ainsi, un système d'exploitation voit un disque dur comme une encyclopédie où chaque demande de l'utilisateur correspond à utiliser la table des matières de l'encyclopédie. Quand l'utilisateur demande d'effacer une structure (un fichier ou une partition par exemple), le système d'exploitation ne le détruit pas directement : il se contente de modifier l'index ; effacer un article équivaut à retirer l'article de la table des matières. L'article effacé est cependant toujours présent au milieu des pages de l'encyclopédie.

Les espaces libres ne sont remplacés que lorsqu'un autre contenu y est déposé.

On peut classer les outils logiciels de récupération en trois familles :

### Les outils basés sur le système d'exploitation

L'idée de base de ces approches est de travailler au niveau des index maintenus par le système d'exploitation.

Grossièrement, ces approches vont essayer de détecter les altérations récentes apportées à la table des matières de l'encyclopédie et d'en déduire les structures (fichiers ou partitions) récupérables. Par exemple, [MS-DOS](#) offrait le programme de restauration "[undelete](#)" et "[unformat](#)".

### Les outils basés sur la structure effacée

L'idée de base consiste à parcourir la totalité du média en essayant de détecter le début et la fin des structures qu'on cherche à récupérer. Grossièrement, ces approches vont donc ouvrir chaque tome de l'encyclopédie, parcourir chaque page et essayer de déterminer le début et la fin de chaque article.

### Les outils mixtes

Les outils mixtes mélangent les deux approches : dans un premier temps, ils explorent les index du système d'exploitation afin d'en déduire une première approximation sur l'emplacement des données effacées. Dans un second temps, ils scannent le voisinage correspondant au début et à la fin des structures à restaurer afin d'arriver à affiner la première approximation.



## Windows Master File Table

AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- \\PHYSICALDRIVE0
- Windows 10 [NTFS]
- [root]
- \$BadClus
- \$Extend
- \$Recycle.Bin
- \$Secure
- \$UpCase
- BGInfo
- Boot
- Documents and Settings
- PerfLogs
- pgData96
- Program Files
- Program Files (x86)

File List

Name	Size	Type	Date Modified
\$Boot	8	Regular File	10/23/2017 4:5...
\$I30	8	NTFS Index All...	1/31/2019 2:59...
\$LogFile	56,016	Regular File	10/23/2017 4:5...
\$MFT	197,632	Regular File	10/23/2017 4:5...
\$MFTMirr	4	Regular File	10/23/2017 4:5...
\$Secure	1	Regular File	10/23/2017 4:5...
\$TXF_DATA	1	NTFS Logged ...	1/31/2019 2:59...
\$UpCase	128	Regular File	10/23/2017 4:5...
\$Volume	0	Regular File	10/23/2017 4:5...
bootmgr	389	Regular File	11/7/2018 5:55...
BOOTNXT	1	Regular File	9/29/2017 1:41...
BOOTSECT.BAK	8	Regular File	10/23/2017 4:5...
pagefile.sys	720,896	Regular File	1/31/2019 5:45...

Custom Content Sources

Evidence:File System|Path|File

Options

New Edit Remove Remove All Create Image

Properties Hex Value Inter... Custom Conte...

Cursor pos = 0; clus = 786432; log sec = 6291456; phy sec = 6293504

For User Guide, press F1

En NTFS, tous les fichiers, répertoires et métadonnées (nom de fichier, date de création, permissions d'accès ACL, taille) sont stockés comme des métadonnées dans la Master File Table (MFT).



# Windows

## Base de registre Windows

La base de registre est partagée en différentes sections logiques. Elles sont généralement connues par les noms les définissant quand on y accède via l'interface graphique de Windows; les noms commencent tous par 'HKEY' (une abréviation de *Handle to a KEY*, gestionnaire de clé).

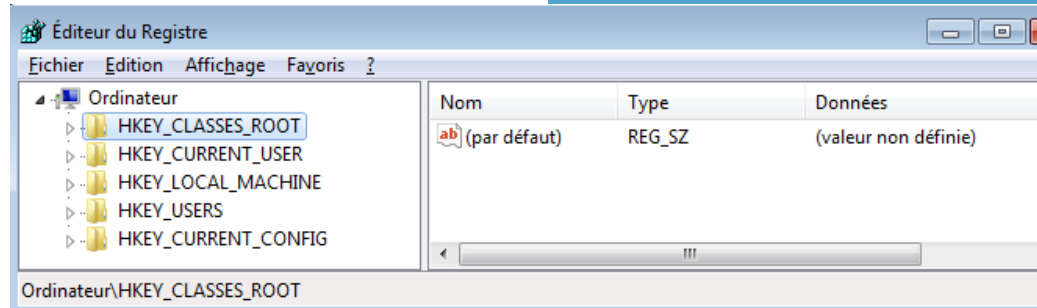
Les 2 HKEY de base sont :

- **HKEY\_LOCAL\_MACHINE (HKLM)** contient les informations qui sont générales à tous les utilisateurs de l'ordinateur :
  - Matériel
  - Sécurité
  - **SAM (Security Account Manager)**
  - Logicielle, la sous-branche "Classes" correspond à **HKEY\_CLASSES\_ROOT**
  - Système, elle contient notamment la sous-branche *CurrentControlSet* (NB : *CurrentControlSet\Control\Class* contient des informations sur les classes).
- **HKEY\_USERS** contient les informations spécifiques de chaque utilisateur. La sous-branche correspondant à l'utilisateur courant est l'équivalent de **HKEY\_CURRENT\_USER**. Attention, cette ruche n'est visible que si l'utilisateur associé est connecté

Les 4 autres HKEY sont

- **HKEY\_CURRENT\_CONFIG** contient des informations qui sont mises à jour immédiatement, elles sont régénérées après chaque boot.
- **HKEY\_CLASSES\_ROOT (HKCR)** contient les informations sur les applications enregistrées ; cela inclut entre autres les associations entre extensions de fichiers et identifiants de classe d'objet **OLE**, ce qui permet de lancer automatiquement l'exécutable correspondant. Cela correspond à **HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes**. Exemple : ".bat" et "XML" sont respectivement associés à "batfile" et "XML script engine".
- **HKEY\_CURRENT\_USER (HKCU)** contient les informations concernant l'utilisateur connecté. Ce n'est qu'une sous-branche de **HKEY\_USERS**.
- **HKEY\_PERFORMANCE\_DATA** (ou **HKEY\_DYN\_DATA** sous Windows 9x) générée dynamiquement (REGEDIT ne l'affiche pas). Vous pouvez voir ces données par l'intermédiaire de l'utilitaire perfmon.msc

Chacune de ces clés est divisée en sous-clé(s), qui peuvent contenir d'autre(s) sous-clé(s) et ainsi de suite, constituant toute une arborescence.







## Windows Shadow copy

**Shadow Copy** (aussi connu sous le nom **Volume Snapshot Service**, **Volume Shadow Copy Service**, ou **VSS**)<sup>1</sup> est une technologie incluse dans [Microsoft Windows](#) qui permet d'effectuer des sauvegardes automatiques ou manuelles de fichiers ou de disques, même s'ils sont en cours d'utilisation.

### Sommaire [masquer]

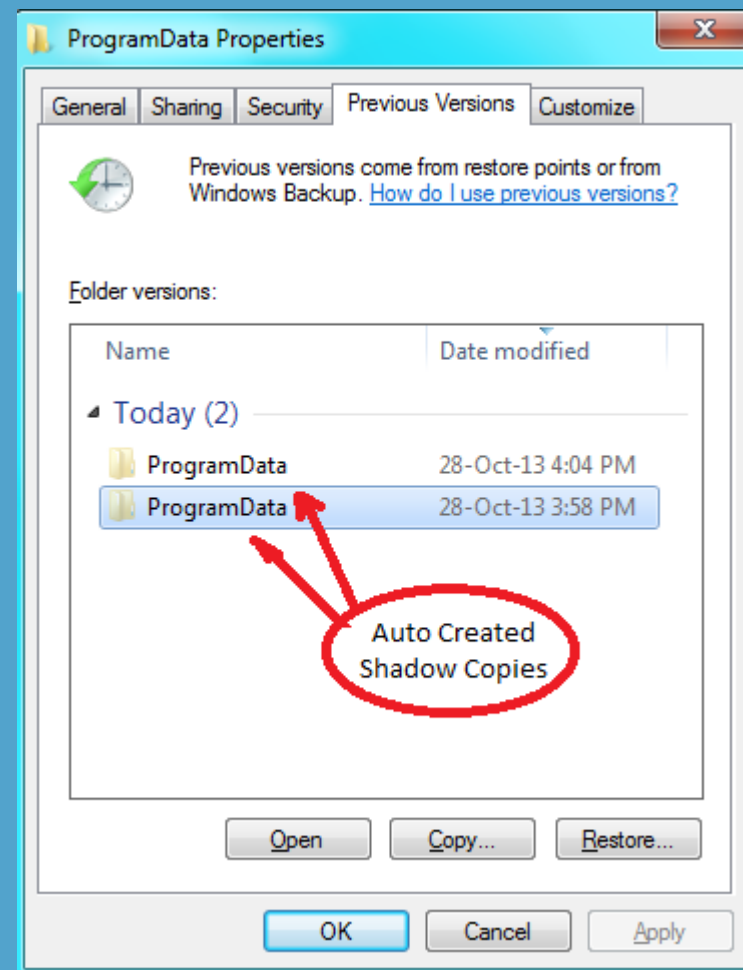
- 1 Historique
- 2 Description
- 3 Principe de fonctionnement
- 4 En environnement virtualisé
- 5 Utilisation
- 6 Bibliographie
- 7 Notes et références
- 8 Liens externes

## Historique [ modifier | modifier le code ]

Shadow Copy a été lancé à l'origine avec [Windows XP](#) (limité aux snapshots temporaires) et surtout [Windows Server 2003](#) (snapshots persistants), et a été adopté par les outils de sauvegarde des environnements Windows<sup>2</sup>. Shadow Copy est disponible aussi sur [Windows 7](#)<sup>3</sup> ("Cliclé instantané des volumes" en français)

## Description [ modifier | modifier le code ]

Shadow Copy est implémenté sous forme d'un service appelé « Volume Shadow Copy ». Un service VSS provider est également fourni pour être utilisé par les applications Windows. Shadow Copy nécessite un système de fichier de type [NTFS](#). Les copies peuvent être stockées sur un disque local ou sur un disque distant à travers le réseau.







## Windows

### Récupération du mot de passe de l'utilisateur-riche

Comment est-il possible pour l'investigateur-riche de récupérer le mot de passe de session Windows de l'utilisateur-riche ?

- A. Depuis les journaux Windows
- B. Depuis les métadonnées de la MFT
- C. Depuis le dump mémoire du processus lsass.exe
- D. En brute-forçant le hash de la base SAM
- E. En le demandant à l'utilisateur
- F. En le récupérant dans la base de registre SYSTEM
- G. En le trouvant en clair dans un fichier effacé
- H. En l'extrayant du service Volume Shadow Copy



## Windows

### Récupération du mot de passe de l'utilisateur-riche

Comment est-il possible pour l'investigateur-riche de récupérer le mot de passe de session Windows de l'utilisateur-riche ?

- A. Depuis les journaux Windows
- B. Depuis les métadonnées de la MFT
- C. Depuis le dump mémoire du processus lsass.exe  
Cela dépend de la configuration de la machine et surtout l'accès à un dump mémoire n'est pas toujours possible !
- D. En brute-forçant le hash de la base SAM  
Si la politique de mot de passe est bonne, c'est une solution peu envisageable.
- E. En le demandant à l'utilisateur  
A condition que l'utilisateur donne signe de vie.
- F. En le récupérant dans la base de registre SYSTEM
- G. En le trouvant en clair dans un fichier effacé  
Ou même dans des fichiers en clair (configuration, Excel...)
- H. En l'extrayant du service Volume Shadow Copy



## Windows Volatility

Volatility est un *framework* open-source d'inforensique de la mémoire pour de la réponse à incident et de l'analyse malware. Il est codé en Python et supporte Microsoft Windows, Mac OS X, et Linux.

```
root@kratos:~/Volatility# python vol.py -f stuxnet.vmem pslist | grep -i lsass
Volatility Foundation Volatility Framework 2.5
0x81e70020 lsass.exe          680    624    19    342    0    0 2010-10-29
17:08:54 UTC+0000
0x81c498c8 lsass.exe          868    668    2    23    0    0 2011-06-03
04:26:55 UTC+0000
0x81c47c00 lsass.exe          1928   668    4    65    0    0 2011-06-03
04:26:55 UTC+0000
root@kratos:~/Volatility# python vol.py -f stuxnet.vmem pslist -p 668
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start
-----
Exit
-----
0x82073020 services.exe ←      668 ← 624   21   431    0    0 2010-10-29
17:08:54 UTC+0000
```

Rappel : Si l'ordinateur prend en charge la veille prolongée, il remplira à la sortie de la veille la mémoire centrale avec le contenu d'un fichier du premier disque dur logique (c:\hiberfil.sys sous Microsoft Windows). Ce fichier est créé (si besoin) et rempli à la mise en veille prolongée de l'ordinateur.





## Windows BitLocker

**BitLocker Drive Encryption** est une spécification de protection des données développée par [Microsoft](#), et qui fournit le chiffrement de [partition](#).

BitLocker est inclus dans les versions *Entreprise* et *Intégrale* de [Windows Vista](#)<sup>1</sup>, dans toutes les éditions de [Windows Server 2008](#) et [Windows Server 2008 R2](#) sauf l'édition *Itanium*, dans les éditions *Entreprise* et *Intégrale* de [Windows 7](#) et, enfin, dans les éditions *Professionnelle* et *Entreprise* de [Windows 8](#), [8.1](#) et [Windows 10](#).

BitLocker fournit trois modes d'opération<sup>2</sup>. Les deux premiers modes requièrent un composant matériel [cryptographique](#) appelé [TPM \(Trusted Platform Module\)](#) (version 1.2 ou supérieure) et un [BIOS](#) compatible :

- **Transparent operation mode**: Mode d'opération transparent ; l'utilisateur n'a pas à s'identifier lors de la phase de pré-boot (avant l'exécution du [BIOS](#)) ;
- **User authentication mode**: Ce mode requiert que l'utilisateur s'identifie (par exemple avec un [périphérique USB](#)).

Le troisième mode ne requiert pas de composant matériel TPM :

- **USB-Key (clé USB)** : cela nécessite que l'accès à un périphérique USB soit possible AVANT le chargement du système d'exploitation (c'est une contrainte sur le BIOS)

Pour que BitLocker fonctionne, il faut que le [disque](#) contienne au moins deux [partitions](#) formatées [NTFS](#) :

- le volume système avec au moins 1,5 gigaoctet ;
- le volume de boot qui contient Vista, 7, 8(.1) Pro.

Depuis la version 1511 de [Windows 10](#) bitLocker prend en charge les clés XTS-AES 128 bits et 256 bits.<sup>3</sup>

## Autres logiciels de chiffrement de disques [\[ modifier | modifier le code \]](#)

- [TrueCrypt](#) (fonctionne sous Windows, Linux et Mac) mais n'est plus maintenu par ses auteurs depuis le 28 mai 2014 (voir l'article).
- [VeraCrypt](#) (fork open source de [TrueCrypt](#))
- Stormshield Endpoint Security (fonctionne sous WindowsXP, Windows Vista, Windows 7 32/64 bits)
- PGP Whole Disk Encryption (Symantec)
- [dm-crypt](#) Intégré au noyau Linux et remplaçant [Cryptoloop](#) [\(en\)](#)



# Windows

## Gestion des journaux

Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local) : 7 940 événements

- Affichages personnalisés
- Journal Windows
  - Application
  - Sécurité
  - Installation
  - Système
  - Événements transférés
- Journal des applications et services
  - Internet Explorer
  - Key Management Service
  - Media Center
  - Microsoft
    - Microsoft Office Alerts
    - Windows PowerShell
    - Événements matériels
- Journal enregistré
- Abonnements

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'audit	15/10/2019 15:07:37	Microsoft Windows security auditing.	4616	Modification de l'état de la sécurité
Succès de l'audit	15/10/2019 11:56:28	Microsoft Windows security auditing.	4616	Modification de l'état de la sécurité
Succès de l'audit	14/10/2019 16:16:37	Microsoft Windows security auditing.	4672	Ouverture de session spéciale
Succès de l'audit	14/10/2019 16:16:37	Microsoft Windows security auditing.	4624	Ouvrir la session
Succès de l'audit	14/10/2019 16:15:59	Microsoft Windows security auditing.	4905	Modification de la stratégie d'audit
Succès de l'audit	14/10/2019 16:15:59	Microsoft Windows security auditing.	4904	Modification de la stratégie d'audit

Événement 4624, Microsoft Windows security auditing.

Général Détails

L'ouverture de session d'un compte s'est correctement déroulée.

Sujet :

ID de sécurité :	Système
Nom du compte :	FRMRSHOLT4910\$
Domaine du compte :	WORKGROUP
ID d'ouverture de session :	0x3e7

Journal : Sécurité

Source : Microsoft Windows security Connecté : 14/10/2019 16:16:37

Événement : 4624 Catégorie : Ouvrir la session

Niveau : Information Mots clés : Succès de l'audit

Utilisateur : N/A Ordinateur : FRMRSHOLT4910

Opcode : Informations

Informations : [Aide sur le Journal](#)

Actions

Sécurité

- Ouvrir le journal enregistré...
- Créer une vue personnalisée...
- Importer une vue personnalisée...
- Effacer le journal...
- Filter le journal actuel...
- Propriétés
- Rechercher...
- Enregistrer tous les événements sous...
- Joindre une tâche à ce journal...

Affichage

- Actualiser
- Aide

Événement 4624, Microsoft Windows security auditing.

- Propriétés de l'événement
- Joindre une tâche à cet événement...
- Copier
- Enregistrer les événements sélectionnés...
- Actualiser
- Aide



## Windows Active Directory

Pourquoi est-ce inquiétant de retrouver des traces de cette commande dans une machine compromise?

- A. Car elle défragmente le disque et efface des traces utiles à l'investigateur-rice
- B. Car elle permet de ne pas respecter les politiques de sécurité des GPO
- C. Car elle permet de récupérer des informations sensibles pour un-e attaquant-e
- D. Car elle joint la machine au domaine de l'AD
- E. Car elle risque d'endommager le système

```
PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_201503242343_VOLUMEC$\
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_201503242343_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit

Defragmentation Status (% complete)

0   10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
```





## Windows Active Directory

Pourquoi est-ce inquiétant de retrouver des traces de cette commande dans une machine compromise?

- A. Car elle défragmente le disque et efface des traces utiles à l'investigateur-rice
- B. Car elle permet de ne pas respecter les politiques de sécurité des GPO
- C. Car elle permet de récupérer des informations sensibles pour un-e attaquant-e
- D. Car elle joint la machine au domaine de l'AD
- E. Car elle risque d'endommager le système

```
PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_201503242343_VOLUMEC$\
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_201503242343_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit

Defragmentation Status (% complete)

0   10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
```



## Windows

### Cas concret d'incident


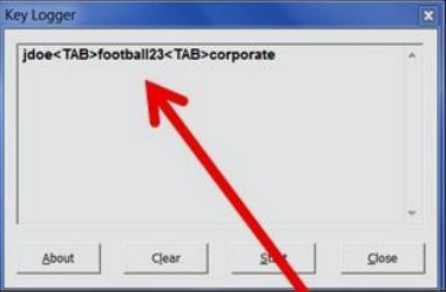
Une alerte remontée par l'antivirus a été détectée sur un serveur. Ce n'était pas exactement un virus mais un driver légitime incorporant un enregistreur de frappes au clavier. L'antivirus remonte ce fichier comme dangereux, avec raison. Ainsi il a été demandé de remplacer le driver par un driver plus récent corrigé.

<https://arstechnica.com/information-technology/2017/05/hp-laptops-covertly-log-every-keystroke-researchers-warn/>

**BIZ & IT —**  
**HP laptops covertly log user keystrokes, researchers warn**

Audio driver supplied by Conexant may put PCs from other makers at risk, too.

**DAN GOODIN** - 5/11/2017, 8:50 PM



**Image above shows Keylogger Stealing VPN credentials**

[Enlarge](#) / Keyloggers like this one surreptitiously store passwords and other confidential data entered into a computer.



## Windows

### Cas concret d'incident

À la suite de la détection d'un incident de sécurité sur ses infrastructures en octobre

a :

- Dans un premier temps, sollicité les sociétés pour établir un diagnostic de l'incident,
- Dans un 2<sup>ème</sup> temps, sollicité la société Microsoft pour procéder à l'éviction des intrus. L'opération d'éviction a eu lieu le week-end du

#### • Besoin

Suite à cette opération d'éviction, souhaite faire appel à un professionnel de la sécurité pour évaluer les résultats de cette opération d'éviction et s'assurer auprès de ce professionnel que son système d'information n'est plus compromis.

En particulier, le fournisseur évaluera la « solidité » du Tier 0, le fournisseur proposera les moyens et procédés pour mener cette évaluation.

a démarré la mise en œuvre de la solution Microsoft ATP, les données collectées par cette plateforme pourront le cas échéant servir d'éléments en entrée pour la mission.

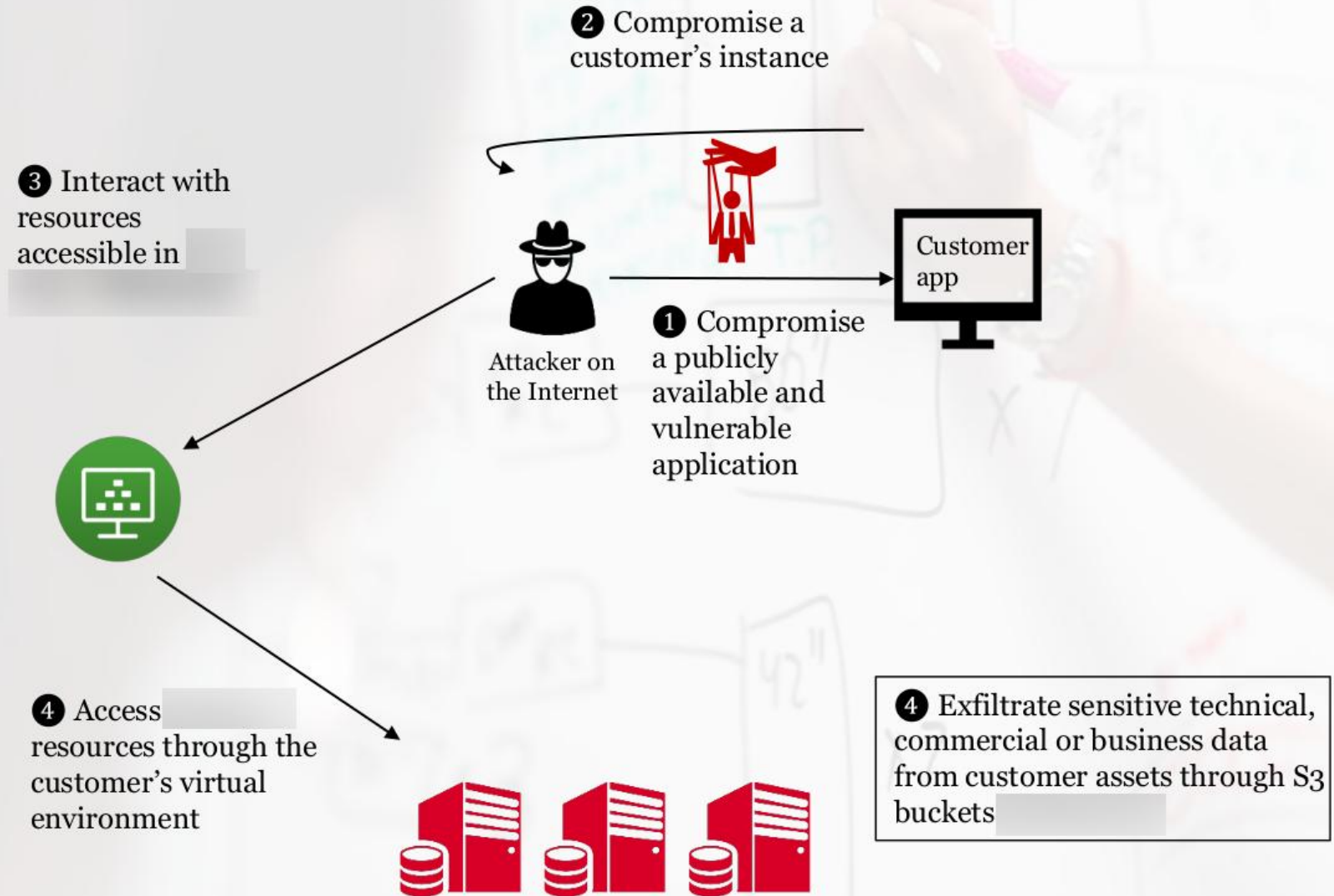
Des connaissances solides en termes de sécurité AD sont nécessaires à la réalisation de cette mission.





# Windows

## Cas concret d'incident sur AWS





Windows



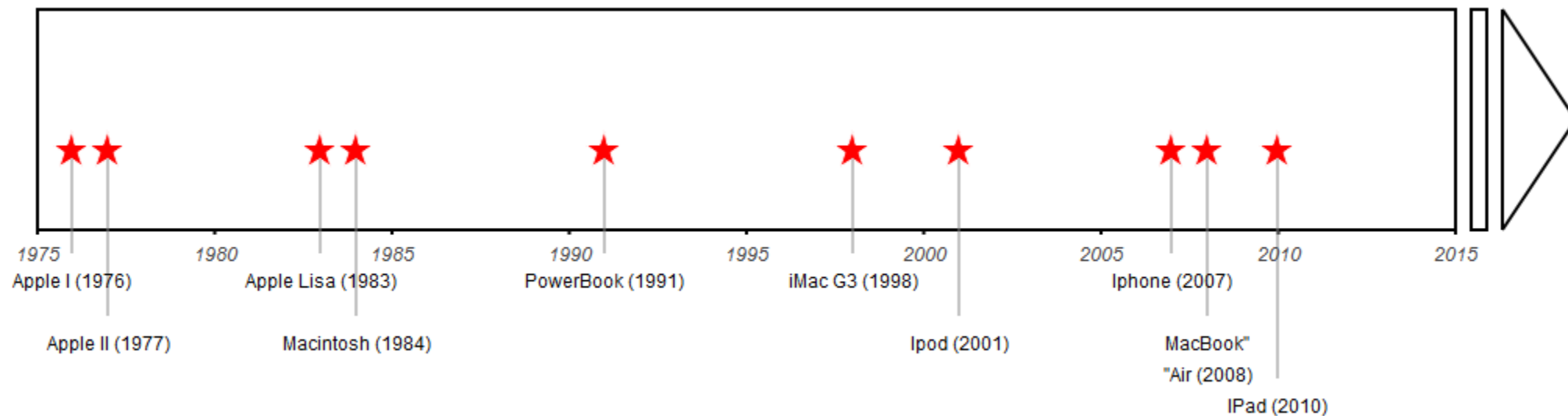
Mac



Linux



## Mac Historique



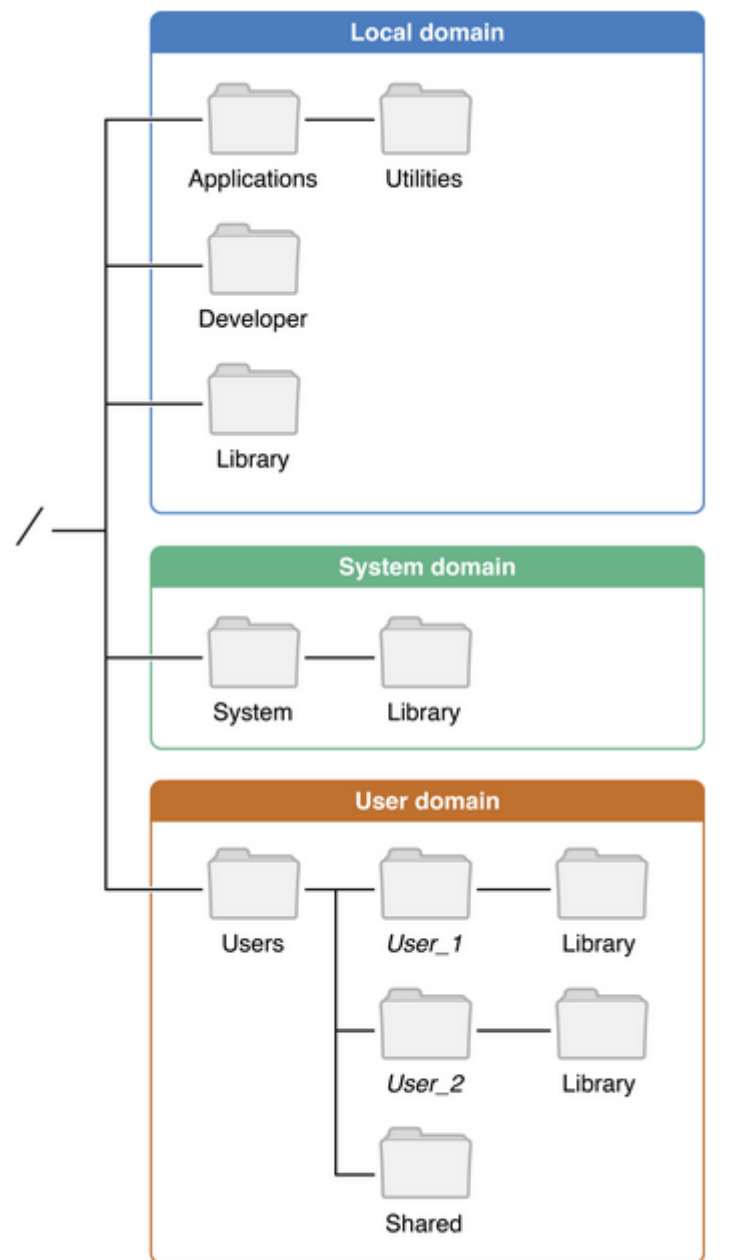


## 2

## Mac Macintosh File Systems

Le **Hierarchical File System (HFS)**, est un système de fichiers propriétaire développé par Apple pour le système d'exploitation Mac OS. Conçu à l'origine pour les disquettes et disques durs, il peut également être utilisé sur des médias en lecture seule, comme les CD-ROM. HFS est généralement désigné par « Mac OS Standard », et son successeur HFS+ par « Mac OS étendu ».

Le *Hierarchical File System*, ou HFS, est aussi un autre système de fichiers utilisé dans z/OS, un système d'exploitation IBM pour mainframe.



1

Windows

2

Mac

3

Linux

**Linux** est, au sens restreint, le [noyau de système d'exploitation Linux](#), et au sens large, tout [système d'exploitation](#) fondé sur le [noyau Linux](#). Cet article couvre le sens large.

À l'origine, le noyau Linux a été développé pour les [ordinateurs personnels compatibles PC](#), et devait être accompagné des [logiciels GNU](#) pour constituer un système d'exploitation. Les partisans du [projet GNU](#) promeuvent depuis le nom combiné [GNU/Linux](#). Depuis les [années 2000](#), le noyau Linux est utilisé sur du matériel informatique allant des [téléphones portables](#) aux [super-ordinateurs](#), et n'est pas toujours accompagné de logiciels GNU. C'est notamment le cas d'[Android](#), qui équipe plus de 80 % des [smartphones](#).

Le noyau Linux a été créé en [1991](#) par [Linus Torvalds](#). C'est un [logiciel libre](#). Les [distributions Linux](#) ont été, et restent, un important vecteur de popularisation du mouvement [open source](#).

### Sommaire [masquer]

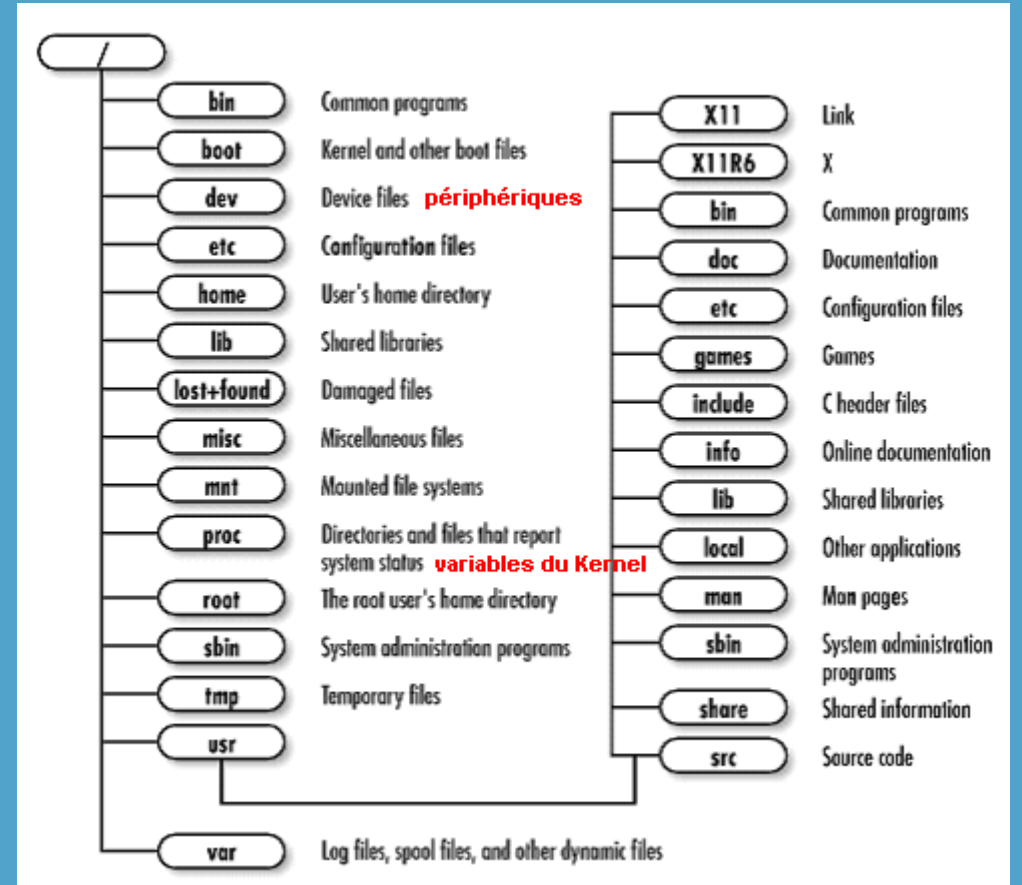
- 1 [Controverse autour du nom](#)
- 2 [Histoire](#)
  - 2.1 [1984-1991 : lancement du projet GNU](#)
  - 2.2 [1991 : naissance du noyau Linux](#)
  - 2.3 [Depuis 1991 : évolution et diffusion du système](#)
- 3 [Philosophie du projet : esprit hacker et logiciel libre](#)
  - 3.1 [Logiciel libre](#)
  - 3.2 [Interopérabilité](#)
  - 3.3 [Communautés](#)

## 3

## Linux

### Système de fichier

Feature	EXT4	XFS	BTRFS
Architecture	Hashed B-tree	B+ tree	Extent based
Introduced	2006	1994	2009
Max volume size	1 Ebytes	8 Ebytes	16 Ebytes
Max file size	16 Tbytes	8 Ebytes	16 Ebytes
Max number of files	4 billion	$2^{64}$	$2^{64}$
Max file name size	255 bytes	255 bytes	255 bytes
Attributes	Yes	Yes	Yes
Transparent compression	No	No	Yes
Transparent encryption	Yes	No	Planned
Copy-on-Write (COW)	No	Planned	Yes
Snapshots	No	Planned	Yes





3

## Linux

Comment s'en sortir avec un disque dur chiffré ?

Comment est-il possible pour l'investigateur-riche d'obtenir la clé de déchiffrement d'un disque dur chiffré ?

- A. Depuis les journaux Linux
- B. Depuis les options de boot
- C. Depuis le dump mémoire
- D. En brute-forçant le hash contenu dans le fichier */etc/shadow*
- E. En le demandant à l'utilisateur
- F. En le récupérant dans la puce CMOS ou autre endroit physique
- G. En le trouvant en clair dans un fichier effacé
- H. En utilisant la commande dd



3

## Linux

Comment s'en sortir avec un disque dur chiffré ?

Comment est-il possible pour l'investigateur-riche d'obtenir la clé de déchiffrement d'un disque dur chiffré ?

- A. Depuis les journaux Linux
- B. Depuis les options de boot
- C. Depuis le dump mémoire
  - A condition de pouvoir l'avoir...
- D. En brute-forçant le hash contenu dans le fichier */etc/shadow*
- E. En le demandant à l'utilisateur
- F. En le récupérant dans la puce CMOS ou autre endroit physique
  - Cela dépend de la machine
- G. En le trouvant en clair dans un fichier effacé
- H. En utilisant la commande dd

### 3

## Linux .bash\_history

Même si l'horodatage des commandes n'est pas disponible, le contenu du fichier `.bash_history` est très TRES utile pour comprendre ce qu'il s'est passé sur un système Linux.

```
tenflo@FRMRSHOLT6809:~$ cat ~/.bash_history | tail -n 50
sudo sh -c 'echo "deb http://dl.google.com/linux/chrome/deb/ stable main" >> /etc/apt/sources.list.d/google-chrome.list'
sudo apt-get update
uname -a
sudo apt upgrade
exit
cat > questionnaire.txt
exit
sudo tripwire --check
sudo tripwire --init
exit
shred -z -n 3 -u questionnaire.txt
exit
cat *.nikto | grep Strict
grep *.nikto Strict
grep Strict *.nikto
exit
java -jar burpsuite_pro_v2.1.04.jar
exit
shred -z -n 3 -u *
exit
sudo tripwire --check
clear
tail /var/log/apt/history.log
sudo tripwire --init
exit
```

Les logs sont très utiles lors d'une investigation, par exemple les journaux web permettent d'identifier une attaque via un serveur web. Les champs les plus intéressants d'une ligne de log d'un serveur Apache sont :

1. L'adresse IP source
2. L'horodatage
3. La méthode de la requête
4. L'URI de la requête
5. Le code de la réponse HTTP
6. Le User-Agent

```
77.36.254.99 - - [29/Aug/2011:00:20:38 -0700] "GET /reset.css HTTP/1.0" 304 212 "http://www.semicon
77.36.254.99 - - [29/Aug/2011:00:20:38 -0700] "GET /style2.css HTTP/1.0" 304 214 "http://www.semicon
77.36.254.99 - - [29/Aug/2011:00:20:38 -0700] "GET /reset.css HTTP/1.0" 304 213 "http://www.semicon
77.36.254.99 - - [29/Aug/2011:00:20:38 -0700] "GET /images/jordan-80.png HTTP/1.0" 304 191 "http://
77.36.254.99 - - [29/Aug/2011:00:20:39 -0700] "GET /images/web/2009/banner.png HTTP/1.0" 304 191 "f
77.36.254.99 - - [29/Aug/2011:00:20:46 -0700] "GET /favicon.ico HTTP/1.0" 304 190 "-" "Mozilla/4.0
66.249.72.239 - - [29/Aug/2011:00:21:07 -0700] "GET /scripts/gaimsort HTTP/1.1" 200 1327 "-" "Mozil
217.86.194.75 - - [29/Aug/2011:00:22:05 -0700] "GET /articles/dynamic-dns-with-dhcp/ HTTP/1.1" 200
217.86.194.75 - - [29/Aug/2011:00:22:05 -0700] "GET /reset.css HTTP/1.1" 200 910 "http://www.semicon
217.86.194.75 - - [29/Aug/2011:00:22:05 -0700] "GET /style2.css HTTP/1.1" 200 1820 "http://www.semicon
217.86.194.75 - - [29/Aug/2011:00:22:05 -0700] "GET /images/jordan-80.png HTTP/1.1" 200 6442 "http:
217.86.194.75 - - [29/Aug/2011:00:22:05 -0700] "GET /favicon.ico HTTP/1.1" 200 3935 "-" "Mozilla/5.
217.86.194.75 - - [29/Aug/2011:00:22:06 -0700] "GET /images/web/2009/banner.png HTTP/1.1" 200 5261
85.93.98.210 - - [29/Aug/2011:00:22:44 -0700] "GET /files/logstash/logstash-1.0.17-monolithic.jar H
119.63.196.12 - - [29/Aug/2011:00:24:00 -0700] "GET /blog/geekery/75.html HTTP/1.1" 200 4414 "-" "M
77.36.254.99 - - [29/Aug/2011:00:24:08 -0700] "GET /files/dynamic-dns-with-dhcp/dhcpd.conf HTTP/1.0
188.221.83.232 - - [29/Aug/2011:00:24:27 -0700] "GET /projects/xdotool/ HTTP/1.1" 200 4551 "http://
188.221.83.232 - - [29/Aug/2011:00:24:27 -0700] "GET /reset.css HTTP/1.1" 200 909 "http://www.semicon
188.221.83.232 - - [29/Aug/2011:00:24:27 -0700] "GET /style2.css HTTP/1.1" 200 1820 "http://www.semicon
188.221.83.232 - - [29/Aug/2011:00:24:27 -0700] "GET /images/jordan-80.png HTTP/1.1" 200 6442 "http:
188.221.83.232 - - [29/Aug/2011:00:24:27 -0700] "GET /images/web/2009/banner.png HTTP/1.1" 200 5261
72.14.199.236 - - [29/Aug/2011:00:24:45 -0700] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 1509
```

```
root@srini:/var/log/apache2# cat access.log.1 | grep ".../etc/passwd"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET ../../../../../../etc/passwd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET ../../../../../../etc/passwd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET ../../../../../../etc/passwd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET ../../../../../../etc/passwd HTTP/1.1" 400 506 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:00:48 -0400] "GET /scripts/fake.cgi?arg=/dir/../../../../../../../../etc/passwd HTTP/1.1" 404 529 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:01:08 -0400] "GET /cgi-bin/pdesk.cgi?lang=../../../../../../../../../../../../etc/passwd HTTP/1.1" 404 530 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:02:04 -0400] "GET /search?NS-query-pat=../../../../../../../../../../../../etc/passwd HTTP/1.1" 404 519 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
127.0.0.1 - - [27/Oct/2014:04:02:09 -0400] "GET /ifk/?LO=../../../../../../../../etc/passwd HTTP/1.1" 404 517 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
root@srini:/var/log/apache2#
```





## CRITICAL Apache Hadoop YARN ResourceManager Unauthenticated RCE (Remote) (Xbash)

The Apache Hadoop YARN ResourceManager running on the remote host is allowing unauthenticated users to create and execute applications. An unauthenticated, remote attacker can exploit this, via a specially crafted HTTP request, to potentially execute arbitrary code, subject to the user privileges of the executing node.

Configure ResourceManager API access control.

<http://www.nessus.org/u?57624ec9>

Nessus was able to exploit the issue using the following request :

```
POST /ws/v1/cluster/apps HTTP/1.1
Host: 10.122.1.90:8088
Accept: */*
User-Agent: Nessus
Content-Length: 205
Content-Type: application/json
```

```

{"am-container-spec": {"commands": {"command": "ping -c 3 -s 500 44.59.96.156"}}, "application-id": "application_1559122293930_2934", "application-type": "YARN", "application-name": "48533951344657705769"}

```

This produced the following truncated output (limited to 10 lines) :

```
----- snip -----
```

Nessus confirmed this issue by examining incoming ICMP traffic. Below is the response :

92461b5d0000000000b290a0000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f0a01a2

Comment peut-on détecter l'exploitation de cette vulnérabilité ?

1. En observant l'horodate des requêtes POST sur cette URI (mais on n'a pas le contenu de la requête POST dans les logs)
2. En observant un nombre anormal de requête vers cette URI
3. En lisant le fichier `.bash_history` (s'il existe) de l'utilisateur faisant tourner le service

Il est également possible d'obtenir les informations suivantes :

4. L'adresse IP source de la requête d'exploitation est disponible dans les logs du serveur web
5. L'écoute du trafic réseau depuis cette machine ou l'analyse des sockets ouvertes peut permettre d'identifier si un flux C&C est en cours vers l'attaquant
6. L'analyse des logs du pare-feu du serveur peut permettre d'identifier la première connexion vers l'attaquant
7. La liste des fichiers modifiés ces derniers jours et la consultation de leurs contenus peut donner des indices sur le déroulement de la post-exploitation
8. ...

3

## Linux

### Etude d'un autre cas

A quoi correspondent ces détections sur un pare-feu Palo-Alto ?

(! name-of-threatid eq 'SSH User Authentication Brute Force Attempt')													
	Generate Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	Severity	File Name
	05/07 17:09:39	vulnerability	Detected										
	05/07 17:09:39	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					8080	web-browsing	reset-server	high	win.ini
	05/07 17:09:38	vulnerability	Struts2 and XWork Remote Command Execution Vulnerability	inside					4242	web-browsing	alert	high	
	05/07 17:09:38	vulnerability	Apache Struts2 Dynamic Method Remote Code Execution Vulnerability	inside					4242	web-browsing	alert	high	
	05/07 17:09:38	vulnerability	Apache Struts2 OGNL Remote Code Execution Vulnerability	inside					4242	web-browsing	alert	high	
	05/07 17:09:38	vulnerability	Apache Struts2 OGNL Expression Injection Vulnerability	inside					4242	web-browsing	alert	high	
	05/07 17:09:37	vulnerability	Bash Remote Code Execution Vulnerability	inside					4242	web-browsing	reset-both	critical	
	05/07 17:09:37	vulnerability	Apache Struts 2 Remote Code Execution Vulnerability	inside					4242	web-browsing	alert	high	\$(436755678+5..
	05/07 17:09:37	vulnerability	Apache Struts ClassLoader Security Bypass Vulnerability	inside					4242	web-browsing	alert	high	
	05/07 17:09:37	vulnerability	PHP CGI Query String Parameter Handling Information Disclosure Vulnerability	inside					4242	web-browsing	alert	medium	php
	05/07 17:09:37	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					4242	web-browsing	reset-server	high	win.ini
	05/07 17:09:35	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					8080	web-browsing	reset-server	high	note.txt
	05/07 17:09:34	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					50070	web-browsing	reset-server	high	win.ini
	05/07 17:09:33	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					4242	web-browsing	reset-server	high	win.ini
	05/07 17:09:31	vulnerability	Netscape iPlanet Search NS-Query-Pat Directory Traversal Vulnerability	inside					20000	web-browsing	alert	medium	search
	05/07 17:09:31	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					20000	web-browsing	reset-server	high	search
	05/07 17:09:31	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					8080	web-browsing	reset-server	high	note.txt
	05/07 17:09:30	vulnerability	Apache Struts Content-Type Remote Code Execution Vulnerability	inside					20000	web-browsing	reset-server	critical	
	05/07 17:09:29	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					9000	web-browsing	reset-server	high	note.txt
	05/07 17:09:27	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					4242	web-browsing	reset-server	high	win.ini
	05/07 17:09:27	vulnerability	Apache Struts2 Redirect/Action Method Remote Code Execution Vulnerability	inside					20000	web-browsing	reset-server	critical	
	05/07 17:09:26	vulnerability	Microsoft Windows win.ini Access Attempt Detected	inside					8080	web-browsing	reset-server	high	note.txt

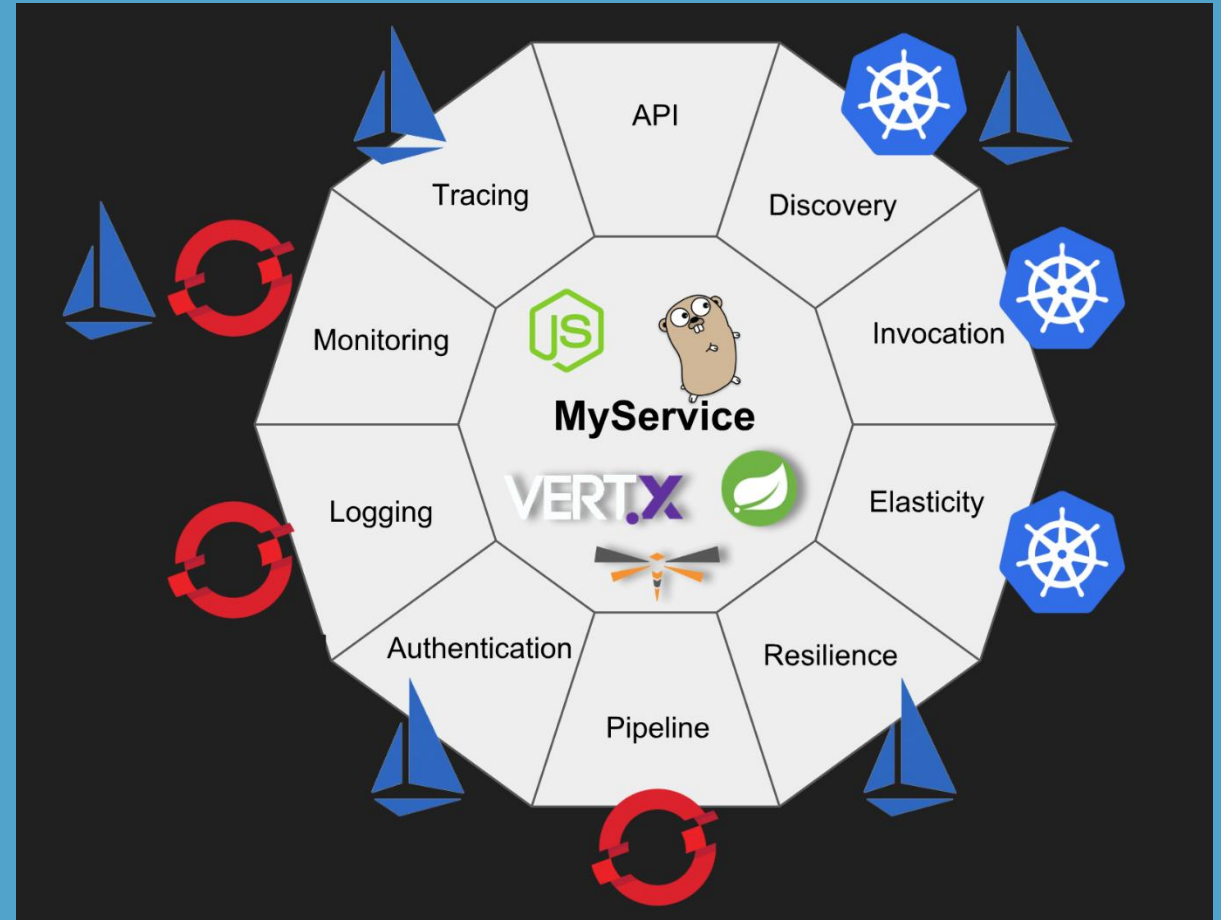
3

## Linux

### Etude d'un autre cas

C'était un scan de vulnérabilité en provenance d'une adresse IP interne. Après investigation, c'était un *pod* de Kubernetes qui était compromis à cause d'un composant applicatif non à jour et qui servait à l'attaquant-e en interne pour scanner le reste du réseau sans laisser trace de son adresse IP.

Les traces laissés par l'attaquant-e n'ont pas permis de trouver son origine mais il-elle a tenté de nombreuses méthodes pour tenter d'élever ses privilèges dans le *pod* ou d'accéder aux autres containers sans succès apparent. Ensuite seulement, il-elle a utilisé le *pod* compromis comme rebond pour attaquer d'autres IP interne.







## Windows

Si on résume ensemble :

- Historique du système de fichier de Windows
- Récupération de fichiers effacés de la Corbeille
- Master File Table
- Base de registre Windows
- Shadow copy
- Récupération du mot de passe de l'utilisateur
- Volatility
- BitLocker
- Gestion des journaux
- Active Directory

Si on résume ensemble :



Mac

- Historique
- Macintosh File Systems

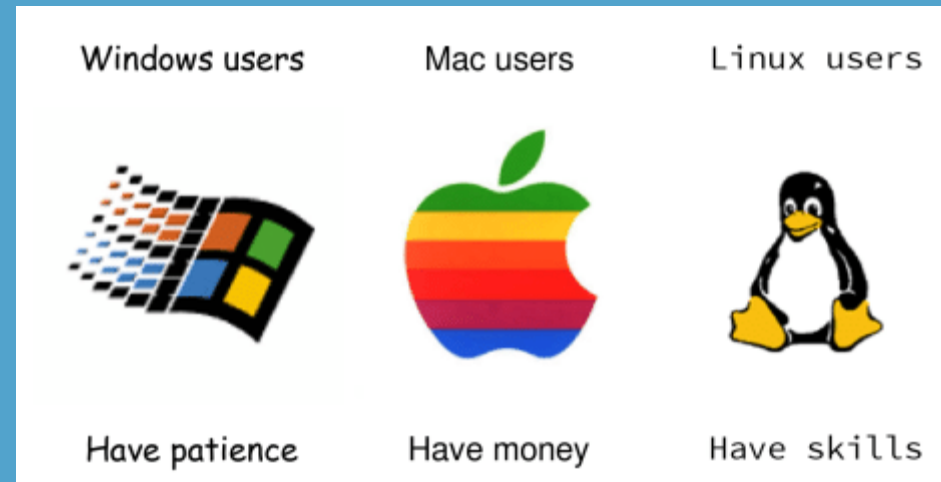
Si on résume ensemble :



Linux

- Historique
- Système de fichier
- Comment s'en sortir avec un disque dur chiffré ?
- .bash\_history
- Journaux web
- Etude de cas

# Conclusion



# MERCI

[www.squad.fr](http://www.squad.fr)

PUBLIC

