

Sécurité et Réseaux

Les risques et menaces

Remarque préliminaire

Il ne sera fait référence qu'à des systèmes et logiciels réseaux grand public ou largement utilisés dans les entreprises :

- Windows – Linux
- Réseau Internet (TCP/IP, UDP/IP)
- Services HTTP, DNS, ICMP, FTP, TELNET , ...

Sécurité et Réseaux

Failles des systèmes informatiques et réseaux

Protection des systèmes - rappels

Niveaux de protection

Identification de l'utilisateur



Droits d'accès aux données



Limites de la protection

Identification de l'utilisateur

Non obligatoire sur les systèmes grand public

Mot de passe non obligatoire sur tous les systèmes

L'utilisateur par défaut possède tous les privilèges

Si le mot de passe est obligatoire :

- Pas de règles imposées pour le changement
- Règles trop contraignantes

Limites de la protection

Droits d'accès aux données

Il est possible de protéger l'accès aux données en précisant les opérations possibles pour chaque utilisateur ou groupe.

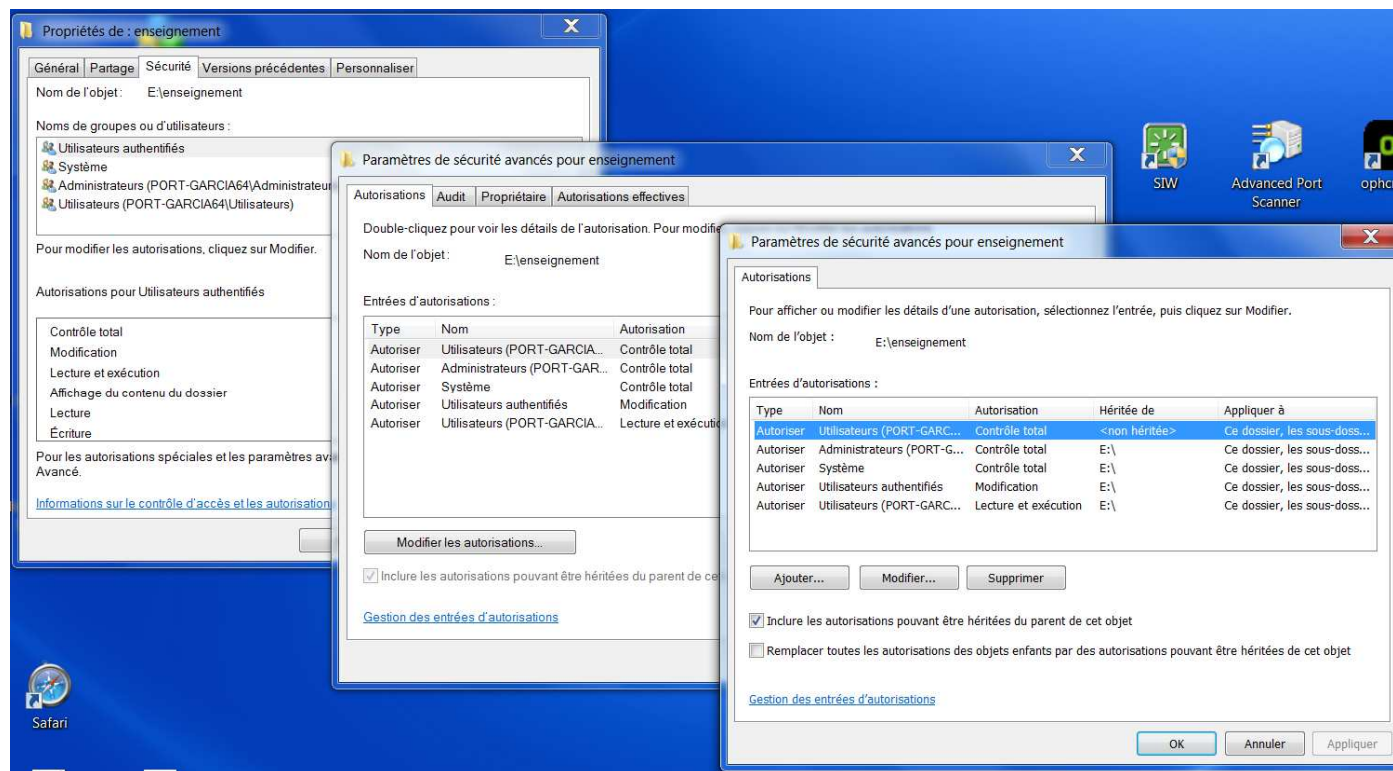
Deux philosophies existent :

- Aucune restriction par défaut
- Restriction d'accès à toutes des données n'appartenant à un utilisateur donné

Limites de la protection

Droits d'accès aux données

Problème : les règles et commandes pour la gestion des droits d'accès sont complexes pour les non initiés.



Limites de la protection

Droits d'accès aux données

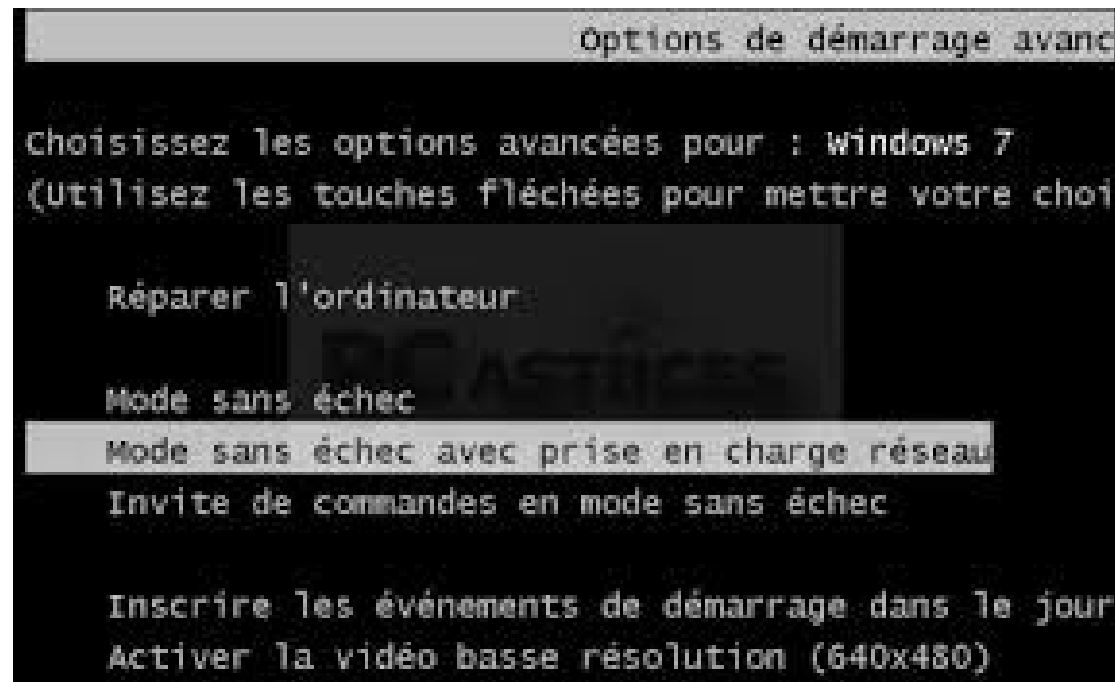
Exemple sous Linux : `chmod 754 fic`

Conséquence : si la gestion des droits devient trop complexe , la tendance sera d'ouvrir tous les droits pour ne plus être limité

Limites de la protection

Autres limites

Démarrage en mode sans échec sous Windows



Démarrage en mode « single » sous Linux

Limites de la protection

Mais encore

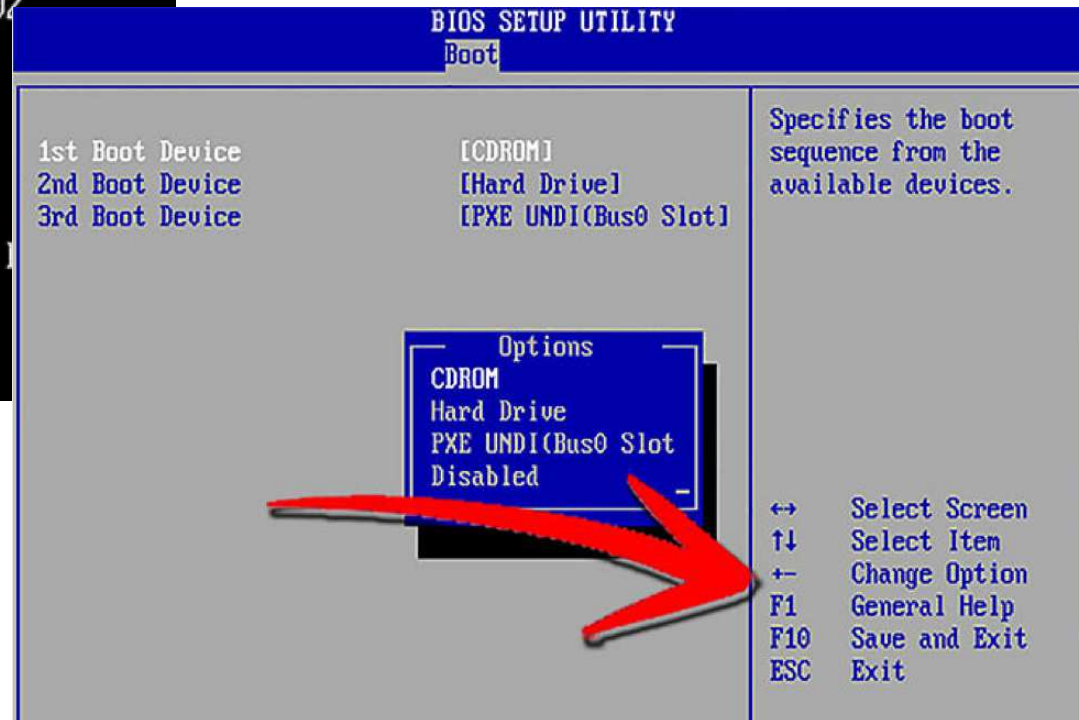
Démarrage avec un « live » linux ou Windows



Limites de la protection

Mais .. Il est possible d'accéder au Bios, facilement

→ Touche « Suppr » au démarrage



→ Il faut mettre un mot de passe pour l'accès au Bios



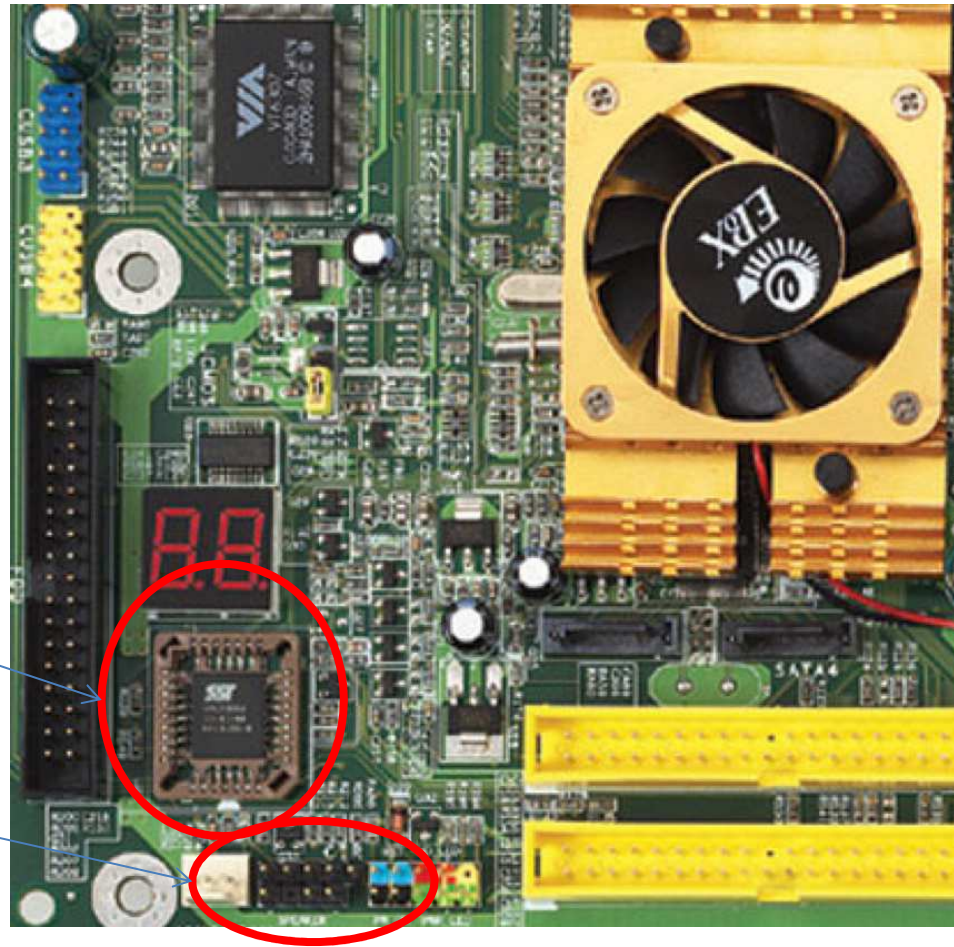
Limites de la protection

Mais ..

Il est possible d'enlever le mot de passe du Bios

Bios

Cavaliers de configuration



→ Il faut mettre l'ordinateur dans un coffre fort ou ne plus l'utiliser

Failles des protocoles réseaux

Modèle Internet

Services (http – dns – ftp - ...)



TCP - UDP



IP



Ethernet - CSMA/CD



Faibles des protocoles réseaux

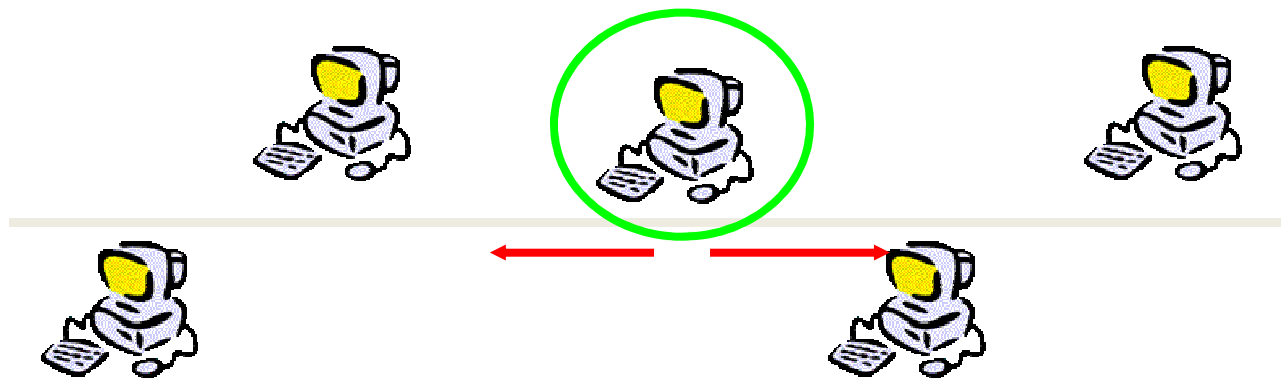
CSMA/CD ou Ethernet

Faibles des protocoles réseaux

CSMA/CD ou Ethernet principe de fonctionnement

Transfert des données = diffusion générale

Dans les réseaux locaux les trames échangées sont vues par toutes les machines reliées sur un même HUB



Failles des protocoles réseaux

CSMA/CD ou Ethernet - Limites du protocole

Le format des trames est public, n'importe qui peut interpréter leur contenu

Les protocoles ne cryptent pas les données échangées.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.67	226.178.217.5	UDP	87	Source port: 55024 Destination port: 21328
2	0.15592500	192.168.1.67	10.10.104.1	TCP	66	49726 > hp-pdl-datastr [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.19372300	109.3.48.154	192.168.1.67	ICMP	94	Destination unreachable (Port unreachable)
4	1.58643500	192.168.1.67	192.168.1.1	DNS	73	Standard query 0x0a9c A www.google.fr
5	1.62708600	192.168.1.1	192.168.1.67	DNS	89	Standard query response 0x0a9c A 173.194.67.94
6	1.63020200	192.168.1.67	173.194.67.94	TCP	66	49730 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	1.67755900	173.194.67.94	192.168.1.67	TCP	66	http > 49730 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=64
8	1.67779300	192.168.1.67	173.194.67.94	TCP	54	49730 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
9	1.67827300	192.168.1.67	173.194.67.94	HTTP	997	GET / HTTP/1.1
10	1.73155200	173.194.67.94	192.168.1.67	TCP	54	http > 49730 [ACK] Seq=1 Ack=944 Win=42304 Len=0
11	1.83167200	173.194.67.94	192.168.1.67	HTTP	555	HTTP/1.1 302 Found (text/html)
12	1.83886800	192.168.1.67	173.194.67.94	TCP	66	49731 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Failles des protocoles réseaux

Protocole IP V4

Failles des protocoles réseaux

Protocole IP V.4

IP défini :

- une fonction d'adressage
- une structure pour le transfert des données (datagramme),
- une fonction de routage,

IP est un protocole à commutation de paquets :

- service sans connexion (paquets traités indépendamment les uns des autres),
- remise de paquets non garantie.

➔ IP V4 = Protocole non fiable

Failles des protocoles réseaux

Adressage IP

Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (n° réseau, n° machine).

Limites :

- les adresses IP ne sont gérées par Ethernet → ARP
- par manque d'adresses IP , on utilise des adresses dynamiques → DHCP
- l'utilisateur manipule des noms de sites au lieu des adresses IP → DNS

```
Adresse IPv4. . . . . : 192.168.1.67(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : lundi 3 mars 2014 08:07:44
Bail expirant. . . . . : mardi 4 mars 2014 08:07:46
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 241227801
DUID de client DHCPv6. . . . . : 00-01-00-01-18-36-5E-C9-D0-67-E5-37-BD
F
Serveurs DNS. . . . . : 192.168.1.1
NetBIOS sur Tcpip. . . . . : Activé
```

Faibles des protocoles réseaux

ARP

Le protocole ARP (Address Resolution Protocol)

Objectif : fournir, à une machine donnée, l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP

Technique : Interroger toutes les machines pour obtenir l'information.

La machine prend la première réponse reçue.

Faibles des protocoles réseaux

ARP

Pour éviter de répéter plusieurs fois cette opération lourde, les informations sont stockées dans un cache local.

```
C:\Users\image-port10-2011>arp -a

Interface : 192.168.1.67 --- 0xd
  Adresse Internet      Adresse physique      Type
  192.168.1.1           e0-a1-d7-2a-d6-bc     dynamique
  192.168.1.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  226.178.217.5         01-00-5e-32-d9-05     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Faibles des protocoles réseaux

ARP - limites

- 1 - Une machine envoie son adresse physique (adresse MAC) en réponse à une requête ARP : **ARP-Poisoning**
- 2 – Le contenu de la mémoire cache peut être modifié intentionnellement : **ARP-Cache Poisoning** :

Failles des protocoles réseaux

DHCP

Le DHCP (Dynamic Host Configuration Protocol)

Objectif : fournir à une machine une adresse IP

Technique :

La machine, qui souhaite une adresse IP, émet au serveur DHCP un message lui demandant une adresse.

Le serveur dispose d'un ensemble d'adresses qu'il peut attribuer. Il répond en renvoyant une adresse IP.

Faibles des protocoles réseaux

DHCP

Épuisement des ressources : Si un pirate génère un grand nombre de requêtes DHCP semblant venir d'un grand nombre de clients différents, le serveur épuisera vite son stock d'adresses. Les «vrais» clients ne pourront donc plus obtenir d'adresse IP : le trafic réseau sera paralysé.

Faux serveurs DHCP : Si un pirate a réussi à saturer un serveur DHCP par épuisement de ressources, il peut très bien en activer un autre à la place. Il pourra ainsi contrôler tout le trafic réseau.

Failles des protocoles réseaux

DNS

Le DNS (Domain Name Service)

Objectif : fournir à une machine donnée l'adresse IP de la machine à atteindre

Technique :

La machine émet au serveur DNS un message contenant le nom de la machine à atteindre

La machine concernée répond en renvoyant l'adresse IP, ou sollicite une autre serveur DNS.

La machine prend la première réponse reçue.

Faibles des protocoles réseaux

DNS

Pour éviter de répéter
plusieurs fois cette
opération lourde, les
informations sont stockées
dans un cache local.

scolariteparis.cnam.fr

Nom d'enregistrement. : sclariteparis.cnam.fr

Type d'enregistrement : 5

Durée de vie : 41329

Longueur de données . : 8

Section : Réponse

Enregistrement CNAME : klingon.cnam.fr

pop.1and1.fr

Nom d'enregistrement. : pop.1and1.fr

Type d'enregistrement : 1

Durée de vie : 1449

Longueur de données . : 4

Section : Réponse

Enregistrement (hôte) : 212.227.15.140

Faibles des protocoles réseaux

DNS - Limites

- 1 – Envoie d'une fausse réponse à une requête DNS avant le serveur DNS. De cette façon, le pirate peut rediriger vers lui le trafic à destination d'une machine qu'il l'intéresse

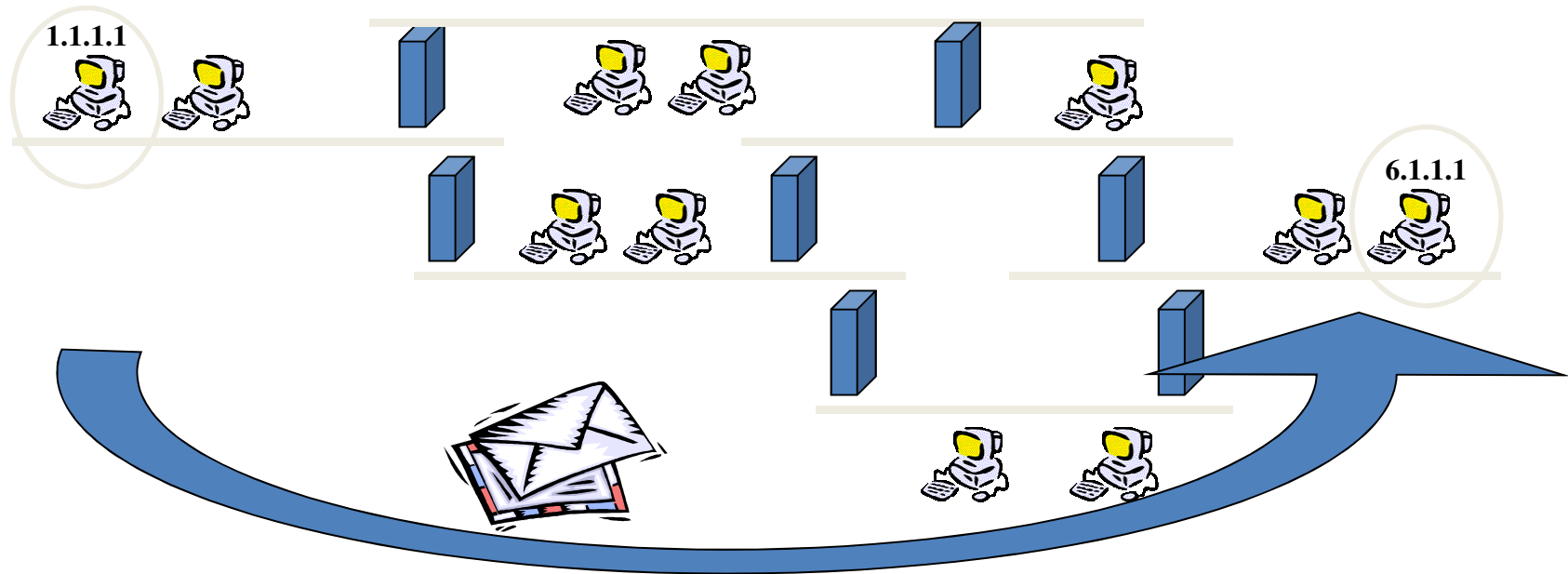
DNS-spoofing

- 2 - Un serveur DNS n'a que la table de correspondance des machines du réseau sur lequel il a autorité. Pour des machines distantes, il doit interroger d'autres serveurs DNS et garde en mémoire (dans un cache), le résultat des précédentes requêtes. L'objectif du pirate est d'empoisonner ce cache avec de fausses informations : **DNS cache poisoning**

- 3 – Blocage du serveur DNS

Faillles des protocoles réseaux

Routage IP

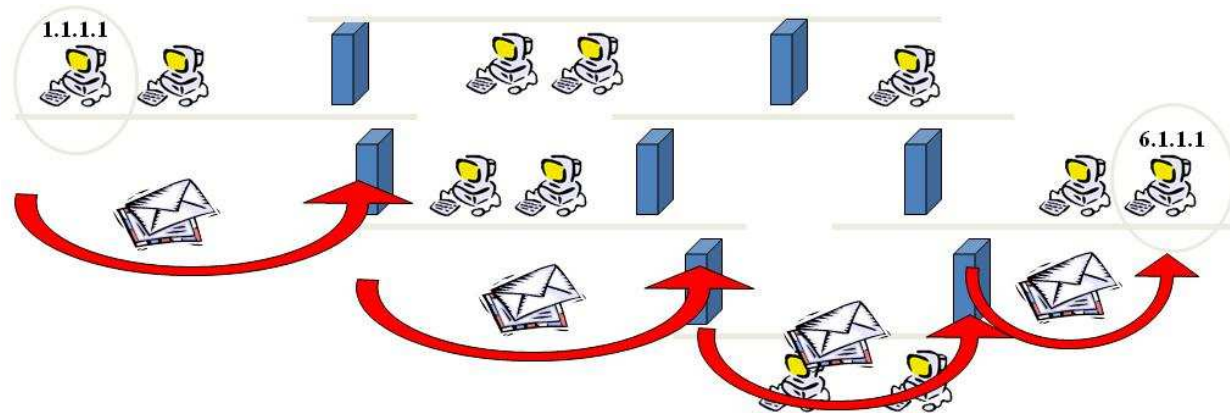


Le routage est le processus permettant à un « datagramme » d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.

Failles des protocoles réseaux

Routage IP

Un datagramme transite alors de passerelle en passerelle jusqu'à ce que l'une d'entre elle le délivre à son destinataire.



```
Détermination de l'itinéraire vers www.google.fr [173.194.66.94]
avec un maximum de 30 sauts :

 1      3 ms      1 ms      1 ms  neufbox [192.168.1.1]
 2      *        *        *      Délai d'attente de la demande dépassé.
 3     30 ms     28 ms     31 ms  189.235.64.86.rev.sfr.net [86.64.235.189]
 4     28 ms     32 ms     30 ms  177.235.64.86.rev.sfr.net [86.64.235.177]
 5     29 ms     33 ms     31 ms  145.50.3.109.rev.sfr.net [109.3.50.145]
 6     29 ms     32 ms     29 ms  17.18.3.109.rev.sfr.net [109.3.18.17]
 7     39 ms     40 ms     38 ms  72.14.219.117
 8     40 ms     44 ms     40 ms  72.14.238.234
 9     41 ms     39 ms     42 ms  209.85.245.83
10     46 ms     57 ms     46 ms  209.85.253.20
11     44 ms     44 ms     46 ms  72.14.238.41
12      *        *        *      Délai d'attente de la demande dépassé.
13     49 ms     46 ms     46 ms  we-in-f94.1e100.net [173.194.66.94]

Itinéraire déterminé.
```

Faillles des protocoles réseaux

Routage IP

1 - La passerelle ne connaît pas le chemin complet pour atteindre la destination, elle prend la décision à partir d'un ensemble d'informations stockées dans une table de routage

```
IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
0.0.0.0                 0.0.0.0        192.168.1.1      192.168.1.67    25
127.0.0.0               255.0.0.0      On-link          127.0.0.1       306
127.0.0.1               255.255.255.255 On-link          127.0.0.1       306
127.255.255.255         255.255.255.255 On-link          127.0.0.1       306
192.168.1.0             255.255.255.0  On-link          192.168.1.67    281
192.168.1.67            255.255.255.255 On-link          192.168.1.67    281
192.168.1.255           255.255.255.255 On-link          192.168.1.67    281
224.0.0.0               240.0.0.0      On-link          127.0.0.1       306
224.0.0.0               240.0.0.0      On-link          192.168.1.67    281
255.255.255.255         255.255.255.255 On-link          127.0.0.1       306
255.255.255.255         255.255.255.255 On-link          192.168.1.67    281
=====
```

Failles des protocoles réseaux

Routage IP

2 – Comme le protocole est orienté sans connexion, le paquet IP transporte l'adresse de l'émetteur pour que le destinataire puisse répondre.

3 – Comme le paquet IP peut se perdre dans le réseau, il comporte une durée de vie.

```
■ Internet Protocol Version 4, Src: 192.168.1.67 (192.168.1.67), Dst: 63.245.217.36 (63.245.217.36)
  Version: 4
  Header length: 20 bytes
  ▣ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 52
  Identification: 0x07a5 (1957)
  ▣ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  ▣ Header checksum: 0x181a [correct]
  Source: 192.168.1.67 (192.168.1.67)
  Destination: 63.245.217.36 (63.245.217.36)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

Faibles des protocoles réseaux

Routage IP - Limites

Déconfiguration IP : on peut supprimer les informations de configuration IP (adresse, masque) dans la machine.

Modification des tables de routage : la commande « route » modifie le contenu d'une table de routage.

Modification de la durée de vie des paquets.

Failles des protocoles réseaux

Routage IP - Limites

Camouflage d'adresse IP : on utilise une machine intermédiaire qui fait les requêtes à la place d'une autre machine.

La configuration technique de votre ordinateur n'a pas de secret pour moi !

Saviez-vous que l'adresse IP de votre machine est : **79.80.214.224** ?
Le nom d'hôte associé à votre adresse IP : **79.80.214.224**

L'IP spoofing : dès qu'un client possède une connexion établie sur le serveur avec un mode d'authentification basée sur l'adresse IP, le pirate va essayer de se faire passer pour le client auprès du serveur. Pour cela, il va empêcher le client de dialoguer avec le serveur et répondra à sa place

Failles des protocoles réseaux

Protocole TCP

Failles des protocoles réseaux

Protocole TCP

TCP (Transport Control Protocol)

Objectif : Service en mode connecté ==> garantie de non perte de messages ainsi que de l'ordonnancement des messages IP

Transport fiable de la technologie TCP/IP :

- Adresse les processus (N° Port)
- Fiabilise IP (Connexion et acquittements)
- Garantie la non perte de messages ainsi que de l'ordonnancement (N° Sequence)
- Optimise les ressources (Fenêtres variables)

Failles des protocoles réseaux

Protocole TCP - Limites

Désynchronisation TCP : pendant un échange, l'attaquant envoie au client des paquets en y plaçant des mauvais numéros de séquences
→ le client croit qu'il a perdu la connexion et stoppera ses échanges . Puis l'attaquant envoie les bons numéros de séquences au serveur, il récupère la connexion pour lui.

```
▣ Transmission Control Protocol, Src Port: http (80), Dst Port: 49506 (49506), Seq: 0, Ack: 1, Len: 0
  Source port: http (80)
  Destination port: 49506 (49506)
  [Stream index: 0]
  Sequence number: 0      (relative sequence number)
  Acknowledgment number: 1  (relative ack number)
  Header length: 32 bytes
  ▣ Flags: 0x012 (SYN, ACK)
  Window size value: 14600
  [Calculated window size: 14600]
  ▣ Checksum: 0x3a46 [validation disabled]
  ▣ Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted,
  ▣ [SEQ/ACK analysis]
```

Interruption d'un échange TCP : pendant un échange, on expédie un message contenant un 'Reset' .

Failles des services réseaux

Les services réseaux

Failles des services réseaux

Considérations générales (1)

Un service est accessible via une @IP et un n° Port

Le dialogue entre service et application cliente est normalisé → il est donc facile de les identifier.

Les services sont conçus pour répondre à toutes les requêtes.

Failles des services réseaux

Considérations générales (2)

- Les services fonctionnent sur le principe de la « confiance »
- Les échanges entre services ne sont pas cryptés.

00	17	33	26	12	b0	9c	b7	0d	2d	54	6a	08	00	45	00	..3&....	.-Tj..E.
02	a7	07	a7	40	00	80	06	15	a5	c0	a8	01	43	3f	f5@...C?.
d9	24	c1	62	00	50	99	56	36	e9	37	33	57	8e	50	18	\$.b.P.V	6.73W.P.
41	3a	00	86	00	00	47	45	54	20	2f	3f	70	72	6f	64	A:....GE	T /?prod
75	63	74	3d	66	69	72	65	66	6f	78	2d	31	38	2e	30	uct=fire	fox-18.0
2e	31	2d	63	6f	6d	70	6c	65	74	65	26	6f	73	3d	77	.1-compl	ete&os=w
69	6e	26	6c	61	6e	67	3d	66	72	20	48	54	54	50	2f	in&lang=	fr HTTP/
31	2e	31	0d	0a	48	6f	73	74	3a	20	64	6f	77	6e	6c	1.1..Hos	t: downl
6f	61	64	2e	6d	6f	7a	69	6c	6c	61	2e	6f	72	67	0d	oad.mozi	lla.org.
0a	55	73	65	72	2d	41	67	65	6e	74	3a	20	4d	6f	7a	.User-Ag	ent: Moz
69	6c	6c	61	2f	35	2e	30	20	28	57	69	6e	64	6f	77	illa/5.0	(window
73	20	4e	54	20	36	2e	31	3b	20	57	4f	57	36	34	3b	s NT 6.1	; WOW64;
20	72	76	3a	31	32	2e	30	29	20	47	65	63	6b	6f	2f	rv:12.0) Gecko/
32	30	31	30	30	31	30	31	20	46	69	72	65	66	6f	78	20100101	Firefox
2f	31	32	2e	30	0d	0a	41	63	63	65	70	74	3a	20	74	/12.0..A	ccept: t
65	78	74	2f	68	74	6d	6c	2c	61	70	70	6c	69	63	61	ext/html	, applica
74	69	6f	6e	2f	78	68	74	6d	6c	2b	78	6d	6c	2c	61	tion/xht	ml+xml,a

Failles des services réseaux

Considérations générales (3)

- Les services sont très bavards

Les informations de votre système

Nous pouvons voir que votre ordinateur utilise le système d'exploitation :

Windows Seven

Votre navigateur est :

Mozilla Firefox

Votre écran a une resolution de :

720x1280 pixels

```
...-Tj.. 3&....E.  
..6S@... 9.?...$..  
.C.P.b73 W .V9hP.  
.....HT TP/1.1 3  
02 Found ..Server  
: Apache ..X-Back  
end-Serv er: boun  
cer10.we bapp.phx  
1.mozill a.com..C  
ache-Con trol: ma  
x-age=15 ..Conten  
t-Type: text/htm  
l; chars et=UTF-8  
..Date: Wed, 06  
Feb 2013 15:34:2
```


Failles des services réseaux

HTTP

Serveurs trop bavards

Les bannières des serveurs web sont trop explicites.

```
GET / HTTP/1.1..  
Host: www.google.fr.  
User-Agent: Mozilla/5.0 (Windows NT 6.1)  
Firefox/26.0..  
Accept: text/html,application/xhtml+xml,  
Accept-Language: fr,fr-fr;q=0.8,en-us;
```

Failles des applications web

- Certains navigateurs peuvent remonter l'arborescence des fichiers du serveur
- Les scripts mal conçus peuvent poser des problèmes

Faibles des services réseaux

FTP

Non cryptage des données

Les mots de passe associés aux logins circulent en clair à la merci des « sniffers ».

FTP	140 Response: 220 Serveur de mise a jour des pages perso de Free.fr version
FTP	67 Request: USER ffctlr
TCP	54 ftp > 49794 [ACK] Seq=87 Ack=14 Win=4380 Len=0
FTP	89 Response: 331 Password required for ffctlr.
FTP	69 Request: PASS ce2f3t
FTP	82 Response: 230 User ffctlr logged in.

FTP anonyme

une mauvaise gestion des droits d'accès peut laisser trop de répertoires en droit d'écriture et/ou d'exécution. Un pirate peut y installer ou y exécuter des codes malveillants.

Attaque par rebonds

Ces attaques consistent à utiliser un serveur FTP anonyme comme relais pour se connecter à d'autres serveurs FTP.

Failles des services réseaux

TELNET

L'échange « Telnet » repose généralement sur une authentification par login et mot de passe. Les mots de passe associés du login circulent en clair sur le réseau.

```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\image-port10-2011>Telnet www.google.fr 80_
```

```
"GET /"
```

```
HTTP/1.0 302 Found
Location: http://www.google.fr/?gfe_rd=ctrl&ei=n9gWU_GtNJKAjwe9-4DIBw&gws_rd=cr
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Set-Cookie: PREF=ID=65a03484b2280177:FF=0:TM=1394006175:LM=1394006175:S=DjKdxU7G
ewwufaGW; expires=Fri, 04-Mar-2016 07:56:15 GMT; path=/; domain=.google.com
Set-Cookie: NID=67=v1BSH9N1-25DBKg9SAfs9GwGrQ8JrMnRBAE3_WXcpNWmuWmNCswk7qYB0ad6e
Kps9AZMseFeS5A1JuYma7-BJZvRNMz878u03w4T5stG7rPXJet6eoEFo1mgE3i0bDy; expires=Thu
, 04-Sep-2014 07:56:15 GMT; path=/; domain=.google.com; HttpOnly
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/bi
n/answer.py?hl=en&answer=151657 for more info."
Date: Wed, 05 Mar 2014 07:56:15 GMT
Server: gws
Content-Length: 274
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Alternate-Protocol: 80:quic

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
```

Failles des services réseaux

Fichiers temporaires

Une **mémoire cache** ou **antémémoire** est, une mémoire qui enregistre temporairement des copies de données que vous utilisez (Fichiers de travail) , afin de diminuer le temps d'accès (en lecture ou en écriture)

Ainsi le navigateur conserve les pages Web, images et autres fichiers sur votre PC.

Grâce à ce cache, le navigateur n'a plus à télécharger, à chaque visite, la (ou les) page(s) Web, car elles sont déjà sur le disque dur. Mettre les pages en cache accélère donc la navigation (notamment si on visite plusieurs fois la même page).

Faibles des services réseaux

Fichiers temporaires

On trouve des zones de cache un peu partout :

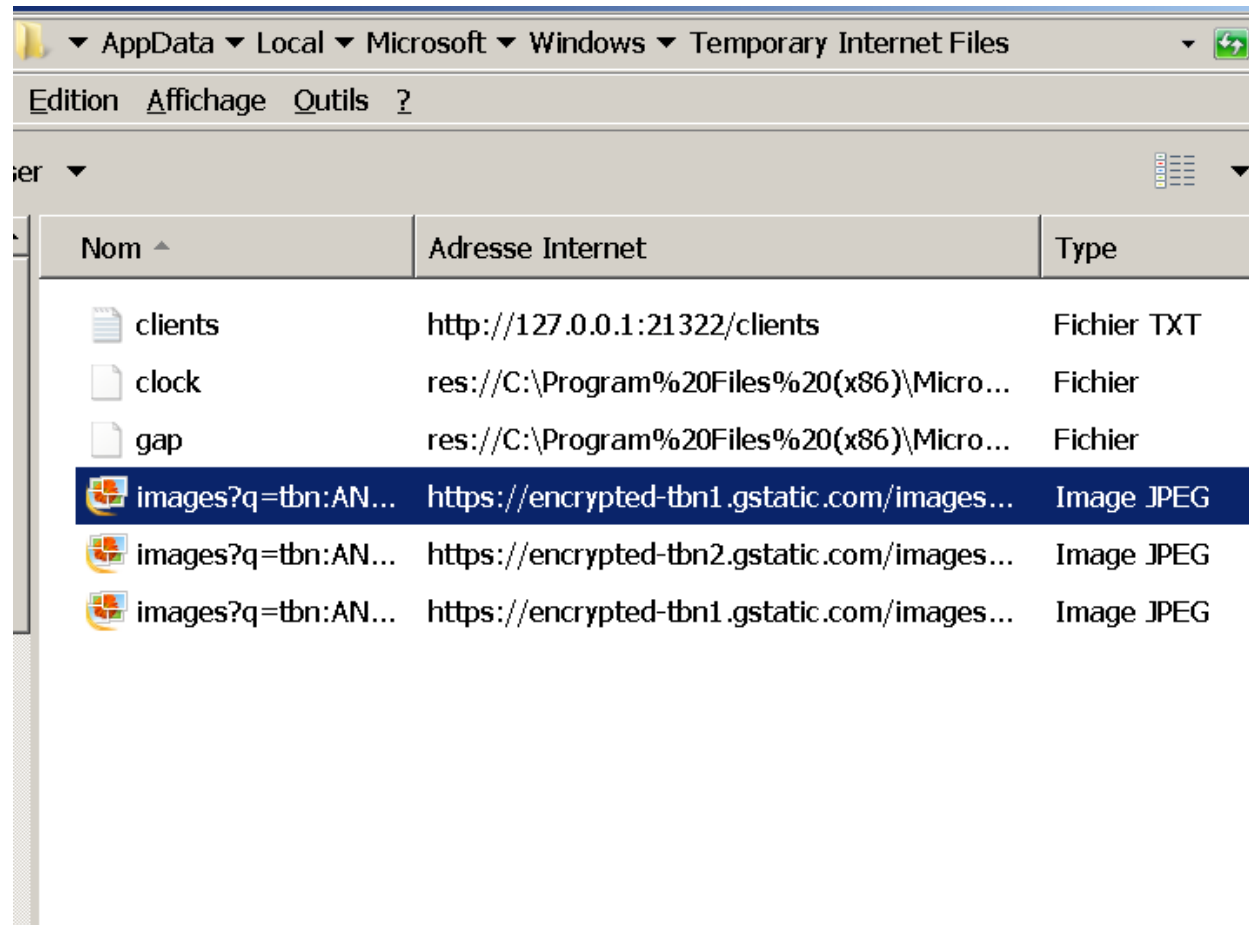
- dans les disques durs ;
- dans les serveurs proxy;
- dans les serveurs de pages dynamiques ;
- dans les mémoires gérées par les bases de données

Problème, c'est que ces zones sont :

- souvent situées dans des dossiers par défaut ;
- facilement accessibles ;

Failles des services réseaux

Fichiers temporaires



The screenshot shows the 'Temporary Internet Files' folder in Windows Explorer. The address bar indicates the path: AppData \ Local \ Microsoft \ Windows \ Temporary Internet Files. The menu bar includes 'Edition', 'Affichage', 'Outils', and '?'. The view is set to 'Icones'. The file list is as follows:

Nom	Adresse Internet	Type
clients	http://127.0.0.1:21322/clients	Fichier TXT
clock	res://C:\Program%20Files%20(x86)\Micro...	Fichier
gap	res://C:\Program%20Files%20(x86)\Micro...	Fichier
images?q=tbn:AN...	https://encrypted-tbn1.gstatic.com/images...	Image JPEG
images?q=tbn:AN...	https://encrypted-tbn2.gstatic.com/images...	Image JPEG
images?q=tbn:AN...	https://encrypted-tbn1.gstatic.com/images...	Image JPEG

Panneau configuration → Options Internet → Paramètres Navigation → Afficher Fichiers

Failles des services réseaux

Fichiers temporaires

```
Répertoire de C:\Users\image-port10-2011\AppData\Local\Microsoft\Windows\Temporary Internet Files
03/03/2014  21:27    <REP>          .
03/03/2014  21:27    <REP>          ..
03/03/2014  20:56    <REP>          Content.IE5
03/03/2014  21:09    <REP>          Content.MSO
12/10/2012  06:51    <REP>          Content.Outlook
03/03/2014  21:36    <REP>          Content.Word
05/05/2013  12:55             128 counters.dat
03/03/2014  21:27             84 desktop.ini
03/03/2014  17:37    <REP>          Low
03/03/2014  17:37    <REP>          Sqm
01/06/2012  08:07    <REP>          Virtualized
                2 fichier(s)                212 octets
                9 Rép(s)  72 720 367 616 octets libres
```

Le même dossier via les commandes Dos

Failles des services réseaux

Fichiers temporaires

Parmi cette liste de sites, vous avez visité....

	Wikipedia : fr.wikipedia.org/	✓
	Twitter : twitter.com/#	✓
	Pages jaunes : www.pagesjaunes.fr	✓
	Google : www.google.fr/	✓
	Facebook : www.facebook.com	✓
	Comment ça marche : www.commentcamarche.net	✓



Autres aspects de la sécurité

Data Center et Big Data

Le Data Center ou Centre de données

Définition : infrastructure physique composée d'un réseau d'ordinateurs et d'espaces de stockage.



Selon le site Data Center Map, il y en aurait **4 081 répartis dans 118 pays**. Les géants du Web, Google, Amazon, Facebook ou Apple, mais aussi des opérateurs télécoms,

Le Data Center ou Centre de données

A quoi ressemble un data center ?



China Telecom Inner Mongolia Information Park – Hohhot

Le plus gros data center mondial
(du moment) , occupe une
surface de 1 million de mètres
carrés

Sa capacité totale doit atteindre 100 000 racks et 1,2 millions de serveurs, pour un coût total évalué à 3 milliards de dollars.

Le Data Center ou Centre de données

Comment on décide-t-on de localiser un Data Center ?

Critères de choix :

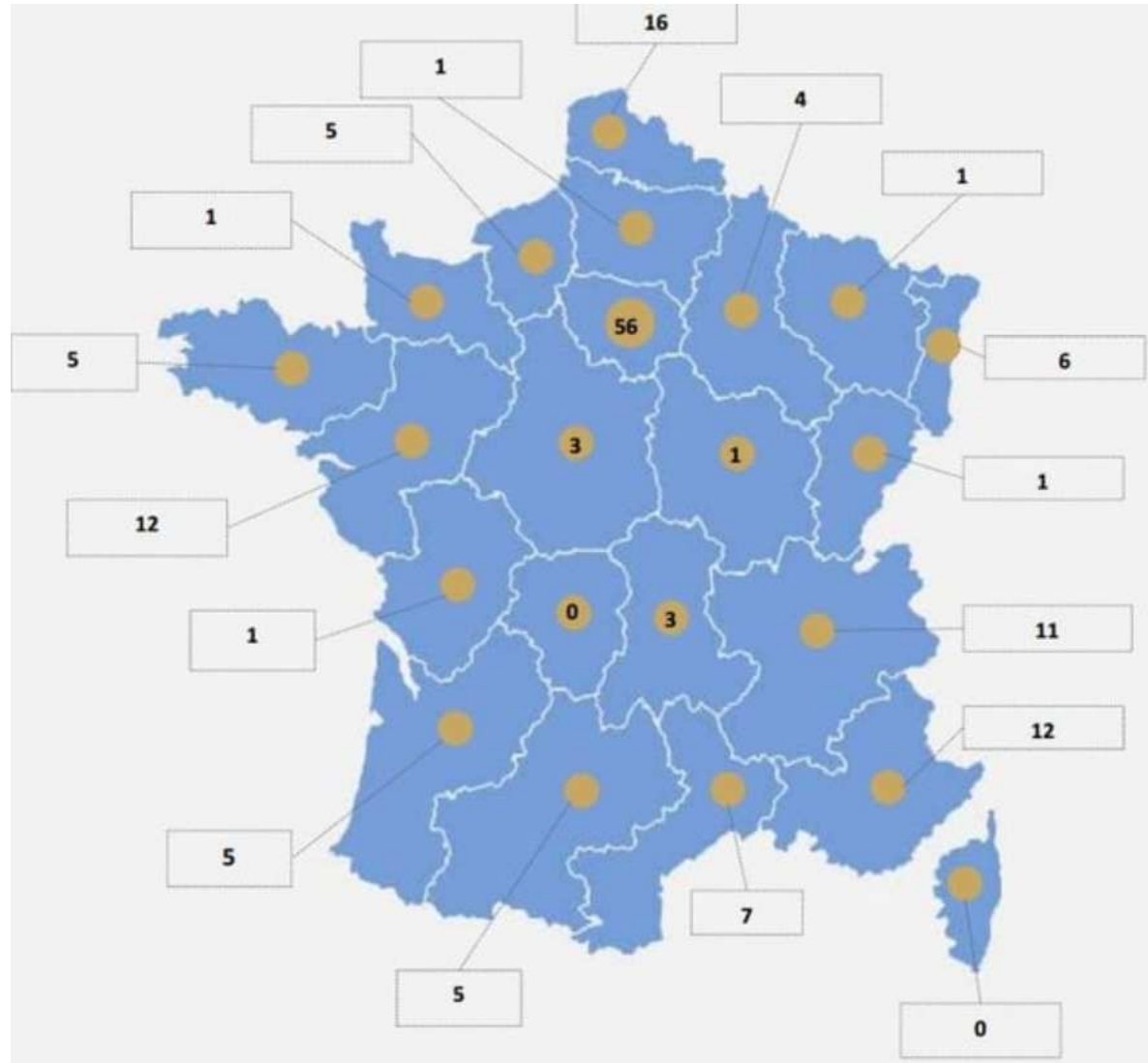
- coût et des taxes,
- localisation géographique,
- stabilité météorologique,
- accès aux routes et aux aéroports,
- disponibilité énergétique,
- télécommunications
- environnement politique.

Le Data Center ou Centre de données

Les Data Center en France

Il existe plus d'une
centaine de data
centre en France.

Chaque région en possède au moins un.



Le Data Center ou Centre de données

Les Data Center a Montpellier



OC3 network



AGS Cloud, nouveau data center à
St aunes – Octobre 2018



Ovea Data
Center à
Montpellier

Le Data Center ou Centre de données

Les Data Center



#Cybersécurité : risques liés à l'hébergement des données dans les #datacenters et le #cloud



INGERENCE ECONOMIQUE

Flash n° 35 - Septembre 2017

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

LE 05 OCTOBRE 2018 / DATACENTER

Des composants espions chinois retrouvés sur des serveurs

La Chine aurait infiltré Amazon, Apple et d'autres sociétés américaines en installant des composants espions sur les cartes mères serveurs fournies par SuperMicro.

GOOGLE PERD DES DONNÉES APRÈS L'ATTAQUE DE LA FOUDRE SUR UN DATA CENTER

Alex 27 août 2015 Data Center Ecrire un commentaire

C'est une actualité qui risque de faire des nuages sur l'image de **Google**. Le plus grand moteur de recherche a été **victime d'une foudre ayant frappé un de ses Data Center en Belgique le 13 août dernier**.

La sécurité, un enjeux stratégique

Le Big Data (Méga Données)

Définition :

Le big data ou mégadonnées désignent l'ensemble des données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles.

Il désigne aussi un ensemble très volumineux de données sur lequel aucun outil classique de gestion de base de données ou de gestion de l'information peut travailler.



Le Data Center est un composant du Big Data.

Le concept date de 1997 mais est connu du public depuis 2012.

Le Big Data ou Grosses Données

Quelles informations y trouve-t-on ?

- Les sites sur lesquels on surfe,
- les mails ou messages envoyés,
- les applications des smartphones, les échanges sur les réseaux sociaux ,
- les transactions de commerce électronique ,
- les conversations téléphoniques,
- ...



mais aussi ...

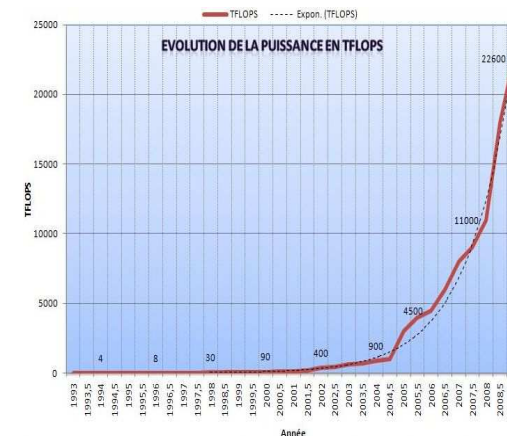
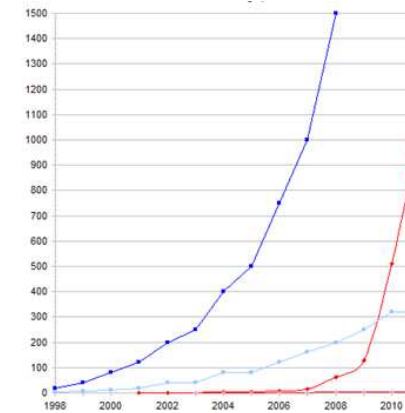
- les données géolocalisées (GPS) ,
- les machines connectées (frigos, téléviseurs, montres connectées, ...),
- les objets connectés (caméras, alarmes des maisons, portes électroniques, thermostats, compteur Linky, ...)

Le Big Data ou Grosses Données

Pourquoi le Big Data se développe ?

Le big data a suivi l'évolution :

- des supports de stockage,
- des traitement des données (notamment avec le cloud),
- des supercalculateurs,
- des réseaux



Le Big Data ou Grosses Données

Quel volume de données ?

On parle de pétaoctets et de zettaoctets pour désigner les volumes que représentent les big data. Selon les prévisions du cabinet IDC, le volume de données produites dans le monde attendra les 40 zettaoctet en 2020.

Quelques chiffres :

En 2003, il s'est enregistré 5 Eo (exaoctets) de données sur l'année (= 1000 Po ou 5 millions de To ou 5 milliards de Go)

En 2011 5 Eo étaient produits en 2 jours

En 2013 5 Eo étaient produits en 10 minutes

En 2017 on produit 1 Zo par an = 1000 Eo

Plus de 90% des données disponibles aujourd'hui ont été produites ces 2 dernières années.

Le Big Data ou Grosses Données

Que fait-on de ces données ?

L'exploitation des big data ouvre de nouvelles perspectives dans : la recherche scientifique, la politique, la communication, la médecine, la météorologie, l'écologie, la finance, le commerce, etc.

Grâce à de nouveaux outils il est possible de :

- faire de l'analyse tendancielle ou prédictive,
- dresser des profils,
- anticiper des risques,
- suivre des phénomènes en temps réel
- ...

→ **Intelligence artificielle**



Le Big Data ou Grosses Données

Que fait-on de ces données ?

Une des applications des plus connues est de mieux connaître le consommateur afin de lui proposer des produits toujours plus adaptés à ses besoins et au final de faire vendre quelque chose.

Vos articles vus récemment et vos recommandations en vedette

Inspiré de votre historique de navigation



 Nikon D3400 pour les Nuls grand format Julie ADAIR KING ★★★★★ 7 Broché EUR 22,95 ✓prime	 Awinner en verre pour Nikon D3200 D3400 D3300 D3100, Camera Protection... ★★★★☆ 4 EUR 7,32 ✓prime	 AFUNTA Films de Protection d'Ecran pour Nikon D3100 D3200 D3300 D3400, 2... ★★★★★ 16 EUR 7,99 ✓prime	 EN-EL14/EL14a Batterie de rechange (2 paquets) et Chargeur Double Intelligent... ★★★★★ 13 EUR 27,99 ✓prime	 Tamron Objectif AF 70-300mm F/4-5,6 Di LD IF Macro 1/2 - Monture Nikon ★★★★☆ 530 EUR 104,90 ✓prime	 Nikon D3400 for Dummies Julie Adair King Broché EUR 17,17
--	--	--	---	---	---

Vous avez vu



Aff
mc
his
na

Le Big Data ou Grosses Données

En conclusion - Les impacts du big data

Le Big Data est considéré comme une nouvelle révolution industrielle semblable à la découverte de la vapeur (début du 19e siècle), de l'électricité (fin du 19e siècle) et de l'informatique (fin du 20e siècle).

Le Big Data est considéré comme une source de bouleversement profond de la société. L'explosion des données oblige les chercheurs à trouver de nouvelles manières de voir et d'analyser le monde.

La majorité des applications qui seront utilisées pour capturer, stocker, analyser et présenter ces gros volumes des données sont encore à créer.