Administration système

Gestion des vulnérabilités

Gestion des correctifs

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)

VM | VULNERABILITY MANAGEMENT

Inventaire des vulnérabilités
Rapports d'audit

IM | INFRASTRUCTURE MANAGEMENT

Découverte réseau
Documentation
Gestion du changement

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

DM | DESKTOP MANAGEMENT

Inventaire
Télé-distribution
Administration à distance
Supervision

PM | PATCH MANAGEMENT

Recherche des patches
Inventaire des patches
Déploiement de patches

...

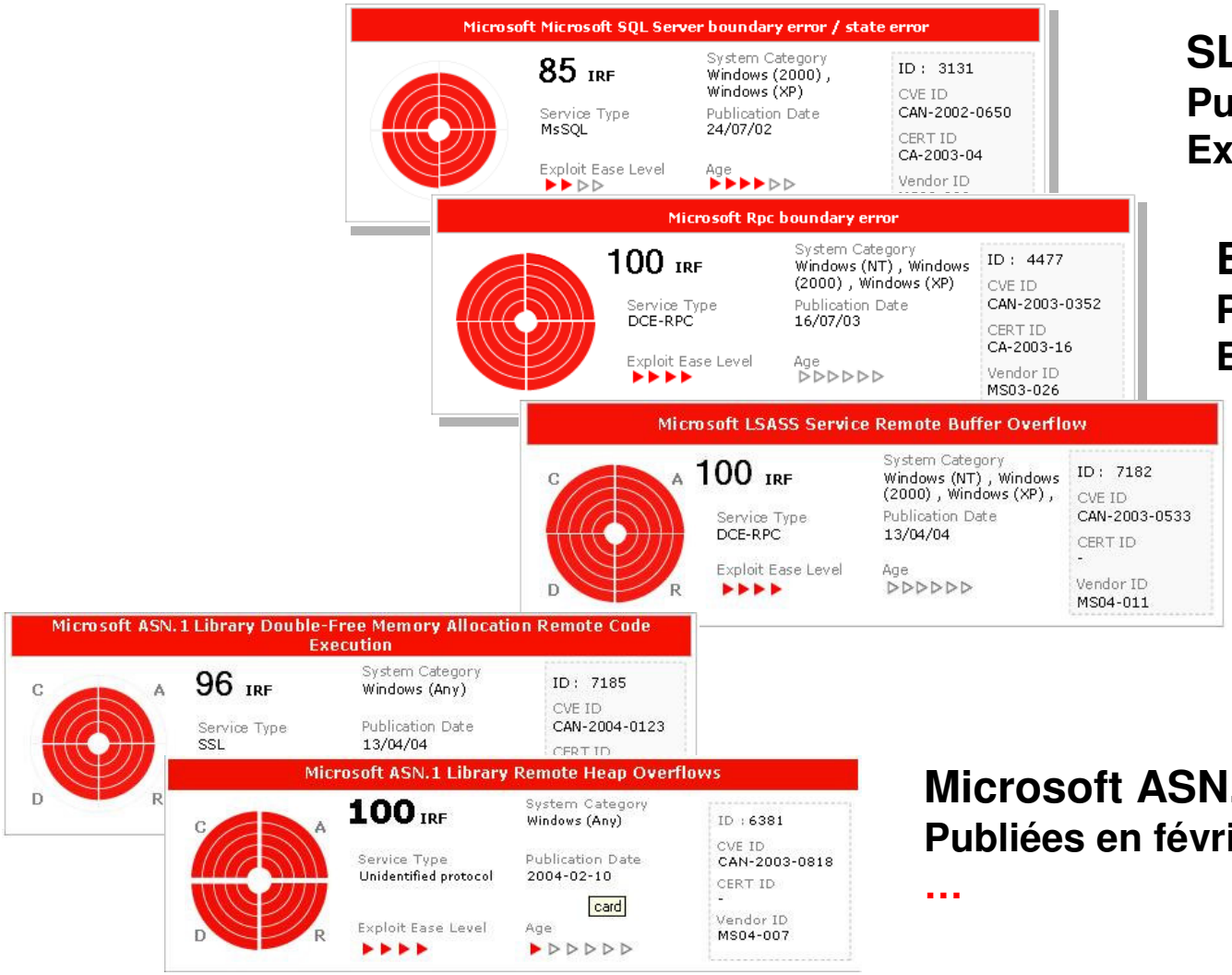
More to come…

criston
Secure Desktop Management

VULNERABILITY MANAGER

VM | VULNERABILITY MANAGEMENT

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



SLAMMER
Publiée en juillet 2002
Exploitée en janvier 2003

BLASTER / SOBIG
Publiée en juillet 2003
Exploitée en août 2003

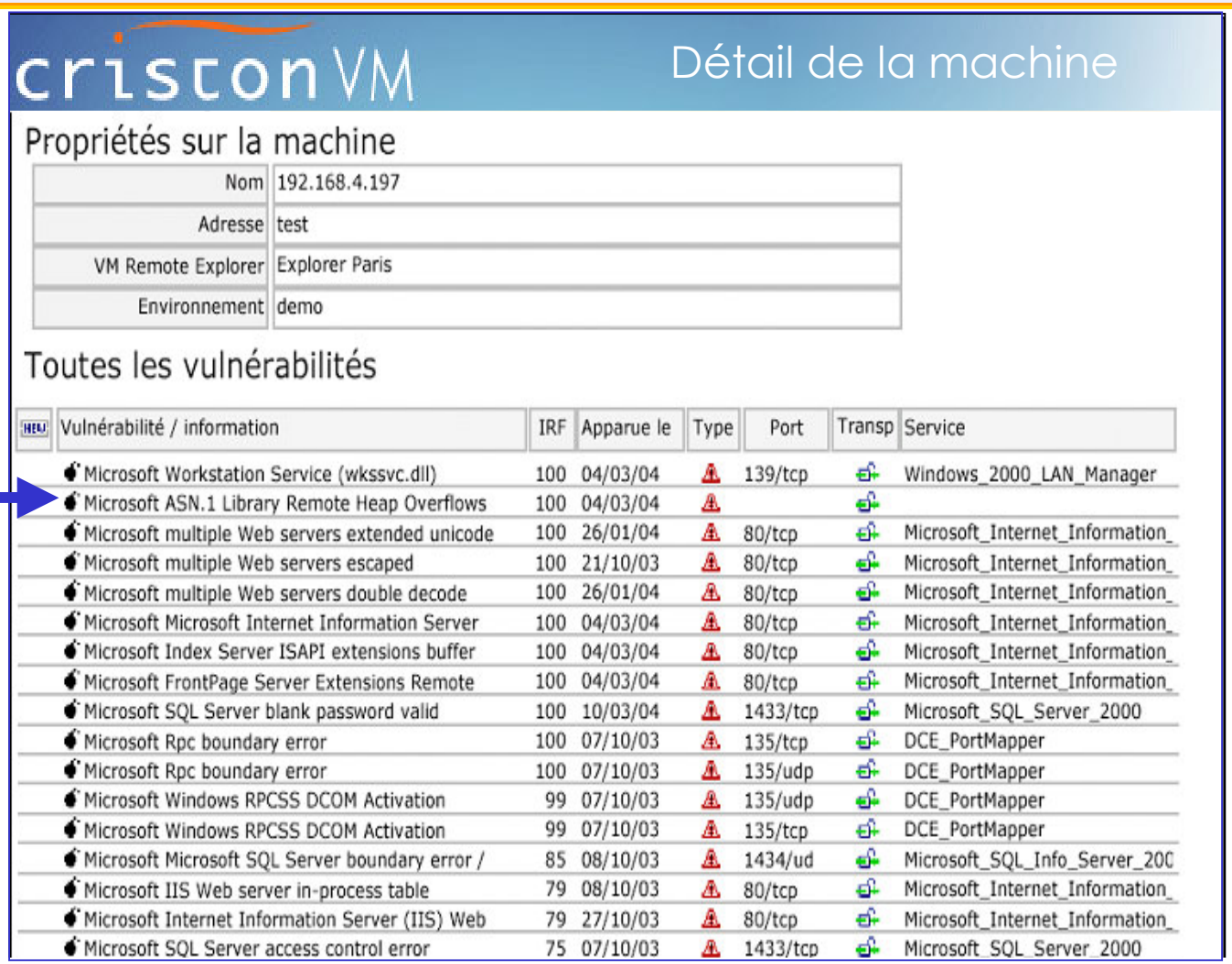
SASSER
Publiée le 13/04/2004
Exploitée le 01/05/2004

Microsoft ASN.1
Publiées en février et avril 2004
…

Choix d'une vulnérabilité critique

VM | VULNERABILITY MANAGEMENT

Microsoft ASN.1



criston VM

Détail de la machine

Propriétés sur la machine

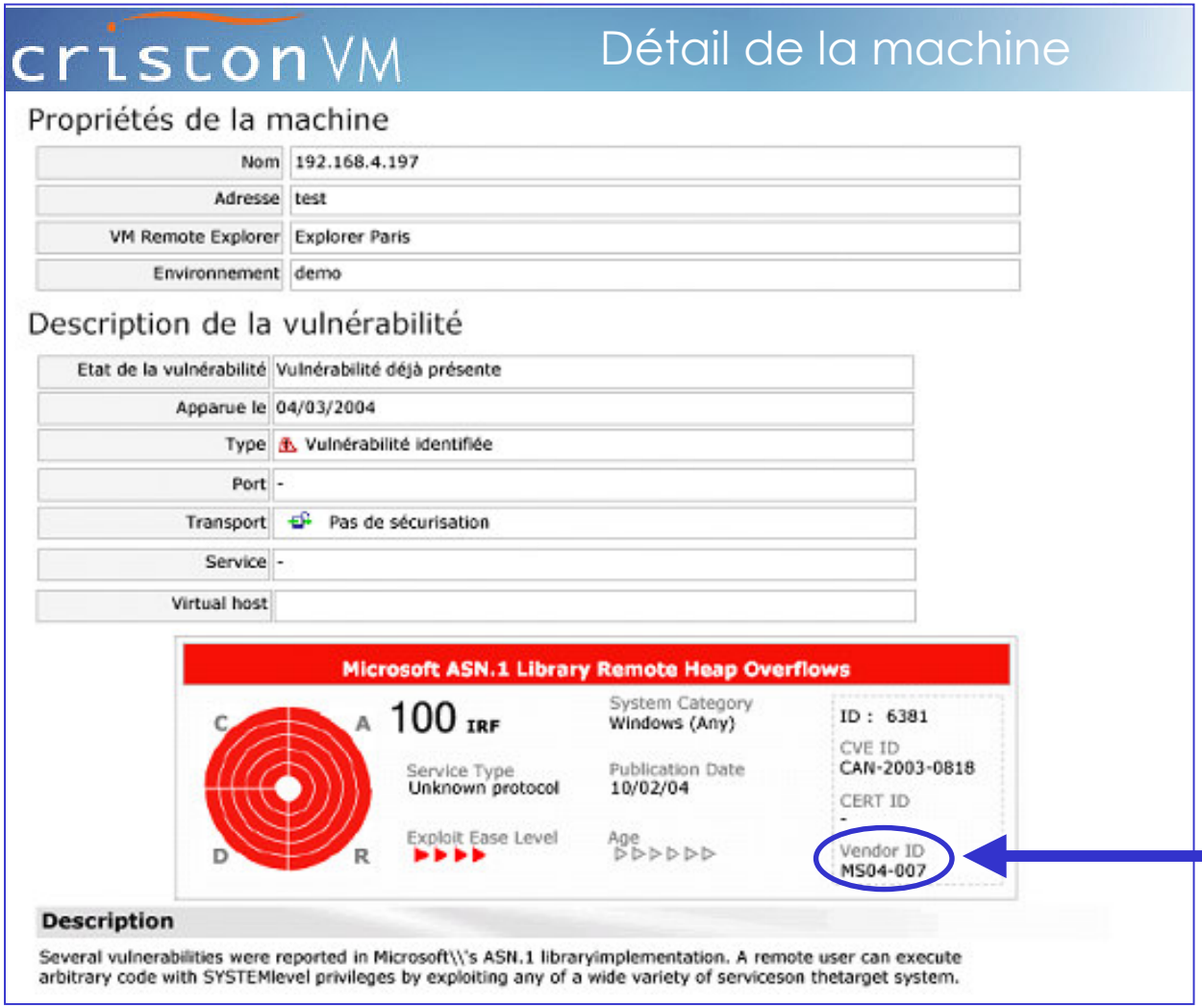
Nom	192.168.4.197
Adresse	test
VM Remote Explorer	Explorer Paris
Environnement	demo

Toutes les vulnérabilités

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

Détail de la faille ASN.1

VM | VULNERABILITY MANAGEMENT

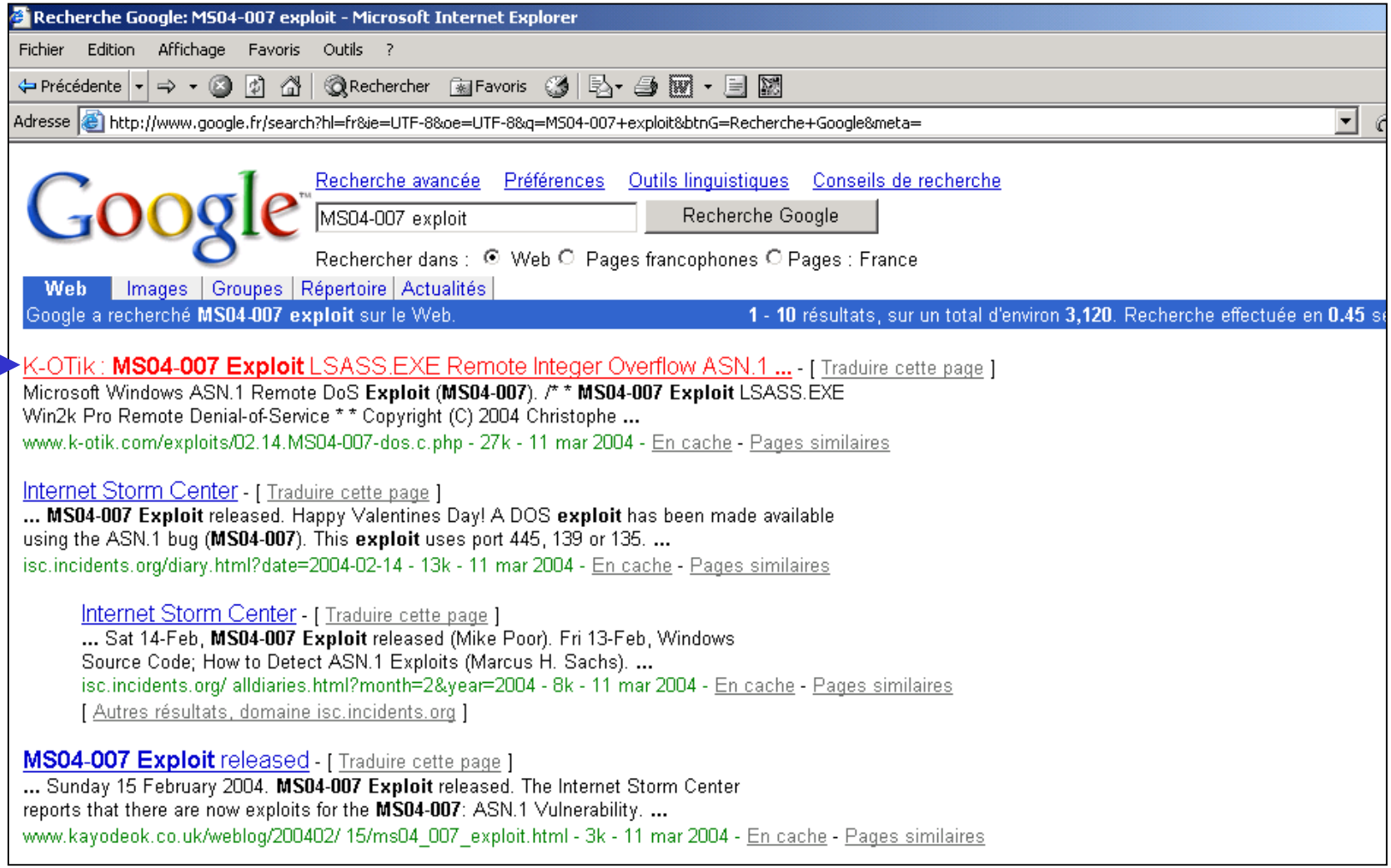


Référence Microsoft

criston
Secure Desktop Management

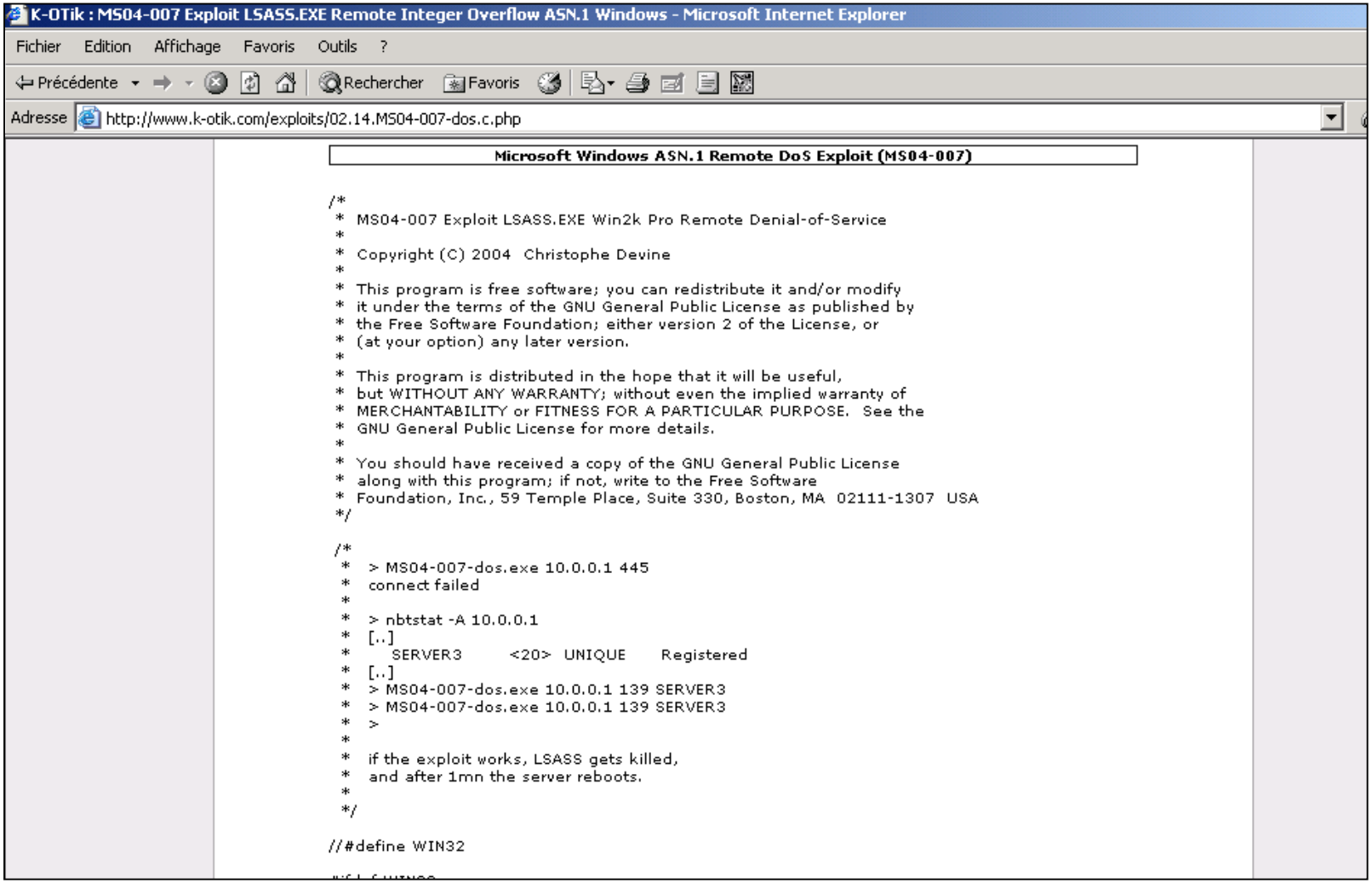
Recherche d'un exploit ASN.1

VM | VULNERABILITY MANAGEMENT



Recherche d'un exploit ASN.1

VM | VULNERABILITY MANAGEMENT



criston
Secure Desktop Management

Exploitation ASN.1 par le port 139

VM | VULNERABILITY MANAGEMENT

Ping de la cible

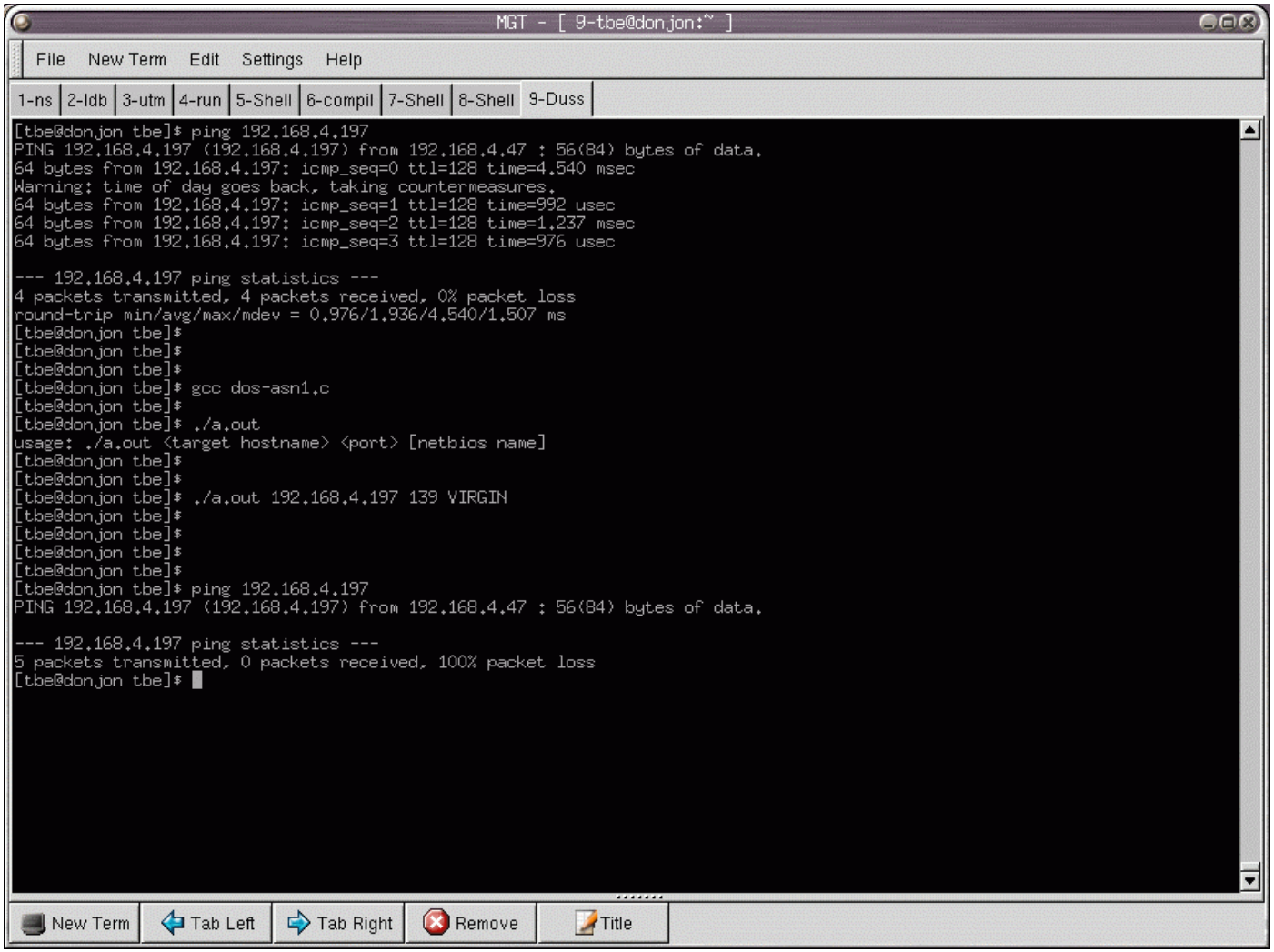
Cible « up »

Compilation exploit

Lancement exploit

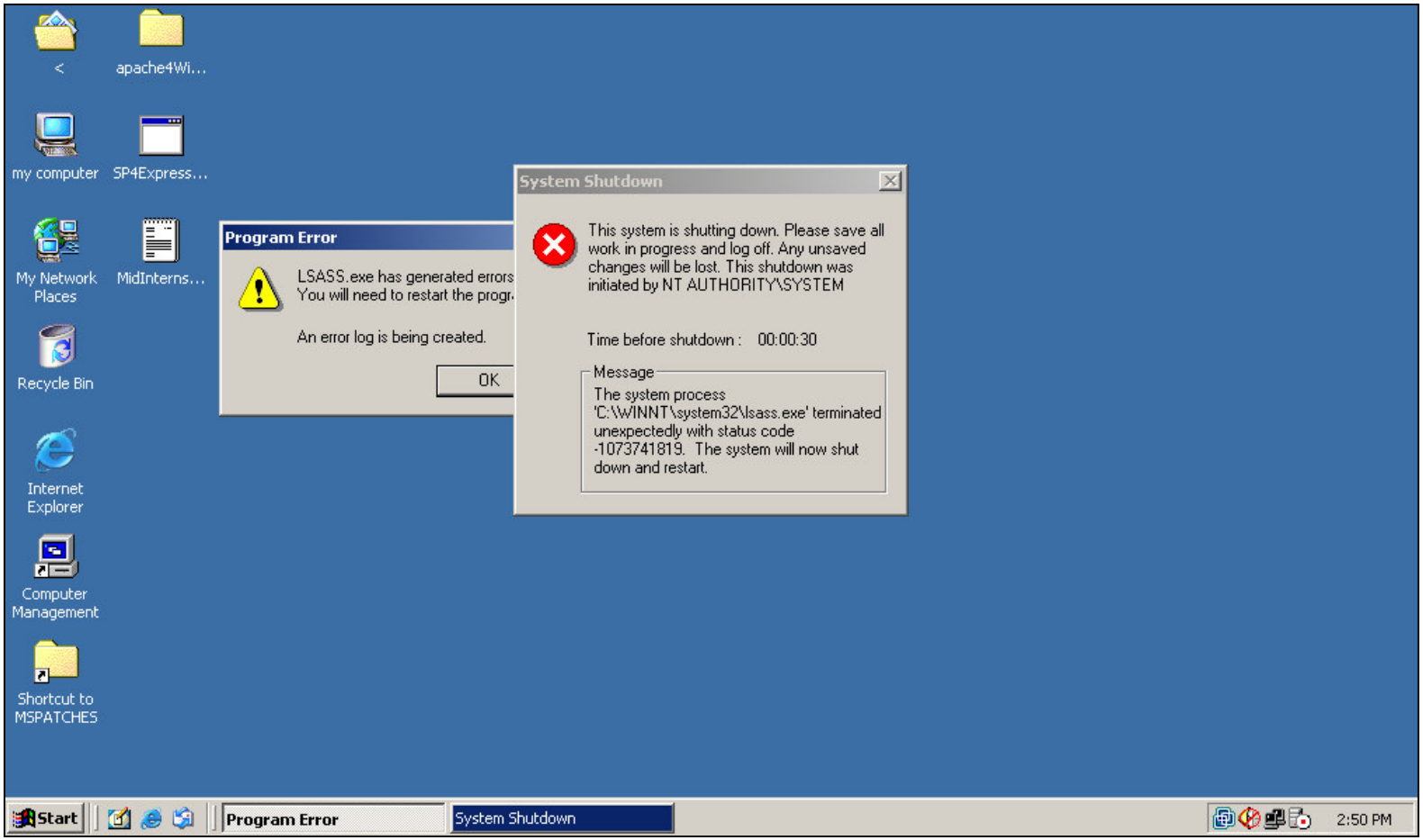
Ping de la cible

OK, Cible « down » !!



Effet sur la cible…

VM | VULNERABILITY MANAGEMENT



Risque inacceptable pour l'entreprise !

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

VM | VULNERABILITY MANAGEMENT

criston VM

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_

criston
Secure Desktop Management

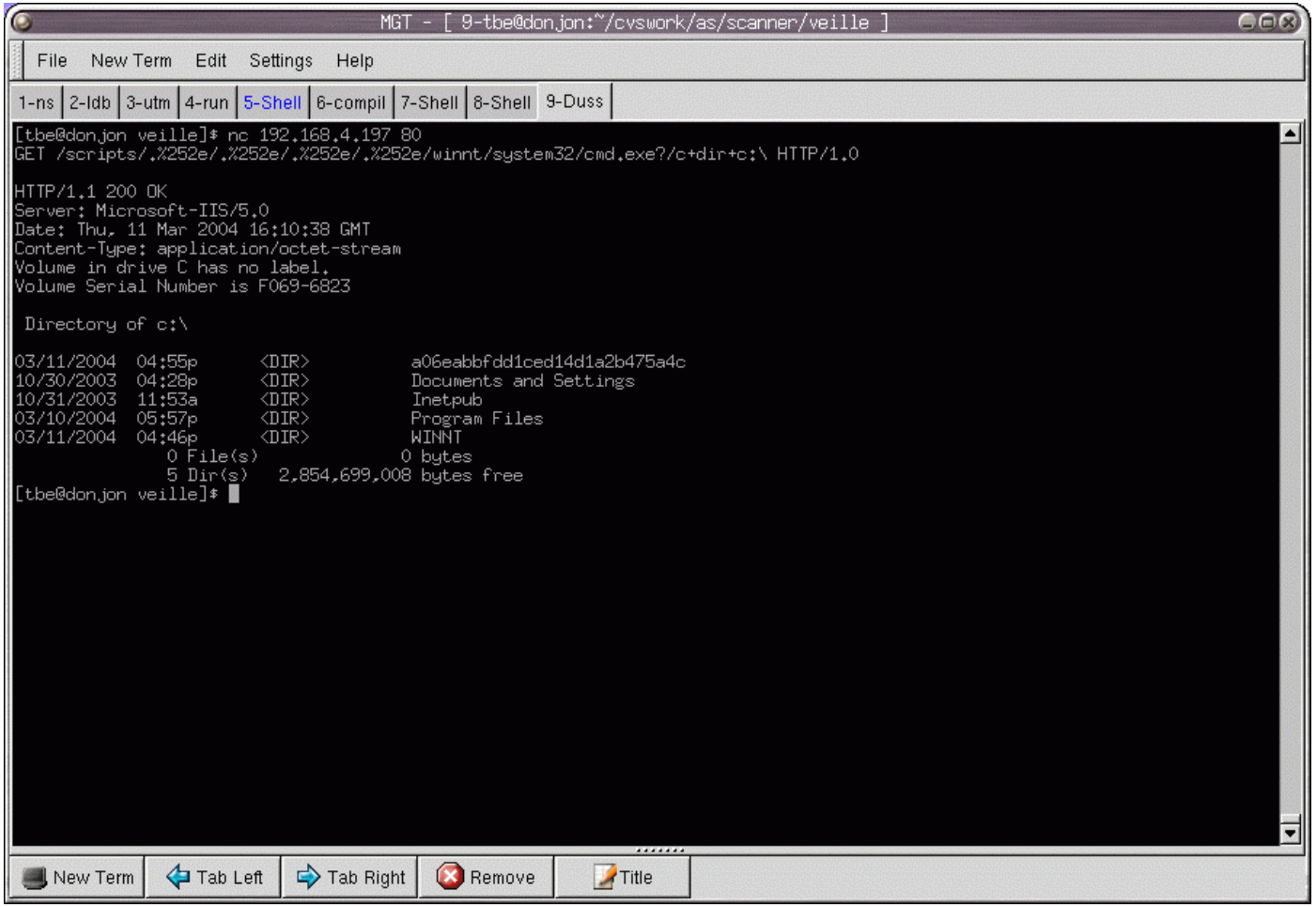
Exécution d'un « DIR » à partir du port 80 grâce à la faille "IIS Double decode"

VM | VULNERABILITY MANAGEMENT

Exécution de la commande « dir »

Ok, ça marche !

Liste des répertoires



criston
Secure Desktop Management

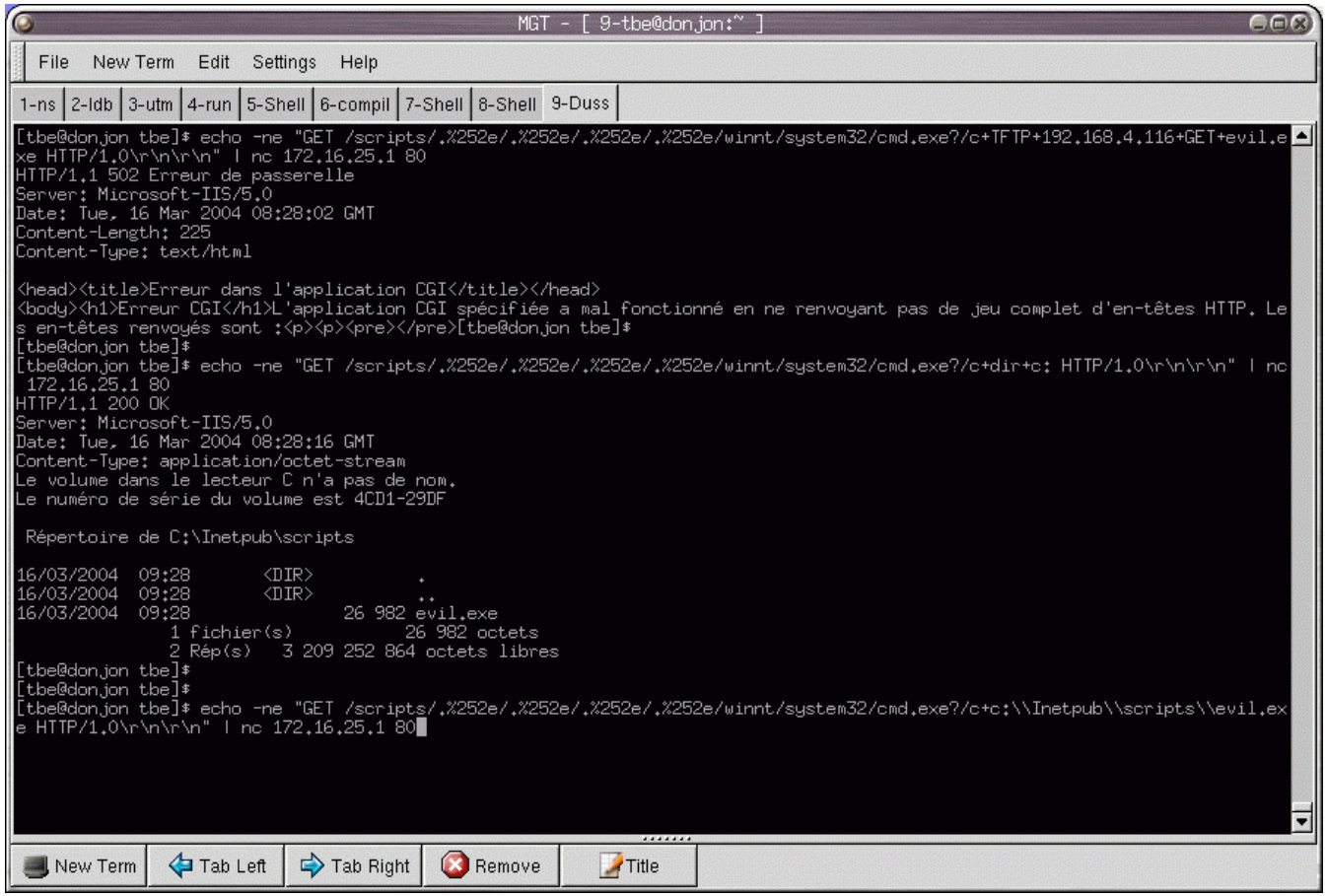
Chargement d'un programme sur la cible à partir du port 80

VM VULNERABILITY MANAGEMENT

Chargement d'un exécutable sur la cible

Exécution d'un "Dir" sur la cible

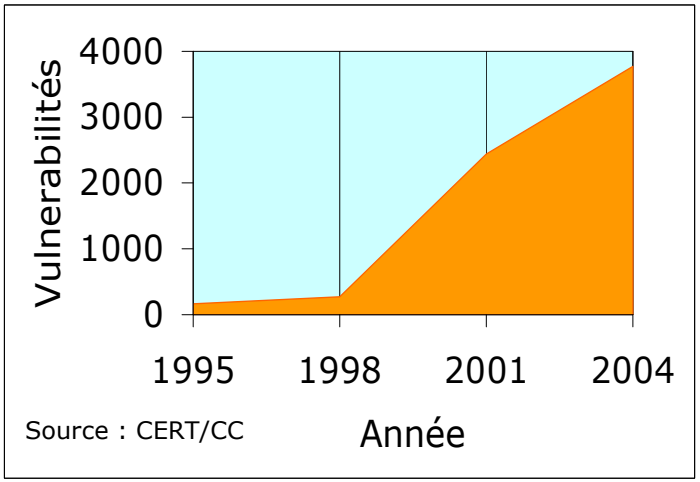
Le programme a bien été chargé sur la cible



Prise de contrôle de la machine malgré le FW !

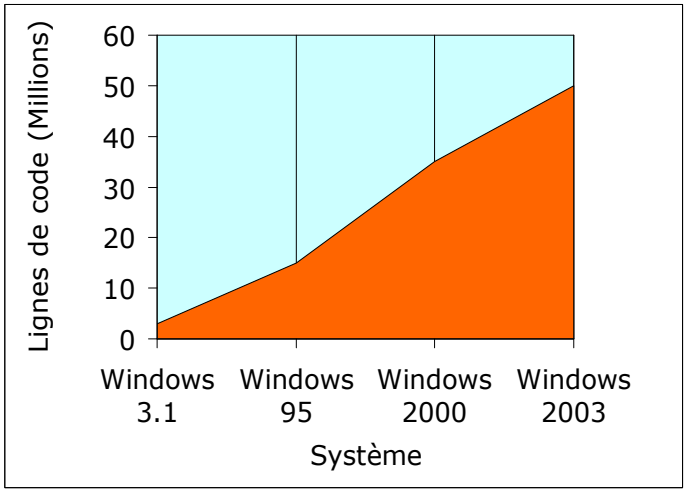
criston
Secure Desktop Management

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 »

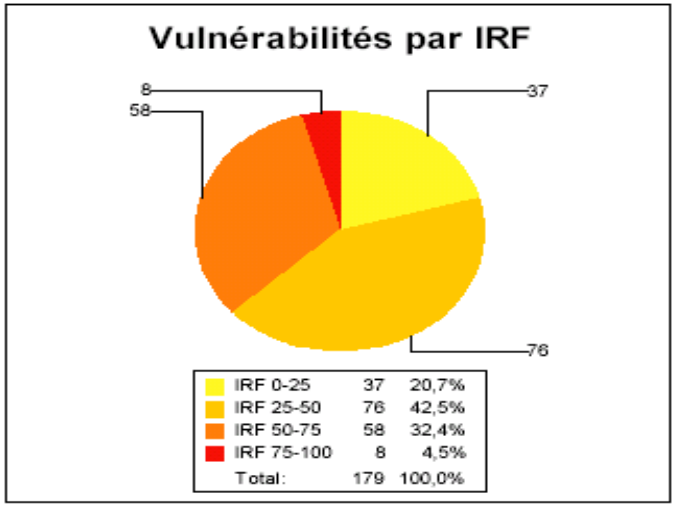
Gartner Inc

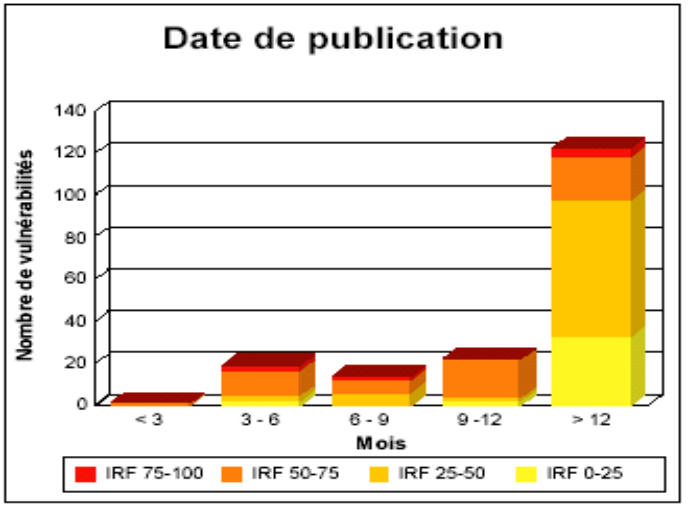
Criston Vulnerability Manager

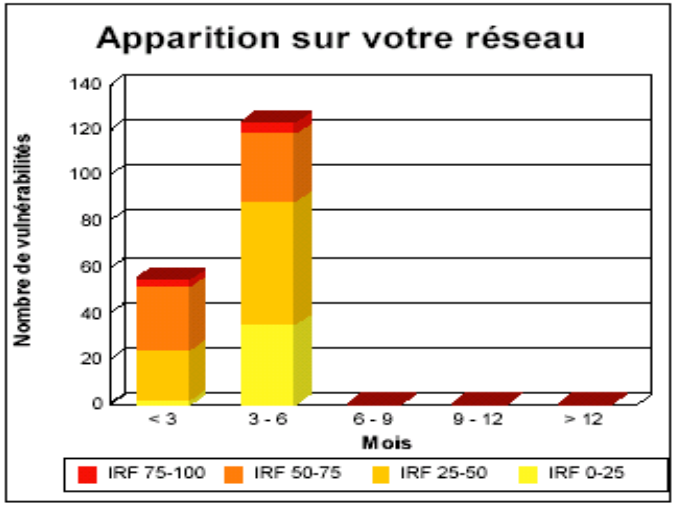
- ✓ Vulnerability Manager analyse votre réseau et réalise un inventaire de l'ensemble des machines réellement connectées.
- ✓ Vulnerability Manager recense automatiquement l'ensemble des vulnérabilités présentes dans votre SI et les classe par criticité.
- ✓ Pour chaque vulnérabilité identifiée, Vulnerability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

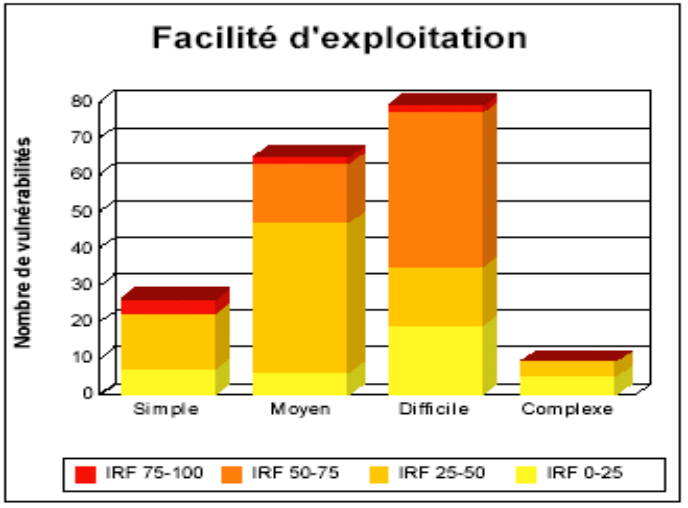
Vision globale des failles d'un domaine

Statistiques sur les vulnérabilités









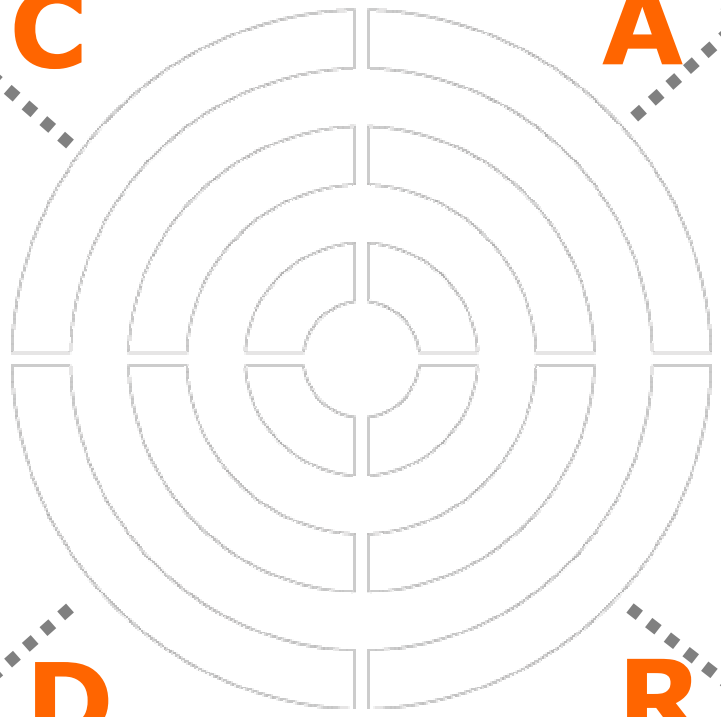
Analyse et mesure de l'impact des vulnérabilités : CARD

Atteinte à l'intégrité des données

C

A

Accès à des des données confidentielles



Indisponibilité de la machine

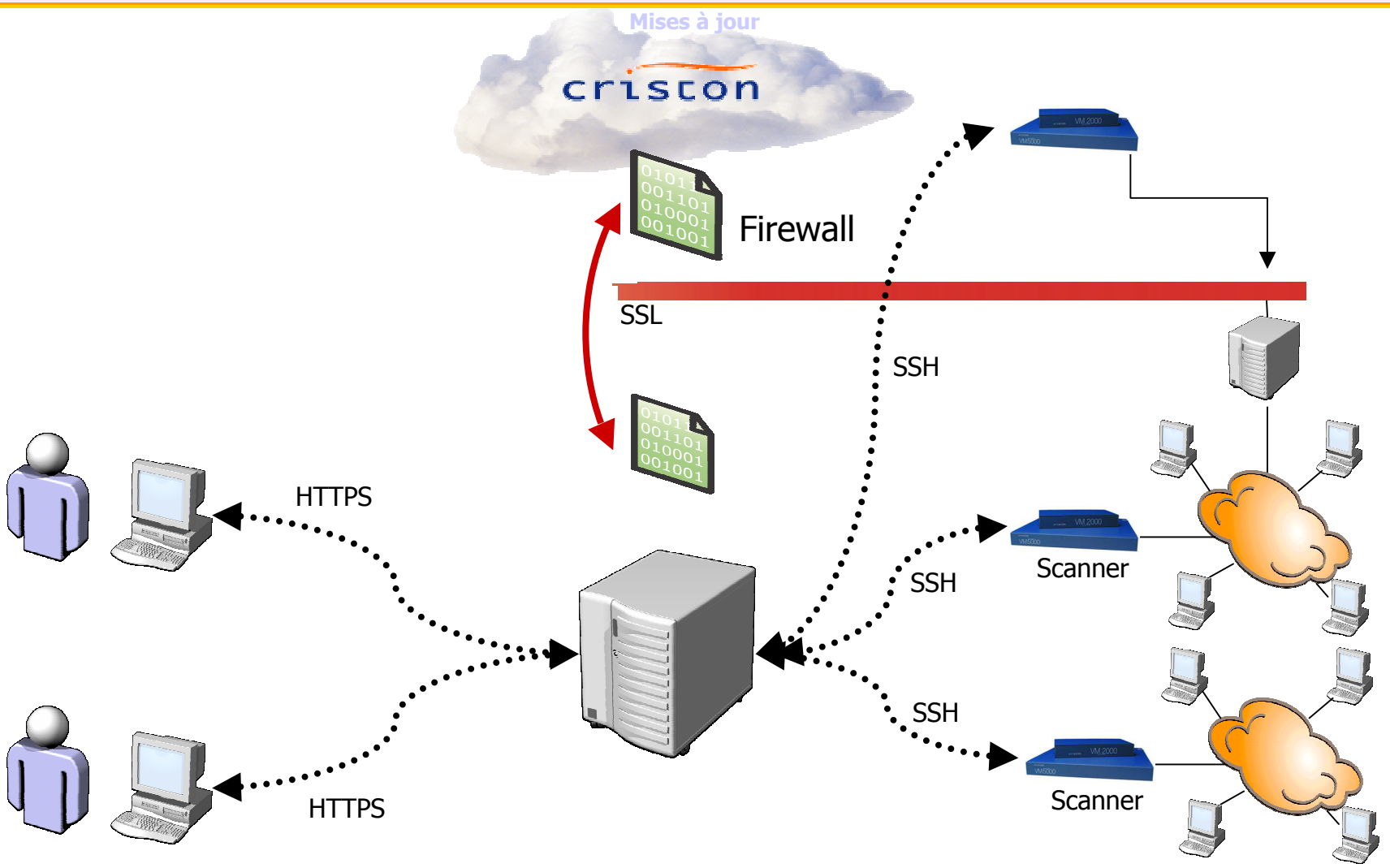
D

R

Prise de contrôle de la machine

Architecture

VM | VULNERABILITY MANAGEMENT



criston
Secure Desktop Management

Equipements et logiciels concernés

VM | VULNERABILITY MANAGEMENT

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