e-Xpert Solutions SA | 3, chemin du Creux | CH 1233 Bernex-Genève | Tél +41 22 727 05 55 | Fax +41 22 727 05 50

La citadelle électronique
Sécurité contre l'intrusion informatique
volume 1

Sylvain Maret / version 1.2

Octobre 2004

“ L’art de fortifier ne consiste pas dans des règles et des systèmes mais uniquement dans le bon sens et l’expérience ”

Sebastien le Prestre de Vauban
Ingénieur Architecte 1633-1707

- Deux grands axes
  - Les attaques
  - Les outils à disposition
- Le cours n'est pas exhaustif
  - Chaque sujet est une spécialité
  - Tous les jours des nouvelles techniques
- Ethical Hacking
  - Connaître les méthodes pour mieux se défendre
  - Aucun nom de programmes de hacking « destructif »

Programme du cours: volume 1

- Définition de la sécurité informatique
- Estimation du risque
- Les menaces
- Les vulnérabilités
- CVE
- Evolution dans le temps

- Programme du cours: volume 1

- Obtention d'informations
- Scanners
- Social Engineering
- Virus, Trojan, Backdoor
- DoS, DDoS
- SMTP
- Compromission Système
- BoF
- Sniffer
- Web
- Wireless
- Etc.

- Programme du cours: volume 2

- Les outils de sécurité
  - Firewall
  - IDS
  - Honeypot, Honeynet
  - Systèmes d'authentification
  - PKI
  - Proxy
  - VPN
  - Etc.

La sécurité informatique ?

- Protection du système d'informations
  - les biens de l'entreprise
- Une démarche globale
  - Engagement de la direction de l'entreprise
  - Classification des biens
    - Estimation des risques
  - Définition d'une politique de sécurité
  - Mise en oeuvre de la politique de sécurité
- Une démarche constante

Définition: système d'informations

- Organisation des activités consistant à acquérir, stocker, transformer, diffuser, exploiter, gérer … les informations
- Un des moyens pour faire fonctionner un système d'information est l'utilisation d'un **système informatique**

Exemple de biens informatiques

- Le système de production
  - Industrie, Banques
- Les informations financières
- Les informations commerciales
- Le système de commerce électronique
- Les bases de données
- Les brevets, inventions
- Etc.

Les objectifs de sécurité

- Diminution des risques (tendre vers zéro…)
- Mettre en œuvre les moyens pour préserver:
  - La confidentialité
  - L'intégrité
  - L'authentification
  - L'autorisation
  - La non-répudation
  - La disponibilité

- Estimation du risque

$

Risque = Coûts * Menaces * Vulnérabilités

Les coûts d'une attaque ?

- Déni de services (perte de productivité)
- Perte ou altération des données
- Vol d'informations sensibles
- Destruction des systèmes
- Compromission des systèmes
- Atteinte à l'image de l'entreprise
- Etc.

- Les menaces: communauté « Black Hat » ou « Hackers »

Source: CERT 2002

- Les « Black Hat » sont de mieux en mieux organisés
  - Sites Web
  - Conférences
- Attaques sur Internet sont faciles et difficilement identifiables (peu de traces)
- Outils d'intrusion sont très évolués et faciles d'accès

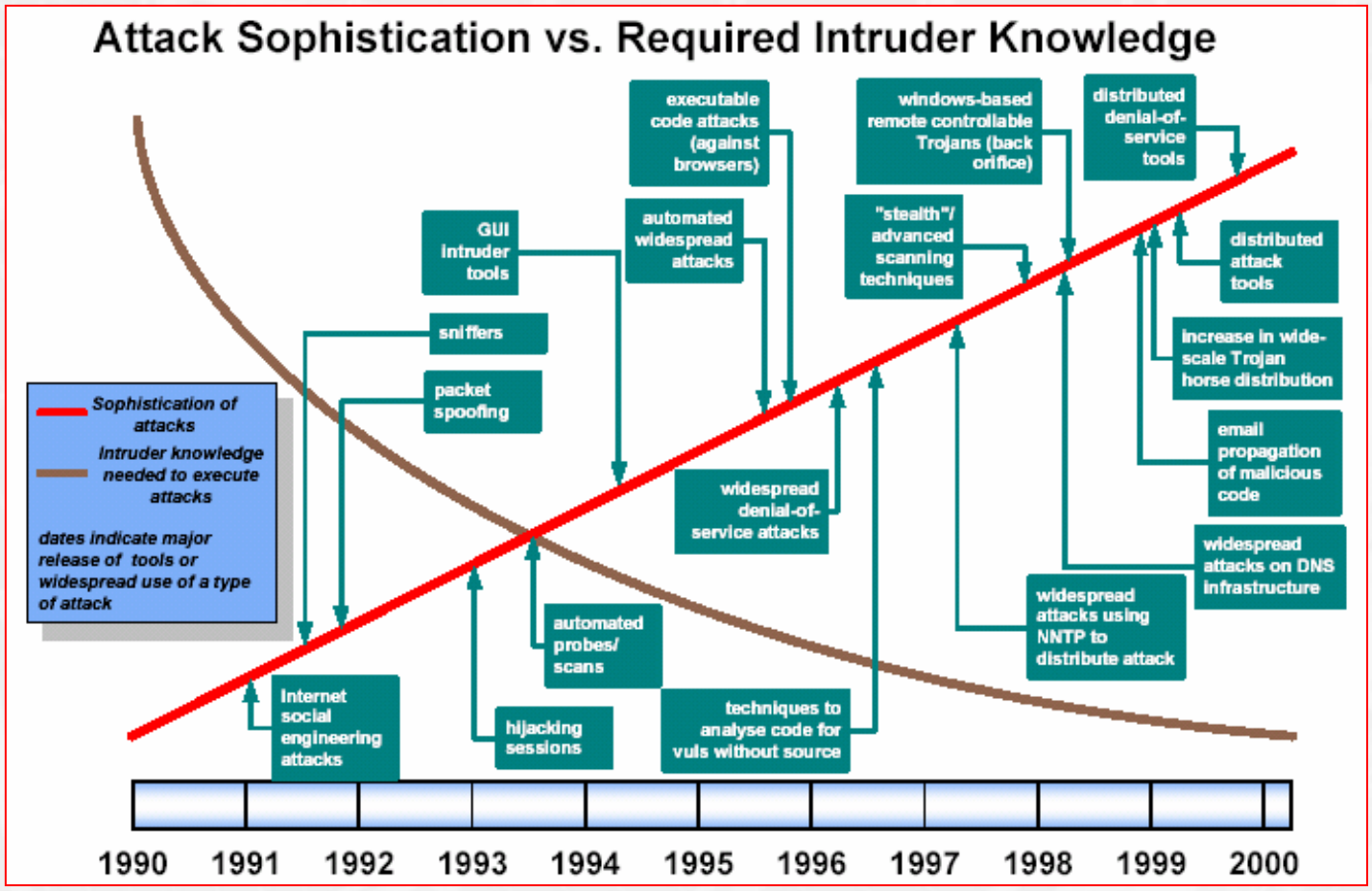
- Sources d'informations

- Sites Internet
- Conférences
  - Black Hat
  - Defcon
  - Etc.
- Journaux
- IRC, Chat
- Publications
- Ecoles de « hacking »
- Etc.

- Leurs motivations ?

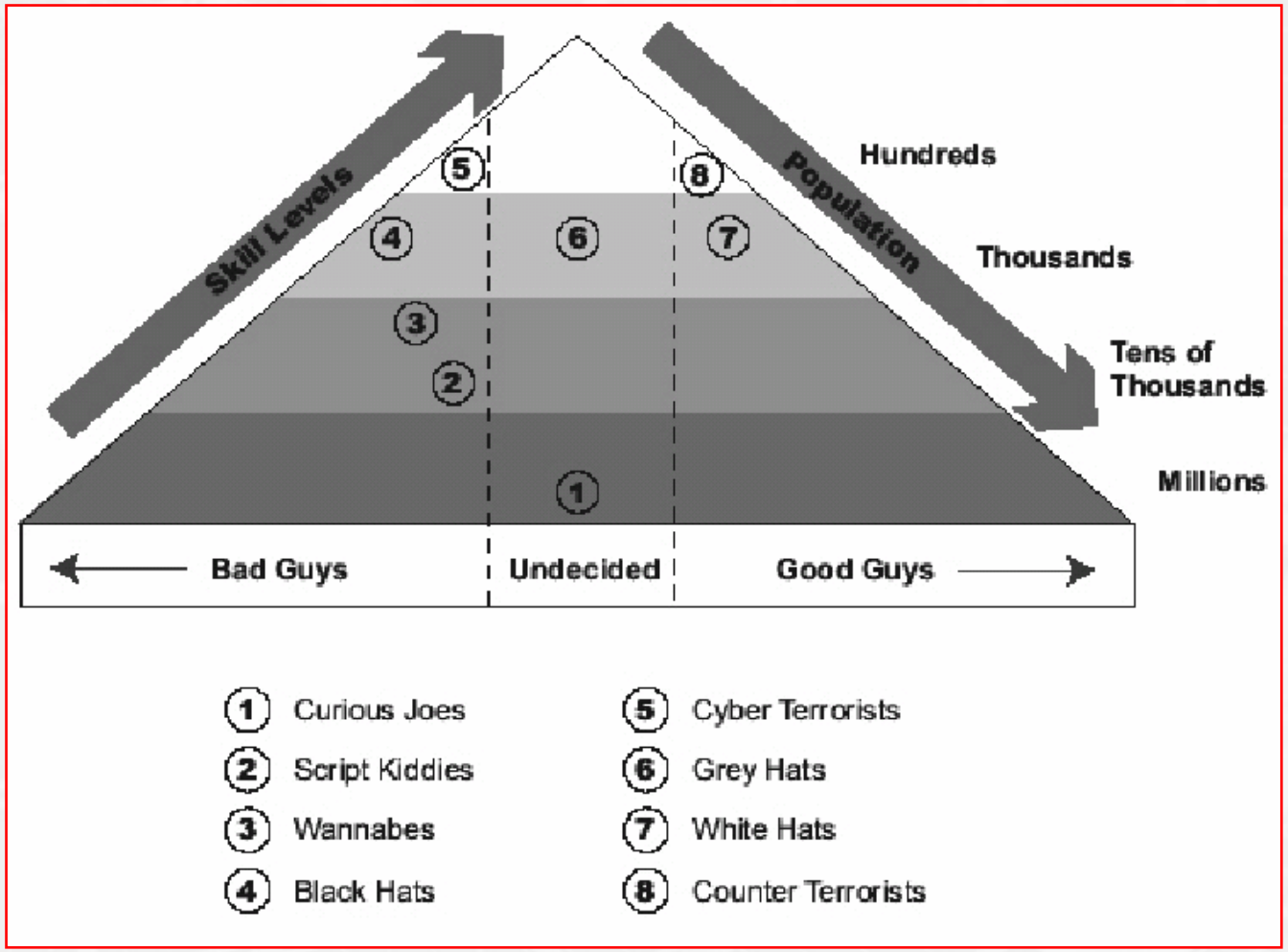
- Le profit et l'argent
- Avantage compétitif
- Espionnage
- Vengeance
- Revendication
- Curiosité
- Gloire
- Etc.

Evolution des attaques

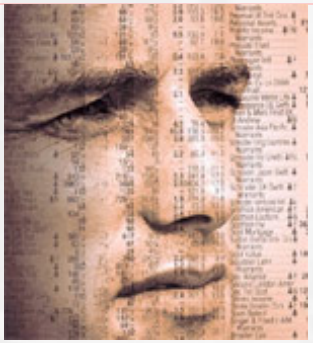


Source: CERT 2001

- Pyramide des menaces

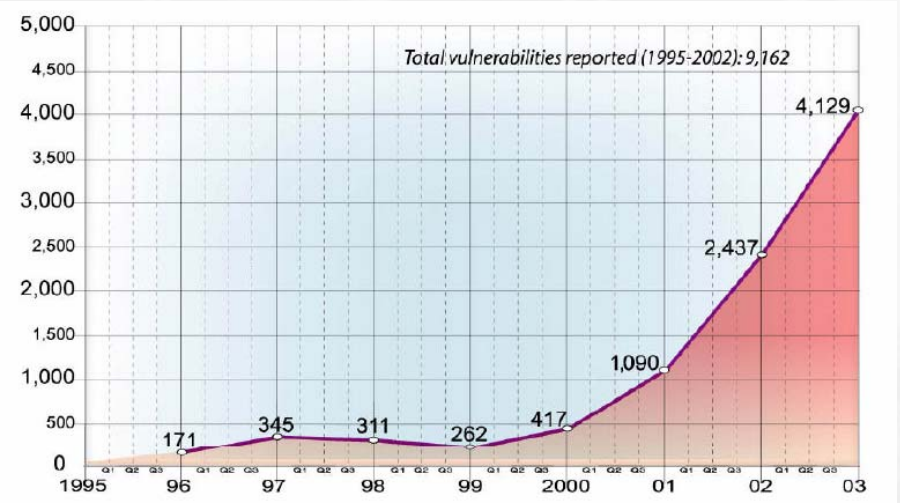


Source: RBC Capital Market



- Augmentation significative des vulnérabilités
  - Pas de « design » pensé sécurité
  - Complexité du système d'information
  - Besoins Marketing (Software)
  - Evolution très (trop) rapide des technologies
  - Etc.
- Le maillon faible est l'humain…
  - L'humain est imparfait par définition !

- Augmentation des vulnérabilités



- Environ 72 nouvelles vulnérabilités par semaine en 2003
- Et 2004, 2005 ?

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

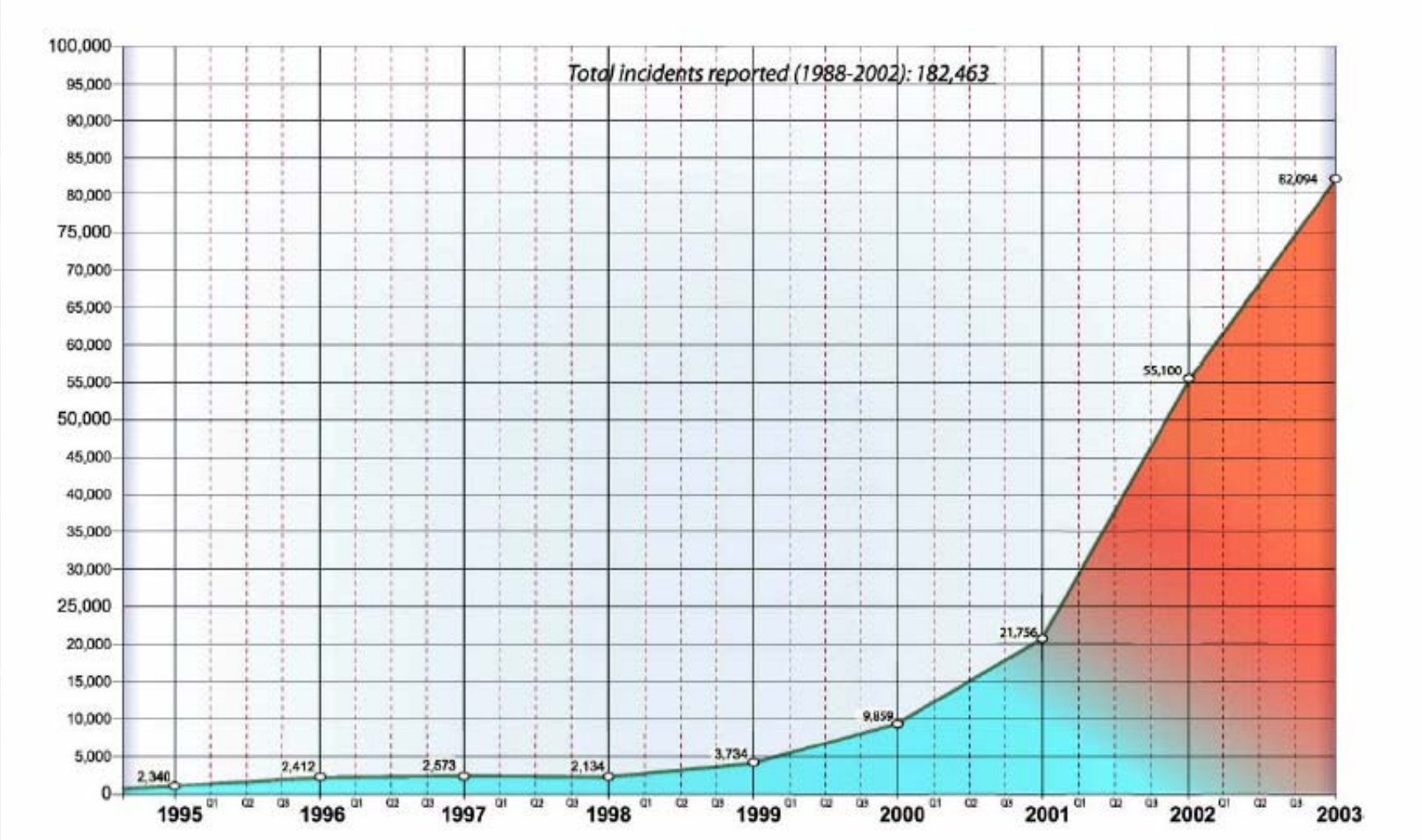
2000-2004

Year	2000	2001	2002	2003	1Q-2Q 2004
Vulnerabilities	1,090	2,437	4,129	3,784	1,740

Total vulnerabilities reported (1995-2Q 2004): **14,686**

Source: CERT octobre 2004

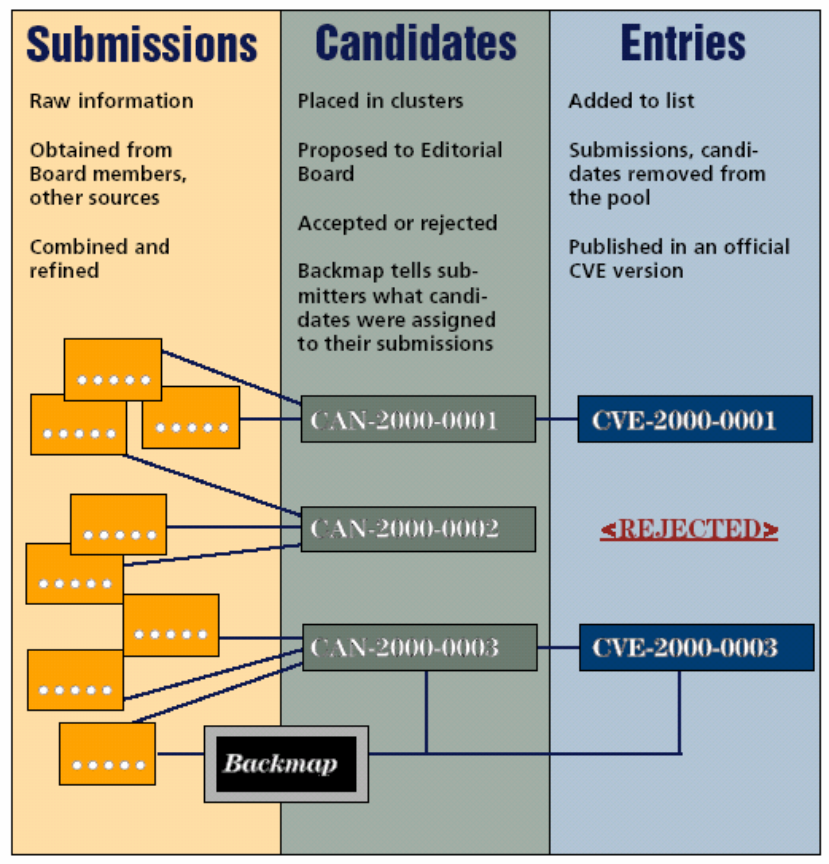
Incidents reportés par le CERT



Source: CERT octobre 2004

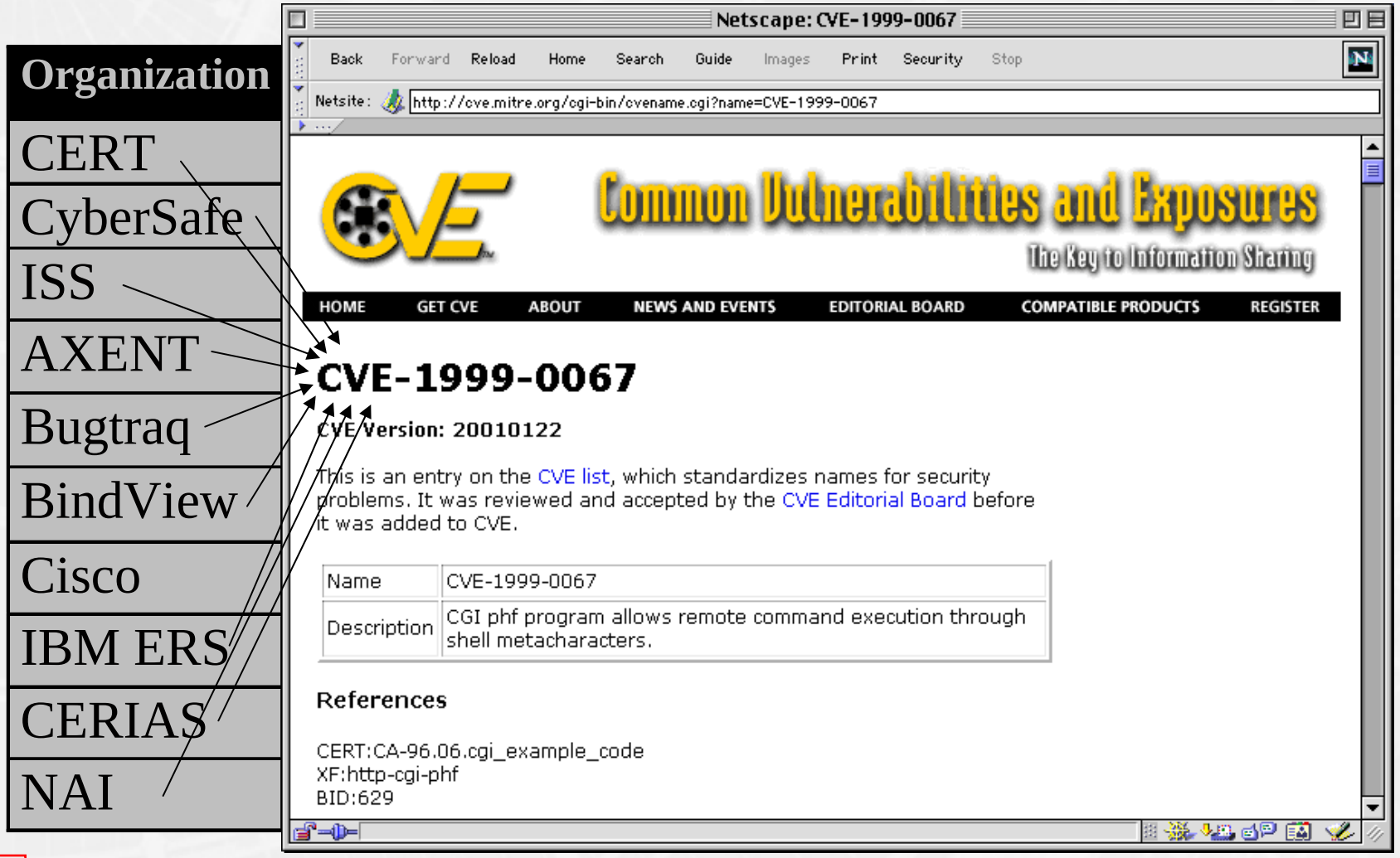
CVE: Common Vulnerabilities and Exposures

- Définition commune d'une vulnérabilité
  - De facto standard pour les constructeurs
- Processus de validation par le CVE
  - 1er phase: canditature → CAN-2004-xxx
  - 2ème phase: acceptation ? → CVE-2004-xxx



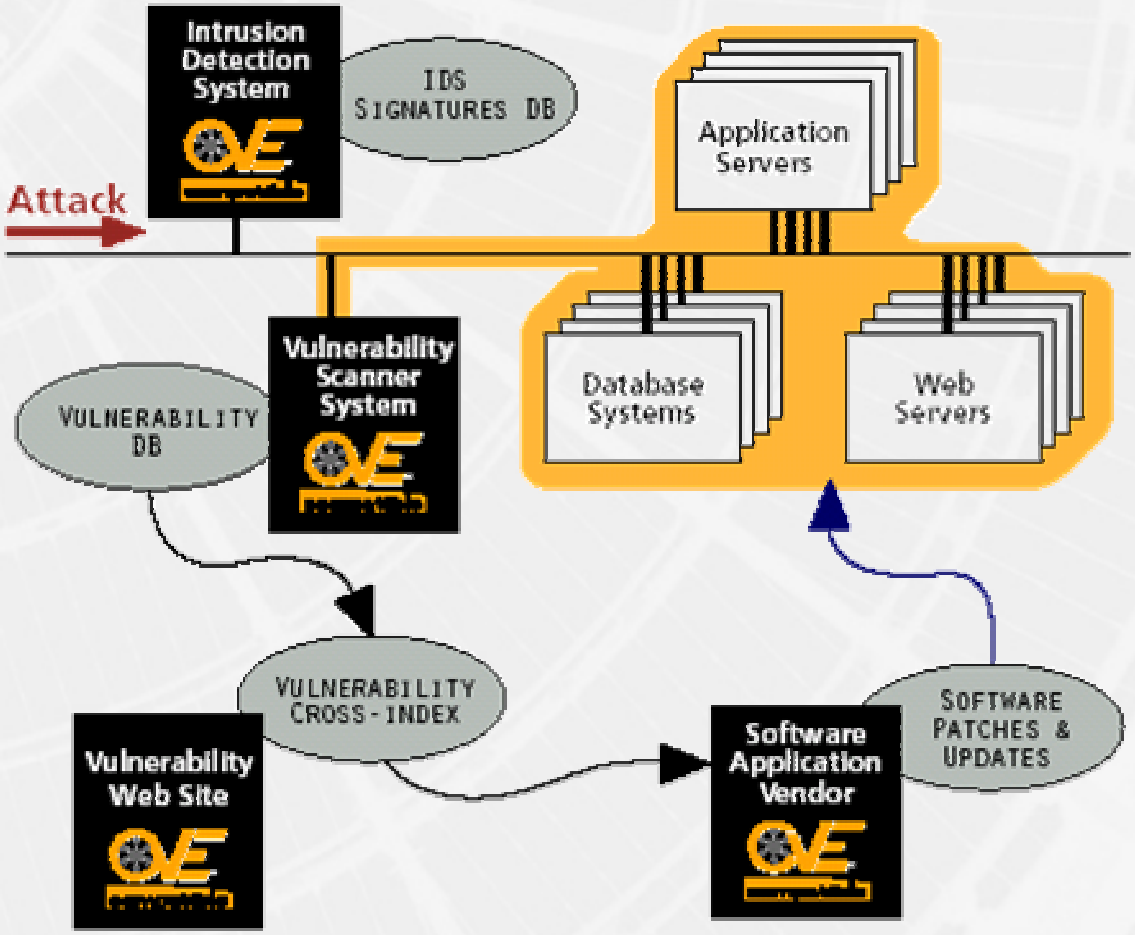
Source: CVE 2002

- CVE: une nouvelle vulnérabilité PHP



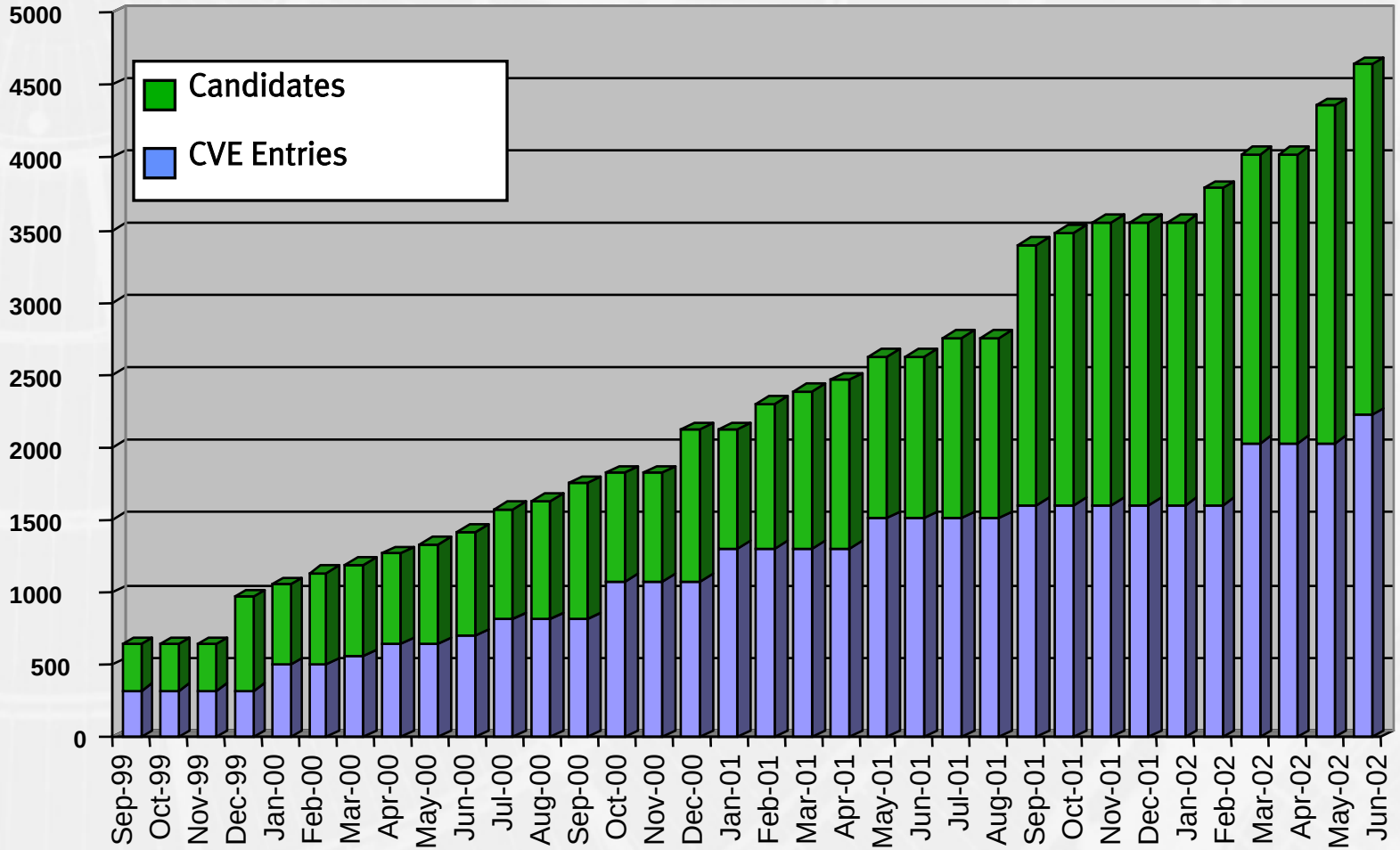
Source: CVE 2002

- CVE: produits de sécurité



Source: CVE 2002

Evolution des entrées CVE



Source: CVE 2002

- Vulnérabilités: Top 20

The Twenty Most Critical Internet Security Vulnerabilities (Updated) – The Experts' Consensus

Version 3.1 October 7, 2002 Copyright © 2001-2002, The SANS Institute

Questions / comments may be directed to top20@sans.org.

www.fbi.gov www.nipc.gov www.sans.org

Top Vulnerabilities to Windows Systems

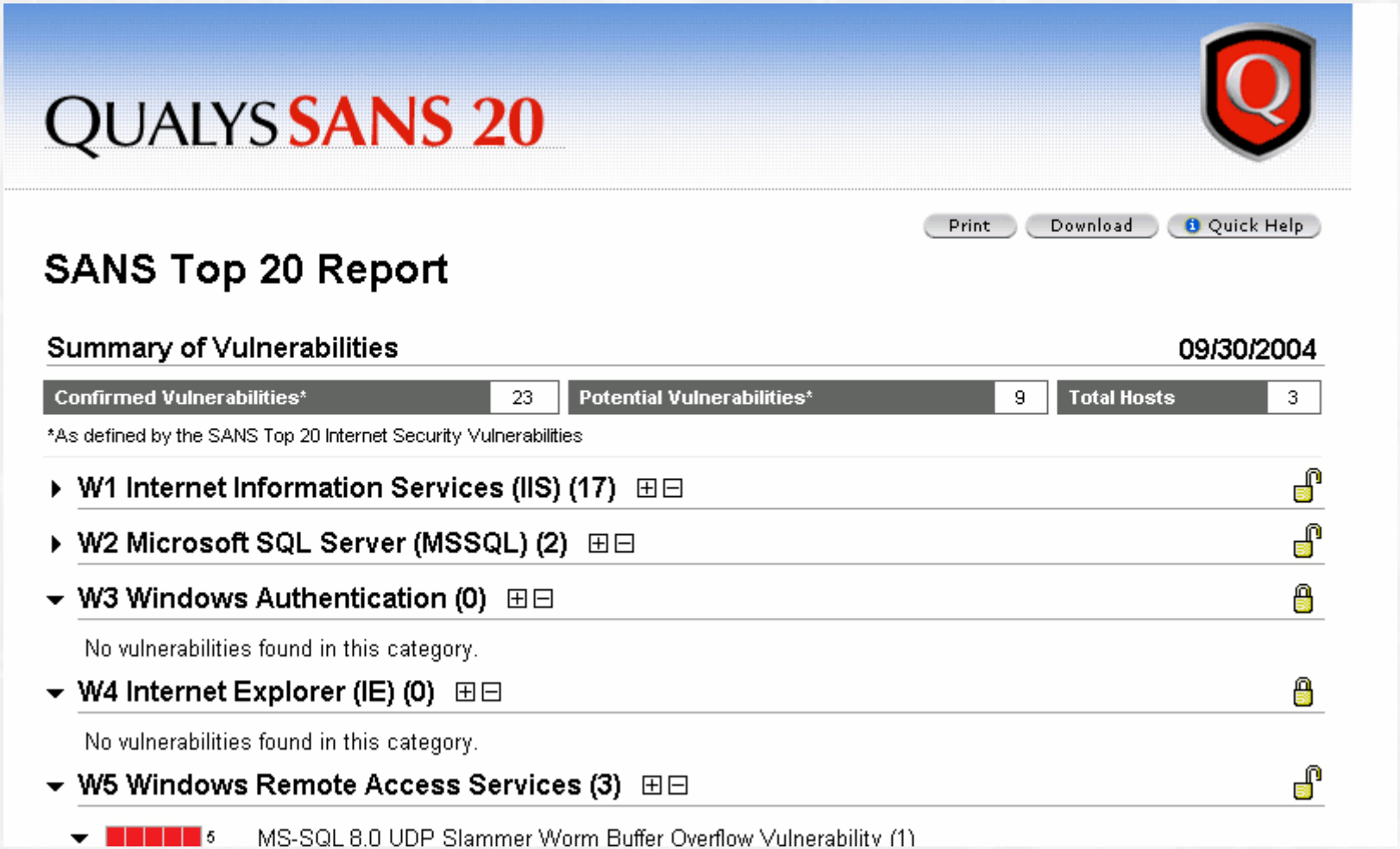
- W1 Web Servers & Services
- W2 Workstation Service
- W3 Windows Remote Access Services
- W4 Microsoft SQL Server (MSSQL)
- W5 Windows Authentication
- W6 Web Browsers
- W7 File-Sharing Applications
- W8 LSAS Exposures
- W9 Mail Client
- W10 Instant Messaging

Top Vulnerabilities to UNIX Systems

- U1 BIND Domain Name System
- U2 Web Server
- U3 Authentication
- U4 Version Control Systems
- U5 Mail Transport Service
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Misconfiguration of Enterprise Services NIS/NFS
- U9 Databases
- U10 Kernel

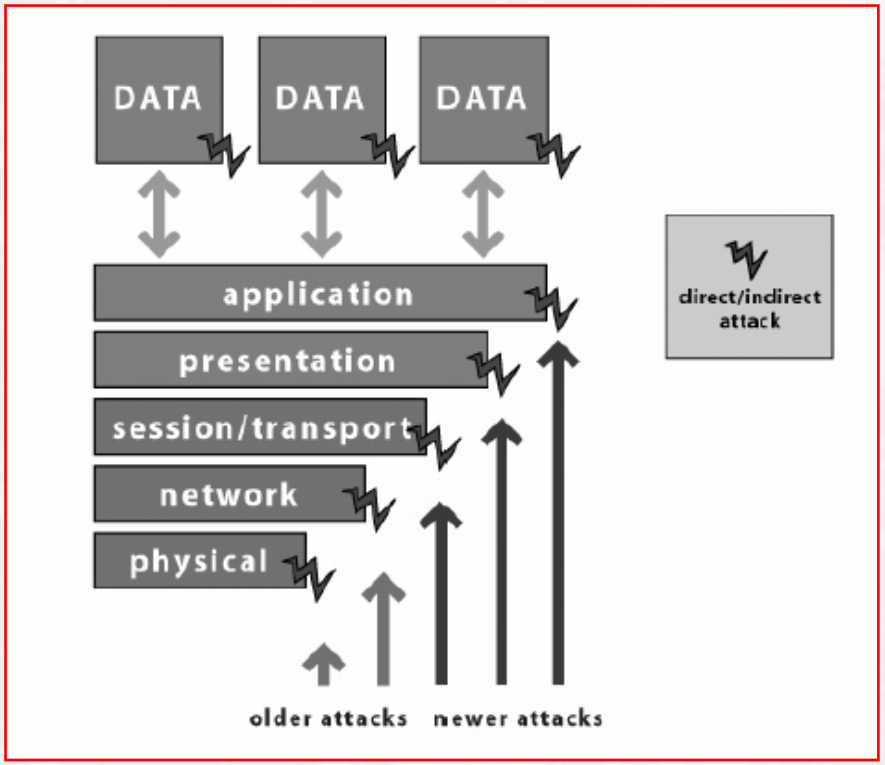
Source: SANS octobre 2004

- http://sans20.qualys.com: Free tool !



- Les tendances: les firewalls ne sont plus suffisants !

- Attaques des applications
  - 70 % des attaques http (Gartner 2004)
  - BoF: 60% des problèmes (CERT 2004)
  - 3 sites Web sur 4 sont vulnérables (Gartner 2004)

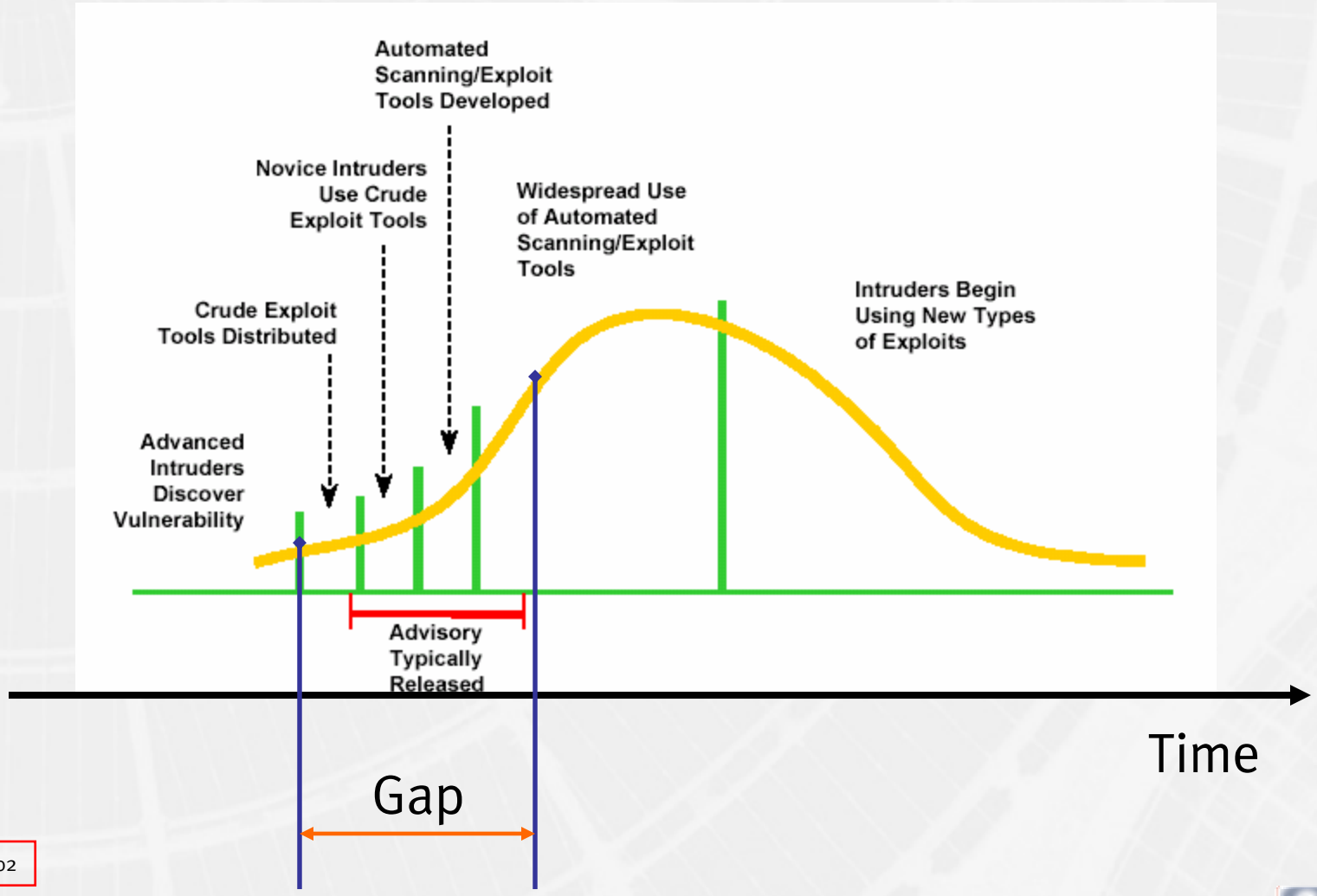


- Influence du temps ?

- La sécurité est un processus permanent
  - Et non un produit…
- L'idée:
  - Maintenir en permanence les vulnérabilités au plus bas
  - Suivre les recommandations des constructeurs (patchs, update, etc.)
  - Amélioration de l'architecture de sécurité
  - Evaluation des systèmes
    - Audit
    - Tests d'intrusions

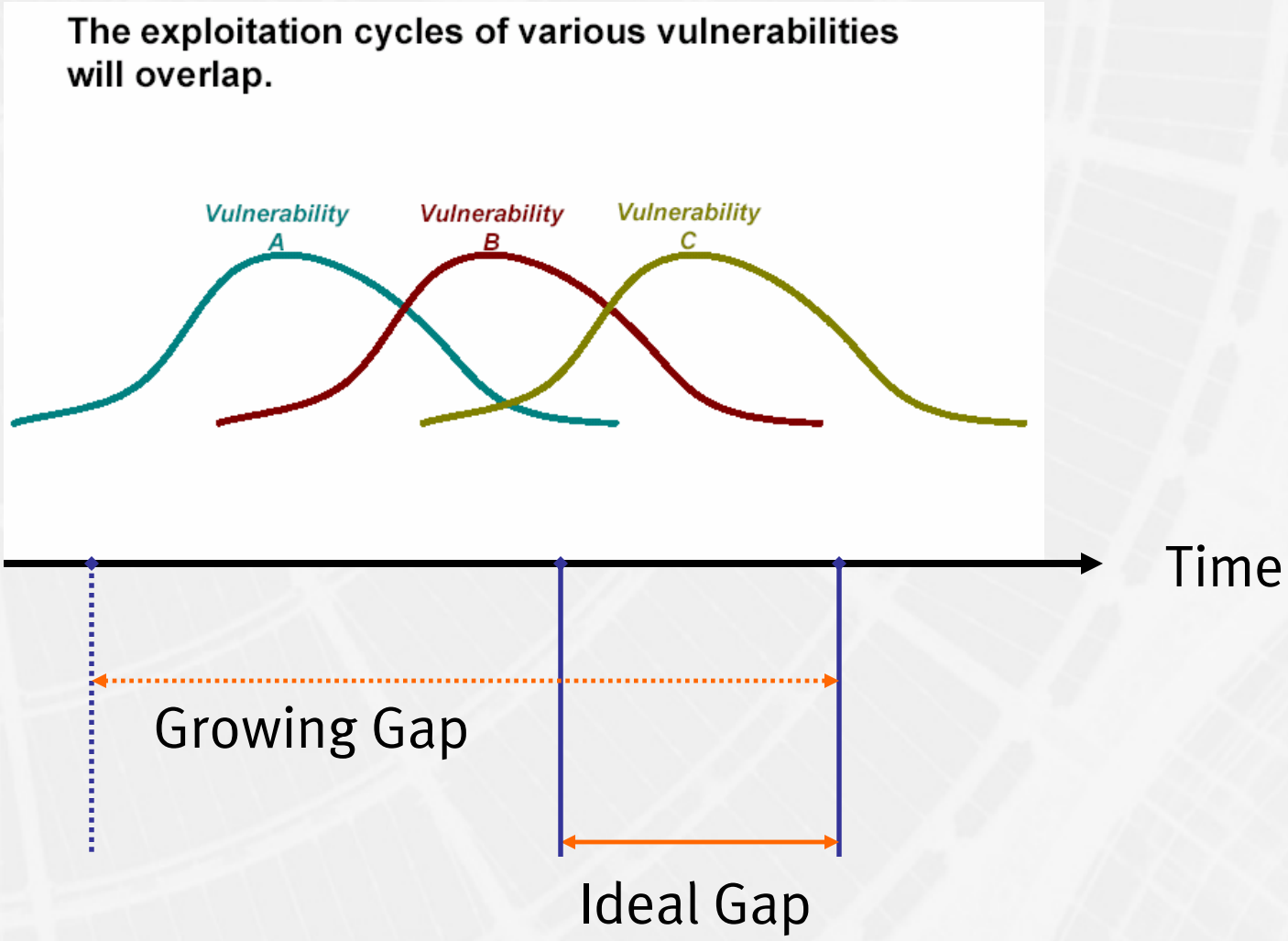
- Evolution des risques dans le temps ?

- Cycle d'une vulnérabilité



Source: CERT 2002

- Evolution dans le temps



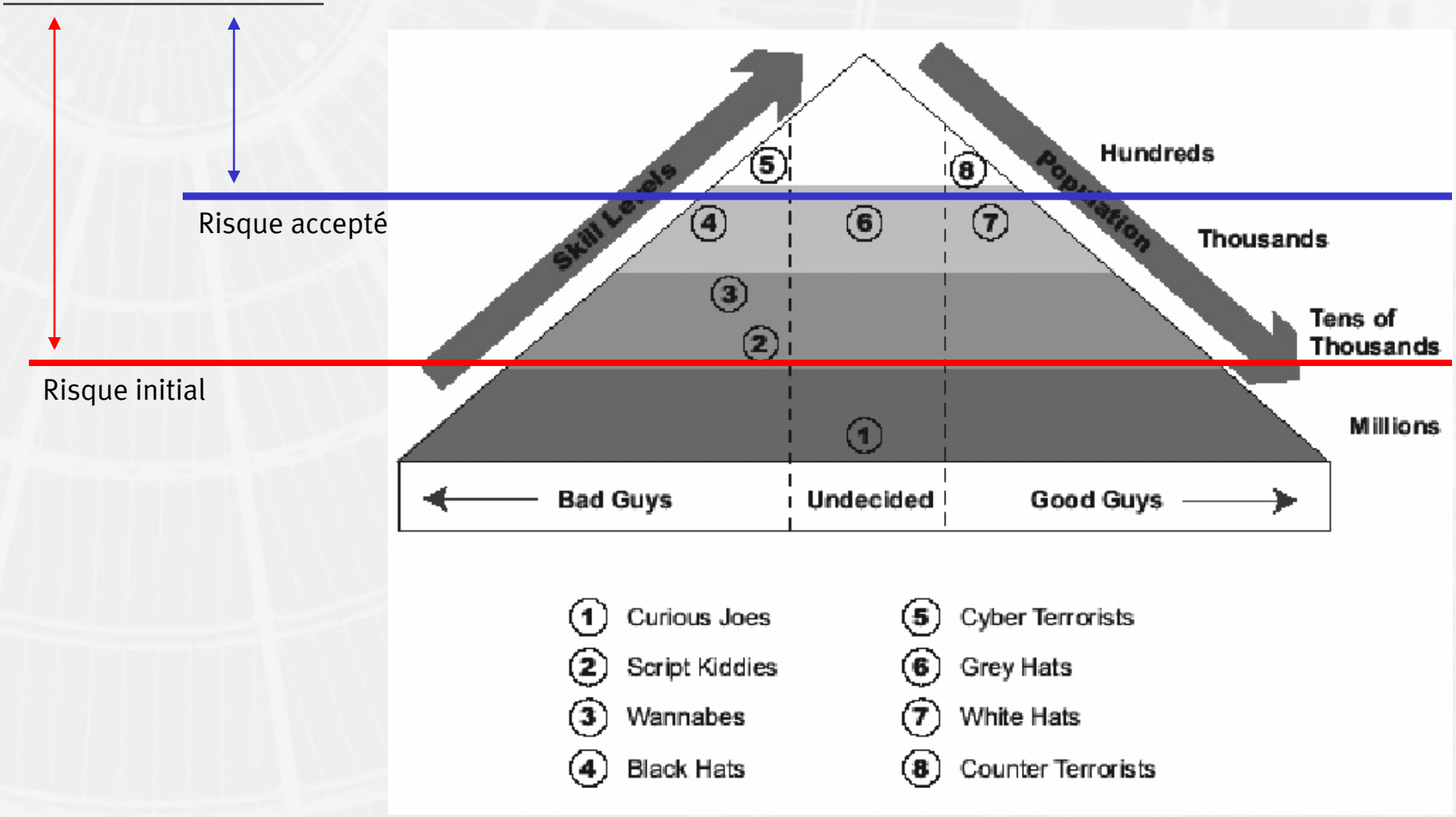
Source: CERT 2002

- Peut-on prévenir les intrusions ?

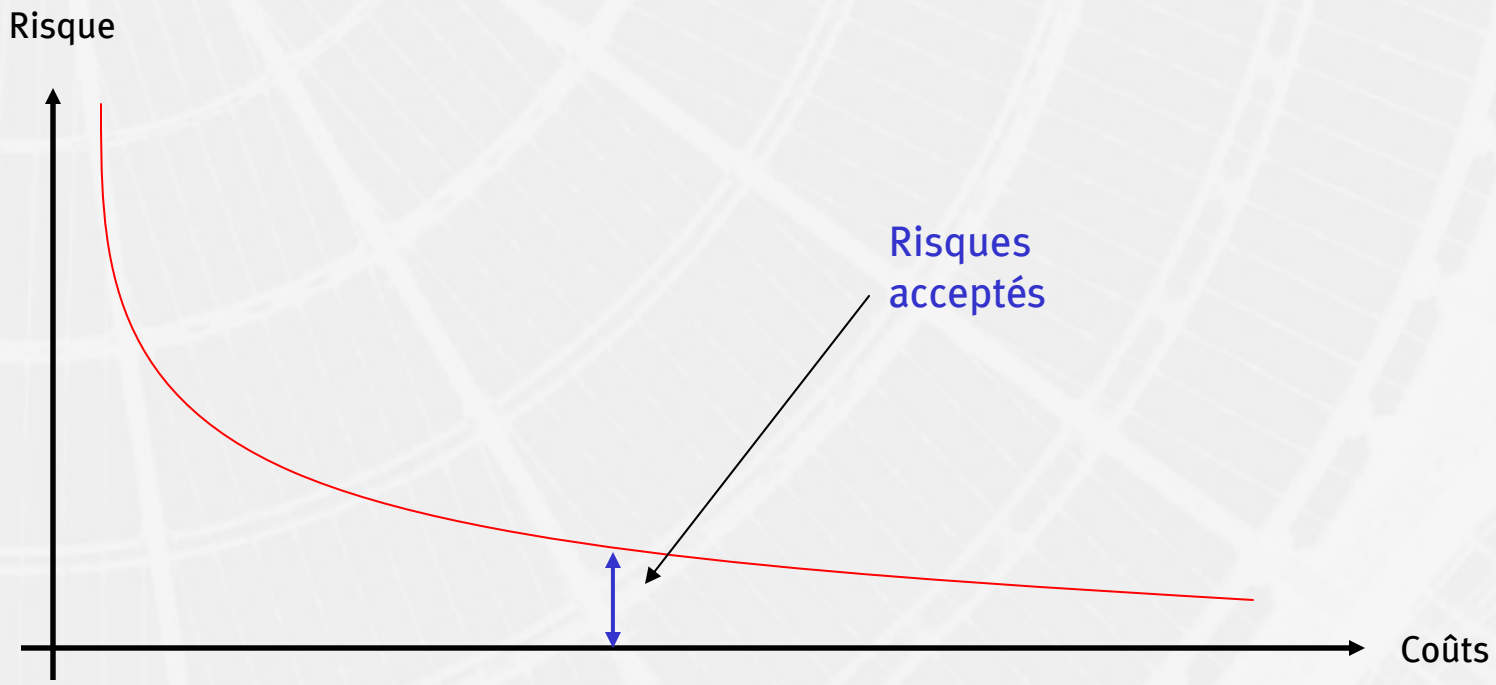
of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available.

Source: CERT 2002

- L'idée: diminuer le risque et maintenir cette démarche



- Quel montant faut il investir ?



Les attaques

- La première phase avant une attaque
- Obtention d'informations passives
  - Recherche par le Web (google)
  - NIC, Ripe
  - Whois
  - Sam Spade
  - Registre du commerce
  - Etc.

- Recherche du nom de domaine

Sam Spade.org

dns e-xpertsolutions.com

e-xpertsolutions.com DNS

www.e-xpertsolutions.com resolves to 212.147.35.20

Mail for e-xpertsolutions.com is handled by mars.e-xpertsolutions.com (10) 212.147.35.18 mx2.vtx.ch (20) 212.147.0.115

whois -h magic e-xpertsolutions.com

e-xpertsolutions.com is registered with REGISTER.COM, INC. - redirecting to whois.register.com

whois -h whois.register.com e-xpertsolutions.com

```
Organization:
   e-Xpert Solutions SA
   Sylvain Maret
   Route de Pré-Marais 29
   Bernex / Geneva, GE 1233
   CH
   Phone: +41 22 727 05 55
   Fax..: +41 22 727 05 50
   Email: smaret@e-xpertsolutions.com

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: E-XPERTSOLUTIONS.COM

   Created on..............: Mon, Jul 31, 2000
   Expires on..............: Sat, Jul 31, 2004
   Record last updated on..: Fri, Sep 20, 2002

Administrative Contact:
   e-Xpert Solutions SA
   Sylvain Maret
   Route de Pré-Marais 29
   Bernex / Geneva, GE 1233
   CH
   Phone: +41 22 727 05 55
   Fax..: +41 22 727 05 50
   Email: smaret@e-xpertsolutions.com
```

SWITCH Internet Domains · Online Registration

Query database: Search Result

Domain name:	e-xpertsolutions.ch
Holder of domain name:	[2650208] Sylvain Maret, route de Pré-Marais, Bernex
Billing address:	[3780608] e-Xpert Solutions SA, Cédric Enzler, Bernex
Technical responsibility:	[2650208] Sylvain Maret, route de Pré-Marais, Bernex
Type of domain name:	inactive
Date of registration:	02.08.2000

new query

FAQ Options Exit © SWITCH

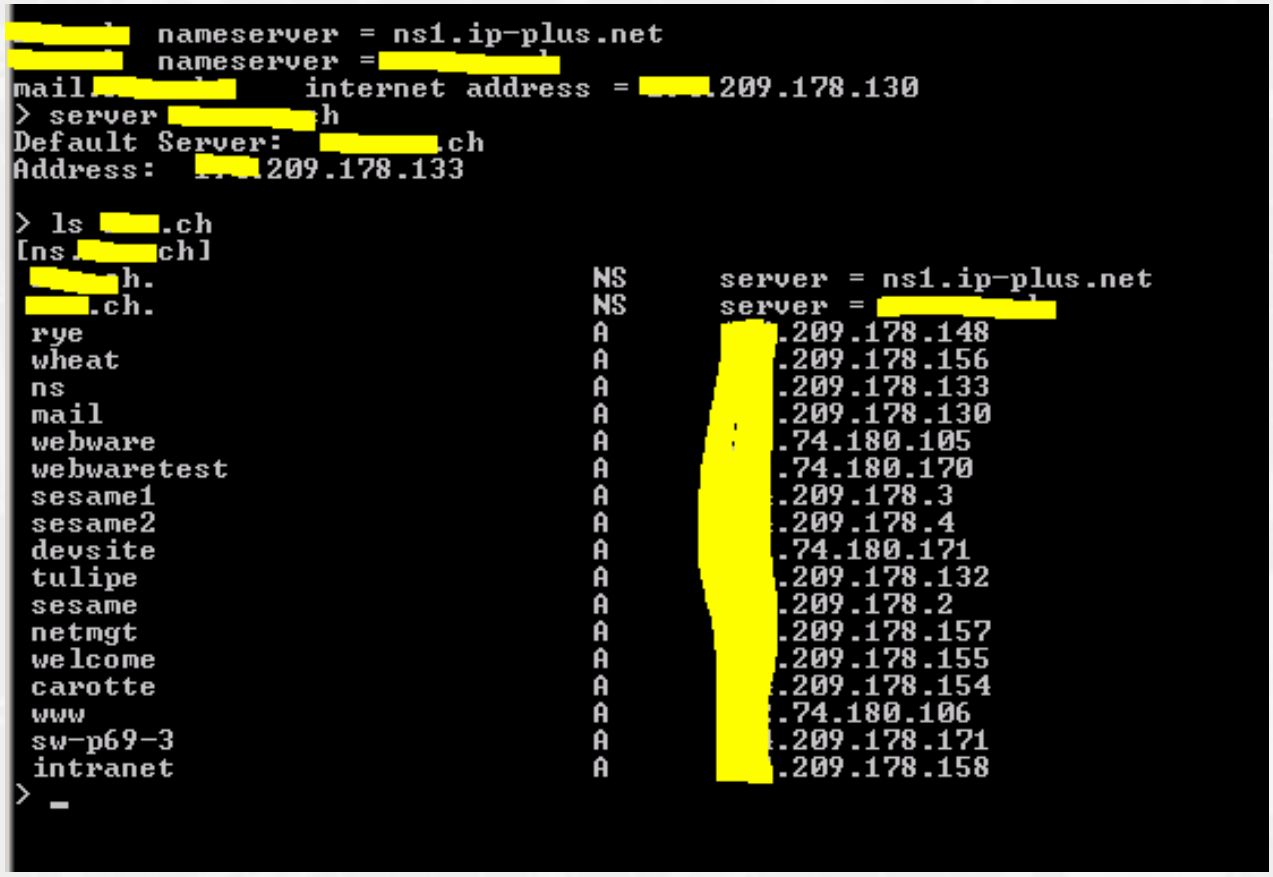
- Obtention d'informations des « Domain Name Server »

- Obtention d'informations techniques
  - DNS
  - MX Record
  - Zone transfert (si possible)
  - Etc.
- Les Outils
  - DIG
  - Nslookup
  - Host
  - Etc.

- Exemple: recherche des entrées de messagerie (MX Record)

```
> server ns.eunet.ch
Default Server:  ns.eunet.ch
Address:  146.228.10.16

>
>
>
> set type=mx
> e-xpertsolutions.com
Server:  ns.eunet.ch
Address:  146.228.10.16

e-xpertsolutions.com    MX preference = 10, mail exchanger = mars.e-xpertsolutions.com
e-xpertsolutions.com    MX preference = 20, mail exchanger = mx2.vtx.ch
e-xpertsolutions.com    nameserver = dns23.register.com
e-xpertsolutions.com    nameserver = dns24.register.com
mars.e-xpertsolutions.com       internet address = 212.147.35.18
mx2.vtx.ch      internet address = 212.147.0.115
dns23.register.com      internet address = 216.21.234.82
dns24.register.com      internet address = 216.21.226.82
>
```

- Exemple: essais d'un « zone transfer »

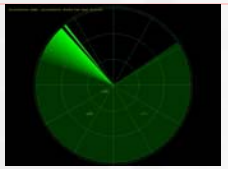


- Exemple: essais d'un « zone transfer »

```
> server 216.21.234.82
Default Server:  dns23.register.com
Address:  216.21.234.82

> ls e-xpertsolutions.com
[dns23.register.com]
*** Can't list domain e-xpertsolutions.com: Query refused
> _
```

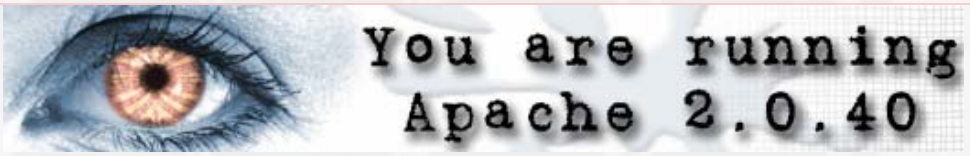
Transfert interdit

Les scanners: identification à distance des systèmes



- Technique d'identification des systèmes et des applications
  - Processus d'obtention d'informations (information gathering)
- Phase d'approche préalable à une attaque
  - Facteur déterminant lors d'une attaque
- Objectif: identifier de manière précise le type de système pour mieux cibler son attaque
  - En déduire ses vulnérabilités

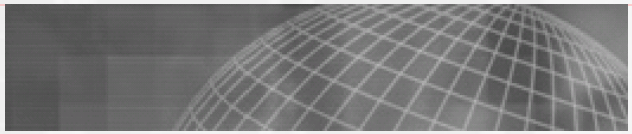
Types de scanners



- Scanner de ports ou services
- Scanner de type « OS Fingerprint »
- Scanner de vulnérabilitées
  - Scanner générique
- Scanner de type « WEB Scanner »
- Scanner de base de données
  - SQL server
  - Oracle
  - Etc.

- Scanner de ports

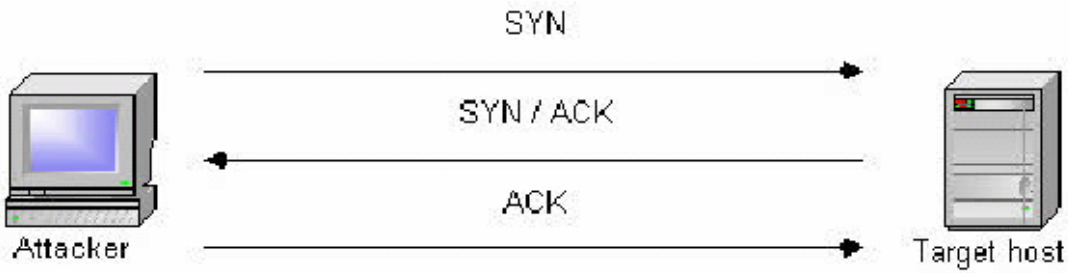
- Objectif: cartographier de manière précise les services offert par une machine ou un réseau de machines
  - Serveur Web
  - Server DNS
  - Messagerie
  - Serveur FTP
  - Server Real
  - Service Microsoft
  - Service SSH
  - IPSEC
  - Firewall
  - Etc.



- Scan de ports TCP et UDP voir ICMP
- Option de scan:
  - Scan ouvert (Vanilla TCP Scan)
  - Scan demi-ouvert
  - Scan furtif
  - Scan très lent
  - Etc.
- L'idée: ne pas se faire détecter par un IDS
- Scanner est un art !

- Scan ouvert (Standard TCP Connect)

A vanilla TCP scan result when a port is open –



1. A SYN probe packet is sent to the target host
2. A SYN / ACK packet is received
3. An ACK packet is sent to complete the three-way handshake

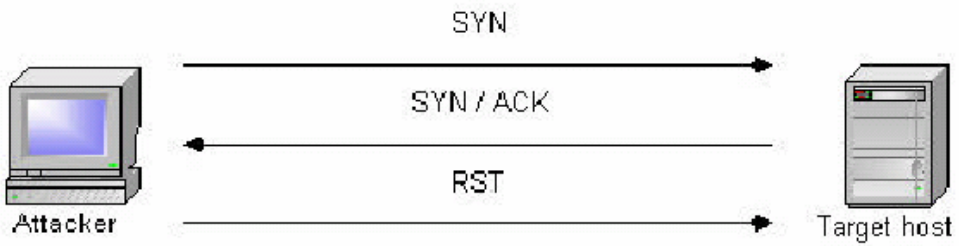
A vanilla TCP scan result when a port is closed –

1. A SYN probe packet is sent to the target host
2. An RST / ACK packet is received

Source:
Matta Security 2002

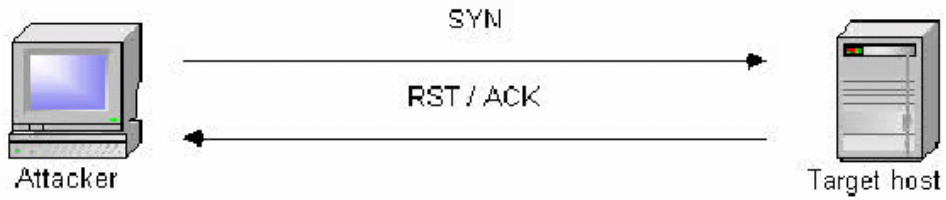
- Scan demi-ouvert (Half-Open Syn Scan)

A half-open SYN scan result when a port is open –



1. A SYN probe packet is sent to the target host
2. A SYN / ACK packet is received
3. An RST packet is sent to abruptly reset the connection

A half-open SYN scan result when a port is closed –

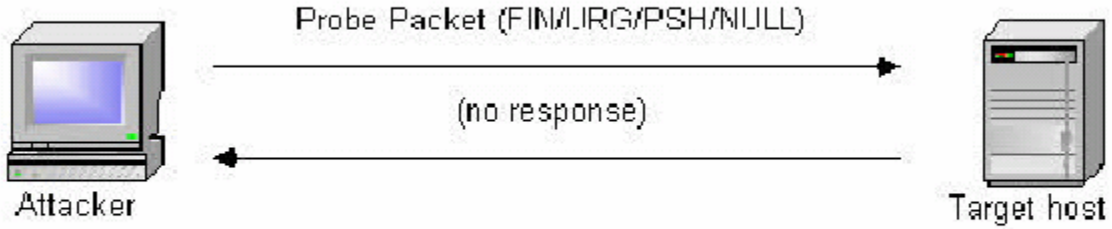


1. A SYN probe packet is sent to the target host
2. An RST / ACK packet is received

Source:
Matta Security 2002

- Scan Furtif (Hosts Unix)

An inverse TCP scan result when a port is open –



1. A FIN, XMAS or NULL probe packet is sent to the target host
2. If no response is seen, it is assumed that the port is listening

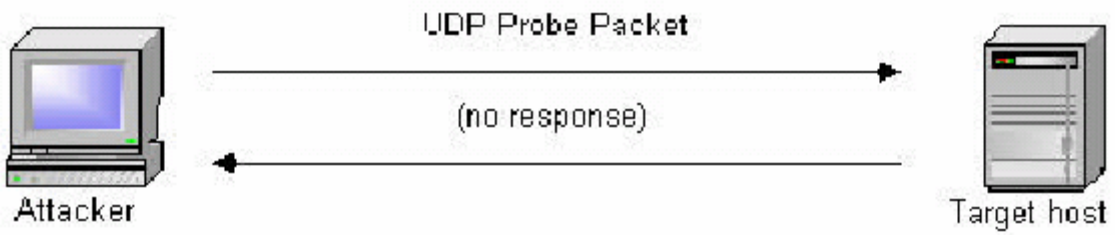
An inverse TCP scan result when a port is closed –

1. A FIN, XMAS or NULL probe packet is sent to the target host
2. An RST / ACK packet is received

Source:
Matta Security 2002

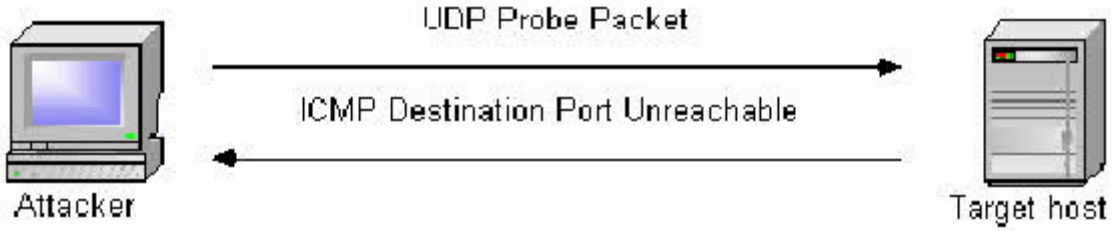
UDP Scan

An inverse UDP scan result when a port is open –



1. A UDP probe packet is sent to the target host
2. If no response is seen, it is assumed that the port is listening

An inverse UDP scan result when a port is closed –

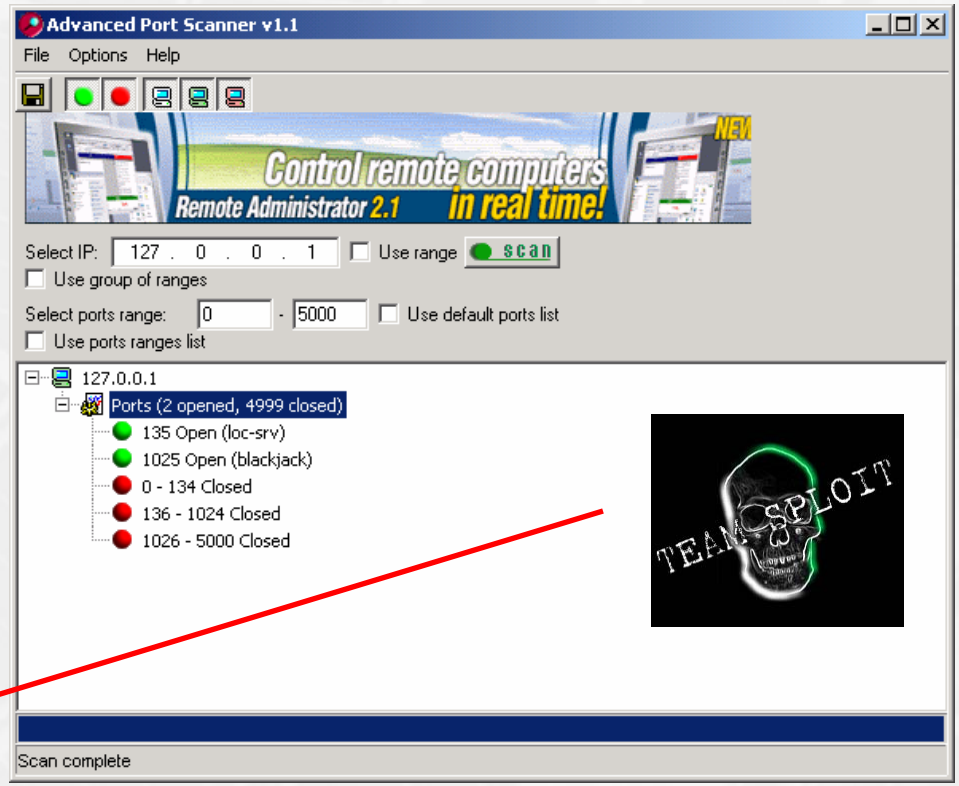


1. A UDP probe packet is sent to the target host
2. An 'ICMP Destination Port Unreachable' message is received

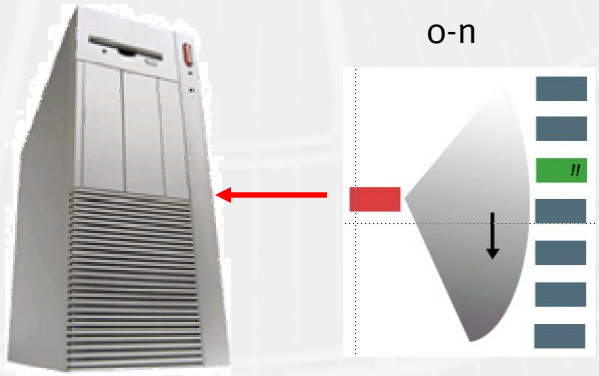
Source:
Matta Security 2002

- Scanner de ports pour Windows

Attaquant

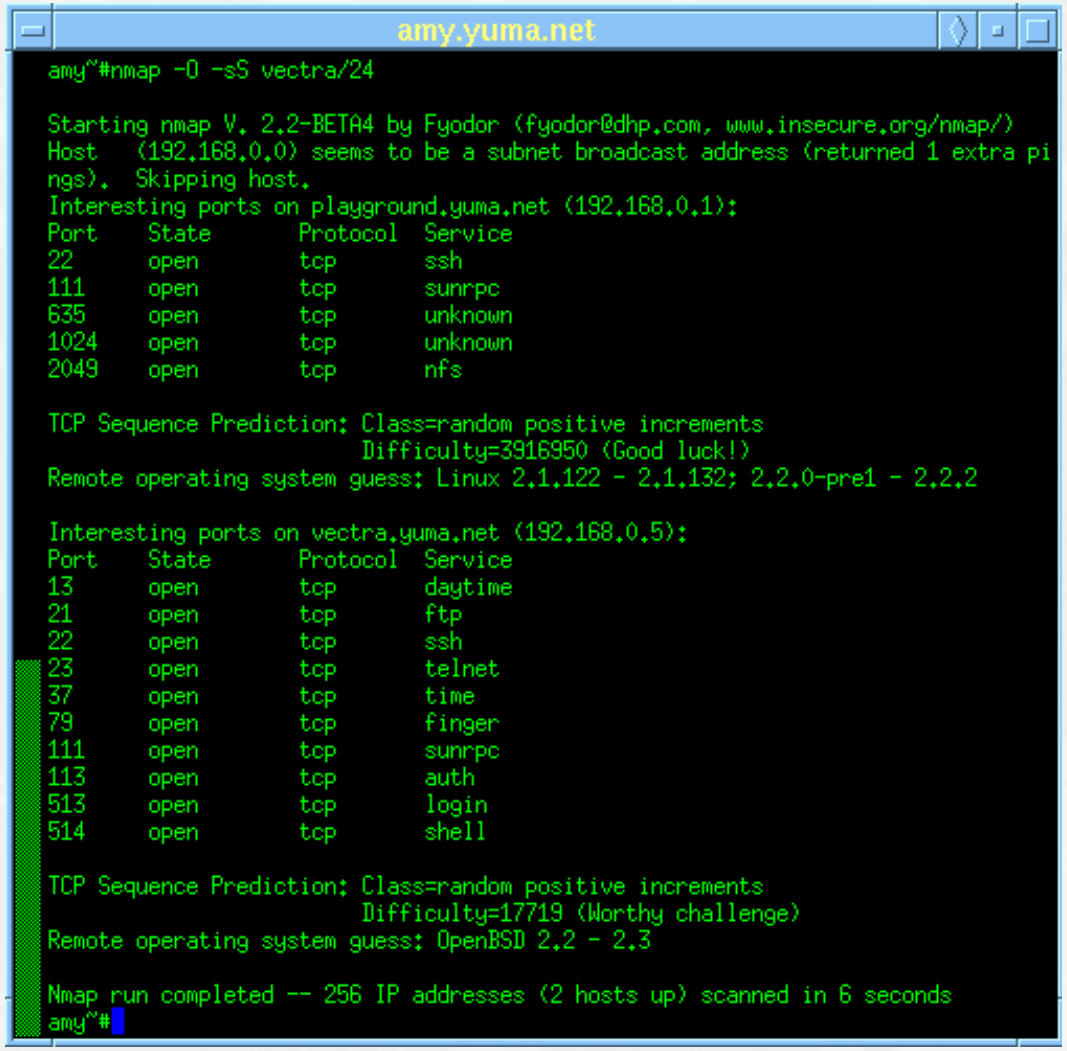


Cible



o-n

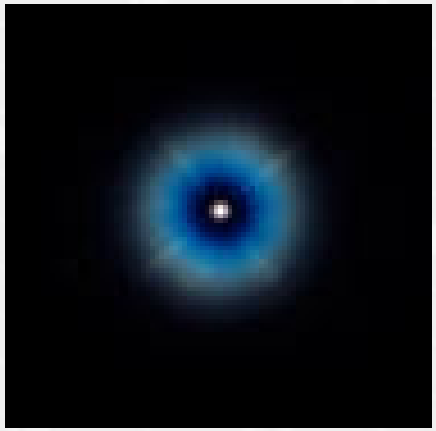
- Scanner de ports: NMAP pour Unix

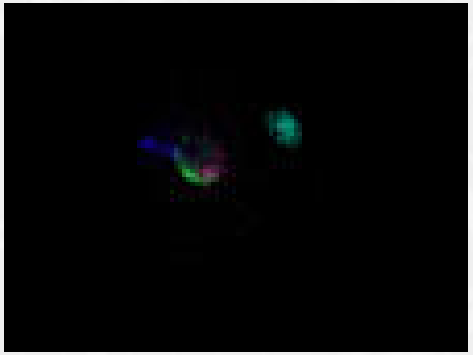


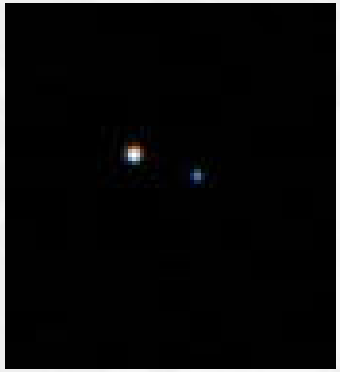
« OS Fingerprint » ou prise d'empreinte

- Objectif: déterminer de manière précise le type de système d'exploitation et de service
  - Win2k, Solaris 2.7, IOS 11.x, Red Hat, Mac, etc.
  - Apache 2.x, Sendmail 8.x, IIS v5, Checkpoint, etc.
- Approche passive et active
- L'idée: ne pas se faire détecter par un IDS

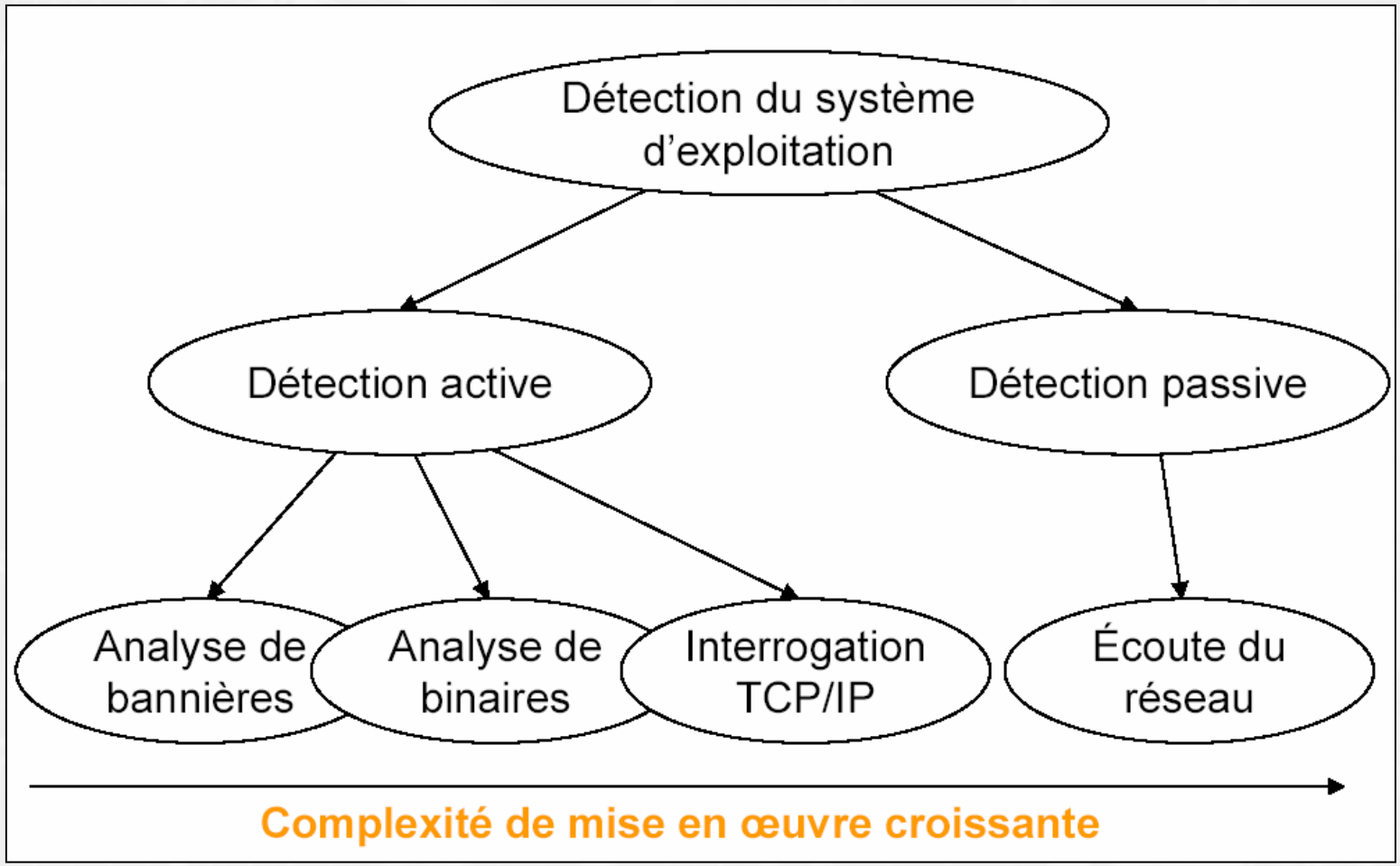
- « OS Fingerprint »: illustration





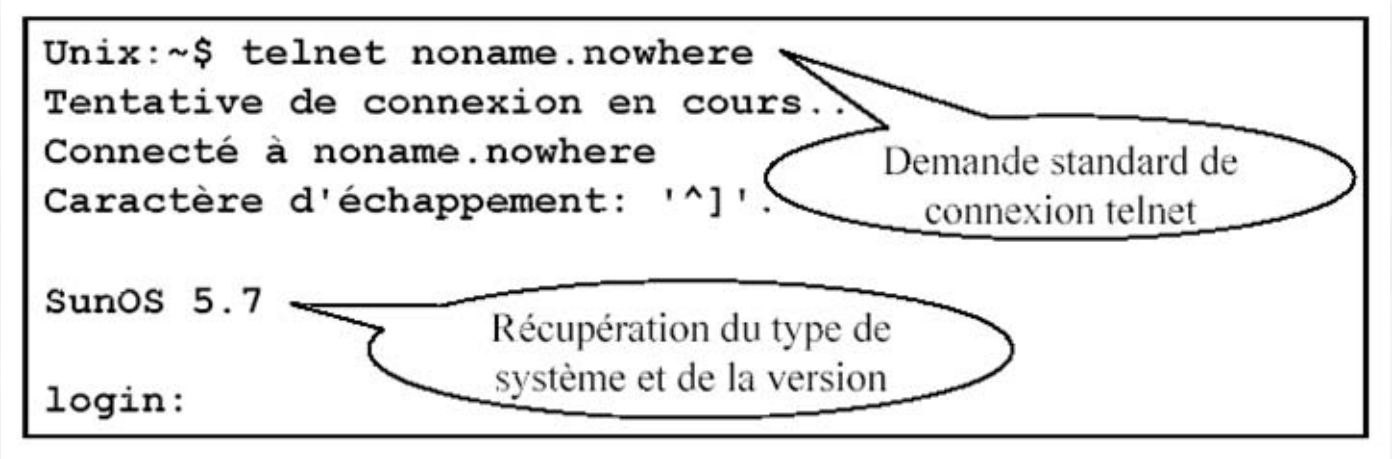


- « OS Fingerprint »: les techniques



Source
Intranode 2001

- « OS Fingerprint »: analyse de banière

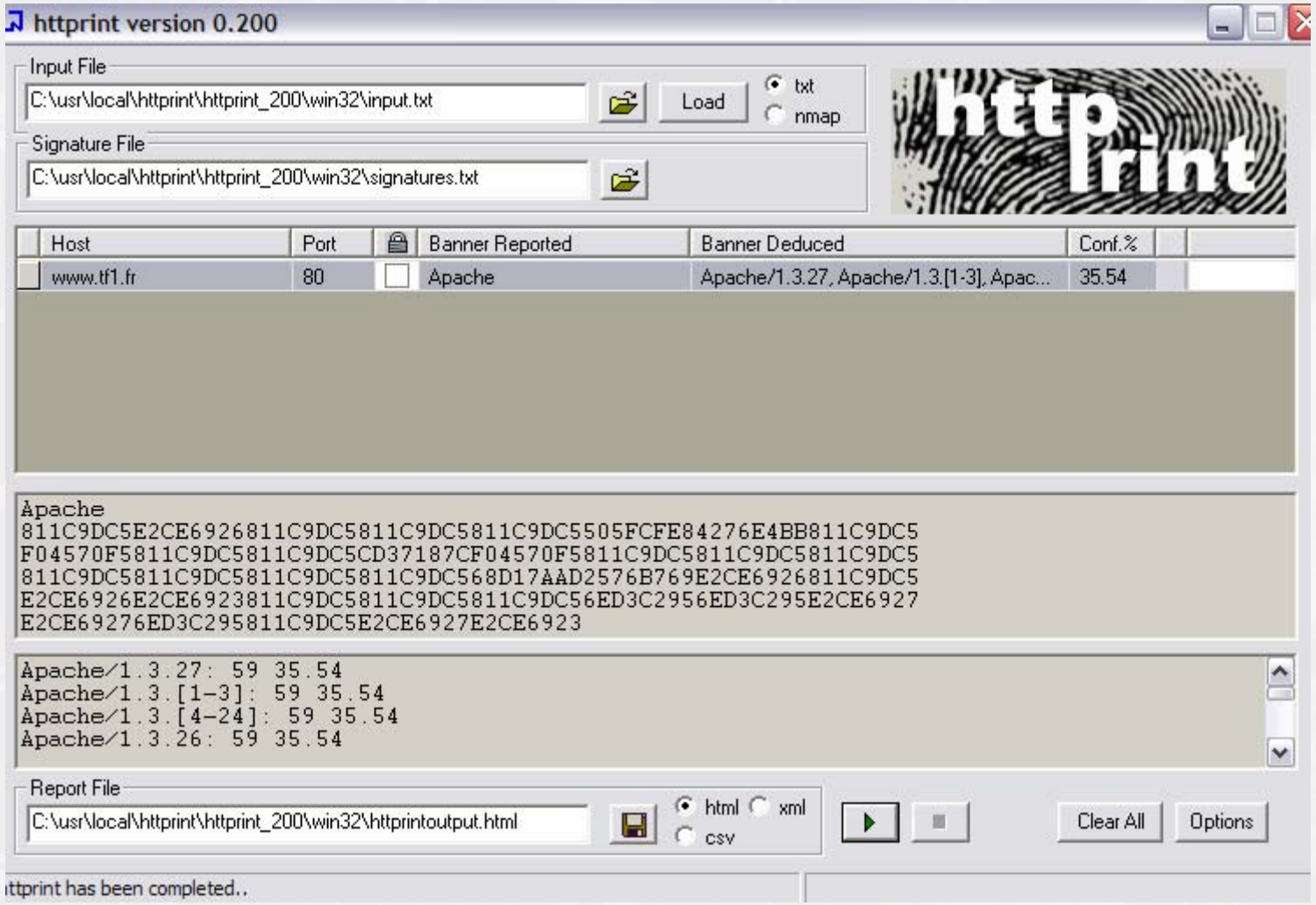


Source
Intranode 2001

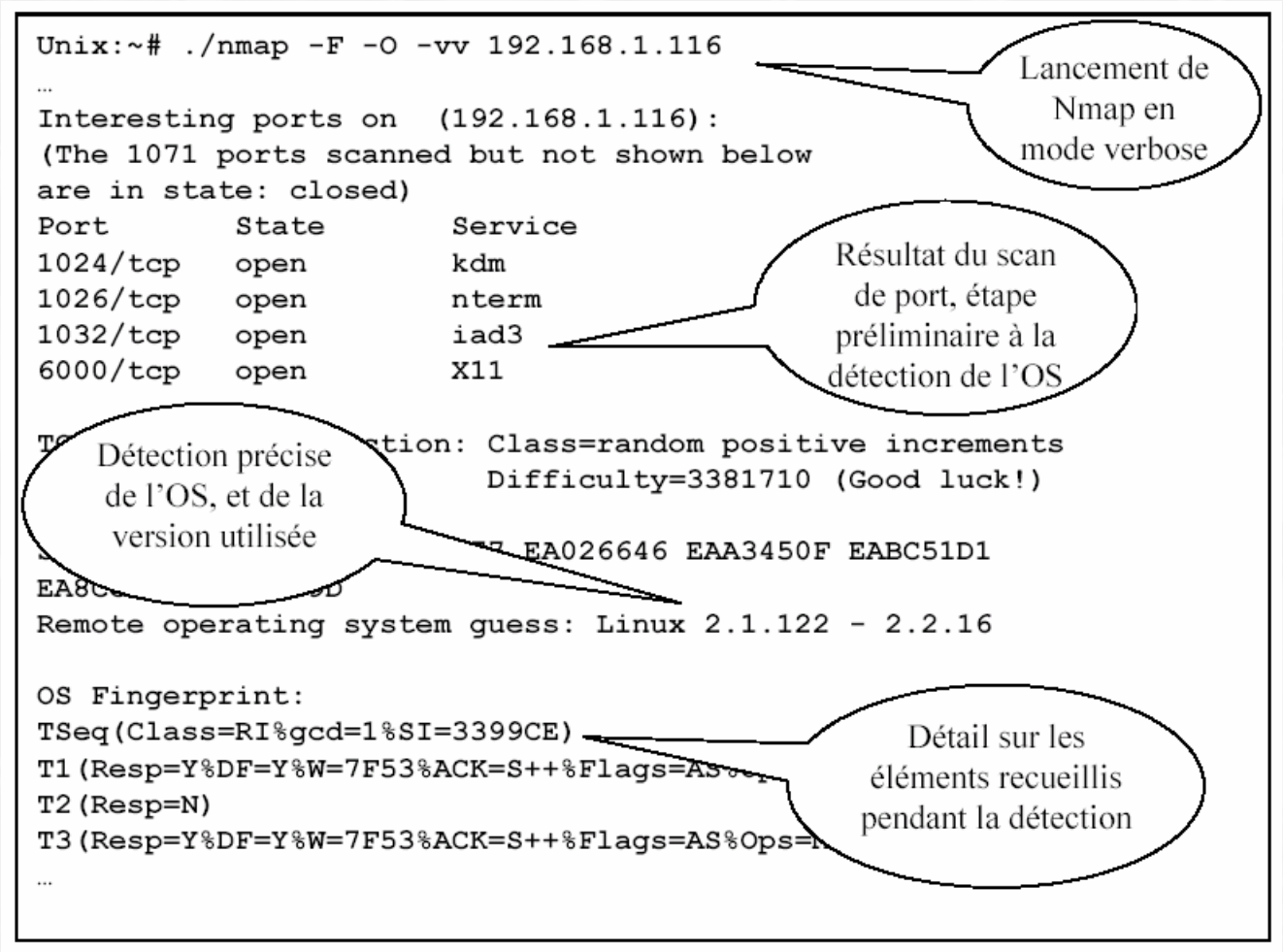
- « OS Fingerprint »: analyse de banière


```
[jeremiah@localhost jeremiah]$ telnet www.apache.org 80
Trying 63.251.56.142...
Connected to www.apache.org.
Escape character is '^]'.
OPTIONS * HTTP/1.1
Host: www.apache.org

HTTP/1.1 200 OK
Date: Thu, 12 Sep 2002 01:11:24 GMT
Server: Apache/2.0.41-dev (Unix)
Cache-Control: max-age=86400
Expires: Fri, 13 Sep 2002 01:11:24 GMT
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Content-Type: text/plain
```

- HTTP Fingerprinting



- « OS Fingerprint »: intérogation TCP/IP



Source
Intranode 2001

« OS Fingerprint »: les outils

- Nmap
- Queso
- XProbe2
- Ring
- HMAP (Web Serveurs)
- HTTPrint
- Smtpscan
- Etc.

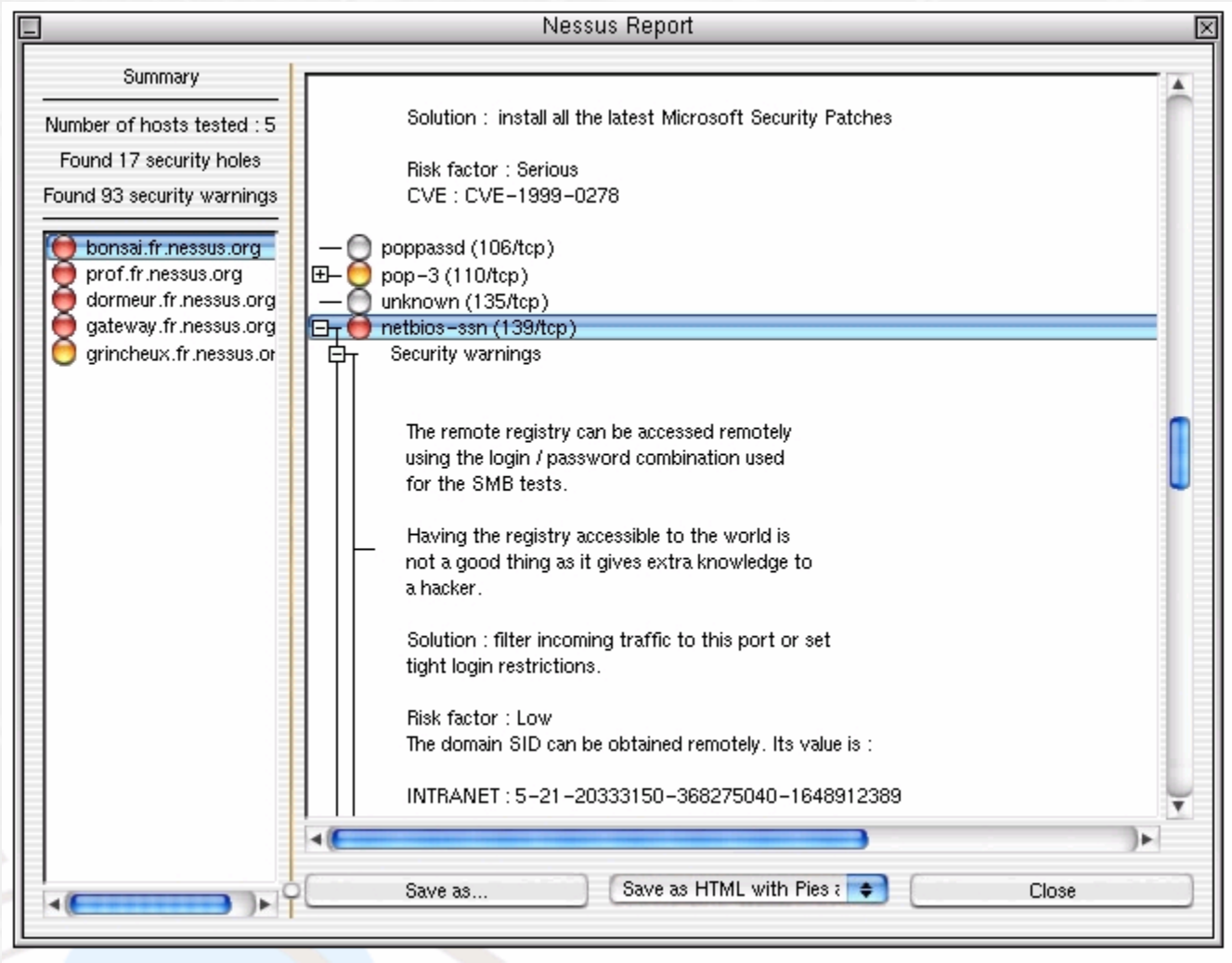
Scanner de vulnérabilités

- Deux grandes familles
  - Product Based Solution
  - Service Based Solution
- Updates automatique
  - Signatures de vulnérabilités
- Généralement compatible CVE
- Certains produits disponibles en Open Source

Scanner de vulnérabilités

- Outils très complets (mais généraliste)
  - Services WEB
  - FTP, DNS, SNMP, etc.
  - NetBios (Microsoft)
  - SSH Servers
  - RPC
  - DoS
  - Database
  - Mail
  - Etc.

- Scanner de vulnérabilités: Nessus



Scanner mode ASP

- Tests d'intrusions réalisés par un centre de tests d'intrusions
- Les tests sont réalisés à la demande ou de façon automatique
- Le résultat est consultable, en ligne, par un navigateur Web
- Les cibles à tester sont principalement des services frontaux (Internet, Extranet)

Exemple: scanner mode ASP

Source: Qualys 2002

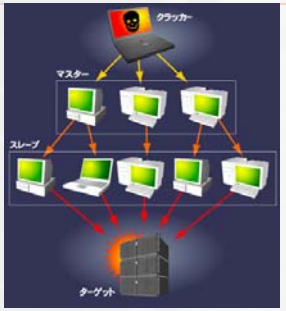
Web Scanner

- Outils de tests d'intrusions pour les services Web
- Outils très spécialisés
- Tests très poussés au niveau des applications
  - CGI
  - Cookies
  - Unicode
  - BoF
  - BackDoor
  - Hiden Field
  - Brute force
  - XSS, CSS
  - Etc.

Déni de services: DoS ou DDoS

- Atteinte au bon fonctionnement d'un système
  - Immobilisation ou « gel »
  - Utilisation massive des ressources CPU
  - Utilisation massive de la bande passante
  - Crash du système
    - Voir perte de données

- Déni de services: DoS ou DDoS

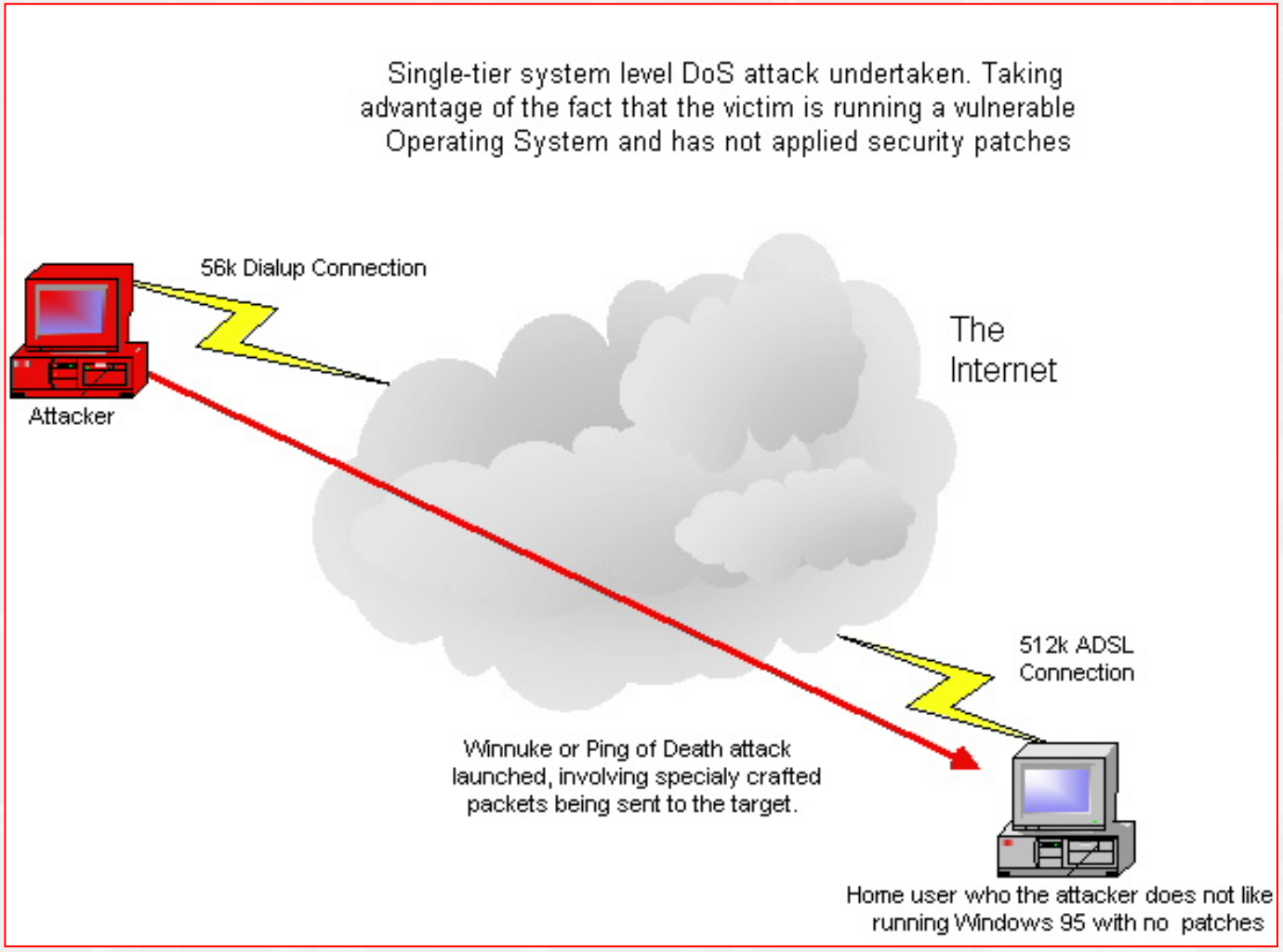


- 4 grandes familles
  - Les « destructeurs » de système
  - Les Floodings
  - Les « dévoreurs » de bande passante ou ressources CPU
  - Les Mails Bombs

Les destructeurs de système

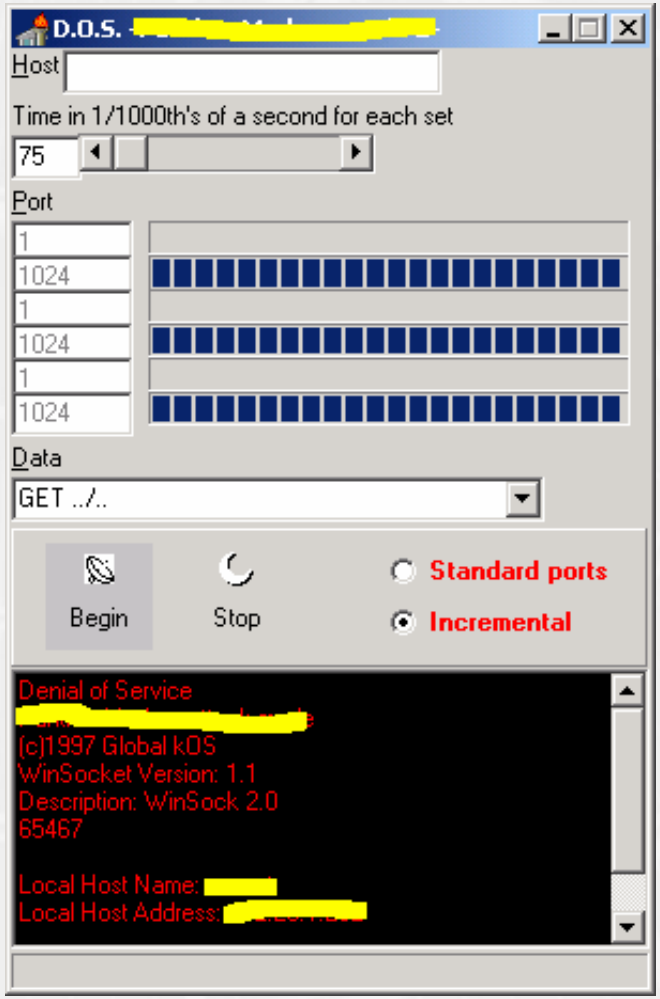
- Attaques qui « crash » les systèmes
  - Pratiquement invisible
- Exploitent les vulnérabilités des systèmes d'exploitation ou des applications
  - Beaucoup de problèmes avec Windows NT
- Attaques de type
  - Ping of death
  - Teardrop
  - Land
  - Targa
  - Etc.

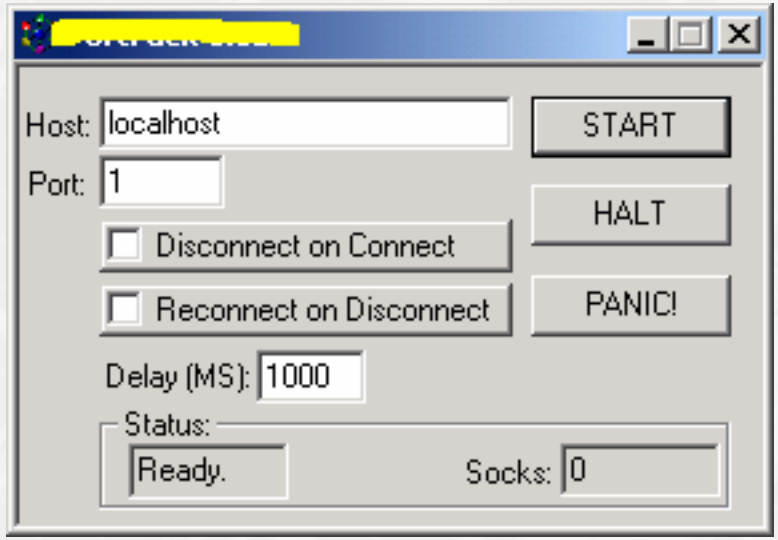
- Exemple: destruction d'un système



Source:
Gibson Research Corparation 2002

- Exemple d'outils DoS pour Microsoft





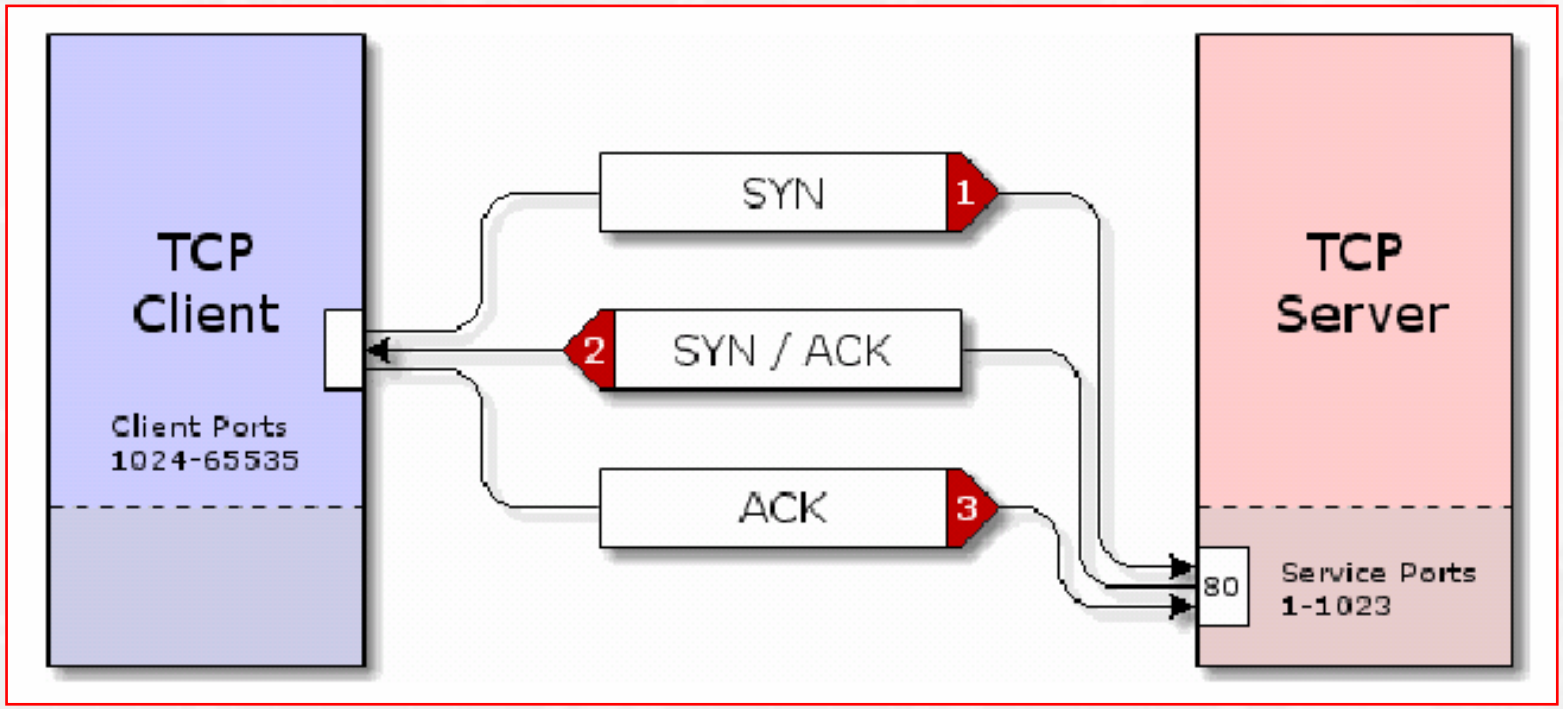
Flooding

- Litéralement: « l'inondation » d'un système
- Attaques de type
  - Syn-Flood
  - Log-Flood
  - Data-Flood

Attaque Syn-Flood

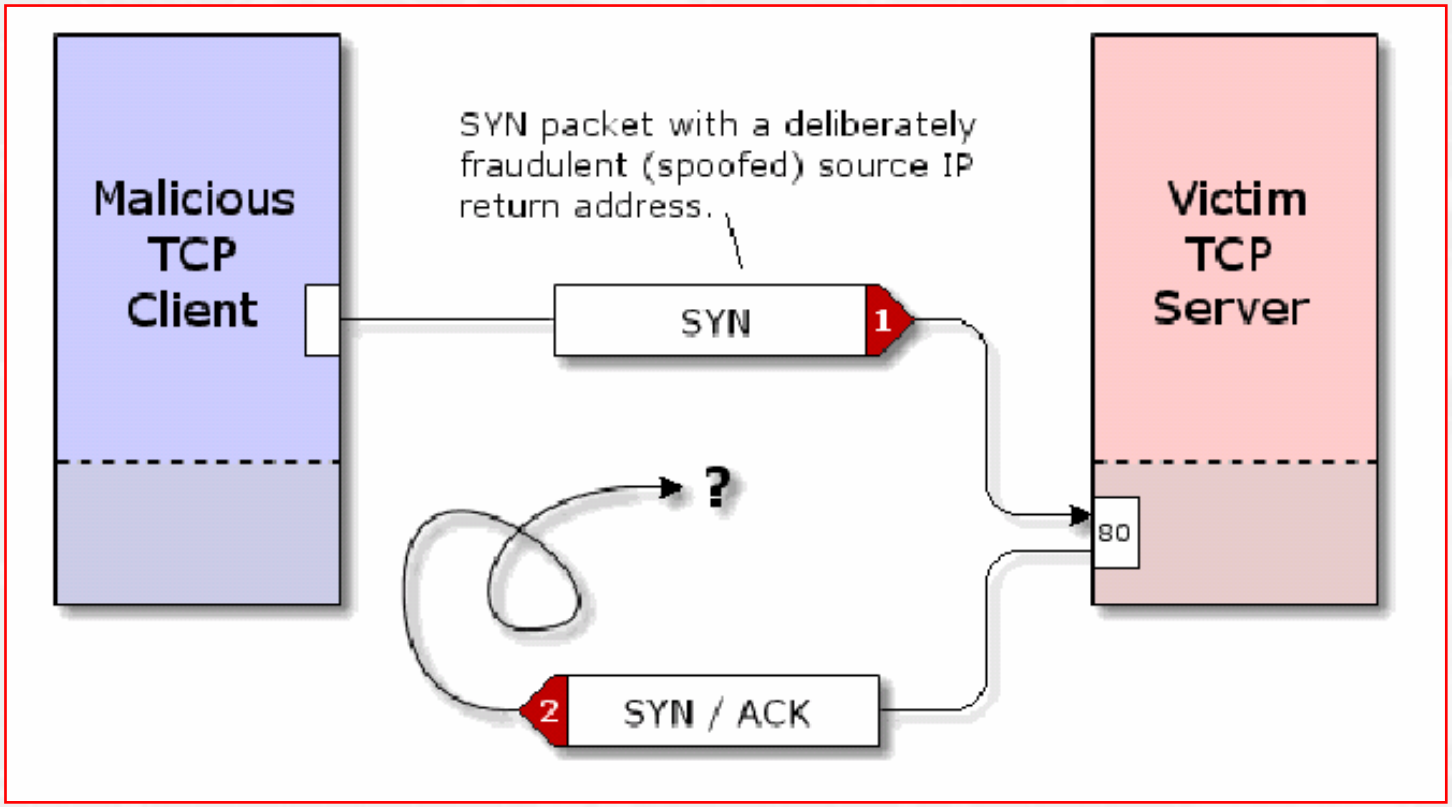
- Exploitation du mécanisme d'établissement d'une connexion TCP
- Immobilisation du système
- Peut dans certains cas « crasher » le système
- Pratiquement anonyme
  - Spoofing d'adresse IP source

- Initialisation d'une connexion TCP en trois phases



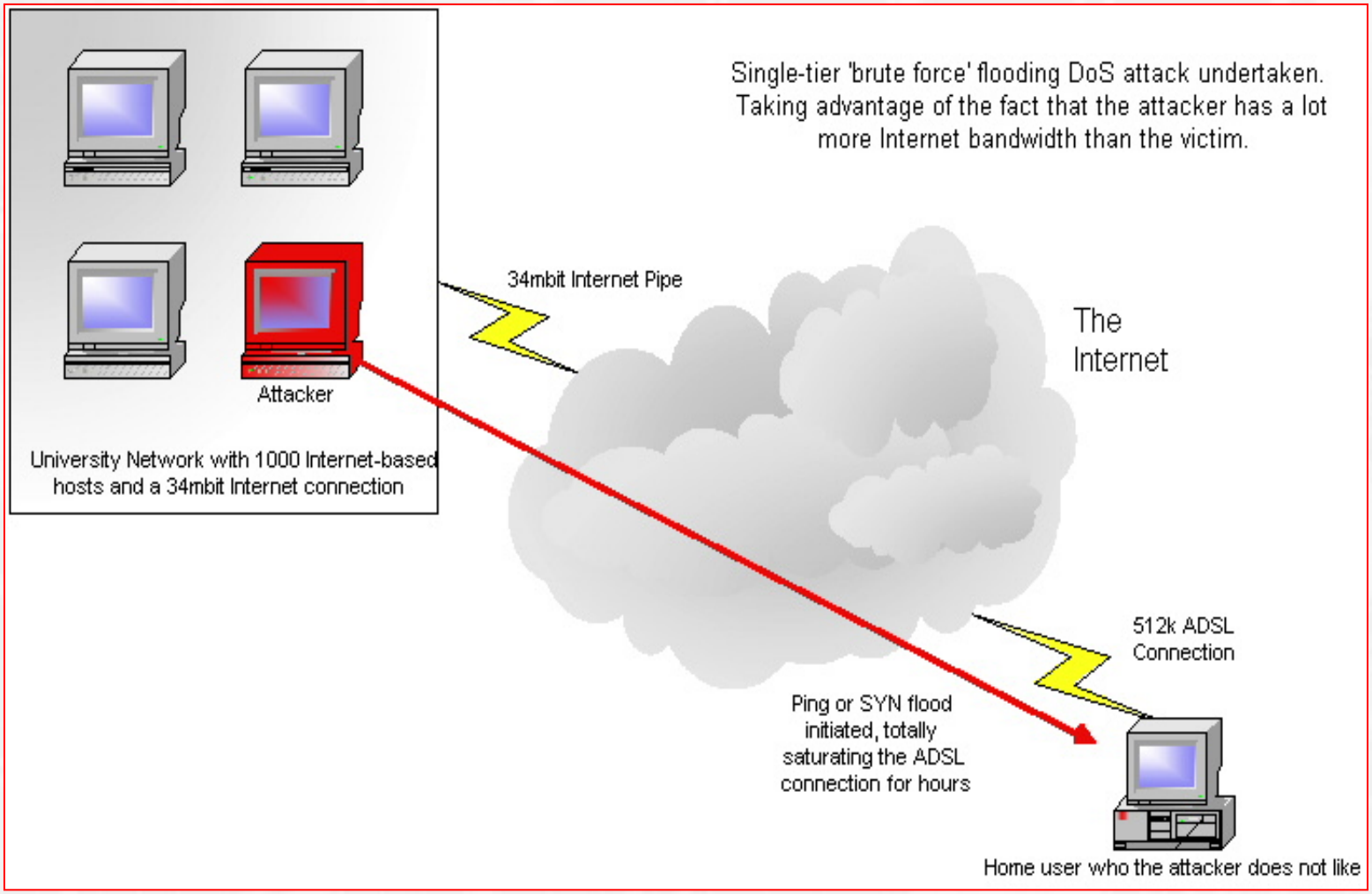
Source:
Gibson Research Corparation 2002

- Attaque de type Syn-Flood



Source:
Gibson Research Corparation 2002

- Exemple: Syn-Flood

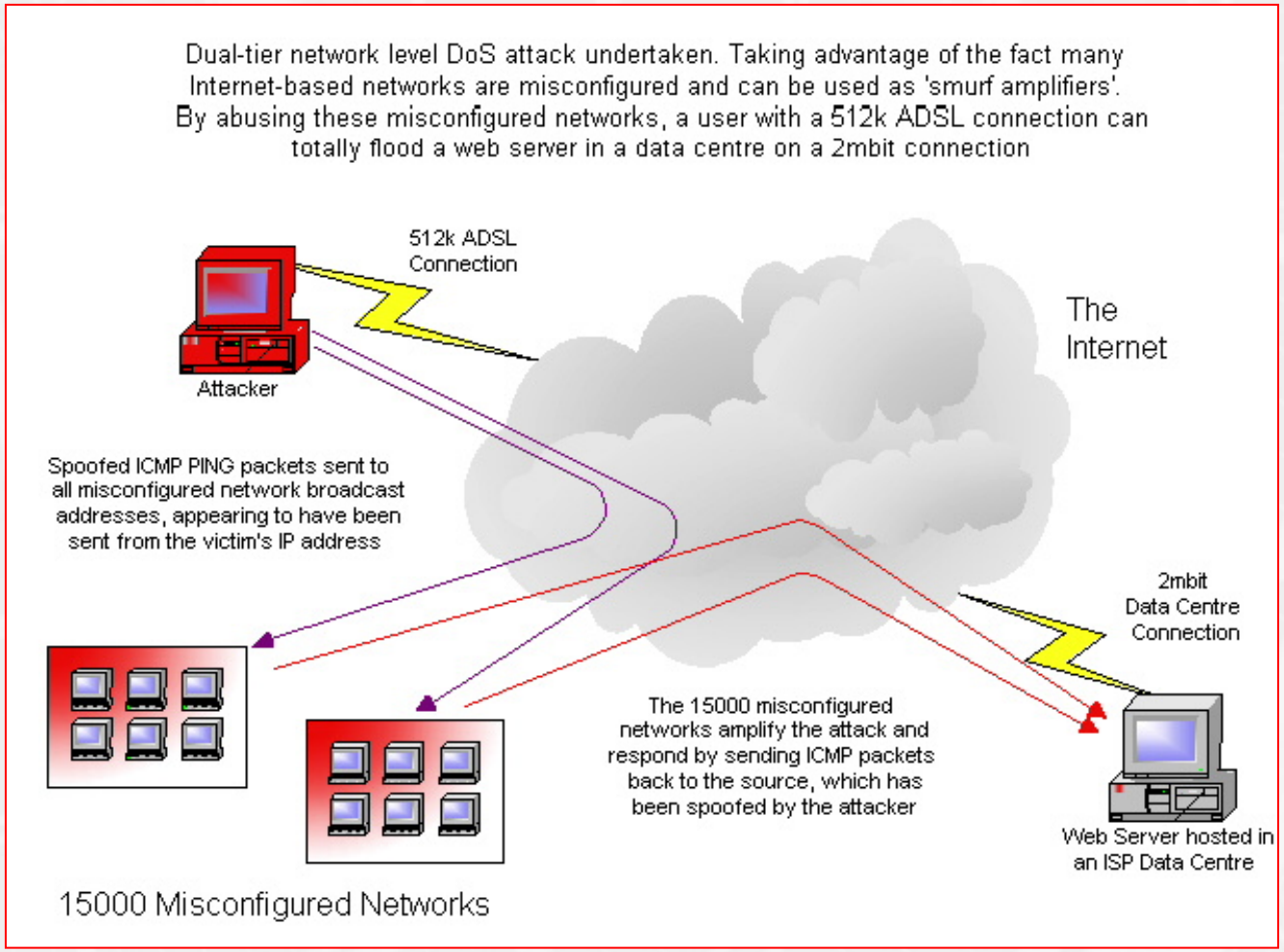


Source:
Gibson Research Corparation 2002

Les dévoreurs de ressources

- Utilisation massive de la bande passante ou des ressources CPU
- La plus connue est Smurf

Exemple: Smurf

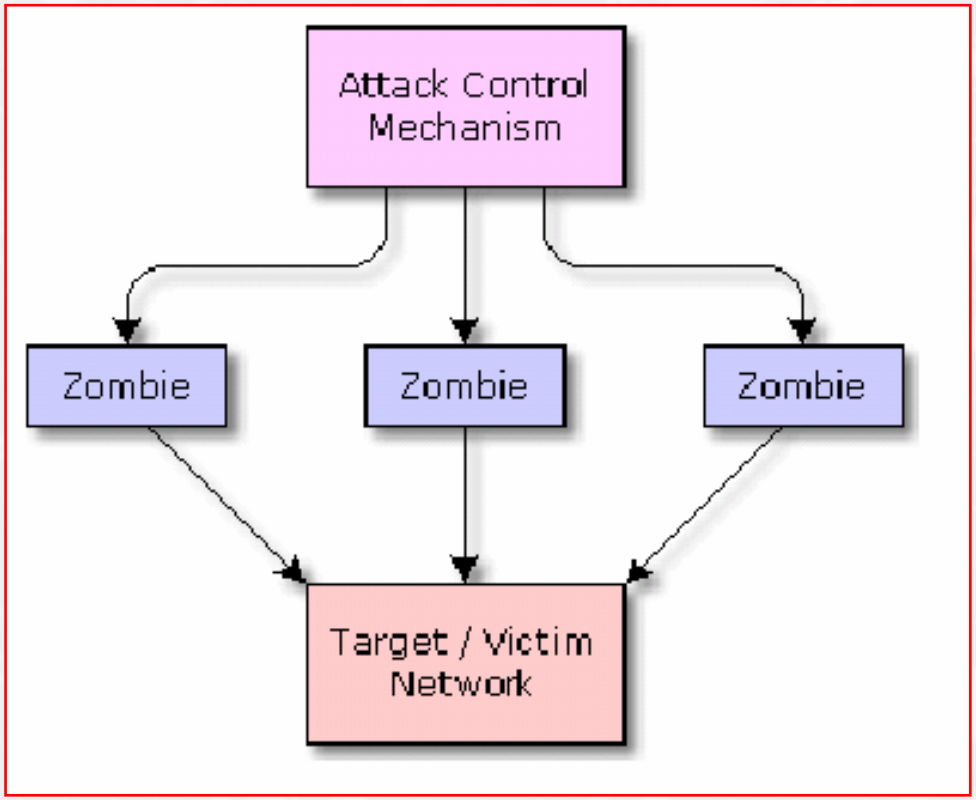


Source:
Gibson Research Corparation 2002

Distributed Denial of Service (DDoS)

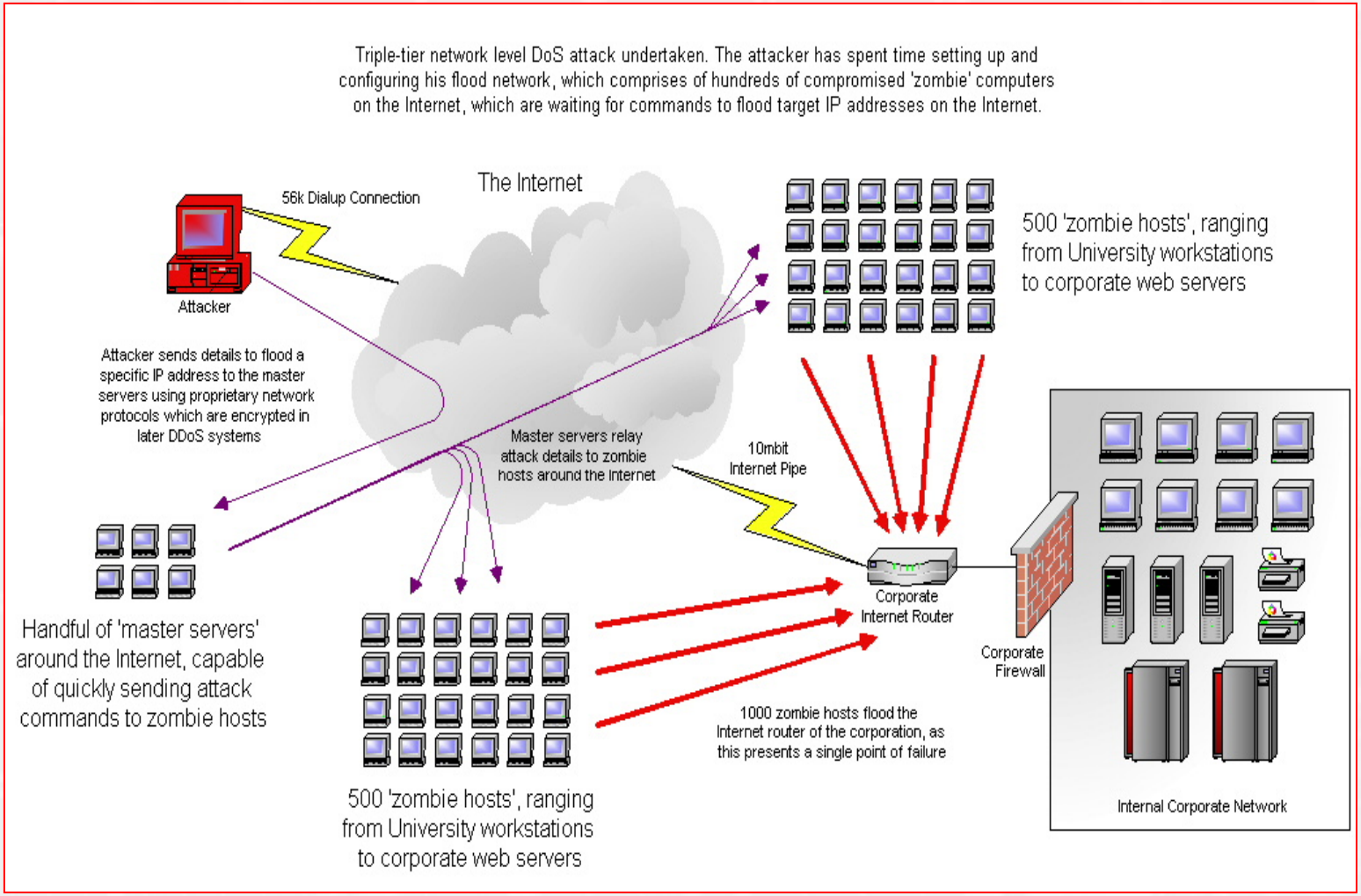
- Amplification des attaques DoS
- Attaques très dangereuses
- Peut impliquer jusqu'à un millier de machines attaquantes
- Outils Open Source

- DDoS: fonctionnement de base



Source:
Gibson Research Corparation 2002

Exemple: DDoS

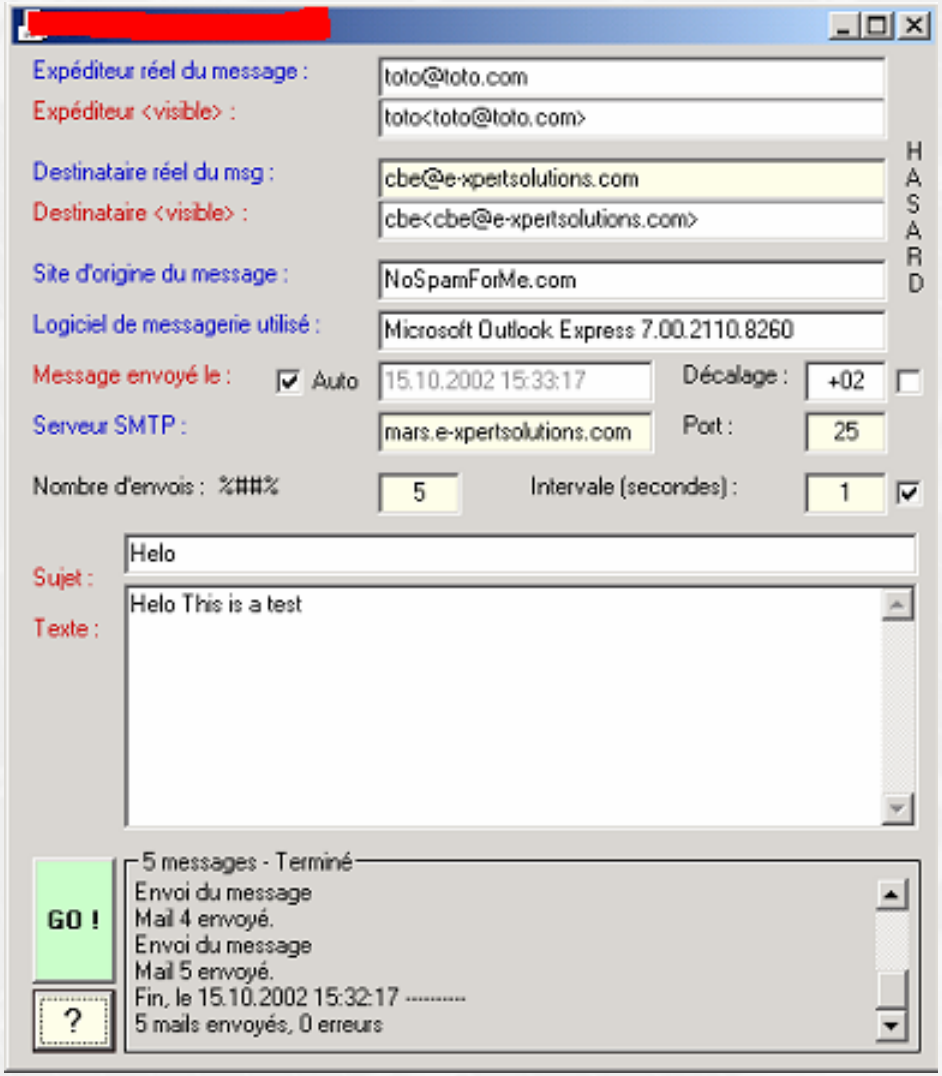


Source:
Gibson Research Corparation 2002

Les Mails Bombs

- Programmes qui envoient des mails en quantité massive
  - Mails obscènes
  - Mails en quantité énormes
  - Abonnement à des mailling lists
  - Fichiers attachés gigantesques
  - Etc.
- Très difficile à stopper
- Très difficile à tracer
  - Relais de messagerie anonyme

- Exemple: mail bomber...



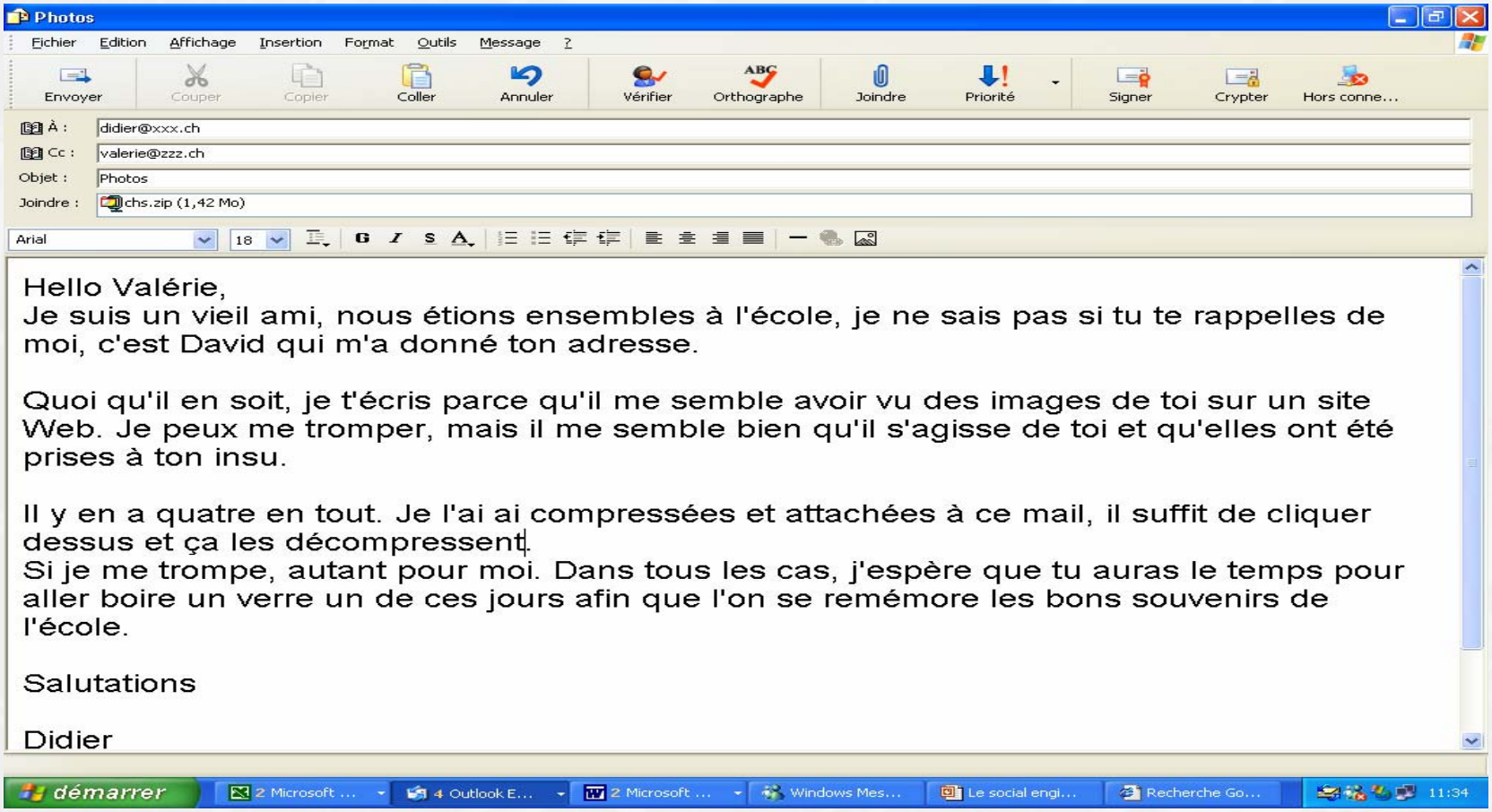
« The weakest link in the chain is the people »

Kevin Mitnik

Social Engineering

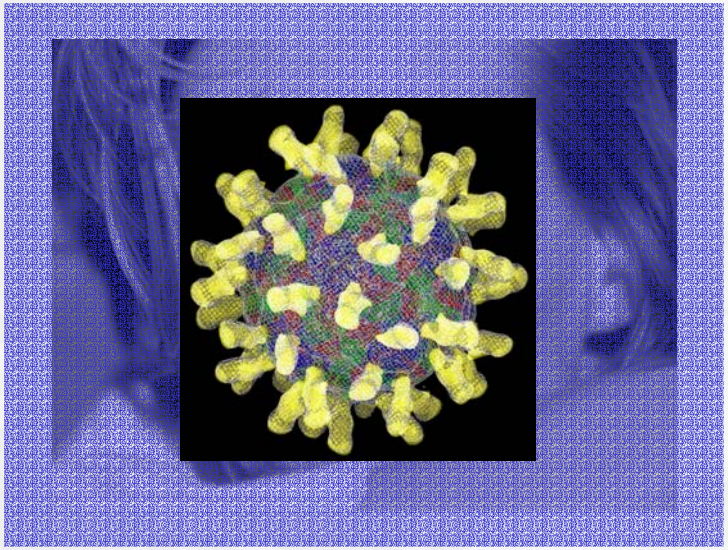
- Technique dans le but d'obtenir des informations confidentielles pour préparer une attaque
  - Utilisation du téléphone
  - Utilisation de l' e-mail
  - Utilisation d'un fax ou du courrier
  - Vol de documents, photos, vol de matériels, etc
  - Manipulation psychologique
  - Etc.

Social Engineering: la messagerie

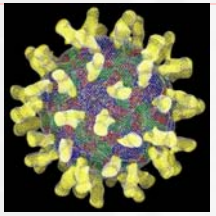


Source: Hacknet 2002

- Social Engineering: le petit cadeau...



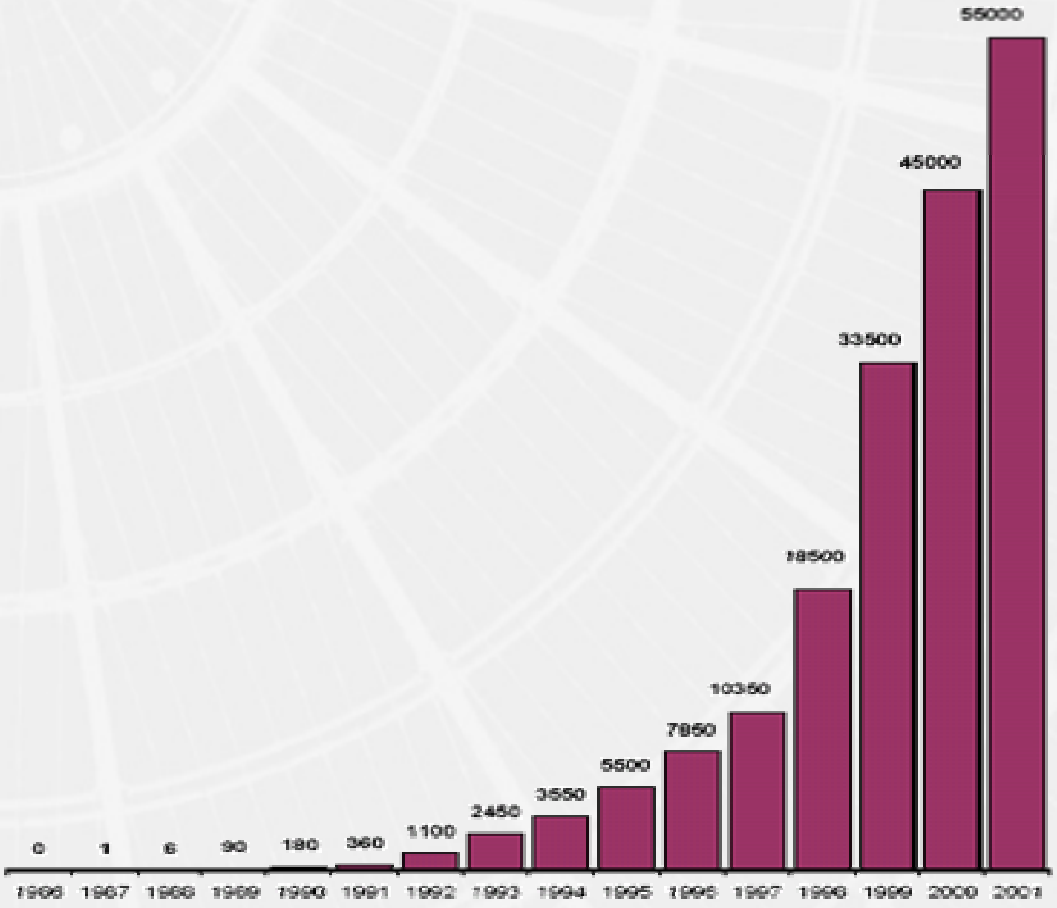
Les virus



- Une des plus grande menace pour les entreprises
- Pus de 90 % des entreprises ont subi des attaques virales
- Le temps de propagation est de plus en plus rapide !
- Coût moyen d'une attaque:
  - 105'000 .- CHF
  - Environ 20 jours / homme de travail

Source: ICSA 2001

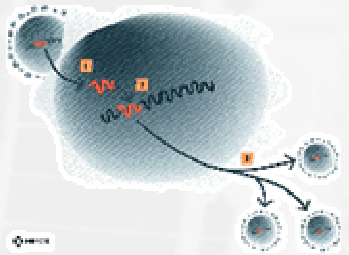
Evolution du nombre de virus



F-Secure
Septembre 2001

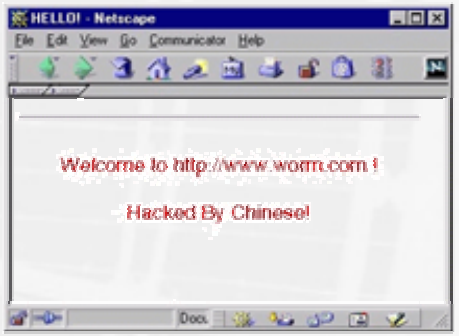
Virus: définition

- Un virus est un programme qui se réplique en s'attachant à un autre objet
- Un ver (Worm) est un programme qui se réplique de façon indépendante



- Une routine de réplication
  - Cette partie est obligatoire pour être un virus
  - Autrement il s'agit d'un « Malware »
- Une routine de type « payload »
  - Partie optionnelle qui effectue une action
    - Destruction, Vol d'information, etc.
    - Affichage d'une image ou vidéo, etc.
    - Son
    - Etc.

- Différents types de virus

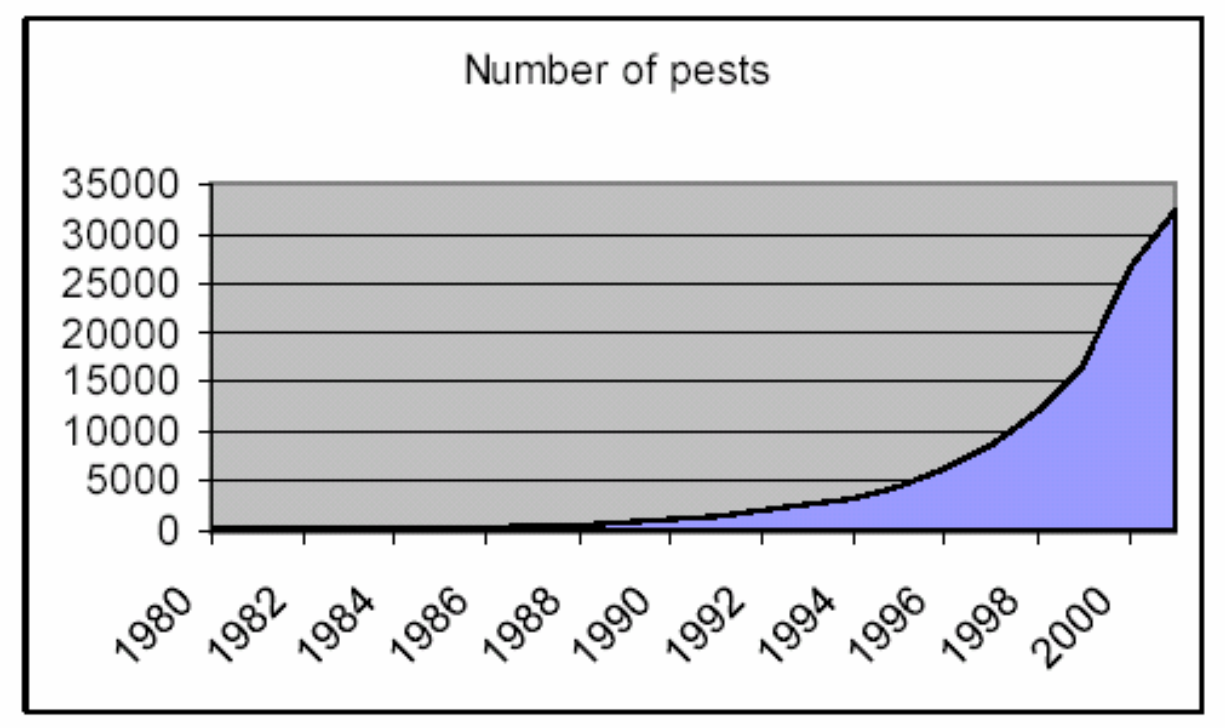


- Boot sector viruses
- Traditional files viruses
- Document et macro viruses
- 32 bits files viruses
- Worms (mail worm / pure worm)
- Malware
  - Cheval de Troie
  - Backdoor
  - Spyware
  - Etc.

- Cheval de Troie ou trojan

- Définition:
  - Un programme légitime qui exécute des actions indésirables
  - Ne se réplique pas
  - Fait partie de la famille des virus au sens large du terme
  - Aussi connu sous le nom de « PESTS »
  - Exemple: un jeux qui installe un key logger
- Le moyen de transport est souvent la messagerie ou un site web
- Une fois executé, il installe:
  - Un Malware, Spyware
  - Une Back Door
  - Etc.

- Evolution des « PESTS »

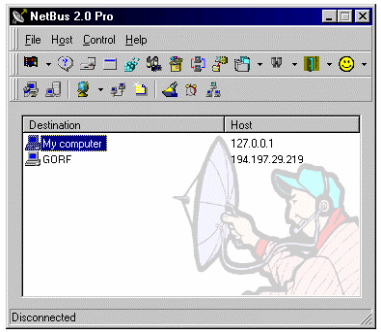


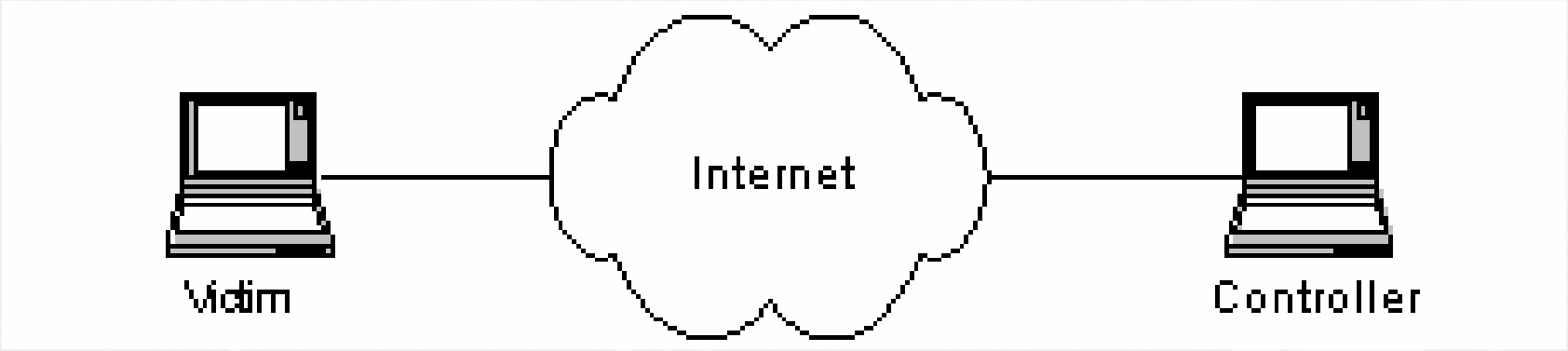
Source: PestPatrol 2001

Backdoor

- Programme malicieux permettant le contrôle total d'une machine
- Fonctionalités
  - Capture écran, clavier, caméra, carte son
  - Transfert de fichiers
  - Capture des mots de passe
  - Registry
  - Exécution de programme
  - Pop up
  - Sniffer, connexion réseau
  - Support de Plug-In
  - Etc.

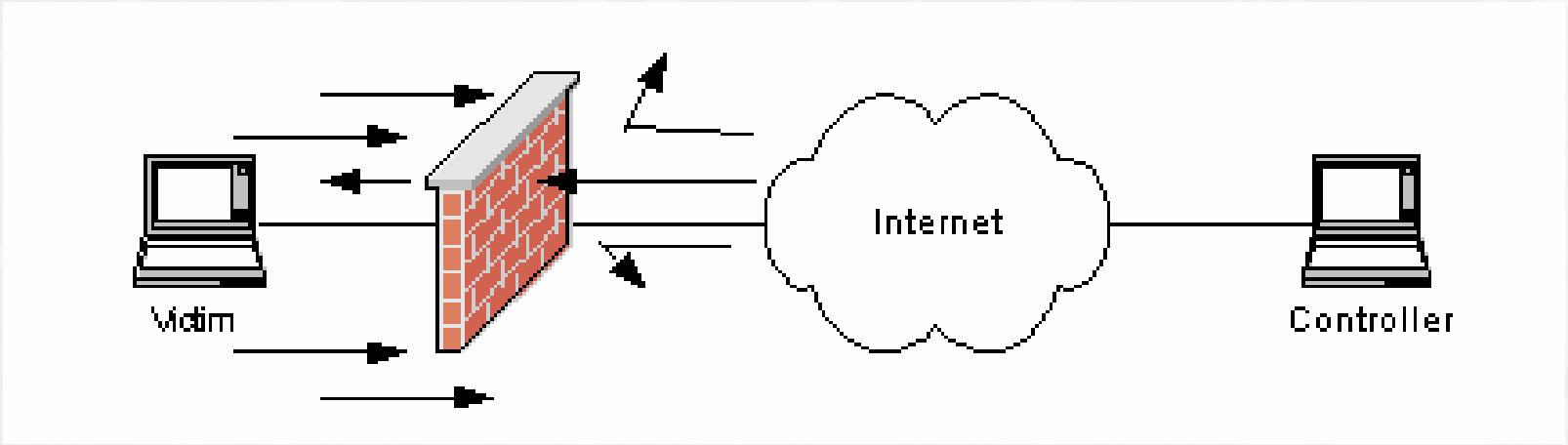
- Backdoor classique: mode de connexion





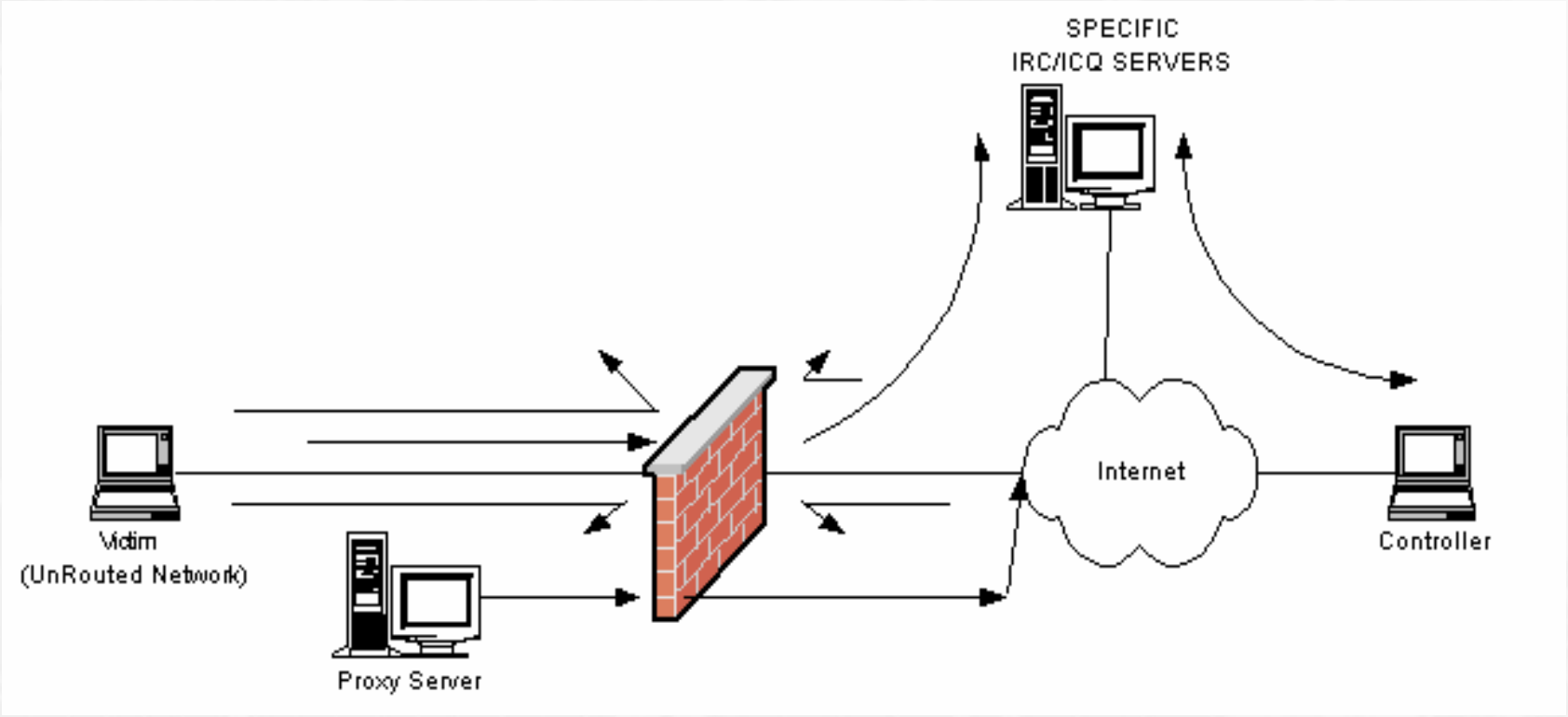
Source: SensePost 2002

- Backdoor classique: firewall



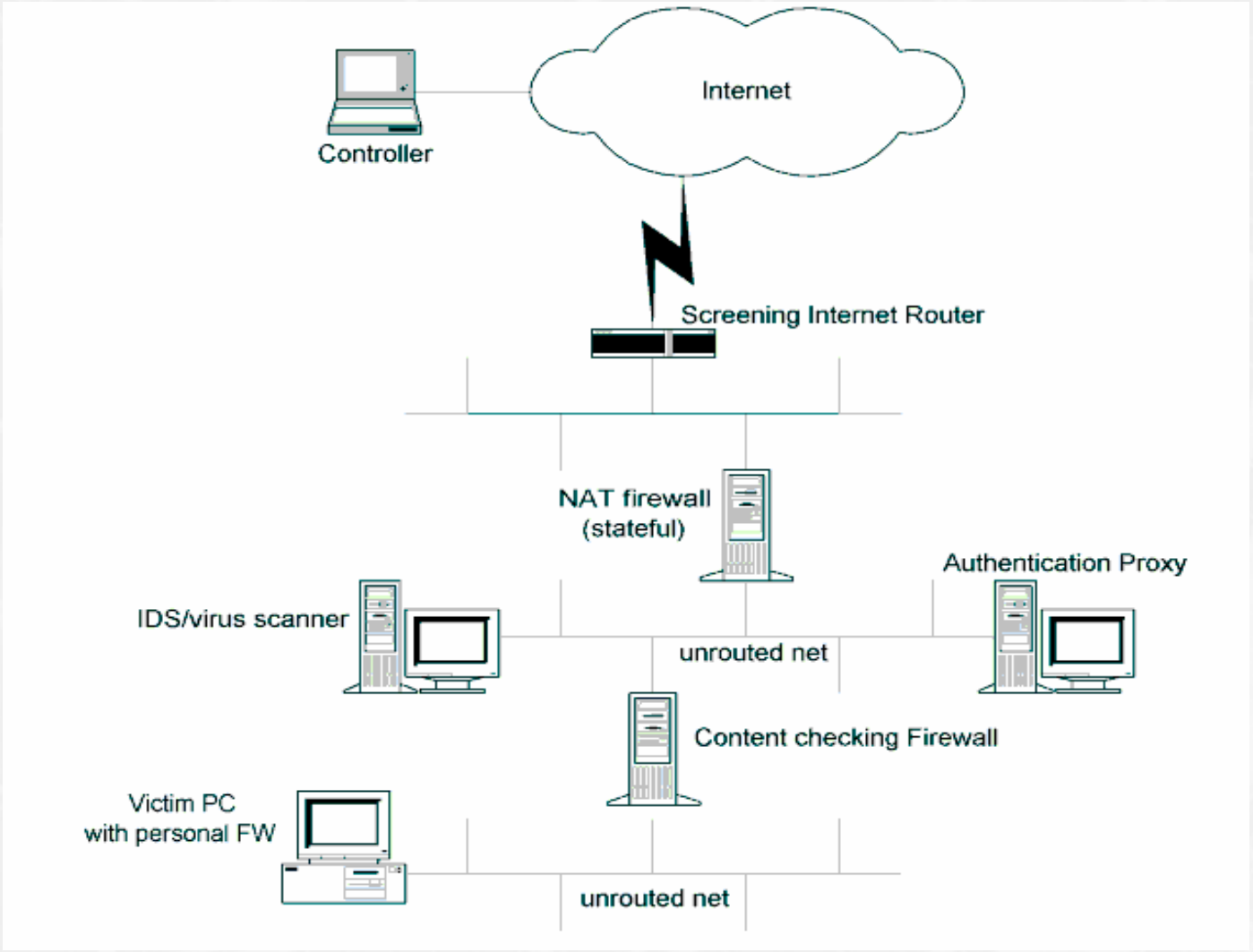
Source: SensePost 2002

- Backdoor évoluée



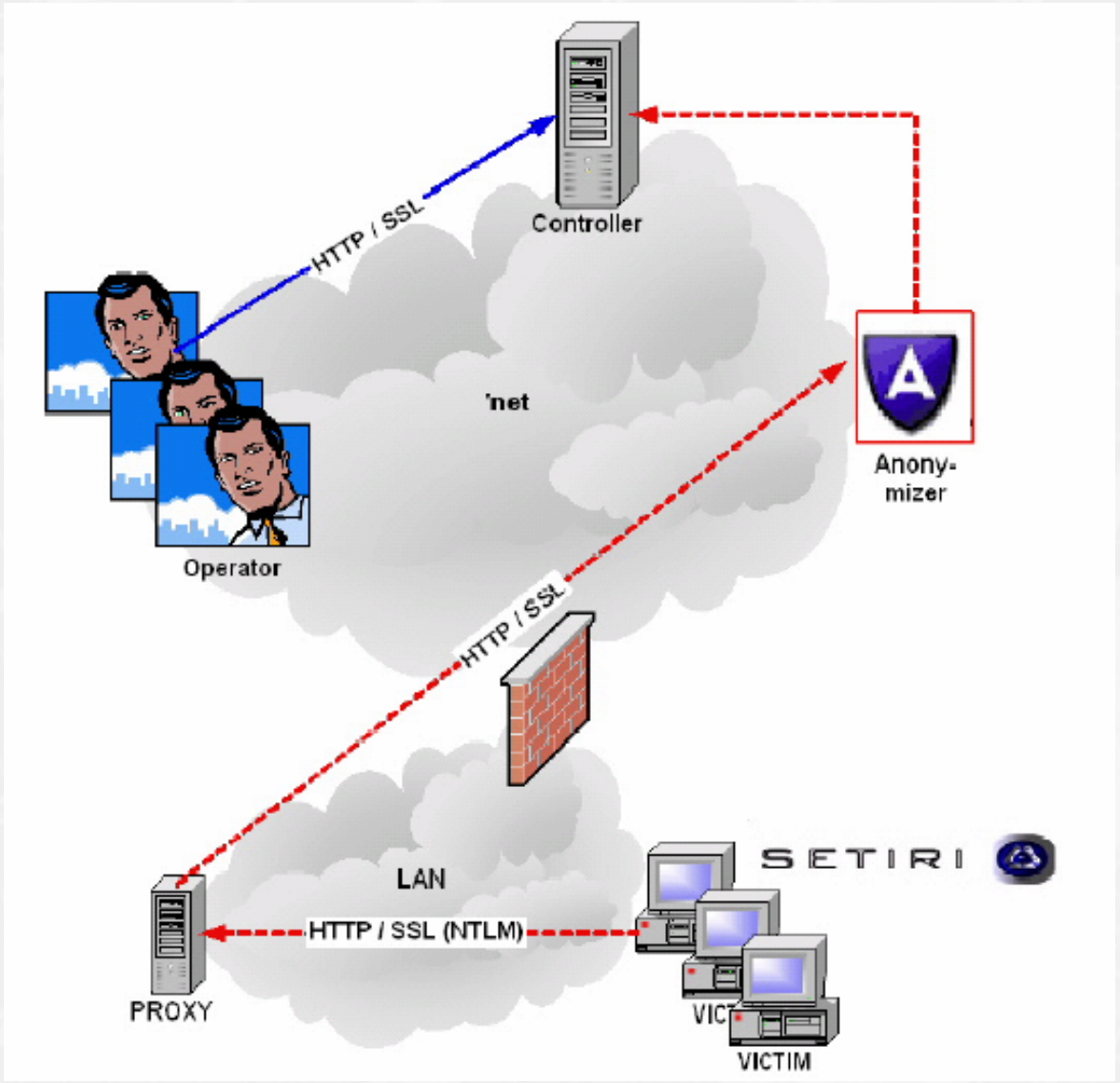
Source: SensePost 2002

- Un réseau « typique »



Source: SensePost 2002

- Backdoor: utilisation de IE (http/ https)

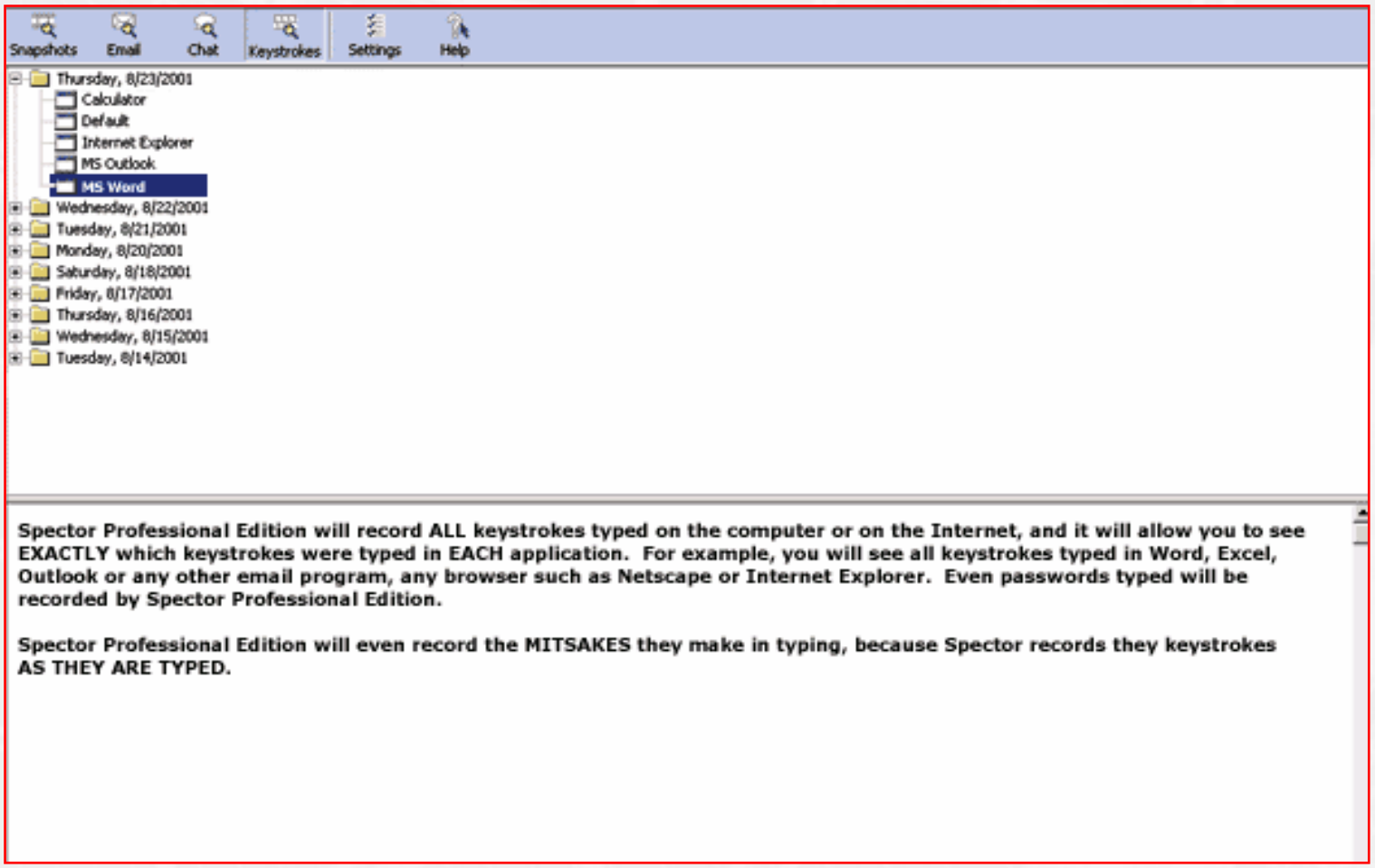


Source: SensePost 2002

Key logger

- Famille des « Malware » ou « SpyWare »
- Permet d'enregistrer toutes les touches du clavier
- Envoie des informations par:
  - Mail
  - FTP
  - HTTP
  - Etc.
- Invisible sur la machine pour un utilisateur « standard »
- Disponible en logiciel commercial…

- Exemple de Key Logger



- Evolution des virus: 1988-2002

Virus type	Widespread	Replication media	Typical time needed to produce a new generation	Typical time to become widespread worldwide
Boot viruses	1988 – 1995	Diskettes	Weeks[15]	> 1 year
16-bit file viruses	1988 – 1995	Program files	Weeks[16]	> 1 year
Macro viruses	1995 -	Document files	Days[17]	1 month
E-mail worms	1999 -	E-mail messages	Hours[18]	24 h[19]
Pure worms	2001 -	TCP/IP connection	Minutes[20]	Hours[21]

Source: F-Secure 2001

- Remote SMTP Server Detection
  - Attaque basée sur une vulnérabilité (DoS, BoF, Root exploit, etc.)
- Relais de messagerie
- Usurpation d'identité
- Spoofing de mail
- Protocole SMTP
  - Protocole non sécurisé
  - Atteinte à l'intégrité des messages
  - Atteinte à la confidentialité des messages
- Spam (mail bomber, publicité, etc.)

- Atteinte à la confidentialité: exemple avec une Backdoor

Personne A

SMTP

Serveur de messagerie

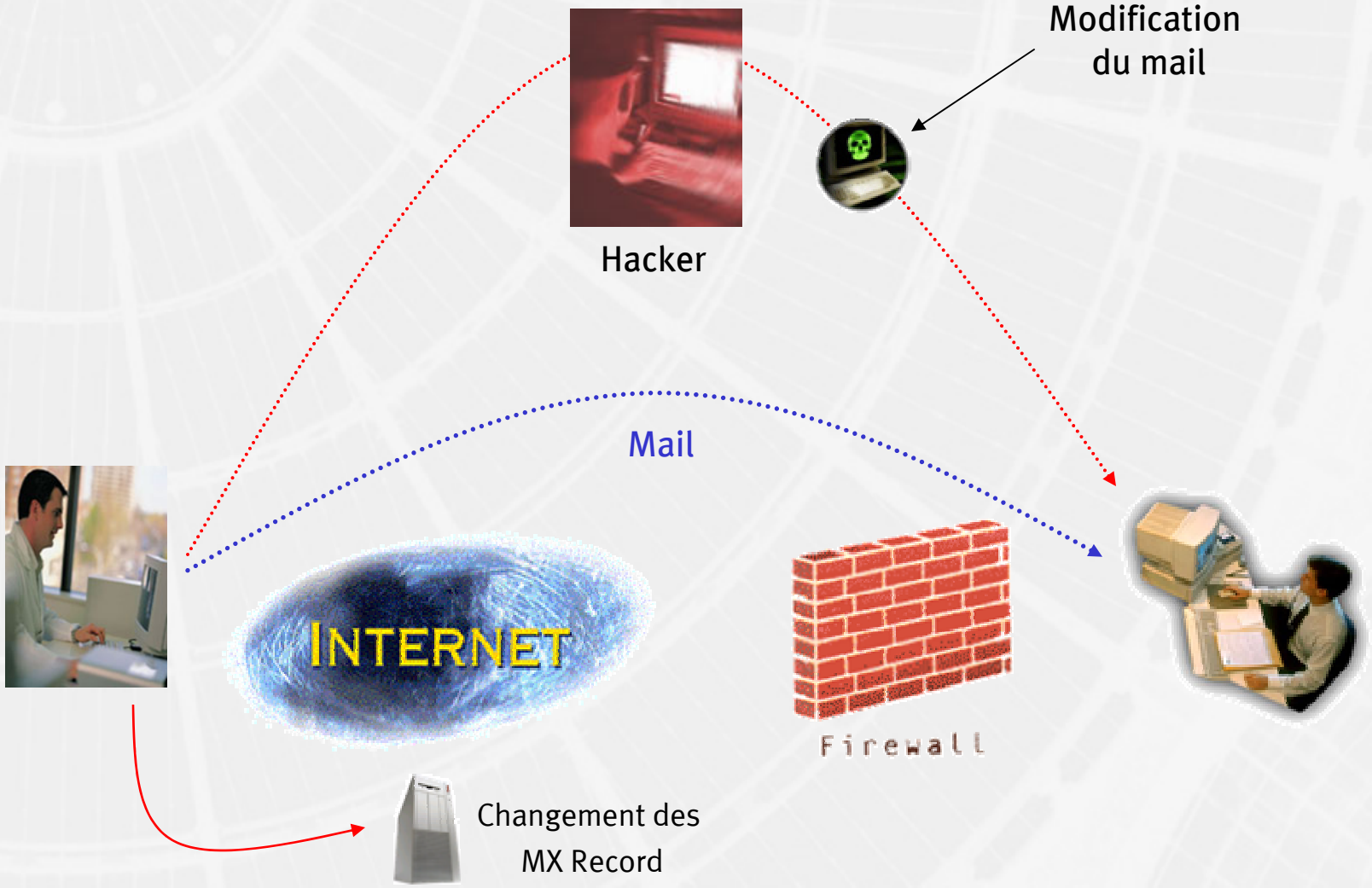
POP3

Personne B

Backdoor invisible

Black Hat

- Atteinte à l'intégrité: exemple avec une attaque sur les DNS



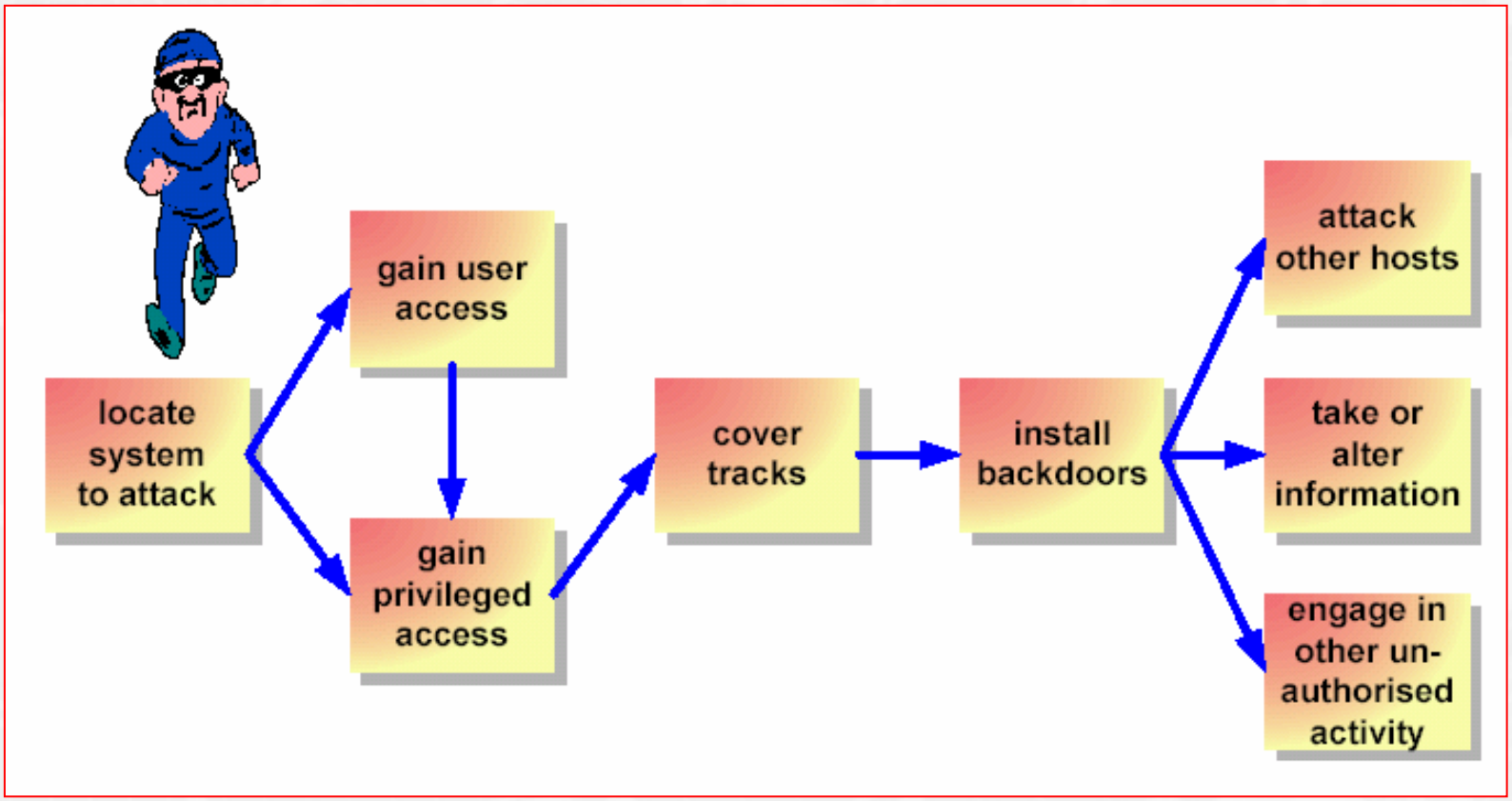
Compromission système

- L’idée est de prendre le contrôle complet de la machine au niveau de son système d’exploitation
- Les cibles sont des machines mal configurées ou/et non « patchées »
  - Microsoft
  - Unix / Linux
  - etc.

- Compromission système

- L’accès permet:
  - Examiner des informations confidentielles
  - Altérer ou détruire des données
  - Utiliser des ressources systèmes
  - Ecouter le traffic sur le réseau local
  - Effectuer des DoS
  - Lancer des attaques vers d’autres systèmes

- Compromission système: scénario classique d'attaque



Source: CERT 2001

- Après la compromission du système:
  - Effacement des fichiers de « logs »
  - Inspection de la machine
    - FIA, etc
  - Installation d'une « Back Door »
  - Installation d'un « Root Kit »
  - Installation de logiciels d'attaques
    - Outils d'attaques « ARP »
    - Un sniffer de mot de passe
    - Un scanner
    - Etc.

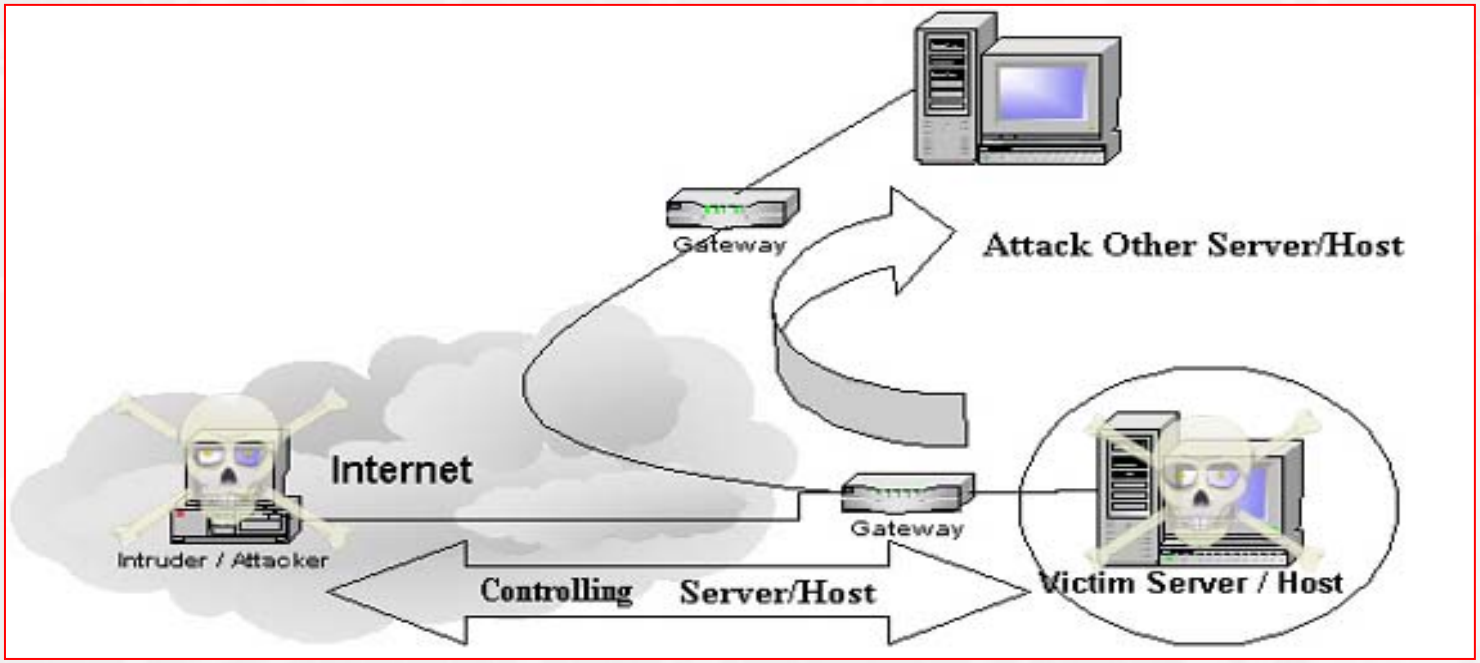
Root Kit

- Kit de programmes pour dissimuler les traces sur une machine et garder le contrôle de la machine (Root)
- Environnement Unix et Microsoft
  - Root Kit Unix
    - Remplacement des commandes: ls, ps, netstat, top, su, tcpd, ssh, etc.
    - Cacher certains fichiers
    - Backdoor
  - Root Kit Microsoft
    - Cache certains processsus
    - Cache certains fichiers
    - Cache certaines « Registries »
    - Backdoor

Root Kit: les deux familles

- Application Root Kit
  - Root Kit conventionnel
  - Remplacement des commandes
  - Programme avec Backdoor
- Kernel Root Kit
  - Manipulation des « Call System »
  - Très difficile à détecter

- Root Kit: compromission d'autres systèmes



- Buffer Overflow

Buffer Overflow: une menace très importante

- BoF
- 60% des attaques (CERT 2002)
- Très puissant
  - Exécution de code hostile (très souvent avec privilèges)
  - Exploit local ou distant
- Extrêmement facile à utiliser
  - Tools pour « Script Kidies » (Exploit)
- Code Red et Nimda en 2001
  - BoF on ISAPI

Buffer Overflow: pourquoi existent ils ?

- Mauvaise programmation
  - Gestion des pointeurs
  - Manipulation des « buffers »
- Peu de contrôle du code (QA)
  - Pas de tests des BoF
- Pas de validation des « buffers »
  - Limitation du nombre de caractères
- Pas de design pensé sécurité
  - Trop chère et trop lent

Buffer Overflow: objectif

```
char shellcode[] =
  "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
  "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
  "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

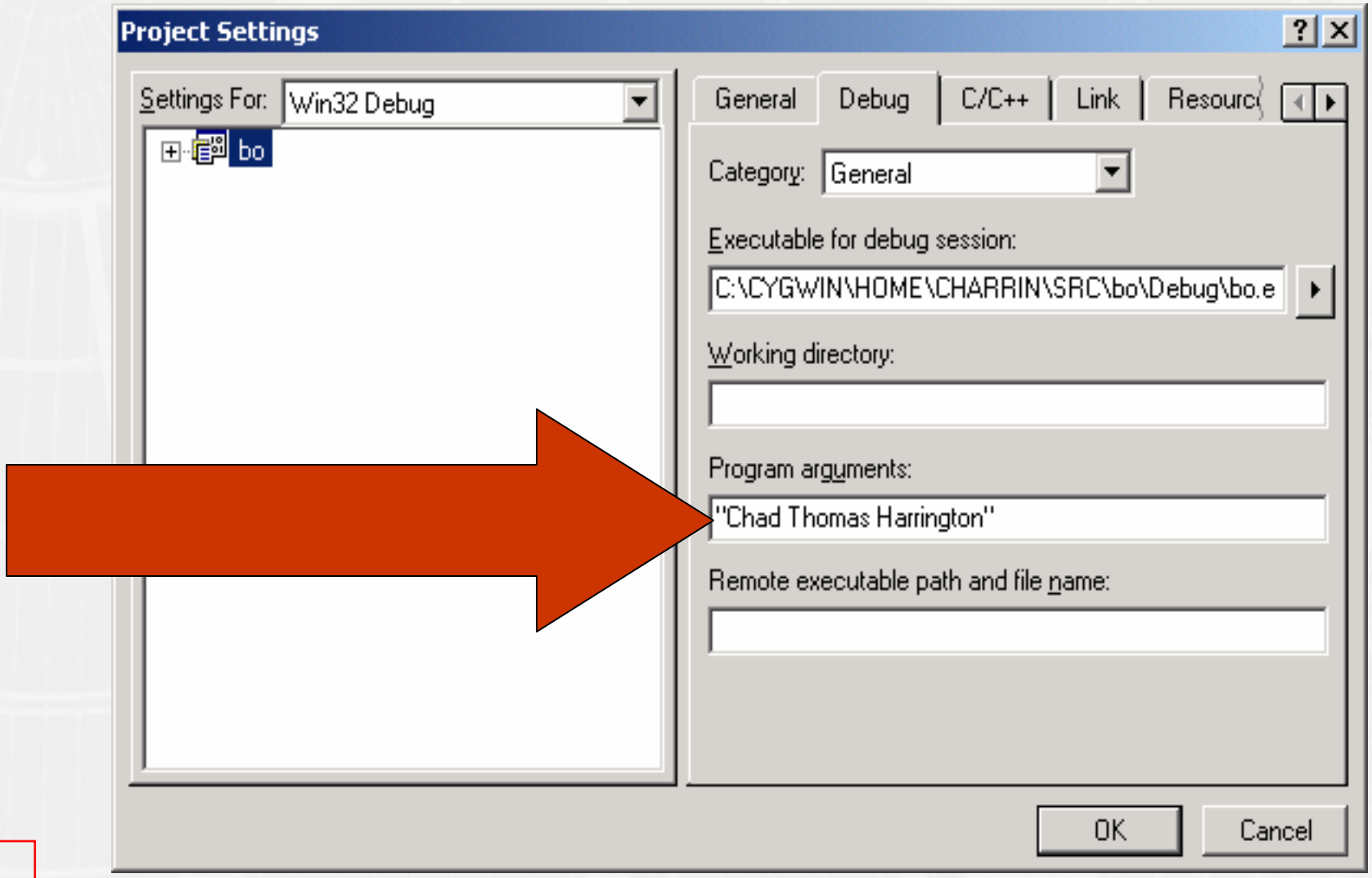
- Forcer l'exécution d'un code hostile dans le but de:
  - D'obtenir un accès Root ou équivalent
  - Exécuter un DoS
  - D'installer une backdoor
  - De corrompre une machine
  - Etc.
    - Pas de limite: dépend du code hostile et de l'imagination de son auteur

Buffer Overflow: démonstration

```
/************* Buffer Overflow Demonstation Program ********************/
/************* Copyright 2002 - Entercept           ********************/
/************* Author: Chad Harrington              ********************/

#include <stdio.h>
#include <string.h>
void SayHello(char* name_specified);


/* --------- THE PROGRAM STARTS HERE ---------------                    */
void main(int argc, char** command_line_arguments)
{
    /* Call the SayHello subroutine with the
       first command-line argument as name                               */
    SayHello(command_line_arguments[1]);

    /* Print the contents of the buffer                                  */
    printf("\n\nAll Done...\n");
}


/* --------- A SUBROUTINE --------------------------                    */
void SayHello(char* name_specified)
{
    /* Allocate a 100 byte buffer for the name                           */
    char name_buffer[100];

    printf("\nEntering the SayHello() subroutine...\n\n");

    /* Copy the name spcified by the user into the buffer                */
    strcpy(name_buffer, name_specified);

    /* Print "Hello, <name>" using the name stored in the buffer         */
    printf("Hello, ");
    printf(name_buffer);
}
```

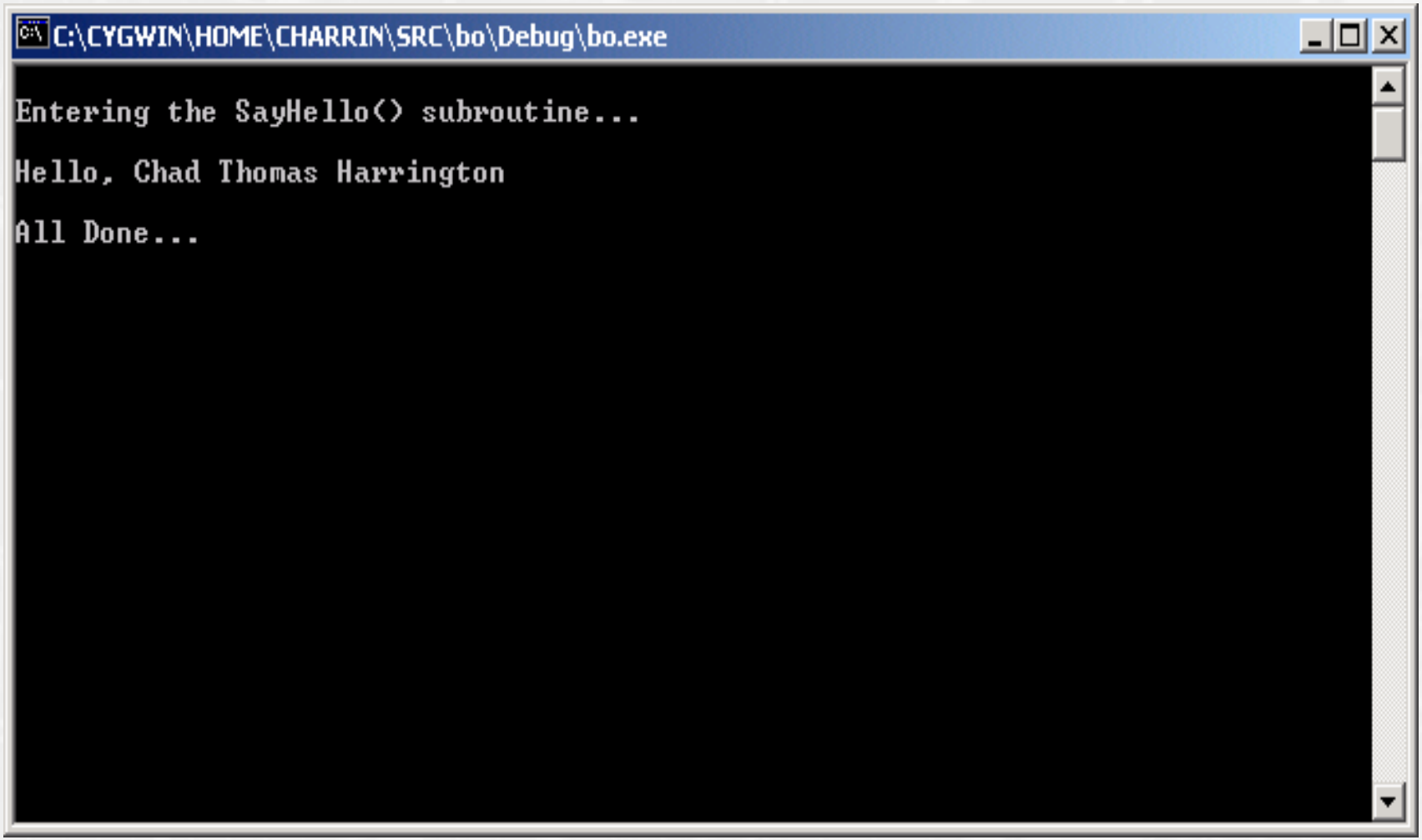
Source:
Entercept 2002

- Buffer Overflow: démonstration



Source:
Entercept 2002

- Buffer Overflow: démonstration



Source:
Entercept 2002

- Buffer Overflow: démonstration

```
0040D728   mov         eax,dword ptr [ebp+0Ch]
0040D72B   mov         ecx,dword ptr [eax+4]
0040D72E   push        ecx
0040D72F   call        @ILT+10(_SayHello) (0040100f)
0040D734   add         esp,4
16:
17:        /* Pr        contents of the buffer                    */
18:        print      nAll Done...\n");
0040D737   push        offset string "\nAll Done...\n" (00422fd4)
0040D73C   call        printf (00401060)
0040D741   add         esp,4
19:    }
0040D744   pop         i
0040D745   pop
0040D746   pop
0040D747   add         10h
0040D74A   cmp         sp
0040D74C   call        sp (004010e0)
0040D751   mov         es
0040D753   pop         ebp
0040D754   r
```

Here is the “Call” instruction that tells the OS to jump to our SayHello subroutine

Source:
Entercept 2002

- Buffer Overflow: démonstration

```
0040D728    mov         eax,dword ptr [ebp+0Ch]
0040D72B    mov         ecx,dword ptr [eax+4]
0040D72E    push        ecx
0040D72F    call        @ILT+10(_SayHello) (0040100f)
0040D734    add         esp,4
16:
17:         /* Print the contents of the buffer                              */
18:         printf("\n\nAll Done...\n");
0040D7     push        offset string "\nAll Done...\n" (00422fd4)
0040D      call        printf (00401060)
0040D741   add         esp,4
19:     }
0040D744                edi
0040D745                esi
0040D746                ebx
0040D747                esp,40h
0040D74A                ebp,esp
0040D74C                __chkesp (004010e0)
0040D751    mov         esp,ebp
0040D753    pop         ebp
0040D754
```

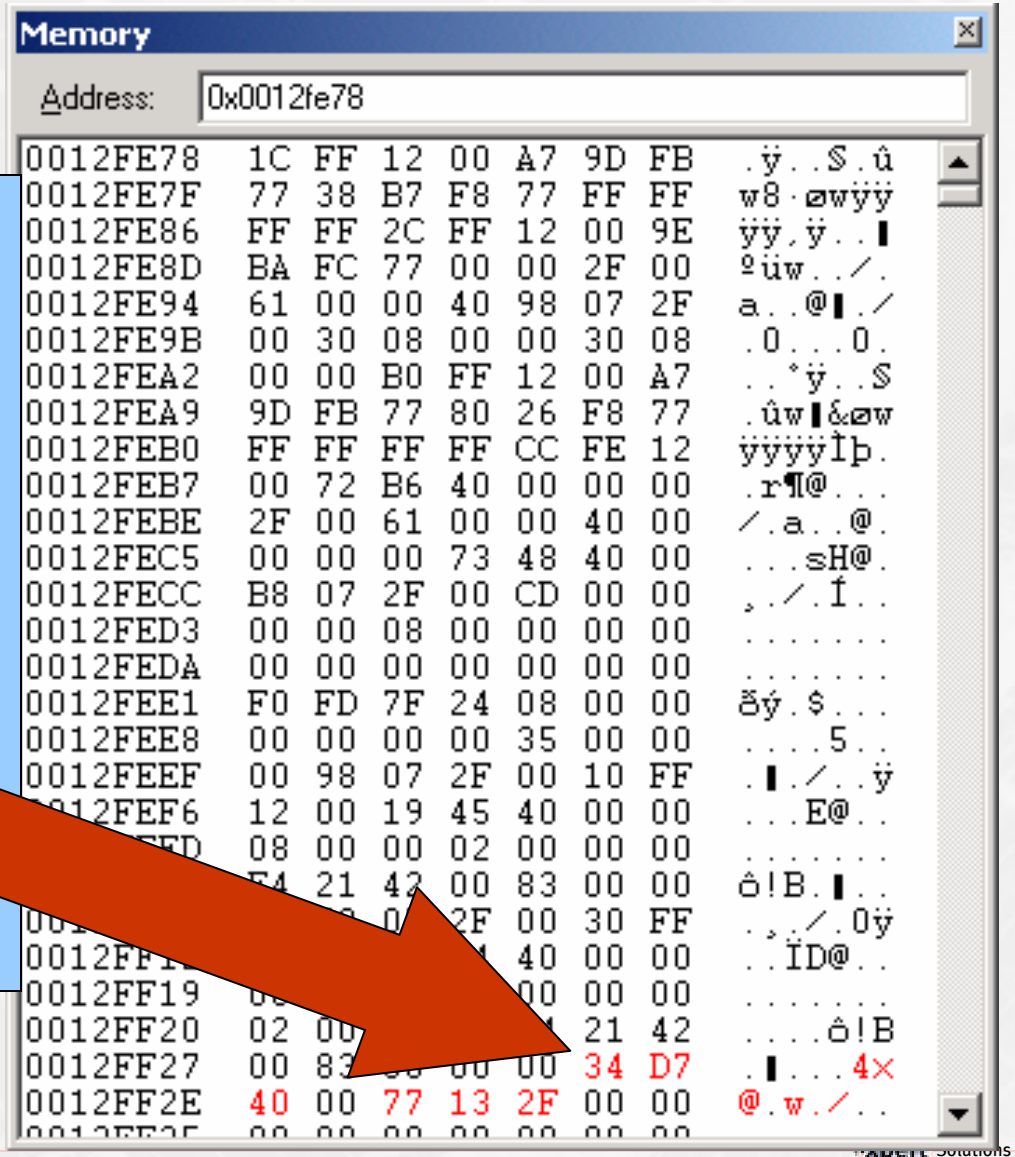
This is where the program SHOULD return after executing SayHello: 0040D734

Source: Entercept 2002

- Buffer Overflow: démonstration

The return address (00 40 D7 34) is now pushed onto the stack. Intel architectures are little-endian, so the address appears reversed:

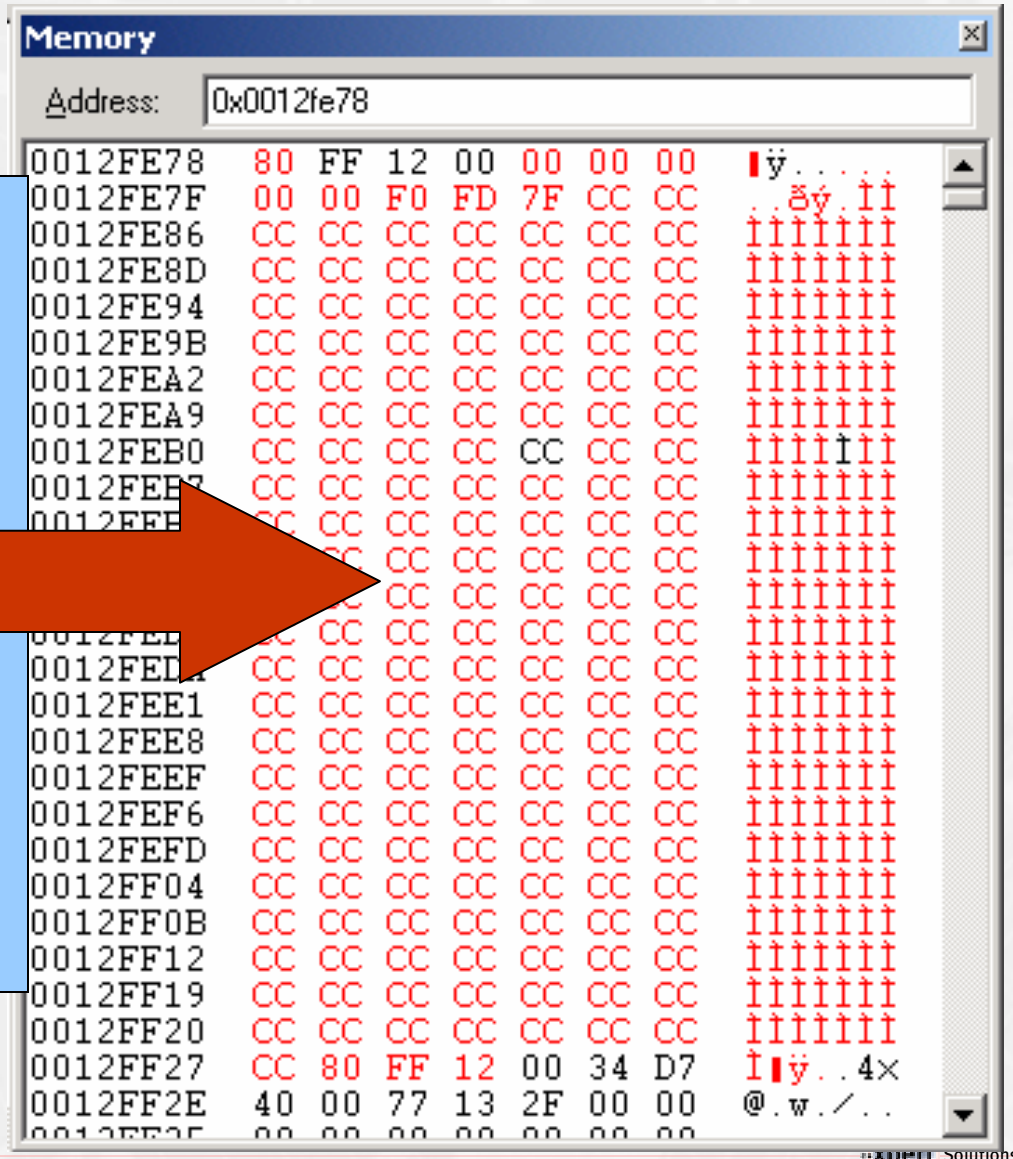
34 D7 40 00



Source: Entercept 2002

- Buffer Overflow: démonstration

The debugger has cleared the stack frame for us by filling it with CC bytes

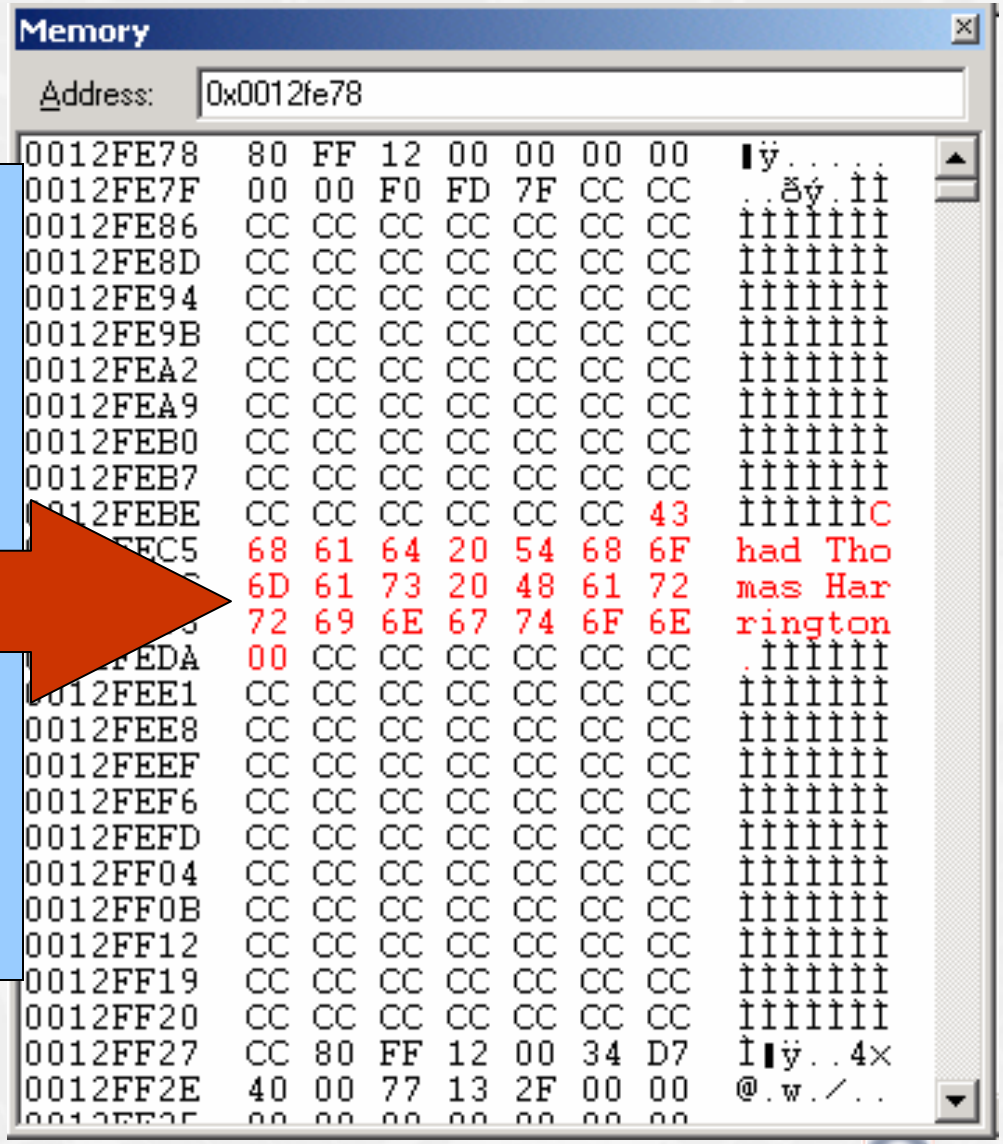


Source:
Entercept 2002

- Buffer Overflow: démonstration

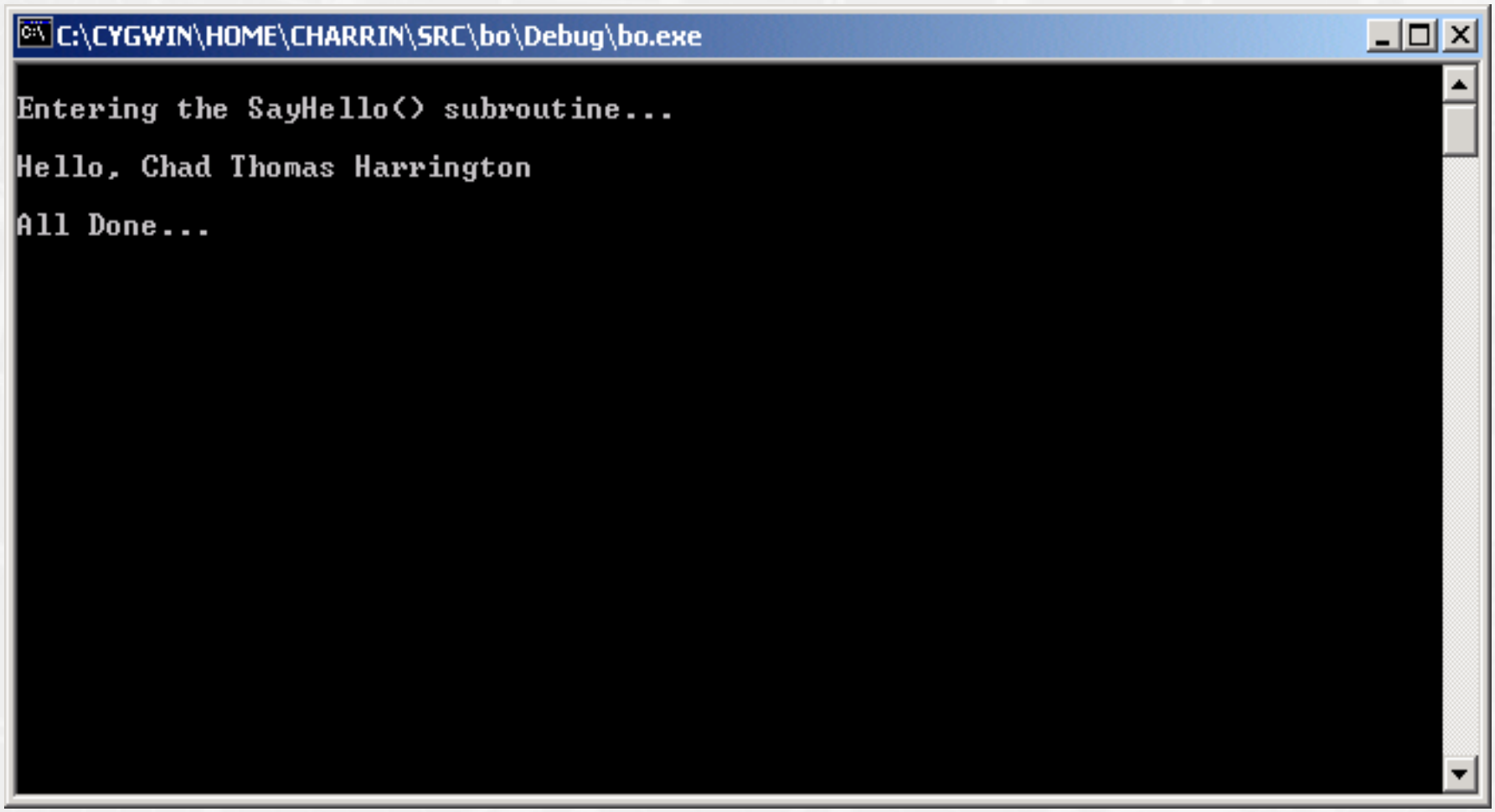
Now the strcpy() function is called.

The data supplied is copied into the buffer.



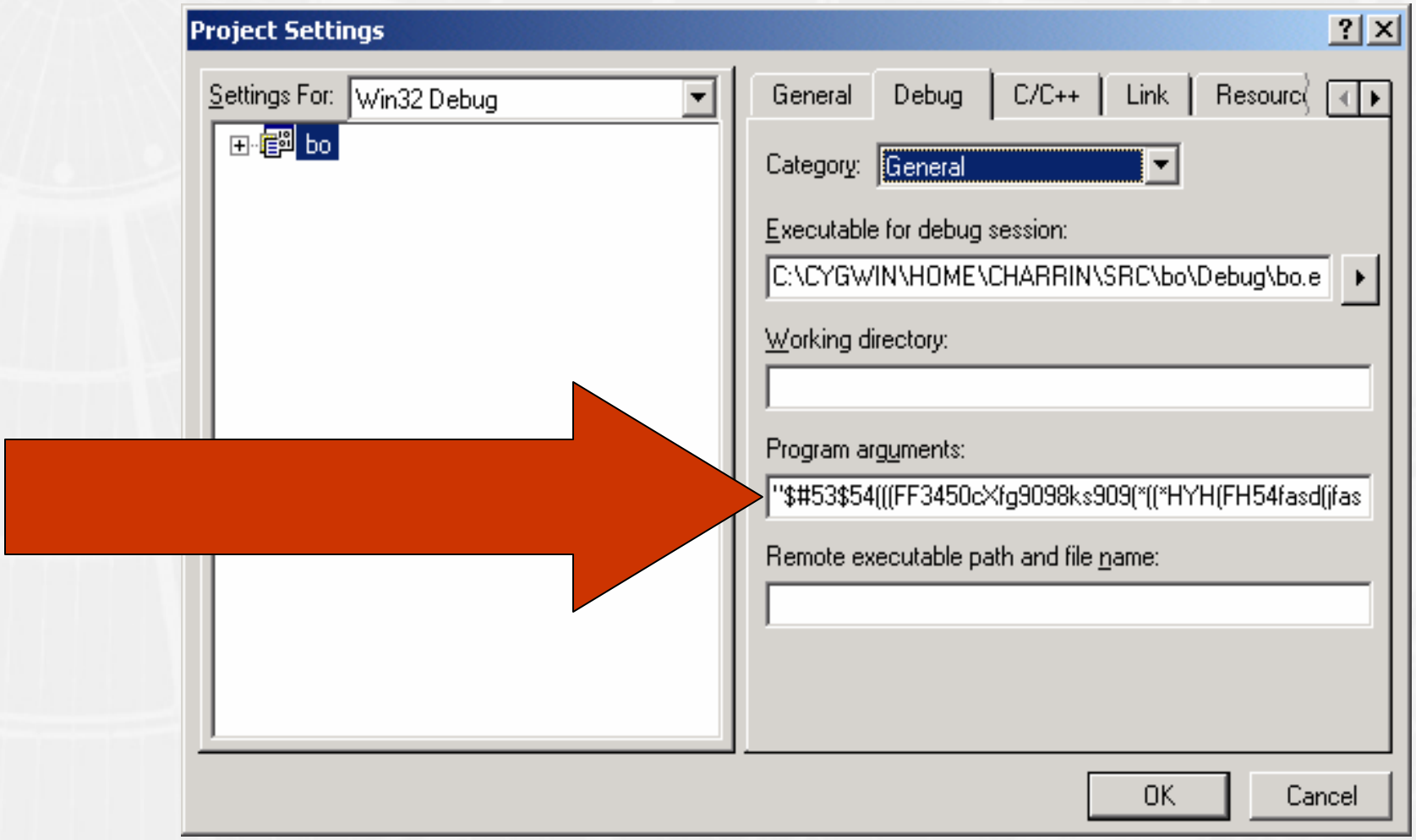
Source:
Entercept 2002

- Buffer Overflow: démonstration



Source:
Entercept 2002

- Buffer Overflow: démonstration

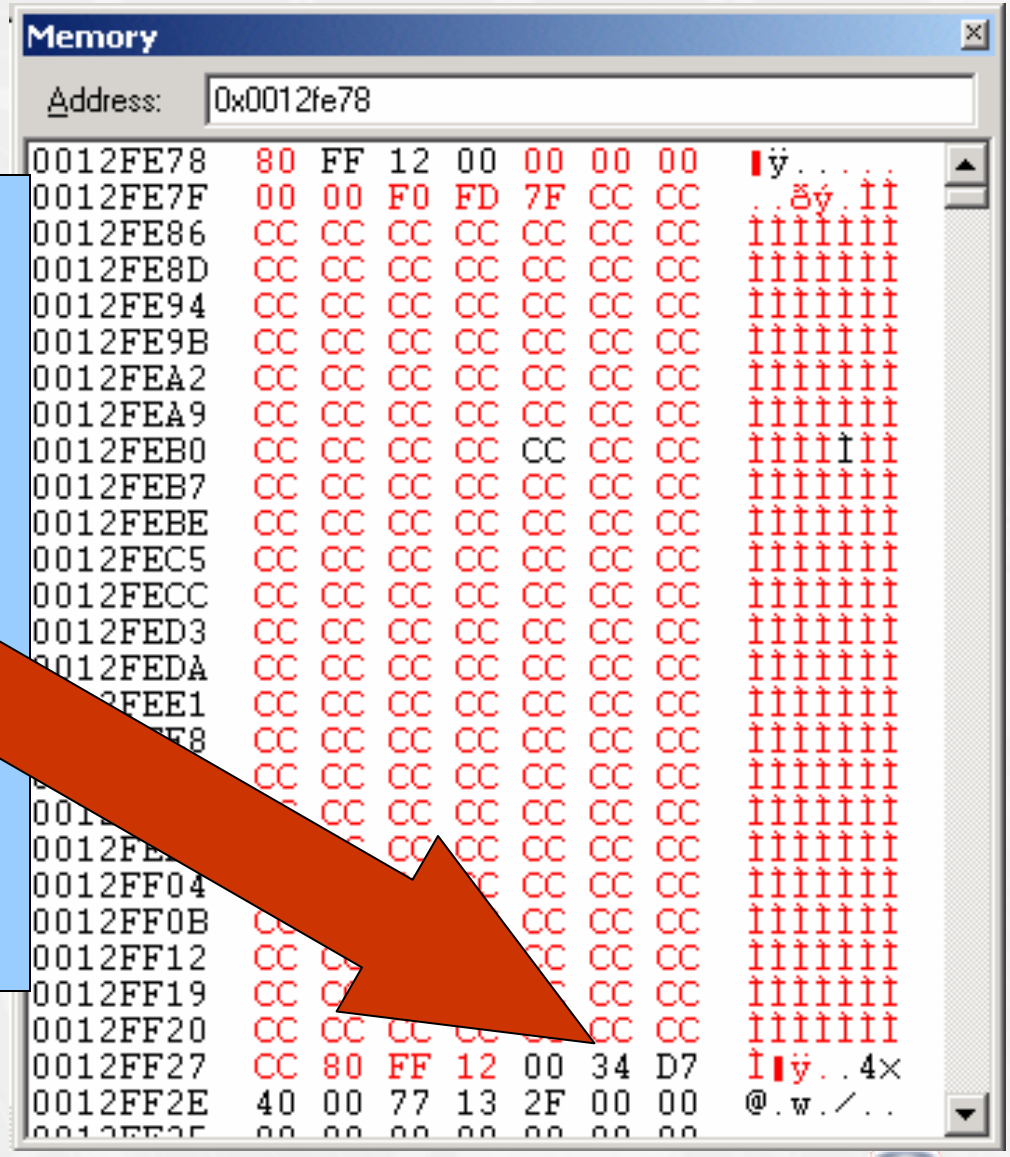


Source:
Entercept 2002

- Buffer Overflow: démonstration

Note the valid return address bytes:

34 D7 40 00

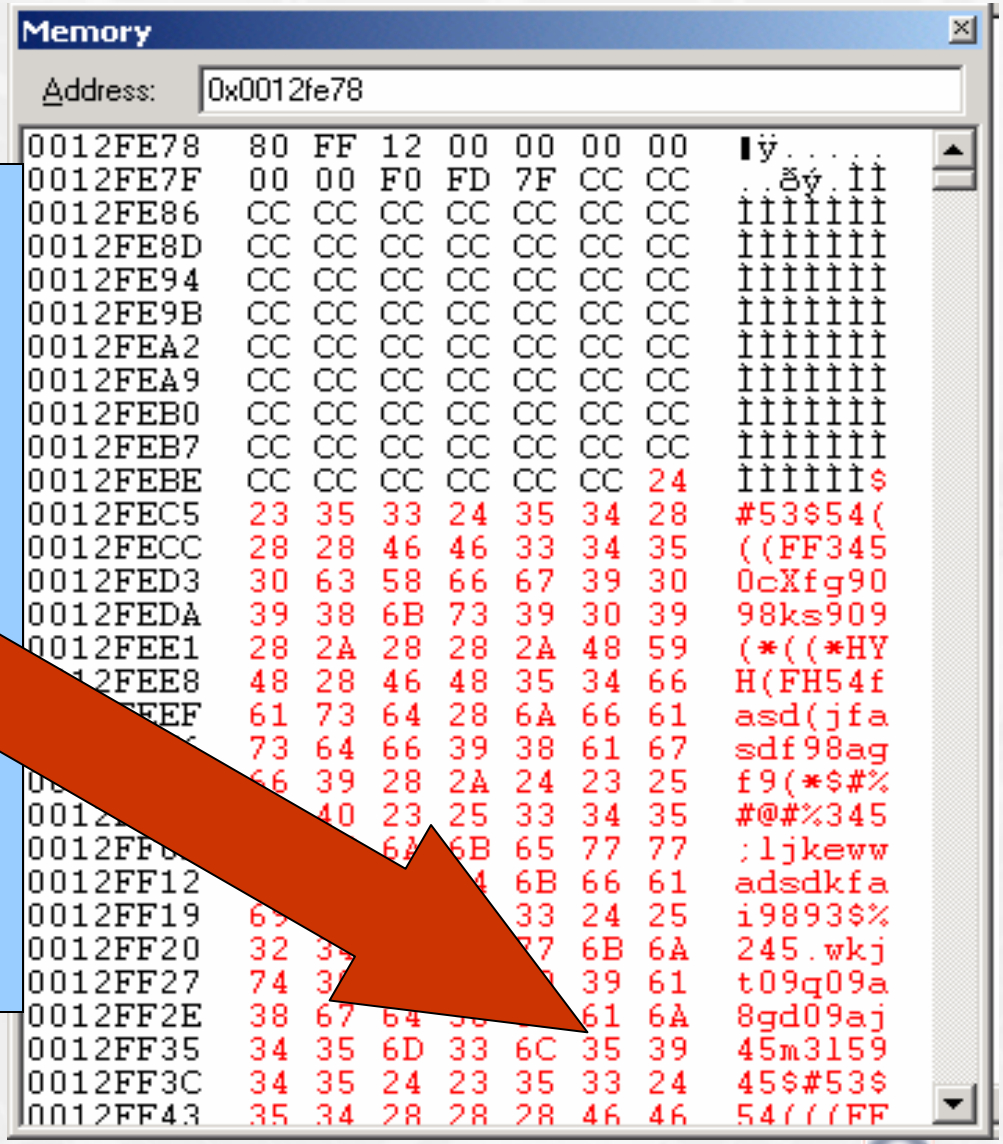


Source:
Entercept 2002

- Buffer Overflow: démonstration

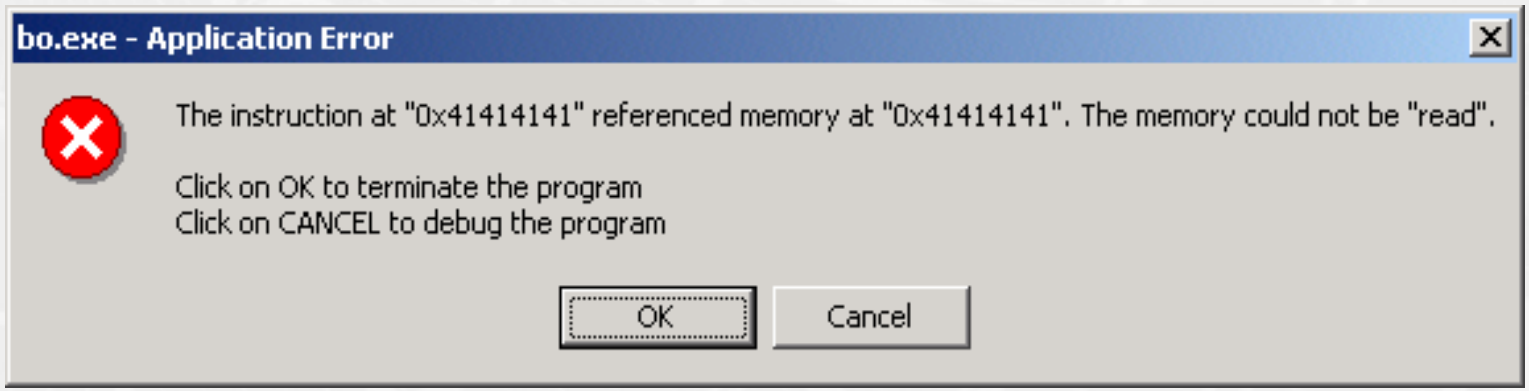
When strcpy() is called, the malicious data is copied into the buffer and overflows it, overwriting the return address.

The bytes of the return address are now 35 39 34 35.



Source:
Entercept 2002

- Buffer Overflow: démonstration



Ou
exécution d'un code hostile

Source:
Entercept 2002

Buffer Overflow: How to be Root !

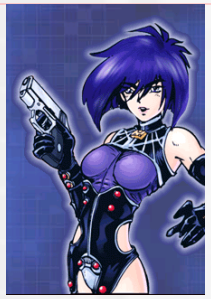
```
#include <stdio.h>
#include <string.h>

char shellcode[] =
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
    "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

char large_string[128];


    int main(int argc, char **argv){
        char buffer[96];
        int i;
        long *long_ptr = (long *) large_string;


        for (i = 0; i < 32; i++)
            *(long_ptr + i) = (int) buffer;
        for (i = 0; i < (int) strlen(shellcode); i++)
            large_string[i] = shellcode[i];
        strcpy(buffer, large_string);
        return 0;
    }
```

Code hostile

```
alfred@atlantis:~$ whoami
alfred
alfred@atlantis:~$ ./a.out
sh-2.05$ whoami
root
```

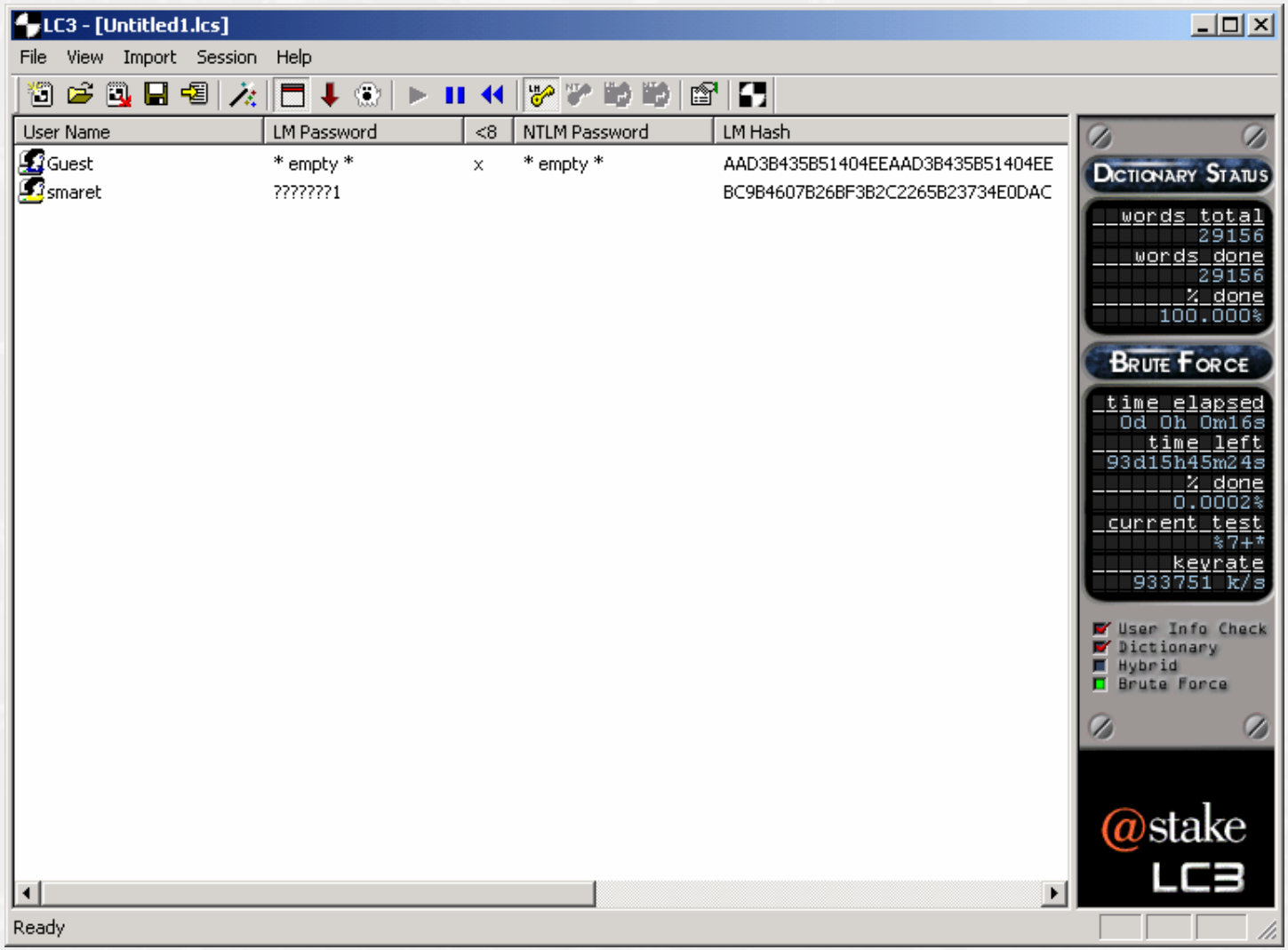
- Les approches
  - Attaque par dictionnaire
    - Basée sur des fichiers de mots de passe
    - Fichiers générique
    - Fichiers thématiques
  - Attaque par « brute force »
    - Essai de toutes les combinaisons
  - Attaque hybride
    - Dictionnaire et « brute force »

Découverte des mots de passe: techniques



- Obtention du fichier des mots de passe
  - /etc/passwd - /etc/shadows (Unix)
  - Fichier Sam Microsoft (Syskey)
  - Etc.
- Capture à l'aide d'un renifleur
  - Microsoft NT 4.0 (NTLM), Win 2000/2003/XP (Kerberos)
  - Telnet, FTP, ldap, etc.
- Attaques par connexion
  - Serveur Telnet, FTP, POP3, HTTP, etc
  - Routeurs, Switchs, Appliance
  - Main Frame
  - ERP
  - Etc.

- Exemple de recherche de mots de passe



- Exemple avec Windows 2000 (Kerberos)

```
C:\usr\local\bin>kerbsniff result.txt

KerbSniff 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Captured packets: **
```

```
C:\usr\local\bin>more result.txt
smaret
E-XPERT
BEAA2B56DED84A6B90A97950ECE335E5DAF94298818D1CF418E1A4E78927BF9AB4882FE2D09F56588B4DAA628843098274 2CF0B8
#
smaret
E-XPERT
BEAA2B56DED84A6B90A97950ECE335E5DAF94298818D1CF418E1A4E78927BF9AB4882FE2D09F56588B4DAA628843098274 2CF0B8
#

C:\usr\local\bin>
```

- Exemple avec Windows 2000 (Kerberos)

```
Usage: kerbcrack <capture file> <crack mode> [dictionary file] [password size]

        crack modes:

        -b1 = brute force attack with (a-z, A-Z)
        -b2 = brute force attack with (a-z, A-Z, 0-9)
        -b3 = brute force attack with (a-z, A-Z, 0-9, special characters)
        -b4 = b1 + swedish letters
        -b5 = b2 + swedish letters
        -b6 = b3 + swedish letters
        -d  = dictionary attack with specified dictionary file

C:\usr\local\bin>kerbcrack result.txt -b2 8

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/


Loaded capture file.

Currently working on:

 Account name     - smaret
 From domain      - E-XPERT
 Trying password - szBa

Number of cracked passwords this far: 0
```

Les renifleurs (Sniffer)

- Outils de capture du trafic réseau
  - Utilisent la carte réseau en mode « promiscuous »
- Les « Black Hat » les utilisent pour:
  - Examiner le traffic entre plusieurs machines
  - Capturer les mots de passe
  - Examiner les emails
  - Etc.
- La plupart des applications sont en « claires »
  - Telnet, FTP, POP3, ldap, http, rlogin, etc.
- Un renifleur est pratiquement indétectable !

- Exemple de sniffer Unix: dsniff

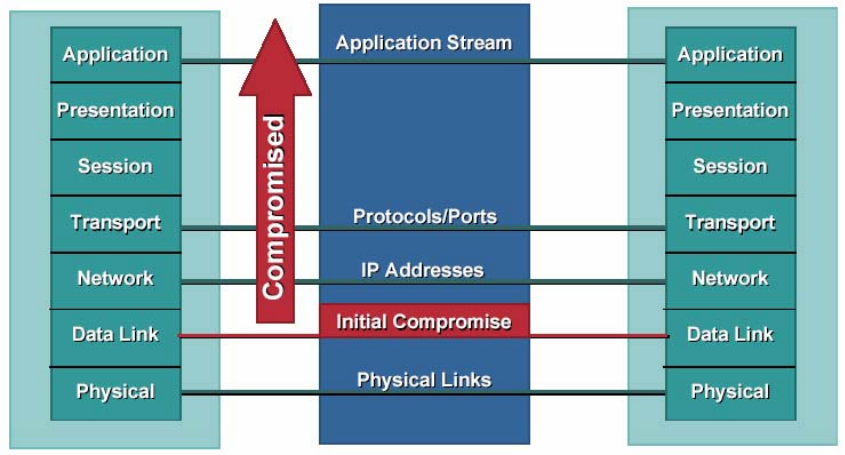
```
[root@attack-lnx dsniff-2.3]# ./dsniff -c
dsniff: listening on eth0
-----------------
07/17/01 10:09:48 tcp 10.1.1.26.1126 -> wwwin-abc.cisco.com.80 (http)
GET /SERVICE/Paging/page/ HTTP/1.1
Host: wwwin-abc.cisco.com
Authorization: Basic c2NvdlghV9UNMRH4lejDmaA== [myuser:mypassword]
```

Supports More than 30 Standardized/Proprietary Protocols:

FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL

- Les renifleurs (Sniffer): environnements « Switché »

- Il est possible de renifler dans un environnement switché
- Techniques utilisées
  - MAC Attacks
  - ARP Attacks
  - Etc.

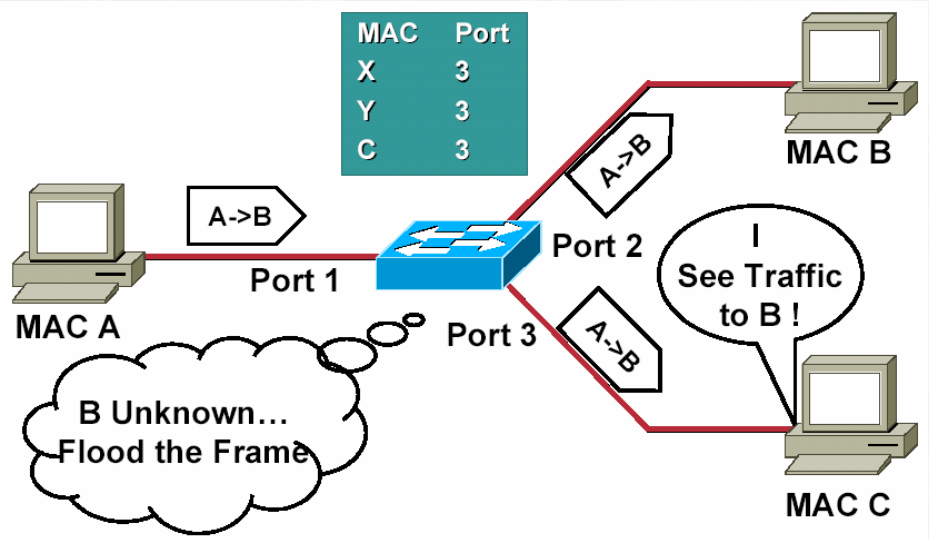


Source: Cisco 2002

- MAC Attacks

```
[root@attack-lnx dsniff-2.3]# ./macof
b5:cf:65:4b:d5:59 2c:01:12:7d:bd:36 0.0.0.0.4707 > 0.0.0.0.28005: S 106321318:106321318(0) win
68:2a:55:6c:1c:1c bb:33:bb:4d:c2:db 0.0.0.0.44367 > 0.0.0.0.60982: S 480589777:480589777(0) wi
1e:95:26:5e:ab:4f d7:80:6f:2e:aa:89 0.0.0.0.42809 > 0.0.0.0.39934: S 1814866876:1814866876(0)
51:b5:4a:7a:03:b3 70:a9:c3:24:db:2d 0.0.0.0.41274 > 0.0.0.0.31780: S 527694740:527694740(0) wi
51:75:2e:22:c6:31 91:a1:c1:77:f6:18 0.0.0.0.36396 > 0.0.0.0.15064: S 1297621419:1297621419(0)
7b:fc:69:5b:47:e2 e7:65:66:4c:2b:87 0.0.0.0.45053 > 0.0.0.0.4908: S 976491935:976491935(0) win
19:14:72:73:6f:ff 8d:ba:5c:40:be:d5 0.0.0.0.867 > 0.0.0.0.20101: S 287657898:287657898(0) win
```

- MAC Flooding
  - Corruption des tables CAM
  - Agit comme un HUB
  - Utilisation d'un sniffer
- Outils disponible sur Internet !
  - macof

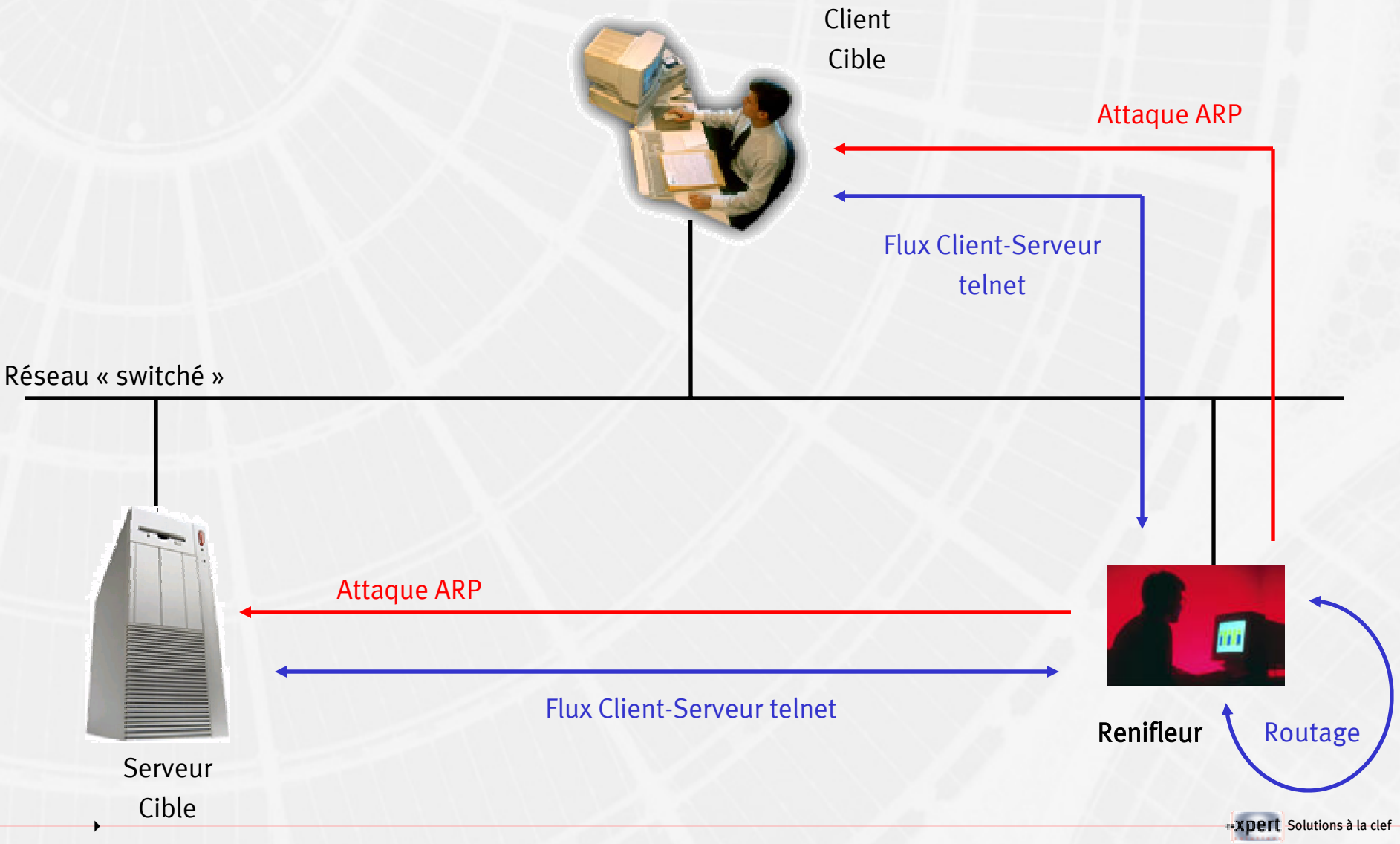


Source: Cisco 2002

ARP attack: ARP Spoofing

- Corruption des tables ARP à l'aide d'outils
- ARP n'offre pas de mécanisme de sécurité !
- Méthode très simple
- Outils les plus connus
  - Dsniff by Dug Song
  - Ettercap
  - Hunt
  - Arp-sk
  - Etc.

- Renifleur dans un environement « switché »



Détournement de session: Hijacking

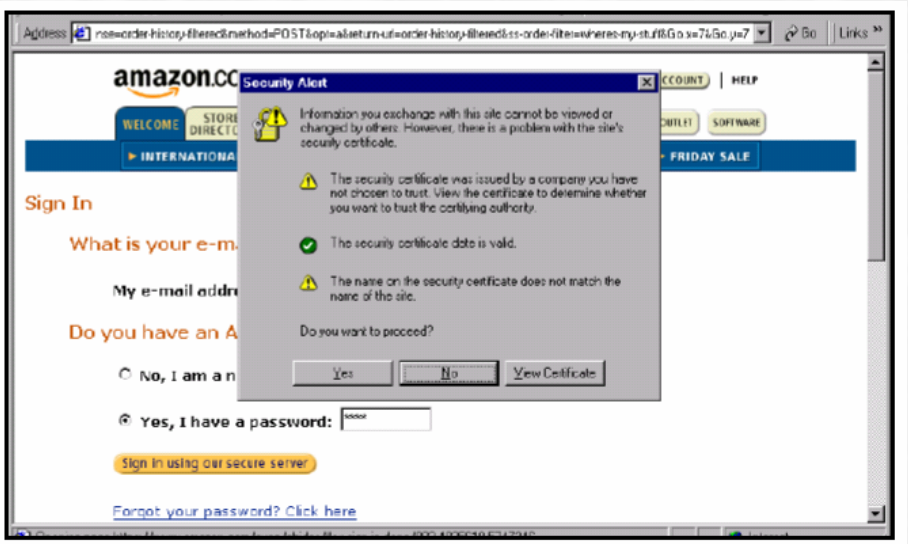
Man in the Midle

SSH, Telnet, SSL, etc.

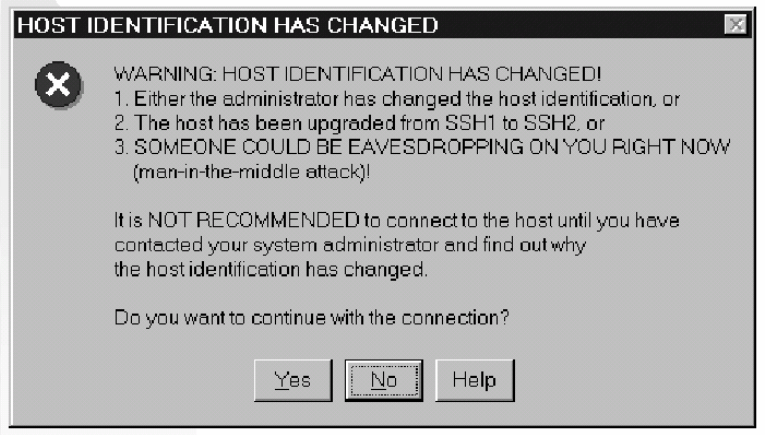
Serveur
Cible

Client
Cible

- Détournement de session: protocoles sécurisés



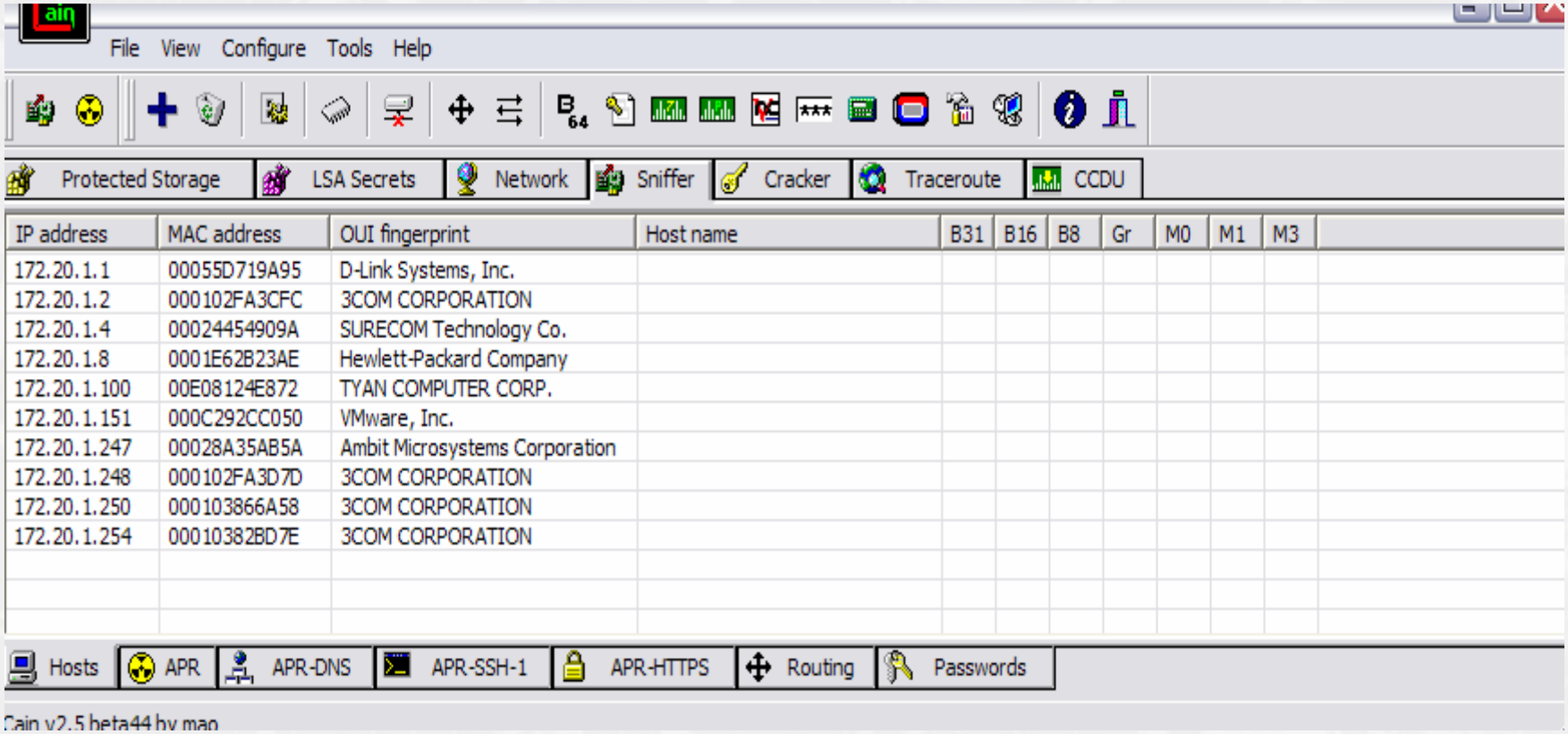
Session SSL



Session SSH

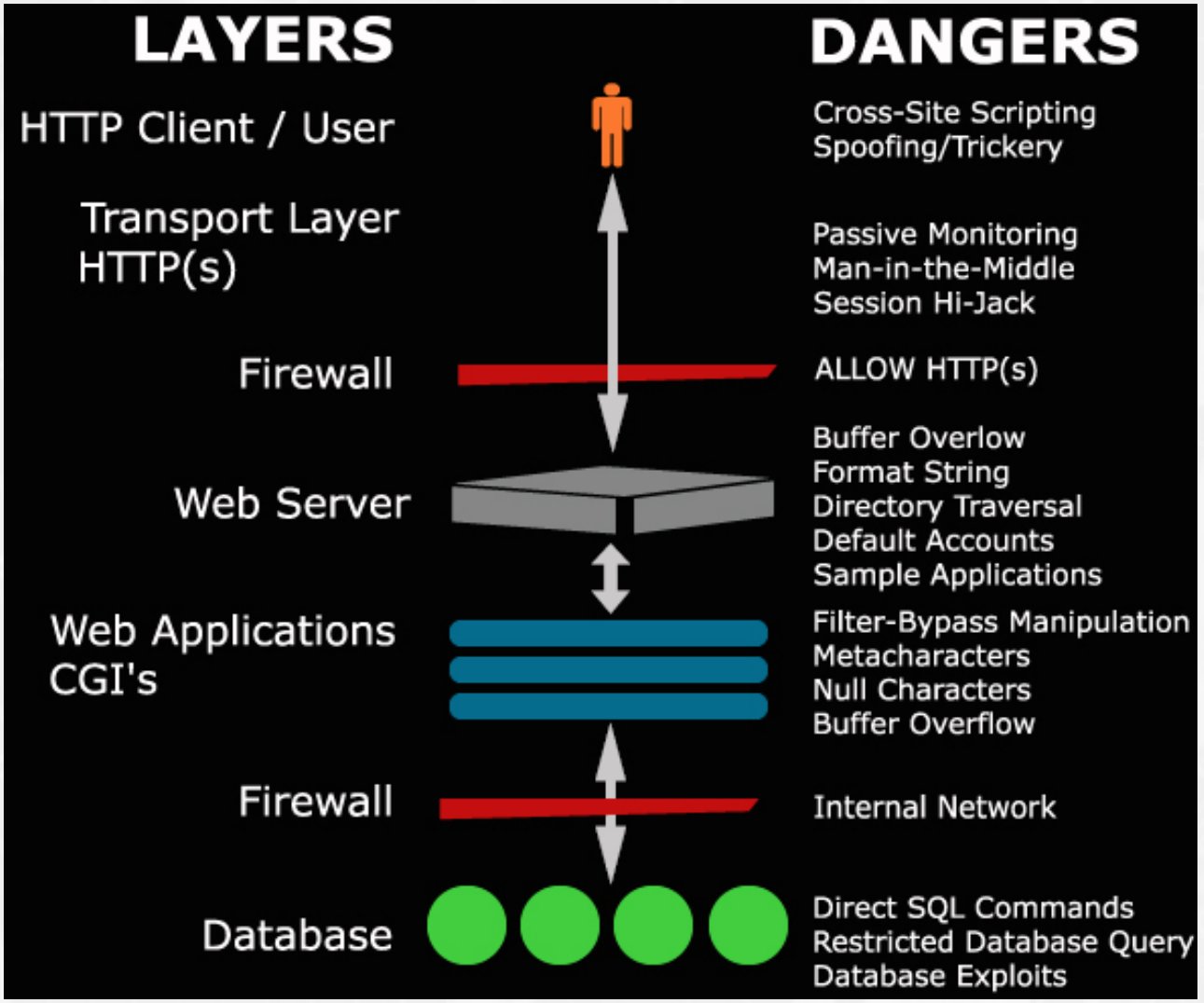
Attention, ces messages ne sont pas anodins !

- Cain: Free Tool



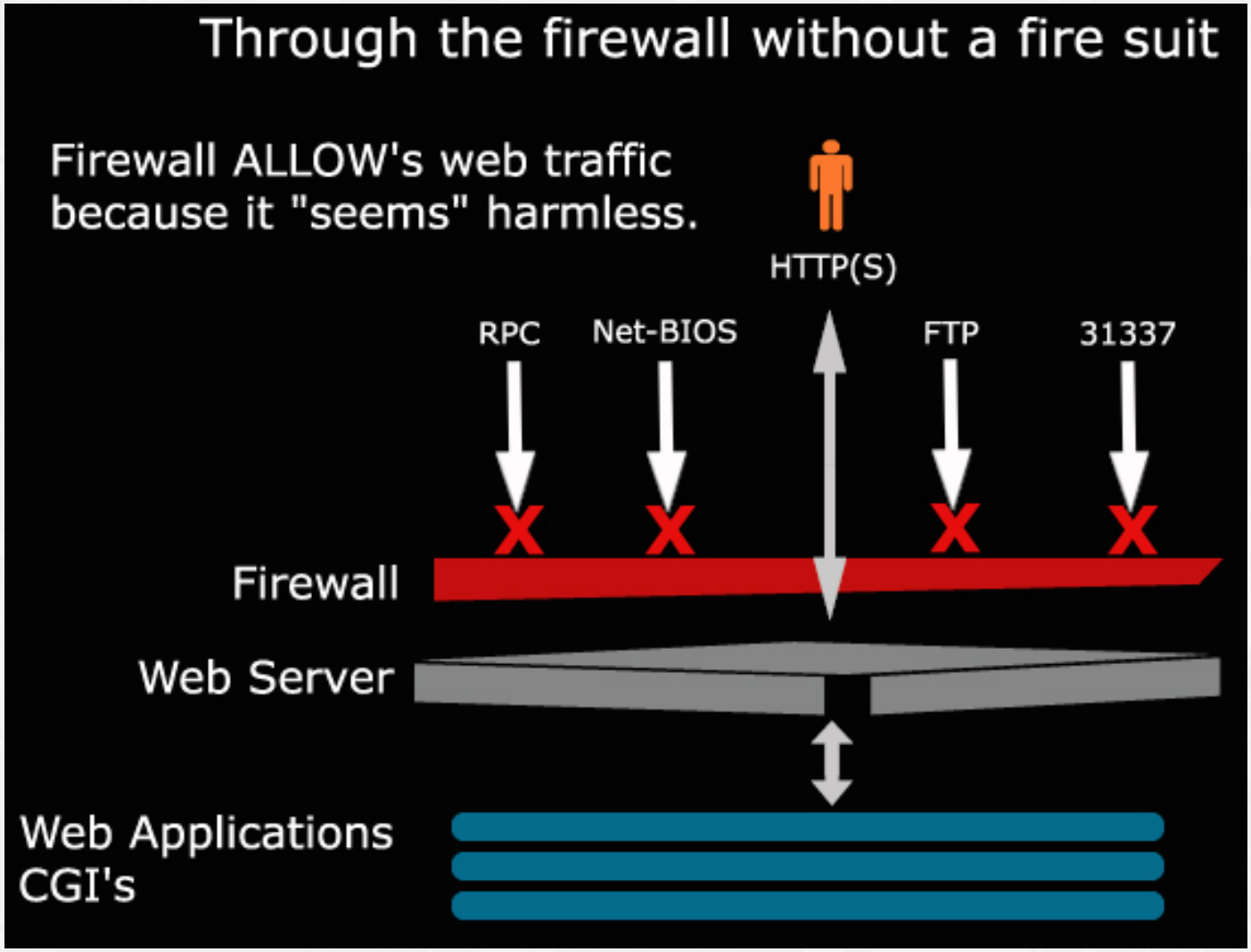
- Application Web: application sofware qui est accessible à l'aide un navigateur en utilisant http et/ou https (ou un « user agent »
  - Si le service est TCP 80 ou TCP 443, il s'agit probablement d'une application Web
- Application très sensible
  - Mauvaise configuration
  - Vulnérabilité
  - Bugs
  - Etc.
- Nouvelle cible des "Black Hat" !

- Application Web: architecture



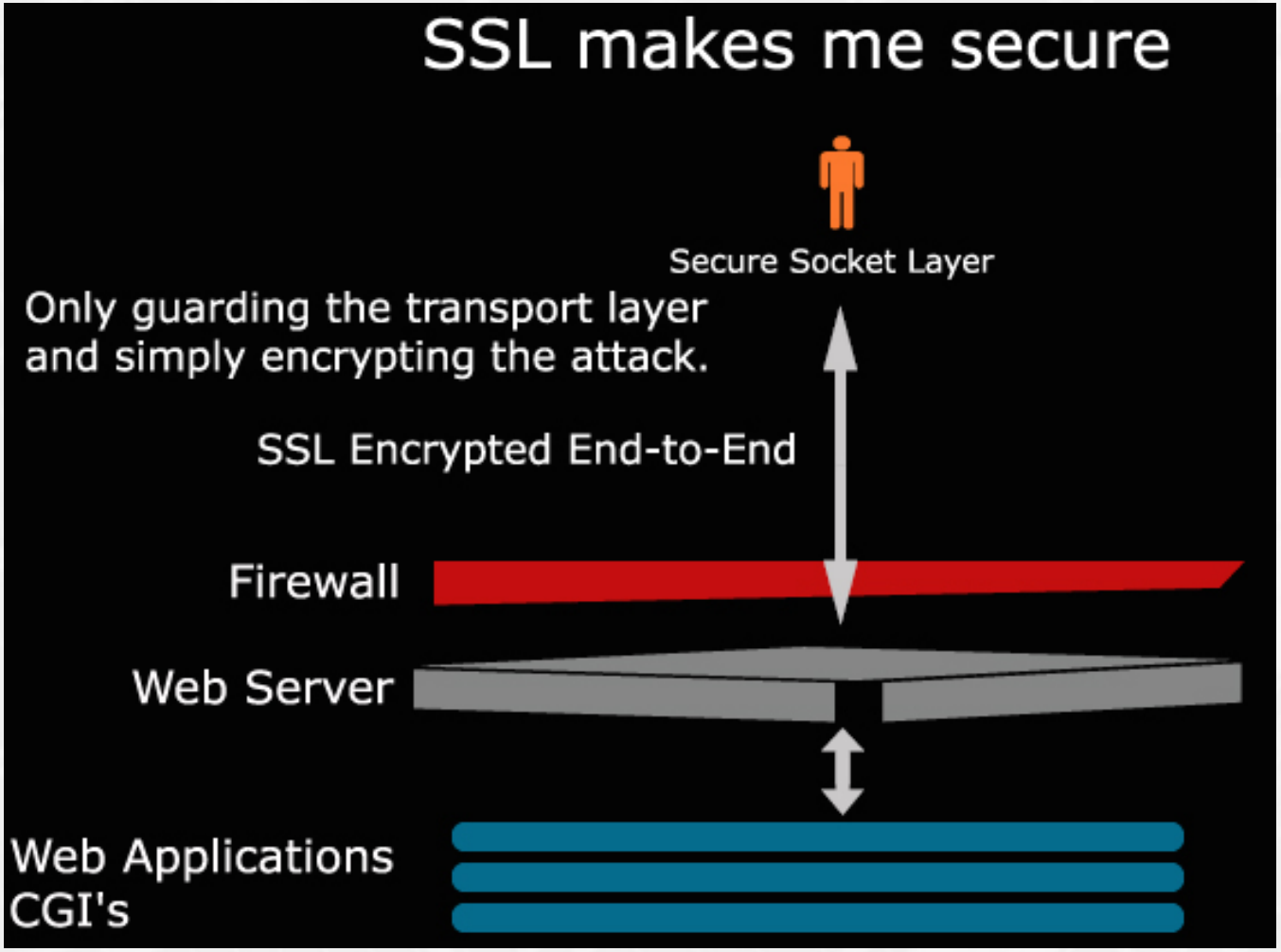
Source:
WhiteHat Security
2002

- Application Web: la futilité du firewall



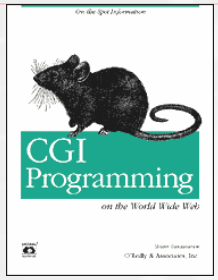
Source:
WhiteHat Security
2002

- Application Web: SSL sécurise mon site Web



Source:
WhiteHat Security
2002

Application Web: les principales attaques



- Vulnérabilités des serveurs Web
  - IIS, Apache, I-Planet, etc.
- Exécution de programme
- Buffer Overflow
- Back Door
- Escalade de privilèges
- SQL
- Cross Site Scripting
- Défiguration (Defacement)
- Etc.

- Projet « Open Web Application Security Project (OWASP) »

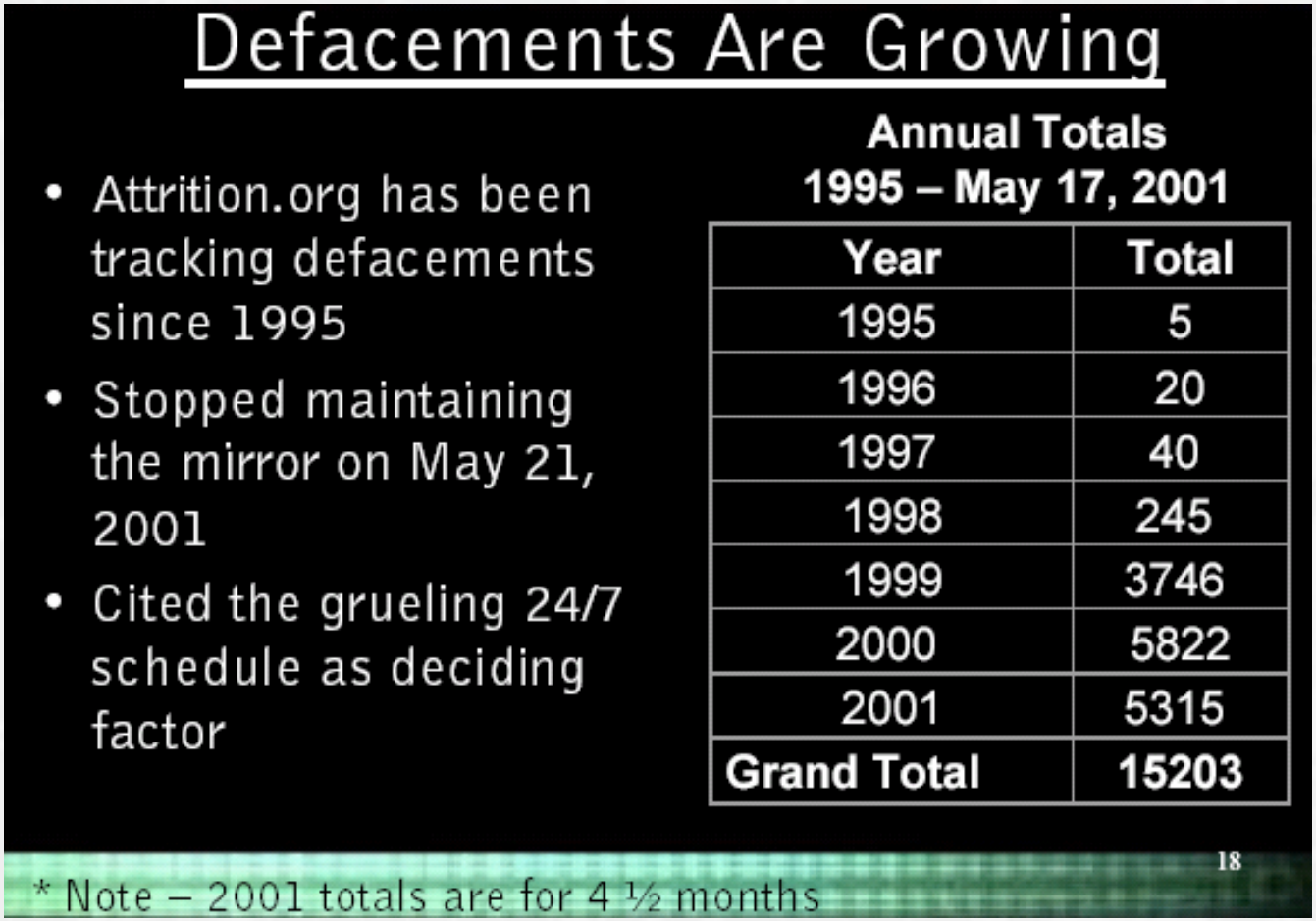
- http://www.owasp.org
  - Publication top 10 des vulnérabilités

- Defacement ou graffiti Web

- Application Web: défiguration

- Définition: changement des pages Web
- Applications Web sont des cibles très visibles
- Les "Black Hat" utilisent ces ressources pour:
  - Revendications
  - Fun
  - Vengeance
  - Etc.
- Partie visible de l'iceberg
- En pleine croissance…
  - http://www.attrition.org
  - http://www.zone-h.org/en/defacements

- Defacements: évolution dans le temps



- Exemple de défiguration politique: « Egyptian Fighter »

Source:
www.alldas.org
Août 2002

- Changement des pages « Web »
  - FTP
  - Compromission du serveur
  - Etc.
- DNS redirection ou « poisoning »
- Piratage de domaine
- Corruption des « proxy caches »
- Etc.

- Microsoft IIS

- Beaucoup de failles de sécurité
  - Top One (CERT)
  - 60% des défigurations
- Année 2001
  - ISAPI Buffer overflow (exécution de commande)
    - Code Red
  - IIS Directory Traversal (Unicode)
    - « HTTP Request » malformées
    - Installation backdoor, voir les fichiers, etc.
  - « Sample Code »
- Code Red et Nimda
  - 13 Juillet 2001 et 18 septembre 2001

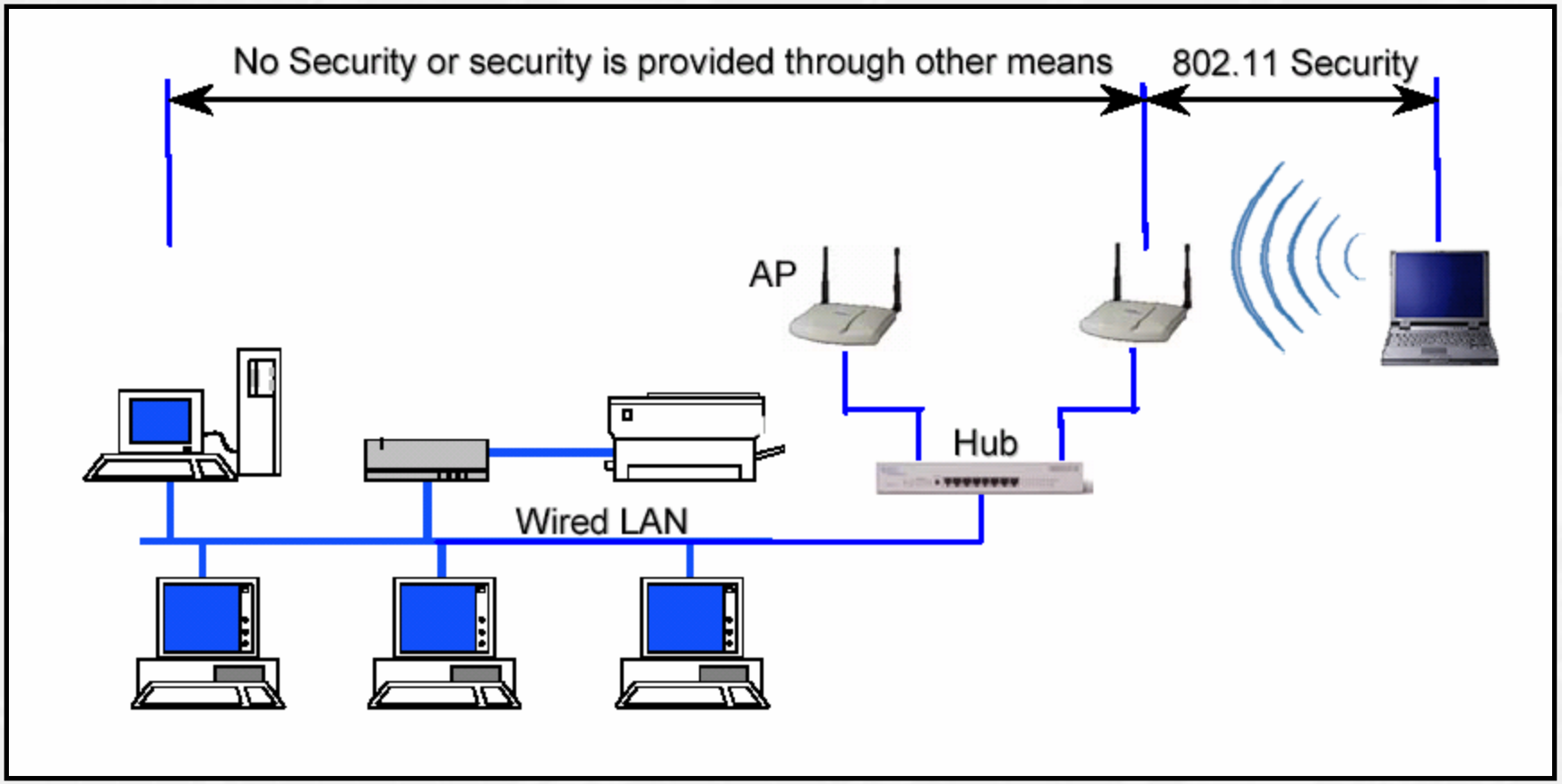
- Microsoft IIS

- Octobre 2001: Gartner Group recommande de trouver une alternative à IIS…
- Microsoft promet une nouvelle version IIS ?

W1.3 CVE Entries
CVE-2001-0241, CVE-2001-0333, CVE-2001-0500, CAN-2002-0079, CVE-2000-0884, CVE-2000-0886, CAN-2002-0071, CAN-2002-0147, CAN-2002-0150, CAN-2002-0364, CAN-2002-0149, CVE-1999-0191, CAN-1999-0509, CVE-1999-0237, CVE-1999-0264, CVE-2001-0151, CAN-1999-0736, CVE-1999-0278, CAN-2002-0073, CVE-2000-0778, CVE-1999-0874, CVE-2000-0226, CAN-1999-1376, CVE-2000-0770, CVE-2001-0507

- Grande popularité du réseau sans fils
  - Coûts abordables
  - Confort d'utilisation
- La contre partie
  - Gros problèmes de sécurité
- Concerne les protocoles 802.11x (a, b et g)
- 802.11x défini une couche de protection:
  - WEP = Wired Equivalent Privacy
  - Encryption rc4
  - Intégrité avec un CRC32

- Réseaux Wireless: l'architecture classique

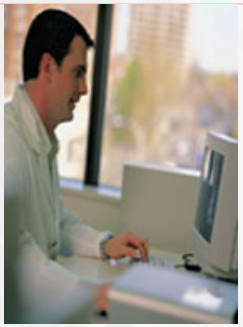


Source:
NIST 2002

Réseaux Wireless: le problème

- Environ 70% des entreprise n'utilisent pas le WEP
  - « Complexité »
  - Performance
- WEP est très vulnérable
  - Difficultés d'implémentation
  - Possible de « cracker » les clés en peu de temps
- Rayonnement très important
  - Possibilité de se connecter à distance (dans la rue par exemple)

Réseaux Wireless: les attaques et les outils



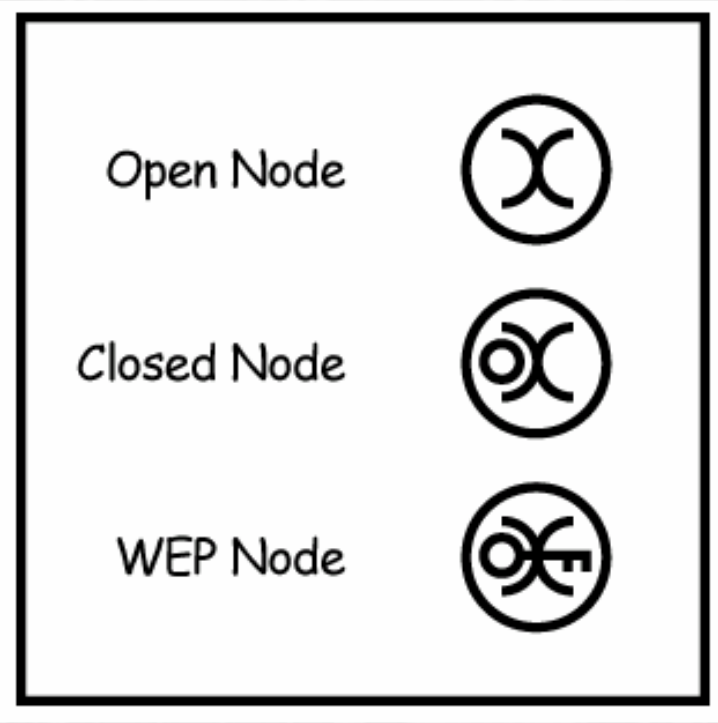
- Attaques passives
  - Ecoute du trafic à distance (crypté ou pas)
- Attaques actives
  - Usurpation d'une station
  - Vol de session
  - Modification de trafic
  - DoS
  - Etc.
- Les outils
  - Un scanner 802.11x
  - Un logiciel de Crackage WEP
  - Un renifleur
  - Etc.

- Réseaux Wireless: le Warchalking

Pringles tube works as an antenna

- Interception des réseaux Wireless depuis la rue
- Marquage des sites à l'aide de symbole
- Partage de l'information sur les sites Internet
  - Coordonées GPS
- Etc.

- Réseaux Wireless: le Warchalking et ces symboles de base



Compilation: CD Linux

Auditor security collection - toollist

Here you can find a list of tools included in the Auditor security collection CD-ROM.
The toollist is not complete yet, but most of them are on this list allready.

The 1 in the column "X11" and "In Menu" means "Yes" a 0 means '

Category	Name	Version	X11	License	In Menu	Description
footprinting	greenwich	0.5.2	1	GPL	1	Whois client
footprinting	gnetutil	1.0-Auditor	1	GPL	1	Networking toolset
footprinting	host	991529	0	GPL	0	Nameresolution
footprinting	dig	9.2.3	0	GPL	0	Nameresolution
footprinting	traceroute	1.4a12	0	GPL	1	Packet traceing
footprinting	itrace	Unknown	0	Phenoelit	1	Packet traceing
footprinting	tctrace	Unknown	0	Phenoelit	1	Packet traceing
footprinting	tkmib	Unknown	1	GPL	1	SNMP tool
footprinting	snmpwalk	5.1	0	GPL	1	SNMP tool
footprinting	LinNeighborhood	0.6.5	1	GPL	1	Netbios browser
footprinting	Xsmbrowser	3.4.0	1	GPL	1	Netbios browser
footprinting	Net utils	3.0.2	0	GPL	1	Netbios tools
footprinting	smbdumpusers	0.9.1	0	GPL	1	Netbios tools
footprinting	smbgetserverinfo	0.9.1	0	GPL	1	Netbios tools
footprinting	nmblookup	Unknown	0	GPL	0	Netbios lookup
footprinting	Nmapfe	3.5.0	1	GPL	1	Network scanner
footprinting	Xprobe2	0.2rc1	0	GPL	1	Fingerprint scanner
footprinting	Cheops	0.61	1	GPL	1	Network scanner
footprinting	p0f	2.0.2	0	GPL	1	Fingerprint scanner
footprinting	queso	Unknown	0	GPL	1	Fingerprint scanner
footprinting	curl	7.11	0	GPL	1	Scriptable Webbrowser

- Links

- http://citadelle.intrinsec.com/
- http://www.net-security.org/
- http://packetstormsecurity.org/
- http://www.securiteam.com/
- http://www.securitynewsportal.com/index.shtml
- http://securitytracker.com/
- http://www.k-otik.com/bugtraq/
- http://www.cert.org
- http://www.sans.org

- Questions ?

e-Xpert Solutions S.A. est une société Suisse de services spécialisée en sécurité informatique dont les fondateurs ont fait de leur passion leur métier :

La sécurité des systèmes d'information

Fort de leurs convictions et de leur expérience, nos ingénieurs conçoivent, déploient et maintiennent au quotidien des architectures de sécurité au moyen de solutions pragmatiques, basées sur des technologies fondamentales et novatrices, adaptées aux exigences de la clientèle.

Cette approche, associée à des collaborateurs motivés, flexibles et au bénéfice d'une intégrité irréprochable, nous a permis d'assurer une croissance continue et de gagner la confiance d'une clientèle issue de tout domaine d'activité et de toute taille.

Notre siège à Bernex/Genève et notre agence de Morges/Lausanne vous garantissent un contact de proximité.

http://www.e-xpertsolutions.com