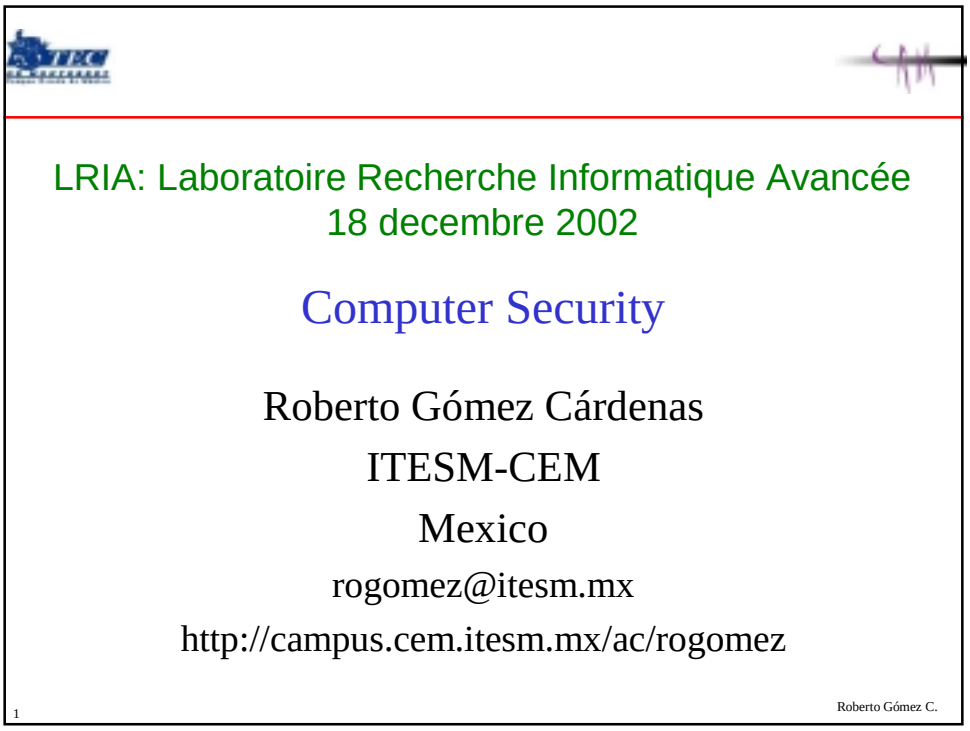
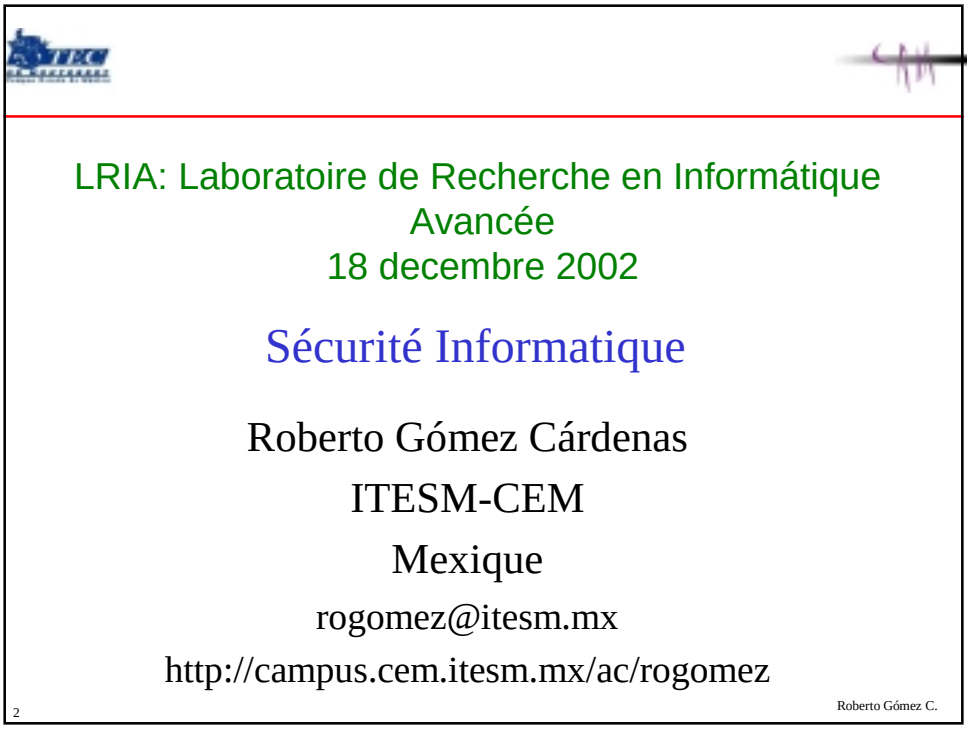


LRIA: Laboratoire Recherche Informatique Avancée
18 decembre 2002

Computer Security

Roberto Gómez Cárdenas
ITESM-CEM
Mexico
rogomez@itesm.mx
http://campus.cem.itesm.mx/ac/rogomez

1 Roberto Gómez C.



LRIA: Laboratoire de Recherche en Informátique Avancée
18 decembre 2002

Sécurité Informatique

Roberto Gómez Cárdenas
ITESM-CEM
Mexique
rogomez@itesm.mx
http://campus.cem.itesm.mx/ac/rogomez

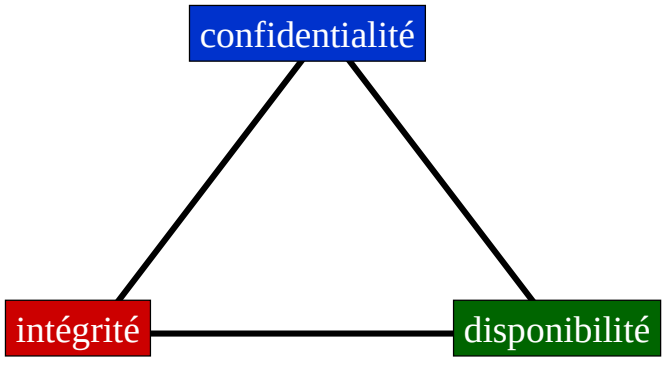
2 Roberto Gómez C.

Sécurité Informatique

Ensemble de politiques et mécanismes que perment garantizer la confidentialité, l'intégrité et la disponibilité des resources d'un système

3 Roberto Gómez C.

Le triangle de la sécurité



4 Roberto Gómez C.

Les champs d'application

- la sécurité physique
- la sécurité personnelle
- la sécurité procédurale (audits de sécurité, procédures informatiques...)
- la sécurité des émissions physiques (écrans, cables d'alimentation, courbes de consommation de courant...)
- la sécurité des systèmes d'exploitation
- la sécurité des communications

5 Roberto Gómez C.

Les attaques

- Des actions qui ont pout but arreter le functionnament d'un système informatique,
- Ceci inclus la destruction, modification ou retard dans le service donné par le systeme.
- Il ne s'agit pas d'un ataque physique
- Il ne se fait pas dans un seul pas, il est composé des differents etapes, selon le but de l'intrus

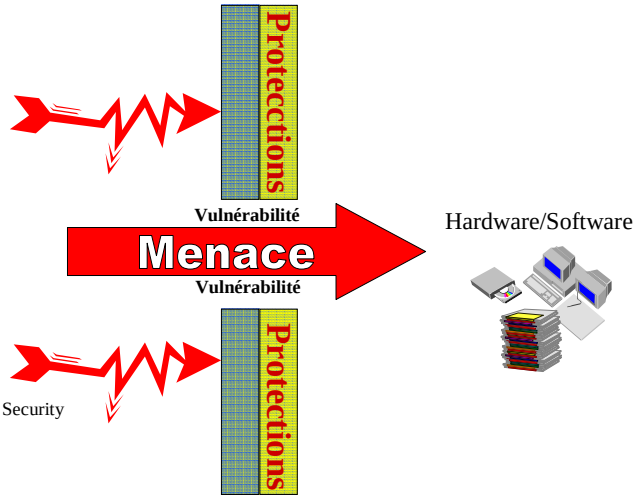
6 Roberto Gómez C.

Menace, vulnerabilité et risques

- Menace
  - est l'action qui pourrait nuire à autrui
  - la menace se veut generique
- Vulnérabilité
  - es le reactif qui permet a la menace de s'exécuter
  - sa présence dépend du contexte étudié
- Risque
  - est l'évaluation de la propabilité d'exécution d'une menace dans un environnement donné, de la faisabilité et de son impact potentiel sur cet environnement
  - sur base de ces évaluations, la décision sera prise quant à l'acceptation ou a l'applicabilité du risque

7 Roberto Gómez C.

Vulnerabité vs menace



Source:
An Introduction to Computer Security
The NIST Handbook
NIST- Serial
Publication 800-12

8 Roberto Gómez C.

L'exploit

- C'est l'utilisation d'une faille, d'un bug, d'une faiblesse ou d'un trou sur un systeme d'exploitation qui peut resulter en un crash, plantage, acces arbitraire ou acces total
- La definition de MadChat c'est qu'un exploit est un acte extraordinaire effectue avec ses simples connaissances en informatique et ayant pour but de trouver une nouvelle facon de penetrer un systeme

9 Roberto Gómez C.

Vulnerabilités, menaces et exploits

- Codes maliciousus
- Le cheval de troie
- Les vers
- Bugs
- Trapdoors
- Stack overflow
- Bombe Logique
- Sniffers
- Spoofing
- Spam
- Ingénierie sociale
- Negación de servicio
- Grafiti

10 Roberto Gómez C.

Le confinement

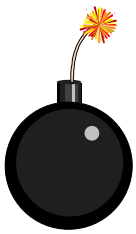
- Le programme ne manipule pas de données de l'utilisateur mais simplement enregistre ses paramètres d'appels (les utilisateurs à qui vous envoyez du courrier par exemple).
  - le problème du confinement est donc de vous protéger contre ce type d'extraction d'informations.
- Exemples
  - cookies
  - codes maliciousus (java applets, etc)

11 Roberto Gómez C.

La bombe logique

- C'est un programme ou une altération d'un programme original qui va se déclencher de manière différée.

```
IF ( professeur == bui ) THEN
   salaire = heures * poste * 1.1
ELSE
    salaire = heures * poste
```



12 Roberto Gómez C.

Le cheval de Troie

- C’est un programme permettant de profiter des droits donnés par l’utilisateur pour consulter, copier, modifier ou altérer des données auxquelles il n’est pas censé accéder

13 Roberto Gómez C.

Les virus

- Suite d’instructions introduite dans un programme de manière à réaliser, en plus des actions néfastes précédentes, une fonction de
- reproduction dans d’autres objets du système de manière à rendre l’éradication la plus difficile possible.

14 Roberto Gómez C.

Le Vers

- Il est similaire au virus
- Sa fonction de reproduction est capable de se propager à travers les réseaux auxquels la machine est connectée.
  - comme par exemple I love You par la messagerie électronique.

15

Hoax

- Le terme énigmatique provient du langage courant et signifie canular.
- A titre d'exemple, les anglophones diront: "hoax bomb" pour une fausse alerte à la bombe
- Fausses alertes aux virus; fausses chaînes de solidarité; fausses promesses; fausses informations; les hoax prennent toutes les formes.

16 Roberto Gómez C.

1er. exemple hoax

Bonjour,
Ralentis ton rythme !
As-tu deja observe les enfants jouer sur un caroussel ou ecouter la pluie tomber sur le toit ? Deja suivi un papillon volant gaiement ou bien admire un coucherdesoleil ? Tu devrais t'y arreter. Ne danse pas trop vite car la vie est courte. La musique ne dure pas eternellement. Est-ce que tu cours toute la journee, toujours presse? Lorsque tu demandes " Comment ca va ? ", est-ce que tu prends le temps d'ecouter la reponse ? Lorsque la journee est terminee, est-ce que tu t'etends dans ton lit avec 10'000 choses a faire qui courent dans ta tete ? Tu devrais ralentir, as-tu deja dit a ton enfant :
La Societe Americaine contre le cancer fera don
de 3 sous pour son traitement et son plan de rehabilitation.
Quelqu'un a envoye cette lettre a 500 personnes!!! Je sais que nous pouvons l'envoyer a au moins 5-6 personnes. Allez, un petit effort..
et si tu es trop egoiste pour prendre 10-15 minutes de ton temps pour passer ce message et l'envoyer a quelques personnes, tu es, toi aussi, une personne malade. Faut juste penser que ca pourrait etre TOI.

17 Roberto Gómez C.

2eme exemple hoax

http://www.hoaxbuster.com/hoaxteam

ATTENTION VIRUS !
La majorité des utilisateurs d'Internet vont être contaminés, si ce n'est déjà fait, par un virus nommé: sulfnbk.exe qui est redoutable car écrasant votre disque dur je viens de le détruire sur mon propre disque dur, il était déjà là.

Procédure: dans menu démarrer: rechercher fichiers ou dossiers et vous saurez si vous l'avez. Dans ce cas, allez le chercher, cliquez une seule fois dessus et supprimer le. Aller ensuite dans corbeille et supprimer le contenu de la corbeille.

Je vous incite très fortement à vérifier si ce virus est déjà sur votre disque dur car il devrait être activé le 25 mai.
Bien à vous.

18 Roberto Gómez C.

Trapdoors

19 Roberto Gómez C.

Les trous de sécurité applicatifs

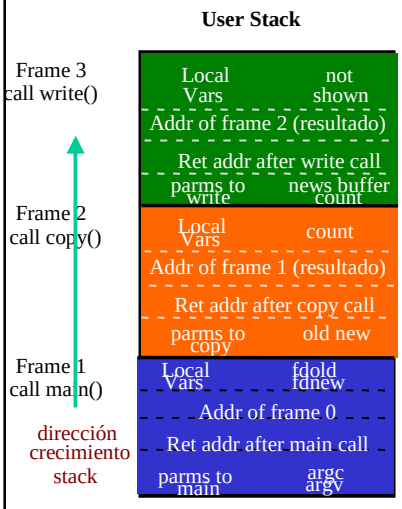
- Il est le résultat d'un fonctionnement anormal d'une application.
  - il en résulte un plantage de l'application, ou bien un état non stable.
  - il s'agit de trouver un fonctionnement que n'a pas prévu le programmeur.
  - il est parfois possible d'en exploiter des failles.
- Cela devient interessant lorsque c'est un programme réseaux (client/serveur, mail, www, architecture distribuée...).
- Ce type d'attaque peut être utilisée en local (pour obtenir l'accès root) ou à distance pour s'introduire dans un réseau, ou planter à distance un serveur.

20 Roberto Gómez C.

Stack ou buffer overflow

- Premiere parution: 1988.
- Details:
  - novembre 1996
  - Phrack Magazine, numero 49
  - www.phrack.org

A quoi sert le stack?




```
copy (int old, int new)
{
      int count;
      while ( (count = read(old, buffer, sizeof(buffer))) > 0 )
        write(new, buffer, count);
}

main(argc, argv)
{
      int fdold, fdnew;
      fdold = open(argv[1], O_RDONLY]);
      fdnew = open(argv[2], 0666);
      copy (fdold, fdnew);
      exit(0);
}
```

Un premier exemple

```
toto@cachafas:1> cat prog1
int main(int argv,char **argc) {
     char buf[25];

     strcpy(buf,argc[1]);
 }
toto@cachafas:2> gcc prog1.c -o prog1
toto@cachafas:3> prog1 'esto es una prueba de un buffer overflow'
????????????????????????????
```

¿¿que pasa si en lugar de strcpy() se usa strncpy()??

23 Roberto Gómez C.

Un deuxieme exemple

```
void function(int a, int b, int c)
{
  char buffer1[5];
  char buffer2[10];
  int *ret;
  ret = buffer1 + 12;
  (*ret) += 8;
}

void main( ) {
  int x;
  x = 0;
  function(1,2,3);
  x = 1;
  printf("%d\n",x);
}
```

```
toto@cachafas:4> gcc prog2.c -o prog2
toto@cachafas:5> prog2
0
toto@cachafas:6>
```

24 Roberto Gómez C.

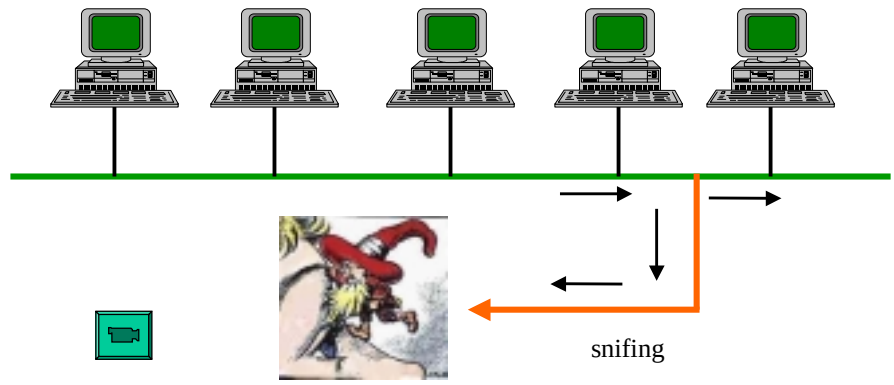
Social Engineering

"Hi Bev, this is Sam from the IS Department. We just got in a new corporate screensaver and since you're the VP's secretary you will get it first. It's really cool wait 'till you see it. All I need is your password so I can log on to your PC from the computer center and install it.

Oh Great!!!!!! My password is rover. I can't wait to see that new screen saver!!!!!"

25 Roberto Gómez C.

Sniffers



26 Roberto Gómez C.

Déni de service

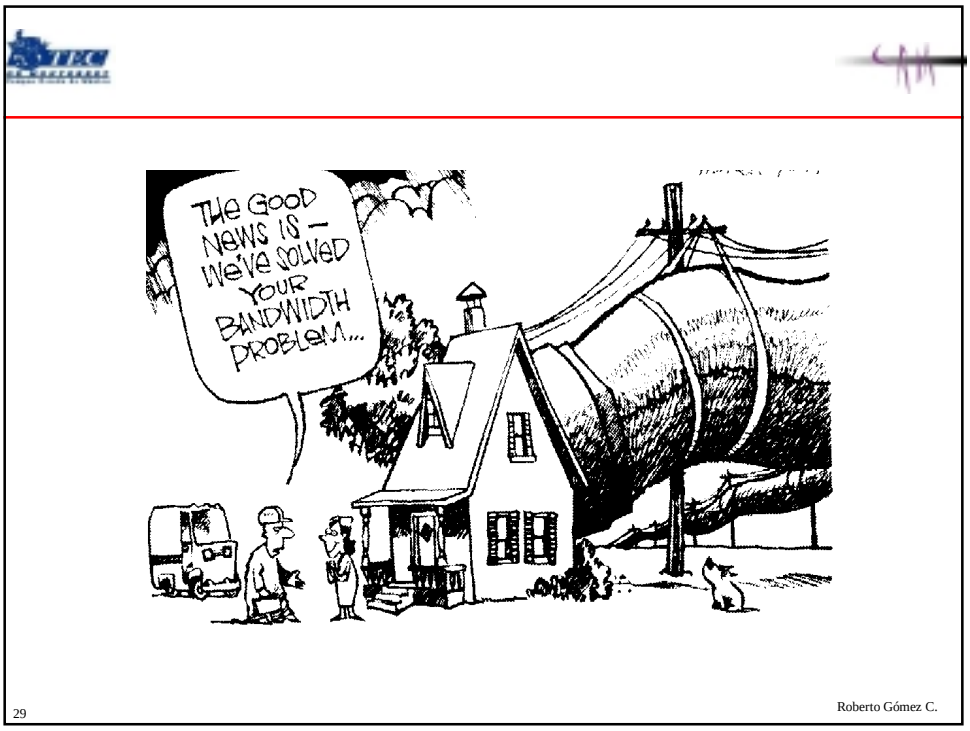
- D'une manière générale, on parle de déni de service quand une personne ou une organisation est privée d'un service utilisant des ressources qu'elle est en droit d'avoir en temps normal
- Il s'agit d'une attaque très évoluée visant à rendre muette une machine en la submergeant de traffic inutile.
- Il peut y avoir plusieurs machines à l'origine de cette attaque (c'est alors une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux, etc.
- D'autre part, elle reste très difficile à contrer ou à éviter.

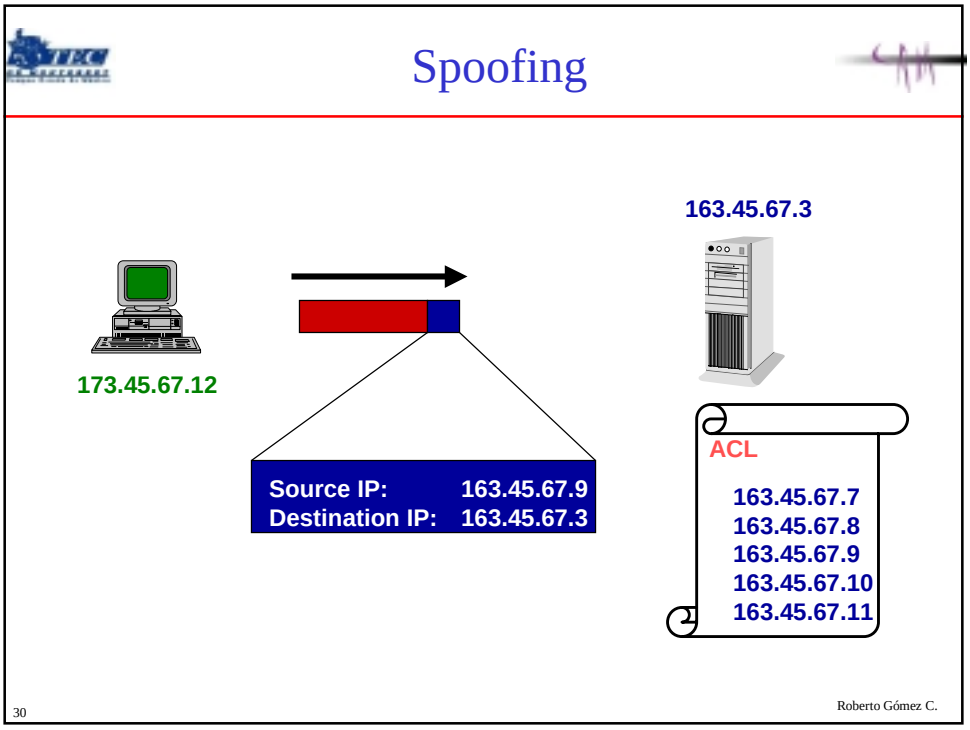
27 Roberto Gómez C.

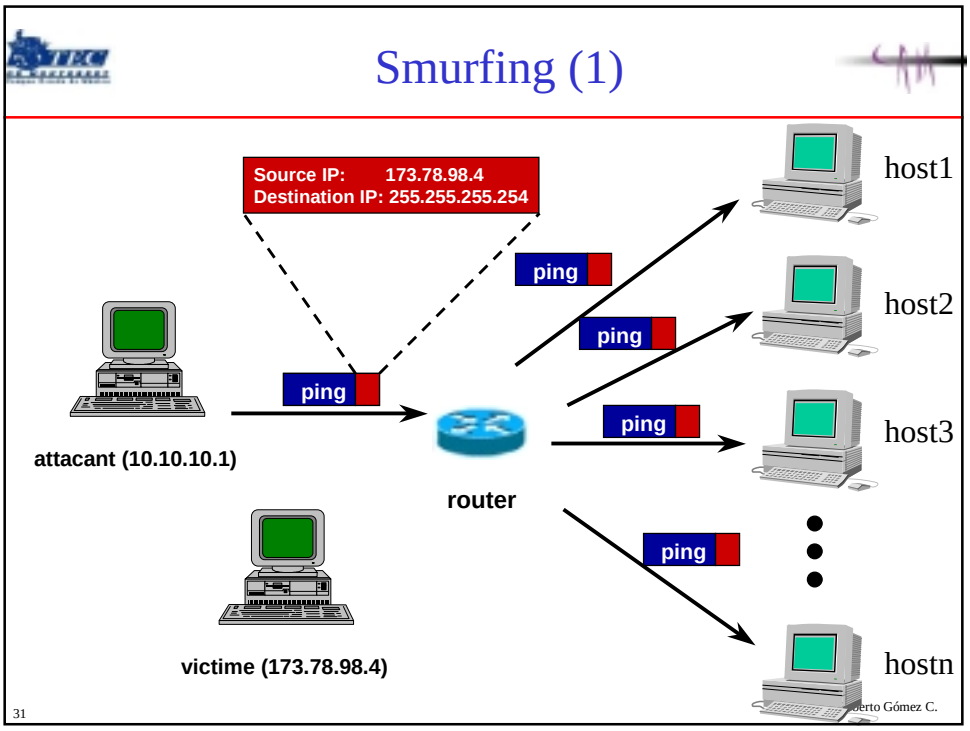
Types d'attaques

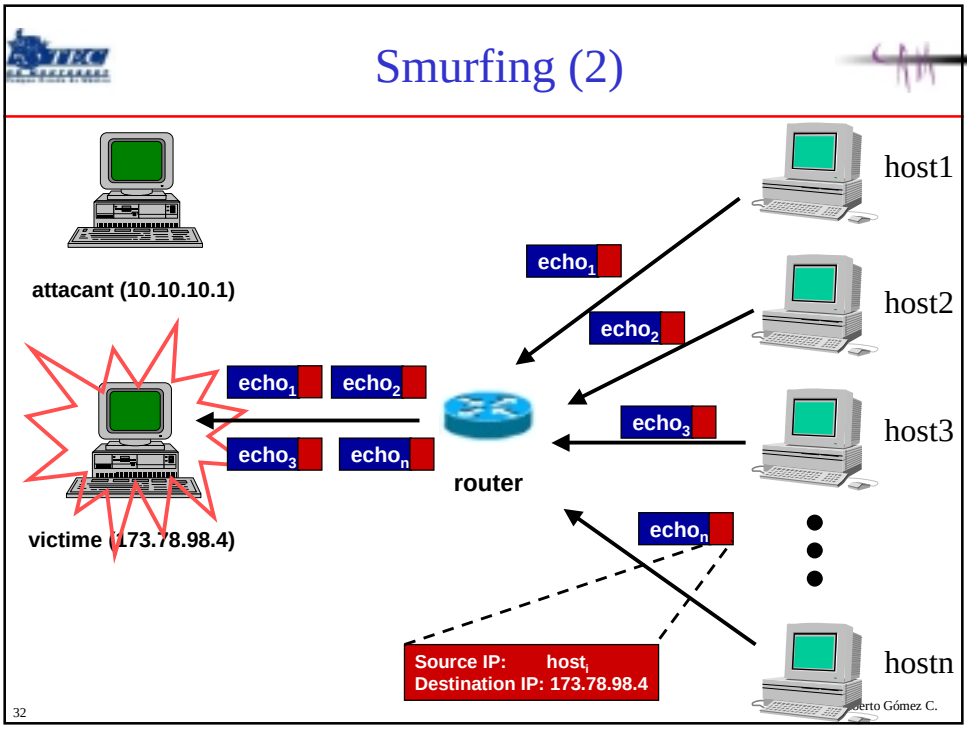
- les buffers overflows (mails, ping of Death...)
- l'attaque SYN
- l'attaque Teardrop
- l'attaque SMURF
- les virus
- les paquets mal formees

28 Roberto Gómez C.


THE GOOD NEWS IS — WE'VE SOLVED YOUR BANDWIDTH PROBLEM...
29
Roberto Gómez C.


Spoofing
163.45.67.3
173.45.67.12
Source IP: 163.45.67.9
Destination IP: 163.45.67.3
ACL
163.45.67.7
163.45.67.8
163.45.67.9
163.45.67.10
163.45.67.11
30
Roberto Gómez C.


Smurfing (1)
Source IP: 173.78.98.4
Destination IP: 255.255.255.254
ping
ping
ping
ping
ping
host1
host2
host3
hostn
attacant (10.10.10.1)
router
victime (173.78.98.4)
31
Roberto Gómez C.


Smurfing (2)
attacant (10.10.10.1)
echo1
echo2
echo3
echon
host1
host2
host3
hostn
router
victime (173.78.98.4)
Source IP: hosti
Destination IP: 173.78.98.4
32
Roberto Gómez C.

L'espiogiciel

- Connaître les habitudes de téléchargement de leurs clients, leurs modes de consommations, leurs centres d'intérêts, ou la périodicité de leurs achats par exemple.
  - les pirates ou espions seront, eux, plus intéressés par le contenu des machines connectées, la réception de ces informations etc
- Il existe des "espiogiciels", en anglais Spywares.
- Ils se trouvent généralement dans le code d'un programme que l'utilisateur téléchargera innocemment sur internet.
  - dans la plupart des cas, ces espogiciels sont des "petits morceaux de codes parasite" (routines) intégrés dans le code principal du programme.

33 Roberto Gómez C.

Graffiti/defaced (1)

34 Gómez C.

Graffiti/defaced (2)

35

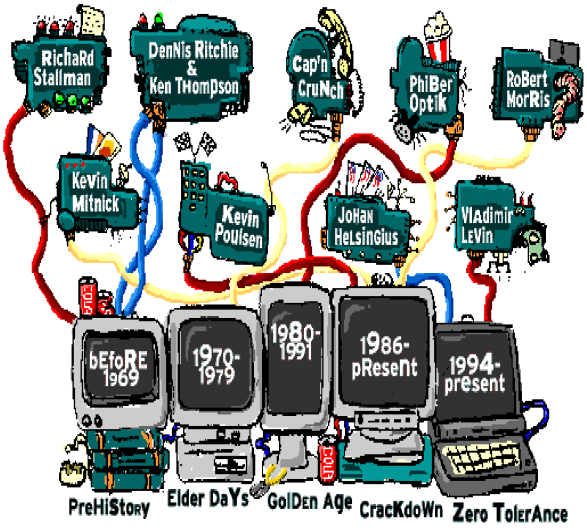
Exemples sites attaques

> date	> original site	> archive	> attacked by	> OS	> comments	> nmap	> class-C
14/05/2002	www.vicavix.de	mirror	haxOrlab	Linux	none	view	history
14/05/2002	www.usfam.com	mirror	Script-Kiddy-Crew	IRIX	none	view	history
14/05/2002	www.pinkcity.info	mirror	Script-Kiddy-Crew	Linux	none	view	history
14/05/2002	www.mp3-blues.org	mirror	Data ChaOs	Linux	none	view	history
14/05/2002	www.inf.org.tw	mirror	Virtual Hell	Windows	none	view	none
14/05/2002	www.autopia.com	mirror	Virtual Hell	Windows	none	view	history
14/05/2002	www.dub-beautiful.org	mirror	Virtual Hell	Windows	none	view	history
14/05/2002	www.artnovela.com.ar	mirror	CyberCrime	Linux	none	view	history
14/05/2002	www.haryobasuki.com	mirror	AntiHiddenLine	FreeBSD	none	view	history
14/05/2002	www.thebucket.org	mirror	Data ChaOs	Linux	Massdefacement	view	history
14/05/2002	www.triarchy.com.tw	mirror	haxOrlab	Linux	none	view	none
14/05/2002	www.abcm.de	mirror	haxOrlab	Linux	none	view	history
14/05/2002	www.trade-telecom.de	mirror	haxOrlab	Linux	none	view	none
14/05/2002	www.goldenfuture24.de	mirror	Rooting Sabotage Forced	Linux	none	view	none
14/05/2002	mail.alitamicrosystems.com	mirror	Unknown	Windows	none	view	none
14/05/2002	pg.ayment.cyberbi.com.cn	mirror	zhazam	Solaris	none	view	history
14/05/2002	mail.cast.org.cn	mirror	zhazam	Solaris	none	view	history
14/05/2002	fyzikus.fmph.uniba.sk	mirror	BHS	Linux	none	view	none
14/05/2002	www.ada-forum.de	mirror	BHS	Linux	none	view	none
14/05/2002	www.zahimo.net	mirror	BHS	Linux	none	view	none
14/05/2002	www.smue.ch	mirror	Data ChaOs	Linux	none	view	none
14/05/2002	www.julix.de	mirror	Data ChaOs	Linux	none	view	history
14/05/2002	www.transitionsoflife.co.uk	mirror	Otacon	Windows	none	view	history
14/05/2002	www.property.co.il	mirror	nerf	FreeBSD	none	view	history
14/05/2002	www.keysign-co.com	mirror	CriminalS	Windows	none	view	history
14/05/2002	www.art-in-canada.com	mirror	Otacon	Windows	none	view	none
14/05/2002	www.fabulousfoods.com	mirror	nerf	Linux	none	view	none
14/05/2002	www.endeavor.org.br	mirror	Otacon	Windows	none	view	history
14/05/2002	www.seram.es	mirror	Evil Angelica	Unknown	none	view	none
14/05/2002	www.kindoroko.com	mirror	Otacon	Windows	none	view	history

36

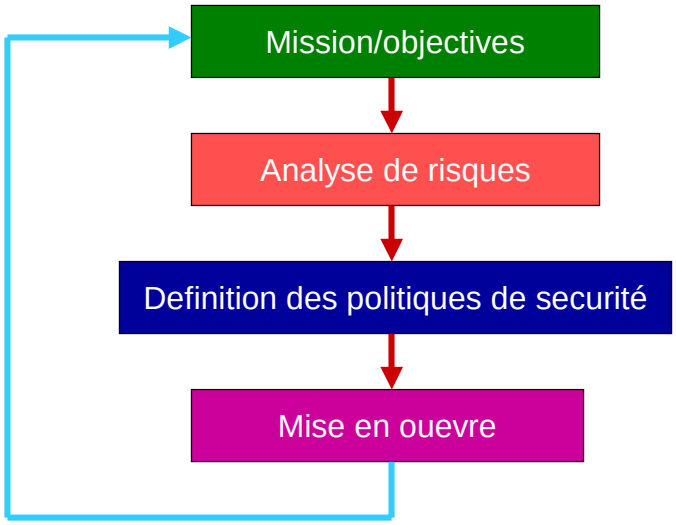
Les acteurs

- Hackers
- Crackers
- Phreaker
- Lammer
- Newbie
- Script-kid



37 Roberto Gómez C.

Etapes pour securiser un système



38 Roberto Gómez C.

Mecanismes de securité

- Ils representent la partie la plus visible d'un système de securité
- Ils devient l'outil de basse qui garantis la protection des systemes ou des reseaux
- On peut les classer:
  - prevention
  - detection
  - recuperation

39 Roberto Gómez C.

Mécanismes prévention

- Prevenir les attaques informatiques
- Exemples des mécanismes
  - protection physique
  - chiffrement
  - listes d'accès
  - authentication par mot de passe
  - firewalls
  - biométrie

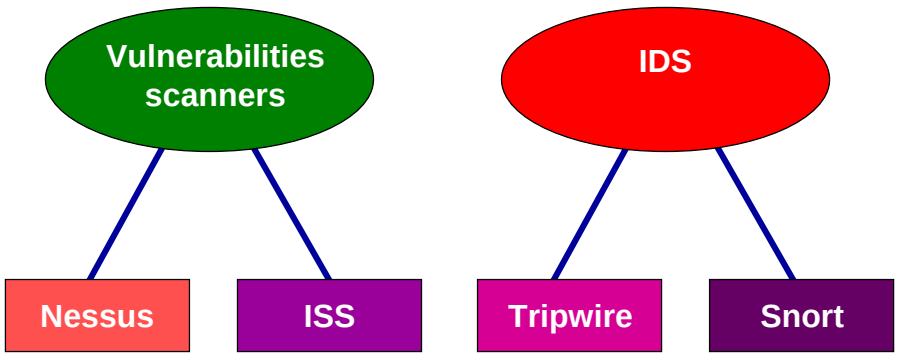
40 Roberto Gómez C.

Mecanismes détection

- L'objectif n'est pas de définir des mécanismes pour empêcher l'occurrence d'attaques mais de les détecter pour préparer la contre-mesure la mieux adaptée.
- Le domaine de la détection d'intrusion existe depuis une quinzaine d'années et est actuellement en pleine expansion.
- Exemples
  - Tripwire
  - Snort

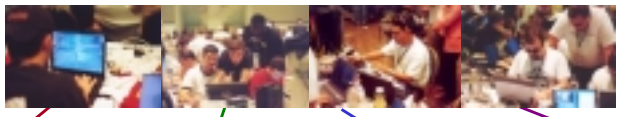
41 Roberto Gómez C.

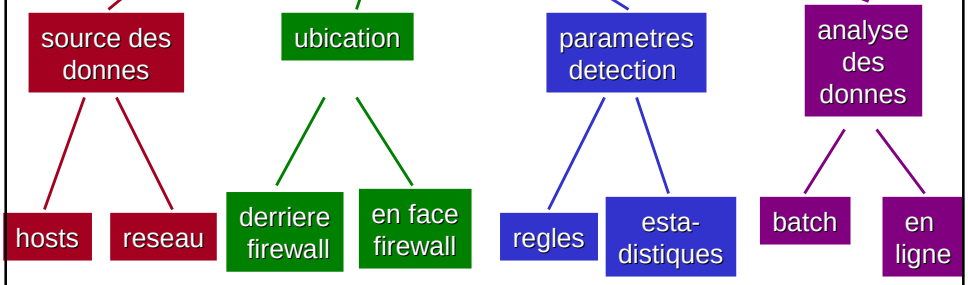
Mecanismes détection



42 Roberto Gómez C.

Parametres a considerer dans les IDS

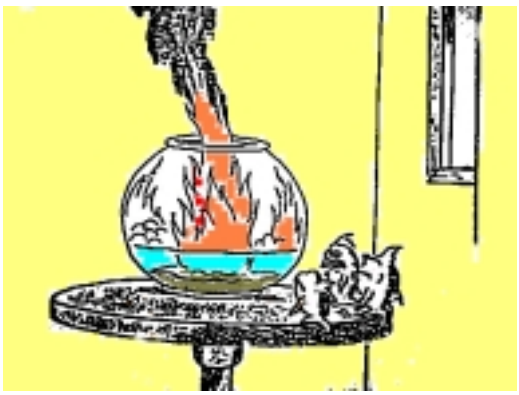




43 Roberto Gómez C.

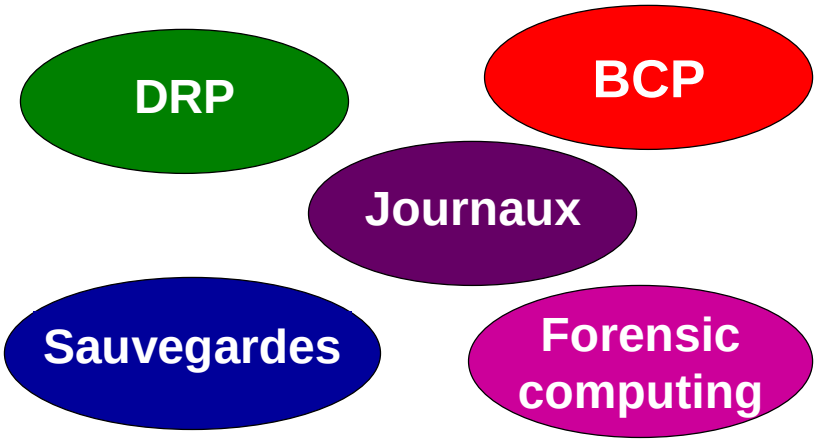
Mecanismes de recuperation

- Ils décrivent les procédures prévues pour le rétablissement du fonctionnement d'un système d'information après un sinistre
- Exemples
  - sauvegarde
  - redundance
  - plan de secours (BCP et DRP)
- Subgroup
  - forensics computing



44 Roberto Gómez C.

Mecanismes de recuperatión



45 Roberto Gómez C.

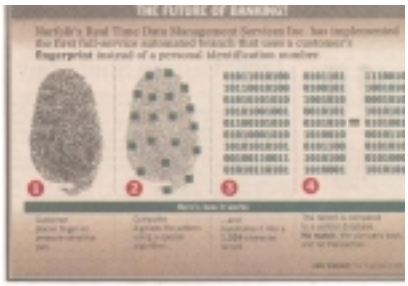
Mecanismes prevención plus habituelles

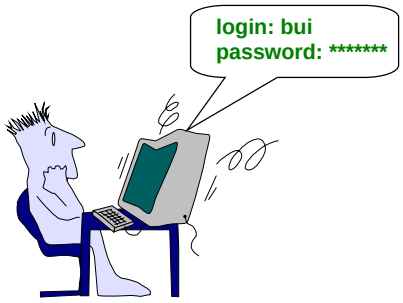
- Mecanismes de authentification
- Mecanismes de contrôle d'accès
  - contrôle d'accès discrétionnaire (DAC)
  - contrôle d'accès obligatoire (MAC)
- Mecanismes de separatión
- Mecanismes de securité dans les telecommunications

46 Roberto Gómez C.

Mecanismes authentification

- Ceux qui reposent en ce qui on connait
- Ceux qui reposent en ce qui on est
- Ceux qui reposent en ce qui on possede





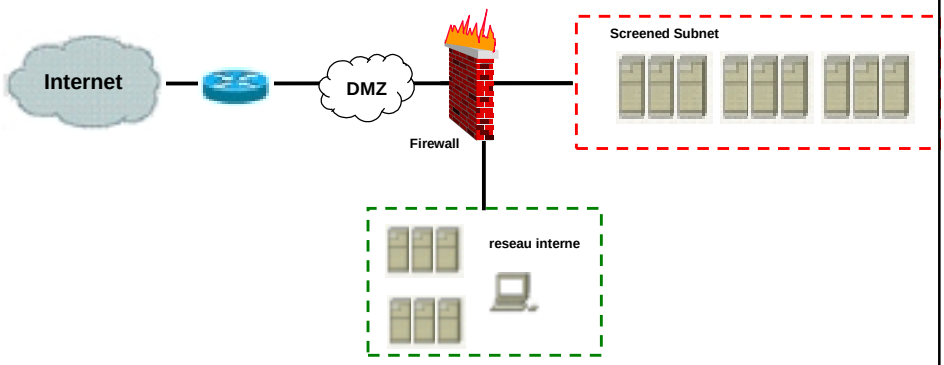
47 Roberto Gómez C.

Mecanismos de separation

- Proteger le perimeter su systeme
- Elements de protection
  - Ruteur de frontiere (border router)
    - Liste de control d'acces
  - Firewall
  - Proxies
  - VPNs
  - NAT

48 Roberto Gómez C.

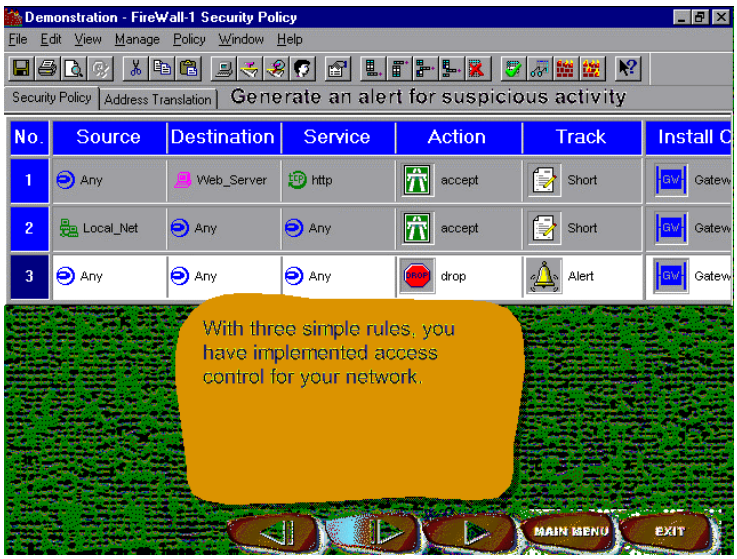
Firewalls, DMZ et screened subnets



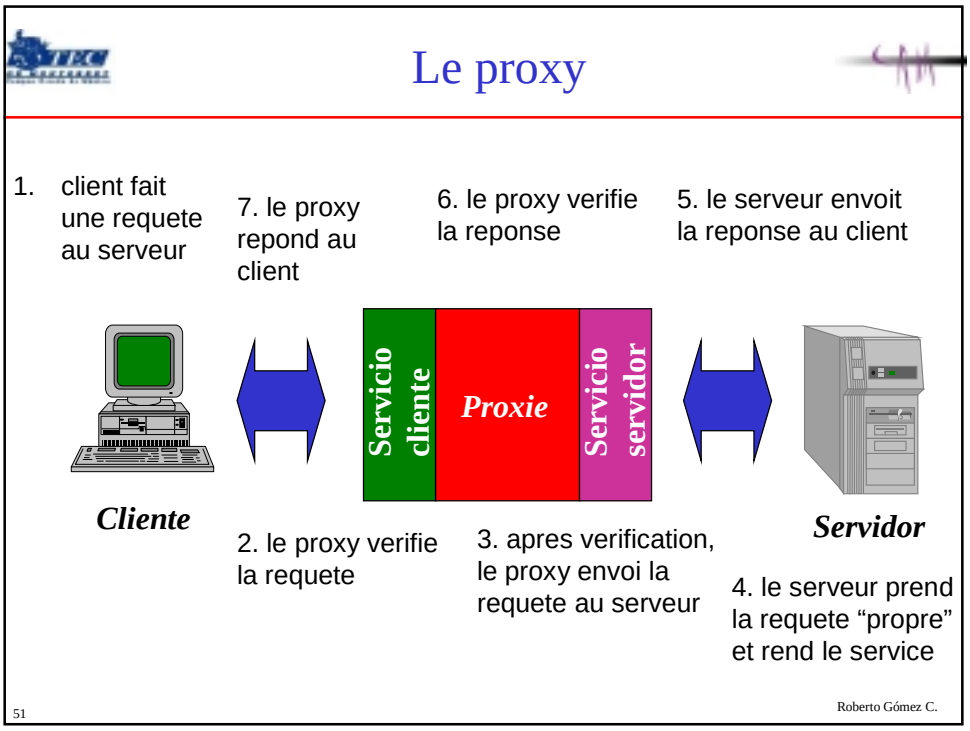
- DMZ se trouve en face du firewall
- Un sous-reseau “screened” est place derriere le firewall

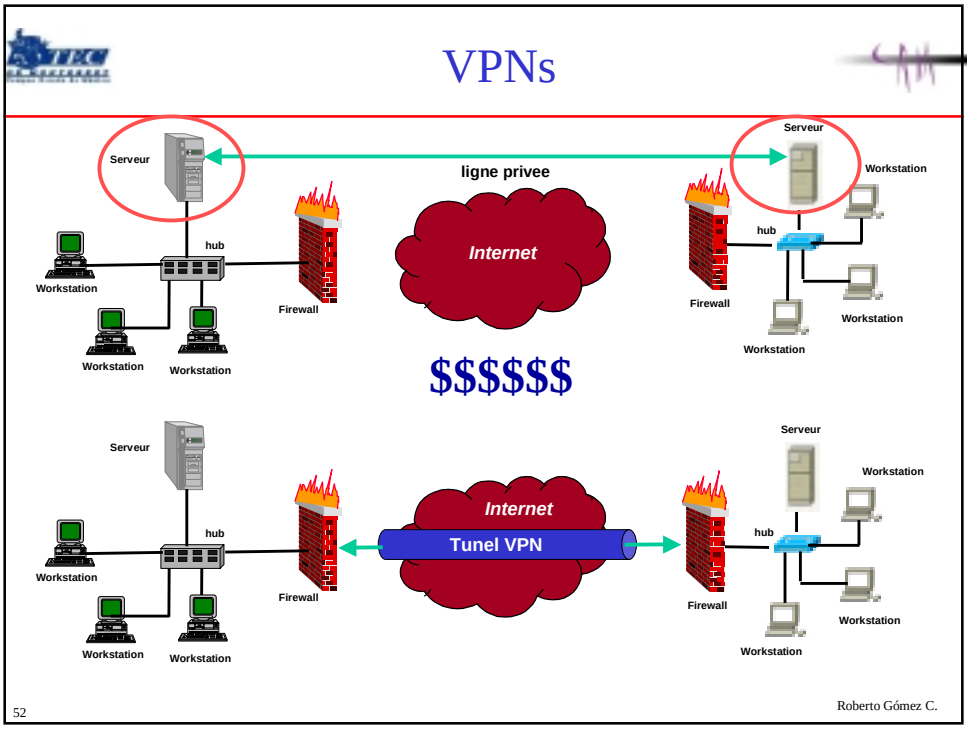
49 Roberto Gómez C.

Exemple d’une regle



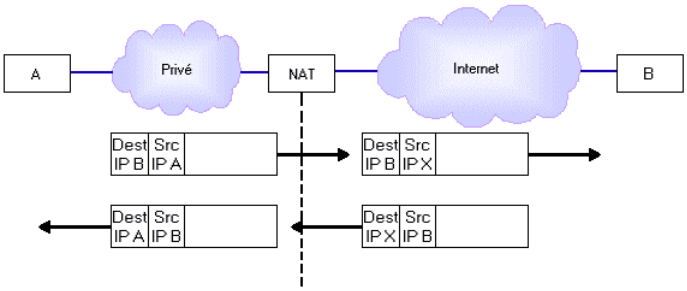
50 Roberto Gómez C.


Le proxy
1. client fait une requete au serveur
7. le proxy repond au client
6. le proxy verifie la reponse
5. le serveur envoit la reponse au client
Servicio cliente
Proxie
Servicio servidor
Cliente
Servidor
2. le proxy verifie la requete
3. apres verification, le proxy envoi la requete au serveur
4. le serveur prend la requete “propre” et rend le service
51
Roberto Gómez C.


VPNs
Serveur
ligne privee
Workstation
hub
Firewall
Internet
$$$$$$
Tunel VPN
52
Roberto Gómez C.

NAT

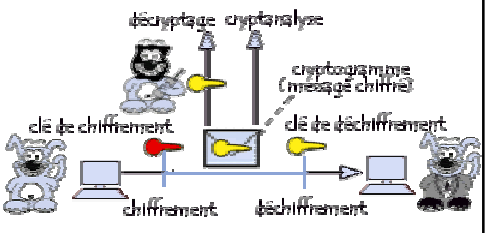
- La technique de translation d'adresses (NAT en anglais, RFC 3022) est une pratique courante qui est apparue à l'origine pour palier au manque croissant d'adresses IPv4 libre



53 Roberto Gómez C.

Mecanismes de securité pour les comunications

- La cryptographie
  - transformation de données dans une forme illisible pour quelqu'un qui ne détient pas la méthode de décryptage (souvent une clé de décryptage).
  - son but est de garantir la confidentialité et authenticité de messages transmis entre diverses entites
- Criptographie clássique
  - substitution
  - permutation
- Criptographie moderne
  - Chiffrement symétrique
  - Chiffrement asymétrique



54 Roberto Gómez C.

Le rol de la cle dans la cryptographie

- Le chiffrement consiste à effectuer une opération entre la clé et les données à chiffrer afin de rendre ces dernières intelligibles
- Exemple cle: DAVID.

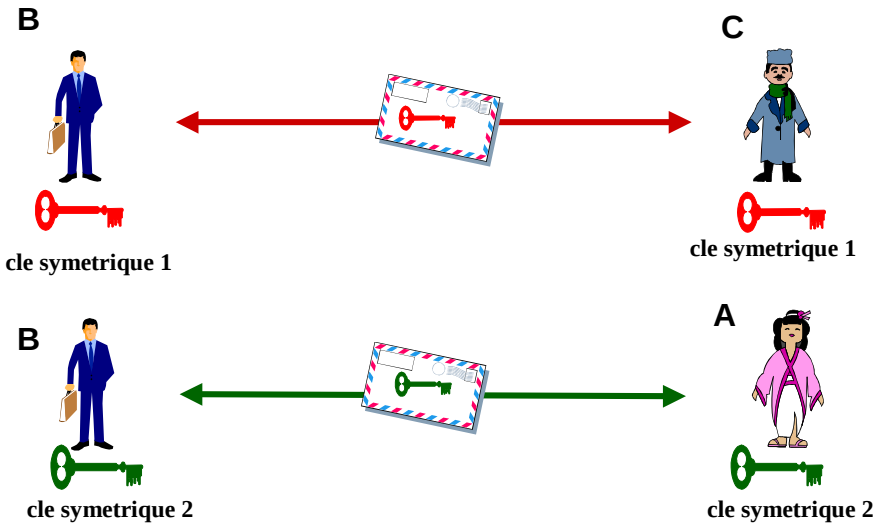
  DAVID = 1000100 1000001 1010110 1001001 1000100

- Pour chiffrer (addition binaire: xor)

Texte original: HELLO
Texte ASCII: 1001000100001011001100100110010011111
Cle: 1000100100000110101101001001100010 0
Cryptogramme: 0001100000010000110100000101000 1011

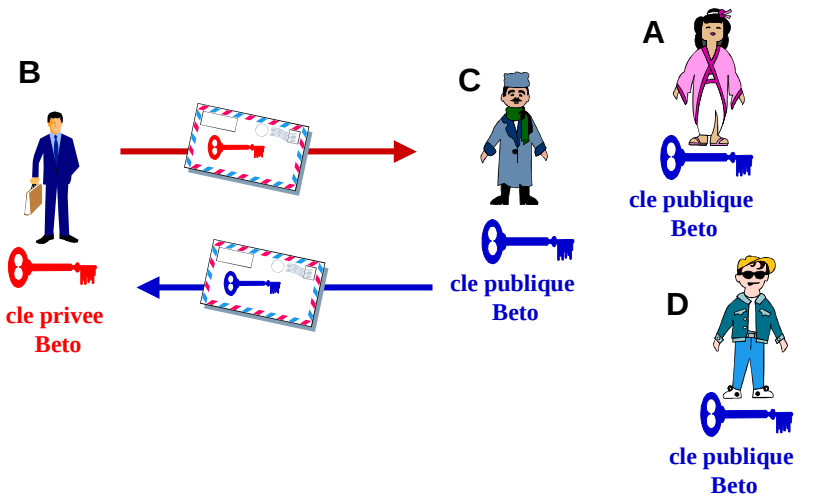
55 Roberto Gómez C.

Chiffrement symétrique



56 Roberto Gómez C.

Chiffrement asymétrique



57 Roberto Gómez C.

Protocoles criptographiques

- SSL
  - Secure Socket Layer
- PCT
  - Private Communication Technology
- TLS
  - Transport Layer Security
- SSH
  - Secure SHell
- S-HTTP
  - Secure HTTP

58 Roberto Gómez C.

Principe de fonctionnement (1)

Salut

Salut

Ca vais?

Tres bien

Pas d'authentification, ni de privacité, ni de chiffrement

Je veux payer

Prend ma cle publique

Je t'envoi une cle neuve chiffree avec ta cle publique

Parlons en securité

Comunication chiffre avec la cle envoie par le client

59 Roberto Gómez C.

Principe de fonctionnement (2)

Parlons de forme secure, voici les protocoles et criptosystemes que je connait

Je choici cet protocole et cryptosysteme. Voici ma cle publique, un certificat binaire et un numero aleatoire

Avec ta cle publique, j'ai chiffre une cle asymetrique aleatoire

Comunication chiffre

60 Roberto Gómez C.

Et les systemes d'exploitation?

- **Un sistema operativo es tan seguro como preparado este su administrador y tan inseguro como incapaz sea el administador.**
- **An operating system is sure as its administrator knows it, and as bad as incapable its adminitrator is.**
- **Un systeme d'exploitation est aussi assure que son administrateur l'en connait, mais aussi vulnerable que la mal connaissance de son administrateur.**

61 Roberto Gómez C.

Conclusions

- La securité est au-dela des produits
- Les attaques existent, ils ne sont pas des illusions.
- Les outils pour assurer un systeme sont deja la
  - il faut les utiliser
- Il n'existe pas un systeme 100% securise
  - n'importe quel systeme peut etre objet d'un attaque
  - on essaie de rendre plus difficile l'attack
- La securité n'est ni noire ni blanche, le context est plus important que la technologie.

62 Roberto Gómez C.

References

- Network Intrusión Detection; Northcutt, Ed. New Riders, 2da. edición
- Network Security; Kaufman, Perlman y Speciner, Ed. Prentice Hall
- Applied Cryptography Protocols, Algorithms and Source in C; B. Schneier, John Wiley & Sons
- Maximum Linux Security, Anonymous, SAMS, 2000
- Secure-Programs-HOWTO
- Security-HOWTO

63 Roberto Gómez C.

Des pages web

- http://www.securityfocus.com
- http://www.cert.org
- http://www.sans.org
- http://www.kriptograma.org
- http://www.packetstorm.com
- http://www.snort.org
- http://www.tripwire.com
- http://www.linux.org
- http://linux.security.com
- http://www.securiteinfo.com (en francais!!)

64 Roberto Gómez C.


Merci de votre attention!
Securite informatique
Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez
La invencibilidad depende de uno mismo; la vulnerabilidad del enemigo, de él.
La invencibilidad reside en la defensa; la posibilidad de la victoria en el ataque.
Sun Tzu, "El arte de la guerra"
65
Roberto Gómez C.