Actions offensives sur Internet

Stratégies et techniques d'intrusion

Plan de la présentation

- Introduction
- Les différentes phases d'une attaque
  - Identification de la cible
  - Scanning
  - Exploitation
  - Progression
- Conclusion, questions

Introduction

- Cadre: uniquement les attaques sur Internet
  - Hors chevaux de Troie, virii, dénis de service
  - Pourquoi ce choix ?
- Internet n'est pas la seule porte d'entrée
  - C'est même souvent la plus dure à forcer !

Identification de la cible

Objectifs et méthodologie

- Collecter le plus de renseignements possibles sur la cible
- En utilisant des informations publiques
- Sans engager quoique ce soit d'hostile

Interrogation DNS

- On recherche tous les domaines enregistrés par la cible grâce au Whois
  - Nous donne aussi noms, adresses, téléphones des administrateurs
- On interroge DNS pour connaître les adresses IP des serveurs www, mail, ...

Interrogation bases d'IP

- Grâce à DNS, nous avons obtenu des adresses IP du réseau cible
- Nous faisons une recherche inverse avec les bases d'IP régionales
- Afin de connaître l'ensemble des IP allouées à la cible

Moteurs de recherches

- Utilisation des moteurs classiques
  - Altavista, Google, Dejanews ...
  - Pour trouver toute information sur la cible (press releases, partenaires, serveurs news ...)
- Utilisation de moteurs dédiés
  - Bases de données d'informations financières, ...
  - Souvent accès à ces bases payant
  - ex: www.societe.com, www.kompass.com, d'autres beaucoup plus pointus

Mail bounce

- Envoi d'un mail à une adresse invalide dans le domaine cible pour obtenir un retour (zefqsdfsdfqsdf@cible.com)
- Examen des en-têtes dans le mail retourné pour obtenir des informations sur la structure du réseau cible

Exemple (1)

```
[root@Evil /root]# whois secway.com@whois.networksolutions.com
[whois.networksolutions.com]
<...>
Registrant:
Secway (SECWAY-DOM)
   25-27, rue de l'Ouest
   Paris, 75014
   FRANCE

   Domain Name: SECWAY.COM

   Administrative Contact, Technical Contact, Billing Contact:
      Nicolas, DUBEE  (DN4404)  ndubee@DF.RU
      SECWAY
      25-27, rue de l'Ouest
      paris
      75014
      FR
      +33 1 43211718

   Record last updated on 21-May-2001.
   Record expires on 07-Mar-2002.
   Record created on 07-Mar-1999.
   Database last updated on 13-Sep-2001 06:38:00 EDT.

   Domain servers in listed order:

   NS1.325I.COM              216.149.77.66
   NS3.NJD.XO.COM             216.156.2.3

[root@Evil /root]#
```

Exemple (2)

```
[root@Evil /root]# host -a secway.com
Trying null domain
rcode = 0 (Success), ancount=3
The following answer is not authoritative:
The following answer is not verified as authentic by the server:
secway.com      172296 IN       NS      NS1.325I.com
secway.com      172296 IN       NS      NS3.NJD.XO.com
secway.com      172296 IN       A       194.221.6.40
For authoritative answers, see:
secway.com      172296 IN       NS      NS1.325I.com
secway.com      172296 IN       NS      NS3.NJD.XO.com
Additional information:
NS1.325I.com    172296 IN       A       216.149.77.66
NS3.NJD.XO.com  172296 IN       A       216.156.2.3
[root@Evil /root]# host -t mx secway.com
secway.com mail is handled (pri=10) by mail.secway.com
[root@Evil /root]# host -a www.secway.com
Trying null domain
rcode = 0 (Success), ancount=1
www.secway.com  3600 IN CNAME   secway.com
For authoritative answers, see:
secway.com      3600 IN NS      secway.com
Additional information:
secway.com      3600 IN A       216.149.77.66
```

Exemple (3)

```
[root@Evil /root]# whois 216.149.77.66@whois.arin.net
[whois.arin.net]
9 Net Avenue, Inc. (NETBLK-NINENETAVE-1)
  110 Meadowland Parkway
  Secaucus, NJ 07094
  US

  Netname: NINENETAVE-1
  Netblock: 216.149.0.0 - 216.149.255.255
  Maintainer: 9NET

  Coordinator:
    Grosso, Patrick  (PG64-ARIN)  patg@9NETAVE.COM
    888-963-8283

  Domain System inverse mapping provided by:

  NS2.9NETAVE.COM          216.156.2.2
  NS3.9NETAVE.COM          216.156.2.3

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

  Record last updated on 27-Jan-2000.
  Database last updated on 10-Sep-2001 23:16:26 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
[root@Evil /root]#
```

Exemple (4)

Received: from relais.xxxxx.com ([123.45.67.89]) by koi.df.ru (8.9.0/8.8.8) with SMTP id QAA21414 for <ndubee@DF.RU>; Fri, 11 Aug 2000 16:20:06 +0400
Received: from **192.1.1.50** by relais.xxx.com (InterScan E-Mail VirusWall NT); Fri, 11 Aug 2000 14:24:14 +0200 (Paris, Madrid (heure d'été))
Received: by **mail.xxxxx.com(Lotus SMTP MTA SMTP v4.6 (462.2 9-3-1997))** id C1256938.0043AF89 ; Fri, 11 Aug 2000 14:19:18 +0200
X-Lotus-FromDomain: ORG
To: Nicolas Dubee ndubee@DF.RU

Received: from relais.xxxx.com ([123.45.67.89]) by koi.df.ru (8.9.0/8.8.8) with SMTP id TAA17429 for <ndubee@df.ru>; Fri, 11 Aug 2000 19:06:50 +0400
Message-Id: <200008111506.TAA17429@shell.dataforce.net>
Received: from **192.1.1.50 by relais.xxxx.com (InterScan E-Mail VirusWall NT)**; Fri, 11 Aug 2000 17:10:58 +0200 (Paris, Madrid (heure d'été))
From: POSTMASTER@mail.xxxxx.com
To: ndubee@df.ru
Date: Fri, 11 Aug 2000 17:05:54 +0200
Objet: message non distribué
X-UIDL: 3864dfdeb927e75e31fd1ea0fe9acfd9

------- Motif de l'échec --------

Utilisateur non recensé dans le Carnet d'adresses public
fdgdfgsdfg@xxxxxxxxx.com

------- Message renvoyé --------
Received: from **relais.xxxx.com ([192.168.20.1])** by mail.xxxxxxxxx.com (Lotus SMTP MTA SMTP v4.6 (462.2 9-3-1997)) with SMTP id C1256938.0052E6F3; Tue, 11 Aug 1970 17:05:30 +0200
Received: from 195.132.98.198 by relais.xxxxx.com (InterScan E-Mail VirusWall NT); Fri, 11 Aug 2000 17:09:57 +0200 (Paris, Madrid (heure d'été))

bounce test.

---
vérifié par interscan (antivirus)

Scanning

Objectifs

- Identifier
  - les IP utilisées
    - ICMP ou TCP ACK
  - les services accessibles
  - toutes informations de topologie détaillée
    - OS
    - versions des services
    - Subnets
    - Règles firewall
    - ...

Identification des IP utilisées

- Technique du « ping-sweep »
  - Envoi séquentielle de ICMP Echo Request à toutes les IP à tester
  - Réponse ICMP Echo Reply pour les IP actives
- Technique ACK-Scan
  - Envoi de paquets ACK vers un port aléatoire
  - Si machine active, réponse RST
  - Passe certains firewalls !

Portscan (1)

- Identifier les services ouverts sur une IP donnée
- Donc identifier les ports TCP ou UDP ouverts
- Envoi de paquets (*probes*) sur l'ensemble des ports à tester
- Port ouvert ou non en fonction de la réponse

Portscan (2)

- Scanning TCP
  - TCP connect
    - Établissement complet d'une connexion TCP (3-way handshake)
    - Visible dans les logs du firewall et du service visé
  - SYN Scan (Half-Scan)
    - Envoi d'un SYN, attente SYN+ACK ou RST
    - Visible dans les logs du firewall, invisible dans les logs du service

Portscan (3)

- FIN/Null/XMAS Scan
  - Combinaison de flags, réponse différente en fonction de l'ouverture/fermeture du port
  - Dépend de l'OS (car certaines piles IP non exactement conformes aux RFC)
- FTP Bounce Scanning
  - Utilisation de la commande PORT vers un serveur FTP
  - Le serveur FTP répond 220 si connexion établie ou 500 sinon
  - Dans les logs, le serveur FTP apparaîtra

Portscan (4)

- Scanning UDP
  - Pas de méthode générique
  - Envoi d'un paquet de test
    - Si réponse UDP: port ouvert
    - Si réponse ICMP Port Unreach: port fermé
    - Si rien: on ne sait pas

Analyse applicative (1)

- Les ports ouverts trouvés, on détermine quel service y écoute
  - Souvent: numéros de ports standards
  - Sinon: réponse à des requêtes standards
- En prime on détermine souvent la version du service
  - Bannière à la connexion

Analyse applicative (2)

```
[root@Evil /root]# telnet www.secway.com 80
Trying 216.149.77.67...
Connected to www.secway.com.
Escape character is '^]'.
GET / HTTP/1.0
Host: www.secway.com

HTTP/1.1 200 OK
Date: Thu, 13 Sep 2001 21:45:25 GMT
Server: Apache/1.3.12 Ben-SSL/1.40 (Unix) PHP/4.0.1pl2 FrontPage/4.0.4.3
Last-Modified: Mon, 20 Sep 1999 15:25:36 GMT
ETag: "555cf-f08-37e651f0"
Accept-Ranges: bytes
Content-Length: 3848
Connection: close
Content-Type: text/html

<HTML>
```

Détermination de l'OS

- Souvent on peut déterminer l'OS par les versions des services trouvées précédemment
- Sinon, les piles IP répondent différemment suivant l'OS
  - On utilise la non-conformité aux RFC
  - Réponse à des paquets types

Topologie

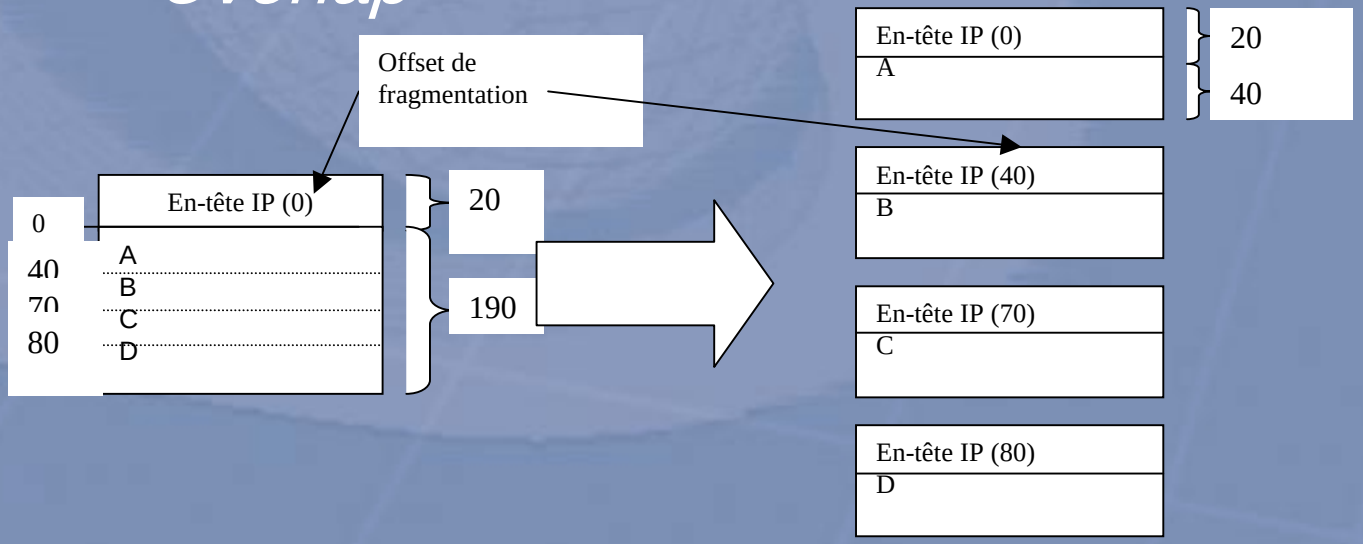
- Traceroute
  - Détermination de tous les intermédiaires (-> routeurs) entre l'agresseur et la cible
  - Envoi de paquets avec TTL incrémenté
- Firewalking
  - Variation de traceroute
  - Détermination des ACL au niveau du firewall

Techniques avancées (1)

- Contournement des IDS et firewalls: utilisation de mauvaises règles ou de bugs de firewalls
  - Ports sources spéciaux
    - 20/TCP: FTP-DATA
    - 53/UDP: DNS
  - Rebonds à partir de proxies applicatifs
    - caches HTTP
    - Socks

Techniques avancées (2)

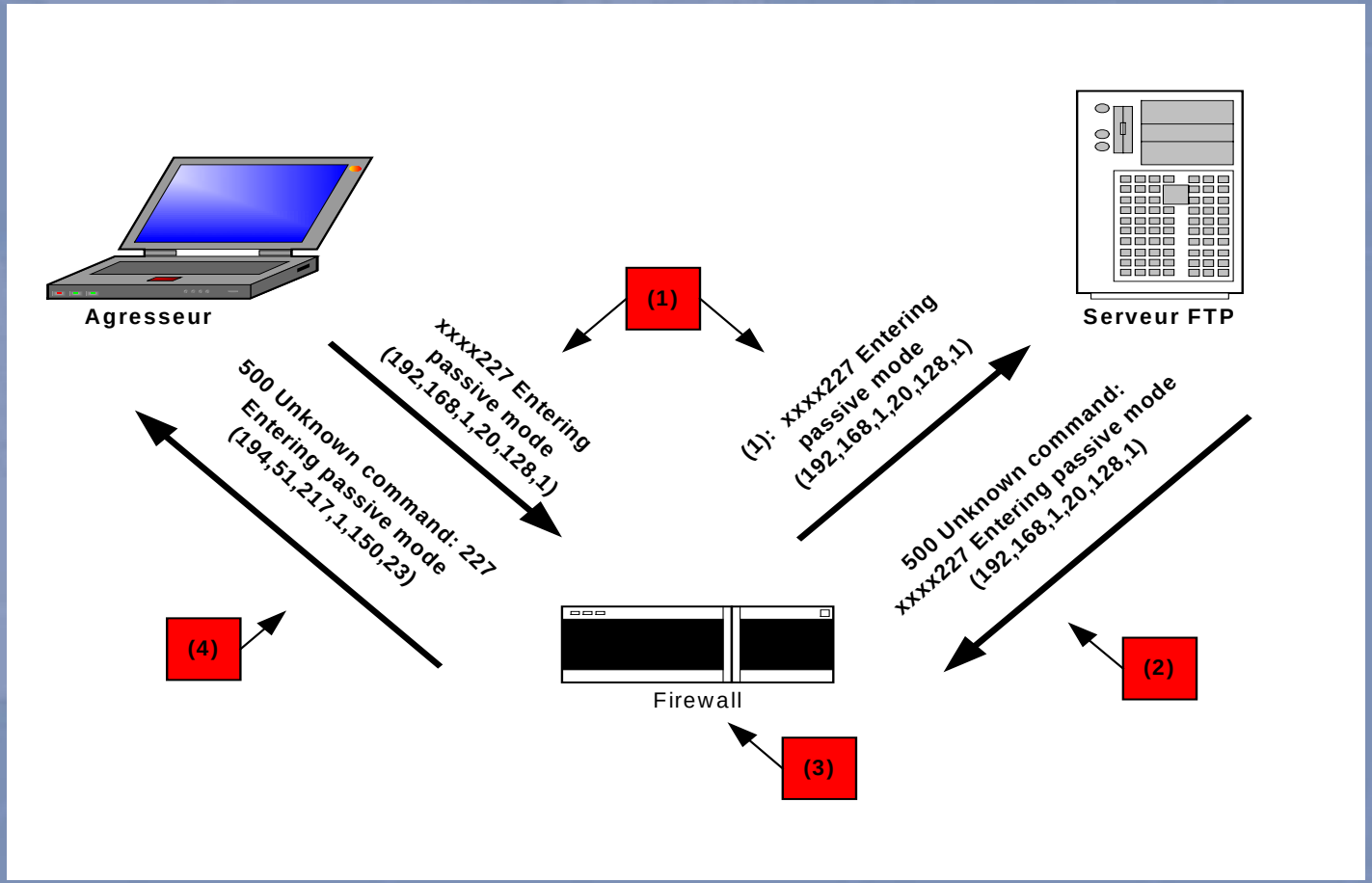
- Fragmentation IP
  - *short frag*
  - *Overlap*



Techniques avancées (3)

- Bugs des firewalls ou des stacks IP
  - Ex: bug FTP PASV de Checkpoint Firewall-1

Techniques avancées (4)

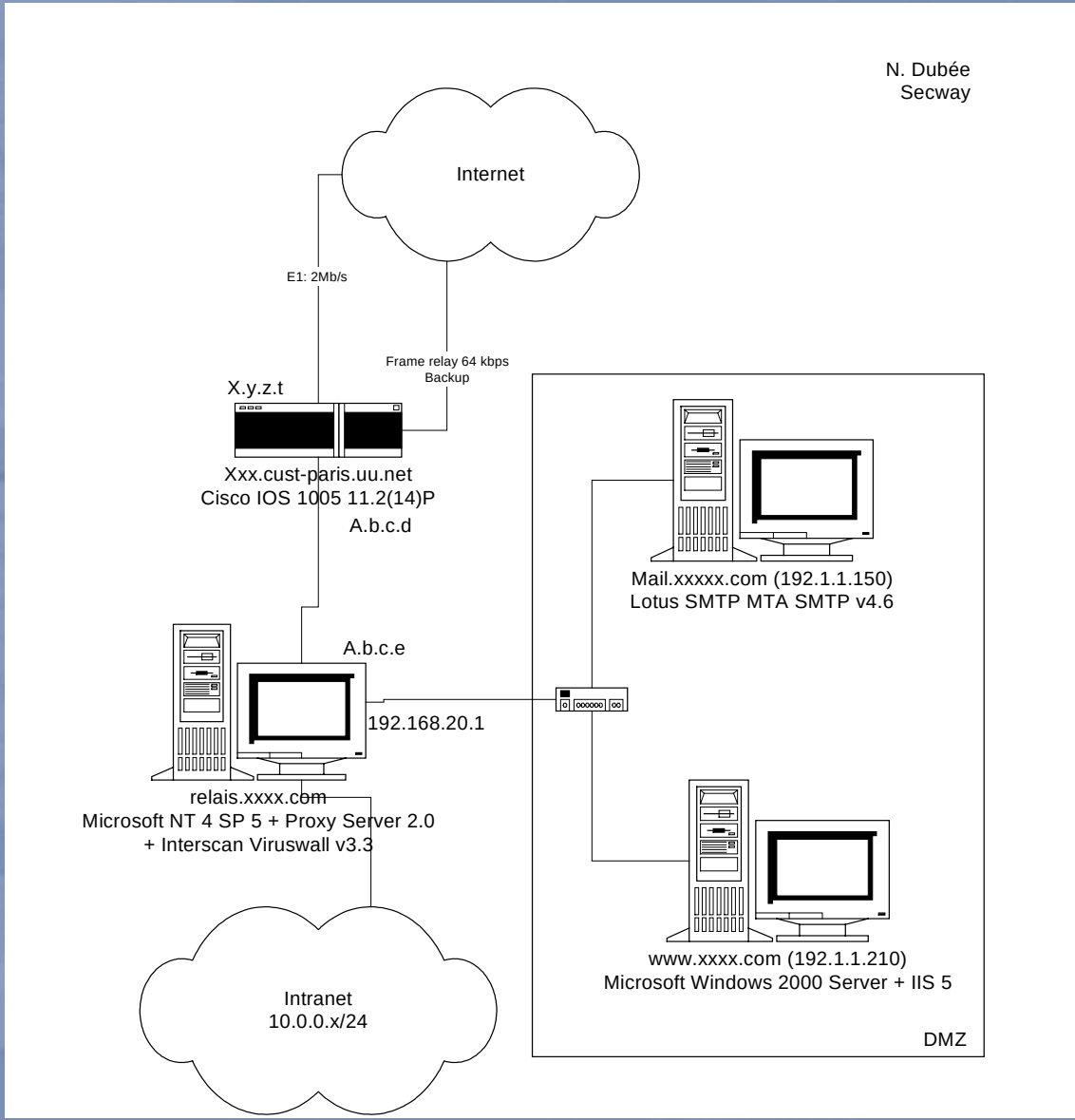


Exemple

- Outil de portscanning nmap

```
scanbox# nmap -sT -O 10.0.0/24

Starting nmap V. 2.54BETA29 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on fw.secway-int.net (10.0.0.1):
(The 1545 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
587/tcp    open        submission

Remote operating system guess: MacOS X 10.0.4 (Darwin V. 1.3-1.3.7 or 4P13)
Uptime 0.143 days (since Tue Sep 18 11:16:58 2001)

Interesting ports on pow.secway-int.net (10.0.0.10):
(The 1544 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        listen

Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, Windows Millenium Edition v4.90.3000

...
```

Au final


N. Dubée
Secway
Internet
E1: 2Mb/s
Frame relay 64 kbps
Backup
X.y.z.t
Xxx.cust-paris.uu.net
Cisco IOS 1005 11.2(14)P
A.b.c.d
Mail.xxxxx.com (192.1.1.150)
Lotus SMTP MTA SMTP v4.6
A.b.c.e
192.168.20.1
relais.xxxx.com
Microsoft NT 4 SP 5 + Proxy Server 2.0
+ Interscan Viruswall v3.3
Intranet
10.0.0.x/24
www.xxxx.com (192.1.1.210)
Microsoft Windows 2000 Server + IIS 5
DMZ

Exploitation

Objectifs

- Etant donné le réseau analysé et les failles qu'il connaît
- Cibler le service le plus favorable
  - absence de traces
  - taux de réussite
  - facilité de réalisation
- Approche opportuniste: une faille suffit!
- Point de non retour atteint

Des constats

- La plupart des services Internet vulnérables
- Des programmes d'attaques, *exploits*, en libre circulation
  - « Local or remote exploit »
- *Exploits* privés (*0-day*) conservés par des groupes d'initiés
  - Pour ceux-là, aucun moyen de se protéger car pas de patch !!!!

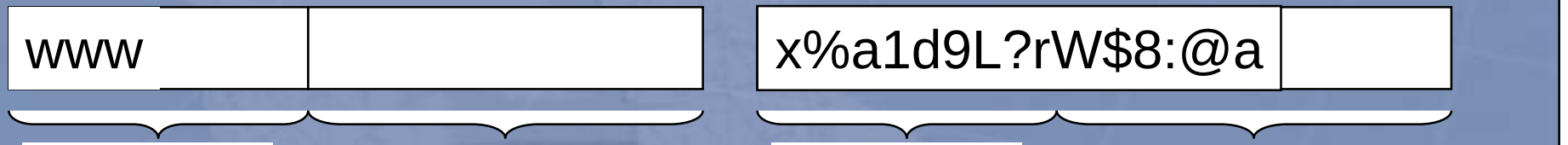
Catégories d'attaques

- Fautes d'implémentation
  - Buffers overflows, métacharactères, *format strings*, ...
- Fautes de conception
  - Mauvais algorithme
- Virii, chevaux de Troie, Worms

Les buffers overflows (1)

- Faute de programmation courante en C et dans les langages ayant la même gestion des tableaux
- Consiste à déborder de la mémoire allouée à un tableau pour écraser d'autres variables en mémoire
- Le type de faille le plus fréquent

Les buffers overflows (2)



Variable buf | Autres variables internes

Variable buf | Autres variables manipulées

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

int  doit(char *host)
{
char buf[64] ;

strcpy(buf, host) ;
...
}

int main(int argc, char **argv)
{
 ...
 doit(argv[1]) ;
 ...
}
```


Les buffers overflows (3)

- Fait: les architectures classiques (i386, Sparc, ...) utilisent la pile pour stocker l'adresse de retour des fonctions
- Les variables locales sont aussi stockées sur la pile
- Un buffer overflow permet donc entre autres de manipuler le flux du programme

Les buffers overflows (4)

- On place dans notre buffer un code exécutant un shell (*shellcode*), ainsi qu'à l'endroit de l'adresse de retour légitime, l'adresse du shellcode.
- Ce type de faille est exploitable en local (élévation de privilèges) ou à distance
  - Ex: buffer overflow dans BIND (serveur DNS)

Métacharactères (1)

- Principalement dans les scripts CGI
- Absence ou mauvais contrôle des champs de formulaires Web
- Possibilité d'introduire des caractères spéciaux

Métacharactères (2)

- Scripts CGI en Perl envoyant un mail:

```
# !/usr/bin/perl
...
open(FD, „|/bin/mail $email“)  || die(„can’t mail!“);
print FD « Nous avons recu votre demain d’information.\n » ;
print FD «Vous recevrez dans quelques jours notre brochure.\n\n » ;
print FD « Cordialement, \n L’équipe blahblah.\n » ;
...
```

- Permet d’exécuter des commandes shell sur le serveur!!!

Fautes de conception

- Mauvais algorithme
  - Les mots de passe des partages sous Microsoft W9x
    - Comparaison des x premiers caractères du mot de passe requis avec le mot de passe envoyé par l'utilisateur, où x est un nombre spécifié par l'utilisateur !!!

Usurpation d'identité (1)

- Utilisation des droits d'un autre utilisateur
- Nécessite la récupération ou la prédiction des identifiants
- En général réalisable sur TOUT système de sécurité
- Prend souvent beaucoup de temps, et pas discret!

Usurpation d'identité (2)

- *Bruteforce* (login/passwd)
- *Trust relationships* (r-services, NFS, ...)
- Interception (*sniffers*, *Man-in-the-middle*)
- Vol de session (*hijacking*)

Usurpation d'identité (3)

- Exemple d'outil d'interception, les sniffers
  - La plupart des protocoles classiques (FTP, POP, HTTP) font circuler les mots de passe en clair
  - Les sniffers analysent le trafic réseau sur lequel ils sont connectés
  - Ils Interceptent les mots de passe qui transitent en clair et les enregistrent

Usurpation d'identité (4)

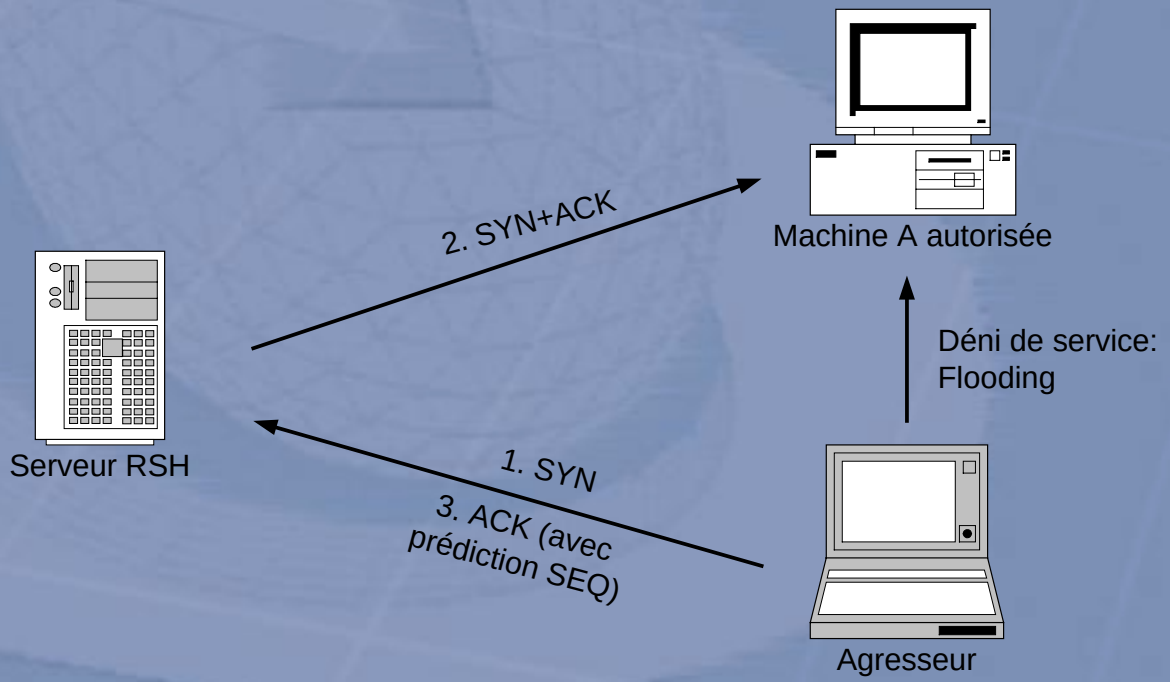
- Exemple d'utilisation de sniffer (sniffer pcs sous Solaris):

```
---
PATH: intra.Secway-int.net(2611) => gaia.Secway-int.net(ftp)
DATE: Wed Mar  7 03:55:25 2001

USER bob
PASS m0nP4sS
SYST
PASV
LIST
CWD /tmp
PASV
LIST
QUIT
[CLOSED]
```

Usurpation d'identité (5)

- Abus de Trust relationships
  - IP blind Spoofing
    - Popularisé par le pirate Kevin Mitnick
    - Attaque contre les r-services BSD (ie: rlogin/rsh)
    - Ces r-services se basent uniquement sur l'adresse IP pour authentifier un utilisateur
    - Si un pirate arrive à se faire passer pour l'IP autorisée, il peut exécuter des commandes sur la cible

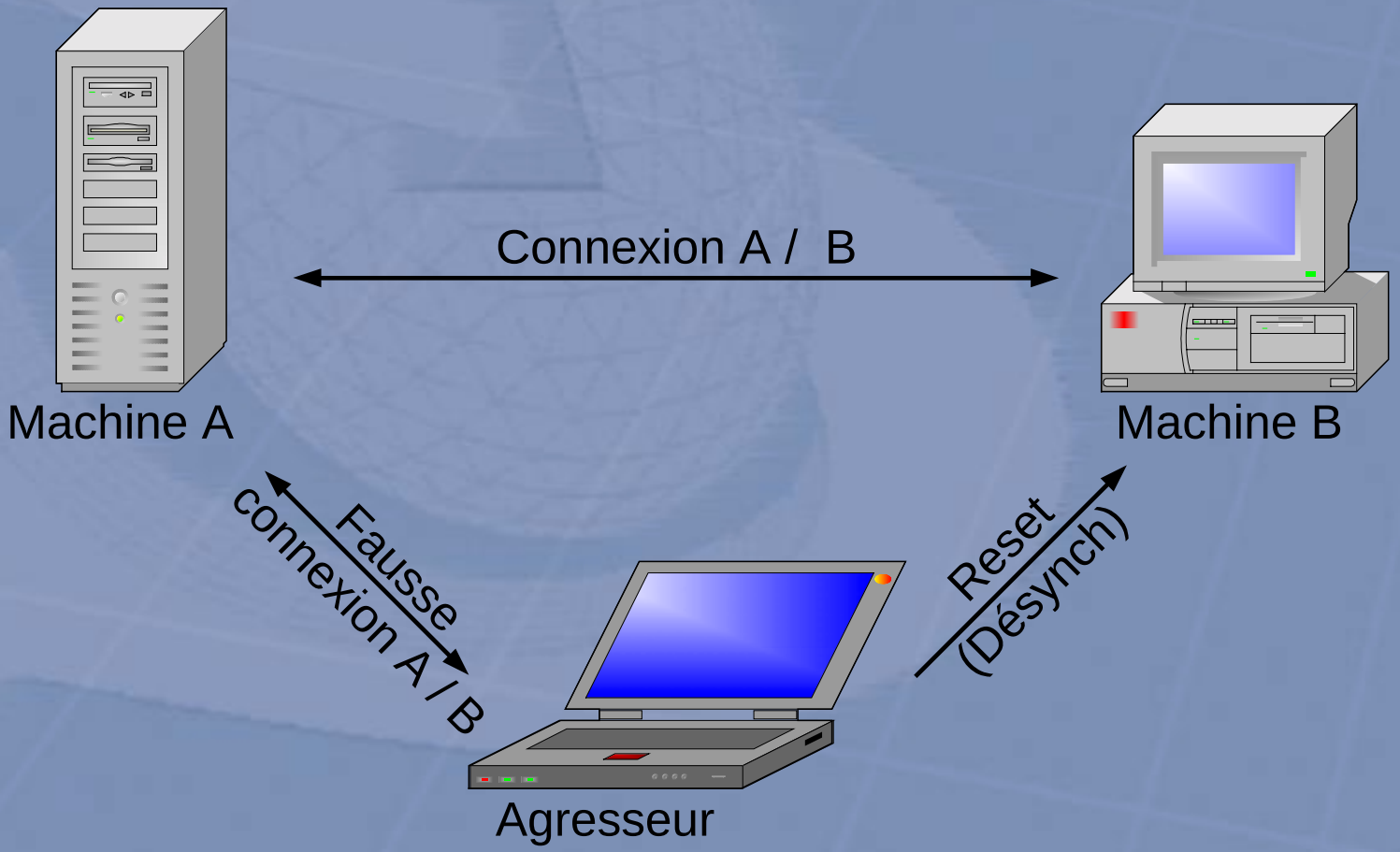
Usurpation d'identité (6)



Usurpation d'identité (7)

- Interception Man-in-the-Middle
  - Agresseur situé (topologiquement) entre deux machines échangeant un flux
  - L'agresseur intercepte le flux, et y insère ses propres données
  - Par exemple: interception de sessions telnet entre 2 machines

Usurpation d'identité (8)



Finalisation de l'exploitation

- Elévation des privilèges: vers root ou SYSTEM
  - Souvent directement le cas
  - Sinon, *exploit* local

Progression

Inspection des machines

- Inspection de la machine
  - Simulation du comportement d'un utilisateur légitime
  - Recherche des fichiers journaux et des copies vers d'autres machines
  - Identification des HIDS/NIDS

Progression (2)

- Nettoyage des traces
  - Pas possible dans tous les cas (Tripwire, backups, ...)
  - Nécessite potentiellement la compromission d'autres machines (serveurs de logs)

Progression (3)
Backdoors

- Intérêts
  - Revenir plus facilement
  - Tromper les systèmes de surveillance
  - Introduire des *covert channels*
- Types
  - Rootkits
  - Backdoors kernel
  - Programmes dissimulés
  - Changements de configuration

Progression (4)

- Prise d'information
  - Repérer les données ciblées
  - Recommencer la phase d'exploitation puis progression
  - Jusqu'à trouver l'information
  - La rapatrier en utilisant un *covert channel*

Conclusion

- L'intrusion sur Internet
  - Des techniques et stratégies complexes
  - A la portée de tous grâce aux outils publics
- La protection
  - Contre-mesures et réactions en conséquence !

Annexes et références

- NMAP: http://www.insecure.org/nmap/
- Firewalk: http://www.packetfactory.net/projects/firewalk/
- Securityfocus, Bugtraq: http://www.securityfocus.org/
- PacketStorm: http://www.packetstormsecurity.com/
- SANS: http://www.sans.org/
- Thomas Lopatic, Dataprotect AG