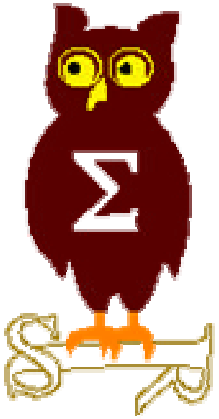
EdelWeb

OSSIR
Groupe Sécurité Windows

Présentation de la base OSWIN

Nicolas RUFF

nicolas.ruff@edelweb.fr



Base OSWIN
Plan

- Introduction
  - Historique
- Sécurisation du serveur
  - Réseau
  - Windows 2000
  - IIS 5.0
  - Application
- Présentation de la base
  - Objectifs
  - Présentation interactive
  - Avenir
- Questions

Base OSWIN
Introduction

- **Historique de la base**
  - Développée initialement par Mathieu DONZEL sous le nom "Demesis"
  - Base multi-rôles (cf. présentation)
    - Vulnérabilités NT4/2000, Exchange, SQL, etc.
    - Guides de configuration et de sécurisation
    - News concernant la sécurité
    - Etc.
  - Arrêt des mises à jour en oct. 2001
  - Don à l'OSSIR en 2002

- **Reprise de la base**
  - Appel d'offres de l'OSSIR
  - Reprise et hébergement par EdelWeb
  - Alimentation :
    - Réunions mensuelles
    - CERT-IST (contributeur)

Base OSWIN
Sécurisation serveur

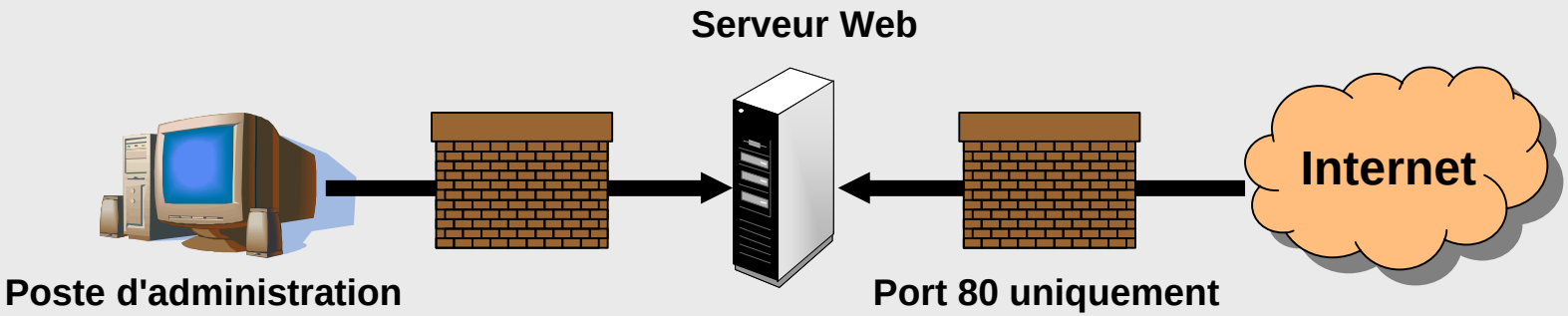
EdelWeb

- **Configuration matérielle**
  - Serveur DELL Poweredge 350
    - Celeron 850 MHz
    - 1 Go RAM
- **Configuration logicielle**
  - Windows 2000 Serveur
    - 2 disques 80 Go en RAID logiciel
    - 3 partitions NTFS : système, serveur Web, logs
  - Base Access 2000
  - Serveur IIS 5.0 + pages ASP

Base OSWIN
Sécurisation serveur

EdelWeb

- **Sécurisation réseau**
  - Schéma "classique"
    - Firewalls en "diodes"
  - Pas de "reverse proxy"
    - Peu de saisies utilisateur
    - Aucune donnée "confidentielle" sur le serveur



Base OSWIN
Sécurisation serveur

EdelWeb

- **Sécurisation Windows**
  - Installation minimale
    - Répertoire et lettre de lecteur non "standard"
  - Arrêt des services inutiles
  - "Options de sécurité" au maximum
    - Machine en WORKGROUP
    - Aucune communication réseau nécessaire
    - Renommage des comptes admin et invité
  - Autres options de sécurité positionnées
    - Sessions nulles interdites
    - Partages administratifs désactivés
    - Protection contre "SYN Flood"
    - Etc.
  - Derniers SP et Hotfixes appliqués
    - Par acquis de conscience ☺

Base OSWIN
Sécurisation serveur

EdelWeb

- **Sécurisation IIS 5.0 (1/2)**
  - Installation minimale
    - Suppression des exemples et des répertoires inutilisés
  - Désactivation des mappings inutilisés (sauf .ASP)
  - Configuration restrictive
    - Pas de "parent path"
    - Message de déboguage simplifiés
    - Droits "write" et "directory browsing" enlevés
  - Journal d'audit
    - Pour le moment, fichier texte local
    - Exploitation par Access

Base OSWIN
Sécurisation serveur

EdelWeb

- **Sécurisation IIS 5.0 (2/2)**
  - **URLScan**
    - **UseAllowVerbs=1**
      - **Allow GET, POST**
    - **UseAllowExtensions=1**
      - **Allow .asp, .asa, .htm, .html, .txt, .jpg, .jpeg, .gif**
    - **NormalizeUrlBeforeScan=1**
    - **VerifyNormalization=1**
    - **AllowHighBitCharacters=0**
    - **AllowDotInPath=0**
    - **RemoveServerHeader=0**
      - **Mais AlternateServerName="OSSIR Web Server 1.0"**
    - **EnableLogging=1**
    - **PerProcessLogging=0**
    - **AllowLateScanning=0**
    - **PerDayLogging=1**
    - **RejectResponseUrl=/<Rejected-by-UrlScan>**
    - **UseFastPathReject=0**
  - **+ Deny**
    - **Translate: If: Lock-Token:**
    - **.. ./ \ : % &**

Base OSWIN
Sécurisation serveur

- **Sécurisation applicative**
  - Ensemble du site en "lecture seule"
  - Lutte contre l'injection de code
    - Filtrage "aggressif" sur toutes les entrées utilisateur
      - < > " ' % ; ( ) & + - * : ,
    - Remarques
      - Bien que développé par un professionnel de la sécurité, le code initial était complètement bogué !
      - Pas de risque de vol de session (aucune authentification)
      - Risque d'injection SQL
  - Lutte contre le spam
    - Adresses email dynamiques
      - document.write('<a href=\"mailto:' + x + '@' + y + '\">');

Base OSWIN
Présentation de la base

EdelWeb

- **Objectifs**
  - **Offrir des ressources autour de la sécurité des systèmes Windows**
    - **Système d'exploitation et logiciels Microsoft les plus utilisés**

- **Organisation**
  - **Leviers de sécurité**
    - **Recherche par objectif ou par mécanisme technique (cf. ci-dessous)**
  - **Mécanisme de sécurité**
  - **Vulnérabilités**
    - **Liste des vulnérabilités par produit et niveau de service pack**
    - **Couvre les bulletins de sécurité MS mais aussi les travaux du groupe**
  - **Correctifs**
  - **Sites (relatifs à la sécurité)**
  - **News (sécurité)**

Base OSWIN
Présentation de la base

EdelWeb

- **Démo**

- **Avenir**
  - **Alimentation en vulnérabilités après chaque réunion**
  - **Améliorations diverses**
    - **Prise en compte de XP et 2003**
    - **"Nettoyage" de la base existante**
    - **Amélioration de l'ergonomie de l'outil de saisie**
  - **Par contre les autres rubriques demandent un travail considérable en alimentation …**

Base OSWIN
Présentation de la base

- **Statistiques d'utilisation (15/04/2003 -> 24/09/2003)**
  - **263 adresses IP servies**
    - **39 consultations**
    - **224 attaques …**
  - **"User Agents"**
    - **1 seul compte par adresse IP**
    - **Toutes versions confondues**
    - **Lorsque précisé le navigateur**
    - **Référence : http://www.psychedelix.com/agents1.html**
    - **Résultats**
      - **"Microsoft-WebDAV-MiniRedir/5.1.2600" : 4**
      - **IE : 7**
      - **Netscape / Mozilla / FireBird / Galeon : 15**
      - **Opera : 3**
      - **Falsifiés : 4**
        - **"Mozilla/3.0" : 3**
        - **"Internet Explorer 4.01" : 1**

Base OSWIN
Présentation de la base

EdelWeb

- Attaques remarquables
  - /default.asp
  - /galaxy_2096.2442
  - /help/us/ysearch/
  - /pr.php
  - /proxy/proxychecker/results.htm
  - /scripts/nsiislog.dll
  - /<Rejected-By-UrlScan>
    - Received a malformed request which resulted in error 50 while modifying the 'Server' header
    - Sent verb 'CONNECT'
    - Sent verb 'get'
    - Sent verb 'OPTIONS'
    - Sent verb 'PUT'
    - Sent verb 'SEARCH'
    - Sent verb 'TRACE'
    - '/c/winnt/system32/cmd.exe'
    - '/d/winnt/system32/cmd.exe'
    - '/MSADC/root.exe'
    - '/scripts/..%c0%2f../winnt/system32/cmd.exe'
    - '/scripts/..%c0%af../winnt/system32/cmd.exe'
    - '/scripts/..%c1%9c../winnt/system32/cmd.exe'
    - '/scripts/root.exe'

Base OSWIN
Présentation de la base

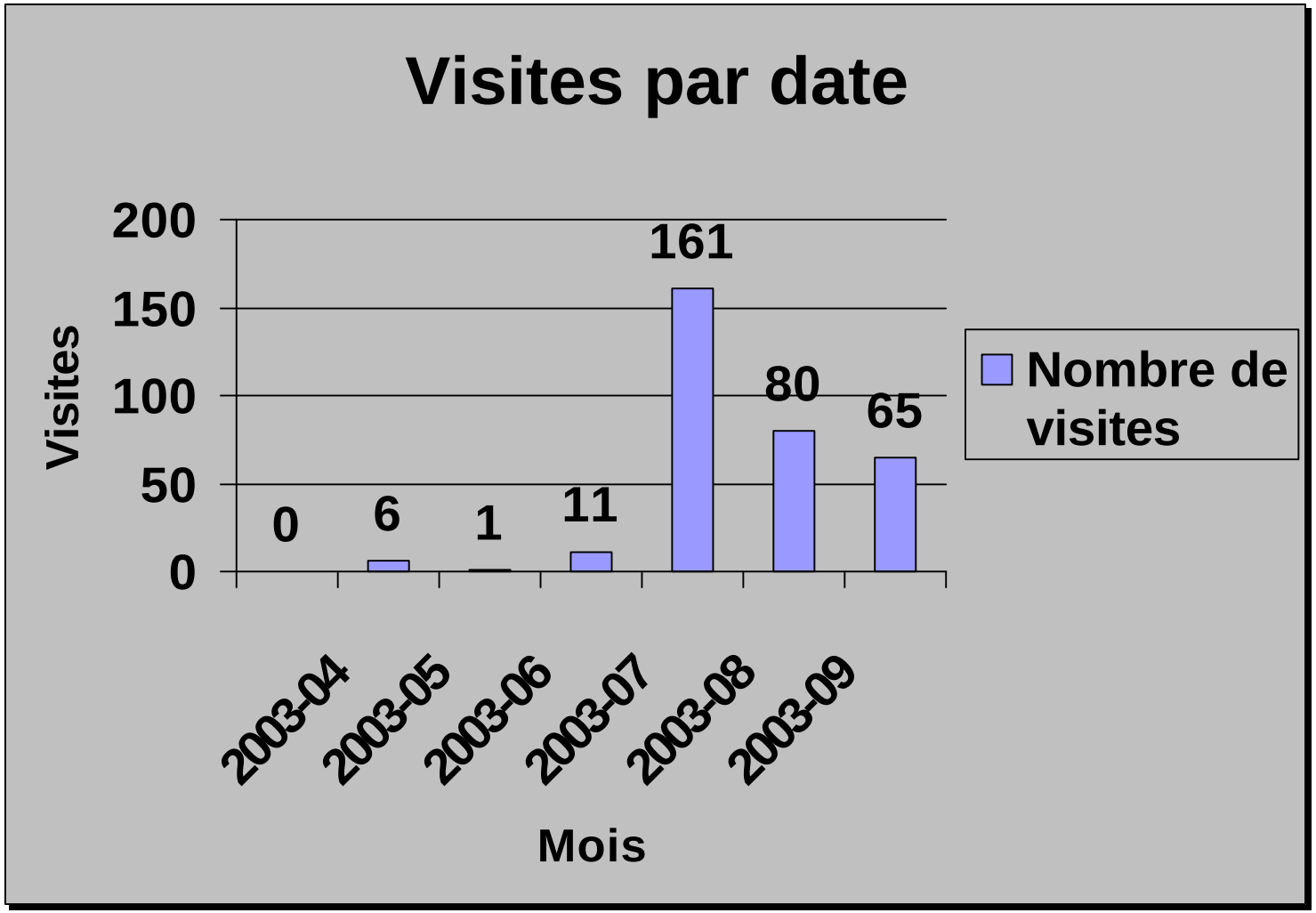
EdelWeb

- '/default.ida'
- '/error/%5c%2e%2e%5clogs%5cinstall.log'
- '/NULL.printer'

- '/scripts/..%c1%1c../winnt/system32/cmd.exe'
- '/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe'
- '/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe'
- '/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe'
- '/scripts/.%252e/.%252e/winnt/system32/cmd.exe'
- '/scripts/..%%35%63../winnt/system32/cmd.exe'
- '/scripts/..%%35c../winnt/system32/cmd.exe'
- '/scripts/..%25%35%63../winnt/system32/cmd.exe'
- '/scripts/..%252f../winnt/system32/cmd.exe'
- '/scripts/..%255c%255c../winnt/system32/cmd.exe'
- '/scripts/..%255c../winnt/system32/cmd.exe'

Base OSWIN
Présentation de la base

EdelWeb



Questions / réponses

EdelWeb

- Questions / réponses