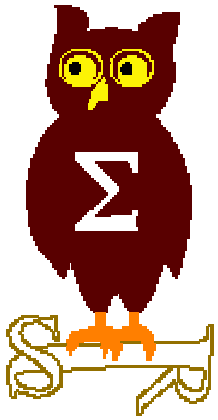
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 10 septembre 2001
La sécurité IP avec Windows 2000



Ordre du jour

- Présentation d'ISA Server
  - Patrick CHAMBET
- Présentation de M>Tunnel et M>Manager (MatraNet)
  - Stéphane SOLIER
- Revue des dernières vulnérabilités de Windows 2000 (EdelWeb)
  - Nicolas RUFF
- Débat autour de la rédaction d'un guide de sécurisation Windows 2000 par le groupe
- Informations diverses et vie de la liste

Présentation d'ISA Server

Patrick CHAMBET

patrick.chambet@edelweb.fr

Durée : 30 minutes

M>Tunnel et M>Manager

Stéphane SOLIER
solier@matranet.com

Durée : 45 minutes

EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Durée : 30 minutes

Avis de sécurité Microsoft (1/2)

- **Depuis le 11/06/2001 :**
  - **MS01-030 v3 : Exécution de scripts dans le webmail Exchange 5.5 et 2000 – erreur dans le correctif**
  - **MS01-032 : Réutilisation du cache de connexion SQL Server 7 et 2000**
  - **MS01-033 : Vulnérabilité dans IDQ.DLL (IIS 4 et 5)**
  - **MS01-034 : Ouverture de macros sans confirmation dans Word**
  - **MS01-035 : Débordement de buffer dans le connecteur FrontPage – Visual Studio**
  - **MS01-036 : Changement de mots de passe par LDAP/SSL**
  - **MS01-037 : Erreur d'authentification permettant le relaying avec le serveur SMTP standard de Windows 2000**
  - **MS01-038 : Contrôle Outlook « View » non sûr**
  - **MS01-039 : Les services Telnet et NFS du SFU contiennent des fuites mémoire**
  - **MS01-040 : Fuite mémoire dans Terminal Server**
  - **MS01-041 : Déni de service sur les services RPC**

Avis de sécurité Microsoft (2/2)

- MS01-042 : Débordement de buffer dans Windows Media Player (fichiers .NSC)
- MS01-043 : Fuite mémoire dans NNTP
- MS01-044 : Patch cumulatif pour IIS (corrige 5 dénis de service supplémentaires)
- MS01-045 : Fuite mémoire dans le module H.323 pour ISA Server
- MS01-046 : Redémarrage de Windows 2000 par un paquet IrDA malformé

- Code Red
  - Exploite la vulnérabilité MS01-033
  - Déni de service distribué tous les 20 du mois vers « whitehouse.gov »
  - Signature : /default.ida?NNN
- Code Red II
  - Offre une console SYSTEM accessible dans /scripts/root.exe
  - Effets de bord : déni de service dans IIS et routeurs CISCO
  - /default.ida?XXX

Autres sources

- Non détection des caractères Unicode « %u » par les IDS les plus courants (eEye)
- Le SP3 pour Windows 2000 en beta-test
- Des nouvelles de Windows XP :
  - Une sortie retardée par le ministère de la justice ?
  - La technologie Microsoft « anti piratage » cassée
- Recrudescence des vers et des virus (CERT/CC)
  - Attaques dirigées vers les « home users »
  - Sircam, W32/Leaves (trojan)
  - Cod Red, BSD telnetd, Solaris in.lpd, …
- Vulnérabilités WireLess (802.11)

Rédaction d'un guide de sécurisation Windows 2000

Groupe Sécurité Windows

Durée : 30 minutes

Présentation

EdelWeb

- **Objectifs**
  - Créer un document de référence en français
  - Contribuer à la notoriété du groupe
- **Réalisation**
  - Sources : documents existants, expérience des participants
  - Rédaction partielle du guide lors de chaque réunion
- **Méthodes proposées**
  - Reformulation d'un guide existant
  - Enrichissement d'un guide existant avec les commentaires des participants
- **Délai**
  - Sortie du guide en mai 2002

Documents existants (1/3)

- **Windows NT4 DC Configuration Checklist**
  http://www.microsoft.com/TechNet/itsolutions/security/tools/dccklst.asp
  - **Éditeur : Microsoft**
  - **Langue : anglais, français**
  - **Coût : gratuit**
  - **Avis : complet mais pas d'impacts, pas d'équivalent pour Windows 2000**

- **« Securing Windows 2000 »**
  http://www.sansstore.org/
  - **Éditeur : SANS**
  - **Langue : anglais**
  - **Coût : $49 pour la version papier, $1800 pour la version électronique sans limite de licence**
  - **Avis : très complet, avec commentaires**

Documents existants (2/3)

- « Hardening Windows 2000 » - Windows 2000 Security HandBook
  http://www.systemexperts.com/literature.html
  - Éditeur : System Experts
  - Langue : anglais
  - Coût : gratuit
  - Avis : quelques clés « rares », comme les paramètres TCP/IP, mais incomplet

- NSA
  http://nsa2.www.conxion.com/win2k/download.htm
  - Éditeur : NSA
  - Langue : anglais
  - Coût : gratuit
  - Avis : très volumineux (17 guides), pratique (fichiers de configuration fournis)

Documents existants (3/3)

EdelWeb

- **Demesis**
  http://www.demesis.com/
  - **Éditeur : Mathieu DONZEL**
  - **Langue : français**
  - **Coût : gratuit**
  - **Avis : une base de vulnérabilités avec correctifs et impacts, mais pas un « guide de sécurisation »**

- **Et bien d'autres …**

Questions / réponses

EdelWeb

- Thèmes proposés pour la prochaine réunion :
  - IP / IPSec par HSC
  - Stratégies de groupe
  - Active Directory
  - Présentation du site Demesis
- Date :
  8 octobre 2001
- Questions / réponses