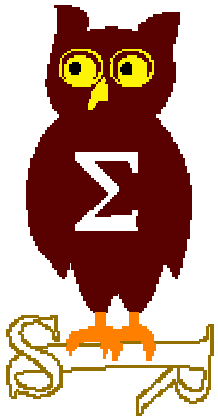
OSSIR

Groupe SWNT

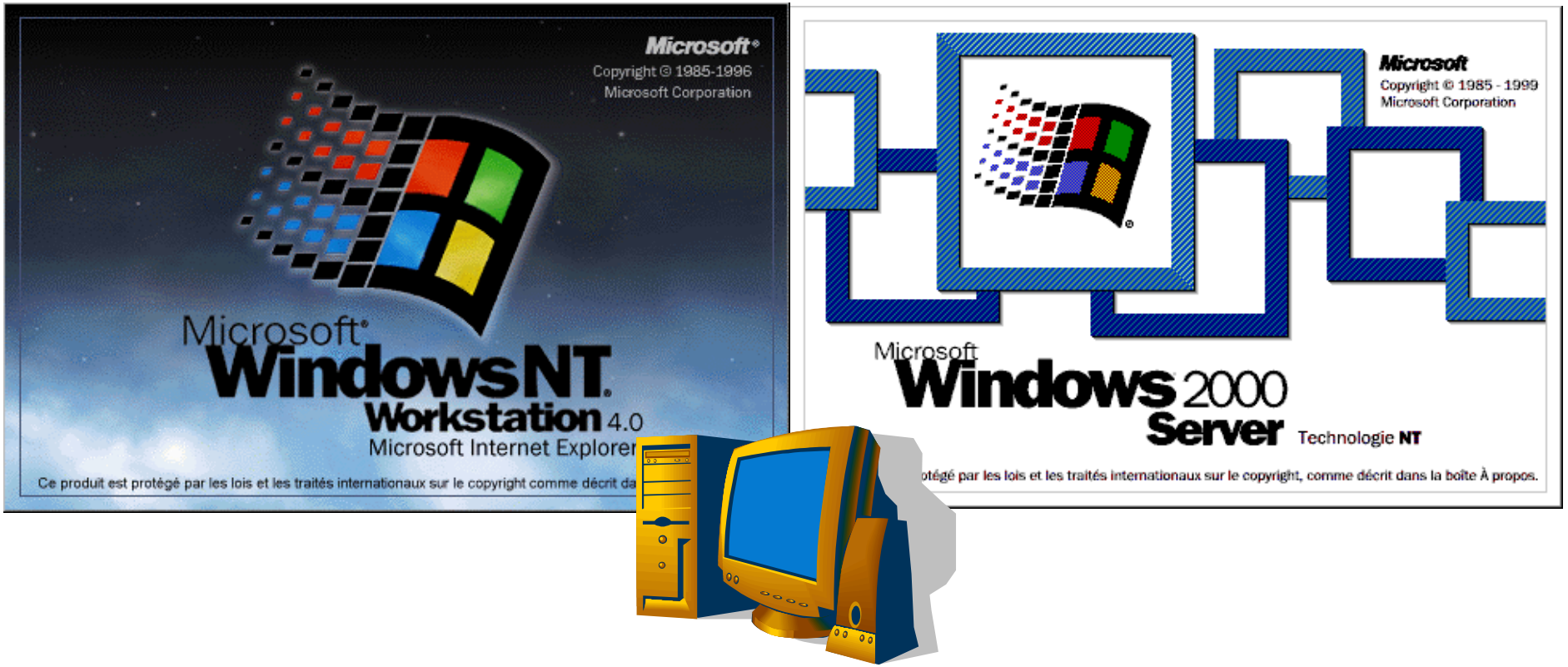
Réunion du 2 avril 2001



Ordre du jour

1. **Modalités 2001 *(30')***
2. **Présentation de la sécurité Windows 2000 *(1h)***
3. **Présentation des produits *(2x45')***
   - **Event Log Monitor (TNT Software)**
   - **LogCaster (RippleTech)**
4. **Revue des vulnérabilités majeures de Windows 2000 *(30')***
5. **Point sur la liste de diffusion et prochaine réunion**

1. Le groupe de travail Sécurité Windows



1. Le groupe de travail Sécurité Windows

- Objectifs 2001
- Calendrier 2001
- Contenu des réunions / suggestions
- Choix des thèmes

1. Le groupe de travail Sécurité Windows

Objectifs 2001

- **Ce qui a changé :**
  - Tous les participants ont une expérience NT4
  - NT4 est voué à disparaître
- **Proposition d'objectifs pour 2001 :**
  - Se former à Windows 2000
    - Nouvelles fonctionnalités de sécurité
    - Impact des outils tiers sur la sécurité
    - Interopérabilité Windows et autres
  - Mutualiser les expériences notamment concernant la migration
  - Répertorier les vulnérabilités et les correctifs
  - Changer le nom du groupe
  - Relancer le site Web (http://www.ossir.org/)

1. Le groupe de travail Sécurité Windows

Calendrier 2001

- **Fréquence : réunions mensuelles *(à valider)***
- **Durée : 3 h *(à valider)***
- **Thèmes proposés :**
  - **Mai : EFS et produits de chiffrement**
  - **Juin : PCAnywhere**
  - **Juillet : Active Directory**
- **Intervenants**
- **Suggestions**

1. Le groupe de travail Sécurité Windows

Contenu des réunions

Proposition d'ordre du jour standard :

- **Retour d'expérience *(environ 1h)***
- **Présentation de produits *(environ 2h)***
- **Revue des nouvelles vulnérabilités**
- **Point sur la liste de diffusion (nt-securite)**
  - **Volume : environ 10 messages par semaine**
  - **Exemple de sujets abordés :**
    - **Sécurité SQL Server 7**
    - **Interopérabilité Kerberos 5**
    - **Firewall sous NT**
    - **…**
- **Validation du programme de la réunion suivante**

1. Le groupe de travail Sécurité Windows

Proposition de thèmes (1/2)

- Accès RAS
- (*) *Active Directory (sécurité, interopérabilité)*
- Administration
- Authentification (Kerberos, SmartCard, biométrie)
- Clustering et haute disponibilité
- (*) *Conception d'architectures (domaines, sites, DNS)*
- Déploiement / migration
- PKI
- (*) *Protection des DLLs (WFP)*
- Sauvegarde et restauration
- Sécurité réseau et protocoles (IPSec, NetBIOS)
- (*) *Stratégies et groupes de sécurité (GPO, SCTS)*
- (*) *Système de fichiers (EFS ; éventuellement quotas, DFS, LDM)*
- Terminal Server

(*) Thèmes pouvant être traités par EdelWeb

1. Le groupe de travail Sécurité Windows

Proposition de thèmes (2/2)

Thèmes adjacents à Windows 2000 :

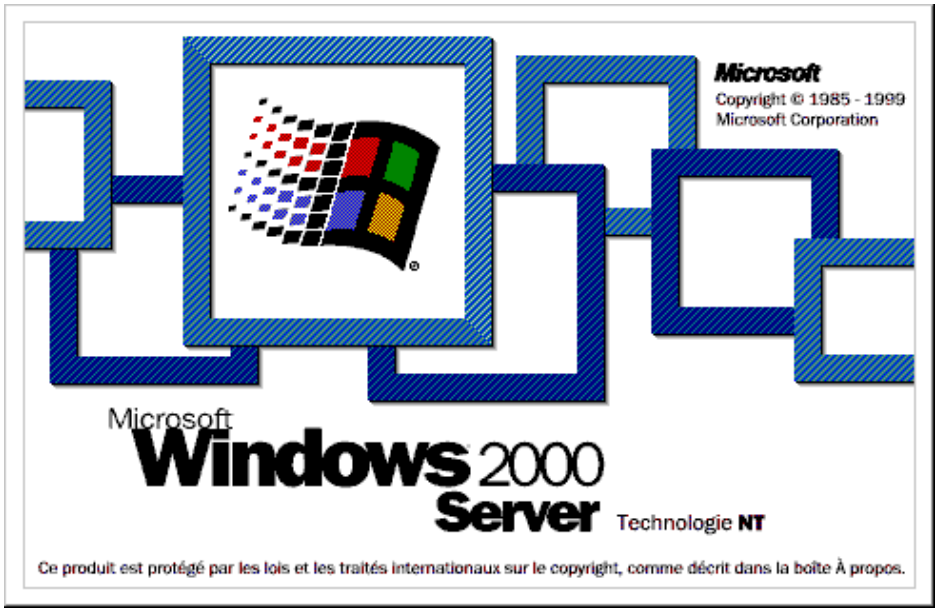
- **Exchange 2000**
- **Exploitation du kit de ressources techniques**
- **(*) *IIS 5.0***
- **(*) *ISA Server***
- **(*) *Logiciels antivirus (Norton, McAfee)***
- **(*) *PCAnywhere***
- **Le service de multidiffusion Windows Media**
- **Les améliorations de Windows XP (ex-Whistler)**
  - **DLLs côte-à-côte**
  - **Sessions persistantes**
  - **Remote Desktop (Terminal Server Personal Edition)**
  - **Intégration du méta-annuaire VIA (ZoomIt Corp.)**

(*) Thèmes pouvant être traités par EdelWeb

2. Présentation de la sécurité Windows 2000

Par Nicolas RUFF (EdelWeb SA)

nicolas.ruff@edelweb.fr



2. Présentation de la sécurité W2K

2.1 Windows 2000 en quelques mots

2.2 Revue des fonctions de sécurité

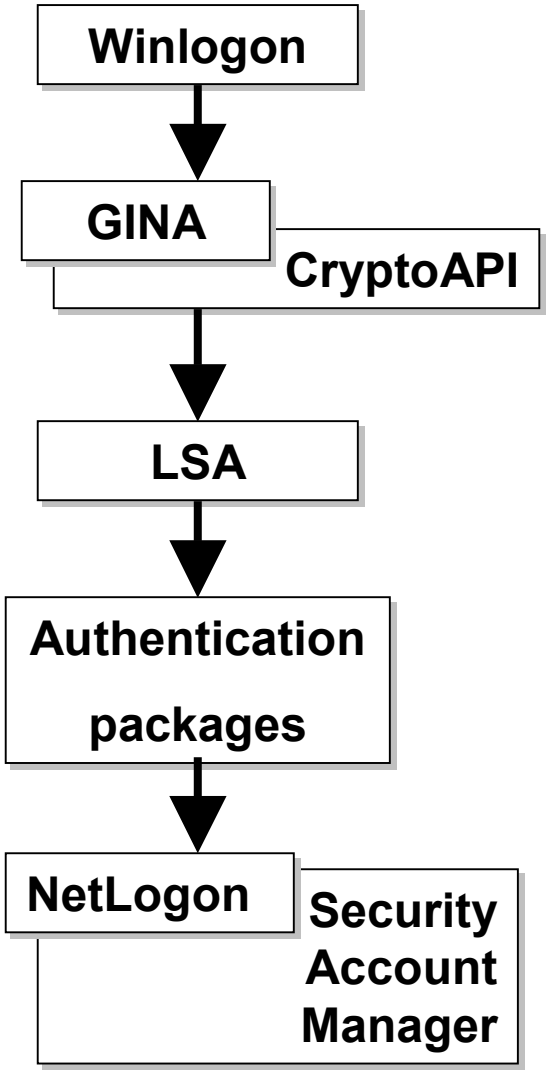
2.3 Écueils

2.4 Journalisation

2. Présentation de la sécurité W2K

2.1 L'héritage de NT4

- L'identification des objets (SID)
- L'accès sécurisé aux fichiers (NTFS)
  - = DACL, SACL
  - + Héritage des permissions
- La génération de traces
  - Toujours pas de télécollecte
- La base de registre
  - Apparition du répertoire « Documents & Settings »
  - Stocke les profils utilisateurs, les préférences, etc.
- Le noyau de sécurité
  - Kerberos est implémenté sous forme d'authentication package supplémentaire
  - La GINA doit être modifiée pour chaque type de SmartCard (JavaCard, ISO-7816, …)



2. Présentation de la sécurité W2K

2.1 Les nouveautés (1/3)

- Windows 2000 intègre les Service Packs (jusqu'au SP6a), les hotfixes et l'Option Pack de NT 4.0
  - Outils intégrés en standard :
    - Terminal Server
    - Moniteur réseau
    - MMC
- Un service d'annuaire LDAP (Active Directory)
- Nouveaux objets système
  - Groupes de sécurité locaux au domaine et universels
  - Stratégies de groupe regroupant toutes les stratégies de sécurité
- Nouveaux outils d'administration
  - Gestionnaire d'ordinateur (outil d'administration unique)
  - SCTS (ex-SCE)
  - RunAs (permet d'exécuter une application dans le contexte d'un autre utilisateur)
- Interface MMC commune à tous les outils

2. Présentation de la sécurité W2K

2.1 Les nouveautés (2/3)

- **Nouvelles propriétés du système**
  - **Droits plus granulaires**
    - **Existence d'un contrôle d'accès au niveau attribut sur les objets LDAP**
    - **MAIS probablement incompatible avec la plupart des outils d'administration (d'après Microsoft)**
  - **Délégation d'administration**
    - **Peu exploitable en pratique car non tracé et absence de fonction inverse**
- **Nouveaux protocoles**
  - **Mode d'authentification natif : Kerberos v5 (interopérabilité ?)**
  - **IPSEC**
  - **Pour les accès distants : PPTP, L2TP, RADIUS**
- **Structure logique du domaine décorrélée de la structure physique**
  - **Unités Organisationnelles (UO)**
- **NTFS v5**
  - **Encrypted File System (EFS)**
  - **Quotas, volumes dynamiques, points de montage**

2. Présentation de la sécurité W2K

2.1 Les nouveautés (3/3)

- **Protection du système améliorée**
  - Les DLL système et applications sont disjointes (WFP)
    - Gestion des versions pas aussi élaborée que dans le futur Windows XP
  - Permissions d'accès par défaut renforcées
    - Utilisateur NT4 = Utilisateur avec pouvoir dans Windows 2000
    - Les clés Run, Debugger, Uninstall sont mieux protégées
    - « Tout le monde » n'a pas « contrôle total » sur C:\WINNT
    - L'utilisateur n'a pas « contrôle total » sur HKCU
- **PKI**
  - Intégrée de manière native au système
  - Requise par IPSEC, Kerberos et EFS
    - Attention à la mise en œuvre des agents de recouvrement EFS qui requiert l'existence d'une autorité racine d'entreprise
  - Support SmartCard pour l'authentification et la gestion des certificats
- **« Look & Feel » Windows 9x**
  - Interface plus intuitive (ex. ajout/suppression de périphériques avec détection automatique des nouveaux périphériques)
  - Interface d'administration unique et personnalisable

2. Présentation de la sécurité W2K

2.2 Structure des domaines

- **Plusieurs niveaux de structuration**
  - **Structures logiques**
    - **Les domaines**
    - **Les unités organisationnelles (UO)**
    - **Les groupes**
  - **Structure physique**
    - **Les sites**
      - **Description de la topologie du réseau et des coûts de transmission**
      - **Description manuelle, indépendante des tables de routage**
- **Attention ! Par rapport à NT4, des termes identiques peuvent parfois désigner des concepts différents**
  - **Les domaines**
    - **Sont basés sur la hiérarchie DNS**
  - **Les groupes**
    - **De nouveaux groupes : locaux au domaine, universels**
    - **Un nouveau type : le groupe de distribution**
  - **Contrôleurs de domaine**
    - **Plus de relation maître/esclave**
    - **Réplication multi-maîtres**

– Réplication multi-maîtres

2. Présentation de la sécurité W2K

2.2 Active Directory (1/3)

- **Qu'est-ce que Active Directory ?**
  - Un annuaire des objets système, accessible par LDAP
  - Disponible obligatoirement et exclusivement sur les contrôleurs de domaine
  - Un annuaire extensible
    - Seuls ISA Server et Exchange 2000 exploitent cette possibilité
  - Sera probablement intégré au méta-annuaire de Windows XP
- **A quoi sert Active Directory ?**
  - Recense les objets système
  - Centralise de la gestion de la forêt (y compris la sécurité)
  - Participe à l'authentification des utilisateurs

Remarque : il existe toujours une base de registre et une SAM sur toutes les machines

2. Présentation de la sécurité W2K

2.2 Active Directory (2/3)

- **Que contient Active Directory ?**
  - **Les objets systèmes**
    - **Stratégies de sécurité**
    - **Unités Organisationnelles**
    - **Groupes universels**
    - **Profils utilisateur**
    - **Certificats**
  - **Les objets étendus (annuaire Exchange, etc.)**
  - **Le schéma (= description des objets Active Directory)**
- **Comment fonctionne Active Directory ?**
  - **Basé sur un moteur Exchange (ESE)**
  - **Un fichier NTDS.DIT sur chaque contrôleur de domaine d'environ 200 à 300 Mo pour 10.000 utilisateurs (estimation)**
  - **Synchronisation des données entre contrôleurs de domaine**
    - **Réplication différentielle dans un domaine ou complète entre domaines**
    - **Paramétrable (planning, périodicité, mécanismes : IP, RPC, SMTP)**
  - **Au moins un serveur de catalogue global par domaine, dont le rôle est d'indexer le contenu des autres catalogues de domaine**

2. Présentation de la sécurité W2K

2.2 Active Directory (3/3)

- **Sécurité d'Active Directory**
  - ACLs au niveau attribut sur les objets
  - Héritage des ACLs
  - Les ACLs sur les objets ne sont pas les ACLs sur leur représentation dans AD
- **Les points faibles**
  - Volume de réplication important
    - Compter environ 200-300 Mo pour 10.000 utilisateurs dans une entreprise
    - Réplication toutes les 3 minutes en intra-site (par défaut)
    - Réplication toutes les 3 heures en inter-site (par défaut)
  - Sécurité et robustesse des mécanismes de réplication : inconnu
    - RPC, IP ou SMTP
  - Le contrôle d'accès au niveau attribut peut engendrer des problèmes avec les services système et les outils d'administration

2. Présentation de la sécurité W2K

2.2 Stratégies de sécurité (1/2)

- Stratégies « classiques »
  - Comptes
  - Droits
  - Audit
- Stratégies apparues avec Windows 2000
  - Options de sécurité
    - Personnalisables
    - Permettent de positionner des clés de la base de registre
  - Paramètres du journal des évènements
  - Groupes restreints
  - Services système
  - Registre
  - Système de fichiers
  - Stratégies de clé publique
  - Stratégies de sécurité IP
- Objets « Stratégies de groupe » (Group Policy Objects)
  - S'appliquent à une machine, un utilisateur ou une UO

2. Présentation de la sécurité W2K

2.2 Stratégies de sécurité (2/2)

- **Nouveautés**
  - Héritage des stratégies
  - Chargées au moment du boot / du logon
  - Rafraîchies périodiquement (toutes les 90 minutes par défaut)
- **Ordre d'application des stratégies**
  1. Stratégies NT 4.0 (NTConfig.pol)
  2. Stratégie locale
  3. Stratégies de site
  4. Stratégies de domaine
  5. Stratégies d'UO
- **Règles d'application**
  - Les dernières stratégies écrasent les premières
  - Les stratégies les plus restrictives sont appliquées lors de l'héritage
  - Utiliser l'outil du Kit de Ressources Techniques GPRESULT pour vérifier le résultat de l'application des stratégies

2. Présentation de la sécurité W2K

2.3 Écueils

- **Richesse fonctionnelle**
  - Active Directory et méta-annuaires : mise en œuvre ?
  - Kerberos : interopérabilité avec Unix ?
  - EFS : quelle stratégie de recouvrement ?
  - PKI : exploitable dans des outils tiers ?
- **Migration de l'architecture**
  - Multi-domaines vs. modèle « plat » avec UO
  - Certains choix sont irréversibles
    - Suppression de domaines
- **Migration**
  - Mode mixte vs. mode natif
  - Migration des applications
    - Protection renforcée des clés de la base de registre
    - Utiliser l'outil du Kit de Ressources Techniques : APCOMPAT
- **Stabilité du système**
  - Des améliorations notables par rapport à NT4
  - Peu de retour d'expérience

2. Présentation de la sécurité W2K

2.4 Les différents journaux

- **Journal sécurité**
  - Consigne les messages issus des stratégies d'audit
  - Par défaut, seuls les processus système ont le droit d'écriture dans ce journal
- **Journal système**
  - Consigne les messages issus des processus non interactifs
  - Tous les processus ont le droit d'écrire dans ce journal
- **Journal application**
  - Consigne les messages issus des applications
  - Tous les processus ont le droit d'écrire dans ce journal
- **Journaux spécialisés**
  - « Directory Service » (activité du moteur Active Directory)
  - « DNS Server »
  - Service de réplication de fichiers

2. Présentation de la sécurité W2K

2.4 Les stratégies d'audit

	NT4	2000
Gestion des comptes	X	X
Accès au service d'annuaire		X
Accès aux objets	X	X
Suivi de processus	X	X
Évènements de connexion		X
Évènements de connexion aux comptes (Ouverture et fermeture de session)	X	X
Évènements système	X	X
Modifications de stratégie	X	X
Utilisation des privilèges	X	X

2. Présentation de la sécurité W2K

2.4 Exploitation des journaux (1/4)

- Une masse d'information importante :
  - 6 journaux
  - 9 stratégies d'audit
- Les journaux doivent être :
  - Remontés
  - Archivés
  - Purgés
  - Protégés
  - Consolidés
  - Analysés
  - Déclencher des alertes

2. Présentation de la sécurité W2K

2.4 Exploitation des journaux (2/4)

- **Remontée**
  - Chaque station et chaque serveur d'applications possède ses propres journaux
  - Les contrôleurs de domaine partagent des entrées de journalisation communes : évènement « connexion à un compte de domaine »
  - Les outils livrés avec Windows 2000 ne sont pas suffisants
- **Archivage / Purge**
  - Stratégie de rotation du journal
    - Effacer le journal / arrêter la journalisation : risque de perte d'information
    - Arrêter le système : risque de déni de service
  - Par défaut la taille des journaux se situe autour de 256 Ko
  - Le journal de sécurité a une limite théorique de 4 Go

2. Présentation de la sécurité W2K

2.4 Exploitation des journaux (3/4)

- **Protection**
  - Les actions d'un administrateur malveillant sont difficilement traçables
  - Utilitaire WinZapper permettant d'effacer des lignes du journal (Pas de chaînage d'intégrité)
  - Les règles de journalisation doivent elles aussi être protégées et surveillées
- **Consolidation des journaux / Analyse**
  - Les outils livrés avec Windows 2000 ne sont pas suffisants
    - CyberSafe Log Analyst se trouve sur le CD d'installation de Windows
  - Resource Kit
    - Dumpel, Elogdmp
  - Utilitaires gratuits
    - ElDump, ElSave, ElFilter, etc.
  - Outils commerciaux
    - Event Log Monitor (TNT Software), LogCaster (RippleTech), Centrax (CyberSafe), Event Admin (Aelita), Syslog (Netal), etc.

2. Présentation de la sécurité W2K

2.4 Exploitation des journaux (4/4)

- **Déclenchement d'alertes (exemples)**
  - Sessions non fermées depuis une date donnée
    - Évènements 528 sans 538
    - Peut poser problème si le script de login est utilisé pour des tâches d'administration (ex. mise à jour antivirus)
  - Sessions multiples
  - Comptes non utilisés depuis une date donnée
    - Penser à détruire ou verrouiller ces comptes
  - Comptes verrouillés
    - Tentative d'attaque en force brute
  - Altération des fonctions d'audit
    - Changements de stratégie
    - Effacement du journal

3. Présentation de produits

LogCaster (RippleTech)

Contact : Richard SAMAMA (Amosdec)

richard.samama@amosdec.fr

4. Revue des vulnérabilités majeures de Windows 2000

4. Revue des vulnérabilités majeures (1/4)

- **Installation et droits par défaut**
  - L'utilisateur a toujours contrôle total sur la racine
    - Exploits Autorun, Explorer, …
  - Les partages administratifs sont toujours présents
    - IPC$, ADMIN$, C$, D$, …
  - Les partages administratifs n'ont pas de mots de passe jusqu'au premier redémarrage
    - Rebooter les serveurs après installation
  - L'installation automatique OEM laisse le répertoire « All Users » en accès complet
    - Vérifier les permissions sur les machines livrées pré-installées
- **Mots de passe**
  - SYSKEY intégré en standard
  - Disparition de PASSPROP
    Le compte administrateur ne peut plus être verrouillé
  - PWDUMP3 permet de récupérer les hashes des mots de passe

4. Revue des vulnérabilités majeures (2/4)

- **Services réseau**
  - Une majorité de services réseau sont vulnérables à des dénis de service (Telnet, FTP, NetBIOS, DNS, Windows Media 7, etc.)
    - Désactiver les services inutiles
    - Partiellement corrigé avec le SP1
  - Il est possible de récupérer le hash du mot de passe utilisateur par Telnet
    - Patch disponible (MS00-067)
  - Le service DNS accepte des réponses de serveurs non sollicités
    - Positionner une clé de la base de registre
  - L'agent IPSec utilise DES à la place de 3DES dans les versions internationales
    - Installer le High Encryption Pack
- **Exploits SYSTEM locaux**
  - « Named Pipes » (MS00-053)
  - NetDDE (MS01-007)

4. Revue des vulnérabilités majeures (3/4)

- **Active Directory**
  - En cas de modifications concurrentes, seules les modifications les plus récentes sont prises en compte
    - Pas de correctif prévu avant Windows XP
  - L'utilitaire « Configurer votre serveur » laisse un mot de passe vide en mode « Restauration des services d'annuaire »
    - Patch disponible (MS00-099)
  - Attaques en force brute sur le compte administrateur par LDAP
- **IIS 5**
  - Nombreuses vulnérabilités graves
    - MS00-086, …
  - Les correctifs sont disponibles mais pas appliqués
  - Tous les sites commerciaux « visités » récemment étaient vulnérables
- **FTP**
  - Les restrictions d'accès ne sont pas prises en compte (Windows 2000 Pro uniquement)

4. Revue des vulnérabilités majeures (4/4)

- **Audit**
  - Toujours pas de séparation des privilèges
  - Utilitaire WinZapper permettant de supprimer des entrées du journal de sécurité
- **Applications**
  - IE 5
  - Windows Media
  - Index Server
  - Office 2000
- **Compromission du certificat Microsoft**
  - MS01-017

4. Revue des vulnérabilités majeures

Vulnérabilités disparues

- Tous les SP et Hotfixes de NT4 jusqu'au SP6a ont été pris en compte dans Windows 2000
- Le compte Invité est verrouillé par défaut
- L'accès « Invité » aux journaux système et application peut être restreint
- Le déverrouillage d'un poste suit la stratégie de verrouillage de compte
- Les clés sensibles de la base de registre sont mieux protégées par défaut
  - Debugger
  - Run, RunEx, RunOnce
  - Uninstall

5. Suites

- Point sur la liste de diffusion NT-SECURITE
- Prochaine réunion
  - Date
  - Lieu
  - Thèmes
- Points divers

Fin de la présentation