



Joel Scambray & Stuart McClure

Sécurité pour Windows® 2000

Ressources anti-hackers

Collection
Référence


CampusPress

www.pearsoned.fr



2-005-420-1

2-005-420-1

Table des matières

Sécurité pour Microsoft® Windows® 2000

Joel Scambray et Stuart Mc Clure



CAMPUSPRESS

Table des matières

| | |
|---|----|
| Avant-propos | 1 |
| Introduction | 3 |
| Sécurité de Windows 2000 : réalité ou fiction | 3 |
| Organisation de ce livre | 5 |
| Attaques et contre-mesures | 7 |
| Ressources et outils en ligne | 8 |
| Un dernier mot à nos lecteurs | 9 |
| Les auteurs | 11 |

Partie I. Les bases

| | |
|---|----|
| Chapitre 1. Les fondamentaux de la sécurité des réseaux et systèmes | 15 |
| Pratiques de base de sécurité | 15 |
| En résumé | 19 |
| Pour aller plus loin | 19 |
| Chapitre 2. L'architecture de sécurité de Windows 2000 vue par un pirate | 21 |
| Modèle de sécurité de Windows 2000 | 22 |
| Principes de sécurité | 23 |
| Forêts, arbres et domaines | 29 |
| SID | 34 |
| Synthèse : authentification et autorisation | 37 |
| Audit | 42 |
| En résumé | 43 |
| Pour aller plus loin | 45 |

Partie II. Analyse de la cible

| | |
|---|-----|
| Chapitre 3. La prise d'empreinte et le scan | 49 |
| Prise d'empreinte | 50 |
| Scan | 55 |
| Importance d'une prise d'empreinte et d'un scan réguliers | 65 |
| En résumé | 66 |
| Pour aller plus loin | 66 |
| Chapitre 4. L'énumération | 69 |
| Prélude : récapitulation des résultats du scan | 70 |
| Énumération de réseau NetBIOS | 71 |
| Énumération DNS Windows 2000 | 77 |
| Énumération SNMP | 93 |
| Énumération Active Directory | 98 |
| En résumé | 102 |
| Pour aller plus loin | 103 |

Partie III. Division et conquête

| | |
|---|-----|
| Chapitre 5. Le piratage de CIFS/SMB | 107 |
| Deviner les mots de passe SMB | 108 |
| Espionner l'authentification SMB | 125 |
| En résumé | 140 |
| Pour aller plus loin | 141 |
| Chapitre 6. L'élévation des droits d'accès | 143 |
| Prédiction des tubes nommés | 144 |
| Requêtes NetDDE exécutées en tant que SYSTEM | 147 |
| Contre-mesures générales à l'élévation des droits | 149 |
| En résumé | 150 |
| Pour aller plus loin | 151 |

| | |
|--|-----|
| Chapitre 7. La prise de contrôle | 153 |
| Prise de contrôle de la ligne de commande | 153 |
| Prise de contrôle de l'interface graphique | 161 |
| En résumé | 163 |
| Pour aller plus loin | 163 |
| Chapitre 8. L'extension du contrôle | 165 |
| Audit | 165 |
| Extraction des mots de passe | 167 |
| Craquage des mots de passe | 170 |
| Recherche de fichiers | 178 |
| Cheval de Troie du système GINA | 183 |
| Reniflage | 185 |
| Progression d'île en île | 187 |
| Redirection de port | 191 |
| En résumé | 194 |
| Pour aller plus loin | 194 |
| Chapitre 9. Le nettoyage | 197 |
| Création de comptes utilisateurs dévoyés | 198 |
| Cheval de Troie de l'écran de connexion | 198 |
| Contrôle à distance | 199 |
| Lieux d'implantation des portes dérobées et chevaux de Troie | 201 |
| Rootkits | 204 |
| Couverture des traces | 206 |
| Contre-mesures générales : petit examen de médecine légale | 211 |
| En résumé | 217 |
| Pour aller plus loin | 218 |

Partie IV.

Les attaques contre les services et les clients vulnérables

| | |
|---|-----|
| Chapitre 10. Le piratage d'IIS 5 et des applications Web | 223 |
| Le piratage d'IIS 5 | 224 |
| Les outils d'audit de la sécurité des serveurs Web | 273 |
| Le piratage des applications Web | 278 |
| En résumé | 282 |
| Pour aller plus loin | 286 |

| | |
|--|------------|
| Chapitre 11. Le piratage de SQL Server | 291 |
| Exemple de compromission d'un serveur SQL | 292 |
| Les concepts de la sécurité de SQL Server | 296 |
| Le piratage de SQL Server | 301 |
| Les recommandations de sécurité pour un serveur SQL | 328 |
| En résumé | 333 |
| Pour aller plus loin | 334 |
| | |
| Chapitre 12. Le piratage de Terminal Server | 337 |
| Présentation de Terminal Server | 338 |
| Identification et énumération des TS | 340 |
| Quelques attaques de Terminal Server | 343 |
| Sécuriser Terminal Services | 347 |
| En résumé | 351 |
| Pour aller plus loin | 352 |
| | |
| Chapitre 13. Le piratage des clients Internet Microsoft | 355 |
| Les catégories d'attaques | 356 |
| L'implémentation des attaques contre les clients Internet | 357 |
| Les attaques | 360 |
| Le problème des vers VBS dans le Carnet d'adresses | 374 |
| Exemple d'un processus d'attaque complet | 382 |
| Les mesures de sécurité d'ordre général | 387 |
| Pourquoi ne pas délaissier les clients Internet de Microsoft ? | 389 |
| Les zones de sécurité d'IE | 390 |
| Les antivirus installés sur les clients et les serveurs | 396 |
| Le filtrage des contenus au niveau des passerelles | 397 |
| En résumé | 398 |
| Pour aller plus loin | 399 |
| | |
| Chapitre 14. Les attaques physiques | 403 |
| Les attaques hors ligne contre le SAM | 403 |
| Les conséquences pour EPS | 407 |
| En résumé | 415 |
| Pour aller plus loin | 416 |

| | |
|---|-----|
| Chapitre 15. Les attaques par déni de service | 419 |
| Les attaques DoS actuelles affectant Windows 2000 | 420 |
| Les recommandations de sécurité pour les attaques DoS | 430 |
| En résumé | 433 |
| Pour aller plus loin | 434 |

Partie V.

L'établissement de lignes de défense

| | |
|---|-----|
| Chapitre 16. Les fonctionnalités et les outils de sécurité de Windows 2000 | 439 |
| Modèles de sécurité et Configuration et analyse de la sécurité | 440 |
| Les stratégies de groupe | 445 |
| IPSec | 450 |
| Kerberos | 464 |
| Le système de fichiers EFS | 465 |
| Runas | 467 |
| La protection des fichiers Windows | 469 |
| En résumé | 471 |
| Pour aller plus loin | 471 |
| Chapitre 17. Le futur de Windows 2000 | 473 |
| Le futur de Windows : feuille de route | 473 |
| .NET Framework | 474 |
| Nom de code Whistler | 476 |
| En résumé | 487 |
| Pour aller plus loin | 487 |
| Chapitre 18. La liste de contrôles de la sécurité Windows 2000 | 489 |
| Attention aux rôles et aux responsabilités | 489 |
| Avant l'installation | 490 |
| Principes élémentaires de renforcement de Windows 2000 | 490 |
| Considérations de sécurité pour IIS 5 | 500 |
| Considérations de sécurité pour SQL Server | 503 |

| | |
|--|------------|
| Considération de sécurité pour Terminal Server | 505 |
| Considérations concernant le déni de service | 506 |
| Sécurité du client Internet | 508 |
| S'auditer ! | 508 |
| Pour aller plus loin | 509 |
| Index | 511 |