Лабораторна робота №1. Частина 2.

Захист реєстру операційної системи Windows 2000/XP

Мета роботи

ознайомити студентів з захистом реєстру ОС Windows 2000/XP.

Теоретичні відомості

Випадки несанкціонованого втручання в роботу комп'ютерних мереж — реальність сьогоднішнього життя. Але набагато частіше шкоду, причому ненавмисну, наносять самі користувачі, що знають ще занадто мало, щоб вважатися грамотними, але вже досить, щоб нашкодити. Відповідно до результатів опитування суспільної думки, проведеного за замовленням корпорації Oracle, 51% співробітників фірми думає, що порушення внутрішньої безпеки – набагато більш серйозна проблема, ніж спроби проникнення в мережу ззовні. Згідно даним дослідження Інституту комп'ютерної безпеки (Computer Security Institute), середній внутрішній витік інформації коштує компанії 2,7 млн. доларів, тоді як середня атака хакера приносить шкоду усього лише в 57 тисяч. Практично в кожній організації є аматори, що запускають усі файли, що виконуються, і якщо їм на очі потрапить один з редакторів реєстру – Regedit.exe чи Regedt32.exe, то й ці файли не стануть винятком. Якщо заходи для безпеки не прийняті, то результатом таких експериментів з великою ймовірністю стануть проблеми з завантаженням системи.

Розглянемо деякі практичні рекомендації з захисту серверів і робочих станцій, що працюють під керуванням Windows 2000/XP, від спроб несанкціонованого доступу.

Огляд стандартних прав доступу в Windows 2000/XP

Стандартні налаштовування системи безпеки Windows 2000/XP визначаються правами за замовчуванням (default), що призначаються наступним групам:

• ***Administrators*** (в російській локалізації системи – ***Администраторы***). Користувачі з цієї групи мають повний набір прав на локальному комп'ютері чи в домені.

• ***Users*** (в російській локалізації – ***Пользователи***). За умови, що нова копія Windows 2000/XP була встановлена на розділі NTFS, стандартне налаштовування системи безпеки таке, що користувачам із групи ***Пользователи*** не дозволяється порушувати цілісність операційної системи і встановлених програм. Користувачі з цієї групи не можуть установлювати програми, що використовувалися б іншими членами цієї групи (це один із

засобів захисту проти «троянських коней»). Крім цього, користувачі не можуть одержати доступ до даних інших користувачів. Однак слід пам'ятати, що коли відбувається перехід на нову версію ОС з попередньої, зокрема, інсталяція Windows 2000/XP на раніше встановлену Windows NT 4 (так зване оновлення операційної системи), то система зберігає більшість налаштовувань, що були зроблені раніше. В цьому випадку ймовірні суттєві недоліки в системі безпеки ОС Windows.

• ***Power Users*** (в російській локалізації – ***Опытные пользователи***). Ця група має менший набір прав, ніж члени групи ***Administrators***, але істотно більш широкий, ніж набір прав, що надані групі ***Users***. Зокрема, вони можуть інсталювати програмне забезпечення, хоча деякі програми вимагають для інсталяції прав адміністратора.

Для побудови захищеної системи Windows 2000/XP Microsoft рекомендує налаштовувати систему так, щоб усі кінцеві користувачі були членами тільки однієї групи (***Users***); а програмне забезпечення, необхідне для роботи, встановлювати так, щоб його міг запускати будь-який член групи ***Users***.

Стандартні параметри системи безпеки встановлюються на етапі інсталяції, при початку графічної фази процесу інсталяції Windows 2000/XP чи оновлення операційної системи з Windows 9x до Windows 2000. Якщо виконується оновлення версії операційної системи з попередніх версій Windows NT до Windows 2000/XP, то, як було зазначено вище, зберігаються параметри системи безпеки, що існували в попередній системі. Параметри налаштування безпеки для об'єктів файлової системи можуть застосовуватися тільки у випадку, якщо диск відформатований для використання NTFS.

Найбільш важливі ключі реєстру Windows 2000/XP, що вимагають захисту

Microsoft офіційно рекомендує адміністраторам обмежувати доступ користувачам до цілого ряду вкладених ключів, що входять до складу ключа **HKEY_LOCAL_MACHINE\SOFTWARE**. Основна мета цих операцій – запобігання доступу некваліфікованих користувачів до параметрів налаштування встановленого в системі ПЗ. Рекомендується обмеження доступу до наступних ключів реєстру:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\ CurrentVersion**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion**

Для групи ***Все*** досить мати права доступу **Query Value**, **Enumerate Subkeys**, **Notify** і **Read Control** до ключа реєстру **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion** і наступним вкладеним підключам, що існують в його складі: **AeDebug**, **Compability**, **Drivers**, **Embedding**, **FontDrivers**, **FontCache**, **FontMapper**, **Fonts**, **FontSubstitutes**, **GRE_Initialize**, **MCI**, **MCI Extensions**,

Ports (і усім вкладеним ключам у складі ключа **Ports**), **Type I Installer**, **Windows 3.1 MigrationStatus** (і усім вкладеним ключам у складі цього ключа), **WOW** (і вкладеним ключам у складі цього ключа).

Microsoft також рекомендує обмежити доступ користувачів до ключа реєстру, що керує даними про продуктивність системи, – **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Perflib**. Доступ до цього ключа повинні мати тільки операційна система (**SYSTEM**), власники ключа (**CREATOR_OWNER**), члени групи ***Administrators*** і користувачі, що зареєструвалися в системі інтерактивно (***Interactive***).

Група ***Все*** повинна мати обмежені права доступу (тільки права типу **Query Value**, **Enumerate Subkeys**, **Notify**, **Read Control**) і до деяких інших ключів реєстру. Такий захист необхідно забезпечити для ключа **HKEY_CLASSES_ROOT** і всіх його вкладених ключів, а також для ключа **HKEY_USERS\.DEFAULT**. Захищаючи їх, ви захищаєте систему від зміни ряду системних параметрів і параметрів налаштовування робочого столу.

Для заборони несанкціонованого використання розділюваних ресурсів системи і застосування параметра **ImagePath** у складі ключа **UPS** для запуску небажаного програмного забезпечення доступ типу ***Полный доступ*** до ключів **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services \LanmanServer\Shares** і **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\UPS** повинні мати тільки операційна система (**SYSTEM**) і члени групи ***Administrators***.

При роботі із сервісом віддаленого доступу система виводить діалогові вікна, у яких користувачі повинні ввести реєстраційну інформацію – логін і пароль. У цих діалогових вікнах є прапорці, встановлення яких дозволяє запам'ятати пароль. Хоча збереження паролів дуже зручно для користувача, така практика являє собою небезпеку, оскільки паролі зберігаються так, щоб система могла швидко їх витягти. Таким чином, одержати цей пароль буде нескладно і зломщику. Щоб не дати йому такої можливості, розкрийте ключ реєстру **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ RemoteAccess\Parameters** і додайте в нього параметр **DisableSavePassword** з типом даних **REG_DWORD**. Тепер система ніколи не буде пропонувати користувачу зберегти введений пароль для доступу до сервера **RAS**.

Захист вуликів SAM і Security

Інформація безпеки Windows 2000/XP зберігається у вуликах реєстру **SAM** (**Security Accounts Manager**) і **Security**. Вулик **SAM** містить паролі користувачів у вигляді таблиці хеш-кодів, а вулик **Security** – інформацію про безпеку локального комп'ютера. Існує цілий набір утиліт, за допомогою яких можна здійснити злом вулика **SAM**. Найбільш відомі з них – PWDUMP, NT Crack, L0phtCrack+.

Microsoft стверджує, що кращий спосіб захисту Windows 2000/XP – це захист адміністративних паролів, але цього явно недостатньо. Доступ до вуликів **SAM** і **Security** одержують багато користувачів (наприклад,

користувачі з групи ***Операторы резервного копирования***). Вулики **SAM** і **Security** зберігаються на диску точно так само, як і інші файли, і єдине, що потрібно для злому, – це роздобути копії цих вуликів. У складі програмних продуктів існують утиліти (Regback у Windows NT 4.0; Resource Kit і REG – у Windows 2000 Resource Kit), за допомогою яких користувачі, що входять до складу груп адміністраторів чи операторів резервного копіювання, можуть одержувати копії реєстру системи, що працює.

Якщо Windows 2000/XP установлена на томі FAT, то потенційну небезпеку представляє будь-який користувач, що володіє правом на виконання перезавантаження системи і що одержав фізичний доступ до комп'ютера. Якщо ж Windows 2000/XP установлена на томі NTFS, то для копіювання можна скористатися утилітою NTFS-DOS (http://www.sysinternals.com/ntfs30.htm), що дозволяє монтувати том NTFS у DOS.

Оскільки найбільшу цінність для злому мають сервера мережі, то для забезпечення належного захисту файлів **SAM** і **Security** від незаконного копіювання варто установити комп'ютери, що захищаються, (сервери) в приміщенні, що охороняється, а також позбавити користувачів груп ***Опытные пользователи*** та ***Пользователи*** права на перезавантаження комп'ютера. У Windows 2000 Server право перезавантаження за замовчуванням мають групи ***Администраторы***, ***Операторы резервного копирования***, ***Опытные пользователи***. У системах Windows 2000/XP Professional цим правом володіють ті ж групи, плюс ***Пользователи***.

Щоб відредагувати права користувачів у Windows 2000/XP, виконайте таку послідовність дій:

- зареєструйтеся в системі від імені користувача з правами адміністратора;
- викличте вікно запуску (**Выполнить**…), наберіть у ньому команду *mmc* та натисніть **ОК**;
- у вікні консолі, що відкриється, відкрийте меню «Консоль» та виберіть команду «Добавить или удалить оснастку… (або натисніть Ctrl+M);
- у вікні, що відкриється, натисніть кнопку **Добавить**, виберіть у вікні «**Добавить изолированную оснастку**» оснастку «Локальные пользователи и группы» та додайте її у консоль;
- розкрийте дерево консолі та виберіть опцію «**Пользователи**».

У правій частині вікна з'явиться список користувацьких прав, що доступні для редагування.

Для запобігання доступу рядових користувачів домену до файлів **SAM** і **Security** необхідно:

- використовувати файлову систему NTFS;
- позбавити кінцевих користувачів права локальної реєстрації на серверах;
- забезпечити належний фізичний захист для серверів;

- у системах Windows NT 4.0 і тих системах Windows 2000/XP, де операційна система встановлювалася як поновлення попередньої версії Windows NT, посилити права доступу до каталогу **%SystemRoot%\Repair**;
- забезпечити безпечні умови збереження резервних копій і дисків аварійного відновлення (Windows NT 4.0), а також копій даних з набору **System State Data** (Windows 2000/XP).

Для злому викрадених вуликів **SAM** і **Security** великих зусиль не потрібно. Для цього можуть використовуватись утиліти:

- PWDUMP
- PWDUMP2
- NT Locksmith (http://www.winternals.com)
- L0phtCrack+ (http://www.l0pht.com/l0phtcrack).

Успіх атаки залежить, в основному, від якості використовуваного для злому словника – чим більше кількість слів, дат, чисел, словосполучень, що використовуються як пароль найчастіше, міститься в цьому файлі, тим вище шанси вдалого злому.

Для захисту каталогу **\repair** призначайте права таким чином, щоб зловмисники не могли одержати доступ до даного каталогу і файлів, що містяться в ньому, особливо до файлу **sam._**, у якому знаходиться база даних **SAM**. В системі Microsoft Windows NT Server 4.0 для захисту файлів у каталозі **\repair** використовуйте утиліту **calcs.exe**, що входить до складу Microsoft Windows NT Server 4.0 Resource Kit, чи іншу аналогічну програму. Для цього:

- у вікні **Командная строка** перейдіть у каталог **%systemroot%** (звичайно це **C:\Windows**);
- виконайте команду **cads repair /g administrators:F system:F /t**.

Або, використовуючи програму Windows Explorer, зробіть наступне:

- відкрийте Windows Explorer;
- перейдіть у каталог **repair** (звичайно це **C:\Windows\repair**);
- натисніть праву клавішу миші і виберіть в меню, що відкрилося, **Свойства**;
- виберіть закладку **Безопасность**;
- натисніть **Дополнительно** та виберіть закладку **Разрешения**;
- відзначте **Наследовать от родительського объекта …** і **Заменить разрешения для всех дочерних объектов …** ;
- видаліть зі списку всіх користувачів, крім **Administrators** і **SYSTEM**;
- переконайтеся, що і **Administrators**, і **SYSTEM** мають права **Полный доступ**;
- натисніть **«OK»**.

Тепер ви призначили користувачам **Administrators** і **SYSTEM** права **Full Control** на даний каталог і на усі файли, що містяться в ньому. Оскільки режим редагування **ACL** обраний не був, права всіх інших користувачів вилучені системою.

У залежності від конфігурації системи, крім каталогів **\repair** і **\config** NT може записувати інформацію, що має відношення до **SAM**, у наступні файли: **pagefile.sys**, **memory.dmp** чи **user.dmp**. NT використовує файл **pagefile.sys** для організації віртуальної пам'яті. Файл **memory.dmp** створюється при аварійному завершенні роботи операційної системи, якщо в конфігурації NT обраний режим запису образу пам'яті на диск. Файл **user.dmp** створюється при аварійному завершенні роботи якої-небудь прикладної програми, якщо в конфігурації програми Dr. Watson обраний режим запису образу пам'яті у файл.

При роботі з цими файлами NT переписує визначену порцію даних з пам'яті на диск. У деяких випадках ці дані можуть містити паролі, що зберігаються резидентно в пам'яті. Відповідно, одержавши доступ до цих файлів, зломщик може без особливої праці заволодіти важливою інформацією, що дозволяє пробити пролом у системі безпеки.

Щоб зменшити небезпеку, пов'язану з використанням файлів **user.dmp** і **memory.dmp**, вам необхідно зробити одну з наступних дій:

- написати командний файл, що буде видаляти зазначені файли при вході в систему;
- встановити права для цих файлів таким чином, щоб доступ до них мали тільки адміністратори;
- установити в реєстрі ключ, що вказує на необхідність видалення системного файлу **pagefile.sys** при завершенні роботи операційної системи;
- у конфігурації програми Dr. Watson відключити режим створення файлів.

Найкраще налаштувати параметри системи так, щоб зазначені два файли не створювалися. Однак при цьому може виникнути ситуація, коли програмісти, що повинні досліджувати проблему аварійного завершення роботи системи, не будуть мати необхідних їм даних.

Щоб відключити створення файлів **user.dmp**, програмою Dr. Watson запустіть утиліту drwtsn32.exe, відключіть параметр **Create Crash Dump File** і закрийте програму.

Щоб відключити в параметрах налаштування NT створення файлу **memory.dmp**, запустіть в Панелі Керування аплет **Система** і виберіть закладку **Дополнительно** та натисніть кнопку **Параметры** у секції **Загрузка и восстановление**. Потім відключіть параметр **Запись отладочной информации**. Якщо вам усе-таки необхідно мати образи пам'яті на момент аварійного завершення роботи Windows, постарайтеся налаштувати параметри ОС і програми Dr. Watson таким чином, щоб файли, що містять образ пам'яті, розміщувалися в захищеному каталозі, що доступний лише адміністраторам.

Що стосується файлу **pagefile.sys**, то його відкриває і захищає від спроб безпосереднього доступу з боку зломщиків тільки операційна система. Однак варто згадати інцидент, коли клієнтська служба NetWare для Windows NT поміщала в пам'ять паролі користувачів NetWare у відкритому вигляді. Ці

паролі могли бути записані у файл **pagefile.sys** при переписуванні відповідної сторінки пам'яті на диск. Кожен, хто мав копію файлу **pagefile.sys** і текстовий редактор, міг без зусиль одержати паролі. Розроблювачі Novell вирішили цю проблему. Тепер паролі, перш ніж бути поміщеними в **pagefile**, шифруються з використанням недокументованого API-інтерфейсу. Однак винахідливі зломщики можуть пробити цей захист, знайшовши спосіб розшифровки інформації, одержуваної з файлу **pagefile.sys** (за деякими відомостями, це вже вдалося російським програмістам).

Щоб захиститися від подібних атак, налаштовуйте Windows таким чином, щоб файл **pagefile.sys** видалявся при завершенні роботи системи. І не забувайте про необхідність фізичного захисту комп'ютера з метою запобігання небажаного доступу до файлу **pagefile.sys**. Але у такий спосіб ви забезпечите захист тільки від тих зломщиків, що копіюють чи змінюють файл, завантажившись з іншої копії ОС (тобто використовуючи завантажувальний диск чи завантаживши NT з іншого системного каталогу). Більшість зломщиків розуміють, що в такому випадку в них є можливість одержання доступу до системи шляхом переміщення бази даних **SAM** – отже, злом файлу **pagefile.sys** стає взагалі не потрібним.

Незважаючи на це, у ситуаціях, коли умови експлуатації системи вимагають установки і використання декількох копій ОС, видалення файлу **pagefile.sys** при нормальному завершенні роботи можна вважати достатньою мірою безпеки. Варто мати на увазі – якщо NT налаштована так, щоб видаляти **pagefile** під час завершення роботи системи, то неминуча деяка затримка в процесі початкового завантаження й зупинки ОС. Однак ця затримка несуттєва, якщо взяти до уваги рівень безпеки, якого ми в результаті досягаємо. Для того щоб включити режим видалення файлу **pagefile.sys** під час нормального завершення роботи ОС, варто модифікувати (чи створити) у системному реєстрі у ключі **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management** параметр **ClearPageFileAtShutdown** (типу REG_SZ) , присвоївши йому значення 1.

Хеш-коди паролів у пам'яті

За замовчуванням Windows кешує необхідні для реєстрації атрибути для десяти останніх користувачів, що входили в систему інтерактивно. Це робиться для того, щоб користувач зміг зареєструватися, навіть якщо ви відключите комп'ютер від мережі чи контролер домену виявиться недоступним. Windows забезпечує деякий захист інформації, що кешується. Однак якщо ваші задачі вимагають більш високого рівня безпеки, ви можете цілком відключити кешування, щоб виключити спроби атак на дані в кеш-пам'яті. Потрібно враховувати, що кешовані дані містять хеш-коди інших хеш-кодів паролів. Тому їх дуже складно зламати і використовувати для несанкціонованого входу в систему. Поки що в практиці не було жодного випадку використання хакерами таких даних з кеш-пам'яті. Щоб відключити кешування, змініть на нуль значення параметра реєстру **CachedLogonsCount**

(типу REG_DWORD) у ключі **HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\WindowsNT\CurrentVersion\Winlogon**.

SAM у мережі

ОС типу Windows NT використовується протокол SMB (Server Message Block – блок серверних повідомлень), розроблений спільно фірмами Microsoft, IBM і Intel. Цей протокол визначає алгоритми функціонування файлової служби в мережевому середовищі. Неважко припустити, що під час сеансу SMB по мережі повинні передаватися пакети, що містять інформацію конфіденційного характеру. Серед іншого, ці пакети звичайно містять у собі зашифровані дані протоколу NTLM, передані NT під час фази автентифікації.

Зломщики, використовуючи існуючі мережні аналізатори, можуть легко перехоплювати дані, що передані по мережі. Задача перехоплення потрібних пакетів і одержання з них інформації про паролі завжди вважалася нелегкою. Але ситуація в корені змінилася з появою продукту SMB Packet Capture, випущеного компанією L0pht Heavy Industries. SMB Packet Capture – це мережевий аналізатор, що тісно інтегрований із програмою L0phtCrack. Маючи у своєму розпорядженні L0phtCrack, можна легко «вихоплювати» з мережі хеш-коди паролів, передані відповідно до протоколу SMB.

Вбудований у L0phtCrack мережевий аналізатор непомітно перехоплює хеш-коди паролів і запам'ятовує їх з метою розшифровки. Після розшифровки паролів зловмиснику нічого не варто добратися до будь-якого мережевого ресурсу, до якого мав доступ відповідний користувач. Ризик тут очевидний, але і методи захисту прості.

Для захисту від подібних атак потрібно використовувати протокол NTLMv2, що поставляється в складі пакетів відновлення SP4 і SP5, або застосовувати механізм створення віртуальних приватних мереж (VPN – Virtual Private Network) типу Microsoft PPTP. Протокол NTLMv2 дозволяє захистити дані, передані по внутрішній локальній мережі, а PPTP забезпечує захист інформації, переданої через такі «небезпечні» мережі, як наприклад Інтернет. Якщо ви реалізуєте PPTP, то обов'язково встановіть останні сервісні пакети, включаючи доповнення і виправлення до них (hotfix). Microsoft внесла необхідні коректування, що усувають недоліки PPTP. Але ці коректування будуть вам недоступні, якщо ви не встановите hotfix до пакета SP3 чи більш пізнього відновлення.

Варто мати на увазі, що при відсутності у вашій системі механізму VPN і технології підписів SMB зломщик може використовувати сеанс SMB для одержання несанкціонованого доступу в систему. Microsoft реалізувала технологію підписів SMB у пакеті відновлення SP3 і також включила її в усі наступні. При використанні підписів пакетів SMB операційна система перевіряє дійсність кожного з них, перш ніж прийняти його до виконання. Однак реалізація підписів SMB не завжди безпечна. Для одержання більш докладної інформації обов'язково прочитайте статті Microsoft «How to Enable SMB Signing in Windows NT» (http://support.microsoft.com/support/ kb/ articles/q161/3/72.asp).

Для боротьби з засобами злому типу L0phtCrack можна заборонити NT посилати в мережу хеш-коди паролів, формовані за протоколом LAN Manager (LM). Останні є більш простими, чим коди NTLM, що дозволяють задіяти паролі, що враховують регістр. Крім того, NTLM припускає можливість застосування додаткових символів клавіатури. Це розширює діапазон символів ключа шифрування на 26. Помітимо, що складні паролі сутужніше піддаються розшифровці навіть при наявності таких інструментів, як L0phtCrack.

Доцільно включати в пароль символ «повернення каретки» (Return), тому що L0phtCrack не вміє нормально обробляти цей символ. Щоби вставити «повернення каретки», натисніть клавіші Alt+0+1+3 на цифровій панелі клавіатури.

Дослідження стійкості паролів до злому програмним забезпеченням L0phtCrack+, що виконувалось на комп'ютері Pentium III/550 з обсягом застосовуваного словника 9 Мб, дало такі результати:

• якщо пароль складається зі стандартних слів англійської (російської) мови, то час злому складе не більш 2 хвилин (у залежності від величини словника);

• при застосуванні паролів довжиною не менш 8 символів і складених з цифр і букв англійського алфавіту час злому – до 40 діб;

• при застосуванні паролів довжиною не менш 8 символів і складених з букв, цифр і спецсимволів час, відповідно, збільшується до 100 діб.

Для рішення цієї проблеми Microsoft реалізувала в складі доповнень і виправлень до сервісного пакета SP3 (Windows NT) новий ключ реєстру. Він був включений в усі сервісні пакети, що вийшли після SP3. Новий параметр реєстру, **LMCompatibilityLevel**, має тип REG_DWORD і розміщається в **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa**.

При використанні NTLMv2 можна установити значення цього параметра рівним 0,1, 2, 3, 4 чи 5:

• якщо це значення дорівнює 0, то NT при автентифікації мережного з'єднання передає по мережі паролі як у форматі NTLM, так і у форматі LM (цей метод автентифікації забезпечує сумісність з іншими системами і використовується в NT за замовчуванням);

• якщо значення дорівнює 1, то NT передає обидва типи хеш-кодів тільки тоді, коли цього вимагає сервер;

• якщо значення дорівнює 2, то хеш-коди паролів у форматі LM не використовуються ні при яких обставинах;

• якщо значення дорівнює 3, застосовується тільки автентифікація за протоколом NTLMv2;

• значення параметра, рівне 4, забороняє контролеру домена використовувати автентифікацію LM;

• значення 5 указує на необхідність застосування при автентифікації тільки протоколу NTLMv2. Найбільш безпечною є встановлення значення цього параметра рівним 2. Але варто мати на увазі, що системи, що підтримують тільки протокол LM (тобто Windows 95 і Windows for

Workgroups), не зможуть установити з'єднання з даною системою NT. Повний перелік особливостей конфігурації описаний у статті «How to Disable LM Authentication on Windows NT».

Ще один спосіб злому системи може мати місце, якщо зломщик має у своєму розпорядженні можливість фізичного доступу до комп'ютера. Використовуючи такі засоби, як NT Locksmith чи ERD Commander (обидва можна знайти на http://www.winintemals.com), нічого не варто одержати доступ у систему з правами будь-якого користувача. Для захисту від цього методу злому варто вжити заходів, що перешкоджають фізичному доступу до комп'ютера

Адміністративні рекомендації з захисту Windows 2000/XP

Далі наведені основні ідеї й особливості конфігурації, які варто враховувати при установці і супроводі ОС Windows 2000/XP та її системи безпеки. Адміністративні рекомендації:

1. Обмежити фізичний доступ до сервера (станції) Windows 2000/XP. Сервер повинний встановлюватися в закритій кімнаті із сигналізацією, виведеною на пульт чергового. Кімната повинна бути обладнана двома замками чи замком із двома різними ключами, що ніколи не повинні зберігатися разом. Один з них повинний зберігатися в системного адміністратора, інший – у відповідного співробітника служби безпеки. Розкриватися кімната повинна тільки цими співробітниками разом.
2. Обмежити можливість завантаження з гнучких дисків, CD-ROM – або шляхом фізичного відключення накопичувача на гнучких дисках і CD-ROM, або установкою в BIOS завантаження тільки з твердого диска і закриття BIOS паролем супервізора з одночасним фізичним відключенням клавіатури.
3. Бажано один із гвинтів на корпусі сервера обладнати «гвинтом із секретом», що виключить можливість підключення стороннього HDD з ОС Windows 2000/XP. Дуже ефективний спосіб опечатування комп'ютера – заливання одного з гвинтів на корпусі звичайним лаком для нігтів, якого на сьогодні існує більш 400 000 відтінків.
4. Комплект дискет відновлення повинен знаходитися в сейфі, обов'язково окремо від самого сервера (тобто в іншому приміщенні).

Хід роботи

1. Увійдіть у систему з адміністративними правами.
2. Відкрийте **Панель управления** та запустіть аплет **Администрирование/Локальная політика безопасности**.
3. Розгорніть у дереві лівого вікна дерево **Локальные политики** та клацніть мишкою по пункту **Политика аудита**. У правому вікні двічі клацніть по пункту **Аудит входа в систему** та постате «галочки» **Успех** та **Отказ**. Закрийте вікно для запуску аудиту системи.
4. Запустіть аплет **Службы** з **Администрирования** та встановіть для служби «Планировщик заданий» (Scheduler) режим запуску **С системной**

учетной записью (**System account**). Запустіть службу «Планувальника» (якщо вона вже була запущена – перезапустіть її).

5. Відкрийте вікно командного рядку і перевірте поточний системний час.
6. Додайте до поточного часу 1-2 хвилини (так, якщо час 11:30, використовуйте 11:32) і введіть команду: **at 11:32 /interactive "regedt32.exe"**. Натисніть Enter. Ця команда вставляє в список «Планувальника» подію, за якою в 11:32 на консолі буде запущена утиліта regedt32 із правами **SYSTEM**.

   Якщо з якихось причин у Вас виникли труднощі з «Планувальником», можна діяти іншим чином. Знайдіть у каталозі **WinNT\SYSTEM32** файл **logon.scr**. Для нього в цьому каталозі система не показує розширення, але його тип (Screensaver) легко впізнати по стандартній іконці для екранних заставок. Ця заставка – системна, вона автоматично запускається системою **з правами SYSTEM**, якщо після перезавантаження проходить визначений в реєстрі час (як правило, 900 секунд, тобто 15 хвилин). Тимчасово збережіть де-небудь цей файл (наприклад, на Desktop). Далі знайдіть в цьому ж каталозі файл **regedt32.exe** і зробіть його копію з ім'ям **logon.scr**. Далі залишається лише почекати після перезавантаження заданий час, не торкаючись консолі, і все – редактор реєстру з правами **SYSTEM** у ваших руках (або в руках того, хто знаходиться в цей момент біля консолі). Не забудьте потім вернути на місце справжній **logon.scr!**
7. Дочекайтеся визначеного часу, коли «Планировщик событий» запустить редактор реєстру. При цьому ви одержите доступ до всього реєстру, включаючи базу даних **SAM**. Будьте уважні при редагуванні реєстру — помилка може вивести з ладу систему.
8. Виберіть **HKEY_LOCAL_MACHINE**, знайдіть дерево **SAM** і виділіть його в лівій панелі екрана.
9. Виберіть у контекстному меню: **Разрешения** =>**Дополнительно**=>**Аудит**
10. У діалоговому вікні **Аудит** натисніть **Добавить=>Дополнительно=> Поиск**.
11. Додайте обліковий запис **SYSTEM**, групу **Администраторы**, всі облікові записи користувачів, що мають адміністративні права, а також всі інші облікові записи, яким привласнені наступні права (права можна подивитися: **Администрирование**=>**Локальная политика безопасности** =>**Назначение прав пользователя**):
    - **Take ownership of files or other objects** (овладение файлами и иными объектами);
    - **Back up files and directories** (архивирование файлов и каталогов);
    - **Manage auditing and security log** (управление аудитом и журналом безопасности);
    - **Restore files and directories** (восстановление файлов и каталогов);
    - **Add workstations to domain** (добавление рабочих станций к домену);
    - **Replace a process-level token** (замена маркера уровня процесса).

12. Відзначте **Этот раздел и подразделы.**
13. Відзначте **Успех** і **Отказ** для наступних полів:

    Запрос значения, **Задание значения**, **Запись DAC**, **Чтение разрешений**.
14. Натисніть кнопки **OK**.
15. Повторіть кроки з 10 по 14 для ключа **SECURITY**, якщо це необхідно. Це не потрібно, якщо Ви хочете активізувати аудит тільки ключів, що містять паролі.
16. Вийдіть з редактора реєстру. Зупиніть службу «Планувальника» і змініть його конфігурацію так, щоб він працював від імені користувача, що вживалося раніше (до кроку 4). Якщо ви не застосовуєте в звичайній роботі системи «Планировщик событий», то просто зупиніть його чи, ще краще, заблокуйте (варіант disabled).

Звіт з лабораторної роботи

Оформіть звіт, який повинен містити протокол ваших дій, значення параметрів, які були до вашого втручання, і ті, які ви встановили, а також відповіді на контрольні запитання.

Контрольні запитання

1. Які функції виконує реєстр Windows?
2. Які функції виконують вулики SAM та Security реєстру?
3. Які функції аудиту в системі безпеки операційних систем?
4. Як можна отримати доступ до реєстру за допомогою планувальника задач? Як заблокувати можливість такої атаки?
5. Як можна отримати доступ до реєстру за допомогою screensaver? Як заблокувати таку можливість?
6. Які основні принципи захисту реєстру Windows?
7. Які основні принципи захисту Windows?