Список використаних джерел:

1. http://topfilm.kiev.ua/motion-design
2. http://eds.co.ua/ru/motion_design.htm
3. https://segd.org/what-motion-design

Кіюмжи Ю., Кіюмжи О., Кухар О.
студенти,
Національний авіаційний університет

СПОСОБИ ЗАХИСТУ ЛОКАЛЬНОЇ СИСТЕМИ WINDOWSNT

На сьогодні існує багато способів зламування локальної системи WindowsNT. Під даним терміном розуміють наступне: отримання паролів інших користувачів та й заміна паролю адміністратора теж не являється винятком. Також нелегальне підвищення до найвищого рівня повноважень користувачів за рахунок свого облікового запису, який має насправді обмежувальні права, дозвіл доступу до заборонених законом файлів і багато інших типів зламувань аккаунтів та облікових записів. Але найнебезпечніший момент це тоді, коли будь-який користувач нелегально отримує повний список усіх паролів локального комп'ютера. Варто пам'ятати що таких випадків і усьому світі дуже багато. Під прикриттям слова оновлення усіх паролів зловмисник може приховувати поняття «зламування». Ось такого плану задачі ставляться для керівництва системних адміністраторів, особливо тоді коли мова йде про людей які тільки-но працевлаштувалися на цю посаду і не знають ані логінів ані паролів своїх співробітників та підлеглих. І не значи правил підприємства новачки можуть використовувати так звані хакерські методи, оскільки користувачів, що позабували випадково паролі набагато більше і практично ніхто не може вчинити супротив подібним зламуванням. Отож будь-який й навіть новий адміністратор змушений вміти захищати систему у якій зберігаються облікові записи. Але варто пам'ятати що поліція та інші силові структури в рамках своїх службових повноважень матимуть право поритися у ваших архівах і якщо ваше підприємство вчинило правопорушення то отримати доступ до усіх даних у справах обшуків. Отже звідси можна зробити висновок що всі знання про типи захисту інформації можуть знадобитися не тільки головному системному адміністратору а насамперед й усім користувачам. На даному етапі існують два способи, які обмежують доступ до комп'ютера стороннім особам: повне блокування публічного зміну комп'ютерних налаштувань CMOSSetup або вимога увести пароль, у той час коли комп'ютер завантажується. У випадках скасування блокування потрібно знати, який пароль налаштованийдля входу у систему. Зустрічаються й інші системи захисту це дуже застосовується у ноутбуках. Це наприклад механічні замки або блокування та налаштування паролю для отримання доступу до інформації яка встановлена у жорсткому диску. Наразі також можна обмежувати доступ до

системи за допомогою зберігання паролю на BIOSабо підтримувати аутентифікацію на так званих смарт – картах або на відбитках своїх пальців. Але ось є одна біда: Професійні зловмисники можуть з легкістю підміняти чіп на інший, але вже з існуючим паролем або – перешивання системи BIOS в цілому. Наслідки таких харкерських забав можуть дуже дорого коштувати як системному адміністратору так й усім підлеглим в цілому. І саме для цього ціна захисту інформації повинна передувати затратам за збитки, які були нанесені від хакерських атак. Але варто знати: Якщо ви намагаєтесь завантажувати комп'ютер більш простими способами або через дискети, то хакери легко можуть отримувати доступ до CMOS налаштувань комп'ютера за допомогою спеціально написаних для цього програм крякерів, які виконують функцію ігнорування паролів. Приклад роботи таких програм: Або не бачить пароль або він відкривається користувачу на екрані комп'ютера [2, с. 95].

Ми вже говорили про те що існує багато способів зламування комп'ютерних систем. Так от повернемося до системи BIOS,програми зламування якого можна достатньо легко знайти, вводячи правильний запит у будь-якій пошуковій системі в мережі Інтернет. Наприклад програми типу: AWARDBIOS, AMIBIOS за допомогою яких можна будь-кому змінити налаштування у BIOSi. Варто лише набрати такі команди у cmd.exe.

BIOS: DEBUG
- 0 70 17
- 0 71 17
Q

Для Phoenix:

BIOS:DEBUG
- 0 70 EE
- 0 71 17
Q

Але якщо у системі існує та й у завантаженні персонального комп'ютера пароль, який вже налаштований то задача лише трохи вважається складною, але все ж таки розгадати ці паролі ще легше – просто треба скасувати усі налаштування у CMOSSetup,повернувши усе як було спочатку тобто за замовчуванням і після цього не буде потреби навіть паролі згадувати. Для того аби правильно провести такі хакерські операції потрібно знайти інструкцію по материнській платі й відповідно правильно переставити так звану перемичку на ній. Зазвичай вона має місце біля батареї ноутбука або десь поблизу процесора і маркується як CLEAR, CLEAR CMOS, CLR, CLRPWD, PASSWD, PASSWORD, PWD.

Якщо ці намагання не приносять ніяких результатів та змін потрібно на декілька рідко годин, а подекуди хвилин, якщо є конденсатор вилучити батарейку або сам чіп з самої материнської плати і бажано відключити блок живлення з міркувань безпеки та успішного проведення такого роду зламування та очищення налаштувань CMOS.Але найцікавіше розпочнеться тоді, коли раптом побачите що акумулятор впаяли у саму плату і може відбутися коротке замикання таких контактів. Але у таких випадках як батареї

комп'ютерів типу IBMThinkpadне рекомендується відокремлювати його від живлення адже ПК просто не зможе завантажитися так як існує ймовірність використання таємного паролю на жорсткому диску який може включатися з системою типу Supervisor [2, с.33].

Функція якого інколи забувати пароль у той час як у комп'ютерів такого плану відсутнє електроживлення. Тому якщо у вас існує бажання закинути пароль без негативних наслідків потрібно детальніше вивчити інструкцію типу CMOSноутбуку джампера на платі [3, с.54].

На деяких машинах можна й взагалі зламати систему захисту шляхами натискання деяких клавіш у той час як ПК завантажується. Наприклад ви можете на ноутбукуToshibaтримати клавішу Shift або Insertна BIOSабо все ж таки натискати по декілька разів водночас натискати дві кнопки комп'ютерної миші які виготовлені по моделі AptivaIBMстандарту. Ви можете користуватися можливістю багатократного натискання клавіші Esc при завантаженні комп'ютера або й взагалі не треба використовувати (до речі пароль на пристрої типу PhoenixAmbraцей пароль скасувати можна у тому випадку якщо відімкнути вінчестер IDE шлейфу при завантаженні ПК.У нашому світі існують ще багато скасування паролю у результаті так званої вішалки спеціальної заглушки LPTпортів на ноутбуці марки Toshibay яких повне зняття живлення не зможе обнулити пароль оскільки він розташований у енергонезалежній памяті. Але існує одна хитра річ потрібно усього лише розпаяти коннектор 25-пин та з'єднати його наступним чином 1-5-10 2-11 3-17 4-12 6- 16 7 – 13 8-14 9-15 18-25.

Саме через це багато BIOS виробників залишають так званні спеціальний чорний хід у своїх програмних забезпеченнях або їх ще називають інженерними паролями хоча вони вже скажімо усім користувачам стали відомими а ось для нової материнської плати сучасних та нових ноутбуків ви вже фактично підібрати не зможете. Отже з цього випливає висновок що пароль який налаштований у CMOSSetupне має аніякого елементарного захисту від навіть звичайних користувачів сучасної техніки і навіть можна не використовувати паралельних методів для розв'язання таких інженерних та комп'ютерних задач [4, с. 161].

А зараз ми поговоримо детальніше про скасування паролю. Якщо вже так занурюватись більш детально то можна зазначити що існують найбільш прості правила отримування системного доступу до даних, якими володіє системний адміністратор хоча цей розділ присвячений для таких адміністраторів що забули або втратили контроль над захистом та зберіганням паролів. Ні для будь-якого користувача вже не секрет що наразі можна дуже просто редагувати або знищити непотрібний пароль. Саме для таких можливостей існують програми типу ERDCommander, OfflineNTPassword&RegistryEditor. На сьогоднішній день варто відмітити програму універсального рівня O&OBlueConXXL (oo-software.com/en/products/oobluecon/index.html) . У складі якого мається дуже непоганий редактор консольного зразка реєстру та схожого таки призначення додаток утиліта типу CIACommander (www.mathcode.com/ciamd.htm). Але ми маємо прекрасні аналоги які найбільше підходять для WindowsNT 4 NTAccess (www.mirider.com/ntaccess.html) NTFSdriver&ChangeNTpassword (www.cgsecurity.org/ntfs.zip). Але є одне але усі

програми мають до нас одну вимогу облікові записи вводити латинськими літерами. Всі ці процедури робляться задля того щоби уникнути серйозних проблем, що виникають при завантаженні ПК. Можуть усі змінити пароль за допомогою інших програм DebPloitta GetAdm2. Але якщо допустити видалення SAMце стане фатальною помилкою для користувачаоскільки може накритися уся операційна система і увійти в неї стане неможливо. Або остання річ така як MSV1_O.DLL (тобто заміна звичайної ліцензованої версії на патчінгову версію у якій відключений будь-який тип захисту у тому числі і відсутність працездатності паролю. Варто лише виправити код такої DLLбібліотеки з метою зміни переходів змістовних на беззмістовні [2, с. 98].

В якості висновку можна лише додати для того щоб захистити інформацію потрібно встановити потужний антивірус.

Список використаних джерел:

1. Храмцов П.Б., Брик С.А., Русак А.М., Сурин А.И.– Основы WEB-технологий. – М.: ИТУИТ.РУ, 2003. – 512 с.
2. Роджерс Д.– Программирование на Microsoft JScript.NET. «Вильямс», 2002. – 352 с.
3. Старыгин А. XML: разработка Web-приложений. – СПб. : «БХВ-Петербург», 2003. – 585 с.
4. Троелсен Э.. C# и платфома.NET. Библиотека программиста. – СПб.: «Питер», 2007. – 796 с.

Кулибаба П.О.
магістр;
Якименко Д.О.
магістр,
Черкаський державний технологічний університет

ПЕРЕВІРКА ПРАВОПИСУ ВВЕДЕНОГО ТЕКСТУ НА ОСНОВІ МОДЕЛІ NOISY CHANNEL

У наш час проблема орфографічної грамотності набуває все більшої актуальності. Адже без знання орфографічних правил неможливо написати лист, який-небудь документ, статтю або просто записку близьким. Для перевірки орфографії все більше використовують комп’ютери. Існує безліч онлайн сервісів та комп’ютерних програм для перевірки орфографії. Тому задача побудови простого і швидкого алгоритму пошуку помилок у тексті є актуальною.

Мета роботи. Проаналізувати роботу алгоритму для перевірки орфографії в тексті основаного на моделі Noisy Channel. Спростити та прискорити роботу алгоритму.

Ми хочемо написати деяке слово Z із m букв, а виходить, що ми написали слово X із n букв. Виявляється, що правильне слово Z викривилось до