КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.214225
УДК 004.056

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет "Львівська політехніка", м. Львів, Україна
ORCID ID 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ КОРПОРАТИВНИХ КОРИСТУВАЧІВ

Анотація. Потреба в захисті облікових даних користувачів мережевих операційних систем є незаперечною на сьогодення, оскільки їх несанкціонована зміна в системі може звести нанівець роботу програмно-апаратних засобів захисту корпоративної інформації. Права доступу користувачам до інформаційних ресурсів корпорації встановлюються згідно розробленої політики інформаційної безпеки організації для збереження конфіденційності, цілісності та доступності корпоративної інформації. З огляду на це, в роботі розглядаються правила створення облікових даних користувачів корпоративної мережі та досліджуються способи забезпечення їх безпеки на основі мережевих операційних систем Windows. Визначено базовий список правил щодо створення, призначення та використання облікових даних, а саме: встановлення максимального обмеження адміністративних привілеїв для користувачів з привілеями адміністратора, надання користувачам та групам підтримки лише тих прав, які необхідні для виконання ними повсякденних завдань, використання облікових записів адміністраторів домену організації лише для керування контролерами домену. Організовано інсталяційний файл, який містить у собі комплекс найбільш поширених утиліт для адміністрування Active Directory (AD). Основою цього комплексу є утиліти: Account Lockout Examiner, Netwrix Auditor, SolarWinds Permissions Analyzer, Active Directory Health Profiler і Semperis DS Protector. Проведене моделювання щодо діагностики AD на предмет його захищеності показує, що використання зібраних утиліт в одному інсталяційному файлі значно спрощує процес моніторингу стану захищеності AD та проведення діагностики встановлених прав доступу користувачів. Встановлено, що найвищий рівень захищеності облікових записів привілейованих користувачів та системних адміністраторів засобами Active Directory досягається починаючи з Windows Server 2012 R2, оскільки ця ОС і пізніші версії володіють функціоналом захищеної групи користувачів, що дає змогу отримати додатковий захист проти компрометації їх облікових даних при виконанні процедури перевірки автентичності.

Ключові слова: мережева операційна система, облікові дані користувачів, контролер домену, права доступу користувачів, служба каталогів, сервер, корпоративна інформація.

ВСТУП

Інформаційна сфера відіграє одну з найбільш важливих ролей у забезпеченні безпеки всіх сфер життєдіяльності суспільства. Будь-який витік інформації у сферах життєдіяльності держави та суспільства може призвести до тяжких наслідків, паралізувати як поодинокі, так і складні високотехнологічні системи управління, збройні сили та спецслужби, спровокувати руйнівні аварії на екологічно небезпечних об'єктах.

Оскільки швидкий розвиток інформаційних технологій спонукає не менш швидкий розвиток методів і засобів отримання інформації незаконним шляхом, інформаційних атак, тощо, в наші дні, надзвичайно важливо прикласти всі зусилля для того, щоб забезпечити інформаційну безпеку.

Забезпечення цілісності, доступності і конфіденційності інформації є пріоритетним завданням будь-якої організації та держави в цілому. В епоху комп'ютеризації та автоматизації проблема комп'ютерної безпеки виходить на перший план. Одним із завдань, яке повинне вирішуватися в контексті інформаційної безпеки, забезпечення безпеки мережевих операційних систем. Однією із загроз для комп'ютерної безпеки є мережеві атаки.

Незважаючи на кроки світової спільноти, спрямовані на розвиток кібербезпеки, злочинці продовжують вдосконалювати і розробляти методи та засоби організації мережевих атак. На сьогодні склалася така ситуація, коли запропоновані методи захисту комп'ютерних систем та мереж не здатні забезпечити належний рівень інформаційної безпеки. Комп'ютерні системи постійно піддаються різним типам загроз, і користувач не може бути впевнений у безпеці важливої інформації, яка опрацьовується і зберігається у них. Сучасна ситуація стимулює пошук та розробку нових методів та рішень, спрямованих на підвищення рівня захисту комп'ютерних систем від шкідливого впливу.

Пошук вразливості є важливою частиною завдання забезпечення безпеки інформаційної системи, яке включає у себе регулярне її тестування. Наприклад, для тестування на вразливість мережевих операційних систем використовуються дистрибутиви Linux такі як Kali Linux, BackBox Parrot Security OS та інші.

Нині, на ринку IT є велика кількість серверних операційних систем, як від компаній Microsoft (Windows Server), Apple (macOS Server) так і операційні системи на базі Linux (Red Hat Enterprise Linux, Ubuntu Server, CentOS та інші). Велика кількість програмного забезпечення тягне за собою велику кількість загроз інформації, яка опрацьовується в системі, і тому виникає потреба у використанні усіх можливих методів та засобів захисту мережевих операційних систем, зокрема, забезпечення безпеки облікових даних користувачів від несанкціонованого витоку.

На цей час основними серверними операційними системами (ОС) є Windows Server та кілька Linux-дистрибутивів різної спрямованості. Кожна з цих операційних систем має свої переваги, недоліки та цілі застосування.

Windows Server популярна ОС в корпоративному сегменті, хоча більшість рядових користувачів і асоціюють Windows виключно з десктопною версією робочої станції. Залежно від завдань і необхідної для підтримки інфраструктури в експлуатації багатьох організацій знаходяться відразу кілька версій Windows Server, починаючи з Windows Server 2003 і закінчуючи останніми версіями — Windows Server 2019. 2008 R2, 2016 та 2019. [1,3]

Основні переваги серверів під керуванням Windows – відносна простота адміністрування, досить великий пласт інформації, мануалів та прикладного програмного забезпечення. Крім того, не можна обійтися без сервера на базі Windows, якщо в системі організації використовується програмне забезпечення або рішення, які використовують бібліотеки та частини ядра систем Microsoft.

Найчастіше Windows Server призначена для адміністрування інтранетів компаній та забезпечення працездатності специфічного програмного забезпечення, роботи баз даних MSSQL, інструментів ASP.NET або іншого спеціально створеного для Windows ПЗ. Це все ще повноцінна ОС, на якій можна розгорнути маршрутизацію, налаштувати DNS або будь-яку іншу службу. [2]

Постановка проблеми. З огляду на сказане, постає проблема щодо захисту інформаційної системи від несанкціонованого доступу до її ресурсів, що вимагає належної організації забезпечення безпеки відповідної мережевої операційної системи, зокрема, організації захисту та ефективного моніторингу облікових даних користувачів.

ISSN 2663 - 4023

Аналіз останніх досліджень і публікацій. Не зважаючи на постійні оновлення операційних систем (ОС), додавання нових програмно-апаратних засобів захисту інформації, кіберзлочинці знаходять і використовують нові вразливості мережевих ОС.

Згідно з [3] за останні 4 роки було виявлено та задекларовано 1428 вразливостей у Windows Server 2019. На діаграмах (рис 1, 2) вказані кількість та тип виявлених вразливостей.

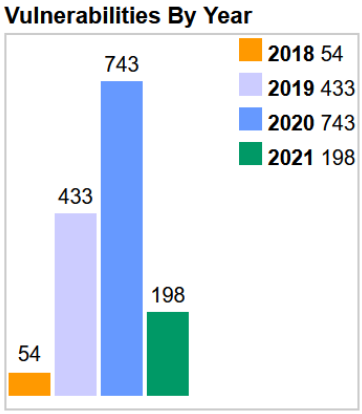

Рис 1. Кількість виявлених вразливостей в період 2018-2021 рр.

Документована інформація про атаки може бути корисною при складанні звітів для служби захисту інформації. Розуміння частоти й характеру атак дозволяє вжити адекватних заходів забезпечення безпеки ІС. Функціонування системи виявлення атак протягом тривалого часу надає інформацію про способи використання системи, що дозволяє виявити вади у здійсненні керування безпекою системи і внести правки у процедури її керування. Це дозволяє одержати корисну інформацію про реалізоване проникнення в захищену систему з наданням покращеної діагностики для виявлення й коригування факторів, які можуть сприяти її компрометації.

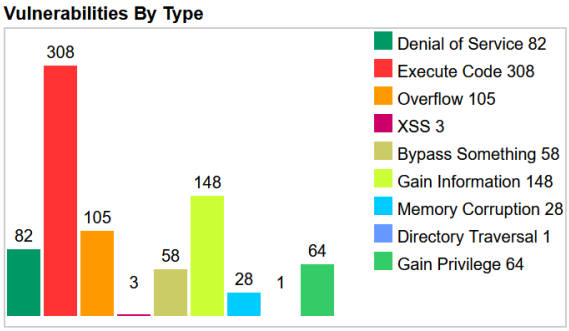

Рис 2. Типи виявлених вразливостей в період 2018-2021 рр.

Проте, головну небезпеку для компанії можуть становити не зовнішні зловмисники, що працюють в Інтернеті, так звані хакери, реальна загроза для сучасної компанії походить від внутрішніх зловмисників. За даними численних досліджень, понад 70-80% усіх порушень у корпоративному середовищі припадає на частку внутрішніх зловмисників [3]. Більше того, причинами порушення безпеки ІС організації можуть бути як неправомірні дії персоналу, так і навмисні дії з їх боку. Отже, за даними світової статистики, частка внутрішніх зловмисників, які навмисно здійснюють протиправні дії,

становить близько 20% усіх інцидентів у компанії, тоді як зовнішні зловмисники винні лише у 5% подібних випадках [4].

У [5] мова йде про основні методи виявлення вразливостей такі як тест на проникнення, аудит мережевої активів та створення Threat Intelligence. У [6] зосереджено увагу на структурі Metasploit Framework. На цей час Metasploit поставляється практично в усі дистрибутиви операційних систем Linux, і володіє найбільшими базами даних вразливостей та приймає близько мільйона завантажень щороку. Він також є одним з найскладніших проектів на сьогодення і призначений для того, щоб адміністратор безпеки був в курсі про вразливості, які знаходяться в тому чи іншому програмному забезпеченні.

Наприклад, у [7] описаний пошук вразливостей в мережі з використання Metasploit та утиліти rdpscan в ОС Kali Linux.

Отже, адміністратору безпеки було б доцільно мати у своєму розпорядженні засоби, які здійснюють аналіз ІС цілком і попереджають про потенційну можливість здійснення атаки на неї.

На рівні операційної системи слід використовувати засоби інформаційної безпеки для обмеження доступу до комп'ютерних ресурсів. Це відноситься і до ідентифікації і автентифікації терміналів і користувачів. Рекомендується, щоб всі користувачі мали унікальні ідентифікатори, які не повинні містити ознак рівня привілеїв користувача. У системі управління паролем повинні бути передбачені ефективні інтерактивні можливості підтримки необхідної їх якості. Використання системних утиліт має бути обмежено і ретельно контролюватися. [7, 8]

Мета статті. Визначити базовий список правил щодо створення, призначення та використання облікових даних користувачів, організувати комплекс найбільш поширених утиліт для адміністрування Active Directory (AD), провести діагностику AD на предмет моніторингу стану його захищеності та діагностики встановлених прав доступу користувачів, запропонувати серверну ОС, яка б володіла ефективним функціоналом захищеної групи користувачів, що дало б змогу отримати додатковий захист проти компрометації їх облікових даних.

НАЛАШТУВАННЯ ACTIVE DIRECTORY ДЛЯ ЗАПОБІГАННЯ ТИПОВИМ АТАКАМ

Основне правило, яким слід користуватися при створенні облікових даних – максимальне обмеження адміністративних привілеїв як для користувачів, так і для адміністраторів. Потрібно прагнути до того, щоб надавати користувачам та групам підтримки лише ті права, які необхідні для виконання ними повсякденних завдань.

Облікові записи адміністраторів домену/організації повинні використовуватися лише для керування доменом та контролерами домену. Ці облікові записи не можна використовувати для доступу та керування робочими станціями. Аналогічна вимога має пред'являтися для облікових записів адміністраторів серверів.

Для облікових записів адміністраторів домену бажано використовувати двофакторну автентифікацію. На своїх робочих станціях адміністратори повинні працювати під обліковими записами із правами звичайного користувача. Для захисту привілейованих облікових записів (адміністратори домену, Exchange, серверів) потрібно розглянути можливість використання групи захищених користувачів (Protected Users).

Заборона використання знеособлених загальних адміністративних облікових записів. Усі акаунти адміністраторів повинні бути персоніфіковані. Не можна запускати сервіси під обліковими записами адміністраторів (а надто адміністратора домену), бажано використовувати виділені облікові записи або Managed Service Accounts.

Заборона роботи користувачів у системі під правами локального адміністратора.

Для запобігання атакам типу Kerberoast рекомендовано налаштувати політику паролів і використовувати генератор випадкових паролів, а також мобільний додаток для зберігання цих паролів. Атака полягає у спробі знайти обліковий запис із певним паролем. Тобто, відбувається вибір імені користувача при зафіксованому паролі.

Політика безпеки AD допомагає вирішити дану проблему. Правильно налаштувавши вимоги до паролів можна значно ускладнити взлом облікового запису користувача. [9]

Рекомендації щодо протидії полягають у реалізації строгої парольної політики: мінімальна довжина пароля становить 10 символів для користувачів та 14 для адміністраторів. Поріг блокування облікового запису становить 5. Тривалість блокування доступу та складність вибирається за замовчуванням. Заборона використання попередніх паролів. Додавання правила, щоб новий пароль відрізнявся від попередніх на не менше ніж 3 символи.

При налаштованому максимальному терміні дії паролю 5-7 днів взлом облікового запису шляхом атаки з використанням словників або брут-форсу стає дуже важким і навіть сучасні потужні машину будуть витрачати на це багато часу.

Також рекомендується використовувати генератор випадкових паролів. В подібних генераторах можна налаштувати мінімальну довжину паролю і використання додаткових символів. Проте, запам`ятати подібний пароль досить важко. В такому випадку буде доречним використання додаткового програмного забезпечення на мобільному пристрої, в якому можна безпечно зберігати паролі окремо від облікових записів. [10]

Для того, щоб процес запам`ятовування подібних паролів став простішим, було використано мобільну версію додатка для зберігання паролів Sticky Password. Перевірити поточні налаштування політики паролів AD можна на будь-якому комп'ютері домену, для цього треба скористатись командою gpresult. [10]

ЗАСТОСУВАННЯ КОМПЛЕКСУ УТИЛІТ ДЛЯ КОНТРОЛЮ ЗА СТАНОМ ЗАХИЩЕНОСТІ ACTIVE DIRECTORY

Оскільки пошук та встановлення кожної потрібної утиліти окремо часозатратний процес, створено один інсталяційний файл, який містить у собі найбільш поширені утиліти для адміністрування AD.

Цей файл містить в собі комплекс утиліт: Account Lockout Examiner, Netwrix Auditor, SolarWinds Permissions Analyzer і Active Directory Health Profiler.

Запропонований комплекс утиліт значно спрощує аналіз та пошук вразливостей в Active Directory. Наприклад, для виводу статистики про стан захищеності AD, достатньо відкрити Netwrix Auditor або Active Directory Health Profiler (рис.3, 4).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

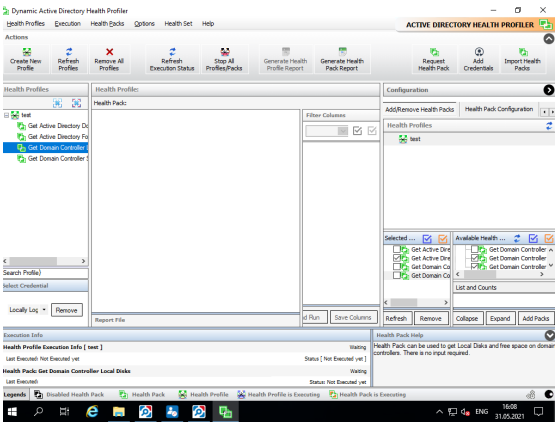

Рис. 3. Графічний інтерфейс AD Health Profiler

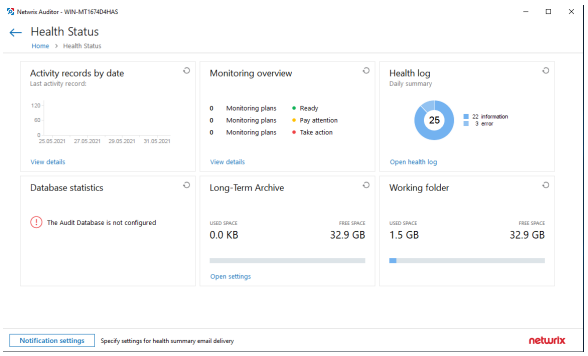

Рис.4. Відомості про стан захищеності AD

Також Netwrix Auditor (рис. 5, 6) надає інформацію про несанкціоноване втручання в систему, яка призводить до зміни або редагування/пошкодження файлів, що в свою чергу дозволяє оперативно прийняти міри для відновлення пошкоджених файлів та зменшення збитків від атаки.

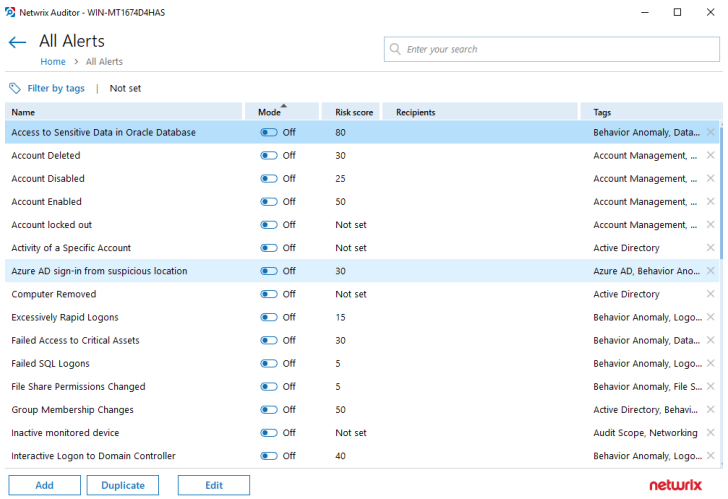

Рис. 5. Налаштування Netwrix Auditor для сповіщень про несанкціоноване втручання у систему

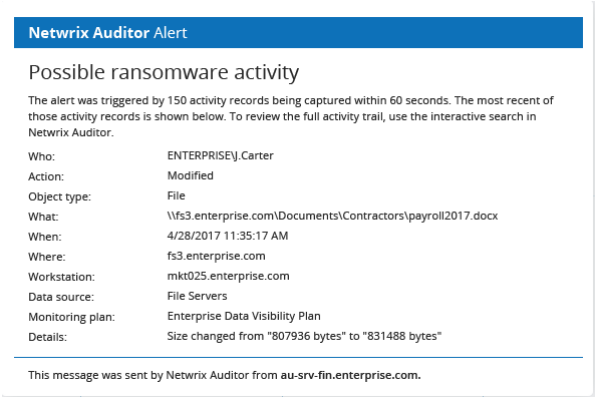

Рис. 6. Повідомлення Netwrix Auditor про втручання в систему

Account Lockout Examiner використано для перевірки облікових даних користувачів щодо їх блокування та виводу інформації про використання облікового запису при спробі уведення неправильного паролю. Використання цього інсталятора значно прискорює процес аналізу системи, пошуку загроз і вразливостей.

Для організації контролю за несанкціонованим доступом і повноваженнями користувачів можна запропонувати утиліту Semperis DS, яка відстежує всі зміни в Active Directory навіть тоді, коли вбудований механізм системного журналювання був відключений, записи реєстру видалені, а агенти зупинені. Semperis Directory Services Protector дозволяє швидко знаходити і усувати проблеми в цілях забезпечення доступності та безпеки системи.

Як приклад, проведено атаку з використанням утиліти mimikatz. Мета цієї атаки – підвищення прав доступу звичайного користувача до прав доступу адміністратора (рис.7).

Для виявлення цієї атаки використано утиліту Semperis DSP Після її запуску здійснено виклик DSP інтерфейсу (рис.8) та здійснено перехід у вкладку «Changes»

Рис. 7. Атака на зміну прав доступу з використанням mimikatz

Рис. 8. Використання інтерфейсу утиліти Semperis DSP для виявлення атаки

У вкладці «Changes» (рис.9) відображені усі користувачі системи, а також зміни над обліковими даними, які було зроблено. Зафіксувавши зміну атрибуту безпеки акаунту (облікових даних) атакованого користувача, необхідно вибрати поле зміненого акаунту правою кнопкою миші, що дозволяє відмінити всі дії, які зробив з обліковими даними користувача зловмисник, а саме – змінити адмінівські повноваження користувача на користувацькі.

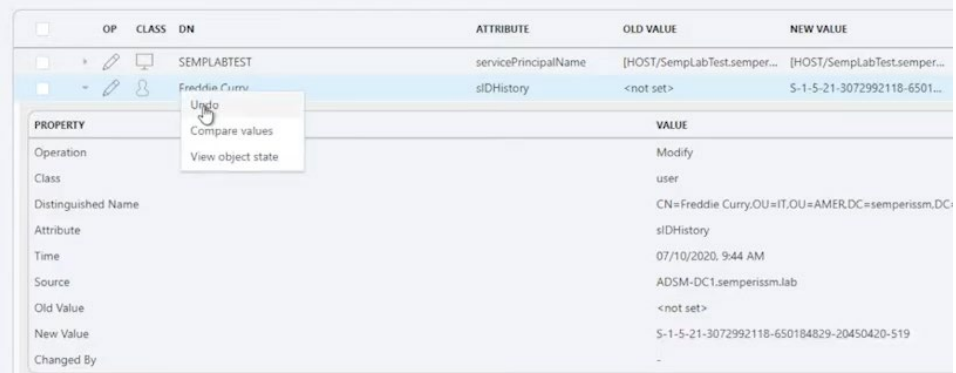

Рис. 9. Скасування змін в облікових даних користувача

Подане моделювання показує, що використання зібраних утиліт в одному інсталяційному файлі значно спрощує процес моніторингу стану захищеності AD та проведення діагностики встановлених прав доступу користувачів.

ЗАХИСТ ОБЛІКОВИХ ДАНИХ ЗАСОБАМИ ACTIVE DIRECTORY

У версії Active Directory, представленої в Windows Server 2012 R2, для підвищення захищеності привілейованих облікових записів користувачів з'явилася така глобальна група безпеки, як «Захищені користувачі» (Protected Users). Передбачається, що користувачі вказаної групи отримають додатковий захист проти компрометації облікових даних при виконанні процедури перевірки автентичності.

На користувачів цієї групи покладені наступні обмеження:

1. Користувачі цієї групи повинні проходити процедуру автентифікації лише за протоколом Kerberos. Пройти автентифікацію за протоколом NTLM (NT LAN Manager), дайджест-перевірки (Digest Authentication) або CredSSP (Credential Security Support Provider) не вдасться.
2. Для користувачів цієї групи в протоколі Kerberos при проходженні ними процедури попередньої автентифікації не повинні використовуватися такі алгоритми шифрування, як DES або RC4 із-за їх слабкої криптостійкості (необхідна підтримка як мінімум AES).
3. Ключі Kerberos з великим періодом використання не зберігаються у будь-якій пам'яті, а це означає, що при закінченні квитка видачі квитка Kerberos (TGT), термін дії якого за замовчуванням становить 4 години, користувач повинен повторно пройти процедуру автентифікації.
4. Для користувачів цієї групи не зберігаються їхні облікові дані для кешованого входу до домену. Тобто. при недоступності контролерів домену, ці користувачі не зможуть пройти процедуру автентифікації на своїх робочих станціях через cached credential.

Група Protected Users доступна лише за умови наявності функціонального рівня домену Windows Server 2012 R2 (і вище). Група з'явиться в консолі AD лише після підвищення рівня домену та закінчення реплікації даних між контролерами домену. Обмеження Protected Users працюють на Windows Server 2012 R2 та Windows 8.1

За замовченням група Protected Users group є порожньою і Microsoft рекомендує додати до неї облікові записи критичних користувачів (адміністраторів домену, серверів тощо). Очевидно, що функціонал захищеної групи користувачів вимагає ретельного тестування перед використанням у середовищі бізнес-процесу. Не варто відразу включати до цієї групи обліковий запис єдиного адміністратора домену.

При вході доменного користувача у Windows, за умовчанням його облікові дані (кешовані облікові дані: ім’я користувача та пароль) зберігаються на локальному комп’ютері. Завдяки цьому користувач зможе увійти на локальний комп’ютер, навіть якщо контролери домену AD недоступні, вимкнені або на комп’ютері відключено мережевий кабель. Функціональне кешування облікових даних доменних облікових записів зручне для користувачів ноутбуків, які можуть отримати доступ до свого локального комп’ютера, коли немає доступу до корпоративної мережі.

Вхід на комп'ютер під кешованими даними для користувача доступний, якщо він раніше хоча б один раз авторизувався на цьому комп'ютері, і пароль в домені не був змінений з моменту входу. Пароль користувача в cashed credentials без терміну давності. Якщо доменна політика паролів змусить змінити пароль користувача, його збережений пароль в локальному кеші комп’ютера не зміниться, поки користувач не вийде на комп’ютер під новим паролем. Тобто якщо пароль користувача в AD був змінений після останнього входу на комп’ютер, і комп’ютер знаходився весь час в офлайн-режимі без доступу до мережі, то користувач зможе увійти на цей комп’ютер під старим паролем.

За допомогою параметрів групових політик можна встановити кількість унікальних користувачів, чиї облікові дані можуть бути збережені в локальному кеші на комп'ютерах домену. Щоб дані потрапили до кешу, користувач повинен хоча б один раз залогінитися на комп'ютері.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З огляду на сказане можна констатувати, що Windows Server доцільно використовувати для вирішення корпоративних завдань. Системному адміністратору варто віддати перевагу Windows Server коли потрібно об'єднати різні об'єкти мережі (комп'ютери, сервери, принтери, різні сервіси) в єдину систему із забезпеченням їх захисту від несанкціонованого доступу. У цьому випадку Active Directory (AD) Windows Server виступають у ролі каталогу (бази даних), в якому зберігається інформація про користувачів, робочі станції, сервери, мережеві та периферійні пристрої. Також встановлено, що найвищий рівень захищеності облікових записів привілейованих користувачів та системних адміністраторів засобами Active Directory досягається починаючи з Windows Server 2012 R2, оскільки ця ОС і пізніші її версії володіють функціоналом захищеної групи користувачів, що дає змогу отримати додатковий захист проти компрометації їх облікових даних.

Напрямки подальших досліджень можуть бути спрямовані на підвищення ефективності моніторингу списку налаштувань безпеки та адміністрування AD шляхом збільшення номенклатури використання утиліт, наприклад, Quest Change Auditor, що дозволить своєчасно виявити зміни навіть у глибоко вкладених групах користувачів.\

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Reimer, M. Malker Active Directory for Windows Server 2003. Administrator's Guide/Per, with English, 2004.
2. Джон Мак-Кейб (John McCabe) і команда Windows Server16. Корпорація Майкрософт (Microsoft Corporation), 2016.
3. Microsoft Windows Server 2019: Secure Vulnerabilities [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26.
4. Symantec Internet Security Threat Report Volume 2015 [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.slideshare.net/WaqasAmir/symantec-internetsecuritythreatreportvolume 2015social-v2.
5. Dosal E. How to Find Security Vulnerabilities [Електронний ресурс] / Eric Dosal – Режим доступу до ресурсу: https://www.compuquip.com/blog/how-to-find-security-vulnerabilities.
6. Robert W. Beggs. (2014). Mastering Kali Linux for Advanced Penetration Testing. Published by Packt Publishing Ltd., p. 356. ISBN 978-1-78216-312-1.
7. Mimikatz DCSync Usage, Exploitation, and Detection [[Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?p=1729.
8. Sneaky Active Directory Persistence Tricks [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?p=1929.
9. Політика паролів облікових записів AD [Електронний ресурс] – Режим доступу до ресурсу: https://mobiz.com.ua/polityka-paroliv-oblikovykh-zapysiv-v-active-directory.html.
10. Finding Passwords in SYSVOL & Exploiting Group Policy Preferences. [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?p=2288.
11. Cracking Kerberos TGS Tickets Using Kerberoast ~ Exploiting Kerberos to Compromisethe Active Directory Domain [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?p=2293.
12. Detecting Kerberoasting Activity [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/2p=3458.

Accidental Sabotage: Beware of CredSSP [Електронний ресурс] – Режим доступу до ресурсу: https://www.powershellmagazine.com/2014/03/06/accidental-sabotage-beware-of-credssp/.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Ivan Tyshyk
Ph.D, Docent,
Associate Professor Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ENSURING THE SECURITY OF CORPORATE USERS ACCOUNTS

Abstract. Today, the need to protect user accounts of network operating systems is beyond doubt, as unauthorized changes to them in the system can negate the operation of software and hardware tools to protect corporate information. User access rights to the corporation's information resources are established in accordance with the organization's information security policy in order to maintain the confidentiality, integrity and availability of corporate information. With this in mind, the article discusses the rules for creating users accounts for a corporate network and explores ways to ensure their security based on Windows network operating systems. The basic list of rules for creating, assigning and using credentials is defined, namely: setting the maximum restriction of administrative rights for users with administrator rights, providing users and support groups with only those rights that they need to perform their daily tasks, using the organization's domain administrator accounts only to manage domain controllers. An installation file is organized that contains a set of the most common Active Directory (AD) administration utilities. The core of this package is made up of the following utilities: Account Lockout Examiner, Netwrix Auditor, SolarWinds Permissions Analyzer, Active Directory Health Profiler, and Semperis DS Protector. Modeling of AD security diagnostics has shown that using the collected tools in a single installation file greatly simplifies the process of monitoring the AD security status and diagnosing the established user access rights. It has been established that the highest level of security for accounts of privileged users and system administrators using Active Directory is achieved starting with Windows Server 2012 R2, since this OS and later versions implement the functionality of a protected user group, which provides additional protection against compromising their credentials during the authentication procedure.

Keywords: network operating system, user accounts, domain controller, user access rights, directory service, server, corporate information.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. S. Reimer, M. Malker Active Directory for Windows Server 2003. Administrator's Guide/Per, with English, 2004.
2. Джон Мак-Кейб (John McCabe) and Windows Server16 staff. Microsoft Corporation, 2016.
3. Microsoft Windows Server 2019: Secure Vulnerabilities [Electronic resource]. – 2019. – Access mode: https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26.
4. Symantec Internet Security Threat Report Volume 2015 [Electronic resource]. – 2015. – Access mode: https://www.slideshare.net/WaqasAmir/symantec-internetsecuritythreatreportvolume 2015social-v2.
5. Dosal E. How to Find Security Vulnerabilities [Electronic resource] / Eric Dosal – Access mode: https://www.compuquip.com/blog/how-to-find-security-vulnerabilities.
6. Robert W. Beggs. (2014). Mastering Kali Linux for Advanced Penetration Testing. Published by Packt Publishing Ltd., p. 356. ISBN 978-1-78216-312-1
7. Mimikatz DCSync Usage, Exploitation, and Detection [Electronic resource] - Access mode: https://adsecurity.org/?p=1729.
8. Sneaky Active Directory Persistence Tricks [Електронний ресурс] – Режим доступу до ресурсу: https://adsecurity.org/?p=1929.
9. AD account password policy [Electronic resource] – Access mode: https://mobiz.com.ua/polityka-paroliv-oblikovykh-zapysiv-v-active-directory.html.
10. Finding Passwords in SYSVOL & Exploiting Group Policy Preferences. [Electronic resource] - Access mode: https://adsecurity.org/?p=2288.

11. Cracking Kerberos TGS Tickets Using Kerberoast ~ Exploiting Kerberos to Compromisethe Active Directory Domain – [Electronic resource] - Access mode: https://adsecurity.org/?p=2293.
12. Detecting Kerberoasting Activity [Electronic resource] - Access mode: https://adsecurity.org/2p=3458.
13. Accidental Sabotage: Beware of CredSSP [Electronic resource] - Access mode: https://www.powershellmagazine.com/2014/03/06/accidental-sabotage-beware-of-credssp/.