Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: **Аналіз вразливостей Active Directory та методи їх усунення**

Виконав(ла): студент(ка) IV курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Теслюк В.А. (прізвище та ініціали)

Керівник (підпис) Стадник М.А. (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Завідувач кафедри (підпис) (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

АНОТАЦІЯ

Аналіз вразливостей Active Directory та методи їх усунення // Кваліфікаційна робота ОР «Бакалавр» // Теслюк Віталій Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. ___ , рис. ___ , табл. – , кресл. – , додат. ___.

КЛЮЧОВІ СЛОВА: ДОМЕН, WINDOWS SERVER, ACTIVE DIRECTORY, КІБЕРАТАКА.

У роботі було розглянуто та описано основні загрози можливих атак на Active Directory, оскільки використання Windows Server є досить популярним.

Було розглянуто головні можливості атак на доменну систему та описано основні процедури, які дозволять запобігти хакерським атакам.

У другому розділі було проаналізовано уразливість домену від програм-вимагачів, які наносять найбільшу шкоду підприємствам, які залежать від корпоративних мережевих структур, особливо важливими компонентами в умовах пандемії та війни.

У третому розділі було проведено дослідження вразливості основних служб Active Directory при ураженні програмами –вимагачами.

Встановлено , що основними аспектами найбільшого посилення захисту є своєчасне оновлення усіх систем корпоративної мережі та підвищення кваліфікації персоналу щодо обізнаності в процедурах запобігання хакерським атакам.

ABSTRACT

Analysis of Active Directory vulnerabilities and methods of their elimination // Qualification work of OR "Bachelor" // Teslyuk Vitaly Andriyovych // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, Group SB-41 / / Ternopil, 2023 // P. ___ , fig. ___ , tables ___ , Diagrams ___, Annexes. ___.

KEYWORDS: DOMAIN, WINDOWS SERVER, ACTIVE DIRECTORY, CYBER ATTACK.

The work considered and described the main threats of possible attacks on Active Directory, since the use of Windows Server is quite popular.

The main possibilities of attacks on the domain system were considered and the basic procedures that will prevent hacker attacks were described.

The second chapter analyzed the vulnerability of the domain to ransomware, which causes the most damage to businesses that depend on corporate network structures, especially important components in the context of a pandemic and war.

In the third chapter, a study of the vulnerability of the main Active Directory services when affected by ransomware programs was conducted.

It has been established that the main aspects of the greatest strengthening of protection are the timely updating of all corporate network systems and the improvement of personnel's qualifications regarding awareness of the procedures for preventing hacker attacks.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IT – інформаційні технології

AD – Active Directory

LDAP – Lightweight Directory Access Protocol

DC – Domain Controller

AD DS – Active Directory Domain Services

Azure AD – Azure Active Directory

RDP – Remote Desktop Protocol

LLMNR – Link-Local Multicast Name Resolution

SPN – Service Principal Name

GPO - об’єкти групової політики

RaaS - Ransomware-as-a-Service

ЗМІСТ

ВСТУП

Немає сумніву в тому, що інформаційні технології (ІТ) і комп'ютери відіграють невід'ємну роль у повсякденній діяльності підприємств і організацій сучасного суспільства. ІТ-системи значно підвищили продуктивність на сучасному робочому місці, і, як наслідок, виникла така залежність від цього, що «ІТ-послуги стають критично важливою інфраструктурою, так само як дороги, електрика, водопровідна вода та фінансові послуги» [1]. Коли ІТ-системи перестають функціонувати в бізнес-середовищі, компанії можуть втратити велику суму грошей через невикористану заробітну плату персоналу, втрачені можливості та шкоду репутації [2]. Кіберзлочинці зрозуміли це й почали використовувати шкоду, спричинену знищенням даних і простоєм, використовуючи особливу форму зловмисного програмного забезпечення під назвою програм-вимагачів. Розроблені для того, щоб утримувати систему або її вміст у заручниках, доки не буде сплачено викуп, вони завдають особливої шкоди організаціям через вищезгадані наслідки простою, що робить організації набагато більш прибутковими цілями. Прибутковість програм-вимагачів залежить від готовності платити викуп, і коли вартість простою в 23 рази перевищує середню вимогу викупу, не дивно, що індустрія програм-вимагачів продовжує розвиватися [2]. Оскільки простої мають найбільші фінансові наслідки, коли йдеться про використання корпоративних ІТ, у поєднанні з загрозою шантажу через викрадені файли, піддатися вимогам викупу стає дуже привабливим. У дослідженні 2018 року дослідникам вдалося відстежити приблизно 16 мільйонів доларів у вигляді викупу протягом дворічного періоду від потенційних 19 750 жертв [3], з подальшими оцінками загальних платежів понад 25 мільйонів доларів в період між 2016 і 2016 роками. 2017 [4]. Лише програма-вимагач SamSam принесла своїм

розробникам 6,5 мільйонів доларів протягом трохи менше 2 років [5], причому її найвища сума викупу зафіксована в 64 000 доларів [6]. Хоча прибутки від програми-вимагача здаються непомірними, вартість збитків ще більш вражаюча. Deep Instinct оцінює, що загальна вартість збитків від програм-вимагачів у 2019 році перевищила прогнозовані 11,5 мільярдів доларів, а також заявляє, що розробники програм-вимагачів спеціально націлювалися на великі підприємства через їх прибутковість [7]. Таким чином, організаціям і підприємствам слід вжити додаткових заходів, щоб зменшити ймовірність стати жертвою програм-вимагачів. Одним із методів зменшення цієї можливості є створення плану, заснованого на всій доступній інформації, і якщо доступної інформації бракує, прогалину необхідно заповнити. Як правило, використання менш технічних навичок користувачів було б найпростішим шляхом для злому, оскільки більшість співробітників компаній за межами IT-індустрії навчаться лише IT-навичок, необхідних для ефективного виконання своєї роботи. Ці IT-навички, в очах користувача, не включатимуть уміння ефективно оцінювати та припиняти будь-які потенційні кіберзагрози. Таким чином, контролери домену, якими в ідеалі керують лише навчені IT-фахівці з обізнаністю про кіберситуацію, теоретично повинні бути менш сприйнятливими до загроз, ніж пристрої, якими керують люди з меншою технологічною кваліфікацією. Однак, оскільки зловмисне програмне забезпечення продовжує розвиватися, вектори загроз зміщуються. WannaCry, один із найвідоміших варіантів програм-вимагачів у новітній історії, має здатність поширюватися між хостами в мережі без взаємодії з користувачем, використовуючи вразливість мережевого протоколу, і аж ніяк не є єдиною формою програм-вимагачів, яка може це робити. Таким чином, контролери домену, що працюють на Windows Server, які стикаються з підвищеним доступом до мережі, щоб пропонувати свої послуги, так само сприйнятливі до сучасних програм-вимагачів, як і звичайні споживчі версії Windows. Незважаючи на наявність

запитів, пов’язаних із програмним забезпеченням-вимагачем щодо Windows Server і, крім того, контролерів домену, опублікованих IT-фахівцями на різних інтернет-форумах і дошках обговорень, схоже, що академічного матеріалу та інформації щодо цієї конкретної теми явно бракує.

1. ОГЛЯД ВИДІВ АТАК НА ACTIVE DIRECTORY

1.1. Аналіз головних можливостей атак на Active Directory

Розуміння хакерських методів і процесів — найкращий спосіб захисту від кібератак, а зосередження на бізнес-ризиках — найкращий спосіб отримати пакет безпеки.

Багато організацій щодня зазнають кібератак; вони піддаються всім видам інцидентів безпеки. Деякі з найшкідливіших програм, як-от програми-вимагачі, можуть повністю зупинити бізнес. Нижче наведено кілька типів інцидентів безпеки, через які керівники служби безпеки не можуть мати нормального функціонування.

Найпопулярнішими з них є представлені на рис. 1.1:

Рисунок 1.1 – Найбілш поширені інциденти безпеки.

Перш ніж перейти до поширених методів злому, давайте зробимо підсумок компонентів Active Directory.

Active Directory (AD) — це служба каталогів, яка допомагає керувати мережевими мережами, автентифікувати, групувати, організовувати та захищати корпоративні доменні мережі. Це дозволяє користувачам і

комп’ютерам отримувати доступ до різних мережевих ресурсів, таких як увійти в систему Windows, друкувати на мережевому принтері, отримувати доступ до спільного доступу до мережевих файлів, отримувати доступ до хмарних ресурсів за допомогою єдиного входу або надсилати простий електронний лист.

Більшості користувачів зазвичай надається просте ім’я користувача та пароль, які пов’язані з їхнім об’єктом облікового запису AD, у якому у фоновому режимі AD використовує LDAP (Lightweight Directory Access Protocol), щоб перевірити правильність пароля та чи справді користувач авторизований як частина групи або політики. Стандартні користувачі зазвичай є частиною групи користувачів домену та мають доступ до будь-якого об’єкта, де авторизовано користувачів домену. Адміністратор AD буде частиною групи під назвою «Адміністратори домену», яка є високопривілейованою групою, що може робити в мережі буквально все, що завгодно. Інколи адміністратора домену називають «ключами від королівства».

AD має численні групи, які дозволяють різні ролі та авторизації, і які, для всіх організацій, повинні бути добре керовані та захищені, щоб зменшити ризик отримання зловмисниками доступу через прості неправильні конфігурації Active Directory.

Active Directory — це ієрархія, яка зазвичай називається деревом (один домен) або лісом (кілька доменів), у якій зберігається інформація, яка називається об’єктами. У верхній частині домену знаходиться контролер домену Domain Controller (DC), який використовується для розміщення копії доменних служб Active Directory Domain Services (AD DS) — це схема для всіх об’єктів, які AD зберігає або надає послуги автентифікації та авторизації.

Name	Type	Description
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords re...
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish cert...
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers ...
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic ...
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative ...
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Cont...
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for ...
HelpLibraryUpdaters	Security Group - Domain Local	
Key Admins	Security Group - Global	Members of this group can perform administrative ...
Protected Users	Security Group - Global	Members of this group are afforded additional prot...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access prop...
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Cont...
Schema Admins	Security Group - Universal	Designated administrators of the schema
SQLServer2005SQLBrowserUser$WIN-01S0KHJ45UC	Security Group - Domain Local	Members in the group have the required access and...

Рисунок 1.2 - Загальні групи в Active Directory

У великих доменах або глобальних організаціях AD DS включає можливість відтворювати зміни на контролерах домену в межах одного домену чи лісу. Контролер домену також дозволяє адміністраторам домену керувати всіма об’єктами всередині, такими як облікові записи користувачів і мережеві ресурси.

Доменні служби Active Directory включають наступні:

Схема об’єктів і атрибутів

Глобальний каталог усіх об’єктів у каталозі

Можливість пошуку та запиту об'єктів

Служба реплікації для доставки каталогу на інші контролери домену.

Сховище даних AD DS є життєво важливим компонентом Active Directory, яка є базою даних, яка зберігає та обробляє всю інформацію для користувачів, служб і програм. Сховище AD DS зазвичай називається ntds.dit і розташоване в папці %systemroot%\NTDS на контролері домену.

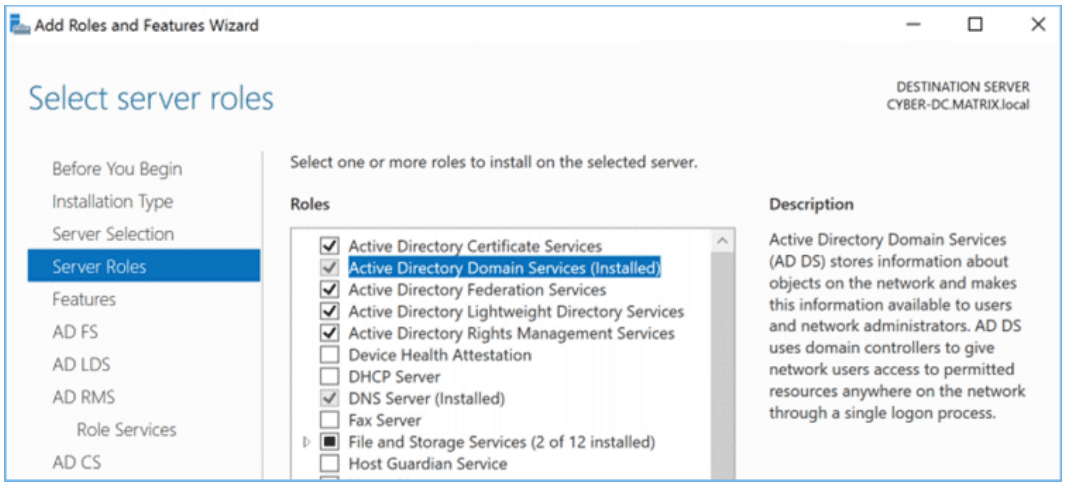


Рисунок 1.2 - Ролі сервера AD

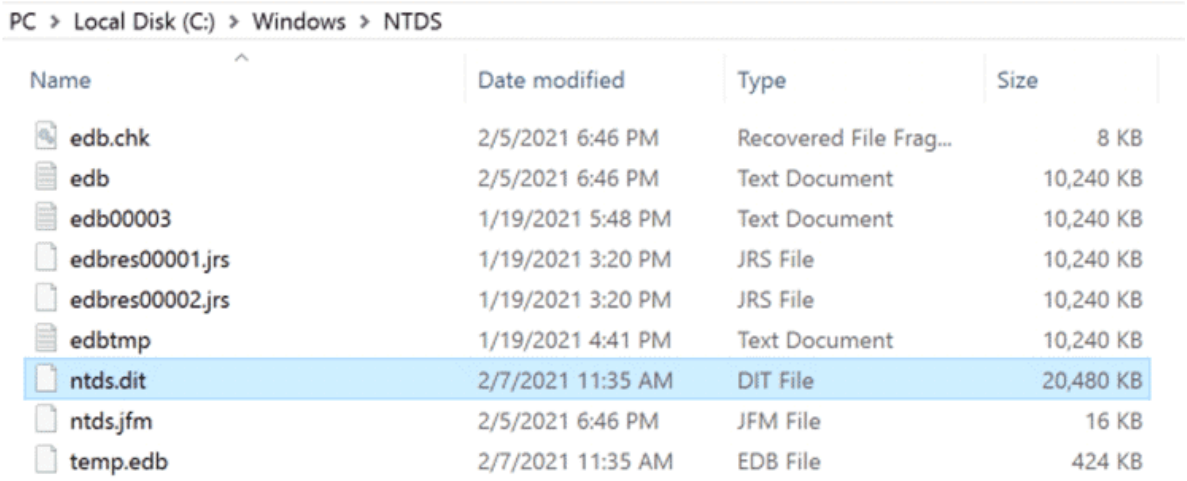


Рисунок 1.3 – Файл ntds.dit, яка знаходиться в %systemroot%

Схема доменних служб Active Directory — це визначення всіх об’єктів, що зберігаються в каталозі, і забезпечує виконання правил щодо нових створених об’єктів і оновлень об’єктів. Вони розділені на типи об’єктів, такі як класи, наприклад, користувачі та комп’ютери, або атрибути, які є інформацією, що міститься в об’єкті, як-от ім’я та прізвище.

Домени зазвичай використовуються для групування та керування об’єктами в організації, наприклад, застосування правил і політик щодо того, як слід використовувати об’єкти, і додавання можливостей для ролей і політик щодо того, хто має доступ до чого, або хто може вносити зміни чи оновлення до Active Directory.

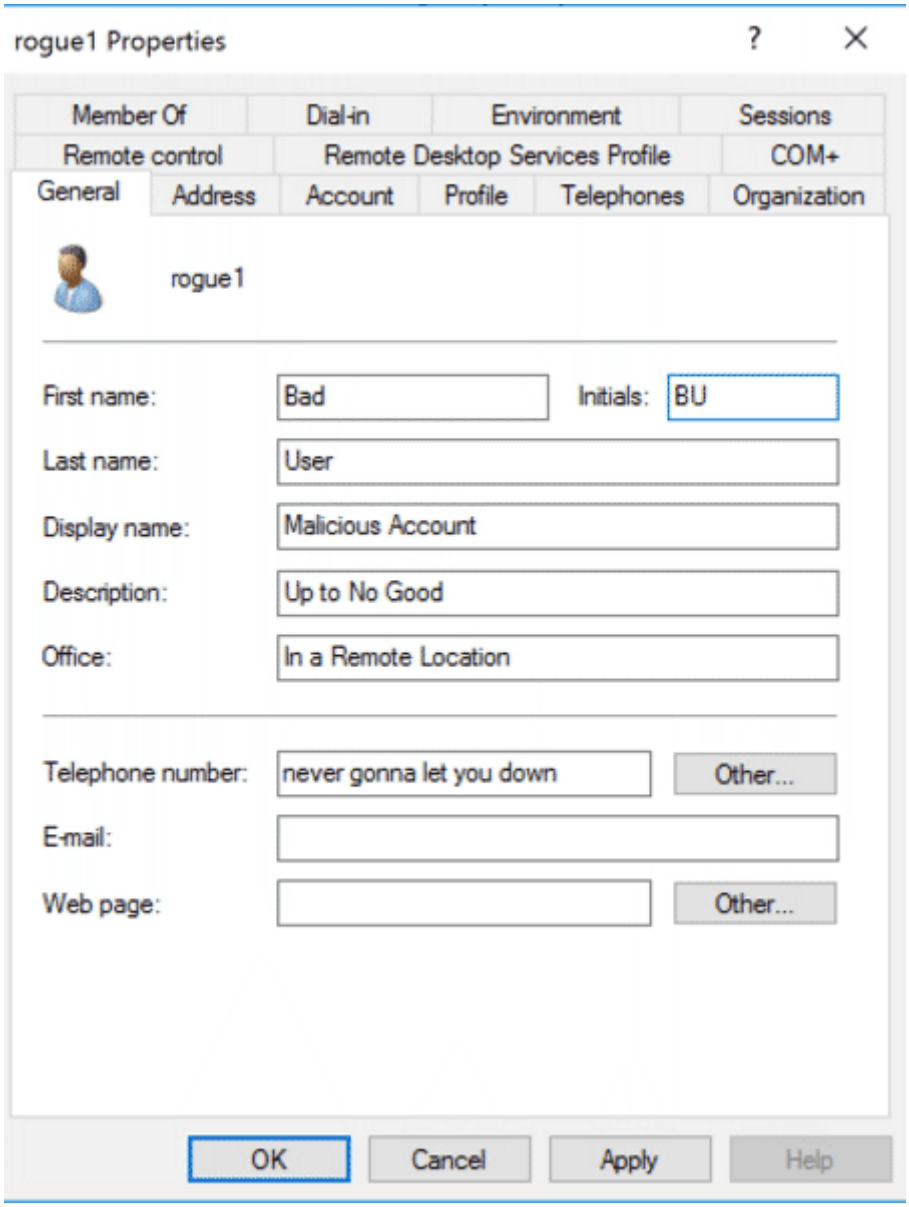


Рисунок 1.4 - Приклад об’єкта класу користувача та атрибутів об’єкта.

Як згадувалося раніше, домени також можна згрупувати в дерево з субдоменами, які мають той самий простір імен, що й батьківський; вони називаються дочірніми доменами.

Наприклад, верхній домен може бути iamthetop.com, а субдомен — child1.iamthetop.com і child2.iamthetop.com. Між доменами створюється двостороння транзитивна довіра.

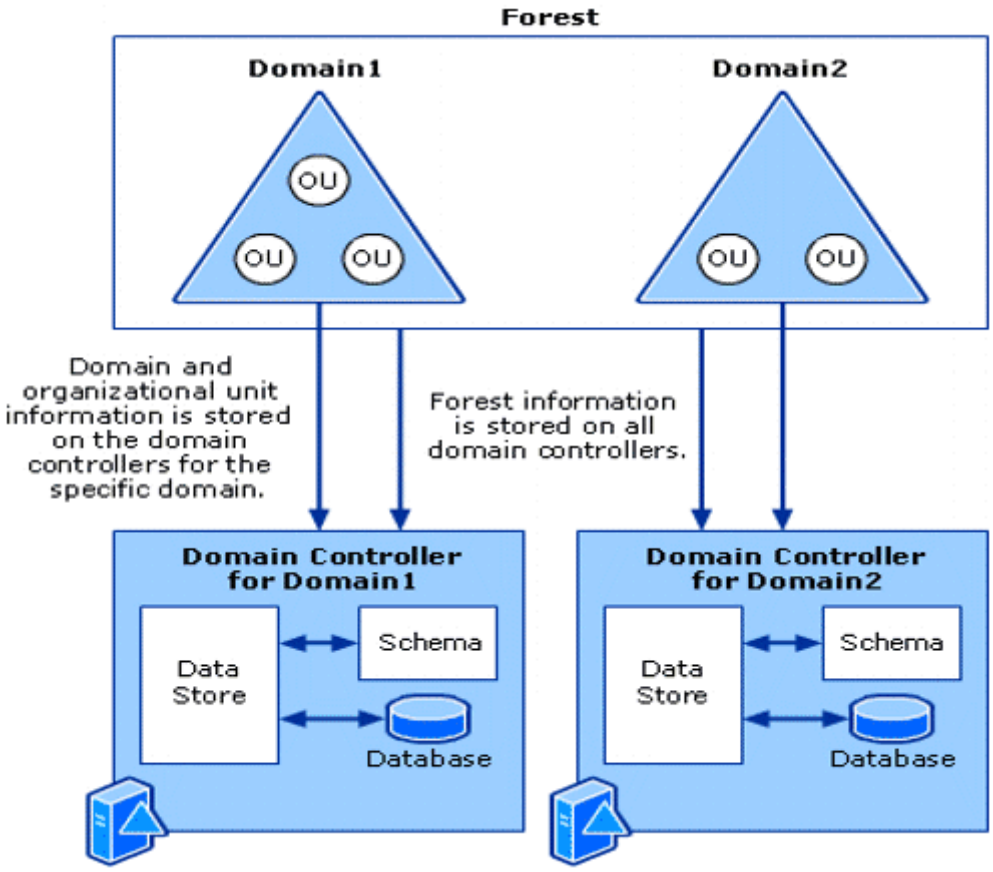


Рисунок 1.5 - Структура AD

Дерева та ліси доменів створюють розділи між доменами, які забезпечують більш детальний контроль над тим, як дані реплікуються між кожним доменом. Це типово для більш складних організацій, які мають кілька бізнес-підрозділів або географічних розташувань і хочуть обмежити доступ і забезпечити відповідність політик, наприклад, місцевим вимогам. Ліси можуть мати спільну схему та конфігурацію. Глобальний каталог, який можна шукати або запитувати в доменах, дає змогу встановлювати різні рівні довіри між доменами та лісом.

Active Directory також надає можливість групувати об’єкти в контейнери або, як я їх називаю з огляду на мій досвід керування системами, — колекції. Ці контейнери називаються організаційними одиницями (OU) і використовуються для структурування бізнесу та полегшення керування. Це дозволяє застосувати підхід до ролі та обсягу. Наприклад, у вас може бути адміністратор домену, який відповідає за Північну Америку, і інший

адміністратор домену, який відповідає за EMEA. Такий підхід дозволяє обмежити обсяг їхніх привілеїв і делегувати права адміністратора лише тим об’єктам у їхньому регіоні. Він також надає можливість застосовувати різні політики в усіх доменах.

Active Directory надає два типи довіри для встановлення рівня довіри між доменами. Один — спрямована довіра, яка є односторонньою довірою між доменами; інша — транзитивна довіра, двостороння довіра домену, яка включає субдомени.

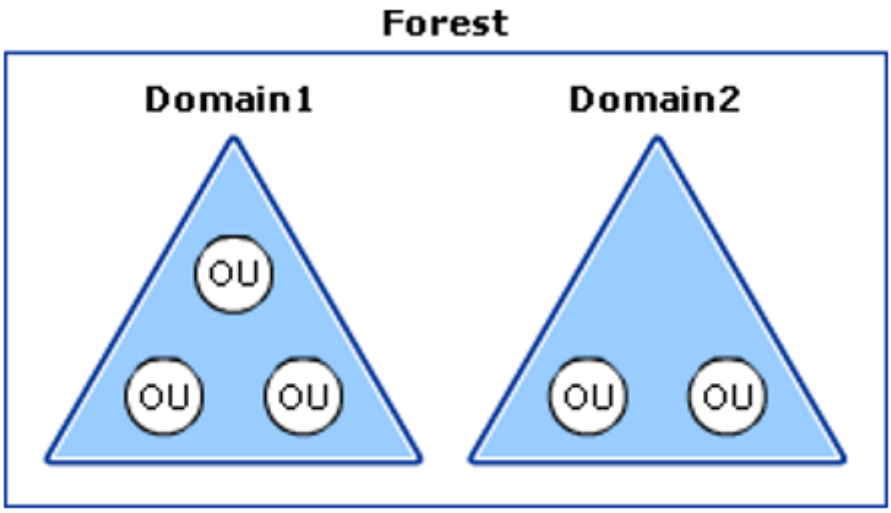


Рисунок 1.6 - Логічна структура AD

Azure Active Directory (Azure AD) — це хмарна служба ідентифікації, яка може синхронізувати ваше сховище даних Active Directory і розширити можливості для ввімкнення додаткових хмарних служб, таких як єдиний вхід і багатофакторна автентифікація. Microsoft Azure можна використовувати для підключення та автентифікації в багатьох програмах на основі SaaS, включаючи Microsoft 365.

Серйозний інцидент із безпекою нещодавно виявив великий ризик. Зловмисники використовували продукт SolarWinds Orion, щоб розгорнути бекдор до мереж багатьох організацій. Вони використовували привілеї локального адміністратора домену, щоб отримати доступ і підробляли токени

SAML. Це дозволило їм перейти з локального середовища жертви до свого хмарного середовища.

Все почалося 9 грудня 2020 року, коли FireEye оприлюднила подробиці про інцидент безпеки, пов'язаний із крадіжкою деяких інструментів проникнення Red Team. Після розслідування компанія FireEye (яка має одні з найкращих у світі аналітиків із реагування на інциденти та зловмисне програмне забезпечення) швидко проаналізувала зловмисне програмне забезпечення та почала з'ясовувати подробиці того, що сталося. 12 грудня вони повідомили SolarWinds про троянський бекдор, прихований у продукті SolarWinds Orion. Деталі цього жахають, оскільки він спрямований на один із наших найважливіших засобів контролю безпеки та довірчих механізмів для вирішення проблем із безпекою — процес оновлення програмного забезпечення/безпеки з цифровим підписом.

FireEye назвав зловмисників UNC2452 (він же Dark Halo, SolarStorm і Solarigate). Через те, що загроза ще не повністю підтверджена, він, ймовірно, пізніше отримає свій псевдонім APT Group. Це всесвітня кампанія, яка має далекосяжні наслідки. Багато постачальників виявили бекдор трояна, і ви можете переглянути результати виявлення ядра VirusTotals. За словами Касперського, UNC2452 може бути пов'язаний з Kazuar.

Отже, як видно, Active Directory відіграє життєво важливу роль у забезпеченні доступу та безпеки в багатьох організаціях, як локальних, так і хмарних. Погане керування та неправильна конфігурація Active Directory може дозволити зловмиснику отримати доступ до критично важливих систем цих організацій і розгорнути зловмисне програмне забезпечення, як-от програми-вимагачі, що може призвести до різкої зупинки бізнесу. Це може призвести до величезних фінансових втрат і публічного розголошення конфіденційних даних компанії та співробітників. Для багатьох підприємств це може бути катастрофічним і спричинити значні фінансові витрати на відновлення або недотримання вимог.

Важливо зробити привілейований доступ і безпеку Active Directory головним пріоритетом. Якщо зловмисник отримує доступ до облікових записів адміністратора вашого домену, для вас гра закінчена.

Повністю скомпрометований обліковий запис адміністратора домену є справжнім інцидентом безпеки; відповідь, швидше за все, означає перебудову вашого домену Active Directory ~Джозеф Карсон

Щоб отримати доступ до жертв, зловмисники використовують різноманітні методи злому, які використовують переваги поганого керування доступом, неправильної конфігурації та невиправлених систем. Створіть хорошу стратегію безпеки на основі надійної оцінки ризиків для бізнесу та надайте пріоритет кіберстійкості бізнесу.

Нижче наведено деякі з найпоширеніших причин інцидентів безпеки. Як ви можете зрозуміти з цього, хороша стратегія безпеки – це та, яка охоплює всі основи та багато іншого.

Рисунок 1.7 – Найпоширеніші причини виникнення інцидентів безпеки

1.2. Головні методи зменшення ризиків Active Directory.

Нижче наведено сім найпоширеніших неправильних налаштувань Active Directory, які зловмисники швидко виявляють і зловживають ними.

Коли зловмисник закріпиться у вашій мережі, він виконає розширений перелік зламаних систем, щоб створити цифровий план вашого Active Directory і структури вашої мережі, включаючи потенційні цілі великої вартості. Зловмисники створюють цей проект на основі мережевих зв'язків, відкритих протоколів, відкритих портів, мережевих сканувань і навіть назв серверів, які ми зазвичай називаємо на основі послуги, яку кожен надає, наприклад SQL Server, ERP DB тощо.

Користувачі домену з правами локального адміністратора

Додавання користувачів домену до групи локальних адміністраторів є типовою помилкою. Хоча зловмисник може не мати прав локального адміністратора в системі, яка забезпечила початкову точку опори, він швидко спробує виявити неправильні конфігурації та ідентифікувати будь-які мережеві системи, які включають користувачів домену в групу локальних адміністраторів. Ця неправильна конфігурація дозволяє зловмиснику переміщатися по мережі та підвищувати облікові дані користувача домену до локального адміністратора.

Ця неправильна конфігурація є величезним ризиком. Якщо зловмиснику вдається ввійти в кінцеву точку Windows як локальний адміністратор, він може використати цю скомпрометовану систему та обліковий запис як проміжну систему, яку потім можна використовувати для внесення змін у мережу, підвищення привілеїв до повного адміністратора домену та відключення будь-яких налаштувань безпеки .

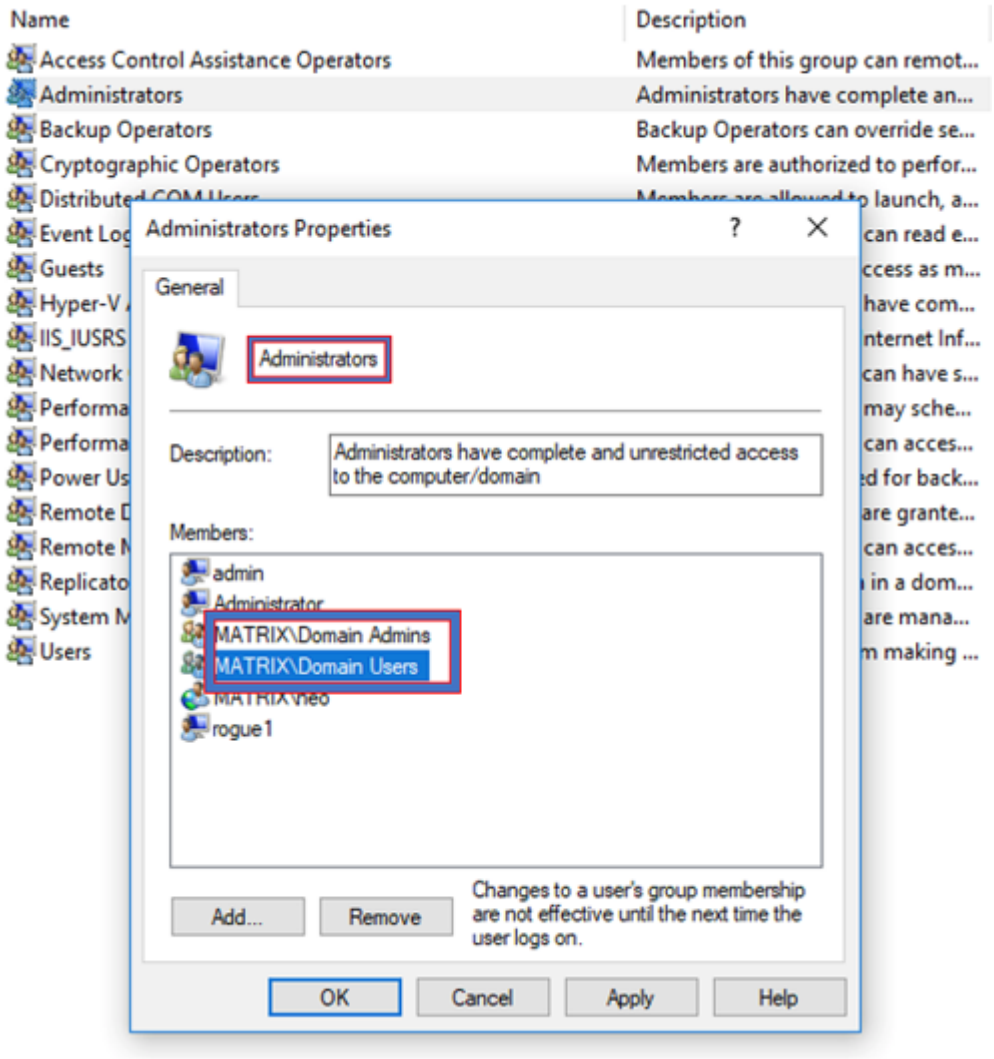


Рисунок 1.8 – Користувачі домену в групі локальних адміністраторів

Для запобігання таких інцидентів ніколи не додавайте користувачів домену до групи локальних адміністраторів. Переконайтеся, що ви постійно виявляєте цю критичну неправильну конфігурацію. Якщо вам потрібно, щоб користувач домену тимчасово отримав привілеї локального адміністратора, застосуйте принцип найменших привілеїв, використовуючи рішення безпеки привілеїв кінцевої точки, яке може підвищувати привілеї за вимогою, навіть не потребуючи, щоб користувач був локальним адміністратором. Ви також можете явно додати користувача до локальної групи адміністратора; однак це має бути тимчасовим явищем і ніколи постійним.

Слабкі та повторно використовувані паролі: улюблена ціль зловмисників.

Це одна з найпоширеніших причин, через яку зловмисники отримують доступ до мережевих систем Active Directory, щоб встановити свою початкову точку опори та налаштувати проміжну зону. За останні роки у зв'язку з піндемією, а далі війною тисячі організацій увімкнули віддалений доступ до численних бізнес-додатків і систем, щоб співробітники могли працювати з дому та мати доступ до критично важливих бізнес-додатків. Однак інколи це означає серйозний ризик для забезпечення безперервних операцій бізнесу.

Для багатьох із цих організацій паролі є єдиним засобом захисту доступу до інфраструктури. Дуже часто ці паролі є слабкими або використовувалися повторно. Нижче наведено деякі методи, які зловмисники використовують для зловживання цими паролями.

Завжди використовуйте надійні паролі. Використовуйте рішення для керування привілейованим доступом, щоб створювати надійні парольні фрази, щоб співробітникам не доводилося це робити.

Brute Forcing атака Remote Desktop Protocol (RDP)

Зловмисники постійно сканують кінцеві точки з увімкненим протоколом віддаленого робочого стола. Вони використовують різні засоби сканування, такі як Massscan або Nmap, щоб виявити системи з відкритим портом 3389.

Використовуючи такі інструменти, як crowbar, зловмисники намагатимуться підібрати слабкі облікові дані при допомозі brute-force. Після успішного перебору зловмисники отримують віддалений доступ до скомпрометованої системи. Це поширена проблема, коли користувачі повторно використовують паролі для свого корпоративного облікового запису Active Directory, які вони також використовували в звичайних Інтернет-службах.

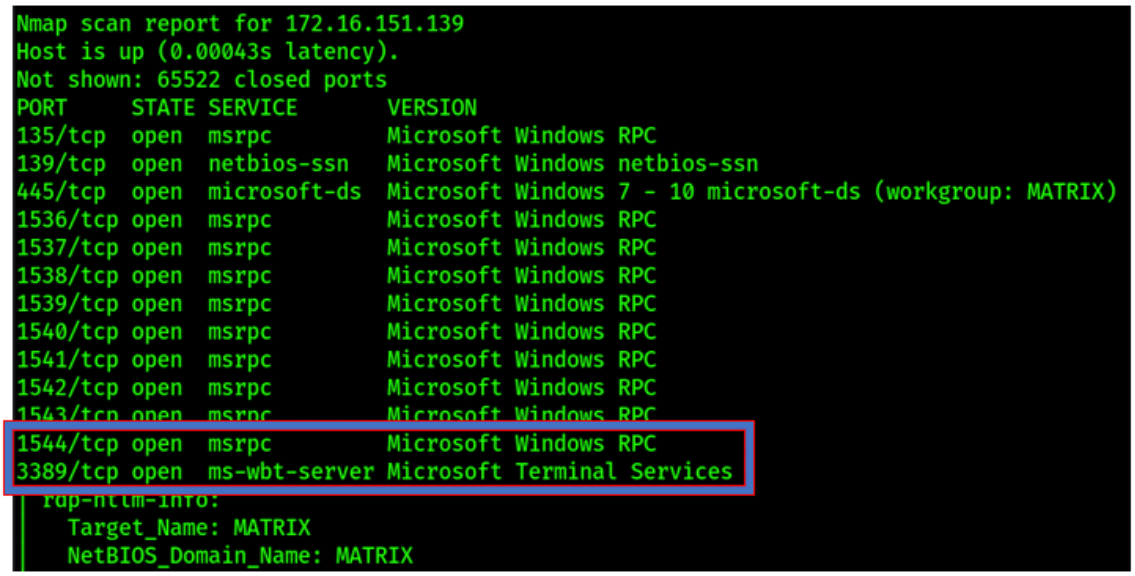


Рисунок 1.9 – NMAP Scan

Порушення даних могло розкрити ці облікові дані, додавши їх до списку мільярдів відомих зламаних паролів. Повторне використання скомпрометованих облікових даних означає, що це питання того, коли, а не якщо зловмисник використає їх і отримає доступ.

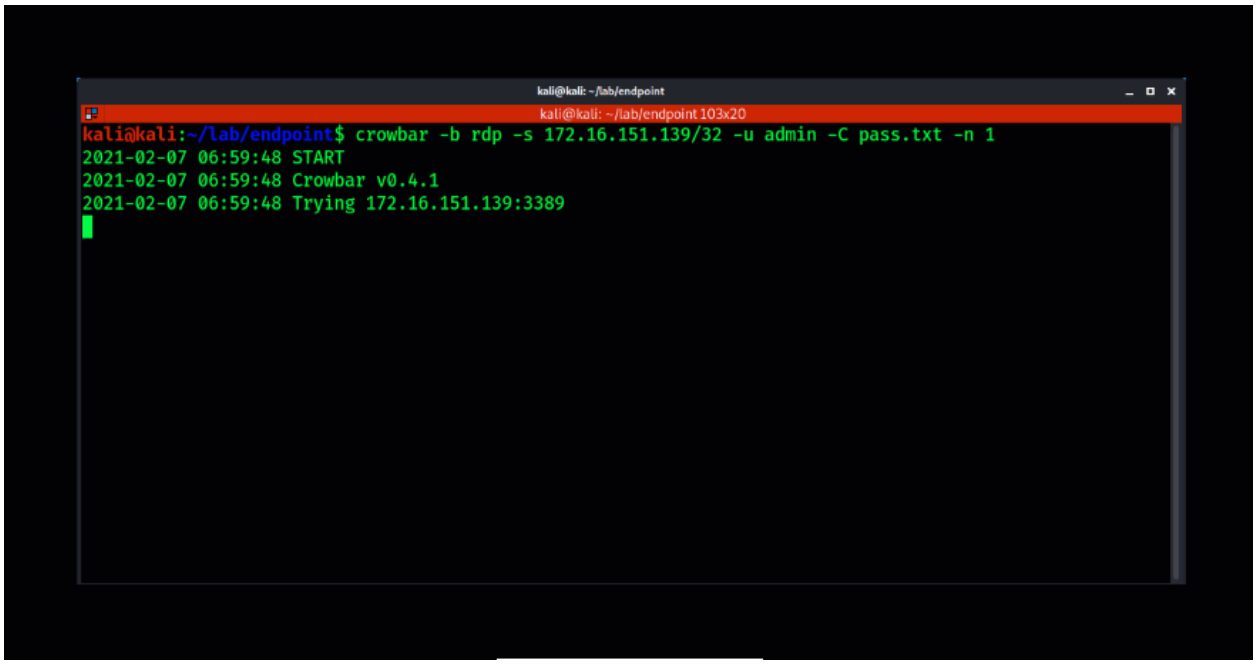


Рисунок 1.9 - Використання crowbar для brute-force RDP

Тоді зловмисник зможе використовувати скомпрометовані облікові дані, щоб отримати віддалений доступ до системи жертви та встановити

точку опори в її середовищі, яке потім можна буде використовувати для інсценування бокового руху або підвищення привілеїв.

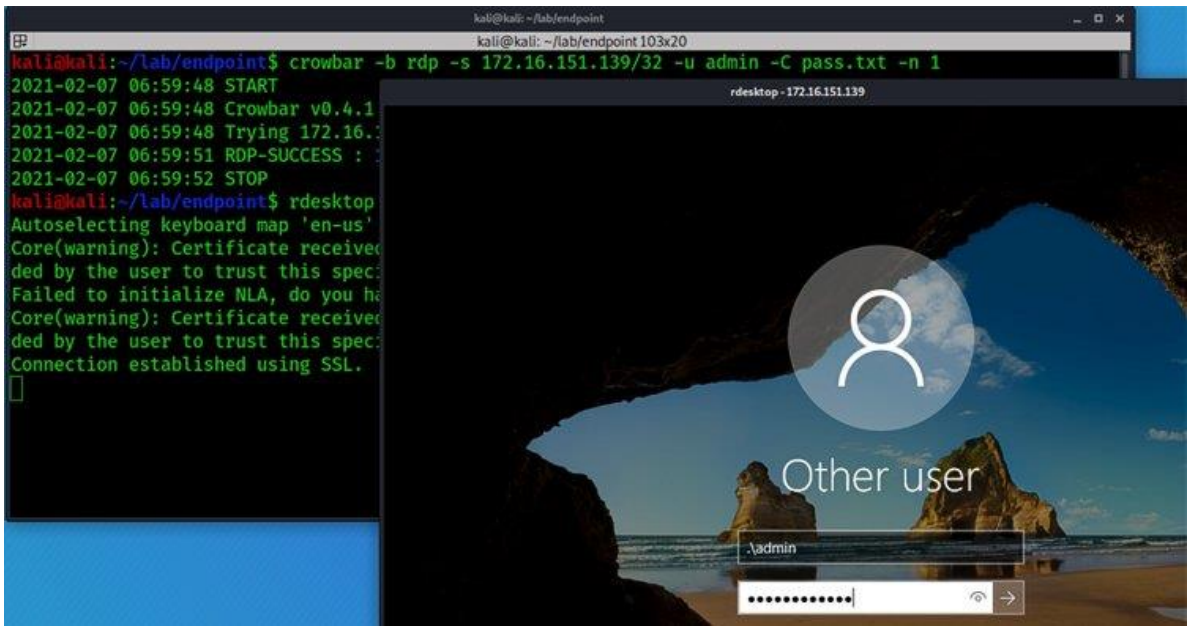


Рисунок 1.10 - Віддалений робочий стіл

Ніколи не залишайте RDP безпосередньо відкритим для загальнодоступного Інтернету без додаткових засобів захисту, таких як багатофакторна автентифікація та безпека привілейованого доступу. Аудит безперервних спроб грубої сили та атак сканування.

Отруєння імен Netbios і LLMNR за допомогою Responder

Netbios і LLMNR (Link-Local Multicast Name Resolution) — старі методи, якими досі легко зловживають, дозволяючи зловмиснику отримати мережевий хеш жертви NTLMv1 або NTLMv2. Знову ж таки, слабкі паролі роблять цю атаку можливою. Ось чому зловмисники продовжують успішно використовувати такі інструменти, як Responder, який можна запустити через електронну пошту, прослуховуючи несанкціонований доступ до мережі або навіть підключивши USB до ноутбука без нагляду.

Рисунок 1.11 - Використання Responder для захоплення хешу NTLM і злому

Саме через погану гігієну пароля ця атака є майже на 100% успішною. Використовуючи Responder, він відповідатиме на мережеві запити щодо спільних ресурсів SMB через LLMNR або NBT-NS. Система жертви, яка нічого не підозрює, із задоволенням поділиться своїм хешем NTLM. Коли зловмисник отримає хеш, це лише питання часу, коли він зможе його зламати за допомогою таких інструментів, як hashcat. Чим довший і складніший пароль, тим менше шансів зловмисника успішно його зламати.

Равжди використовуйте надійні паролі. Використовуйте рішення для керування доступом за паролем, щоб створювати надійні парольні фрази, щоб працівники не потребували цього.

Використання облікових записів адміністратора домену для всіх операцій

Одна річ, яка знайдена у багатьох середовищах Active Directory, це те, що системні адміністратори використовують облікові записи адміністратора домену для всього. Це може означати що завгодно: від облікових записів служб до віддаленого доступу до систем або залишення автоматизованих запланованих завдань для запуску резервних копій, а також ряд інших типів мережевого керування. Хоча це найпростіший метод, він також є основним вектором атаки для зловмисників. Вони хочуть, щоб ви зробили це, оскільки це дозволяє їм легко підвищити рівень від локального адміністратора до отримання повних прав адміністратора домену. Ось чому важливо дотримуватися принципу найменших привілеїв. Зведіть до мінімуму потребу у використанні облікових записів адміністратора домену, де це можливо.

Зловмисник, який має права локального адміністратора, використовуватиме цю систему як проміжну жертву, вносячи деякі невеликі зміни та чекаючи, поки адміністратор домену зробить типову помилку: увійде в систему, де зловмисник має права локального адміністратора.

Зловмисник змінить реєстр скомпрометованої системи, яка зберігатиме кешовані облікові дані в пам’яті у відкритому вигляді. Ця зміна сталася в

Windows 2012, де вона була вимкнена за замовчуванням, однак зловмисник може легко додати наступний розділ реєстру, щоб увімкнути це.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest] "UseLogonCredential"=dword:00000001.

Зловмисник чекатиме, час від часу отримуватиме віддалений доступ до проміжної системи, щоб перевірити, чи залишив адміністратор домену відбиток пароля, який можна витягнути у відкритому вигляді.

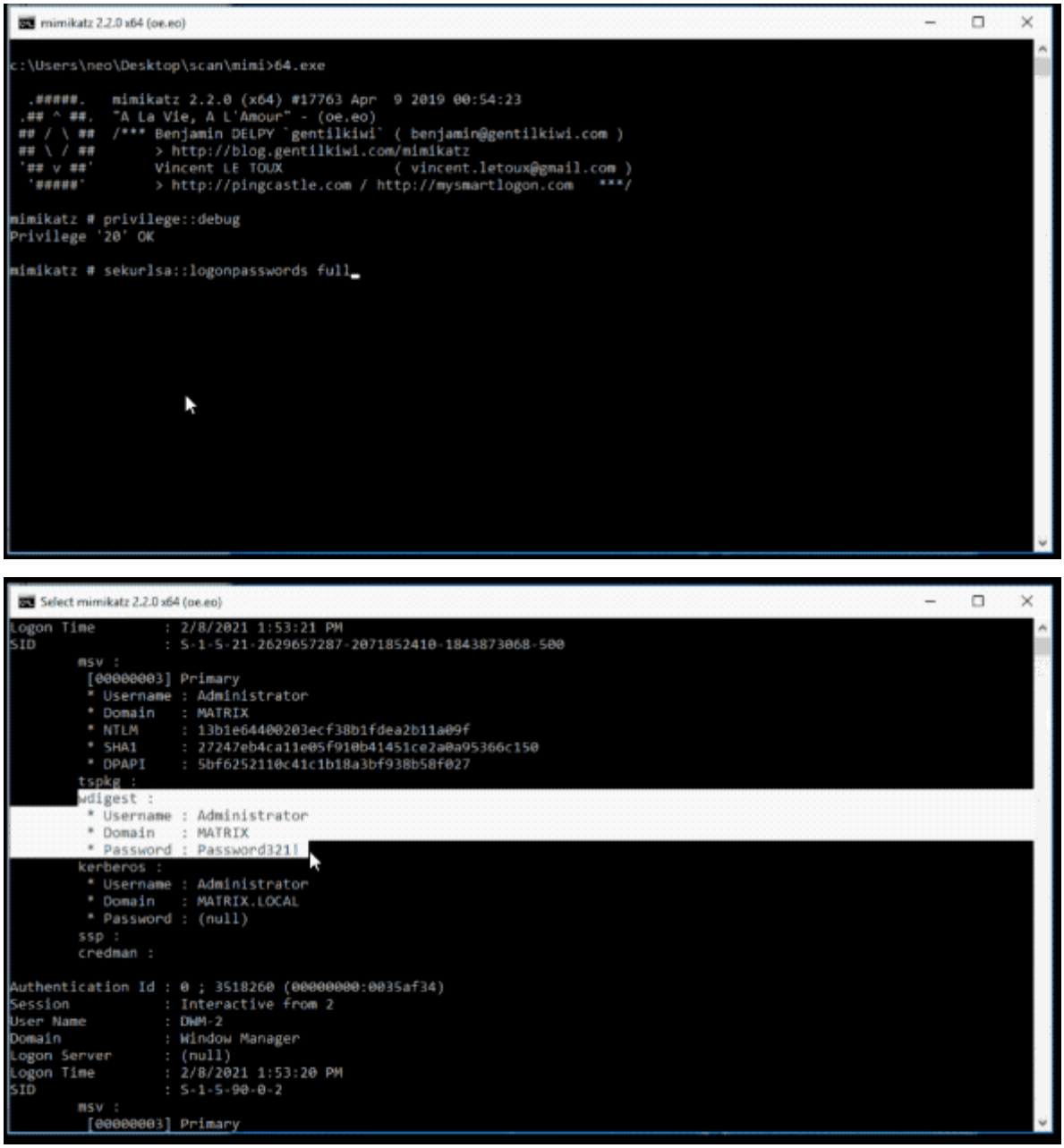


Рисунок 1.13 - Використання mimikatz для отримання відкритого текстового пароля адміністратора домену.

Забороніть користувачам із надлишковими правами мати права локального адміністратора в усіх системах. Переконайтеся, що контроль програм кінцевої точки використовується для запобігання запуску неавторизованих програм, таких як mimikatz, навіть якщо зловмисник отримує права локального адміністратора. Перевірте середовище на наявність налаштувань реєстру, які дозволяють зловмиснику отримувати паролі у відкритому вигляді.

Обмежте використання адміністратора домену, але якщо потрібно, використовуйте рішення безпеки привілейованого доступу, щоб паролі адміністраторів домену змінювалися після кожного використання. Таким чином, навіть якщо зловмисники можуть виконати цю шкідливу дію, пароль більше не буде дійсним.

Надпривілейовані та некеровані сервісні облікові записи

Зловмисники атакуватимуть привілейовані облікові записи у вашій мережі. Ваші сервісні облікові записи є однією з їхніх головних цілей. Багато організацій зазвичай створюють і налаштовують сервісні облікові записи з підвищеними привілеями домену, щоб мати доступ до необхідних мережевих ресурсів.

Це техніка, яка використовується, коли облікові записи служб налаштовано на використання SPN (Service Principal Name), щоб, коли користувачу або системі потрібно отримати доступ до цієї служби, вони отримували квиток Kerberos, підписаний хешем NTLM облікового запису.

Kerberoasting — поширена техніка злому, яку використовують зловмисники та червоні команди для підвищення привілеїв і отримання привілейованого доступу до Active Directory. Техніка успішна в основному завдяки поширеній практиці використання облікових даних слабкого сервісного облікового запису. Зловмисник використовує стандартного користувача домену для запиту SPN, який підписаний хешем NTLM облікового запису служби, і коли використовуються погані паролі, це лише питання часу, перш ніж машина для злому зможе зламати хеш, відкриваючи

простий текстовий пароль. і дозволити зловмиснику зловживати службовим обліковим записом (який зазвичай є користувачем із високими привілеями).

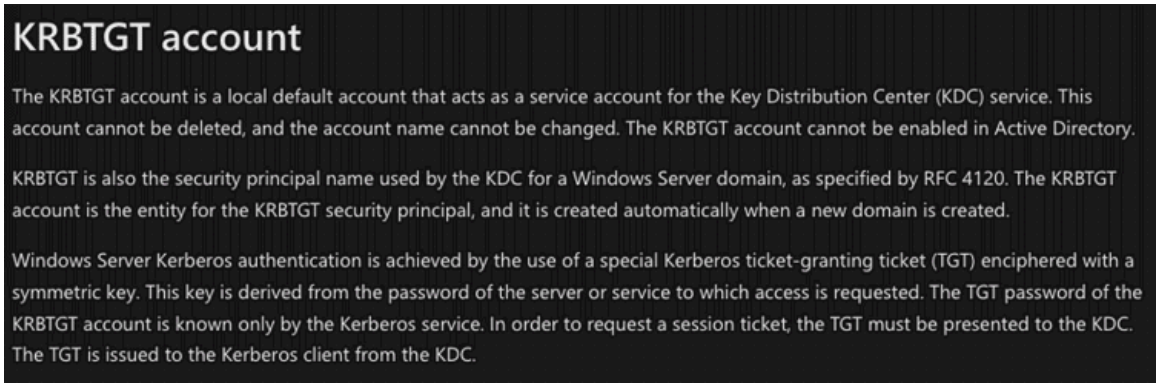
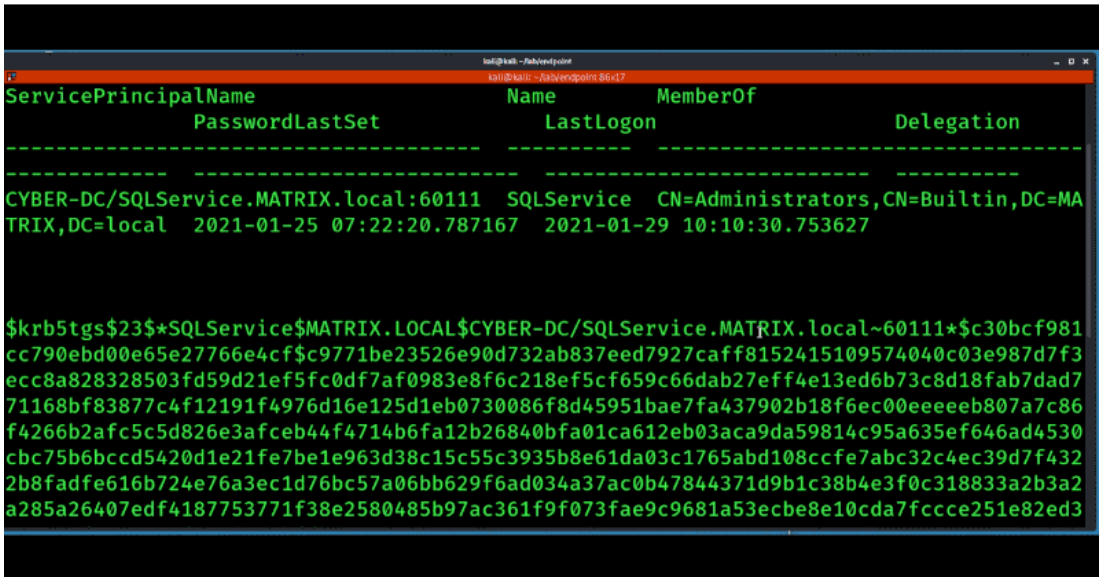
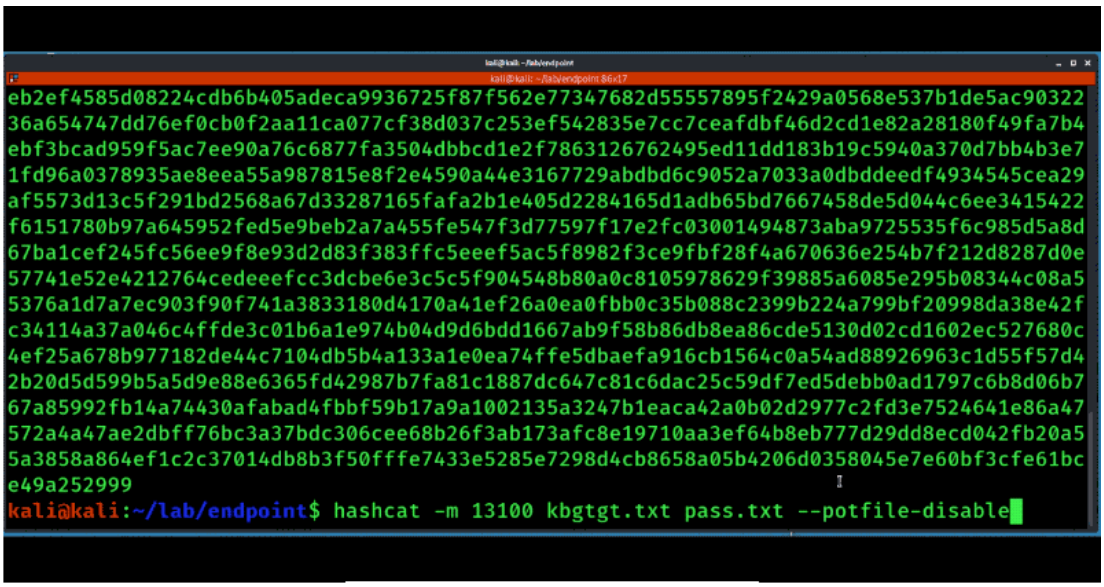


Рисунок 1.14 – техніка злому Kerberoasting

У наступному прикладі показано використання GetUserSPN.py з Impacket. Для цього потрібно мати автентифіковані скомпрометовані облікові дані домену, щоб запитувати SPN служби. Після запиту ви отримаєте копію хешу NTLM, і якщо використовуються слабкі облікові дані, зловмисник може скористатися інструментом для відновлення пароля та аудиту, таким як hashcat.

Запобігайте Kerberoasting, використовуючи надійні паролі облікових записів служби та періодично скидаючи обліковий запис служби Kerberos KDC. Рекомендується скинути обліковий запис служби Kerberos KDC двічі, роблячи це, оскільки DC зберігатиме історію двох паролів. Використовуйте рішення для керування привілейованим доступом, щоб допомогти виявити облікові записи служб, керувати ними та захистити їх.





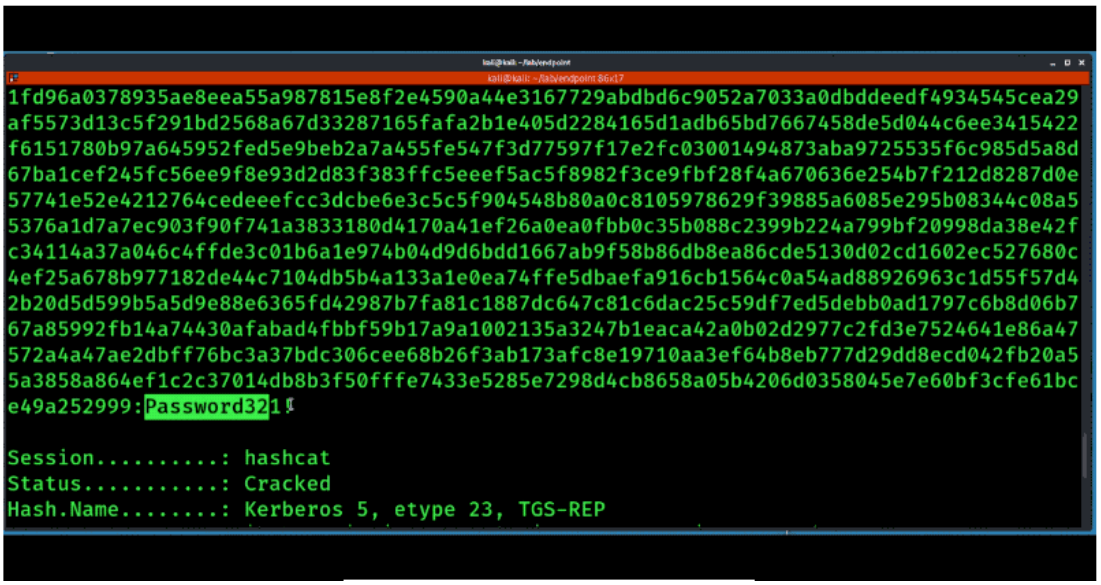


Рисунок 1.15 – Використання Impacket GetUserSPN.py для запиту SPN служби

Ось як скинути обліковий запис служби Kerberos KDC, який можна знайти в меню «Перегляд» > «Додаткові функції» > «Вибрати об’єкт «Користувачі» в домені. Ви знайдете krbtgt, де тепер можна вибрати та скинути свій пароль.

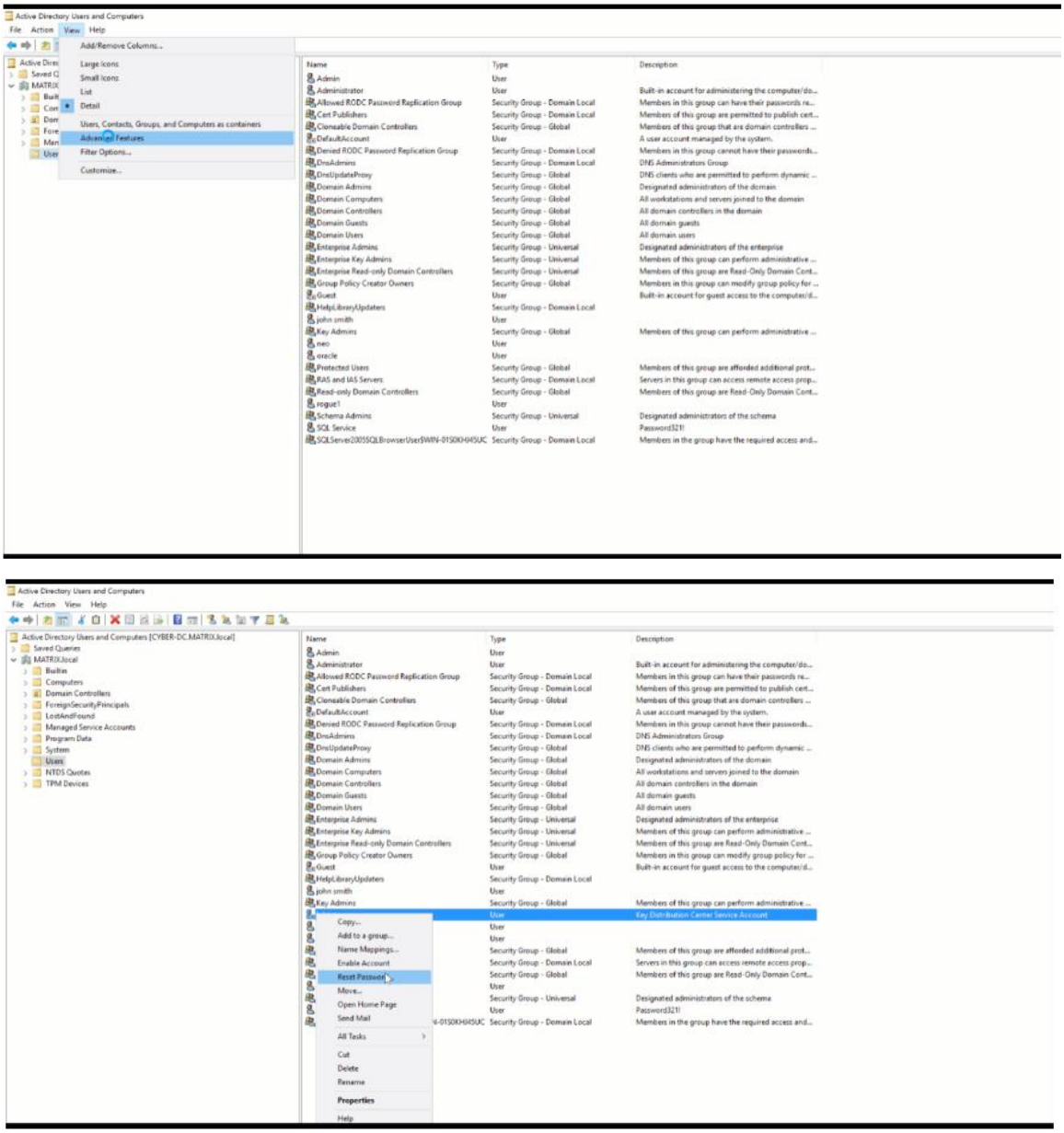


Рисунок 1.16 - Скидання облікового запису служби Kerberos KDC

Використання програмного продукту BloodHound для знаходження привілейованих облікових записів

BloodHound — це односторінкова веб-програма на Javascript, створена на основі Linkurious, скомпільована за допомогою Electron, з БД Neo4j, що подається за допомогою власне збирача даних C#.

BloodHound використовує теорію графів, щоб виявити приховані та часто ненавмисні зв’язки в середовищі AD. Хакери можуть застосовувати BloodHound, щоб легко визначити дуже складні шляхи атаки, які інакше було б неможливо швидко визначити. Адміністратори можуть використовувати цю утиліту для виявлення та запобігання тих самих напрямків атак. І сині, і червоні команди можуть застосовувати BloodHound, щоб легко отримати глибше розуміння зв’язків привілеїв у середовищі AD.

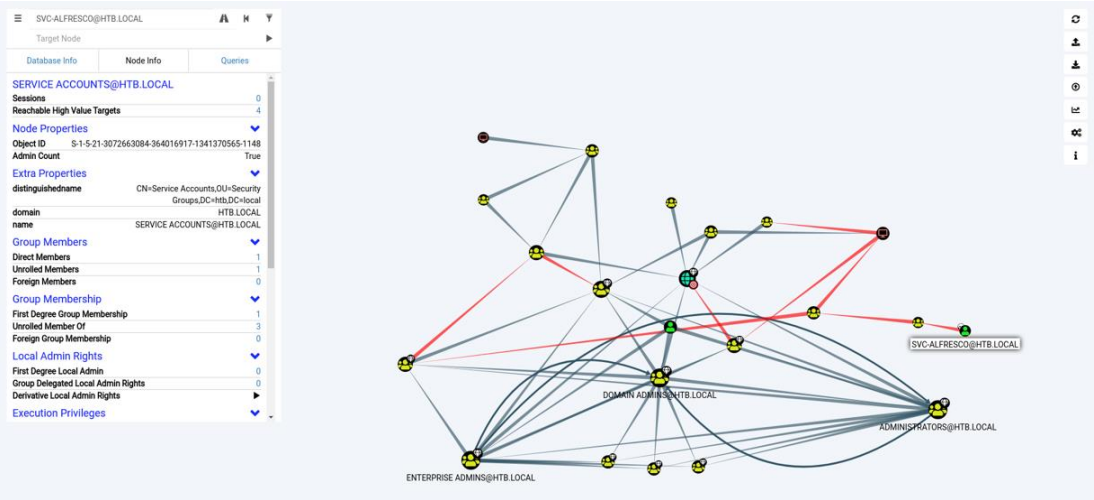


Рисунок 1.17 – Використання Hackthebox Bloodhound

Використовуйте Bloodhound, щоб допомогти вам виявити привілейовані облікові записи та стосунки у вашому оточенні. Використовуйте рішення для керування привілейованим доступом, щоб виявити та захистити привілейований доступ.

Підсумки аналізу безпеки та зміцнення Active Directory

Як видно, Active Directory є основною мішенню для зловмисників, і вони використовуватимуть методи, описані вище, щоб зловживати неправильними конфігураціями, слабкою безпекою та некерованими обліковими записами, що дозволить їм переміщатися та підвищувати рівень до облікових записів домену з високим рівнем привілеїв.

Інші прийоми, які зазвичай використовують зловмисники:

Eternal Exploits and unpatched systems such as CVE-2017-0144

Old and Unmanaged AD Accounts

SMB Relay

Legacy Systems that require backward compatibility

Mitm6

2. АНАЛІЗ ВПЛИВУ АТАК НА WINDOWS ACTIVE DIRECTORY DOMAIN SERVICES

2.1. Active Directory і її впровадження на підприємствах

Active Directory — це служба каталогів користувачів від Microsoft, яка, мабуть, є найпопулярнішим рішенням для організацій, що дозволяє керувати та впорядковувати IT-профілі своїх співробітників для автентифікації, авторизації та обліку. Active Directory працює в структурі мережевого домену, тому для запуску служби в якості контролера домену потрібен комп’ютер під керуванням Windows Server 2000 або новішої версії. У цьому контексті домен можна визначити як «окрему підмножину Інтернету з адресами, що мають спільний суфікс або знаходяться під контролем певної організації чи особи».

Active Directory пропонує кілька служб, корисних для керування IT-інфраструктурою організації. Основна мета Active Directory — забезпечити заходи авторизації, автентифікації та обліку для організацій для використання системними/мережевими адміністраторами. Профілі користувачів потрібні для входу на комп’ютери, підключені до домену.

Після того, як користувач увійшов до комп’ютера за допомогою автентифікації, його дії будуть обмежені на основі авторизації та зареєстровані через облік. З цих облікових записів користувачів політики можна застосовувати через об’єкти групової політики (GPO) для різних робочих цілей, наприклад призначення груп користувачів на основі відділу, а потім призначення принтера чи спільного доступу до файлів для цих користувачів або будь-якої політики, яка потрібна організації. Для багатьох організацій ці послуги є критично важливими для ведення бізнесу.

Контролери домену є критично важливим компонентом більшості сучасних корпоративних мережевих структур, тому час простою цих хостів є

несприятливим навіть для виконання необхідних завдань, таких як оновлення програмного забезпечення для виправлення недоліків безпеки. Організаціям ще більше не рекомендується оновлюватися до найновішої основної версії операційної системи, наприклад, із Server 2008 на Server 2012, через відмінності та несумісність інтерфейсу користувача та функціональних можливостей служби, а також ще більше збільшення часу простою. Microsoft зазвичай підтримує свої останні операційні системи протягом 10 років після випуску [8].

Ця підтримка охоплює нові функції, покращення, виправлення помилок і, що найважливіше, виправлення вразливостей системи безпеки. Через 10 років після розширеного плану підтримки корпорація Майкрософт більше не надаватиме оновлення системи безпеки для своїх операційних систем, незважаючи на ймовірність і неминучість появи вразливостей системи безпеки після цього часу.

Незважаючи на вразливість операційної системи, є незліченна кількість організацій, які або нехтують, або відмовляються оновлювати свою операційну систему до останньої основної версії. У 2019 році Microsoft підрахувала, що близько 60% установок Windows Server були версії 2008, що становить приблизно 24 мільйони серверів Windows Server 2008, це досить велика кількість серверів, до завершення підтримки яких залишилося менше року.

Окрім нехтування оновленнями програмного забезпечення, організації часто не виділяють достатньо ресурсів для IT-інфраструктури, такої як резервний контролер домену, який був би надзвичайно корисним для відновлення після атаки програм-вимагачів.

Компанії можуть навіть зовсім не мати IT-персоналу, не залишаючи жодної людини, здатної підтримувати контролер домену. Оскільки контролери домену пропонують різні мережеві служби, вони залишають відкритими багато вразливостей. Усі ці фактори призводять до того, що контролери домену є основою IT-структури будь-якої організації, яка, якщо її

пошкодити, матиме великий вплив на функціонування решти хостів у мережі.

2.2. Програмне забезпечення для вимагання коштів

Хоча програмне забезпечення можна створювати для будь-якої бажаної мети, від розваги до підвищення продуктивності на робочому місці, воно також може використовуватися для хакерських цілей. Зловмисне програмне забезпечення визначається як «програмне забезпечення, яке спеціально розроблене для порушення роботи комп'ютерної системи, її пошкодження або отримання несанкціонованого доступу до неї». Програми-вимагачі – це підмножина шкідливих програм, призначених для цифрового вимагання від своїх жертв сплати необхідної суми викупу, і робить це двома основними методами.

Перший тип програми-вимагача, відомий як крипто-вимагач, шифрує файли користувача, залишаючи машину в іншому робочому стані. У більшості випадків сплата викупу повертає ключ розшифровки для розшифровки файлів користувача. Інша основна форма програм-вимагачів, яку часто називають locker ransomware, не шифрує файли користувача, а натомість блокує користувачу його пристрій, щоб запобігти його використанню, доки не буде сплачено викуп. Зловмисне програмне забезпечення, як правило, дуже залежить від мережевих можливостей свого хоста, і програмне забезпечення-вимагач — від ботнетів до шпигунського ПЗ — не виняток.

Щоб жертва сплатила викуп, потрібне підключення до Інтернету; отже, програма-вимагач має залишити мережеві можливості функціональними або наказати користувачеві сплатити викуп за допомогою іншого пристрою. Останній варіант не є кращим рішенням, оскільки в ідеалі зловмисник намагатиметься заразити якомога більше пристроїв, не залишаючи інших пристроїв вільними для будь-яких інших дій, окрім сплати викупу.

Крім того, програмне забезпечення-вимагач може поширюватися мережею, щоб інфікувати додаткові хости, посилюючи шкоду або потенціал викупу для зловмисника. Цей мережевий аспект особливо шкодить компаніям, які використовують і залежать від мереж внутрішньої доменної структури з великою кількістю хостів для використання співробітниками.

Процес виконання крипто-вимагачів складається з кількох етапів, а саме:

1. На першому етапі програма-вимагач використовує вектор атаки, щоб знайти шлях до комп'ютера потенційної жертви. Вектори атак можуть включати фішинг електронної пошти, впровадження через скомпрометоване чи застаріле законне програмне забезпечення або використання мережевих протоколів, при цьому деякі варіанти програм-вимагачів використовують кілька методів для досягнення успіху.

2. Після того, як програма-вимагач отримала доступ до системи, вона починає виконувати початкову фазу виконання. На цьому етапі зловмисне програмне забезпечення заривається в систему та реалізує механізми збереження для автоматичного перезапуску після таких подій, як перезавантаження системи [9].

3. Наступна дія, яку виконує виконуваний файл програми-вимагача, — це видалення всіх резервних копій, які користувач може використати, щоб обійти виплату викупу. У Windows поширеним методом програм-вимагачів, зокрема WannaCry, є служба Volume Shadow Copy [10].

4. Після цього програма-вимагач почне процес шифрування. Цей процес також не є однорідним, оскільки алгоритми та методи шифрування відрізняються для різних варіантів програм-вимагачів. Більшість варіантів програм-вимагачів використовують симетричне шифрування закритим ключем, зазвичай AES, для шифрування файлової системи за допомогою пари асиметричних відкритих ключів, зазвичай RSA, із сервера командування та керування (C&C) для шифрування випадково згенерованого закритого ключа. WannaCry використовує комбінацію AES і RSA.

Однак це не стосується деяких варіантів програм-вимагачів, таких як SamSam, які не зв’язуються з C&C-сервером і натомість завершують фазу шифрування локально, оскільки зловмисник дистанційно керує машиною.

Компонент шифрування є найвідмітнішою особливістю кожного сімейства програм-вимагачів, поряд із сумою викупу. Це також, очевидно, найруйнівніший компонент крипто-вимагачів, оскільки після початку процесу шифрування процес вимагачів стає майже незворотним. Хоча деякі варіанти програм-вимагачів мають свої інструменти розшифровки, які є вільними та загальнодоступними завдяки роботі, проведеній дослідниками, вони зазвичай стають такими лише після початкового спалаху, коли організації вже вжили рішучих дій щодо того, як продовжити роботу зі своїми інфікованими системами.

5. Останньою подією процесу виконання програми-вимагача є сповіщення про вимогу викупу. Це означає, що користувачеві буде запропоновано вікно сповіщення про те, що він заражений. У цьому вікні буде вказано необхідну суму викупу та інструкції щодо оплати, а в деяких випадках також містить зворотний відлік, який після закінчення терміну або збільшить вимогу викупу та перезапустить зворотний відлік, або знищить систему. У той час як інші зловмисні програми, такі як шпигунські програми, ботнети та руткіти, залишаються непоміченими для користувача, програми-вимагачі – навпаки.

Здатність програми-вимагача «виводити з ладу основні бізнес-функції системи» робить її особливо шкідливою та неприємною, що призводить до того, що підприємства стають набагато більш готовими вживати заходів, зокрема сплачувати викуп, щоб повернути функціональність до нормального стану. Іншим фактором, що впливає на готовність компанії платити викуп, є репутація.

Ще один важливий момент для розуміння екосистеми програм-вимагачів полягає в тому, що «здатність заробляти гроші на програмах-вимагачах критично залежить від віри жертв у те, що користувач заплатить

викуп». У третьому та четвертому кварталах 2019 року 98% компаній, які заплатили викуп, отримали робочий інструмент розшифровки, що доводить, що розробники програм-вимагачів налаштовані зберегти довіру [11].

Розробники варіанту програм-вимагачів SamSam зайшли так далеко, що пропонували своїм жертвам технічну підтримку, щоб забезпечити відновлення їхніх даних після оплати. Розробники UltraCrypter також застосували цей підхід після того, як було виявлено, що їхня платіжна система, здається, не працює.

Однак, мабуть, найвпливовішим стимулом для сплати викупу є страхування кібербезпеки. З організацій, які заплатили викуп, 94% отримали відшкодування через свою страховку [12].

2.3. Ransomware як сервіс.

Все більшою тенденцією в кіберсфері програм-вимагачів є використання Ransomware-as-a-Service (RaaS). RaaS дозволяє тим, хто не має технічних навичок розробки зловмисного програмного забезпечення, брати участь у діяльності з розгортання та використання програм-вимагачів, використовуючи для цього створення іншого розробника програм-вимагачів.

Розробники програм-вимагачів можуть пропонувати свій код прямо за встановлену ціну або просто надавати програми-вимагачі безкоштовно за умови, що зловмисник ділиться відсотком прибутку з розробником. Хоча для розробників програм-вимагачів може здатися контрпродуктивним дозволяти іншим використовувати їх творіння та частково отримувати прибуток, а не виконувати дії самостійно, існує кілька причин для існування цієї галузі.

Пропонуючи RaaS, розробники зменшують свій ризик оприлюднення, оскільки вони продають свій продукт анонімно через даркнет і залишають фінансовий слід лише через майже невідстежувану криптовалюту, так що навіть кінцевий клієнт не зможе ідентифікувати розробника, якщо його спіймають.

Крім того, звичайні особи мають доступ до областей, до яких розробники шкідливих програм не можуть. Наприклад, незадоволений співробітник може використовувати свій корпоративний доступ для розгортання програм-вимагачів у доменах і мережах, куди в іншому випадку було б важко або неможливо проникнути початковому розробнику.

Це відкрило ще один канал для процвітання програм-вимагачів у сучасному кібернетичному середовищі. Оскільки програмне забезпечення-вимагач продовжує розвиватися, змінюються й стратегії, які розробники використовують для отримання більших прибутків. Розробники програм-вимагачів «повільно виявлятимуть і переходитимуть до оптимальних стратегій», щоб отримати більш бажані результати.

Це вже можна побачити з кількох прикладів, які використовуються в сучасних варіантах програм-вимагачів. Нова поширена стратегія, яка використовується для ефективного націлювання на підприємства, — це загроза витоку або надання загальнодоступних конфіденційних файлів, отриманих під час зараження програмою-вимагачем.

Це означає крадіжку конфіденційних файлів, таких як патенти компаній, або особисту інформацію таких цілей, як лікарні, і їх надсилання назад зловмиснику програм-вимагачів для подальшого вимагання та спонукання до оплати. Хоча контролер домену, як правило, не використовується для роботи з конфіденційними документами, він все одно може використовуватися для їх зберігання у формі спільного мережевого файлу. Таким чином, мережевий файлообмінний сервер був би прибутковою ціллю, оскільки він є сукупністю роботи кількох користувачів, на відміну від отримання доступу до хосту, що належить і зберігає роботу одного користувача.

2.4. Роль криптовалют в індустрії програм-вимагачів.

Хоча програми-вимагачі використовують шифрування для виконання своїх функцій, розробник залежить від криптовалюти, щоб отримати прибуток. Криптовалюта — це термін, який використовується для опису цифрової валюти, у якій криптографія використовується для перевірки записів транзакцій і права власності на облікову книгу.

Роль криптовалюти у програмному забезпеченні-вимагачі полягає в тому, що вона надає зловмиснику майже анонімний фінансовий рахунок для отримання прибутку від своїх атак, не залишаючи чіткого фінансового сліду до його справжньої фізичної особи. Це зробило розгортання програм-вимагачів кіберзлочинністю з дуже низьким ризиком і потенційно високою винагородою. Біткойн, безсумнівно, є найвідомішим, оскільки він був першою децентралізованою цифровою валютою і зрештою став однією з найдорожчих.

Хоча біткойн можна вважати анонімним у тому сенсі, що жодна інформація щодо облікового запису не представляє реальну ідентифікаційну інформацію, яка може бути пов’язана з особою, обліковий запис все одно представлено адресою, яку, як валюту на основі блокчейну, можна легко приписати. і публічно пов’язані з усіма його транзакціями. Як результат, біткойн не є повністю анонімним і натомість позначений як псевдонім [13]. Під час обміну на реальну валюту слідчий міг би використати платіж із реєстру, керованого програмами-вимагачами, на обмін, а потім зіставити відповідну вартість обміну з реальним банківським рахунком підозрюваного.

Крім того, криптовалютні біржі часто є реальними бізнесами, які регулюються місцевою владою, і тому підпадають під дію будь-яких місцевих законів, які можуть змусити біржі надавати інформацію щодо транзакцій на реальні банківські рахунки, зрештою розкриваючи справжню особу кіберзлочинця [14]. Незважаючи на те, що зловмисники можуть використовувати кілька облікових записів біткойн для поділу та ефективного

відмивання валюти, слід транзакцій завжди залишатиметься відкритим і доступним для відстеження завдяки інфраструктурі блокчейну біткойна. Однак, якщо кіберзлочинець використовує централізований міксер для обміну біткойнів на більш орієнтовану на конфіденційність криптовалюту, таку як Monero, і повторює цей процес на кількох різних біржах, відстеження транзакцій стає неможливим, оскільки ці криптовалюти маскують записи транзакцій, таким чином видалення публічного сліду транзакцій. Використання кількох обмінів міксерами в різних правоохоронних юрисдикціях робить відстеження транзакцій значно складнішим з юридичної точки зору. Зважаючи на всі ці фактори, не дивно, що поширення програм-вимагачів продовжується з року в рік.

2.4. TeslaCrypt, Jigsaw, WannaCry

Для практичного експерименту використовуються два відомі варіанти програм-вимагачів: TeslaCrypt і Jigsaw. Існування TeslaCrypt було вперше виявлено на початку 2015 року та, як повідомляється, поширювалося через списки розсилки спаму та скомпрометовані веб-сайти. Спочатку він був розроблений для націлювання на дані, що належать до відеоігор, включаючи файли збереження та профілі; однак у якийсь момент розробники змінили його, щоб включити ширший діапазон файлів, щоб збільшити прибутковість за рахунок ширшого кола жертв. TeslaCrypt вимагала викуп у розмірі 500 доларів США в еквіваленті біткойнів, який подвоювався б кожні 60 годин. Шифрування AES256 використовувалося TeslaCrypt; однак через помилку, виявлену в першій ітерації TeslaCrypt, процес шифрування був оборотним. Це було вирішено у версії 2, і програмне забезпечення-вимагач залишалося таким у наступних версіях, доки кампанія не завершилася. Кампанія TeslaCrypt завершилася, коли в травні 2016 року розробники випустили головний ключ дешифрування на своєму платіжному веб-сайті Tor.

Це дозволило зараженим розшифрувати свої файли, а розробникам програмного забезпечення випустити інструменти розшифровки.

У порівнянні з більш відомими варіантами програм-вимагачів, TeslaCrypt здається неважливим для сцени програм-вимагачів. однак це все ще має великий вплив на постраждалих. Відсутність розголосу, можливо, робить програму-вимагач більш впливовою, оскільки вона привертає менше уваги аналітиків зловмисного програмного забезпечення, які б працювали над вирішенням. Jigsaw — це відносно невідомий варіант програм-вимагачів, який не отримав такої популярності, як інші варіанти програм-вимагачів. Jigsaw отримав свою назву завдяки зображенню персонажа популярного серіалу фільмів «Пила» в записці про викуп. Зображення фільмів жахів також спричинили те, що Jigsaw було класифіковано дехто як страшне програмне забезпечення. Викуп, який вимагає Jigsaw, становить еквівалент 150 доларів США в біткойнах або 0,4 біткойна.

12 травня 2017 року почався спалах WannaCry. Програмне забезпечення-вимагач привернуло значну увагу ЗМІ за кілька годин, оскільки воно пошкодило кілька великих установ та критично важливу інфраструктуру в Європі, наприклад Національну службу охорони здоров'я Сполученого Королівства, Deutsche Bahn, Renault, FedEx та кілька інших відомих організацій. WannaCry вразила понад 300 000 підприємств у 150 країнах у перші кілька днів спалаху. Багато дослідників та аналітиків у сфері кібербезпеки, включно з Національним центром кібербезпеки Великобританії, припустили, що за атакою стояла Корейська Народно-Демократична Республіка (Північна Корея) через схожість попередніх атак, які також приписувалися їм. Щоб виконати своє завдання, WannaCry використав два експлойти, розроблені Агентством національної безпеки США (NSA), які були злиті на початку року групою хакерів, яка називала себе «The Shadow Brokers». Перший використовуваний інструмент відомий як «DoublePulsar» і є бекдором, який дозволяв будь-яким неавторизованим користувачам запускати зловмисне програмне забезпечення на машині без

взаємодії користувача. Це було використано в поєднанні з іншим експлойтом, відомим як «EternalBlue». EternalBlue — це назва експлойта, який дозволив програмі-вимагачу швидко поширюватися мережею. Він робить це, використовуючи вразливість у протоколі Server Message Block (SMB), протоколі, який найчастіше використовується Microsoft для мережевого обміну файлами та принтерами в Active Directory. Хоча існує кілька оновлених версій SMB, лише версія 1 містить вразливість і все ще ввімкнена службою Active Directory, щоб пропонувати свої послуги старішим клієнтам, які можуть не підтримувати нові версії протоколу. Windows відображає цю службу обміну файлами як «LanmanServer», яка автоматично запускається після завантаження Windows, включаючи підтримку SMB версії 1. Проте в останніх інсталяціях Windows SMB версії 1 не інстальовано за замовчуванням, а для старіших інсталяцій Microsoft тепер рекомендує вимкнути підтримку версії 1, якщо це можливо [15, 16]. Таким чином, майже суперечливо, цей експлойт зробив використання Windows Active Directory великою вразливістю безпеки для організацій, таким чином, це стало причиною широкомасштабного націлювання WannaCry на корпоративні інформаційні системи.

Як зазначалося раніше, підприємства зазвичай не оновлюють програмне забезпечення так часто, як це потрібно. Спалах WannaCry яскраво це продемонстрував, оскільки вразливість, яку використовував EternalBlue, було виправлено в оновленні безпеки MS17-010, яке було випущено майже за 2 місяці до спалаху WannaCry. Незважаючи на те, що оновлення MS17-010 позначено як критичне, WannaCry знадобилося всього кілька годин, щоб поширитися по всьому світу

У випадку з WannaCry інструмент розшифровки став доступним через тиждень після його початкового спалаху, у цей момент перемикач блокування вже був активований, щоб запобігти новим зараженням, а раніше заражені користувачі вже вжили заходів, сплативши викуп або відновивши з резервних копій.

Атака змусила організації за межами IT-індустрії оцінити власні заходи безпеки та розглянути, чи варто їм покращувати свою IT-інфраструктуру. Його широка популярність навіть мала наслідки, не пов'язані з практикою кібербезпеки, оскільки фінансовий сектор скористався цією подією та побачив надмірну позитивну віддачу від біржових фондів кібербезпеки в результаті WannaCry. Незважаючи на оприлюднений вплив програм-вимагачів на той момент, здається, що підприємства не змогли винести урок із тих, хто раніше постраждав. Рівно через 2 роки після дебюту WannaCry за допомогою пошукової системи Інтернет-пристроїв Shodan було виявлено, що понад один мільйон комп'ютерів і серверів все ще мають увімкнену версію SMB 1. Це число не враховує пристрої, які не були загальнодоступними, і тому не включає пристрої, які Shodan не зміг знайти. Ще більше занепокоєння викликає те, що незважаючи на те, що Національна служба охорони здоров'я (NHS) кілька днів була скалічена через WannaCry, приблизно в той самий період у 2019 році було виявлено, що приблизно 2300 комп'ютерів NHS все ще працювали на Windows XP, що на той час перевищувало 5 років після закінчення терміну підтримки.

2.5. NotPetya

Одним із помітних прикладів програм-вимагачів є варіант NotPetya, який був випущений у червні 2017 року, незабаром після WannaCry, і навіть використовував той самий експлойт EternalBlue. Однак мета, виконання та метод розгортання значно відрізнялися від WannaCry. Зараження почалося, коли кіберзлочинцям вдалося проникнути на сервер оновлень українського бухгалтерського програмного забезпечення, яким користуються приблизно 80% компаній в Україні. Після цього зловмисники розробили бекдор у програмному забезпеченні бухгалтерського обліку та розповсюдили його всім користувачам через сервер оновлень, над яким вони отримали контроль.

Через цю вразливість зловмисники розгортають програму-вимагач, яка потім поширюється на інші машини в мережі за допомогою експлойта EternalBlue.

Це призвело до масштабних корпоративних заражень, які лише сприяли відсутності запобіжних заходів безпеки SMB версії 1, які слід було впровадити не лише до, а й після руйнування WannaCry. Хоча програма-вимагач спочатку була націлена на Україну, транснаціональні компанії з офісами в Україні спричинили поширення програми-вимагача по всьому світу.

Після зараження комп'ютера NotPetya виконає звичайні кроки запуску програми-вимагача. Однак, особливо, NotPetya не тільки шифрує файли, але й змінює головний завантажувальний запис. Щойно NotPetya завершить виконання, він змусить машину перезавантажитися, де головний завантажувальний запис відобразить вимоги викупу NotPetya замість завантаження встановленої операційної системи Windows. У результаті контролери домену, що працюють під керуванням Windows Server, не зможуть запропонувати свої послуги.

Що робить NotPetya особливо унікальним, так це те, що процес шифрування є незворотнім, тобто якщо викуп буде сплачено, зловмисники все одно не зможуть запропонувати жертві повернути функціональність своєї машини. На цьому етапі класифікація програм-вимагачів NotPetya стає спірною, оскільки деякі стверджують, що це зловмисне програмне забезпечення, класифіковане як «очисник», призначене виключно для стирання даних машини, незважаючи на вимогу викупу, наявну поряд із процесом дешифрування [18, 19]. Атака була настільки руйнівною, що тільки американська фармацевтична компанія Merck & Co підрахувала, що станом на кінець 2017 року вона коштувала їй 870 мільйонів доларів збитків, ця цифра згодом зросте до 1,3 мільярда доларів, якщо подавати страхові претензії. У жовтні 2020 року уряд Сполучених Штатів висуне звинувачення шістьом російським офіцерам ГРУ у різних кіберзлочинах, стверджуючи, що один випадок їхніх дій стосувався поширення NotPetya у 2017 році, тоді як

уряд Великої Британії також викриє інші атаки, здійснені цими людьми [19-21]. Це був настрій, висловлений ще в 2018 році, коли уряди Великої Британії, США та Австралії заявили, що за атакою NotPetya стоїть Росія.

Отже, причетність Росії до цієї атаки програм-вимагачів, спрямованої конкретно на Україну, не повинна бути несподіванкою для тих, хто обізнаний про поточну російсько-українську війну, і повинна служити демонстрацією гібридної війни сучасної цивілізації.

Можливо, NotPetya використовувала вимогу викупу, щоб приховати свою справжню мету знищення даних, або розробники також хотіли отримати прибуток від своєї атаки; однак очевидно, що це явно не було звичайне програмне забезпечення-вимагач, орієнтоване на гроші. Від нездатності розшифрувати до походження зловмисника, схоже, що в цьому випадку програмне забезпечення-вимагач еволюціонувало від простого зловмисного програмного забезпечення, яке гонилося за прибутком, і стало ще однією політичною кіберзброєю, яку потрібно додати до арсеналу.

3 ДОСЛІДЖЕННЯ ВПЛИВУ ШКІДЛИВИХ ПРОГРАМ НА ІУНКЦІОНУВАННЯ ACTIVE DIRECTORY

3.1. Загальні інструменти, що використовувались для аналізу програм-вимагачів.

Одним з рішень, яке широко поширене не лише в академічній, а й у комерційній сфері, є використання віртуалізації. Віртуалізація передбачає віртуальне програмне забезпечення, від додатків до повністю емульованих машин під керуванням операційних систем, без прямого доступу та контролю апаратного забезпечення головної машини.

Віртуалізація використовує гіпервізори, які розподіляють фізичні системні ресурси, такі як ядра процесора, пам’ять і дисковий простір, для віртуальних машин.

Гіпервізори використовують два різні методи емуляції віртуальних машин.

Гіпервізори типу 1, відомі як голі гіпервізори, які працюють безпосередньо на апаратному забезпеченні хоста для розміщення кількох віртуальних машин. Вони поширені в корпоративній сфері, оскільки сервери великої ємності встановлюються разом із гіпервізорами, такими як Hyper-V від Microsoft або ESXi від VMware.

Гіпервізори типу 2 не запускаються безпосередньо з апаратного забезпечення, натомість це програми, які запускаються з операційної системи хоста, наприклад, VMware Workstation або VirtualBox. Що робить віртуалізацію особливо вигідною та майже необхідною для динамічного аналізу та дослідження зловмисного програмного забезпечення, так це можливість створювати знімки пристрою та керувати ними. Знімки — це копія точного стану машини в певний момент часу.

Під час аналізу зловмисного програмного забезпечення за допомогою віртуальних машин можна створити знімок до зараження машини. Після зараження машини та проведення дослідження стану машини можна швидко та легко повернути її до попереднього знімка, зберігаючи при цьому хост-машину в безпеці та ізоляції від дій, що виконуються на віртуальній машині.

Ця функція доступна з VirtualBox, гіпервізором з відкритим кодом, розробленим Oracle, який доступний для кількох різних операційних систем. Використання VirtualBox майже усуває ризик, пов’язаний із обробкою зловмисного програмного забезпечення, і забезпечує додаткові переваги, які полегшать налаштування цього експерименту.

Process Monitor — це програмне забезпечення для моніторингу з відкритим вихідним кодом, яке спочатку було розроблено для Windows компанією Microsoft, але зараз також доступне для Linux.

Process Monitor надає повну інформацію про системний реєстр, файлову систему, мережу та активність процесу, а також дозволяє експортувати записану активність у файл журналу для подальшого аналізу.

Ці записані значення особливо корисні для динамічного аналізу зловмисного програмного забезпечення, оскільки охоплюють кілька основних системних індикаторів, щоб повністю зрозуміти, як працює перевірений зразок шкідливого програмного забезпечення.

Як наслідок, Process Monitor став звичним явищем в академічному динамічному аналізі шкідливих програм. Оскільки різновиди програм-вимагачів часто заражають і шифрують тисячі файлів в одній скомпрометованій системі, ручний аналіз їх впливу може бути проблематичним.

Тому було розроблено низку підходів машинного навчання для виявлення та аналізу цієї великої кількості даних саме в операційній системі Windows. Ці методи можна додатково розширити за допомогою підходів навчання передачі, щоб також захистити клієнтські машини в Windows Active Directory. Однак часто системи виявлення вторгнень машинного

навчання стають цілями зловмисників, які прагнуть використати їх для своєї вигоди; отже, будь-який алгоритм машинного навчання повинен ретельно розглядати ці агресивні атаки, і слід вживати подальших контрзаходів для захисту систем від них.

3.2. Дослідження впливу програм-вимагачів на Active Directory.

Метою цієї роботи є створення відповідного тестового середовища для спостереження за моделями поведінки перевірених варіантів програм-вимагачів щодо мережевих служб. Бажаним результатом практичного дослідження є визначення того, чи працює служба Windows Server, перебуваючи під контролем перевіреного варіанту програми-вимагача.

Однак можливо, що хоча служба може реагувати, вона може бути неповно функціональною та може бути порушена непередбачуваним чином.

Таким чином, окрім визначення того, чи працює служба, пріоритетом також є визначення того, наскільки це вплинуло на службу.

У дослідженні щодо динамічного аналізу WannaCry стверджується, що значна частина динамічного аналізу передбачає встановлення базового середовища та порівняння відмінностей із середовищем зараженого. Важливою технікою динамічного аналізу зловмисного програмного забезпечення є використання лічильників продуктивності обладнання або інших індикаторів зміни обладнання.

Важливою частиною будь-якого аналізу зловмисного програмного забезпечення є належне поводження з ним. Недбале поводження зі шкідливим програмним забезпеченням може завдати небажаної шкоди; тому краще уникати використання живого середовища. Таким чином, віртуалізація приймається як частина стратегії тестування шляхом створення та налаштування віртуальної мережі та будь-якої кількості машин.

Після створення віртуального середовища базовий рівень записується для порівняння з кожною зі змінних, змінених протягом експерименту.

Схема дослідження приведена на рис. 3.1.

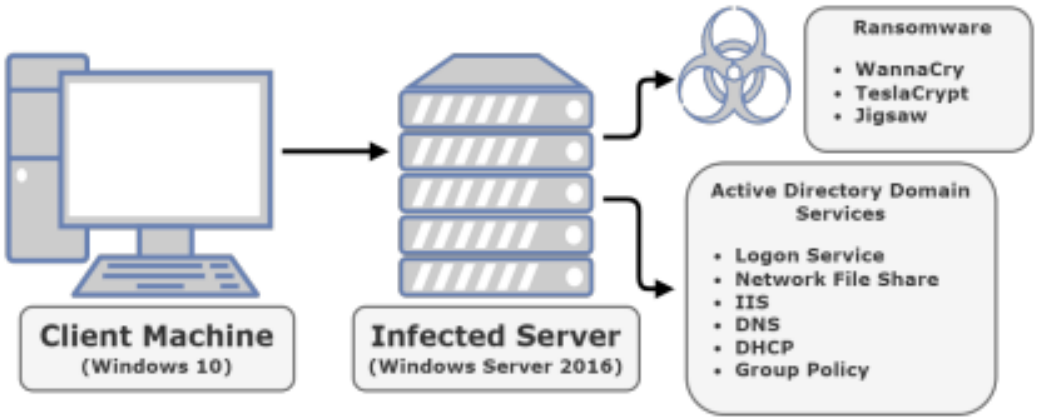


Рисунок 3.1 – Огляд підходу для аналізу вразливостей.

Для запропонованого дослідження базовим є повністю робочий сервер, тоді як змінними є кожен варіант програми-вимагача, який перевіряється під час експерименту.

Щоб забезпечити відсутність втручання у виконання програм-вимагачів і функціональність служб контролера домену, необхідно застосувати відповідну конфігурацію з кількома заходами для забезпечення стерильного віртуального середовища. Для впровадження необхідно видалити будь-яке підключення до Інтернету як з віртуальних машин, так і з хост-машини.

Це робиться не тільки для того, щоб програма-вимагач не вийшла з хост-комп’ютера та не поширилася мережею хост-комп’ютера, але й для того, щоб програма-вимагач не мала контакту з будь-якими зовнішніми серверами. Це потрібно для WannaCry, оскільки він намагається зв’язатися з доменом kill switch під час запуску, але видалення доступу до Інтернету також використовується під час тестування інших варіантів, щоб переконатися, що зовнішні фактори не впливають на виконання.

Як правило, при перевірці впливу шкідливих програм рекомендується заповнювати файлову систему штучними файлами. Хоча це не є пріоритетом у цьому випадку, оскільки метою є служби, штучні файли все одно

використовуються у випадку тестування спільного доступу до файлів у мережі та веб-сервера.

Каталоги цих служб заповнюються файлами, які легко створюються на цільовій машині, наприклад папками, текстовими файлами та файлами зображень, а не файлами, отриманими з Інтернету.

Щоб гарантувати відсутність перешкод із боку вбудованих заходів безпеки Window, попередньо встановлену програму захисту від зловмисного програмного забезпечення Windows Defender також слід вимкнути на контролері домену. Навпаки, Windows Defender слід постійно оновлювати на головній машині, щоб запобігти будь-якому випадковому виконанню за межами віртуального середовища.

У рамках стратегії тестування необхідно визначити, які служби підлягають тестуванню. Включення послуг, які зазвичай використовуються, є пріоритетом, а також включені додаткові служби, які легко налаштовуються, для отримання додаткової інформації. Щодо доменної структури та служби входу, під час входу в систему з клієнтської машини служба Центру розподілу ключів (KDC) відповідає за автентифікацію користувача, отже, його функціональність перевірена. Служба KDC також використовує базу даних облікових записів Active Directory для надання послуги автентифікації.

Щоб експериментально перевірити функціональність мережевих можливостей обміну файлами, домашній каталог може бути створений на користувачеві клієнта та доступ до нього ззовні. Без використання переспрямування папок метод доступу до домашнього каталогу за замовчуванням не вмикає автономне кешування та доступність, тому не потрібно налаштовувати додаткові об’єкти групової політики. Якщо спільний файл залишається в робочому стані, можливо, програма-вимагач може вплинути на збережені файли. Оперативний файловий ресурс із зараженими файлами все ще є цінною інформацією, оскільки він дозволяє системному адміністратору реалізовувати інші конфігурації безпеки, такі як

блокувальники змін розширення файлу або розміщення файлового ресурсу на окремому, частіше оновлюваному сервері.

Інформаційні служби Інтернету (IIS) — це власна програма веб-сервера Microsoft, призначена для використання з Windows Server. Створення та налаштування веб-сторінки з IIS на контролері домену буде оптимальною послугою для тестування можливостей програм-вимагачів.

На основі веб-сервера також можна перевірити службу доменних імен (DNS). DNS використовується для налаштування доменного імені для сервера IIS, щоб до нього можна було отримати доступ без використання IP-адреси веб-сервера. Служба DNS приймає запити для перетворення доменного імені веб-сайту, більш зручного для людини, на IP-адресу веб-сервера. Microsoft припускає, що одним із методів перевірки того, чи є цільова машина функціонуючим сервером DNS, є використання команди PowerShell. Команда «Test-DnsServer» може використовуватися з IP-адресою DNS-сервера як цільовим параметром і може вказати зону для пошуку на цільовому сервері.

Щоб перевірити функціональність служби протоколу динамічної конфігурації хоста (DHCP), клієнтська машина може видати команду «ipconfig /release», щоб видалити автоматично призначену IP-адресу. Після зараження контролера домену можна ввести команду «ipconfig /renew», щоб отримати нову адресу з сервера DHCP. Тоді клієнт має отримати IP-адресу в межах діапазону, визначеного сервером DHCP, якщо це не впливає на служби. Якщо клієнту не вдається отримати адресу від сервера, він натомість отримає її за допомогою вбудованої в Windows функції автоматичної приватної IP-адреси.

Діапазон цих адрес легко визначити, оскільки він коливається від «169.254.0.1» до «169.254.255.254» з маскою підмережі «255.255.0.0». Об’єкти групової політики можна легко налаштувати в редакторі керування груповою політикою. Контролер домену автоматично реалізує політику домену за замовчуванням, яка обмежує адміністративні привілеї та права

стандартних облікових записів користувачів. Щоб перевірити, чи служба групової політики все ще працює, можна змінити політику домену за замовчуванням після того, як клієнтська машина вже ввійшла в систему, оскільки отримання групової політики є частиною процесу входу.

Після зараження контролера домену клієнтська машина може видати команду «gpupdate /force», щоб активно отримати будь-які оновлення групової політики з моменту останнього отримання. Зміна або її відсутність у груповій політиці спостерігатиметься для визначення функціональності. В ідеалі бажаним тестом було б встановлення групової політики, яка примусово використовує певний файл зображення як фон робочого столу Windows; однак, якщо файл зображення зашифрований і його неможливо завантажити, буде важко визначити, чи групова політика в цілому залишається функціональною.

Впровадження було виконано на комп'ютері з чотирьохядерним процесором Intel i5-3570K і 16 ГБ оперативної пам'яті DDR3. Машину було відформатовано та встановлено лише необхідне програмне забезпечення для проведення експериментів. Для емуляції як контролера домену, так і клієнтської машини VirtualBox використовувався на одній хост-машині. VirtualBox використовувався через його набір функцій, які могли б значно допомогти в експерименті, а також через його природу з відкритим кодом.

Використання VirtualBox для експерименту, який включає кілька машин, позбавляє від необхідності фізичного джерела апаратного забезпечення для цих машин і дає набагато більше свободи щодо конфігурації апаратного забезпечення. Виконання розслідування за допомогою віртуальних машин також забезпечує додатковий буфер безпеки, щоб запобігти виходу з пісочниці.

Можливо, найбільш корисною для експерименту є функція знімка VirtualBox, яка дозволяє зберегти точний стан машини та згодом повернутися до нього, якщо необхідно. Після того, як сервер і клієнтська машина були повністю налаштовані, було зроблено знімок стану кожної машини. Після

запуску програмного забезпечення-вимагача та реєстрації відповідних результатів машини поверталися до незараженого стану, щоб знову почати роботу з наступним варіантом програмного забезпечення-вимагача.

Windows Server 2016 використовувався для контролера домену, оскільки це остання велика версія операційної системи Windows Server, що робить її більш актуальною для поточних і майбутніх інтересів використання. Незважаючи на те, що Server 2019 замінив 2016, 2019 не приніс помітних змін, які б вплинули на експеримент, і все ще побудовано на тій самій базовій платформі, що й Server 2016 і Windows 10, що робить його менш популярним і, ймовірно, є непотрібною зміною, яку багато організацій пропустять.

Клієнтська машина працювала під керуванням Windows 10 Consumer Edition, яка також є останньою основною споживчою операційною системою Windows. Клієнтську машину було повністю оновлено для оновлень безпеки Windows і Windows Defender, щоб клієнтська машина не була заражена та не вплинула на результати відповідей контролера домену.

Насправді в корпоративному середовищі комп’ютери персоналу автоматично оновлюватимуться через політику операційної системи Windows, тоді як сервери та комп’ютери інфраструктури залишатимуться в робочому стані, доки неочікуваний простой не змусить користувача взаємодіяти.

Крім того, штатним машинам потрібен потужний локально встановлений антивірус, щоб захистити машину від користувача, у той час як серверні машини, які відкриті для з’єднання з безлічі машин, перешкоджатимуть лише настирливому антивірусу.

Віртуальні машини були налаштовані для роботи у внутрішньому середовищі віртуальної локальної мережі (LAN), вбудованому у VirtualBox. На рис. 3.2 показано налаштування середовища віртуальної мережі.

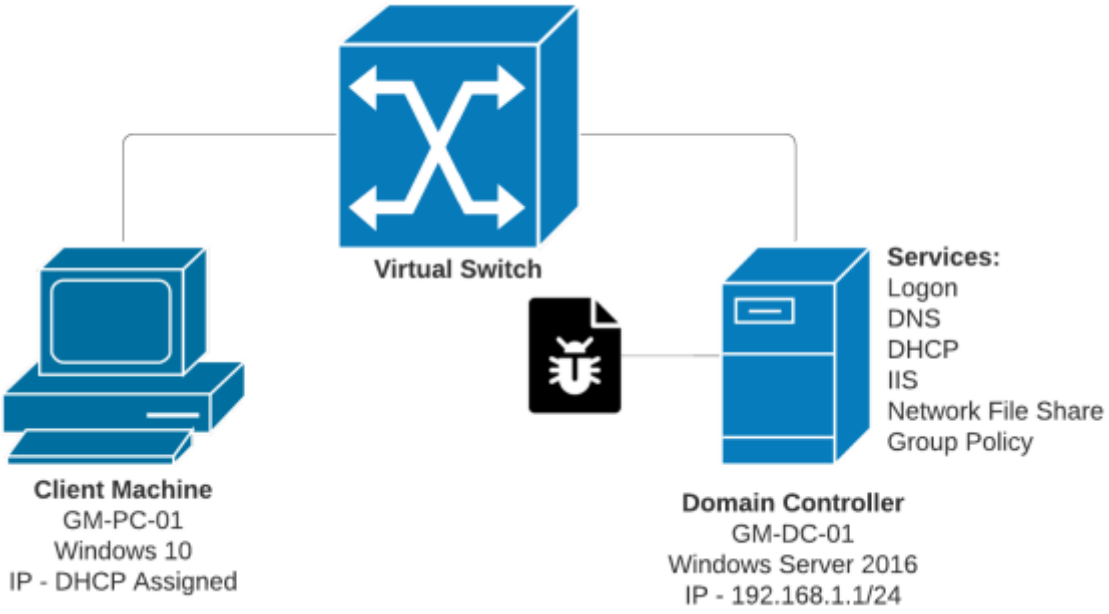


Рисунок 3.2 - Діаграма середовища віртуальної мережі.

Для дослідження було обрано три варіанти програм-вимагачів. Виконувані файли WannaCry, TeslaCrypt і Jigsaw були отримані з репозиторію GitHub «theZoo». Репозиторій було створено з метою архівування автентичних, легкодоступних зразків шкідливого програмного забезпечення для дослідницьких цілей.

Після завантаження виконуваних файлів їх було завантажено до VirusTotal для перевірки їх автентичності. Подання для WannaCry можна побачити на рис. 3.3.

У рамках підготовки контролера домену до зараження Windows Defender було видалено за допомогою «Майстра видалення ролей і функцій» у програмі Server Manager, щоб уникнути втручання у виконання програми-вимагача. Однак інсталяційний пакет Server 2016, отриманий від Microsoft, містив оновлення безпеки, датовані 2018 роком.

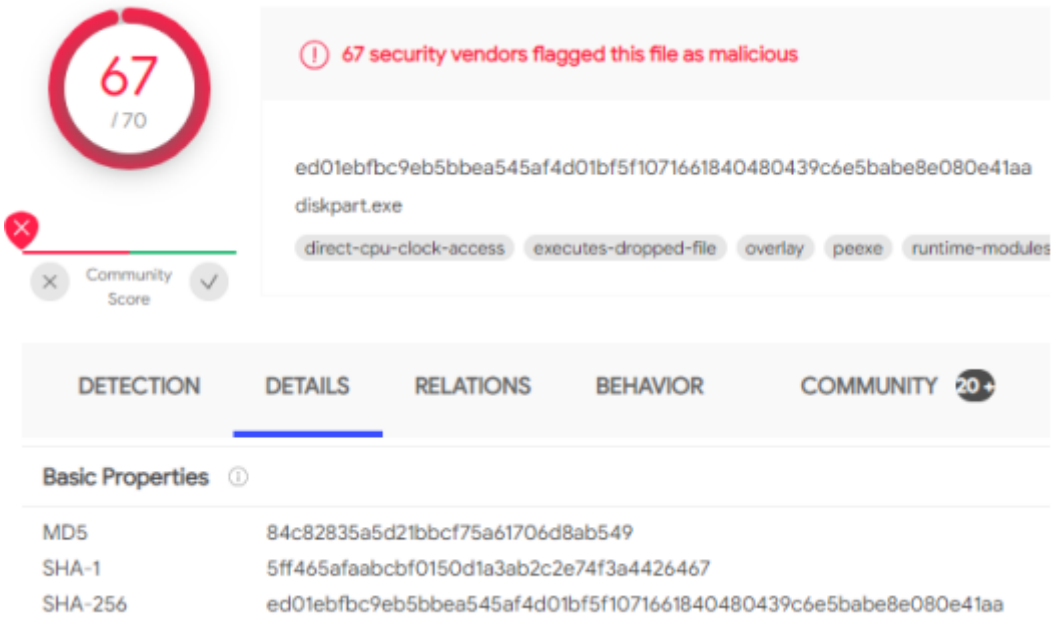


Рисунок 3.3 - Надсилання виконуваного файлу WannaCry до VirusTotal із згенерованими хешами.

Сценарій PowerShell, опублікований Microsoft, використовувався для визначення того, що встановлені оновлення забезпечуватимуть захист від WannaCry та CVE-2017-0144, результати показані на рис 3.4.

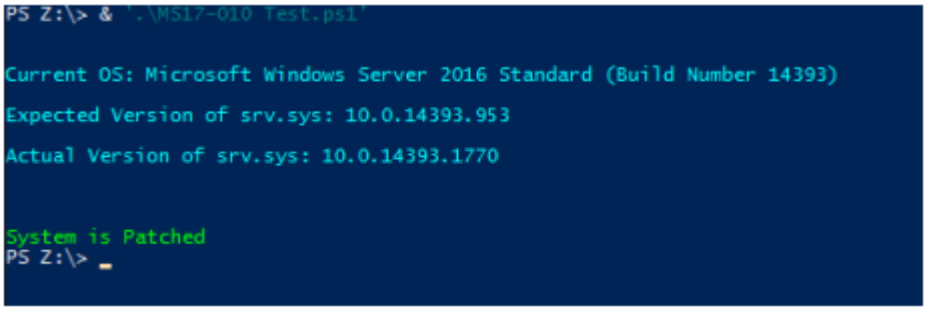


Рисунок 3.4 - Вивід сценарію PowerShell із зазначенням статусу виправлення.

Подальше дослідження показало, що встановлені оновлення безпеки мали запобігати уразливості SMB, яку WannaCry буде використовувати для своїх можливостей поширення в мережі. Однак, оскільки цей експлойт стосується лише мережевої передачі WannaCry, він не заважає процесу

виконання, оскільки ця відповідальність лежить на Windows Defender, який не лише застарів, але й видалено з сервера. Спосіб передачі WannaCry не має відношення до цього дослідження, оскільки програму-вимагач було розміщено безпосередньо на віртуальній машині з хоста; тому оновлення безпеки можна проігнорувати.

Під час тестування використовувався додатковий програмний монітор процесу спеціально для запису активності процесу на контролері домену. Дія процесу, яку слід контролювати для цього дослідження, є операцією «виходу з процесу», що стосується відповідних послуг. Після успішного зараження було створено звіт із детальним описом процесів, які завершилися. Існує небагато програмного забезпечення для автоматизованих звітів, яке б точно перевіряло кожну службу та виконувало бажані завдання після налаштування, наприклад тестування додаткових налаштованих параметрів. Можливо, сценарій PowerShell може бути створений і використаний на клієнтській машині для перевірки необхідних служб на контролері домену.

Кожну з наведених нижче служб було налаштовано для легкого тестування функціональності служби та, де це можливо, налаштовано з додатковими параметрами, які дозволять дослідити вплив на типові налаштування служби в реальному світі.

3.3. Результати досліджень вразливостей

Результати, наведені в таблиці 3.1, ілюструють, чи була зазначена служба принципово працездатною після зараження веб-сервера програмою-вимагачем. Усі служби певною мірою працювали під час тестування на всі три варіанти програм-вимагачів. Цей висновок був очікуваним; однак представлена таблиця не відображає ступінь впливу на кожну службу.

Таблиця 3.1

Результати тестування роботи служб при інфікуванні

Services	WannaCry	TeslaCrypt	Jigsaw
Logon Service	✓	✓	✓
Network File Share	✓	✓	✓
IIS	✓	✓	✓
DNS	✓	✓	✓
DHCP	✓	✓	✓
Group Policy	✓	✓	✓

Рівень ударних перешкод, створених кожним варіантом, детальніше описано в наступних підрозділах. Метод ручного тестування, який використовувався під час розслідування, не міг виявити, як на кожну службу вплинули її системні процеси. Монітор процесу також використовувався для перевірки результатів, отриманих за допомогою методу ручного тестування, щоб перевірити процес обробки, який відбувався під час зараження програмою-вимагачем. Файли журналів, створені Process Monitor, не показали жодних змін перевірених процесів обслуговування. Однак файли журналу створили інші помітні записи, зокрема варіанти програм-вимагачів, які припиняють процес «vssadmin.exe», відповідальний за резервне копіювання тіньових копій томів. Це поширена тактика, яку використовують програми-вимагачі, щоб завадити користувачам і деяким комерційним програмам резервного копіювання відновити свої дані через тіньову копію диска до зараження програмою-вимагачем. Показавши, що варіанти програм-вимагачів припинили цей процес, ми можемо визначити, що варіанти програм-вимагачів успішно запущені та не змінили процес виконання в результаті виявлення.

3.3.1. Глибина впливу на служби.

Під час розслідування було досліджено кілька каталогів і файлів на контролері домену, щоб визначити рівень впливу, завданого кожним варіантом програми-вимагача. Файли, відображені в таблиці 3.2, являють собою файли, критичні для роботи певних служб, а також створені вручну штучні файли для подальшого тестування.

Таблиця 3.2

Результати тестування роботи служб при інфікуванні

Domain Service	Relevant File Path	Description of Relevant Data
Logon Service	C:\Windows\NTDS\ntds.dit	Database file containing credentials belonging to Active Directory users
Network File Share	C:\Share\ChristopherGuzman\ and \\GM-DC-01\Share\ChristopherGuzman	Mapped home directory path, local and network, respectively, for the user "Christopher Guzman"
IIS	C:\inetpub\wwwroot\	Default directory designated to IIS to store files relevant to displaying the web page
DNS	C:\Windows\System32\dns\	Directory containing DNS records
DHCP	C:\Windows\System32\dhcp\dhcp.mdb	Database file responsible for storing DHCP scope information
Group Policy	C:\Share\CommonFiles\wallpaper.png	Path of wallpaper image used for the second test policy
	C:\Windows\SYSVOL\domain\policies	Default path for storing group policy objects

У рамках стратегії тестування команди використовувалися або для ручного тестування служб, або для виявлення ступеня впливу інфекції. Здебільшого вони виконувалися на клієнтському пристрої, за винятком команди «TestDnsServer», яку не можна було виконати з клієнтського пристрою.

У наступних підрозділах ми докладно представляємо вплив варіантів програм-вимагачів на служби входу, спільний доступ до файлів у мережі, IIS, DNS, DHCP і, нарешті, групову політику.

У кожному підрозділі представлено окрему службу Windows Active Directory і докладну інформацію в її межах.

3.3.2. Вплив на служби входу.

Під час дослідницьких експериментів жоден із перевірених варіантів програм-вимагачів не спричинив невдачу клієнтської машини в тесті входу. База даних, у якій зберігаються облікові дані Active Directory, що використовуються службою входу (розташована на шляху, показаному в таблиці 3.2), є каталогом, який було виключено зі сфери шифрування WannaCry, можливо, через його критичний характер для системи. Цей висновок показує, що варіанти програм-вимагачів не тільки не закрили відповідну службу, але й не зашифрували та не вплинули на базу даних, що містить облікові дані користувача, які використовувалися для входу з клієнтської машини.

3.3.3. Вплив на спільний доступ до файлів у мережі.

Під час усіх трьох тестів кожен варіант програми-вимагача дав однакові результати. Спільний мережевий файл залишався доступним для клієнтської машини; однак усі три варіанти програм-вимагачів шифрували файли, що зберігаються в спільному ресурсі. Цікаво, що шлях до файлу спільного мережевого ресурсу був новостворeним каталогом у корені диска C, що свідчить про те, що протестовані варіанти програм-вимагачів не задовольнялися стандартними вбудованими каталогами користувача (такими як «Завантаження, Документи, Зображення тощо) і натомість просувається далі, шифруючи будь-який створений користувачем каталог.

Ця інформація дозволяє досліджувати подальші шляхи захисту спільного файлу від програм-вимагачів, наприклад використання каталогу системних файлів, прихованого каталогу або зіставлення з каталогом на іншому сервері.

3.3.4. Вплив на IIS.

Крім того, усі варіанти програм-вимагачів дозволяли серверу IIS залишатися онлайн, але також мали подібний вплив на кореневий каталог IIS. Першим розгортанням було WannaCry, яке націлювалося на каталог «wwwroot», видаляючи свій підписний текстовий файл і програму, а також зашифровані вже існуючі файли в каталозі.

З іншого боку, TeslaCrypt і Jigsaw вибрали лише шифрування файлів у каталозі. Файл зображення в каталозі, на який посилався файл HTML, було зашифровано всіма трьома варіантами; однак сам файл HTML не був. Це було підтверджено як для TeslaCrypt, так і для Jigsaw, вибравши їхню опцію для виведення списку зашифрованих файлів, що показало, що жодна з них не націлилася на файл HTML. Перелік файлів і доданих до них розширень у каталозі «wwwroot» після шифрування WannaCry можна побачити на рис. 3.5.

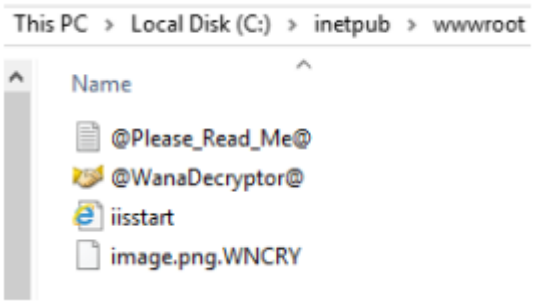


Рисунок 3.5 - Кореневий каталог IIS під зараженням WannaCry

Це призвело до відображуваної HTML-сторінки, яка правильно відображала обидва текстові розділи, але неправильно відображала зображення. Замість зображення була піктограма, яка представляла «X», як показано на рис. 3.6.

Рисунок 3.6 - Помилка відображення зображення, на яке посилається файл «.html».

Після отримання результатів і виявлення помилки шифрування HTML-файлу зі всіма трьома варіантами, слід відзначити, що, оскільки служба IIS вже була запущена, коли було запущено програму-вимагач, вона могла захистити та заблокувати файл HTML під час його використання.

Другий тест із незначними змінами спростував це, оскільки кожен варіант програми-вимагача все ще вирішив не націлювати HTML-файл для шифрування, поки службу IIS було зупинено. Подальші дослідження в літературі виявили повний список розширень файлів, на які націлені три протестовані варіанти, і дійшли висновку, що всі три виключають розширення «.html» зі своєї цільової області.

3.3.5. Вплив на DNS.

Як видно вище, служба DNS залишалася працездатною разом із зараженням усіх трьох варіантів. Коли IIS працював, веб-сторінка відповідала клієнтській машині, яка зверталася до веб-сторінки за допомогою URL-адреси «www.gm-site.com», усуваючи потребу тестувати службу IIS за допомогою IP-адреси сервера.

Використання параметра команди «displaydns» на клієнтській машині, також показало, що DNS-сервер надав повний правильний запис. Крім того,

команда PowerShell для перевірки служби DNS використовувалася для перевірки того, чи IP цільового сервера представляв функціональний DNS-сервер. Завдяки методу зберігання даних, орієнтованих на DNS, мало місця для втручання в службу DNS. Усі записи DNS зберігаються в критичному для системи підкаталозі “system32” і додаються з розширенням файлу “.dns”, отже, було б надзвичайно незвичайно, щоб варіант програми-вимагача націлився на самі записи DNS, навіть за допомогою загальної стратегії шифрування, якщо він не був створений спеціально для націлювання на серверне середовище.

3.3.6. Вплив на DHCP

Подібно до DNS, у службу DHCP важко втручатися, окрім повної зупинки служби, чого не вдалося зробити жодному з трьох варіантів. Служба DHCP також зберігає свої файли в підкаталозі «system32» і не використовує інші файли зі стандартних каталогів, зручних для користувача. Клієнтська машина не виявила проблеми з отриманням IP-адреси від сервера DHCP за допомогою відповідних команд усіх трьох варіантів.

Менеджер DHCP-сервера чітко показував випуск і оновлення в реальному часі IP-адреси, коли клієнтська машина видавала відповідні команди, які можна було побачити в графічному інтерфейсі програми диспетчера DHCP-сервера, оскільки він також залишався робочим усіма трьома варіантами програм-вимагачів.

3.3.7. Вплив на групову політику

Не дивно, що групова політика також залишалася функціональною з подібними перебоями в тестованій області служби. Перший тест передбачав використання політики, яка забороняє доступ до командного рядка для стандартного облікового запису користувача, що виявилося успішним під час

оновлення політики на клієнтській машині, коли контролер домену був заражений.

Другий тест, який встановив шпалери за замовчуванням для використання клієнтською машиною, передбачав визначення шляху до файлу зображення, який використовується як шпалери. Це вказувало на файл у каталозі, на який націлювалися всі три варіанти, і, як наслідок, файл зображення було зашифровано.

Результатом тесту стало те, що на клієнтській машині не вдалося застосувати політику та замінити фонове зображення логотипа Windows за замовчуванням на порожні чорні шпалери. Це демонструє здатність групової політики залишатися працездатною під час зараження; однак це також показує нездатність захистити та приховати відповідні додаткові файли для служби.

З трьох перевірених варіантів програми-вимагача всі перевірені служби залишалися робочими. Служби, які використовували файли, що не належать до конфігурацій служби за замовчуванням, і шляхи до файлів мали перебої в їх функціональності, тоді як критичні для системи шляхи залишалися недоторканими. Це підтвердило вірність попередньої гіпотези.

Незважаючи на те, що протестовані служби залишалися в робочому стані, це були власні послуги Microsoft, які пропонувалися в пакеті Windows Server, які варіанти крипто-вимагачів могли помилково ідентифікувати як критичні для системи, а не системні процеси, які можна було зупинити без наслідків. У майбутньому дослідженні тестування програм сторонніх розробників від комп’ютерно-орієнтованого програмного забезпечення до програмного забезпечення, відповідального за фізичні e ntities можуть дати дуже різні результати, оскільки програмне забезпечення третіх сторін зазвичай не використовує критичні для системи шляхи до файлів.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

4.1 Долікарська допомога при шоку.

Розглянемо порядок, що визначає механізм надання домедичної допомоги при підозрі на шок не медичними працівниками.

Шок – це стан між життям та смертю; загальний тяжкий розлад життєво важливих функцій організму, спричинений порушенням нервової регуляції життєво важливих процесів; характеризується розладами гемодинаміки, дихання, обміну речовин.

Ознаки шоку у постраждалого:

бліда, холодна і волога шкіра;

слабкість;

неспокій;

сухість в роті, відчуття спраги;

часте дихання (більш ніж 20 вдихів за хвилину);

порушення свідомості; непритомність.

Причинами виникнення шоку можуть бути:

зовнішня кровотеча;

внутрішня кровотеча;

травми різного ґенезу;

опіки;

серцевий напад тощо.

Послідовність дій при наданні домедичної допомоги постраждалим при підозрі на шок не медичними працівниками:

1) переконатися у відсутності небезпеки;

2) провести огляд постраждалого, визначити наявність свідомості, дихання;

3) викликати бригаду екстреної (швидкої) медичної допомоги;

4) якщо у постраждалого відсутнє дихання, розпочати проведення серцево-легеневої реанімації;

5) усунути причину виникнення шокового стану: зупинити кровотечу, іммобілізувати перелом тощо;

6) надати постраждалому протишокове положення:

а) перевести постраждалого в горизонтальне положення;

б) покласти під ноги постраждалого ящик, валик з одягу тощо таким чином, щоб ступні ніг знаходились на рівні його підборіддя;

в) підкласти під голову постраждалого одяг/подушку;

г) вкрити постраждалого термопокривалом/покривалом;

7) забезпечити постійний нагляд за постраждалим до приїзду бригади екстреної (швидкої) медичної допомоги;

8) при погіршенні стану постраждалого до приїзду бригади екстреної (швидкої) медичної допомоги повторно зателефонувати диспетчеру екстреної медичної допомоги.

4.2. Розробка, оформлення кімнати для психологічного розвантаження працівників

Напружений ритм життя шкільних працівників, інтенсифікація їх праці на тлі низької рухової активності породжують відомий дисонанс між вимогами, що пред'являються до інтелекту, емоційній сфері, і порівняно малої фізичним навантаженням. Робота нервової системи в подібному режимі часто веде до підвищеного напрузі, невміння розслаблятися, виходити з напруженого стану, знаходити психічну рівновагу. У більшості випадків у людей, схильних "хворобам століття" - неврозів, гіпертонії та ішемічної хвороби серця, - можна фіксувати підвищену м'язову напруженість, втрату навику довільного розслаблення м'язів. Крім того, інтенсивне навчання деяких предметів викликає необхідність зняття психічної напруги. Все це ставить перед психологічною службою школи нагальну задачу створення кабінету психологічного розвантаження (КПР).

Кабінет психологічного розвантаження в школі працює в п'яти режимах:

1. Психологічна розвантаження співробітників і школярів після напруженої роботи в кінці робочого (навчального) дня або в спеціально відведений для цього час.

2. Психологічний настрій (мобілізація) тих співробітників і школярів, які насилу включаються в напружений ритм роботи на початку робочого дня, навчання навичкам мобілізації в стресі (контрольна, іспит і т.п.).

3. Зняття психологічного навантаження викладачів і школярів відповідно до курсу, призначеним психотерапевтом.

4. Психопрофілактична робота з практично здоровими вчителями та школярами (навчання методам релаксації, медитації, аутогенного тренування, навичкам безконфліктного спілкування, тренінг спілкування і т.д.).

5. Забезпечення процесу інтенсивного навчання, включаючи методи суггестопедии, релаксопедії, гіпнопедії, а також використання кімнати психологічного розвантаження як експериментальної бази для розробки нових методів навчання.

Питання про можливість і необхідність відвідування сеансів психологічного розвантаження вирішується співробітниками психологічної служби на основі даних психодіагностики в залежності від характеру впливу. Для індивідуальної роботи відводиться від 5 до 30 хвилин на одну людину, на групу - 60 хвилин. При наявності в КПР 12-15 місць його пропускна здатність становить 60-80 чоловік у зміну, а курсове лікування можуть отримати одночасно до 200 чоловік, оскільки заняття проводяться два-три рази на тиждень. При проведенні занять інтенсивного навчання пропускна можливість КПР знижується, однак особи, які проходять інтенсивний курс, одночасно випробовують і психопрофілактичний вплив.

До облаштування КПР пред'являються певні технічні вимоги. Кабінет повинен складатися з двох зв'язаних між собою кімнат. Перша кімната є одночасно і робочим кабінетом психологічної служби. Сюди винесена вся апаратура, обслуговуюча сеанси психотерапії і заняття інтенсивного навчання. Крім того, з операторської через спеціальне дзеркальне скло з одного боку можна проводити невключенное спостереження за поведінкою відвідувачів в психотерапевтичному залі. Такий зал обладнується 10-15 м'якими кріслами з високими підголовниками і вмонтованими в них роз'ємами для підключення індивідуальних навушників. Площа залу повинна бути не менше 40 кв. м, стелі повинні бути досить високими, щоб відвідувачі не відчували себе в тісноті і щоб в затемненому залі у них виникало почуття усамітнення.

Інтер'єр кабінету психологічного розвантаження повинен викликати у відвідувачів позитивні емоції, надавати сприятливий вплив на організм людини. Шумоізольовані стіни КПР повинні бути блакитного або світло-зеленого кольору. В якості будівельного матеріалу використовуються

перфопліти або акустична штукатурка, в декоративній обробці застосовуються шкірозамінник, дерматин та інші матеріали, за допомогою яких можна створити затишок, що позитивно впливає на настрій людини.

Психотерапевтичний зал також повинен бути обладнаний автоматичною системою затемнення вікон, екраном, світломузичним пристроєм, акустичними колонками, апаратами для іонізації, зволоження та кондиціонування повітря, великим акваріумом з підсвічуванням і технічними засобами управління станом людини (ТСУС), запропонованими С. М. Зоріна. Будучи головною частиною керованої цветозвукового середовища, ТСУС являє собою поліфункціональну систему для реалізації специфічних аудіовізуальних впливів з метою управління увагою, релаксацією, активізацією, а також для зниження рівня антісуггестівних бар'єрів. У систему ТСУС входить два функціональних блоку:

1. Установка керованого колірного клімату. Вона має вигляд рами з алюмінієвого сплаву П-образного профілю, розташованої по периметру кімнати у стелі. П'ять груп ламп накачування, змонтовані на цій рамі, дозволяють здійснювати управління яскравістю і спектральним складом освітлюваної аудиторії. Всі світильники спрямовані в стелю, щоб забезпечувати м'який, розсіяне світло в залі. Освітлення психотерапевтичного залу може змінюватися як вручну оператором, так і автоматично, за заздалегідь розробленою для кожного виду впливу програмою.

2. Светодінамінеская система (СДС). На відміну від установки керованого колірного клімату, що змінює лише яскравість і кольоровість освітлення, СДС дозволяє здійснити на екрані синтез керованих параметрів світлодинамічних символів. Ці символи, змінюючи за бажанням оператора або за заданою програмою свої обриси, колір, яскравість, насиченість, швидкість і спрямованість руху, можуть з'єднуватися в складні, що розвиваються у часі динамічні композиції, що мають багатопланове застосування.

Все управління психотерапевтичним сеансом здійснюється з операторської кімнати, де на стелажах розташовані стереомагнітофони з Мікшерський пультом, діа- та кінопроектори, що забезпечують за допомогою спеціально підібраних слайдів, кінозарісовок і музики емоційно-естетичний вплив на людину.

.

ВИСНОВКИ

У роботі було розглянуто та описано основні загрози можливих атак на Active Directory, оскільки використання Windows Server є досить популярним.

Було розглянуто головні можливості атак на доменну систему та описано основні процедури, які дозволять запобігти хакерським атакам.

У другому розділі було проаналізовано уразливість домену від програм-вимагачів, які наносять найбільшу шкоду підприємствам, які залежать від корпоративних мережевих структур, особливо важливими компонентами в умовах пандемії та війни.

У третому розділі було проведено дослідження вразливості основних служб Active Directory при ураженні програмами –вимагачами.

Встановлено , що основними аспектами найбільшого посилення захисту є своєчасне оновлення усіх систем корпоративної мережі та підвищення кваліфікації персоналу щодо обізнаності в процедурах запобігання хакерським атакам.

БІБЛІОГРАФІЯ

1. Franke U. The cyber insurance market in Sweden / Comput. Secur., 2017. – C. 130–144
2. Datto Inc. Ransomware Report. 2020. URL: https://www.datto.com/resources/dattos-global-state-of-the-channelransomware-report.
3. Huang D.Y., Aliapoulios M.M., Li V.G. Tracking Ransomware End-to-end. In Proceedings of the 2018 39th IEEE Symposium on Security and Privacy (SP) / San Francisco, 21–23 May 2018.- C. 618–631.
4. Ramsey D. Google, UC San Diego and NYU Estimate $25 Million in Ransomware Payouts. URL : https:// ucsdnews.ucsd.edu/pressrelease/google_uc_san_diego_and _nyu_estimate_25_million_in_ransomware_payouts.
5. Sophos Labs 2019 Threat Report. 2019. URL: https://www.sophos.com/en-us/medialibrary/PDFs/technicalpapers/sophoslabs-2019-threat-report.pdf.
6. SamSam: The (Almost) Six Million Dollar Ransomware. 2018. URL : https://www.sophos.com/ en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf.
7. Deep Instinct. Cyber Threat Landscape Report 2019–2020. 2020. URL: https://info.deepinstinct.com/hubfs/Cyber_ Threat_Landscape_Report_2019-2020.pdf.
8. Microsoft. How to Detect, Enable and Disable SMBv1, SMBv2, and SMBv3 in Windows. 2020. URL: https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3.
9. Brewer, R. Ransomware attacks: Detection, prevention and cure / Netw. Secur 2016, 2016. – C. 5–9.
10. Adamov A., Carlsson A. The state of ransomware. Trends and mitigation techniques / In Proceedings of the 2017 IEEE East-West Design & Test

Symposium (EWDTS) : Novi Sad, Serbia, 29 September 2 October, 2017. - С. 1–8.

11. Coveware. Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate. 2020. URL : https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate.

12. Sophos. The State of Ransomware 2020. 2020. URL : https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf.

13. Bistarelli S., Parroccini M., Santini, F. Visualizing Bitcoin Flows of Ransomware: WannaCry One Week Later / InProceedings of the Italian Conference on Cybersecurity (ITASEC), Milan, Italy, February 201. – С. 6–9.

14. Kshetri N.; Voas J. Do Crypto-Currencies Fuel Ransomware? / IT Prof., 19, 2017.- С. 11–15.

15. Microsoft. SMBv1 Is Not Installed by Default in Windows 10 Version 1709, Windows Server Version 1709 and Later Versions. 2020. URL: https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installedby-default-in-windows.

16. Microsoft. Overview—Product End of Support. 2020. URL: https://docs.microsoft.com/en-us/lifecycle/overview/ product-end-of-support-overview.

17. Mamedov O., Ivanov A. ExPetr/Petya/NotPetya is a Wiper, Not Ransomware 2017. URL: https://securelist.com/ expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/.

18. Suiche M. Petya.2017 Is a Wiper Not a Ransomware. 2017. URL: https://blog.comae.io/petya-2017-is-a-wiper-not-aransomware-9ea1d8961d3b.

19. Government of the United Kingdom. UK Exposes Series of Russian Cyber Attacks against Olympic and Paralympic Games. 2020. URL : https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-andparalympic-games.

20. Starks T. US Charges Russian GRU Officers for NotPetya, Other Major Hacks. 2020. URL: https://www.cyberscoop.com/ russian-hackers-notpetya-charges-gru/.

21. United States Department of Justice. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. 2020. URL: https://www.justice.gov/opa/pr/six-russian-gruofficers-charged-connection-worldwide-deployment-destructive-malware-and.