(19) Евразийское патентное ведомство

(11) 044131 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.07.26

(21) Номер заявки
202293427

(22) Дата подачи заявки
2022.12.22

(51) Int. Cl. ***G06F 21/50*** (2013.01)
G06F 21/55 (2013.01)

(54) СПОСОБ И СИСТЕМА ПРЕДОТВРАЩЕНИЯ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ОБЪЕКТАМ КОРПОРАТИВНОЙ СЕТИ

(31) **2022131236**
(32) **2022.11.30**
(33) **RU**
(43) **2023.07.25**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Балашов Александр Викторович, Черепанов Павел, Нагорнов Иван Григорьевич, Глазунов Никита Сергеевич, Соломатин Александр Игоревич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-B2-10313382
US-B2-11012472
US-B2-11308211
US-A1-20200293917
US-10986121

(57) Изобретение относится к области обеспечения безопасности корпоративной сети, в частности, с помощью предотвращения получения несанкционированного доступа к объектам корпоративной сети, являющимися высокопривилегированными активами (англ. High Value Asset или HVA). Техническим результатом является повышение эффективности защиты корпоративной сети от компрометации объектов и получения доступа к высокопривилегированными активам. Заявленный технический результат достигается за счет способа предотвращения компрометации объектов службы каталогов (MS AD) в корпоративной сети, выполняемого с помощью вычислительного устройства и содержащего этапы, на которых: получают данные из хранилища MS AD корпоративной сети, характеризующие объекты сети и их атрибуты, включающие в себя по меньшей мере дескриптор безопасности, содержащий списки (ACL) и записи (ACE) контроля доступа объектов; выполняют парсинг атрибутов объектов MS AD; определяют высокопривилегированные объекты (HVA) MS AD в корпоративной сети на основании правил и парсинга ACL и ACE, причем правила представляют собой по меньшей мере количество связей HVA объекта с другими объектами MS AD; определяют объекты MS AD, связанные с HVA, которые позволяют получить к ним доступ посредством текущих привилегий доступа, или их изменения или посредством горизонтального продвижения по сети; формируют граф на основе собранных данных, где узлами являются объекты MS AD, а ребрами - параметры доступа между объектами MS AD; выполняют моделирование пути атаки на HVA на основе полученного графа, на котором определяют по меньшей мере один подграф с объектами MS AD, содержащий узлы, позволяющие получить управление над HVA или связанными с ним объектами MS AD с помощью по меньшей мере одного из: передачи текущих прав доступа, изменения текущих прав доступа, добавления новых прав доступа, или использования текущих прав доступа; осуществляют мониторинг объектов MS AD для определения изменений параметров привилегий доступа на узлах, выявленных на подграфе; передают данные по выявленным на подграфе объектам в систему контроля при изменении их привилегий доступа; выполняют управление привилегиями доступа на выявленных объектах MS AD в части их изолирования от других объектов MS AD и/или понижения их привилегий доступа.

044131 B1

044131 B1

Область техники

Изобретение относится к области обеспечения безопасности корпоративной сети, в частности, с помощью предотвращения получения несанкционированного доступа к объектам корпоративной сети, являющимся высокопривилегированными активами (англ. High Value Asset или HVA).

Уровень техники

Понятие HVA относится к объектам сети, которые хранят критичную информацию для полноценного функционирования сетевой инфраструктуры и компрометация которых может привести к критическим или необратимым последствиям в ее работе. К примерам такого рода активов можно отнести:

Контроллеры домена;

Список администраторов домена;

Группы, такие как: Enterprise Admins, Domain Admins, Backup Operators, Server Operators;

Сервера баз данных;

AD CS (сервера центров сертификации) и др.

Другим примером определения HVA в корпоративной сети может являться подход, предложенный компанией Microsoft® (https://docs. microsoft.com/ru-ru/security/compass/privileged-access-access-model).

Из-за огромного количества объектов, их списков и записей контроля доступа (ACL - Access control list и ACE - Access control entries), которые находятся в службе каталогов Microsoft Active Directory (MS AD) для управления предоставлением доступа каждому из объектов, управлять такими разрешениями чрезвычайно трудно. Также возможность управления усложняется ввиду отсутствия графического представления объектов управления и связей между ними. Ошибка настройки списков и записей контроля доступа (ACL и ACE) представляет собой типовой недостаток настройки безопасности. Находясь внутри корпоративной сети и имея сетевой доступ к службе каталогов, домену или даже в группе доменов (лес), злоумышленник будет анализировать полномочия и привилегии всех объектов относительно скомпрометированной учетной записи или хоста, к которому он имеет доступ и, возможно, контроль. Предметом анализа будет являться поиск короткого маршрута до высокопривилегированного актива, которым может являться хост или учетная запись разного типа (как администратора, так и сервисная или учетная запись компьютера). Реализуя набор действий по повышению привилегий и горизонтальному продвижению, злоумышленник будет производить эксплуатацию недостатков настройки безопасности списков и записей контроля доступа (ACL и ACE) контролируемого объекта, пока не получит контроль над необходимым высокопривилегированным активом.

Из уровня техники известно решение при формировании представления структуры сети в виде графа для последующего моделирования вектора атаки на узлы сети (US 20170032130 A1, 02.02.2017). Решение описывает систему событийного информирования и реагирования (SIEM), в которую передаются данные моделирования векторов атак, которые могут свидетельствовать об аномальной активности в сети. Формируется список рангов и критерий сложности доступа к тому или иному активу внутри сети, который может стать целью злоумышленников.

Непокрытой областью вышеупомянутого SIEM решения является отсутствие анализа непосредственно службы каталогов и анализа существующих ACL и ACE объектов, что не позволяет определять существующие пути атак на HVA внутри корпоративной сети.

Сущность изобретения

Решаемой технической проблемой в рамках заявленного решения является создание нового эффективного подхода для предотвращения компрометации объектов, позволяющих получить доступ к HVA.

Техническим результатом является повышение эффективности защиты корпоративной сети от компрометации объектов и получения доступа к высокопривилегированными активам.

Заявленный технический результат достигается за счет способа предотвращения компрометации объектов службы каталогов (MS AD) в корпоративной сети, выполняемый с помощью вычислительного устройства и содержащий этапы, на которых:

получают данные из хранилища MS AD корпоративной сети, характеризующие объекты сети и их атрибуты, включающие в себя по меньшей мере дескриптор безопасности, содержащий списки (ACL) и записи (ACE) контроля доступа объектов;

выполняют парсинг атрибутов объектов MS AD;

определяют высокопривилегированные объекты (HVA) MS AD в корпоративной сети на основании правил и парсинга ACL и ACE, причем правила представляют собой по меньшей мере количество связей HVA объекта с другими объектами MS AD;

определяют объекты MS AD, связанные с HVA, которые позволяют получить к ним доступ посредством текущих привилегий доступа, или их изменения или посредством горизонтального продвижения по сети;

формируют граф на основе собранных данных, где узлами являются объекты MS AD, а ребрами - параметры доступа между объектами MS AD;

выполняют моделирование пути атаки на HVA на основе полученного графа, на котором определяют по меньшей мере один подграф с объектами MS AD, содержащий узлы, позволяющие получить управление над HVA или связанными с ним объектами MS AD с помощью по меньшей мере одного из:

передачи текущих прав доступа, изменения текущих прав доступа, добавления новых прав доступа или использования текущих прав доступа;

осуществляют мониторинг объектов MS AD для определения изменений параметров привилегий доступа на узлах, выявленных на подграфе;

передают данные по выявленным на подграфе объектам в систему контроля при изменении их привилегий доступа;

выполняют управление привилегиями доступа на выявленных объектах MS AD в части их изолирования от других объектов MS AD и/или понижения их привилегий доступа.

В одном из частных примеров осуществления параметры доступа между объектами MS AD представляют собой по меньшей мере одно из: связи привилегий между объектами, на которые эти привилегии распространяются, разрешения между объектами, параметры доверия между доменами.

В другом частном примере осуществления привилегии объектов MS AD представляют собой токены доступа с ассоциированными привилегиями пользователя.

В другом частном примере осуществления привилегии токена доступа являются способом изменения уровня доступа к объекту MS AD корпоративной сети.

В другом частном примере осуществления каждый объект MS AD представляет собой по меньшей мере одно из: пользователи, компьютеры, группы безопасности, групповые политики (Group Policy Object), организационные подразделения (Organizational Unit), доверительные отношения между доменами.

В другом частном примере осуществления на выявленном подграфе осуществляют мониторинг ошибок в конфигурации безопасности MS AD, на основании правил проверки ошибок в конфигурации объектов MS AD.

В другом частном примере осуществления выполняют корректировку конфигураций привилегий доступа на объектах MS AD.

Заявленное решение также осуществляется с помощью системы предотвращения компрометации объектов службы каталогов (MS AD) в корпоративной сети, при этом система содержит по меньшей мере один процессор и память, хранящую машиночитаемые инструкции, которые при их выполнении процессором реализуют вышеуказанный способ.

Краткое описание чертежей

Фиг. 1 иллюстрирует блок-схему выполнения заявленного способа.

Фиг. 2 иллюстрирует пример графа объектов MS AD.

Фиг. 3 иллюстрирует пример подграфа объектов MS AD.

Фиг. 4 иллюстрирует пример вычислительной системы.

Осуществление изобретения

На фиг. 1 представлена блок-схема выполнения этапов заявленного способа (100) предотвращения компрометации объектов MS AD в корпоративной сети. На первом этапе (101) выполняется обращение к MS AD для получения информации по объектам. Сбор данных может выполняться автоматизированным модулем сбора данных. Сбор данных выполняется с помощью Windows API и функции пространства имен LDAP для сбора данных с контроллеров домена и систем на базе ОС Windows, присоединенных к домену. При сборе информации автоматически определяется, к какому домену принадлежит хост, и осуществляется сбор основных данных об объекте, например, следующего вида:

Членство в группе безопасности;

Доверие домена;

Права на объекты Active Directory;

Ссылки на групповую политику;

Структура дерева OU;

Свойства объектов компьютера, группы и пользователя;

Права администратора SQL;

И другие.

Дополнительно с каждого компьютера может собираться дополнительный набор данных:

Члены группы локальных администраторов, удаленных рабочих столов, распределенных COM и групп удаленного управления;

Активные сеансы, соотнесенные с системами и хостами, в которых пользователи в интерактивном режиме вошли в систему.

По итогам сбора данных может формироваться текстовый файл в одном из форматов: json, .csv, .html или передача данных по одному из известных протоколов передачи (syslog, smtp и др.) в базу данных. Перед тем, как сохранить данные в любом из форматов (либо в БД, либо в текстовом файле), происходит парсинг атрибутов объектов MS AD, представляющих собой, например, дескрипторы безопасности (Security Descriptor), представленных в формате SDDL (Security Descriptor Definition Language)-записей. Дескриптор безопасности, в свою очередь, содержит SID владельца, SID основной группы объекта и два списка(ACL) - SACL (системный список управления доступом), DACL (дискреционный список управления доступом). ACL - представляет собой список записей (ACE), который идентифицирует доверенные для управления объекты и определяет права доступа - разрешающие, запрещающие или ау-

дирующие для этих объектов. ACE включает список записей с полями: SID объекта, для которого определяются права доступа, маска доступа, тип ACE, признак наследования прав доступа к объекту.

При сборе данных могут использоваться также систему фильтров, позволяющих собирать только нужный набор данных в зависимости от настроек. Сбор данных осуществляется по планировщику или циклично.

На этапе (102) определяют высокопривилегированные объекты (HVA) MS AD в корпоративной сети на основании правил и парсинга ACL и ACE. Указанные правила представляют собой, например, анализ количества связей HVA объекта с другими объектами MS AD (например, связь с пятью и более объектами). HVA также могут быть технические или сервисные учетные записи с большим количеством связей или расширенными привилегиями доступа.

В зависимости от объекта контроллера домена и выделенных HVA, сбор данных происходит поэтапно для каждого класса объектов. Например, изменения по HVA собираются в первую очередь, и информация по связанным с ним объектам обновляется тоже в первую очередь и в максимально короткое время. Сбор ведется с использованием многопоточных технологий, что в свою очередь позволяет обеспечить максимально быстрое получение данных и обновлений по этим данным. Сбор осуществляется в рамках специального LDAP - подключения между модулем сбора данных и контроллером домена. Подключение защищенно дополнительными организационными методами защиты информации (жесткие правила межсетевого экрана, специфические разрешения устройств защиты (УЗ) и так далее), а также средствами мониторинга. Передача данных осуществляется с использованием SSL для протокола LDAP.

После сбора данных объектов MS AD на этапе (103) определяются объекты, связанные с HVA, которые могут при условии использования текущих привилегий доступа, или их изменения, либо с помощью горизонтального продвижения по сети, получить доступ над HVA. В табл. 1 ниже приведены несколько примеров такого рода привилегий доступа.

Таблица 1

Примеры привилегий доступа

Привилегия	Возможные действия
GenericAll	Полные права на объект (добавление пользователей в группу или сброс пароля пользователя)
GenericWrite	Обновление атрибутов объекта (т.е. скрипт входа в систему)
WriteOwner	Изменение владельца объекта на контролируемого злоумышленником пользователя, который возьмет на себя объект
WriteDACL	Изменение ACE объекта и предоставление полного контроля над объектом
AllExtendedRights	Возможность добавить пользователя в группу или сбросить пароль
ForceChangePassword	Возможность изменить пароль пользователя

Выявление всех объектов MS AD, связанных с HVA, необходимо для анализа связей в целях последующего построения графа на этапе (104) для поиска коротких маршрутов до HVA. На формируемом графе узлами являются объекты MS AD, а ребрами - параметры доступа между объектами MS AD.

В качестве узла графа может выступать: групповая политика, компьютер, пользователь, структура дерева OU или группа. В качестве связей (ребер) выступают параметры доступа, в частности, привилегии одного объекта над другим, пользовательские сессии, членство в группах, доступ с уровнем локального администратора, и т.п. Например, примером связи будут являться следующие сущности: объект является членом группы, пользователь имеет административные привилегии на компьютере, на объект распространяется групповая политика, активная сессия пользователя на компьютере и другие типы сущностей. На фиг. 2 представлен пример графа (200), сформированного на этапе (104), отображающего текущие связи между объектами MS AD. На этапе (105) выполняется автоматизированное моделирование пути атаки на HVA на основе полученного графа на этапе (104). В ходе моделирования путей атак определяется подграф (300), представленный на фиг. 3. На подграфе (300) определяют узлы, позволяющие получить управление над HVA или связанными с ним объектами MS AD с помощью по меньшей мере одного из: передачи текущих прав доступа, изменения текущих прав доступа, добавления новых прав доступа, или использования текущих прав доступа.

Под терминами "граф" и "подграф" стоит понимать моделирование отображение объектов MS AD, по которым выполняется автоматизированная обработка сведений с помощью автоматизированного аналитического алгоритма, направленного на мониторинг состояния доменных зон корпоративной сети и реагирование на изменения в ее объектах.

Как показано на примере на фиг. 3 группа пользователей USER-ADM и все ее члены (участники)

имеет привилегии ForceChangePassword (есть возможность смены пароля без запроса старого) над пользователем Exchange Admin. Пользователь Exchange Admin имеет привилегии GenericAll (эта привилегия позволяет выполнять любые действия, например, добавлять новых пользователей в эту группу) над группой ADMSYSTEMS. Группа ADMSYSTEMS имеет привилегии WriteDacl (привилегия, позволяющая изменить ACL объекта Domain Admins, например, добавить полные права (GenericAll) над группой Domain Admins) над группой администраторов домена - Domain Admins, который является в данном случае HVA.

Таким образом, злоумышленник, скомпрометировав учетную запись, например - Пользователя 1, может получить привилегии администратора домена, став членом группы Domain Admins. Вектор атаки может быть такой: Пользователь 1 является членом группы User-ADM. Пользователь 1 меняет пароль пользователю Exchange Admin, используя УЗ этого пользователя добавляет свою УЗ Пользователь 1 в группу ADMSYSTEMS, затем для группы ADMSYSTEMS дает полные привилегии на Domain Admins и делает свою УЗ Пользователь 1 членом группы Domain Admins.

При анализе объектов MS AD, определенных на подграфе (300), выделяется стартовый узел или группа объектов, от которых будет строиться путь атаки. Стартовым узлом может выступать любой объект, либо группа объектов, по умолчанию не обладающих критичными привилегиями, но имеющими возможность расширить свои права, либо объекты, исходно имеющие критичные права, влияющие на доступ к HVA. Например, некоторые объекты могут иметь разрешение "WriteDACL", которое позволяет изменить запись контроля доступа (ACE) объекта и дать злоумышленнику полный контроль над объектом - фактически получить привилегии "GenericAll" над целевым объектом. При моделировании вектора атаки будет предполагаться, что стартовым узлом будет хост или УЗ скомпрометированная злоумышленником.

Пути атак (вектора) могут строиться в противоположном направлении - от HVA до объектов с критичными привилегиями или другими связями, позволяющими расширить привилегии горизонтально. При построении путей всех возможных атак на HVA для объектов учитываются наследования и приоритет записей контроля доступа (ACE) в следующем порядке:

Явный запрет;

Явное разрешение;

Унаследованный запрет;

Унаследованное разрешение.

Таким образом, если объект будет иметь две конфликтующие записи контроля доступа (ACE) на явное разрешение и явный запрет (например, пользователь входит в две группы, у одной из которых есть разрешение на доступ к папке, а у второй явный запрет, то сработает запрет и пользователю будет отказано в доступе), то приоритет будет у второго, так как запрещающие правила всегда имеют приоритет над разрешающими. На этапе (105) выполняется в режиме реального времени анализ графового отображения структуры MS AD. Анализ может выполняться с помощью специального автоматизированного модуля аналитики, который обеспечивает выполнение мониторинга текущего состояния прав доступа объектов MS AD и реагирует на изменения полномочий относительно HVA. При анализе состояния прав доступа в MS AD производится оценка угроз информационной безопасности в режиме реального времени для своевременного реагирования и сигнализации об изменениях относительно трендов безопасности. Примером резкого изменением тренда безопасности может быть добавление нового пользователя в группу администраторы домена, предоставление прав на управление каким-либо HVA и др.

Анализ изменений привилегий доступа на формируемых подграфах (300) позволяет генерировать уведомления и выполнять автоматизированное реагирование по заданным правилам, разработанным с помощью логических операторов, объектов, атрибутов и их значений. Такая проверка итеративно осуществляется на этапе (106) для всех формируемых подграфов (300) общего графа MS AD (200). При определении объектов MS AD, для которых на подграфе (300) происходит изменение привилегий их доступа и которые могут получить доступ над HVA, выполняется применение одной из выбранных политик реагирования на этапе (107), в частности, информация по такого рода узлам (объектам) передается в систему контроля для последующего реагирования. С помощью системы контроля выполняется управление привилегиями доступа на выявленных объектах MS AD в части их изолирования от других объектов MS AD и/или понижения их привилегий доступа. Данная реакция системы контроля выполняется на основании установленных правил и политик безопасности в части реагирование на конкретный тип изменения привилегий доступа на объектах MS AD.

Одним из частных примеров правил реагирования на объекты MS AD могут быть следующие ситуации:

Если после обновления информации у какого-либо объекта появляются привилегии "DS-Replication-Get-Changes"/"DS-Replication-Get-Changes-All"(DCSync), то в качестве реакции системы контроля происходит понижение привилегий объекта до исходного значения. Система информирует об устраненной угрозе;

Если в группе администраторов появляется новая учетная запись и данная учетная запись не добавлена в соответствующий лист значений, то в качестве реакции системы происходит ее удаление из груп-

пы, таким образом понижаются привилегии учетной записи до исходных. Команды по удалению исполняются от привилегированных учетных записей, в качестве переменных передаются учетные записи и имена групп. Система информирует об устраненной угрозе.

Также заявленное решение может дополнительно осуществлять выявление ошибок в конфигурации безопасности MS AD, на основании правил проверки ошибок в конфигурации объектов MS AD. Для этого реализуется проверка пользователей на наличие определенных привилегий в токенах доступа (Access Tokens), которые позволяют ему выполнять действия в обход ACL объектов. Данная проверка может также выполняться с помощью автоматизированного модуля, обеспечивающего функционал по осуществлению поиска типовых ошибок конфигурации в контроллере домена. Анализ ошибок конфигурации выполняется с помощью механизма проверки (чекер) для верификации известных уязвимостей контроллера домена.

Одним из вариантов проверки привилегий в токенах доступа является выполнение команды "whoami /priv" в командной оболочке, парсинг и анализ полученных результатов, при анализе учитывается наименование привилегии в токене доступа и статус (включена/отключена).

Ниже в табл. 2 приведены некоторые примеры привилегий в токенах доступа, выявляемых в ходе выявления ошибок конфигурации.

Таблица 2

Примеры привилегий в токенах доступа

Наименование привилегии	**Описание**
SeEnableDelegationPrivilege	Позволяет управлять параметрами Kerberos Unconstrained и Constrained Delegation в домене, которые злоумышленник может использовать для повышения привилегий
SeDebugPrivilege	Позволяют пользователю для любого процесса в ОС Windows выполнить код в рамках отладки, что может привести к повышению привилегий или чтению области резервированной памяти процесса. Примером эксплуатации является чтение секретов процесса lsass УЗ пользователей, авторизованных в системе.
SeImpersonatePrivilege	Любой процесс, обладающий этой привилегией, может олицетворять (но не создавать, имперсонироваться) любой токен, для которого он может получить дескриптор. В некоторых ситуациях можно имперсонироваться в процесс, который принадлежит другой УЗ или создать привилегированный токен от службы Windows (DCOM), заставив ее выполнить аутентификацию NTLM против эксплойта, а затем выполнить процесс как SYSTEM.

В рамках данной проверки ошибок конфигурации выполняется поиск типовых ошибок конфигурации и уязвимостей контроллера домена. Одним из примеров таких ошибок может служить отключенная предварительная аутентификация Kerberos для пользователя (появляется возможность проведения атаки ASREPRoast). Одним из вариантов проверки является выполнение команды "Get-DomainUser -PreauthNotRequired -verbose" через расширение командной оболочки. Результатом выполнения команды является список уязвимых учетных записей.

Другим примером ошибки может выступать наличие доменных пользователей, имеющих права локального администратора на компьютерах (атака на Local Administrator Password Solution (LAPS)). Одним из вариантов проверки является выполнение команды "Get-LAPSComputers" с помощь расширения командной строки PowerShell и библиотеки дополнительных функций и методов LAPSToolkit. Результатом работы команды является список компьютеров с включенным механизмом LAPS. Как правило, разрешение на чтение паролей LAPS назначается на группу пользователей. Для поиска таких групп используется метод "Find-LAPSDelegatedGroups", для поиска членов этих групп(пользователей) используется метод "Get-NetGroupMember -GroupName "group_name"" библиотеки LAPSToolkit.

Еще одним примером типовой ошибки может выступать присутствие доменных пользователей в группах MS AD по умолчанию с повышенными привилегиями, не содержащих никаких пользователей. Например, такими группами являются Account Operators, Backup Operators, Server Operators и другие. Одним из вариантов проверки пользователей этих групп является выполнение команды "Get-DomainGroupMember -Identity "group_name"" с помощью расширения командной строки PowerShell и

библиотеки дополнительных функций и методов PowerView. Результатом работы является список пользователей с расширенными привилегиями.

Заявленное решение может также использовать механизм рекомендаций. Рекомендации представляют собой последовательность системных команд PowerShell на ОС Windows и комментариев. Данный механизм может быть реализован с помощью автоматизированного модуля, который обеспечивает вывод контекстной информации для пользователя с целью их исполнения и компенсирования возникающих рисков безопасности. Рекомендации имеют связи с атрибутами объектов MS AD, таким образом определённый набор значений атрибутов характеризуется рекомендацией для пользователя системы. В частном случае рекомендации могут быть представлены в json формате и выводиться в интерфейс пользователя для определённых объектов/связей. Для удаления разрешений у объекта службы каталогов MS AD PowerShell используется командлет "Remove-ADPermission".

Примером является выполнение следующей команды: Remove-ADPermission -identity "Replication Database"-User "domain/ivanpetrov" -AccessRights "WriteDacl". Синтаксис использования командлета "Remove-ADPermission":

Remove-ADPermission -Identity <ADRawEntryIdParameter> -User <SecurityPrincipalIdParameter> [-AccessRights <ActiveDirectoryRights[]>] [-ChildObjectTypes <ADSchemaObjectIdParameter[]>] [-Deny <SwitchParameter>] [-DomainController <Fqdn>] [-ExtendedRights <ExtendedRightIdParameter[]>] [-InheritanceType <None | All | Descendents SelfAndChildren | Children>] [-InheritedObjectType <ADSchemaObjectIdParameter>] [-Properties <ADSchemaObjectIdParameter[]>]

Remove-ADPermission [-Identity <ADRawEntryIdParameter>] –Instance <ADAcePresentationObject> [-AccessRights <ActiveDirectoryRights[]>] [-ChildObjectTypes <ADSchemaObjectIdParameter[]>] [-Deny <SwitchParameter>] [-DomainController <Fqdn>] [-ExtendedRights <ExtendedRightIdParameter[]>] [-InheritanceType <None | All | Descendents SelfAndChildren | Children>] [-InheritedObjectType <ADSchemaObjectIdParameter>] [-Properties <ADSchemaObjectIdParameter[]>] [-User <SecurityPrincipalIdParameter>]

Remove-ADPermission -Identity <ADRawEntryIdParameter> [-DomainController <Fqdn>]

Дополнительно может использоваться также генератор отчетности, выполненный в виде автоматизированного модуля, который реализует функционал формирование отчетов. Входными данными для модуля отчетности являются объекты и их атрибуты из БД. Результатом формирования отчетности является текстовый файл в одном из форматов: pdf, html, xlsx. Одним из частных примеров отчета может быть статистический отчет с элементами аналитики, содержащий информацию по следующим объектам:

Общее количество администраторов. Изменения в количестве за определенный промежуток времени;

Наименование групп администраторов и количество участников в каждой из групп. Также возможно включить необходимые группы, если они являются высокопривилегированными активами;

Список пользователей без предварительной аутентификации (ASREPRoast);

Список объектов с ограниченным делегированием.

Инфраструктура практически всех компаний включает домены, построенные на базе MS AD. Заявленное решение позволяет достичь вышеуказанный технический результат за счет постоянного мониторинга разрешений объектов службы каталогов и ошибок конфигурации MS AD, что значительно повышает эффективность обеспечения безопасности для предотвращения компрометации объектов сети. Злоумышленник, попадая в сеть и предпринимая попытки горизонтального продвижения и повышения привилегий с целью компрометации HVA, вынужден изменять разрешения объектов, либо использовать ошибки в конфигурации службы каталогов. Постоянный мониторинг разрешений объектов позволяет оперативно выявлять такие попытки и незамедлительно реагировать на них, изолируя злоумышленника от дальнейшего продвижения, а в некоторых случаях отключая его от сети. Преимуществом настоящего решения является анализ ACL и ACE объектов сети, а также ошибок конфигурации MS AD. Другие решения не предполагают такого рода функционал, что приводит к тому, что такого рода системы безопасности не в состоянии замечать и реагировать на такие инциденты.

На фиг. 4 представлен общий вид вычислительной системы, реализованной на базе вычислительного устройства (300). В общем случае, вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305), и устройство для сетевого взаимодействия (306).

Процессор (301) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором также необходимо учитывать графический процессор, например, GPU NVIDIA или ATI, который также является пригодным для полного или частичного выполнения способа (100). При этом средством памяти может выступать доступный объем памяти графической карты или графического процессора. ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машино-

читаемых инструкций для выполнения необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с вычислительным устройством (300) применяются различные средства (305) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например, GPS, ГЛОНАСС, BeiDou, Galileo.

Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ предотвращения компрометации объектов службы каталогов (MS AD) в корпоративной сети, выполняемый с помощью вычислительного устройства и содержащий этапы, на которых:

получают данные из хранилища MS AD корпоративной сети, характеризующие объекты сети и их атрибуты, включающие в себя по меньшей мере дескриптор безопасности, содержащий списки (ACL) и записи (ACE) контроля доступа объектов;

выполняют парсинг атрибутов объектов MS AD;

определяют высокопривилегированные объекты (HVA) MS AD в корпоративной сети на основании правил и парсинга ACL и ACE, причем правила представляют собой по меньшей мере количество связей HVA объекта с другими объектами MS AD;

определяют объекты MS AD, связанные с HVA, которые позволяют получить к ним доступ посредством текущих привилегий доступа, или их изменения или посредством горизонтального продвижения по сети;

формируют граф на основе собранных данных, где узлами являются объекты MS AD, а ребрами - параметры доступа между объектами MS AD;

выполняют моделирование пути атаки на HVA на основе полученного графа, на котором определяют по меньшей мере один подграф с объектами MS AD, содержащий узлы, позволяющие получить управление над HVA или связанными с ним объектами MS AD с помощью по меньшей мере одного из: передачи текущих прав доступа, изменения текущих прав доступа, добавления новых прав доступа или использования текущих прав доступа;

осуществляют мониторинг объектов MS AD для определения изменений параметров привилегий доступа на узлах, выявленных на подграфе;

передают данные по выявленным на подграфе объектам в систему контроля при изменении их привилегий доступа;

выполняют управление привилегиями доступа на выявленных объектах MS AD в части их изолирования от других объектов MS AD и/или понижения их привилегий доступа.

2. Способ по п.1, в котором параметры доступа между объектами представляют собой по меньшей мере одно из: связи привилегий между объектами, на которые эти привилегии распространяются, разрешения между объектами, параметры доверия между доменами.

3. Способ по п.1, в котором привилегии объектов службы каталогов представляют собой токены доступа с ассоциированными привилегиями пользователя.

4. Способ по п.3, в котором привилегии токена доступа являются способом изменения уровня дос-

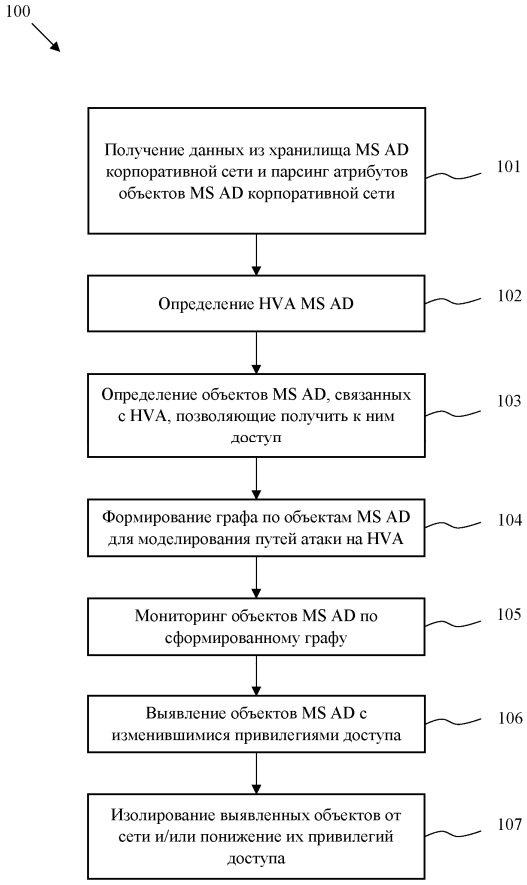
тупа к объекту службы каталогов корпоративной сети.

5. Способ по п.1, в котором каждый объект сети представляет собой по меньшей мере одно из: пользователи, компьютеры, группы безопасности, групповые политики (Group Policy Object), организационные подразделения (Organizational Unit), доверительные отношения между доменами.

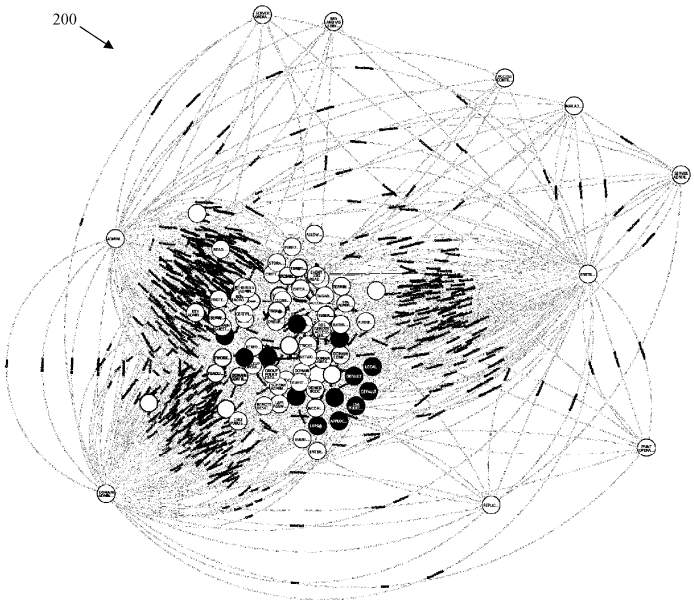
6. Способ по п.1, в котором на выявленном подграфе осуществляют мониторинг ошибок в конфигурации безопасности MS AD, на основании правил проверки ошибок в конфигурации объектов MS AD.

7. Способ по п.6, в котором осуществляют корректировку конфигураций привилегий доступа на объектах MS AD.

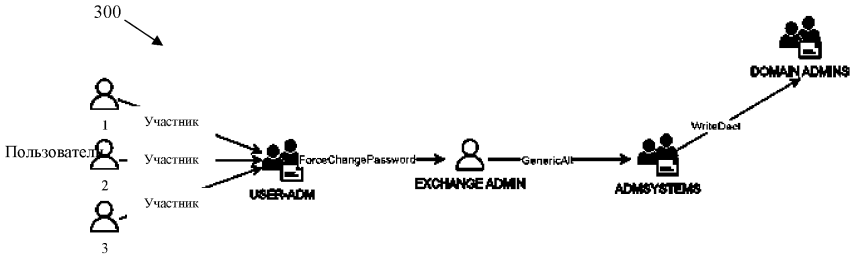
8. Система предотвращения компрометации объектов службы каталогов (MS AD) в корпоративной сети, содержащая по меньшей мере один процессор и память, хранящую машиночитаемые инструкции, которые при их выполнении процессором реализуют способ по любому из пп.1-7.



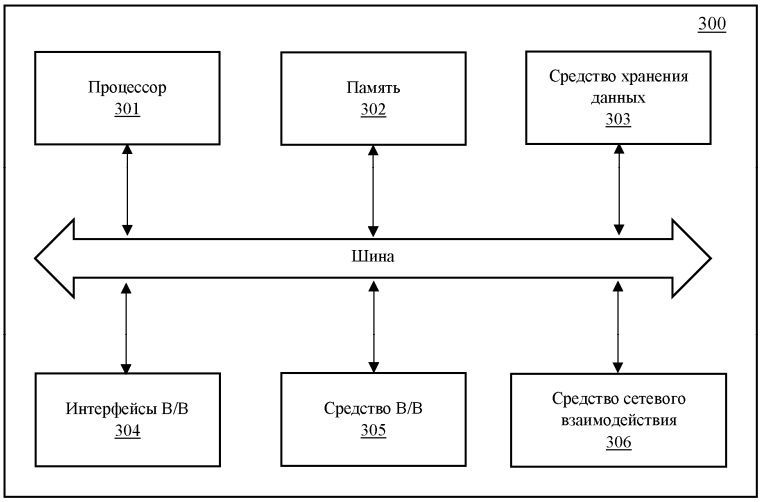
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4