ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

Видункина Карина Борисовна

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ И МЕР ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СИСТЕМ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА LDAP

Выпускная квалификационная работа
по специальности 10.05.01 «Компьютерная безопасность»
студента образовательной программы специалитета
«Компьютерная безопасность»

Студент

_____ Видункина К.Б.
подпись И.О. Фамилия

Руководитель
приглашенный преподаватель

_____ Шубин М.А.
подпись И.О. Фамилия

Рецензент
Руководитель информационной безопасности ООО «Платиус»

Булкин В.А.
И.О. Фамилия

Соруководитель
к.т.н., доцент

Кабанов А.С.
И.О. Фамилия

Москва 2020

Аннотация

В рамках данной выпускной квалификационной работы рассматривается протокол LDAP, структура LDAP-каталога и Active Directory в качестве примера системы, построенной с использованием LDAP. Исследованы существующие уязвимости и атаки на протокол LDAP и Active Directory в частности, предложены меры защиты для актуальных угроз, включая написанный скрипт на языке программирования Python. Полученные рекомендации для защиты системы, построенной с использованием LDAP, могут быть использованы как и при разворачивании новой информационной системы, так и для применения к уже эксплуатируемой в целях повышения существующего уровня защищённости системы.

Abstract

The object of the research is LDAP, LDAP directory and Active Directory as an example of a system built using LDAP. The existing vulnerabilities and attacks on LDAP and Active Directory protocol are investigated, in particular, protection measures for actual threats are offered. Devised protection method is script in Python language. The received recommendations for protection of the system constructed with use LDAP, can be used both at opening of new information system, and for application to already operated for increase of existing level of protection.

Оглавление

Список используемых обозначений

Авторизация — предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ

Антивирусное ПО — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом

Атака — это совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех свойств информации — доступности, целостности или конфиденциальности

Аутентификация — действия по проверке подлинности субъекта доступа в информационной системе

База данных — совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных

Дамп — снятие информации о состоянии компьютерной системы

Данные — это информация, представленная в виде, позволяющем запоминать, хранить, передавать или обрабатывать её с помощью технических средств

Доступность — состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно

Злоумышленник (нарушитель, атакующий) — это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов

или ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства

Идентификация — действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов

Информационная база каталога (DIB) — информация, содержащаяся в каталоге

Информационное дерево каталога (DIT) — полученная в результате представления данных древовидная структура

Информация — сведения независимо от формы их представления

Каталог — то "ряд открытых систем, взаимодействующих друг с другом для предоставления сервисов каталога"; в общем случае некий список информации об объектах, составленный с целью облегчения поиска этих объектов по какому-то признаку

Конфиденциальность — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

Межсетевой экран — это локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС

Модель угроз — физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации

Парольная политика — набор правил, направленных на повышение безопасности компьютера путем использования надежных паролей и их правильного использования

Политика безопасности организации — совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности

Служба каталогов — средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах

Схема данных — это совокупность определений и ограничений, касающихся структуры DIT, возможных способов именования записей, информации, которая может содержаться в записи, атрибутов, используемых для представления этой информации, и их организации в иерархии для упрощения поиска и извлечения информации, а также способов, по которым значения атрибутов могут быть сопоставлены в утверждениях значений атрибута и в утверждениях правил соответствия

Уязвимость — недостатка в системе, используя который, можно нарушить её целостность, конфиденциальность и доступность

Хеширование — преобразование, производимое хеш-функцией

Целостность — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

IDS (Intrusion Detection System) — система обнаружения вторжений

IPS (Intrusion Prevention System) — система предотвращения вторжений

KDC (key distribution center) — центр выдачи ключей в протоколе Kerberos

LDAP (Lightweight Directory Access Protocol) — протокол прикладного уровня для доступа к службе каталогов X.500

LDAP-браузер — программное обеспечение, позволяющее осуществить простой доступ к LDAP-каталогу

LDIF (LDAP Data Interchange Format) — формат представления записей службы каталогов или их изменений в текстовой форме

SASL(Simple Authentication and Security Layer) — метод для добавления поддержки аутентификации в протоколы соединения

SIEM (security information and event management) — технология, обеспечивающая анализ событий безопасности в реальном времени и позволяющая реагировать на них до наступления существенного ущерба

SPN (service principal name)— имя службы в Active Directory

SSO (Single Sign-On) — это механизм, позволяющий пользователю пройти аутентификацию единовременно и получить доступ к различным программным продуктам, используя один идентификатор

TLS (transport layer security) — протокол защиты транспортного уровня

X.500 — серия стандартов ITU-T (International Telecommunication Union) для службы распределенного каталога сети

Введение

Актуальность работы

С каждым днем IT-индустрия становится все больше и больше, но даже в больших компаниях, не имеющих отношение к данной сфере, заметна тенденция к повышению интереса в области информационной безопасности и удобству администрирования, связанного с управлением доступом. Одним из распространённых и наиболее предпочтительных способов контроля доступа является заведение учетных записей в домен и представления ресурсов компании в виде древовидной структуры. Представление ресурсов компании в виде древовидной структуры называется службой каталогов, а протоколом доступа к этой службе является протокол LDAP. Наиболее популярной службой каталогов на данный момент является Active Directory, разработанная Microsoft в 1999 году для операционных систем семейства Windows Server. Данная служба каталогов позволяет применять групповые политики на все множество устройств и учетных записей компании, которые, в свою очередь, помогут администратору обеспечить настройку рабочей среды пользователя, своевременную установку обновлений операционной системы и многое другое. Помимо Active Directory, существуют также решения: OpenLDAP, RedHat Directory Server, Apple Open Directory, Apache Directory Server, Oracle Directory Server, IBM Domino LDAP.

В связи с популярностью Active Directory на рынке и отсутствию сильных конкурентов злоумышленники в постоянном поиске уязвимостей именно данной службы каталогов. В последнее время ни одна конференция, посвящённая информационной безопасности, не обходится без докладов на данную тему. Несмотря на то что операционные системы Windows становятся все безопаснее от обновления к обновлению, тема уязвимостей протокола LDAP и LDAP-каталога Active Directory остается актуальной.

Цель и задачи работы

Целью данной работы является исследование непосредственно самого протокола LDAP, его принцип работы, уязвимости, а также будет рассмотрена конкретная реализация — Active Directory, известные атаки на эту службу каталогов и возможные меры защиты по их предотвращению.

Для реализации поставленной цели выпускной квалификационной работы были поставлены следующие задачи:

- изучение теоретических основ протокола LDAP;
- исследование известных уязвимостей протокола:
- изучение службы каталогов Active Directory;
- изучение известных атак на службу каталогов;
- изучение известных мер защиты и предложение своего метода.

Глава 1. Теоретические сведения

Протокол LDAP – это легковесный протокол доступа к каталогам, которые организованы в соответствии со стандартом X.500, он определяет методы, с помощью которых будет осуществляться доступ к данным и не определяет, как именно эти данные будут храниться. Описать протокол можно с помощью четырёх моделей: информационная, функциональная, именования и безопасности[6].

Информационная модель описывает, каким образом информация представлена в LDAP-каталоге. Данные представлены в виде иерархии объектов, где каждый объект называется записью. Верхнюю часть информационного дерева называют базой (base), корнем (root) или суффиксом (suffix). Ниже представлен список характеристик, применимый к любой записи.

- У каждой записи должна обязательно присутствовать родительская запись и могут быть дочерние;
- Каждая запись является экземпляром как минимум одного объектного класса (objectClass), который содержит атрибуты, содержащие данные;
- Каждая дочерняя запись является братской по отношению к другим дочерним записям своей родительской записи;
- Каждая запись будет уникально идентифицироваться в DIT данными, которые содержатся в атрибутах ее объектного класса, относительно своей родительской записи.
- Новую запись можно добавить с помощью специальных LDIF файлов, LDAP-браузера, web- или другого программного интерфейса.

Стоит также подробнее остановиться на характеристиках, которые справедливы для любого объектного класса.

- Объектный класс можно назвать «контейнером» для атрибутов;
- Объектный класс должен определять обязательность атрибутов в нем;

- Объектный класс должен быть структурным, абстрактным или вспомогательным;
- От абстрактного объектного класса наследуются определения других объектных классов;
- Запись не может принадлежать абстрактному классу напрямую;
- Абстрактный класс может быть унаследован только от другого абстрактного класса;
- Если объектный класс является частью иерархии, то он наследует все характеристики всех своих родительских объектных классов;
- Объектный класс имеет уникальное имя и идентификатор;
- Структурный объектный класс записи не должен изменяться.

Ниже представлены характеристики, которые должны выполняться для любого атрибута.

- Каждый атрибут является членом одного или нескольких объектных классов;
- Атрибут может быть необязательным или обязательным объектного класса, членом которого он является;
- Атрибут может быть необязательным в одном объектном классе и обязательным в другом;
- Каждый атрибут определяет тип данных, которые он может содержать;
- Атрибут может быть частью иерархии, в этом случае дочерний атрибут наследует все характеристики родительского атрибута;
- Атрибут может иметь больше одного значения;
- Если у атрибута есть возможность иметь больше одного значения, то тогда он может появляться в записи несколько раз с разными значениями данных;
- Данные, содержащиеся в каком-то из атрибутов, могут использоваться для однозначной идентификации записи на всех уровнях иерархии. Это

может быть любой атрибут в записи или комбинация двух или более атрибутов.

- Объектный класс тоже является атрибутом.
- Для использования атрибута в записи необходимо включить в определение это записи его объектный класс, а этот объектный класс необходимо включить в набор схемы данных.

В каждом каталоге обязательно должны присутствовать схемы данных, которые находятся в специальных LDIF файлах. С помощью LDIF файлов также можно делать резервные копии данных или экспортировать их для других целей.

Модель именования позволяет задать систему, благодаря которой можно уникально идентифицировать каждый объект, что является одним из условий успешного манипулирования записями. Для этого используется механизм отличительных имен. Отличительное имя однозначно определяет положение объекта в DIT, представляя информацию о всех узлах дерева, которые необходимо пройти, чтобы добраться от самого объекта до корня DIT. Данных механизм схож с полным путем расположения файла в файловой системе. Помимо отличительного имени у записи есть и относительные уникальные имена, которые уникальны относительно родительской записи.

Функциональная модель представляет собой описание операций, которые определены в протоколе. Определены следующие операции: bind, unbind, search, modify, modifyDN, delete, add, compare, abandon, extended, startTLS. Далее будет разбираться функция каждой из них подробнее. Обмен операциями происходит на уровне сообщений протокола LDAP, которые инкапсулируются в общий конверт LDAPMessage, назначение которого — предоставление общих полей, требуемых во всех сообщениях протокола, одно из таких — MessageID.

Функция операции bind заключается в аутентификации клиента на LDAP-сервере, установке идентификатора авторизации, который будет использоваться при следующих операциях по этому соединению и оповещении о версии протокола LDAP на стороне клиента. Аутентификация состоит из информации, которая содержит данные о идентифицируемом, например, DN, и предоставления доказательства данной идентичности, например, пароль. Операция bind позволяет использовать разные виды аутентификации, которые будет подробнее описаны в модели безопасности.

Операция unbind используется для завершения сессии LDAP, клиент посылает серверу запрос на закрытие соединения, сервер, в свою очередь, закрывает его. Данную операцию не стоит рассматривать как противоположную к bind, она не переводит соединение в неаутентифицированное состояние.

Функция операции search – возвращение соответствующего критериям поиска набора записей с сервера. Ответом сервера будет либо нуль и более сообщений с результатом, либо переадресация на другой LDAP-сервер, где можно повторить запрос.

Операция modify используется клиентом, если необходимо, чтобы сервер изменить какую-либо запись от имени клиента. В ответ клиент получается сообщение об успешности или с причиной неуспеха изменения. Данная операция не может использоваться для удаления из записи уникальных значений, то есть которые используются для формирования уникального имени записи.

Операция add позволяет добавлять запись в каталог. Для успешного завершения операции необходимо, чтобы добавляемая запись еще не существовала.

С помощью операции delete можно удалить запись из каталога, кроме тех, у которых есть дочерние записи.

Операция modifyDN дает возможность изменить относительное уникальное имя записи в каталоге и/или переместить поддерево записей в новое местоположение в дереве в пределах одного сервера.

Функция операции compare – сравнение значения утверждения со значениями конкретного атрибута конкретной записи в каталоге.

Операция abandom позволяет клиенту отправить серверу запрос на отказ от выполнения незавершенной операции. Нельзя отказаться от выполнения abandon, bind, unbind и startTLS. В запросе серверу отправляется MessageID операции, выполнение которой необходимо прекратить.

С помощью extended можно определить дополнительные операции.

Функция startTLS — инициирование установки соединение уровня TLS. После отправки такого запроса клиент не должен посылать другие запросы до получения ответа от сервера о возможности вести переговоры TLS. При закрытии соединения TLS сторона-инициатор разрыва должна дождаться ответа от второй стороны, прежде, чем посылать следующие запросы. Подробнее о TLS будет рассматриваться в модели безопасности.

Модель безопасности LDAP описывает предоставляемые механизмы защиты протокола. Предлагаются следующие меры защиты: различные методы аутентификации, обеспечение целостности и конфиденциальности данных с помощью TLS и SASL, настройка по ограничению использования ресурсов сервера.

При взаимодействии клиента и сервера предлагаются следующие методы аутентификации: анонимная аутентификация, аутентификация без проверки подлинности, аутентификация по логину и паролю и SASL.

При анонимной аутентификации отправляется bind с полями DN и пароль нулевой длины и способом аутентификации simple.

При аутентификации без проверки подлинности bind отправляется поле пароля нулевой длины и DN ненулевой, механизм аутентификации, как и в

предыдущем варианте — simple. Данный метод небезопасен в случае отсутствия защиты конфиденциальности данных при передаче по незащищённым сетям.

При аутентификации по логину и паролю, поля DN и пароль отправляются ненулевой длины, механизм — simple. Этот метод имеет аналогичные с предыдущим проблемы в безопасности.

При использовании последнего метода аутентификации, ее проведение и установка авторизационной идентификационной сущности происходят с помощью защищенных удостоверяющих данные, обмен которыми произошел на более низком уровне обеспечения безопасности, если такой обмен не произошел, то сессия будет в анонимом состоянии. Данный метод является более безопасным, чем предыдущие два, так как в случае с SAML EXTRENAL пароль передается серверу в зашифрованном виде, но, тем не менее, без механизмом обеспечения целостности данных, злоумышленник может модифицировать передаваемые по сети ответы сервера со значениями атрибута 'supportedSASLMechanisms', и таким образом понизить качество доступных в списке механизмов SASL, включив в него только наименее безопасные механизмы.

С помощью SASL можно осуществлять аутентификацию через протокол Kerberos, предлагающий клиенту и серверу перед обменом информацией провести взаимную аутентификацию, учитывая тот факт, что начальный обмен может происходить в незащищённой среде. При реализации механизма взаимной аутентификации, помимо сервера и клиента, в процессе участвует центр распределения ключей (KDC). Принцип работы Kerberos заключается в следующем:

- Если клиенту необходимо обратиться к серверу, то сначала посылается запрос в KDC;
- Из KDC выдается сеансовый ключ клиента, зашифрованный клиентским долговременным ключом, и сеансовый ключ сервера,

объединённый с информацией о клиенте в блок данных и зашифрованный долговременным ключом сервера. Блок данных, содержащий сеансовый ключ сервера и информацию о клиенте, называется «session ticket»;

- Клиент помещает полученные «session ticket» и свою копию сеансового ключа в свою операционную память;
- При необходимости связаться с сервером клиентом посылается «session ticket» и зашифрованный в помощью сеансового ключа аутентификатор. «Session ticket» и аутентификатор составляют удостоверение клиента;
- Из полученного удостоверения сервер сначала расшифровывает «session ticket» с помощью своего секретного ключа, извлекает из него сеансовый ключ и дешифрует аутентификатор клиента;
- По требованию взаимной аутентификации клиентом, сервер с помощью своего сеансового ключа шифрует метку о времени из аутентификатора клиента и посылает в качестве аутентификатора

«Session ticket» может многократно использоваться. К достоинствам данного механизма относится еще тот факт, что сервер не хранит сеансовые ключи для связи с клиентами, также у клиента отпадает необходимость обращаться в KDC каждый раз перед связью с сервером. Для «session ticket» можно указать время жизни.

Протокол TLS используется в LDAP для обеспечения конфиденциальности и целостности данных, а также для предоставления данных для аутентификации. Использование TLS в LDAP возможно только при использовании SASL EXTERNAL аутентификации. Переговоры TLS идут следующим образом:

- Сервер запрашивает у клиента предоставление сертификата пользователя;

- В случае отсутствия сертификата у пользователя, сервер может использовать локальную политику безопасности и принять решение об успешности завершения переговоров TLS;
- В случае предоставления клиентом подходящего сертификата, выполняется операция bind с SASL EXTERNAL. Информация из этоо сертификата может использоваться сервером для идентификации и аутентификации клиента;
- Клиент со своей стороны тоже проводит проверку идентификационной сущности сервера, например, DNS-имя или IP-адрес;
- В случае, когда клиент не получил совпадений при проверке идентификационной сущности сервера, он либо уведомляет об этом пользователя, либо закрывает соединение и помещает в журнал событий сообщение об ошибке;
- После завершения переговоров TLS обе стороны должны удостовериться, что предоставляемые принятым в ходе переговоров набором шифров сервисы обеспечения безопасности достаточны для предполагаемого использования данной сессии LDAP. Если это не так, уровень TLS должен быть закрыт;
- После завершения переговоров TLS и установке соединения, клиенту следует отбросить или обновить всю информацию о сервере, полученную до инициации переговоров TLS. После установления уровня TLS сервер может опубликовать возможности, отличные от тех, что были опубликованы до этого.

Уровень безопасности, обеспечиваемый использованием TLS зависит не только от качества реализации TLS, но и от методов использования этой реализации.

1.1. Служба каталогов. Active Directory

Службой каталогов называется сетевой сервис, который предоставляет средства для централизованного управления всеми компонентами сетевой

инфраструктуры, должна состоять из базы данных с выше упомянутыми компонентами и механизма для доступа к ней. Под средствами для централизованного управления стоит, в первую очередь, понимать такие функции как создание, удаление учетных записей пользователей и настройка их прав доступа, предоставление общего доступа к ресурсам и распространение сетевых политик для отдельных объектов или групп объектов.

Самой популярной в мире реализацией службы каталогов является Active Directory от Microsoft. Согласно опросам ISDecisions[16], 80% специалистов по информационным технологиям согласились, что AD является лучшим решением для администрирования пользователей в локальной сети, и 83,9%, что их пользовательские политики доступа эффективно работают, тем не менее, почти половина из опрошенных признают, что в AD есть лазейки для нарушения режимов безопасности, 83% находится в постоянном поиске новых мер защиты.

LDAP-сервер в случае Active Directory называется контроллер домена. Объекты представлены в соответствии с информационной моделью LDAP каталога, за исключением добавления некоторых дополнительных терминов, связанных с тем, что AD, в первую очередь, используется в организациях для единой регистрации в сети:

- Домен — группа компьютеров, которые используют один и тот же каталог;
- Дерево доменов— иерархия доменов с единым корнем;
- Лес доменов — множество деревьев с различными степенями доверия между друг другом, которые используют одни и те же схемы данных.

В рассматриваемой службе каталогов также используется разобранные ранее модель именования, модель безопасности и функциональная модель. В модели безопасности добавляется еще один метод аутентификации,

разработанный специально для Windows — NTLM. При использовании этого метода, пароль клиента не передается в открытом виде.

Несмотря на то, что Active Directory является разработкой Microsoft, служба обеспечивает взаимодействие с UNIX-подобными системами через LDAP-клиенты, хотя и есть Windows-ассоциированные атрибуты, которые не будут восприниматься данными системами.

Active Directory является самой популярной реализацией LDAP-сервера, но не единственной. Существуют и свободно распространяемые решения: OpenLDAP, Samba4 LDAP (взаимодействует с AD), Apache Directory Server, 389 Directory Server. В рамках данной работы в качестве системы, построенной с использованием LDAP, будет рассматриваться именно Active Directory.

Глава 2. Уязвимости LDAP и систем построенных с его использованием, известные атаки на них

При рассмотрении модели безопасности в предыдущей главе, уже затрагивались вопросы о нарушении конфиденциальности данных, которые передаются по незащищенным сетям. В случае, когда нарушитель имеет доступ к сети, он может перехватить трафик с логином и паролем, отсортировав трафик по протоколу LDAP. Уязвимость эксплуатируется с помощью программного обеспечения для захвата траффика, в примере использовалась программа WireShark. Использование данной уязвимости продемонстрировано на рисунках 1 и 2.

Рисунок 1. Скриншот запроса из Wireshark

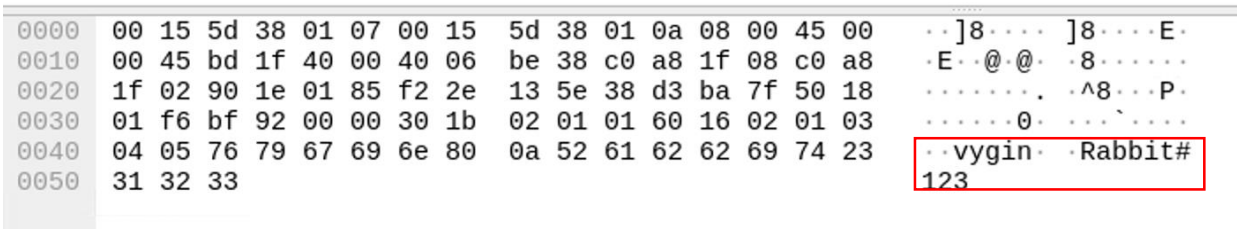

Рисунок 2. Скриншот части тела запроса из Wireshark

Как можно видеть на рисунке 1 клиентом отправляется запрос bind с методом simple, что было описано в функциональной модели в главе 1. На рисунке 2 можно заметить, что после логина «vygin» следует пароль «Rabbit#123» в незашифрованном виде. Полученную информацию можно использовать для дальнейшего захвата LDAP-сервера. В случае аутентификации только по логину без проверки перехваченную информацию можно будет использовать для атаки Brute Force при переборе паролей. Стоит отметить, что Active Directory не дает возможность эксплуатировать

данную уязвимость в таком виде, так как там используется протокол сетевой аутентификации NTLM, который, как уже было сказано ранее, передает пароль в зашифрованном виде.

Архитектурная особенность протокола NTLM заключается в том, что хеш пароля пользователя хранится в памяти самого компьютера, который оттуда можно извлечь, также данный хеш можно перехватить тем же программным обеспечением, что и в прошлом примере. Таким образом, это даёт возможность злоумышленнику использоваться полученный хеш для авторизации, что приводит к атаке Pass-the-Hash. Из захваченного хеша также можно получить пароль в открытом виде с помощью hashcat. Инструмент mimikatz был специально разработан для снятия дампа аутентификационных данных из памяти компьютера в открытом виде. С помощью полученных данных вышеописанными способами удаленное выполнение команд можно реализовать с помощью PsExec.

После получения учетных данных одного пользователя появляется для эксплуатации еще одной уязвимости для пользователей, который находятся в одном домене. Злоумышленнику с доступом к компьютеру, который введён в домен Active Directory, и с помощью ранее полученных учетных данных достаточно в cmd.exe ввести команду «net user /domain», которая, в свою очередь, выведет список всех пользователей домена. Полученную информацию можно использовать далее в атаке Brute Force при подборе паролей.

Непосредственно LDAP-сервер может быть подвержен атаке типа «отказ в обслуживании» с помощью некорректных LDAP-запросов, которые он не может обработать. Если какой-либо веб-сервис использует LDAP-авторизацию, то это дает злоумышленнику возможность использовать LDAP-инъекции, подобно SQL-инъекциям, для получения списка пользователей и другой информации из каталога, к которому сервис подключен.

В случаях, когда администратор Active Directory в целях безопасности настраивает парольную политику таким образом, что учетная запись блокируется после определенного конечного числа неудачных попыток входа, у злоумышленника появляется возможность эксплуатировать этот механизм для блокировки учетных записей и привести к атаке типа «отказ в обслуживании». Для реализации этого необходимо иметь доступ к учетным данным одного пользователя, выполнить от его имени команду «net user /domain», в результате получить список всех пользователей домена и воспроизводить неудачные попытки входа в домен. Таким образом, пользователи, в том числе и администраторы, не смогут зайти в домен.

В 2018 была найдена уязвимость (CVE-2018-1057) в Samba 4 AD DC, которая заключалась в неправильной проверке разрешений пользователя при изменении пароля, что позволяло изменять пароли любым другим пользователям, включая администраторов и учетные записи привилегированных служб.

Если в качестве протокола аутентификации выбран Kerberos, то становится возможна эксплуатация уязвимости, заключающейся в получении «session ticket», который зашифрован сеансовым ключом сервера. После захвата «session ticket» злоумышленник может его с помощью Brute Force попытаться расшифровать, если атака закончится успехом, будет получен пароль от учетной записи, которая ассоциирована с сервером. Атака носит название Kerberoasting.

Все вышеописанные атаки преимущественно используются в комплексе для захвата Active Directory[18], что дает возможность, например, далее распространять вредоносные программы по корпоративной сети. Процесс получения полного контроля над AD можно разделить на четыре этапа: разведка, продвижение по Active Directory, эксплуатация, захват домена. На этапе разведки используются такие инструменты, как PowerView и bloodhound, с помощью которых введется поиск всех доменных

администраторов и хостов, на которых они авторизованы, также bloodhound позволяет построить граф связей между объектами AD и кратчайший путь до сессии авторизованного админа. Далее атакующему могут понадобиться учетные записи сервисов или служб, так как они, как правило, являются привилегированными. Обнаружить такие учетные записи можно и сканированием портом с помощью nmap, но злоумышленнику удобнее использовать SPN сканирование, реализующее задачу через LDAP -запросы к контроллеру домена. Выполнение сканирования происходит через скрипт на PowerShell. Помимо bloodhound, получить список сессий в домене можно с помощью скрипта в nmap под названием *smb-enum-sessions.nse*, которые, далее, атакующий будет использовать для удалённо подключения. Описанная атака, направленная на поиск удаленных сессий называется Remote Sessions Enumeration.

Следующим этапом в захвате Active Directory является продвижение, то есть злоумышленнику нужно авторизоваться на удаленные хосты, которые он нашел в предыдущем этапе, для этого ему необходимы учетные данные. Реализовать это можно через уже описанный атаку Pass-the-Hash, но если используется протокол аутентификации Kerberos этого будет недостаточно. В этом случае будет осуществляться атака Overpass-the-Hash, основанная на особенностях работы Kerberos в Windows. Как уже было описано ранее, при использовании данного протокола клиент шифрует своим хешированным паролем запрос на аутентификацию к KDC, в ответ KDC выдает ему билет на выдачу других билетов (Ticket-Granting Ticket), таким образом, если атакующих перехватит хеш пользователя, то он сможет выдавать себе билет на пропуск в другие системы. В случае, если злоумышленник смог перехватить хеш учетной записи krbtgt, которая является привилегированной, чьим хешом подписываются остальные билеты на получение TGT, теряется необходимость во взаимодействии с KDC, так как он сам имеет возможность генерировать себе TGT, он получается Golden Ticket, позволяющий

отправлять запросы на аутентификацию на сервисы внутри структуры AD на неограниченное время.

На этапе эксплуатации после аутентификации и авторизации на нужных машинах, атакующий начинает удалённое выполнение команд. Для реализации этого есть встроенный механизм в Windows — WMI (Windows Management Instrumentation). Реализация происходит из cmd.exe утилитой wmic, параметры которой — адрес подключения, учетные данные, «process call create» для выполнение команды на удалённом хосту и, соответственно, сама команда.

Последняя стадия — захват домена, после получения удаленного доступа к нужному хосту, атакующий может получить возможность реплицировать вредоносные объекты и вносить изменения в AD, создав теневой контроллер домена и тем самым реализовав атаку DCShadow. Атака реализовывается с помощью уже упомянутого инструмента mimikatz, вносятся изменения в схему данных и меняется SPN хоста, к которому злоумышленник подключился.

Проанализировав описанные атаки, можно прийти к выводу, что большинство невозможно реализовать без удаленного доступа к машинам в домене и без знания учетных данных. В следующей главе будут описаны меры защиты для предотвращения реализации атаки и способы для обнаружения, если атака будет совершена.

Глава 3. Меры защиты

Первая рассматриваемая уязвимость была связана с передачей логина и пароля пользователя в открытом виде при запросе к LDAP-серверу (рисунки 1 и 2), данная уязвимость актуальна больше к LDAP-серверам на Linux, так как в Windows, начиная с NT 3.1, в доменах используется протокол аутентификации NTLM, а с Windows 10 — Kerberos 5. Данная уязвимость на серверах, развёрнутых на Linux, и Windows Server, 2012 и младше, устраняется шифрованием всего трафика с помощью TLS, либо с помощью использования Kerberos. Тем не менее, как уже было сказано, данные методы тоже подвержены атакам при захвате трафика, например, с помощью WireShark. Если злоумышленник смог получить доступ к учетным данным, необходимо пресечь попытки входа в систему, для этого администратором домена должна быть разработана и настроена политика безопасности, включающая в себя включение автоматической блокировки рабочего места после фиксированного времени бездействия и дополнительный фактор аутентификации, например, использовать смарт-карты, предварительно обеспечив рабочие места специальным считывателем, или технологию 2015 года — Windows Hello, — которая позволяет добавить в качестве дополнительного фактора пин-код, распознавание лица и отпечаток пальца. Помимо включения дополнительной проверки при аутентификации, должна быть разработана парольная политика в рамках политики безопасности о сложности пароля. Например, пароль должен содержать не менее 10 символом, обязательно содержать цифры, специальные символы, буквы обоих регистров, что при знании злоумышленником только логина, затрудняет перебор пароля с помощью словаря и увеличивает затраченное время на атаку Brute Force. Защититься от Brute Force также можно с помощью правила, которое будет блокировать учетную запись после определенного количества неудачных попыток входа. Но стоит помнить, что данная настройка дает атакующему возможность осуществить «отказ в

обслуживании» учетных записей, имена которых ему известны, особенно атака опасна, если у организации реализована технология SSO, так как в результате пользователь потеряет доступ сразу к нескольким ИС. Необходимо отметить, что даже без SSO, пользователь может потерять доступ к нескольким системам, если в них реализована LDAP-авторизация. Например, можно рассмотреть случай, когда LDAP-авторизация реализована в таких системах, как GitLab, Jira, Confluence, TeamCity, которые используются при разработке какого-либо продукта ИТ-компанией. В случае, если злоумышленник будет перебирать пароли в одной из систем, в которой неудачное количество попыток для блокировки будет такое же, как и установленное на LDAP-сервере, в конечном итоге, будет заблокирован доступ ко всем системам. Устранение уязвимости. — ограничение количества попыток в системах, которые доступны извне корпоративной среды, на меньшее, чем на LDAP-сервере, или организация доступа к системам только через VPN.

Многие атаки на Active Directory реализовываются с помощью инструмента mimikatz, далее будут рассмотрены меры, которые необходимо принять для уменьшения возможности его применения. В первую очередь, необходимо включить групповую политику «Debug programs» в домене и применять ее только к группам, которым необходима привилегия SeDebugPrivilege. Также необходимо проконтролировать, что в настройках парольной политики стоит запрет на хранение паролей в открытом виде. Изначально mimikatz была создана для получения хешей паролей пользователей, которые используются при недоступности машины к контроллеру домена. Отключить хранение хешей паролей можно с помощью включения политики «Interactive Logon: Number of previous logons to cache (in case domain controller is not available)».

От сканирования портов, которые используются для выявления работающих служб, необходимо установить IDS/IPS систему и настроить

правило, которое будет помечать адрес, за короткий промежуток времени присылающий множество запросов на соединение, и отбрасывать следующие пакеты с этого адреса.

В предыдущей главе была также описана атака DCShadow, с помощью которой можно добавлять новые объекты в Active Directory, внедрять вредоносные объекты и распространять их с помощью групповых политик. В связи с тем, что события, происходящие в «теневом» контроллере домена не отражаются в журнале событий, необходимо осуществлять другим способом проверку новых объектов в дереве. В рамках данной работы был разработан скрипт на языке программирования Python, осуществляющий поиск всех контроллеров домена, а также проверяющий список машин, и пользователей в домене путем сравнения провалидированного списка и актуального, выгружаемого из Active Directory (см. приложение 1). Все обнаруженные нелегитимные домены, пользователи и машины будут записаны в специальный файл. Данный скрипт можно запускать через планировщик заданий в Windows или же через cron в Linux с необходимой периодичностью.

Неотъемлемой частью обеспечению безопасности является мониторинг и своевременное реакция на инциденты, для более эффективной работы необходимо внедрение SIEM. В SIEM систему могут поступать сообщения от журнала событий, IPS/IDS систем, межсетевых экранов, антивирусного ПО и так далее. Далее будут рассматриваться примеры, как с помощью данной технологии можно обеспечить обнаружение некоторые атаки, описанные в предыдущей главе.

Прежде всего, необходимо включить политику аудита Active Directory и настроить расширенный аудит Windows. Если на доменных машинах используется PowerView, работающий по протоколу LDAP, обнаружить его можно с помощью логирования события 1644 и по анализу трафика по LDAP, так как в LDAP информация передается в открытом виде. Также в

связи с тем, что PowerView написан на PowerShell, можно осматривать события 4104 в расширенном аудите PowerShell. Обнаружить сканирование в поисках SPN, можно также с помощью события 1644. Далее, когда злоумышленник будет искать все активные сессии пользователей, это отразится в событиях 4624 (успешная авторизация по сети) и 5145 (получение доступа к общему ресурсу IPC$, созданного Windows). Также нужно искать в трафике отправку запроса NetSessEnum, который перечисляет активные сессии. Для обнаружения запуска mimikatz, необходимо искать в событии аудита PowerShell 4104 строчки с названием данного инструмента. В случае реализации атаки Overpass-the-Hash, обнаружить ее можно путем анализа запросов, которые отправляются в KDC. Нормальное поведение для такого запроса — это шифрование AES256, в то время как mimikatz шифрует запрос с помощью RC4. При реализации атаки Golden Ticket, злоумышленник посылает запрос в контроллер домена на выдачу билета для доступа к конкретному сервису, но не запрашивает билет на получение других билетов. Таким образом ситуация, когда в журнале есть событие 4769, которое свидетельствует о выдаче пропуска к конкретному сервису, но нет события 4768, возможно, свидетельствует об атаке Golden Ticket. Для отслеживания удаленного выполнения команд с командной строки необходимо отслеживать события 4624 и 4688, где первое говорит об удаленном удачном входе в систему, а второе о выполнении команд с командной строки. Поле Logon ID должно быть одинаковым у обоих событий, оно даст информацию о машине, на которой запущено удаленное выполнение.

Для того, чтобы обезопасить ИС от LDAP-инъекций, необходимо экранировать символы, которые могут использоваться в имени объектов. Если необходимо проверить LDAP-сервер на уязвимости, связанные с «аномальными» запросы, то следует использовать инструмент PROTOS LDAP.

В последних версиях и обновлениях Microsoft Windows память с хешами NTLM и Kerberos защищена, что затрудняет изъятие их из памяти с помощью mimikatz, таким образом, для обеспечения безопасности необходимо своевременно устанавливать обновления.

Не стоит забывать о том, что, в первую очередь, большой угрозой в информационной безопасности является человеческий фактор, поэтому необходимо разработать политику безопасности организации, с которой должны ознакомиться все сотрудники. Необходимо также периодически проводить обучение сотрудников по противодействию фишингу и осуществлять рассылку на корпоративную почту с памяткой по информационной безопасности. Роли пользователей должны быть строго разграничены, роли администратора домена, администратора организации, отдельных подразделений не должны быть привязаны к одной учетной записи.

Еще одной мерой защиты при любых угрозах является наличие антивирусного программного обеспечения и своевременное обновление антивирусных баз знаний.

Глава 4. Модель угроз

Для демонстрации пригодности перечисленных в предыдущей главе мер защиты, было построена модель угроз Active Directory по методике ФСТЭК[3][4].

4.1. Описание информационной системы

Данная информационная система предназначена для эффективной работы корпоративной среды, позволяет создавать домен организации, с помощью которого можно контролировать учетные записи пользователей и их вход на корпоративные устройства. Серверная часть Active Directory представляет собой службу каталогов Microsoft, развёрнутую на Windows Server 2019. Пользователи получают доступ к ИС только из локальной сети.

ИС имеет подключение к локальной вычислительной сети организации и к сетям международного обмена. Все компоненты ИС находятся внутри контролируемой зоны.

Active Directory позволяет:

1. создавать и администрировать домен;
2. создавать учетные записи пользователей;
3. осуществлять авторизацию на устройства;
4. централизованно управлять объектами организации;
5. осуществлять быстрый поиск объектов.

В ИС обрабатывается следующая информация, относящаяся к ПДн: имя и фамилия сотрудника, его электронная почта, должность и телефон.

Работа в AD производится в многопользовательском режиме с разграничением прав доступа, которое обеспечивается за счет идентификации объектов.

4.2. Модель нарушителя

К внешним нарушителям (тип I) относятся:

1. Бывшие сотрудники организации (пользователи);
2. Конкурирующие организации;
3. Преступные группы;
4. Неустановленные внешние нарушители, действующие по идеологическим или политическим убеждениям.

К внутренним нарушителям (тип II) относятся:

1. Пользователи ИС;
2. Технический персонал, обслуживающий здания;
3. Персонал, обслуживающий технические средства;
4. Администраторы ИС и администраторы ИБ.

Разделение нарушителей на группы по их потенциалу в таблице 1.

Таблица 1

Низкий потенциал	**Средний потенциал**
бывшие сотрудники организации (пользователи), неустановленные внешние нарушители, пользователи ИС, технический персонал, персонал, обслуживающий технические средства	администраторы ИС и администраторы ИБ, преступные группы, конкурирующие организации

Возможные мотивации нарушителей представлены в таблице 2.

Таблица 2

Нарушитель	**Мотивация**
Бывшие сотрудники организации	Причинение имущественного и репутационного ущерба путем мошенничества или иным преступным путем.

	Месть за ранее совершенные действия
Конкурирующие организации	Получение конкурирующего преимущества Причинение репутационного и имущественного ущерба
Преступные группы	Причинение имущественного ущерба путем мошенничества или иным преступным путем Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
Неустановленные внешние нарушители	Идеологические или политические мотивы. Причинение имущественного и репутационного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.
Администраторы ИС и администраторы ИБ	Причинение имущественного и репутационного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации Месть за ранее совершенные действия.

	Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.
Пользователи ИС	Причинение имущественного и репутационного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.
Технический персонал, обслуживающий здания	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
Персонал, обслуживающий технические средства	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.

Предполагается, что:

- У всех нарушителей есть возможность получить информацию об уязвимостях отдельных компонент ИС, а также о методах и средствах реализации угроз, которые опубликованы в общедоступных источниках.

- Все нарушители имеют возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны.
- Пользователи ИС, администраторы ИС и администраторы ИБ имеют возможность проводить подготовку и проведение атак в пределах контролируемой зоны с доступом к ИС
- Конкурирующие организации, преступные группы, администраторы ИС и администраторы ИБ имеют осведомлённость о мерах защиты информации, применяемых в информационной системе данного типа; имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения; имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Согласно ФСТЭК[2], в качестве показателя актуальности угрозы безопасности информации принимается двухкомпонентный вектор в случае отсутствия данных для оценки вероятности угрозы.

$$\text{УБИ}_j^{\text{A}} = [\text{возможность реализации угрозы } (Y_j);\ \text{степень ущерба } (\text{X}j)]$$

Возможность реализации угрозы определяется с помощью оценки уровня защищенности ИС и потенциала нарушителя, необходимого для реализации угрозы j.

$$Y_j = [\text{уровень защищенности ИС}(Y_1); \text{потенциал нарушителя } (Y_2)]$$

Степень ущерба определяется на основе оценки степени последствий от нарушения доступности, конфиденциальности и целостности в результате реализации угрозы j.

Так как в данной ИС еще не реализованы никакие меры защиты, необходимо сперва оценить уровень проектной защищенности. Оценка уровня проектной защищенности в таблице 3.

Таблица 3

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	**Уровень проектной защищенности информационной системы ($Y_{1п}$)**
По структуре информационной системы	Высокий
По используемым информационным технологиям	Низкий
По архитектуре информационной системы	Низкий
По наличию (отсутствию) взаимосвязей с иными информационными системами	Низкий
По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования	Низкий
По размещению технических средств	Высокий
По режимам обработки информации в информационной системе	Низкий
По режимам разграничения прав доступа	Средний
По режимам разделения функций по управлению информационной системой	Средний
По подходам к сегментированию информационной системы	Низкий

Высокий — 2

Средний — 2

Низкий — 6

20% характеристик соответствуют уровню «высокий», 20% характеристик соответствуют уровню не ниже «средний», таким образом уровень проектной защищённости ИС — **низкий**. Для ИС с таким уровнем проектной защищенности возможность всех рассматриваемых угроз является **высокой** и все они будут **актуальными**, согласно методологии, определенной в ФСТЭК [2]. Определение актуальности угрозы происходит согласно таблице 4.

Таблица 4

Возможность реализации угрозы (Y_j)	**Степень возможного ущерба (X_j)**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Возможность реализации угрозы определяется согласна таблице 5.

Таблица 5

Потенциал нарушителя (Y_2)	**Уровень защищенности ($Y_1, Y_{1п}$)**		
	Высокий	**Средний**	**Низкий**
Низкий	Низкая	Средняя	Высокая
Средний	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Актуальные угрозы для данной ИС, которые можно сопоставить с угрозами и атаками, перечисленными в главе 2 расположены в приложении 2. Далее угрозы, описанные в приложении 2, будут рассматриваться более подробно.

Оценка опасности при реализации каждой угрозы будет производиться с помощью системы оценки защищенности CVSS v3, основу которой составляет набор метрик: базовые, временные и контекстные. В базовые метрики входят:

- Вектор атаки (AV)
- Сложность атаки (AC)
- Требуемые привилегии (PR)
- Взаимодействие с пользователем (UI)
- Границы эксплуатации (S)
- Метрики воздействия на конфиденциальность, целостность и доступность (C, I, A)

Во временные метрики входят:

- Степень зрелости доступных средств эксплуатации(E)
- Доступные средства устранения (RL)
- Степень доверия к информации об уязвимости (RC)

Контекстные метрики применяются, когда необходимо уточнить уже полученную оценку с помощью двух других метрик из-за особенностей среды конкретного пользователя. Определяется, какое из свойств информации наиболее важное в атакуемом компоненте.

Расчёты производились с помощью калькулятора CVSS v3, представленного на сайте NIST[19]. Формулы и возможные значения метрик представлены в приложении 3. Качественная оценка степени серьезности определяется согласно таблице 6.

Таблица 6

Степень серьезности	Нет	Низкая	Средняя	Высокая	Критическая
Значение	0	0,1-3,9	4,0-6,9	7,0-8,9	9,0-10,0

Угроза восстановления аутентификационной информации

Угроза заключается в возможности подбора аутентификационной информации дискредитируемой учётной записи пользователя в системе. Реализация возможна как с помощью специальных инструментов, так и «вручную» (атака Brute Force).

Угроза оказывает воздействие на **конфиденциальность**. $X = X^{К} =$ **низкая**.

Данная угроза имеет следующие метрики, согласно CVSS v3:

Таблица 7

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*N*	*U*	*L*	*N*	*N*	*H*	*X*	*C*	*X*	*M*	*X*

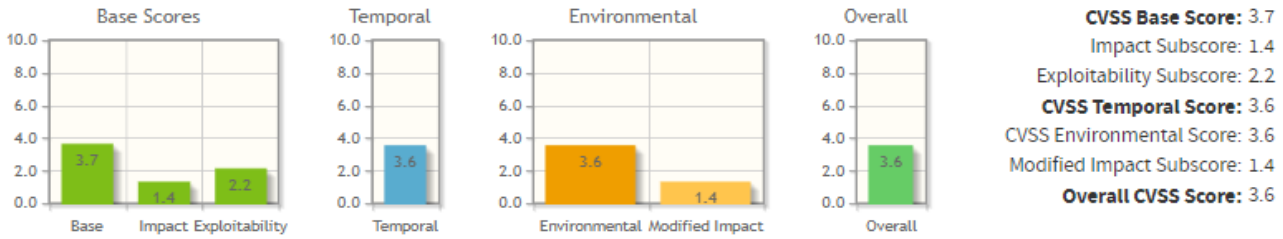

Рисунок 3. Значения метрик из калькулятора CVSS nvd.nist.gov

Итоговое значение – 3,6, что соответствует **низкой** степени серьезности.

Меры защиты:

- Административные: разработка политики безопасности и парольной политики, обучение персонала по формированию стойких паролей;
- Морально-этические: периодические рассылки пользователям по обеспечению информационной безопасности;
- Программное-технические: включение расширенного аудита событий, внедрение SIEM системы.

После применения парольной политики по добавлению дополнительного фактора аутентификации, степень серьезности упадет до 2,0.

Угроза внедрения вредоносной программы или кода из недоверенных источников

Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями или автоматически при выполнении определённого условия, а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов. Реализация угрозы возможна в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников, при посещении зараженных сайтов, получении «почтового червя» или при наличии у него привилегий установки программного обеспечения.

Угроза оказывает воздействие на **конфиденциальность**, **целостность** и **доступность**.

$X^{К} =$ низкая, $X^{Д} =$ высокая, $X^{Ц} =$ средняя; $X = \max(X^{К}, X^{Д}, X^{Ц}) =$ **высокая**.

Таблица 8. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*N*	*C*	*L*	*L*	*H*	*H*	*X*	*C*	*L*	*M*	*H*

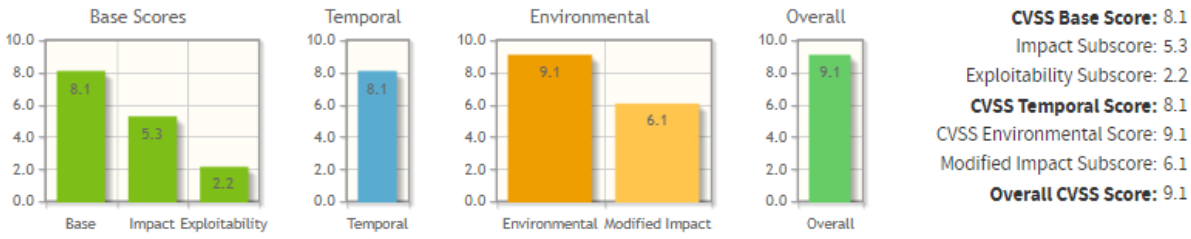

Рисунок 4. Значения метрик

Итоговое значение – 9,1, что соответствует **критической** степени серьезности.

Меры защиты:

- Административные: разработка политики безопасности с включением правила о запрете установки стороннего ПО пользователям без прав администратора;
- Морально-этические: периодические рассылки пользователям о правилах обеспечения безопасности в сети;
- Программно-технические: установка на все рабочие места антивирусной защиты, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: $AV = L$, $UI = R, RL = O$. В результате, значение стало 4,6, что соответствует **средней** степени серьезности, в случае более строгой настройки политики в антивирусном ПО, AV примет значение P, а уровень серьезности станет 3,9 -- **низким.**

Угроза «незаметного» добавления объектов

Угроза заключается в возможности несанкционированного добавления нарушителем еще одного контроллера домена, события с которого не будут отражаться в журнале событий и с помощью которого он далее может внедрять вредоносный код и создавать новые объекты (атака DCShadow). Реализация угрозы возможна в случае наличия слабостей в конфигурации системы.

Угроза оказывает влияние на **конфиденциальность** и **целостность**.

$X^{\text{К}} =$ низкая, $X^{\text{Ц}} =$ низкая; $X = \max(X^{\text{К}}, X^{\text{Ц}}) =$ **низкая**.

Таблица 9. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
L	*H*	*H*	*N*	*C*	*H*	*H*	*L*	*F*	*X*	*C*	*H*	*H*	*H*

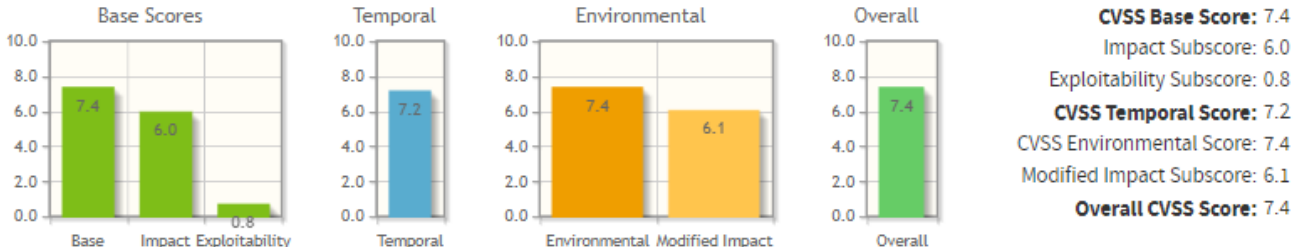

Рисунок 5. Значения метрик

Итоговое значение – 7.4, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, включение политик безопасности, разработка сервиса для выявления нелегитимных объектов, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=P, RL=T, I=L, A=L. В результате, значение стало 6.9, что соответствует **средней** степени серьезности.

Угроза приведения системы в состояние «отказ в обслуживании»

Угроза заключается в возможности отказа системой в доступе легальным пользователям при посылке нарушителем некорректного LDAP-запроса.

Реализация данной угрозы возможна при отсутствии настройки для обработки LDAP-запросов.

Угроза оказывает влияние на **доступность.** $X = X^{Д}$ **= высокая**.

Таблица 10. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
L	*H*	*L*	*N*	*C*	*N*	*N*	*H*	*H*	*X*	*C*	*N*	*N*	*H*

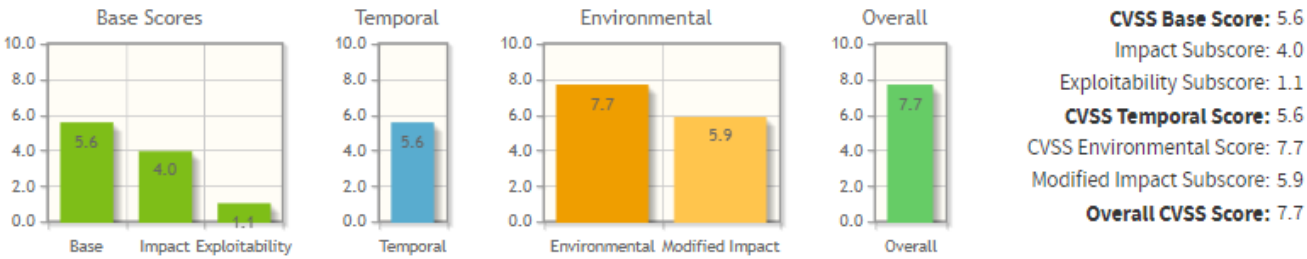

Рисунок 6. Значения метрик

Итоговое значение – 7.7, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: использование инструментов для проверки обработки системой некорректных запросов и исправление выявленных ошибок, заведение дополнительного контроллера домена, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=P, RL=T, A=L. В результате, значение стало 3,4, что соответствует **низкой** степени серьезности.

Угроза использования LDAP-инъекции

Угроза заключается в некорректного LDAP-запроса, в ответ на который система может позволить раскрыть конфиденциальную информацию и модифицировать ее. Реализация данной угрозы возможна при отсутствии настройки для обработки LDAP-запросов.

Угроза оказывает влияние на **целостность** и **конфиденциальность**.

$X^{К} =$ низкая, $X^{Ц} =$ средняя; $X = \max(X^{К}, X^{Ц}) =$ **средняя**.

Таблица 11. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*L*	*N*	*U*	*L*	*L*	*N*	*H*	*X*	*C*	*H*	*M*	*X*

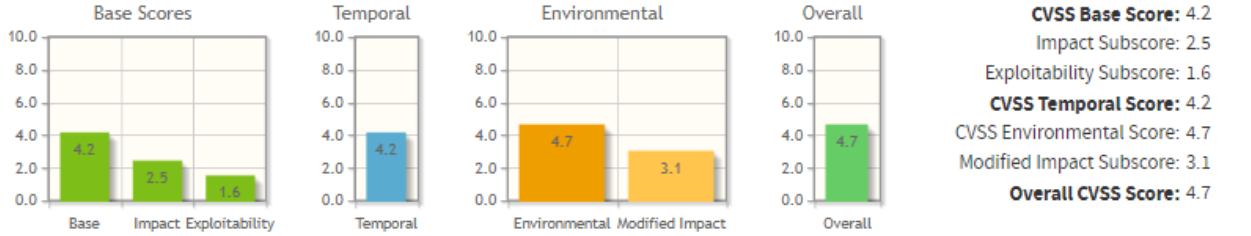

Рисунок 7. Значения метрик

Итоговое значение – 4.7, что соответствует **средней** степени серьезности.

Меры защиты:

- Программно-технические: использование инструментов для проверки обработки системой некорректных запросов и исправление выявленных ошибок, внедрение SIEM системы

После применения мер защиты изменились следующие метрик: AV=L, E=P, RL=W. В результате, значение стало 3,9, что соответствует **низкой** степени серьезности.

Угроза несанкционированного удаленного подключения

Угроза заключается в возможности нарушителя получения удаленного доступа с помощью специальных инструментов (mimikatz,PowerSploit,wmi). Реализация угрозы возможна при наличии уязвимостей в операционной системе, на которой развернута дискредитируемой информационной системе и в наличии слабостей в конфигурации ИС.

Угроза оказывает воздействие на **конфиденциальность**. $X = X^{К} =$ **низкая.**

Таблица 12. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*R*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

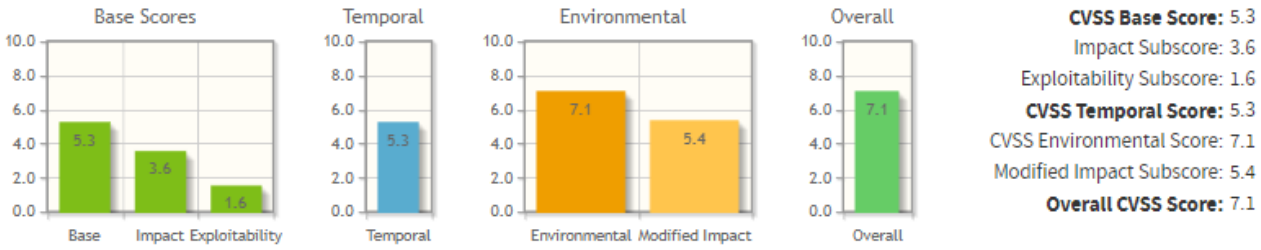

Рисунок 8. Значения метрик

Итоговое значение – 7.1, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, установка антивирусного программного обеспечения на все рабочие места, проведение своевременных обновлений, исправление ошибок в конфигурации, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: PR=L, E=P, RL=O. В результате, значение стало 5,9, что соответствует **средней** степени серьезности.

Угроза использования механизмов авторизации для повышения привилегий

Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе из-за ошибок в конфигурации.

Угроза оказывает воздействие на **конфиденциальность**. $X = X^{K} =$ **низкая.**

Таблица 13. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
L	*H*	*L*	*N*	*U*	*L*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

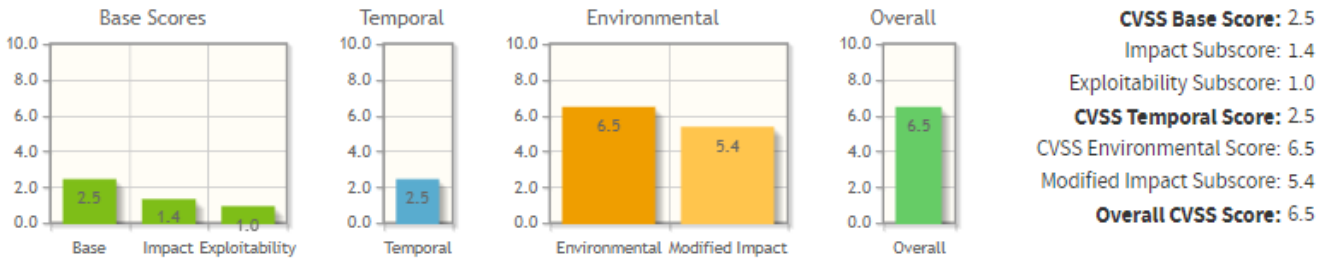

Рисунок 9. Значения метрик

Итоговое значение – 6.5, что соответствует **средней** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, проведение своевременных обновлений, исправление ошибок в конфигурации, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=P, RL=W. В результате, значение стало 3.0, что соответствует **низкой** степени серьезности.

Угроза использования слабостей и особенностей протоколов сетевого/локального обмена данными

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации и использованию особенностей работы протоколом. К данной угрозе можно отнести описанные во второй главе атаки, связанные с протоколами аутентификации NTLM и Kerberos.

Угроза оказывает влияние на **конфиденциальность**. $X = X^{К}$ **= низкая.**

Таблица 14. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
L	*H*	*L*	*N*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

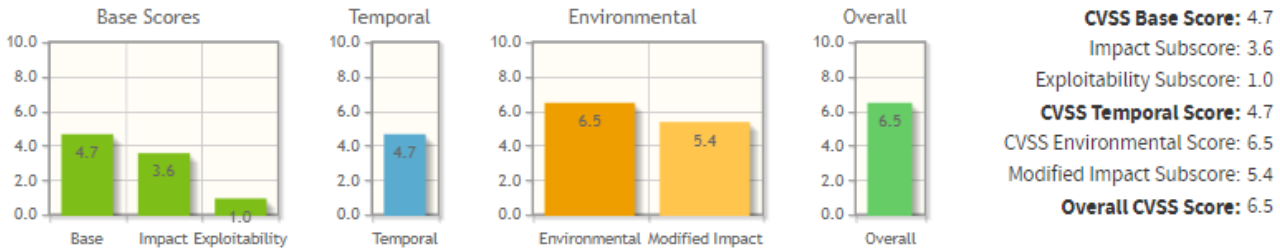

Рисунок 10. Значения метрик

Итоговое значение – 6.5, что соответствует **средней** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, проведение своевременных обновлений, исправление ошибок в конфигурации, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=F, RL=W, C=L. В результате, значение стало 3.1, что соответствует **низкой** степени серьезности.

Угроза несанкционированного доступа к аутентификационной информации

Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. К реализации можно отнести атаку, связанную с использованием инструмента mimikatz.

Угроза оказывает влияние на **конфиденциальность**. $X = X^{К} =$ **низкая.**

Таблица 15. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*L*	*N*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

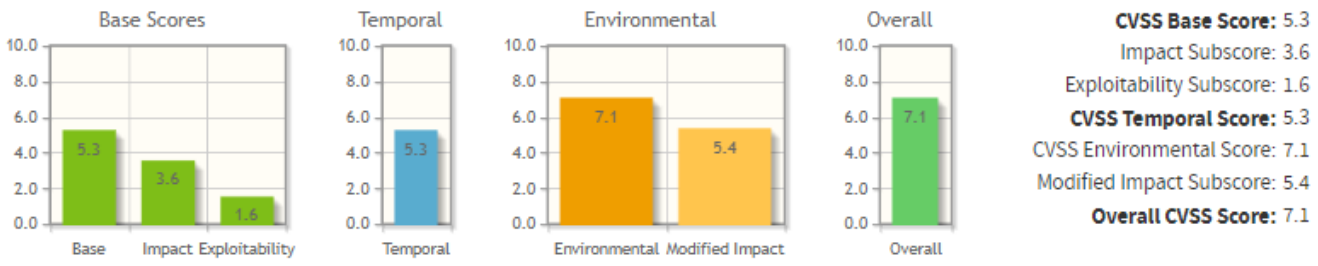

Рисунок 11. Значения метрик

Итоговое значение – 7.1, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, проведение своевременных обновлений, исправление ошибок в конфигурации, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=F, RL=O, C=L. В результате, значение стало 3.6, что соответствует **низкой** степени серьезности

Угроза несанкционированного изменения аутентификационной информации

Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств.

Угроза оказывается воздействие на **целостность** и **доступность**.

$X^{Ц} =$ средняя, $X^{Д} =$ высокая; $X = \max(X^{Д}, X^{Ц}) =$ **высокая**.

Таблица 16. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*L*	*N*	*U*	*N*	*H*	*H*	*H*	*X*	*C*	*X*	*H*	*H*

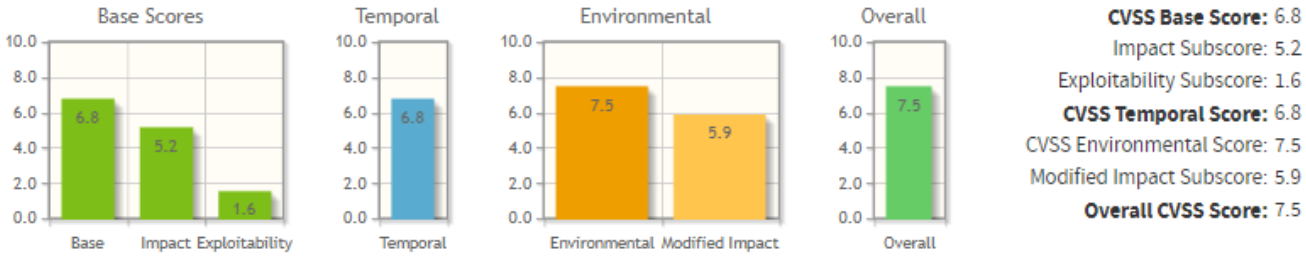

Рисунок 12. Значения метрик

Итоговое значение – 7.5, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: включение расширенного аудита событий, использование инструментов для проверки обработки системой некорректных запросов и исправление выявленных ошибок, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=F, RL=O, I=L, A=H. В результате, значение стало 4.8, что соответствует **средней** степени серьезности

Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб

Угроза заключается в возможности нарушителя проведения сканирования портов для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика. К данной угрозе можно отнести SPN сканирование.

Угроза оказывает влияние на **конфиденциальность**. $X = X^{К}$ **= низкая.**

Таблица 17. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*R*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

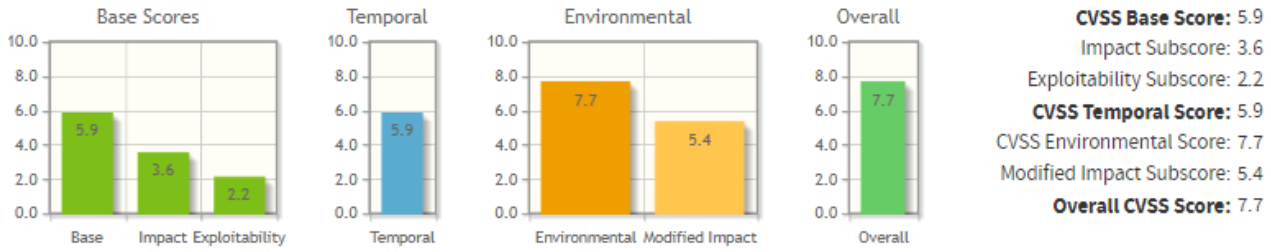

Рисунок 13. Значения метрик

Итоговое значение – 7.7, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: исправление ошибок в конфигурации, внедрение IPS/IDS системы, корректная настройка межсетевого экрана, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=F, RL=W, C=L. В результате, значение стало 4.2, что соответствует **средней** степени серьезности, при более строгой настройке AV примет значение L, уровень серьезности станет **низким** (3,4).

Угроза обнаружения хостов

Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика. К данной угрозе можно отнести атаку Remote Sessions Enumeration с использованием инструмента bloodhound.

Угроза оказывает влияние на **конфиденциальность**. $X = X^{К}$ **= низкая.**

Таблица 18. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*R*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

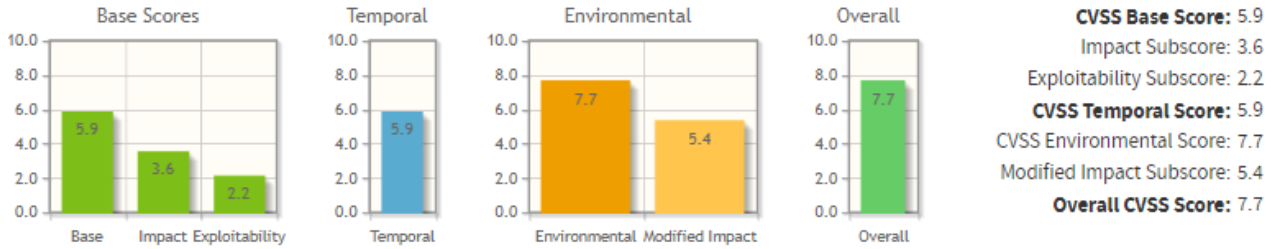

Рисунок 14. Значения метрик

Итоговое значение – 7.7, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: исправление ошибок в конфигурации, внедрение IPS/IDS системы, корректная настройка межсетевого экрана, внедрение SIEM системы.

После применения мер защиты изменились следующие метрик: E=F, RL=W, C=L. В результате, значение стало 4.2, что соответствует **средней** степени серьезности, при более строгой настройке AV примет значение L, уровень серьезности станет **низким** (3,4).

Угроза перехвата данных, передаваемых по вычислительной сети

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети.

Угроза оказывает влияние на **конфиденциальность**. $X = X^{К}$ **= низкая.**

Таблица 19. Метрики, согласно CVSS v3

AV	***AC***	***PR***	***UI***	***S***	***C***	***I***	***A***	***E***	***RL***	***RC***	***CR***	***IR***	***AR***
N	*H*	*N*	*R*	*U*	*H*	*N*	*N*	*H*	*X*	*C*	*H*	*X*	*X*

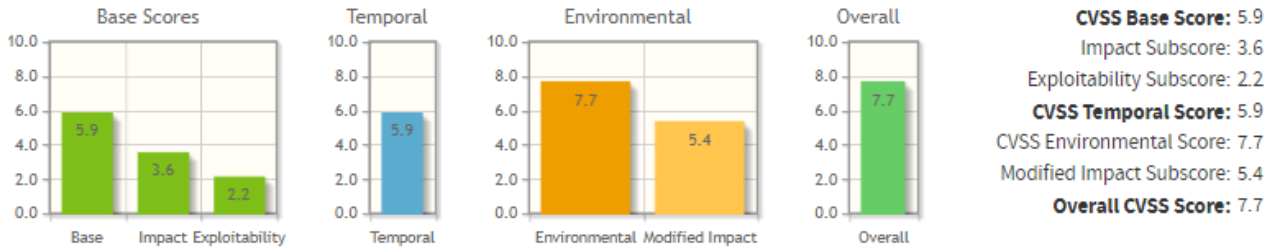

Рисунок 15. Значения метрик

Аналогично двум предыдущим угрозам, итоговое значение – 7.7, что соответствует **высокой** степени серьезности.

Меры защиты:

- Программно-технические: передача данных через VPN.

После применения мер защиты изменились следующие метрик: E=F, RL=W, C=L. В результате, значение стало 4.2, что соответствует **средней** степени серьезности.

После применения мер защиты для нейтрализации актуальных угроз появилась новая угроза — **блокировка доступа к системе легитимного пользователя.** Угроза заключается в возможности злоумышленника реализовать отказ в доступе легитимному пользователю к ИС. Реализация данной угрозы становится возможной после введения политики безопасности с настройкой о блокировке учетной записи после определенного количества неудачных попыток входа. В случае, когда LDAP-сервер используется для авторизации в других системах, доступ блокируется к ним тоже. Значение степени серьезности такой угрозы – 8,9, что соответствует **высокому** уровню.

Данную появившуюся угрозу возможно нейтрализовать с высокой оперативностью, благодаря уже внедренной системе SIEM, от которой придет оповещение о блокировке, и добавлением дополнительного фактора аутентификации, ее уровень серьезности опустится до **низкого**, со значением 3,9. Таким образом, система стала обладать **высоким** уровнем защищенности.

Актуальными угрозами в системе будут только при их реализации нарушителем с высоким потенциалом, согласно методике определения актуальности угрозы ФСТЭК.

Заключение

В настоящее время Active Directory является одним из самых удобных и распространённых инструментов для управления доступом на рабочих устройствах и ресурсах в корпоративной среде, что не может не повлиять на изобретение все новых атак и поиск уязвимостей в данной системе и в LDAP — протоколе, на основе которого работает ИС.

В результате выполнения выпускной квалификационной работы был изучен протокол LDAP, его информационная и функциональная модель, модель именования и модель безопасности. Подробнее была рассмотрена Active Directory, современные атаки на нее и рекомендуемые методы защиты. В главе 4 была построена модель угроз и составлены рекомендации для нейтрализации актуальных угроз. В рамках работы был написан скрипт на языке Python, который позволяет обнаружить одну из современных атак DCShadow, а также контролировать своевременное удаление невалидных объектов с контроллера домена.

В результате применения рекомендованных мер защиты, уровень защищенности системы переходит из низкого уровня в высокий.

Список используемых источников

[1] Р 50.1.056 – 2005. Техническая защита информации. Основные термины и определения. — Издание официальное — М.: Стандартинформ, 2005.

[2] ФСТЭК России, «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 года.

[3] ФСТЭК России, «Методика определения угроз безопасности информации в информационных системах» (проект) от 2015 года.

[4] ФСТЭК России, «Банк данных угроз безопасности информации» от 26.06.2018 года.

[5] Гостехкомиссия России, «Руководство по разработке профилей защиты и заданий по безопасности», 2003 год.

[6] URL: https://www.zytrax.com/books/ldap/,«LDAP for Rocket Scientists»

[7] URL: https://pro-ldap.ru

[8] Гостехкомиссия России, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25.07.1997 года.

[9] RFC 4512. «Lightweight Directory Access Protocol (LDAP):Информационные модели каталога», июнь 2006.

[10] RFC 4513. «Lightweight Directory Access Protocol (LDAP): Методы аутентификации и механизмы обеспечения безопасности», июнь 2006.

[11] RFC 4522. «Simple Authentication and Security Layer (SASL)», июнь 2006.

[12] RFC 4511. «Lightweight Directory Access Protocol (LDAP): Определение протокола», июнь 2006.

[13] URL: https://ldap.com

[14] David Chadwick. Threat modelling for Active Directory. University of Salford, 2004.

[15] URL: https://www.varonis.com/blog/active-directory-security/

[16] URL: https://www.isdecisions.com/insider-threats-manifesto/active-directory/users-security-awareness.htm

[17] URL: https://www.blackhat.com/docs/us-16/materials/us-16-Metcalf-Beyond-The-MCSE-Active-Directory-For-The-Security-Professional-wp.pdf

[18] URL: https://www.ptsecurity.com/ru-ru/research/webinar/290582/

[19] URL: https://www.first.org/cvss/specification-document, Specification Document

Приложение 1

Данное приложение содержит исходный код скрипта на языке Python, предназначенный для обнаружения невалидных объектов в ИС, в частности, для обнаружения реализации атаки DCShadows.

```
from ldap3 import Server, Connection, ALL
import datetime

'''
   Формирование списка валидных объектов из файлов
   Из заданного файла считывается построчно информация и добавляется в список
   :param name_list: список, в которой будет записываться информация из файла
   :param type: тип объекта
'''
   def get_list_from_file(name_list, type):
       print("Enter PATH to the list of valid " + type + "s:")
       path = input()
       f = open(path, "r")
       for line in f:
           line = line.split('\n')
           line = line[0]
           name_list.append(line)
       f.close()


   '''
      Подключение к LDAP серверу
      :param domain: адрес LDAP-сервера
      :param username: имя учетной записи, под которой будет осуществляться проверка
      :param password: пароль от учетной записи, под которой будет осуществляться проверка
      :return ldap_connection: подключение к LDAP-серверу
   '''
   def ldap_connect(domain, username, password):
       ldap_server = Server(domain, get_info=ALL)
       ldap_connection = Connection(ldap_server, user=username, password=password, authentication="NTLM", auto_bind=True)
       return ldap_connection
```

```
32.
33.
34.    '''
35.       Обнаружение невалидных объектов
36.       :param ldap_connection: подлкючение к LDAP-серверу
37.       :param search_base: база для поиска объектов на LDAP-сервере
38.       :param path_to_log: путь для логирования
39.       :param search_filters: фильтр для поиска на LDAP-сервере
40.       :param type: тип объекта
41.
42.       Сравнение зараннее сформированного списка валидных объектов с
   актуальным списком по sAMAccountName
43.       В случае обнаружения объекта, которого нет в списке валидных,
   об этом событии добавляется запись в лог-файл
44.    '''
45.    def check_ilvalid(ldap_connection, search_base, path_to_log, sear
   ch_filters, type):
46.        ldap_connection.search(search_base, search_filters, attribute
   s=['sAMAccountName'])
47.        actual_list = ldap_connection.entries
48.        valid_list = list()
49.        get_list_from_file(valid_list, type)
50.        for k in range(len(actual_list)):
51.            name = actual_list[k]
52.            name = str(name['sAMAccountName'])
53.            name = name.lower()
54.            valid_flag = False
55.            for i in range(len(valid_list)):
56.                valid_name = valid_list[i]
57.                if valid_name == name:
58.                    valid_flag = True
59.                    break
60.            if valid_flag == False:
61.                now = datetime.datetime.now()
62.                date = now.strftime("[%d/%m/%Y %H:%M]")
63.                log = date + " " + type + " " + name + " is illegal!"
64.                with open(path_to_log, "a+", encoding="utf=8") as fil
   e_list:
65.                    file_list.write(log)
66.                    file_list.write('\n')
67.
68.
69.    print("Enter domain controller:")
70.    domain = input()
71.    print("Enter username:")
```

```
72.    username = input()
73.    print("Enter password:")
74.    password = input()
75.    print("Enter search base:")
76.    search_base = input()
77.    print("Enter PATH to the log:")
78.    path_log = input()
79.    ldap_connection = ldap_connect(domain, username, password)
80.    check_ilvalid(ldap_connection, search_base, path_log, search_filt
   ers='(primaryGroupID=516)', type="Domain Controller")
81.    check_ilvalid(ldap_connection, search_base, path_log,search_filte
   rs='(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol
   :1.2.840.113556.1.4.803:=2)))',type="User")
82.    check_ilvalid(ldap_connection, search_base, path_log, search_filt
   ers='(objectCategory=computer)', type="Machine")
```

Примечание. В определении `ldap_connection` используется тип аутентификации NTLM, при реализации метода с использованием TLS на LDAP-сервере, необходимо использовать его и в данной программе.

Приложение 2

Угроза	**Источник угрозы**	**Нарушение целостности (ущерб)**	**Нарушение доступности (ущерб)**	**Нарушение конфиденциальности (ущерб)**	**Степень ущерба**
Угроза восстановления аутентификационной информации	Внутренний/внешний нарушитель с низким потенциалом	-	-	+ (низкий)	низкая
Угроза внедрения вредоносной программы или кода из недоверенных источников	Внутренний/внешний нарушитель с низким потенциалом	+ (средний)	+ (высокая)	+ (низкий)	высокая
Угроза блокировки доступа к системе легитимного пользователя	Внутренний/внешний нарушитель с низким потенциалом	-	-	+ (низкий)	высокая

Угроза «незаметного» добавления объектов	Внутренний нарушитель со средним потенциалом/Внешний нарушитель с низким потенциалом	+ (низкий)	-	+ (низкий)	низкая
Угроза приведения системы в состояние «отказ в обслуживании»	Внешний/внутренний нарушитель с низким потенциалом	-	+ (высокий)	-	высокая
Угроза использования LDAP-инъекции	Внутренний/внешний нарушитель с низким потенциалом	-	+ (высокий)	+ (низкий)	высокая

Угроза несанкционированного удаленного подключения	Внешний нарушитель с низким потенциалом	-	-	+ (низкий)	средняя
Угроза использования механизмов авторизации для повышения привилегий	Внешний/внутренний нарушитель с низким потенциалом	-	-	+ (низкий)	низкая
Угроза использования слабостей и особенностей протоколов сетевого/локального обмена данными	Внешний/внутренний нарушитель с низким потенциалом	-	-	+ (низкий)	низкая
Угроза несанкционированного доступа к аутентификационной информации	Внешний/внутренний нарушитель с низким потенциалом	-	-	+ (низкий)	низкая

Угроза несанкционированного изменения аутентификационной информации	Внешний/внутренний нарушитель с низким потенциалом	+ (средний)	+ (высокий)	-	высокая
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Внешний нарушитель с низким потенциалом	-	-	+ (низкая)	низкая
Угроза обнаружения хостов	Внешний нарушитель с низким потенциалом	-	-	+ (низкая)	низкая
Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель с низким потенциалом	-	-	+ (низкая)	низкая

Приложение 3

Формулы для расчёта степени серьезности угрозы.

Базовые метрики:

ISS =	**1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]**
Impact =	
If Scope is Unchanged	6.42 × ISS
If Scope is Changed	$7.52 \times (ISS - 0.029) - 3.25 \times (ISS - 0.02)^{15}$
Exploitability =	8.22 × AttackVector × AttackComplexity ×
	PrivilegesRequired × UserInteraction
BaseScore =	
If Impact \<= 0	0, *else*
If Scope is Unchanged	Roundup (Minimum [(Impact + Exploitability), 10])
If Scope is Changed	Roundup (Minimum [1.08 × (Impact + Exploitability), 10])

Временные метрики:

TemporalScore =	**Roundup (BaseScore × ExploitCodeMaturity × RemediationLevel × ReportConfidence)**

Контекстные метрики:

MISS =	**Minimum (1 - [(1 - ConfidentialityRequirement × ModifiedConfidentiality) × (1 - IntegrityRequirement × ModifiedIntegrity) × (1 - AvailabilityRequirement × ModifiedAvailability)], 0.915)**
ModifiedImpact =	
If ModifiedScope is Unchanged	6.42 × MISS
If ModifiedScope is Changed	$7.52 \times (MISS - 0.029) - 3.25 \times (MISS \times 0.9731 - 0.02)^{13}$
ModifiedExploitability =	8.22 × ModifiedAttackVector × ModifiedAttackComplexity × ModifiedPrivilegesRequired × ModifiedUserInteraction

Ниже представлены принимаемые значения метрик и их числовой эквивалент.

Attack Vector (AV):

Network (N)	**Adjacent (A)**	**Local (L)**	**Physical (P)**
0.85	0.62	0.55	0.2

Attack Complexity(AC):

Low (L)	**High(H)**
0.77	0.44

Privileges Required(PR):

None(N)	**Low(L)**	**High(H)**
0.85	0.62 (or 0.68 if Scope is Changed)	0.27 (or 0.5 if Scope is Changed)

User Interaction(UI):

None(N)	**Required(R)**
0.85	0.62

Confidentiality / Integrity / Availability (C, I, A):

High(H)	**Low(L)**	**None(N)**
0.56	0.22	0

Exploit Code Maturity (E):

Not Defined(X)	**High(H)**	**Functional(F)**	**Proof of Concept(P)**	**Unproven(U)**
1	1	0.97	0.94	0.91

Remediation Level(RL):

Not Defined(X)	Unavailable(U)	Workaround (W)	Temporary Fix (T)	Official Fix(O)
1	1	0.97	0.96	0.95

Report Confidence(RC):

Not Defined(X)	Confirmed (C)	Reasonable(R)	Unknown(U)
1	1	0.96	0.92

Confidentiality Requirement / Integrity Requirement / Availability Requirement(CR, IR, AR):

Not Defined(X)	High(H)	Medium(M)	Low(L)
1	1.5	1	0.5