**Содержание**

[**Рекомендации по защите службы каталогов Active Directory** 2](#_Toc178590314)

[Повышение безопасности службы Kerberos 2](#_Toc178590315)

[Рекомендации по повышению безопасности: 3](#_Toc178590316)

[Повышение безопасности учетных записей 5](#_Toc178590317)

[Рекомендации по повышению безопасности: 5](#_Toc178590318)

[Повышение безопасности центра сертификации 6](#_Toc178590319)

[Рекомендации по усилению защищенности: 7](#_Toc178590320)

[**Защита от основных типов атак в среде Active Directory** 9](#_Toc178590321)

[Credential dumping 9](#_Toc178590322)

[Kerberoasting 10](#_Toc178590323)

[DCSync 11](#_Toc178590324)

[DCShadow 12](#_Toc178590325)

[Pass-the-hash, overpass-the-hash (pass-the-key) и pass-the-ticket 13](#_Toc178590326)

[Golden ticket 14](#_Toc178590327)

[Silver ticket 15](#_Toc178590328)

[AS-REP roasting 16](#_Toc178590329)

[NTLM relay 18](#_Toc178590330)

[sAMAccountName spoofing 19](#_Toc178590331)

[Shadow credentials 20](#_Toc178590332)

[Атаки на службы сертификатов 21](#_Toc178590333)

[ShadowCoerce 24](#_Toc178590334)

# **Рекомендации по защите службы каталогов Active Directory**

Необходимо знать слабые места своей инфраструктуры, а также тактики и техники злоумышленников (MITRE ATT&CK), которые они используют, чтобы атаковать организации. Эти техники постоянно меняются и развиваются, а значит, следует не только отслеживать деятельность хакеров, но и проверять инфраструктуру компании, устраивая периодические тестирования и участвуя в программах bug bounty.

Атака злоумышленника на инфраструктуру часто затрагивает систему каталогов Active Directory (AD). Компрометация AD – один из шагов на пути развития атаки на пути к целевой системе. К компрометации домена может привести ряд факторов, таких как пробелы в разворачивании антивирусной защиты, запоздалое обновление приложений, операционных систем и их компонентов, неправильная конфигурация систем.

## Повышение безопасности службы Kerberos

Служба AD использует протокол Kerberos для аутентификации и авторизации пользователей и сетевых служб. Протокол обладает особенностями, используя которые злоумышленник может осуществить успешную атаку. Ниже приведены примеры популярных атак в доменной инфраструктуре с использованием Kerberos.

**Атака Golden Ticket.** Злоумышленник с правами администратора домена может создать билет Kerberos с максимальным уровнем привилегий и с очень длинным сроком действия. В итоге злоумышленник может получить возможность аутентифицироваться под любым пользователем домена, длительное время находиться и скрытно передвигаться по доменной инфраструктуре.

**Атака Silver Ticket.** Злоумышленник с привилегиями пользователя домена со скомпрометированного узла может создать билет Kerberos для доступа к конкретному сервису или ресурсу без знания пароля. В итоге злоумышленник может получить доступ к указанному сервису или ресурсу.

**Атака Kerberoasting.** Злоумышленник с привилегиями пользователя домена может запросить билет TGS (Ticket Granting Service) ко всем SPN (Service Principal Name) в домене. В итоге злоумышленник может получить пароль сервисной учетной записи.

**Атака ShadowCoerce.** Злоумышленник без прав в доменной инфраструктуре через общедоступный [эксплойт](https://github.com/ShutdownRepo/ShadowCoerce) может проэксплуатировать уязвимость протокола MS-FSRVP службы теневого копирования (VSS) Active Directory. В итоге злоумышленник может получить учетную запись с правами контроллера домена.

**Атака Shadow Credentials.** Злоумышленник без прав в доменной инфраструктуре может использовать атрибут msDS-KeyCredentialLink для компрометации атакуемой учетной записи Active Directory. В итоге злоумышленник может получить доступ к доменной учетной записи.

**Атака AS-REP Roasting.** Злоумышленник без прав в доменной инфраструктуре может осуществить поиск учетной записи, для которой установлено свойство Do not require Kerberos preauthentication, и далее запросить билет Kerberos. В итоге злоумышленник может получить билет Kerberos для учетной записи, с помощью которого может быть получен пароль соответствующей учетной записи.

**Атака sAMAccountName spoofing**. Злоумышленник без прав в доменной инфраструктуре может использовать уязвимости «Подмена имени в Active Directory» (Name impersonation, [CVE-2021-42278](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42278)) и «Подделка запросов к службе KDC» (KDC bamboozling, [CVE-2021-42287](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42287)) для создания учетной записи с именем, похожим на имя легитимной учетной записи в Active Directory. В итоге злоумышленник может получить доступ к ресурсам, предназначенным для легитимной учетной записи.

**Неограниченное делегирование Kerberos.** Злоумышленник, обладающий привилегированным доступом на скомпрометированном узле, на котором разрешено неограниченное делегирование, может использовать данный механизм протокола Kerberos для получения доступа к ресурсам без знания пароля. В итоге злоумышленник может получить доступ к ресурсам, для которых настроено делегирование.

## Рекомендации по повышению безопасности:

* не применять в инфраструктуре устаревшие версии операционных систем и программного обеспечения;
* настроить для протокола Kerberos использование алгоритма шифрования AES вместо RC4;
* осуществлять проверку подлинности сертификата атрибутов привилегий (Privilege Attribute Certificate, PAC) для билетов TGS;
* использовать сложные и длинные (не менее 25 символов) пароли для сервисных учетных записей и регулярно их менять. Использовать MFA для всех пользователей домена;
* использовать механизм управляемых учетных записей служб ([Managed Service Accounts](https://blogs.technet.microsoft.com/ru_forum_support/2010/11/25/753/" \t "_blank), MSA). MSA поддерживает ряд основных сервисов и служб, применяемых в корпоративной инфраструктуре (например, IIS, AD LDS, SQL Server, MS Exchange). Этот механизм автоматически меняет пароли, генерирует комплексный случайный пароль из 240 символов, что значительно повышает сложность подбора пароля, а с учетом смены пароля по умолчанию раз в 30 дней — делает подбор почти невозможным;
* придерживаться принципа минимальных привилегий для всех типов учетных записей, включая привилегии, получаемые в результате членства в группах, например в группе администраторов домена;
* ограничить привилегии администратора домена контроллерами домена и отдельными серверами. Выделить под остальные административные функции отдельные учетные записи;
* установить минимально возможную периодичность смены пароля для учетной записи krbtgt;
* отключить на контроллерах домена службу теневого копирования (VSS) с помощью консоли управления;
* использовать механизмы EPA (Extended Protection for Authentication) и SSO (single sign-on) совместно с MFA для защиты узлов/ресурсов от атаки ShadowCoerce;
* обеспечить подпись SMB-пакетов со стороны как серверов, так и клиентов во всей доменной инфраструктуре;
* запретить участникам группы Everybody изменять атрибут msDS-KeyCredentialLink для любой учетной записи в домене. Если это по какой-то причине невозможно выполнить, организовать такой запрет для привилегированных учетных записей;
* настроить аудит всего входящего управления объектами для учетных записей с высоким уровнем привилегий;
* использовать механизм [Flexible Authentication Secure Tunneling](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831747(v=ws.11)) (FAST, Kerberos armoring) для усиления защиты аутентификации и обмена TGS-билетами. Этот механизм обеспечивает защищенный канал связи между клиентом Kerberos и центром распространения ключей;
* настроить регулярное обновление службы AD и ее компонентов. Следует организовать предварительное тестирование обновлений перед их установкой;
* определить учетные записи, для которых отключена предварительная аутентификация, и, если возможно, активировать ее;
* не использовать неограниченное делегирование. Вместо этого настроить ограниченное делегирование, поскольку серверы с ограниченным делегированием хранят только Service Ticket (ST), а не TGT;
* для привилегированных учетных записей включить параметр Account is sensitive and cannot be delegated;
* использовать группу Protected Users. Начиная с Windows Server 2012 члены этой группы не могут быть делегированы;
* провести в инфраструктуре аудит учетных записей, обладающих правами на запись атрибута msDS-AllowedToActOnBehalfOfOtherIdentity, и оставить эту привилегию только для тех учетных записей, которым она необходима;
* проводить аудит информационной безопасности домена с помощью [PingCastle](https://www.pingcastle.com/) или его аналогов.

## Повышение безопасности учетных записей

AD позволяет реализовать централизованное управление пользовательскими и сервисными учетными записями, включая предоставление прав доступа к ресурсам организации. Ниже приведены типичные ошибки при настройке доступа к ресурсам доменной инфраструктуры, а также рекомендации по их устранению.

**Использование одинаковых учетных данных.** Злоумышленник, получивший информацию об идентификаторе и пароле пользователя одного ресурса, может получить доступ к другим.

**Небезопасное использование встроенных групп.** Злоумышленник, получивший доступ к учетной записи, состоящей в группах Account Operators или Organization Management, может осуществить компрометацию домена.

**Недостаточные ограничения на создание учетных записей рабочих станций.** Злоумышленник, получивший учетные данные пользователя, способного создавать учетные записи рабочих станций, может использовать это для проведения дальнейших атак.

**Недостаточный контроль прав доступа.** Злоумышленник, использующий учетные записи пользователей домена, обладающих избыточной привилегией AllExtendedRights, может получить полный контроль над различными узлами ЛВС, так как указанная привилегия позволяет среди прочего с помощью специальных запросов к службе Active Directory получить пароли локальных администраторов ряда узлов.

## Рекомендации по повышению безопасности:

* не использовать одинаковые учетные данные для доступа к различным ресурсам. Установить стойкие пароли для доступа к ресурсам. Использовать двухфакторную аутентификацию для доступа к критически важным ресурсам. Реализовать строгую парольную политику;
* для централизованного управления паролями локальных администраторов в доменной инфраструктуре рекомендуется использовать Local Administrator Password Solution (LAPS). С помощью LAPS можно настроить автоматическую генерацию паролей локальных администраторов для каждого узла в домене, а также установить расписание их смены. При настройке LAPS важно ограничить возможность получения учетных данных из LAPS для непривилегированных пользователей домена;
* удалить учетные записи из групп Account Operators и Organization Management, не использовать их для делегированного администрирования. Для удаления членов группы можно воспользоваться утилитой из пакета [AD\_Sec\_Tools](https://github.com/davidprowe/AD_Sec_Tools/tree/master/AD_User_AccountOpsCleanup);
* обнулить значение атрибута MachineAccountQuota, определяющего, какое количество учетных записей рабочих станций может создать пользователь в домене. Для этого необходимо выполнить следующую команду: Set-ADDomain (Get-ADDomain) .distinguishedname -Replace @{"ms-ds-MachineAccountQuota"="0"}.

## Повышение безопасности центра сертификации

Центр сертификации (certification authority, CA) обеспечивает выдачу и управление сертификатами для аутентификации узлов, пользователей и других объектов в AD. *Ниже приведены примеры ошибок конфигурации центра сертификации*, которые злоумышленник может использовать для проведения атаки, а также рекомендации по их исправлению и повышению общего уровня безопасности CA.

**Небезопасная конфигурация CA-сервера.** Наличие флага EDITF\_ATTRIBUTESUBJECTALTNAME2 позволяет задать произвольное альтернативное имя субъекта (Subject Alternative Name, SAN) для всех сертификатов, несмотря на конфигурацию шаблона сертификата. Злоумышленник с привилегиями пользователя домена может выбрать любой шаблон сертификата, который разрешает аутентификацию клиента, доступный в том числе другим непривилегированным пользователям (например, шаблон User по умолчанию), и получить с его помощью привилегии администратора домена (или любого другого активного пользователя / учетной записи рабочей станции).

**Небезопасная конфигурация шаблона сертификата.** Шаблон сертификата Template на узле может содержать известные недостатки конфигурации, которые позволяют злоумышленнику получить сертификат на имя любой учетной записи путем указания альтернативного имени.

**Небезопасное использование веб-служб в центре сертификации.** Если в центре сертификации настроена веб-служба регистрации сертификатов Web Enrollment и при этом на веб-сервере Microsoft IIS не используется Extended Protection forAuthentification, то в случае, если доступен подходящий шаблон сертификата, возможно использование NTLM-аутентификации учетной записи рабочей станции для получения сертификата доступа к этой рабочей станции.

**Небезопасные права доступа к шаблону сертификата.** Если пользователям группы Authenticated Users доступны права на изменение владельца шаблона (право WriteOwner), права доступа к шаблону (право WriteDACL), а также право изменять любые свойства шаблона сертификата (право WriteProperty), злоумышленник может воспользоваться такой учетной записью, чтобы изменить конфигурацию шаблона для дальнейшего развития атаки.

## Рекомендации по усилению защищенности:

* отключить на CA-сервере использование флага EDITF\_ATTRIBUTESUBJECTALTNAME2. Если этот флаг необходим, рекомендуется использовать функции подтверждения запросов диспетчером центра сертификации и подписания запросов авторизованным сертификатом;
* если нет необходимости получать альтернативное имя в запросе шаблона сертификата, эту опцию следует отключить. Если указание альтернативного имени в запросе является необходимым, то рекомендуется:
  + ограничить список пользователей, которые могут использовать этот шаблон;
  + убедиться, что шаблон сертификата не содержит избыточных целей Extended Key Usage (EKU);
  + если не требуется сопоставление альтернативного имени субъекта с учетной записью домена при Kerberos-аутентификации, рекомендуется отключить эту возможность. Для этого необходимо задать нулевое значение ключа реестра UseSubjectAltName в ветке HKLM\SYSTEM\CurrentControlSet\Services\Kdc на всех контроллерах домена. В этом случае злоумышленник сможет указать альтернативное имя в запросе на получение сертификата, но не сможет использовать альтернативное имя при аутентификации;
* для снижения риска проведения подобных атак в центре сертификации рекомендуется реализовать меры, подготовленные компанией [Microsoft](https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429);
* рассмотреть возможность отключения веб-службы регистрации сертификатов Web Enrollment;
* рассмотреть возможность отключения аутентификации с использованием протокола NTLM;
* настроить Extended Protection for Authentication на веб-сервере Microsoft IIS;
* пересмотреть права доступа и убедиться, что такие разрешения безопасности, как WriteOwner, WriteDACL, WriteProperty, FullControl и Owner, выданы только ограниченному числу привилегированных пользователей;
* реализовать контроль за хранением сертификатов в файловых системах;
* провести аудит информационной безопасности всех шаблонов сертификатов для устранения известных недостатков конфигурации. Для этого могут быть использованы следующие утилиты:
  + PSPKIAudit Invoke-PKIAudi;
  + Certify Certify.exe find /vulnerable [/hideAdmins];
  + Certutil certutil.exe -TCAInfo (вывод шаблонов сертификатов) certutil.exe -v –dsTemplate (вывод разрешений шаблонов).

Уровень защиты системы Active Directory от атак злоумышленников неразрывно связан с реализацией парольной политики и системы мониторинга событий ИБ в организации.

# **Защита от основных типов атак в среде Active Directory**

## Credential dumping

Credential dumping — метод, при котором хакеры извлекают учетные данные из памяти системы или из файловой системы. Он часто используется для получения хеш-сумм паролей, токенов аутентификации и других учетных данных, которые могут быть применены в ходе дальнейших атак, таких как pass-the-hash, pass-the-ticket и др. Как правило, credential dumping выполняется с использованием специальных инструментов (например, mimikatz), которые позволяют извлекать учетные данные из памяти LSASS, ветвей реестра и других источников. Примеры источников получения учетных данных:

1. LSASS (Local Security Authority Subsystem Service). Это процесс в Windows, который управляет политиками безопасности и хранит в памяти различные аутентификационные данные.
2. SAM и SYSTEM. В Windows учетные данные могут храниться в ветках реестра SAM (Security Account Manager) и SYSTEM. Получив доступ к этим веткам, хакер может извлечь хеш-суммы паролей и подобрать их.
3. Cached credentials. Windows хранит кэшированные учетные данные, которые хакер также может извлечь. Учетные данные кэшируются для того, чтобы мы имели доступ к нашим компьютерам даже без постоянного подключения к сети.

**Рекомендации:**

* Минимизация прав доступа учетных записей, имеющих доступ к процессу LSASS, предоставляя административные права только тем сотрудникам, которым это действительно необходимо для выполнения рабочих задач.
* Внедрение политики использования сложных паролей и требуйте их регулярной смены, уделяя особое внимание административным учетным записям.
* Защита ветки реестра SAM и SYSTEM, ограничив доступ к ним только доверенными учетными записями. Это поможет предотвратить извлечение хеш-сумм паролей и их подбор.
* Отключить сохранение паролей пользователей в системе LSA. Для этого параметру реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\disabledomaincreds присвоить значение 1.
* Рассмотреть возможность запрета использования кэшированных данных для доступа к узлам домена. Для этого параметру реестра HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount присвойте значение 0.
* Осуществлять мониторинг обращений к следующим разделам реестра: HKEY\_LOCAL\_MACHINE\SAM, HKEY\_LOCAL\_MACHINE\SECURITY, HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets (включая подразделы) и HKEY\_LOCAL\_MACHINE\SYSTEM. При настройке мониторинга через групповые политики Active Directory, при обращении к ветви реестра на контроллере домена будут регистрироваться события [4656](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4656) (A handle to an object was requested).
* Отслеживать запуск процессов и использование аргументов командной строки для выполнения утилит, которые могут указывать на извлечение учетных данных.

## Kerberoasting

Kerberos — это протокол, который используется для безопасной аутентификации пользователей и служб в Active Directory (AD). Он основан на использовании секретных ключей и билетной системе. Когда пользователь хочет получить доступ к какому-либо ресурсу, он сначала проходит аутентификацию на сервере, который выдает ему билет. Затем этот билет используется для доступа к ресурсу без необходимости повторной аутентификации. Kerberoasting — это атака на протокол аутентификации Kerberos, которая позволяет получить пароли доменных пользователей. Она состоит из нескольких шагов:

1. **Сбор информации об учетных записях, обладающих доступом к целевому ресурсу.** Это могут быть учетные записи сервисов, приложений и т. д.
2. **Запрос билетов для сервисных учетных записей.** Хакер отправляет запрос на выдачу билета для сервисной учетной записи. В ответ он получает билет, который зашифрован с использованием хеш-суммы пароля этой учетной записи.
3. **Локальный взлом хеш-суммы и получение пароля.** Хакер экспортирует полученный билет на локальный компьютер, взламывает хеш-сумму и получает пароль.

**Рекомендации:**

* Реализовать строгую парольную политику и смените используемые словарные пароли. Используйте двухфакторную аутентификацию для привилегированных пользователей домена Active Directory. Для сервисных учетных записей применяйте сложные и длинные пароли (не менее 25 символов) и регулярно меняйте их.
* Внедрить механизм [«Групповых управляемых учетных записей служб»](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/group-managed-service-accounts-overview) (group managed service accounts, gMSA). Этот механизм поддерживает основные сервисы и службы, используемые в корпоративной инфраструктуре, такие как IIS, AD LDS, SQL Server, MS Exchange. gMSA автоматически меняет пароли, генерируя сложные случайные пароли длиной до 240 символов, что значительно затрудняет их подбор. Пароли меняются по умолчанию каждые 30 дней — их подбор практически невозможен.
* Использовать механизм [flexible authentication secure tunneling](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831747(v=ws.11)) (FAST, Kerberos armoring) для усиления защиты аутентификации и обмена TGS-билетами. Этот механизм обеспечивает защищенный канал связи между клиентом Kerberos и центром распространения ключей (key distribution center, KDC).
* Придерживаться принципа минимальных привилегий для сервисных учетных записей, включая привилегии, получаемые в результате членства в группах (таких, как группа администраторов домена).
* Настроить использование алгоритма шифрования AES (или другого надежного алгоритма) для протокола Kerberos вместо RC4.
* Для обнаружения атак в инфраструктуре включить в Active Directory мониторинг запрашиваемых билетов Kerberos (Audit Kerberos Service Ticket Operations) и ищите пользователей с избыточными событиями [4769](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769) (A Kerberos service ticket was requested). Используйте метод SPN honeypot, который заключается в создании учетной записи и SPN, которые никогда не будут использоваться (SPN не связан ни с одним реальным приложением). Появление в журнале безопасности контроллера домена события 4769 будет свидетельствовать о попытке проведения атаки типа Kerberoasting.
* Проводить регулярный аудит безопасности домена с помощью ПО [PingCastle](https://www.pingcastle.com/).

## DCSync

DCSync — это атака, которая применяется хакерами для получения учетных данных из базы данных домена Active Directory. Она использует возможности протокола репликации AD, который предназначен для синхронизации данных между контроллерами домена. Хакеры могут имитировать контроллер домена и запросить у настоящего контроллера домена информацию об учетных записях. Основные этапы атаки:

1. **Получение привилегированного доступа.** Для проведения атаки хакеру нужно получить привилегированную учетную запись.
2. **Имитация контроллера домена.** Могут использоваться инструменты типа mimikatz, чтобы отправить команды репликации на контроллер домена.
3. **Получение учетных данных.** Контроллер домена отправляет учетные данные (включая хеш-суммы паролей) хакеру.

DCSync позволяет атакующему получить доступ к хеш-суммам паролей всех пользователей домена, включая учетные записи с высокими привилегиями. Злоумышленник может использовать эти хеш-суммы для проведения других атак, таких как pass-the-hash или golden ticket, чтобы обеспечить себе неограниченный доступ к ресурсам домена. Рекомендации:

* Осуществлять мониторинг запросов протокола DRSUAPI с операцией DsGetNCChanges (opcode 3) от серверов, не являющихся легитимными участниками процесса репликации. В журнале Security на контроллерах домена и в событиях аудита [4662](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4662) (An operation was performed on an object) необходимо отслеживать использование привилегий Replicating Directory Changes, Replicating Directory Changes All и Replicating Directory Changes In Filtered Set. Для обнаружения источника атаки следует коррелировать события 4662 и [4624](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624) (An account was successfully logged on) с одинаковыми идентификаторами входа.
* Включить в Active Directory мониторинг событий [4932](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4932) (Synchronization of a replica of an Active Directory naming context has begun) и [4937](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4937) (Replication failure begins) для обнаружения атак типа DCSync.
* Дополнительно проводить аудит безопасности домена.

## DCShadow

Атака DCShadow позволяет злоумышленникам регистрировать новый контроллер домена в AD и использовать его для внесения скрытых изменений в конфигурацию AD. В обычных условиях только легитимные контроллеры домена могут вносить изменения в конфигурацию AD, но DCShadow позволяет обойти этот механизм. Хакеры могут зарегистрировать свой собственный контроллер домена и использовать его для изменения данных в AD (например, для изменения атрибутов учетных записей пользователей или групп). Основные этапы атаки:

1. **Получение привилегированного доступа.** Для проведения атаки хакеру нужно получить привилегированную учетную запись.
2. **Имитация контроллера домена.** Хакер создает и регистрирует в инфраструктуре AD поддельный контроллер домена.
3. **Внесение и синхронизация изменений в AD.** Хакер, используя поддельный контроллер домена, вносит изменения в AD, которые затем распространяются на остальные контроллеры домена. Эти изменения могут включать в себя добавление новых пользователей, повышение привилегий существующих пользователей, создание новых групп или изменение политик безопасности. Поскольку механизм репликации AD доверяет всем зарегистрированным контроллерам домена, то изменения, внесенные поддельным контроллером домена, быстро распространятся по всей инфраструктуре.

**Рекомендации:**

* Отслеживать события регистрации новых контроллеров домена — [5137](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5137) (A directory service object was created) и [5141](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5141) (A directory service object was deleted).
* В журнале Security на контроллерах домена и в событиях аудита [4662](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4662) (An operation was performed on an object) отслеживать операции с привилегиями Domain Admin или Enterprise Admin, а также изменения в конфигурации домена. Для выявления источника атаки необходимо коррелировать события 5137 и 4662 с одинаковыми идентификаторами входа и временем.
* Дополнительно рекомендуется включить мониторинг событий [4929](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4929) (An Active Directory replica source naming context was established) и [4930](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4930) (An Active Directory replica source naming context was removed) для отслеживания изменений в конфигурации репликации.
* Также рекомендуется регулярно проводить аудит безопасности домена с помощью ПО [PingCastle](https://www.pingcastle.com/).

## Pass-the-hash, overpass-the-hash (pass-the-key) и pass-the-ticket

**Pass-the-hash (PtH)** — это техника, используемая хакерами для получения несанкционированного доступа к сетевым ресурсам. Основа техники заключается в том, что вместо пароля злоумышленник использует для аутентификации хеш-сумму этого пароля. Когда пользователь входит в систему, его пароль преобразуется в хеш-сумму. Эта хеш-сумма используется для аутентификации, чтобы доказать, что пользователь знает пароль, не передавая его напрямую. Если хакер получает доступ к этим хеш-суммам, он может использовать их для аутентификации без необходимости вводить исходный пароль. **Overpass-the-hash (pass-the-key)** — атака, при которой хакер использует хеш-сумму пароля для создания билета Kerberos и последующей аутентификации по нему. Если overpass-the-hash (pass-the-key) использует хеш-сумму пароля для создания новых билетов Kerberos, то **pass-the-ticket** использует для аутентификации ранее сгенерированные Kerberos билеты.

**Рекомендации:**

* Включить мониторинг событий аутентификации. В журнале Security на контроллерах домена и серверах следует отслеживать события [4624](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624) (An account was successfully logged on) и [4625](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625) (An account failed to log on) с целью выявления подозрительных попыток входа. Особое внимание следует уделять событиям, связанным с использованием NTLM и Kerberos.
* Отслеживать события [4768](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768) (A Kerberos authentication ticket was requested), [4769](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769) (A Kerberos service ticket was requested) и [4770](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4770) (A Kerberos service ticket was renewed) для выявления аномалий в запросах билетов Kerberos. Корреляция этих событий с одинаковыми идентификаторами входа и IP-адресами может помочь обнаружить источник атаки.
* Ограничить использование NTLM, по возможности отключите его и используйте Kerberos для аутентификации.
* Использовать двухфакторную аутентификацию для доступа к критически важным системам.
* Регулярно проводить аудит безопасности домена с помощью ПО [PingCastle](https://www.pingcastle.com/).

## Golden ticket

Golden ticket — это атака, при которой злоумышленник создает поддельный билет Kerberos (TGT) с целью получения неограниченного доступа к ресурсам домена. Проведение атаки возможно благодаря получению хеш-суммы пароля учетной записи krbtgt, которая является учетной записью службы Kerberos ticket-granting service. Основные этапы атаки:

1. **Получение хеш-суммы пароля учетной записи krbtgt.** Это специальная учетная запись в Active Directory, которая отвечает за выдачу и проверку билетов Kerberos.
2. **Создание поддельного билета Kerberos.** Для этого хакер использует хеш-сумму пароля krbtgt.
3. **Получение доступа ко всем ресурсам домена** с использованием TGT.

Golden ticket — одна из самых мощных атак на Active Directory: она предоставляет злоумышленнику практически неограниченный доступ к ресурсам домена. Хакер может аутентифицироваться от имени любой учетной записи, включая учетные записи с самыми высокими привилегиями.

**Рекомендации:**

* Настроить для протокола Kerberos использование алгоритма шифрования AES (или другого надежного алгоритма) вместо RC4.
* Ограничить привилегии администратора домена, предоставив их только контроллерам домена и отдельным серверам. Для остальных административных функций создайте отдельные учетные записи.
* Осуществлять мониторинг подозрительной активности, такой как использование шифрования RC4 внутри TGT (ticket-granting ticket), а также запросы TGS (ticket-granting service) без предшествующего запроса TGT.
* Отслеживать время жизни билетов TGT для выявления отклонений от значений, установленных по умолчанию в домене.
* Осуществлять мониторинг аномальных событий Kerberos-аутентификации, содержащих вредоносные или пустые поля. Для этого рекомендуется отслеживать события [4624](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624) (An account was successfully logged on), [4634](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4634) (An account was logged off) и [4672](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4672) (Special privileges assigned to new logon).
* В случае если атака golden ticket была осуществлена, для предотвращения ее последствий **рекомендуется дважды сбросить пароль** служебной учетной записи krbtgt. Это приведет к аннулированию всех существующих «золотых билетов», полученных с использованием хеш-суммы NT учетной записи krbtgt, а также остальных билетов, полученных на ее основе. Кроме того, следует установить максимально возможную частоту смены пароля для учетной записи krbtgt.

## Silver ticket

Silver ticket — это атака, при которой злоумышленник создает поддельный билет на конкретную службу, а не на весь домен. В отличие от golden ticket, который предоставляет доступ ко всему домену, silver ticket позволяет атакующему получить доступ только к конкретным сервисам, например к файловым серверам или веб-приложениям. Эта атака менее заметна, чем golden ticket, так как нацелена на конкретные службы и может оставаться незамеченной стандартными средствами мониторинга. Основные этапы атаки:

1. **Получение хеш-суммы пароля учетной записи службы.** Сначала хакер получает хеш-сумму пароля учетной записи службы (service account).
2. **Создание поддельного service ticket.** Используя полученную хеш-сумму, злоумышленник создает поддельный service ticket. Он содержит имя пользователя, список групп и другие атрибуты, которые определяют уровень доступа к ресурсу. Поддельный билет подписывается хеш-суммой пароля учетной записи службы.
3. **Получение доступа к целевой службе.** Злоумышленник отправляет поддельный service ticket на сервер службы, который считает этот билет легитимным и предоставляет хакеру доступ к запрашиваемому ресурсу.

**Рекомендации:**

* Использование сервисных билетов является легитимным действием в системе, поэтому в первую очередь необходимо выполнить действия, рекомендованные для предотвращения или усложнения получения учетных данных пользователей доменов, от имени которых возможен запрос сервисных билетов к значимым узлам и ресурсам.
* Не применять в инфраструктуре устаревшие версии операционных систем и программного обеспечения, не поддерживающие современные методы аутентификации.
* Настроить для протокола Kerberos использование алгоритма шифрования AES вместо RC4.
* Осуществлять проверку подлинности сертификата атрибутов привилегий (Privilege Attribute Certificate, PAC) для билетов TGS.
* Использовать сложные и длинные (не менее 25 символов) пароли для сервисных учетных записей для защиты от подбора, а также регулярно производите их смену.
* Использовать механизм [«Управляемых учетных записей служб»](https://learn.microsoft.com/en-us/archive/blogs/ru_forum_support/753) (Managed Service Accounts). MSA поддерживает основные сервисы и службы, применяемые в корпоративной инфраструктуре (например, IIS, AD LDS, SQL Server, MS Exchange). Этот механизм автоматически производит смену паролей, генерирует комплексный случайный пароль из 240 символов, что значительно повышает сложность подбора пароля, а с учетом смены пароля по умолчанию раз в 30 дней — делает подбор практически невозможным.
* Придерживаться принципа минимальных привилегий для сервисных учетных записей, включая привилегии, получаемые в результате членства в группах, например в группе администраторов домена.
* Осуществлять мониторинг аномальных событий Kerberos-аутентификации, содержащих вредоносные или пустые поля. Для этого рекомендуется отслеживать события [4624](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624) (An account was successfully logged on), [4634](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4634) (An account was logged off) и [4672](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4672) (Special privileges assigned to new logon).
* Осуществлять мониторинг аномальных обращений к процессу lsass.exe на рабочих станциях и серверах. Общедоступные инструменты, предназначенные для снятия дампа учетных записей (например, ПО mimikatz), позволяют злоумышленнику, получившему доступ к процессу LSASS (Local Security Authority Subsystem Service), узнать секретный ключ LSA и расшифровать разделы памяти, где хранится информация об учетных записях, в том числе билеты Kerberos.

## AS-REP roasting

AS-REP roasting представляет собой атаку на протокол аутентификации Kerberos, направленную на получение хеш-сумм паролей учетных записей, которые не защищены предварительной аутентификацией (pre-authentication). Этот тип атаки позволяет злоумышленникам извлекать хеш-суммы паролей учетных записей и использовать их для дальнейших атак на систему. Центральным компонентом в Kerberos является центр распространения ключей (key distribution center, KDC), который состоит из двух основных служб — authentication service (AS) и ticket-granting service (TGS). Процесс аутентификации пользователя включает следующие этапы:

1. **Authentication service request (AS-REQ).** Пользователь отправляет запрос на аутентификацию, содержащий его имя и метку времени, зашифрованную с использованием его пароля.
2. **Authentication service response (AS-REP).** KDC проверяет учетные данные пользователя и возвращает зашифрованный ticket-granting ticket (TGT), который пользователь может использовать для получения доступа к другим ресурсам.

В обычных условиях процесс предварительной аутентификации (pre-authentication) требует, чтобы пользователь предоставил доказательства своей «подлинности» перед выдачей TGT. Однако, если предварительная аутентификация отключена, KDC сразу и без дополнительной проверки отправляет AS-REP, содержащий зашифрованный TGT. Основные этапы атаки:

1. **Поиск уязвимых учетных записей.** Для этого хакер отправляет LDAP-запросы к контроллерам домена, чтобы выявить учетные записи, не защищенные предварительной аутентификацией.
2. **Отправка запроса AS-REQ.** Злоумышленник отправляет AS-REQ к KDC от имени уязвимой учетной записи.
3. **Получение AS-REP.** KDC отвечает сообщением AS-REP, содержащим зашифрованный TGT.
4. **Взлом хеш-суммы.** Хакер извлекает зашифрованную часть AS-REP, взламывает хеш-сумму и получает пароль.

**Рекомендации:**

* Использовать двухфакторную аутентификацию для привилегированных пользователей домена Active Directory. Для сервисных учетных записей используйте сложные и длинные пароли (не менее 25 символов), а также регулярно меняйте их.
* Применять механизм [«Управляемых учетных записей служб»](https://learn.microsoft.com/ru-ru/archive/blogs/ru_forum_support/753) (managed service accounts, MSA). MSA поддерживает ряд основных сервисов и служб, используемых в корпоративной инфраструктуре (например, IIS, AD LDS, SQL Server, MS Exchange). Этот механизм автоматически меняет пароли, генерируя сложные случайные пароли длиной до 240 символов, что значительно усложняет подбор пароля. Смена пароля по умолчанию раз в 30 дней делает подбор практически невозможным.
* Определять учетные записи, для которых отключена предварительная аутентификация, и, если возможно, активируйте ее.
* Настроить для протокола Kerberos использование алгоритма шифрования AES (или другого надежного алгоритма) вместо RC4.
* Осуществлять мониторинг событий изменения значения UAC, которые отражают отключение предварительной аутентификации. Для этого следует отслеживать события [4738](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4738) (A user account was changed) и [5136](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5136) (A directory service object was modified).
* Проводить мониторинг запрашиваемых билетов Kerberos (Audit Kerberos Service Ticket Operations) и определяйте учетные записи с избыточными событиями [4768](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768) (A Kerberos authentication ticket (TGT) was requested) и [4769](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4769) (A Kerberos service ticket was requested), в дополнительных параметрах которых указан тип шифрования RC4 (ticket encryption type — 0x17) и не требуется предварительная аутентификация (pre-authentication type — 0x0).
* Проводить аудит безопасности домена.

## NTLM relay

NTLM relay — это атака, при которой злоумышленник перехватывает и перенаправляет учетные данные для аутентификации на другом сервере. Эта атака эксплуатирует уязвимости в протоколе NTLM, который позволяет передавать учетные данные на другой сервер без их расшифрования. Когда пользователь пытается получить доступ к ресурсу (например, файлу или принтеру) в сети, NTLM использует серию сообщений между клиентом (устройством пользователя) и сервером для проверки подлинности. Этот процесс включает в себя три основные шага:

1. **Negotiate.** Клиент отправляет запрос на сервер на установление соединения по протоколу NTLM.
2. **Challenge.** Сервер отвечает случайным числом.
3. **Authenticate.** Клиент хеширует это случайное число вместе с хешированным паролем пользователя и отправляет обратно серверу.

**Основные этапы атаки:**

1. **Перехват трафика.** Хакер перехватывает сетевой трафик, содержащий учетные данные.
2. **Передача аутентификационных данных.** Вместо взлома аутентификационных данных злоумышленник просто перенаправляет их на целевой сервер. Таким образом, он использует легитимные аутентификационные данные для получения доступа к другому ресурсу.
3. **Доступ к целевому ресурсу.** Если атака прошла успешно, то хакер получает доступ к целевому ресурсу.

**Рекомендации:**

* Отключить протокол WPAD. Для этого измените значение параметра Start с 3 на 4 в ветке реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WinHttpAutoProxySvc. Если необходима автоматическая настройка параметров прокси, укажите полный путь к конфигурационному PAC-файлу.
* Обеспечить [подпись](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always) SMB-пакетов как со стороны серверов, так и со стороны клиентов во всей доменной инфраструктуре.
* Обеспечить [подпись](https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/active-directory/enable-ldap-signing-in-windows-server) LDAP-пакетов и настройте [безопасную аутентификацию](https://support.microsoft.com/en-us/topic/kb4034879-use-the-ldapenforcechannelbinding-registry-entry-to-make-ldap-authentication-over-ssl-tls-more-secure-e9ecfa27-5e57-8519-6ba3-d2c06b21812e) протокола LDAP.
* Заблокировать протоколы LAN Manager и NTLMv1 на уровне групповых политик.
* Использовать механизм [Extended Protection for Authentication (EPA)](https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/).
* Для уменьшения площади атаки добавить пользователей с правами администратора в группу Protected Users и (или) установите для них атрибут Account is sensitive and cannot be delegated, что предотвратит делегирование полномочий. Также рекомендуется рассмотреть возможность перехода с NTLM-аутентификации на Kerberos-аутентификацию на всех узлах инфраструктуры.

## sAMAccountName spoofing

Атрибут sAMAccountName — это имя учетной записи пользователя или компьютера в Active Directory. Оно должно быть уникальным в пределах домена и служит для идентификации пользователя при входе в систему. Однако злоумышленник может провести атаку sAMAccountName spoofing, во время которой создаст учетную запись с таким же именем. В результате он сможет использовать эту учетную запись для получения несанкционированного доступа к ресурсу.

**Рекомендации:**

* Установить последние обновления безопасности [KB5008380](https://support.microsoft.com/ru-ru/topic/kb5008380-%D0%BE%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F-%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D0%BA%D0%B8-%D0%BF%D0%BE%D0%B4%D0%BB%D0%B8%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041) и [KB5008102](https://support.microsoft.com/ru-ru/topic/kb5008102-%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B9-%D0%B4%D0%B8%D1%81%D0%BF%D0%B5%D1%82%D1%87%D0%B5%D1%80%D0%B0-%D1%83%D1%87%D0%B5%D1%82%D0%BD%D1%8B%D1%85-%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-active-directory-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e).
* Для выявления атак включить мониторинг ошибок objectClass и UserAccountControl, а также ошибок проверки имени учетной записи SAM. Важно отслеживать событие [4741](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4741) (a computer account was created) и проверять наличие символа "$" в атрибуте sAMAccountName, а также событие [4742](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4742) (a computer account was changed) с аналогичной проверкой. Также следует мониторить событие [4743](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4743) (a computer account was deleted).
* Следует включить мониторинг запрашиваемых билетов Kerberos (Audit Kerberos Service Ticket Operations). Отслеживайте события, указывающие на то, что служба KDC обнаружила сервисный билет, не содержащий PAC, или билет с противоречивой информацией об учетной записи.
* Проводить аудит безопасности домена.

## Shadow credentials

Shadow credentials — это атака, которая позволяет хакеру изменить значения атрибута msDS-KeyCredentialLink атакуемой учетной записи. В результате проведения атаки хакер может добавить свой ключ в этот атрибут и использовать его для выпуска сертификата или запроса TGT, что обеспечит злоумышленнику легитимный доступ к целевым ресурсам. Основные этапы атаки: хакер получает административный доступ к системе, после чего модифицирует атрибут msDS-KeyCredentialLink атакуемой учетной записи, добавляя свои ключи или сертификаты для дальнейшей аутентификации под этой учетной записью.

**Рекомендации:**

* Запретить участникам группы Everyone изменять атрибут msDS-KeyCredentialLink для любой учетной записи в домене. Если по какой-либо причине это невозможно, необходимо организовать такой запрет для привилегированных учетных записей.
* Настроить аудит всех операций с объектами для учетных записей с высоким уровнем привилегий.
* Дополнительно провести аудит безопасности домена с помощью ПО [PingCastle](https://www.pingcastle.com/).
* Если в инфраструктуре (или для определенных пользователей) не используется механизм аутентификации PKINIT, следует осуществлять мониторинг события [4768](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768) (A Kerberos authentication ticket was requested) для выявления инцидентов, когда в атрибуты сертификата была внесена информация.
* Если список управления доступом к объектам (system access control list, SACL) настроен на аудит изменений объектов Active Directory для целевой учетной записи, событие [5136](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-5136) (A directory service object was modified) позволяет выявлять изменение атрибута msDS-KeyCredentialLink. Важно отметить, что если это действие будет выполняться от имени учетной записи Azure AD Connect synchronization или службы AD FS, то оно не будет зафиксировано как инцидент, поскольку данные типы пользователей имеют легитимные права на изменение этого атрибута.

## Атаки на службы сертификатов

Сертификаты в AD используются для различных целей, например для аутентификации пользователей, шифрования данных и построения безопасных соединений. Шаблоны сертификатов в AD — это наборы параметров, определяющих, как, кому и на что могут быть выданы сертификаты. Недостатки конфигурации шаблонов сертификатов могут использоваться хакерами для повышения привилегий.

**Существует несколько типов атак:**

* **Modifiable SAN (ESC1).** Хакер использует возможность изменения параметра SAN в шаблоне сертификата для создания сертификата с правами другого пользователя, включая администраторов.
* **Any or none purpose attack (ESC2).** Злоумышленник использует шаблон с универсальными правами для получения сертификатов, которые могут аутентифицировать любого пользователя. Эти шаблоны не требуют специфической цели использования (extended key usage), что позволяет использовать их для аутентификации любых пользователей, включая администраторов.
* **Enrollment agent (ESC3).** Атака через шаблон, который позволяет выпускать сертификаты от имени других пользователей. Злоумышленник получает сертификат Request Agent и затем использует его для создания сертификатов от имени учетных записей с высокими привилегиями.
* **Certificate ACL abuse (ESC4).** Хакер использует слабую настройку ACL (списков контроля доступа) для захвата прав на шаблоны сертификатов. Они позволяют изменять параметры шаблона, чтобы сделать его уязвимым для других атак, таких как ESC1, что позволит получить привилегированные сертификаты.
* **Vulnerable PKI object access control (ESC5).** Атака на другие объекты в инфраструктуре AD CS с уязвимыми параметрами доступа, которые могут позволить злоумышленнику компрометировать систему. Например, недостатки в конфигурации доступа к серверу CA могут быть использованы для выполнения операций с повышенными привилегиями.
* **Everything and for everyone (EDITF\_ATTRIBUTESUBJECTALTNAME2).** Хакеры используют флаг EDITF\_ATTRIBUTESUBJECTALTNAME2 для добавления произвольных значений в поле SAN, чтобы аутентифицироваться от имени любого пользователя, включая администраторов домена.
* **ManageCA & managecertificate (ESC7).** Злоумышленник может использовать права ManageCA для изменения параметров CA, что может включать активацию флага EDITF\_ATTRIBUTESUBJECTALTNAME2 или других параметров, создающих уязвимости.
* **Relay на AD CS Web Enrollment (ESC8).** Хакер может перенаправить NTLM-аутентификацию на уязвимый HTTP-эндпойнт, чтобы получить сертификат для клиентской аутентификации и использовать его для получения TGT (ticket-granting ticket) доменного контроллера.
* **No Security Extension (ESC9).** Хакер использует значение CT\_FLAG\_NO\_SECURITY\_EXTENSION (0x80000) в атрибуте msPKI-Enrollment-Flag, чтобы предотвратить добавление расширения безопасности szOID\_NTDS\_CA\_SECURITY\_EXT в сертификат. Это позволяет обойти ограничения маппинга сертификатов, заданные значением 1 ключа реестра StrongCertificateBindingEnforcement, и использовать userPrincipalName (UPN) при аутентификации.
* **Weak Certificate Mappings (ESC10).** Эта атака использует небезопасную конфигурацию маппинга сертификатов на контроллере домена, которая связана с параметрами CertificateMappingMethods со значением 0x18 (или содержащим флаг UPN) и StrongCertificateBindingEnforcement со значением 0. Эти настройки позволяют злоумышленнику, обладающему правом GenericWrite, получать сертификаты от имени других учетных записей.
* **Relaying NTLM to ICPR (ESC11).** Хакер использует отсутствие атрибута IF\_ENFORCEENCRYPTICERTREQUEST на сервере CA для выполнения ретрансляции NTLM (NTML relay) без подписи через службу RPC. Это позволяет запрашивать сертификаты через уязвимый сервер CA, используя учетные данные администратора домена.
* **Shell Access to ADCS CA with YubiHSM (ESC12).** Эта атака предполагает, что частный ключ CA хранится на внешнем устройстве YubiHSM2, подключенном к серверу CA. Если злоумышленник получает доступ к реестру, где хранится пароль к YubiHSM, он может использовать этот пароль для доступа к закрытому ключу и подделки сертификатов через CA.
* **OID Group Link Abuse (ESC13).** Шаблон сертификата может содержать политику выдачи, которая является OID в атрибуте msPKI-Certificate-Policy. Политика выдачи содержит атрибут msDS-OIDToGroupLink, который позволяет привязать политику к группе AD для того, чтобы пользователь мог авторизоваться в системе в качестве ее члена. Если злоумышленник обладает правами на выпуск сертификата по уязвимому шаблону, он может получить привилегии группы, связанной с этой политикой, и таким образом получить доступ к целевым ресурсам.
* **Weak Explicit Mapping (ESC14).** Эта атака основана на небезопасной конфигурации явного маппинга сертификатов. Злоумышленник, скомпрометировавший атакуемую учетную запись и обладающий возможностью запрашивать сертификаты, может использовать небезопасную конфигурацию сопоставления для аутентификации от имени целевой учетной записи.

**Рекомендации (зависят от** [**типа атаки**](https://learn.microsoft.com/ru-ru/training/modules/implement-manage-active-directory-certificate-services/) **на службы сертификатов):**

* Отслеживать события [4899](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786432(v=ws.11)#monitoring-changes-to-certificate-templates) (A Certificate Services template was updated), в котором отображаются измененные атрибуты, и [4900](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786432(v=ws.11)#monitoring-changes-to-certificate-templates) (Certificate Services template security was updated), в котором отображаются изменения разрешений безопасности. Стоит отметить, что эти события срабатывают не в момент внесения изменений в шаблон, а только при запросе сертификата с новыми свойствами.
* Для выявления подозрительных запросов на получение сертификата следует отслеживать событие [4898](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786432(v=ws.11)#monitoring-changes-to-certificate-templates) (Certificate Services loaded a template), в котором содержатся свойства шаблона выпускаемого сертификата. Наличие в этом событии флага ct\_flag\_enrollee\_supplies\_subject указывает на то, что пользователю разрешено указывать альтернативное имя субъекта в запросе. Также нужно отслеживать события [4886](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn319076(v=ws.11)) (Certificate Services received a certificate request), [4887](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn319076(v=ws.11)) (Certificate Services approved a certificate request and issued a certificate) и [4888](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn319076(v=ws.11)) (Certificate Services denied a certificate request), в которых содержатся сведения о пользователе, запросившем сертификат, и узле, с которого запрос получен, а также время создания запроса.
* Выполнять мониторинг события [4768](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4768) (A Kerberos authentication ticket was requested) для выявления использования нелегитимных сертификатов по их серийному номеру при аутентификации.

## ShadowCoerce

В системе Windows есть служба Volume Shadow Copy Service (VSS), предназначенная для создания теневых копий файлов и томов. VSS позволяет выполнять резервное копирование системных файлов, не прерывая работу приложений и пользователей. Атака ShadowCoerce использует уязвимости протокола MS-FSRVP службы VSS и позволяет принудить учетную запись контроллера домена Active Directory авторизоваться на узле, подконтрольном злоумышленнику. В результате проведения атаки он сможет получить учетную запись контроллера домена.

**Рекомендации:**

* [Отключить](https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/volume-shadow-copy-service) на контроллерах домена службу теневого копирования (VSS) с помощью консоли управления.
* Использовать механизм [Extended Protection for Authentication (EPA)](https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/).
* [Настроить](https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always) обязательную подпись SMB-пакетов как на серверах, так и на клиентах.
* Проводить регулярный аудит безопасности домена с помощью ПО [PingCastle](https://www.pingcastle.com/).