AD PENTEST INTERVIEW BOOK

Active Directory / Windows-based Infrastructure

Практическая брошюра по AD-пентесту: архитектура, hands-on логика, типовые misconfig, интервью-вопросы и инженерный майндсет без воды и без «магии ради магии».

ИВАН ПИСКУНОВ | WHITE2HACK

Version 1.1 | January 2026

Starter Edition • Free Distribution

Оглавление

Перед стартом: правила игры и как читать брошюру

ATTENTION. Эта брошюра распространяется бесплатно и является вкладом в индустрию, который должен помочь ребятам подготовиться к техническим интервью и лучше понять AD-пентест.

Несанкционированное воспроизведение, перепродажа, включение в коммерческие курсы или учебные продукты без разрешения автора запрещены.

Использование фрагментов и идей разрешено с обязательной ссылкой на автора.

Дополнительные материалы по penetration testing и смежным темам можно искать в Telegram-канале White2Hack.

Важно. Материал ориентирован на подготовку к интервью и санкционированное тестирование. Даже если у тебя есть технические навыки, это не дает права применять их вне согласованного scope. Любые действия на production-среде без явного разрешения - плохая идея и с инженерной, и с юридической точки зрения.

Как пользоваться оглавлением. Оглавление здесь сделано простым и практичным. Это не декоративная часть. Используй его как маршрут подготовки: сначала база и методология, потом инструменты и типовые проблемы, затем интервью и словарь.

Материал собран из открытых источников, официальной документации Microsoft, лабораторий, whitepaper'ов, книг, публичных GitHub-репозиториев и практических заметок по AD-пентесту.

Это не курс и не рекламная брошюра. Это рабочая шпаргалка для инженеров, которые хотят увереннее понимать доменную инфраструктуру Microsoft и сильнее отвечать на technical interview.

Материал предназначен только для обучения, внутренней подготовки, lab-safe упражнений и санкционированного тестирования в рамках согласованного scope. Автор не поддерживает незаконный доступ, несанкционированное вмешательство и любой вредоносный use case.

Там, где тема по природе опасная, в книге сделан акцент на логику, признаки, артефакты, цепочки доверия, безопасные read-only примеры и то, как грамотно обсуждать проблему на интервью или в отчете.

Подробные weaponized инструкции, которые выходят за рамки этичного применения, здесь намеренно не даются.

- Сначала пройди вводную по AD, архитектуре и kill chain, чтобы не путаться в терминах.
- Потом изучи методологию, протоколы, misconfiguration и инструментальный набор.
- После этого переходи к interview-блоку, STAR-кейсам и глоссарию.
- Если тема новая, не зубри названия. Учись видеть объект, право, отношение и potential impact.

1. Что такое Active Directory и почему AD – жирная мишень для пентестера

Active Directory - это каталожная служба Microsoft для управления идентичностями, компьютерами, серверами, политиками и доверием внутри корпоративной сети. Если говорить очень по-простому, AD отвечает за то, чтобы пользователь или сервис в домене могли доказать, кто они такие, получить нужные права и обратиться к нужному ресурсу без ручного зоопарка локальных учеток на каждом сервере.

Исторически AD пришла на смену модели Windows NT domains и начиная с Windows 2000 стала стандартом корпоративной аутентификации и централизованного управления Windows-инфраструктурой. Внутри этой экосистемы постепенно срослись LDAP как интерфейс каталога, Kerberos как основной механизм аутентификации, DNS для поиска сервисов, Group Policy для массового применения настроек, а позже - плотная связка с PKI, Exchange, SQL Server, IIS, SCCM и другими инфраструктурными компонентами.

Для инженера по penetration testing AD важна не сама по себе, а как центр распределения доверия. Кто контролирует пользователей, группы, ACL, доверительные отношения, билеты Kerberos, сертификаты, GPO и сервисные учетные записи, тот фактически контролирует инфраструктуру. Поэтому одна ошибка в делегации, одна забытая сервисная учетка или один неудачный сертификатный шаблон иногда стоят дороже, чем пачка внешних CVE на периферии.

На современном интервью по AD уже мало сказать: «домен - это когда есть контроллер». Нужно понимать архитектуру, основные сущности, поверхность атаки, типовые ошибки эксплуатации и то, как из

стартового low-priv доступа строится путь до более сильных прав. Именно это и является опорой для всей книги.

С практической точки зрения AD-пентестер почти всегда думает в терминах: **объект -> право -> отношение -> следующий объект.** Не «я знаю модную атаку», а «у этой учетки есть право записывать атрибут на тот объект, этот объект доверяет такому-то сервису, а дальше это открывает путь к другому уровню контроля». Такой подход гораздо полезнее на интервью, чем бесконечный пересказ названий техник.

Почему Active Directory до сих пор остается жирной мишенью даже в 2025-2026 годах? Во-первых, из-за огромной поверхности атаки: **LDAP, Kerberos, NTLM, SMB, RPC, WinRM, RDP, PKI, GPO, service accounts, trusts и legacy-настройки.** Во-вторых, из-за инерции enterprise: совместимость с легаси, старые ACL, забытые группы, shared accounts, шаблоны сертификатов «чтобы работало», исторические делегации. В-третьих, из-за цепочечности. Один finding сам по себе может выглядеть умеренно, но в связке с соседним превращается в короткий путь до доминирования в домене.

С инженерной точки зрения домен сегодня часто крутится вокруг **Windows Server 2022 и Windows Server 2025,** а рабочие станции - вокруг Windows 10 и Windows 11. Microsoft в Windows Server 2025 добавила новый functional level, продолжает усиливать Windows LAPS и ввела delegated Managed Service Account (dMSA) как новый тип управляемой сервисной идентичности. Это важно знать хотя бы на уровне архитектуры: современный домен - это уже не музейный набор старых техник, а живая смесь классического AD, PKI, управляемых сервисных аккаунтов, EDR и иногда гибридной связки с облаком.

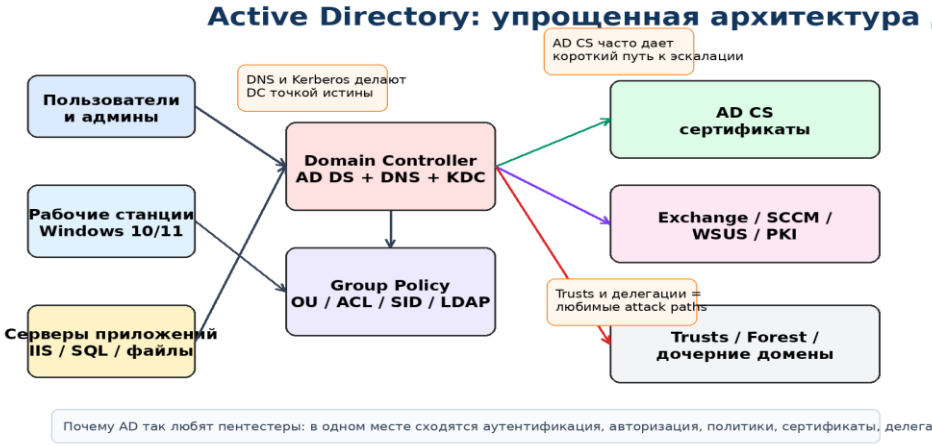

Схема: верхнеуровневый обзор AD и связных инфраструктурных ролей.

Верхнеуровневая схема AD полезна не как картинка ради картинки, а как карта объектов, прав и доверия.

Из каких элементов состоит живая AD-инфраструктура

Короткая историческая справка

Если сильно упростить, путь AD выглядел так: централизованная аутентификация -> групповое управление -> плотная интеграция с сервисами Microsoft -> появление сложных identity-path сценариев вокруг PKI, делегации, сервисных аккаунтов и trust'ов.

Именно поэтому современный AD-пентест - это уже давно не только про пароли и контроллеры домена. Он про весь control plane Windows-инфраструктуры.

Элемент	Комментарий
Forest	Верхний логический контейнер. Внутри леса могут жить один или несколько доменов, связанные общим каталогом, схемой и доверительными отношениями.
Domain	Базовая административная и аутентификационная единица. Здесь живут пользователи, группы, компьютеры, OU, GPO и контроллеры домена.
Domain Controller	Сервер с ролью AD DS. На нем находятся каталог, KDC, часто DNS, а иногда и дополнительные роли. С точки зрения impact это один из самых ценных

	узлов.
OU	Организационные подразделения, которые помогают структурировать объекты и делегировать администрирование.
GPO	Group Policy Objects. Механизм массового управления конфигурацией пользователей и машин.
Trusts	Доверительные отношения между доменами и лесами. Часто именно здесь появляются неочевидные paths между сегментами инфраструктуры.
AD CS	Служба сертификатов Active Directory. Критически важная поверхность атаки в современных доменах.
Service Accounts	Обычные сервисные учетки, gMSA и dMSA, под которыми работают приложения и службы.

Что особенно актуально в 2025-2026

Windows Server 2025 ввел новый functional level, а Microsoft продолжает развивать Windows LAPS и dMSA. Для кандидата это значит простую вещь: на интервью полезно уметь говорить не только про legacy-дырки, но и про современную модель сервисных идентичностей, PKI и доменный харденинг.

2. Майндсет инженера и логика kill chain

Хороший AD-пентест начинается не с запуска модной утилиты, а с понимания того, кто ты в этой инфраструктуре прямо сейчас. *Ты обычный доменный пользователь? Локальный админ на одной машине? Сервисная учетка? Машинная учетка? У тебя есть только read-only доступ к каталогу или уже есть точка для lateral movement?* Ответ на этот вопрос влияет буквально на всё, от выбора инструментов до уровня шума.

Вторая важная мысль - думать не командами, а объектами и отношениями. Пользователь входит в группу. Группа имеет право на OU. OU тянет GPO. GPO меняет локальных админов на серверах. Сервер запускает сервис под сервисной учеткой. Сертификатный шаблон позволяет запросить не тот субъект. Вот из таких связей и строятся реальные attack path'ы.

Третья мысль - не шуметь без причины. Даже если ты работаешь в lab, полезно с junior-уровня привыкнуть: *бездумный spray, агрессивный collector, лишняя запись в AD или попытка старого noisy трюка могут испортить и engagement, и интервью*. Сильный инженер умеет объяснить, почему он сначала идет в enumeration и validation, а не сразу пытается «сломать все подряд».

Четвертая мысль - переоценивать картину после каждого нового факта. Получил новый credential material, увидел новый ACL, нашел LAPS rights или certificate template - пересобери гипотезы. В AD тупики часто исчезают после одной новой детали.

GitHub[3]. It has several steps, but it always follows the same cycle –

recon, **compromise**, **lateral movement** – just with more privileged access:

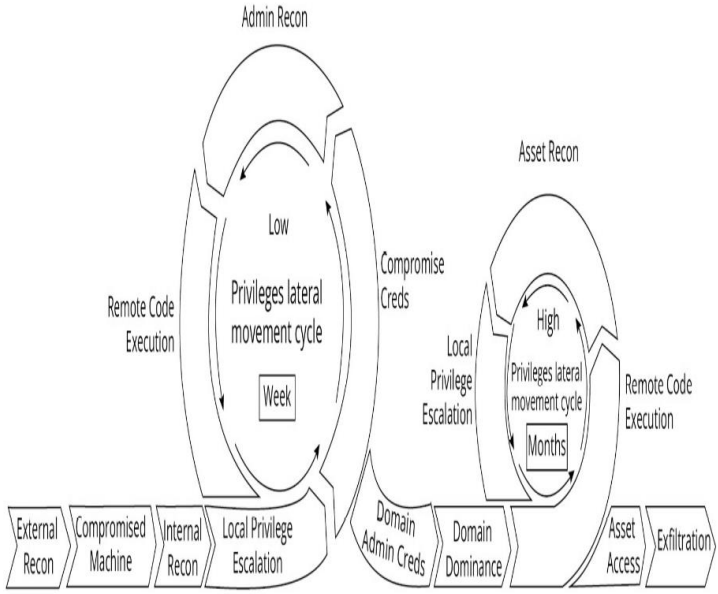

Figure 1.4 – Active Directory kill chain

Схема: упрощенная kill chain для доменной среды.

Упрощенная kill chain для AD: от карты домена и credential material до более сильного контроля.

Kill chain в практическом виде

Стартовая точка: low-priv user, подрядчик, локальный админ на одной машине, сервисная учетка или уже скомпрометированная рабочая станция.

Discovery и recon: forest, domain, DC, trusts, группы, SPN, OU, GPO, AD CS, LAPS, gMSA/dMSA, ключевые сервисы и опорные серверы.

Credential access: всё, что помогает получить или валидировать credential material без лишнего риска - roastable exposure, password policy, local admin reuse, LAPS rights, gMSA readability, certificates, delegation side effects.

Privilege escalation: ACL abuse, делегации, GPO control, certificate template abuse, replication rights exposure, admin tier drift, уязвимые service account paths.

Латеральное движение: каналы администрирования и аутентификации - SMB, WinRM, PSRemoting, WMI, RDP, MSSQL, IIS, SCCM, file shares.

Domain dominance: подтверждение контроля над критичными объектами, а не «цирк ради цирка». Нужно показать blast radius, а не коллекционировать громкие названия.

Reporting и remediation: объяснить, почему цепочка работает, какие условия ей помогают, как ее заметить и как закрыть с минимальным operational pain.

Mindmap 2k25 - удобная карта тем и связей, чтобы не потерять ветку анализа.

Ключевая мысль

В AD почти никогда не выигрывает тот, кто знает больше громких названий. Выигрывает тот, кто умеет строить гипотезу, валидировать ее самым тихим способом и переводить результат в понятный evidence и remediation.

3. Практическая методология AD-пентеста

Ниже - practical flow, который обычно хорошо работает и в реальном домене, и как каркас ответа на интервью. Он специально описан по-инженерному, а не как продающая статья о взломе.

Шаг 0. Scope и безопасные рамки. До любой технической работы надо понять: что в scope, что out of scope, разрешены ли spraying, relay, изменение объектов каталога, активные проверки AD CS, действия на DC, взаимодействие с почтой, SQL и SCCM. На интервью это тоже хороший признак зрелости: кандидат думает не только про «что можно сделать», но и про «что разрешено и что безопасно».

Шаг 1. Определи identity context. Кто ты сейчас и какие у тебя реальные права. Одинаковые команды, запущенные от обычного пользователя и от локального админа на доменной машине, дают совершенно разную ценность.

Шаг 2. Собери карту домена. Названия доменов, контроллеры, DNS, trusts, важные серверы, jump hosts, PKI, SQL, SCCM, Exchange, file shares, админские станции. В AD почти всегда выигрывает тот, у кого лучше карта.

Шаг 3. Сформируй быстрые гипотезы. Есть ли roastable users, есть ли опасные service accounts, включен ли LAPS и кто его читает, есть ли gMSA/dMSA, есть ли AD CS, кто контролирует GPO, какие группы выглядят «толстыми», есть ли уязвимые trust'ы и странные ACL.

Шаг 4. Иди от тихого к шумному. Сначала read-only enumeration. Затем проверка прав и отношений. Потом controlled validation. Нормальный инженер умеет объяснить, почему он оставил наиболее рискованные действия на конец.

Шаг 5. После каждой удачной находки перестраивай graph. В доменной среде один новый credential или одно право на OU способны открыть цепочку, которую ты не видел час назад.

Шаг 6. После высоких прав не теряй фокус. Не надо «трогать все подряд». Нужно подтвердить impact, зафиксировать evidence, оценить blast radius и перейти к findings и remediation.

Стартовый чек-лист

Что делать после получения высоких прав

Подтвердить scope контроля и не превращать работу в бессмысленный «сафари-тур».

Оценить blast radius: какие домены, серверы, сервисы и trust'ы реально затронуты.

Зафиксировать точные evidence: группы, ACL, шаблоны, SID, DN, hostname, время.

Сразу думать о remediation: кому именно придется исправлять проблему и насколько болезненно это будет.

Элемент	Комментарий
Identity context	Кто ты прямо сейчас: обычный пользователь, локальный админ, сервисная учетка, машинная учетка, helpdesk, backup operator и т.д.
DC / DNS map	Какие контроллеры домена, какие site'ы, какие ключевые SRV-записи и доменные сегменты.
Critical services	Есть ли AD CS, Exchange, SCCM, WSUS, SQL, jump hosts, admin workstations, backup-серверы.
Fast hypotheses	Roastable exposure, delegation, LAPS, gMSA, dangerous ACL, trust'ы, GPO control.
Movement channels	SMB, WinRM, RDP, WMI, MSSQL, PSRemoting и прочие реальные каналы управления.
Noise budget	Что можно делать активно, а что надо оставить как read-only validation.

3.1 MITRE ATT&CK как mental map для AD-интервью

MITRE ATT&CK удобно использовать не как коллекцию «страшных слов», а как карту того, на каком этапе kill chain ты находишься и зачем вообще делаешь очередную проверку.

Тактика ATT&CK	Что это значит в AD-пентесте
Discovery / TA0007	не лезть сразу в шум, а сначала читать структуру: trust'ы, группы, SPN, сессии, shares, PKI.
Credential Access / TA0006	в AD это не только dump, но и roastable exposure, weak service accounts, NTLM/Kerberos артефакты.
Privilege Escalation / TA0004	ACL abuse, delegation, GPO control, AD CS misconfig, replication rights.
Lateral Movement / TA0008	WinRM, SMB, RDP, WMI, remote services, service control и другие законные админские каналы.
Persistence / TA0003	изменения групп, ACL, GPO, сертификатных шаблонов, сервисов и сервисных аккаунтов.
Defense Evasion / TA0005	не только «обойти защиту», но и уметь не шуметь там, где это вообще не нужно.

Полезный лайфхак для интервью: если тебя спрашивают про технику, привяжи ее к ATT&CK-тактике, условиям и impact. Это сразу звучит взрослее, чем просто «ну это когда можно сделать X».

3.2 IoC, которые SOC часто детектирует в доменной истории

Когда инженер понимает не только offensive-логику, но и следы, которые она оставляет, его ответы становятся намного сильнее. Ниже - типовые IoC и поведенческие маркеры, которые часто всплывают при расследовании атак на AD.

всплеск TGS-запросов на сервисные SPN с нетипичного хоста или от нетипичной учетки;

- **серии 4625/4771/4776** по множеству аккаунтов или с одного источника - намек на spray или плохую automation;
- новые члены привилегированных групп, неожиданные изменения ACL/GPO/сертификатных шаблонов;
- создание сервисов, запуск новых админских процессов, явное использование alternate credentials;

- подозрительная активность вокруг DC, CA, jump host, management server, SCCM/WSUS/backup-инфры;
- массовый доступ к шарам со скриптами, install-пакетами, backup-файлами и конфигами;

3.3 Windows Event ID, на которые действительно стоит смотреть

События из журналов Windows нельзя читать в вакууме. Один event сам по себе редко доказывает взлом; ценность дает цепочка: кто, где, когда, с какого хоста, после какого изменения и в каком контексте.

Event ID	О чем сигнал	Комментарий для расследования
4624	успешный логон	не всякий 4624 зло, но логон-тип и хост очень важны
4625	неуспешный логон	серии по одной учетке или по многим хостам намекают на spray/bruteforce
4648	явное использование альтернативных credentials	часто интересно при lateral movement и admin tooling
4672	специальные привилегии назначены новому логону	хороший маркер появления «сильной» сессии
4688	создан новый процесс	очень полезен, если включена расширенная командная строка
4697 / 7045	установка сервиса	классический признак service-based execution/persistence
4720	создан новый пользователь	редко бывает безобидным на чувствительных узлах
4728	добавление в security-enabled global group	для доменных групп почти всегда worth a look
4732	добавление в локальную security group	полезно на серверах и рабочих станциях
4738	учетка пользователя изменена	важен для паролей, флагов, SPN и sensitive-атрибутов
4742	изменена учетная запись компьютера	интересно для machine-account abuse и делегаций
4768	запрошен TGT	полезен для Kerberos-потока и странных источников
4769	запрошен service ticket	всплеск по сервисным SPN часто виден при Kerberoast-похожих сценариях

4771	ошибка Kerberos pre-auth	может подсветить плохие пароли или AS-REP/kerberos noise
4776	NTLM validation	важно там, где legacy NTLM все еще жив
4662	операция над объектом каталога	один из ключевых сигналов для репликационных злоупотреблений при правильном auditing
5136	объект каталога изменен	золото для отслеживания ACL/GPO/атрибутов
5140	доступ к сетевой шаре	помогает видеть lateral movement и живые интересы атакующего

3.4 Слабые места и operational debt разных поколений Windows Server

Сама версия Windows Server редко является «волшебной дырой». Но версия очень часто подсказывает, какой багаж legacy, какой baseline и какие operational компромиссы тебя ждут. На интервью сильнее звучит именно такой разговор, а не «старое = дырявое, новое = безопасно».

Версия	**Практические слабые места / риски**	**Что сказать на интервью**
Windows Server 2008 / 2008 R2	исторический багаж, legacy crypto/protocols, старые привычки админов, out-of-support	на интервью скажи не «дырявая ОС сама по себе», а «высокий шанс legacy и operational debt»
Windows Server 2012 / 2012 R2	часто живет дольше, чем надо; много наследованных политик и слабых совместимостей	смотри на NTLM/подписи/делегации/старые сервисные аккаунты и EOS-контекст
Windows Server 2016	часто встречается как DC/infra role, но уже не самый современный baseline	важно понимать, чего тут еще нет из более свежих защитных удобств
Windows Server 2019	обычно уже чище, но все решают настройки и tiering	если hygiene плохая, версия сама по себе не спасет
Windows Server 2022	лучше baseline и современная платформа, но AD CS/ACL/GPO все равно могут гореть	сильный ответ: «свежая версия снижает класс legacy-рисков, но не отменяет design flaws»
Windows	новые security-	думай не только про новые

Server 2025	возможности, dMSA, более жесткий baseline	фичи, но и про гибридный зоопарк рядом с ними

4. Лаборатории и стенды: где набирать руки безопасно

AD-пентест невозможно выучить только по тексту. Если не трогать руками домен, термины будут звучать умно, но в голове не сложится карта объектов. Поэтому ниже - набор стендов, которые реально помогают нарастить muscle memory.

GOAD / GOADv2 - один из лучших open-source стендов для понимания attack path'ов в AD. Он хорош тем, что в нем уже есть несколько доменов, trust-связи, SQL, IIS, AD CS и другие элементы, которые делают лабу похожей на живую инфраструктуру.

DetectionLab полезен тем, что показывает не только offensive side, но и защитную телеметрию. Это особенно ценно для интервью, потому что зрелый пентестер понимает, какие артефакты он создает и что может увидеть blue team.

HTB Academy / CAPE path и TryHackMe Active Directory полезны как управляемая учебная дорожка. Они не заменяют свою лабораторию, но дают хорошую структуру, повторяемость и тренировку объяснять шаги.

Splunk Attack Range и похожие стенды полезны, если хочется понимать связку offensive действий и detection view. Для product security и purple-style собеседований это плюс.

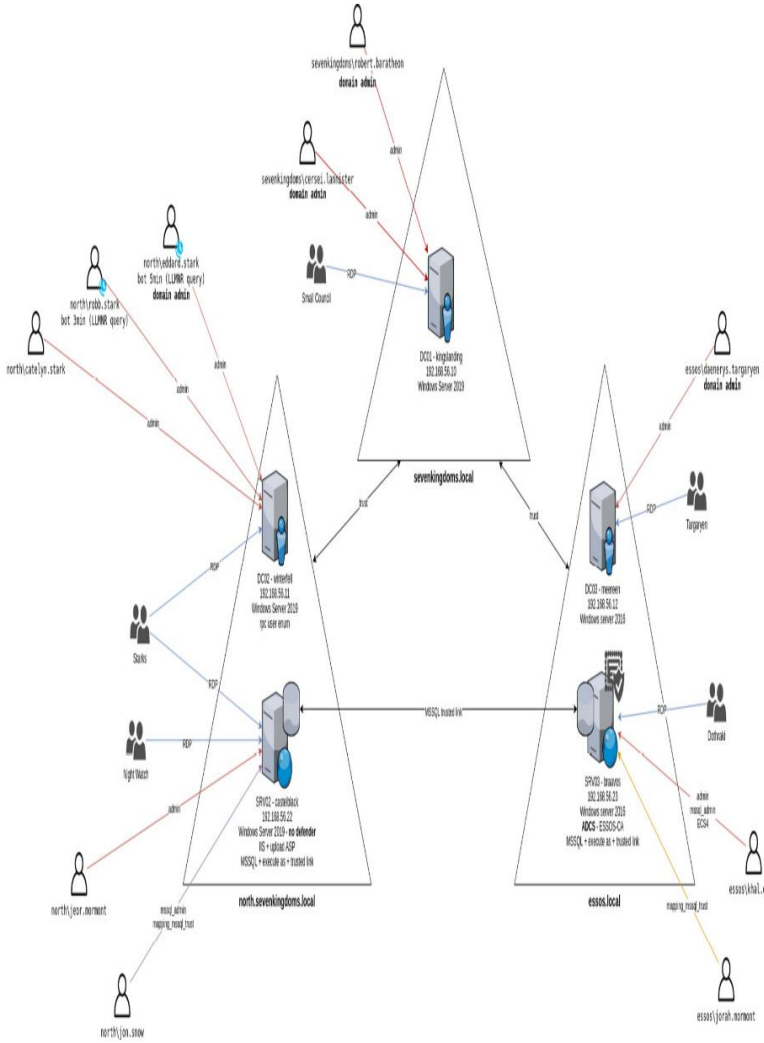

Figure 1.3 – GOADv2 overview

GOAD - один из лучших стендов, чтобы учиться видеть не одну машину, а всю историю trust'ов и ролей.

GOAD полезен тем, что показывает не один сервер, а связную инфраструктурную историю с trust'ами и дополнительными сервисами.

Рекомендованный практический минимум

1 локальная лаба, которую ты сам поднимаешь и переинициализируешь.

1 управляемая обучающая дорожка вроде HTB Academy или TryHackMe.

1 стенд, где видна телеметрия защитной стороны.

Привычка вести собственный runbook: что увидел, какую гипотезу проверял, какой artifact получил и какой вывод сделал.

Что развернуть у себя на машинке

Элемент	Комментарий
База	1 DC, 1-2 member server, 1-2 workstation, DNS и минимум один сервисный аккаунт.
Дополнительно	AD CS, SQL Server, IIS или file server, чтобы увидеть связку сервисов и идентичностей.
Для продвинутого уровня	Второй домен или дочерний домен, trust, jump host, SCCM/WSUS-подобный сервис.
Хост	VMware Workstation, VirtualBox, Proxmox или похожая платформа. Желательно Linux-хост, чтобы часть tooling была под рукой.

4.1 Официальные репозитории и документация

Стенд / ресурс	Официальная ссылка
GOAD / docs	https://github.com/Orange-Cyberdefense/GOAD https://orange-cyberdefense.github.io/GOAD/
DetectionLab	https://github.com/clong/DetectionLab https://detectionlab.network/
Splunk Attack Range	https://github.com/splunk/attack_range https://attack-range.readthedocs.io/
HTB Academy path	https://academy.hackthebox.com/path/preview/active-directory-penetration-tester
HTB CAPE	https://academy.hackthebox.com/preview/certifications/htb-certified-active-directory-pentesting-expert
THM WinAD Basics	https://tryhackme.com/room/winadbasics
THM Exploiting AD	https://tryhackme.com/room/exploitingad
THM AD Hardening	https://tryhackme.com/room/activedirectoryhardening
THM Holo	https://tryhackme.com/room/hololive

4.2 Что брать у HTB и THM для системной подготовки

Hack The Box и TryHackMe не заменяют свою лабу, но отлично закрывают две задачи: структурируют прогресс и помогают не расползаться по теме. Идеальная схема такая: ***теория/упражнения на платформе -> повтор у себя в локальном домене -> короткие заметки в runbook.***

Модуль / room	Что внутри	Зачем тебе это
HTB Academy: Introduction to Active Directory	история AD, объекты, структура, auth-протоколы	вход в тему без магии и без «я просто видел BloodHound»
HTB Academy: Active Directory LDAP	LDAP, built-in enumeration, каталог и атрибуты	чтобы не путать каталог с аутентификацией
HTB Academy: Active Directory Enumeration & Attacks	enumeration, trusts, Kerberoast, ACL, hardening	самый полезный hands-on мостик к интервью
HTB Academy: ADCS Attacks	PKI/CA/шаблоны/сертификатные misconfig	сильно бустит понимание современной поверхности AD
HTB Academy: Windows Attacks & Defense	атаки плюс detection/hardening	хорошо для ответа с обеих сторон стола
HTB CAPE certification	большой практический экзамен по AD	проверяет реально ли ты работаешь руками
TryHackMe: WinAD Basics	базовые доменные концепции	если нужно мягко зайти в тему
TryHackMe: Exploiting Active Directory	делегации, GPO, сертификаты, trust'ы	хорошо для быстрой ревизии типовых путей
TryHackMe: Active Directory Hardening	атаки + mitigation	удобно для секции remediation на интервью
TryHackMe: Holo	смешанный web + AD сценарий	учит видеть домен не изолированно, а в инфраструктуре

4.3 Типовая архитектура Windows-домена на CTF и в учебных стендах

На CTF и в тренировочных лабах обычно не строят гигантский enterprise. Там собирают компактную, но очень показательную доменную экосистему, чтобы на ней можно было показать сразу несколько классов проблем и путей движения.

- один основной домен и 1-2 контроллера домена, чтобы было на чем показать auth/replication/GPO;
- пара member server'ов под IIS, MSSQL, fileshare или CA, чтобы атака не сводилась к одному DC;
- одна-две рабочие станции, где живут админские сессии, кэш и operational следы;
- service account со SPN, misconfigured delegation или читаемый LAPS/gMSA;
- AD CS или child domain / trust для более «взрослого» attack path'а;
- типовые находки: web-shell -> сервисная учетка -> read-only recon -> ACL path -> GPO/AD CS -> high privilege.

Типовые findings, от которых раскручивается атака, тоже довольно земные: пароль в конфиге, доступ к шаре со скриптами, web-to-AD pivot, service account со SPN, ACL на группе, dangerous enrollment rights в AD CS, misconfigured GPO, избыточные права на LAPS/gMSA или забытый trust. Это как раз та архитектура, где рука быстро начинает чувствовать real-world логику.

ВНИМАНИЕ!!!

На собеседовании красиво звучит не «я знаю 20 лаб», а «я могу объяснить, какой элемент стенда моделирует какой реальный риск в enterprise».

5. Базовые протоколы и объекты, которые надо понимать

В AD очень легко захлебнуться в названиях. Поэтому здесь логика простая: не учить аббревиатуры как заклинания, а понимать, какую задачу каждая сущность решает и почему пентестеру это важно.

Если ты видишь LDAP, Kerberos, NTLM, SPN, ACL, GPO, LAPS, gMSA или dMSA и не можешь одной фразой объяснить их роль, значит на интервью будет тяжело. Ниже - короткая инженерная расшифровка.

LDAP

Язык запросов к каталогу и способ читать свойства объектов AD. Для пентестера это главный read-only источник правды о пользователях, группах, OU, trust'ах, SPN и ACL.

Kerberos

Основной протокол аутентификации в домене. Важно понимать TGT, TGS, KDC, delegation, SPN и то, почему некоторые легитимные свойства протокола превращаются в attack surface.

NTLM

Legacy-механизм аутентификации, который до сих пор встречается в enterprise. Часто становится опорой для relay-сценариев и lateral movement, если не включены нужные меры защиты.

SMB и RPC

Каналы доступа к шарам, удаленным сервисам и части административных операций. Очень часто именно они показывают, куда реально можно двигаться после получения новых прав.

DNS

Без него невозможно нормально находить контроллеры домена и сервисы. Для пентестера это и карта сервисов, и способ понять структуру домена.

SPN

Service Principal Name - привязка сервиса к учетной записи. Критично для Kerberos и очень полезно для поиска сервисных аккаунтов.

ACL

Списки контроля доступа на объектах AD. Это одна из самых недооцененных тем junior-кандидатами. Права на изменение объектов, групп, OU и атрибутов часто важнее прямого членства в Domain Admins.

Delegation

Механизм, позволяющий сервису действовать от имени пользователя. Ошибки в делегации - один из мощнейших классов проблем в AD.

Trust

Отношения доверия между доменами и лесами. Если не понимать trust'ы, легко недооценить blast radius.

GPO

Механизм массовой настройки систем. Контроль над GPO - это фактически управляемое влияние на машины и пользователей.

LAPS

Windows LAPS автоматически управляет паролем локального администратора и умеет хранить его в AD или Entra. Для пентестера важно не только наличие LAPS, но и то, кто может читать секреты и DSRM-пароль на DC.

gMSA / dMSA

Управляемые сервисные аккаунты. gMSA давно живет в enterprise, а dMSA появился в Windows Server 2025 как более безопасная эволюция service account модели.

AD CS

Служба сертификатов. Там, где PKI настроена неаккуратно, появляются очень короткие пути к эскалации и персисту.

LSASS и credential material

LSASS - процесс, связанный с аутентификацией и хранением чувствительных артефактов. На интервью важно объяснять не только «можно снимать секреты», но и почему это критично и как защищаться.

Как это обычно проверяют на интервью

Тебя редко просят пересказать RFC. Обычно смотрят, можешь ли ты объяснить роль механизма простыми словами и связать его с реальным риском: почему SPN важен для сервисных аккаунтов, почему ACL дают неочевидные пути, почему LAPS надо смотреть не только на наличие, но и на права чтения, почему dMSA и gMSA важны для современной сервисной модели.

6. Must-have инструментальный набор

Ниже - не список «самых хакерских» игрушек, а рабочий belt инженера, который понимает, зачем он берет инструмент в руки. В этой книге сознательно делается упор на read-only use case, inventory, validation и понимание артефактов, а не на reckless exploitation.

Встроенные Windows и админские команды

whoami /all - Быстрый снимок identity context: группы, привилегии, SID.

hostname / ipconfig /all - Привязка к машине и сетевому контексту.

nltest - Проверка домена, доверий и списка DC.

klist - Просмотр Kerberos-кэша и понимание текущей аутентификации.

setspn - Поиск SPN и валидация сервисных регистраций.

gpresult - Понимание, какие GPO реально применяются.

certutil - Базовый обзор сертификатной инфраструктуры и шаблонов.

wevtutil - Чтение логов локально в рамках анализа артефактов.

PowerShell и RSAT

Get-ADDomain / Get-ADForest - База по структуре домена и леса.

Get-ADUser / Get-ADComputer / Get-ADGroup - Чтение объектов и атрибутов.

Get-ADObject - Точный поиск по LDAP-фильтрам.

Get-ADTrust - Карта trust-отношений.

Get-GPO / Get-GPResultantSetOfPolicy - Работа с GPO.

Get-LapsADPassword - Только для разрешенного read-only доступа, чтобы валидировать модель прав на LAPS.

Граф и каталог

BloodHound / SharpHound / bloodhound-python - Построение графа отношений и неочевидных путей управления.

ldapsearch - Linux-side запросы к каталогу без GUI.

PowerView - Классика для анализа доменных объектов и прав.

AD Explorer - Локальный просмотр каталога и ACL в удобном виде.

Linux-side utility belt

Impacket - Набор сценариев для работы с протоколами Windows. Использовать аккуратно и только в согласованном scope.

NetExec / CME-подобные фреймворки - Ускоряют валидацию доступа, но легко становятся шумными.

CrackMapExec исторически - Часто упоминается на интервью как семейство подходов, а не как повод бездумно стрелять по сети.

Responder / Inveigh - Важно знать как класс forced-auth/NTLM-сценариев, но применять только при явном разрешении.

Certipy - Главный инструмент для анализа AD CS с точки зрения исследователя.

pkinittools - Полезны для понимания PKI/Kerberos-связки в lab.

rpcclient / smbclient / enum4linux-ng - Полезны для ручной валидации открытых каналов и публикации ресурсов.

Специализированные средства

PingCastle / Purple Knight - Быстрый аудит доменной гигиены и hardening-состояния.

Seatbelt - Сбор системных артефактов на Windows-хосте.

winPEAS - Широкий локальный audit checklist; использовать осознанно.

Rubeus - Нужно знать как семейство Kerberos-утилит и уметь объяснить, где оно помогает на анализе.

Mimikatz - Нужно понимать как класс инструмента по credential material. На интервью важнее объяснить риски, ограничения и защиту, чем хвастаться запуском.

linWinPwn / AD-Suit - Швейцарские ножи для лабораторной автоматизации и быстрой проверки гипотез.

Защитная и гибридная сторона

Defender for Identity - Понимание детектов по reconnaissance, DCSync, roasting и coercion-сценариям.

Sysmon + SIEM - Полезны, чтобы объяснить, какие следы оставляет tooling.

Wireshark - Разбор протоколов и понимание, что реально ходит по сети.

Как пользоваться инструментами зрело

- Знай минимум одну тихую альтернативу шумной утилите.
- Понимай, какой протокол использует инструмент и какие следы он оставляет.
- Не подменяй понимание среды автоматизацией. BloodHound не заменяет мозг, он ускоряет graph thinking.
- Если интервьюер спрашивает про tool, отвечай не только «что он делает», но и «когда его лучше не трогать».

Безопасные стартовые сниппеты для инвентаризации

```
whoami /all

USER INFORMATION
----------------
User Name      SID
============== ============================================
CORP\analyst   S-1-5-21-1111111111-2222222222-3333333333-1107

GROUP INFORMATION
-----------------
* Domain Users
* Remote Management Users
* Helpdesk Tier 1
```

С этого вывода начинается нормальная работа. Он показывает не только имя пользователя, но и группы, которые часто сразу подсказывают scope доступа: WinRM, helpdesk-роли, backup-операторы, локальные админы и т.д.

```
nltest /dclist:corp.local

Get list of DCs in domain 'corp.local' from '\\dc01.corp.local'
   dc01.corp.local [PDC] [DS] Site: HQ
   dc02.corp.local [DS] Site: DR
The command completed successfully
```

Команда быстро показывает контроллеры домена и иногда подсвечивает распределение по сайтам. Для интервью это хороший пример тихой первичной рекогносцировки.

```
nslookup -type=srv _ldap._tcp.dc._msdcs.corp.local

_ldap._tcp.dc._msdcs.corp.local SRV service location:
        priority = 0
        weight = 100
        port = 389
        svr hostname = dc01.corp.local
```

Через DNS легко понять, какие DC обслуживают домен. Это полезно и на практике, и как признак системного мышления.

6.1 Коммерческие фреймворки и платные платформы: что знать без фанатизма

На техинтервью иногда спрашивают не только про open-source belt, но и про коммерческий стек. Зрелый ответ здесь звучит так: платформа может ускорить validation и reporting, но не должна подменять инженерное мышление и понимание шумов/ограничений.

Платформа	Что это	Как о ней говорить на интервью
Core Impact	классическая коммерческая платформа для автоматизации validation и controlled exploitation	может ускорить демонстрацию impact, но не заменяет голову
Metasploit Pro	коммерческая обвязка вокруг Metasploit с reporting/campaign-функциями	полезно знать как экосистему, но на интервью ценят мышление, а не кнопку
Cobalt Strike	licensed adversary emulation / post-exploitation framework	чаще red team, чем «чистый» pentest; отвечай про scope, OPSEC и telemetry
Brute Ratel C4	коммерческий framework для emulation/post-exploitation	упоминать аккуратно, без романтизации и без «сейчас я всех обману»
BloodHound Enterprise	эксплуатационный graph уже в defensive/exposure-management плоскости	хорош для разговора про path management и identity attack paths
AttackIQ / SafeBreach / Pentera	BAS/automated validation платформы	это не ручной pentest, а регулярная проверка устойчивости и coverage

6.2 Интересные Windows-сервисы и роли, которые помогают раскрутить домен

В живой Windows-инфраструктуре домен редко ломается в вакууме. Очень часто атаку раскручивают не сам DC и не одна громкая техника, а соседние сервисы и роли, которые живут на доменной auth, сервисных учетках, GPO, шарах и операционке. Это как раз тот кусок инженерного опыта, который аудитория справедливо хочет видеть.

Сервис / роль	На что смотреть	Почему это интересно пентестеру
AD CS	сертификаты, шаблоны, enrollment rights, mapping идентичности	одна из самых коротких дорожек к high-impact finding'ам
DNS	SRV-записи, имена DC, service discovery	тихий recon, который помогает понять карту домена
IIS	пулы приложений, web.config, app	часто web-точка опоры превращается

	secrets, интеграция с доменными учетками	в доменную историю
MSSQL	service account, linked servers, xp_cmdshell-политики, backup share'ы	SQL в enterprise часто живет не сам по себе
SCCM / MECM	управление парком, деплой, клиентские права	если настроено криво, blast radius может быть очень жирным
WSUS	цепочка обновлений и админские практики вокруг нее	интересен не сам по себе, а как operational pivot
Exchange / mail infra	глубокая интеграция с AD, сервисные права, адресные книги	на старых и неопрятных инсталляциях это целый отдельный роман
ADFS / federated auth	федерация, токены, доверие между мирами	важно для hybrid-контекстов и понимания identity plane
Print Spooler	исторически шумный, но показательный сервис из coercion-класса	хорошо знать как риск-паттерн и предмет hardening
WinRM / PSRemoting	законный админский канал	часто именно через него видно, куда реально можно двигаться
SMB / File Server	шары, скрипты, GPP-артефакты, документы, install пакеты	очень приземленная, но часто золотая жила для recon
Backup / virtualization tooling	Veeam, Hyper-V, SCVMM, backup creds и orchestration	в инфраструктуре это нередко «тихая боковая дверь»

Вот тут как раз начинается взрослая инфраструктурная история. Домен часто добивается не «супер-эксплойтом», а пониманием того, какие сервисы кормятся от AD, где лежат их secrets и кто реально имеет operational control. Это звучит скучнее, чем кино про хакеров, зато в жизни работает чаще. А тебе ведь нужен резалт, а не сказ «как все круто поломали», м?

7. Топ misconfiguration и security issues в AD

Хороший AD-пентестер умеет быстро отличать яркую, но малореальную историю от misconfiguration, которая действительно дает короткий и воспроизводимый путь к impact. Ниже - набор проблем, которые часто всплывают и в реальных проектах, и на технических собеседованиях.

1. LDAP signing / channel binding не enforced

Открывает пространство для relay-класса проблем. Проверять надо не лозунгом, а в контексте совместимости и реальной конфигурации.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

2. SMB signing не обязателен

Повышает риск relay и упрощает ряд доменных цепочек.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

3. Учетки без Kerberos pre-auth

Создают AS-REP roast exposure и избыточный офлайн-риск.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

4. Сервисные аккаунты с SPN и слабыми паролями

Повышают ценность Kerberos service tickets и offline cracking exposure.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

5. Избыточные права на LAPS / DSRM секреты

Обычный low-priv пользователь не должен видеть такие секреты.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

6. Чтение gMSA паролей лишними субъектами

Очень ценный finding, потому что gMSA часто имеет реальные сервисные права.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

7. Опасные ACL на группах, OU и пользователях

WriteDacl, GenericWrite, AllExtendedRights и смежные права нередко оказываются короче, чем прямая эскалация через CVE.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

8. Неаккуратные delegation-настройки

Unconstrained, криво спроектированная constrained delegation или RBCD могут открыть критичные пути.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

9. GPO-control не у того круга лиц

Контроль над GPO - это контроль над поведением машин и иногда прямой путь к высокому impact.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

10. AD CS с опасными шаблонами и enrollment rights

Одна из самых результативных поверхностей атаки в современных доменах.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

11. Admin tier drift

Админские аккаунты логинятся не на те станции, что создает lateral movement opportunities.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

12. Local admin reuse / poor workstation hardening

Старый добрый operational debt, который до сих пор убивает сегментацию.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

13. Trust'ы без нормального контроля и обзора

Опасность в том, что blast radius уходит за пределы одного домена.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

14. Сервисные серверы вроде SCCM, WSUS, Exchange или SQL с избыточными привилегиями

Именно через такие платформы часто строятся самые короткие цепочки.

На что смотреть: конкретные права, затронутые объекты, кто реально может воспользоваться проблемой, какой у нее blast radius.

Как описывать: не просто «опасно», а «позволяет субъекту X получить доступ/влияние на Y при наличии условий Z».

Как ремедиировать: минимально необходимыми изменениями, которые не ломают живой бизнес-процесс.

15. Слабый аудит и отсутствие baseline по identity changes

<заготовка ответа>

Будет позже, котаны 😊

8. 25 техник и паттернов, которые надо знать на интервью

Это не список «20 красивых слов, чтобы выглядеть умно». Это набор паттернов мышления, которые реально показывают, видишь ли ты AD как живую систему. Ниже я специально расширяю каждый паттерн, чтобы было понятно, как про него говорить не по-джуновски.

1. Identity context first

Начинай не с магии, а с реального identity context: кто ты, какие группы, какие привилегии, откуда запущен процесс. Интервьюер хочет услышать, что ты не стреляешь в темноту и не устраиваешь цирк из tooling'a.

Как не надо отвечать: не своди identity context first к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

2. Forest/domain mapping

Карта леса, домена, сайтов, DC и ключевых ролей - это не бюрократия, а способ не потеряться. Без такой карты даже хороший finding легко превращается в «ну что-то вроде опасно».

Как не надо отвечать: не своди forest/domain mapping к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

3. Trust review

Trust review нужен, чтобы понять blast radius. Один забытый child domain или внешний trust иногда ценнее десяти локальных findings на одной рабочей станции.

Как не надо отвечать: не своди trust review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

4. SPN review

SPN review - это не только про Kerberoast, а вообще про сервисные аккаунты и их бизнес-роль. Сильный кандидат связывает SPN с сервисом, правами и вероятным impact, а не только с хэшами.

Как не надо отвечать: не своди spn review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

5. Password policy review

Password policy review показывает, насколько клиент вообще держит базовую гигиену. Хорошо звучит ответ, где ты говоришь не «хочу брутить», а «оцениваю вероятность и шум такого пути».

Как не надо отвечать: не своди password policy review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

6. LAPS rights review

LAPS rights review проверяет, кто реально читает локальные админские секреты. На интервью это хороший пример того, как read-only finding уже тянет на серьезный lateral movement risk.

Как не надо отвечать: не своди laps rights review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

7. gMSA visibility review

gMSA visibility review важна, потому что управляемая сервисная учетка часто живет на критичных узлах. Если пароль gMSA доступен не тому кругу лиц - дальше домен может поехать очень быстро.

Как не надо отвечать: не своди gmsa visibility review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

8. Delegation review

Delegation review - это разговор про доверие между сервисами и пользователями. Если кандидат не различает unconstrained, constrained и RBCD хотя бы на уровне идеи - это красный флаг.

Как не надо отвечать: не своди delegation review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

9. ACL path analysis

ACL path analysis - одна из самых взрослых тем в AD. Здесь интервьюер проверяет, видишь ли ты косвенный контроль через права, а не только прямое членство в админских группах.

Как не надо отвечать: не своди acl path analysis к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

10. GPO influence mapping

GPO influence mapping показывает, кто реально управляет поведением машин и пользователей. Это мощный пример того, что «не Domain Admin» не значит «неопасно».

Как не надо отвечать: не своди gpo influence mapping к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

11. AD CS inventory

AD CS inventory сегодня почти mandatory. Если в домене есть PKI, а кандидат даже не смотрит туда - это ощущается как пропущенный этаж в здании.

Как не надо отвечать: не своди ad cs inventory к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

12. Tier-0 asset identification

Tier-0 asset identification помогает не смешивать критичные сущности с обычным зоопарком. Иначе репорт получается красивый, но priorities у remediation-команды ломаются.

Как не надо отвечать: не своди tier-0 asset identification к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

13. Admin session hunting mindset

Admin session hunting mindset - это не про шпионаж ради шпионажа, а про понимание, где реально пересекаются привилегии и человеческая операционка. Особенно важно на серверах и jump host'ах.

Как не надо отвечать: не своди admin session hunting mindset к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

14. Share and script review

Share and script review часто дает очень земные, но ценные артефакты: скрипты, конфиги, install-пакеты, service secrets. Не glamour, зато практично - а интервьюеры это любят.

Как не надо отвечать: не своди share and script review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

15. SQL as infrastructure pivot

SQL как инфраструктурный pivot - недооцененная тема. MSSQL живет рядом с доменной auth, сервисными учетками и linked server'ами, а значит может стать мостом в более жирный сегмент.

Как не надо отвечать: не своди sql as infrastructure pivot к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

16. Exchange / mail infra awareness

Exchange / mail awareness полезна даже если ты не exchange-гуру. В enterprise почта часто глубоко интегрирована с доменом и исторически давала мощные пути влияния.

Как не надо отвечать: не своди exchange / mail infra awareness к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

17. SCCM / WSUS awareness

SCCM / WSUS awareness показывает, что ты понимаешь operational control plane. Если кто-то управляет массовым деплоем и агентами, impact здесь может быть очень неприятным.

Как не надо отвечать: не своди sccm / wsus awareness к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

18. Certificate lifecycle review

Certificate lifecycle review - это про шаблоны, auto-enrollment, EKU, mapping субъекта и жизненный цикл сертификатов. Сильный ответ звучит как история про доверие и идентичность, а не про «какой-то pfx».

Как не надо отвечать: не своди certificate lifecycle review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

19. Machine account logic

Machine account logic важна потому, что компьютеры в домене - тоже identities с правами. Много junior-кандидатов фокусируются только на user accounts и упускают половину поля.

Как не надо отвечать: не своди machine account logic к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

20. Protected Users / legacy protocol exposure

Protected Users / legacy protocol exposure - тема про разрыв между policy и реальностью. Если legacy протоколы живут, современная бумажная политика часто не спасает.

Как не надо отвечать: не своди protected users / legacy protocol exposure к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

21. Replication rights review

Replication rights review - это короткий путь к разговору про DCSync без unsafe деталей. Здесь ценится умение объяснить механику и контроль доступа, а не только громкое слово.

Как не надо отвечать: не своди replication rights review к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

22. Detection-aware enumeration

Detection-aware enumeration отличает зрелого инженера от «скрипт-кидди с красивым словарем». Нужно понимать, какие действия оставляют какой шлейф в логах и сети.

Как не надо отвечать: не своди detection-aware enumeration к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

23. Blast radius thinking

Blast radius thinking - это язык бизнеса и лидов. Даже технически сильный finding слабнет, если ты не можешь объяснить, сколько систем и ролей реально попадает под риск.

Как не надо отвечать: не своди blast radius thinking к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

24. Evidence discipline

Evidence discipline - твоя страховка и твоя валюта. Без точных DN, SID, имен групп, шаблонов, хостов и временных меток любой спорный finding рассыпается.

Как не надо отвечать: не своди evidence discipline к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

25. Remediation-minded finish

Remediation-minded finish - это то, что делает из пентестера партнера, а не туриста по домену. Сильный ответ всегда заканчивается не только «как взял», но и «как закрыть без пожара в проде».

Как не надо отвечать: не своди remediation-minded finish к одной команде или одной утилите. Интервьюер обычно проверяет не клавиши, а причинно-следственную цепочку.

Практический совет

Если тебя на интервью спрашивают про технику, старайся отвечать в одном и том же шаблоне: что это такое -> какие условия нужны -> какой practical impact -> как бы ты это валидировал безопасно -> как бы исправлял.

9. Deep dive: Kerberos, DCSync, Golden Ticket, Mimikatz, AD CS

Ниже - блок про темы, которые почти всегда всплывают на AD-интервью. Здесь важно не превратить ответ в «легенду про супер-хакера». Интервьюеры обычно проверяют, понимаешь ли ты механику, риск, prerequisites, ограничения и защитные меры.

Kerberos. Хороший ответ начинается с того, что **Kerberos - это доменный протокол аутентификации,** где клиент сначала получает TGT у KDC, а затем запрашивает сервисные билеты TGS для конкретных сервисов. Для пентестера важны SPN, delegation, типы шифрования, pre-auth, кеширование билетов и то, что часть этой логики можно использовать как источник attack surface, если операционная гигиена слабая.

DCSync. Это не «магическая команда», а злоупотребление правами репликации каталога. Если субъект имеет соответствующие extended rights, он может имитировать поведение контроллера домена и

запрашивать чувствительные данные репликации. На интервью нужно уметь спокойно объяснить: главный вопрос здесь - кто вообще имеет такие права и почему это критично.

Golden Ticket. По сути это концепт подделки Kerberos TGT при наличии материала, связанного с krbtgt. На интервью достаточно четко проговорить: это уже стадия глубокой доменной компрометации, а не стартовая техника. Ценность темы в том, что она показывает последствия компрометации доверенного ядра домена.

Mimikatz и credential dumping. Здесь зрелый ответ звучит так: инструмент известен не потому, что «все его запускают», а потому, что он исторически показал, насколько опасны слабые настройки хранения credential material, отсутствие изоляции секретов, неправильная tiering-модель и админский беспорядок. На интервью плюс дает фокус на защиту: Credential Guard, LSA protection, Windows LAPS, admin tiering, минимизация интерактивных логонов админов и контроль доступа к памяти процесса.

AD CS. Если в домене есть служба сертификатов, зрелый кандидат обязан хотя бы на базовом уровне понимать CA, шаблоны сертификатов, enrollment rights, subject name handling, web enrollment и то, что сертификат в домене может быть равнозначен очень сильной идентичности. Многие громкие цепочки последних лет крутились именно вокруг неаккуратной PKI.

Что интервьюер хочет услышать

- Ты понимаешь механику, а не только громкое имя техники.
- Ты различаешь prerequisites, ограничение и стадию kill chain.
- Ты умеешь объяснить, чем тема опасна для бизнеса и инфраструктуры.
- Ты не превращаешь ответ в unsafe пошаговую инструкцию.

10. Safe snippets и разбор типовых выводов

Ниже даны несколько безопасных read-only примеров, которые полезны как для собственной тренировки, так и для интервью. Цель не в том, чтобы заучить выводы, а в том, чтобы научиться читать артефакты и превращать их в гипотезы.

```
whoami /all

USER INFORMATION
----------------
User Name      SID
============== ============================================
CORP\analyst   S-1-5-21-1111111111-2222222222-3333333333-1107

GROUP INFORMATION
-----------------
* Domain Users
* Remote Management Users
* Helpdesk Tier 1
```

С этого вывода начинается нормальная работа. Он показывает не только имя пользователя, но и группы, которые часто сразу подсказывают scope доступа: WinRM, helpdesk-роли, backup-операторы, локальные админы и т.д.

Что можно спросить себя: какой следующий безопасный шаг даст больше контекста, не увеличивая шум без причины?

```
nltest /dclist:corp.local

Get list of DCs in domain 'corp.local' from '\\dc01.corp.local'
  dc01.corp.local [PDC] [DS] Site: HQ
  dc02.corp.local [DS] Site: DR
The command completed successfully
```

Команда быстро показывает контроллеры домена и иногда подсвечивает распределение по сайтам. Для интервью это хороший пример тихой первичной рекогносцировки.

Что можно спросить себя: какой следующий безопасный шаг даст больше контекста, не увеличивая шум без причины?

```
nslookup -type=srv _ldap._tcp.dc._msdcs.corp.local

_ldap._tcp.dc._msdcs.corp.local SRV service location:
      priority = 0
      weight = 100
      port = 389
      svr hostname = dc01.corp.local
```

Через DNS легко понять, какие DC обслуживают домен. Это полезно и на практике, и как признак системного мышления.

Что можно спросить себя: какой следующий безопасный шаг даст больше контекста, не увеличивая шум без причины?

```
Get-ADTrust -Filter *

Direction : Bidirectional
ForestTransitive : True
Name : child.corp.local
Source : corp.local
Target : child.corp.local
```

Такой вывод показывает, что у нас есть trust и его тип. На интервью важно не просто прочитать строки, а объяснить, что trust расширяет поверхность анализа и blast radius.

Что можно спросить себя: какой следующий безопасный шаг даст больше контекста, не увеличивая шум без причины?

```
certutil -CATemplates

TemplatePropCommonName = User
TemplatePropCommonName = Machine
TemplatePropCommonName = WebServer
TemplatePropCommonName = CorpVPNUser
```

Даже такой скромный вывод уже подсказывает, что в домене есть CA и набор шаблонов, которые стоит анализировать с точки зрения enrollment rights и subject handling.

Что можно спросить себя: какой следующий безопасный шаг даст больше контекста, не увеличивая шум без причины?

11. Как упаковывать findings и объяснять impact

Слабый finding звучит так: «нашли опасную настройку». Сильный finding звучит так: *«субъект X имеет право Y над объектом Z, что при реалистичных условиях позволяет получить A и затем повлиять на B».* Разница колоссальная.

Рабочая структура finding'a

Название: коротко и предметно, без маркетинга.

Что обнаружено: объект, право, конфигурация, affected scope.

Почему это работает: краткая механика без лишнего шума.

Impact: какой путь к контролю или lateral movement это открывает.

Evidence: точные артефакты, команды, выводы, SID, DN, имя шаблона, имя GPO, группа, хост.

Remediation: что поменять и в каком порядке, чтобы закрыть риск.

Микро-шаблоны finding'ов

Excessive read access to Windows LAPS secrets

Низкопривилегированный субъект или широкая operational group может читать пароли локального администратора или DSRM-секреты, что создает путь к lateral movement и расширению blast radius.

Unsafe certificate template configuration in AD CS

Шаблон сертификата сочетает опасные настройки выдачи и избыточные enrollment rights, что позволяет субъекту получить более сильную доменную идентичность, чем ему положено.

Dangerous ACL on privileged AD object

Учетная запись или группа без обоснованной административной роли имеет право изменять критичный объект AD, включая его membership, ACL или чувствительные атрибуты.

Delegation settings create privilege escalation path

Сервисная или компьютерная идентичность настроена так, что цепочка доверия позволяет повысить привилегии или имитировать пользователя на более чувствительном сервисе.

Replication rights granted beyond intended administrators

Права, связанные с репликацией каталога, выданы более широкому кругу субъектов, чем требуется, что создает риск компрометации доменных секретов.

Tiering breakdown on admin workstations

Привилегированные аккаунты интерактивно используют машины вне выделенного admin tier, что увеличивает риск кражи токенов и несанкционированного lateral movement.

12. Технические вопросы с правильными ответами

Ниже - не просто вопросы, а готовые векторы ответа. Задача не выучить их как стихи, а понять структуру: ***определение -> механика -> risk/impact -> validation/remediation.***

1. Что такое Active Directory и почему она так привлекательна для пентестера?

AD - это центр идентичности и доверия внутри Windows-инфраструктуры. Она управляет пользователями, группами, машинами, GPO, Kerberos, trust'ами и часто PKI. Поэтому компрометация AD или даже одного из ее критичных компонентов редко остается локальной - обычно она влияет на широкую часть инфраструктуры.

2. Чем отличается аутентификация от авторизации в доменной среде?

Аутентификация отвечает на вопрос «кто ты», а авторизация - «что тебе можно». В AD это важно разделять, потому что valid identity сама по себе еще не означает контроль над объектом. Но плохие ACL, GPO, delegation или certificate template могут сделать так, что после аутентификации субъект получает больше авторизации, чем должен.

3. Чем LDAP отличается от Kerberos в практическом смысле?

LDAP нужен для чтения и изменения данных каталога. Kerberos - для аутентификации и выдачи билетов доступа к сервисам. Для пентестера LDAP - это карта объектов и отношений, а Kerberos - карта доверия и сервисной идентичности.

4. Почему ACL abuse часто важнее прямого членства в Domain Admins?

Потому что права на запись или изменение ACL на нужном объекте могут дать более короткий путь к контролю, чем попытка искать прямое членство в привилегированной группе. Многие реальные доменные цепочки строятся именно на праве менять группы, пользователей, OU или GPO.

5. Почему AD CS считается high-value surface?

Потому что сертификат в домене может выступать как очень сильная идентичность. Ошибка в шаблоне или правах на выпуск может дать

субъекту аутентификацию или делегирование на уровень, который ему изначально не положен.

6. Что такое tiering и зачем он нужен?

Tiering - это разделение административных уровней и рабочих станций так, чтобы высокие привилегии не утекали на обычные пользовательские хосты. Если доменные админы логинятся куда попало, lateral movement становится намного проще.

7. Почему Windows LAPS - это не серебряная пуля?

Потому что важно не только наличие LAPS, но и качество прав на чтение секретов, ротация, защита DSRM, дисциплина админов и отсутствие других identity-path проблем.

8. Как бы ты описал роль BloodHound на интервью?

Это инструмент графового анализа отношений в AD. Его сила не в «магии», а в том, что он помогает увидеть неочевидные цепочки контроля между объектами и быстро проверить гипотезы по blast radius.

9. Что важнее после получения высоких прав - продолжать exploration или фиксировать impact?

В зрелом engagement обычно важнее аккуратно подтвердить impact, зафиксировать evidence и перейти к контролируемому анализу blast radius и remediation. Бездумное расширение действий часто только повышает риск шума и инцидента.

10. Как отличить пентест от red team в контексте AD?

Пентест чаще строится вокруг согласованной проверки конкретных рисков и цепочек с понятным доказательством impact. Red team больше имитирует противника, уделяет внимание скрытности, C2, длительным операциям и проверке процессов обнаружения.

Практические и сценарные вопросы

1. Тебе дали обычную доменную учетку и одну доменную рабочую станцию без локального администратора. С чего начнешь?

С безопасной инвентаризации контекста: identity, группы, домен, DC, trust'ы, примененные GPO, ключевые сервисы, наличие AD CS, LAPS, gMSA и потенциально интересных ACL. Я не начинаю с шумных действий. Сначала хочу понять карту домена и быстрые гипотезы.

2. Увидел, что в домене есть AD CS. Что проверяешь в первую очередь?

Сам факт наличия CA, роль CA, web enrollment, набор шаблонов, кто имеет enrollment rights, кто может менять шаблоны и не совмещаются ли опасные настройки subject handling с широкими правами на выпуск.

3. Нашел gMSA. Что для тебя важно?

Кто имеет право читать managed password, на каких серверах эта учетка используется, к каким сервисам привязана и какой blast radius у компрометации этой идентичности.

4. В BloodHound видишь путь через GenericWrite на пользователя. Как думаешь?

Я не радуюсь раньше времени. Сначала валидирую, на какой именно объект есть право, какие атрибуты значимы, не false positive ли это, не ограничен ли путь политиками и к какому practical impact он действительно ведет.

5. Видишь, что helpdesk-группа может читать LAPS на части серверов. Это всегда критично?

Не автоматически. Нужно смотреть, какие именно сервера, есть ли там админские сессии, какая роль у этих хостов и может ли это чтение стать реальным каналом lateral movement. Но как finding это очень сильный сигнал.

6. Как бы ты объяснил интервьюеру DCSync без запуска команды?

Это злоупотребление правами репликации AD. Если субъект получил нужные extended rights, он может вести себя как партнер по репликации и запросить чувствительные данные каталога. Главный риск здесь -

кому вообще выданы такие права и насколько это соответствует модели администрирования.

7. Если у тебя высокие права на GPO, что это означает?

Потенциально очень широкий уровень влияния на машины и пользователей, к которым GPO применяется. Важно понять scope GPO, link order, inheritance и какие параметры можно изменить безопасно для валидации.

8. Чем опасен сервисный аккаунт с SPN и слабым паролем?

Тем, что сервисные билеты могут дать материал для офлайн-анализа, а сама сервисная идентичность часто имеет реальные прикладные права в инфраструктуре.

9. Как бы ты обосновал, что SMB signing и LDAP signing важны?

Потому что они влияют на возможность ряда relay-классов сценариев. На интервью я бы подчеркнул не только offensive сторону, но и то, что их включение надо оценивать вместе с совместимостью и operational impact.

10. Что скажешь, если интервьюер спросит: «Почему не запустить сразу Mimikatz?»

<заготовка ответа>

И снова ответ будет позже, котаны 😊

Ну, погнали дальше!

13. STAR для penetration tester'a и interview red flags

Методика STAR популярна в США и Европе, потому что помогает быстро понять, умеет ли кандидат не просто перечислять технологии, а рассказывать о реальной работе через контекст, действие и результат.

Расшифровка простая: **Situation** - в какой ситуации ты оказался; **Task -** что нужно было решить; **Action** - что именно ты сделал; **Result** - к какому результату пришел и что это изменило.

В security-интервью по инженерным ролям STAR особенно полезен там, где тебя спрашивают про сложный pentest, спор с заказчиком, noisy finding, ограниченный scope, хороший technical judgement или перевод findings в remediation.

Базовый шаблон STAR-ответа

- Situation - где ты оказался и почему ситуация была нетривиальной.
- Task - что именно от тебя требовалось как от инженера.
- Action - какие шаги ты сделал и почему выбрал именно их.
- Result - что получилось, как это повлияло на риск, процесс или remediation.

Три боевых STAR-кейса из прошлых мест работы

Кейс 1. Опасные права на LAPS в серверном сегменте

Situation: во время внутреннего теста мне дали только low-priv доменную учетку и одну обычную рабочую станцию.

Task: нужно было понять, можно ли из этого доступа дотянуться до более чувствительных сегментов без noisy действий.

Action: я начал с read-only enumeration прав на объекты и быстро увидел, что одна operational group имеет избыточный доступ к чтению Windows LAPS для группы серверов. Дальше я проверил, какие это именно хосты, есть ли там админские сессии и какой у них инфраструктурный вес. Вместо массовых действий я аккуратно подтвердил модель доступа на ограниченном наборе объектов и собрал evidence по ACL и примененным политикам.

Result: мы показали реалистичный путь к lateral movement без громких техник, а заказчик получил очень точечную рекомендацию - пересмотреть группы чтения LAPS, отделить helpdesk от серверного сегмента и ужесточить tiering.

Кейс 2. AD CS как неожиданный кратчайший путь

Situation: у клиента уже был достаточно неплохой baseline по паролям и классическим admin groups, поэтому лобовые гипотезы быстро закончились.

Task: нужно было найти non-obvious path, если он вообще существует.

Action: я сместил фокус на PKI и начал разбирать, какие CA и шаблоны реально есть в домене, кто имеет права на enrollment и где web enrollment увеличивает поверхность атаки. Я не уходил в risky exploitation, а сначала валидировал архитектуру, сочетание шаблонов и прав.

Result: нам удалось показать, что основная проблема не в 'слабых паролях', а в неаккуратной модели выдачи сертификатов. Это было особенно полезно для клиента, потому что remediation лежал не в области password reset, а в исправлении PKI-процессов и шаблонов.

Кейс 3. GPO и blast radius вместо «красивой атаки»

Situation: в одном тесте команда уже нашла несколько локальных проблем, но заказчик не понимал, почему это должно его серьезно беспокоить.

Task: надо было показать бизнесу реальный blast radius на языке инфраструктуры, а не на языке 'хакерских трюков'.

Action: я собрал цепочку от конкретного права на изменение GPO до потенциального влияния на набор серверов и рабочих станций, к которым этот GPO применяется. В отчете я отдельно вынес scope, affected assets, условия срабатывания и варианты remediation, чтобы команда эксплуатации могла быстро отработать изменения без долгого reverse engineering наших находок.

Result: finding перестал выглядеть как абстрактная техническая придирка и был принят как инфраструктурный риск высокого приоритета. Для меня это хороший пример того, что сильный pentester продает не эффектность, а ясность.

!!!!Red flags на интервью!!!!

Говорить только названия техник без объяснения prerequisites, impact и ограничений.

Отвечать так, будто любая найденная misconfiguration автоматически равна «взял домен».

Хвастаться noisy tooling без понимания detection surface и scope.

Не различать read-only enumeration, validation и destructive действия.

Не уметь объяснить бизнес- и инфраструктурный impact finding'a простыми словами.

Путать аутентификацию, авторизацию, identity context и членство в группах.

Игнорировать AD CS, GPO, ACL и service accounts, сводя весь AD только к паролям и Mimikatz.

Не думать про blast radius, remediation и evidence discipline.

14. Расширенный глоссарий

Этот блок нужен не для зубрежки, а чтобы быстро освежить базовые термины перед интервью и привести голову в порядок.

Элемент	Комментарий
ACL	Access Control List. Набор правил, определяющих, кто и что может делать с объектом.
AD CS	Active Directory Certificate Services. Служба сертификатов Microsoft.
AD DS	Active Directory Domain Services. Основная роль каталога в Windows.
AS-REP	Ответ KDC на запрос аутентификации без pre-auth. Важен при анализе exposure аккаунтов без Kerberos pre-auth.
Blast radius	Насколько далеко по инфраструктуре уходит влияние finding'a.
BloodHound	Графовый инструмент анализа отношений и путей управления в AD.
CA	Certification Authority. Центр сертификации.
Credential material	Любые артефакты, которые помогают удостоверить личность: пароли, хэши, билеты, сертификаты, токены.
DACL	Discretionary ACL - часть ACL, определяющая права доступа.

DCSync	Концепт злоупотребления правами репликации каталога.
DC	Domain Controller. Контроллер домена.
Delegation	Механизм, позволяющий сервису действовать от имени пользователя.

Элемент	**Комментарий**
DFSR	Distributed File System Replication. Репликация SYSVOL и не только.
dMSA	Delegated Managed Service Account. Новый тип управляемого сервисного аккаунта в Windows Server 2025.
DN	Distinguished Name. Полное имя объекта в LDAP-иерархии.
Domain Admins	Классическая привилегированная доменная группа.
EDR	Endpoint Detection and Response. Система обнаружения и реагирования на конечных точках.
Enrollment rights	Права на запрос и выпуск сертификатов.
ESC	Семейство известных классов проблем в AD CS по терминологии сообщества.
Forest	Самый верхний логический контейнер AD.
gMSA	Group Managed Service Account. Управляемая сервисная учетка для нескольких серверов.
GPO	Group Policy Object. Политика, применяемая к пользователям и компьютерам.
Helpdesk tier	Операционный уровень поддержки, который не должен обладать лишним доступом к Tier 0/1.
Impacket	Популярный набор Python-инструментов для работы с протоколами Windows.

Элемент	**Комментарий**
KDC	Key Distribution Center. Компонент Kerberos на DC.
Kerberos	Основной протокол аутентификации в домене Windows.
LAPS	Local Administrator Password Solution. Механизм автоматического управления локальными админ-паролями.
LDAP	Протокол и модель запросов к каталогу.
Lateral movement	Переход с одного хоста или идентичности

	на другую внутри инфраструктуры.
LSASS	Процесс Windows, связанный с аутентификацией и чувствительными артефактами.
Mimikatz	Известное семейство инструментов для работы с credential material и Windows security internals.
NTLM	Legacy-протокол аутентификации Windows.
OU	Organizational Unit. Логический контейнер объектов в AD.
PKI	Public Key Infrastructure. Инфраструктура открытых ключей.
Pre-auth	Kerberos preauthentication - защита, которая усложняет часть офлайн-сценариев.
RBCD	Resource-Based Constrained Delegation. Делегация, задаваемая на целевом ресурсе.

Элемент	**Комментарий**
Remediation	План исправления проблемы.
RSAT	Remote Server Administration Tools. Набор админских модулей для Windows.
Scope	Границы разрешенных действий и систем в тесте.
SID	Security Identifier. Уникальный идентификатор субъекта безопасности.
SIEM	Платформа для централизованного сбора и анализа событий безопасности.
SPN	Service Principal Name. Идентификатор сервиса для Kerberos.
SYSVOL	Каталог на DC, где хранятся GPO и связанные данные.
Tier 0	Самые критичные identity- и control-plane-активы домена.
TGT	Ticket Granting Ticket. Билет Kerberos для запроса сервисных билетов.
TGS	Ticket Granting Service ticket. Сервисный билет Kerberos для доступа к конкретному сервису.
Trust	Отношение доверия между доменами и/или лесами.
WinRM	Windows Remote Management. Канал удаленного управления.

Элемент	Комментарий
WriteDacl	Право изменять ACL объекта. Очень опасно на чувствительных объектах.

15. Книги и ресурсы для дальнейшей прокачки

Книги

- Denis Isakov, Pentesting Active Directory and Windows-based Infrastructure - Amazon
- Ed Skoudis, The Art of Network Penetration Testing - Amazon
- Peter Kim, The Hacker Playbook 3 - Amazon
- Phil Bramwell, Hands-On Penetration Testing on Windows - Amazon
- Dishan Francis, Mastering Active Directory, Third Edition - Amazon
- Steve Syfuhs, Windows Security Internals - Amazon
- Joe Vest, Red Team Development and Operations - Amazon

Полезные публичные ресурсы и референсы

Microsoft Learn - AD DS overview - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft Learn - Kerberos authentication overview - https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Microsoft Learn - AD CS overview - https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview

Microsoft Learn - Windows Server 2025 functional levels - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels

Microsoft Learn - Windows LAPS overview - https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview

Microsoft Learn - dMSA overview - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/delegated-managed-service-accounts/delegated-managed-service-accounts-overview

zer1t0 - Attacking Active Directory: 0 to 0.9 - https://zer1t0.gitlab.io/posts/attacking_ad/

Mayfly - AD Pentest Mindmap 2k25 - https://mayfly277.github.io/posts/AD-mindmap-2k25/

GitHub - geeksniper/active-directory-pentest - https://github.com/geeksniper/active-directory-pentest

GitHub - esidate/pentesting-active-directory - https://github.com/esidate/pentesting-active-directory

GitHub - linWinPwn - https://github.com/lefayjey/linWinPwn

GitHub - Awesome-Active-Directory-PenTest-Tools - https://github.com/JoasASantos/Awesome-Active-Directory-PenTest-Tools

GitBook - The Ultimate Active Directory CheatSheet - https://karim-ashraf.gitbook.io/karim_ashraf_space/the-ultimate-active-directory-cheatsheet

Habr - Active Directory глазами Impacket - https://habr.com/ru/companies/ruvds/articles/743444/

Habr - Типичные ошибки настройки Active Directory - https://habr.com/ru/companies/vkusvill/articles/1010812/

Hack The Box - Active Directory hardening checklist - https://www.hackthebox.com/blog/active-directory-hardening-checklist-and-best-practices

Как работать с референсами

Не пытайся проглотить все сразу. Возьми одну лабораторию, один mindmap-ресурс, один обзорный гайд и одну хорошую книгу. После каждой темы делай свои короткие заметки: объект, риск, artifact, impact, remediation.

16. Финальный чек-лист перед интервью

Я могу одной-двумя фразами объяснить, что такое LDAP, Kerberos, SPN, ACL, GPO, LAPS, gMSA, dMSA и AD CS.

Я понимаю разницу между identity context, членством в группах, прямыми правами и косвенным контролем через ACL/GPO/delegation.

Я могу описать базовый practical flow AD-пентеста без шоу и без опасных лишних действий.

Я знаю, какие 10-15 misconfiguration чаще всего дают реальный impact в домене.

Я не путаю read-only enumeration, controlled validation и destructive actions.

Я умею спокойно объяснить DCSync, Golden Ticket, Kerberoast, AS-REP exposure, delegation abuse и AD CS misconfig на уровне механики и риска.

Я могу рассказать хотя бы два своих STAR-кейса или качественно адаптировать демо-кейсы под свой опыт.

Я умею формулировать finding как цепочку: что нашли -> почему это работает -> к чему ведет -> как исправить.

Я помню, что сильный ответ на интервью - это не набор громких слов, а ясность, дисциплина и инженерная логика.

Последний совет

На AD-интервью сильнее всего работает не бравада, а спокойная инженерная логика. Когда ты умеешь связать объект, право, риск, impact и remediation, собеседование обычно идет в твою пользу.

Эта брошюра не должна заменить практику. Ее задача - помочь тебе быстрее собрать в голове систему. А дальше уже все решают руки, дисциплина и умение думать.

Иван Пискунов | White2Hack