Сканер уязвимостей ADPulse DC

ADPulse — это инструмент аудита безопасности Active Directory с открытым исходным кодом, который подключается к контроллеру домена через LDAP(S), выполняет 35 автоматических проверок безопасности и создает подробные отчеты в консольном формате, формате JSON и HTML.

Он предназначен для ИТ-администраторов, специалистов по тестированию на проникновение и групп безопасности, которым необходима быстрая оценка неправильных настроек Active Directory и поверхности атаки в режиме только для чтения.

> ADPulse работает в режиме только для чтения и не вносит изменений в инфраструктуру — но это не делает его использование безобидным с правовой точки зрения.

Используйте инструмент только если:

- Вы администратор или сотрудник ИБ своей организации
- У вас есть письменное разрешение на проведение аудита (scope of work, договор, приказ)
- Вы проводите работы в рамках официального пентеста с согласованным техническим заданием

Проверки безопасности

#	Проверять	Описание
1	**Политика паролей**	Минимальная длина, история, сложность, порог блокировки, обратимое шифрование, детализированные PSO.
2	**Привилегированные учетные записи**	Членство в группах администраторов домена, администраторов предприятия, администраторов схем и других группах с конфиденциальной информацией; устаревшие данные участников, пароли, срок действия которых не истекает, пароли в описаниях, встроенный статус администратора, возраст krbtgt.
3	**Kerberos**	Учетные записи, допускающие завышение рейтинга Kerberos (SPN в объектах пользователей), учетные записи, допускающие завышение рейтинга AS-REP, шифрование только DES, высокоприоритетные цели, объединяющие adminCount=1 + SPN + PasswordNeverExpires

4	**Неограниченное делегирование**	Компьютеры и учетные записи пользователей, не относящиеся к центру обработки данных, используются для неограниченного делегирования полномочий Kerberos.
5	**Ограниченное делегирование**	Учетные записи с переходом протокола (S4U2Self) и стандартными целями с ограниченным делегированием.
6	**ADCS / PKI**	ESC1, ESC2, ESC3, ESC6, ESC8, ESC9, ESC10, ESC11, ESC13, ESC15, слабые размеры ключей, перечисление ACL участников
7	**Доверительное использование доменов**	Двустороннее доверие без фильтрации SID, доверие между лесами, внешнее доверие.
8	**Гигиена аккаунта**	Устаревшие пользователи/компьютеры, учетные записи, в которые никогда не входили, флаг PASSWD_NOTREQD, обратимое шифрование для каждой учетной записи, старые пароли, повторяющиеся SPN.
9	**Безопасность протокола**	Подписание LDAP/привязка каналов, версии операционных систем контроллеров домена, функциональный уровень домена/леса, рекомендации по NTLMv1/WDigest.
10	**Объекты групповой политики**	Отключенные, осиротевшие, несвязанные и пустые групповые политики; чрезмерное количество групповых политик.
11	**LAPS**	Обнаружение устаревших схем LAPS и схем Windows LAPS; компьютеры без паролей LAPS.
12	**LAPS coverage**	Процентное покрытие всех компьютеров, не являющихся центрами обработки данных, с паролем, управляемым LAPS.
13	**DNS и инфраструктура**	Использование подстановочных DNS-записей, рекомендации по отравлению LLMNR/NetBIOS-NS.
14	**Контроллеры домена**	Обнаружение отдельного контроллера домена, устаревшие ОС на контроллерах домена, роли FSMO, политика репликации паролей RODC.
15	**ACL / Права доступа**	Права доступа ESC4, ESC5, ESC7, DCSync для непривилегированных субъектов, группа защищенных пользователей, списки контроля доступа (ACL) для делегирования.
16	**Дополнительные функции**	Корзина Active Directory, управление привилегированным доступом (PAM)
17	**Replication Health**	Количество сайтов, интервалы репликации связей между сайтами, объекты nTDSDSA
18	**Служебные аккаунты**	Внедрение gMSA, обычные учетные записи пользователей, учетные записи пользователей с adminCount=1
19	**Miscellaneous Hardening**	Квота для учетных записей машин, время жизни удаленных файлов, членство в группах администраторов схемы/корпоративных администраторов, гостевая учетная запись, рекомендации по политике аудита.
20	**Устаревшие операционные системы**	Включены учетные записи компьютеров, сообщающие об окончании поддержки версий Windows.
21	**Устаревшие протоколы**	Обнаружение SMBv1, обеспечение подписи SMB, принятие нулевых сессий (проверка сети в реальном времени)

22	**Exchange**	Группа разрешений Windows Exchange (PrivExchange / CVE-2019-0686), доверенная подсистема Exchange
23	**Защищенные администраторы**	adminCount=1 inventory — orphaned, ghost (disabled) and stale accounts
24	**Пароли в описаниях**	Обнаружение учетных данных, хранящихся в поле «Описание» пользователей, администраторов и компьютеров, на основе ключевых слов.
25	**GPP / cpassword (MS14-025)**	Программа выполняет обход файлов XML с атрибутами групповых политик в каталоге SYSVOL `cpassword` и расшифровывает их с помощью общеизвестного ключа AES от Microsoft.
26	**AdminSDHolder ACL**	Считывает двоичный список `CN=AdminSDHolder` контроля доступа (DACL) и помечает непривилегированные учетные записи с правами на запись — эти записи автоматически распространяются на все защищенные учетные записи каждые 60 минут через SDProp.
27	**История SID**	Обнаруживает учетные записи с `sIDHistory` заполненными данными; повышает статус до CRITICAL, если какой-либо внедренный SID соответствует привилегированной группе (администраторы домена, администраторы предприятия и т. д.).
28	**Shadow Credentials**	Функция помечает неожиданные `msDS-KeyCredentialLink` записи в объектах пользователей и компьютеров, позволяя использовать аутентификацию на основе сертификатов без знания пароля учетной записи.
29	**RC4 / Устаревшее шифрование Kerberos**	Проверяет `msDS-SupportedEncryptionTypes` учетные записи служб, контроллеров домена и администраторов, чтобы выявить те, которые по-прежнему разрешают использование RC4-HMAC — уязвимого типа шифрования, специально запрашиваемого злоумышленниками для взлома в автономном режиме.

30	**Foreign Security Principals in Privileged Groups**	Выявляет `CN=ForeignSecurityPrincipals` и помечает любые FSP из доверенного домена, являющиеся членами конфиденциальной локальной группы (администраторы домена, операторы резервного копирования и т. д.).

31	**Доступ, совместимый с версиями до Windows 2000.**	Проверяет, являются ли
		`Everyone`
		или
		`Anonymous Logon`
		являются членами этой группы, что позволяет осуществлять неаутентифицированное перечисление SAMR/LSARPC из любой точки сети.

32	**Dangerous Constrained Delegation Targets**	Проводит перекрестную проверку целевых объектов делегирования на основе имен хостов контроллеров домена и помечает учетные записи, делегирующие делегирование приоритетным классам обслуживания (
		`ldap/`
		,
		`cifs/`
		,
		`host/`
		,
		`gc/`
		,
		`krbtgt/`
		) на контроллерах домена.

33	**Orphaned AD Subnets**	Обнаруживает подсети без `siteObject` назначений, в результате чего клиенты получают случайный контроллер домена и потенциально маршрутизируют трафик аутентификации через каналы WAN.
34	**Legacy FRS SYSVOL Replication**	Определяет, продолжает ли SYSVOL реплицироваться с помощью устаревшей службы репликации файлов (File Replication Service) вместо DFSR, и помечает состояния, остановившиеся в процессе миграции.

35	**RBCD on Domain Object / DCs**	Проверяет `msDS-AllowedToActOnBehalfOfOtherIdentity` состояние головного узла домена NC и всех объектов компьютеров контроллера домена — любая из конфигураций предоставляет фактические права администратора домена разрешенным субъектам через S4U2Proxy.

Требования

- Python 3.8+
- Сетевой доступ к контроллеру домена (порт 636 для LDAPS, 389 для LDAP, 445 для SMB-зондов)
- Учетная запись домена с правами на чтение (для большинства проверок права администратора не требуются).
- Для проверки 25 (GPP/cpassword): SYSVOL должен быть доступен с сканирующего хоста (UNC-путь в Windows или монтирование Samba в Linux/macOS).

Установка:

```
git clone https://github.com/yourorg/adpulse.git
cd adpulse

# Содание виртуальной среды
python -m venv venv
source venv/bin/activate        # Linux / macOS
venv\Scripts\activate           # Windows

# Устанвока зависимостей
pip install -r requirements.txt
```

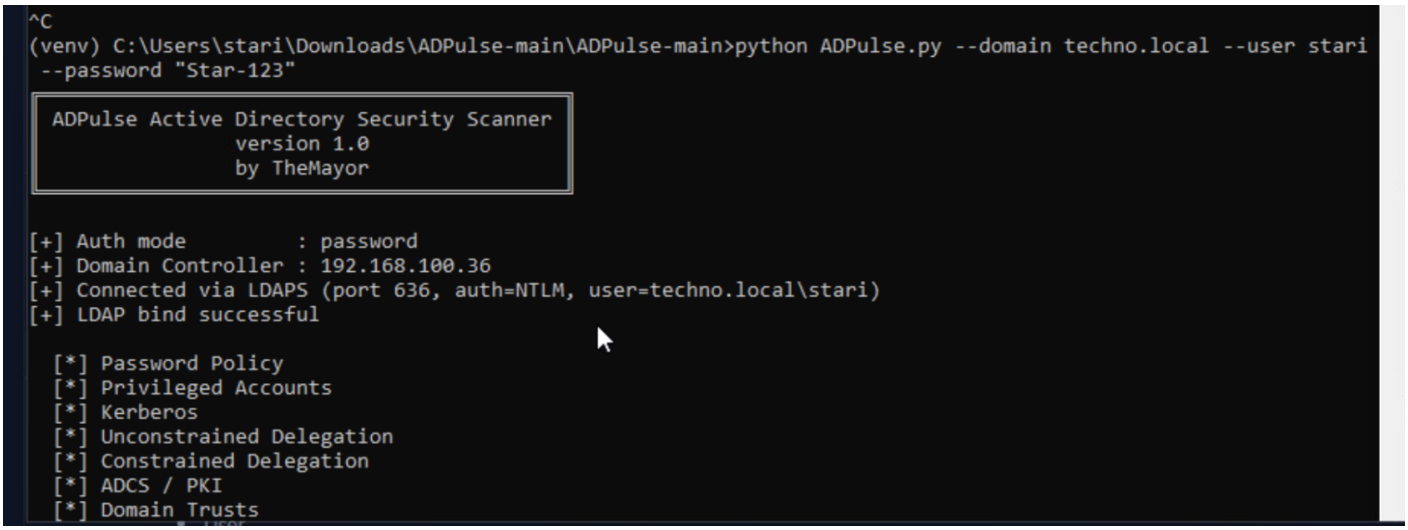
Возможные аргументы

Аргумент	Необходимый	По умолчанию	Описание
`--domain`	Да	—	Целевой домен AD (например `corp.local`)
`--user`	Да	—	Имя пользователя домена
`--password`	Да	—	пароль домена
`--hash`	Только без пароля	—	Хэш домена NTLM

Аргумент	Необходимый	По умолчанию	Описание
`--dc-ip`	Нет	Автоматически решено	IP-адрес контроллера домена
`--report`	Нет	`all`	Формат отчета: `console`, `json`, `html`, или `all`
`--output-dir`	Нет	`.`	Родительский каталог для `Reports/` папки
`--no-color`	Нет	`false`	Отключить цвет в выводе на консоль

Базовое сканирование

```
python ADPulse.py --domain corp.local --user user --password "P@ssw0rd!"
```



После сканирования вы увидите в командной строке все обнаруженные уязвимости

```
================================================================================
  ADPulse ACTIVE DIRECTORY SECURITY SCAN REPORT
================================================================================
  Domain      : techno.local
  DC          : 192.168.100.36
  Scanned     : 2026-05-12 08:50:45
  Risk Score  : 0/100  [CRITICAL]
================================================================================

SUMMARY:
  CRITICAL  : 6 finding(s)
  HIGH      : 5 finding(s)
  MEDIUM    : 12 finding(s)
  LOW       : 1 finding(s)
  INFO      : 29 finding(s)

--------------------------------------------------------------------------------
AT A GLANCE — MOST CRITICAL FINDINGS:
--------------------------------------------------------------------------------
  [CRITICAL]  ESC1 - Enrollee-Supplied SAN + Client Auth
    2 template(s) allow domain privilege escalation via SAN manipulation.
    >> Disable 'Supply in the request' or enable manager approval.
  [CRITICAL]  ESC15 - Schema Version 1 Template with Enrollee-Supplied SAN
    1 schema v1 template(s) allow SAN supply and client auth.
    >> Upgrade template schema version or disable enrollee-supplied SAN.
  [CRITICAL]  ESC4 - Writable Certificate Template ACLs
    4 template/trustee combination(s).
```

• KerberosAuthentication

Также автоматически создаются отчеты на устройстве

```
[+] JSON report -> Reports\ad_scan_techno.local_20260512_085045.json
[+] HTML report -> Reports\ad_scan_techno.local_20260512_085045.html
```

откроем html отчет: 

ADPulse Active Directory Security Report

Domain: **techno.local** | DC: **192.168.100.36** | Scanned: **2026-05-12 08:50:45**

0 / 100 — CRITICAL RISK

CRITICAL	HIGH	MEDIUM	LOW	INFO
6	5	12	1	29

AT A GLANCE — MOST CRITICAL FINDINGS

CRITICAL **ESC1 - Enrollee-Supplied SAN + Client Auth** -25 pts

2 template(s) allow domain privilege escalation via SAN manipulation.

Disable 'Supply in the request' or enable manager approval.

CRITICAL **ESC15 - Schema Version 1 Template with Enrollee-Supplied SAN** -25 pts

1 schema v1 template(s) allow SAN supply and client auth.

Upgrade template schema version or disable enrollee-supplied SAN.

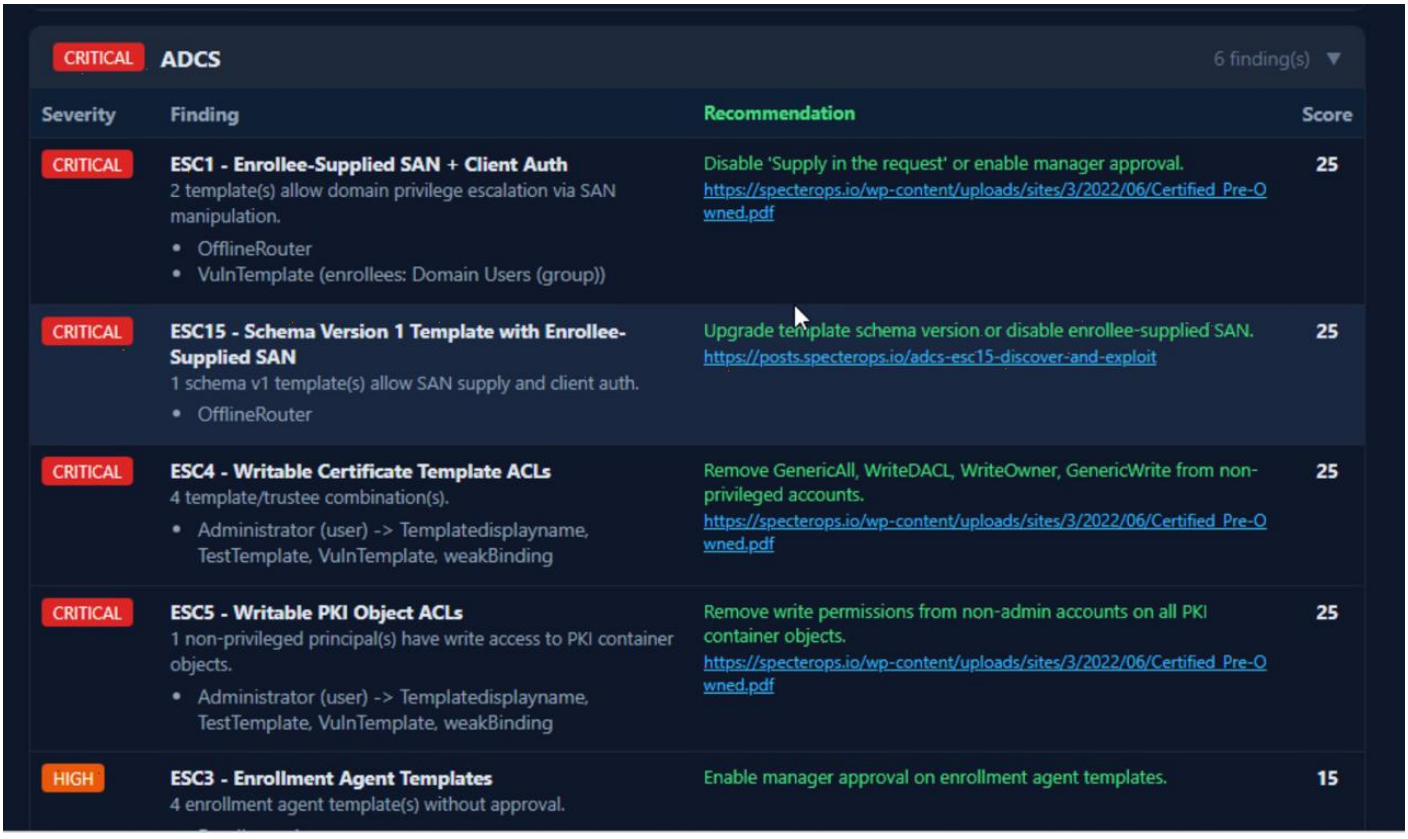
Подсчет очков

За каждое обнаруженное нарушение начисляется штраф в виде снижения оценки риска. Общий балл начинается со **100** и уменьшается за каждое обнаруженное нарушение:

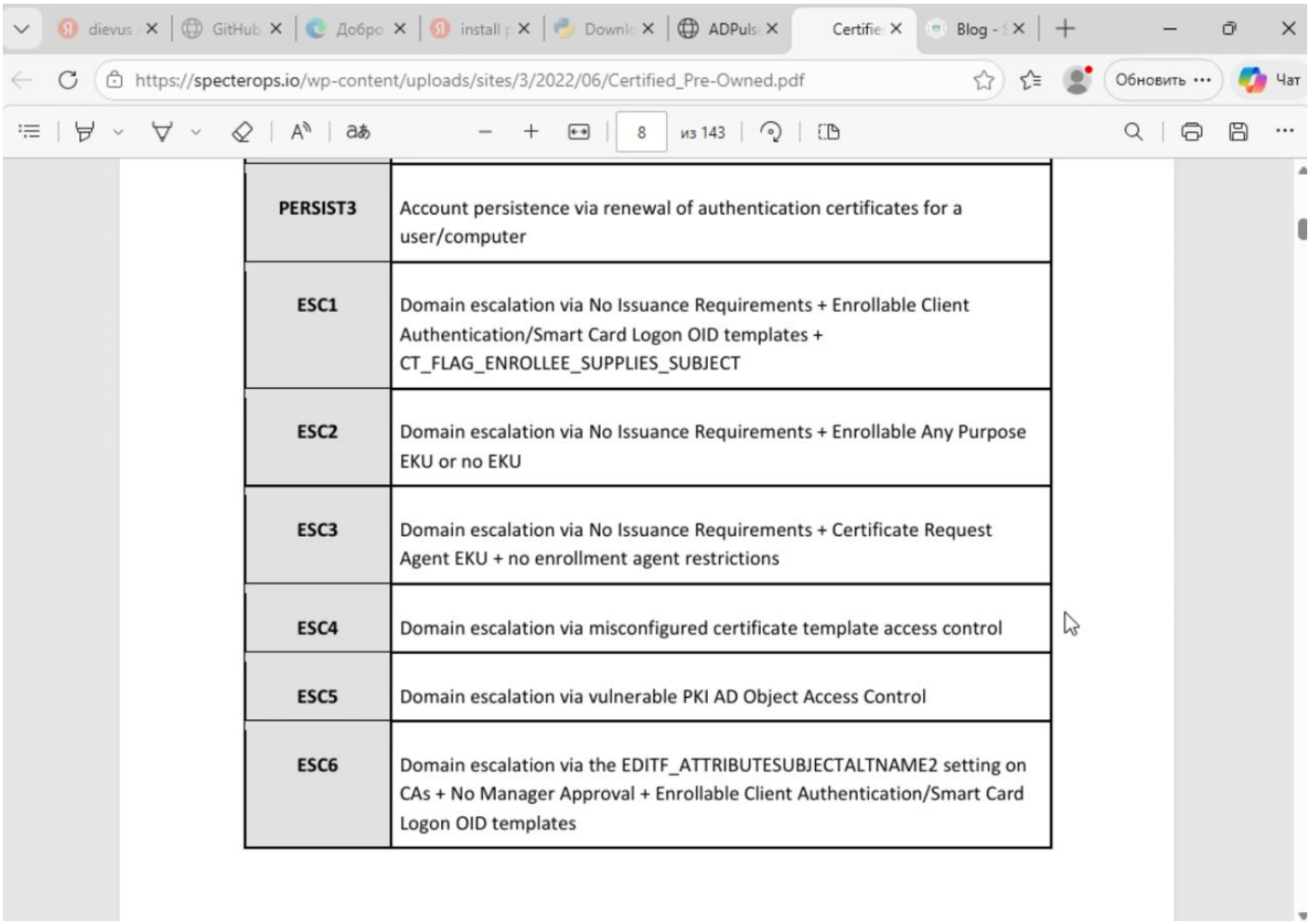
Счет	Уровень риска	Значение
80–100	НИЗКИЙ	Хорошая система безопасности, лишь незначительные проблемы.
60–79	СЕРЕДИНА	Существенные недостатки, которые следует устранить.
40–59	ВЫСОКИЙ	Присутствуют существенные уязвимости.
0–39	КРИТИЧЕСКИЙ	Серьезные риски — требуется немедленное устранение последствий.

Устранение уязвимостей

В отчете будут уже указаны рекомендации для устранения:



При переходе по предложенным ссылкам, вы сможете подробно изучить их



PERSIST3	Account persistence via renewal of authentication certificates for a user/computer
ESC1	Domain escalation via No Issuance Requirements + Enrollable Client Authentication/Smart Card Logon OID templates + CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT
ESC2	Domain escalation via No Issuance Requirements + Enrollable Any Purpose EKU or no EKU
ESC3	Domain escalation via No Issuance Requirements + Certificate Request Agent EKU + no enrollment agent restrictions
ESC4	Domain escalation via misconfigured certificate template access control
ESC5	Domain escalation via vulnerable PKI AD Object Access Control
ESC6	Domain escalation via the EDITF_ATTRIBUTESUBJECTALTNAME2 setting on CAs + No Manager Approval + Enrollable Client Authentication/Smart Card Logon OID templates

Revision #3
Created 2026-05-27 11:42:32 UTC by lerat
Updated 2026-05-27 11:56:58 UTC by lerat