Как навести порядок в доменной структуре?

Горшунов Никита Витальевич

Руководитель отдела ИБ ООО НПЦ «ВирТэк»

Инструменты и средства защиты для информационной безопасности

- МСЭ – межсетевые экраны (современное UTF или NGFW)
- АВЗ – антивирусная защита.
- Сканеры уязвимостей.
- IPS/IDS.
- DLP.
- WAF.
- SIEM.

Привилегированные права.

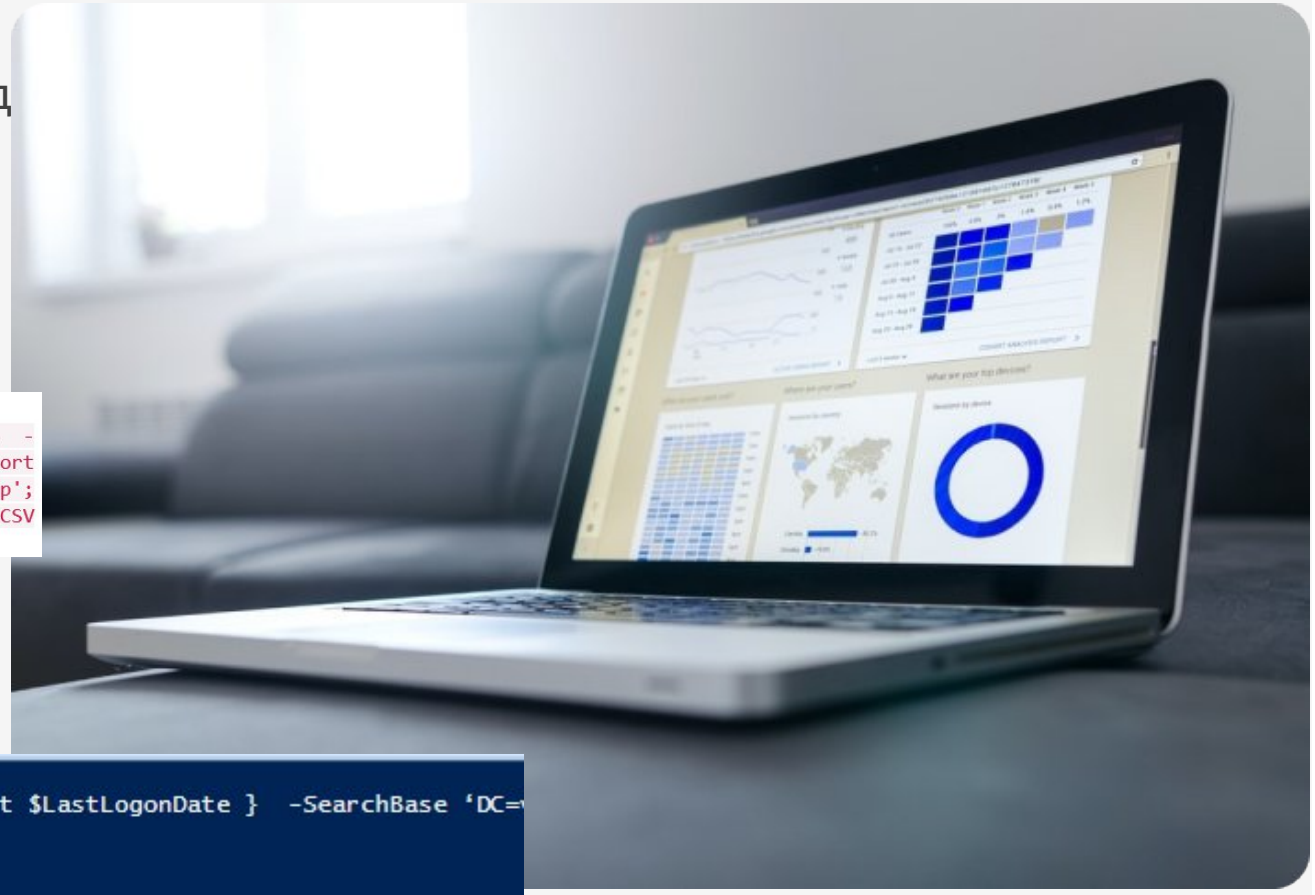
- Проверка и анализ прав пользователей в до
- Корректировка прав пользователей
- Контроль прав пользователей

Неактивные пользователи

- Не всегда своевременно блокируются УЗ сотруд при увольнении
- Не блокируются УЗ подрядчиков, контрагентов

Все легко проверяется через PowerShell

```
$LastLogonDate=(Get-Date).AddDays(-180)
Get-ADUser -Properties LastLogonTimeStamp -Filter {LastLogonTimeStamp -lt $LastLogonDate } -SearchBase 'OU=Users,OU=UFA,dc=company,dc=ru'| ?{$_.Enabled -eq $True} | Sort LastLogonTimeStamp| FT Name, @{N='lastlogontimestamp'; E={[DateTime]::FromFileTime($_.lastlogontimestamp)}} -AutoSize | Export-CSV c:\ps\inactive_users.csv
```

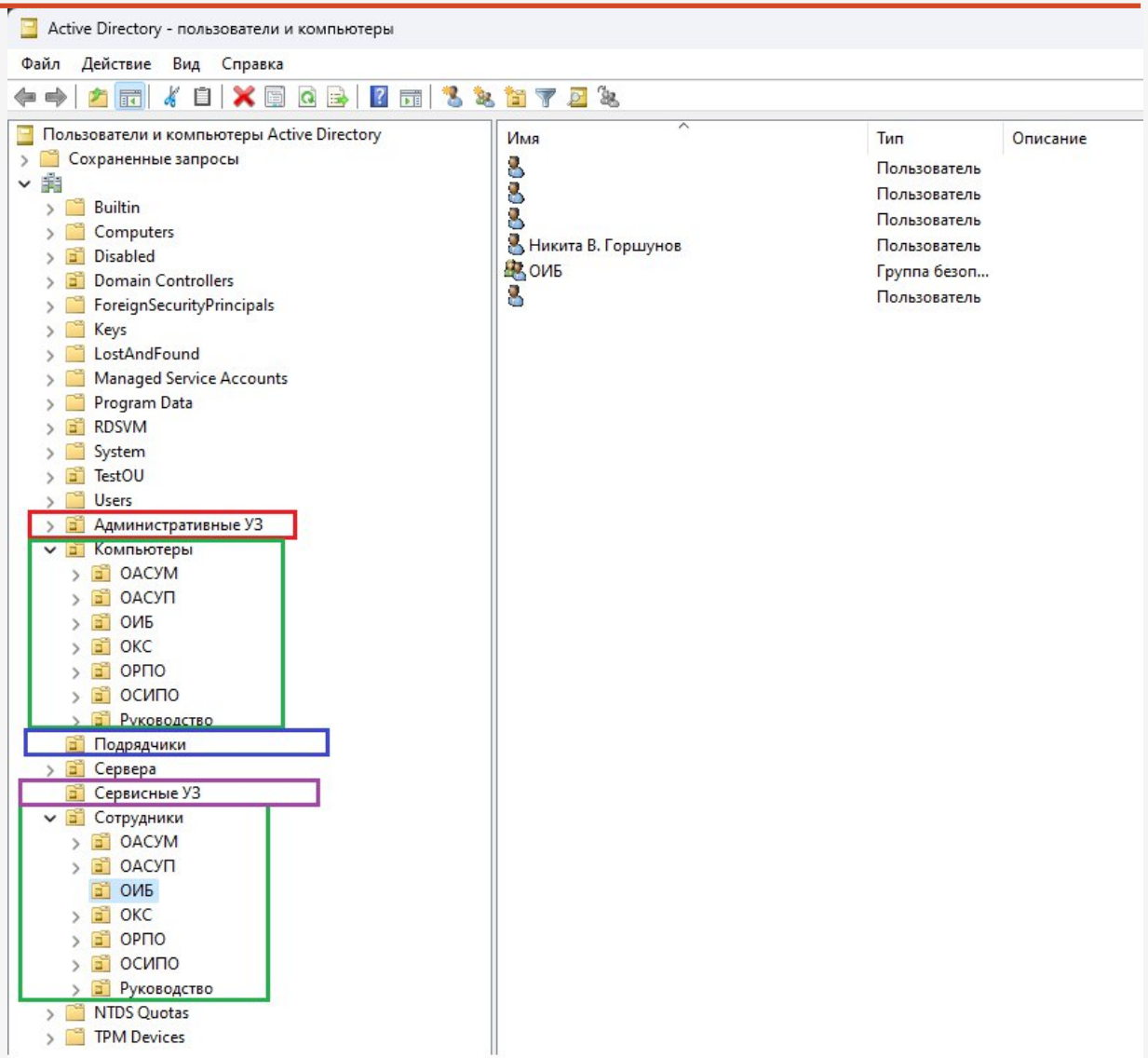


```
PS C:\Users\gorshunovnv> $LastLogonDate=(Get-Date).AddDays(-180)
Get-ADUser -Properties LastLogonTimeStamp -Filter {LastLogonTimeStamp -lt $LastLogonDate }  -SearchBase 'DC=

Name         lastlogontimestamp
----         ------------------
testuser     26.12.2022 10:28:57
ComConnector 19.05.2023 16:14:15


PS C:\Users\gorshunovnv>
```

Структура AD

Отдельные каталоги пользователей:

- Разделение пользователей и компьютеров по отделам, филиалам.
- Отдельный каталог для серверов
- Отдельный каталог для УЗ с привилегированными правами
- Отдельный каталог для сервисных УЗ
- Отдельный каталог для подрядчиков



Групповые политики GPO

- Настройка политик парольной защиты
- Настройка расширенного аудита
- Настройка установки антивирусных программ, программ удаленного доступа, агентов DLP и/или SIEM
- Распределение привилегированных прав

Настройка расширенного аудита для рабочих станций, серверов и контроллера домена:

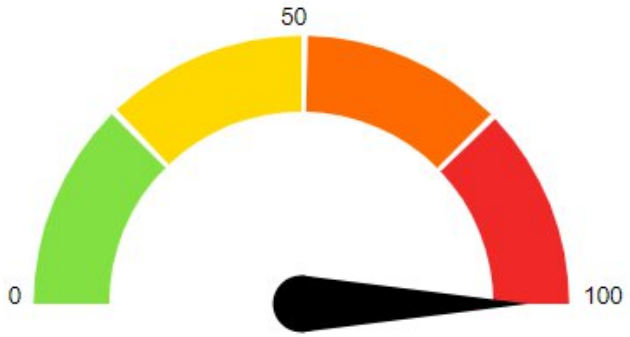
Категория	Описание	DC(Домен)	C(Сервер)	K(АРМ)
Вход учетной записи (Account Logon) — содержит события, регистрируемые при проверке учетных данных. Доменные учет станц				
Аудит проверки учетных данных (Audit Credential Validation)	Содержит событие 4776 «Попытка проверить учетные данные для учетной записи компьютера». На рабочих станциях регистрируется большое количество событий	Успех, Отказ	Успех, Отказ	Успех, Отказ
Аудит службы проверки подлинности Kerberos (Audit Kerberos Authentication Service)	События регистрируются только на контроллерах домена. Регистрируется большое количество событий. При включении аудита успехов регистрируются события запроса ticket granting ticket (TGT). При включении аудита отказов регистрируются события неудачных запросов TGT (неправильно имя, пароль и т.д.)	Успех, Отказ	-	-
Аудит операций с билетами службы Kerberos (Audit Kerberos Service Ticket Operations)	События регистрируются только на контроллерах домена. Регистрируется большое количество событий. При включении аудита успехов регистрируются события успешных запросов ticket granting service (TGS). При включении аудита отказов регистрируются события неудачных запросов TGS и их причины	Успех, Отказ	-	-
Аудит других событий входа учетных записей (Audit Other Logon/Logoff Events)	Включение аудита успехов на контроллере домена, серверах и рабочих станциях позволит отслеживать подключение и отключение к удаленному рабочему столу, блокировку и разблокировку рабочего стола. Число событий небольшое. Если определена политика делегирования учетных записей, включите аудит отказов на контроллерах домена, серверах и рабочих станциях	Успех, Отказ	Успех, (Отказ)	Успех, (Отказ)
Управление учетными записями (Account Management) — содержит события, связанные с новыми пользователями и группа учетными				
Аудит управления группами приложений (Audit Application Group	Содержит события, относящиеся к группам пользователей приложений (Application Group): создание, изменение, удаление группы и ее членов. Нет событий аудита отказов.	(Успех)	(Успех)	(Успех)

PingCastle

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Stale Object : 81 /100 — 10 rules matched

It is about operations related to user or computer objects

Privileged Accounts : 75 /100 — 8 rules matched

It is about administrators of the Active Directory

Trusts : 21 /100 — 2 rules matched

It is about connections between two Active Directories

Anomalies : 100 /100 — 16 rules matched

It is about specific security control points

PingCastle

Stale Objects

Stale Objects : 81 /100

It is about operations related to user or computer objects

Stale Objects rule details [10 rules matched on a total of 50]

Presence of wrong primary group for users: 11	+ 15 Point(s)
The LAN Manager Authentication Level allows the use of NTLMv1 or LM.	+ 15 Point(s)
Number of computers without password change for at least 3 months: 2	+ 15 Point(s)
Relatively high number of inactive user accounts: 89% (more than 25% of all users)	+ 10 Point(s)
Presence of non-supported versions of Windows 10 or Windows 11 = 6	+ 10 Point(s)

Privileged Accounts

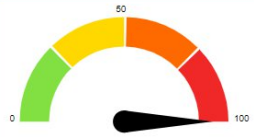
Privileged Accounts : 75 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [8 rules matched on a total of 45]

Presence of Admin accounts which do not have the flag "This account is sensitive and cannot be delegated": 16	+ 20 Point(s)
Presence of accounts with non-expiring passwords in the domain admin group (at least 2 accounts): 12	+ 15 Point(s)
The group Schema Admins is not empty: 12 account(s)	+ 10 Point(s)
Number of admin with a password older than 3 years: 1	+ 10 Point(s)

Anomalies analysis



Anomalies : 100 /100

It is about specific security control points

Anomalies rule details [16 rules matched on a total of 69]

Suspicious admin activities detected on 40 user(s)	+ 40 Point(s)
Last change of the Kerberos password: 1460 day(s) ago	+ 40 Point(s)
LAPS doesn't seem to be installed	+ 15 Point(s)
The audit policy on domain controllers does not collect key events.	+ 10 Point(s)
Policy where the password length is less than 8 characters: 1	+ 10 Point(s)

LAPS doesn't seem to be installed — + 15 Point(s)

Check if the LAPS tool to handle the native local administrator passwords is installed

Rule ID:
A-LAPS-Not-Installed

Description:
The purpose is to make sure that there is a proper password policy in place for the native local administrator account.

Technical explanation:
LAPS (Local Administrator Password Solution) is the advised solution to handle passwords for the native local administrator account on all workstations, as it is a simple way to handle most of the subject.

Advised solution:
If you don't have any provisioning process or password solution to manage local administrators, you should install the LAPS solution. If you mitigate the risk differently, you should add this rule as an exception, as the risk is covered.

Points:
15 points if present

Documentation:
https://www.microsoft.com/en-us/download/details.aspx?id=46899
[US]STIG V-36438 - Local administrator accounts on domain systems must not share the same password.
[FR]ANSSI CERTFR-2015-ACT-046
[MITRE]T1078.003 Valid Accounts: Local Accounts
[MITRE]Mitre Att&ck - Mitigation - Privileged Account Management

Details:
The detail can be found in LAPS

DSInternals

Часто встречающиеся пароли пользователей из практики:

- Ctynz,hm2023, Yjz,hm2024 – месяц и год смены пароля
- Gfhjkm2023, GFhjkm01 – слово «пароль» и год или номер по порядку применения
- Anastasia1, Nikita022024 – имя (свое, жены, дочери) и какой то номер
- Qwerty, Password, Qaz – самые распространенные слова

Инструмент показывает:

- Пароли, хранящиеся с использованием обратимого шифрования
- УЗ без пароля
- УЗ, пароли которых имеются в базе
- УЗ имеющие одинаковые пароли
- УЗ, у которых пароль не требуется

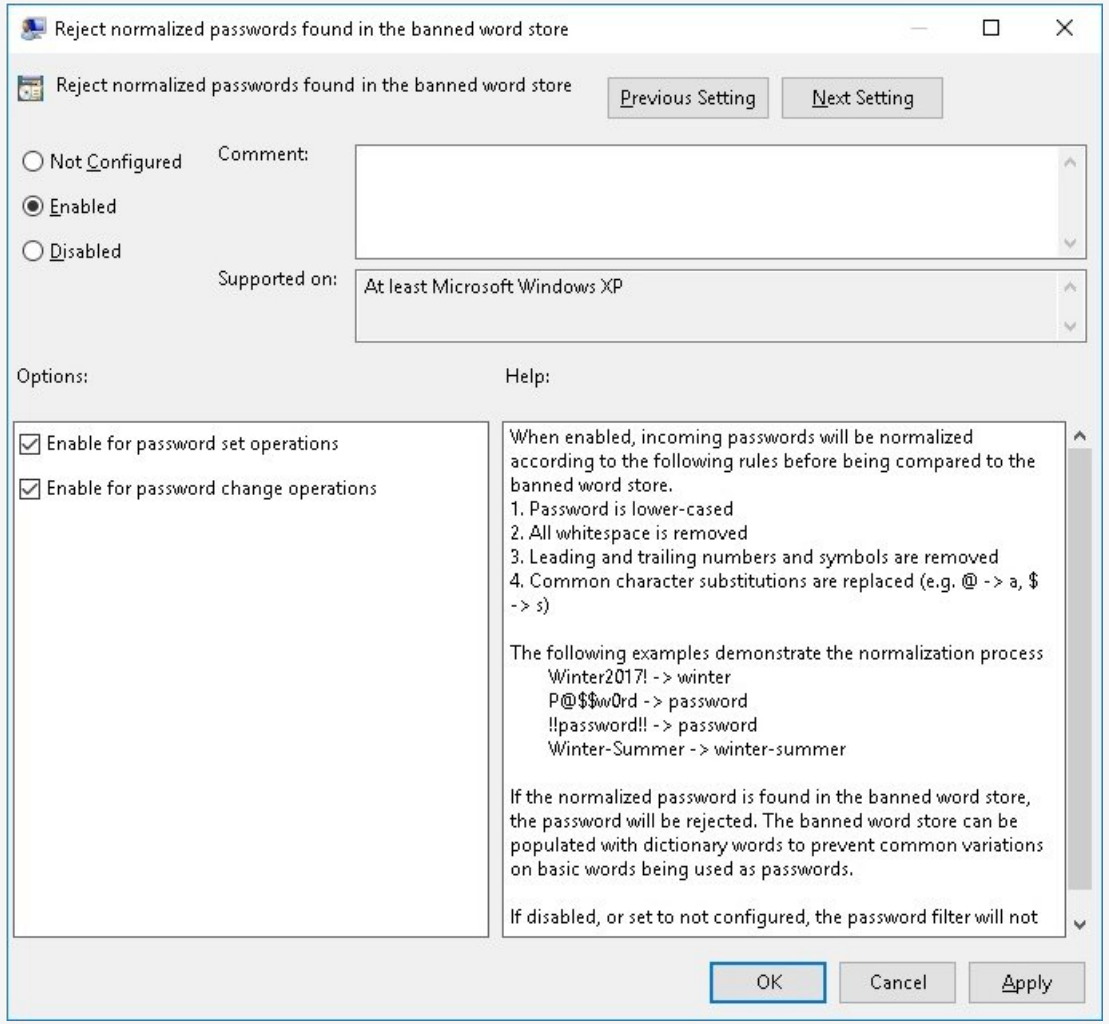
```
Active Directory Password Quality Report
----------------------------------------

Passwords of these accounts are stored using reversible encryption:

LM hashes of passwords of these accounts are present:

These accounts have no password set:
  User1

Passwords of these accounts have been found in the dictionary:
  User2                 Qwerty12345
  USer3                 Ctynz,hm2023

Historical passwords of these accounts have been found in the dictionary:
  History               Qaz123

These groups of accounts have the same passwords:
  Group 1:
  User4
  User5

  Group 2:
  User7
  User8

These computer accounts have default passwords:

Kerberos AES keys are missing from these accounts:

Kerberos pre-authentication is not required for these accounts:

Only DES encryption is allowed to be used with these accounts:

These administrative accounts are allowed to be delegated to a service:

Passwords of these accounts will never expire:

These accounts are not required to have a password:
```

Lithnet Password Protection

Настройка проводится через GPO. Возможно настроить:

- Запрет слов из словаря
- Запрет определенных слов в пароле (нормализированное представление)
- Запрет использования имени УЗ в пароле

Состояние	Состояние
Passwords must match a specified regular expression	Не задана
Passwords must meet specified number of complexity points	Не задана
Enable length-based complexity rules	Не задана
Minimum password length	Не задана
Reject passwords that contain the user's account name	Включена
Reject passwords that contain the user's display name	Включена
Reject passwords found in the compromised password store	Включена
Reject normalized passwords found in the compromised password sto...	Не задана
Reject normalized passwords found in the banned word store	Включена
Passwords must not match a specified regular expression	Не задана



Рекомендации

Пароли:

- Смена паролей год для пользователей, полгода для администраторов;
- Сложность пароля включена
- Необратимое шифрование
- Настройка проверки паролей по словарям
- При возможности двухфакторная авторизация
- 5 попыток ввода пароля до блокировки

Общие:

- Автоматическое оповещение сотрудников ИТ и ИБ при планировании увольнения сотрудников (скриптами из 1С)
- В случае увольнения администраторов – изменение всех известных ему паролей
- Использование менеджеров паролей
- Установка срока действия УЗ для временных работников, подрядчиков, контрагентов.
- Максимальное заполнение полей карточки пользователя в AD
- Обучение/оповещение сотрудников в части киберграммотности
- Проведение тренировок по фишингу
- Настройка LAPS

Спасибо за внимание!