## MSSQL Server bilgi toplama

**AMAÇ:** metasploit enum modülü veritabanı hakkında bilgi toplanması

**GEREKSİNİMLER:** Kali Linux, nmap, metasploit

**Adım 1 –** Putty ile Kali Linux üzerinde oturum açılır.

**Adım 2** – Komut satırında Metasploit çalıştırılır.

```
msfconsole
```

**Adım 3 –** mssql_enum modülü yüklenir, gerekli parametreler girilir.

```
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
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(mssql_enum) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
msf auxiliary(mssql_enum) > set PASSWORD 123
PASSWORD => 123
```

**Adım 4 –** SQL Server konfigürasyon bilgisi, üzerinde bulunan veritabanları, veritabanlarının veri dosyaları, kullanıcı bilgileri görüntülenir.

```
msf auxiliary(mssql_enum) > run

[*] Running MS SQL Server Enumeration...
[*] Version:
[*]     Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
[*]             Feb 10 2012 19:39:15
[*]             Copyright (c) Microsoft Corporation
[*]             Express Edition (64-bit) on Windows NT 6.2 <X64> (Build 9200: ) (Hypervisor)
[*] 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\MSSQL11.SQLEXPRESS\MSSQL\DATA\master.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\mastlog.ldf
[*]     Database name:tempdb
[*]     Database Files for tempdb:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\tempdb.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\templog.ldf
[*]     Database name:model
[*]     Database Files for model:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\model.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\modellog.ldf
[*]     Database name:msdb
[*]     Database Files for msdb:
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\MSDBData.mdf
[*]             c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA\MSDBLog.ldf
[*] System Logins on this Server:
[*]     sa
[*]     ##MS_SQLResourceSigningCertificate##
[*]     ##MS_SQLReplicationSigningCertificate##
[*]     ##MS_SQLAuthenticatorCertificate##
[*]     ##MS_PolicySigningCertificate##
[*]     ##MS_SmoExtendedSigningCertificate##
[*]     ##MS_PolicyEventProcessingLogin##
[*]     ##MS_PolicyTsqlExecutionLogin##
[*]     ##MS_AgentSigningCertificate##
[*]     DESKTOP-TSI14TN\sqlegitim
[*]     NT SERVICE\SQLWriter
[*]     NT SERVICE\Winmgmt
[*]     NT Service\MSSQL$SQLEXPRESS
[*]     BUILTIN\Users
[*]     NT AUTHORITY\SYSTEM
[*]     sge_user
```

**Adım 5 –** Kullanıcılar hakkında bilgi toplanır.

```
[*] Disabled Accounts:
[*]     ##MS_PolicyEventProcessingLogin##
[*]     ##MS_PolicyTsqlExecutionLogin##
[*] No Accounts Policy is set for:
[*]     All System Accounts have the Windows Account Policy Applied to them.
[*] Password Expiration is not checked for:
[*]     sa
[*]     ##MS_PolicyEventProcessingLogin##
[*]     ##MS_PolicyTsqlExecutionLogin##
[*]     sqe_user
[*] System Admin Logins on this Server:
[*]     sa
[*]     DESKTOP-TSI14TN\sqlegitim
[*]     NT SERVICE\SQLWriter
[*]     NT SERVICE\Winmgmt
[*]     NT Service\MSSQL$SQLEXPRESS
[*] Windows Logins on this Server:
[*]     DESKTOP-TSI14TN\sqlegitim
[*]     NT SERVICE\SQLWriter
[*]     NT SERVICE\Winmgmt
[*]     NT Service\MSSQL$SQLEXPRESS
[*]     NT AUTHORITY\SYSTEM
[*] Windows Groups that can logins on this Server:
[*]     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.
```

**Adım 6 –** Procedure hakkında bilgiler toplanır.

```
[*] 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
```

**Sonuç:** Sql server üzerinde güvenlik denetlemesi gerçekleştirilmiş olur.