Ağ üzerinde yer alan MsSQL sunucularının msfconsole ile tespit edilmesi

AMAÇ: Ağ üzerinde yer alan MsSQL Serverlarının tespit edilmesi

GEREKSİNİMLER: Kali Linux, msfconsole

Adım 1 – Putty ile Kali Linux üzerinde oturum açılır.

Adım 2 – komut satırında aşağıda yer alan kod çalıştırılır.

```
msfconsole
```

Adım 4 – Mssql_ping modülü metasploit üzerinde yüklenir.

```
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
   THREADS     1                yes       The number of concurrent threads
   USERNAME    sa               no        The username to authenticate as
```

Adım 5 - Gerekli parametreler girilerek sonuçlar izlenir.

```
msf auxiliary(mssql_ping) > set RHOSTS 192.168.1.200-254
RHOSTS => 192.168.1.200-254
msf auxiliary(mssql_ping) > [redacted]
[redacted]
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
```

Sonuç: Çalışan sql server versiyon hakkında bilgi edinilmiş olur.