

## Ağ üzerinde yer alan MsSQL sunucularının tespit edilmesi

**AMAÇ:** Ağ üzerinde yer alan MsSQL Serverlarının tespit edilmesi

**GEREKİNİMLER:** Kali Linux, nmap

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

**Adım 2** – Aşağıda yer alan nmap komutu çalıştırılır.

```
root@kali:~# nmap -sS 192.168.10.1/24 -p1433 -n -open -sV
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-11-01 09:32 EET
Nmap scan report for 192.168.10.1
Host is up (0.075s latency).
PORT      STATE SERVICE VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2008 10.00.1600; RTM
MAC Address: 00:50:56:80:00:00 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (59 hosts up) scanned in 12.31 seconds
```

**Adım 3** – Elde edilen sunucu IP bilgisiyle detaylı bilgiye ulaşılmaya çalışılır.

```
root@SGE:~# nmap --script ms-sql-info 192.168.30.10 -p 1433
Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-04 16:31 EEST
Nmap scan report for 192.168.30.10
Host is up (0.0010s latency).
PORT      STATE SERVICE
1433/tcp open  ms-sql-s

Host script results:
|_ ms-sql-info:
|_   Windows server name: WIN-2TV451E8PRJ
|_   [192.168.30.10\PENTEST_EGITIM]
|_   Instance name: PENTEST_EGITIM
|_   Version: Microsoft SQL Server 2008 R2 RTM
|_     Version number: 10.50.1600.00
|_     Product: Microsoft SQL Server 2008 R2
|_     Service pack level: RTM
|_     Post-SP patches applied: No
|_   TCP port: 1433
|_   Clustered: No

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

**Sonuç:** Çalışan sql server versiyon hakkında bilgi edinilmiş olur.