MsSQL Server Nmap taraması

AMAÇ: MsSQL Server bilgisine Nmap aracılığı ile ulaşılması bulunması

GEREKSİNİMLER: Kali linux

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

Adım 2 – Nmap ağ taraması ile ağda yer alan SQL Serverlar listelenir

```
nmap –sS 192.168.0.1/24 –p1433 –open –sV –O
```

Adım 3 – Listelenen Sql sunuculardan bir tanesi hakkında bilgi almak için aşağıda yer alan komut çalıştırılır.

```
nmap -p1433 --script ms-sql-info --script-args mssql.instance-port=1433 192.168.0.XXX –O –sV –open
```

Adım 4 – Sql sunucu üzerinde çalışan portlar hakkında bilgi edinilir.

```
nmap –sS 192.168.0.XXX –sV –O -open
```

Sonuç: Çalışan sql server versiyon hakkında bilgi edinilmiş olur.