MSSQL Server hashdump uygulaması

AMAÇ: metasploit hashdump modülü ile şifre hash bilgilerinin elde edilmesi ve john ile açık şifrelerin bulunması

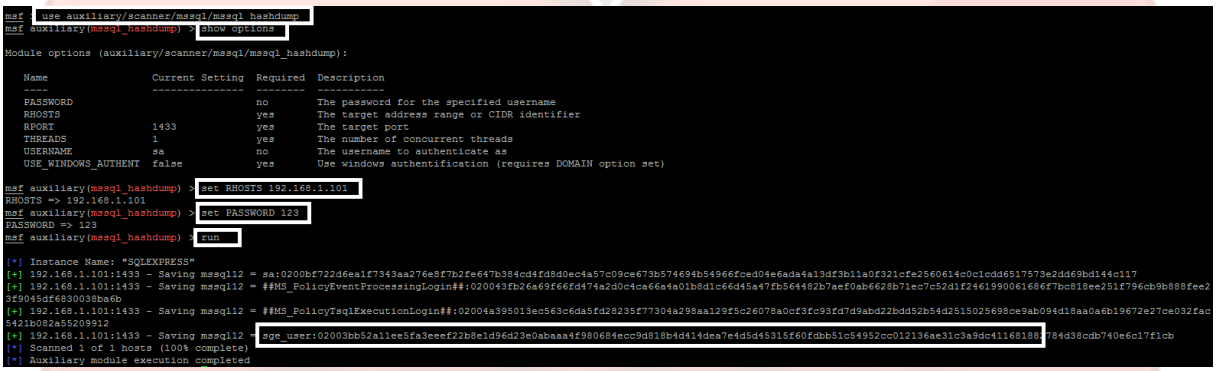
GEREKSİNİMLER: Kali Linux, nmap, metasploit

Adım 1 – Putty ile Kali Linux üzerinde oturum açılır.

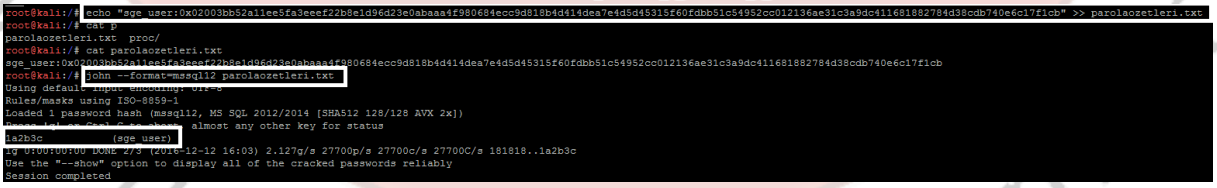
Adım 2 – Komut satırında Metasploit çalıştırılır.

```
msfconsole
```

Adım 3 – mssql_hashdump modülü yüklenir, gerekli parametreler girilir.



Adım 4 – SQL Server üzerinde bulunan sge_user kullanıcısının hash değeri echo komutu ile bir dosyaya yazılır. "John the ripper" uygulaması ile hash değerinden şifre elde edilir.



Sonuç: Sql server üzerinde yer alan veritabanı kullanıcısının açık şifresi elde edilir.