İç Ağa Sızma

(+) *Bu yazı gerçek sistemlerde denenmememiştir. Ancak birazdan göreceğin üzere sanal makinalarla başarılı bir şekilde simule edilebilmiştir.*

Diyelim ki bir arkadaşımızın public IP'sini öğrendik. Bunun üzerine hedef Public IP'yi (yani hedef network'ün en önündeki router'ı) port taramasına tabi tuttuğumuzu ve hedef router'da telnet servisinin açık olduğunu öğrendiğimizi varsayalım. Ayrıca telnet servisine anonymous girişini test ettiğimizde

```
saldirgan@saldirgan-MJKL:~$ telnet arkadasiminPublicIPsi

netmaster-38LQ login: anonymous
Password:                                   // boş bir şekilde enter'larız
```

komut satırını ele geçirebildiğimizi varsayalım.

```
netmaster@netmaster-38LQ:~$
```

Bu durumda hedef network'e, yani router'a sızmış durumdayız. Şimdi router'ın arkasındaki bir bilgisayara sızabilmek için router'daki arp tablosunu gösteren arp tool'unu kullanalım ve böylece hedef network'teki yerel IP'leri öğrenelim.

```
netmaster@netmaster-38LQ:~$ arp

Output:
        Address         HWtype      HWaddress           Flags Mask      Iface
        192.168.0.1     ether       00:10:18:de:ad:05   C               eth0
        192.168.0.15    ether       68:ab:27:cd:06:55   C               eth0
        192.168.0.19    ether       12:ac:87:fg:81:71   C               eth0
```

Belirlediğimiz bir yerel IP'ye anonymous olarak telnet bağlantısı kurmaya çalışalım.

```
netmaster@netmaster-38LQ:~$ telnet 192.168.0.15

tufan-KJQM login: anonymous
Password:                                   // boş bir şekilde enter'larız
```

Dikkat ederseniz telnet ile bağlandığımız router'ın konsolundan telnet ile iç ağdaki bilgisayara bağlanmaya çalıştık. Bunun sonucunda ekrana aşağıdaki gibi iç ağda yer alan bilgisayarın komut satırı geldiğinde

```
tufan@tufan-KJQM:~$
```

iç ağa sızmış oluruz. Burada yapılan işleme göre zincirleme iki tane telnet bağlantısı kurmuş durumdayız.

Tufan ---------- Router ---------- Saldırgan
telnet telnet

Özetle saldırganın konsol ekranında sırasıyla şu kodları çalıştırır:

```
saldirgan@saldirgan-MJKL:~$ telnet arkadasiminPublicIPsi        // Hedef router'a bağlanır
netmaster@netmaster-38LQ:~$ telnet 192.168.0.15                 // İç ağdaki host'a bağlanır
tufan@tufan-KJQM:~$
```

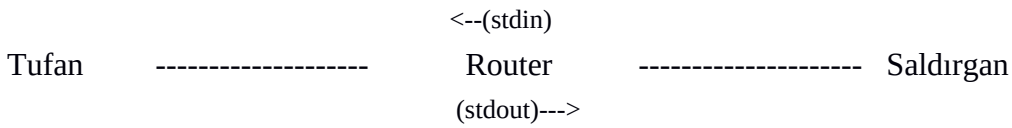
Yani yukarıdaki işlemler tamamen saldırganın konsol ekranında cereyan eder. Ancak bağlantılar gereği zincirleme bir telnet bağlantısı yapılmış olur.

Olayın Detaylı İzahı

İlk telnet bağlantısı ile biz router'a bağlanacağız. Böylece gireceğimiz her kod router'a sıçrayacaktır, orada çalışacaktır ve çıktısı bize dönecektir. İkinci telnet bağlantı kodunu girdiğimizde ise bu kod router'a sıçrayacaktır. Orada çalışacaktır ve router iç ağdaki bilgisayara bağlanacaktır. Böylece router'ın gireceği her kod iç ağdaki bilgisayara sıçrayacaktır, orada çalışacaktır, çıktısı ise geri router'a dönecektir.

Şimdi son duruma göre biz bir kod girdiğimizde kodumuz router'a sıçrayacaktır. Normalde router'da kodumuzun çalışması gerekir. Fakat router iç ağdaki bilgisayara telnet ile bağlı olduğundan router'daki kod iç ağdaki bilgisayara sıçrayacaktır. İç ağdaki bilgisayar kodu kendi sisteminde çalıştıracaktır, çıktısını router'a döndürecektir. Router ise bize çıktı olarak iç ağdaki bilgisayardan aldığı stdout'u verecektir. Sonuç olarak biz bir kod girdiğimizde kodumuz iç ağdaki bilgisayara doğru gidecektir, orada çalışacaktır ve çıktısı gene bize doğru dönecektir. Yani router arada transit rolü oynayacaktır.

Yukarıdaki şemaya göre saldırgan Tufana bağlanmaktadır. Yani iki kere telnet bağlantısı yaparak saldırgandan kurbana bağlanmaktayız. Aradaki router transit olmuş olur. Şimdi olayın somutlaşması için teknik olarak açıklayalım. Yukarıdaki telnet bağlantıları sayesinde Router'ın stdin'i Tufan'a gidiyor, stdout'u ise saldırgana gidiyor. Yani Router hiçbir şekilde ne kodları kendi konsoluna giriyor ne de çıktısını kendi konsoluna basıyor. Yaptığı şey sadece stdin'ini Ubuntu'ya vermek, stdout'unu ise Kali'ye vermektir.



Birinci telnet bağlantısı Router'ın stdout'unu saldırgana gönderirken, ikinci telnet bağlantısı Router'ın stdin'ini Tufan'a göndermektedir. Böylece Router transit olmuş olur.

Bir başka şekilde ifade edecek olursak router bizden stdin alacaktır. stdin'i iç ağdaki bilgisayarın stdin'ine iletecektir. İç ağdaki bilgisayar kendi stdin'ini komut satırında çalıştıracaktır. Oluşan stdout'u router'a gönderecektir. Router da aldığı stdout'u bize gönderecektir. Böylece ekranımıza stdout çıktısı yansıyacaktır. Yani ekranımıza iç ağdaki bilgisayarın stdout'u yansıyacaktır.

Zincirleme Telnet Bağlantısı Kurma Denemesi

(+) *Birebir denenmiştir ve başarıyla uygulanmıştır*

Saldırgan -> Router -> Kurban üçlüsüyle yaptığımız zincirleme telnet bağlantısını simule etmek için Kali -> Metasploitable -> Ubuntu üçlüsüyle telnet bağlantısı kuralım. Kali saldırgan olacaktır. Metasploitable router olacaktır. Ubuntu ise kurban olacaktır.

Not: Kali telnet istemcisidir. Metasploitable ve Ubuntu ise telnet server'dır. Metasplotaible da telnet server kurulu, ancak Ubuntu'da kurulu değilse kurmayı unutma. [bkz. Yaz Tatili 2014 / Ubuntu - Kali Telnet Kurulumu.docx]

Şimdi önce IP adreslerini verelim:

Metasploitable IP : 192.168.0.13

Ubuntu IP : 192.168.0.15

Ardından saldırgan olarak Kali konsolundan Metasploitable'a telnet ile bağlanalım.

Kali Terminal:

root@kali:~# telnet 192.168.0.13

Trying 192.168.0.13
Connected to 192.168.0.13
Escape character is '^]'.

metasploitable login: msfadmin // msfadmin girilir
Password: // msfadmin girilir

Last login: Sun Nov 27 13:32:10 EST 2016 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:50:00 UTC 2008

msfadmin@metasploitable:~$

Görüldüğü üzere Metasploitable'a bağlandık. Şimdi Metasploitable'dan Ubuntu'ya bağlanalım:

Kali Terminal:

msfadmin@metasploitable:~$ telnet 192.168.0.15

Trying 192.168.0.15
Escape character is '^]'

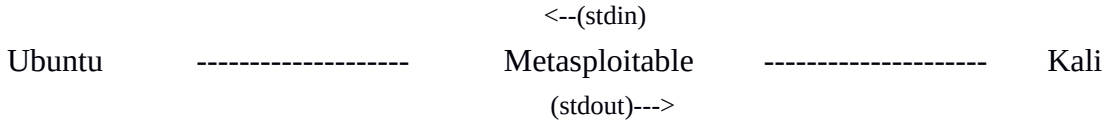
Ubuntu 14.04.5 LTS
hefese-N61JQ login: hefese // hefese girilir.
Password: // W.karabuk1992 girilir.

Last Login: Sun Nov 27 00:38:54 +03 2016
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-101-generic x86_64)

* Documentation: http://help.ubuntu.com

hefese@hefese-N61JQ:~$

Görüldüğü üzere Ubuntu'ya bağlandık. Yani iki kere telnet bağlantısı yaparak Kali'den Ubuntu'ya bağlanmış olduk. Aradaki Metasploitable transit olmuş oldu. Metasploitable'ın stdin'i Ubuntu'ya gidiyor, stdout'u ise Kali'ye gidiyor. Yani Metasploitable hiçbir şekilde ne kodları kendi konsoluna giriyor ne de çıktısını kendi konsoluna basıyor. Yaptığı şey sadece stdin'i Ubuntu'ya vermek, stdout'u ise Kali'ye vermektir.



Birinci telnet bağlantısı Metasploitable'ın stdout'unu Kali'ye gönderirken, ikinci telnet bağlantısı Metasploitable'ın stdin'ini Ubuntu'ya göndermektedir. Böylece Metasploitable transit olmuş olur.

(Benim Not)