Remote SSH Tunneling with Plink.exe

U.Y. · Follow
5 min read · Jul 24, 2020

We will demonstrate how we can create remote ssh tunneling between a Windows Machine having a blocked service and a Linux Machine (Kali Machine). To get some more definitions about SSH tunneling, what is remote and local ssh tunneling (aka ssh port forwarding), please google it (I recommend you to visit https://www.ssh.com/).

Starting with Kali Machine:

Let's first check the initial case by dumping sockets with **ss** and grepping **sshd** to see if there is already running *sshd* service.

Command: `kali@kali:~$ sudo ss -antlp | grep sshd`

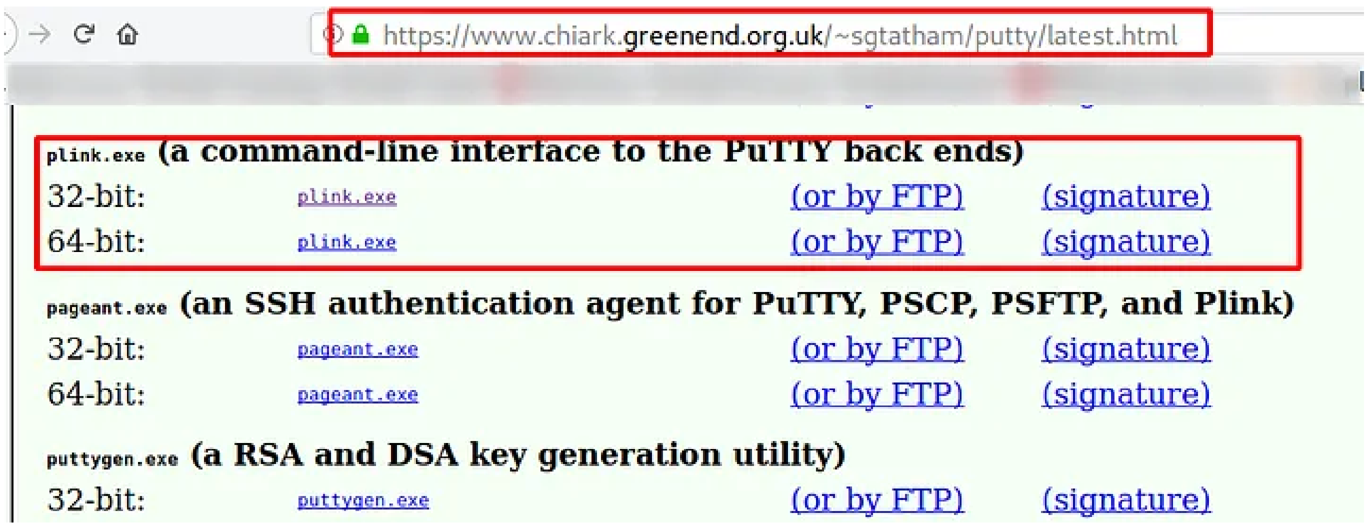
I had no output which means that *sshd* is not active.

Now, we have an active *sshd* running and can start playing with *plink.exe* on
ou

. . .

Downloading *plink.exe:*

Assuming that we don't have plink.exe on our Windows Machine, let's browse to https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html and download the file:



https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

plink.exe (a command-line interface to the PuTTY back ends)

32-bit:	plink.exe	(or by FTP)	(signature)
64-bit:	plink.exe	(or by FTP)	(signature)

pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)

32-bit:	pageant.exe	(or by FTP)	(signature)
64-bit:	pageant.exe	(or by FTP)	(signature)

puttygen.exe (a RSA and DSA key generation utility)

32-bit:	puttygen.exe	(or by FTP)	(signature)

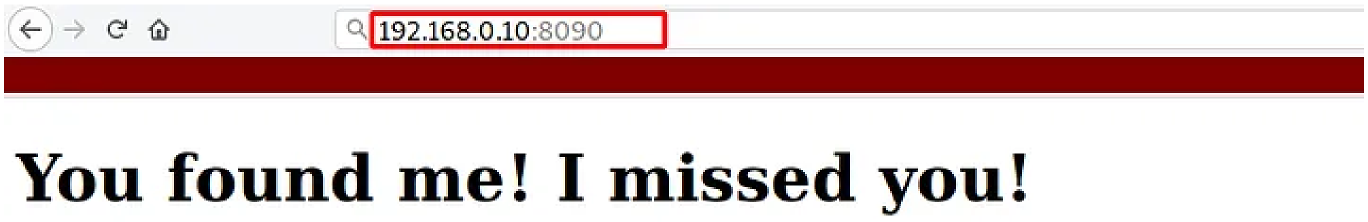
Main website for downloading plink.exe

There are two binaries available; as you can guess, 32-bit and 64-bit (There are also ARM architecture executables for Windows, if you scroll down)

Let's check if our windows machine is 32-bit or 64-bit.

We use the following command:

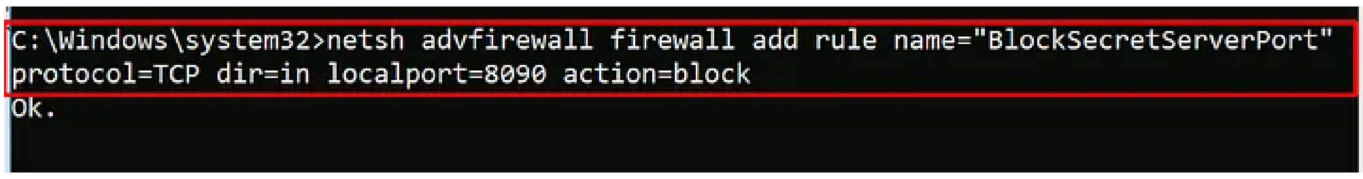
For our demonstration, let's start a web server at <IP_ADDRESS>:8090 (I had an Apache server, but you may also use python based simple HTTP Server, or a similar one). It's initialy active at port 8090.



You found me! I missed you!

Then block 8090 for our exercise by opening Command Prompt (Run as Administrator) and entering related firewall command:

```
C:\Windows\system32>netsh advfirewall firewall add rule
name="BlockSecretServerPort" protocol=TCP dir=in localport=8090
action=block
```



```
C:\Windows\system32>netsh advfirewall firewall add rule name="BlockSecretServerPort"
protocol=TCP dir=in localport=8090 action=block
Ok.
```

Blocking a port (inbound)

Let's check if we could block it successfully or command prompt lied to us:

Use the following command and scroll to find your new rule:

Port 8090 is now for sure blocked.

We are now ready to begin playing with plink.exe.

. . .

What we need in this scenario is to create a remote ssh tunneling such that Kali machine can reach our HTTP server at port 8090.

We have the SSH server running on Kali side and we will initiate the tunneling from the client side (which is Windows machine):

Command: `C:\>plink32.exe -ssh -l <MYUSERNAME> -pw <MYPASSWORD> -R <MYIP>:<MYPORT>:127.0.0.1:8090 <MYIP>`

> *Then we need the following command:*
>
> `p` **`90`**
>
> ***`192.168.0.3`***

Here is the console output in my case:

Remote SSH Tunneling using plink.exe

When you run the ssh command for first time, you will be prompted to store key in cache or not. Then this key will be stored under *"HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys"* for future connections and you will have trust established to the Kali machine. You will not be asked again until you remove this key from registry.

We included **-N** option to tell plink that we don't want to have shell started. If you want a shell after the tunnel is establised, remove -N option.

After session is started, we try again and we are now able to reach our

55

Written by U.Y.

14 Followers

Follow

More from U.Y.

U.Y.

Delete vs. Clear vs. Purge vs. Destroy

Let's begin with "Delete". Initially, "delete" was confusing for me as I was reading about data...

U.Y.

Nmap -Pn (No Ping) Option Analysis

When we explore our target machine(s), nmap is almost the first step tool for most of...

Recommended from Medium

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

✦ Jun 18 1.6K 54

Niman Ransindu

Brute Forcing SSH on Metasploitable 2 Using Metasploit

Introduction

Jun 12 50

Lists

Staff Picks
755 stories · 1416 saves

Stories to Help You Level-Up at Work
19 stories · 852 saves

Jose Campo

OSCP Tip: Reverse Shell with BusyBox!

As an OSCP aspirant, we're always on the lookout for quick and efficient ways to obtain...

✦ Oct 13 5

bonguides.com

How To Install Netcat on Windows 10/11

Jul 29 8

Satyam Pathania in InfoSec Write-ups

Secret Linux Commands: The Ones Your Teacher Never Told You...

oh yeah — I m your teacher gg

✦ Sep 20 1.8K 20

Alexander Nguyen in Level Up Coding

The resume that got a software engineer a $300,000 job at Google.

1-page. Well-formatted.

✦ Jun 1 25K 483

See more recommendations