SSH for Windows: plink.exe

Plink, short for PuTTY Link, is a Windows command-line SSH tool that comes as a part of the PuTTY package when installed. Similar to SSH, Plink can also be used to create dynamic port forwards and SOCKS proxies. Before the Fall of 2018, Windows did not have a native ssh client included, so users would have to install their own. The tool of choice for many a sysadmin who needed to connect to other hosts was PuTTY.

> Imagine that we are on a pentest and gain access to a Windows machine. We quickly enumerate the host and its security posture and determine that it is moderately locked down. We need to use this host as a pivot point, but it is unlikely that we will be able to pull our own tools onto the host without being exposed. Instead, we can live off the land and use what is already there. If the host is older and PuTTY is present (or we can find a copy on a file share), Plink can be our path to victory. We can use it to create our pivot and potentially avoid detection a little longer.

That is just one potential scenario where Plink could be beneficial. We could also use Plink if we use a Windows system as our primary attack host instead of a Linux-based system.

Getting To Know Plink

In the below image, we have a Windows-based attack host.

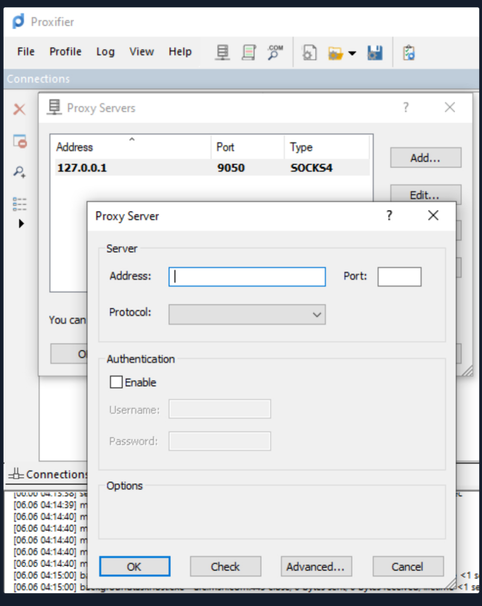
The Windows attack host starts a plink.exe process with the below command-line arguments to start a dynamic port forward over the Ubuntu server. This starts an SSH session between the Windows attack host and the Ubuntu server, and then plink starts listening on port 9050.

Using Plink.exe

Using Plink.exe

```
plink -D 9050 ubuntu@10.129.15.50
```

Another Windows-based tool called Proxifier can be used to start a SOCKS tunnel via the SSH session we created. Proxifier is a Windows tool that creates a tunneled network for desktop client applications and allows it to operate through a SOCKS or HTTPS proxy and allows for proxy chaining. It is possible to create a profile where we can provide the configuration for our SOCKS server started by Plink on port 9050.



After configuring the SOCKS server for `127.0.0.1` and port 9050, we can directly start `mstsc.exe` to start an RDP session with a Windows target that allows RDP connections.

> Note: We can attempt this technique in any interactive section of this module from a personal Windows-based attack host. Once you've completed this module from a Linux-based attack host feel free to try to go back through it from a personal Windows-based attack host. Also, when spawning your target we ask you to wait for 3 - 5 minutes until the whole lab with all the configurations is set up so that the connection to your target works flawlessly.

Start Instance

∞ / 1 spawns left

Waiting to start...

Optional Exercises

Challenge your understanding of the Module content and answer the optional question(s) below. These are considered supplementary content and are not required to complete the Module. You can reveal the answer at any time to check your work.

Target: Click here to spawn the target system!

Attempt to use Plink from a Windows-based attack host. Set up a proxy connection and RDP to the Windows target (172.16.5.19) on the internal network. When finished, submit "I tried Plink" as the answer.

Submit your answer here...

Submit

Reveal Answer

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left