

SSH for Windows: plink.exe

w1j0y

SSH for Windows: plink.exe

Windows 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.

`plink -ssh -D 9050 ubuntu@10.129.15.50`

Windows Attack Host

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.