SSH tunneling

context

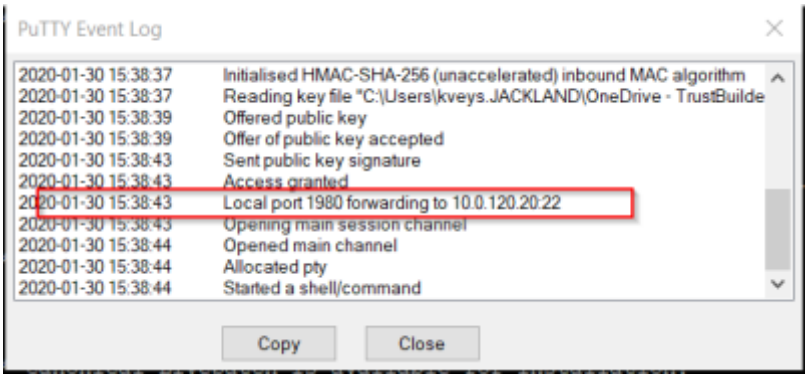
dit document beschrijft SSH tunneling, een mechanisme waarbij je netwerk verkeer over een bestaande SSH verbinding kunt sturen.

werking

1. bestaat ook onder de naam SSH Port Forwarding
2. je maakt gebruik van een bestaande SSH verbinding tussen
    1. een client (bv je computer met PuTTY)
    2. een SSH server (die bv luistert op poort 22)
3. local forwarding:
    1. op de client wordt een poort in listing mode gezet
    2. bij verbinding op die poort (dmv een browser, SSH sessie, ...) stuurt de client het verkeer door naar de SSH server
    3. de SSH server stuurt op zijn beurt het verkeer door naar een andere poort (op een andere server OF op de SSH server zelf)
    4. de SSH server fungeert dus als een soort jumphost.

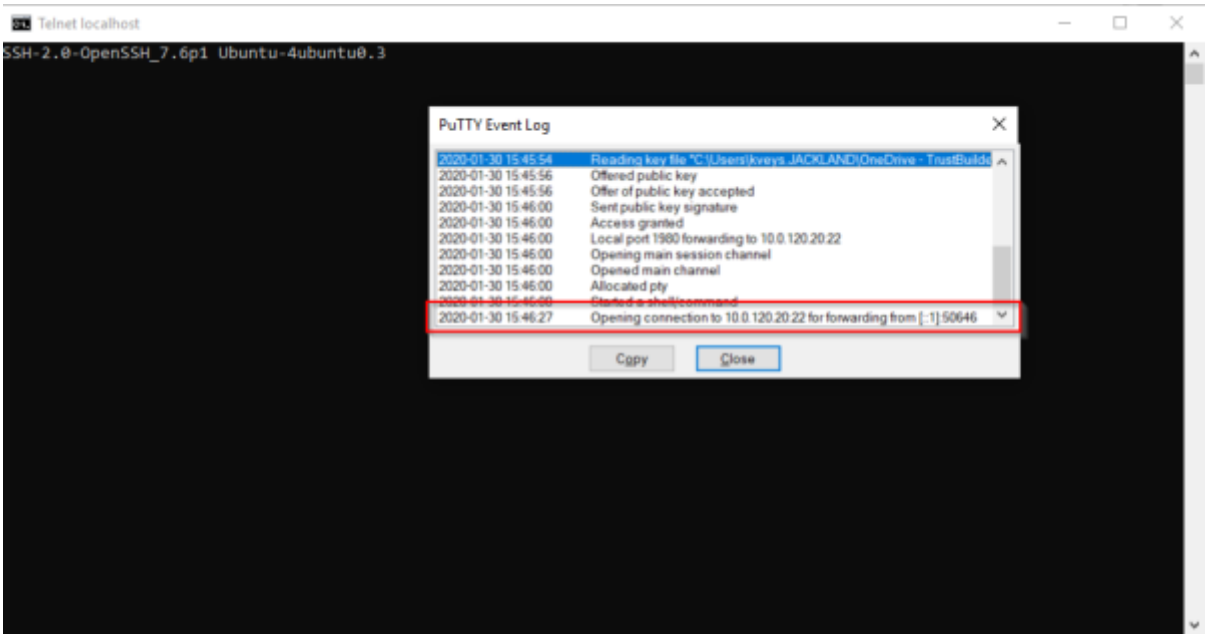
voorbeeld

1. open **PuTTY** en selecteer de sessie met de SSH server (of maak een nieuwe aan).
2. kies: **Connection** > **SSH** > **Tunnels**
3. vink aan: **Local ports accept connection from other hosts**
4. **Source port**: poort waarop je SSH client zal luisteren (bv: 2020)
   Neem zeker een poort >1024
5. **Destination**: server:poort van de server die je wilt bereiken, **Add**
   De server moet dus bereikbaar zijn vanaf de SSH server
6. **Sla** de sessie op.
7. **open** de sessie
8. rechterklik op de sessie en kies: **Event Log**
9. controleer dat de forwarding actief is:



(Je kan ook op je client computer kijken of er op de aangegeven poort wordt geluisterd). Nu is de tunnel actief en zal alle verkeer op localhost:2020 via deze tunnel doorgestuurd worden.

10. maak nu een verbinding op localhost:2020 (via telnet, bv)
11. controleer dat de tunnel het verkeer doorstuurt



meer info

- SSH Port Forwarding Example

Linux