Dynamic Port Forwarding with SSH and SOCKS Tunneling

w1j0y

Attack Host

- Scanning the Pivot Target
  - -p22 SSH Open
  - -p3306 MYSQL Closed
- Executing the Local Port Forward
  - `ssh -L 1234:localhost:3306 ubuntu@10.129.202.64`
    - The -L command tells the SSH client to request the SSH server to forward all the data we send via the port 1234 to localhost:3306 on the Ubuntu server. By doing this, we should be able to access the MySQL service locally on port 1234.
  - Confirming Port Forward with Netstat — `netstat -antp | grep 1234`
- Confirming Port Forward with Nmap — `nmap -v -sV -p1234 localhost`
- Forwarding Multiple Ports — `ssh -L 1234:localhost:3306 -L 8080:localhost:80 ubuntu@10.129.202.64`