Web Server Compromise  
(Blue)

Summary

Technique Explains: establishing socks proxy connections enable to perform pentesting with extra layers of connection, which allows us to hide our true connection. This technique can be use in Metasploit, nmap, or many testing tools.

Target Address: 172.26.1.229

Target Account: vagrant (compromised account)

Tools: OpenVPN, Proxychains4.conf, Proxychains, Socks4, Reverseshell

After connected to vpn, we are going to perform the result of socks proxy using 52000 and 8989port to reverse to our on kali. Which allows us to pivot the hosts in the network using qdpm server.

Text

Description automatically generated

First, add and modify “proxychains4.conf” in /etc directory, this allows traffic socks address to tunnel back to our own machis

Add “socks4 127.0.0.1 52000”

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Use nmap to test out if the proxychains works, and it shows it using nmap to executing via proxychains.

Text

Description automatically generated