90.00 - Intro

The scenario here is: Imagine we are doing an assessment. What typically happens is, "we would be sending the client a laptop and on that laptop there is a VPN connection that when plugged in "phones" home. We are able to connect to that VPN connection and share that tunnel. So, then we can run these attacks while having the laptop without the need to travel on site." Heath Adams.

We are assuming we already have an initial access (Internal Pentesting). So, a computer/account/system has already been compromised/exploited. This would be the privilege scalation type of Pentesting in an Active Directory Domain.

Before starting exploiting the domain, we need to set our attack machine IP Address, in my case Kali Linux, to the same Network where our lab is set up. Meaning we need to set our IP Address to be in the same network as the Windows Server 2022 (Domain Controller), and the Client Machines. Make sure all machines (DC, Clients, and Attacker Machine) are set to NAT in the Virtual Machine settings.

First, check if your attacker machine is not already in the same network. If it is set to NAT in the Virtual Machine settings, then most likely it will be in the same network as the Domain. If you suspect you are, but you are not sure. Get the IP Address of the DC, and the Clients. Go to your attacker machine, and issue an arp scan. The command to do so in Kali Linux is : "#sudo arp-scan -l".

This will probe for machines in the same network, and will show the ones encountered. You should recognize the IP Addresses listed. Don't worry about .1, and .254 .