90.09 - IPv6 Attacks

This is going to be mainly DNS Take Over.

This is much more reliable attack, than the other Relay attacks we learnt so far.

As we are typically running IPv4, it is possible that IPv6 is not being, but it is turned on. And, if that is the case, and we are using only IPv4, the question is "Who is doing DNS for IPv6?". If nobody is doing DNS for IPv6, we can spin a fake DNS Server, and listen to all the IPv6 data that comes through, and tell the IP Addresses intercepted we are DNS, so they can send all their IPv6 traffic data to our fake DNS Server, so we can pass that along. The issue is that when this happen, we can get authentication to the Domain Controller via LDAP or SMB.

On the example, when we reboot the machine, that creates an event. The event comes through to us, and we can use that machine to login to the Domain Controller. It is not required to be an Administrator login or anything, and we can gather a lot of information that way. We can potentially use that machine to create another machine, and we can wait for someone to login into the network, and that will come to us in NTLM format, and we relay the NTLM credentials, and log in the DC, and creates an account for us. This tool that is going to do all this for us is called MITM6 (Man In THe Middle 6). We are going to combine it with "#ntlmrelayx.py", and it is going to relay into LDAP. It is going to create the account to us and everything.