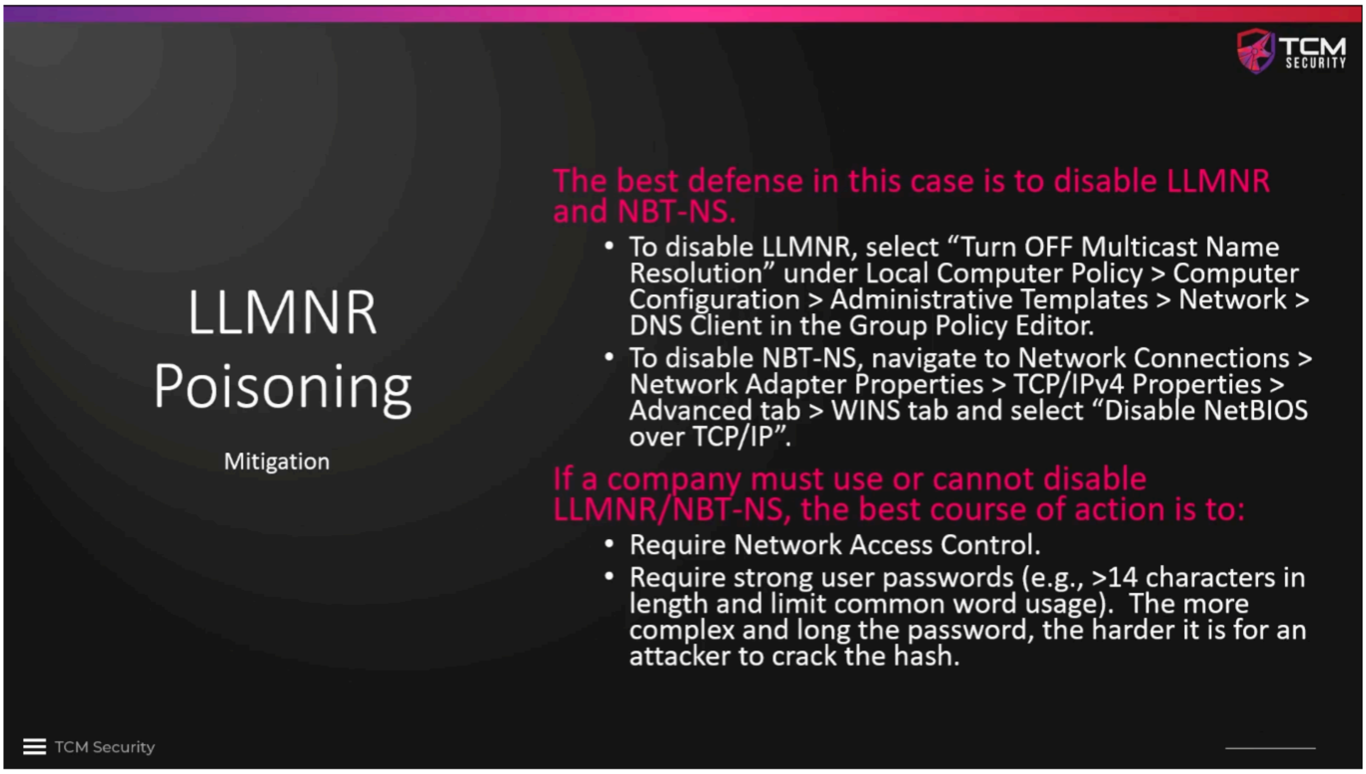
LLMNR Poisoning Mitigations



LLMNR Poisoning

Mitigation

The best defense in this case is to disable LLMNR and NBT-NS.

- To disable LLMNR, select “Turn OFF Multicast Name Resolution” under Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client in the Group Policy Editor.
- To disable NBT-NS, navigate to Network Connections > Network Adapter Properties > TCP/IPv4 Properties > Advanced tab > WINS tab and select “Disable NetBIOS over TCP/IP”.

If a company must use or cannot disable LLMNR/NBT-NS, the best course of action is to:

- Require Network Access Control.
- Require strong user passwords (e.g., >14 characters in length and limit common word usage). The more complex and long the password, the harder it is for an attacker to crack the hash.

Very straight forward. Just follow instruction. We are going to do this in the "Group Policy Management", which is the place where all the policies are set.