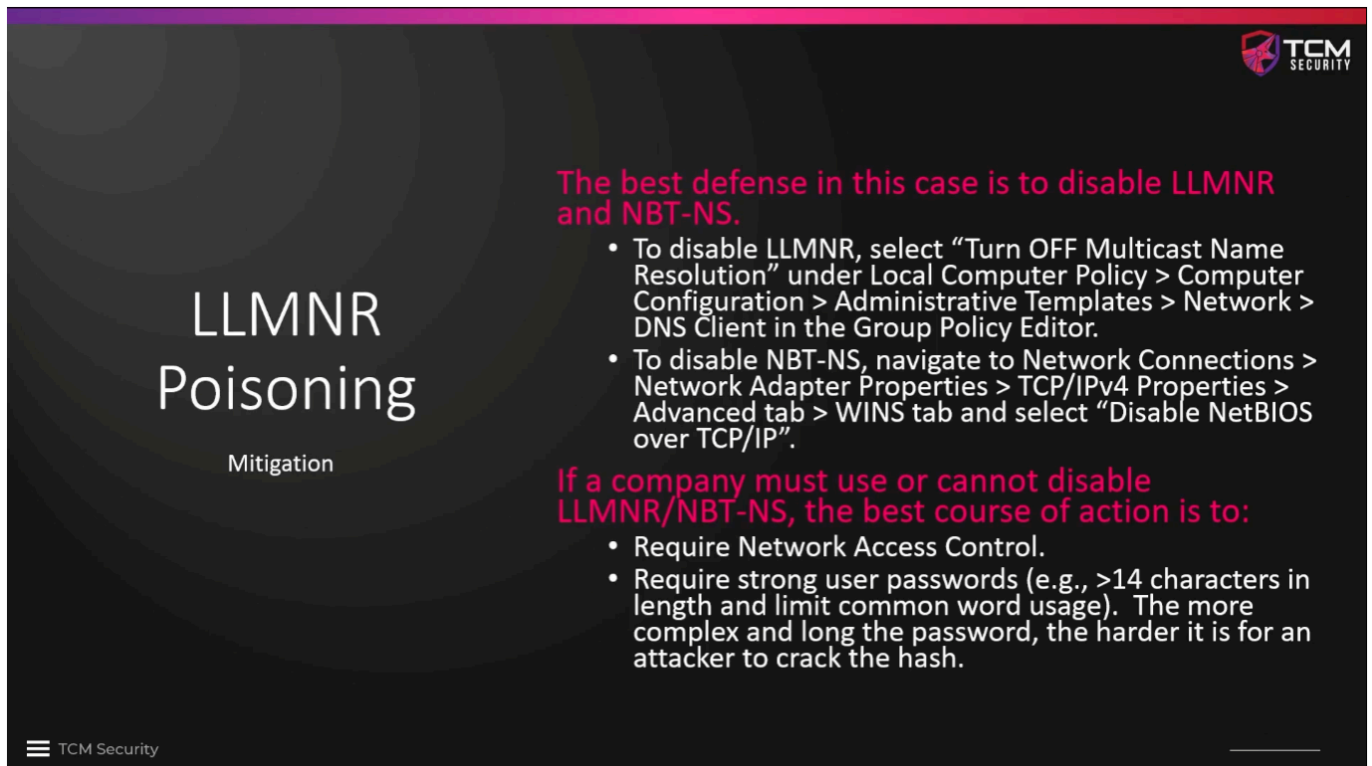


# LLMNR Poisoning Mitigations

A presentation slide with a dark background and a purple-to-pink gradient header. On the left, the text 'LLMNR Poisoning' is written in large white font, with 'Mitigation' in smaller white font below it. On the right, there are two sections of text in pink, each followed by a bulleted list of instructions in white. The top section states that the best defense is to disable LLMNR and NBT-NS, with instructions on how to do so via Group Policy Editor and Network Connections. The bottom section states that if a company must use or cannot disable these services, the best course of action is to require Network Access Control and strong user passwords. The TCM Security logo is in the top right corner, and a hamburger menu icon with 'TCM Security' is in the bottom left corner.

LLMNR  
Poisoning  
Mitigation

TCM  
SECURITY

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.

TCM Security

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.