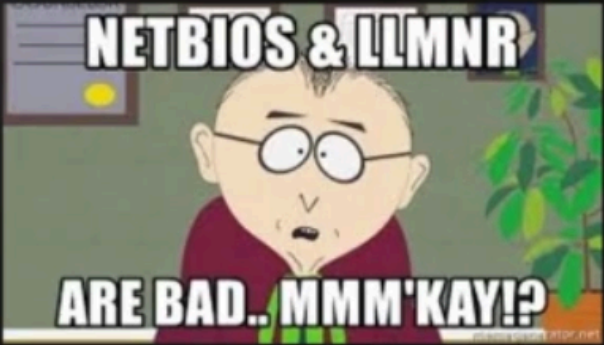


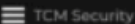

90.01 - LLMNR - Poisoning Overview

LLMNR Poisoning

What is LLMNR?

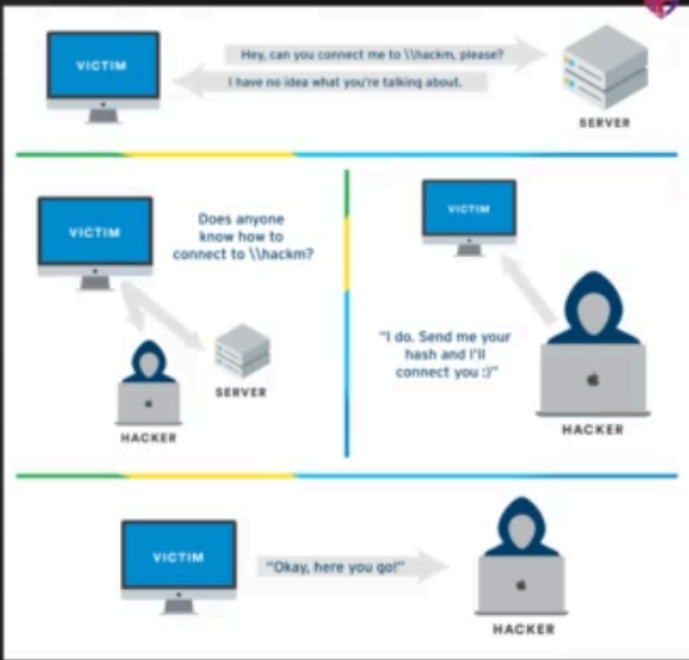
- Used to identify hosts when DNS fails to do so.
- Previously NBT-NS
- Key flaw is that the services utilize a user's username and NTLMv2 hash when appropriately responded to





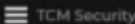

LLMNR Poisoning

Overview



The diagram illustrates the LLMNR poisoning process in three stages:

- Initial Query:** A VICTIM computer asks a SERVER, "Hey, can you connect me to \\hackm, please?". The SERVER responds, "I have no idea what you're talking about."
- Discovery:** The VICTIM asks, "Does anyone know how to connect to \\hackm?". A HACKER (represented by a laptop) responds, "I do. Send me your hash and I'll connect you :)"
- Connection:** The VICTIM responds to the HACKER, "Okay, here you go!".



Step 4: Crack Dem Hashes

```
hashcat -m 5600 hashes.txt rockyou.txt
```