What is LLMNR poisoning?

LLMNR poisoning is a local-network attack where an attacker answers LLMNR and NBT-NS name-resolution broadcasts that Windows sends when DNS fails, posing as the requested host. The victim then tries to authenticate to the attacker, sending its NetNTLM hash, which the attacker captures and cracks offline (or relays). Because Windows broadcasts these requests by default, the attack often needs no credentials, just a foothold on the network. The tool Responder automates it. Disabling LLMNR/NBT-NS is the fix.

HOW IT WORKS

01 The attack and payload

On a foothold in the local network, the attacker listens and answers:

- Run a poisoner: `responder -I eth0` (answers LLMNR/NBT-NS, captures NetNTLMv2 hashes).
- Victims trying to reach mistyped or stale hosts hand over their NetNTLMv2 hashes.
- Crack them offline: `hashcat -m 5600 netntlm.txt rockyou.txt`, or relay them to another host (see NTLM relay) without cracking.

Documented for defensive context.

> NO CREDENTIALS NEEDED
>
> *LLMNR poisoning needs only a position on the network, no account. Windows broadcasts these requests by default, so a quiet poisoner harvests NetNTLM hashes from normal user mistakes.*

HOW TO DEFEND

- Disable LLMNR and NBT-NS via Group Policy and DHCP options, the direct fix; ensure DNS is correct so they are not needed.
- Enforce SMB signing so captured hashes cannot be relayed.
- Use strong passwords so any captured NetNTLMv2 hashes resist cracking.
- Segment the network to limit where a poisoner can listen.
- Monitor for LLMNR/NBT-NS responders and unusual authentication patterns.

SOURCES

[1] MITRE ATT&CK: Adversary-in-the-Middle (T1557)

[2] Microsoft: Windows name resolution

[3] MITRE ATT&CK: Credential Access (TA0006)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-llmnr-poisoning

Open online