Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS)

LLMNR and NetBIOS are two name resolution services built in to Windows to help systems find address names from other devices on the network. However, addresses and address providers on the network are not verified, since Windows assumes that anyone on the network is automatically trusted. When a DNS request fails, Windows will attempt to ask other devices on the network to resolve that address over LLMNR or NBT-NS.

Spoofing Addresses over LLMNR/NBT-NS

For a service like SMB, if a host is configured to automatically authenticate over SMB then by spoofing addresses over LLMNR/NBT-NS, an attacker can easily grab credentials by simply passively replying to every single LLMNR/NBT-NS request.

Responder.py

Responder is one of the most popular LLMNR/NBT-NS spoofer/poisoners available. This program is free and open source, with its code available on Github, and is capable of impersonating for a variety of malicious services. One of the most effective ways Responder operates is by spoofing failed SMB requests in order to grab LLMR password hashes sent over the network. An attacker can then begin to crack the hashes or even conduct a pass-the-hash attack, if a system on the network is particularly vulnerable. Other tools like Rapid7's Metasploit LLMNR spoofer module are also available and work similarly

Defending against LLMNR/NBT-NS attacks

The number one way to protect a system from being exploited is to disable LLMNR and NBT-NS. Responder uses these two protocols in order to grab password hashes from other systems on the network. Ensure that both of these protocols are disabled, since Windows defaults to using the other when the other fails/is disabled.

Disabling LLMNR:

1. Open the Group Policy Editor in your version of Windows
2. Navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client
3. Under DNS Client, make sure that "Turn OFF Multicast Name Resolution" is set to Enabled

Disabling NBT-NS:

1. Open your Network Connections and view the properties of your network adapter.
2. Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties.
3. On the General tab click Advanced and navigate to the WINS tab, then select "Disable NetBIOS over TCP/IP.