# TTP Detail – T1557.001

## TTP Information

Name: LLMNR/NBT-NS Poisoning and SMB Relay

Description: By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR)(Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords.

In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv1/v2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also be independent of it.(Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay) Additionally, adversaries may encapsulate the NTLMv1/v2 hashes into various protocols, such as LDAP, SMB, MSSQL and HTTP, to expand and use multiple services with the valid NTLM response.

Several tools may be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174).(Citation: GitHub NBNSpoof)(Citation: Rapid7 LLMNR Spoofer)(Citation: GitHub Responder)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: collection

## Tools

* Empire
* Impacket
* PoshC2
* Pupy
* Responder

## APTs (Intrusion Sets)

* Lazarus Group
* Wizard Spider