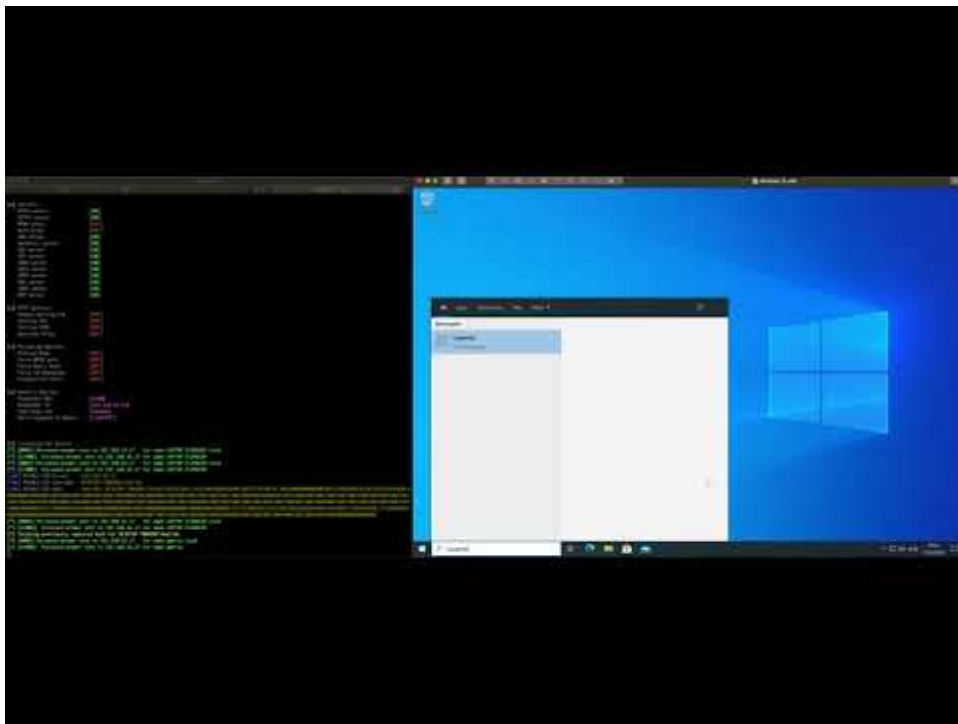


[illegible]

I made a little POC video back in April, showing the dangers of leaving LLMNR enabled on your Windows computers.



<https://youtu.be/GUr4U8irXZ0>

Your Windows computer gladly hands out the netNTLM-hash of the logged on user. Those hashes could easily be cracked by an attacker if the password is easy or/and short, but it can also be relayed to other services on your network, giving the attacker access to them, without even bothering trying to crack the hash.

There have been written tons about this on blogs/articles around on the Internet. If you're not familiar with it, you can read more about Responder and relaying in this [excellent](#) article.


The same problem exists if your computer has NBT-NS (Netbios Name-Service) enabled. So, one should absolutely disable those two protocols, as they are really not needed in a corporate network.

[This](#) great article, will tell you how to go around to get that task done.

The other day I read this post on [LinkedIn](#), showing you could use a tool named [mitm6](#), to set up a rogue IPv6 DHCP server, and then be able to catch the hashes over IPv6 instead.


That sounded really scary and was news for me.

I had to see this for myself, so I put up Responder on a computer in my lab network. I first had to verify everything was locked down as it should, and did a testrun from a freshly installed Windows 11 with LLMNR and NBT-NS disabled.

 Skjerm bilde%202021-12-04%20kl.%2012.38.00

I was in for a surprise...

I didn't even get around to start mitm6! The hashes just started to furiously hit my Responder. Something had clearly changed since the last time I visited the topic. This was really strange and unexpected behaviour.

 Skjerm bilde%202021-12-04%20kl.%2012.40.09

This time, it looked like mDNS was the culprit!? I wasn't even aware Microsoft had implemented native [mDNS](#) support, but apparently they did at some point in Windows 10 and of course Windows 11 and Windows server 2022 has it enabled by default too!

I tested it out on a Windows 2022 Domain controller and a Windows 10 computer too. Hashes all over! mDNS had no qualms about help telling anyone interested, what my netNTLM-hash looked like...

Trying to get to the core of the problem, I inspected services running on the computer and figured out mDNS is a part of the DNSCache service, now.

 dnscache

Disabling DNSCache is not an option. (tried it) It stops mDNS, but it also breaks a lot of other stuff.


Checking the registry, it turns out there is only a key named mDNS under the DNSCache service, nothing else. No parameters to be set/changed.



Spent a whole day and evening Googling for parameters, but couldn't find anything documented anywhere about the "new" mDNS feature.

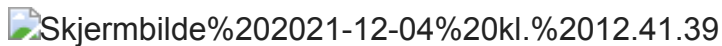
Using Procmon from [Sysinternals](#), I saw the DNSCache process querying the registry for some nonexisting entries.



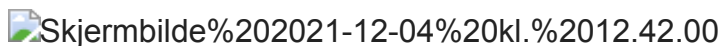
EnableMDNS sounded exactly like what i was looking for. I added the entry, with a value of 0.  Skjerm bilde%202021-12-04%20kl.%2012.41.05

Confirming it being found by the DNS Caching service  disabled

Then testing again from my Windows 11 computer.



And....



Nothing...

mDNS stopped its promiscuous behaviour and everything was again good in the LANd.

**My two cents:** mDNS doesn't serve any purpose at all in a corporate network and should be disabled the instance you join the domain.

Don't think Microsoft have implemented control over the feature in an GPO yet.

## How to disable mDNS using Powershell

---

```
set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\" -  
Name EnableMDNS -Value 0 -Type DWord
```

## How to disable mDNS using the reg command

---

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" /v "  
EnableMDNS" /t REG_DWORD /d "0" /f
```

It is worth to mention; This mDNS behaviour is seen only in Windows domain environments. Not if you are running it in a Workgroup. This is really strange and I don't know why. If anyone does, I would be happy to be enlightened.