

LLMNR POISONING

AND HOW TO PREVENT IT

ACTIVE DIRECTORY

Active Directory (AD) stands as a foundational piece for many organizational networks, streamlining administrative tasks and enhancing productivity. However, out of the box, AD comes bundled with various “features” that can be a goldmine for attackers. Notably, protocols like LLMNR can pose significant security risks, especially for organizations that have never undergone a penetration test. This blog delves deep into the intricacies of LLMNR and the vulnerabilities it introduces, offering insights into its potential impacts and mitigation strategies.



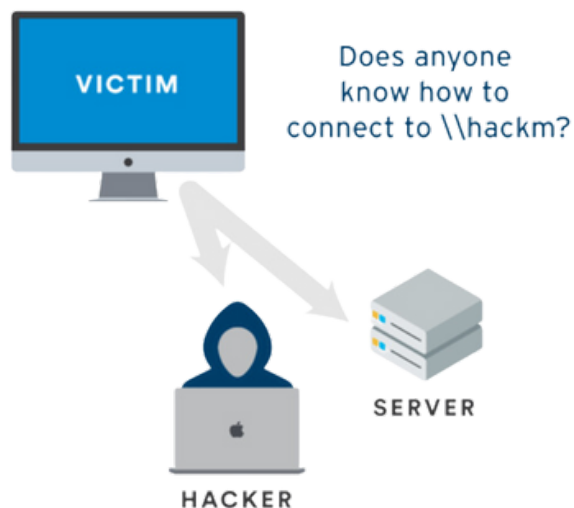
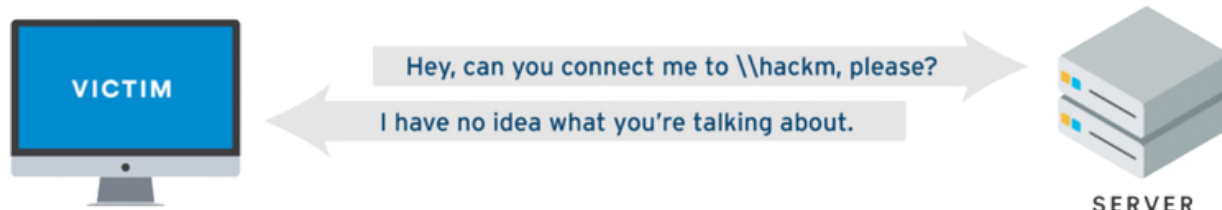
WHAT IS LLMNR?

LLMNR is a protocol that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local network without requiring a DNS server or DNS configuration.

When a host's DNS query fails (i.e., the DNS server doesn't know the name), the host broadcasts an LLMNR request on the local network to see if any other host can answer.

LLMNR is the successor to NetBIOS. **NetBIOS** (Network Basic Input/Output System) is an older protocol that was heavily used in early versions of Windows networking. **NBT-NS** is a component of NetBIOS over TCP/IP (NBT) and is responsible for name registration and resolution. Like LLMNR, NBT-NS is a fallback protocol when DNS resolution fails. It allows local name resolution within a LAN.

HOW IS LLMNR VULNERABLE?



LLMNR has no authentication mechanism. Anyone can respond to an LLMNR request, which opens the door to potential attacks. When a computer tries to resolve a domain name and fails via the standard methods (like DNS), it sends an LLMNR query across the local network. An attacker can listen for these queries and respond to them, leading to potential unauthorized access

AKA LLMNR POISONING

LLMNR poisoning is an attack where a malicious actor listens for LLMNR requests and responds with their own IP address (or another IP of their choosing) to redirect the traffic. This can lead to credential theft and relay attacks. Here is a sample walkthrough.

STEP 1: THE ATTACKER RUNS RESPONDER

```
sudo responder -I eth0 -dWP
```

[illegible]

AKA LLMNR POISONING

04/11

AKA LLMNR POISONING

We can now use a password cracking tool, such as **Hashcat**, to attempt to crack the victim's hash.

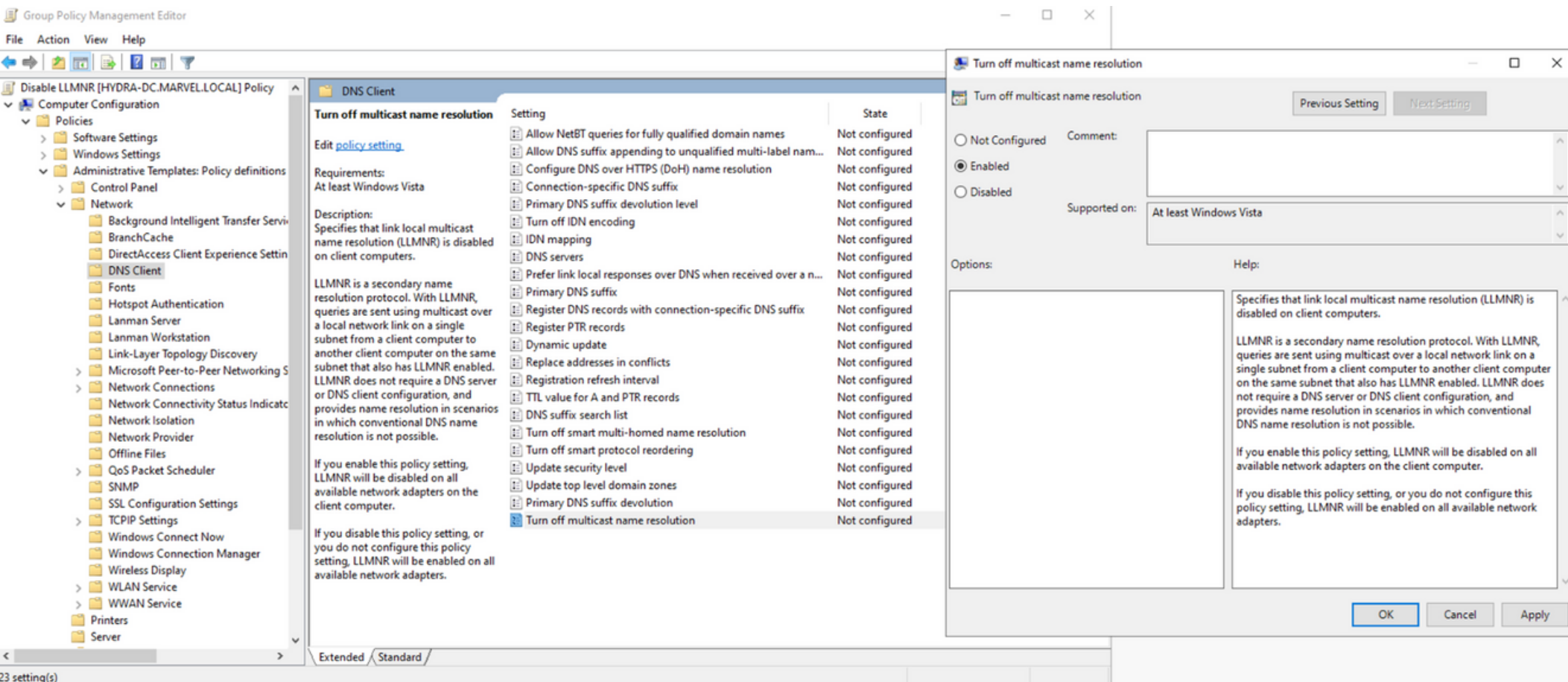
```
Dictionary cache hit:  
* Filename..: rockyou.txt  
* Passwords.: 14347430  
* Bytes.....: 139951895  
* Keyspace...: 14347430  
  
FCASTLE::MARVEL:61dde887aeb2af2a:76dd8039b96061195586bc9a4ef5f3c1:0101000000000000c0653150de09d20107929b9d6080f5bb000  
000000200080053004d004200330001001e00570049004e002d00500052004800340039003200520051004100460056000400140053004d004200  
33002e006c006f00630061006c0003003400570049004e002d00500052004800340039003200520051004100460056002e0053004d00420033002  
e006c006f00630061006c000500140053004d00420033002e006c006f00630061006c0007000800c0653150de09d2010600040002000000080030  
0030000000000000000100000000200000234d5dd50acc5817bf563c8c2c532cede6c7b288f5623e3055e34ec3de0f8d7f0a0010000000000000  
00000000000000000000001a0063006900660073002f00310030002e0038002e0030002e00320000000000000000000000000000000000000000:Password1  
  
Session.....: hashcat  
Status.....: Cracked
```

05/11

MITIGATING LLMNR POISONING

MAIN DEFENSE – DISABLE LLMNR

To disable LLMNR, select “Turn OFF Multicast Name Resolution” under Computer Configuration > Administrative Templates > Network > DNS Client in the Group Policy Editor.



The screenshot displays the Group Policy Management Editor interface. On the left, the tree view shows the path: Computer Configuration > Administrative Templates > Network > DNS Client. The main pane shows the 'Turn off multicast name resolution' policy, which is currently 'Not configured'. The 'Description' pane provides details about LLMNR and the policy's effect. The 'Options' pane shows the 'Turn off multicast name resolution' policy setting, which is currently 'Not configured'.

Setting	State
Allow NetBT queries for fully qualified domain names	Not configured
Allow DNS suffix appending to unqualified multi-label nam...	Not configured
Configure DNS over HTTPS (DoH) name resolution	Not configured
Connection-specific DNS suffix	Not configured
Primary DNS suffix devolution level	Not configured
Turn off IDN encoding	Not configured
IDN mapping	Not configured
DNS servers	Not configured
Prefer link local responses over DNS when received over a n...	Not configured
Primary DNS suffix	Not configured
Register DNS records with connection-specific DNS suffix	Not configured
Register PTR records	Not configured
Dynamic update	Not configured
Replace addresses in conflicts	Not configured
Registration refresh interval	Not configured
TTL value for A and PTR records	Not configured
DNS suffix search list	Not configured
Turn off smart multi-homed name resolution	Not configured
Turn off smart protocol reordering	Not configured
Update security level	Not configured
Update top level domain zones	Not configured
Primary DNS suffix devolution	Not configured
Turn off multicast name resolution	Not configured

Turn off multicast name resolution

Turn off multicast name resolution

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

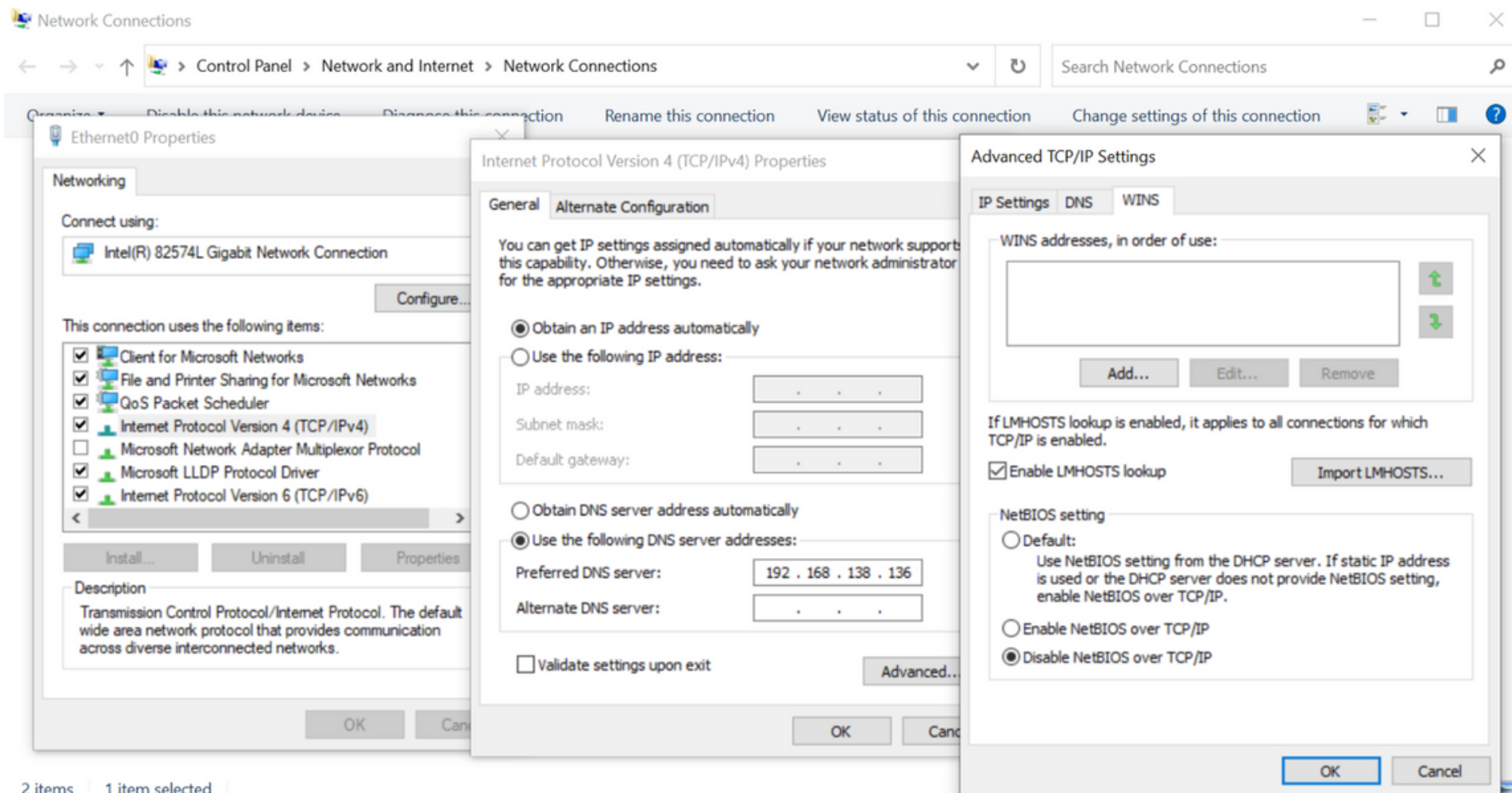
If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer.

If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.

MITIGATING LLMNR POISONING

MAIN DEFENSE – DISABLE NBT-NS

To disable NBT-NS, navigate to Network Connections > Network Adapter Properties > TCP/IPv4 Properties > Advanced tab > WINS tab and select “Disable NetBIOS over TCP/IP”. **This only works locally.**

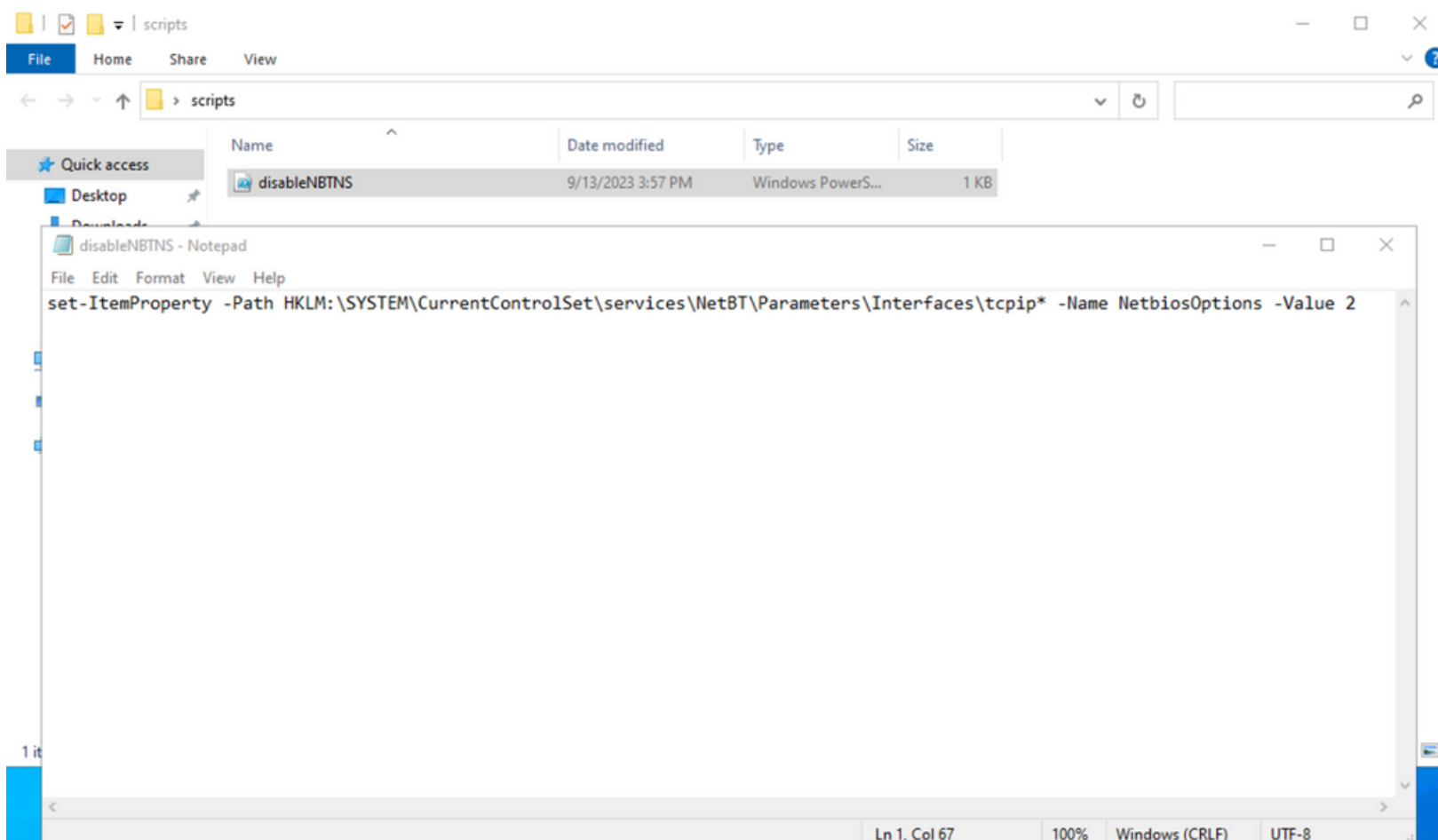


MITIGATING LLMNR POISONING

MAIN DEFENSE – DISABLE NBT-NS VIA GPO

To disable NBT-NS via GPO, we can simply write a PowerShell script (see below) and save it in Startup Scripts.

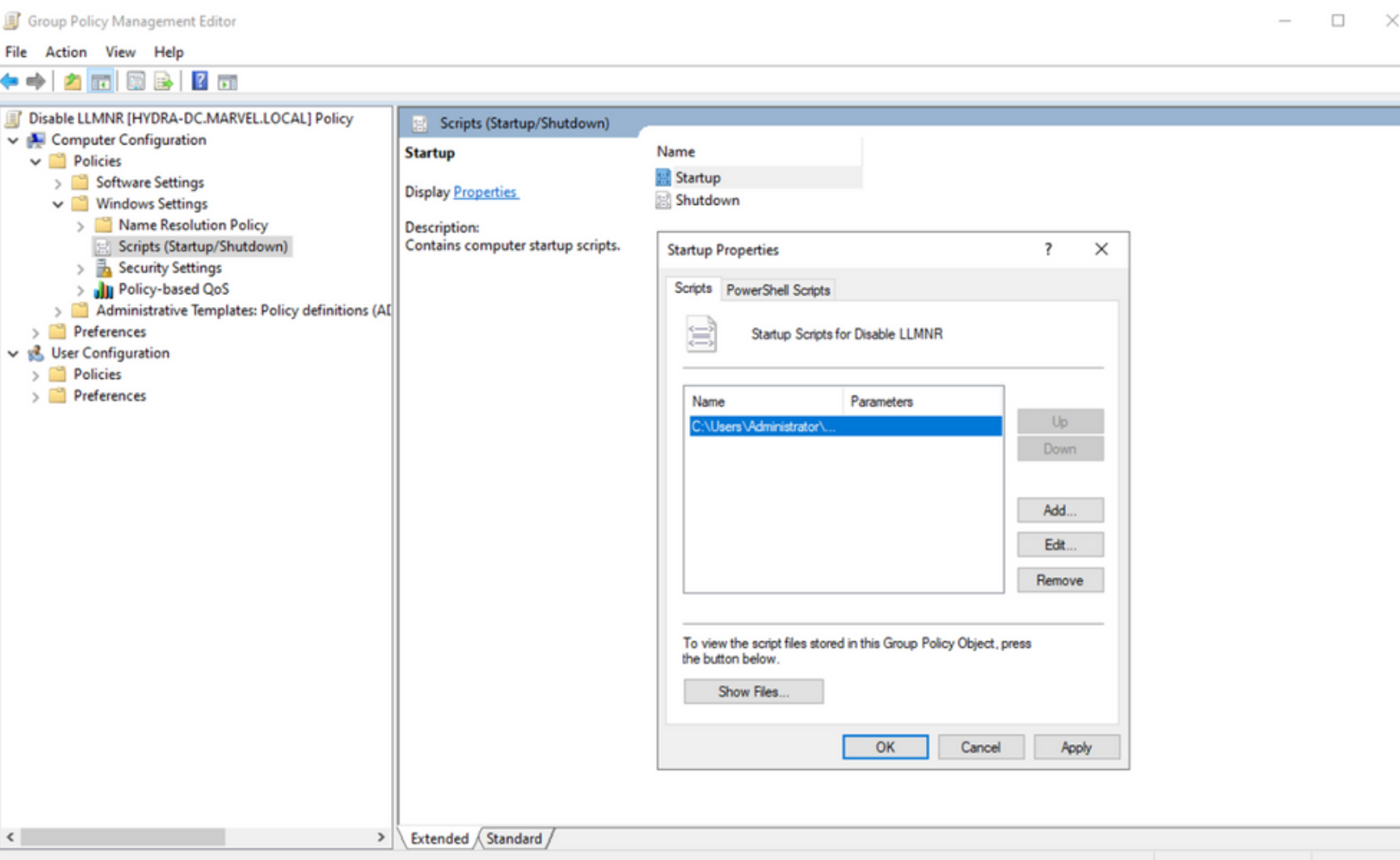
```
set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\tcpip  
Name NetbiosOptions -Value 2
```



MITIGATING LLMNR POISONING

MAIN DEFENSE – DISABLE NBT-NS VIA GPO

Now add the script to Startup Scripts in Computer Configuration > Policies > Windows Settings > Scripts > Startup



CONFIRMING MITIGATION

We can confirm that we have mitigated LLMNR by running the following command in PowerShell and receiving a '0' in return:

```
$(Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient" -name EnableMulticast).EnableMulticast
```

```
C:\Users\fcastle>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\fcastle> $(Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient" -name EnableMulticast).EnableMulticast
0
```

We can confirm that we have mitigated NBT-NS by running the following command in cmd.exe and receiving a '2' in return:

```
wmic nicconfig get caption,index,TcpipNetbiosOptions
```

```
C:\Users\fcastle>wmic nicconfig get caption,index,TcpipNetbiosOptions
```

Caption	Index	TcpipNetbiosOptions
[00000000] Microsoft Kernel Debug Network Adapter	0	
[00000001] Intel(R) 82574L Gigabit Network Connection	1	2
[00000002] Bluetooth Device (Personal Area Network)	2	
[00000003] WAN Miniport (SSTP)	3	
[00000004] WAN Miniport (IKEv2)	4	
[00000005] WAN Miniport (L2TP)	5	
[00000006] WAN Miniport (PPTP)	6	
[00000007] WAN Miniport (PPPOE)	7	
[00000008] WAN Miniport (IP)	8	
[00000009] WAN Miniport (IPv6)	9	
[00000010] WAN Miniport (Network Monitor)	10	

ALTERNATIVE DEFENSES

If a company must use or cannot disable LLMNR/NBT-NS, the best course of action is to:

- Require Network Access Control.
- Require strong user passwords (e.g., >14 characters in length and limit common word usage). The more complex and longer the password, the harder it is for an attacker to crack the hash.

PENETRATION TESTING

Conducting a penetration test is instrumental in uncovering the vulnerabilities associated with protocols like LLMNR. When left unchecked, LLMNR can be a prime target for attackers, given its susceptibility to poisoning and man-in-the-middle attacks. Through penetration testing, organizations can actively simulate these potential attack vectors, obtaining a clear picture of their existing vulnerabilities. Beyond mere identification, the insights gleaned from such tests offer a roadmap to remediate these weaknesses, ensuring that the organization's network remains resilient against real-world cyber threats leveraging LLMNR vulnerabilities

ABOUT TCM SECURITY

TCM Security is a veteran-owned, cybersecurity services and education company founded in Charlotte, NC. Our services division has the mission of protecting people, sensitive data, and systems. With decades of combined experience, thousands of hours of practice, and core values from our time in service, we use our skill set to secure your environment. The TCM Security Academy is an educational platform dedicated to providing affordable, top-notch cybersecurity training to our individual students and corporate clients including both self-paced and instructor-led online courses as well as custom training solutions. We also provide several vendor-agnostic, practical hands-on certification exams to ensure proven job-ready skills to prospective employers.