BLOCKING LOCAL NETWORK HIJACKING ATTACKS

MATHEW WEEKS
@SCRIPTJUNKIE1
NOVEMBER 2016

BLOCKING LOCAL NETWORK HIJACKING ATTACKS

Adversaries who have compromised one system in a network frequently hijack the network traffic of other systems on the same subnet to intercept passwords, infect software downloads and updates, spy on browsing or email traffic, or launch other denial-of-service or man-in-the-middle attacks. The easiest and most common ways adversaries accomplish this is by responding to NetBIOS or LLMNR broadcast name resolution requests. NetBIOS is a legacy protocol supported in the early days of Windows while LLMNR support was added to Windows Vista and Server 2008. Windows and other operating systems send out these requests while trying to locate network resources when you open your web browser or try to visit a website or open a network share or drive. Praetorian listed this layer 4 attack as one of their top 5 most common and effective attacks over 100 penetration tests. With a little more work, attackers may also accomplish the same result by spoofing ARP requests (layer 3 attack), or with a lot more work, by spoofing entire wireless networks (layer 2 & layer 1 attacks).

NetBIOS and LLMNR resolution are rarely required, and can almost always be disabled to stop these attacks, while ARP spoofing can be detected or prevented by network devices, and malicious wireless network threats can be mitigated by the use of VPN's.

BLOCKING BROADCAST NAME RESOLUTION ATTACKS

NETBIOS

The best solution to block layer-4 name resolution spoofing attacks is to disable NetBIOS broadcast name resolution and disable LLMNR on each system. To disable NetBIOS broadcast name resolution, run this PowerShell command with administrative rights:

```
gwmi Win32_NetworkAdapterConfiguration -Filter "TcpipNetbiosOptions = 0 or
TcpipNetbiosOptions = 1" | %{$_.SetTcpipNetbios(2)}
```

Or run this command with administrative rights:

```
wmic nicconfig where "TcpipNetbiosOptions=1 or TcpipNetbiosOptions=0" call
SetTcpipNetbios 2
```

LLMNR

To disable LLMNR broadcast name resolution, run these PowerShell commands with administrative rights:

```
ni "HKLM:\Software\Policies\Microsoft\Windows\Windows NT\DNSClient" -Type
Directory -Force
```

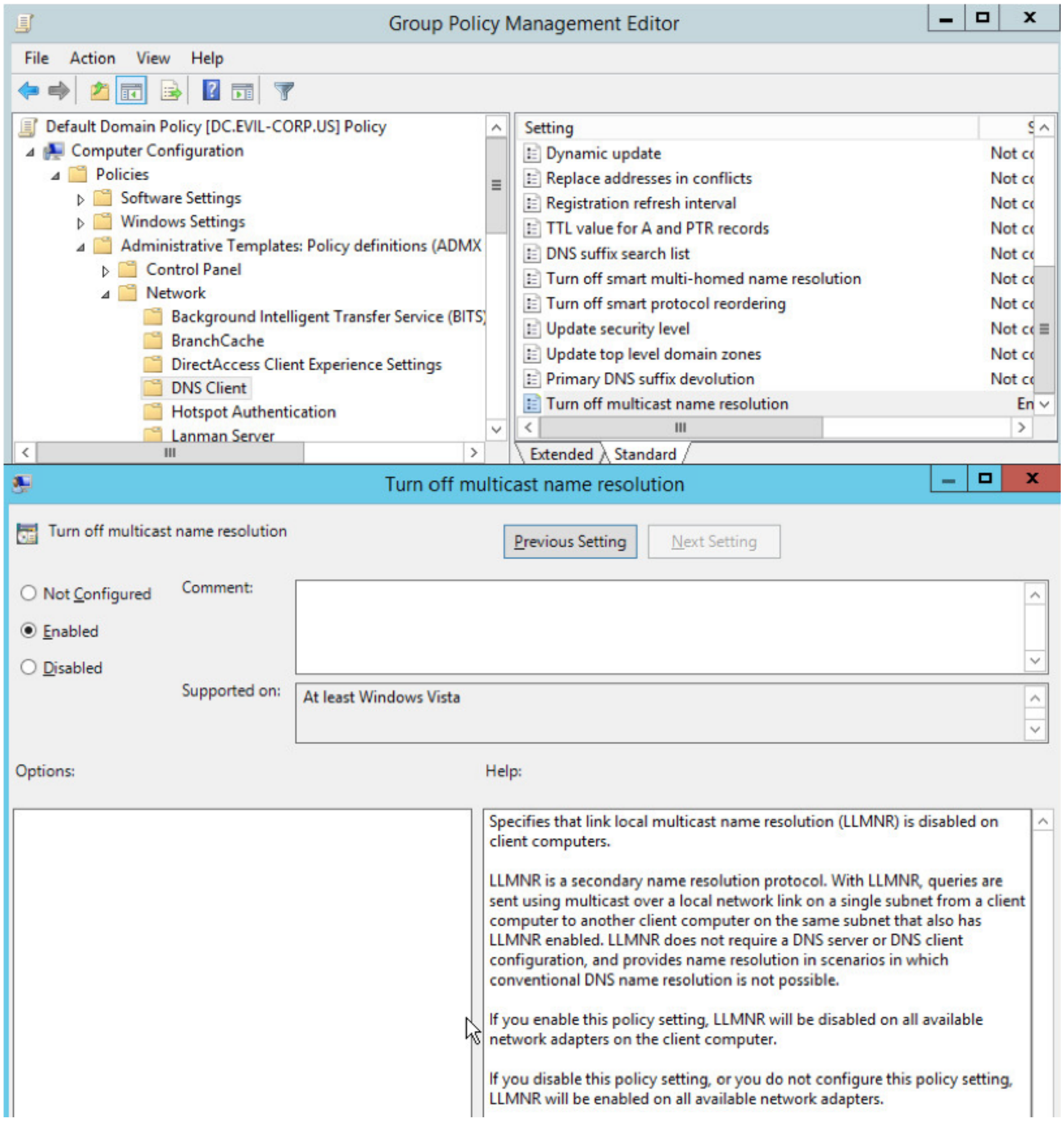
```
sp "HKLM:\Software\Policies\Microsoft\Windows\Windows NT\DNSClient"
EnableMulticast 0
```

Or run this command with administrative rights:

```
reg add "HKLM\Software\Policies\Microsoft\Windows\Windows NT\DNSClient" /v
EnableMulticast /t REG_DWORD /d 0 /f
```

Or, via Group Policy, edit your local or a domain group policy object. Expand Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> DNS Client then double-click on the "Turn Off Multicast

Name Resolution" setting and make sure the State is set to "Enabled".



Default Domain Policy [DC.EVIL-CORP.US] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX
      - Control Panel
      - Network
        - Background Intelligent Transfer Service (BITS)
        - BranchCache
        - DirectAccess Client Experience Settings
        - DNS Client
        - Hotspot Authentication
        - Lanman Server

Setting	S
Dynamic update	Not c
Replace addresses in conflicts	Not c
Registration refresh interval	Not c
TTL value for A and PTR records	Not c
DNS suffix search list	Not c
Turn off smart multi-homed name resolution	Not c
Turn off smart protocol reordering	Not c
Update security level	Not c
Update top level domain zones	Not c
Primary DNS suffix devolution	Not c
Turn off multicast name resolution	En

Turn off multicast name resolution

Turn off multicast name resolution

Previous Setting | Next Setting

○ 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.

BLOCKING ARP SPOOFING ATTACKS

ARP poisoning can still be used, however it is a much more involved process. Many personal firewall and internet security software products have the ability to detect ARP poisoning on any network you are connected to, but the best way to combat ARP poisoning is by using features of your network switches and routers to block it. For example, on most managed network equipment, you should either enable Private VLANs (a.k.a. Port Isolation) or enable DHCP Snooping and Dynamic ARP Inspection. On many wireless routers, you can enable Wireless Isolation (sometimes called Client Isolation) which will block ARP poisoning (and NetBIOS/LLMNR spoofing), at least on that wireless network.

COMBATTING WIRELESS NETWORK SPOOFING ATTACKS

Adversaries might also use low-level wireless spoofing attacks such as the KARMA attack to achieve the same result against wireless network clients, but they are more difficult to perform in common attack scenarios. Tools to do this generally require a Linux system with special drivers and a compatible card or a Windows system with specialized hardware physically close to the target. If someone can perform the attack, it is difficult to prevent, since nearly every wireless client is configured to connect to at least one open wireless network (or a network with a known pre-shared key). Connecting to open wireless networks is not practical to prevent, since they are required to access the internet in most hotels and airports and aircraft, etc.

The best way to defend against spoofed or otherwise untrusted wireless networks is to use a VPN to tunnel your data over the untrusted wireless network, but even those can be attacked by malicious pre-VPN landing pages and cache poisoning.

For the ultimate in untrusted local network isolation, we recommend using a separate device to serve as the VPN router to handle the untrusted network connection, landing page negotiation, and encryption and authentication of the trusted tunnel.

WWW.ROOT9B.COM

WWW.ROOT9B.COM