Broadcast/Multicast Protocol Poisoning

For years, LANMAN was the worst thing in Windows. Then LLMNR said, "Stand Back and Hold My Beer!" Basically, LLMNR lets a host ask for name resolution from any system on the same network. The attackers perform Broadcast/Multicast protocol poisoning on your Active Directory Network.

DETECTION

Cyber Deception
User and Entity Behavior Analytics
Firewall Log Review

TOOLS

mitm6 attacks DHCPv6
Responder attacks LLMNR, NBT-NS, WPAD, and mDNS.

https://github.com/fox-it/mitm6

https://github.com/lgandx/Responder

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to

CDV2_0421

Backdoors & Breaches™

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security