

Forum: [Hack Forums](#)

Thread: [Hacking a Windows LAN network](#)

liamap - May 2, 2017, 2:41 am

I have an organization which has an isolated LAN Network without any connection to WAN.

[edit: Forgot to mention- I can get physical access to one main switch rack there]

Their protection is mostly layer 2. (MAC filtering and OS detection)

So I guess bypassing it is just listening to broadcasts and spoofing an existing MAC and for the OS detection, changing the TTL to 128 (even though, they allow linux and realtime OS's).

So let's assume the layer 2 protection is out of the way; how do I gain access to the Domain? (hijacking priviledged domain users, etc)

Thanks!

Mr. Robot - May 2, 2017, 2:50 am

Well depending on the entire setup and security you can start looking at Man In The Middle attacks, if you have physical access to any machine at any point in time, you could invest in a LanTurtle <https://lanturtle.com/>

Plug their existing cat5 into it and plug the device into the USB port as you can see on the home page.

Otherwise you could try a RubberDucky or Arduino BadUSB to drop a shell <https://hakshop.com/products/usb-rubber-ducky-deluxe>

If the machine you have access to has domain credentials logged, you may try mimikatz to obtain them and/or attempt psexec on the network to other machines to execute payloads or other commands.

It all depends on the setup, access and security.