

Forum:[Hack Forums](#)

Thread: [Hacked in to the LAN, and now need help gaining access to workstation](#)

snitch321 - August 3, 2023, 12:09 pm

So i managed to gain access to a LAN using the Evil Twin attack, now my next step is gaining control/access to a machine on that lan. I have used nmap and sparta for some reconnaissance, and although i do not have the OS version, and the firewall is on, there are 3 open ports available:

27036 - Valve Steam home streaming service
28649 - Utorrent
57621 - Spotify

I am not sure how to use this information to build my next steps of gaining access, would anyone be able to guide me next? bear in mind, man in the middle i know doesn't really work nowadays with HSTS.

DrDemonic - August 3, 2023, 12:39 pm

If you aren't sure what to do from there, look up exploit databases. Often times you can find common security flaws that can be used to attack through the services that are running. If you're sure that the firewall is on, you are going to need to find a way past it first though. Do more recon and see if you can uncover the firewall version, etc.

Ideally, you want to fingerprint the entire network to the best of your ability before actually performing any kind of attack.

DramaKing - August 3, 2023, 1:49 pm

(Aug 3, 2023 12:09 PM)snitch321 Wrote: [\[CITE\]](#) So i managed to gain access to a LAN using the Evil Twin attack, now my next step is gaining control/access to a machine on that lan. I have used nmap and sparta for some reconnaissance, and although i do not have the OS version, and the firewall is on, there are 3 open ports available:

27036 - Valve Steam home streaming service
28649 - Utorrent
57621 - Spotify

I am not sure how to use this information to build my next steps of gaining access, would anyone be able to guide me next? bear in mind, man in the middle i know doesn't really work nowadays with HSTS.

That Steam port is only for inbound game streaming. The Spotify port is in the dynamic port range and only used for Spotify's P2P network. I can't find anything about the uTorrent port, but BitTorrent clients have configurable port assignments to avoid detection. There's one RCE exploit from 2018 that uses XMLHttpRequest(), but I don't know if what you have is the HTTP RPC service.

I would move on since file and printer sharing does not seem to be enabled.

snitch321 - August 4, 2023, 10:31 am

Thanks for your advice guys, i cannot do any more reconnaissance on that machine, because nmap doesn't detect any other open ports. Yea, those ports seem limited with flaws, which is ashame

DramaKing - August 4, 2023, 10:34 am

(Aug 4, 2023 10:31 AM)snitch321 Wrote: [\[CITE\]](#) Thanks for your advice guys, i cannot do any more reconnaissance on that machine, becausr nmap doesn't detect any other open ports. Yea, those ports seem limited with flaws, which is ashame
It isn't for the user being attacked.

snitch321 - August 4, 2023, 10:36 am

Not the best place for victim sympathy hehe