

Forum:[Hack Forums](#)

Thread: [ARP spoofing the gateway \(for "legitimate" redirection of traffic\)](#)

mulletman87 - May 31, 2017, 11:13 pm

Hi everyone!

Is it possible to introduce a linux SoC (running something like Debian) into a network and have it continuously arp spoof a DSL gateway so that all clients push their WAN traffic to the SoC device (without changing their default gateway), without various antivirus IDS systems (and various Android/iOS devices) going crazy?

This is not mean't to be a malicious activity, I just want to make a filtering solution automated to the point where they just plug it into their network, without having to change default gateways, set up various routing rules, etc. Basically, it will be a "plug and play" filtering solution (will run DNS filtering, etc. on the linux SoC).

I have already done some research and ettercap looks like it can do bidirectional spoofing automatically.

Does the logic look good here? If so, then is it possible to get away with this as a solution to route traffic to my filtering SoC without clients having to do anything from their side? Will software packages like ESET (that have an IDS) detect this type of behavior?

This is just brainstorming, any advice would be appreciated.

UPDATE: I have done a little more research, it seems that if I do this, the DSL router and the linux SoC device will compete for ARP updates. In doing this, sometimes traffic will be sent to the DSL router, and sometimes to the other device. This won't be a reliable option, but is there any way to stop this from happening? I don't want to configure static ARP entries on the PC's on the network, but if anyone has any ideas, that would be great!