

Forum:[Hack Forums](#)

Thread: [Remote MITM attack??](#)

trish - April 24, 2019, 11:53 am

ok after cracking a network i was wondering whether i could leave a "virtual device" on the network performing a MITM even while i'm absent? Is there already a technique for this?

Cooooool - April 24, 2019, 12:02 pm

Just a fair warning, I am really not that experienced when it comes to network sniffing but you could plant a physical device like a raspberry pi zero looping a sniffing script. With the right tools you could even make it so you have FTP access to it so you can access the logs remotely.

ombudsman - April 24, 2019, 12:12 pm

(Apr 24, 2019 12:02 PM)Cooooool Wrote: [\[CITE\]](#) Just a fair warning, I am really not that experienced when it comes to network sniffing but you could plant a physical device like a raspberry pi zero looping a sniffing script. With the right tools you could even make it so you have FTP access to it so you can access the logs remotely.

What he said, but also you can't have a mitm account without having the ability to sniff traffic, which is mostly done from close proximity but, you could also hack target 1 which is in proximity of the target 2 and then do a MITM from that target, you can't run a MITM attack 100kms away tho.

Sitrep - April 25, 2019, 3:42 pm

Just a note first, this is highly illegal and I do not want you to do it...

But, if you have access to the network already, you could try to plant a RAT or some FUD backdoor on a target machine if you have access to it.

Otherwise try to use SSLsplit on the network to watch all traffic going in and out from that network. Those are some pretty old and outdated techniques that I listed but it's worth a shot I guess.

CyberStrike - April 25, 2019, 10:51 pm

A virtual device ? Hmm initially I'd think that rooting the router and performing a BGP hijacking attack would be easier than getting a machine putting a hypervisor and hopefully keeping it all "silent" as to not allow users to detect what's going on. Also you would have to change the routing on all the machines in the network. BGP hijacking generally will require quite a function set from a router's firmware such as an ssh.

Asdethprime - April 26, 2019, 12:57 am

This is generally done only by APTs but the way they go about doing this is slightly different.

Once u get into the network this is normally achieved by dropping a logging module on the wifi box. This can require you to drop a malicious driver on the wifi box or on rare occasion require you to flash and upgrade the device firmware.

CIA were using a similar tool and was name Flytrap.

xtdozo - May 8, 2019, 12:03 am

You could leave a virtual machine connected to the network running anything you want using ARP poisoning and DNS spoofing

