

Forum:[Hack Forums](#)

Thread: [bettercap network probe, recon, sniff attack](#)

hdawg12 - September 10, 2022, 12:01 am

I have a quick question. In regards to bettercap. If I perform a net.probe, net.recon and/or net.sniff attack, will that be to loud of a network scan and will it give me away?

DramaKing - September 12, 2022, 9:50 am

If you use net.probe in a way that would create unusual activity, then an IDS/IPS may detect it. The others are completely passive, and the only thing that might give you away is an unrecognized MAC address.

hdawg12 - September 12, 2022, 8:35 pm

in your opinion , when doing an nmap scan of the network, what would you use to be under the radar/stealthy, but still capture important information. I

DramaKing - September 13, 2022, 5:45 am

I found this on nmap.org:

System logs alone are rarely sufficient for detecting port scans. Usually only scan types that establish full TCP connections are logged, while the default Nmap SYN scan sneaks through. Even full TCP connections are only logged if the particular application explicitly does so. Such error messages, when available, are often cryptic. However, a bunch of different services spouting error messages at the same time is a common indicator of scanning activity. Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly. The vast majority of log messages go forever unread. Log monitoring tools such as Logwatch and Swatch can certainly help, but the reality is that system logs are only marginally effective at detecting Nmap activity.

It also mentions port scan detectors, but you're highly unlikely to encounter such a thing. And if you're doing a security assessment, no worries. If you're not, I would assume that you're remote, so just hide yourself.

hdawg12 - September 13, 2022, 10:15 pm

thanks for the info. What if you create a whole different network separate from you home network(pretending this is a victims home network) and you try to hack their pc. Using nmap to scan for open ports allows you to try and find a vulnerability and get access to his PC, correct?(i know its not just finding open ports that gets access to a PC, but also other methods like performing a reverse-shell)

Another question that has to do with ports. I created a VM(virtualbox) with windows 10 installed and I purposely activated Telnet. when I did an nmap -A(aggressive scan), I noticed telnet popped up ,but the status said CLOSED. Why do you think that is, even though I activated it in my Windows VM?