Tracy Harvey

10/27/2023

Module 6 Group Drop Box

I ended up using my Microsoft surface to scan my main gaming computer, my cell phone, and my unRaid File/Media Server.

The Basic network scan was probably the most different between the three targets. My phone came back with 7 vulnerabilities all of which were just info. My Gaming computer came back with 22 vulnerabilities of which one was a medium for SMB signing not required. I kind of knew about that already as I have a Linux based server (my unRaid file/media server) on my network, and I have had to do some jerry rigs to get things to talk to each other at least until I can have time to sit down and figure out the issues with my home network. The largest surprise was the unRaid server scan it came back with 30 vulnerabilities two of which were medium, two were mixed, and 2 were high. The medium ones were mostly more SMB stuff which like I said earlier it is a compromise to get the server to talk to the Microsoft products on the network. One of the mixed ones is SSL in nature which it was just telling me that my security certificates were self-signed which I knew already. One of the high ones kind of caught me off guard it was because my unRaid server uses VNC to connect to the VMs that I can build on the server but it does so with basically no authentication to get into the VNC instance which I knew about but did not realize that it was that big of an issue. The other high one I will have to look into as it has to do with Microsoft Windows SMB Shares Unprivileged access which I can only assume has something to do with some of my SMB shares being open to the public on my network. Those are for things I want my family or friends or even myself to have access to with out having to go through authentication and reading the vulnerability it seems that it is basically telling me that the general public on my network has unfettered access to these shares which I know about already. The question is can an attacker take that an jump to the privileged access somehow? The other scans didn’t turn up anything other than informational things. I could not run the Malware scan against my phone as it kept telling me that I needed to provide admin credentials which I don’t even know what that would be on my phone.

Most of the issues I already know about, but I would recommend to myself to look into that VNC one and work out how to lock VNC sessions down.