Matthew Ryan

Security Hardening

After installing Lynix, I was surprised at how thorough it was with the audit of my system. It helped me discover methods of security and vulnerabilities in my system that I would’ve never been aware of, it really helped me learn more about security.

I’ve already looked into password hashing and aging. Lynix also suggests that I use a file integrity tool, which I will definitely look into as our acme servers have a lot of file exchange going on. I will also make my home directory’s permissions more strict – something I would’ve forgotten about without this audit, as right now any user is able to take a look into my home directory and view all sorts of data. And lastly, I will look into getting a malware scanner on my server, I’m already looking into Sophos which seems to have a decent reputation in the Linux community.

Network health monitoring script:

In my monitoring script, I chose to have commands such as ‘free’ and ls -laSh, sorted by ‘memory’ in order to make sure the server doesn’t overload on disk space, as I’m sure we’ll be using a lot of files on the acme corp servers. I think it’s a good idea to run this script at least once per session, so that we can take note of changes made per login session and keep a log of changes to better monitor the health of the system. In addition to that, the script calls a ‘last’ command so we can see the most recent users logged on, could be useful for tracking down any malicious intent or to pinpoint the cause of something going wrong. In addition, I have included an iostat call in the script to monitor the health of the disks so that we don’t lose data, and can pinpoint of there is something wrong with our disks, making sure everything is running smoothly. And lastly, I call a ps aux command, sorted by the top 10 highest memory usage processes. I think this command could be very useful to see if there is a corrupted process running, or seeing if we have too many processes running, taking up too much memory space. I think this is a very useful command to have to begin looking into possible issues we could have.

Running the script remotely:

The script can be run remotely, by SSH into the server. You will enter:

**ssh <username>@mryanserver /home/<username>/healthcheck.sh.**

This will also create a file called networkCheck in your current directory, that will append the contents of this script to the file as well.

I will provide each user with this script in their home directory for usage, and it should be run at least once per session. The script creates a log file in the same directory (networkCheck) that we can use for logging.