Security, Hardening, and Compliance

Health Monitoring Script

Health monitoring is very important in ensuring our servers are secure and running properly. The script below monitors and can pull information that we would like to keep an eye out on within our servers. Some things include networking traffic, memory, cpu usage, and drive and system usage. This gives us an understanding of our hardware’s health state.

The health monitoring script is always located in the **/root/class/linux/** directory with the file name: **health\_script**. Ensure the file permissions are set to **755** using the **chmod** command

The script looks like this:

#!/bin/sh

# Load average

dstat -l 5 6 >> /root/class/linux/health\_log

# Network statistics

dstat -n 4 5 >> /root/class/linux/health\_log

# Tcp statistics

dstat --tcp 10 5 >> /root/class/linux/health\_log

# CPU statistics

dstat -c 2 6 >> /root/class/linux/health\_log

# Memory usage and statistics

dstat --mem-adv 4 6 >> /root/class/linux/health\_log

# Disk activity

dstat -a 2 5 >> /root/class/linux/ health\_log

To execute the script cd into the given directory and run this command:

**# ./health\_script**

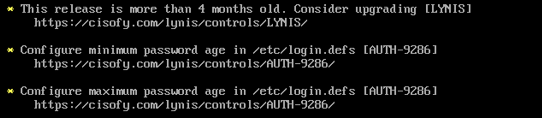
The script will output to the same location and be named **health\_log**.

Lynis Report

Lynis is a security tool that preform health scans to our systems that include compliance and hardening tests. This ensures are system is safe and running correctly giving us reports and audits of our machines.

<https://cisofy.com/lynis/>

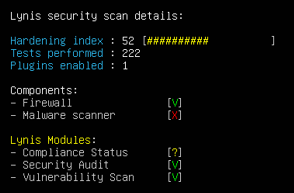
While running Lynis on my VM’s I was proposed 25 suggestions on my CentOS and a extensive list on my Ubuntu virtual machine. A few of the suggestions I received on my CentOS VM included these..



The first one tells me that my version is 4 months old which can cause some security loopholes. It is not incrediablly out of date and can be ignored but is best to keep our systems up to date to ensure top level security. This allows us to keep an eye out on our version and how out of date it is getting.

The other two suggestions include password age limits. It is good to change passwords semi regularly. At least once a year to ensure the password is more secure and prone to getting cracked. Which I had gone in and changed my password, just in case.

Another report I received was to install and have a malware scanner to ensure nothing is on my machines that we may be unaware about.



This ensure that if anything has found its way onto our servers file system it will be scanned and automatically removed. I did some research and found a service called **ClamAV**. This is a antivirus engine that detects virus, malware, trojans, and rootkits. Which can be installed by running the following commands in order below:

**sudo apt-get install clamav**

**yum -y update**

**yum -y install clamav**

Once installed we can run the command by :

**freshclam**

**clamscan -r -I “directory”**

The operators -r is a recursively scan and -i shows infected files.

I had installed this service because it is good to ensure our file system and server is safe with no hidden infected files, we may be unaware about. This is good practice to run this scan at least once a week. It can also be put on a schedule which I had not done. Although I would do if the server had high levels of traffic every day.