**Security Controls**

**MariaDB**

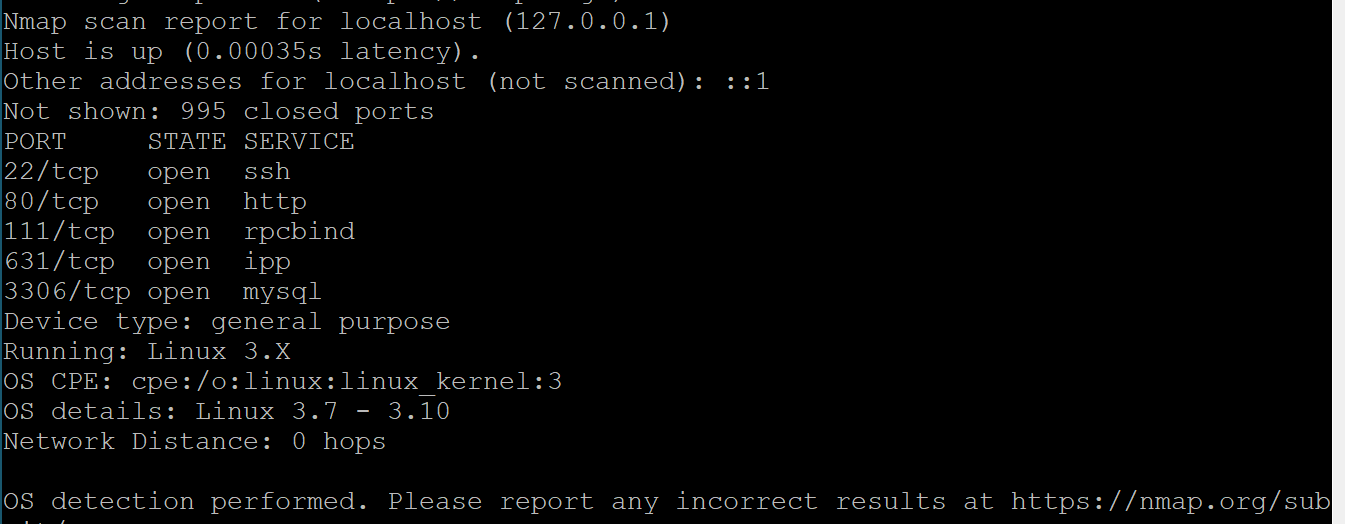
* **Install logging plugin**
* **Stronger password on DB**
* **Encrypt data on DB;**
* **User/groups with passwords and permissions**

**Apache Server**

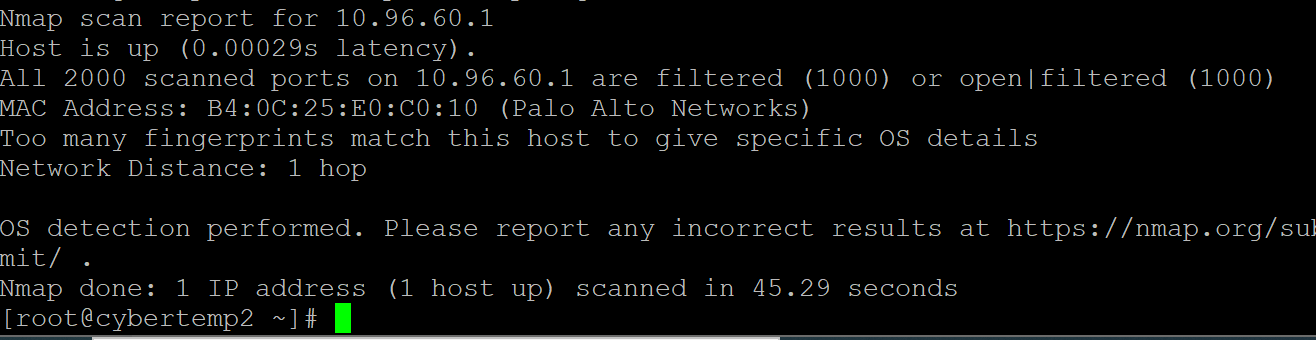
* **Disable the server-info directive-** displays information about the server’s configuration
* **Disable the server-status directive-** displays information about server performance, such as server uptime, server load, current HTTP requests, and clients’ IP addresses.
* **Disable the server-signature directive**- displays information about server configuration such as version of Apache and the operating system.
* **Disable the directory listing**- allows users to view complete directory contents.
* **Enable logging**
* **ModSecurity WAF (prevents SQL injection/XSS)**
* **Force users to use HTTPS**

**VM**

* **Stronger password for root**
* **User group with passwords and permissions**
* **Logging**
* **Disable open port 631 IPP (Internet Printing Protocol), unused port**
* **Disable open port 80 HTTP; after HTTPS redirect is established on web server**



*\*The image above shows all open ports on our* ***local host (VM)****. All ports are necessary except for port 631/IPP. Also, notice how OS/kernel information was retrieved from Nmap. We need to disable this feature it can be extremely useful to a hacker.*



*\*The image above shows an attempt to run port discovery using Nmap on the default gateway. No port information was given due to the ports are filtered implying that there is a firewall rejecting ICMP traffic to those ports. Therefore, we should just focus on securing the ports we have control of, the local host.*