I am building a **beginner-level project** for someone who wants to practice and understand how we can build a project which can in the future lead to a monitoring tool for a system admin to be alerted if any vulnerability happens by adding additional configurations, which I will be adding too in the following days and share with you all!

Note: Here we have to make sure that the permissions are made open just in case anyone else from the team wants to work on the project

sudo chown ubuntu /var/www/html
sudo chmod 777 /var/www/html

(POV: do it at your own risk but do change it once you are done experimenting)

Step 1

We will have to Install Apache2, PHP and nmap
sudo apt-get install apache2
sudo apt-get install php
sudo apt-get install nmap

What is Linux Crontab?

Linux Crontab is a powerful utility used for **Scheduling and Automating Tasks** in Unix-like operating systems. It allows users to run the scripts or Linux Commands at specified times and intervals. It is ideal for repetitive tasks such as system maintenance, backups, and updates.

Each user can have their **Crontab file**, where they can define the scheduling commands that are to be executed. It helps in simplifying the task automation enhancing the system efficiency and reliability. Crontab stands for "cron table, " because it uses the job scheduler cron to execute tasks; cron itself is named after "Chronos, " the Greek word for time.

Step 2

Cron Job Configuration
sudo crontab -e
*/10 * * * * nmap 192.*.*.* /24 -oN /var/www/html/nmap.html

Here 10 * * * * * means that every 10 minutes we will be running the Nmap script which will be stored in an nmap.html file.

Step 3

Network.php

```php
<?php
echo "Server Timestamp: ";
# here we are using data function to show the exact time when the process ran # and also confirm that our code is running
echo date("h:i:sa");
echo "<pre>";
include("nmap.html");
echo "</pre>";
?>
```

In the end, we will be creating a network.php file in the same folder as nmap.html it will run the output from the nmap.html .

The output will look like this :

```
Server Timestamp: 05:19:57am

# Nmap 7.94SVN scan initiated Wed Oct 16 16:19:01 2024 as: /usr/lib/nmap/nmap -oN /var/www/html/nmap.html ███████████
Nmap scan report for ███████████
Host is up (0.00s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp open  http

# Nmap done at Wed Oct 16 16:19:14 2024 -- 1 IP address (1 host up) scanned in 13.07 seconds
```