Skynet

Escaneo

Hacemos el escaneo tradicional y guardamos todo los datos que veamos utiles

```bash
nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn ipvictima -oN escaneo
```

```
❯ nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.10.95.188 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-25 00:49 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:49
Completed NSE at 00:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:49
Completed NSE at 00:49, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:49
Completed NSE at 00:49, 0.00s elapsed
Initiating SYN Stealth Scan at 00:49
Scanning 10.10.95.188 [65535 ports]
Discovered open port 80/tcp on 10.10.95.188
Discovered open port 445/tcp on 10.10.95.188
Discovered open port 143/tcp on 10.10.95.188
Discovered open port 22/tcp on 10.10.95.188
Discovered open port 139/tcp on 10.10.95.188
Discovered open port 110/tcp on 10.10.95.188
Completed SYN Stealth Scan at 00:49, 11.95s elapsed (65535 total ports)
```

Aqui esta los datos importantes

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKeTyrvAfbRB4onlz23fmgH5DPnSz07voOYaVMKPx5bT62zn7eZzecIVvfp5LBCetcOyiw2Yhocs0oO1/RZSqXlwTVzRNKzznG4WTPtkvD7ws/4tv2cAGy1lzRy9b+361HHIXT8
GNteq2mU+boz3kdZiiZHIml4oSGhI+/+IuSMl5clB5/FzKJ+mfmu4MRS8iahHlTciFlCpmQvoQFTA5s2PyzDHM6XjDYH1N3Euhk4xz44Xpo1hUZnu+P975/GadIkhr/Y0N5Sev+Kgso241/v0GQ2lKrYz3RPgmNv93AIQ4t3i3P6qDn
ta/06bfYDSEEJXaON+A9SCpk2YSrj4A7
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI0UWS0x1ZsOGo510tgfVbNVhdE5LkzA4SWDW/5UjDumVQ7zIyWdstNAm+lkpZ23Iz3t8joaLcfs8nYCpMGa/xk=
|   256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICHVctcvlD2YZ4mLdmUlSwY8Ro0hCDMKGqZ2+DuI0KFQ
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Skynet
110/tcp open  pop3        syn-ack ttl 63 Dovecot pop3d
|_pop3-capabilities: UIDL CAPA RESP-CODES SASL TOP AUTH-RESP-CODE PIPELINING
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        syn-ack ttl 63 Dovecot imapd
|_imap-capabilities: have ID LOGINDISABLEDA0001 SASL-IR Pre-login more post-login listed capabilities IDLE ENABLE LITERAL+ OK IMAP4rev1 LOGIN-REFERRALS
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Aqui vemos lo que estaa corriendo que version de la web esta en la IP

```
❯ whatweb http://10.10.95.188
http://10.10.95.188 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.95.188], Title[Skynet]
```

Elegimos un puerto y empezamos a intetar vulnerarlo

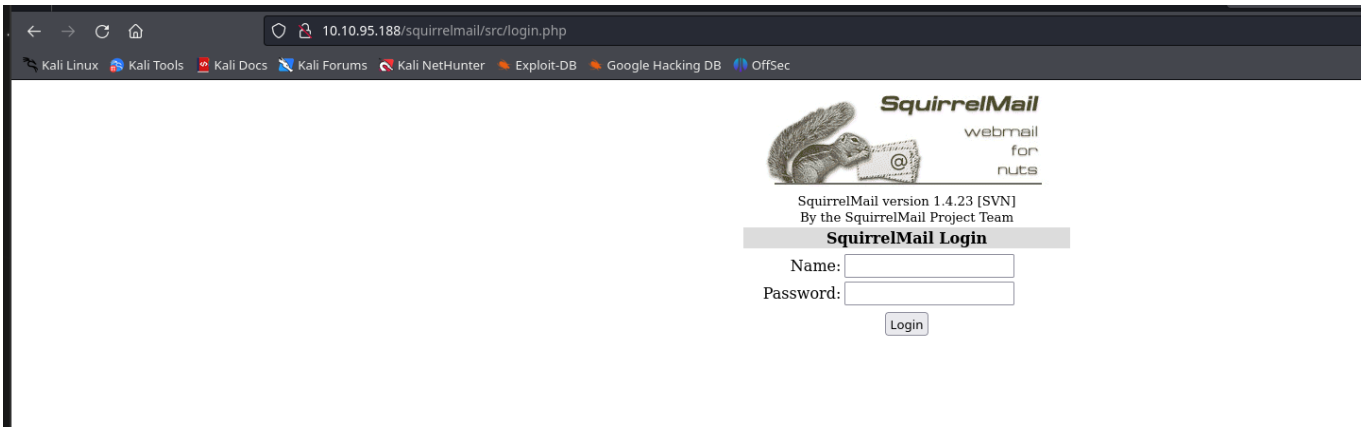
Puerto 80

Ahora vamos a hacer Fuzzing

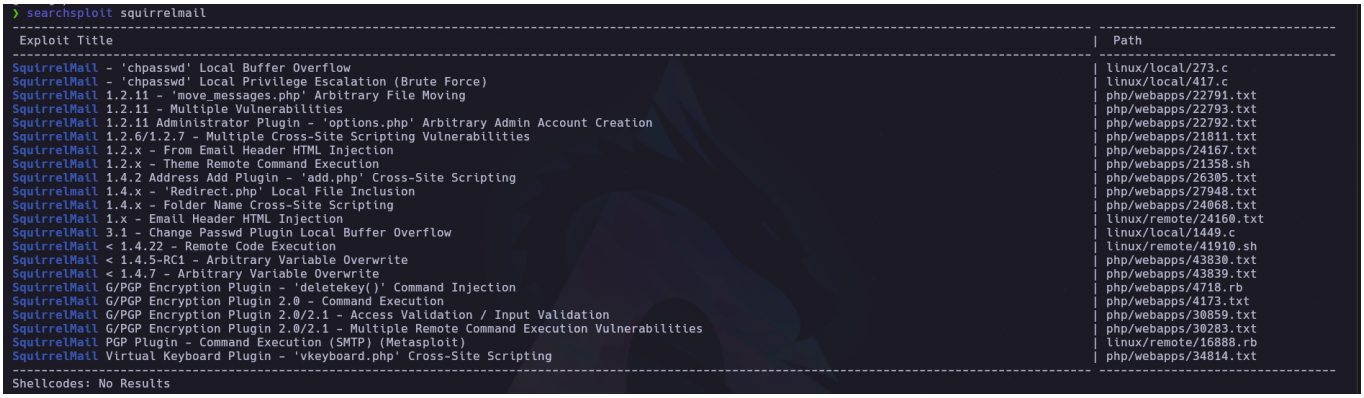
```
❯ wfuzz -c -L -t 400 --sc=200,301 -w /usr/share//wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.95.188/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.95.188/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        18 L     43 W       523 Ch      "# directory-list-2.3-medium.txt"
000000003:   200        18 L     43 W       523 Ch      "# Copyright 2007 James Fisher"
000000014:   200        18 L     43 W       523 Ch      "http://10.10.95.188/"
000000004:   200        18 L     43 W       523 Ch      "#"
000000002:   200        18 L     43 W       523 Ch      "#"
000000006:   200        18 L     43 W       523 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000005:   200        18 L     43 W       523 Ch      "# This work is licensed under the Creative Commons"
000000009:   200        18 L     43 W       523 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000010:   200        18 L     43 W       523 Ch      "#"
000000011:   200        18 L     43 W       523 Ch      "# Priority ordered case sensative list, where entries were found"
000000012:   200        18 L     43 W       523 Ch      "# on atleast 2 different hosts"
000000013:   200        18 L     43 W       523 Ch      "#"
000000008:   200        18 L     43 W       523 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000007:   200        18 L     43 W       523 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000020087:   200        76 L     277 W      2912 Ch     "squirrelmail"
000045240:   200        18 L     43 W       523 Ch      "http://10.10.95.188/"

 /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Pycurl error 28: Operation timed out after 90003 milliseconds with 0 bytes received
Total time: 90.15288
Processed Requests: 65281
```

Pero lo he hecho tambien con otra herramienta dirsearch

```
❯ dirsearch -u http://10.10.95.188 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /usr/share/seclists/Discovery/Web-Content/reports/http_10.10.95.188/_24-01-25_01-40-44.txt

Target: http://10.10.95.188/

[01:40:44] Starting:
[01:40:46] 301 -  312B  - /admin  ->  http://10.10.95.188/admin/
[01:40:47] 301 -  310B  - /css  ->  http://10.10.95.188/css/
[01:40:49] 301 -  309B  - /js  ->  http://10.10.95.188/js/
[01:40:50] 301 -  313B  - /config  ->  http://10.10.95.188/config/
[01:40:57] 301 -  309B  - /ai  ->  http://10.10.95.188/ai/
[01:41:53] 301 -  319B  - /squirrelmail  ->  http://10.10.95.188/squirrelmail/
CTRL+C detected: Pausing threads, please wait...

Task Completed
```



Lo que encontramos



```
❯ searchsploit squirrelmail
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
SquirrelMail - 'chpasswd' Local Buffer Overflow                                                                                                       | linux/local/273.c
SquirrelMail - 'chpasswd' Local Privilege Escalation (Brute Force)                                                                                    | linux/local/417.c
SquirrelMail 1.2.11 - 'move_messages.php' Arbitrary File Moving                                                                                       | php/webapps/22791.txt
SquirrelMail 1.2.11 - Multiple Vulnerabilities                                                                                                        | php/webapps/22793.txt
SquirrelMail 1.2.11 Administrator Plugin - 'options.php' Arbitrary Admin Account Creation                                                             | php/webapps/22792.txt
SquirrelMail 1.2.6/1.2.7 - Multiple Cross-Site Scripting Vulnerabilities                                                                              | php/webapps/21811.txt
SquirrelMail 1.2.x - From Email Header HTML Injection                                                                                                 | php/webapps/24167.txt
SquirrelMail 1.2.x - Theme Remote Command Execution                                                                                                   | php/webapps/21358.sh
SquirrelMail 1.4.2 Address Add Plugin - 'add.php' Cross-Site Scripting                                                                                | php/webapps/26305.txt
SquirrelMail 1.4.x - 'Redirect.php' Local File Inclusion                                                                                              | php/webapps/27948.txt
SquirrelMail 1.4.x - Folder Name Cross-Site Scripting                                                                                                 | php/webapps/24068.txt
SquirrelMail 1.x - Email Header HTML Injection                                                                                                        | linux/remote/24160.txt
SquirrelMail 3.1 - Change Passwd Plugin Local Buffer Overflow                                                                                         | linux/local/1449.c
SquirrelMail < 1.4.22 - Remote Code Execution                                                                                                         | linux/remote/41910.sh
SquirrelMail < 1.4.5-RC1 - Arbitrary Variable Overwrite                                                                                               | php/webapps/43830.txt
SquirrelMail < 1.4.7 - Arbitrary Variable Overwrite                                                                                                   | php/webapps/43839.txt
SquirrelMail G/PGP Encryption Plugin - 'deletekey()' Command Injection                                                                                | php/webapps/4718.rb
SquirrelMail G/PGP Encryption Plugin 2.0 - Command Execution                                                                                          | php/webapps/4173.txt
SquirrelMail G/PGP Encryption Plugin 2.0/2.1 - Access Validation / Input Validation                                                                   | php/webapps/30859.txt
SquirrelMail G/PGP Encryption Plugin 2.0/2.1 - Multiple Remote Command Execution Vulnerabilities                                                      | php/webapps/30283.txt
SquirrelMail PGP Plugin - Command Execution (SMTP) (Metasploit)                                                                                       | linux/remote/16888.rb
SquirrelMail Virtual Keyboard Plugin - 'vkeyboard.php' Cross-Site Scripting                                                                            | php/webapps/34814.txt
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

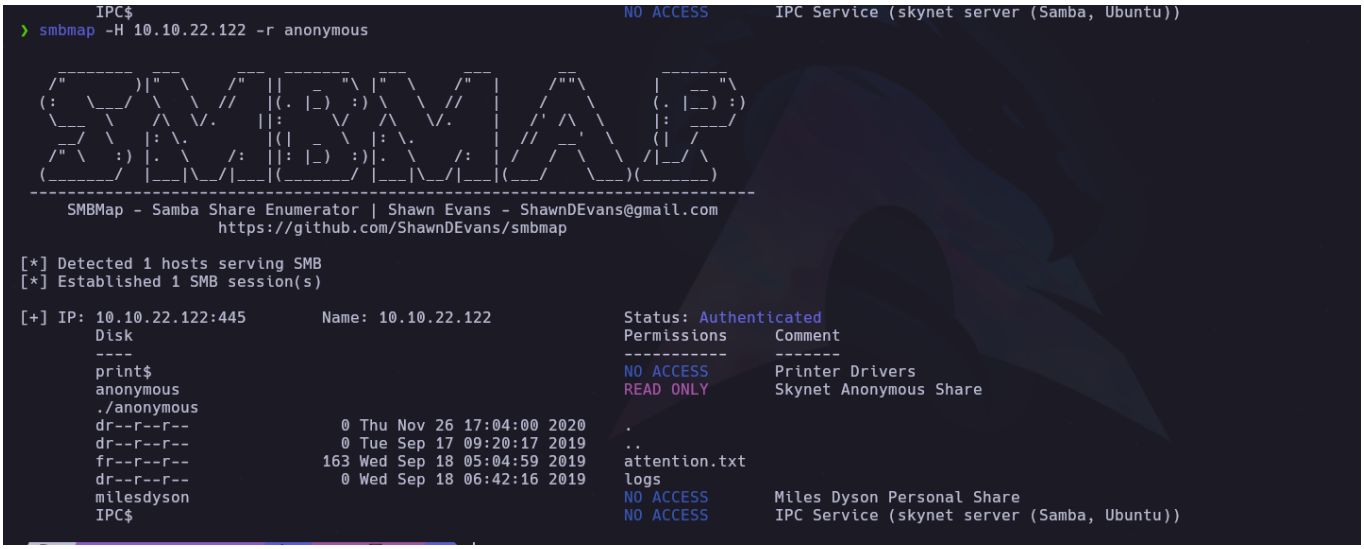
Si ya nos quedamos parados aqqui seguimos con el siguiente puerto

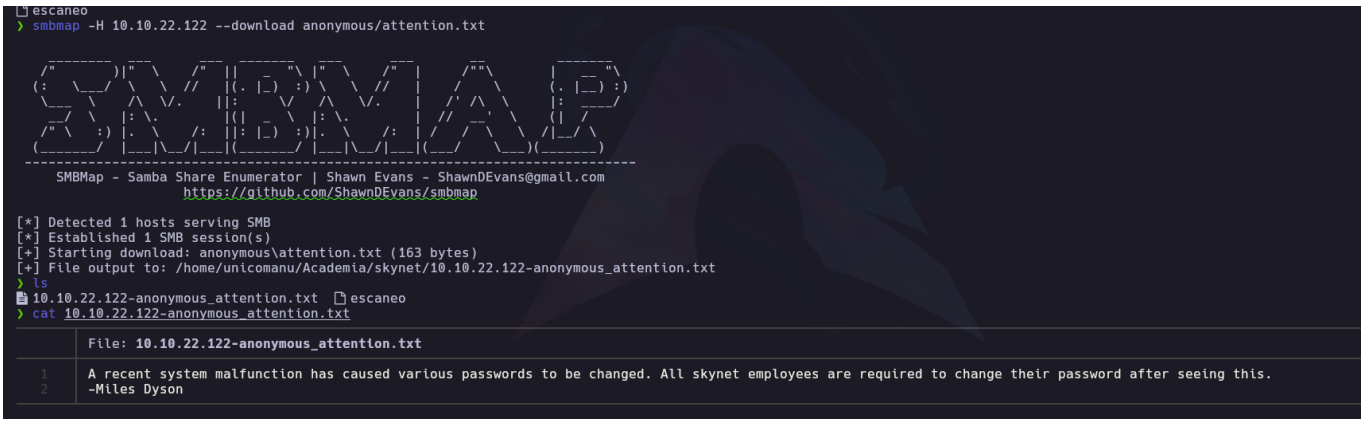
que el es

Puerto 139

```
❯ smbmap -H 10.10.22.122

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.22.122:445        Name: 10.10.22.122              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))

 /home/unicomanu
```

Al tener la lectura del usuarios anonymous continuamos con ese usuario

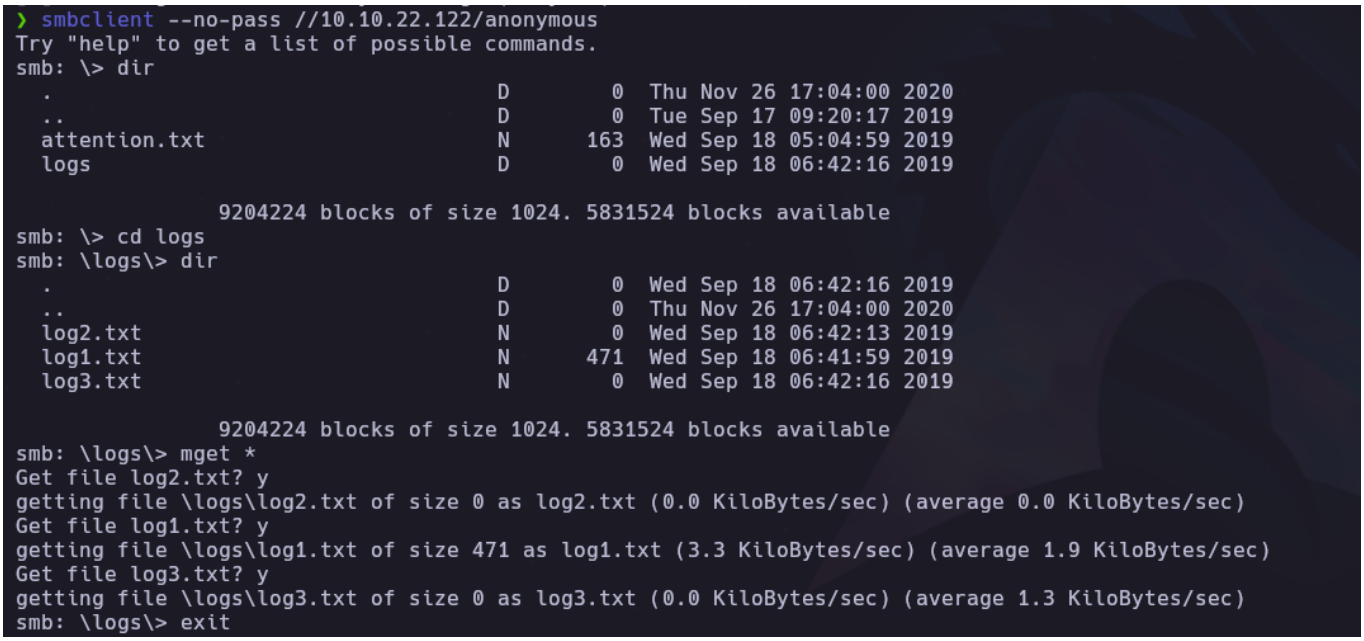




Para obtener lo del directorio logs

haremos estos pasos

```
smbclient --no-pass //ipvictima/usuario/o/anonymous
```



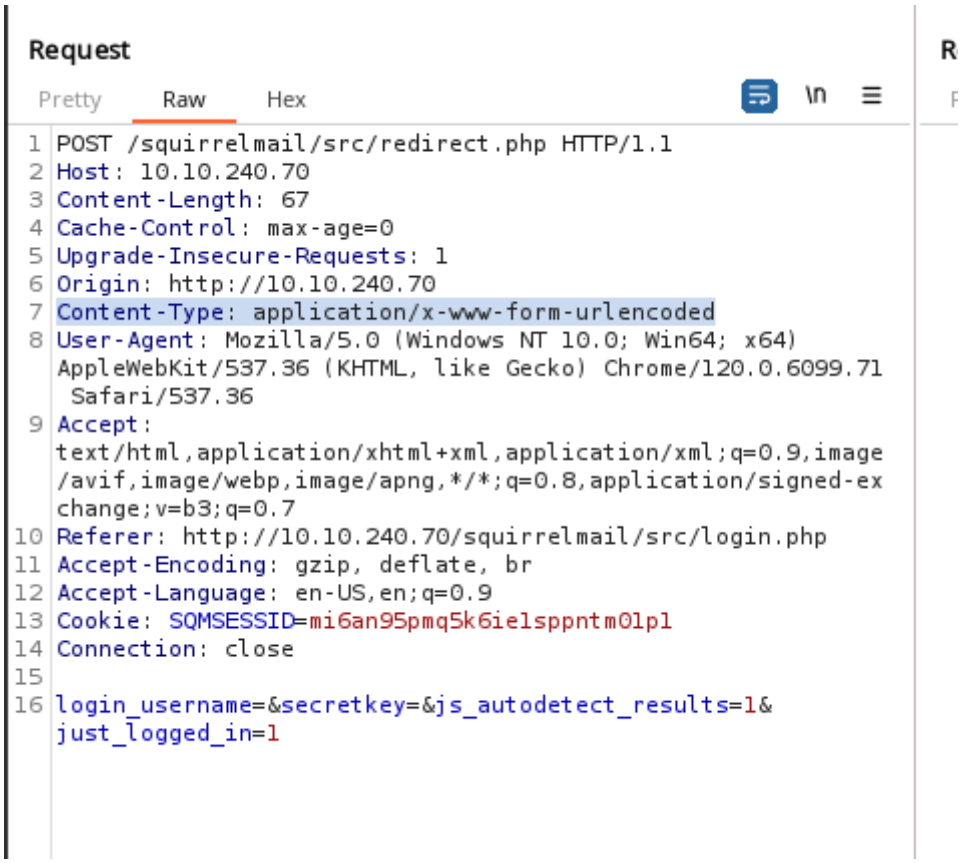
Una vez descargados vemos lo que contiene el dir LOGS

```
❯ cat log1.txt
       File: log1.txt
   1   cyborg007haloterminator
   2   terminator22596
   3   terminator219
   4   terminator20
   5   terminator1989
   6   terminator1988
   7   terminator168
   8   terminator16
   9   terminator143
  10   terminator13
  11   terminator123!@#
  12   terminator1056
  13   terminator101
  14   terminator10
  15   terminator02
  16   terminator00
  17   roboterminator
  18   pongterminator
  19   manasturcaluterminator
  20   exterminator95
  21   exterminator200
  22   dterminator
  23   djxterminator
  24   dexterminator
  25   determinator
  26   cyborg007haloterminator
  27   avsterminator
  28   alonsoterminator
  29   Walterminator
  30   79terminator6
  31   1996terminator
```

```
❯ cat log2.txt
       File: log2.txt   <EMPTY>
❯ cat log3.txt
       File: log3.txt   <EMPTY>
```

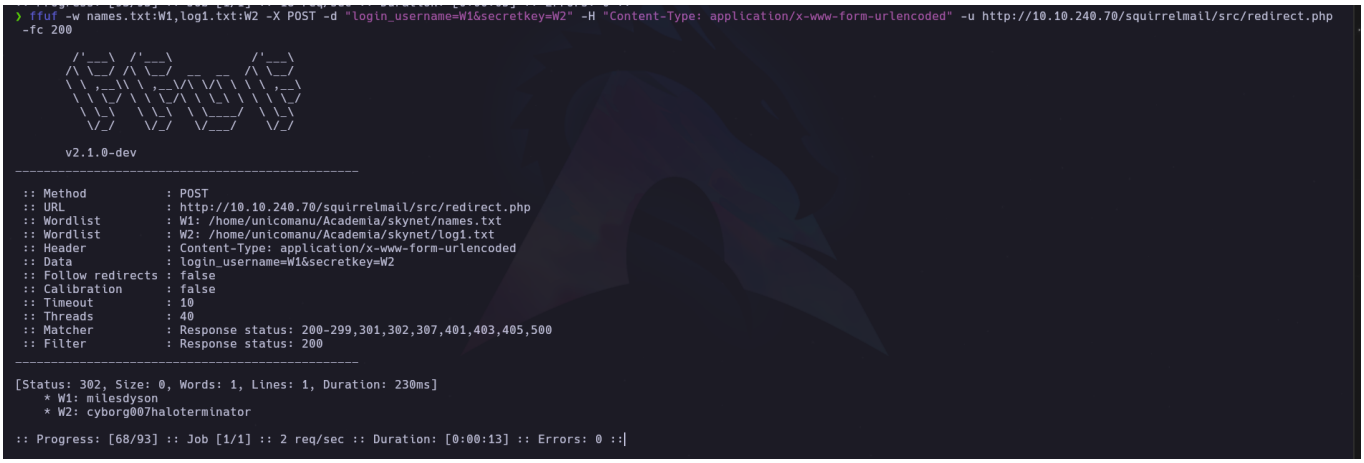
Despues de ver el archivo de log1.txt vemos que vamos a utilizar la fuerza bruta por diccionario

Para ello tenemos qeu dirigirnos al burpsuite y hacemos en el reapeter el POST y lo que tenemos que tener en cuenta es este apartado



Content-Type: application/x-www-form-urlencoded

Para poner en el -H

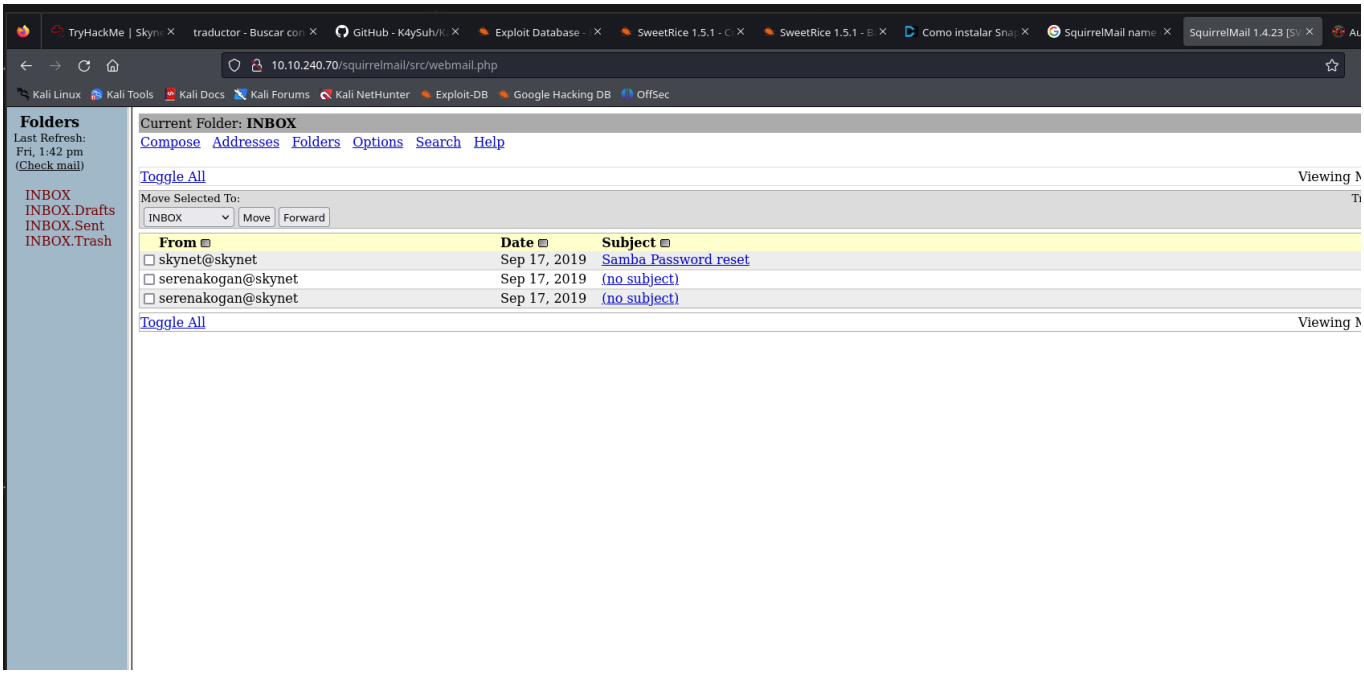


Una vez hecho esto hacemos el ffuf y nos sale el usuario y el pass

Ponemos el usuario y la contraseña

Y ya estamos dentro

Aqui


10.10.240.70/squirrelmail/src/webmail.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Folders
Last Refresh:
Fri, 1:42 pm
(Check mail)
INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash
Current Folder: INBOX
Compose Addresses Folders Options Search Help
Toggle All
Move Selected To:
INBOX
Move
Forward
From
Date
Subject
skynet@skynet
Sep 17, 2019
Samba Password reset
serenakogan@skynet
Sep 17, 2019
(no subject)
serenakogan@skynet
Sep 17, 2019
(no subject)
Toggle All