Chain

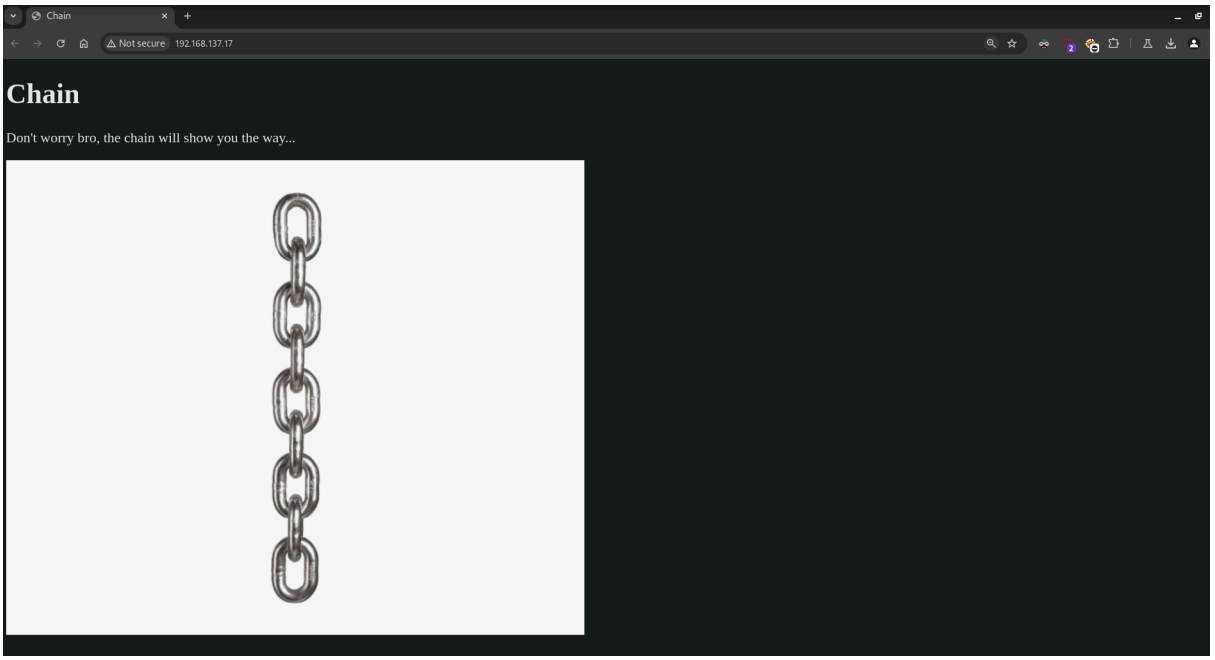
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sS -p- -Pn -n -vvv 192.168.137.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 11:40 -03
Initiating ARP Ping Scan at 11:40
Scanning 192.168.137.17 [1 port]
Completed ARP Ping Scan at 11:40, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:40
Scanning 192.168.137.17 [65535 ports]
Discovered open port 80/tcp on 192.168.137.17
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.53% done; ETC: 11:40 (0:00:42 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.81% done; ETC: 11:40 (0:00:02 remaining)
Completed SYN Stealth Scan at 11:40, 14.20s elapsed (65535 total ports)
Nmap scan report for 192.168.137.17
Host is up, received arp-response (0.0019s latency).
Scanned at 2025-02-02 11:40:03 -03 for 14s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 00:0C:29:6E:7C:A0 (VMware)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap --script http-enum -p80 -Pn -n -vvv 192.168.137.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 11:40 -03
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 0.00s elapsed
Initiating ARP Ping Scan at 11:40
Scanning 192.168.137.17 [1 port]
Completed ARP Ping Scan at 11:40, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:40
Scanning 192.168.137.17 [1 port]
Discovered open port 80/tcp on 192.168.137.17
Completed SYN Stealth Scan at 11:40, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.137.17.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:40
Completed NSE at 11:40, 1.00s elapsed
Nmap scan report for 192.168.137.17
Host is up, received arp-response (0.00085s latency).
Scanned at 2025-02-02 11:40:37 -03 for 1s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 00:0C:29:6E:7C:A0 (VMware)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.17
http://192.168.137.17 [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.137.17], Title[Chain]
```

Descargo la imagen



usando el comando strings vemos una id_rsa embebida en el png

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# strings chain.png
```

usamos john para desencriptar

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nano hash

┌──(root💀miguel)-[/home/miguel/Work]
└─# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
blue12           (id_rsa)
1g 0:00:00:02 DONE 3/3 (2025-02-02 12:10) 0.4237g/s 149198p/s 149198c/s 149198C/s blase1..blue09
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

continuamos enumerando pues no tenemos puerto 22 para conectarnos ni usuario

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt   -u "http://192.168.137.17/" -t 200 -x php
html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.17/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 279]
/wordpress           (Status: 301) [Size: 320] [--> http://192.168.137.17/wordpress/]
/javascript          (Status: 301) [Size: 321] [--> http://192.168.137.17/javascript/]
/index.html          (Status: 200) [Size: 202]
```

incluimos en el etc/hosts

```
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.17 chain.yx
```

segui buscando pero nada por subdominios ni extensiones asi que lo unico que me quedaba era por UDP luego de varios fallos y demora encontramos el snmp

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sU -p-  -sV -vvv --min-rate 2000 192.168.137.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 13:20 -03
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 13:20
Scanning 192.168.137.17 [1 port]
Completed ARP Ping Scan at 13:20, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:20
Completed Parallel DNS resolution of 1 host. at 13:20, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating UDP Scan at 13:20
Scanning 192.168.137.17 [65535 ports]
Increasing send delay for 192.168.137.17 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.137.17 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.137.17 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.137.17 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.137.17 from 400 to 800 due to max_successful_tryno increase to 8
Increasing send delay for 192.168.137.17 from 800 to 1000 due to max_successful_tryno increase to 9
Warning: 192.168.137.17 giving up on port because retransmission cap hit (10).
UDP Scan Timing: About 8.58% done; ETC: 13:26 (0:05:30 remaining)
UDP Scan Timing: About 16.94% done; ETC: 13:26 (0:04:59 remaining)
UDP Scan Timing: About 25.32% done; ETC: 13:26 (0:04:28 remaining)
UDP Scan Timing: About 33.64% done; ETC: 13:26 (0:03:59 remaining)
UDP Scan Timing: About 41.99% done; ETC: 13:26 (0:03:29 remaining)
Discovered open port 161/udp on 192.168.137.17
UDP Scan Timing: About 50.34% done; ETC: 13:26 (0:02:59 remaining)
```

usando la tool onesixtyone vemos que la community string es security

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# onesixtyone -c /usr/share/seclists/Discovery/SNMP/snmp-onesixtyone.txt 192.168.137.17
Scanning 1 hosts, 3218 communities
192.168.137.17 [security] Linux chain 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64
```

tool snmpwalk

```
┌──(miguel💀miguel)-[~]
└─$ sudo su
[sudo] password for miguel:
┌──(root💀miguel)-[/home/miguel]
└─# snmpwalk -v2c -c security 192.168.137.17
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Linux chain 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (857474) 2:22:54.74
iso.3.6.1.2.1.1.4.0 = STRING: "Blue <blue@chaincorp.nyx>"
iso.3.6.1.2.1.1.5.0 = STRING: "Chain"
iso.3.6.1.2.1.1.6.0 = STRING: "VulNyx.com"
iso.3.6.1.2.1.1.8.0 = Timeticks: (29) 0:00:00.29
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
```

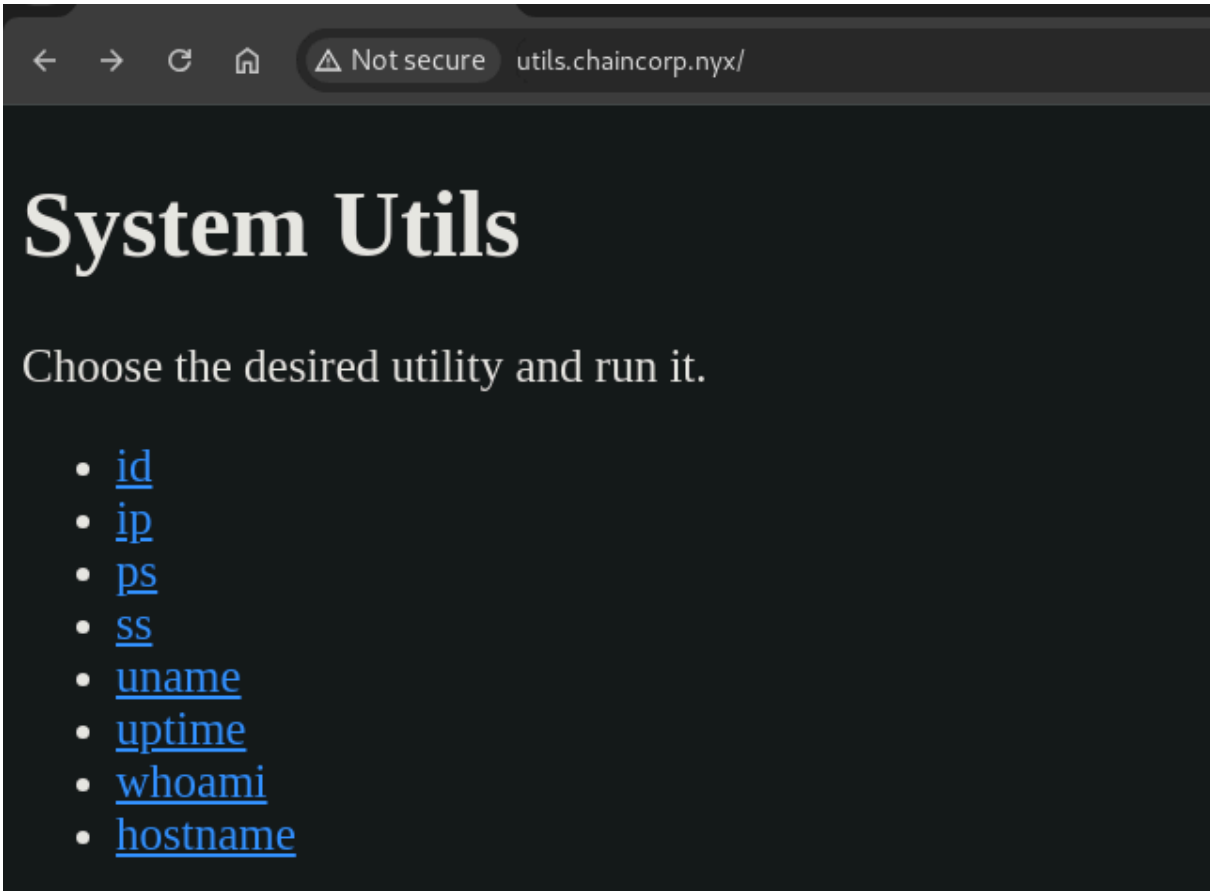
lo metemos en el /etc/hosts

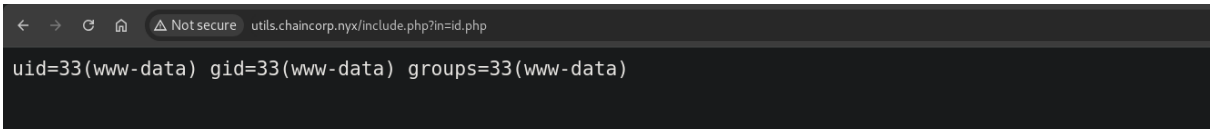
por dominio tenemos lo mismo de antes

```
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://chaincorp.nyx/" -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://chaincorp.nyx/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 318] [--> http://chaincorp.nyx/wordpress/]
/javascript           (Status: 301) [Size: 319] [--> http://chaincorp.nyx/javascript/]
/server-status        (Status: 403) [Size: 278]
Progress: 102039 / 220560 (46.26%)
```

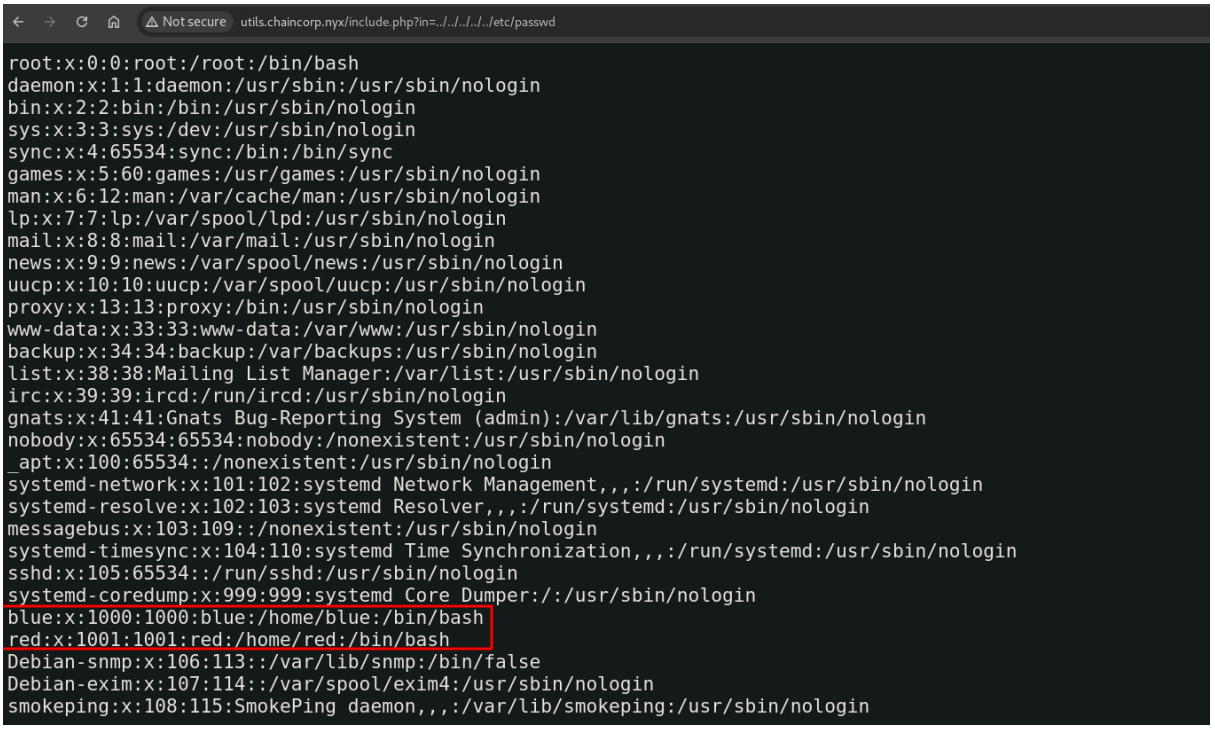
finalemnte algo nuevo buscando por subdominios XD vamos a meterlo al /etc/hosts

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# gobuster vhost  -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -u "http://chaincorp.nyx/" -t 200 --append-
domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://chaincorp.nyx/
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: utils.chaincorp.nyx Status: 200 [Size: 628]
```

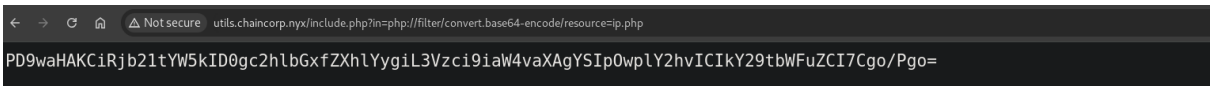




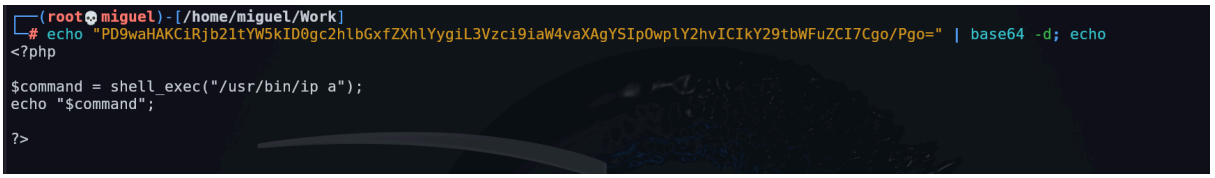
tenemos un LFI y vemos los usuarios por el /etc/passwd



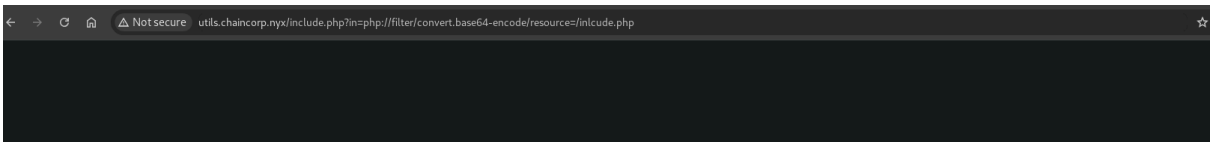
mediante el uso de filter chain vemos por el contenido de cada archivo/link



vemos que es el contenido de cada archivo en base64

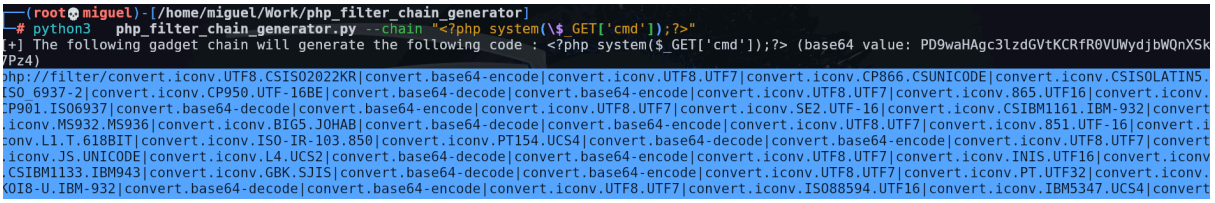


el include no me da nada en el sitio



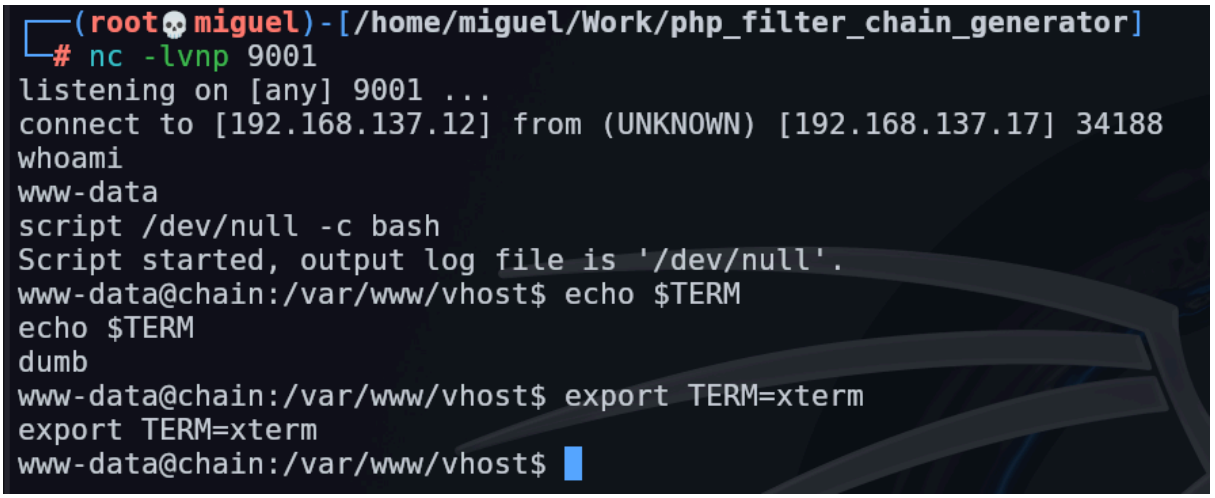
vamos a ver por curl y nada. nos descargamos la tool https://github.com/synacktiv/php_filter_chain_generator para ejecutar comando y quiza suvir un archivo malicioso

nos creamos el filter para tener RCE

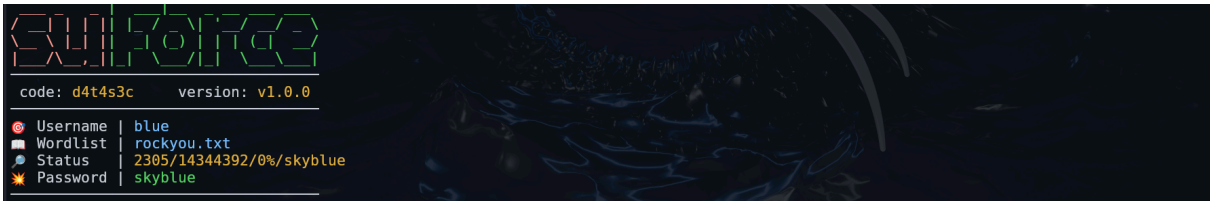


aca le hago un ls a home y veo

entonces nos ponemos en escucha con nc y nos tiramos un reverse shell urlencodeada

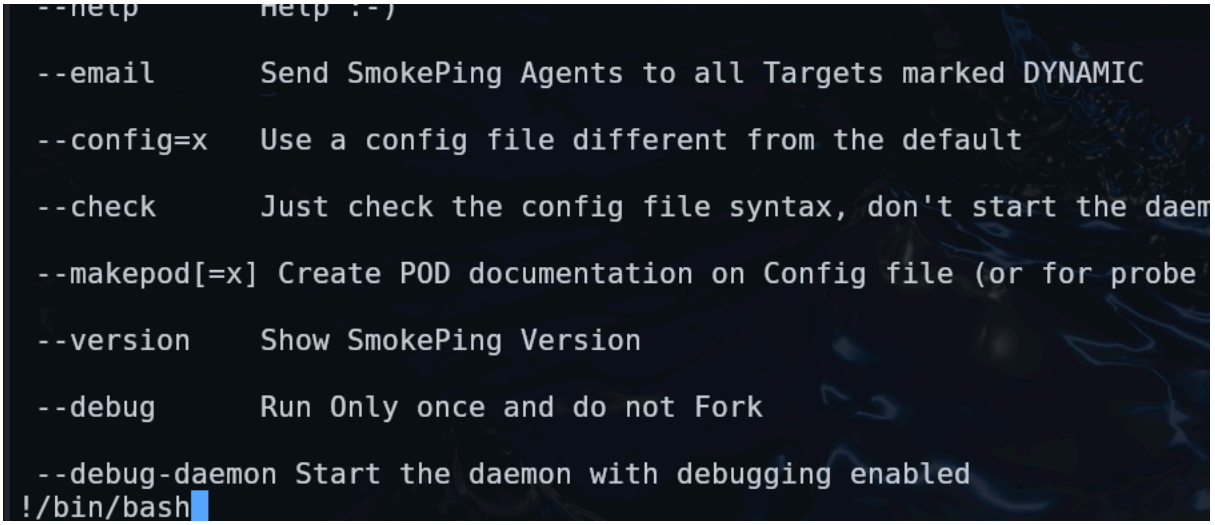


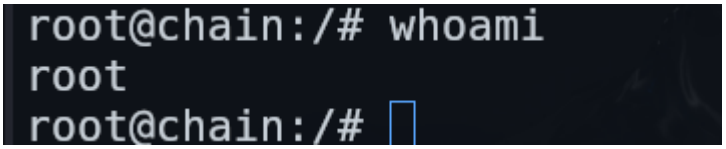
no encuentro nada entonces como la maquina la hizo d4t4s3ec me descargo su tool suForce para hacer fuerza bruta por usuario



de blue a red

de red a root


--help Help :-)
--email Send SmokePing Agents to all Targets marked DYNAMIC
--config=x Use a config file different from the default
--check Just check the config file syntax, don't start the daem
--makepod[=x] Create POD documentation on Config file (or for probe
--version Show SmokePing Version
--debug Run Only once and do not Fork
--debug-daemon Start the daemon with debugging enabled
!/bin/bash


root@chain:/# whoami
root
root@chain:/#