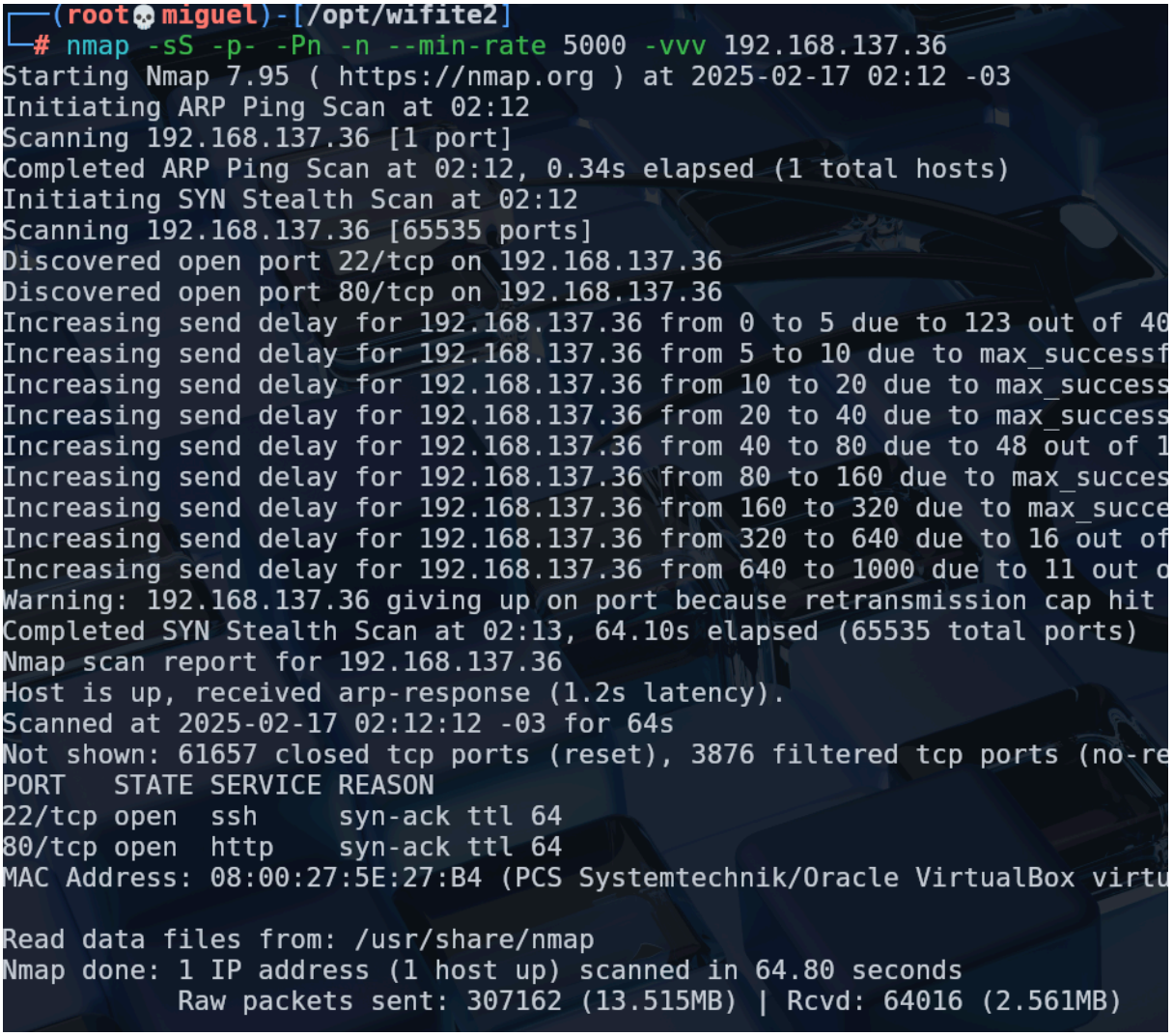
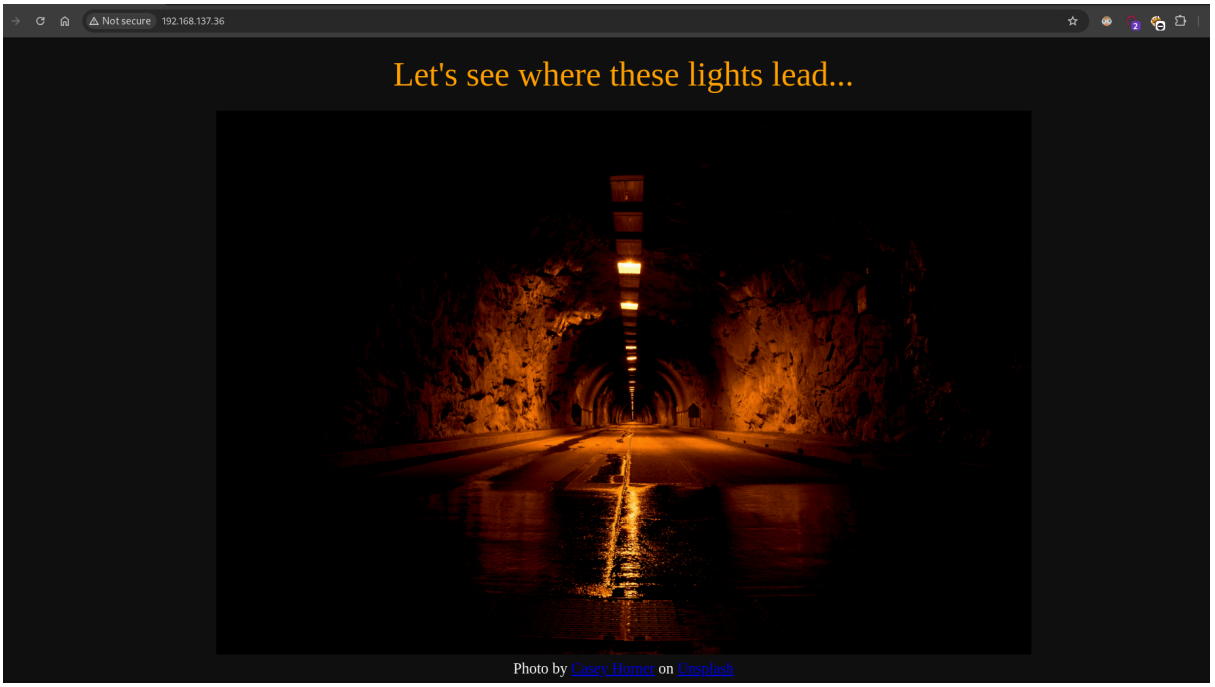
Deeper


┌──(root💀miguel)-[/opt/wifite2]
└─# nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.36
Starting Nmap 7.95 (https://nmap.org) at 2025-02-17 02:12 -03
Initiating ARP Ping Scan at 02:12
Scanning 192.168.137.36 [1 port]
Completed ARP Ping Scan at 02:12, 0.34s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 02:12
Scanning 192.168.137.36 [65535 ports]
Discovered open port 22/tcp on 192.168.137.36
Discovered open port 80/tcp on 192.168.137.36
Increasing send delay for 192.168.137.36 from 0 to 5 due to 123 out of 40
Increasing send delay for 192.168.137.36 from 5 to 10 due to max_successf
Increasing send delay for 192.168.137.36 from 10 to 20 due to max_success
Increasing send delay for 192.168.137.36 from 20 to 40 due to max_success
Increasing send delay for 192.168.137.36 from 40 to 80 due to 48 out of 1
Increasing send delay for 192.168.137.36 from 80 to 160 due to max_succes
Increasing send delay for 192.168.137.36 from 160 to 320 due to max_succe
Increasing send delay for 192.168.137.36 from 320 to 640 due to 16 out of
Increasing send delay for 192.168.137.36 from 640 to 1000 due to 11 out o
Warning: 192.168.137.36 giving up on port because retransmission cap hit
Completed SYN Stealth Scan at 02:13, 64.10s elapsed (65535 total ports)
Nmap scan report for 192.168.137.36
Host is up, received arp-response (1.2s latency).
Scanned at 2025-02-17 02:12:12 -03 for 64s
Not shown: 61657 closed tcp ports (reset), 3876 filtered tcp ports (no-re
PORT   STATE SERVICE REASON
22/tcp open ssh   syn-ack ttl 64
80/tcp open http   syn-ack ttl 64
MAC Address: 08:00:27:5E:27:B4 (PCS Systemtechnik/Oracle VirtualBox virtu
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 64.80 seconds
Raw packets sent: 307162 (13.515MB) | Rcvd: 64016 (2.561MB)

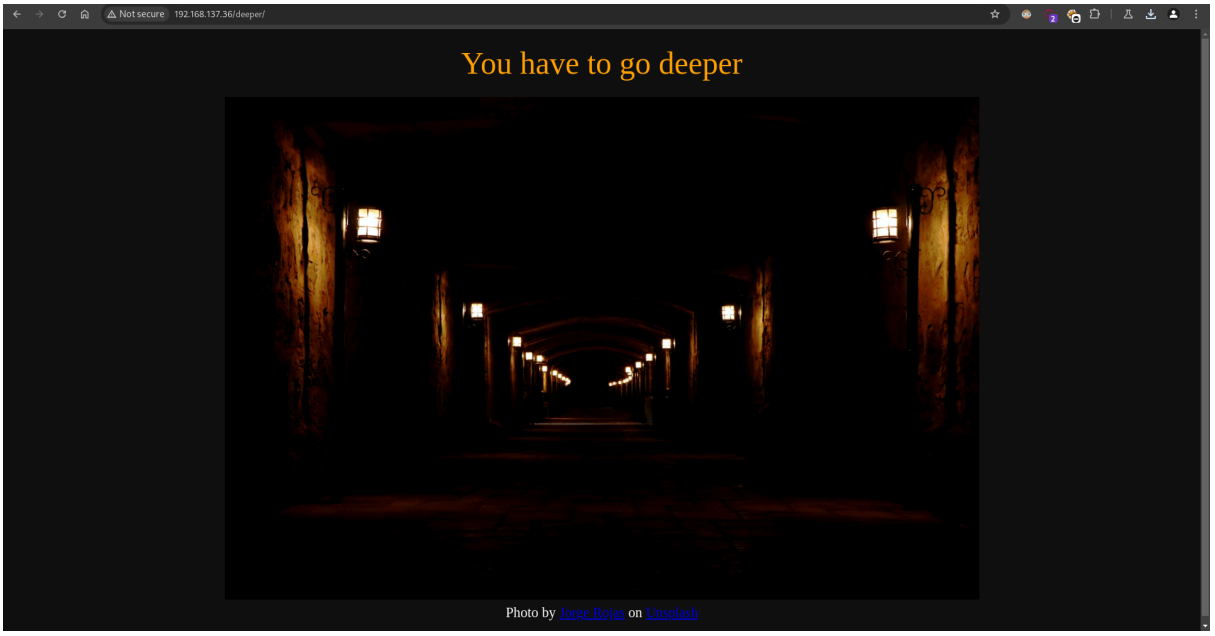

┌──(root💀miguel)-[/opt/wifite2]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.36
Starting Nmap 7.95 (https://nmap.org) at 2025-02-17 02:14 -03

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 37:d1:6f:b5:a4:96:e8:78:18:c7:77:d0:3e:20:4e:55 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP0G2tWy4w/Qxs8qOXl67kW08
b3qa5OxGXxqfEjU=
|   256 cf:5d:90:f3:37:3f:a4:e2:ba:d5:d7:25:c6:4a:a0:61 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMznQqkhSVgCjaHlx4JkgMQc2Ecl+JjVdL7tTAgj9Fyy
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Deeper
|_http-server-header: Apache/2.4.57 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 08:00:27:5E:27:B4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan
```

```
┌──(root💀miguel)-[/opt/wifite2]
└─# whatweb 192.168.137.36
http://192.168.137.36 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.137.36]
 Title[Deeper][Title element contains newline(s)!]
```



```
Line wrap
<!DOCTYPE html>
<html>
    <head>
        <title>
            Deeper
        </title>
    </head>
    <body bgcolor="#101010"><center>

        <p>
            <font size="6" color="ffa200">
            Let's see where these lights lead...
            <!-- GO "deeper" -->
        </font>
        </p>
        <p>
            <img src="/img/index.jpg" width="960" height="640"/>
            <br />
            <font size="2" color="FFFFFF">
            Photo by <a href="https://unsplash.com/@mischievous_penguins?utm_source=un
            </font>
        </p>

    </center></body>
</html>
```



Not secure view-source:192.168.137.36/deeper/

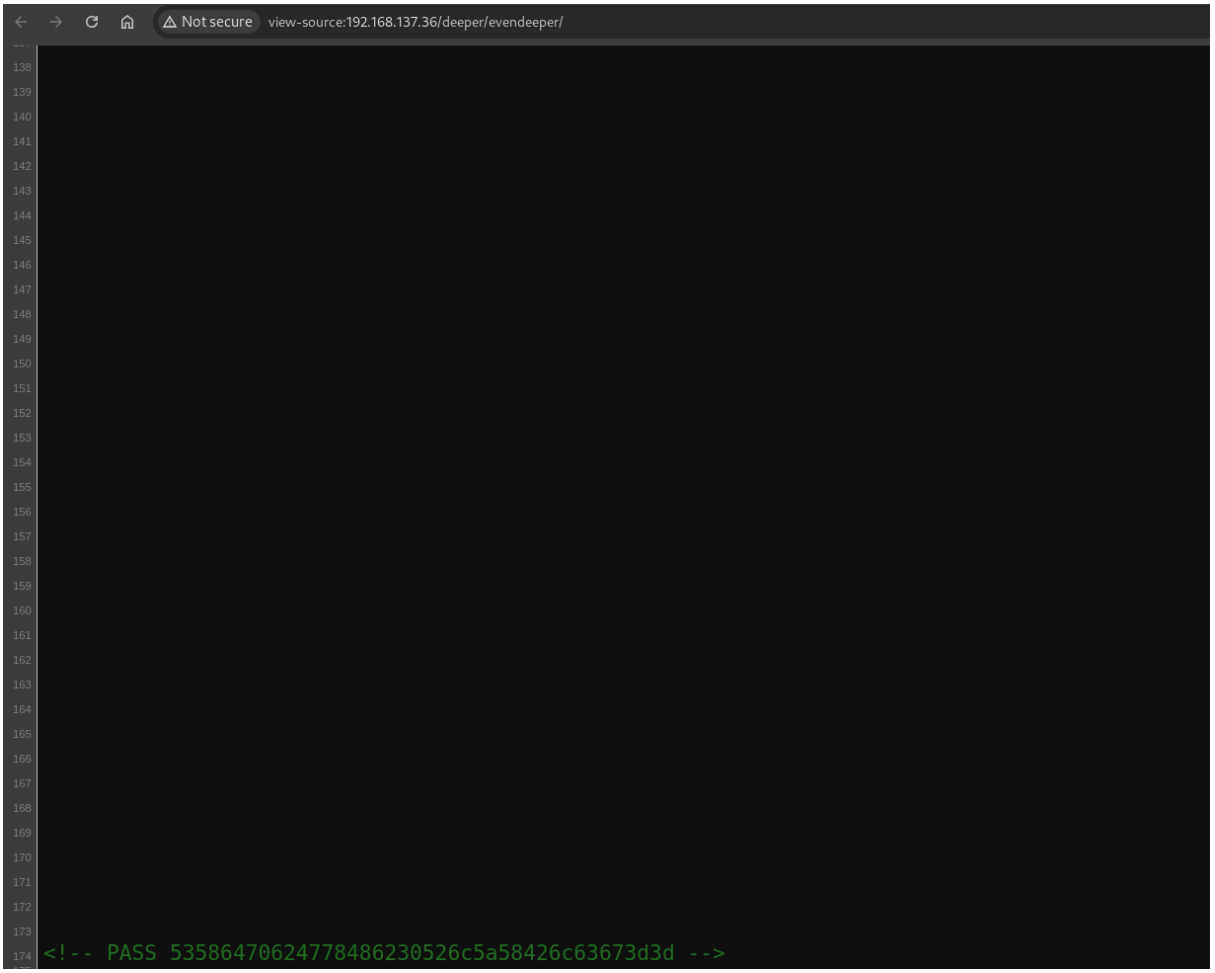
ine wrap

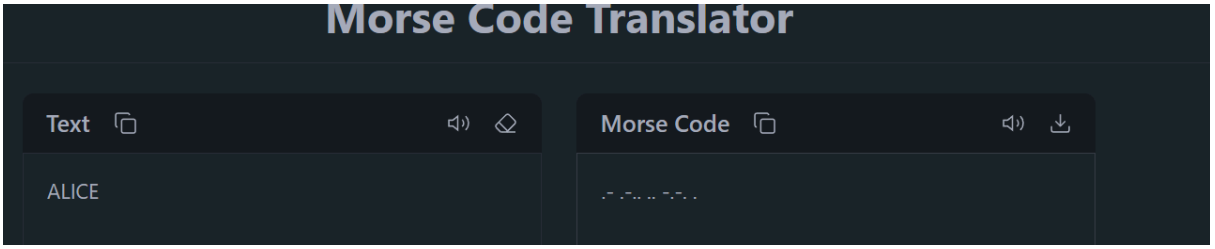
```
<!DOCTYPE html>
<html>
    <head>
        <title>
            Deeper
        </title>
    </head>
    <body bgcolor="101010"><center>

        <p>
            <font size="6" color="FFA200">
            You have to go deeper
        </font>
        </p>
        <p>
            <img src="/img/index2.jpg" width="960" height="640"/>
            <br />
            <font size="2" color="FFFFFF">
            Photo by <a href="https://unsplash.com/@jorgerojas?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyTex
            </font>
        </p>
        <!-- GO evendeeper -->
    </center></body>
</html>
```

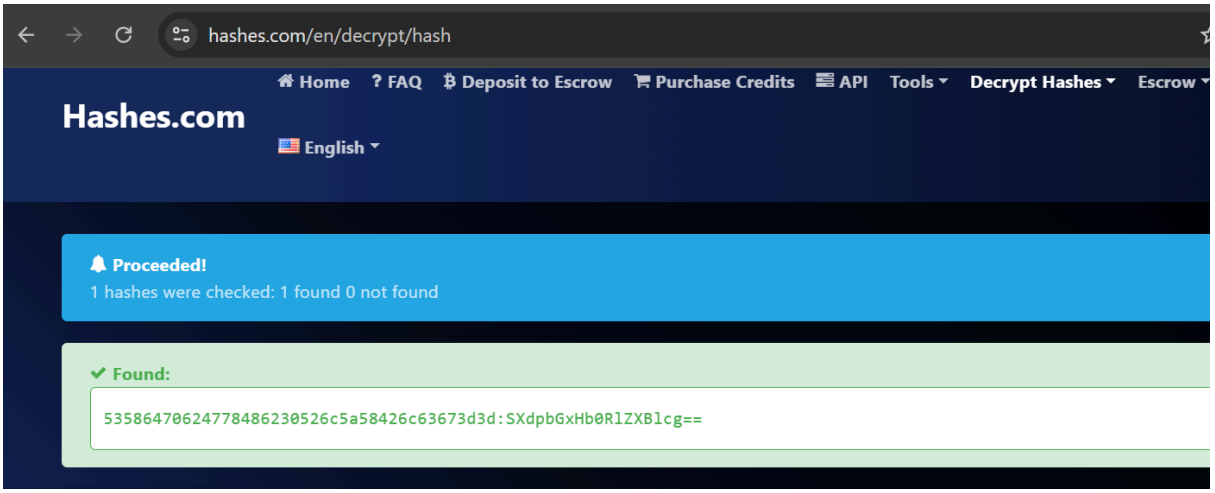
Not secure 192.168.137.36/deeper/evendeeper/

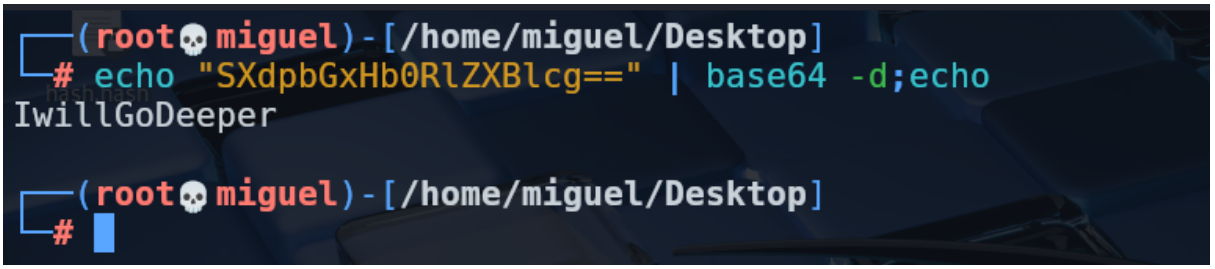
Now start digging

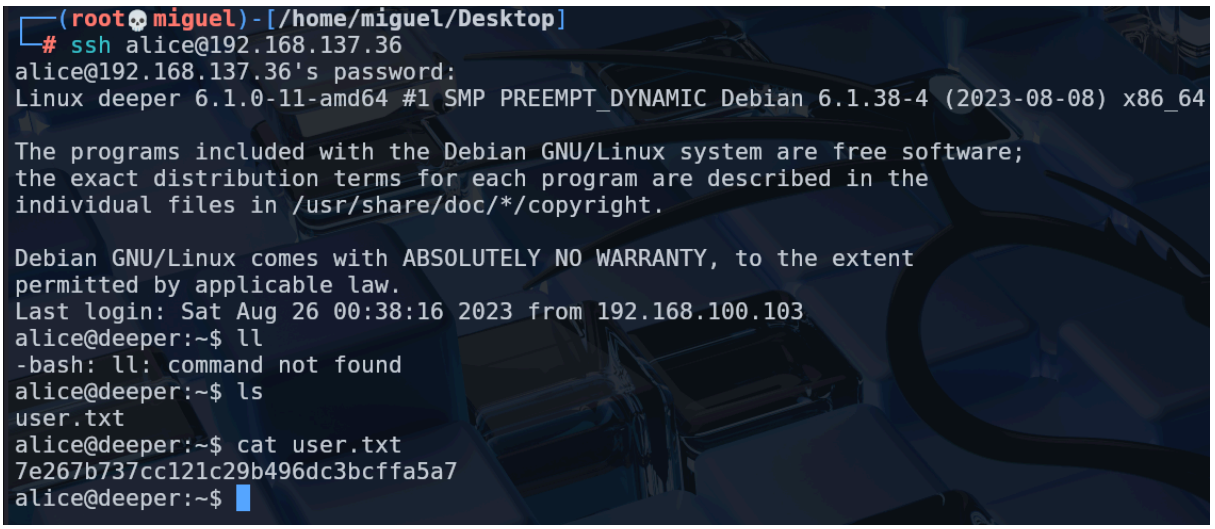
Photo by Luca Mallets on Unsplash

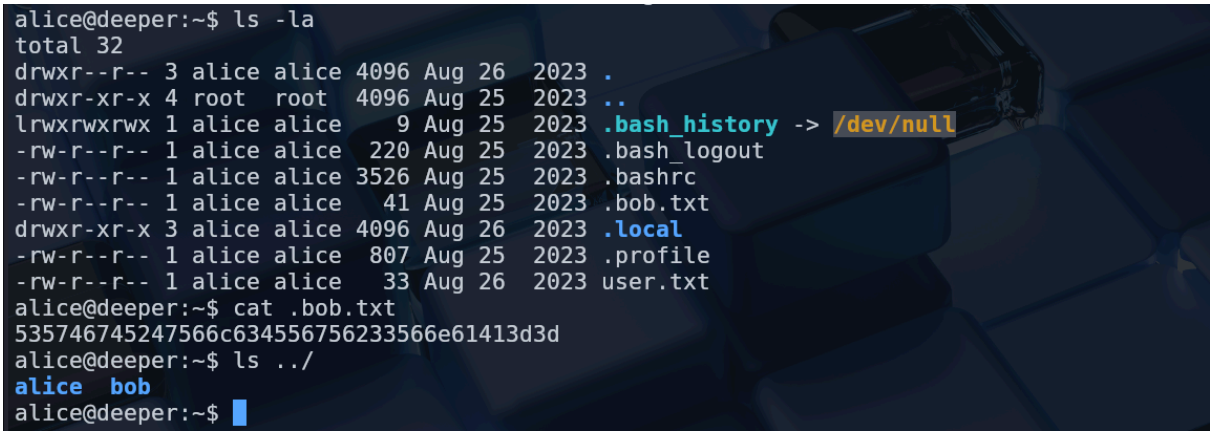

Not secure
view-source:192.168.137.36/deeper/evendeeper/
<!-- PASS 53586470624778486230526c5a58426c63673d3d -->
Not secure
view-source:192.168.137.36/deeper/evendeeper/
PAGE TOP RIGTH
<!-- USER .- .-.. .. -.-. . -->
Deeper
5

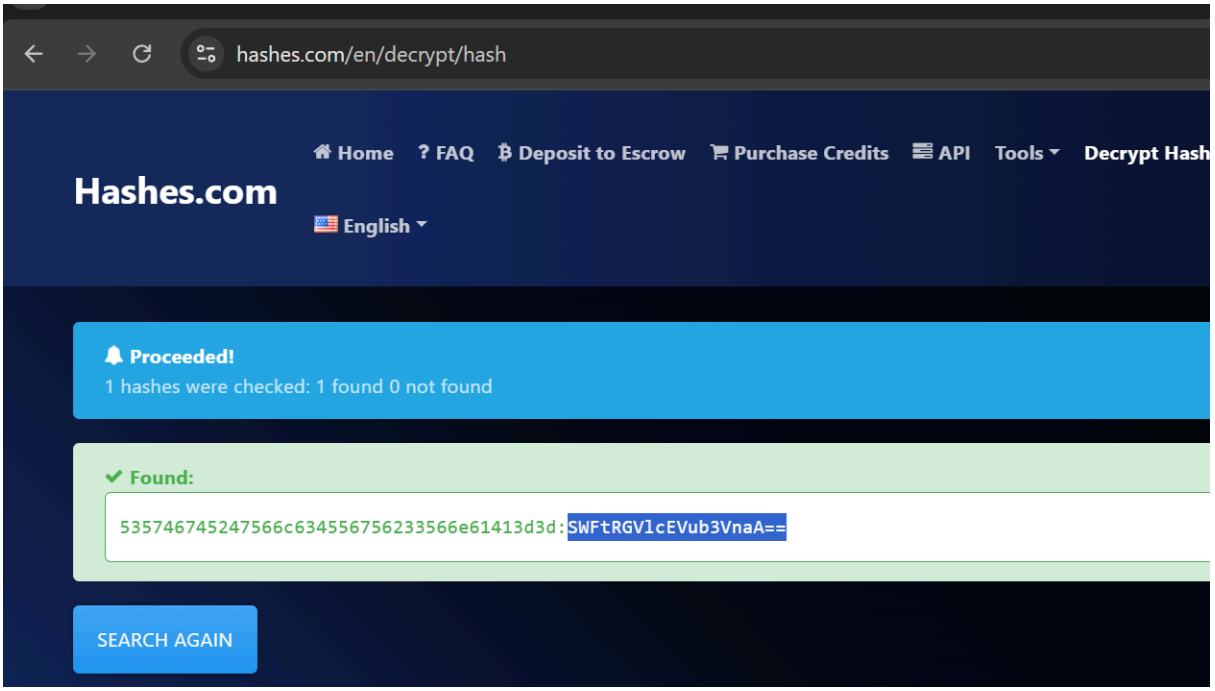

Morse Code Translator
Text
ALICE
Morse Code
.- .-.. .. -.-. .

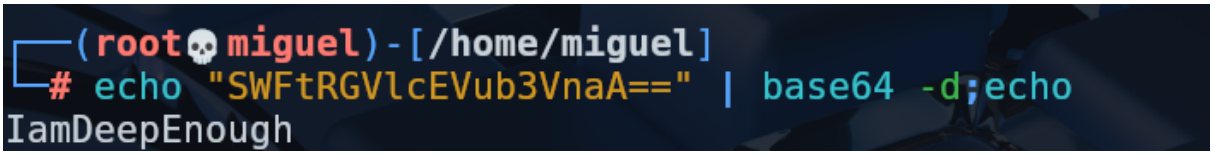

hashes.com/en/decrypt/hash
Home
FAQ
Deposit to Escrow
Purchase Credits
API
Tools
Decrypt Hashes
Escrow
Hashes.com
English
Proceeded!
1 hashes were checked: 1 found 0 not found
Found:
535864706247784862305 26c5a58426c63673d3d:SXdpbGxHb0RlZXBlcg==


(root miguel)-[/home/miguel/Desktop]
echo "SXdpbGxHb0RlZXBlcg==" | base64 -d;echo
IwillGoDeeper
(root miguel)-[/home/miguel/Desktop]
#


(root miguel)-[/home/miguel/Desktop]
ssh alice@192.168.137.36
alice@192.168.137.36's password:
Linux deeper 6.1.0-11-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-4 (2023-08-08) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Aug 26 00:38:16 2023 from 192.168.100.103
alice@deeper:~$ ll
-bash: ll: command not found
alice@deeper:~$ ls
user.txt
alice@deeper:~$ cat user.txt
7e267b737cc121c29b496dc3bcffa5a7
alice@deeper:~$


alice@deeper:~$ ls -la
total 32
drwxr--r-- 3 alice alice 4096 Aug 26 2023 .
drwxr-xr-x 4 root root 4096 Aug 25 2023 ..
lrwxrwxrwx 1 alice alice 9 Aug 25 2023 .bash_history -> /dev/null
-rw-r--r-- 1 alice alice 220 Aug 25 2023 .bash_logout
-rw-r--r-- 1 alice alice 3526 Aug 25 2023 .bashrc
-rw-r--r-- 1 alice alice 41 Aug 25 2023 .bob.txt
drwxr-xr-x 3 alice alice 4096 Aug 26 2023 .local
-rw-r--r-- 1 alice alice 807 Aug 25 2023 .profile
-rw-r--r-- 1 alice alice 33 Aug 26 2023 user.txt
alice@deeper:~$ cat .bob.txt
535746745247566c634556756233566e61413d3d
alice@deeper:~$ ls ../
alice bob
alice@deeper:~$

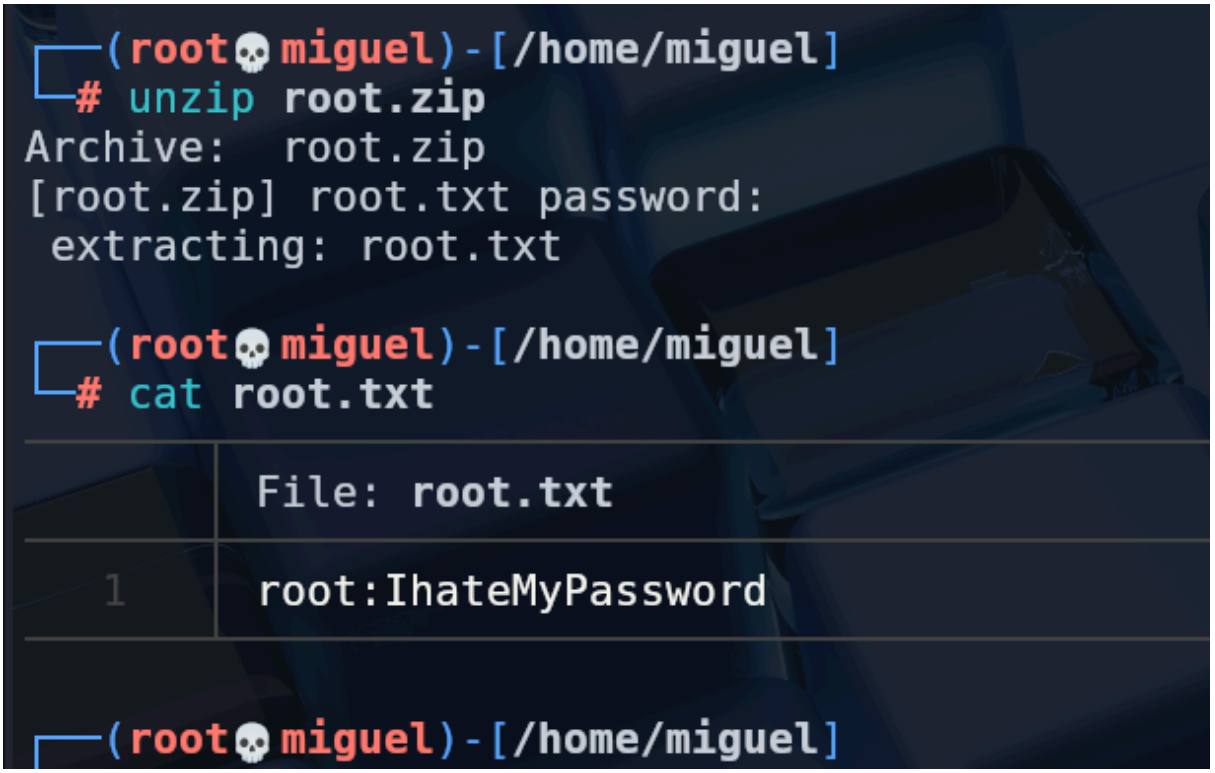

hashes.com/en/decrypt/hash
Hashes.com
Home
FAQ
Deposit to Escrow
Purchase Credits
API
Tools
Decrypt Hash
English
Proceeded!
1 hashes were checked: 1 found 0 not found
Found:
535746745247566c634556756233566e61413d3d:SWFtRGVlcEVub3VnaA==
SEARCH AGAIN

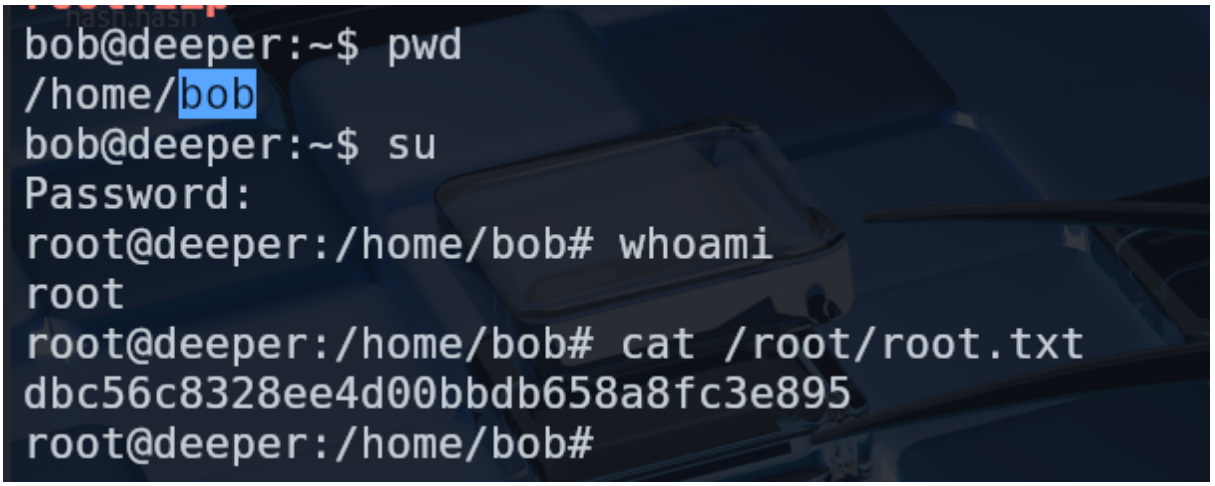

(root miguel)-[/home/miguel]
echo "SWFtRGVlcEVub3VnaA==" | base64 -d;echo
IamDeepEnough

```
┌──(root💀miguel)-[/home/miguel]
└─# ssh bob@192.168.137.36
bob@192.168.137.36's password:
Linux deeper 6.1.0-11-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-4 (2023-
08-08) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Aug 26 00:05:57 2023 from 192.168.100.103
bob@deeper:~$
```

```
┌──(root💀miguel)-[/home/miguel]
└─# scp bob@192.168.137.36:/home/bob/root.zip .
bob@192.168.137.36's password:
root.zip                                      100%  215     8.3KB/s   00:00

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

```
┌──(root💀miguel)-[/home/miguel]
└─# unzip root.zip
Archive:  root.zip
[root.zip] root.txt password:

┌──(root💀miguel)-[/home/miguel]
└─# zip2john root.zip> hashzip
ver 1.0 efh 5455 efh 7875 root.zip/root.txt PKZIP Encr: 2b chk, TS_chk,

┌──(root💀miguel)-[/home/miguel]
└─# john hashzip --wordlist=/usr/share/wordlists/seclists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bob              (root.zip/root.txt)
1g 0:00:00:00 DONE (2025-02-17 03:23) 16.66g/s 546133p/s 546133c/s 5461
Use the "--show" option to display all of the cracked passwords reliabl
Session completed.

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


(root💀miguel)-[/home/miguel]
unzip root.zip
Archive: root.zip
[root.zip] root.txt password:
 extracting: root.txt
(root💀miguel)-[/home/miguel]
cat root.txt
File: root.txt
1 root:IhateMyPassword
(root💀miguel)-[/home/miguel]


bob@deeper:~$ pwd
/home/bob
bob@deeper:~$ su
Password:
root@deeper:/home/bob# whoami
root
root@deeper:/home/bob# cat /root/root.txt
dbc56c8328ee4d00bbdb658a8fc3e895
root@deeper:/home/bob#